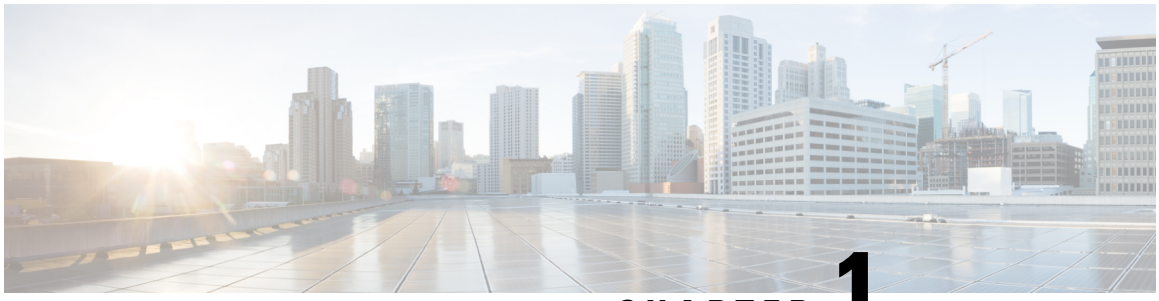
Release Change Reference, StarOS Release 21.22

First Published: 2020-12-17

Last Modified: 2021-08-31

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



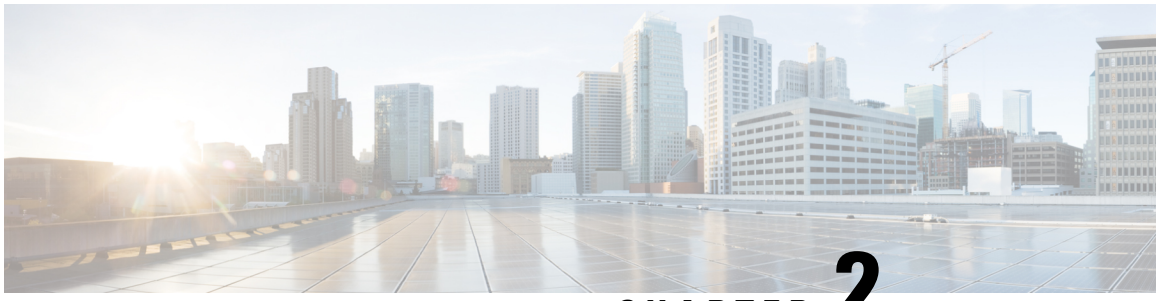
CHAPTER 1

Release 21.22 Features and Changes Quick Reference

Release 21.22 Features and Changes

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
5G Non Standalone, on page 13	P-GW	21.22
Cisco Ultra Traffic Optimization, on page 23	P-GW	21.22
Dynamic Transport Selection based on Transaction or Origin-Host, on page 69	P-GW	21.22
Enabling EMM and ESM Cause Code Mapping, on page 83	MME	21.22
Extraction of IPv4 Addresses Embedded in IPv6 Addresses, on page 87	ECS	21.22.8
Non-IP PDN Support, on page 91	C-SGN	21.22
P-GW Buffering Optimization, on page 111	P-GW	21.22.3
RedHat Software Version Update, on page 115	All	21.22.4
Rf Interface Support, on page 117	P-GW	21.22
Source Port Randomization on VPP for GTP-U Traffic, on page 157	P-GW	21.22
S6b Interface Enhancement, on page 159	P-GW	21.22
Support for Common access-type in twan-profile for EoGRE-PMIP Calls, on page 161	SaMOG	21.22.11

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
UE Overload Protection, on page 175	P-GW	21.22
User Location Information in P-GW CDR, on page 189	P-GW	21.22
Update Bearer Request Enhancements to Close Charging Gap, on page 185	P-GW	21.22



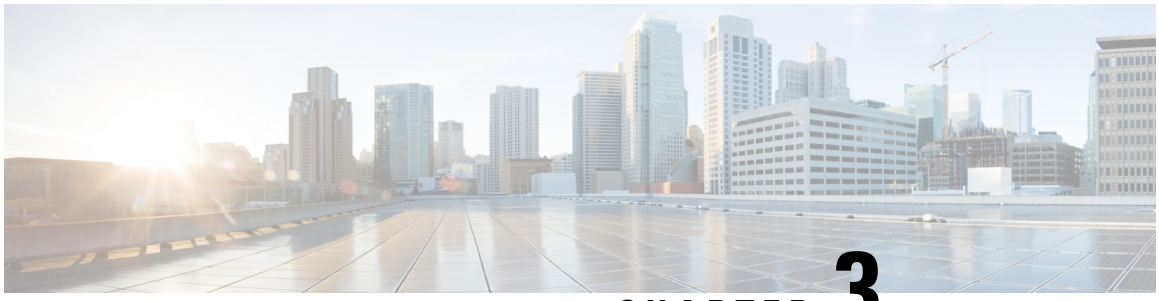
CHAPTER 2

Feature Defaults Quick Reference

Feature Defaults

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

Feature	Default
5G Non Standalone	Disabled - Configuration Required
Cisco Ultra Traffice Optimization	Disabled - License Required
Dynamic Transport Selection based on Transaction or Origin-Host	Disabled - Configuration Required
Enabling EMM and ESM Cause Code Mapping	Enabled - Always-on
Extraction of IPv4 Addresses Embedded in IPv6 Addresses	Disabled - License Required
Non-IP PDN Support	Disabled - License Required
P-GW Buffering Optimization	Enabled - Configuration Required
RedHat Software Version Update	Enabled - Always-on
Rf Interface Support	
Source Port Randomization on VPP for GTP-U Traffic	Disabled - License Required
S6b Interface Enhancement	Disabled - License Required
UE Overload Protection	Disabled - Configuration Required
User Location Information in P-GW CDR	Enabled - Always-on
Update Bearer Request Enhancements to Close Charging Gap	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 21.22 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 21.22 include:

- New Bulk Statistics, on page 5
- Modified Bulk Statistics, on page 9
- Deprecated Bulk Statistics, on page 9

New Bulk Statistics

This section identifies new bulk statistics and new bulk statistic schemas introduced in release 21.22.

ECS Schema

The following bulk statistics are added in the ECS schema to support Large and Managed flows:

Bulk Statistics	Description
tcp-active-base-large-flow-count	Indicates the number of TCP active-base-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-base-managed-large-flow-count	Indicates the number of TCP active-base-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-base-unmanaged-large-flow-count	Indicates the number of TCP active-base-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-ext-large-flow-count	Indicates the number of TCP active-ext-large-flow count for Cisco Ultra Traffic Optimization.

Bulk Statistics	Description
tcp-active-ext-managed-large-flow-count	Indicates the number of TCP active-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-ext-unmanaged-large-flow-count	Indicates the number of TCP active-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-base-large-flow-count	Indicates the number of TCP total-base-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-base-managed-large-flow-count	Indicates the number of TCP total-base-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-base-unmanaged-large-flow-count	Indicates the number of TCP total-base-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-ext-large-flow-count	Indicates the number of TCP active-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-ext-managed-large-flow-count	Indicates the number of TCP total-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-ext-unmanaged-large-flow-count	Indicates the number of TCP total-ext-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-base-large-flow-count	Indicates the number of UDP active-base-large-flow-count count for Cisco Ultra Traffic Optimization.
udp-active-base-managed-large-flow-count	Indicates the number of UDP active-base-managed-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-base-unmanaged-large-flow-count	Indicates the number of UDP active-base-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-ext-large-flow-count	Indicates the number of UDP active-ext-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-ext-managed-large-flow-count	Indicates the number of UDP active-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-ext-unmanaged-large-flow-count	Indicates the number of UDP active-ext-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-base-large-flow-count	Indicates the number of UDP total-base-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-base-managed-large-flow-count	Indicates the number of UDP total-base-managed-large-flow count for Cisco Ultra Traffic Optimization.

Bulk Statistics	Description
udp-total-base-unmanaged-large-flow-count	Indicates the number of UDP total-base-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-ext-large-flow-count	Indicates the number of UDP total-ext-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-ext-managed-large-flow-count	Indicates the number of UDP total-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-ext-unmanaged-large-flow-count	Indicates the number of UDP total-ext-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.

APN Schema

The following bulk statistics are introduced in support of the new feature:

Bulk Statistics	Description
invalid-dst-port-pkt-drop	This statistics indicates the total number of downlink packets dropped due to invalid destination port for a Non-IP APN PDN
pdn-non-ip-actsess	This statistics indicates the total number of active Non-IP sessions at APN.
pdn-non-ip-setupsess	This statistics indicates the total number of Non-IP session setup at APN.
pdn-non-ip-relsess	This statistics indicates the total number of Non-IP session release at APN.
invalid-tun-proto-pkt-drop	This statistics indicates the total number of downlink packets dropped due to invalid SGi tunnel protocol for a Non-IP APN PDN.
invalid-as-src-pkt-drop	This statistics indicates the total number of downlink packets dropped due to invalid application server source address for a Non-IP APN PDN.

P-GW Schema

The following bulk statistics are introduced in support of the new feature:

Bulk Statistics	Description
sessstat-pdn-non-ip-active	This statistic indicates the total number of active Non-IP PDNs at P-GW.

Bulk Statistics	Description
sessstat-pdn-non-ip-setup	This statistic indicates the total number of Non-IP PDNs setup at P-GW.
sessstat-pdn-non-ip-rel	This statistic indicates the total number of Non-IP PDNs released at P-GW.
sessstat-non-ip-ipv4addaloc	This statistic indicates the total number of times IPv4 address is allocated for Non-IP P-GW PDNs.
sessstat-non-ip-ipv6addaloc	This statistic indicates the total number of times IPv6 address is allocated for Non-IP P-GW PDNs.
sessstat-non-ip-addaloc-ipv4loacalpool	This statistic indicates the total number of times IPv4 address is allocated from local pool for Non-IP P-GW PDNs.
sessstat-non-ip-addaloc-ipv6loacalpool	This statistic indicates the total number of times IPv6 address is allocated from local pool for Non-IP P-GW PDNs.
udptunstat-ipv4sessact	This statistic indicates the total number of active UDP-IPv4 SGi tunnel.
udptunstat-ipv4sesssetup	This statistic indicates the total number of UDP-IPv4 SGi tunnel setup at P-GW.
udptunstat-ipv4sessrel	This statistic indicates the total number of UDP-IPv4 SGi tunnel setup at P-GW.
udptunstat-ipv6sessact	This statistic indicates the total number of active UDP-IPv6 SGi tunnel.
udptunstat-ipv6sesssetup	This statistic indicates the total number of UDP-IPv6 SGi tunnel setup at P-GW.
udptunstat-ipv6sessrel	This statistic indicates the total number of UDP-IPv6 SGi tunnel released at P-GW.
non-ip-pdn-to-user-pkt	This statistics indicates the total number of downlink packets sent on Non-IP P-GW PDNs.
non-ip-pdn-to-user-byte	This statistics indicates the total number of downlink bytes sent on Non-IP P-GW PDNs.
non-ip-pdn-from-user-pkt	This statistics indicates the total number of uplink packets received for Non-IP S-GW PDNs.
non-ip-pdn-from-user-byte	This statistic indicates the total number of uplink bytes with Non-IP S-GW PDNs.
sessstat-invalid-port-dnlkpktdrop	This statistics indicates the total number of downlink packets dropped due to invalid destination port for a Non-IP P-GW PDN.

Bulk Statistics	Description
sessstat-invalid-port-dnlkbytedrop	This statistics indicates the total number of downlink bytes dropped due to invalid destination port for a Non-IP P-GW PDN.
sessstat-invalid-tun-proto-dnlkpktdrop	This statistics indicates the total number of downlink packets dropped due to invalid SGi tunnel protocol for a Non-IP P-GW PDN.
sessstat-invalid-tun-proto-dnlkbytedrop	This statistics indicates the total number of downlink bytes dropped due to invalid SGi tunnel protocol for a Non-IP P-GW PDN.
sessstat-invalid-as-src-dnlkpktdrop	This statistics indicates the total number of downlink packets dropped due to invalid application server source address for a Non-IP P-GW PDN.
sessstat-invalid-as-src-dnlkbytedrop	This statistics indicates the total number of downlink bytes dropped due to invalid application server source address for a Non-IP P-GW PDN.

IMSA Schema

The following bulk statistics are included in the IMSA Schema to track high and low priority categories for WPS and Non-WPS users:

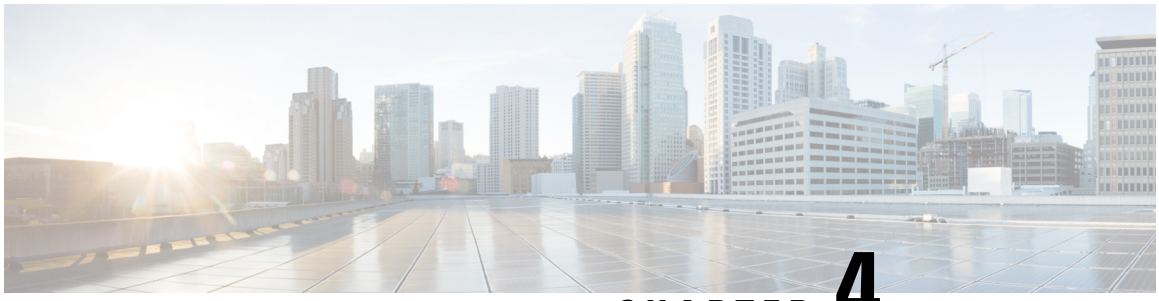
Bulk Statistics	Description
dpca-imsa-total-session-priority-channel	Shows the cumulative number of Wireless Priority subscribers.
dpca - imsa - total - sessions-switched -from - priority - channel	Shows the cumulative number of subscribers moved from Wireless Priority to Normal.
dpca - imsa- total- sessions-switched - to- priority- channel	Shows the cumulative number of subscribers moved from Normal to Wireless Priority.

Modified Bulk Statistics

None in this release.

Deprecated Bulk Statistics

None for this release.



CHAPTER 4

SNMP MIB Changes in StarOS 21.22

This chapter identifies SNMP MIB objects, alarms and conformance statements added to, modified for, or deprecated from the StarOS 21.22 software release.

SNMP MIB Alarm Changes for 21.22

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

SNMP MIB Conformance Changes for 21.22

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

SNMP MIB Object Changes for 21.22

This section provides information on SNMP MIB alarm changes in release 21.22.

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

New SNMP MIB Object

This section identifies new SNMP MIB alarms available in release 21.22.

- starDiameterEndPointContextName
- starDiameterEndPointId
- starDiameterPeerCauseType
- starDiameterEndPointPriorityPeersUnAvailable

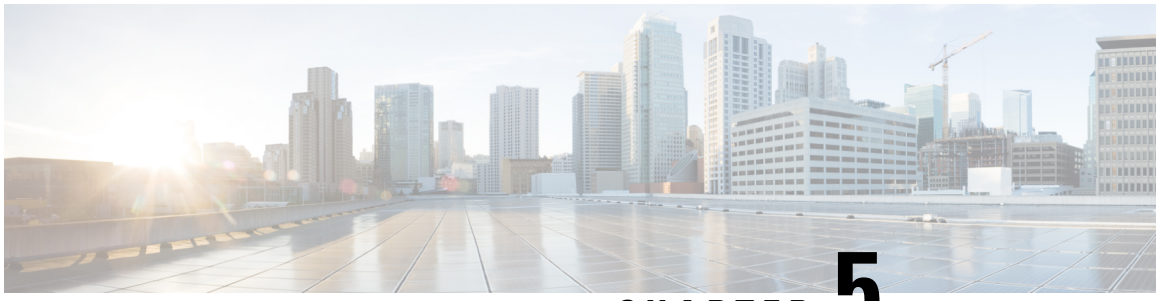
- starDiameterEndPointPriorityPeersAvailable
- starDiameterEndPointNonPriorityPeersUnAvailable
- starDiameterEndPointNonPriorityPeersAvailable

Modified SNMP MIB Object

- starRCMChassisState
- starRCMChassisReload

Deprecated SNMP MIB Object

None in this release.



CHAPTER 5

5G Non Standalone

This chapter describes the 5G Non Standalone (NSA) feature in the following sections:

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • S-GW • SAEGW
Applicable Platform(s)	• ASR 5000 • ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *5G Non Standalone Solution Guide* • *AAA Interface Administration and Reference* • *Command Line Interface Reference* • *P-GW Administration Guide* • *S-GW Administration Guide* • *SAEGW Administration Guide* • *Statistics and Counters Reference*

Revision History

With this release, support is added for Secondary RAT Usage IE during GnGp handover.	21.22
The 5G NSA solution for SAEGW supports dcca-custom1, dcca-custom7 and dcca-custom8 dictionaries additionally.	21.11
The 5G NSA solution for SAEGW supports the following functionality in this release: • P-GW Custom Dictionaries support over Gz for extended bitrate • S-GW Custom Dictionaries support over Gz for extended bitrate • P-GW Custom Dictionaries support over Gy and Rf for extended bitrate • S-GW support of Secondary RAT Data Usage Report in Gz CDRs	21.10
The 5G NSA solution for SAEGW supports the following functionality in this release: • P-GW support of Secondary RAT Data Usage Report in Gz CDRs • P-GW support of Secondary RAT Data Usage Report in Rf CDRs • S-GW and P-GW support of statistics for DCNR PDNs	21.9
The 5G NSA solution is qualified on the ASR 5000 platform.	21.5
The 5G NSA solution for SAEGW supports the following functionality in this release: • Feature License • Dedicated Bearers • Gy interface • URLLC QCI	21.8
First introduced.	21.6

Feature Description

Cisco 5G Non Standalone (NSA) solution leverages the existing LTE radio access and core network (EPC) as an anchor for mobility management and coverage. This solution enables operators using the Cisco EPC Packet Core to launch 5G services in shorter time and leverage existing infrastructure. Thus, NSA provides a seamless option to deploy 5G services with very less disruption in the network.

Overview

5G is the next generation of 3GPP technology, after 4G/LTE, defined for wireless mobile data communication. The 5G standards are introduced in 3GPP Release 15 to cater to the needs of 5G networks.

The two solutions defined by 3GPP for 5G networks are:

- 5G Non Standalone (NSA): The existing LTE radio access and core network (EPC) is leveraged to anchor the 5G NR using the Dual Connectivity feature. This solution enables operators to provide 5G services with shorter time and lesser cost.

  Note The 5G NSA solution is supported in this release.

- 5G Standalone (SA): An all new 5G Packet Core will be introduced with several new capabilities built inherently into it. The SA architecture comprises of 5G New Radio (5G NR) and 5G Core Network (5GC).

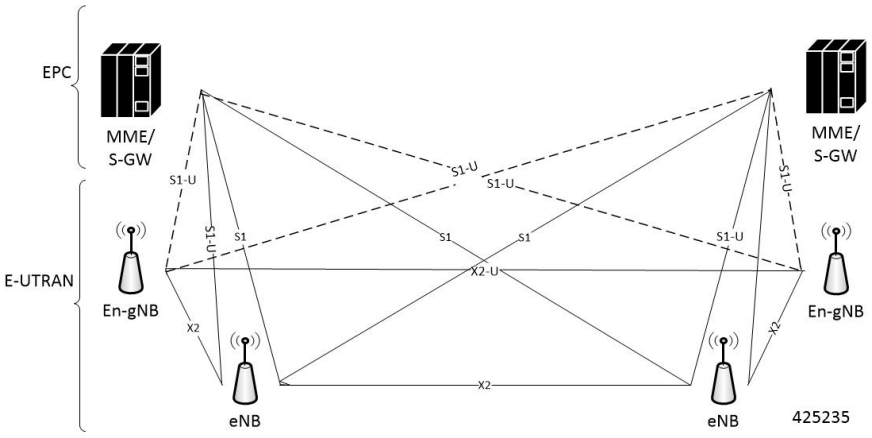
  Network Slicing, CUPS, Visualization, Multi-Gbps support, Ultra low latency, and other such aspects will be natively built into the 5G SA Packet Core architecture.

Dual Connectivity

The E-UTRA-NR Dual Connectivity (EN-DC) feature supports 5G New Radio (NR) with EPC. A UE connected to an eNodeB acts as a Master Node (MN) and an en-gNB acts as a Secondary Node (SN). The eNodeB is connected to the EPC through the S1 interface and to the en-gNB through the X2 interface. The en-gNB can be connected to the EPC through the S1-U interface and other en-gNBs through the X2-U interface.

The following figure illustrates the E-UTRA-NR Dual Connectivity architecture.

Figure 1: EN-DC Architecture



If the UE supports dual connectivity with NR, then the UE must set the DCNR bit to "dual connectivity with NR supported" in the UE network capability IE of the Attach Request/Tracking Area Update Request message.

If the UE indicates support for dual connectivity with NR in the Attach Request/Tracking Area Update Request message, and the MME decides to restrict the use of dual connectivity with NR for the UE, then the MME

sets the RestrictDCNR bit to "Use of dual connectivity with NR is restricted" in the EPS network feature support IE of the Attach Accept/Tracking Area Update Accept message.

If the RestrictDCNR bit is set to "Use of dual connectivity with NR is restricted" in the EPS network feature support IE of the Attach Accept/Tracking Area Update Accept message, the UE provides the indication that dual connectivity with NR is restricted to the upper layers.

If the UE supports DCNR and DCNR is configured on MME, and if HSS sends ULA/IDR with "Access-Restriction" carrying "NR as Secondary RAT Not Allowed", MME sends the "NR Restriction" bit set in "Handover Restriction List" IE during Attach/TAU/Handover procedures. Similarly, MME sets the RestrictDCNR bit to "Use of dual connectivity with NR is restricted" in the EPS network feature support IE of the Attach Accept/Tracking Area Update Accept message. Accordingly, UE provides the indication that dual connectivity with NR is restricted to the upper layers.

The "Handover Restriction List" IE is present in the "Initial Context Setup Request" message for Attach and TAU procedure with data forwarding procedure, in the "Handover Required" message for S1 handover procedure, in the "Downlink NAS Transport" message for TAU without active flag procedure.

Important 5G NSA feature is license controlled from release 21.8 onwards. Contact your Cisco account representative for detailed information on specific licensing requirements.

The 5G NSA solution for SAEGW supports the following functionalists:

- **High Throughput**

  5G NR offers downlink data throughput up to 20 Gbps and uplink data throughput up to 10 Gbps. Some interfaces in EPC have the support to handle (encode/decode) 5G throughput. For example, NAS supports up to 65.2 Gbps (APN-AMBR) and S5/S8/S10/S3 (GTP-v2 interfaces) support up to 4.2 Tbps. The diameter interfaces S6a and Gx support only up to 4.2Gbps throughput, S1-AP supports only up to 10 Gbps and NAS supports up to 10 Gbps (MBR, GBR). New AVP/IE have been introduced in S6a, Gx , S1-AP, and NAS interfaces to support 5G throughput. See the *How It Works* section for more information.

- **DCNR Support on P-GW:**

  Supports configuration of DCNR feature at the P-GW-service, by configuring “Extended-BW-NR” feature in IMSA service. Advertises the DCNR feature support by sending “Extended-BW-NR” feature bit in “Feature-List-ID-2” towards PCRF. Forwards AVP "Extended-APN-AMBR-UL" and "Extended-APN-AMBR-DL" in CCR messages when it receives APN-AMBR values greater than 4.2Gbps from MME/S-GW. Decodes the extended AVP "Extended-APN-AMBR-UL" and "Extended-APN-AMBR-DL" when it is received from PCRF.

- Sends AVP "Extended-Max-Requested-BW-UL", "Extended-Max-Requested-BW-DL", "Extended-GBR-UL" and "Extended-GBR-DL" when it receives MBR and GBR values greater than 4.2Gbps from MME/S-GW. Decodes the AVP "Extended-Max-Requested-BW-UL", "Extended-Max-Requested-BW-DL", "Extended-GBR-UL" and "Extended-GBR-DL" when received from PCRF. Supports dedicated bearer establishment with extended QoS. Sends AVP Extended-Max-Requested-BW-UL and "Extended-Max-Requested-BW-DL" in Gy records.

- **Ultra Low Latency Support**:

  Supports 5G requirements of Ultra-Reliable and Low Latency Communications (URLLC). 3GPP introduced URLCC QCI 80 (Non-GBR resource type), QCI 82 and 83 (GBR resource type). P-GW establishes default bearers with URLLC QCI 80, which is typically used by low latency eMBB applications. P-GW establishes dedicated bearers with URLLC QCI 82 and 83 (also with QCI 80 if

dedicated bearers of Non-GBR type to be established), which is typically used by discrete automation services (industrial automation).

- **ICSR Support**

  With release 21.10 onwards ICSR for 5G NSA on SAEGW is supported.

- **Dynamic S-GW and P-GW selection by MME for DCNR capable UE**

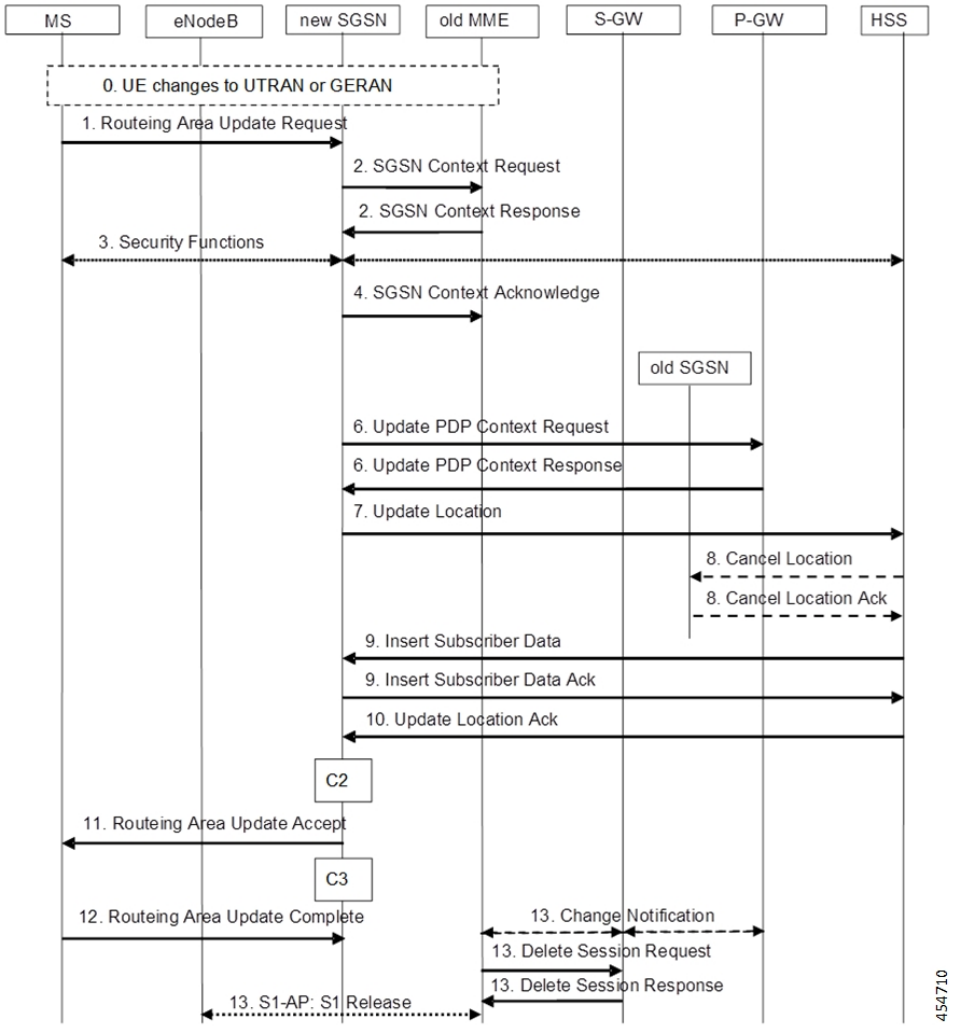
  When DCNR capable UE attempts to register in MME and when all DCNR validations are successful (for example DCNR feature configuration on MME, HSS not sending access-restriction for NR, and son on), the MME sets “UP Function Selection Indication Flags” IE with DCNR flag set to 1 in “Create Session Request” message. This feature is relevant for CUPS architecture to help SGW-C and PGW-C to select SGW-U and PGW-U which supports dual connectivity with NR. When S-GW receives this IE over S11, it sends this IE over S5 to P-GW. S-GW ignores IE if it receives it in Non-CUPS deployment.

- **P-GW Secondary RAT Usage Data Report Handling:**

  P-GW supports custom24 and custom44 for Gz and aaa-custom3, aaa-custom4 and aaa-custom6 dictionaries for Rf to support Secondary RAT Data Usage Report in CDRs.

Support for Secondary RAT Usage During GnGp Handover

This feature supports the Secondary RAT usage reported in change notification request during 4G to 3G handover. The support is for handling the change notification with Secondary RAT Usage during the GnGp handover. Step 13 is added in the following diagram in support of this feature. The usage must be reported in next CDR generation.



IMSI Not Known

If there's no context found for IMSI specified in Secondary RAT Usage IE of change notification request Message, it returns the change notification response with cause value "IMSI/IMEI not known".

Limitations

Following are the known limitations for this feature:

- This feature only supports the handling of the secondary RAT usage IE.
- During the 4G to 3G handover, dedicated bearers are retained and Secondary RAT usage is reported for both Default and Dedicated bearers.

Enabling Secondary RAT Data Usage Report

Use the following configuration to enable Secondary RAT Data Usage Report:

```
configure
   context context_name
      pgw-service service_name
         dcnr
         end
```

Note The GGSN service associated with the P-GW service must have the DCNR enabled using the preceding CLI.

- **Statictics support for DCNR PDNs:**

  S-GW and P-GW statistics support for DCNR PDNs

- **S-GW Secondary RAT Usage Data Report Handling:**

  S-GW supports custom24 and custom6 dictionaries to support Secondary RAT Data Usage Report in CDRs over Gz.

- **P-GW Custom Dictionaries Support over Gz:**

  P-GW supports Custom44 and Custom24 dictionaries to support sending the following AVPs when it receives MBR, GBR and APN-AMBR values greater than 4.2Gbps:

  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL
  - Extended-GBR-UL
  - Extended-GBR-DL
  - Extended-APN-AMBR-UL
  - Extended-APN-AMBR-DL

- **Multiple Presence Reporting Area Support:**

  S-GW supports Multiple-PRA action and Multiple-PRA Information over S11/S4 and S5/S8 interfaces. P-GW supports Multiple-PRA Action and Multiple-PRA Information over S5/S8 and Gx interfaces.

- **S-GW Custom Dictionaries Support over Gz :**

  S-GW supports custom24 and custom6 dictionaries to support sending the following AVPs when it receives MBR, GBR and APN-AMBR values greater than 4.2Gbps:

  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL
  - Extended-GBR-UL
  - Extended-GBR-DL
  - Extended-APN-AMBR-UL
  - Extended-APN-AMBR-DL

- **P-GW Custom Dictionaries Support over Gx:**

P-GW supports dpca-custom15, dpca-custom11, dpca-custom23, dpca-custom19 and dpca-custom17, dictionarie to support sending the following AVPs when it receives GBR and APN-AMBR values greater than 4.2Gbps:

- Extended-Max-Requested-BW-UL
- Extended-Max-Requested-BW-DL
- Extended-GBR-DL
- Extended-GBR-UL
- Extended-APN-AMBR-UL
- Extended-APN-AMBR-DL

- **P-GW Custom Dictionaries Support over Gy:**

  P-GW supports dcca-custom1, dcca-custom7, dcca-custom8 and dcca-custom13 dictionaries to support sending the following AVPs when it receives GBR and APN-AMBR values greater than 4.2Gbps:

  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL
  - Extended-GBR-DL
  - Extended-GBR-UL
  - Extended-APN-AMBR-UL
  - Extended-APN-AMBR-DL

- **P-GW Custom Dictionaries Support over Rf:**

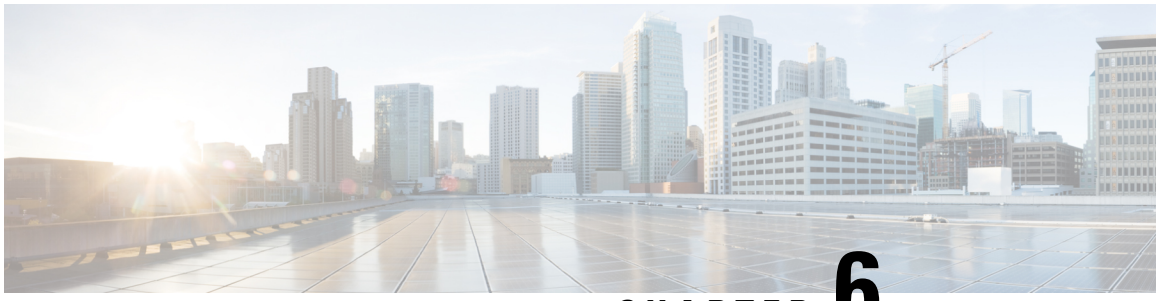
  P-GW supports aaa-custom3, aaa-custom4 and aaa-custom6 dictionaries to support sending the following AVPs when it receives GBR and APN-AMBR values greater than 4.2Gbps:

  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL
  - Extended-GBR-UL
  - Extended-GBR-DL
  - Extended-APN-AMBR-UL
  - Extended-APN-AMBR-DL

Multiple Presence Reporting Area

P-GW supports negotiation of Multiple-Presence Reporting Area feature in Feature-List-ID 2 over Gx interface with PCRF. The CNO-ULI feature will be used only when the P-GW and/or the PCRF does not support Multiple-PRA and both P-GW and PCRF support CNO-ULI.

Note This feature is introduced in release 21.9.1. For more information, refer to the *Presence Reporting Area* chapter in the *P-GW Administration Guide*.



CHAPTER 6

Cisco Ultra Traffic Optimization

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

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

Revision History

Important Revision history details are not provided for features introduced before release 21.2 and N5.1.

Revision Details	Release
In this release, Cisco Ultra Traffic Optimization P-GW supports high throughput (4G or 5G) optimization of the traffic.	21.22

Revision Details	Release
In this release, P-GW supports MBR/GBR handling in optimization library.	21.21
In this release the following three new parameters are added in Large TODR: **1.** International Mobile Subscriber Identity (IMSI) **2.** Flow-ID and Flow-ID list **3.** User Location Information (ULI) For more information, refer the *Large TODR Enhancement* section.	21.19.1
The Cisco Ultra Traffic Optimization library version has been upgraded from 3.0.9 to 3.0.11.	21.14.2
With this release, new keywords **large-flows-only** and **managed-large-flows-only** are implemented as part of the **data-record** command to enable the CUTO library to stream respective statistics to the external server. New bulk statistics are added in support of this enhancement	21.14
With this release, Cisco Ultra Traffic Optimization solution is enhanced to support basic Quick UDP Internet Connections (QUIC) UDP traffic along with the existing support for TCP traffic.	21.3.17
Reboot of chassis is no longer required to enable Cisco Ultra Traffic Optimization related configuration.	21.3.x
Multi-Policy support for Cisco Ultra Traffic Optimization solution.	21.6
Cisco Ultra Traffic Optimization solution is supported in Ultra Gateway Platform (UGP).	21.6
Cisco Ultra Traffic Optimization solution is enhanced to support basic Quick UDP Internet Connections (QUIC) UDP traffic along with the existing support for TCP traffic.	21.5
Reboot of chassis is no longer required to enable Cisco Ultra Traffic Optimization related configuration.	21.5
First introduced.	21.2

Overview

In a high-bandwidth bulk data flow scenario, user experience is impacted due to various wireless network conditions and policies like shaping, throttling, and other bottlenecks that induce congestion, especially in the RAN. This results in TCP applying its saw-tooth algorithm for congestion control and impacts user experience, and overall system capacity is not fully utilized.

The Cisco Ultra Traffic Optimization solution provides clientless optimization of TCP and HTTP traffic. This solution is integrated with Cisco P-GW and has the following benefits:

- Increases the capacity of existing cell sites and therefore, enables more traffic transmission.
- Improves Quality of Experience (QoE) of users by providing more bits per second.
- Provides instantaneous stabilizing and maximizing per subscriber throughput, particularly during network congestion.

How Cisco Ultra Traffic Optimization Works

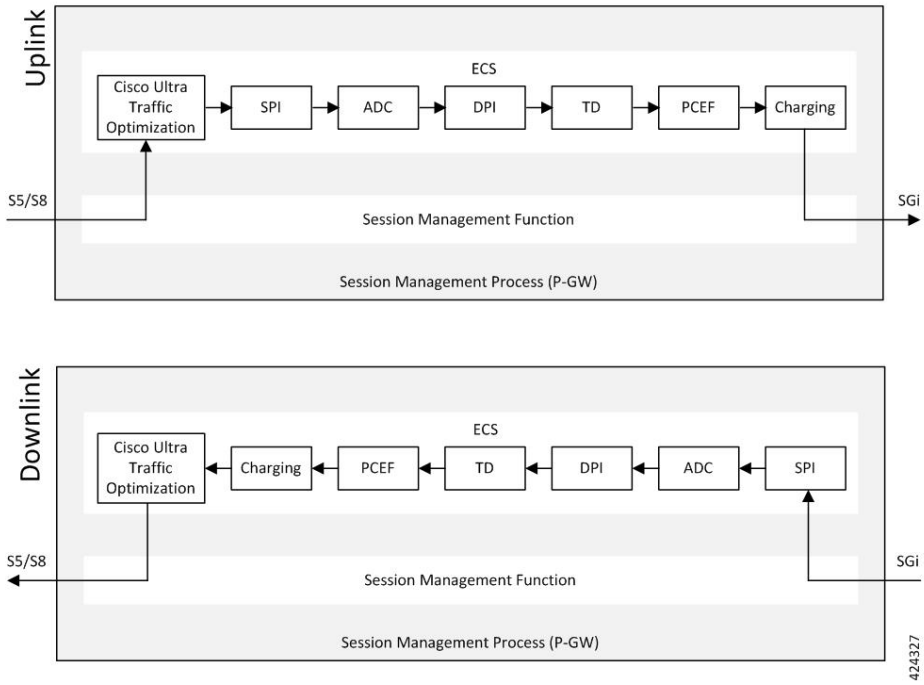
The Cisco Ultra Traffic Optimization achieves its gains by shaping video traffic during times of high network load/congestion. It monitors and profiles each individual video flow that passes through the gateway and uses its machine learning algorithms to determine whether that flow is traversing a congested channel. Cisco Ultra Traffic Optimization then flow-controls video to varying levels and time, depending on the degree of detected congestion, and efficiently aligns delivery of the video traffic to less-congested moments while still providing adequate bandwidth to videos to maintain their quality. The result is less network latency and higher user throughputs while maintaining HD video. Cisco Ultra Traffic Optimization does not drop packets or modify data payloads in any way.

The Cisco Ultra Traffic Optimization integrates with standard Cisco P-GW functions such as Application Detection and Control (ADC), allowing mobile operators to define optimization policies that are based on the traffic application type as well as APN, QCI, and other common traffic delineations. Cisco Ultra Traffic Optimization is fully radio network aware, allowing management on a per eNodeB cell basis.

Architecture

StarOS has a highly optimized packet processing framework, the Cisco Ultra Traffic Optimization engine, where the user packets (downlink) are processed in the operating systems user space. The high-speed packet processing, including the various functions of the P-GW, is performed in the user space. The Cisco Ultra Traffic Optimization engine is integrated into the packet processing path of Cisco's P-GW with a well-defined Application Programming Interface (API) of StarOS.

The following graphic shows a high-level overview of P-GW packet flow with traffic optimization.



Licensing

The Cisco Ultra Traffic Optimization is a licensed Cisco solution. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Limitations and Restrictions

- The values which the P-GW chooses to send to the Cisco Ultra Traffic Optimization engine are the values associated from the bearer GBR and bearer MBR.
- In the current implementation, only downlink GBR and MBR are sent to the engine for traffic optimization.
- UDP/QUIC based Traffic Optimization is supported only on PORT 443.
- The traffic-optimization data-records are generated in the same folder as that of EDRs. Also, the file rotation criteria will be similar to that of EDRs.
- A povision to dynamically load the library without statically linking it is restricted.
- OP works on ‘per flow’ level GBR/MBR to optimize the flows However, P-GW supports only sending bearer level GBR/MBR.
- The sending GBR and MBR values to Optimation library functionality is applicable only for P-GW product.

Handling of Traffic Optimization Data Record

The Traffic Optimization Data Record (TODR) is generated only on the expiry of idle-timeout of the Cisco Ultra Traffic Optimization engine. No statistics related to session or flow from P-GW is included in this TODR. The data records are a separate file for the Traffic Optimization statistics, and available to external analytics platform.

Large TODR Enhancement

In 21.19.1 and later releases, the following three new parameters are added in large TODR:

1. International Mobile Subscriber Identity (IMSI)
2. Flow-ID and Flow-ID list
3. User Location Information (ULI)

   The Flow-ID is used to correlate the ACS Flow ID that is visible in End Point Detection and Response ("sn-flow-id" attribute) and then the ULI is correlated with RAN counters.

Note These new fields are only available in Large TODRs generated on non-VPP based P-GW and SAEGW.

Enhancing Large TODR

Use the following configuration to enable enhanced large TODR.

```
configure
  active-charging service service_name
    traffic-optimization-profile
      data-record
        enhanced-large-todr [ imsi | acs-flow-id | uli ]
        end
```

Example 1: When all fields are to be displayed:

```
enhanced-large-todr
```

Example 2: When IMSI and ULI are to be displayed:

```
enhanced-large-todr imsi
enhanced-large-todr uli
```

Show Commands and Outputs

```
show active-charging traffic-optimization info
```

Output Example 1:

```
[local]laas-setup# show active-charging traffic-optimization info
        Version   : 3.1.1
        Mode      : Active
        Configuration:
                Data Records(TODR): ENABLED     TODR Type: ALL_FLOWS
                Statistics Options: DISABLED
                EFD Flow Cleanup Interval: 1000(milliseconds)
                Statistics Interval: 60(seconds)
```

```
                Enhanced Large TODR: DISABLED
[local]laas-setup#
```

Output Example 2 for IMSI and ULI:

```
[local]laas-setup# show active-charging traffic-optimization info
        Version   : 3.1.1
        Mode      : Active
        Configuration:
                Data Records(TODR): ENABLED     TODR Type: ALL_FLOWS
                Statistics Options: DISABLED
                EFD Flow Cleanup Interval: 1000(milliseconds)
                Statistics Interval: 60(seconds)
                Enhanced Large TODR: ENABLED, Fields: imsi uli
[local]laas-setup#
```

The output of this command includes the following fields:

- Enhanced Large TODR

Enhancement to the Existing Large TODRs

1. **Large TODRs with IMSI**

   IMSI: Indicates the International Mobile Subscriber Identity.

   IMSI value is 0 if it is a trusted build.

2. **ACS Flow ID**

   ACS Flow ID is a newly introduced field. As there could be a lot of flow, it is limited to a maximum of 20 flows as a part of TODR.

   acs_flow_id_count: Number of ACS Flow Ids present in this TODR. A Maximum of 20 ACS Flow IDs is present.

   acs_flow_id_list: List of individual ACS Flow Ids. For examples, acs_flow_id1, acs_flow_id2 and so on.

   a. **EDR ACS Flow ID**

      In EDR, each ACS flow ID is printed by enabling the attribute ‘sn-flow-id’ in EDR config as given below :

      ```
      config
      active-charging service ACS
          edr-format EDR_SN
          delimiter comma
            attribute sn-flow-id priority 10
            rule-variable bearer 3gpp imsi priority 15
            rule-variable bearer qci priority 20
      ```

      It is printed out in EDR in the following format **92:30278:14786055** where:

      - 92 is the Session Manager instance
      - 30278 is the Session Handle orsession number
      - 14786055 is the ACS flow identifier

   b. **TODR ACS Flow ID**

      TODR ACS flow idshould follow the same format as in EDR so customers can correlate TODRs with EDRs. Therefore, each flow ID in the list acs_flow_id_list that is acs_flow_id1, acs_flow_id2, and so on should get printed out in TODR as `smgr instance:session handle: flow id`.

An example is **92:30278:14786055** where:

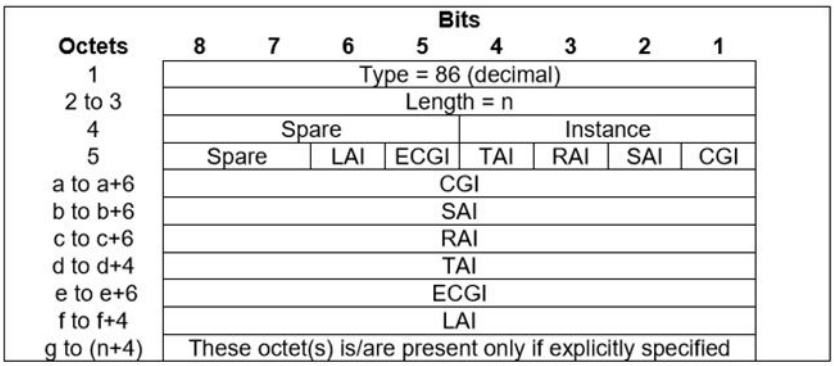
- 92 is the Session Manager instance
- 30278 is the Session Handle orsession number
- 14786055 is the ACS flow identifier

3. **ULI**

Even though the original requirment was to print ECGI, it does not cover all the scenarios. For example, when PGW is the anchor for a call that moves from 4G to 3G, ECGI does not make sense as the ULI (User Location Information) indicates CGI rather than ECGI as the user is now in 3G. Normally, MME informs PGW through SGW of the changes happened in ULI. This feature supports ULI that is s superset of ECGI.

The new field is called ULI. However, ULI is a complex IE composed of multiple identifiers and of variable length. For more details, refer the 3GPP TS 29.274.

Figure 2: User Location Information (ULI)



An ULI can be composed of one or more identifiers For example, there could be TAI and ECGI both in the ULI. Supporting such identifiers is problematic since the total length of ULI goes beyond 8 bytes and on per packet level, and have to pass an byte array and that has performance implications. In order, to overcome this issuse, ULI is formed as a combined type (for example, TAI AND ECGI together), then alone the ECGI part is shown in TODRs. This is done to ensure that identifier portion of ULI is accommodated in `uint64_t` (8 bytes). Specifically,

a. If TAI and ECGI both are present as a combined type, then only ECGI is shown.

b. If CGI and RAI both are present as a combined type, then only CGI is shown.

c. If both SAI and RAI both are present as a combined type, then only RAI is shown .

Every TODR can have multiple phases with a granularity of 2 seconds. ULI is added to the list of Phase attributes:

a. *ULI*: Newly introduced field.

ULI Details

ECGI is stored in ULI as given in the figure below. It needs to be printed in this format:

ULI Type: ULI Value

ULI Type can be any one of these:

- 1–CGI
- 2–SAI
- 4–RAI
- 8–TAI
- 16–ECGI

ECGI is stored in ULI as given in the figure below. It needs to be printed in this format:

ULIType:ULIValue

An example is given below when ULI Type is ECGI:

16:0x21635401234567

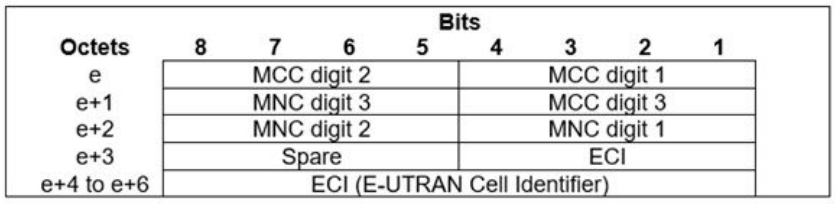
Here 16 represents that ULI Type is ECGI

0x21635401234567 is the hexadecimal representation of ECGI

MCC is '123' i.e. the three digits of MCC are '1', '2' and '3' MNC is '456', that is. the three digits of MNC are '4', '5' and '6'

ECI is '19088743' in decimal ('1234567' in hexadecimal)

Figure 3: ECGI Field



List of Attributes and File Format

All TODR attributes of traffic optimization is enabled by a single CLI command. The output is always comma separated, and in a rigid format.

Standard TODR

The following is the format of a Standard TODR:

```
instance_id,flow_type,srcIP,dstIP,policy_id, proto_type, dscp,
flow_first_pkt_rx_time_ms,flow_last_pkt_rx_time_ms,flow_cumulative_rx_bytes
```

Example:

```
1,0,173.39.13.38,192.168.3.106,0,1,0,
 1489131332693,1489131335924,342292
```

Where:

- *instance_id*: Instance ID.

- *flow_type*: Standard flow (0)
- *srcIP*: Indicates the source IP address.
- *dstIP*: Indicates the destination IP address.
- *policy_id*: Indicates the traffic optimization policy ID.
- *proto_type*: Indicates the IP protocol being used. The IP protocols are: TCP and UDP.
- *dscp*: Indicates the DSCP code for upstream packets.
- *flow_first_pkt_rx_time_ms*: Indicates the timestamp when the first packet was detected during traffic optimization.
- *flow_last_pkt_rx_time_ms*: Indicates the timestamp when the last packet was detected during traffic optimization.
- *flow_cumulative_rx_bytes*: Indicates the number of bytes transferred by this flow.

Large TODR

The following is a sample output of a Large TODR.

```
19,1,404005123456789,22.22.0.1,1.1.1.8,custom1,2,0,1588858362158,1588858952986,16420806,1588858364162,419,351,7000,0,0,1,
19:2:15,2,0,0,2,1,1,16:0x12546300012345,
1588858364162,80396,1472,0,0,0,2,1,16:0x12546300012345,1588858366171,146942,1937,7000,0,0,2
```

Where:

- *instance_id*: Instance ID.
- *flow_type*: Large flow (1)
- *imsi_id*: Indicates the International Mobile Subscriber Identity.
- *srcIP*: Indicates the source IP address.
- *dstIP*: Indicates the destination IP address.
- *policy_name*: Identifies the name of the configured traffic optimization policy.
- *policy_id*: Indicates the traffic optimization policy ID.
- *proto_type*: Indicates the IP protocol being used. The IP protocols are: TCP and UDP.
- *dscp*: Indicates the DSCP code for upstream packets.
- *flow_first_pkt_rx_time_ms*: Indicates the timestamp when the first packet was detected during traffic optimization.
- *flow_last_pkt_rx_time_ms*: Indicates the timestamp when the last packet was detected during traffic optimization.
- *flow_cumulative_rx_bytes*: Indicates the number of bytes transferred by this flow.
- *large_detection_time_ms*: Indicates the timestamp when the flow was detected as Large.
- *avg_burst_rate_kbps*: Indicates the average rate in Kbps of all the measured bursts.
- *avg_eff_rate_kbps*: Indicates the average effective rate in Kbps.

- *final_link_peak_kbps*: Indicates the highest detected link peak over the life of the Large flow.
- *recovered_capacity_bytes*: Indicates the recovered capacity in Kbps for this Large flow.
- *recovered_capacity_ms*: Indicates the timestamp of recovered capacity for this Large flow.
- *acs_flow_id_count*: Indicates the number of ACS Flow IDs present in this TODR. A maximum of 20 ACS Flow IDs is present.
- *acs_flow_id_list*: Indicates the list of individual ACS Flow IDs. For example, acs_flow_id1, acs_flow_id2, and so on.
- *phase_count*: Indicates the Large flow phase count.
- *min_gbr_kbps*: Indicates the Minimum Guaranteed Bit Rate (GBR) in Kbps.
- *max_gbr_kbps*: Indicates the Maximum Guaranteed Bit Rate (MBR) in Kbps.
- *phase_count_record*: Indicates the number of phases present in this record.
- *end_of_phases*: 0 (not end of phases) or 1 (end of phases).
- Large flow phase attributes:
  - *phase_type*: Indicates the type of the phase. This field represents that the flow was in one of the following three possible states where each state is represented by a numeric value:
    - 0 - Ramp-up Phase (if the Flow was previously idle)
    - 1 - Measurement Phase (required)
    - 2 - Flow Control Phase (if congestion detected during Measurement Phase)
  - *uli_type*: Indicates the type of ULI.
  - *phase_start_time_ms*: Indicates the timestamp for the start time of the phase.
  - *burst_bytes*: Indicates the burst size in bytes.
  - *burst_duration_ms*: Indicates the burst duration in milliseconds.
  - *link_peak_kbps*: Indicates the peak rate for the flow during its life.
  - *flow_control_rate_kbps*: Indicates the rate at which flow control was attempted (or 0 if non-flow control phase). This field is valid only when flow is in ‘Flow Control Phase’.
  - *max_num_queued_packets*: Identifies the maximum number of packets queued.
  - *policy_id*: Identifies the traffic optimization policy ID.

Sending GBR and MBR Values to Optimization Library

P-GW sends:

- GBR and MBR values based on the classification of traffic optimization selection
- Flow level GBR and MBR values to the optimization library
- Only downlink GBR and MBR to the optimization library

P-GW passes Zero GBR value for flows on a non-GBR bearer towards optimization library.

Optimatization library maintains logical flow based on Source IP, Destination IP, and Protocol IP (3-tuple). Whereas, P-GW provides GBR and MBR values based on Source IP, Destination IP, Source Port, Destination Port, and Protocol IP (5-tuple) to the optimization library. Because of these, multiple StarOS 5-tuple entries can belong to same 3-tuple entry in optimization library. Optimization library uses:

- Minimum of all MBR values that belong to the same 3-tuple entry as upper-limit.
- Maximum of all GBR values that belong to same 3-tuple entry as lower-limit.

High Throughput Traffic Optimization Support

Cisco Ultra Traffic Optimization feature is enhanced to support the subscribers through the optimization of traffic. With High Throughput Traffic Optimization Support feature, support is added for optimization of traffic for 5G subscribers (high throughput). The feature also allows automatic switching of traffic optimization parameters depending on throughput characteristics (which is in turn based on 4G or 5G).

Note This is a licensed feature. Contact your Cisco Account representative for detailed information on specific licensing requirements.

The existing Cisco Ultra Traffic Optimization single flow logic is enhanced to dynamically toggle between algorithms depending on the profile packet pattern real time (for example, 4G LTE vs 5G mm and wave traffic pattern).

Cisco Ultra Traffic Optimization library is updated to introduce two separate sets of policy parameters under a traffic optimization policy:

- Base policy parameters - these parameters are applied by the Cisco Ultra Traffic Optimization algorithm when it detects normal throughput (for example, 4G throughput). They are called 'Base' policy parameters. These parameters are the same as the parameters that existed before the High Throughput Traffic Optimization Support feature was introduced.
- Extended policy parameters - these parameters are applied by the Cisco Ultra Traffic Optimization algorithm when it detects high throughput for a flow (for example, 5G throughput). They are called ‘Extended’ policy parameters.

The two separate policy parameters under the same policy quickly switch from one set to the other without requiring any intervention from session managers when there is a change in throughput.

Hence, having two separate sets of policy parameters in the same policy helps meet the requirement that the Cisco Ultra Traffic Optimization algorithm automatically, dynamically, and immediately adjusts to the change in throughput. This change in throughput could be due to a change in RAN characteristics, for example, when UE enters a 5G or high speed 4G coverage area.

How High Throughput Optimization Support Works

Cisco Ultra Traffic Optimization algorithm monitors the traffic and automatically transitions between Base and Extended policy parameters based on the following logic:

1. Start with base policy.
2. If measurement phase burst rate > extended link profile initial-rate then move to the extended policy.

3. If measurement phase burst rate < base link profile max-rate then move to the base policy.
4. Repeat steps 2,3 for every measurement phase.

.

Multi-Policy Support for Traffic Optimization

Cisco Ultra Traffic Optimization engine supports Traffic Optimization for multiple policies and provides Traffic Optimization for a desired location. It supports a maximum of 32 policies that include two pre-configured policies, by default. Operators can configure several parameters under each Traffic Optimization policy.

This feature includes the following functionalities:

- By default, Traffic Optimization is enabled for TCP and UDP data for a particular Subscriber, Bearer, or Flow that use the Service-Schema.

Important PORT 443 supports UDP or QUIC-based Traffic Optimization.

- Selection of a policy depends on the priority configured. A trigger-condition is used to prioritize a traffic optimization policy. The priority is configurable regardless of a specific location where the traffic optimization policy is applied. Based on the configured priorities, a traffic optimization policy can be overridden by another policy.
- A configuration to associate a traffic optimization policy with a Trigger Action, under the Service-Schema.
- A configuration to select a Traffic Optimization policy for a Location Trigger. Currently, only ECGI Change Detection is supported under the Local Policy Service Configuration mode.

Important Location Change Trigger is not supported with IPSG.

Important Policy ID for a flow is not recovered after a Session Recovery (SR) or Inter-Chassis Session Recovery (ICSR).

Important The Multi-Policy Support feature requires the same Cisco Ultra Traffic Optimization license key be installed. Contact your Cisco account representative for detailed information on specific licensing requirements.

How Multi-Policy Support Works

Policy Selection

Cisco's Ultra Traffic Optimization engine provides two default policies – Managed and Unmanaged. When Unmanaged policy is selected, traffic optimization is not performed.

When Managed policy is selected, traffic optimization is performed using default parameters. Managed policy is applied when a policy is not specified in a Trigger Action where traffic optimization is enabled without specifying a policy.

When Managed policy is selected, traffic optimization is performed using default parameters. Managed policy is applied when a policy is not specified in a Trigger Action where traffic optimization is enabled without specifying a policy.

- Session Setup Trigger – If a Trigger Action is applied only for a Session Setup in a Service-Schema, then the trigger action is only applied to new sessions only.
- Bearer Setup Trigger – If a trigger action is applied only for a Bearer Setup, changes in the trigger action will be applicable to newly created bearers and its flows.
- Flow Creation Trigger – Under a trigger condition corresponding to a flow create, conditions can be added based on a rule-name, local-policy-rule or an IP protocol in addition to the trigger condition: any-match.

When traffic optimization on existing flows is disabled because of a trigger condition, then the traffic optimization engine will apply the default Unmanaged policy on them.

Deleting a Policy

Before deleting a Policy profile, all association to a traffic optimization policy should be removed.

For more information on deletion of a policy, refer to the *Traffic Optimization Policy Configuration* section.

Configuring Multi-Policy Support

The following sections describes the required configurations to support the Multi-Policy Support.

Configuring a Traffic Optimization Profile

Use the following CLI commands to configure a Traffic Optimization Profile.

```
configure
  require active-charging
  active-charging service service_name
    traffic-optimization-profile profile_name
      data-record[ large-flows-only | managed-large-flows-only ]
      no data record
      [ no ] efd-flow-cleanup-interval cleanup_interval
      [ no ] stats-interval stats_interval
      [ no ] stats-options { flow-analyst [ flow-trace ] | flow-trace [
 flow-analyst ] }
      end
```

NOTES:

- **require active-charging**: Enables the configuration requirement for an Active Charging service.

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

- **data-record**: Enables the generation of traffic optimization data record.

  large-flows-only: Enables the traffic optimization data record generation for large flows.

  managed-large-flows-only: Enables the traffic optimization data record generation for managed large flows.

  The keywords - **large-flows-only** and **managed-large-flows-only** when configured along with **data-record** enables the CUTO library to stream the respective statistics as part of the **stats-options** command, to the external server. The operator can configure a combination of the **stats-options** keywords **flow-trace** and **flow-analyst** and the **data-record** command to notify the CUTO library accordingly.

  Note One of the above the two keywords can be configured as part of the data-record, which enables the CUTO library to stream the respective statistics.

  The default behavior of the **data-record** command is not affected with the above implementation . If configured without any of the options, then TODRs are generated for all standard and large flows, which is the existing behavior.

- **efd-flow-cleanup-interval**: Configures the EFD flow cleanup interval. The interval value is an integer that ranges 10–5000 milliseconds.
- **stats-interval**: Configures the flow statistics collection and reporting interval in seconds. The interval value is an integer that ranges 1–60 seconds.
- **stats-options**: Configures options to collect the flow statistics. It only specifies whether the stream must be a Flow Trace or a Flow Analyst or both, to an external server.

Note From Release 21.6 onwards, the **heavy-session** command is deprecated.

Configuring a Traffic Optimization Policy

Use the following CLI commands to configure a Traffic Optimization Policy.

```
configure
   require active-charging
   active-charging service service_name[extended]
      [ no ] traffic-optimization-policy policy_name[extended]
        bandwidth-mgmt { backoff-profile [ managed | unmanaged ] [
min-effective-rate effective_rate [ min-flow-control-rate flow_rate ] |
min-flow-control-rate flow_rate [ min-effective-rate effective_rate ] ] |
min-effective-rate effective_rate [ backoff-profile [ managed | unmanaged ]
 [ min-flow-control-rate flow_rate ] | min-flow-control-rate control_rate [
```

backoff-profile [managed | unmanaged]] | min-flow-control-rate [[backoff-profile [managed | unmanaged] [min-effective-rate *effective_rate* **] | [min-effective-rate** *effective_rate* **] [backoff-profile [managed | unmanaged]] }**

extended-bandwidth-mgmt { backoff-profile [managed | unmanaged] [min-effective-rate *effective_rate* **[min-flow-control-rate** *flow_rate* **] | min-flow-control-rate** *flow_rate* **[min-effective-rate** *effective_rate* **]] | min-effective-rate** *effective_rate* **[backoff-profile [managed | unmanaged] [min-flow-control-rate** *flow_rate* **] | min-flow-control-rate** *control_rate* **[backoff-profile [managed | unmanaged]] | min-flow-control-rate [[backoff-profile [managed | unmanaged] [min-effective-rate** *effective_rate* **] | [min-effective-rate** *effective_rate* **] [backoff-profile [managed | unmanaged]] }**

[no] bandwidth-mgmt

[no] extended-bandwidth-mgmt

curbing-control { max-phases *max_phase_value* **[rate** *curbing_control_rate* **[threshold-rate** *threshold_rate* **[time** *curbing_control_duration* **]]] | rate** *curbing_control_rate* **[max-phases [threshold-rate** *threshold_rate* **[time** *curbing_control_duration* **]]] | threshold-rate [max-phases** *max_phase_value* **[rate** *curbing_control_rate* **[time** *curbing_control_duration* **]]] | time [max-phases** *max_phase_value* **[rate** *curbing_control_rate* **[threshold-rate** *threshold_rate***]]] }**

extended-curbing-control { max-phases *max_phase_value* **[rate** *curbing_control_rate* **[threshold-rate** *threshold_rate* **[time** *curbing_control_duration* **]]] | rate** *curbing_control_rate* **[max-phases [threshold-rate** *threshold_rate* **[time** *curbing_control_duration* **]]] | threshold-rate [max-phases** *max_phase_value* **[rate** *curbing_control_rate* **[time** *curbing_control_duration* **]]] | time [max-phases** *max_phase_value* **[rate** *curbing_control_rate* **[threshold-rate** *threshold_rate***]]] }**

[no] curbing-control

[no] extended-curbing-control

heavy-session { standard-flow-timeout [threshold *threshold_value* **| threshold** *threshold_value* **[standard-flow-timeout** *timeout_value* **] }**

extended-heavy-session { standard-flow-timeout [threshold *threshold_value* **| threshold** *threshold_value* **[standard-flow-timeout** *timeout_value* **] }**

[no] heavy-session

[no] extended-heavy-session

link-profile { initial-rate *initial_seed_value* **[max-rate** *max_peak_rate_value* **[peak-lock]] | max-rate [initial-rate** *initial_seed_value* **[peak-lock]] | peak-lock [initial-rate** *initial_seed_value* **[max-rate** *max_peak_rate_value* **]] }**

extended-link-profile { initial-rate *initial_seed_value* **[max-rate** *max_peak_rate_value* **[peak-lock]] | max-rate [initial-rate** *initial_seed_value* **[peak-lock]] | peak-lock [initial-rate** *initial_seed_value* **[max-rate** *max_peak_rate_value* **]] }**

[no] link-profile

[no] extended-link-profile

session-params { tcp-ramp-up *tcp_rampup_duration* **[udp-ramp-up** *udp_rampup_duration* **] | udp-ramp-up** *udp_rampup_duration* **[tcp-ramp-up** *tcp_rampup_duration* **] }**

```
      extended-session-params { tcp-ramp-up tcp_rampup_duration [ udp-ramp-up
 udp_rampup_duration ] | udp-ramp-up udp_rampup_duration [ tcp-ramp-up
tcp_rampup_duration ] }
       [ no ] session-params
       [ no ] extended-session-params
       end
```

NOTES:

- Only when **extended** keyword is used after the policy name, you will be able to see the '**extended-***' parameters, for example **extended-bandwidth-mgmt**.
- **no**: Overwrites the configured parameters with default values. The operator must remove all associated policies in a policy profile before deleting a policy profile. Otherwise, the following error message is displayed:

  ```
  Failure: traffic-optimization policy in use, cannot be deleted.
  ```

- **bandwidth-mgmt**: Configures Base bandwidth management parameters.
  - **backoff-profile**: Determines the overall aggressiveness of the back off rates.
  - **managed**: Enables both traffic monitoring and traffic optimization.
  - **unmanaged**: Only enables traffic monitoring.
  - **min-effective-rate**: Configures minimum effective shaping rate in Kbps.
  - **min-flow-control-rate**: Configures the minimum rate that is allowed in Kbps to control the flow of heavy-session-flows during congestion.
- **extended-bandwidth-mgmt**: Configures Extended bandwidth management parameters.
  - **backoff-profile**: Determines the overall aggressiveness of the back off rates.
  - **managed**: Enables both traffic monitoring and traffic optimization.
  - **unmanaged**: Only enables traffic monitoring.
  - **min-effective-rate**: Configures minimum effective shaping rate in Kbps.
  - **min-flow-control-rate**: Configures the minimum rate that is allowed in Kbps to control the flow of heavy-session-flows during congestion.
- **curbing-control**: Configures Base curbing flow control related parameters.
  - **max-phases**: Configures consecutive phases where the target shaping rate is below **threshold-rate** to trigger curbing flow control. .
  - **rate**: Configures the curbing flow-control at a fixed rate in Kbps instead of a dynamic rate.
  - **threshold-rate**: Configures the minimum target shaping rate in kbps to trigger curbing..
  - **time**: Configures the duration of a flow control phase in milliseconds.
- **extended-curbing-control**: Configures Extended curbing flow control related parameters.

  - **max-phases**: Configures consecutive phases where the target shaping rate is below **threshold-rate** to trigger curbing flow control. The maximum phase value is an integer ranging 2–10 for extended parameter. The default value inherits base.
  - **rate**: Configures the curbing flow-control at a fixed rate in Kbps instead of a dynamic rate. The control rate value is an integer ranging 0-100000 kbps for extended parameter. The default value inherits base.
  - **threshold-rate**: Configures the minimum target shaping rate in kbps to trigger curbing.The threshold rate is an integer ranging 100-100000 kbps for extended parameter. The default value inherits base.
  - **time**: Configures the duration of a flow control phase in milliseconds.

    The flow control duration value is an integer ranging 0–600000 for extended parameter. The default value inherits base.

- **heavy-session**: Configures parameters for Base heavy-session detection.
  - **standard-flow-timeout**: Configures the idle timeout in milliseconds, for expiration of standard flows.
  - **threshold**: Configures heavy-session detection threshold in bytes. On reaching the threshold, the flow is monitored and potentially managed..
- **extended-heavy-session**: Configures parameters for Extended heavy-session detection.
  - **standard-flow-timeout**: Configures the idle timeout in milliseconds, for expiration of standard flows. .
  - **threshold**: Configures heavy-session detection threshold in bytes. On reaching the threshold, the flow is monitored and potentially managed.
- **link-profile**: Configures Base link profile parameters.
  - **initial-rate**: Configures the initial seed value of the acquired peak rate in Kbps for a traffic session.
  - **max-rate**: Configures the maximum learned peak rate that is allowed in Kbps for a traffic session.
  - **peak-lock**: Confirms with the link peak rate available at the initial link peak rate setting.
- **extended-link-profile**: Configures Extended link profile parameters.
  - **initial-rate**: Configures the initial seed value of the acquired peak rate in Kbps for a traffic session.
  - **max-rate**: Configures the maximum learned peak rate that is allowed in Kbps for a traffic session.
  - **peak-lock**: Confirms with the link peak rate available at the initial link peak rate setting.
- **session-params**: Configures Base session parameters.
  - **tcp-ramp-up**: Configures the ramp-up-phase duration in milliseconds, for TCP traffic.
  - **udp-ramp-up**: Configures the ramp-up-phase duration in milliseconds, for the UDP traffic..
- **extended-session-params**: Configures Extended session parameters.
  - **tcp-ramp-up**: Configures the ramp-up-phase duration in milliseconds, for TCP traffic.

- **udp-ramp-up**: Configures the ramp-up-phase duration in milliseconds, for the UDP traffic..

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

The following table shows the parameter ranges for both Base and Extended set parameters, the default values of those parameters and, the validated Range/value for configuring the parameters for Cisco Ultra Traffic Optimization library.

Parameter category (Base/Extended)	Parameter	Base Parameter Range	Base default value	Extended Parameter Range	Extended default value	Range/value check	Comment
bandwidth-mgmt /extended-bandwidth-mgmt	**backoff-profile**	**managed /unmanaged**	**managed**	**managed /unmanaged**	Inherits base	require match base	If you enter a value different from Base, the value from Base parameter and an appropriate message will be displayed.
	min-effective-rate	100-100000 kbps	600	100-500000 kbps	45000	allow full range	
	min-flow-control-rate	100-100000 kbps	250	100- 500000 kbps	1000	allow full range	

Parameter category (Base/Extended)	Parameter	Base Parameter Range	Base default value	Extended Parameter Range	Extended default value	Range/value check	Comment
curbing-control / **extended-curbing-control**	**max-phases**	2-10	2	2-10	Inherits base	allow full range	
	rate	0-100000 kbps	0	0-100000 kbps	Inherits base	allow full range	
	threshold-rate	100-100000 kbps	600	100-100000 kbps	Inherits base	allow full range	
	time	0-600000 ms	0	0-600000 ms	Inherits base	allow full range	
heavy-session / **extended-heavy-session**	**standard-flow-timeout**	100-10000 ms	500	100-10000 ms	Inherits base	allow full range	
	threshold	100000–100000000 bytes	3000000	100000–100000000 bytes	Inherits base	allow full range	

Parameter category (Base/Extended)	Parameter	Base Parameter Range	Base default value	Extended Parameter Range	Extended default value	Range/value check	Comment
link-profile / **extended-link-profile**	**initial-rate**	100-100000 kbps	7000	100-500000 kbps	50000	require greater than or equal to base max-rate	If you enter a value different from Base, the value from Base parameter and an appropriate message will be displayed.
	max- rate	100-100000 kbps	15000	100-500000 kbps	100000	require greater than or equal to base max-rate	If you enter a value different from Base, the value from Base parameter and an appropriate message will be displayed.
	peak-lock	enabled/disabled	disabled	enabled/disabled	disabled	allow either	

Parameter category (Base/Extended)	Parameter	Base Parameter Range	Base default value	Extended Parameter Range	Extended default value	Range/value check	Comment
session-params / **extended- session-params**	**tcp-ramp-up**	0-10000 ms	2000	0-10000 ms	2000	allow full range	
	udp-ramp-up	0-10000 ms	2000	0-10000 ms	2000	allow full range	

Traffic Optimization Policy - Default Values

```
Bandwidth-Mgmt:

   Backoff-Profile         : Managed
   Min-Effective-Rate      : 600 (kbps)
   Min-Flow-Control-Rate   : 250 (kbps)

Curbing-Control:

   Time                    : 0 (ms)
   Rate                    : 0 (kbps)
   Max-Phases              : 2
   Threshold-Rate          : 600 (kbps)

Heavy-Session:

   Threshold               : 3000000(bytes)
   Standard-Flow-Timeout   : 500 (ms)

Link-Profile:

   Initial-Rate            : 7000 (kbps)
   Max-Rate                : 15000 (kbps)
   Peak-Lock               : Disabled

Session-Params:

   Tcp-Ramp-Up             : 2000 (ms)
   Udp-Ramp-Up             : 2000 (ms)
```

Associating a Trigger Action to a Traffic Optimization Policy

Use the following CLI commands to associate a Trigger Action to a Traffic Optimization Policy.

```
configure
   require active-charging
   active-charging service service_name
      trigger-action trigger_action_name
         traffic-optimization policy policy_name
         [ no ] traffic-optimization
         end
```

NOTES:

- **traffic-optimization policy**: Configures a traffic optimization policy.
- **no**: Removes the configured traffic optimization policy.

Enabling TCP and UDP

Use the following CLI commands to enable TCP and UDP protocol for Traffic Optimization:

```
configure
  require active-charging
  active-charging service service_name
    trigger-condition trigger_condition_name
      [ no ] ip protocol = [ tcp | udp ]
      end
```

NOTES:

- **no**: Deletes the Active Charging Service related configuration.
- **ip**: Establishes an IP configuration.
- **protocol**: Indicates the protocol being transported by the IP packet.
- **tcp**: Indicates the TCP protocol to be transported by the IP packet.
- **udp**: Indicates the UDP protocol to be transported by the IP packet.

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

Service-Scheme Configuration for Multi-Policy Support

The service-schema framework enables traffic optimization at APN, rule base, QCI, and Rule level. In 21.6, with the Multi-Policy Support feature, traffic optimization in a service-schema framework allows the operator to configure multiple policies and to configure traffic optimization based on a desirable location.

The service-schema framework helps in associating actions based on trigger conditions, which can be triggered either at call-setup time, Bearer-creation time, or flow-creation time.

Session Setup Trigger

The **any-match = TRUE**, a wildcard configuration, is the only supported condition for this trigger and so this is applicable to all the flows of the subscriber.

Use the following configuration to setup a Session Trigger:

```
configure
    active-charging service service_name
      trigger-action trigger_action_name
         traffic-optimization
         exit
      trigger-condition trigger_condition_name1
         any-match = TRUE
         exit
      service-scheme service_scheme_name
         trigger sess-setup
            priority priority_value trigger-condition trigger_condition_name1
trigger-action trigger_action_name
```

```
            exit
        subs-class sub_class_name
            apn = apn_name
            exit
        subscriber-base subscriber_base_name
           priority priority_value subs-class sub_class_name bind service-scheme
 service_scheme_name
            end
```

Sample Configuration

Following is a sample configuration for Session Setup Trigger:

```
service-scheme SS1
     trigger sess-setup
       priority 1 trigger-condition sess-setup trigger-action sess-setup
     #exit
   trigger-condition sess-setup
     any-match = TRUE
   #exit
   trigger-action sess-setup
     traffic-optimization policy sess-setup
   #exit
```

Bearer Creation Trigger

The trigger conditions related to QCI can be used for this trigger, and so this is applicable to all the flows of specific bearers.

Use the following configuration to configure a Bearer Creation Trigger:

```
configure
  active-charging service service_name
    service-scheme service_scheme_name
      trigger bearer-creation
        priority priority_value trigger-condition trigger_condition_name2
trigger-action trigger_action_name
        exit
      trigger-condition trigger_condition_name2
        qci = qci_value
        exit
      trigger-action bearer-creation
        traffic-optimization policy bearer-creation
        exit
```

Sample Configuration

The following is a sample configuration for Bearer Creation Trigger:

```
service-scheme SS1
     trigger bearer-creation
       priority 1 trigger-condition bearer-creation trigger-action bearer-creation
     #exit
   trigger-condition bearer-creation
     qci = 1 to 2
   #exit
   trigger-action bearer-creation
```

```
    traffic-optimization policy bearer-creation
  #exit
```

Flow Creation Trigger

The trigger conditions related to rule-name and QCI can be used here, and so this is related to specific flow.

Use the following configuration to configure a flow creation trigger:

```
configure
   active-charging service service_name
      service-scheme service_scheme_name
         trigger bearer-creation
            priority priority_value trigger-condition trigger_condition_name
trigger-action trigger_action_name
            exit
         trigger-condition trigger_condition_name
            ip-protocol = protocol_type
            rule-name = rule_name
               **Multi-line or All-lines**
            exit
```

Sample Configuration

The following is a sample configuration for Flow Creation Trigger using the default Cisco Ultra Traffic Optimization policy:

```
service-scheme SS1
    trigger flow-create
      priority 1 trigger-condition TC5 trigger-action TA4
    #exit
    trigger-condition TC5
      ip protocol = tcp
      ip protocol = udp
      multi-line-or all-lines
    #exit
    trigger-action TA4
      traffic-optimization
    #exit
```

Configuring: ecgi-change

The following demonstrates ecgi-change sample configuration:

Trigger Condition and Trigger Action in ACS Configuration

```
configure
active-charging-service ACS
   trigger-action TA1
      traffic-optimization policy flow-create-ecgi-change
    #exit
    trigger-condition TC4
      local-policy-rule = ruledef-ecgi
    #exit
 end
```

Service Schema Configuration

```
configure
active-charging-service ACS
```

```
    service-scheme SS1
      trigger flow-create
        priority 2 trigger-condition TC4 trigger-action TA1
      #exit
    subs-class SC1
      any-match = TRUE
    #exit
    subscriber-base SB1
      priority 1 subs-class SC1 bind service-scheme SS1
    #exit
end
```

Local Policy Configuration

```
local-policy-service LP
    ruledef anymatch
      condition priority 1 imsi match *
    #exit
    ruledef ecgi-1
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AE7F0A 1AE7F0B 1AE7F28 1AE7F29
1AE7F46 1AE7F47 1AEAC00 1AEAC01 1AEAC02 1AEAC0A 1AEAC0B 1AEAC0C 1AEAC14 1AEAC15 1AEAC16
1AEAC28 1AEAC29 1AEAC2A 1AEAC46 1AEAC47 1AEAC48 1AEAC50 1AEAC51 1AEAC52 1AEAC6E 1AEAC6F
1AEAC70 1AEAC78 1AEAC79 1AEAC7A
    #exit
    ruledef ecgi-10
      condition priority 1 ecgi mcc 300 mnc 235 eci match 1F36C52 1F36C6E 1F36C6F 1F36C70
1F36C78 1F36C79 1F36C7A
    #exit
    ruledef ecgi-2
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AEBE01 1AEBE02 1AEBE0B 1AEBE0C
1AEBE15 1AEBE16 1AEBE29 1AEBE2A 1AEBE47 1AEBE48 1AEBF00 1AEBF01 1AEBF02 1AEBF0A 1AEBF0B
1AEBF0C 1AEBF14 1AEBF15 1AEBF16 1AEBF1E 1AEBF1F 1AEBF20 1AEBF28 1AEBF29 1AEBF2A 1AEBF46
    #exit
    ruledef ecgi-3
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AEBF47 1AEBF48 1AEBF50 1AEBF51
1AEBF52 1AEBF6E 1AEBF6F 1AEBF70 1AEBF78 1AEBF79 1AEBF7A 1AF0E00 1AF0E01 1AF0E02 1AF0E0A
1AF0E0B 1AF0E0C 1AF0E14 1AF0E15 1AF0E16 1AF0E28 1AF0E29 1AF0E2A 1AF0E46
    #exit
    ruledef ecgi-4
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AF0E47 1AF0E48 1AF4A0A 1AF4A0B
1AF4A14 1AF4A15 1AF4A28 1AF4A29 1AF4A46 1AF4A47 1AF4D00 1AF4D01 1AF4D0A 1AF4D0B 1AF4D14
1AF4D15 1AF4D28 1AF4D29 1AF4D46 1AF4D47 1AF4D50 1AF4D51 1AF4D6E 1AF4D6F
    #exit
    ruledef ecgi-5
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AF4D78 1AF4D79 1AF7200 1AF7201
1AF7202 1AF720A 1AF720B 1AF720C 1AF7214 1AF7215 1AF7216 1AF721E 1AF721F 1AF7444 1AF7228
1AF7229 1AF722A 1AF7246 1AF7247 1AF7248 1AF7250 1AF7251 1AF7252 1AF726E
    #exit
    ruledef ecgi-6
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AF726F 1AF7270 1B04C00 1B04C01
1B04C02 1B04C03 1B04C0A 1B04C0B 1B04C0C 1B04C0D 1B04C14 1B04C15 1B04C16 1B04C17 1B04C1E
1B04C1F 1B04C20 1B04C21 1B04C28 1B04C29 1B04C2A 1B04C2B 1B04C46 1B04C47
    #exit
    ruledef ecgi-7
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1B04C48 1B04C49 1B04C50 1B04C51
1B04C52 1B04C53 1B04C6E 1B04C6F 1B04C70 1B04C71 1B04C78 1B04C79 1B04C7A 1B04C7B 1B05300
1B05301 1B05302 1B0530A 1B0530B 1B0530C 1B05314 1B05315 1B05316 1B05328 1B05329
    #exit
    ruledef ecgi-8
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1B0532A 1B05346 1B05347 1B05348
1B32F00 1B32F01 1B32F02 1B32F0A 1B32F0B 1B32F0C 1B32F14 1B32F15 1B32F16 1B32F28 1B32F29
1B32F2A 1B32F46 1B32F47 1B32F48 1B76400 1B76401 1B76402 1B7640A 1B7640B 1B7640C 1B76428
    #exit
    ruledef ecgi-9
```

```
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1B76429 1B7642A 1B76446 1B76447
1B76448 1F36C00 1F36C01 1F36C02 1F36C0A 1F36C0B 1F36C0C 1F36C14 1F36C15 1F36C16 1F36C1E
1F36C1F 1F36C20 1F36C28 1F36C29 1F36C2A 1F36C46 1F36C47 1F36C48 1F36C50 1F36C51
    #exit
    actiondef activate_lp_action
      action priority 1 activate-lp-rule name ruledef-tai
    #exit
    actiondef activate_lp_action1
      action priority 3 event-triggers ecgi-change
    #exit
    actiondef ecgi_change
      action priority 1 activate-lp-rule name ruledef-ecgi
    #exit
    eventbase default
     rule priority 1 event new-call ruledef anymatch actiondef activate_lp_action1 continue

      rule priority 11 event new-call ruledef ecgi-1 actiondef ecgi_change continue
      rule priority 12 event new-call ruledef ecgi-2 actiondef ecgi_change continue
      rule priority 13 event new-call ruledef ecgi-3 actiondef ecgi_change continue
      rule priority 14 event new-call ruledef ecgi-4 actiondef ecgi_change continue
      rule priority 15 event new-call ruledef ecgi-5 actiondef ecgi_change continue
      rule priority 16 event new-call ruledef ecgi-6 actiondef ecgi_change continue
      rule priority 17 event new-call ruledef ecgi-7 actiondef ecgi_change continue
      rule priority 18 event new-call ruledef ecgi-8 actiondef ecgi_change continue
      rule priority 19 event new-call ruledef ecgi-9 actiondef ecgi_change continue
      rule priority 20 event new-call ruledef ecgi-10 actiondef ecgi_change continue
      rule priority 21 event ecgi-change ruledef ecgi-1 actiondef ecgi_change continue
      rule priority 22 event ecgi-change ruledef ecgi-2 actiondef ecgi_change continue
      rule priority 23 event ecgi-change ruledef ecgi-3 actiondef ecgi_change continue
      rule priority 24 event ecgi-change ruledef ecgi-4 actiondef ecgi_change continue
      rule priority 25 event ecgi-change ruledef ecgi-5 actiondef ecgi_change continue
      rule priority 26 event ecgi-change ruledef ecgi-6 actiondef ecgi_change continue
      rule priority 27 event ecgi-change ruledef ecgi-7 actiondef ecgi_change continue
      rule priority 28 event ecgi-change ruledef ecgi-8 actiondef ecgi_change continue
      rule priority 29 event ecgi-change ruledef ecgi-9 actiondef ecgi_change continue
      rule priority 30 event ecgi-change ruledef ecgi-10 actiondef ecgi_change continue
    #exit
  #exit
end
```

Traffic Optimization Policy Configuration

```
configure
active-charging-service ACS
traffic-optimization-policy Config:
    traffic-optimization-policy flow-create-ecgi-change
      heavy-session threshold 400000
    #exit
end
```

Local Policy Configuration

Important Configuring Local Policy needs a Local Policy Decision Engine License. Contact your Cisco account representative for information on specific licensing requirements.

This section describes the traffic optimization policy configuration that is based on location.

Use the following sample configuration to enable a eCGI change rule:

```
configure
   active-charging service service_name
     local-policy-service service_name
       ruledef ruledef_name
         condition priority priority_value ecgi mccmcc_value mnc mnc_value eq
eq_value
          exit
        actiondef actiondef_name1
          action priority priority_value event-triggers actiondef_name2
          exit
        actiondef actiondef_name2
          action priority priority_value activate-lp-ruleruledef_name
          exit
        eventbase eventbase_name
          rule priority priority_value event event_name ruledef ruledef_name
actiondef actiondef_name1continue
          rule priority priority_value event event_name ruledef ruledef_name
actiondef actiondef_name1continue
          exit
```

Service-Scheme Configuration

```
configure
   active-charging service service_name
      service-scheme service_scheme_name
         trigger flow-create
            priority priority_value trigger-condition trigger_condition_name
trigger-action trigger_action_name
            exit
         trigger condition trigger_condition_name
            local-policy-rule = rule_name
            exit
         trigger action trigger_action_name
            traffic-optimization policy policy_name
            exit
```

Configuring L7 Rule

Important Configuring L7 Rule needs an Application Detection Control License. Contact your Cisco account representative for detailed information on specific licensing requirements.

Use the following CLI to configure an L7 rule:

```
configure
   active-charging service service_name
      service-scheme service_scheme_name
         trigger bearer-creation
            priority priority_value trigger-condition trigger_condition_name
trigger-action trigger_action_name
            exit
         trigger-condition trigger_condition_name
```

```
        rule-name = rule_name
        rule-name = rule_name
          **Multi-line or All-lines**
    trigger-action trigger_action_name
        traffic-optimization policy policy_name
        exit
```

Sample Configuration

The following is a sample configuration for L7 Rules:

```
service-scheme SS1
    trigger flow-create
      priority 1 trigger-condition TC6 trigger-action TA6
    #exit
    trigger-condition TC6
      rule-name = whatsapp
      rule-name = http
      multi-line-or all-lines
    #exit
    trigger-action TA6
      traffic-optimization policy flow-create-L7-Rules
    #exit
```

Ookla Speedtest

Use the configuration information discussed in the section Configuring L7 Rule, on page 49.

Sample Configuration

The following is a sample configuration for Ookla Speedtest:

```
service-scheme SS1
     trigger flow-create
       priority 1 trigger-condition ookla trigger-action ookla
     #exit
   trigger-condition ookla
     rule-name = speedtest
   #exit
   trigger-action ookla
     no traffic-optimization
   #exit
```

Location and App-based Configuration

Sample Configuration

```
service-scheme SS1
   trigger flow-create
     priority 1 trigger-condition TC3 trigger-action TA2
   #exit
   trigger-condition TC3
     local-policy-rule = ruledef-ecgi
     rule-name = youtube
     rule-name = whatsapp
     multi-line-or all-lines
   #exit
   trigger-action TA2
     traffic-optimization policy flow-create-ecgi-change
   #exi
```

Selective Configuration by Disabling TCP and UDP

Sample Configuration

```
service-scheme SS1
    trigger flow-create
      priority 1 trigger-condition tcponly trigger-action tcponly
      priority 2 trigger-condition udponly trigger-action udponly
    #exit
    trigger-condition tcponly
      ip protocol = tcp
    #exit
    trigger-condition udponly
      ip protocol = udp
    #exit
    trigger-action tcponly
      no traffic-optimization
    #exit
    trigger-action udponly
      no traffic-optimization
    #exit
```

L7/ADC and Location Trigger based Configuration

Sample Configuration

This sample configuration describes a scenario where an operator wants to always disable Traffic Optimization for Speedtest. The configuration disables traffic optimization regardless of the location. It applies a specific policy for a specific location (ECGI) (except for Speedtest) and overrides any other policy set by any trigger condition.

Also, for a specific policy optimization, for example: YouTube, the policy selection is prioritized as follows:

```
Service Scheme Configuration:
service-scheme SS1
trigger flow-create
  priority 1 trigger-condition speedtest-tc trigger-action speedtest-ta
  priority 2 trigger-condition location-tc trigger-action location-ta
  priority 3 trigger-condition youtube-tc trigger-action youtube-ta
  #exit
  trigger-condition location-tc
    local-policy-rule = ruledef-ecgi
  #exit
  trigger-action location-ta
    traffic-optimization policy flow-create-ecgi-change
  #exit
  trigger-condition speedtest-tc
    *rule-name = speedtest
  #exit
  trigger-action speedtest-ta
    no traffic-optimization
  #exit
  trigger-condition youtube-tc
    rule-name = youtube
  #exit
  trigger-action youtube-ta
    traffic-optimization policy youtube-policy
  #exit
* Provided rule-name = speedtest, is configured such that it always detects this traffic.
```

Configuring Cisco Ultra Traffic Optimization

This section provides information on enabling support for the Cisco Ultra Traffic Optimization solution.

Loading Traffic Optimization

Use the following configuration under the Global Configuration Mode to load the Cisco Ultra Traffic Optimization as a solution:

```
configure
   require active-charging traffic-optimization
   end
```

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

Important Enabling or disabling the traffic optimization can be done through the Service-scheme framework.

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

Important In 21.3, and 21.5 and later releases, the dependency on the chassis reboot is not valid anymore. The Cisco Ultra Traffic Optimization engine is loaded by default. The Cisco Ultra Traffic Optimization configuration CLIs are available when the license is enabled. As such, the **traffic-optimization** keyword has been deprecated.

Enabling Cisco Ultra Traffic Optimization Configuration Profile

Use the following configuration under ACS Configuration Mode to enable the Cisco Ultra Traffic Optimization profile:

```
configure
   active-charging service service_name
      traffic-optimization-profile
      end
```

NOTES:

- The above CLI command enables the Traffic Optimization Profile Configuration, a new configuration mode.

Configuring the Operating Mode

Use the following CLI commands to configure the operating mode under Traffic Optimization Profile Configuration Mode for the Cisco Ultra Traffic Optimization engine:

```
configure
   active-charging service service_name
      traffic-optimization-profile
         mode [ active | passive ]
         end
```

Notes:

- **mode**: Sets the mode of operation for traffic optimization.
- **active**: Active mode where both traffic optimization and flow monitoring is done on the packet.
- **passive**: Passive mode where no flow-control is performed but monitoring is done on the packet.

Enabling Cisco Ultra Traffic Optimization Configuration Profile Using Service-scheme Framework

The service-scheme framework is used to enable traffic optimization at APN, rule base, QCI, and Rule level. There are two main constructs for the service-scheme framework:

- **Subscriber-base** – This helps in associating subscribers with service-scheme based on the subs-class configuration.
  - **subs-class** – The conditions defined under subs-class enables in classifying the subscribers based on rule base, APN, v-APN name. The conditions can also be defined in combination, and both OR as well as AND operators are supported while evaluating them.
- **Service-scheme** – This helps in associating actions based on trigger conditions which can be triggered either at call-setup time, Bearer-creation time, or flow-creation time.
  - **trigger-condition** – For any trigger, the trigger-action application is based on conditions defined under the trigger-condition.
  - **trigger-actions** – Defines the actions to be taken on the classified flow. These actions can be traffic optimization, throttle-suppress, and so on.

Session Setup Trigger

The **any-match = TRUE**, a wildcard configuration, is the only supported condition for this trigger and so this is applicable to all the flows of the subscriber.

Following is a sample configuration:

```
configure
   active-charging service service_name
     service-scheme service_scheme_name
         trigger sess-setup
            priority priority_value trigger-condition trigger_condition_name1
```

```
trigger-action trigger_action_name
            exit
         trigger-condition trigger_condition_name1
            any-match = TRUE
            exit
         trigger-action sess-setup
         traffic-optimization policy sess-setup
            exit
```

Bearer Creation Trigger

The trigger conditions related to QCI can be used for this trigger, and so this is applicable to all the flows of specific bearers.

The following is a sample configuration:

```
configure
   active-charging service service_name
      trigger-action trigger_action_name
         traffic-optimization
         exit
      trigger-condition trigger_condition_name1
         any-match = TRUE
         exit
      trigger-condition trigger_condition_name2
         qci = qci_value
         exit
      service-scheme service_scheme_name
         trigger bearer-creation
            priority priority_value trigger-condition trigger_condition_name2
trigger-action trigger_action_name
            exit
         exit
      subs-class sub_class_name
         apn = apn_name
         exit
      subscriber-base subscriber_base_name
         priority priority_value subs-class sub_class_name bind service-scheme
 service_scheme_name
         end
```

Flow Creation Trigger

The trigger conditions related to rule-name and QCI can be used here, and so this is related to specific flow.

The following is a sample configuration:

```
configure
   active-charging service service_name
      trigger-action trigger_action_name
         traffic-optimization
         exit
      trigger-condition trigger_condition_name1
         any-match = TRUE
```

```
        exit
      trigger-condition trigger_condition_name2
        qci = qci_value
        exit
      trigger-condition trigger_condition_name3
        rule-name = rule_name
        exit
      service-scheme service_scheme_name
        trigger bearer-creation
          priority priority_value trigger-condition trigger_condition_name3
trigger-action trigger_action_name
          exit
        exit
      subs-class sub_class_name
        apn = apn_name
        exit
      subscriber-base subscriber_base_name
        priority priority_value subs-class sub_class_name bind service-scheme
 service_scheme_name
        end
```

Notes:

- *trigger_condition_name3* can have only rules, only QCI, both rule and QCI, or either of rule and QCI.

The following table illustrates the different levels of Traffic Optimization and their corresponding Subscriber Class configuration and Triggers.

Traffic Optimization Levels	Subscriber Class configuration and Triggers
Applicable to all the calls or flows	**subs-class** *sc1* **any-match = TRUE** **exit** Sessetup trigger condition is **any-match** = **TRUE**
Applicable to all calls or flows of a rulebase	**subs-class** *sc1* **rulebase = prepaid** **exit** Sessetup trigger condition is **any-match** = **TRUE**
Applicable to all calls or flows of an APN	**subs-class** *sc1* **apn = cisco.com** **exit** Sessetup trigger condition is **any-match** = **TRUE**
Applicable to all flows of a Bearer	**trigger-condition** *TC1* **qci = 1** **exit** Bearer creation trigger condition is TC1

Traffic Optimization Levels	Subscriber Class configuration and Triggers
Applicable to a particular flow	**trigger-condition** *TC1* **qci = 1** **rule-name = tcp** **multi-line-or all-lines** **exit** Flow creation trigger condition is TC1

Important In case of LTE to eHRPD handover, since QCI is not valid for eHRPD, it is recommended to configure rule-name as the trigger-condition under service-scheme.

Generating TODR

Use the following CLI commands under ACS Configuration Mode to enable Traffic Optimization Data Record (TODR) generation:

```
configure
   active-charging service service_name
      traffic-optimization-profile
         data-record
         end
```

NOTES:

- If previously configured, use the **no data-record** command to disable generating TODR.

Monitoring and Troubleshooting

This section provides information regarding commands available to monitor and troubleshoot the Cisco Ultra Traffic Optimization solution on the P-GW.

Cisco Ultra Traffic Optimization Show Commands and/or Outputs

This section provides information about show commands and the fields that are introduced in support of Cisco Ultra Traffic Optimization solution.

show active-charging traffic-optimization counters

The **show active-charging traffic-optimization counters sessmgr { all | instance** *number* **}** CLI command is introduced where:

- **counters** – Displays aggregate flow counters/statistics from Cisco Ultra Traffic Optimization engine.

Important This CLI command is license dependent and visible only if the license is loaded.

Following are the new field/counters:

- Traffic Optimization Flows:
  - Active Normal Flow Count
  - Active Large Flow Count
  - Active Managed Large Flow Count
  - Active Unmanaged Large Flow Count
  - Base Policy:
    - Active Large Flow Count
    - Active Managed Large Flow Count
    - Active Unmanaged Large Flow Count
  - Extended Policy:
    - Active Large Flow Count
    - Active Managed Large Flow Count
    - Active Unmanaged Large Flow Count
  - Total Normal Flow Count
  - Total Large Flow Count
  - Total Managed Large Flow Count
  - Total Unmanaged Large Flow Count
  - Base Policy:
    - Total Large Flow Count
    - Total Managed Large Flow Count
    - Total Unmanaged Large Flow Count
  - Extended Policy:
    - Total Large Flow Count
    - Total Managed Large Flow Count
    - Total Unmanaged Large Flow Count
  - Total IO Bytes
  - Total Large Flow Bytes

- Total Recovered Capacity Bytes
- Total Recovered Capacity ms

On executing the above command, the following new fields are displayed for the Multi-Policy Support feature:

Important This CLI command is license dependent and visible only if the license is loaded.

- TCP Traffic Optimization Flows:
  - Active Normal Flow Count
  - Active Large Flow Count
  - Active Managed Large Flow Count
  - Active Unmanaged Large Flow Count
  - Base Policy:
    - Active Large Flow Count
    - Active Managed Large Flow Count
    - Active Unmanaged Large Flow Count
  - Extended Policy:
    - Active Large Flow Count
    - Active Managed Large Flow Count
    - Active Unmanaged Large Flow Count
  - Total Normal Flow Count
  - Total Large Flow Count
  - Total Managed Large Flow Count
  - Total Unmanaged Large Flow Count
  - Base Policy:
    - Total Large Flow Count
    - Total Managed Large Flow Count
    - Total Unmanaged Large Flow Count
  - Extended Policy:
    - Total Large Flow Count
    - Total Managed Large Flow Count
    - Total Unmanaged Large Flow Count

- Total IO Bytes
- Total Large Flow Bytes
- Total Recovered Capacity Bytes
- Total Recovered Capacity ms

- UDP Traffic Optimization Flows:
  - Active Normal Flow Count
  - Active Large Flow Count
  - Active Managed Large Flow Count
  - Active Unmanaged Large Flow Count
  - Base Policy:
    - Active Large Flow Count
    - Active Managed Large Flow Count
    - Active Unmanaged Large Flow Count
  - Extended Policy:
    - Active Large Flow Count
    - Active Managed Large Flow Count
    - Active Unmanaged Large Flow Count

-
  - Total Normal Flow Count
  - Total Large Flow Count
  - Total Managed Large Flow Count
  - Total Unmanaged Large Flow Count
  - Base Policy:
    - Total Large Flow Count
    - Total Managed Large Flow Count
    - Total Unmanaged Large Flow Count
  - Extended Policy:
    - Total Large Flow Count
    - Total Managed Large Flow Count
    - Total Unmanaged Large Flow Count
  - Total IO Bytes:

- Total Large Flow Bytes
- Total Recovered Capacity Bytes
- Total Recovered Capacity ms

show active-charging traffic-optimization info

This show command has been introduced in Exec Mode, where:

- **traffic-optimization** – Displays all traffic optimization options.
- **info** – Displays Cisco Ultra Traffic Optimization engine information.

The output of this CLI command displays the version, mode, and configuration values.

Following are the new fields/counters:

- Version:
- Mode:
- Configuration:
  - Data Records (TODR)
  - Statistics Options
  - EFD Flow Cleanup Interval
  - Statistics Interval

show active-charging traffic-optimization policy

On executing the above command, the following new fields are displayed for the Multi-Policy Support feature:

- Policy Name
- Policy-Id
- Bandwidth-Mgmt
  - Backoff-Profile
  - Min-Effective-Rate
  - Min-Flow-Control-Rate
- Extended-Bandwidth-Mgmt
  - Backoff-Profile
  - Min-Effective-Rate
  - Min-Flow-Control-Rate
- Curbing-Control
  - Time

    - Rate
    - Max-phases
    - Threshold-Rate
- Extended-Curbing-Control
    - Time
    - Rate
    - Max-phases
    - Threshold-Rate
- Heavy-Session
    - Threshold
    - Standard-Flow-Timeout
- Extended-Heavy-Session
    - Threshold
    - Standard-Flow-Timeout
- Link-Profile
    - Initial-Rate
    - Max-Rate
    - Peak-Lock
- Extended-Link-Profile
    - Initial-Rate
    - Max-Rate
    - Peak-Lock
- Session-Params
    - Tcp-Ramp-Up
    - Udp-Ramp-Up
- Extended-Session-Params
    - Tcp-Ramp-Up
    - Udp-Ramp-Up

Bulk Statistics

The following bulk statistics are added in the ECS schema to support Large and Managed flows:

Bulk Statistics	Description
tcp-active-base-large-flow-count	Indicates the number of TCP active-base-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-base-managed-large-flow-count	Indicates the number of TCP active-base-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-base-unmanaged-large-flow-count	Indicates the number of TCP active-base-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-ext-large-flow-count	Indicates the number of TCP active-ext-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-ext-managed-large-flow-count	Indicates the number of TCP active-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-ext-unmanaged-large-flow-count	Indicates the number of TCP active-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-base-large-flow-count	Indicates the number of TCP total-base-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-base-managed-large-flow-count	Indicates the number of TCP total-base-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-base-unmanaged-large-flow-count	Indicates the number of TCP total-base-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-ext-large-flow-count	Indicates the number of TCP active-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-ext-managed-large-flow-count	Indicates the number of TCP total-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-ext-unmanaged-large-flow-count	Indicates the number of TCP total-ext-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-base-large-flow-count	Indicates the number of UDP active-base-large-flow-count count for Cisco Ultra Traffic Optimization.

Bulk Statistics	Description
udp-active-base-managed-large-flow-count	Indicates the number of UDP active-base-managed-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-base-unmanaged-large-flow-count	Indicates the number of UDP active-base-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-ext-large-flow-count	Indicates the number of UDP active-ext-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-ext-managed-large-flow-count	Indicates the number of UDP active-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-ext-unmanaged-large-flow-count	Indicates the number of UDP active-ext-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-base-large-flow-count	Indicates the number of UDP total-base-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-base-managed-large-flow-count	Indicates the number of UDP total-base-managed-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-base-unmanaged-large-flow-count	Indicates the number of UDP total-base-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-ext-large-flow-count	Indicates the number of UDP total-ext-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-ext-managed-large-flow-count	Indicates the number of UDP total-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-ext-unmanaged-large-flow-count	Indicates the number of UDP total-ext-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-normal-flow-count	Indicates the number of TCP active-normal-flow count for Cisco Ultra Traffic Optimization.
tcp-active-large-flow-count	Indicates the number of TCP active-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-managed-large-flow-count	Indicates the number of TCP active-managed-large-flow count for Cisco Ultra Traffic Optimization.

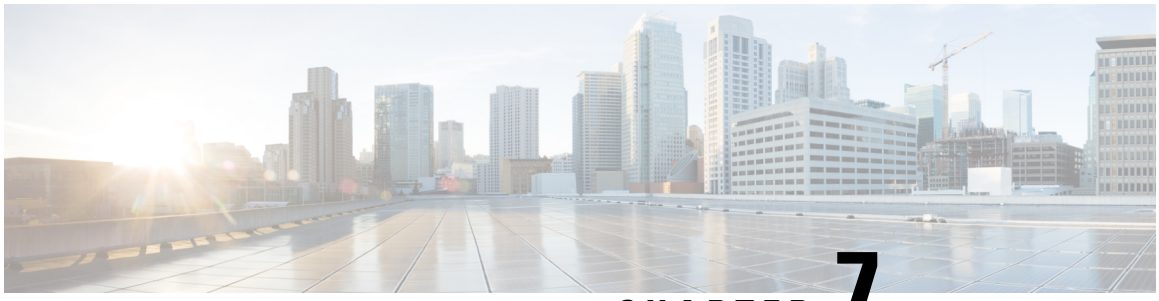
Bulk Statistics	Description
tcp-active-unmanaged-large-flow-count	Indicates the number of TCP active-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-normal-flow-count	Indicates the number of TCP total-normal-flow count for Cisco Ultra Traffic Optimization.
tcp-total-large-flow-count	Indicates the number of TCP total-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-managed-large-flow-count	Indicates the number of TCP total-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-unmanaged-large-flow-count	Indicates the number of TCP total-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-io-bytes	Indicates the number of TCP total-IO bytes for Cisco Ultra Traffic Optimization.
tcp-total-large-flow-bytes	Indicates the number of TCP total-large-flow bytes for Cisco Ultra Traffic Optimization.
tcp-total-recovered-capacity-bytes	Indicates the number of TCP total-recovered capacity bytes for Cisco Ultra Traffic Optimization.
tcp-total-recovered-capacity-ms	Indicates the number of TCP total-recovered capacity ms for Cisco Ultra Traffic Optimization.
udp-active-normal-flow-count	Indicates the number of UDP active-normal-flow count for Cisco Ultra Traffic Optimization.
udp-active-large-flow-count	Indicates the number of UDP active-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-managed-large-flow-count	Indicates the number of UDP active-managed-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-unmanaged-large-flow-count	Indicates the number of UDP active-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-normal-flow-count	Indicates the number of UDP total-normal-flow count for Cisco Ultra Traffic Optimization.
udp-total-large-flow-count	Indicates the number of UDP total-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-managed-large-flow-count	Indicates the number of UDP total-managed-large-flow count for Cisco Ultra Traffic Optimization.

Bulk Statistics	Description
udp-total-unmanaged-large-flow-count	Indicates the number of UDP total-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-io-bytes	Indicates the number of UDP total-IO bytes for Cisco Ultra Traffic Optimization.
udp-total-large-flow-bytes	Indicates the number of UDP total-large-flow bytes for Cisco Ultra Traffic Optimization.
udp-total-recovered-capacity-bytes	Indicates the number of UDP total-recovered capacity bytes for Cisco Ultra Traffic Optimization.
udp-total-recovered-capacity-ms	Indicates the number of UDP total-recovered capacity ms for Cisco Ultra Traffic Optimization.
tcp-uplink-drop	Indicates the number of TCP uplink-drop for Cisco Ultra Traffic Optimization.
tcp-uplink-hold	Indicates the number of TCP uplink-hold for Cisco Ultra Traffic Optimization.
tcp-uplink-forward	Indicates the number of TCP uplink-forward for Cisco Ultra Traffic Optimization.
tcp-uplink-forward-and-hold	Indicates the number of TCP uplink-forward and hold for Cisco Ultra Traffic Optimization.
tcp-uplink-hold-failed	Indicates the number of TCP uplink-hold-failed for Cisco Ultra Traffic Optimization.
tcp-uplink-bw-limit-flow-sent	Indicates the number of TCP uplink-bw limit-flow sent for Cisco Ultra Traffic Optimization.
tcp-dnlink-drop	Indicates the number of TCP downlink-drop for Cisco Ultra Traffic Optimization.
tcp-dnlink-hold	Indicates the number of TCP downlink-hold for Cisco Ultra Traffic Optimization.
tcp-dnlink-forward	Indicates the number of TCP downlink-forward for Cisco Ultra Traffic Optimization.
tcp-dnlink-forward-and-hold	Indicates the number of TCP downlink-forward and hold for Cisco Ultra Traffic Optimization.
tcp-dnlink-hold-failed	Indicates the number of TCP downlink-hold-failed for Cisco Ultra Traffic Optimization.
tcp-dnlink-bw-limit-flow-sent	Indicates the number of TCP downlink-bw limit-flow sent for Cisco Ultra Traffic Optimization.

Bulk Statistics	Description
tcp-dnlink-async-drop	Indicates the number of TCP downlink-async-drop for Cisco Ultra Traffic Optimization.
tcp-dnlink-async-hold	Indicates the number of TCP downlink-async-hold for Cisco Ultra Traffic Optimization.
tcp-dnlink-async-forward	Indicates the number of TCP downlink-async-forward for Cisco Ultra Traffic Optimization.
tcp-dnlink-async-forward-and-hold	Indicates the number of TCP downlink-async-forward and hold for Cisco Ultra Traffic Optimization.
tcp-dnlink-async-hold-failed	Indicates the number of TCP downlink-async-hold-failed for Cisco Ultra Traffic Optimization.
tcp-process-packet-drop	Indicates the number of TCP process-packet-drop for Cisco Ultra Traffic Optimization.
tcp-process-packet-hold	Indicates the number of TCP process-packet-hold for Cisco Ultra Traffic Optimization.
tcp-process-packet-forward	Indicates the number of TCP process-packet-forward for Cisco Ultra Traffic Optimization.
tcp-process-packet-forward-failed	Indicates the number of TCP process-packet-forward-failed for Cisco Ultra Traffic Optimization.
tcp-process-packet-forward-and-hold	Indicates the number of TCP process-packet-forward and hold for Cisco Ultra Traffic Optimization.
tcp-process-packet-forward-and-hold-failed	Indicates the number of TCP process-packet-forward and hold-failed for Cisco Ultra Traffic Optimization.
tcp-pkt-copy	Indicates the number of TCP packet-copy for Cisco Ultra Traffic Optimization.
tcp-pkt-Copy-failed	Indicates the number of TCP packet-copy-failed for Cisco Ultra Traffic Optimization.
tcp-process-pkt-copy	Indicates the number of TCP process-packet-copy for Cisco Ultra Traffic Optimization.
tcp-process-pkt-copy-failed	Indicates the number of TCP process-packet-copy-failed for Cisco Ultra Traffic Optimization.
tcp-process-pkt-no-packet-found-action-forward	Indicates the number of TCP process packet, no packet found, and action forward for Cisco Ultra Traffic Optimization.
tcp-process-pkt-no-packet-found-forward-and-hold	Indicates the number of TCP process packet, no packet found, action forward and hold for Cisco Ultra Traffic Optimization.

Bulk Statistics	Description
tcp-process-pkt-no-packet-found-action-drop	Indicates the number of TCP process packet, no packet found, action drop for Cisco Ultra Traffic Optimization.
tcp-todrs-generated	Indicates the number of TCP TODRs generated for Cisco Ultra Traffic Optimization.
udp-uplink-drop	Indicates the number of UDP uplink-drop for Cisco Ultra Traffic Optimization.
udp-uplink-hold	Indicates the number of UDP uplink-hold for Cisco Ultra Traffic Optimization.
udp-uplink-forward	Indicates the number of UDP uplink-forward for Cisco Ultra Traffic Optimization.
udp-uplink-forward-and-hold	Indicates the number of UDP uplink-forward and hold for Cisco Ultra Traffic Optimization.
udp-uplink-hold-failed	Indicates the number of UDP uplink-hold failed for Cisco Ultra Traffic Optimization.
udp-uplink-bw-limit-flow-sent	Indicates the number of UDP uplink-bw limit-flow sent for Cisco Ultra Traffic Optimization.
udp-dnlink-drop	Indicates the number of UDP downlink-drop for Cisco Ultra Traffic Optimization.
udp-dnlink-hold	Indicates the number of UDP downlink-hold for Cisco Ultra Traffic Optimization.
udp-dnlink-forward	Indicates the number of UDP downlink-forward for Cisco Ultra Traffic Optimization.
udp-dnlink-forward-and-hold	Indicates the number of UDP downlink-forward and hold for Cisco Ultra Traffic Optimization.
udp-dnlink-hold-failed	Indicates the number of UDP downlink-hold failed for Cisco Ultra Traffic Optimization.
udp-dnlink-bw-limit-flow-sent	Indicates the number of UDP downlink-bw limit-flow sent for Cisco Ultra Traffic Optimization.
udp-dnlink-async-drop	Indicates the number of UDP downlink-async-drop for Cisco Ultra Traffic Optimization.
udp-dnlink-async-hold	Indicates the number of UDP downlink-async-hold for Cisco Ultra Traffic Optimization.
udp-dnlink-async-forward	Indicates the number of UDP downlink-async-forward for Cisco Ultra Traffic Optimization.
udp-dnlink-async-forward-and-hold	Indicates the number of UDP downlink-async-forward and hold for Cisco Ultra Traffic Optimization.

Bulk Statistics	Description
udp-dnlink-async-hold-failed	Indicates the number of UDP downlink-async-hold failed for Cisco Ultra Traffic Optimization.
udp-process-packet-drop	Indicates the number of UDP process-packet-drop for Cisco Ultra Traffic Optimization.
udp-process-packet-hold	Indicates the number of UDP process-packet-hold for Cisco Ultra Traffic Optimization.
udp-process-packet-forward	Indicates the number of UDP process-packet-forward for Cisco Ultra Traffic Optimization.
udp-process-packet-forward-failed	Indicates the number of UDP process-packet-forward failed for Cisco Ultra Traffic Optimization.
udp-process-packet-forward-and-hold	Indicates the number of UDP process-packet-forward and hold for Cisco Ultra Traffic Optimization.
udp-process-packet-forward-and-hold-failed	Indicates the number of UDP process-packet-forward and hold failed for Cisco Ultra Traffic Optimization.
udp-pkt-copy	Indicates the number of UDP packet-copy for Cisco Ultra Traffic Optimization.
udp-pkt-Copy-failed	Indicates the number of UDP packet-copy-failed for Cisco Ultra Traffic Optimization.
udp-process-pkt-copy	Indicates the number of UDP process-packet-copy for Cisco Ultra Traffic Optimization.
udp-process-pkt-copy-failed	Indicates the number of UDP process-packet-copy failed for Cisco Ultra Traffic Optimization.
udp-process-pkt-no-packet-found-action-forward	Indicates the number of UDP process packet, no packet found, action forward for Cisco Ultra Traffic Optimization.
udp-process-pkt-no-packet-found-forward-and-hold	Indicates the number of UDP process packet, no packet found, action forward and hold for Cisco Ultra Traffic Optimization.
udp-process-pkt-no-packet-found-action-drop	Indicates the number of UDP process packet, no packet found, action drop for Cisco Ultra Traffic Optimization.
udp-todrs-generated	Indicates the number of UDP TODRs generated for Cisco Ultra Traffic Optimization.



CHAPTER 7

Dynamic Transport Selection based on Transaction or Origin-Host

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	Not applicable

Revision History

Revision Details	Release
First introduced **Important** This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.	21.22

Feature Description

Reliable and secure telecommunications systems are necessary for effectively managing national security incidents and emergencies. The National Security and Emergency Preparedness (NS/EP) is a set of voice, video, and data services that belong to services available from public packet-switched Service Providers and that provide priority services in support of NS/EP communications. The NS/EP communication systems include landline, wireless, broadcast, and cable television, radio, public safety systems, satellite communications, and the Internet.

Wireless Priority Services (WPS) is one of the NS/EP communications programs that provide personnel priority access and prioritized processing in all nationwide and several regional cellular networks, increasing the probability of call completion.

WPS users, also known as first responders, are responsible for the command and control functions that are critical to the management of response to national security and emergencies. When your network carries the traffic for WPS users' all the network elements individually and collectively must adhere to the following conditions:

- **Prioritization of Control Plane Traffic**:WPS user’s control plane traffic is prioritized over other subscribers between different Network Functions in the LTE Core.
- P1, P2, and P3 are the three priority levels available for WPS users:
  - P1 and P2 users are identified in HSS/PCRF and GW uses their priority (ARP) during default and dedicated bearer creation, modification, update, or deletion.
  - P1 and P2 WPS users are always treated as High Priority.
  - DSCP markings for prioritized user’s control plane IP packets is marked with DSCP=47 while all other users control packets IP packets is marked with DSCP=32
- **Diameter Interfaces**:
  - P-GW, Policy Change Rule Function (PCRF) and Diameter Routing Agent (DRA) uses the configuration of Diameter interfaces such as Gx and Rx interfaces to support policy and charging control for subscribers.
  - P-GW and SGW uses non-diameter interfaces such as S5, S8, S11, or S1U with its peer respectively.

Characteristics of Low and High Priority Channels for Diameter-based Interfaces

Low Priority channels indicate normal priority users and High Priority channels indicate WPS users during Differentiated Services Code Point (DSCP) markings. The peer connections towards DRA for PGW (Gx) is shown in the figure.

Figure 4: High-Level Overview of Low and High Priority Channels over Gx Interface

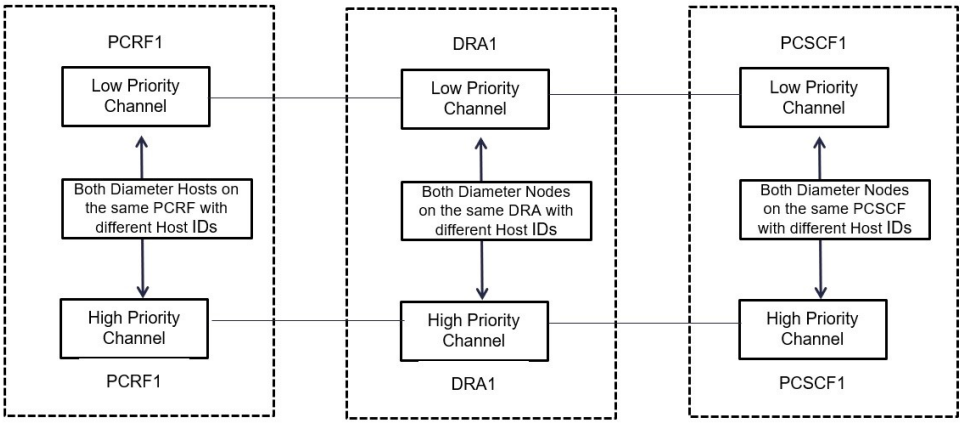


Table 1: Low and High Priority Channels on Gx Interface

Priority Channel	Diameter Interfaces	IP Layer DSCP	TCP Connection over IP layer	Diameter Host FQDN
Low Priority	Gx	Equal to 32	32 **Note** This channel is for non-WPS diameter messages but may carry WPS diameter messages in error scenarios, for example when all the Red Peers are down.	Not Modified Examples: 0 0 0 1-diamproxy. PGW-Gx', 'dra1', 'pcrf1
High Priority	Gx	Equal to 47	47	Specific to High Priority Examples: 0001-diamproxy. PGW-Gx-wps', ' dra1-wps', 'pcrf1-wps'.

Characteristics of Low Priority and High Priority Channels for S11, S5, or S8 interfaces

The S5 and S11 interfaces are GTPv2 based (which uses UDP as the transport protocol), Low and High Priority channels have the following characteristics.

Table 2: Low and High Priority Channels on Other Interfaces

Priority Channel	Diameter Interfaces	IP Layer DSCP	TCP Connection over IP layer	Diameter Host FQDN
Low Priority	S11 or S5 or S8	32	—	—
High Priority	S11 or S5 or S8	47	—	—

How it Works

The following is a high-level overview of how this feature works. The PGW selects either High Priority or Low Priority channels based on the **wps profile**. If APN name, QCI, and ARP are matched as shown in the table, session is detected as WPS session at IMSA.

Table 3: WPS Message Prioritization based on APN, QCI, and ARP Priority Level

APN Name	QCI	ARP	DSCP
IMS	66,69	*	47
IMS	*	1,2	47
IMS	8	3	47
IMS	9	5	47
IMS	2	4	47

The following table explains the process of dynamic transport selection based on transaction or Origin Host:

Table 4: Procedure

Process	Description
Identifying WPS and Non-WPS users	• Use the CLI command **priority-select** at diameter end point to enable or disable WPS users. This CLI command is at policy-control configuration in IMS-authorization service. • PGW receives Create session request with every eMPS session is tagged with the Allocation and Retention Priority (ARP) value. • PGW verifies whether that ARP value is matching the WPS. • Session Manager checks whether the received ARP value matches the eMPS session or not. • If the above criteria of matching eMPS session and enabling of priority select is met, then, the user is called as WPS user. Else, the user is called as Normal user.
Prioritizing Session	At Policy Change Rule Function (PCRF), you can define two priority levels such as Low Priority session for non-WPS users and high priority session for WPS users. • **Always-On WPS Sessions**: GTPv2-S5, GTPv2-S11, GTPv2-S8, and Gx sessions, which belong to WPS users are always treated as high priority. • **On-Demand WPS Sessions**: GTPv2-S5, GTPv2-S11, GTPv2-S8, and Gx sessions, which belong to Non-WPS users can be uplifted to higher priority (lower ARP PL value) dynamically. The most common example of this is when a WPS user makes a WPS call (that is initiated by dialing a call starting with *272) to non-WPS user. These types of sessions are called On-Demand eMPS sessions. • Control plane Gx messages that belong to high priority sessions uses High Priority channels. • Control plane Gx messages that belong to nonhigh priority sessions uses high priority channels.

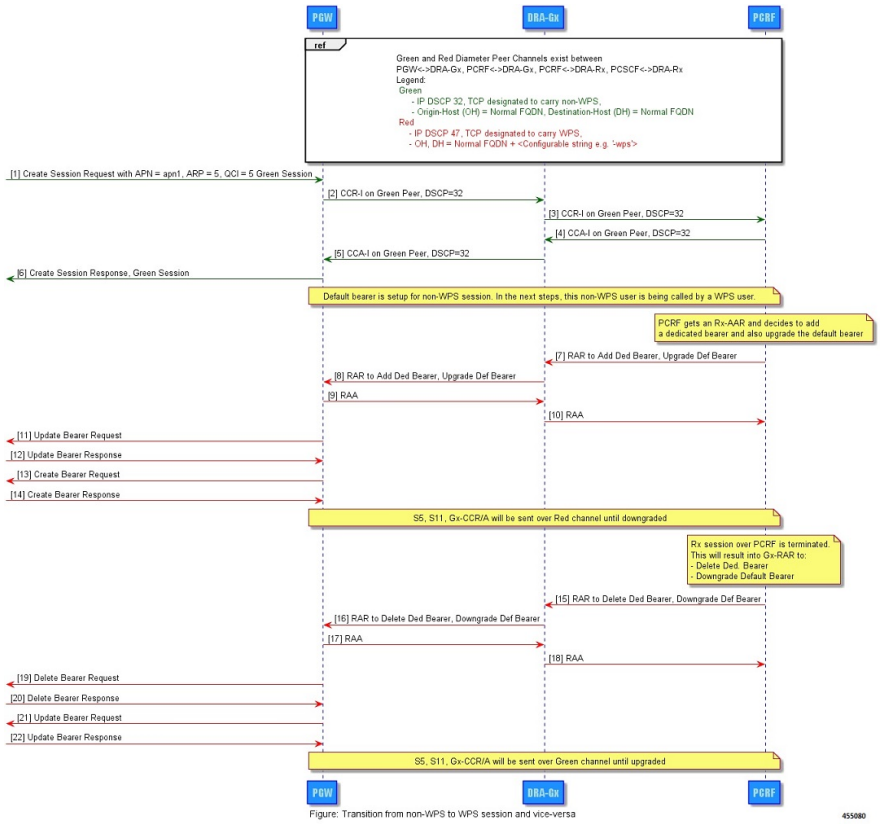
Process	Description
Differentiating paths between normal users and WPS users	On Gx interface, different connections are made to form the second path at the CLI level: • P-GW creates two sets of DRA peer connections. One set for higher priority and other for normal priority messages. • P-GW sends CCR-Initial and CCR-Update Gx messages on specific pair of connections based on type of session (WPS session or Non-WPS session). • After the peer is configured with **priority-select** flag, all CCR messages for WPS session are initiated over High Priority peer. If P-GW identifies the users as a WPS user, it binds to the high priority peer with DSCP marking as 47. However, non-WPS subscriber's Diameter message is initiated over Low Priority peer and the DSCP is set to 32. **Note** If the dscp configuration for peer is not specified, then global dscp value configured under diameter endpoint is used. If global dscp value under diameter endpoint is not configured, then dscp value "0" is used. The following actions are performed before triggering CCR-I message with respect to WPS users: • Selection of High Priority peer. • If an existing AVP string is configured in peer configuration, Origin Host ID is appended with a string. If string is not configured, default **-wps** string is appended to Origin Host ID. • DRA/PCRF responds with CCA-I over high priority channel upon reception of the CCR-I. The subsequent messages follow the high priority channel.

The key call flow for this feature include transitioning from non-WPS to WPS Session and PCRF initiated Bearer Deletion.

If CSR (Creation Session Request) has one bearer and ARP does not match with ARP defined in eMPS profile, the Session is treated as low priority Session. All Gx messages follow low priority channel to PCRF. However, if any dedicated bearer triggered by Mobile has ARP matched with ARP defined in eMPS profile, low priority session is transitioned to WPS session.

Note In this document Low priority channel and Green channel are used interchangeably and the same is true for Red and High priority channel.

Figure 5: Transitioning from Non-WPS to WPS Session and Vice Versa



Note In the StarOS 21.22 release, WPS session is the same as eMPS session and is based on eMPS profile.

Table 5: Procedure

Step	Description
1 through 6	Low Priority channels are used for a non-WPS session.
7 through 14	P-GW receives RAR with an ARP defined in eMPS profile, the following operations are performed. • Internally, the session is updated to an eMPS session. • P-GW identifies high priority peer and appends the string "-wps" (or configured origin-host-suffix string) to Origin Host AVP in the outgoing messages. The subsequent outgoing messages on Gx, S5 and S11 will follow the high priority channel until the session is downgraded again.
15 through 22	P-GW receives RAR with ARP not defined in eMPS profile, the session is downgraded from eMPS (WPS) session to non-WPS.

Step	Description
Note	When the session is in eMPS state and if there is no High priority Gx peer available, a Low Priority Peer shall be used for Gx traffic. If there is no peer is available, then the call gets dropped

Configuring Dynamic Transport Selection based on Transaction or Origin-Host

This section describes how to configure the Dynamic Transport Selection based on Transaction or Origin-Host.

1. Configuring eMPS Profile
2. Associating an eMPS profile with P-GW Service
3. Enabling Gx Prioritization for eMPS Sessions
4. Enabling WPS feature and priority services for APN services

Configuring eMPS Profile

This section describes how to configure eMPS profile. Use the following commands to configure eMPS profile, which is used to identify/mark a bearer/session as an eMPS bearer/session

```
configure
   [ no ] emps-profile emps_profile_name -noconfirm
      [ no ] earp { [string value] }
      [ no ] dscp-marking { dscp-value }
      end
```

Notes:

- **emps-profile emps_profile_name**: Configures eMPS profile for defining attributes of an eMPS session. The *emps_profile_name* is a string of size from 1 to 63.
- **-noconfirm**: Creates a new eMPS profile without prompting for confirmation.
- **earp**: Configures a maximum of 8 eARP priority level (PL) values so that sessions with configured eARP priority values can be marked as eMPS sessions. Maximum of 8 eARP values can be configured under an eMPS profile.
- **dscp-marking**: Specifies the DSCP value to be applied to eMPS sessions. The dscp_value is a hexadecimal number between 0x0 and 0x3F.

Note For supplemental information related to eMPS profile configuration (configuring the eMPS ARPs, which are used to identify a bearer/session as an eMPS bearer/session), and eMPS statistics, refer to the *Expanded Prioritization for VoLTE/Emergency Calls* chapter in the *P-GW Administration Guide or the SAEGW Administration Guide*.

Associating an eMPS-Profile with P-GW and S-GW Service

This section describes how to associate an eMPS profile with P-GW and S-GW services.

```
configure
  context context_name
    pgw-service service_name
      associate emps-profile emps_profile_name
      end
```

```
configure
  context context_name
    Sgw-service service_name
      associate emps-profile emps_profile_name
      end
```

Notes:

- **no**: Disables a emps-profile association with P-GW or S-GW service.
- **associate emps-profile***emps_profile_name*: Associates an eMPS profile with either P-GW or S-GW service.

Enabling Gx Prioritization for eMPS Sessions and Wireless Priority Services

This section describes how to enable Gx prioritization levels for eMPS sessions

```
configure
  context context_name
    [ no ]ims-auth-service service_name
      [ no ] policy control
         [ no ] diameter origin endpoint endpoint_name priority-select
         [ no ] diameter session-prioritization
      end
```

Notes:

- **priority-select**: Enables Wireless Priority Services (WPS) for the selected IMS authorization service.

  Note The **priority-select** keyword is mandatory for WPS feature.

- **[no] diameter session-prioritization**: Enables or disables Gx signalling prioritization for eMPS sessions:
  - By default, the **diameter session-prioritization** CLI command is disabled and Gx messages does not get prioritized based on WPS value.
  - If previously configured, use the **no diameter session-prioritization** CLI command to set the default behavior
  - The **diameter session-prioritization** CLI takes effect when Gx, along with eMPS profile, is enabled in the configuration.

- The **diameter session-prioritization**configuration attaches DRMP-0 AVP to Diameter Messages going over the High Priority channel. DRA/PCRF takes appropriate actions based on DRMP-0, incase fallback from High Priority to Low Priority channel takes place on P-GW to DRA or DRA to PCRF Gx links.

Note Diameter session-prioritization is an existing CLI and it is not mandatory for configuring WPS feature.

Differentiating Low Priority and High Priority Peers

This section describes how to differentiate between low and priority peers. Priority Endpoint configuration under policy-control ensures WPS feature is only applicable to IMS-auth-service under policy control area. It is applicable for Gx interface.

```
configure
  context context_name
     [ no] diameter endpoint pgw-gx
      peer PGW-Gx-green-1  realm_address ipv4 address | ipv6 address portport_number

       peer PGW-Gx-wps-1  realm_address ipv4 address | ipv6 address port port_number
priority-select origin-host-suffix value dscp value
     end
```

NOTES:

- **priority-select**: Defines peer as high priority wps peer. It is optional to configure to both parameters. Following conditions apply during peer configuration:
  - If **priority-select** is not configured, peer is not treated as high priority **wps** peer.
  - **origin-host-suffix**: If **priority-select** is set for a peer, it is treated as **wps** peer. If **Origin-host-suffix** is configured for **wps** peer, configured string is appended to Origin Host ID otherwise, default **-wps** string is appended to Origin Host ID (for example, pgw-gx-wps).
  - **dscp**: If DSCP is not configured for high priority peer, endpoint level DSCP is filled in IP packets towards DRA/PCRF. Otherwise, configured DSCP is filled in IP packet.

Monitoring and Troubleshooting

This section describes troubleshooting information, show commands and Outputs, IMSA level statistics, diameter statistics, and Bulk statistics.

Show Commands and Outputs

Use this CLI command to view the output field details of `Rule Installation Failure` statistics, number of prioritized DRMP messages, WPS and Non-WPS session statistics.

show ims-authorization policy-control statistics

Use this CLI command to view the output field details of `Rule Installation Failure` statistics, number of prioritized DRMP messages, WPS and Non-WPS session statistics

Field	Description
DPCA WPS Session Stats	
Total Current Sessions	The total number of DPCA WPS session currently running on this system
Switched from Priority Chnl	Indicates the total subscribers moved from Wireless Priority to Normal
Switched to Priority Chnl	Indicates the total subscribers moved from Normal to Wireless Priority
DPCA WPS Message Stats	
Priority Channel Indicates message statistics for WPS session, which is sent or received on high priority channel.	
Total messages Received	Total policy control messages received for IMS authorization policy control.
Total Messages Sent	Total messages sent to IMS authorization policy control server.
Total CCR	Total Credit Control Request (CCR) messages received.
Total CCA	Total Credit Control Answer (CCA) messages sent in response to CCRs.
CCR-Initial	Total number of initial CCR messages received.
CCA-Initial	Total number of initial CCA messages sent in response to initial CCR messages.
CCA-Initial Accept	Total number of initial CCA messages accepted in response to initial CCR messages.
CCA-Initial Reject	Total number of initial CCA messages rejected in response to initial CCR messages.
CCA-Initial Dropped	Total number of CCA-I messages that are dropped due to S-GW restoration, DPCA is off, or not present, or if the IMSA session is in preservation mode.
CCA-Initial Timeouts	Total number of initial CCA messages timed out in response to initial CCR messages.
CCR-Update	Total number of Credit Control Request (CCR) messages received after initial CCR for update.
CCA-Update	Total Credit Control Answer (CCA) messages sent in response to update CCRs.

Field	Description
CCA-Update Timeouts	Total Credit Control Answer (CCA) messages sent in response to update CCRs but timed out.
CCA-Update Errors	Total number of errors in parsing the CCA-Update Message.
CCA-Update Dropped	Total number of CCA-U messages that are dropped due to S-GW restoration, DPCA is off, or not present, or if the IMSA session is in preservation mode.
CCR-Final	Total number of final CCR messages received to end application.
CCA-Final	Total number of final CCA messages sent in response to final CCR messages to end sessions.
CCA-Final Timeouts	Total number of final CCA messages sent in response to final CCR messages to end sessions but timed out.
CCA-Final Errors	Total number of errors in parsing the CCA-Terminate Message.
CCA-Final Dropped	Total number of CCA-T messages, which are dropped due to S-GW restoration, DPCA is off ,or not present, or if the IMSA session is in preservation mode.
ASR	Total number of Abort-Session-Requests (ASRs) received.
ASA	Total number of Abort-Session-Accept (ASA) messages sent in response to Abort-Session-Requests (ASRs).
RAR	Total number of Re-Auth-Requests (RARs) received for re-authorization..
RAA	Total number of Re-Auth-Requests(RARs) answered with Re-Auth-Answer (RAA) message.
RAR-CCR collision	Total number of Re-Auth-Request (RAR) messages received from PCRF when there is any outstanding Credit Control Request (CCR) message.
Non-Priority Channel	**Indicates message statistics for WPS session, which is supposed to be sent/received on Priority channel but sent/received on Non-priority channel**
Total messages Received	Total policy control messages received for IMS authorization policy control.
Total Messages Sent	Total messages sent to IMS authorization policy control server.
Total CCR	Total Credit Control Request (CCR) messages received.
CCR-Initial	Total number of initial CCR messages received.
CCA-Initial	Total number of initial CCA messages sent in response to initial CCR messages.

Field	Description
CCA-Initial Accept	Total number of initial CCA messages accepted in response to initial CCR messages.
CCA-Initial Reject	Total number of initial CCA messages rejected in response to initial CCR messages.
CCA-Initial Dropped	Total number of CCA-I messages which are dropped due to S-GW restoration, DPCA is off, or not present, or if the IMSA session is in preservation mode
CCA-Initial Timeouts	Total number of initial CCA messages timed out in response to initial CCR messages.
CCR-Update	Total number of Credit Control Request (CCR) messages received after initial CCR for update.
CCA-Update	Total Credit Control Answer (CCA) messages sent in response to update CCRs.
CCA-Update Timeouts	Total Credit Control Answer (CCA) messages sent in response to update CCRs but timed out.
CCA-Update Errors	Total number of errors in parsing the CCA-Update Message
CCA-Update Dropped	Total number of CCA-U messages which are dropped due to S-GW restoration, DPCA is off or not present or if the IMSA session is in preservation mode.
CCR-Final	Total number of final CCR messages received to end application.
CCA-Final	Total number of final CCA messages sent in response to final CCR messages to end session/s..
CCA-Final Timeouts	Total number of final CCA messages sent in response to final CCR messages to end session/s but timed out.
CCA-Final Errors	Total number of errors in parsing the CCA-Terminate Message.
CCA-Final Dropped	Total number of CCA-T messages which are dropped due to S-GW restoration, DPCA is off or not present or if the IMSA session is in preservation mode.
ASR	Total number of Abort-Session-Requests (ASRs) received.
ASA	Total number of Abort-Session-Accept (ASA) messages sent in response to Abort-Session-Requests (ASRs).
RAR	Total number of Re-Auth-Requests (RARs) received for re-authorization.
RAA	Total number of Re-Auth-Requests (RARs) answered with Re-Auth-Answer (RAA) message.

Field	Description
RAR-CCR collision	Total number of Re-Auth-Request (RAR) messages received from PCRF when there is any outstanding Credit Control Request (CCR) message.

show diameter peers full all

Use this CLI command to view peer details.

Field	Description
Priority Channel	Indicates peer is high priority or not. The options are: • **Yes**: Indicates peer is WPS. • **No**: Indicates Peer is Non-WPS.
DSCP Configured	Indicates the dscp value to be used in Gx IP Packet. • If configured, displays peer specific DSCP. • If not configured, then it will display the dscp configured in endpoint.

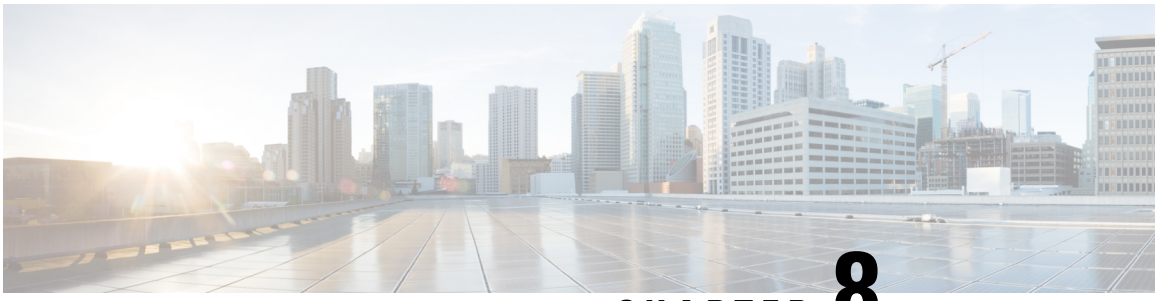
Bulk Statistics

This section provides information on the bulk statistics for the Dynamic Transport Selection based on Transaction or Origin-Host feature on P-GW

IMSA Schema

The following bulk statistics are included in the IMSA Schema to track high and low priority categories for WPS and Non-WPS users.

Counters	Description
dpca-imsa-total-session-priority-channel	Shows the cumulative number of Wireless Priority subscribers.
dpca - imsa - total - sessions-switched -from - priority - channel	Shows the cumulative number of subscribers moved from Wireless Priority to Normal.
dpca - imsa- total- sessions-switched - to- priority- channel	Shows the cumulative number of subscribers moved from Normal to Wireless Priority.



CHAPTER 8

Enabling EMM and ESM Cause Code Mapping

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
First Introduced	21.22

Feature Description

The User Equipment (UE) suffers failure, during attach process with an `EMM Attach Reject` message sent from MME to UE. When UE attach request is sent from MME to P-GW, the DNS server responds back with “Server failure", causing the MME to reject the UE attach request with the following error messages:

1. EMM Cause Code 17 `Network Failure`
2. ESM PDN Connectivity Reject Container message with ESM Cause Code 31 `Request Rejected Unspecified`.

To overcome the impact in MME 4G attach SR calculations, the Cause Codes introduced in the EMM Attach Reject/ESM PDN Connectivity Reject message to be EMM Cause Code 19 `ESM Failure` and ESM Cause Code 27 `Missing or Unknown APN`, instead of the current cause codes EMM 17 and ESM 31.

To overcome the UE attach request failure, the following new configuration commands are introduced:

1. `ESM-failure` with EMM Cause Code
2. `ESM-cause-code` with ESM Cause Code option `missing-or-unknown-apn`

Enabling EMM/ESM Cause Code Mapping (Cause Code 27) under MME-Service

Use the following configuration commands to enable cause code mapping under mme-service:

```
configure
   context context_name
     mme-service service_name { local-cause-code-mapping{
pgw-selection-failure( emm-cause-code ){ esm-failure ( esm-cause-code )(
 unknown-apn ) }}}
       end
```

Enabling EMM/ESM Cause Code Mapping (Cause Code 27) under Call Control Profile

Use the following configuration commands to enable cause code mapping under call control profile:

```
configure
     call-control-profile profile_name { local-cause-code-mapping{
pgw-selection-failure( emm-cause-code ){ esm-failure ( esm-cause-code )
( unknown-apn )}}}
       end
```

Show Commands and Outputs

show mme-service all

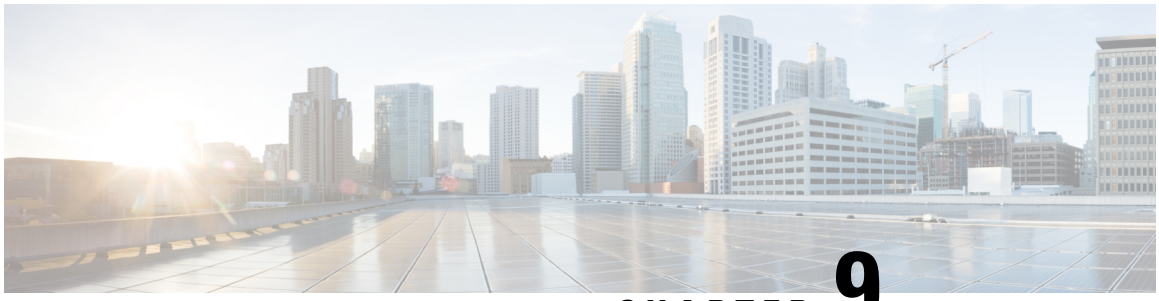
The output of this command displays the following newly introduced field:

ESM Failure (EMM-19)	Displays the EMM Cause Code of EMM Attach Reject/ESM PDN Connectivity Reject message.
Missing-or-Unknown-APN (ESM-27)	Displays the ESM Cause Code of EMM Attach Reject/ESM PDN Connectivity Reject message.

show call-control-profile full all

The output of this command displays the following newly introduced field:

ESM Failure (EMM-19)	Displays the EMM Cause Code of EMM Attach Reject/ESM PDN Connectivity Reject message.
Missing-or-Unknown-APN (ESM-27)	Displays the ESM Cause Code of EMM Attach Reject/ESM PDN Connectivity Reject message.



CHAPTER 9

Extraction of IPv4 Addresses Embedded in IPv6 Addresses

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
ECS is enhanced to support extraction of IPv4 Addresses Embedded in IPv6 Addresses feature.	21.22.8

Feature Description

Learning the IPv4 address, which is embedded in IPv6 address through DNS snooping, requires matching of IPv4 format against the address learnt from the DNS response.

In this release, IPv4 extraction is done by enhancing the existing Command Line Interface (CLI) for Well-known prefix and Network-specific prefix. For more information on prefixes, refer RFC6052 document.

After the required changes are done in the CLI, IPv4 address extraction happens and the lookup of IPv4 address is done using the learnt address pool.

Relationships to other Features

This feature is related to DNS Snooping feature. For more information about DNS Snooping feature, refer the *DNS Snooping* chapter in the *ECS Administration Guide.*

License Requirements

The Extraction of IPv4 Addresses Embedded in IPv6 Addresses requires the same DNS Snooping license. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

How it Works

The following procedure describes the steps to be followed for IPv4 address extraction:

1. P-GW monitors all responses sent to the UE.
2. P-GW snoops only the DNS response and identifies all the IP addresses resulting from the DNS response.
3. The first data packet from IPv4 device reaches P-GW.
4. The Session Manager receives data indication and routes the packet to the ACS manager.
5. The ACS manager analyzes the packet and assigns data session for the flow.
6. Prefix matching is done based on the configured prefix.

Based on the matching, IPv4 address is extracted and it is stored in the ACS data session. Then, IPv4 address starts the lookup in the IPv4 address pool and if it matches, then the traffic is matched with the DNS snooping rule. If match does not happen, then it starts to check for other rules.

Restrictions

This section identifies the restrictions to be applied in CLI for IPv4 address extraction.

Prefix-Set Restrictions:

- Allows network-specific prefixes, well-known prefixes but restricts other prefixes.
- Restricts configuring multiple mask values under the same prefix-set.

- Restricts prefix removal from prefix-set, if the same prefix-set is associated with rule base-strip CLI.
- Restricts prefix-set removal, if the same prefix-set is associated with rule base-strip CLI.

Rule base Restrictions:

- Allows network-specific prefixes, well-known prefixes but restrict other prefixes.
- Restricts strip CLI configuration, if rulebase prefix length is not matched to the associated prefix-set mask value.
- Restricts strip CLI configuration, if the rule base associated prefix-set is invalid.
- Restricts strip CLI configuration, if the available prefix-set is empty.

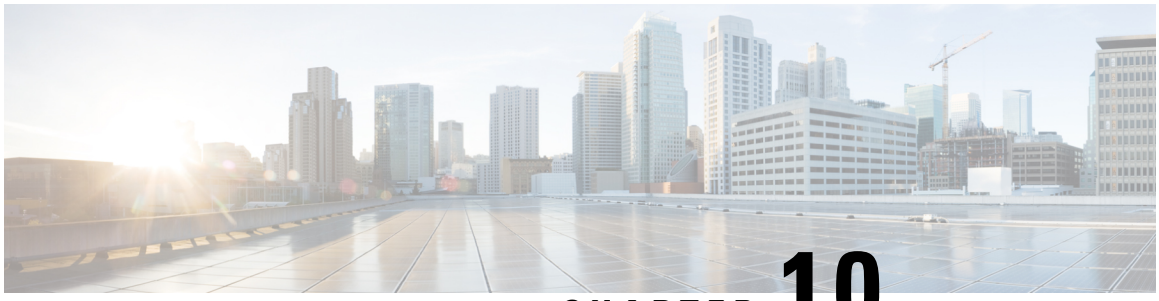
Associating Rulebase to Prefix-Set

Use the following configuration to associate rulebase to the prefix-set.

```
configure
  active-charging service ecs_service_name
    prefix-set prefix_set_name
      exit
    rulebase <rulebase_name>
      strip server-ipv6 prefix_length prefix-set prefix_set_name
      exit
```

NOTES:

- **strip server-ipv6** : Matches the prefix of server IPv6 address with the configured prefixset and prefix length. If match is found then extracts the IPv4 address from the server IPv6 address.
- *prefix_length*: Enter values 32,40,48,56,64 or 96.
- **prefix-set**: Configures the active configuration for Well-known prefix or Netowrk-specific prefix. You can configure a maximum of 10 IPv6 prefixes in a prefix-set.



CHAPTER 10

Non-IP PDN Support

This chapter describes the support of Non-IP PDN on P-GW and S-GW.

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• C-SGN • P-GW • S-GW
Applicable Platform(s)	• UGP • VPC-DI • VPC-SI
Feature Default	Disabled - License Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
Non IP UE P-GW support for SGi through RADIUS is tested on P-GW. This feature is tested and qualified on VPC-DI platform.	21.22
S-GW CDR support is added for Non-IP PDN subscribers.	21.13
The feature is tested and qualified on the ASR 5500 platform. A new PDP Type, Non-IP, is introduced along with the existing IPv4, IPv6, and IPv4v6 in S-GW CDR. Volume traffic fields are also updated for Non-IP PDN subscribers.	21.3
First introduced.	N5.1 (21.1.V0)

Feature Description

There are specific protocol optimizations already defined for low-power networking (For example, IPv6 over Low-power Wireless Personal Area Networks - 6LoWPAN). These protocol adaptations provided efficient ways of header compression and operation optimization to allow effective transmission of data with small frame size. Due to this, some of the Cellular Internet of Things (CIoT) devices may not use normal IP services. Therefore, it is useful to support a Non-IP PDN connection to allow such protocol to be used by the CIoT UE toward the Non-IP protocols destination node, like Application Server (AS) or a Non-IP gateway. The C-SGN/P-GW, in this case, can act as a transparent passthrough by a direct forwarding interface between itself and the AS or Non-IP gateway, and the CIoT UE can interact with the specific Non-IP destination node directly using appropriate protocols.

As part of this feature, along with Non-IP PDN, support is also added for extended Protocol Configuration Options (ePCO) IE at P-GW, and S-GW. Support is also added for Radius authentication and radius accounting for NoN-IP UE with 3GPP compliant Radius dictionary.

How It Works

Support for the SGi based delivery of Non-IP data can be used by any UE. The P-GW decides at PDN connection establishment, based on pre-configuration, which point-to-point (PtP) tunneling technique is used for the SGi based delivery between the P-GW and the AS.

SGi PtP tunneling based on UDP/IP

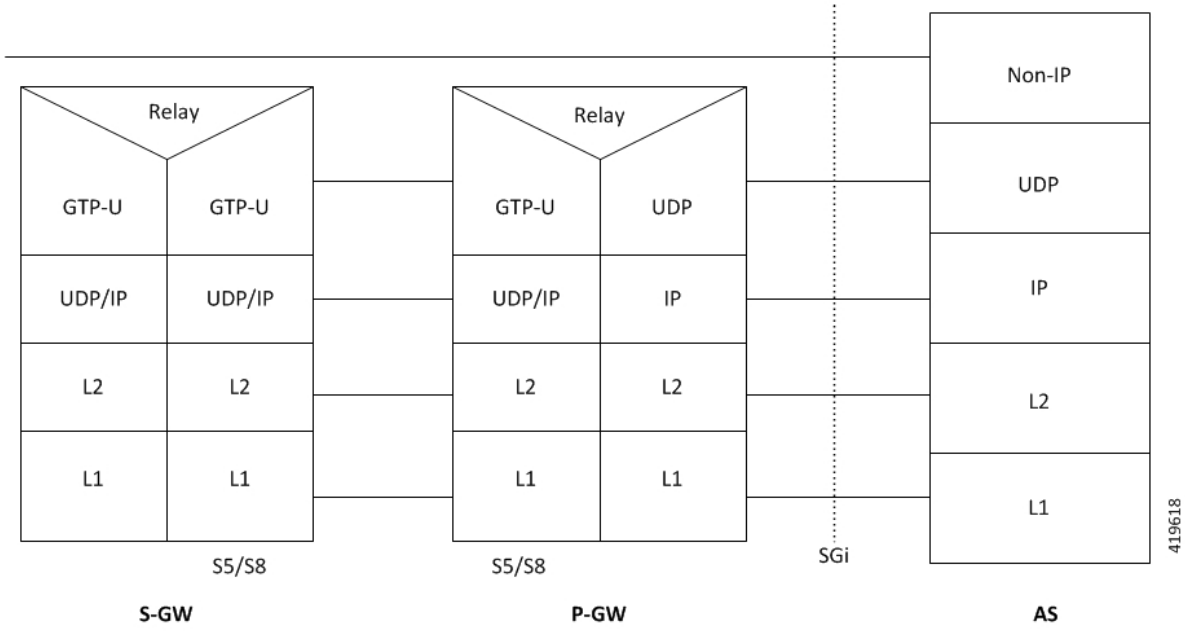
A PtP tunnel is used by the P-GW toward the AS. The tunnel parameters (that is, destination IP address and UDP port) for SGi PtP tunneling based on UDP/IP are pre-configured on the P-GW. The IP address allocation procedure for PDN connections is performed locally by the P-GW based on APN configuration. And, according

to 3GPP defined existing IP address allocation procedures, only single IP address is used (that is, both IPv4 and IPv6 addresses are not allocated).

The P-GW acts as a transparent forwarding node for the payload between the UE and the AS. For uplink Non-IP data, the P-GW forwards the received data to the AS over the SGi PtP tunnel using UDP/IP encapsulation. For downlink Non-IP data, the AS sends the data using UDP/IP encapsulation with the IP address of the UE and the 3GPP defined UDP port for "Non-IP" data. The P-GW decapsulates the received data (that is, removes the UDP/IP headers) and forwards the data to S-GW on the GTP-U tunnel, identified by the IP address of the UE, for delivery to the UE.

The P-GW performs the IP-related operations but the IP address or IP prefix is not provided to the UE. For IPv6, the P-GW assigns an Interface Identifier for the PDN connection. The allocated IP address or IPv6 prefix identifies the PDN connection of the UE.

The following image illustrates the protocol configuration for Non-IP data (user plane) using SGi PtP tunneling.



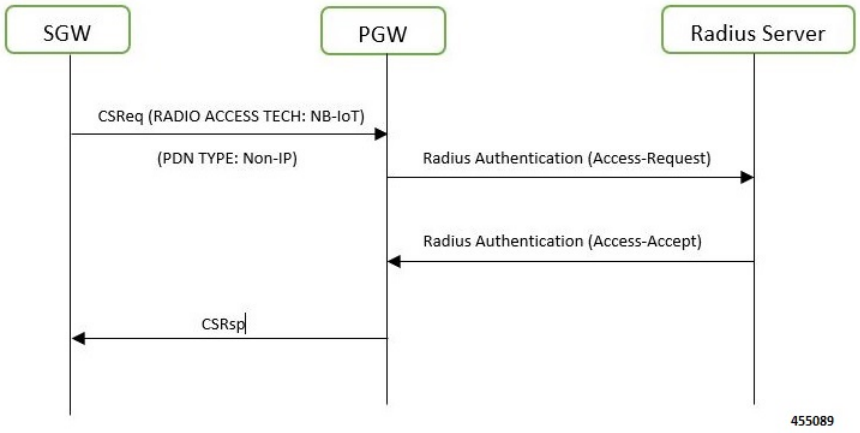
Important For Non-IP data, IP protocol-related functionalities are not applicable.

SGi based delivery of Non-IP data is used by any UE. The P-GW decides at PDN connection establishment, based on pre-configuration, where a point-to-point (PtP) tunneling technique is used for the SGi-based delivery between the P-GW and the AS. Radius authentication and radius accounting are supported for Non-IP UE with 3GPP compliant radius dictionary.

Radius Authentication and Accounting Support at P-GW

P-GW supports Radius authentication. Following call flow describes Radius authentication workflow.

Figure 6: Call Flow



Following call flow describes the radius accouting workflow at P-GW.

Figure 7: Call flow

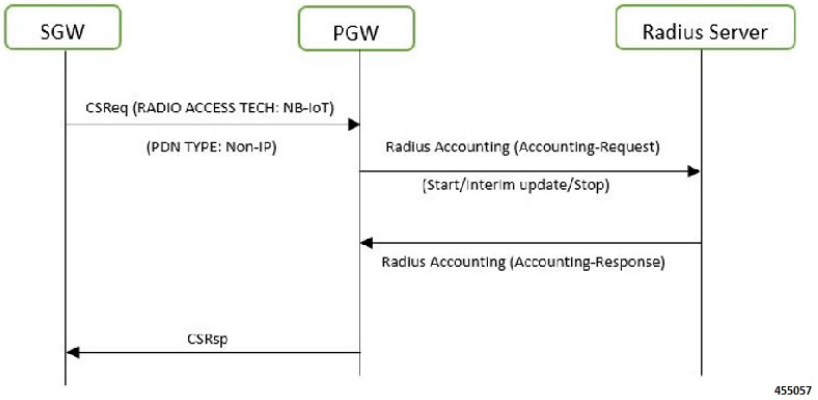


Table 6: Procedure

Step	Description
1	P-GW sends radius accounting start to radius server when it receives an NB-IOT/EUTRAN call with PDN type as Non-IP.
2	PGW continously sends radius accounting interim-updates to radius server after configured timer expiration.
3	Finally, it sends a radius accounting stop to radius server when the subscriber is detached

Inter-RAT and Intra-RAT Handovers for Non-IP PDNs

The following table shows the current behavior of Inter-RAT and Intra-RAT Handovers for Non-IP PDNs.

Handover	Type	Non-IP PDNs
S-GW Relocation	Intra/Inter-RAT	Supported (Handover successful).
MME <-> S4-SGSN	Inter-RAT	Supported (Handover successful).
GnGp (4G -> 3G)	Inter-RAT	Not Supported (Handover Reject with cause 'Non-existent' followed by drop of existing 4G call).
LTE -> eHRPD	Inter-RAT	Not Supported (Handover Reject with status code 'Insufficient Resources'. Existing 4G call continues).
LTE -> Wi-Fi (S2a/S2b)	Inter-RAT	Not Supported (Handover Reject with cause 'pdn type not supported'. Existing 4G call continues).

ePCO IE Support

With this feature, ePCO IE for Non-IP PDN is supported at P-GW and S-GW.

ePCO IE Support at P-GW

Following is a gist of requirements supported for the ePCO IE at P-GW:

- Support is added for EPCOSI bit in Indication Flags IE in CSReq and MBReq at the P-GW.
- The P-GW includes PCO in ePCO IE based on EPCOSI bit received in CSReq message.
- Currently supported PCOs in ePCO IE is added.
- Support is added for Non-IP link MTU in both PCO as well as in ePCO. Depending on EPCOSI Indication Flag, the P-GW communicates Non-IP link MTU in PCO or ePCO. The Non-IP link MTU is sent for Non-IP PDNs when requested in CSreq message.
- When EPCOSI is received, requested options in ePCO IE are considered. When EPCOSI is not received, then ePCO IE is ignored at P-GW.

ePCO IE Support at S-GW

Following is a gist of requirements supported for the ePCO IE at S-GW:

- Support is added for EPCOSI bit in Indication Flags IE in CSReq and MBReq at the S-GW.
- The S-GW sets ePCO support for a PDN under following condition:
  1. During new call establishment:
     a. When EPCOSI is received from MME in CSReq.
     b. When ePCO IE is received in CSRsp from PGW.

2. During inter-SGW relocation:
   a. When EPCOSI is received from MME in CSReq toward S-GW.
3. During inter-MME intra-SGW relocation:
   a. When EPCOSI is received from MME in MBReq toward S-GW.

- During inter-MME intra-SGW handover scenario, if S-GW detects any change in ePCO IE support on MME, the S-GW initiates MBReq toward P-GW to notify the change accordingly by setting or re-setting EPCOSI flag in Indication Flags IE.
- The S-GW transparently forwards the received PCO/ePCO IE from the peer. As such, the S-GW does not put any restriction or checks, if ePCO is received for a PDN, for which ePCO is not supported and the other way around.
- For any PDN supporting ePCO IE, if MBReq without EPCOSI is received, the S-GW assumes that the ePCO IE support for the PDN is discontinued at MME and S-GW triggers MBReq toward P-GW without sending EPCOSI flag, or without sending Indication Flag IE. Similarly, if ePCO IE support is indicated in MBReq for an existing PDN not supporting ePCO, the S-GW triggers MBReq toward P-GW with EPCOSI set.

Important During initial PDN establishment messages, it is expected that MME sends the same EPCOSI support in CSReq and the followed MBReq (MBReq for S1 establish). If there is any change, it is considered as a misbehavior by MME and S-GW uses the final value received in MBReq. As such, signaling toward P-GW is triggered to indicate the change.

The ePCO IE supported at P-GW and S-GW has the following limitations:

- Lawful Intercept (LI) is not supported for ePCO IE.
- Currently supported PCO in MBR is not sent in MBRsp for PDN supporting ePCO IE.
- ePCO IE is not supported in DSReq/DSRsp messages. This is in parity with PCO IE.

Limitations

Following are the known limitations or restrictions of Non-IP PDN feature:

- Non-IP PDN connection is not supported on GGSN and SAEGW in this release.
- For Non-IP PDN at P-GW, following interfaces are not supported in this release:
  - S6b
  - LI Interface
  - Gx
  - Gy
  - Gz

- Rf

Important We recommend the operator to not configure these interfaces or CLI commands related to these interfaces for Non-IP PDN connections.

- P-GW does not support Local Policy for Non-IP PDN connections in this release.
- P-GW does not support other SGi PtP tunneling mechanisms (like PMIPv6/GRE, L2TP, GTP-C/U) to deliver Non-IP data to AS via SGi.
- P-GW does not support APN-AMBR rate limit for non-IP PDN connections.
- P-GW does not support shaping and policing for Non-IP data in this release.
- P-GW/S-GW does not support session trace for Non-IP PDNs in this release.
- P-GW/S-GW does not support RTT for Non-IP PDNs in this release.
- P-GW does not support NEMO for Non-IP PDNs in this release.
- P-GW does not support VRF for Non-IP PDNs in this release.
- P-GW does not support MPLS for Non-IP PDNs in this release.
- P-GW does not support IPSec for Non-IP PDNs in this release.
- For Non-IP PDNs, P-GW does not support VLAN tagging based on private pool configuration and next-hop address.
- P-GW does not support Framed Route for Non-IP PDNs in this release.
- ICSR upgrade/downgrade is not supported for Non-IP PDN sessions in this release.
- S-GW does not support Local IP Access (LIPA) for Non-IP PDN in this release.
- In-sequence delivery of Non-IP data cannot be guaranteed and data PDUs may be lost, requiring higher protocol layers to ensure guaranteed delivery when needed.
- P-GW supports reassembly of fragmented packets received on SGi UDP-IP tunnel, but currently does not send Internet Control Message Protocol (ICMP) “reassembly time exceeded” error message to the sender.
- Non-IP UE user-plane traffic is not supported on ICUPS.
- Following existing APN configuration are not supported for Non-IP PDNs:
  - accounting-mode gtpp

Note The accounting-mode with RADIUS configuration is supported.

  - active-charging
  - apn-ambr
  - authorize-with-hss

- backoff timer-value
- data-tunnel mtu
- ppp mtu
- dcca
- emergency-apn
- fw-and-nat
- gtpp
- ignore-alt-config
- ims-auth-service
- ip hide-service-address
- l3-to-l2-tunnel
- nai-construction
- pco-options
- reporting-action event-record
- ip pool <*pool_name*> <*ip_address/subnet_mask*> private nexthop-forwarding-address <*ip_address*> overlap vlanid <*vlan_id*>.

License Requirements

This feature is license controlled. Contact your Cisco account representative for information on how to obtain a license.

Standards Compliance

The Non-IP PDN feature complies with the following standards:

- 3GPP TS 23.060 - General Packet Radio Service (GPRS); Service description; Stage 2.
- 3GPP TS 23.401 - General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access.
- 3GPP TS 24.008 - Mobile radio interface Layer 3 specification; Core network protocols; Stage 3.
- 3GPP TS 24.301 - Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3.
- 3GPP TS 29.274 - 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3.

Configuring Non-IP PDN

Enabling Support for Non-IP PDP-Type for APN

Use the following commands under APN Configuration Mode for configuring APN to support Non-IP context types:

```
configure
  context context_name
    apn apn_name
      pdp-type non-ip
     end
```

Notes:

- By default, the command is disabled.
- This CLI command takes effect during new subscriber call creation on S5/S8 interface to the APN.

Configuring UDP-IPv4 or UDP-IPv6 Tunneling Parameters

Use the following commands under APN Configuration Mode to configure UDP-IPv4 or UDP-IPv6 tunneling parameters between the P-GW and an external application server for the APN.

```
configure
 context context_name
  apn apn_name
   tunnel udpip peer-address peer_address peer-port peer_udp_port [ local-port
<local_udp_port> ]
    end
```

Notes:

- **udpip** - Specifies the per subscriber UDP/IPv4 or UDP/IPv6 tunnel. Based on IPv4/IPv6 peer and local address, tunnel will be UDP/IPv4 or UDP/IPv6.
- **peer-address** *peer_address* - Specifies the Peer address for the tunnel. *peer_address* must be expressed in dotted decimal notation.
- **peer-port** *peer_udp_port* - Specifies the port number of the peer for the tunnel.
- **local-port** - Specifies the local UDP port number. Default value is 49152.
- If previously configured, use the no tunnel udpip CLI command to disable the UDP-IPv4/UDP-IPv6 tunneling for the APN.
- For local and peer UDP port number, it is recommended to use unregistered port number with IANA.
- This CLI command takes effect during new subscriber call creation on S5/S8 interface to the APN.

Enabling Support for Non-IP PDP Type for Radius Accounting and Authentication

Use the following commands for configuring radius accounting:

```
configure
  context context_name
    aaa group default
      radius dictionary 3gpp
      exit
     apn apn_name
      pdp-type non-ip
      tunnel udp peer-address peer_address peer-port peer_UDP_port local-port
 local_UDP_port
      no ims-auth-service service_name
      no active-charging rulebase
      authentication imsi-auth username-strip-apn
      accounting-mode radius
      mediation-device context-name ISP1 delay-GTP-respo
   end
```

Notes:

- By default, the command is disabled.
- This CLI command is applicable only for legacy PDN features.
- **radius dictionary 3gpp**: Configures 3GPP radius dictionary for radius accounting.

Verifying the Non-IP PDN Configuration

Use the **show apn name** *apn_name* command to verify the configuration that you have entered following the steps outlined earlier. The output appears similar to the following:

```
show apn name intershat

access point name (APN):  intershat
authentication context:  ingress
pdp type:  non-ip
emergency: no
.
.
.
Tunnel peers
  udp peer-address 10.0.0.1 peer-port 65535 local-port 49152
.
.
.
```

The following show commands can also be used for verifying the Non-IP PDP-Type and UDP-IP tunnel configurations for the APN:

- **show configuration apn** *apnname*
- **show configuration**
- **show configuration apn** *apnname* **verbose**

- **show configuration verbose**

Monitoring and Troubleshooting the Non-IP PDN

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

Non-IP PDN Show Command(s) and/or Outputs

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

show session progress

The following new field is added to the output of this command to show the number of Non-IP PDN sessions that are in CONNECTED state:

- **In-progress calls @ PDN-TYPE-Non-IP CONNECTED state**

show session subsystem

The following new field is added to the output of this command to show the number of Non-IP PDN sessions that are in CONNECTED state:

- **In-progress calls @ PDN-TYPE-Non-IP CONNECTED state**

show session summary

The following new fields are added to the show output to display the summary information of sessions active or dormant along with total sessions for each access-type:

- **pgw-gtp-non-ip** – Total number of Non-IP subscribers on GTP-PGW.
- **sgw-gtp-non-ip** – Total number of Non-IP subscribers on GTP-SGW.

These new fields are also introduced in the output of following show commands:

- **show subscribers**
- **show subscribers summary**

show subscribers aaa-configuration

The output of this show command displays the following new fields under Access Type and Network Type:

- **Access Type: sgw-pdn-type-non-ip | gtp-pdn-type-non-ip**
- **Network Type: Non-IP | UDP-IPv4 | UDP-IPv6**

Notes:

- **Access Type: sgw-pdn-type-non-ip** is displayed for S-GW sessions, when PDN-type is Non-IP.
- **Access Type: gtp-pdn-type-non-ip** is displayed for P-GW sessions, when PDN-type is Non-IP.

- **Network Type: (N) – Non-IP** is displayed for S-GW sessions with PDN-type Non-IP.
- **Network Type: (x) – UDP-IPv4** is displayed for P-GW sessions with PDN-type Non-IP and IP address allocated to the session is IPv4.
- **Network Type: (X) – UDP-IPv6** is displayed for P-GW sessions with PDN-type Non-IP and IP address allocated to the session is IPv6.

These new fields are also introduced in the output of following show commands:

- **show subscribers activity all**
- **show subscribers full all**

show subscribers pgw-only full all

The output of this show command displays the following new fields under Access Type and Network Type:

- **Access Type: gtp-pdn-type-non-ip**
- **Network Type: UDP-IPv4 | UDP-IPv6**

Notes:

- **Access Type: gtp-pdn-type-non-ip** is displayed for P-GW sessions, when PDN-type is Non-IP.
- **Network Type: (x) – UDP-IPv4** is displayed for P-GW sessions with PDN-type Non-IP and IP address allocated to the session is IPv4.
- **Network Type: (X) – UDP-IPv6** is displayed for P-GW sessions with PDN-type Non-IP and IP address allocated to the session is IPv6.

show subscribers sgw-only full all

The output of this show command displays the following new fields under Access Type and Network Type:

- **Access Type: sgw-pdn-type-non-ip**
- **Network Type: Non-IP**

Notes:

- **Access Type: sgw-pdn-type-non-ip** is displayed for S-GW sessions, when PDN-type is Non-IP.
- **Network Type: Network Type: (N) – Non-IP** is displayed for S-GW sessions with PDN-type Non-IP.

show pgw-service statistics all

The output of this show command displays the following new fields:

1. PDNs By PDN-Type:
    - **Non-IP PDNs:**
        - **Active:**
        - **Setup:**

- **Released:**

2. VAPNs Selected Based on Configured PDP-Type:
   - **Non-IP PDNs:**
     - **Setup:**
     - **Rejected:**
3. Data Statistics Per Interface:
   - **Drop Due To Non-IP Port Violation:**
     - **Packets:**
     - **Bytes:**
   - **Drop Due To Non-IP Protocol Violation:**
     - **Packets:**
     - **Bytes:**
   - **Drop Due To Non-IP Invalid AS Source Address:**
     - **Packets:**
     - **Bytes:**
4. Data Statistics Per Interface:
   - **Non-IP Reassembly Statistics:**
     - **Packets:**
     - **Bytes:**
5. IP Address Allocation Statistics:
   - **Non-IP PDN:**
     - **Total IPv4 addrs allocated:**
       - **Local pool assignment:**
     - **Total IPv6 addrs allocated:**
       - **Local pool assignment:**
6. SGi tunneling statistics:
   - **UDP-IPv4 Tunnels:**
     - **Active:**

- **Setup:**
- **Released:**

- **UDP-IPv6 Tunnels:**
  - **Active:**
  - **Setup:**
  - **Released:**

7. Data Statistics Per PDN-Type:
   - **Non-IP PDNs:**
     - **Uplink:**
       - **Total Pkts:**
       - **Total Bytes:**
     - **Downlink:**
       - **Total Pkts:**
       - **Total Bytes:**

Where:

1. Number of Active, Setup and Release session counters for Non-IP PDN type.
2. Setup and Rejected counters for Virtual APN selection based on Non-IP PDP type.
3. Packets and bytes drop counters for invalid port, invalid protocol and invalid application server source address.
4. Packets and bytes reassembled counters for Non-IP downlink data on UDP-IPv4/UDP-IPv6 tunnel.
5. Counters for locally allocated IPv4/IPv6 address for Non-IP PDN type UEs.
6. SGi tunneling statistics for UDP-IPv4 and UDP-IPv6.
7. Data statistics (uplink/downlink) for Non-IP PDN types.

show sgw-service statistics all

The output of this show command displays the following new fields:

1. PDNs By PDN-Type:
   - **Active:**
   - **Setup:**
   - **Released:**
   - **Rejected:**

2. Data Statistics Per PDN-Type:
    - **Non-IP PDNs:**
        - **Uplink:**
            - **Total Pkts:**
            - **Total Bytes:**
        - **Downlink:**
            - **Total Pkts:**
            - **Total Bytes:**

Where:

1. Number of Active, Setup, Release, and Rejected session counters for Non-IP PDN type.
2. Data statistics (Uplink and Downlink) for Non-IP PDN types.

show subscribers network-type

The output of the show subscribers network-type udp-ipv4 | udp-ipv6 | non-ip command displays the following new fields:

1. Access Type:
    - **(B) - pgw-gtp-non-ip**
    - **(J) - sgw-gtp-non-ip**
2. Network-Type:
    - **(N) - NON-IP**
    - **(x) - UDP-IPv4**
    - **(X) - UDP-IPv6**

Where:

1. Non-IP PDNs for GTP-PGW and S-GW based on Access Type.
2. Non-IP network type for S-GW and UDP-IPv4/UDP-IPv6 network type for P-GW.

show subscribers pgw-only summary

The following new field is added to the output of this command which displays the summary information for P-GW subscribers, based on defined parameters:

- **gtp-pdn-type-non-ip**

show subscribers sgw-only summary

The following new field is added to the output of this command which displays the summary information for S-GW subscribers, based on defined parameters:

- **gtp-pdn-type-non-ip**

show subscribers pgw-only

The following new field is added to the output of this command to display Non-IP PDN Access Type:

- **(B) - pgw-gtp-non-ip**

show subscribers sgw-only

The following new field is added to the output of this command to display Non-IP PDN Access Type:

- **(J) - sgw-gtp-non-ip**

show apn statistics

The output of this show command displays the following new fields:

1. Data Statistics:
   - **Non-IP port violations drop:**
   - **Non-IP protocol violation drop:**
   - **Non-IP invalid AS src addr drop:**
2. Data Statistics:
   - **Non-IP reassembled pkts:**
3. Total PDN-Type stats:
   - **PDN-Type Non-IP sessions:**
     - **Active:**
     - **Setup:**
     - **Released:**

Where:

1. Non-IP drop statistics for port violation, protocol violation, and application server source address violations for the APN.
2. Number of reassembled packets from fragmented downlink packets on SGi UDP-IP tunnel for Non-IP PDNs for the APN.
3. Number of Active, Setup and Release session counters for Non-IP PDN type.

show apn statistics name

Use the **show apn statistics name** *apn_name* command to verify the Non-IP UE APN statistics. The output appears similar to the following:

```
show apn name intershat

access point name (APN):  intershat
authentication context:  ingress
pdp type:  non-ip
emergency: no
.
.
.
Tunnel peers
  udp peer-address 10.0.0.1 peer-port 65535 local-port 49152
.
.
.
```

Monitor Protocol

When using the monitor protocol command, enable the following options::

- 26 (GTPU)and 33 (L3 Tunnel)
- 12 (RADIUS Auth),13 (Acct),31(RADIUS COA) for RADIUS messages

Show Configuration Errors

The following APN configuration error is displayed when APN pdp-type is Non-IP and UDP-IP tunnel is not configured under APN:

```
#######################################################
          Displaying APN-configuration errors
#######################################################
Error   : UDP tunnel not configured in Non-IP APN <apn_name> in the context <context>
Total 1 error(s) in this section !
```

Non-IP PDN Bulk Statistics

The following statistics are introduced in support of the feature:

APN Schema

- invalid-dst-port-pkt-drop – This statistics indicates the total number of downlink packets dropped due to invalid destination port for a Non-IP APN PDN.
- pdn-non-ip-actsess – This statistics indicates the total number of active Non-IP sessions at APN.
- pdn-non-ip-setupsess – This statistics indicates the total number of Non-IP session setup at APN.
- pdn-non-ip-relsess – This statistics indicates the total number of Non-IP session release at APN.
- invalid-tun-proto-pkt-drop – This statistics indicates the total number of downlink packets dropped due to invalid SGi tunnel protocol for a Non-IP APN PDN.
- invalid-as-src-pkt-drop – This statistics indicates the total number of downlink packets dropped due to invalid application server source address for a Non-IP APN PDN.

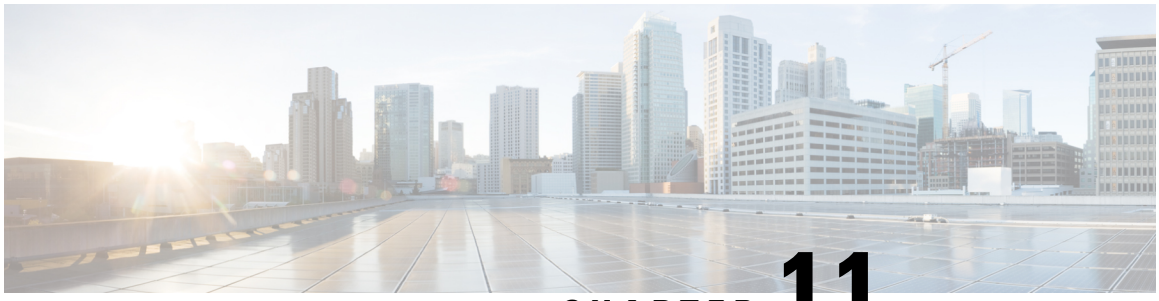
P-GW Schema

- sessstat-pdn-non-ip-active – This statistic indicates the total number of active Non-IP PDNs at P-GW.
- sessstat-pdn-non-ip-setup – This statistic indicates the total number of Non-IP PDNs setup at P-GW.
- sessstat-pdn-non-ip-rel – This statistic indicates the total number of Non-IP PDNs released at P-GW.
- sessstat-non-ip-ipv4addaloc – This statistic indicates the total number of times IPv4 address is allocated for Non-IP P-GW PDNs.
- sessstat-non-ip-ipv6addaloc – This statistic indicates the total number of times IPv6 address is allocated for Non-IP P-GW PDNs.
- sessstat-non-ip-addaloc-ipv4loacalpool – This statistic indicates the total number of times IPv4 address is allocated from local pool for Non-IP P-GW PDNs.
- sessstat-non-ip-addaloc-ipv6loacalpool – This statistic indicates the total number of times IPv6 address is allocated from local pool for Non-IP P-GW PDNs.
- udptunstat-ipv4sessact – This statistic indicates the total number of active UDP-IPv4 SGi tunnel.
- udptunstat-ipv4sesssetup – This statistic indicates the total number of UDP-IPv4 SGi tunnel setup at P-GW.
- udptunstat-ipv4sessrel – This statistic indicates the total number of UDP-IPv4 SGi tunnel setup at P-GW.
- udptunstat-ipv6sessact – This statistic indicates the total number of active UDP-IPv6 SGi tunnel.
- udptunstat-ipv6sesssetup – This statistic indicates the total number of UDP-IPv6 SGi tunnel setup at P-GW.
- udptunstat-ipv6sessrel – This statistic indicates the total number of UDP-IPv6 SGi tunnel released at P-GW.
- non-ip-pdn-to-user-pkt – This statistics indicates the total number of downlink packets sent on Non-IP P-GW PDNs.
- non-ip-pdn-to-user-byte – This statistics indicates the total number of downlink bytes sent on Non-IP P-GW PDNs.
- non-ip-pdn-from-user-pkt – This statistics indicates the total number of uplink packets received for Non-IP S-GW PDNs.
- non-ip-pdn-from-user-byte – This statistic indicates the total number of uplink bytes with Non-IP S-GW PDNs.
- sessstat-invalid-port-dnlkpktdrop – This statistics indicates the total number of downlink packets dropped due to invalid destination port for a Non-IP P-GW PDN.
- sessstat-invalid-port-dnlkbytedrop – This statistics indicates the total number of downlink bytes dropped due to invalid destination port for a Non-IP P-GW PDN.
- sessstat-invalid-tun-proto-dnlkpktdrop – This statistics indicates the total number of downlink packets dropped due to invalid SGi tunnel protocol for a Non-IP P-GW PDN.
- sessstat-invalid-tun-proto-dnlkbytedrop – This statistics indicates the total number of downlink bytes dropped due to invalid SGi tunnel protocol for a Non-IP P-GW PDN.
- sessstat-invalid-as-src-dnlkpktdrop – This statistics indicates the total number of downlink packets dropped due to invalid application server source address for a Non-IP P-GW PDN.
- sessstat-invalid-as-src-dnlkbytedrop – This statistics indicates the total number of downlink bytes dropped due to invalid application server source address for a Non-IP P-GW PDN.

S-GW Schema

- sessstat-totcur-pdn-non-ip – This statistic indicates the total number of current Non-IP S-GW PDN.
- sessstat-pdnsetuptype-non-ip – This statistic indicates the total number of Non-IP PDNs setup at S-GW.
- sessstat-pdnrel-non-ip – This statistic indicates the total number of Non-IP PDNs released at S-GW.
- sessstat-pdnrej-non-ip – This statistic indicates the total number of Non-IP PDNs rejected by S-GW.

- non-ip-pdn-to-user-pkt – This statistic indicates the total number of downlink packets with Non-IP S-GW PDNs.
- non-ip-pdn-to-user-byte – This statistic indicates the total number of downlink bytes with Non-IP S-GW PDNs.
- non-ip-pdn-from-user-pkt – This statistic indicates the total number of uplink packets with Non-IP S-GW PDNs.
- non-ip-pdn-from-user-byte – This statistic indicates the total number of uplink bytes with Non-IP S-GW PDNs.



CHAPTER 11

P-GW Buffering Optimization

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	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide*

Revision History

Revision Details	**Release**
First Introduced	21.22.3

Feature Description

The P-GW Buffering Optimization enables the P-GW to handle the Presence Reporting Area (PRA) messages efficiently. When two or more PRAs are received, while UBResp is still pending, there are chances that P-GW buffer queue can become full or even a message drop can happen. This enhancement enables the PRA response from Policy and Charging Rules Function (PCRF) to be handled efficiently as the chances of message drop is less.

When a new message arrives, the P-GW merges the message with the existing similar type of message in the queue. This allows the P-GW to process similar type of messages at the same time without increasing the queue size and reducing the message drop ratio. When messages are read from the queue, the Gx Rule Level Attribute -value pairs (AVPs) defined actions are triggered. The Rule Level AVPs validity is not checked when messages are buffered.

Relationship to Other Feature

The P-GW Buffering Optimization feature is related to P-GW Buffering Mechanism functionality. For details, see the *P-GW Buffering Mechanism* chapter in the *P-GW Administration Guide*.

How it Works

Under Active Charging Service (ACS) mode, a CLI command - **optimze-update** is enabled or disbaled to enable or disable the buffering mechanism.

Configuring the P-GW Buffering Optimization

Use the following configuration to enable or disable the P-GW buffering optimization to process the similar type of messages in the queue.

```
configure
          active-charging service service_name
            [ no ] policy control optimze-update pra-change
        end
```

NOTES:

- **optimize-update**: Enables the optimization for multiple policies received from PCRF, when the earlier response is pending. Default is Disabled.
- **no**: Disables the optimization for multiple policies.
- **pra-change**: Enables policy optimization only during the Presence Reporting Area (PRA) change.

Monitoring and Troubleshooting

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

Show Commands and Outputs

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

show Active-Charging Sessions Full All

The output of the Show Active-Charging Sessions Full All.

Table 7: show active-charging sessions full all Command Output Descriptions

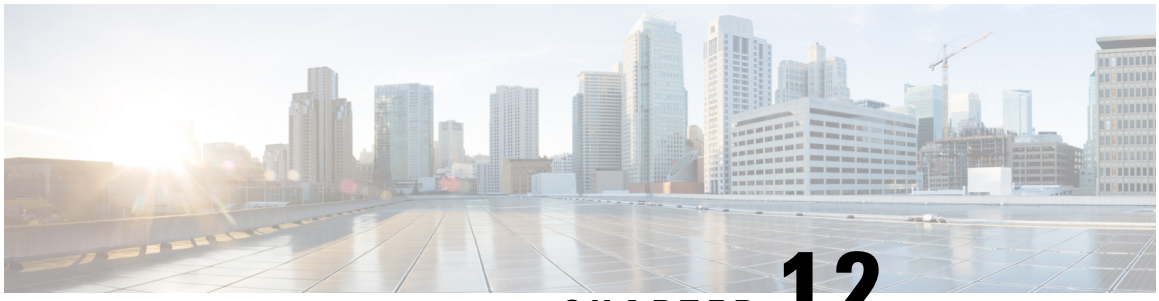
Field	Description
Current P-GW-Buffer Queue Length	Displays the currently utilized queue length.
Total P-GW Buffer Merge Count	Displays the merged count of PRA messages.

show Active-Charging Service All

The output of the Show Active-Charging Service All.

Table 8: show active-charging service all Command Output Descriptions

Field	Description
optimize-update	Enables multiple policy optimization.
pra-change	Enables optimization policies for PRA changes.



CHAPTER 12

RedHat Software Version Update

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	All
Applicable Platform(s)	VPC-DI
Feature Default	Enabled - Always-on
Related Features in this Release	Not Applicable
Related Documentation	Not Applicable

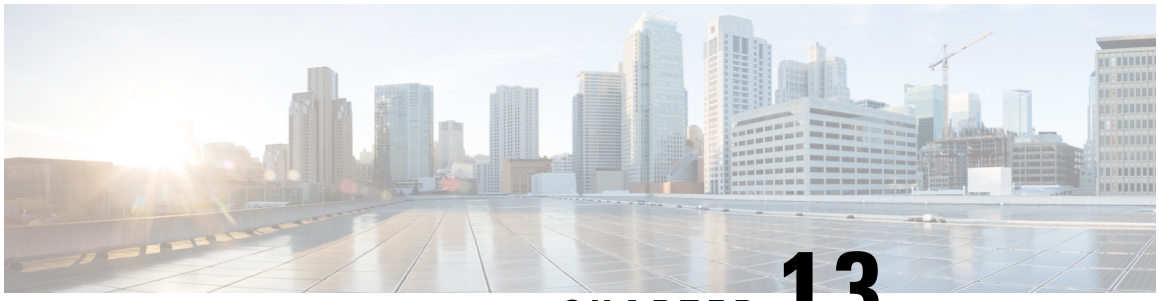
Revision History

Revision Details	Release
First introduced.	21.22.4

Feature Description

This release includes support for RedHat version 16.1 (Train). The RedHat 16.1 (Train) has been validated and is recommended for use with all the VPC-DI based deployments.

For more information, contact your Cisco Account representative.



CHAPTER 13

Rf Interface Support

This chapter provides an overview of the Diameter Rf interface and describes how to configure the Rf interface.

Rf interface support is available on the Cisco system running StarOS 10.0 or later releases for the following products:

- Gateway GPRS Support Node (GGSN)
- Proxy Call Session Control Function (P-CSCF)
- Packet Data Network Gateway (P-GW)
- Serving Call Session Control Function (S-CSCF)

Important In StarOS version 19 and later releases, the Rf interface is not supported on the S-GW.

It is recommended that before using the procedures in this chapter you select the configuration example that best meets your service model, and configure the required elements for that model as described in the administration guide for the product that you are deploying.

This chapter includes the following topics:

Introduction

The Rf interface is the offline charging interface between the Charging Trigger Function (CTF) (for example, P-GW, P-CSCF) and the Charging Collection Function (CCF). The Rf interface specification for LTE/GPRS/eHRPD offline charging is based on 3GPP TS 32.299 V8.6.0, 3GPP TS 32.251 V8.5.0 and other 3GPP specifications. The Rf interface specification for IP Multimedia Subsystem (IMS) offline charging is based on 3GPP TS 32.260 V8.12.0 and 3GPP TS 32.299 V8.13.0.

Offline charging is used for network services that are paid for periodically. For example, a user may have a subscription for voice calls that is paid monthly. The Rf protocol allows the CTF (Diameter client) to issue offline charging events to a Charging Data Function (CDF) (Diameter server). The charging events can either be one-time events or may be session-based.

The system provides a Diameter Offline Charging Application that can be used by deployed applications to generate charging events based on the Rf protocol. The offline charging application uses the base Diameter protocol implementation, and allows any application deployed on chassis to act as CTF to a configured CDF.

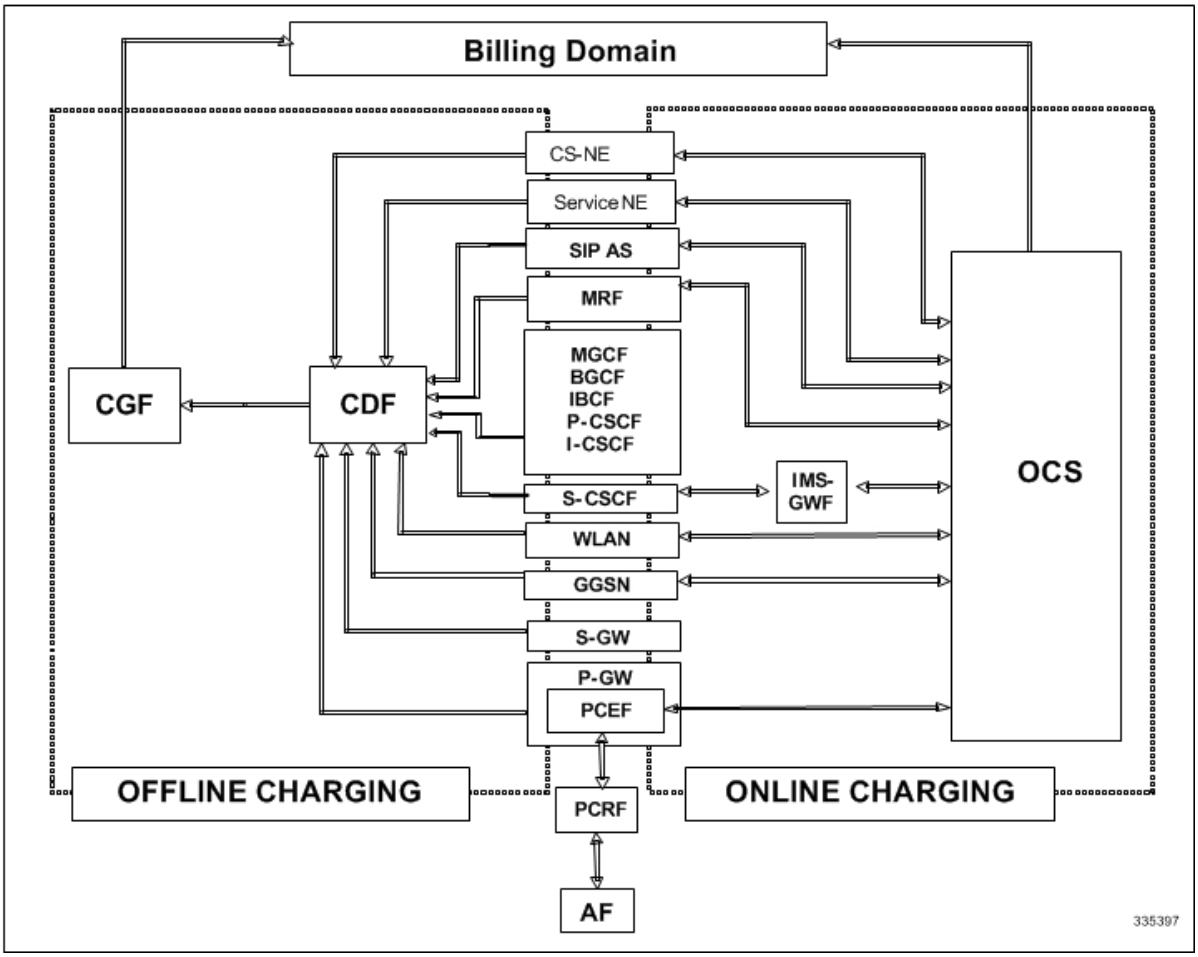
In general, accounting information from core network elements is required to be gathered so that the billing system can generate a consolidated record for each rendered service.

The CCF with the CDF and Charging Gateway Function (CGF) will be implemented as part of the core network application. The CDF function collects and aggregates Rf messages from the various CTFs and creates CDRs. The CGF collects CDRs from the CDFs and generates charging data record files for the data mediation/billing system for billing.

Offline Charging Architecture

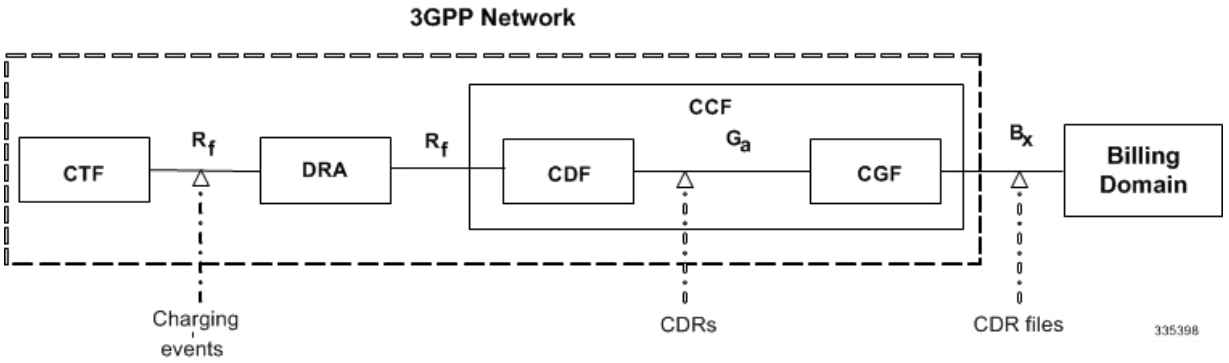
The following diagram provides the high level charging architecture as specified in 3GPP 32.240. The interface between CSCF, P-GW and GGSN with CCF is Rf interface. Rf interface for EPC domain is as per 3GPP standards applicable to the PS Domain (e.g. 32.240, 32.251, 32.299, etc.).

Figure 8: Charging Architecture



The following figure shows the Rf interface between CTF and CDF.

Figure 9: Logical Offline Charging Architecture



The Rf offline charging architecture mainly consists of three network elements CCF, CTF and Diameter Dynamic Routing Agent (DRA).

Charging Collection Function

The CCF implements the CDF and CGF. The CCF will serve as the Diameter Server for the Rf interface. All network elements supporting the CTF function should establish a Diameter based Rf Interface over TCP connections to the DRA. The DRA function will establish Rf Interface connection over TCP connections to the CCF.

The CCF is primarily responsible for receipt of all accounting information over the defined interface and the generation of CDR (aka UDRs and FDRs) records that are in local storage. This data is then transferred to the billing system using other interfaces. The CCF is also responsible for ensuring that the format of such CDRs is consistent with the billing system requirements. The CDF function within the CCF generates and CGF transfers the CDRs to the billing system.

The CDF function in the CCF is responsible for collecting the charging information and passing it on to the appropriate CGF via the GTP' based interface per 3GPP standards. The CGF passes CDR files to billing mediation via SCP.

Charging Trigger Function

The CTF will generate CDR records and passes it onto CCF. When a P-GW service is configured as CTF, then it will generate Flow Data Record (FDR) information as indicated via the PCRF. The P-GW generates Rf messages on a per PDN session basis. There are no per UE or per bearer charging messages generated by the P-GW.

The service data flows within IP-CAN bearer data traffic is categorized based on a combination of multiple key fields (Rating Group, Rating Group and Service -Identifier). Each Service-Data-Container captures single bi-directional flow or a group of single bidirectional flows as defined by Rating Group or Rating Group and Service-Identifier.

Dynamic Routing Agent

The DRA provides load distribution on a per session basis for Rf traffic from CTFs to CCFs. The DRA acts like a Diameter Server to the Gateways. The DRA acts like a Diameter client to CCF. DRA appears to be a CCF to the CTF and as a CTF to the CCF.

The DRA routes the Rf traffic on a per Diameter charging session basis. The load distribution algorithm can be configured in the DRA (Round Robin, Weighted distribution, etc). All Accounting Records (ACRs) in one

Diameter charging session will be routed by the DRA to the same CCF. Upon failure of one CCF, the DRA selects an alternate CCF from a pool of CCFs.

License Requirements

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

Supported Standards

Rf interface support is based on the following standards:

- IETF RFC 4006: Diameter Credit Control Application; August 2005
- 3GPP TS 32.299 V9.6.0 (2010-12) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Diameter charging applications (Release9)

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	• 5G Non Standalone Solution Guide • AAA Interface Administration and Reference • Command Line Interface Reference • MME Administration Guide • Statistics and Counters Reference

Revision History

Revision Details	Release
The StarOS 21.22 is enhanced, where an existing User Location Information (ULI) is sent to the Accounting Record (ACR) Stop message on offline charging (RF) interface for GGSN, P-GW, and SAEGW.	21.22

Features and Terminology

This section describes features and terminology pertaining to Rf functionality.

Offline Charging Scenarios

Offline charging for both events and sessions between CTF and the CDF is performed using the Rf reference point as defined in 3GPP TS 32.240.

Basic Principles

The Diameter client and server must implement the basic functionality of Diameter accounting, as defined by the RFC 3588 Diameter Base Protocol.

For offline charging, the CTF implements the accounting state machine as described in RFC 3588. The CDF server implements the accounting state machine "SERVER, STATELESS ACCOUNTING" as specified in RFC 3588, i.e. there is no order in which the server expects to receive the accounting information.

The reporting of offline charging events to the CDF is managed through the Diameter Accounting Request (ACR) message. Rf supports the following ACR event types:

Table 9: Rf ACR Event Types

Request	Description
START	Starts an accounting session
INTERIM	Updates an accounting session
STOP	Stops an accounting session
EVENT	Indicates a one-time accounting event

ACR types START, INTERIM and STOP are used for accounting data related to successful sessions. In contrast, EVENT accounting data is unrelated to sessions, and is used e.g. for a simple registration or interrogation and successful service event triggered by a network element. In addition, EVENT accounting data is also used for unsuccessful session establishment attempts.

Important The ACR Event Type "EVENT" is supported in Rf CDRs only in the case of IMS specific Rf implementation.

The following table describes all possible ACRs that might be sent from the IMS nodes i.e. a P-CSCF and S-CSCF.

Table 10: Accounting Request Messages Triggered by SIP Methods or ISUP Messages for P-CSCF and S-CSCF

Diameter Message	Triggering SIP Method/ISUP Message
ACR [Start]	SIP 200 OK acknowledging an initial SIP INVITE
	ISUP:ANM (applicable for the MGCF)
ACR [Interim]	SIP 200 OK acknowledging a SIP
	RE-INVITE or SIP UPDATE [e.g. change in media components]
	Expiration of AVP [Acct-Interim-Interval]
	SIP Response (4xx, 5xx or 6xx), indicating an unsuccessful SIP RE-INVITE or SIP UPDATE
ACR [Stop]	SIP BYE message (both normal and abnormal session termination cases)
	ISUP:REL (applicable for the MGCF)
ACR [Event]	SIP 200 OK acknowledging non-session related SIP messages, which are: • SIP NOTIFY • SIP MESSAGE • SIP REGISTER • SIP SUBSCRIBE • SIP PUBLISH
	SIP 200 OK acknowledging an initial SIP INVITE
	SIP 202 Accepted acknowledging a SIP REFER or any other method
	SIP Final Response 2xx (except SIP 200 OK)
	SIP Final/Redirection Response 3xx
	SIP Final Response (4xx, 5xx or 6xx), indicating an unsuccessful SIP session set-up
	SIP Final Response (4xx, 5xx or 6xx), indicating an unsuccessful session-unrelated procedure
	SIP CANCEL, indicating abortion of a SIP session set-up

Event Based Charging

In the case of event based charging, the network reports the usage or the service rendered where the service offering is rendered in a single operation. It is reported using the ACR EVENT.

In this scenario, CTF asks the CDF to store event related charging data.

Session Based Charging

Session based charging is the process of reporting usage reports for a session and uses the START, INTERIM & STOP accounting data. During a session, a network element may transmit multiple ACR Interims' depending on the proceeding of the session.

In this scenario, CTF asks the CDF to store session related charging data.

Diameter Base Protocol

The Diameter Base Protocol maintains the underlying connection between the Diameter Client and the Diameter Server. The connection between the client and server is TCP based.

In order for the application to be compliant with the specification, state machines should be implemented at some level within the implementation.

Diameter Base supports the following Rf message commands that can be used within the application.

Table 11: Diameter Rf Messages

Command Name	Source	Destination	Abbreviation
Accounting-Request	CTF	CDF	ACR
Accounting-Answer	CDF	CTF	ACA

There are a series of other Diameter messages exchanged to check the status of the connection and the capabilities.

- Capabilities Exchange Messages: Capabilities Exchange Messages are exchanged between the diameter peers to know the capabilities of each other and identity of each other.
  - Capabilities Exchange Request (CER): This message is sent from the client to the server to know the capabilities of the server.
  - Capabilities Exchange Answer (CEA): This message is sent from the server to the client in response to the CER message.
- Device Watchdog Request (DWR): After the CER/CEA messages are exchanged, if there is no more traffic between peers for a while, to monitor the health of the connection, DWR message is sent from the client. The Device Watchdog timer (Tw) is configurable and can vary from 6 through 30 seconds. A very low value will result in duplication of messages. The default value is 30 seconds. On two consecutive expiries of Tw without a DWA, the peer is considered to be down.

Important DWR is sent only after Tw expiry after the last message that came from the server. Say if there is continuous exchange of messages between the peers, DWR might not be sent if (Current Time - Last message received time from server) is less than Tw.

- Device Watchdog Answer (DWA): This is the response to the DWR message from the server. This is used to monitor the connection state.
- Disconnect Peer Request (DPR): This message is sent to the peer to inform to shutdown the connection. There is no capability currently to send the message to the Diameter server.
- Disconnect Peer Answer (DPA): This message is the response to the DPR request from the peer. On receiving the DPR, the peer sends DPA and puts the connection state to "DO NOT WANT TO TALK TO YOU" state and there is no way to get the connection back except for reconfiguring the peer again.

  A timeout value for retrying the disconnected peer must be provided.

Timer Expiry Behavior

Upon establishing the Diameter connection, an accounting interim timer (AII) is used to indicate the expiration of a Diameter accounting session, and is configurable at the CTF. The CTF indicates the timer value in the ACR-Start, in the Acct-Interim-Interval AVP. The CDF responds with its own AII value (through the DRA), which must be used by the CTF to start a timer upon whose expiration an ACR INTERIM message must be sent. An instance of the AII timer is started in the CCF at the beginning of the accounting session, reset on the receipt of an ACR-Interim and stopped on the receipt of the ACR-Stop. After expiration of the AII timer, ACR INTERIM message will be generated and the timer will be reset and the accounting session will be continued.

Rf Interface Failures/Error Conditions

The current architecture allows for primary and secondary connections or Active-Active connections for each network element with the CDF elements.

DRA/CCF Connection Failure

When the connection towards one of the primary/Active DRAs in CCF becomes unavailable, the CTF picks the Secondary/Active IP address and begins to use that as a Primary.

If no DRA (and/or the CCF) is reachable, the network element must buffer the generated accounting data in non-volatile memory. Once the DRA connection is up, all accounting messages must be pulled by the CDF through offline file transfer.

No Reply from CCF

In case the CTF/DRA does not receive an ACA in response to an ACR, it may retransmit the ACR message. The waiting time until a retransmission is sent, and the maximum number of repetitions are both configurable by the operator. When the maximum number of retransmissions is reached and still no ACA reply has been received, the CTF/DRA sends the ACRs to the secondary/alternate DRA/CCF.

Detection of Message Duplication

The Diameter client marks possible duplicate request messages (e.g. retransmission due to the link failover process) with the T-flag as described in RFC 3588.

If the CDF receives a message that is marked as retransmitted and this message was already received, then it discards the duplicate message. However, if the original of the re-transmitted message was not yet received, it is the information in the marked message that is taken into account when generating the CDR. The CDRs are marked if information from duplicated message(s) is used.

CCF Detected Failure

The CCF closes a CDR when it detects that expected Diameter ACRs for a particular session have not been received for a period of time. The exact behavior of the CCF is operator configurable.

Rf-Gy Synchronization Enhancements

Both Rf (OFCS) and Gy (OCS) interfaces are used for reporting subscriber usage and billing. Since each interface independently updates the subscriber usage, there are potential scenarios where the reported information is not identical. Apart from Quota enforcement, OCS is utilized for Real Time Reporting (RTR), which provides a way to the user to track the current usage and also get notifications when a certain threshold is hit.

In scenarios where Rf (OFCS) and Gy (OCS) have different usage information for a subscriber session, it is possible that the subscriber is not aware of any potential overages until billed (scenario when Rf is more than Gy) or subscriber believes he has already used up the quota whereas his actual billing might be less (scenario when Gy is more than Rf). In an attempt to align both the Rf and Gy reported usage values, release 12.3 introduced capabilities to provide a way to get the reported values on both the interfaces to match as much as possible. However, some of the functionalities were deferred and this feature implements the additional enhancements.

In release 15.0 when time/volume quota on the Gy interface gets exhausted, Gy triggers "Service Data Volume Limit" and "Service Data Time Limit". Now in 16.0 via this feature, this behavior is CLI controlled. Based on the CLI command " **trigger-type { gy-sdf-time-limit { cache | immediate } | gy-sdf-unit-limit { cache | immediate } | gy-sdf-volume-limit { cache | immediate } }**" the behavior will be decided whether to send the ACR-Interim immediately or to cache the containers for future transactions. If the CLI for the event-triggers received via Gy is not configured, then those ACR-Interims will be dropped.

Releases prior to 16.0, whenever the volume/time-limit event triggers are generated, ACR-Interims were sent out immediately. In 16.0 and later releases, CLI configuration options are provided in policy accounting configuration to control the various Rf messages (ACRs) triggered for sync on this feature.

This release supports the following enhancements:

- Caches containers in scenarios when ACR-I could not be sent and reported to OFCS.
- Triggers ACR to the OFCS when the CCR to the OCS is sent instead of the current implementation of waiting for CCA from OCS.

If an ACR-I could not be sent to the OFCS, the PCEF caches the container record and sends it in the next transaction to the OFCS.

In releases prior to 16.0, once a CCR-U was sent out over Gy interface, ACR-I message was immediately triggered (or containers were cached) based on policy accounting configuration and did not wait for CCA-U.

In 16.0 and later releases, the containers are closed only after receiving CCA-U successfully. That is, Rf trigger will be sent only after receiving CCA-U message.

For more information on the command associated with this feature, see the *Accounting Policy Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

In 17.0 and later releases, a common timer based approach is implemented for Rf and Gy synchronization. As part of the new design, Gy and Rf will be check-pointed at the same point of time for periodic as well as for full check-pointing. Thus, the billing records will always be in sync at all times regardless of during an ICSR switchover event, internal events, session manager crashes, inactive Rf/Gy link, etc. This in turn avoids any billing discrepancies.

Cessation of Rf Records When UE is IDLE

Releases prior to 16.0, when the UE was identified to be in IDLE state and not sending any data, the P-GW generated Rf records. During this scenario, the generated Rf records did not include Service Data Containers (SDCs).

In 16.0 and later releases, the Rf records are not generated in this scenario. New CLI configuration command "**session idle-mode suppress-interim**" is provided to enable/disable the functionality at the ACR level to control the behavior of whether an ACR-I needs to be generated or not when the UE is idle and no data is transferred.

That is, this CLI configuration is used to control sending of ACR-I records when the UE is in idle mode and when there is no data to report.

For more information on the command, see the *Accounting Policy Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

QoS Change Scenarios

QOS_CHANGE Trigger in Rf Records During eHRPD-LTE Handoff

In releases prior to 20, QOS_CHANGE is reported as the value for Change-Condition AVP in the Service-Data-Container (SDC) of Rf accounting records (for accounting level SDF/SDF+accounting keys QCI) when eHRPD to LTE handoff occurs. Typically, the QOS_CHANGE should not be present as the PCRF does not enforce QoS via any QoS IE in eHRPD/CDMA RAT. In 20 and later releases, the SDC in the generated Rf record does not include QOS_CHANGE trigger during handoff from eHRPD to LTE.

QoS Change for Default Bearer

Releases prior to 20, in a multi-bearer call, when an update message (CCA-U or RAR) from PCRF changes the QoS (QCI/ARP) of default bearer and in the same message installs a predefined or dynamic rule on the newly updated default bearer, spurious Normal Release (NR) Service Data Volume (SDV) containers were added to Rf interim records for the dedicated bearers. In this scenario, the system used to send Normal Release buckets for the non-default bearers even if these bearers were not changed.

In release 20 and beyond, for a change in the QoS of default bearer, NR SDV containers will not be seen unless the corresponding bearer is torn down. Only QoS change containers are closed/released for the bearer that underwent QoS Change, i.e. the default bearer.

Diameter Rf Duplicate Record Generation

This section describes the overview and implementation of Rf Duplicate Record Generation feature.

This section discusses the following topics for this feature:

Feature Description

This feature is introduced to support creation and communication of duplicate Rf records to secondary AAA group servers configured for the Rf interface.

To achieve this functionality, the following configurations must be enabled –

- **aaa group** CLI command under APN to configure a maximum of 2 AAA groups - primary and secondary AAA groups, or two different endpoints for Rf Diameter accounting servers
- **diameter accounting duplicate-record** under AAA group to allow Rf duplicate record creation

The **diameter accounting duplicate-record** is a new CLI command introduced in this release for duplicating the Rf START, INTERIM and STOP accounting records.

Important This is a license-controlled CLI command. For more information, contact your Cisco account representative.

In releases prior to 21, gateway allows only one AAA group configuration per APN for Rf accounting. The AAA group is configured to load balance across multiple servers to pass the Rf traffic and also expect an accounting answer. Note that the secondary AAA group configuration is allowed currently but is restricted to only RADIUS accounting.

In release 21 and beyond, the gateway is provided with the ability to configure a secondary AAA group per APN for the Rf interface, and send the duplicate Diameter Rf accounting records to the secondary AAA group servers. The secondary AAA group is used for non-billing purposes only.

Important The failed duplicate records will neither be written to HDD nor added to the archival list.

There is no change in the current behavior with the primary AAA group messages. The primary AAA group is independent of the secondary AAA group, and it has multiple Rf servers configured. When the Rf servers do not respond even after multiple retries as per the applicable configuration, the Rf records are archived and stored in HDD. This behavior continues as is irrespective of the configuration of secondary aaa-group.

Secondary aaa group has a very similar configuration as the primary aaa group except that the new CLI command **diameter accounting duplicate-record** is additionally included to configure the secondary aaa-group. It is also important to note that different Diameter endpoints and a separate set of Rf servers should be provisioned for both primary and secondary AAA groups.

If all the configured servers are down, the request message will be discarded without writing it in HDD or archiving at aaamgr.

The original and duplicate Rf messages use two different aaa-groups and two different Diameter endpoints. Hence, the values for Session-ID AVP will be different. Based on the configuration of primary and secondary endpoints the values for Origin-Host, Origin-Realm, Destination-Realm, and Destination-Host AVPs may be different. Also based on the configuration under policy accounting for inclusion of virtual/gn apn name for secondary group Called-Station-ID AVP might change. All other AVPs will have the same values as with the primary aaa group Rf message.

Also, note that the values such as Acct-Interim-Interval (AII) interval received in ACA from secondary group of AAA servers will be ignored.

Relationships to Other Features

This feature can be used in conjunction with Virtual APN Truncation feature to achieve the desired results.

The Virtual APN Truncation feature is new in release 21. For more information on this feature, see the administration guide for the product you are deploying.

Limitations

The following are the limitations of this feature:

- Only one secondary AAA group can be configured per APN.
- If all the Rf peers under secondary aaa group are down and duplicate Start Record is not sent, then the duplicate Interim and Stop records will also not be sent to any of the secondary aaa group servers even though they arrived later. However if the servers are up and duplicate Start record was sent but the server did not respond, duplicate Start will be dropped after all the retries. In this case, the duplicate Interim and Stop records may be sent out to the server.
- In cases when duplicate Start record was sent, but during duplicate Interim/Stop record generation peers were not responding/down, after all retries duplicate Interim and Stop records will be dropped and will not be written to HDD.
- Minimal impact to memory and CPU is expected due to the duplicate record generation for every primary Rf record.

Configuring Rf Duplicate Record Generation

The following section provides the configuration commands to enable the Rf duplicate record generation.

Configuring Secondary AAA Group

Use the following configuration commands to configure the secondary AAA group for receiving the duplicate Rf records.

```
configure
   context context_name
      apn apn_name
         aaa group group_name
         aaa secondary-group group_name
         exit
```

Notes:

- **aaa group** *group_name*: Specifies the AAA server group for the APN. *group_name* must be an alphanumeric string of 1 through 63 characters.

- **secondary group** *group_name*: Specifies the secondary AAA server group for the APN. *group_name* must be an alphanumeric string of 1 through 63 characters.

Configuring Duplication of Rf Records

Use the following configuration commands to configure the system to create a secondary feed of Rf records and send them to the secondary AAA group.

```
configure
   context context_name
      aaa group group_name
         diameter accounting duplicate-record
         exit
```

Notes:

- **duplicate-record**: Sends duplicate Rf records to configured secondary AAA group. This keyword is license dependent. For more information, contact your Cisco account representative.
- The default configuration is **no diameter accounting duplicate-record**. By default, this feature is disabled.
- The secondary aaa group must be configured under APN configuration mode before enabling the **diameter accounting duplicate-record** CLI command.

Verifying the Rf Duplicate Record Generation Configuration

Use the following commands to verify the configuration status of this feature.

show configuration

show aaa group all

- or -

show aaa group *group_name*

group_name must be the name of the AAA group specified during the configuration.

This command displays all the configurations that are enabled within the specified AAA group.

The following is a sample configuration of this feature.

```
configure
   context source
      apn domainname.com
         associate accounting-policy policy_accounting_name
         aaa group group1
         aaa secondary-group group2
         exit
      aaa group group1
         diameter accounting dictionary aaa-custom4
         diameter accounting endpoint rf_endpoint1
         diameter accounting server rf_server1 priority 1
         diameter accounting server rf_server2 priority 2
         exit
      aaa group group2
         diameter accounting dictionary aaa-custom4
```

```
            diameter accounting endpoint rf_endpoint2
            diameter accounting duplicate-record
            diameter accounting server rf_server3 priority 3
            diameter accounting server rf_server4 priority 4
            exit
        diameter endpoint rf-endpoint1
            use-proxy
            origin host rf-endpoint1.carrier.com address 192.50.50.3
            no watchdog-timeout
            response-timeout 20
            connection retry-timeout 5
            peer rf_server1 realm domainname.com address 192.50.50.4 port 4872
            peer rf_server2 realm domainname.com address 192.50.50.4 port 4873
            exit
        diameter endpoint rf-endpoint2
            use-proxy
            origin host rf-endpoint2.carrier.com address 192.50.50.2
            no watchdog-timeout
            response-timeout 20
            connection retry-timeout 5
            peer rf_server3 realm domainname.com address 192.50.50.5 port 4892
            peer rf_server4 realm domainname.com address 192.50.50.5 port 4893
end
```

Notes:

- The **diameter accounting duplicate-record** CLI is license specific. So, the corresponding license must be enabled for the CLI command to be configured.
- Both primary and secondary aaa groups are preferred to have different accounting endpoint names.

Monitoring and Troubleshooting the Rf Duplicate Record Generation

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

The following operations can be performed to troubleshoot any failure related to this feature:

- Verify if the feature is enabled using **show configuration** or **show aaa group all** CLI command. If not enabled, configure the diameter accounting duplicate-record CLI command and check if it works.
- Collect the output of **show diameter aaa statistics** command and analyze the debug statistics. Also, check the reported logs, if any. For further analysis, contact Cisco account representative.

show diameter aaa-statistics

The following statistics are added to the output of this show command for duplicate Rf records which were dropped because of the failure in sending the Accounting records instead of adding them to HDD or archival list.

- Duplicate Accounting Records Stats
  - ACR-Start Dropped
  - ACR-Interim Dropped

- ACR-Stop Dropped

These statistics are maintained per aaamgr instance level. For descriptions of these statistics, see the *Statistics and Counters Reference* guide.

These statistics can also be collected per group basis/server basis for duplicate records i.e. through **show diameter aaa-statistics group** <*group_name*> and **show diameter aaa-statistics server** <*server_name*> CLI commands.

Truncation of Virtual APN for Rf Records

This feature enables the truncation of Virtual APN (VAPN) returned by S6b server to be sent to Gx, Gy and Rf interfaces.

Feature Description

Currently there is no way to quickly turn on the Rf accounting to the Data Streaming Service (DSS) server per Virtual APN (S6b-VAPN) without reaching all nodes in the network and provision the Virtual APN on each of them. This feature is implemented to truncate the virtual APN name returned by S6b server with the configured standard delimiters. In this way a single configuration per node can be utilized for all enterprises based on a virtual APN. This approach will significantly reduce the size and time to provision new enterprises with the requested feature.

To achieve this functionality, a configuration is added per APN to enable truncation of S6b-VAPN and also to configure the delimiter(s) where the APN name is to be truncated. Standard delimiters like (.) and (-) are used since APN name supports only these two characters apart from the alphanumeric ones.

If AAA server returns both hyphen and dot delimiters or the same delimiter twice or more as a virtual-apn, then the first delimiter will be considered as a separator. For example, if the AAA server returns the virtual-apn as xyz-cisco.com, then hyphen is the separator.

AAA manager performs the truncation of the Virtual APN name based on the APN configuration and provides the correct APN profile for the truncated APN name. If the truncation is successful, the full virtual APN name will be sent to Gx, Gy and Rf interfaces.

Accounting records are required to support real-time usage notification and device management functionality. So, the **apn-name-to-be-included** CLI command is extended to enable actual APN (Gn-APN) or virtual APN (S6b returned virtual APN) name to be included in Called-Station-ID AVP in the secondary Rf accounting records (secondary server group) under policy accounting configuration. Currently, policy accounting configuration supports sending the Gn-APN/S6b-VAPN in Called-Station-ID for primary Rf server. With this CLI command, this functionality is extended for the secondary Rf server.

A new AAA attribute “Secondary-Called-Station-ID” is added to support sending Gn/Virtual APN name in the Called-Station-ID AVP for duplicate Rf records sent to secondary group Rf server.

Configuring Virtual APN Truncation for Rf Records

The following section provides the configuration commands to enable the Virtual APN Truncation feature for Rf records.

Configuring Gn-APN/VAPN for Rf Accounting

Use the following configuration commands to configure the actual APN or Virtual APN (VAPN) for Rf accounting.

```
configure
  context context_name
    policy accounting policy_name
      apn-name-to-be-included { gn | virtual } [ secondary-group { gn |
 virtual } ]
      end
```

Notes:

- **apn-name-to-be-included**: Configures the APN name to be included in the Rf messages for primary server group.
- **secondary-group { gn | virtual }**: Configures the APN name to be included in the Rf messages for secondary server group.
- **gn**: Configures the Gn APN name to be included in the Rf messages.
- **virtual**: Configures the virtual APN name to be included in the Rf messages.
- By default, the apn name to be included in Called-Station-ID AVP is Gn-APN for both primary and secondary Rf server groups.
- If the secondary group configuration is not available, the default behavior is to have Gn APN for secondary Rf group duplicate records.

Configuring Truncation of Virtual APN

Use the following configuration commands to configure the gateway to truncate the APN name returned from S6b interface.

```
configure
  context context_name
    apn apn_name
      virtual-apn { gcdr apn-name-to-be-included { gn | virtual } |
truncate-s6b-vapn delimiter { dot [ hyphen ] | hyphen [ dot ] } }
      end
```

Notes:

- For information on the existing keywords, see the *Command Line Interface Reference* guide.
- **truncate-s6b-vapn**: Allows truncation of virtual APN received from S6b at the configured delimiter character.
- **delimiter { dot [hyphen] | hyphen [dot] }**: Configures the delimiter for truncation of virtual APN received from S6b. If the CLI command is configured, the S6b returned virtual APN will be truncated at the configured delimiter.
  - **dot**: Configures the delimiter to dot (.) for truncation of S6b-VAPN
  - **hyphen**: Configures the delimiter to hyphen (-) for truncation of S6b-VAPN
- Both dot and hyphen delimiters can be configured in the same line or a new line.
- **no virtual-apn truncate-s6b-vapn**: Disables the truncation of virtual APN name. If both delimiters should be disabled at once, use the **no virtual-apn truncate-s6b-vapn** CLI command.

If a particular delimiter needs to disabled, it should be done explicitly. For example, if the dot delimiter should be disabled, use the **no virtual-apn truncate-s6b-vapn delimiter dot** CLI command.

- By default this feature will be disabled and no delimiter will be configured.
- This CLI command takes effect only when S6b server returns virtual APN name in Authentication Authorization Accept (AAA) message.
- If the separator character is not present in the received S6b virtual APN name, then the whole virtual APN name will be considered for configuration look-up.

Verifying the Virtual APN Truncation Configuration

Use the following command to verify the configuration status of this feature.

show configuration apn *apn_name*

apn_name must be the name of the APN specified during the feature configuration.

This command displays all the configurations that are enabled within the specified APN name. The following is a sample output of this show command.

```
[local]st40# show configuration apn intershat
configure
   context ingress
      apn intershat
         pdp-type ipv4 ipv6
         bearer-control-mode mixed
         virtual-apn truncate-s6b-vapn delimiter hyphen
         end
```

Monitoring and Troubleshooting the Virtual APN Truncation

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

The following operations can be performed to troubleshoot any failure related to this feature:

- Verify if the feature is enabled using **show configuration apn** *apn_name* CLI command. If not enabled, configure the **virtual-apn truncate-s6b-vapn delimiter { dot [hyphen] | hyphen [dot] } }** CLI command and check if it works.
- Collect the output of **show apn statistics** CLI command and analyze the debug statistics. For further assistance, contact Cisco account representative.

Important For P-GW, GGSN and SAEGW services, if the truncation of S6b returned virtual APN name fails and the virtual APN name is not configured, the call will be rejected with ‘unknown-apn-name’ cause.

show apn statistics

This show command uses the existing APN statistics to populate the truncated virtual APN name, if this feature is enabled.

show subscribers ggsn-only full all

The following field added newly to the output of this show command displays the S6b returned full virtual APN name, if this feature is enabled. Otherwise, it displays 'n/a’.

- S6b Returned Virtual APN

show subscribers pgw-only full all

The following field added newly to the output of this show command displays the S6b returned full virtual APN name, if this feature is enabled. Otherwise, it displays 'n/a’.

- S6b Returned Virtual APN

show subscribers saegw-only full all

The following field added newly to the output of this show command displays the S6b returned full virtual APN name, if this feature is enabled. Otherwise, it displays 'n/a’.

- S6b Returned Virtual APN

Accounting Record Stop Location Report

Previous Behavior: When P-GW or S-GW sends new User Location Information (ULI) message in an ACR stop message to Offline Charging System (OFCS) through the Rf interface, the reported location at the end of sessions was not aligning with the expected location reporting. The location used in the Accounting Stop Record (ACR Stop) was inconsistent and during location reporting it caused an `ACR stop` interim messages rather than the location before the ACR was sent

New Behavior: In the StarOS 21.22 and later releases, an existing User Location Information (ULI) is sent to the Accounting Record (ACR) Stop message on offline charging (RF) interface for GGSN, P-GW, and SAEGW when Delete Session Request is received with a New ULI.

How it Works

This section describes how offline charging for subscribers works with Rf interface support in GPRS/eHRPD/LTE/IMS networks.

The following figure and table explain the transactions that are required on the Diameter Rf interface in order to perform event based charging. The operation may alternatively be carried out prior to, concurrently with or after service/content delivery.

Figure 10: Rf Call Flow for Event Based Charging

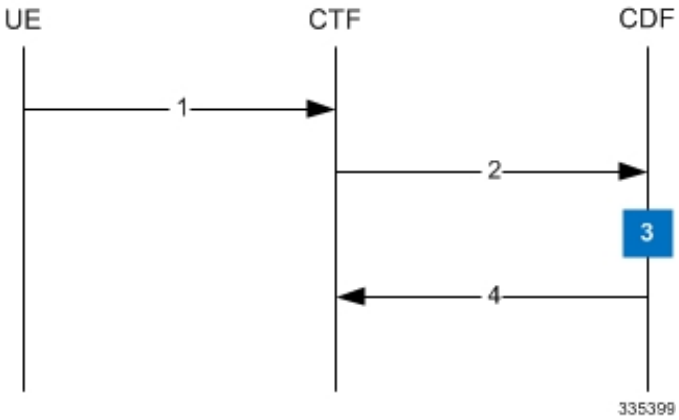


Table 12: Rf Call Flow Description for Event Based Charging

Step	Description
1	The network element (CTF) receives indication that service has been used/delivered.
2	The CTF (acting as Diameter client) sends Accounting-Request (ACR) with Accounting-Record-Type AVP set to EVENT_RECORD to indicate service specific information to the CDF (acting as Diameter server).
3	The CDF receives the relevant service charging parameters and processes accounting request.
4	The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type AVP set to EVENT_RECORD to the CTF in order to inform that charging information was received.

The following figure and table explain the simple Rf call flow for session based charging.

Figure 11: Rf Call Flow for Session Based Charging

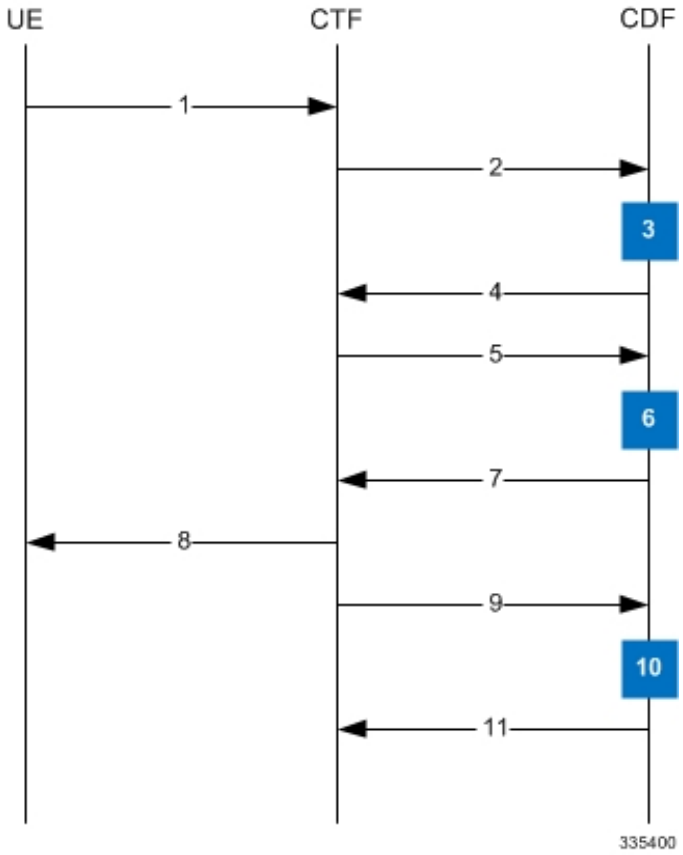


Table 13: Rf Call Flow Description for Session Based Charging

Step	Description
1	The CTF receives a service request. The service request may be initiated either by the user or the other network element.
2	In order to start accounting session, the CTF sends a Accounting-Request (ACR) with Accounting-Record-Type AVP set to START_RECORD to the CDF.
3	The session is initiated and the CDF opens a CDR for the current session.
4	The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type set to START_RECORD to the CTF and possibly Acct-Interim-Interval AVP (AII) set to non-zero value indicating the desired intermediate charging interval.

Step	Description
5	When either AII elapses or charging condition changes are recognized at CTF, the CTF sends an Accounting-Request (ACR) with Accounting-Record-Type AVP set to INTERIM_RECORD to the CDF.
6	The CDF updates the CDR in question.
7	The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type set to INTERIM_RECORD to the CTF.
8	The service is terminated.
9	The CTF sends a Accounting-Request (ACR) with Accounting-Record-Type AVP set to STOP_RECORD to the CDF.
10	The CDF updates the CDR accordingly and closes the CDR.
11	The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type set to STOP_RECORD to the CTF.

Configuring Rf Interface Support

To configure Rf interface support:

1. Configure the core network service as described in this Administration Guide.
2. Enable Active Charging Service (ACS) and create ACS as described in the *Enhanced Charging Services Administration Guide*.

Important The procedures in this section assume that you have installed and configured your chassis including the ECS installation and configuration as described in the *Enhanced Charging Services Administration Guide*.

3. Enable Rf accounting in ACS as described in Enabling Rf Interface in Active Charging Service, on page 138.
4. Configure Rf interface support as described in the relevant sections:
   - Configuring GGSN / P-GW Rf Interface Support, on page 138
   - Configuring P-CSCF/S-CSCF Rf Interface Support, on page 153

Important In StarOS versions 19 and later, the Rf interface is not supported on the S-GW.

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

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

Enabling Rf Interface in Active Charging Service

To enable the billing record generation and Rf accounting, use the following configuration:

```
configure
   active-charging service <service_name>
      rulebase <rulebase_name>
         billing-records rf
        active-charging rf { rating-group-override | service-id-override
 }
         end
```

Notes:

- Prior to creating the Active Charging Service (ACS), the **require active-charging** command should be configured to enable ACS functionality.
- The **billing-records rf** command configures Rf record type of billing to be performed for subscriber sessions. Rf accounting is applicable only for dynamic and predefined ACS rules.

  For more information on the rules and its configuration, refer to the *ACS Charging Action Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- The **active-charging rf** command is used to enforce a specific rating group / service identifier on all PCC rules, predefined ACS rules, and static ACS rules for Rf-based accounting. As this CLI configuration is applied at the rulebase level, all the APNs that have the current rulebase defined will inherit the configuration.

  For more information on this command, refer to the *ACS Rulebase Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Configuring GGSN / P-GW Rf Interface Support

To configure the standard Rf interface support for GGSN/P-GW, use the following configuration:

```
configure
   context <context_name>
      apn <apn_name>
         associate accounting-policy <policy_name>
         exit
      policy accounting <policy_name>
         accounting-event-trigger { cgi-sai-change | ecgi-change |
```

```
flow-information-change | interim-timeout | location-change | rai-change
 | tai-change } action { interim | stop-start }
         accounting-keys qci
accounting-level { flow | pdn | pdn-qci | qci | sdf | subscriber }
         cc profile index { buckets num | interval seconds | sdf-interval
seconds | sdf-volume { downlink octets { uplink octets } | total octets |
uplink octets { downlink octets } }  | serving-nodes num | tariff time1 min
hrs [ time2 min hrs...time4 min hrs ] | volume { downlink octets { uplink octets
 } | total octets | uplink octets { downlink octets } } }
         max-containers { containers | fill-buffer }
         end
```

Notes:

- The policy can be configured in any context.
- For information on configuring accounting levels/policies/modes/event triggers, refer to the *Accounting Policy Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- Depending on the triggers configured, the containers will either be cached or released. In the case of GGSN/P-GW, the containers will be cached when the event trigger is one of the following:
  - QOS_CHANGE
  - FLOW_INFORMATION_CHANGE
  - LOCATION_CHANGE
  - SERVING_NODE_CHANGE
  - SERVICE_IDLE
  - SERVICE_DATA_VOLUME_LIMIT
  - SERVICE_DATA_TIME_LIMIT
  - IP_FLOW_TERMINATION
  - TARIFF_CHANGE

  If the event trigger is one of the following, the containers will be released:
  - VOLUME_LIMIT
  - TIME_LIMIT
  - RAT_CHANGE
  - TIMEZONE_CHANGE
  - PLMN_CHANGE

Important Currently, SDF and flow level accounting are supported in P-GW.

The following assumptions guide the behavior of P-GW, GGSN and CCF for Change-Condition triggers:

- Data in the ACR messages due to change conditions contain the snapshot of all data that is applicable to the interval of the flow/session from the previous ACR message. This includes all data that is already sent and has not changed (e.g. SGSN-Address).
- All information that is in a PDN session/flow up to the point of the Change-Condition trigger is captured (snapshot) in the ACR-Interim messages. Information about the target Time-Zone/ULI/3GPP2-BSID/QoS-Information/PLMN Change/etc will be in subsequent Rf messages.

Table 14: P-GW/GGSN and CCF Behavior for Change-Condition in ACR-Stop and ACR-Interim for LTE/e-HRPD/GGSN

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Stop	Normal Release	YES	NO	YES	Normal Release	Normal Release	When PDN/IP session is closed, C-C in both level will have Normal Release.
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Normal Release	YES	NO	NO	N/A	Normal Release	Flow is closed, SDC CC is populated and closed container is added to record. The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or AII trigger (Interim) trigger.
Stop	Abnormal Release	YES	NO	YES	Abnormal Release	Abnormal Release	When PDN/IP session is closed, C-C in both level will have Abnormal Release.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Abnormal Release	YES	NO	NO	N/A	Abnormal Release	Flow is closed, SDC CC is populated and closed container is added to record. The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or AII trigger (Interim) trigger.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	QoS-Change	YES	NO	NO	N/A	QoS-Change	The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or AII trigger (Interim) trigger.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Interim	Volume Limit	YES	YES	NO	Volume Limit	Volume Limit	For PDN/IP Session Volume Limit. The Volume Limit is configured as part of the Charging profile and the Charging Characteristics AVP will carry this charging profile that will passed on from the HSS/AAA to P-GW/GGSN through various interfaces. The charging profile will be provisioned in the HSS.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Interim	Time Limit	YES	YES	NO	Time Limit	Time Limit	For PDN/IP Session Time Limit. The Time Limit is configured as part of the Charging profile and the Charging Characteristics AVP will carry this charging profile that will passed on from the HSS/AAA to P-GW/GGSN through various interfaces. The charging profile will be provisioned in the HSS.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Serving Node Change	YES	NO	NO	N/A	Serving Node Change	The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or AII trigger (Interim) trigger.
Interim	Serving Node PLMN Change	YES	YES	NO	Serving Node PLMN Change	Serving Node PLMN Change	

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	User Location Change	YES	NO	NO	N/A	User Location Change	This is BSID Change in eHRPD. The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or AII trigger (Interim) trigger.
Interim	RAT Change	YES	YES	NO	RAT Change	RAT Change	
Interim	UE Timezone Change	YES	YES	NO	UE Timezone change	UE Timezone change	This is not applicable for eHRPD.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Tariff Time Change	YES	NO	NO	N/A	Tariff Time Change	Triggered when Tariff Time changes. Tariff Time Change requires an online charging side change. The implementation of this Change Condition is dependent on implementation of Online Charging update.
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Service Idled Out	YES	NO	NO	N/A	Service Idled Out	Flow Idled out. The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or AII trigger (Interim) trigger.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Service Data Volume Limit	YES	NO	NO	N/A	Service Data Volume Limit	Volume Limit reached for a specific flow. The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or AII trigger (Interim) trigger.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Service Data Time Limit	YES	NO	NO	N/A	Service Data Time Limit	Time Limit reached for a specific flow. The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or AII trigger (Interim) trigger.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Interim	Max Number of Changes in Charging Conditions	YES	YES	NO	YES	YES, Will include SDC that correponds to the CCs that occurred (Normal Release of Flow, Abnormal Release of Flow, QoS-Change, Serving Node Change, User Location Change, Tariff Time Change, Service Idled Out, Service Data Volunme Limt, Service Data Time Limit)	

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
							This ACR[Interim] is triggered at the instant when the Max Number of changes in charging conditions takes place. Max Change Condition is applicable for QoS-Change, Service-Idled Out, ULI change, Flow Normal Release, Flow Abnormal Release, Service Data Volume Limit, Service Data Time Limit, AII Timer ACR Interim and Service Node Change CC only. The Max Number of Changes in Charging Conditions is set at 10. Example assuming 1 flow in the PDN Session: [1] Max Number of Changes in Charging Conditions

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
							set at P-GW/GGSN = 2. [2] Change Condition 1 takes place. No ACR Interim is sent. P-GW/GGSN stores the SDC. [3] Change Condition 2 takes place. An ACR Interim is sent. Now Max Number of Changes in Charging conditions is populated in the PS-Information 2 Service Data Containers (1 for each change condition) are populated in the ACR Interim. [4] CCF creates the partial record.
Stop	Management Intervention	YES	NO	YES	YES	YES	Management intervention will close the PDN session from P-GW/GGSN.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Interim	-	YES	NO	NO	N/A	N/A	This is included here to indicate that an ACR[Interim] due to AII timer will contain one or more populated SDC/s for a/all flow/s, but Change-Condition AVP will NOT be populated.

Configuring P-CSCF/S-CSCF Rf Interface Support

To configure P-CSCF/S-CSCF Rf interface support, use the following configuration:

```
configure
   context vpn
      aaa group default
         diameter authentication dictionary aaa-custom8
         diameter accounting dictionary aaa-custom2
         diameter accounting endpoint <endpoint_name>
         diameter accounting server <server_name> priority <priority>
         exit
      diameter endpoint <endpoint_name>
         origin realm <realm_name>
         use-proxy
         origin host <host_name> address <ip_address>
         peer <peer_name> address <ip_address>
         exit
      end
```

Notes:

- For information on commands used in the basic configuration for Rf support, refer to the *Command Line Interface Reference*.

Gathering Statistics

This section explains how to gather Rf and related statistics and configuration information.

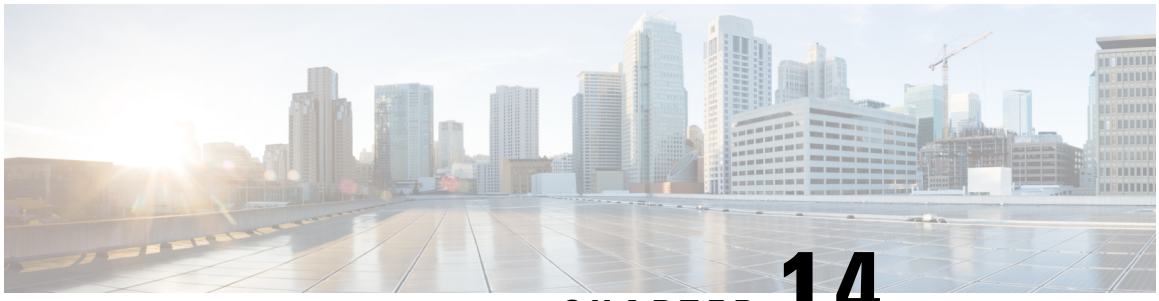
In the following table, the first column lists what statistics to gather, and the second column lists the action to perform.

Statistics/Information	Action to perform
Complete statistics for Diameter Rf accounting sessions	**show diameter aaa-statistics**

The following is a sample output of the **show diameter aaa-statistics** command:

```
Authentication  Servers Summary
 ------------------------------
Message Stats :
  Total MA Requests:            0        Total MA Answers:              0
  MAR - Retries:                0        MAA Timeouts:                  0
  MAA - Dropped:                0
  Total SA Requests:            0        Total SA Answers:              0
  SAR - Retries:                0        SAA Timeouts:                  0
  SAA - Dropped:                0
  Total UA Requests:            0        Total UA Answers:              0
  UAR - Retries:                0        UAA Timeouts:                  0
  UAA - Dropped:                0
  Total LI Requests:            0        Total LI Answers:              0
  LIR - Retries:                0        LIA Timeouts:                  0
  LIA - Dropped:                0
  Total RT Requests:            0        Total RT Answers:              0
  RTR - Rejected:               0
  Total PP Requests:            0        Total PP Answers:              0
  PPR - Rejected:               0
  Total DE Requests:            0        Total DE Answers:              0
  DEA - Accept:                 0        DEA - Reject:                  0
  DER - Retries:                0        DEA Timeouts:                  0
  DEA - Dropped:                0
  Total AA Requests:            0        Total AA Answers:              0
  AAR - Retries:                0        AAA Timeouts:                  0
  AAA - Dropped:                0
  ASR:                          0        ASA:                           0
  RAR:                          0        RAA:                           0
  STR:                          0        STA:                           0
  STR - Retries:                0
Message Error Stats:
  Diameter Protocol Errs:       0        Bad Answers:                   0
  Unknown Session Reqs:         0        Bad Requests:                  0
  Request Timeouts:             0        Parse Errors:                  0
  Request Retries:              0
Session Stats:
  Total Sessions:               0        Freed Sessions:                0
  Session Timeouts:             0        Active Sessions:               0
STR Termination Cause Stats:
  Diameter Logout:              0        Service Not Provided:          0
  Bad Answer:                   0        Administrative:                0
  Link Broken:                  0        Auth Expired:                  0
  User Moved:                   0        Session Timeout:               0
  User Request:                 0        Lost Carrier                   0
  Lost Service:                 0        Idle Timeout                   0
  NAS Session Timeout:          0        Admin Reset                    0
  Admin Reboot:                 0        Port Error:                    0
  NAS Error:                    0        NAS Request:                   0
  NAS Reboot:                   0        Port Unneeded:                 0
  Port Preempted:               0        Port Suspended:                0
  Service Unavailable:          0        Callback:                      0
  User Error:                   0        Host Request:                  0
 Accounting Servers Summary
```

```
 ---------------------------
Message Stats :
  Total AC Requests:             0        Total AC Answers:              0
  ACR-Start:                     0        ACA-Start:                     0
  ACR-Start  Retries :           0        ACA-Start  Timeouts:           0
  ACR-Interim:                   0        ACA-Interim:                   0
  ACR-Interim  Retries :         0        ACA-Interim  Timeouts:         0
  ACR-Event:                     0        ACA-Event:                     0
  ACR-Stop :                     0        ACA-Stop:                      0
  ACR-Stop  Retries :            0        ACA-Stop  Timeouts:           0
  ACA-Dropped :                  0
AC Message Error Stats:
  Diameter Protocol Errs:        0        Bad Answers:                   0
  Unknown Session Reqs:          0        Bad Requests:                  0
  Request Timeouts:              0        Parse Errors:                  0
  Request Retries:               0
```



CHAPTER 14

Source Port Randomization on VPP for GTP-U Traffic

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 - License Required
Related Changes in This Release	Not Applicable
Related Documentation	*Command Line Interface Reference*

Revision Details	Release
First introduced.	21.22

Feature Description

Some Routers and switches in the core network balances packet load that crosses multiple links in LAG or ECMP by calculating a hash value based on packet header fields. To have a better load balance of traffic on core network fabric, it is essential to support randomized GTP-U source port functionality on the VPP-enabled ASR 5500 platform.

On the S5/S8 interface, the GTP header encapsulates the downlink user traffic with same destination/source IP address, destination/source port, and subscriber TEID. If there are incoming packets of 5 Gbps or higher single UE throughput traffic, the GTP-U traffic's IP addresses, ports, and TEID are all the same. GTP-U header fields hash polarization leads to uneven load distribution among LAG and ECMP member links and causes packets drop.

For the Downlink Traffic, the VPP does source port randomization based on the inner packet flow. The source port of the outer header (GTP-U packet) is randomized on the S5/S8 interface.

To enable randomized GTP-U source port, in the GTP-U Service Configuration Mode, the **source-port non-standard** CLI command is added. The port range supported is 32768–33791.

Note P-GW uses GTP-U interheader to do hashing for load balance and distributes the load evenly to all LAG/interfaces.

Enabling Source Port Randomization for GTP-U Traffic

Use the following configuration command to enable source port randomization.

```
configure
  context context_name
    gtpu-service service_name
      source-port non-standard
  end
```

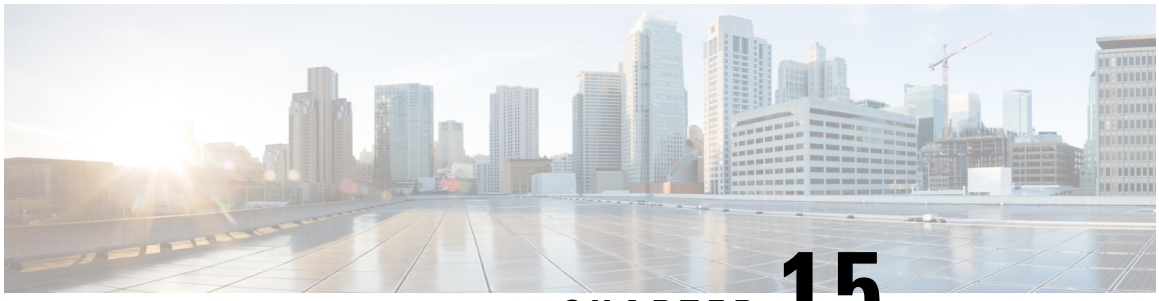
NOTES:

- **source-port non-standard**: Configures randomized non-standard source port downlink to GTP-U data packets.

Verifying GTP-U Source Port Randomization

show gtpu-service name

The **show gtpu-service name** *gtpu_service_name* CLI command now includes the value for the **GTPU Source-port non-standard** value.



CHAPTER 15

S6b Interface Enhancement

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 - License Required
Related Changes in This Release	Not Applicable
Related Documentation	• *P-GW Administration Guide*

Revision History

Revision Details	Release
In this release, the S6b interface is enhanced to align with the 3GPP AAA with the allocation of static and dynamic IP addresses through AVPs.	21.22

Feature Description

In the StarOS 21.22 and later releases, the S6b interface is enhanced to align with the 3GPP AAA with the allocation of static and dynamic IP addresses through the following AVPs:

- **Class AVP**

- **User-Name AVP**
- **Origination-Time-Stamp AVP**

Class AVP: The following enhancement is supported:

During the initial PDN connection request, PGW/GGSN receives the CLASS AVP, if available, in the AA Answer message from 3GPP AAA. Then, P-GW/GGSN sends Answer to 3GPP AAA. While sending AA_request message to 3GPP AA, P-GW/GGSN drops the CLASS AVP. PGW/GGSN has the option to initiate re-authorization. However, if P-GW/GGSN has previously received the CLASS AVP from 3GPP AAA, it includes Class AVP in subsequent session termination requests but not re-authorization requests. It results in removal of Class AVP from all messages except AA Answer and Session-Termination messages (STR and STA messages).

If Auth-Session-State is negotiated as STATE_MAINTAINED, then on session termination, P-GW initiates a Session-Termination-Request {Session-Id, Origin-Host, Origin-Realm, Destination-Realm, Auth-Application-Id=(16777999), Destination-Host, Termination-Cause, User-Name } to the 3GPP AAA.

Note The Class AVP can only be removed from the instances wherever `aaa-custom15` dictionary is used.

User-Name AVP: The following enhancement is supported.

When P-GW/GGSN sends subsequent session termination (STR) requests to 3GPP AAA, it includes the mandatory parameter, **User-Name AVP**.

Note During backward compatibility, 3GPP AAA accepts STR without **User-Name AVP**.

Ensure that the User-Name doesn't include prefix.

For Example:

```
<IMSI>@nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org.
```

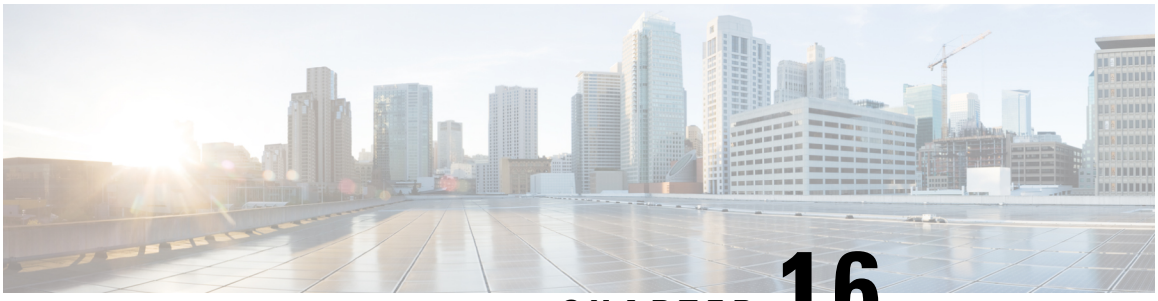
Origination-Time-Stamp AVP: The following enhancement is supported.

The **Origination-TimeStamp AVP** is replaced with the 3GPP standard Origination-Time-Stamp AVP.

Maximum-Wait-Time AVP: The following enhancement is supported.

The **Max-Wait-Time AVP** is replaced with 3GPP standard Maximum-Wait-Time AVP **Maximum-Wait-Time AVP**.

Note For more details about S6b Interface, refer the *S6b Interface* section in the *PDN Gateway Overview* chapter of the *P-GW Administration Guide*.



CHAPTER 16

Support for Common access-type in twan-profile for EoGRE-PMIP Calls

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SaMOG
Applicable Platform(s)	Cisco ASR 5500
Default Setting	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *SaMOG Administration Guide*

Revision History

Revision Details	Release
In this release, SaMOG access-type, supports cisco-mpc-protocol-interface attribute-value pair.	21.22.11
First introduced.	21.21

Feature Description

SaMOG supports the common access-type, **eogre-pmip**, in a twan-profile to handle both PMIP and EoGRE calls. Because of this common access-type the RADIUS client is mapped with two different access types by defining in one twan-profile. SaMOG allows same RADIUS Client IP to be used for PMIP and EoGRE calls.

AVP Enhancement: In this StarOS release 21.22 and later releases, SaMOG access-type, **eogre-pmip**, supports cisco-mpc-protocol-interface attribute-value pair (AVP) to configure one of the following values:

- none: Selecting this value configures cisco-mpc-protocol-interface AVP as none. It is neither eogre nor pmipv6.
- eogre: Selecting this value configures cisco-mpc-protocol-interface AVP as eogre.
- pmipv6: Selecting this value configures cisco-mpc-protocol-interface AVP as pmipv6.
- suppress: Selecting this value suppresses cisco-mpc-protocol-interface AVP and it is not sent to the Access-Accept message.

How it Works

This section describes how common access types work in the following scenarios:

- Attach Call flow with PMIP Access-Type
- Attach Call Flow with EoGRE Access-Type
- EoGRE to PMIP Handover
- PMIP to EoGRE Handover

Attach Call Flow with PMIP Access-Type

Attaching call flows with Proxy Mobile IP (PMIP) and Ethernet over GRE (EoGRE) are performed simultaneously in SaMOG. The access-type is set up after receiving Proxy Binding Update (PBU) or DHCP request from Wireless LAN Controller (WLC). The call flows explain the twan-profile that is configured with new access-type **eogre-pmip**.

Figure 12: Call Flow

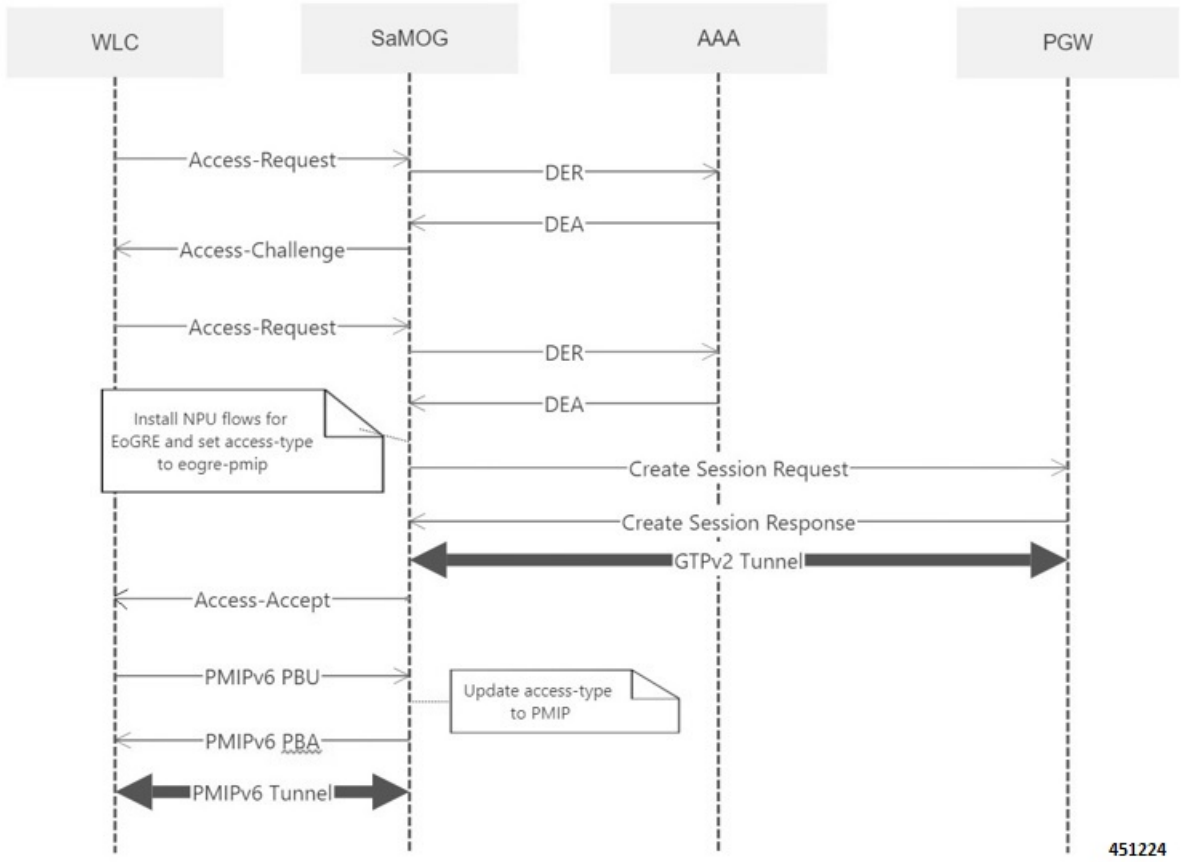


Table 15: Procedure

Step	Description
1	The UE initiates an initial attach procedure towards the WLC. The WLC forms an Access-Request message with the EAP-Identity payload, User-Name and Acct-Session-Id, and sends the same to SaMOG.
2	SaMOG forms a Radius Access-Request or Diameter DER message towards the AAA server using the attributes received from the WLC.
3	The AAA server performs an Extensible Authentication Protocol (EAP) authentication and sends the Access-Challenge or DEA to SaMOG with the EAP payload
4	SaMOG copies the EAP payload to the Access-Challenge towards WLC. The WLC sends an EAP request towards UE.
5	The UE sends an EAP response. The WLC sends the Access-Request to SaMOG with the EAP payload received from the UE.

Step	Description
6	SaMOG sends the Access-Request or DER to the AAA server with the EAP payload.
7	The AAA server fetches the subscriber profile from HLR/HSS and validates the EAP Challenge response sent from the UE. The Access-Accept/DEA is sent to SaMOG with the user profile and EAP Success payload. SaMOG saves the user profile information. After UE authentication, SaMOG installs the NPU flows related to EoGRE and sets the access-type to **eogre-pmip**.
8	SaMOG performs DNS procedures towards the DNS server to get the P-GW/GGSN IP address.
9	SaMOG delays sending the Access-Accept to the WLC and initiates S2a/Gn procedures towards P-GW/GGSN, by including the IMEIs V IE with the UE MAC value received as **Calling-Station-ID** AVP in the Access-Request, if sending of IE is enabled through configuration.
10	SaMOG sends Access-Accept to the WLC with EAP-Success payload after completion of S2a or Gn procedures. The WLC sends EAP-Success to the UE.
11	The UE sends DHCP discover (broadcast) request to the WLC. The WLC acts as a DHCP server and initiates PMIPv6 PBU towards SaMOG for L3 Attachment by including the NAI and Service-Selection parameters
12	SaMOG processes the received PMIPv6 PBU and responds back with a PMIPv6 PBA by including the allocated home-address by P-GW/GGSN and the default gateway IP address. SaMOG updates the access-type to PMIP based on the received PBU message
13	The WLC sends a DHCP offer towards the UE with the allocated UEs IP address and the default gateway.
14	The UE sends DHCP request to the WLC for DHCP, by including router options and the allocated UE's IP address for further confirmation. The WLC sends DHCP Ack message to the UE. If proxy accounting is enabled, SaMOG will proxy accounting messages between the WLC and AAA server.
15	The UE performs ARP request for the default gateway received from SaMOG. The WLC includes the virtual MAC address in the ARP response for the received Default gateway IP address in the ARP.

Attach Call Flow with EoGRE Access-Type

This section explains the initilizaton call flow and procedure of EoGRE calls.

Figure 13: Call Flow

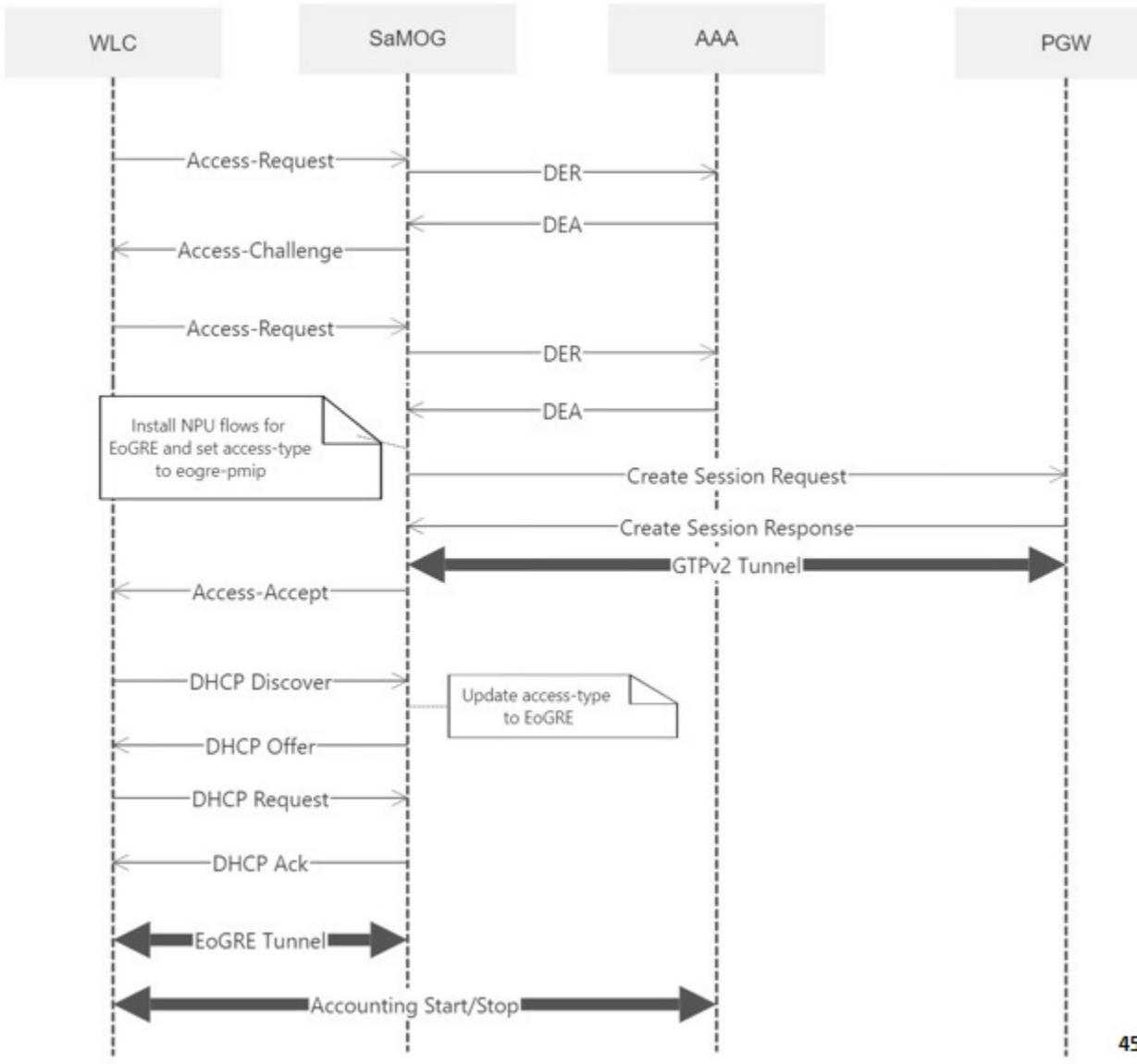


Table 16: Procedure

Step	Description
1	The UE initiates an initial attach procedure towards the Wireless LAN Controller (WLC). The WLC forms an Access-Request message with the EAP-Identity payload, User-Name and Acct-Session-Id, and sends the same to SaMOG.
2	SaMOG forms a Radius Access-Request or Diameter DER message towards the AAA server using the attributes received from the WLC.

Step	Description
3	The AAA server performs an EAP authentication and sends the Access-Challenge or DEA to SaMOG with the EAP payload.
4	SaMOG copies the EAP payload to the Access-Challenge towards WLC. The WLC sends an EAP Request towards UE.
5	The UE sends an EAP response. The WLC sends the Access-Request to SaMOG with the EAP payload received from the UE.
6	SaMOG sends the Access-Request or DER to the AAA server with the EAP payload.
7	The AAA server fetches the subscriber profile from HLR/HSS and validates the EAP Challenge response sent from the UE. The Access-Accept/DEA is sent to SaMOG with the user profile and EAP Success payload. SaMOG saves the user profile information. After UE authentication, SaMOG installs the NPU flows related to EoGRE and sets the access-type to **eogre-pmip**.
8	SaMOG performs DNS procedures towards the DNS server to get the P-GW/GGSN IP address.
9	SaMOG delays sending the Access-Accept to the WLC and initiates S2a/Gn procedures towards P-GW/GGSN, by including the IMEIs V IE with the UE MAC value received as **Calling-Station-ID** AVP in the Access-Request, if sending of IE is enabled through configuration.
10	SaMOG sends Access-Accept to the WLC with EAP-Success payload after completion of S2a/Gn procedures. The WLC sends EAP-Success to the UE.
11	The UE sends DHCP discover (broadcast) request to the WLC. The WLC acts as a DHCP server and initiates DHCP discover over EoGRE tunnel towards SaMOG for L3 Attachment.
12	SaMOG processes the received PMIPv6 PBU and responds back with a PMIPv6 PBA by including the allocated home-address by P-GW/GGSN and the default gateway IP address. SaMOG updates the access-type to EoGRE based on the received DHCP Discover message.
13	The WLC sends a DHCP offer towards the UE with the allocated UE's IP address and the default gateway. The UE sends DHCP request to the WLC for DHCP, by including router options and the allocated UE's IP address for further confirmation. The WLC acts as a DHCP server and initiates a DHCP Request over the EoGRE tunnel towards SaMOG.
14	SaMOG processes the received DHCP Request over the EoGRE tunnel and respond back with a DHCP Ack over the EoGRE tunnel by including the DNS Parameters in the router options. The WLC sends a DHCP Acknowledgement towards the UE. If proxy accounting is enabled, SaMOG will proxy accounting messages between the WLC and AAA server.

Step	Description
15	The UE performs an ARP request for the default gateway received from SaMOG. The WLC sends the ARP request packets over the EoGRE tunnel and SaMOG responds back with an ARP Response over the EoGRE tunnel by including the virtual MAC address of the default gateway.

EoGRE to PMIP Handover

This section explains the handover call flow and procedure of EoGRE to PMIP calls.

Figure 14: Call Flow

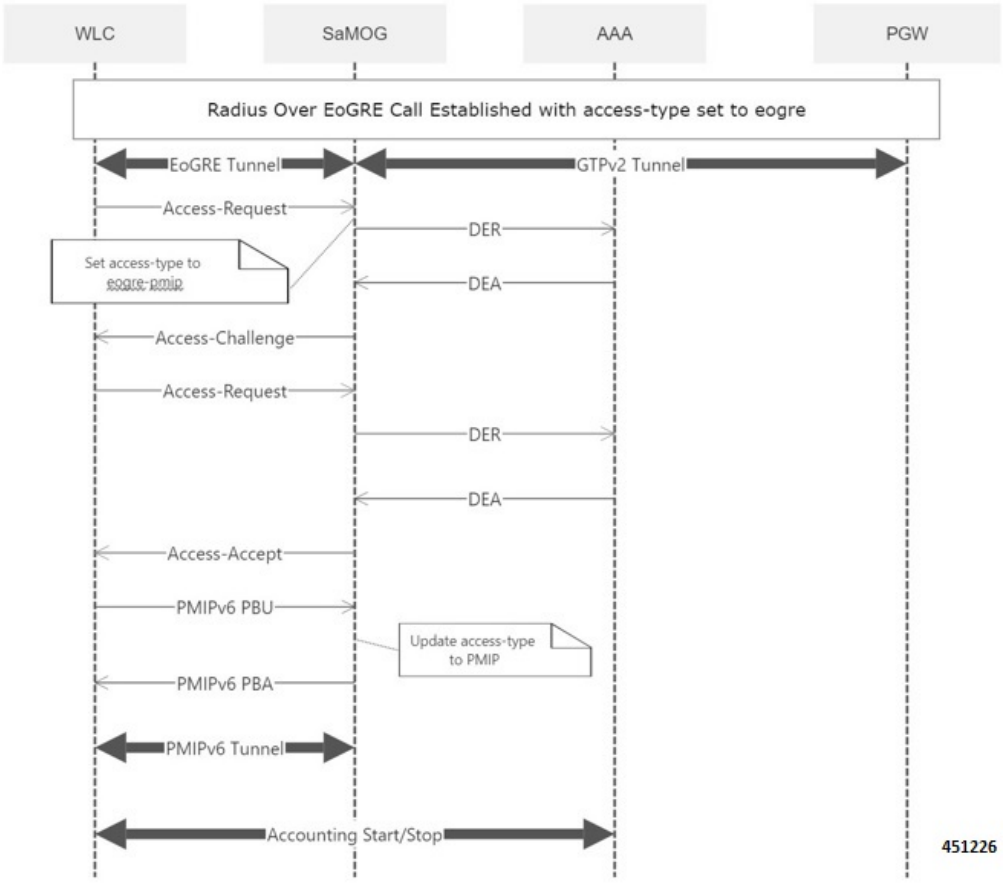


Table 17: Procedure

Step	Description
1	UE is attached to the network as described in the PMIP call flow.
2	The WLC forms an Access-Request message with the EAP-Identity payload, User-Name and Acct-Session-Id, and sends the same to SaMOG.

Step	Description
3	SaMOG treats the call as a handoff request based on the twan-profile configuration (with access-type as eogre-pmip). The access-type is set to eogre-pmip as this could be an EoGRE to PMIP or an EoGRE to EoGRE case.
4	SaMOG forms a Radius Access-Request or Diameter DER message towards the AAA server using the attributes received from the WLC.
5	The AAA server performs an EAP authentication and sends the Access-Challenge/DEA to SaMOG with the EAP payload.
6	SaMOG copies the EAP payload to the Access-Challenge towards WLC. The WLC sends an EAP Request towards UE.
7	The UE sends an EAP response. The WLC sends the Access-Request to SaMOG with the EAP payload received from the UE.
8	SaMOG sends the Access-Request/DER to the AAA server with the EAP payload.
9	The AAA server fetches the subscriber profile from HLR/HSS and validates the EAP Challenge response sent from the UE. The Access-Accept/DEA is sent to SaMOG with the user profile and EAP Success payload. SaMOG saves the user profile information.
10	SaMOG sends Access-Accept to the WLC with EAP-Success payload after completion of authentication procedures. The WLC sends EAP-Success to the UE.
11	The UE sends DHCP discover (broadcast) request to the WLC. The WLC acts as a DHCP server and initiates PMIPv6 PBU towards SaMOG for L3 Attachment by including the NAI and Service-Selection parameters.
12	SaMOG will process the received PMIPv6 PBU and responds back with a PMIPv6 PBA by including the allocated home-address by P-GW/GGSN and the default gateway IP address. SaMOG updates the access-type to PMIP based on the received PBU message.
13	The WLC sends a DHCP offer towards the UE with the allocated UEs IP address and the default gateway. The UE sends DHCP request to the WLC for DHCP, by including router options and the allocated UE's IP address for further confirmation. The WLC sends DHCP Ack message to the UE.
14	If proxy accounting is enabled, SaMOG will proxy accounting messages between the WLC and AAA server.

PMIP to EoGRE Handover

This section explains the handover call flow and procedure of Proxy Mobile IP (PMIP) to Ethernet over GRE (EoGRE) calls.

Figure 15: Call Flow

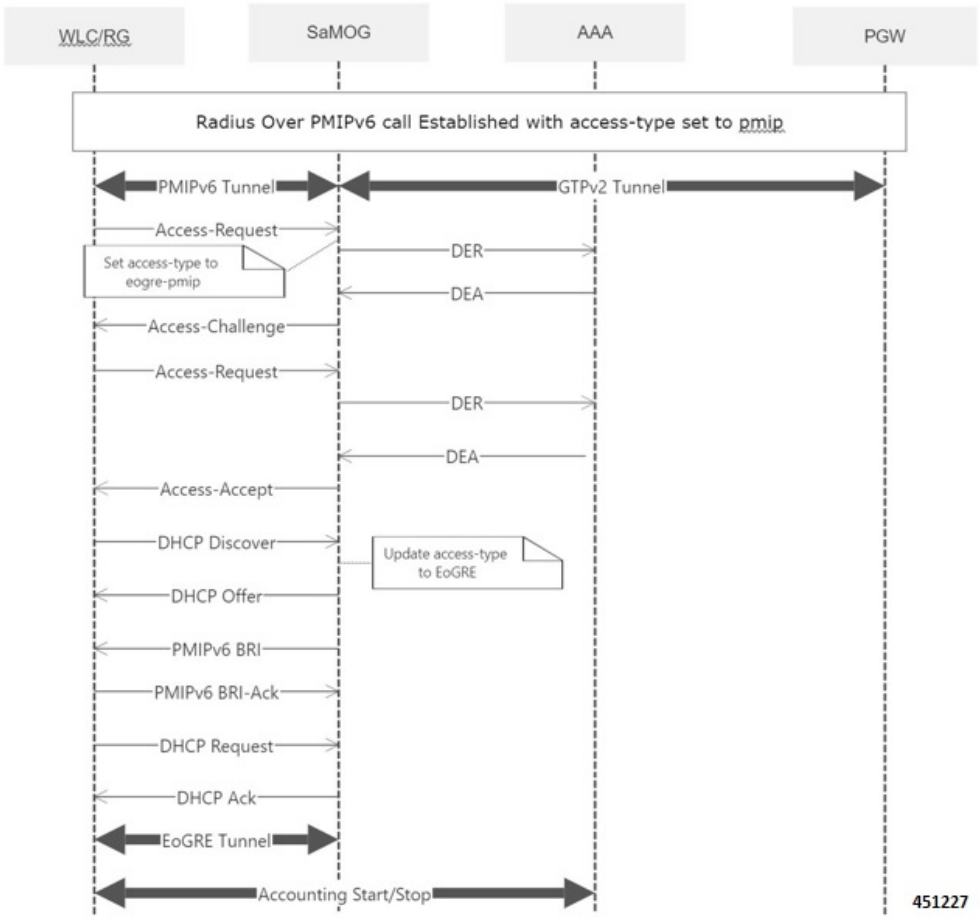


Table 18: Procedure

Step	Description
1	UE is attached to the network as described in the PMIP call flow.
2	The UE initiates an initial attach procedure towards the Wireless LAN Controller (WLC). The WLC forms an Access-Request message with the **EAP-Identity payload** , **User-Name** and **Acct-Session-Id**, and sends the same to SaMOG.
3	SaMOG treats the call as a handoff request based on the twan-profile configuration (with access-type as eogre-pmip). The access-type is set to eogre-pmip as this could be a PMIP to PMIP or a PMIP to EoGRE case.

Step	Description
4	SaMOG forms a Radius Access-Request or Diameter DER message towards the AAA server using the attributes received from the WLC.
5	The AAA server performs an Extensible Authentication Protocol (EAP) authentication and sends the Access-Challenge/DEA to SaMOG with the EAP payload.
6	SaMOG copies the EAP payload to the Access-Challenge towards WLC. The WLC sends an EAP Request towards the UE.
7	The UE sends an EAP response. The WLC sends the Access-Request to SaMOG with the EAP payload received from the UE.
8	SaMOG sends the Access-Request/DER to the AAA server with the EAP payload.
9	The AAA server fetches the subscriber profile from HLR/HSS and validates the EAP Challenge response sent from the UE. The Access-Accept/DEA is sent to SaMOG with the user profile and EAP Success payload. SaMOG saves the user profile information.
10	SaMOG sends Access-Accept to the WLC with EAP-Success payload after completion of S2a/Gn procedures. The WLC sends EAP-Success to the UE.
11	The UE sends DHCP discover (broadcast) request to the WLC. The WLC acts as a DHCP server and initiates DHCP discover over EoGRE tunnel towards SaMOG for L3 Attachment.
12	SaMOG will process the received DHCP discover over EoGRE tunnel and responds back with a DHCP Offer over the EoGRE tunnel by including the allocated home-address by P-GW/GGSN and the default gateway IP address. SaMOG updates the access-type to EoGRE based on the received DHCP Discover message.
13	The WLC sends a DHCP offer towards the UE with the allocated UE's IP address and the default gateway. The UE sends DHCP request to the WLC for DHCP, by including router options and the allocated UE's IP address for further confirmation. The WLC acts as a DHCP server and initiates a DHCP Request over the EoGRE tunnel towards SaMOG.
14	SaMOG processes the received DHCP Request over the EoGRE tunnel and respond back with a DHCP Ack over the EoGRE tunnel by including the DNS Parameters in the router options. The WLC sends a DHCP Ack towards the UE. If proxy accounting is enabled, SaMOG will proxy the accounting messages between the WLC and the AAA server.

Configuring Eogre-PMIP access-type in twan-profile

Use the following configuration to configure **eogre-pmip** access type. The **eogre-pmip** access type is configured only with radius trigger type.

```
configure
   context context_name
      twan-profile profile_name
        access-type eogre-pmip
          end
```

Notes:

- **access-type eogre-pmip** : Enables EoGRE or PMIP Access type for all clients under profile.

Note The **eogre-pmip** cannot be configured in combination with other access-types like EoGRE, PMIP and IP.

Configuring AVP

Use the following command to configure cisco-mpc-protocol interface.

```
configure
   context context_name
     twan-profile profile_name
       [ no ] radius cisco-mpc-protocol-interface
cisco-mpc-protocol-interface_value
   end
```

NOTES:

- **cisco-mpc-protocol-interface**: Configures cisco-mpc-protocol-interface AVP for access-type eogre-pmip.
- *cisco-mpc-protocol-interface_value*: cisco-mpc-protocol-interface value. You can enter one of the values, none, eogre, pmipv6, suppress.
- **no**: Removes configuration for cisco-mpc-protocol-interface AVP.

Limitations

The Common access-type in twan-profile feature has the following limitations:

- Supports only Access-Types (EoGRE/PMIPv6). IP Access-Type is not supported.
- Supports only Radius Access-Request trigger type. DHCP, PMIP, and Accounting-based trigger types are not supported.
- Support is limited to GTPv2 based s2a interface.

- Because IP Access-Type is not supported, Handover (HO) scenarios from/to IP Access-Type to/from EoGRE/PMIP access-types are not supported.
- The new access-type **eogre-pmip** is applicable only for radius Access-Request trigger type.
- The new access-type **eogre-pmip** cannot be configured with other access-types (EoGRE, PMIP, IP) in other twan-profiles.

Monitoring and Troubleshooting

Show commands and Outputs

Show twan-profile

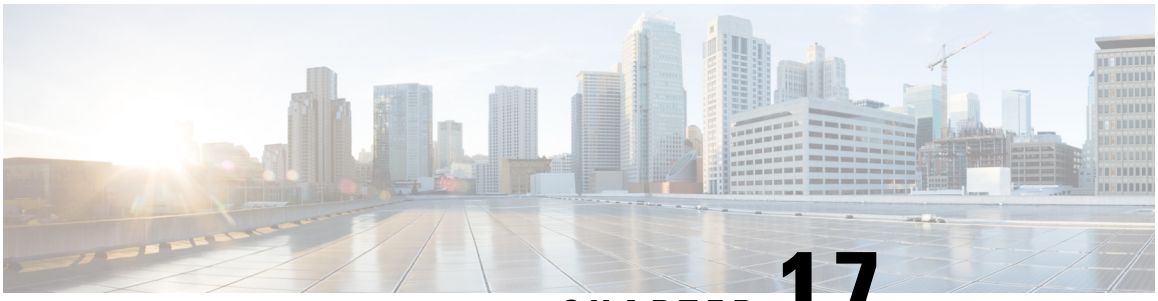
The following details are displayed to the output of the **show twan-profile { all | name** *profile_name* **}** command in support of this feature:

```
TWAN Profile Name         : twan1
    Access-Type Client List
        Default Access Type                : EOGRE-PMIP
        Default Radius Dictionary          : custom 70
        Session Trigger Type               : Radius
       Location reported from DHCP Option 82 : Not Enabled
```

Table 19: show twan-profile Command Output Descriptions

Field	Description
TWAN Profile Name	Name of the TWAN profile
Access-Type Client List	
cisco-mpc-protocol-interface	Indicates cisco-mpc-protocol-interface AVP configuration for access-type eogre-pmip.
Default Access Type	Default access type set for the TWAN profile. Access type for the TWAN profile for RADIUS-based session trigger is Eogre-PMIP. If access-type is not configured, then default value would be PMIP. When configured, the appropriate access-type is displayed in this field.
Default Radius Dictionary	Default RADIUS dictionary used for the TWAN profile. The default RADIUS dictionary can be one of the following: • custom70 for non-Cisco WLC

Field	Description
Session Trigger Type	The session trigger type set for the TWAN profile. Session Trigger type must be only **Radius**.
Location reported from DHCP Option 82	Shows whether the Location reported from DHCP Option 82 is enabled or disabled.



CHAPTER 17

UE Overload Protection

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.22

Feature Description

The UE Overload Protection feature provides a mechanism to monitor resource utilization of system bandwidth, channel drop rate, SM CPU, SM memory and VPP CPU. When resources exceed configured threshold, certain identified UEs shall be impacted. For example, when system bandwidth resource, which is global, exceeds the configured threshold, the UEs across the system enabled for this feature shall be impacted. Remaining resources are considered as local to CPU complex.

Currently, P-GW supports managing or throttling of traffics and includes the following functions as part of the UE Overload protection functionality:

- Identification of subscriber impact to a P-GW
- Setting thresholds or conditions on the impact of subscriber to a P-GW
- Sending responses to these thresholds by throttling one or more subscribers who exceeded the threshold.

The UE Overload protection feature works only with VPP-enabled ASR 5500 with DPC2 card and other platforms. Threshold handling is applicable only for DPC2 cards (maximum of 6DPC2 cards) that does not include any Demux card. Now you can configure this feature through CLI globally: The following functions are supported:

- Configuration of UE Overload control profiles.
- Managed through PCRF– Enables or disables *ue overload protection* feature for each subscriber and based on the AVP received during the session establishment.
- Allows you to specify configuration actions when thresholds are met. You can adjust the APN-AMBR-DL and APN-AMBR-UL temporarily until the overload condition persists. UE Overload APN AMBR UL/DL values applied to the UEs are reverted to their original values in case of Session Manager restarts, Card migration, and ICSR.

Note If an UE session is under throttling, then APN-AMBR values get modified immediately if the new APN_AMBR values are lesser than the currently applied values. Otherwise, the values are not programmed in the fast path, instead, it gets applied once the threshold is relaxed.

- Allows you to receive periodic load condition (including VPP load) from Resource manager and provision to set up overload condition in Session Manager.
- **show status**: To optimize the system load the **show status** command is organized to show the recent status for up to 18 records and along with system-wide criteria. When the system criteria is met as a lower priority criteria, complex wide higher priority can still override for every complex level based on the complex level threshold crossing. You can view the following results through **show status**:
  - All "met" parameters, when a CPU complex is in throttled state due to one threshold parameter and if other threshold parameters meet on that same CPU complex.

    All threshold parameters, if multiple threshold parameters are met within a given configured criteria.

    The system bandwidth threshold, if met, is displayed as a separate row (last row) in the **show status**. The **Activation Time** for system bandwidth can be any one of the CPU complex activation times.

How it Works

In StarOS, all sessions are distributed across multiple Session Managers. Demux Manager acts as a central element of resource utilization collection at the CPU complex level. When the network traffic speed increases in conjunction with the deployment of 5G, P-GW allows subscribers to manage the performance of the network, such as high-speed downloads, User Equipment (UE) overload detection or recovery scenarios with the help of Demux Manager.

The UE Overload protection feature works on a detection algorithm, which is designed to work and targeted for the DPC2 card-based architecture. However, this algorithm works across different line cards. Following table explains the Overload detection algorithm steps.

Table 20: Workflow

Step	Description
1	Collects resource information at CPU complex level.
2	CLI defines the threshold of the resource utilization.
3	A programmable timer (time provided through CLI) runs the detection algorithm on its expiry and checks against the upper threshold for any of the resource utilizations has crossed the upper threshold limit: • If crossed, then scans for the offending users part of the instance of VPP thread or Session Manager and applies the temporary **APN-AMBR-DL** and **APN-AMBR-UL** threshold values. • Else, waits for the next cycle.
4	Checks recovery algorithm loop (with checks for resource utilization have gone below lower threshold value, which is configured through CLI. If the condition is crossed, then scans for the **APN-AMBR-DL** and **APN-AMBR-UL** instances and replaces with the original **APN-AMBR-DL** and **APN-AMBR-UL** values.
5	Records incidents in the counters to update statistics.
6	Applies timestamp when a criterion is met and used for checking the dampening expiry.

Limitations

The limitations are:

- Works only with VPP-enabled ASR 5500 whereby the load monitoring is performed on the DPC2 card.
- As the intent of this feature is to bring down the system load by throttling the user traffic through AMBR parameters, the operator should take care of enabling the sessions to be throttled.

- The operator must enter the actual name of the APNs at the time of entering the APN names in the list. This is because there is no validation on this list with respect to the APN names used in the system. For APN name, which is not available in the system, the error is not displayed during configuration.You can view the error through the **show config errors** command.

Configuring ue-overload-control-profile

UE Overload feature is applicable only to the new UE sessions that come up after the UE Overload configuration. When you enable the UE Overload configuration for a valid virtual APN(s) or base APN(s), you cannot modify any existing UE sessions to apply the feature.

Use the following commands to configure the ue- overload control profile settings on ASR5500:

```
configure
    context context_name
     ue-overload-control-profile name
        end
```

Notes:

- **ue-overload-control-profile**: Creates a new UE Overload Control Profile without prompting for confirmation.

Note Deletion of an UE Overload profile or an applied/active criteria or applied/active action profile or parameters results in relaxing of applied threshold(s) on a Card/CPU complex immediately.

Any modification of configuration takes effect only in the next *check-interval*.

Configuring ue-overload Criteria

Use the following commands to configure ue-overload criteria.

```
configure
   context context_name
    ue-overload-control-profile overload-criteria  value priority priority_value

        system
           bandwidth-threshold value
           drop-rate-threshold value
        exit
        sessmgr
           cpu-threshold value
           memory-threshold value
        exit
        vpp
           cpu-threshold value
        exit
```

```
overload action name
exit
apn name
    overload-actionname
    downlink-ambrvalue
    uplink-ambrvalue
check-intervalseconds
dampen-intervalseconds
exit
```

Notes:

- **overload-criteria**: Configures Overload criteria thresholds for system, sessmgr, vpp parameters along with criteria priority.

  overload-action: Configures overload action associated with this overload criteria.

- **sessmgr** : Configures Session Manager threshold for various overload criteria parameters.
- **system** : Configures System threshold for various overload criteria parameters.
- **vpp**: Configures VPP threshold for various overload criteria parameters.
- **apn**: Includes APN names to apply for this UE Overload control profile. APN is added in the UE Overload configuration in the following two ways:
  - enable-by-default – UE Overload feature is applicable to the UE sessions if the **UEOVERLOAD** field is enabled in the Service-Feature AVP or if **UEOVERLOAD** field or Service-Feature AVP is altogether missing.
  - enable-by-gx – UE Overload feature is applicable to the UE sessions only if the **UEOVERLOAD** field is enabled in the Service-Feature AVP.

  check-interval: Configures UE Overload parameters monitoring interval (in seconds). The default value is 30 seconds.

- **dampen-interval** : Configures minimum time defined for the system to be in the Overloaded State or Normal State (in seconds). The default value is 300 seconds.
- **default** : Restores default value assigned for following options.
  - **do** : Spawns an exec mode command which displays information to the administrator.
  - **end**: Exits configuration mode and returns to Exec Mode.
  - **exit**: Exits current configuration mode, returns to previous mode.
  - **no**: Enables or disables the following option:
    - **overload-criteria**: Configures Overload criteria thresholds for system, session manager, and VPP parameters along with criteria priority.

Monitoring and Troubleshooting

Show Commands and Outputs

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

show ue-overload-control-profile

The output of this command includes the following fields:

Field	Description
all	Displays all UE Overload Control Profiles.
full	Displays UE Overload Control profile in detail.
name-Displays UE Overload Control Profile names.	
Status	Displays the current status of an UE Overload Control profile.
APN List	Displays APN list that are configured under UE Overload Control profile.

show ue-overload-action

The output of this command includes the following fields:

Field	Description
ue-overload-action	Displays all UE overlaoad action information or criteria and its statistics..
Statistics	Displays total collected information about criteria applied on UEs since its activation.

show ue-overload-control-profile name

The output of this command includes the following fields:

Field	Description
UE Overload Control Profile	
Profile Name	Displays name of the ue-overload control profile.
Status	Displays the current status of the ue-overload control profile.

show ue-overload-profile full all

The output of this command includes the following fields:

Field	Description
UE Overload Control Profiles	
UE Overload Control Profile Name	Displays name of the ue-overload control profile.
Overload-Criteria (s)	
Name	Displays name of the overload criteria.
Priority	Displays the priority of the ue-overload profile.
System	Displays System threshold for various overload criteria parameters.
Sessmgr	Displays Session Manager threshold for various overload criteria parameters. The percentage must be an integer between 0 to100.
vpp	Displays a VPP CPU utilization threshold in percentage.
Bandwidth threshold	Displays a System bandwidth threshold in percentage.
drop-rate threshold	Displays System drop-rate in pps.
cpu threshold	Displays Session Manager CPU threshold in percentage.
memory threshold	Displays Session Manager memory threshold in percentage.
overload-action	Displays the associated UE Overload action profile.
APN (s)	
enable-by-default	Displays all the APNs enabled by default.
enable-by-gx	Displays all APNs enabled by Gx interface.
Check-interval: Displays check interval in seconds. **check-interval** must be an integer ranging from 15 through 300 seconds.	
Dampen-interval: Displays dampen interval in seconds. The **dampen-interval** must be an integer ranging from 30 through 3000 seconds.	

show ue-overload-action statistics full

To optimize the system load, the statistics entries are limited to seven records (six for the complex level and one for the system wide). System-Wide statistics entry is always shown as the last row.

The output of this command includes the following fields.

Field	Description
Profile-name: Displays name of the UE overload profile. **Note** If an UE Overload profile is deleted or if association is removed from SAEGW service, then any statistics collected gets erased.	

Field	Description
Criteria Name (Priority)	Displays Overload criteria name and priority. **Note** In a given criteria, if multiple thresholds are met along with System Bandwidth, then post relaxing the threshold, statistics are collected as part of the System Bandwidth entry.
Activation Time	The activation time of the overload criteria. **Note** For statistics collected post EGTPMGR recovery, the **Activation Time** is displayed as blank.
Activation Duration	The duration up to which the overload criteria was active. **Note** For statistics collected post EGTPMGR recovery, the **Activation Duration** is displayed as blank.
No.of Impacted UEs	Displays the number of UEs for which the temporary UL-AMBR values are applied.
Total UEs	Displays the total number of UEs on the Card/CPU complex **Note** If the **Total UEs** entries are less than the **No.of Impacted UEs**, some UE sessions might go down as the statistics are collected at the Card/CPU-complex when it comes out of threshold.
Card/CPU	The Card/CPU complex for which the particluar criteria was active. If there is a sytem-wide overload action criteria, then it will display as **SYSTEM**. If no UE sessions were throttled on a Card/CPU-complex, then UE session entries are not shown in the statistics even though the Card/CPU complex exceeds any of the configured threshold parameters.

show configuration bulkstats

The following example shows the Bulk Statistics Server Configuration:

```
config
  bulkstats collection
  bulkstats historical collection
  bulkstats mode
    sample-interval 1
    transfer-interval 2
    file 1
      remotefile format data/bulkstats/%host%-%date%-%time%.csv
     receiver 10.105.84.124 primary mechanism ftp login root encrypted password +B3qmvomy0b
 fenh0p6bitcxn3lfs19 febnhcv66ry0uocxu3s2zrze0zompd le3gc7d2bjdm 199d61ny1360gwn1 zr8332rg
 vnjsjvanb4
    #exit
    file 2
      header format UE-AMBR-drop-stats
      remotefile format data/bulkstats/%host%-%date%-%time%.csv
      receiver 10.105.84.124 primary mechanism ftp login root encrypted password +B0nu
axjhro0b lg2lspsbf12eupo2cxv6ljisgtxb01ap 2239iddb925p69epd in6cc05jm1v96b59uz0moxiz1gsk9qx
 3ijqpsossxi89
```

```
    #exit
    file 3
      header format UE-Overload-drop-stats
      remotefile format data/bulkstats/%host%-%date%-%time%.csv
      receiver 10.105.84.124 primary mechanism ftp lo gin root encrypted password
+B3iw43muh3b2j62d9ib6t2jo50232r3dt9ih97iq1ga70qh7r0cbq2a0z j68wpxki22fn9b2t
9i69td06rq782uc83vs2xlfi96h64bi3
      saegw schema ueoverload-stats format
Server1,pgw-apnambrratelimit-ulpktdrop:%pgw-apnambrratelimit-ulpktdrop%,pgw-apnambrratelimit-dlpktdrop:
 %pgw-apnambrratelimit-dlpktdrop%, pgw-apnambrratelimit-ulbytedrop:%pgw-apnambr
ratelimit-ulbytedrop%,
       pgw-apn ambrratelimit-dlbytedrop:%pgw-apn ambrratelimit-
dlbytedrop%,pgw-ueoverload-apnambrratelimit-ulpktdrop:%pgw-ueoverload-apnambrratelimit-ulpktdrop%,
 pgw-ueoverload-apnambrratelimit-dlpktdrop: %pgw-ueoverload-apnambr ratelimit-dlpktdrop%,
       pgw-ueov erload-apnamb rratelimit-ulbytedrop:% pgw-ueoverload-
apnambrratelimit-ulbytedrop%,pgw- ueoverload-apnambrratelimit-dlbytedrop:
%pgw-ueoverload-apnambrratelimit-dlbytedrop%
    #exit
  #exit
end
```

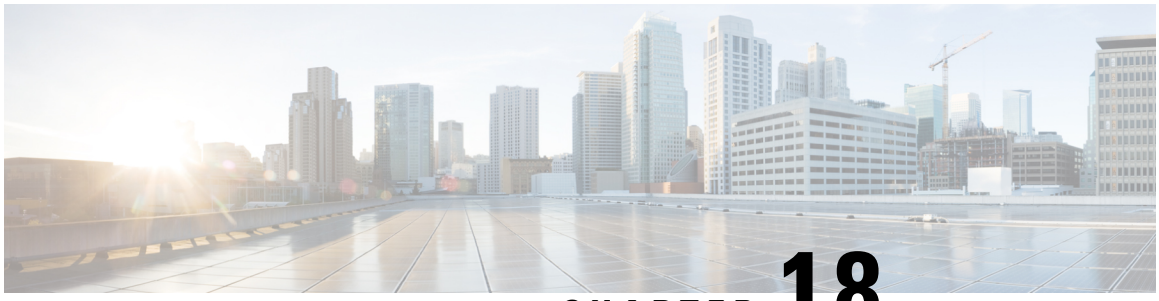
Bulkstats Output on server

```
UE-Overload-drop-stats
Server1,pgw-apnambr ratelimit-ulpktdrop:11060, pgw-apnambrr
atelimit-dlpktdrop:14231,pgw-apnambrra telimit-ulbytedrop:888455,
pgw-apnambrratelimit-dlbytedrop:14965964,
pgw-ueoverload-apnamb rratelimit-ulpktdrop:11060,pgw-ueov erload-apnam br
ratelimit-dlpktdrop:14231,pgw-ueover load-apnambrratelimit-ulbytedrop:888455,
pgw-ueoverload-apnambrratelimit-dl bytedrop:14965964
```

show saegw-service all

The following example shows the results on UE Overload Contol Profile for SAEGW service.

```
Service name                     : SAEGW21
  Service-Id                     : 12
  Context                        : EPC2
  Status                         : STARTED
  sgw-service                    : SGW21
  pgw-service                    : PGW21
  sx-service                     : Not defined
  User Plane Tunnel GTPU Service : Not defined
  Ue Overload Control Profile    : prof-1
  Newcall policy                 : n/a
  downlink-dscp-per-call-type    : n/a
  CUPS Enabled                   : No
```



CHAPTER 18

Update Bearer Request Enhancements to Close Charging Gap

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* • *P-GW Administration Guide*

Revision History

Revision Details	Release
In this release, the P-GW supports deferred rule removal policy to avoid charging discrepancies	21.22

Feature Description

When Re-Auth-Request (RAR) is received on P-GW with **charging-rule-install** and **charging-rule-remove** Attribute Value Pairs (AVPs) with changes in the default bearer Quality of Service Class Index (QCI), P-GW removes the old dynamic charging rule and triggers Update Bearer Request. Only on receiving the Update Bearer Response, the new rule gets applied. This results in charging discrepancies for the time period when no policies are associated with default bearer.

In the StarOS 21.22 and later releases, to avoid charging discrepancies, the rule removal is deferred until Update Bearer Response is received for the above case. This new deferred rule removal policy is applicable only for default bearer with a change in QOS parameters (QCI, GBR, MBR or ARP) and the above condition of **charging-rule-install** and **charging-rule-remove** is satisfied .

How it Works

The Charging rule remove policy is applied after receiving bearer update response and not immediately when RAR is received. This change is supported through CLI configurations and following functions happen::

1. RAR or Credit Control Answer-Update is received by P-GW with Rule remove for Rule1, default bearer QCI update, and Rule install for Rule2.
2. ACS manager verifies the following:
   - Checks for defer rule removal policy.
   - Checks if there is a QOS change for the default bearer and rule remove for default bearer.
   - After Update Bearer Request response is received, removes the stored policy.
3. Verifies if correct QCI, MBR, and GBR values are sent for the Update Bearer Request. Also, verifies if correct default bearer QOS is reflected on the bearer.
4. If update bearer response is not received, then:
   - Performs a timeout handling when you want to cancel the deferred rule removal.
   - Validates the correct bearer QOS restored

Enabling defer default-bearer-rule-removal

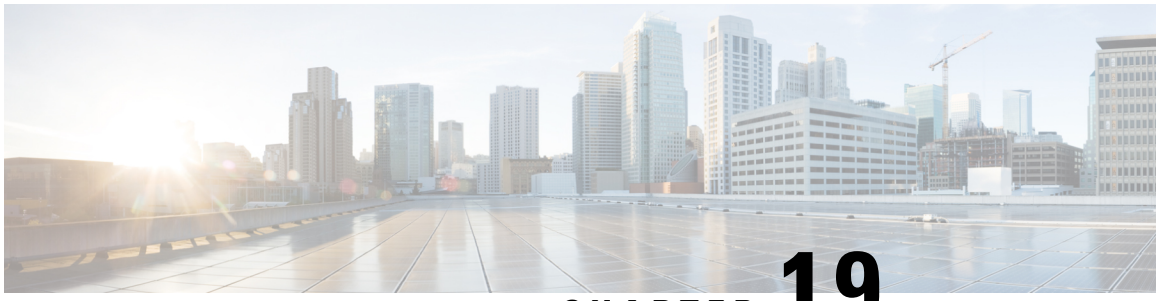
Use the following configuration command to enable or disable default bearer rule removal policy.

```
configure
  active-charging service service_name
    [no] policy-controldefer default-bearer-rule-removal
   end
```

Notes:

- **active-charging service**:: Charging actions define the action to take when a rule definition is matched.

- **no**: Disables deferring of dynamic rule remove.
- **defer default-bearer-rule-removal**: Defers removal of rule from default bearer until Update Bearer Response or timeout.



CHAPTER 19

User Location Information in P-GW CDR

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	Enabled - Always-on
Related Changes in This Release	Not applicable
Related Documentation	• *GTPP Interface Administration and Reference*

Revision History

Revision Details	Release
First introduced.	21.22

User Location Information in P-GW CDR

The P-GW CDR contains the User Location Information (ULI) in the following two attribute fields:

- User Location Information (32)
- User Location Information (34-0-20)

As per the current behavior above two fields contain the “User Location information” in P-GW CDR. These fields are getting updated only when ULI-change trigger is enabled. If ULI-change trigger is not configured, the P-GW CDRs keeps the user location as it was reported in the initial CDR, even after the “Radio Access Technology” gets changed.

To overcome this issue, this feature was introduced, that even if “ULI-change trigger” is disabled, Every CDR contains the latest “User Location Information”. Functionality overview of this feature is as follows:

- This feature allows the P-GW CDRs to update User Location Information (32) and User Location Information (34-0-20) attributes with the latest User Location Information provided by the MME and S-GW.
- The implementation of the feature is through the different filler function specific to feature.
- To use this feature, customer/user requires to make the software changes at two places. First one is to update the CDR custom/customer’s dictionary ULI fields with the newly implemented filler functions. Current implementation is in the custom dictionary 38, as per requirement. Parallelly, the support for the same dictionary need to be added under the MACRO: “ACS_CHK_DICT_SUPPORT_FOR_LATEST_ULI”.

If the dictionary with the new filler functions are used, it packs the latest ULI in case of the following events:

Events to send/generate partial PGW-CDR for a subscriber:

- When the number of QoS changes or tariff time changes reaches the configured maximum number of charging condition changes.
- Before this, service containers are added to the CDR for every change.
- Every x seconds configured using "interval x".
- Every x octets configured using "volume x" (up/down/total).
- Command gtpp interim now active-charging egcdr.
- Transferring the context to a new S-GW/SGSN (serving Node Change).
- Changing the access type within the same P-GW (RAT Change).

Events to send or generate the final P-GW CDR for a subscriber:

- Detach Request received from UE
- Delete bearer context request received from S-GW.
- Manual subscriber clearing
- Abnormal Releases such as path failures.

Sample Configuration

Following are the sample configurations:

```
Customer dictionary: custom38
Customer running configuration:
    gtpp group pgwhdd
      gtpp attribute local-record-sequence-number
      gtpp attribute node-id-suffix PGW11
      no gtpp attribute twanuli
      gtpp dictionary custom38
```

```
      no gtpp trigger dcca
      no gtpp trigger service-idle-out
      no gtpp trigger serving-node-change-limit
      no gtpp trigger inter-plmn-sgsn-change
      no gtpp trigger qos-change
      no gtpp trigger ms-timezone-change
      gtpp trigger egcdr max-losdv
      no gtpp trigger uli-change
      gtpp egcdr lotdv-max-containers 1
      gtpp egcdr losdv-max-containers 1
      gtpp suppress-cdrs zero-volume-and-duration gcdrs egcdrs
      gtpp egcdr service-data-flow threshold interval 43200
     gtpp egcdr service-data-flow threshold volume total 104857600
     gtpp storage-server mode local
gtpp storage-server local file purge-processed-files file-name-pattern

            ACQ* purge-interval 2880
      gtpp storage-server local file format custom3
      gtpp storage-server local file rotation volume mb 30
      gtpp storage-server local file rotation cdr-count 65000
      gtpp storage-server local file rotation time-interval 600
      gtpp storage-server local file name prefix PGW11_Laca
    #exit.
```

User Location Information in P-GW CDR