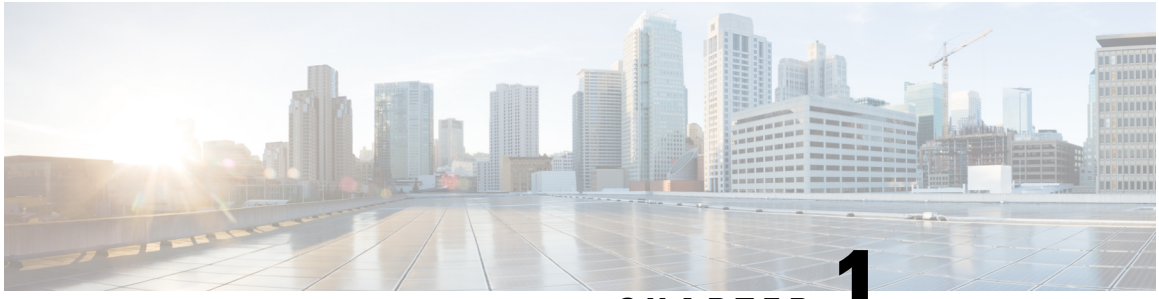
# Release Change Reference, StarOS Release 21.21

**First Published:** 2020-10-01

**Last Modified:** 2021-04-22

**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

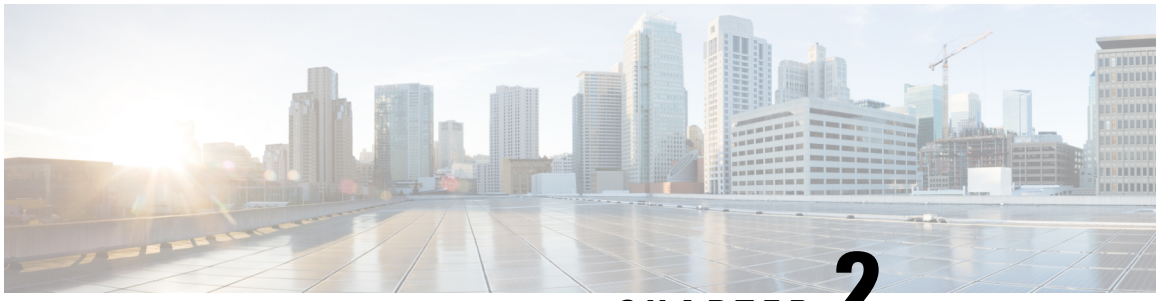
# Release 21.21 Features and Changes Quick Reference



## Release 21.21 Features and Changes

| Features / Behavior Changes | Applicable Product(s) / Functional Area | Release Introduced / Modified |
|---|---|---|
| Adding Cause Code 38 to Bulkschema Counters | MME | 21.21 |
| Cisco Ultra Traffic Optimization, on page 17 | P-GW | 21.21 |
| Diameter Result Code Specific Counters on Gy Interface, on page 67 | SaMOG | 21.21 |
| Enabling S6b for IMS APN | • GGSN<br>• P-GW<br>• SAEGW | 21.21 |
| Enabling Multicast Services over L2TP, on page 75 | P-GW | 21.21.1 |
| IPv4/IPv6 Address Encoding Change in Flow-Description AVP for APPLICATION-START Event Trigger from P-GW, on page 77 | P-GW | 21.21.1 |
| P2P Detection Analysis and Performance Enhancements, on page 79 | All | 21.21 |
| QUIC IETF Implementation, on page 81 | ADC | 21.21 |
| Sessmgr Restart While Processing Secondary RAT Usage CDR Records, on page 83 | P-GW | 21.21.3 |
| Support for Common access-type in twan-profile for EoGRE-PMIP Calls, on page 85 | SaMOG | 21.21 |

| Features / Behavior Changes | Applicable Product(s) / Functional Area | Release Introduced / Modified |
|---|---|---|
| Support for Diameter Error Code Counters, on page 97 | • ePDG<br>• SaMOG | 21.21 |
| Support to List Non-Fatal Snaps and Fatal Crashes in StarOS , on page 109 | StarOS | 21.21 |
| TCP Information Fields in EDR, on page 113 | ECS | 21.21 |



CHAPTER 2

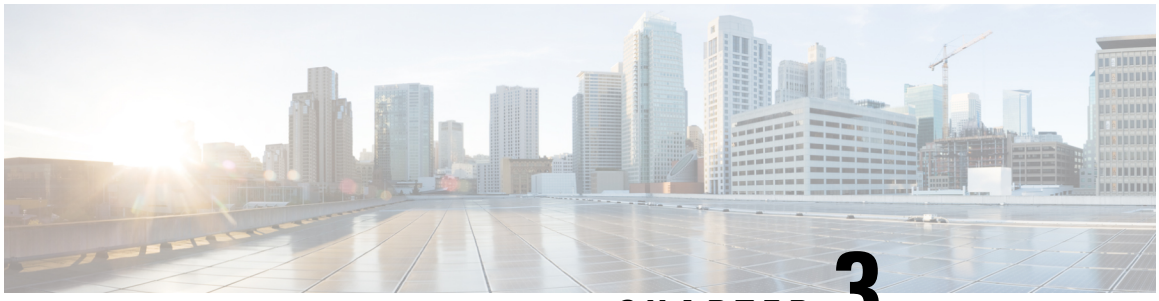
# Feature Defaults Quick Reference



## Feature Defaults

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

| Feature | Default |
|---|---|
| Adding Cause Code 38 to Bulkschema Counters | Disabled - Configuration Required |
| Cisco Ultra Traffic Optimization | Disabled - License Required |
| Diameter Result Code Specific Counters on Gy Interface | Enabled - Always-on |
| Enabling S6b for IMS APN | Disabled -Configuration Required |
| Enabling Multicast Services over L2TP | Disabled - Configuration Required |
| IPv4/IPv6 Address Encoding Change in Flow-Description AVP for APPLICATION-START Event Trigger from P-GW | Enabled - Always-on |
| P2P Detection Analysis and Performance Enhancements | Enabled - Always-on |
| QUIC IETF Implementation | Disabled - Configuration Required |
| Sessmgr Restart While Processing Secondary RAT Usage CDR Records | Enabled - Configuration Required |
| Support for Common access-type in twan-profile for EoGRE-PMIP Calls | Disabled - Configuration Required |
| Support for Diameter Error Code Counters | Enabled - Always-on |
| Support for Presence Reporting Area and Extended QOS on Offline Charging Interface for P-GW and SAEGW | Disabled - Configuration Required |
| Support to List Non-Fatal Snaps and Fatal Crashes in StarOS | Enabled - Configuration Required |
| TCP Information Fields in EDR | Disabled - Configuration Required |



CHAPTER 3

# SNMP MIB Changes in StarOS 21.21

This chapter identifies SNMP MIB objects, alarms and conformance statements added to, modified for, or deprecated from the StarOS 21.21 software release.



# SNMP MIB Object Changes for 21.21

This section provides information on SNMP MIB alarm changes in release 21.21.

**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 21.21.

- starX3ContextId

### Modified SNMP MIB Object

- starX3MDConnDown
- starX3MDConnUp

### Deprecated SNMP MIB Object

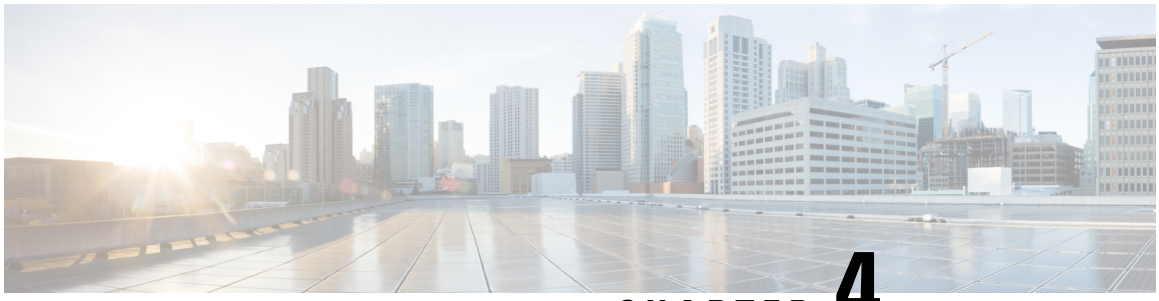
- starX3ContextName

# SNMP MIB Alarm Changes for 21.21

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

# SNMP MIB Conformance Changes for 21.21

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



CHAPTER 4

# Bulk Statistics Changes Quick Reference

This chapter identifies bulk statistics changes added to, modified for, or deprecated from the StarOS 21.21 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 21.21 include:


- New Bulk Statistics, on page 7
- Modified Bulk Statistics, on page 11
- Deprecated Bulk Statistics, on page 11


# New Bulk Statistics

This section identifies new bulk statistics and new bulk statistic schemas introduced in release 21.21.

### Diameter Accounting Schema

The following bulk statistics are added in the diameter-acct schema in support of the Diameter Error Code Counters feature.

| Bulk Statistics | Description |
|---|---|
| acct-result-unable-to-deliver | Shows the total number of Diameter account results with a result code 3002, which cannot be delivered to the destination. |
| acct-result-too-busy | Shows the total number of Diameter account results with a result code 3004, which cannot be allowed for the requested service, when specific servers are requested for. |
| acct-result-loop-detected | Shows the total number of Diameter account results with a result code 3005. This Diameter error code is received when an agent detected a loop while trying to get the message to the inteded recipient. |

| Bulk Statistics | Description |
|---|---|
| acct-result-invld-hdr-bits | Shows the total number of Diameter account results with a result code 3008 for an invalid header bits request received. A request received could be related to bits in the diameter header, which is set either to an invalid combination or to a value that is inconsistent with the defintion of the Command Code. |
| acct-result-invld-avp-bits | Shows the total number of Diameter account results with a result code 3009. The request received includes an AVP whose flag bits are set to an unrecognized value or that is inconsistent with the AVP definition. |
| acct-result-authen-rej | Shows the total number of Diameter account results with a result code 4001. The results received is for the user authentication failure due to an invalid password used by the user. |
| acct-result-out-of-space | Shows the total number of Diameter account results with a result code 4002. The results received is for a Diameter node but was unable to perform stable commit due to a temporary lack of space. |
| acct-exp-result-user-unknown | Shows the total number of Diameter account expected results with a result code 5001 for the unknown user error. |
| acct-result-unk-sess-id | Shows the total number of Diameter account results with a result code 5002 that contains unknown session Identifiers. |
| acct-result-author-rej | Shows the total number of Diameter account results with a result code 5003 where, the user requests could not be authorized. |
| acct-exp-result-roaming-not-allowed | Shows the total number of Diameter expected account results with a result code 5004 for which roaming calls are not allowed. |
| acct-result-missing-avp | Shows the total number of Diameter account results with a result code 5005 that does not contain an AVP. |
| acct-result-resrc-exceed | Shows the total number of account results with result code 5006 that caanot be authorized because the user has already expended allowed resources. |
| acct-result-unable-to-comply | Shows the total number of account results with result code 5012 rejected for unspecified reasons. |
| acct-result-user-unknown | Shows the total number of account results with a result code 5030 that contains unknown users. |

| Bulk Statistics | Description |
|---|---|
| acct-exp-result-no-wlan-subs | Shows the total number of expected account results with a result code 5041 for no VLAN Sub band. |

### Diameter Authentication Schema

The following bulk statistics are added in the diameter-auth schema in support of the Diameter Error Code Counters feature.

| Bulk Statistics | Description |
|---|---|
| auth-result-unable-to-deliver | Shows the total number of Diameter authentiction/authroization results with a result code 3002 that cannot be delivered to the destination. |
| auth-result-too-busy | Shows the total number of Diameter authentication/authorization results with a result code 3004 that cannot be allowed for the requested service, when specific servers are requested for. |
| auth-result-loop-detected | Shows the total number of Diameter authentication/authorization results for a result code 3005. This Diameter error code is received when an agent detects a loop while trying to get the message to the inteded recipient. |
| auth-result-invld-hdr-bits | Shows the total number of Diameter authentication/authorization results with a result code 3008 for an invalid header bits request received. A request received could be related to bits in the diameter header, which is set either to an invalid combination or to a value that is inconsistent with the defintion of the Command Code. |
| auth-result-invld-avp-bits | Shows the total number of Diameter authentication/authorization results received with a result code 3009. The request received includes an AVP whose flag bits are set to an unrecognized value or that is inconsistent with the AVP definition. |
| auth-result-authen-rej | Shows the total number of Diameter authentication/authorization results with a result code 4001. This Diameter error code is received for the user authentication failure due to an invalid password used by the user. |
| auth-result-out-of-space | Shows the total number of Diameter authentication/authorization results with a result code 4002 for a Diameter node received but was unable to perform stable commit due to a temporary lack of space. |

| Bulk Statistics | Description |
|---|---|
| auth-exp-result-user-unknown | Shows the total number of Diameter authentication/authorization expected results with a result 5001 for the unknown user error. |
| auth-result-unk-sess-id | Shows the total number of Diameter authentication/authorization results with a result code 5002 that contains unknown session Identifiers. |
| auth-result-author-rej | Shows the total number of Diameter authentication/authorization results with a result code 5003 where, the user requests could not be authorized. |
| auth-exp-result-roaming-not-allowed | Shows the total number of Diameter authentication/authorization expected results with a result code 5004 for which roaming calls are not allowed. |
| auth-result-missing-avp | Shows the total number of Diameter authentication/authorization results with a result code 5005 that does not contain an AVP. |
| auth-result-resrc-exceed | Shows the total number of Diameter authentication/authorization results with a result code 5006 that caanot be authorized because the user has already expended allowed resources. |
| auth-result-unable-to-comply | Shows the total number of Diameter authentication/authorization results with a result code 5012 rejected for unspecified reasons. |
| auth-result-user-unknown | Shows the total number of Diameter authentication/authorization results with a result code 5030 that contains unknown users. |
| auth-exp-result-no-wlan-subs | Shows the total number of expected Diameter authentication/authorization results with a result code 5041 for no VLAN Sub band. |

### System Schema

The following bulk statistics in the SaMOG schema supports Diameter Result Code specific counters on Gy interface.

| Bulk Statistics | Description |
|---|---|
| cca-init-4010-rc | Shows the total number of responses received for diameter end user service denied messages. |
| cca-init-5031-rc | Shows the total number of responses received for diameter rating failed messages. |

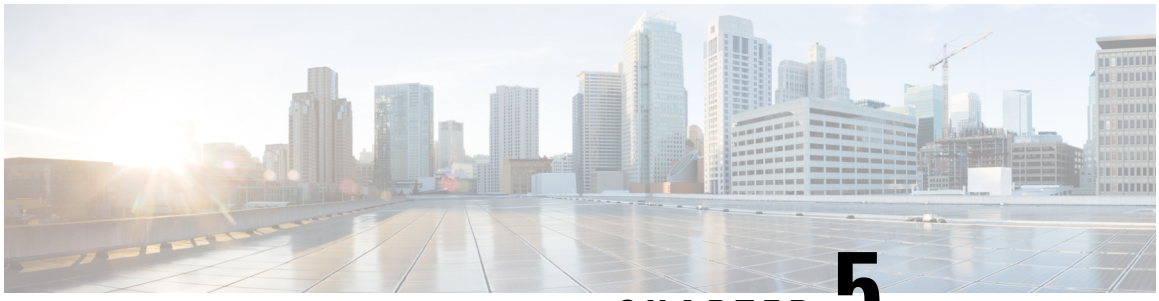
| Bulk Statistics | Description |
|---|---|
| cca-updt-4010-rc | Shows the total number of responses received for diameter end user service denied messages. |
| cca-updt-5031-rc | Shows the total number of responses received for diameter rating failed messages. |
| cca-5031-rc | Shows the aggregate number of responses received for diameter rating failed messages. |

# Modified Bulk Statistics

None in this release.

# Deprecated Bulk Statistics

None in this release.



CHAPTER 5

# Adding Cause Code 38 to Bulkschema Counters



## Feature Summary and Revision History

### Summary Data

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

### Revision History

| Revision Details | Release |
|---|---|
| First introduced | 21.21 |

# Feature Description

EPS Session Management (ESM) network failures are caused by a rejection of P-GW/S-GW and this failure occurs during UE attachment process. The failure contributes to around 3% decrease in SR statistics calculations resulting in ESM Failure Cause Code 38 network failure.

As this failure is not added as a part of the EMM/ESM statistics, it is not used to exclude the failure during 4G attach SR statistic calculations. To overcome the decreasing calculation value in SR Statistics, a new schema MME Bulk statistics is implemented in EMM and ESM Failure Statistics.

It is done by isolating the Network Failure while performing the required SR calculations. These "Network Failure" is added in EMM, ESM, TAI, and PEER-ID statistics in MME-SERVICE.

# Verifying the Added Bulk Statistics Network Failure in EMM and ESM MME-Service Statistics

Use the following command to display and verify the network failure fields in EMM and ESM MME-Service Statistics.

**show mme-service statistics { { emm-only verbose } | { esm-only verbose } | { tai taidb** *taidb_value* **mcc** *mcc_value***mnc** *mnc_value* **tac** *tac_value* **} | { peer-id** *id_value* **}}**

# Monitoring and Troubleshooting

This section provides information regarding the show commands and bulk statistics network failure in emm and esm mme-service.

## Show Commands and Outputs

**show mme-service statistics emm-only verbose | tai taidb <taidb_value> mcc <mcc_value> mnc <mnc_value> tac <tac_value> | peer-id <peer_id>**

The output of this command displays the total ESM failure in EMM control messages including the following newly introduced field:

- Network failure—Displays the total number of network failures during UE attachment with pdn process.

**show mme-service statistics esm-only verbose | tai taidb <taidb_value> mcc <mcc_value> mnc <mnc_value> tac <tac_value> | peer-id <peer_id>**

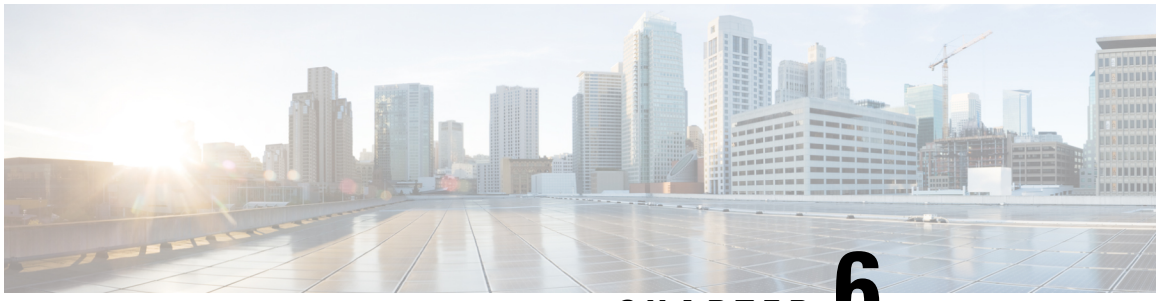
The output of this command displays the PDN Connectivity Reject fields in ESM control messages including the following newly introduced field under PDN connectivity reject:

- Network failure—Displays the total number of network failures during seperate PDN request after attach complete process.

# Bulk Statistics

The following bulk statistics are added in the MME and TAI Schema:

| | |
|---|---|
| emm-msgtx-attach-rej-38network-fail | Displays the total number of attach reject with cause code 38 in attach with PDN request. |
| esm-msgtx-pdncon-rej-38network-fail | Displays the total number of PDN request reject with cause code 38 in additional PDN request |
| tai-emm-msgtx-attach-rej-38network-fail | Displays the total number of attach reject with cause code 38 in attach with PDN request using mcc, mnc and tac value. |
| tai-esm-msgtx-pdncon-rej-38network-fail | Displays the total number of PDN request reject with cause code 38 in additional PDN request using mcc, mnc and tac value. |



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<br>• Ultra Gateway Platform |
| Feature Default | Disabled - License Required |
| Related Changes in This Release | Not Applicable |
| Related Documentation | • *Command Line Interface Reference*<br>• *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, ranges of configurable policy parameters for Cisco Ultra Traffic Optimization are modified. | 21.20.4 |
| In this release the following three new parameters are added in Large TODR:<br>**1.** International Mobile Subscriber Identity (IMSI)<br>**2.** Flow-ID and Flow-ID list<br>**3.** User Location Information (ULI)<br>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.<br>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

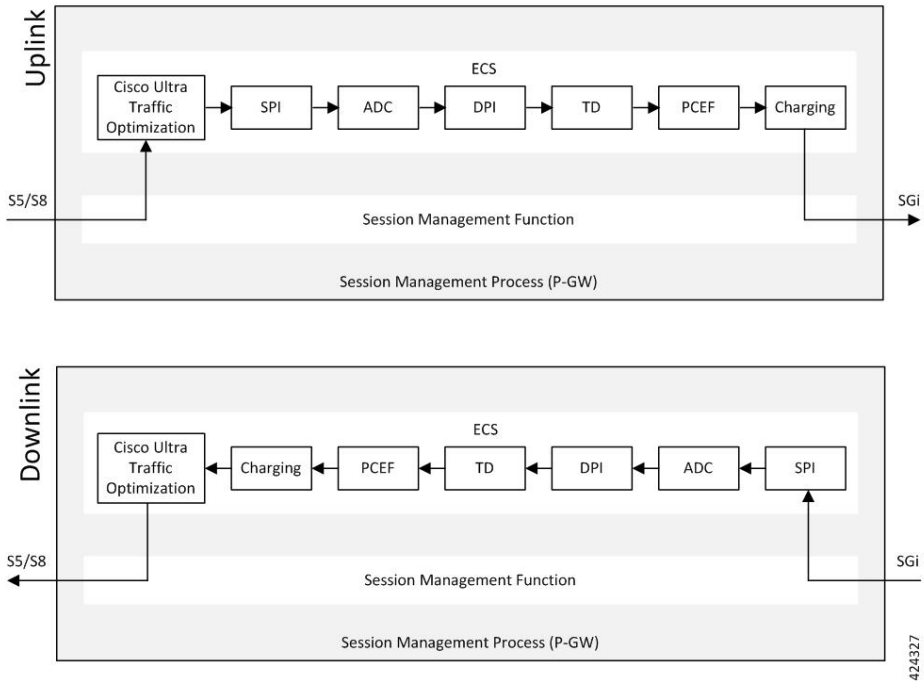
The Cisco Ultra Traffic Optimization achieves its gains by shaping video traffic during times of high network load/congestion. It monitors and profiles each individual video flow that passes through the gateway and uses its machine learning algorithms to determine whether that flow is traversing a congested 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:

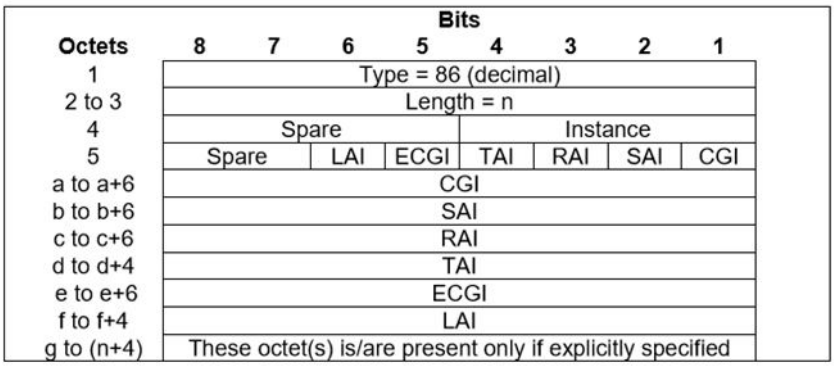
- 92 is the Session Manager instance
- 30278 is the Session Handle orsession number
- 14786055 is the ACS flow identifier

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 1: 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**

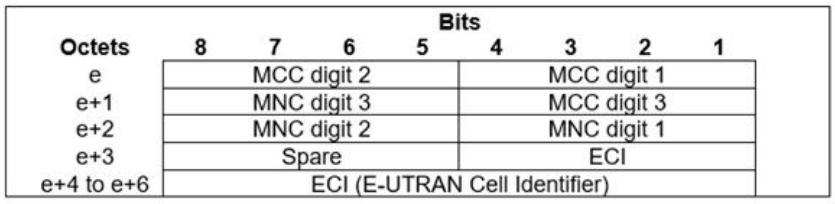
Here 16 represents that ULI Type is ECGI

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 2: 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-time out** | 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 43.

### 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.
```

# Cisco Ultra Traffic Optimization Bulk Statistics Enhancements

## Feature Description

In this StarOS 21.23 release, the following show commands and bulk statistics schema counters are enhanced to show Rx/Tx packet statistics for Uplink and Downlink for UDP and TCP split in Cisco Ultra Traffic Optimization solution.

- show active-charging traffic-optimization counters sessmgr all
- show active-charging traffic-optimization counters tcp sessmgr all
- show active-charging traffic-optimization counters udp sessmgr all

## Monitoring and Troubleshooting

### Show Commands and Outputs

*show active-charging traffic-optimization counters sessmgr all*

You can view CUTO Control Plane statistics for the following show command.

***Table 1: show active-charging traffic-optimization counters sessmgr all***

| Field | Description |
|---|---|
| **CUTO Control Plane Stats**: | |
| Total Active Streams | Displays total number of active streams. |
| Active TCP Streams | Displays total number of active TCP uplink and downlink streams received. |
| Active UDP(QUIC) Streams | Displays total number of active UDP uplink nd downlink streams transmitted. |

You can also view similar outputs for the folowing show commands:

- **show active-charging traffic-optimization counters tcp sessmgr all**
- **show active-charging traffic-optimization counters udp sessmgr all**

*show bulkstats variables ecs*

The following ECS level statistic variables are added for the Cisco Ultra Traffic Optimization feature.

*Table 2: Bulk Statistic Variables in the ECS Schema*

| Variables | Description | Data Type |
|---|---|---|
| cuto-tcp-uplink-rx | **Description:** Displays the total number of TCP packets received from the UE for Cisco Ultra Traffic Optimization<br>**Type:** Counter<br>**Triggers**: Increments whenever a TCP packet is received from the UE for Cisco Ultra Traffic Optimization.<br>**Availability**: Per Active Charging Service. | Int64 |
| cuto-tcp-uplink-tx | **Description:** Displays the total number of TCP packets sent towards the UE for Cisco Ultra Traffic Optimization.<br>**Type:** Counter<br>**Triggers**: Increments whenever a TCP packet is sent towards the UE for Cisco Ultra Traffic Optimization.<br>**Availability**: Per Active Charging Service. | Int64 |
| cuto-tcp-dnlink-rx | **Description:** Displays the total number of TCP packets received from the internet for Cisco Ultra Traffic Optimization.<br>**Type:** Counter<br>**Triggers**: Increments whenever a TCP packet is received from the internet for Cisco Ultra Traffic Optimization.<br>**Availability**: Per Active Charging Service. | Int64 |
| cuto-tcp-dnlink-tx | **Description:** Displays the total number of TCP packets sent towards the internet for Cisco Ultra Traffic Optimization<br>**Type:** Counter<br>**Triggers**: Increments whenever a TCP packet is sent towards the internet for Cisco Ultra Traffic Optimization.<br>**Availability**: Per Active Charging Service. | Int64 |

| Variables | Description | Data Type |
|---|---|---|
| cuto-udp-uplink-rx | **Description:** Displays the total number of UDP packets received from the UE for Cisco Ultra Traffic Optimization.<br>**Type:** Counter<br>**Triggers**: Increments whenever a UDP packets is received from the UE for Cisco Ultra Traffic Optimization.<br>**Availability**: Per Active Charging Service. | Int64 |
| cuto-udp-uplink-tx | **Description:** Displays the total number of UDP packets sent towards the UE for Cisco Ultra Traffic Optimization<br>**Type:** Counter<br>**Triggers**: Increments whenever a UDP packet is sent towards the UE for Cisco Ultra Traffic Optimization.<br>**Availability**: Per Active Charging Service. | Int64 |
| cuto-udp-dnlink-rx | **Description:** Displays the total number of UDP packets received from the internet for Cisco Ultra Traffic Optimization.<br>**Type:** Counter<br>**Triggers**: Increments whenever a UDP packets is received from the internet for Cisco Ultra Traffic Optimization.<br>**Availability**: Per Active Charging Service. | Int64 |
| cuto-udp-dnlink-tx | **Description:** Displays the total number of UDP packets sent towards the internet for Cisco Ultra Traffic Optimization.<br>**Type:** Counter<br>**Triggers**: Increments whenever a UDP packet is sent towards the internet for Cisco Ultra Traffic Optimization.<br>**Availability**: Per Active Charging Service. | Int64 |

## Bulk Statistics

The following bulk statistics are added in the ECS schema.

*ECS Schema*

***Table 3: Bulk Statistics Variables in the ECS Schema***

| Variables | Description |
|---|---|
| cuto-tcp-uplink-rx | Indicates that the total number of TCP packets received from the UE for Cisco Ultra Traffic Optimization. |
| cuto-tcp-uplink-tx | Indicates that the total number of TCP packets sent towards the UE for Cisco Ultra Traffic Optimization. |
| cuto-tcp-dnlink-rx | Indicates that the total number of TCP packets received from the internet for Cisco Ultra Traffic Optimization. |
| cuto-tcp-dnlink-tx | Indicates that the total number of TCP packets sent towards the internet for Cisco Ultra Traffic Optimization. |
| cuto-udp-uplink-rx | Indicates that the total number of UDP packets received from the UE for Cisco Ultra Traffic Optimization. |
| cuto-udp-uplink-tx | Indicates that the total number of UDP packets sent towards the UE for Cisco Ultra Traffic Optimization. |
| cuto-udp-dnlink-rx | Indicates that the total number of UDP downlink packets received from the internet for Cisco Ultra Traffic Optimization. |
| cuto-dnlink-tx | Indicates that the total number of downlink packets received from the internet for Cisco Ultra Traffic Optimization. |

# 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*<br>**any-match = TRUE**<br>**exit**<br>Sessetup trigger condition is **any-match** = **TRUE** |
| Applicable to all calls or flows of a rulebase | **subs-class** *sc1*<br>**rulebase = prepaid**<br>**exit**<br>Sessetup trigger condition is **any-match** = **TRUE** |
| Applicable to all calls or flows of an APN | **subs-class** *sc1*<br>**apn = cisco.com**<br>**exit**<br>Sessetup trigger condition is **any-match** = **TRUE** |
| Applicable to all flows of a Bearer | **trigger-condition** *TC1*<br>**qci = 1**<br>**exit**<br>Bearer creation trigger condition is TC1 |
| Applicable to a particular flow | **trigger-condition** *TC1*<br>**qci = 1**<br>**rule-name = tcp**<br>**multi-line-or all-lines**<br>**exit**<br>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. |

| Bulk Statistics | Description |
|---|---|
| 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. |
| 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. |
| 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. |

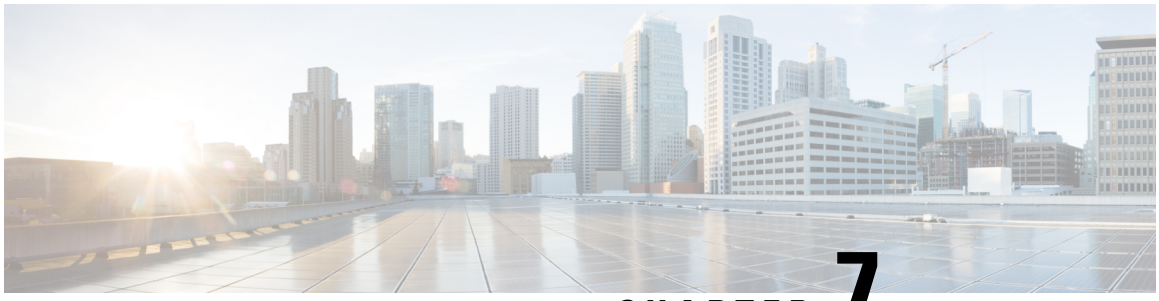
| Bulk Statistics | Description |
|---|---|
| udp-active-normal-flow-count | Indicates the number of UDP active-normal-flow count for Cisco Ultra Traffic Optimization. |
| udp-active-large-flow-count | Indicates the number of UDP active-large-flow count for Cisco Ultra Traffic Optimization. |
| udp-active-managed-large-flow-count | 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. |
| 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. |

| Bulk Statistics | Description |
|---|---|
| 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. |
| 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. |

| Bulk Statistics | Description |
|---|---|
| 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. |
| 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. |

| Bulk Statistics | Description |
|---|---|
| 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. |
| 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. |

| Bulk Statistics | Description |
|---|---|
| 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

# Diameter Result Code Specific Counters on Gy Interface



## Feature Summary and Revision History

### Summary Data

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

### Revision History

| Revision Details | Release |
|---|---|
| This release supports additional Diameter error code counters for Transient Failures [4XXX] and Permanent Failures [5XXX] on SaMOG (web-auth) service through P-GW LBO module. | 21.21 |

# Feature Description

SaMOG supports Diameter result code counters for all failure transactions and diameter interfaces on SaMOG (Web-auth) services through P-GW Local Breakout (LBO) module on various StarOS platforms ASR5500/ASR5700.

The following set of result code-specific counters is supported for the responses received from the OCS (Online Charging System), on Gy interface. DCCA (Diameter Credit Control Application) is the protocol used on the Gy interface.

***Table 4: Result Code Specific Counters***

| Error Category | Result Code | Result Code Value |
|---|---|---|
| Transient Failures [4XXX] | DIAMETER_END_USER_SERVICE_DENIED | 4010 |
| Permanent Failures [5XXX] | DIAMETER_RATING_FAILED | 5031 |

# Monitoring and Troubleshooting

## Show Commands and Outputs

### show active-charging credit-control statistics

**show active-charging credit-control statistics {group <group_name> | {server <server_name>| ip-address <ip-address>} }**

This output of this command displays the result code-specific counters for initial and update CCA responses, in addition to aggregate of CCA response messages.

***Table 5: Result Code Specific Counters***

| Field | Description |
|---|---|
| **CCA Initial Message Stats** | |
| Result Code 4012 | This counter shows the number of responses received for CCA-I messages with a Diameter Result-Code=4012. |
| Result Code 5031 | This counter shows the number of responses received for CCA-I messages with a Diameter Result-Code=5031. |
| **CCA Update Message Stats** | |
| Result Code 4012 | This counter shows the number of responses received for CCA-U messages with a Diameter Result-Code=4012. |
| Result Code 5031 | This counter shows the number of responses received for CCA-U message with a Diameter Result-Code=5031. |

| Field | Description |
|---|---|
| **CCA Result Code 4xxx Stats** | |
| Result Code 4010 | This counter shows the number of responses received for CCA messages with a Diamter Result-Code=4010. |
| **CCA Result Code 5xxx Stats** | |
| Result Code 5031 | This counter shows the number of responses received for CCA messages with a Diamter Result-Code = 5031. |

# Bulk Statistics

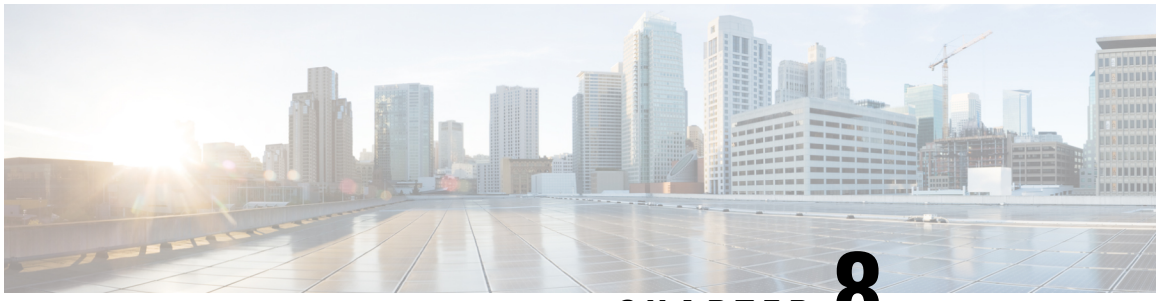
## System Schema Statistics

The following bulk statistics in the SaMOG schema support this feature.

***Table 6: System-level Schema Statistics***

| Reason No. | Description | Data Type |
|---|---|---|
| **Init**: | | |
| cca-init-4010-rc | **Name:** DIAMETER_END_USER_SERVICE_DENIED (4010)<br>**Description:** The total number of responses received for diameter end-user service denied messages.<br>**Type:** Counter | String |
| cca-init-5031-rc | **Name:** DIAMETER_RATING_FAILED (5031)<br>**Description: The** total number of responses received for diameter rating failed messages.<br>**Type:** Counter | String |
| **Update**: | | |
| cca-updt-4010-rc | **Name:** DIAMETER_END_USER_SERVICE_DENIED (4010)<br>**Description:** The total number of responses received for diameter end-user service denied messages<br>**Type: Counter** | String |

| Reason No. | Description | Data Type |
|---|---|---|
| cca-updt-5031-rc | **Name:**DIAMETER_RATING_FAILED (5031)<br>**Description:** The total number of responses received for diameter rating failed messages.<br>**Type:** Counter | String |
| **Aggregate** | | |
| cca-4010-rc | **Name:** DIAMETER_END_USER_SERVICE_DENIED (4010)<br>**Description:** The aggregate number of responses received for diameter end-user service denied messages.<br>**Type: Counter** | String |
| cca-5031-rc | **Name:** DIAMETER_RATING_FAILED (5031)<br>**Description:** The aggregate number of responses received for diameter rating failed messages.<br>**Type: Counter** | String |



CHAPTER 8

# Enabling S6b for IMS APN

This chapter describes the following topics:



## Feature Summary and Revision History

### Summary Data

| | |
|---|---|
| Applicable Product(s) or Functional Area | • GGSN<br>• P-GW<br>• SAEGW |
| Applicable Platform(s) | All |
| Feature Default | Disabled - Configuration Required |
| Related Changes in This Release | Not Applicable |
| Related Documentation | • *Command Line Interface Reference*<br>• *GGSN Administration Guide*<br>• *P-GW Administration Guide*<br>• *SAEGW Administration Guide* |

### Revision History

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

| Revision Details | Release |
|---|---|
| In this release, S2a authorization is enabled to separate the authentication request for LTE and Wi-Fi interfaces using authorize-with-hss eGTP configuration. It enables s6b authentication in both APN and P-GW service for S2a interface only. | 21.21 |
| With this feature, S6b authorization is enabled for 3G access at the APN level to allows P-GW to update the new P-GW ID to HSS. | 21.6 |
| First introduced. | Pre 21.2 |

# Feature Changes

Currently, P-GW supports enabling S6b authentication for 3G access on GGSN service level configuration.

For LTE or Wi-Fi access, S6b authentication is supported on both P-GW service level and APN level configuration. If the S6b authentication is enabled for particular APN, when the subscriber joined on LTE transfers to Wi-Fi then 3G, UE does re-registration of the IMS session on 3G. Different P-GW is selected. However, SGSN does not update the new P-GW. HSS has the history of the old P-GW. When the subscriber transfers back to LTE and then to Wi-Fi, it hands over to the old P-GW. However, the old P-GW does not have the new IMS session and this result in the handover failure. With this feature, S6b authorization is enabled for 3G access at the APN level to let P-GW update the new P-GW ID to HSS. This addresses the inconsistency. Following two **authorize-with-hss** CLI keywords are added at the APN level to enable S6b authentication for 3G access and GnGp handover.

- **gn-gp-enabled**: Enables the S6b authentication for 3G access during the call connect and gn-gp handover.
- **gn-gp-disabled**: Terminates S6b connection when the subscriber moves to 3G access. This is used to override the legacy handover behavior where the session was continued irrespective of the configuration.

**Note** These new keywords are not configured by default when **authorize-with-hss** or **authorize-with-hss egtp** are configured. You have to explicitly enable this customized behavior by configuring the CLI commands introduced for this feature.

**Enhancement to S6b Authentication**: In StarOS 21.21 and later releases, S2a authorization is enabled to separate the authentication request for LTE and Wi-Fi interfaces using **authorize-with-hss egtp** configuration. It enables s6b authentication in both APN and P-GW service for S2a interface only.

# Configuring Commands for Enabling S6b for IMS APN

S6b authentication can be enables at the APN level, two new keywords have been added to the **authorize-with-hss** CLI command.

To enable or disable S6b, execute the following command:

```
configure
```

```
  context context_name
    apn apn_name
      authorize-with-hss [ egtp [ gn-gp-enabled ] [ s2b [ gn-gp-enabled
[ report-ipv6-addr ] ] ] [ s5-s8 [ gn-gp-disabled | gn-gp-enabled ] ] [
report-ipv6-addr ] | lma [ s6b-aaa-group aaa-group-name | report-ipv6-addr
] | report-ipv6-addr ]
       [ default | no ] authorize-with-hss
       exit
```

**NOTES**:

- **gn-gp-disabled:** Disables S6b authorization for 3G initial attach and GNGP handover.
- **gn-gp-enabled:** Enables S6b authorization for 3G initial attach and GNGP handover.
- **s2b:** Enable S6b authorization for egtp-S2b.
- **s5-s8:** Enable S6b authorization for egtp-S5S8.
- **report-ipv6-addr:** Enables IPv6 reporting through AAR toward the S6b interface.

# Enabling S6b Authentication for Trusted Wi-Fi

### Enabling S6b Authentication for Trusted Wi-Fi

S6b authentication is enabled for all LTE and Wi-Fi interface using HSS authentication process. To separate this authentication request for LTE and Wi-Fi interfaces a new configuration is introduced. The parameter S2a is added to represent the trusted Wi-Fi interface in the configuration part of **authorize-with-hss egtp** and this enables the S6b authentication for S2A interface only and this is done in both APN and P-GW service configuration.

Use the following S2a configuration command to indicate Trusted Wi-FI at authorize-with-hss egtp:

```
configure
  context context_name
    apn apn_name| pgw-service service_name
      authorize-with-hss [ egtp [s2a [gn-gp-enabled [report-ipv6-addr]
] ] ]
       [ default | no ] authorize-with-hss
       exit
```

**Note** Enabling the S6b authentication is allowed with a combination of S2a and S2b, or S2a and S5-S8, or S2b and S5-S8.

Below are the examples to enable the s6b authentication for S2a interface alone in APN and P-GW Service.

**Example for APN Service**

```
apn intershat
      pdp-type ipv4 ipv6
      bearer-control-mode mixed
      selection-mode subscribed sent-by-ms chosen-by-sgsn
```

```
    authorize-with-hss egtp s2a
    ims-auth-service ims-ggsn-auth
    ip access-group acl4-1 in
    ip access-group acl4-1 out
    ip context-name egress
    ipv6 access-group acl6-1 in
    ipv6 access-group acl6-1 out
    active-charging rulebase prepaid
  exit
```

**Example for P-GW Service**

```
pgw-service pgw_service
    authorize-with-hss egtp s2a
    associate ggsn-service ggsn-service
    associate egtp-service egtp_service
    associate peer-map map_pgw
    egtp create-session-rsp apn-ambr-always-include
  exit
```

# Show Commands and Outputs

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

## show apn name

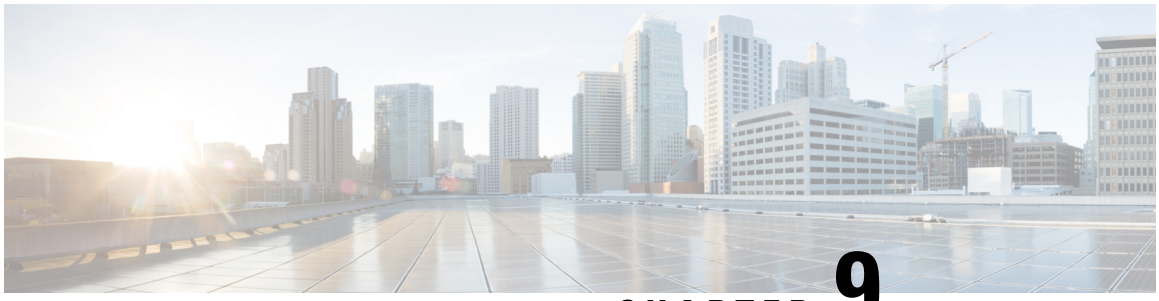
This CLI command is modified to include the gn-gp enabled or disabled status:

- Authorization with S6b : HSS-EGTP-S5S8 GN-GP-Disabled
- Authorization with S6b : HSS-EGTP-S5S8 GN-GP-Enabled

## show config apn intershat

The following new fields are added to the show command to indicate the gn-gp enabled or disabled status:

- authorize-with-hss egtp s5-s8 gn-gp-enabled
- authorize-with-hss egtp s5-s8 gn-gp-disabled



CHAPTER 9

# Enabling Multicast Services over L2TP



## Feature Summary and Revision History

### Summary Data

| | |
|---|---|
| Applicable Product(s) or Functional Area | P-GW |
| Applicable Platform(s) | • ASR 5500<br>• VPC-DI<br>• VPC-SI |
| Feature Default | Disabled - Configuration Required |
| Related Changes in This Release | Not Applicable |
| Related Documentation | Not Applicable |

### Revision History

| Revision Details | Release |
|---|---|
| In this release, P-GW supports Multicast Services over L2TP. | 21.21.1 |

## Feature Description

When a multicast service is set up for the mobile Customer Premises Equipment (CPE), the APN is configured with L2TP tunnel and P-GW works as L2TP Access Concentrator (LAC). To set up the multicast session, the video client/mobile CPE need to send or receive the PIM (Protocol Independent Multicast) message (with TTL=1) to or from Video headend server over SGi L2TP tunnel.

The P-GW follows the default L2TP LAC to inspect and process the encapsulated IP traffic inside the L2TP tunnel. This process prevents certain applications between CPE and LNS that sends TTL=1 traffic to function. Prior to 21.21.1 release, when an IP packet is sent, the Time to Live (TTL) value (for example, 255) was decremented by 1 at each hop. The P-GW dropped the packet with TTL value 0 or 1, decremented (when TTL > 1) the TTL value and the new checksum for the data packet was calculated. In this release, by enabling multicast session over L2TP feature through CLI:

- P-GW ignores the TTL value and forwards the packet.
- The L2TP and regular packets gets differentiated by L2TP tunnel type at sessmgr_ipv4.c and it verifies the CLI configuration mode enabled.

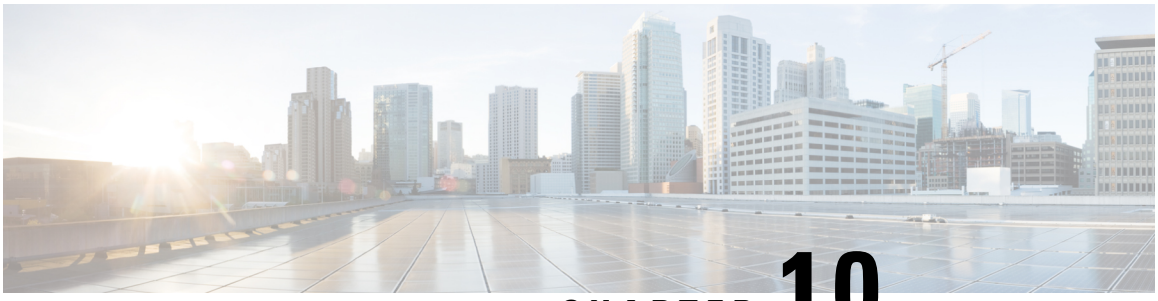
# Configuring Multicast Services over L2TP

Use the following CLI commands to enable or disable the multicast session over L2TP feature. By default, this feature is disabled.

```
configure
  context context_name
    lac-service service_name
      ttl-ignore
      end
```

**Notes**:

- **ttl-ignore**: Ignores the TTL value and forwards the packets.



CHAPTER 10

# IPv4/IPv6 Address Encoding Change in Flow-Description AVP for APPLICATION-START Event Trigger from P-GW



## Feature Summary and Revision History

### Summary Data

| | |
|---|---|
| Applicable Product(s) or Functional Area | P-GW |
| Applicable Platform(s) | • ASR 5500<br>• VPC-DI<br>• VPC-SI |
| Feature Default | Enabled-Always on |
| Related Changes in This Release | Not Applicable |
| Related Documentation | *P-GW Administration Guide* |

### Revision History

| Revision Details | Release |
|---|---|
| The StarOS 21.20.11 is enhanced with IPv4/IPv6 address encoding change in Flow-Description AVP under Application-Detection-Information AVP for APPLICATION-START event trigger from P-GW. | 21.21.1 |
| The StarOS 21.20.11 is enhanced with IPv4/IPv6 address encoding change in Flow-Description AVP under Application-Detection-Information AVP for APPLICATION-START event trigger from P-GW. | 21.20.11 |

| Revision Details | Release |
|---|---|
| The StarOS 21.15.52 is enhanced with IPv4/IPv6 address encoding change in Flow-Description AVP under Application-Detection-Information AVP for APPLICATION-START event trigger from P-GW. | 21.15.52 |

# Feature Changes

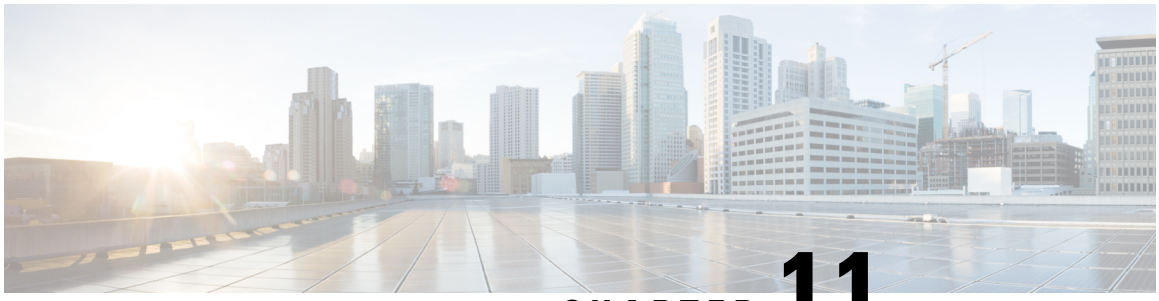
**Previous Behavior:** In CCR-U for APPLICATION-START event trigger from P-GW, Flow-Description AVP under Application-Detection-Information AVP towards PCRF was encoded as:

- For ipv4 flows a netmask of /0 was used
- For ipv6 flows prefix length of 0 was used

**New Behavior**: In the release 21.15.52, in CCR-U for APPLICATION-START event trigger from P-GW, Flow-Description AVP under Application-Detection-Information AVP towards PCRF is encoded as:

- For ipv4 flows a netmask of /32 is used
- For ipv6 flows prefix length of 128 is used

**Customer Impact**: PCRF receives flow description value with 32/128 netmask/prefix. If PCRF rejects the value, ADC over Gx will not work.



CHAPTER 11

# P2P Detection Analysis and Performance Enhancements



# Overview

Three new ACS level CLI, **p2p_force_bailout_value**, **fb_insta_video_detection** , and **voip_subtype_detection** are added for enhancing performance impacts in p2p detection analysis.

**Important** Ensure to enter the CLIs manually to boot the configuration. This is because the plugin CLI is not part of show/ save configuration.

# Configuring Force Bailout and Subtype Detection

### Force Bailout Value

Use the following configuration to force p2p analysis to bailout based on the number of packets configured.

```
configure
      active-charging service acsservice_name
            [ no ] p2p-detection debug-param protocol-param
p2p_force_bailout_value  value
            end
```

**Notes**:

- **p2p_force_bailout_value** *value*: Based on the number of packets configured, p2p analysis is forced to bailout. The values are:
  - Default value is 300.
  - Minimum value allowed is 2.
  - Maximum value allowed is 300.

**Note** Recommended value is 300. Lower values have an impact on detection.

### Enable or Disable Subtype Detection

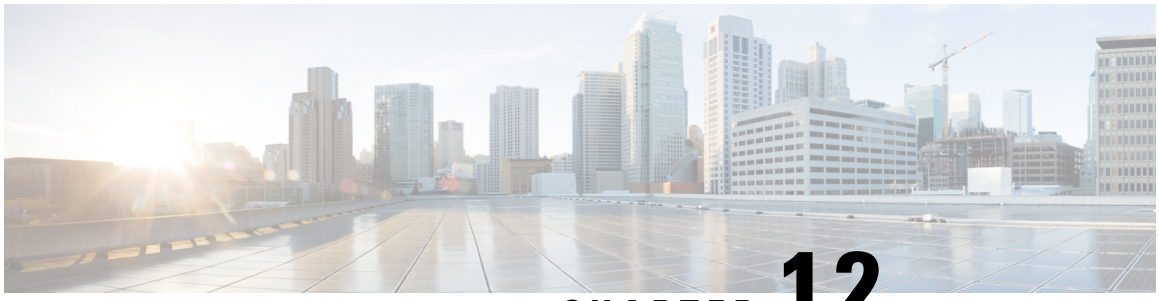
Use the following configuration to enable or disable subtype (unknown, streaming-video) detection for TLS flows in Facebook (FB) or Instagram, which multiplexes multiple media types in a single TCP 5-tuple.

```
configure
      active-charging service acsservice_name
            [ no ] p2p-detection debug-param protocol-param
fb_insta_video_detection value  voip_subtype_detection  value
            end
```

Notes:

- **fb_insta_video_detection** *value*:
  - If the value is set to 1, video detection for Facebook (FB) and Instagram is enabled. The flows with certain SNI for Instagram or Facebook (FB) permanently remains in slow path to detect the media types exchanged in the flow.
  - If the value is set to 0, the video detection for Facebook and Instagram is disabled. The flow will be marked based on first media type exchanged in the flow and offloaded.
- **voip_subtype_detection** *value* : Enable this **voip_subtype_detection** CLI to differentiate audio and video flows in a VOIP call from Facebook/Viber application

**Note**
- If the **voip_subtype_detection** CLI is disabled, both audio and video will be detected as audio.
- To retain the **voip_subtype_detection** CLI across reloads, enter the configuration in boot configuration.



CHAPTER 12

# QUIC IETF Implementation



## Feature Summary and Revision History

### Summary Data

| | |
|---|---|
| Applicable Product(s) or Functional Area | ADC |
| Applicable Platform(s) | • ASR 5500<br>• VPC-DI<br>• VPC-SI |
| Feature Default | Disabled - Configuration Required |
| Related Changes in This Release | Not applicable |
| Related Documentation | • *ADC Administration Guide* |

### Revision History

| Revision Details | Release |
|---|---|
| First Introduced. | 21.21 |

## QUIC IETF Implementation

In the current framework, Deep Packet Inspection (DPI) is done for every packet in a flow when it reaches the plugin. The DPI is done by analyzing the packets and extracting deterministic patterns. The DPI is done in-order to detect the application and to classify its subtype. Plugin excludes the flow after the DPI. The flow is offloaded after the detection. As part of QUIC IETF, the initial QUIC handshake packets (Client/Server Hello) are encrypted over the network. Hence, there are no deterministic patterns available for detection of

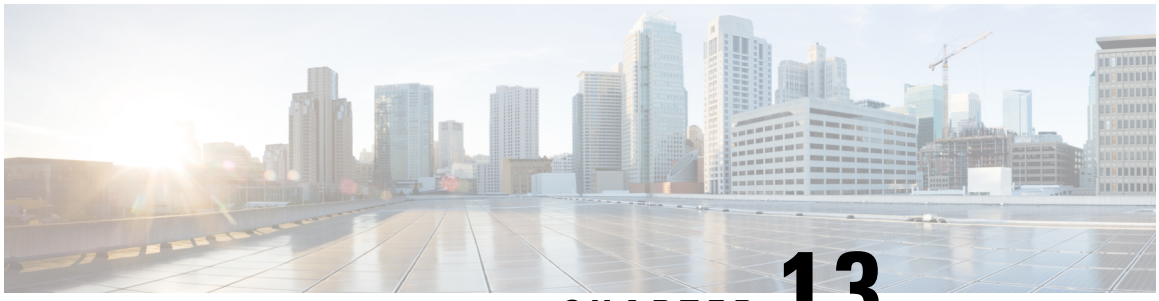
the application. Support is added in P2P plugin to decrypt and obtain the SNI (Server Name Indication) for detection.

# Configuring QUIC IETF

Use the following configuration to enable or disable the QUIC IETF decryption.

```
configure
  active-charging service service_name
    p2p-detection debug-param protocol-param p2p_quic_ietf_decrypt x
    end
```

**Note** By default, the CLI is disabled and there's minimal impact on the performance due to TLS decryption. The CLI needs to be entered manually to boot configuration as plugin CLI is not part of show/save configuration.



CHAPTER 13

# Sessmgr Restart While Processing Secondary RAT Usage CDR Records



## Feature Summary and Revision History

### Summary Data

| | |
|---|---|
| Applicable Product(s) or Functional Area | P-GW |
| Applicable Platform(s) | • ASR 5500<br>• VPC-DI<br>• VPC-SI |
| Feature Default | Enabled - Configuration Required |
| Related Changes in This Release | Not Applicable |
| Related Documentation | • P-GW Administration Guide<br>• Command Line Interface Reference |

### Revision History

| Revision Details | Release |
|---|---|
| In this release, a new CLI command *limit-secondary-rat-usage* is introduced to limit the RAT usage report in CDR. | 21.21.3 |
| First Introduced | 21.19.7 |

# Feature Changes

**Previous Behavior:** Session Manager (SessMgr) is restarted while Charging Data Record (CDR) process is triggered. The restart occurs when the buffer reaches 64K bytes with different stacks.

**New Behavior:** In thisStarOS 21.21.3 release , the SessMgr restart can be avoided by limiting the number of Secondary Radio Access Technology (RAT) usage reports in CDR to a maximum of 32 records. A new CLI command limit-secondary-rat-usage is introduced to limit the Secondary RAT usage report in CDR.

**Note** By default, limit-secondary-rat-usage is disabled. This CLI is not applicable for CUSTOM38 dictionary.

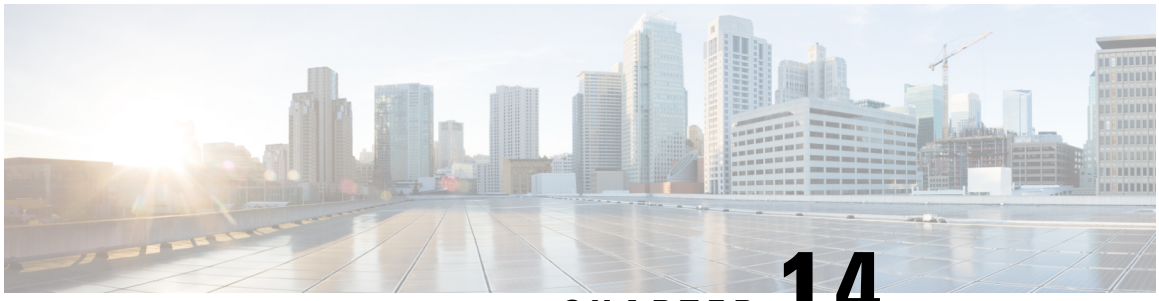
# Command Changes

Use the following CLI configuration to limit the Secondary RAT Usage in CDR.

```
configure
   context context_name
   gtpp group group_name
      [no] limit-secondary-rat-usage
      end
```

**NOTES**:

- **limit-secondary-rat-usage**: Enables limiting the number of Secondary RAT Usage reports in CDR.
- **no**: Disables limiting the number of Secondary RAT Usage reports in CDR.



CHAPTER 14

# 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 | • *SaMOG Administration Guide* |

### Revision History

| Revision Details | Release |
|---|---|
| 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.

# 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 3: Call Flow*

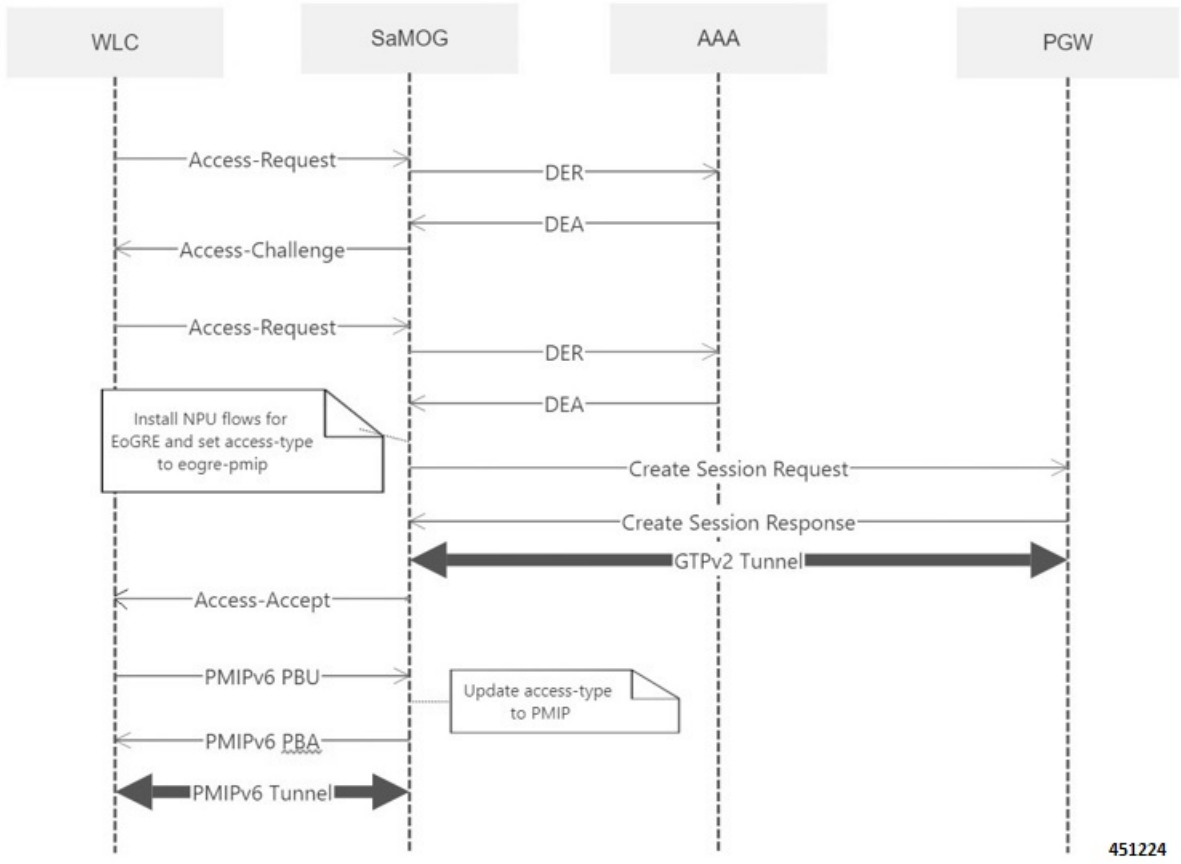



*Table 7: Procedure*

| 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.<br>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 4: Call Flow*

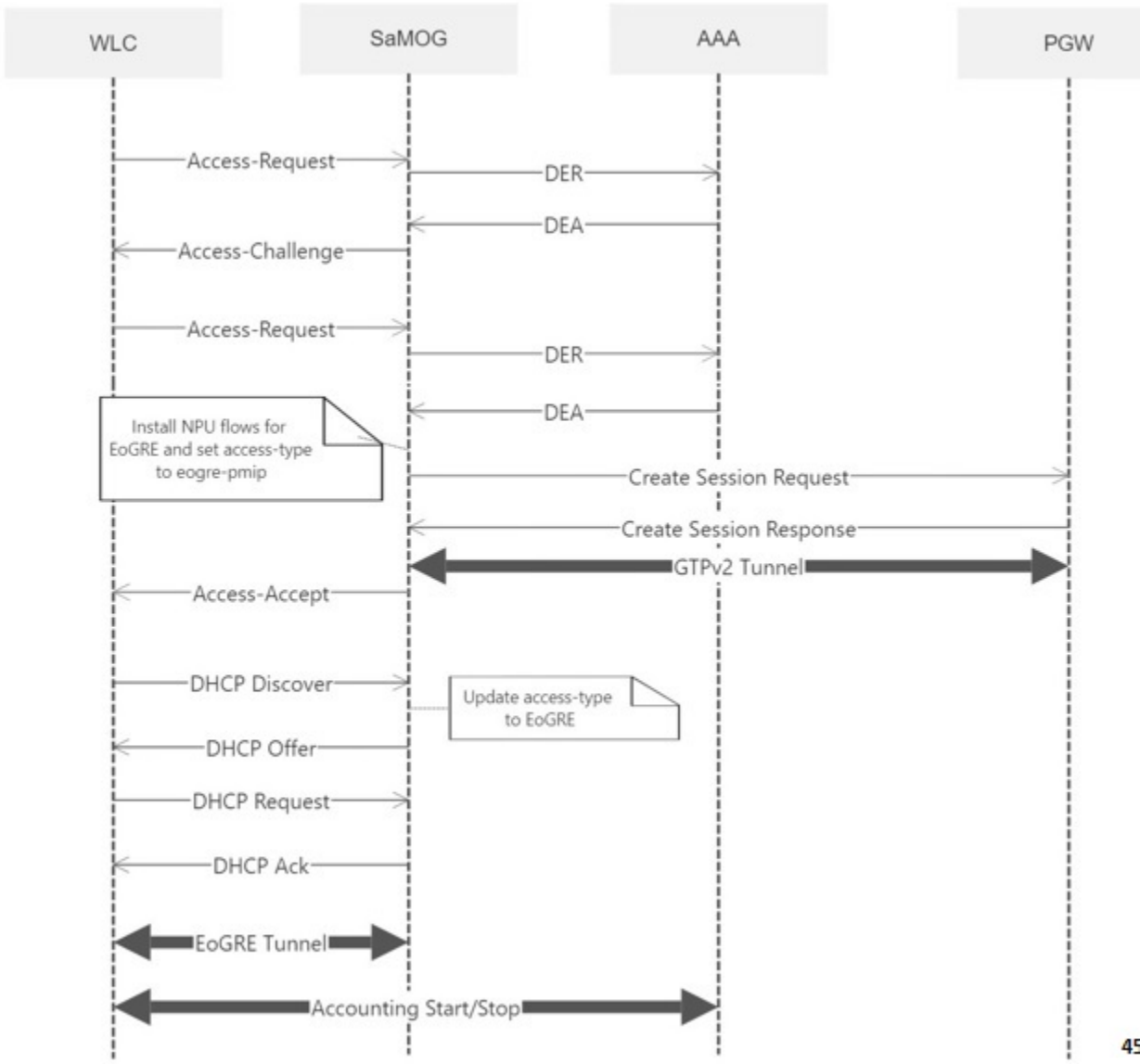



*Table 8: Procedure*

| 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.<br>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 5: Call Flow***

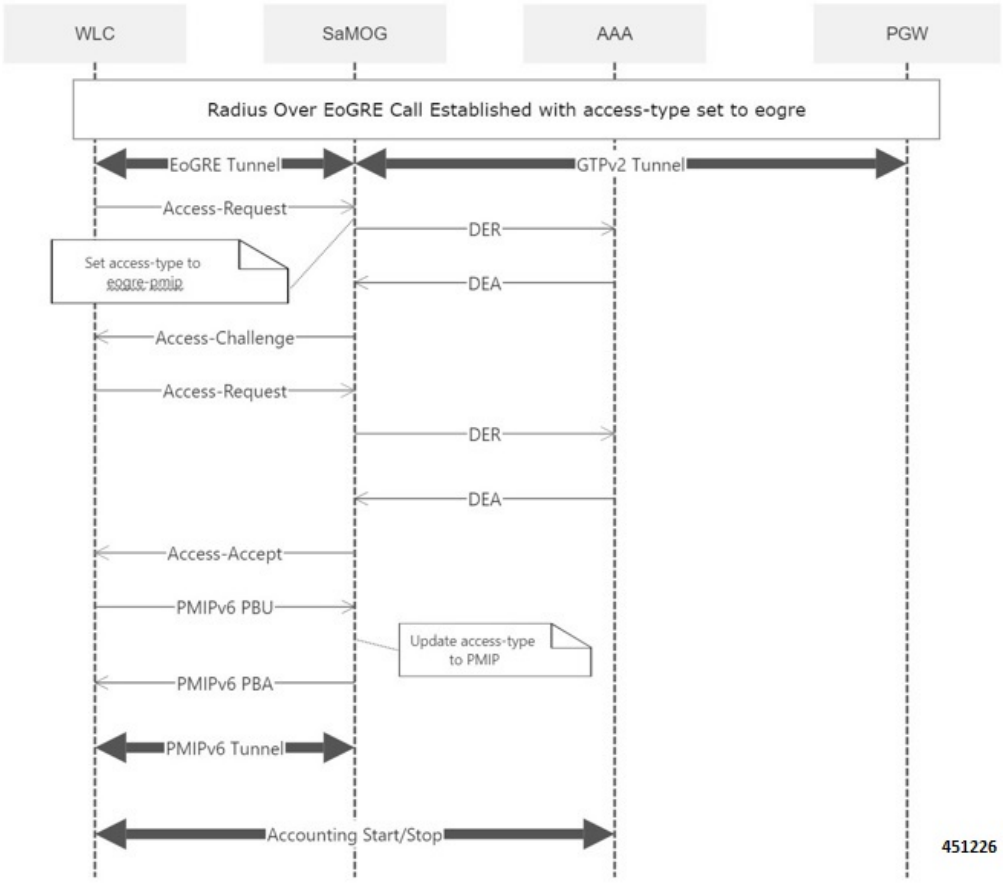



***Table 9: Procedure***

| 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.<br>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 6: Call Flow***

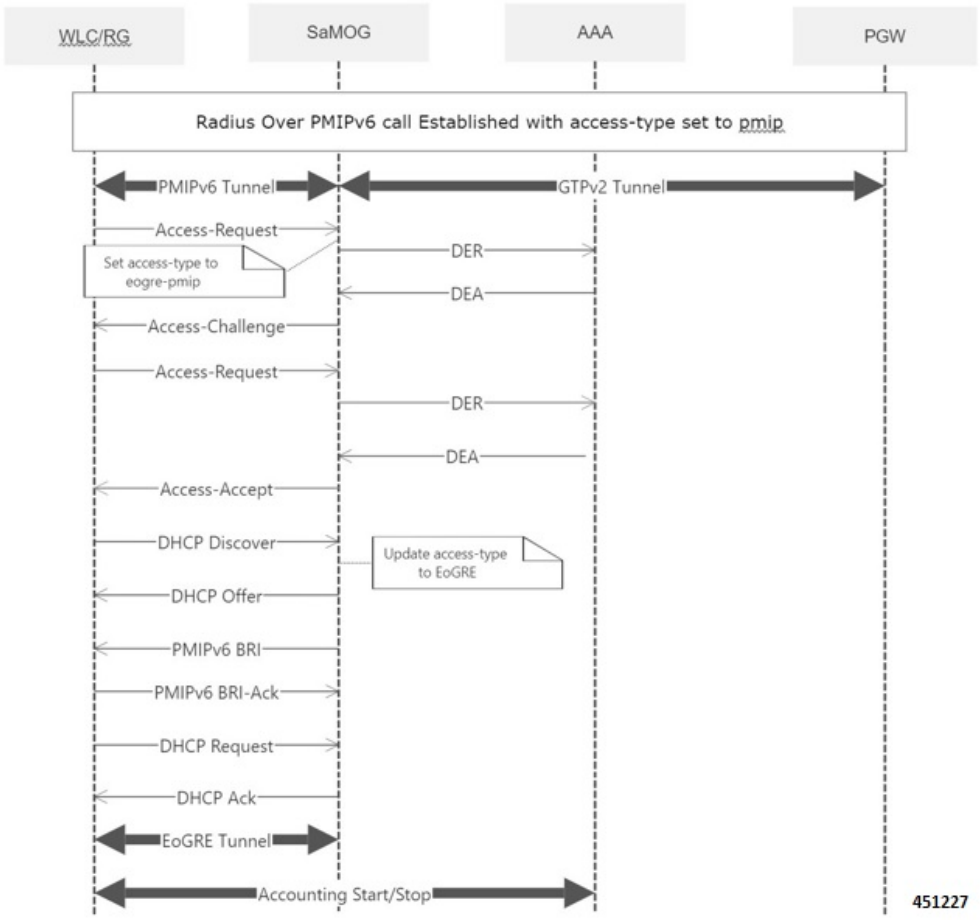



***Table 10: Procedure***

| 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.<br>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.<br>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.

# 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

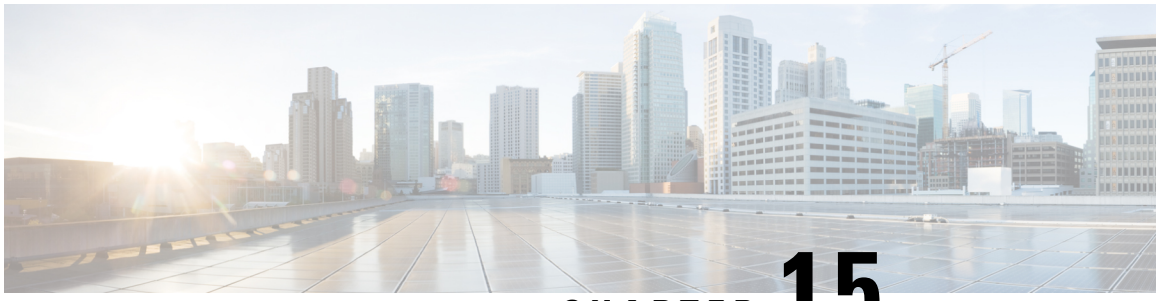
### Show twan-profile

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 11: show twan-profile Command Output Descriptions***

| Field | Description |
|---|---|
| TWAN Profile Name | Name of the TWAN profile |
| **Access-Type Client List** | |
| 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.<br>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.<br>The default RADIUS dictionary can be one of the following:<br>• custom70 for non-Cisco WLC |
| Session Trigger Type | The session trigger type set for the TWAN profile.<br>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 15

# Support for Diameter Error Code Counters



## Feature Summary and Revision History

### Summary Data

| | |
|---|---|
| Applicable Product(s) or Functional Area | ePDG<br>SaMOG |
| Applicable Platform(s) | • ASR 5500<br>• VPC-DI<br>• VPC-SI |
| Feature Default | Enabled - Always-on |
| Related Changes in This Release | Not applicable |
| Related Documentation | • *ePDG Administration Guide*<br>• *SaMOG Administration Guide*<br>• *AAA Interface Administration and Reference*<br>• *Statistics and Counters Reference, StarOS Release Guide* |

### Revision History

| Revision Details | Release |
|---|---|
| This release supports Diameter error code counters and 5001, 5004 and 5041 experimental result codes for ePDG and SaMOG services. | 21.21 |

# Feature Description

In ePDG and SaMOG services, the diameter result code counters are displayed as aggregate counters for different result code ranges, such as 1000-1999, 2000-2999, 3000-3999, 4000-4999 and 5000-5999. For example, 3xxx counter is the cumulative of all result codes that range 3000–3999. These counters are displayed at the global level, for each AAA server group and AAA server levels.

Each answer message from the diameter server, for the request sent from the ePDG and SaMOG, includes a result code or/and an experimental result code AVP. If both, result code and experimental result code AVPs are present, the result code AVP takes precedence. The result codes and experimental result codes are classified as follows:

- 1xxx (Informational) – Errors that fall within this Informational category are used to inform the requester that a request could not be satisfied, and more action is required on its part before access is granted.
- 2xxx (Success) – Result-code that fall within the Success category are used to inform a peer that a request has been successfully completed..
- 3xxx (Protocol Errors) – Errors that fall within the Protocol Errors category is treated on a per-hop basis, and Diameter proxies attempts to correct the error.

  **Note** Protocol errors must only be used in answer messages whose 'E' bit is set.

- 4xxx (Transient Failures) – Errors that fall within the Transient failures category are used to inform a peer that the request could not be satisfied at the time it was received but may be able to satisfy the request in the future.

  **Note** Transient errors must be used in answer messages whose 'E' bit is not set.

- 5xxx (Permanent Failure) – Errors that fall within the Permanent failures category are used to inform the peer that the request failed and should not be attempted again.

  **Note** Permanent errors should be used in answer messages whose 'E' bit is not set.

Counters on each diameter result code help the operators to understand the type of failures. Result code-specific counters are available in the new show command output and in bulk statistics. These counters are available at each AAA server level or as summary of all the AAA servers associated with this ePDG/SaMOG service.

ePDG and SaMOG support the following set of result code-specific counters.

*Table 12: Result Code Specific Counters*

| Error Category | Result Code | Result Code Value |
|---|---|---|
| Protocol Errors [E-bit set] [3XXX] | DIAMETER_UNABLE_TO_DELIVER | 3002 |
| | DIAMETER_TOO_BUSY | 3004 |
| | DIAMETER_LOOP_DETECTED | 3005 |
| | DIAMETER_INVALID_HDR_BITS | 3008 |
| | DIAMETER_INVALID_AVP_BITS | 3009 |
| Transient Failures [Could not satisfy request at this moment] [4XXX] | DIAMETER_AUTHENTICATION_REJECTED | 4001 |
| | DIAMETER_OUT_OF_SPACE | 4002 |
| Permanent Failures [To inform peer, request is failed, should not be attempted again] [5XXX] | DIAMETER_ERROR_USER_UNKNOWN | 5001 |
| | DIAMETER_UNKNOWN_SESSION_ID | 5002 |
| | DIAMETER_AUTHORIZATION_REJECTED | 5003 |
| | DIAMETER_ERROR_ROAMING_NOT_ALLOWED | 5004 |
| | DIAMETER_MISSING_AVP | 5005 |
| | DIAMETER_RESOURCES_EXCEEDED | 5006 |
| | DIAMETER_UNABLE_TO_COMPLY | 5012 |
| | DIAMETER_USER_UNKNOWN | 5030 |
| | DIAMETER_ERROR_USER_NO_WLAN_SUBSCRIPTION | 5041 |

# Monitoring and Troubleshooting

## Show Commands and Outputs

### Show diameter aaa-statistics result-code [all ] | [server <server_name>] [group <group_name> ]

This command displays the following error codes and descriptions.

*Table 13:*

| Field | Description |
|---|---|
| **Authentication Servers Summary** | |

| Field | Description |
|---|---|
| **Protocol Errors (3xxx]** | |
| Result Code 3002 | Shows the aggregate total count of DIAMETER_UNABLE_TO_DELIVER result code value (3002) for all the AAA servers associated with the ePDG service.<br>This error is displayed, if Diameter cannot deliver the message to the destination, either because no host within the realm supporting the required application was available to process the request or because the Destination-Host AVP was specified without the associated Destination-Realm AVP. |
| Result Code 3004 | Shows the aggregate total count of DIAMETER_TOO_BUSY error result code value (3004) only when a specific server is requested and it cannot provide the requested service. |
| Result Code 3005 | Shows the aggregate total count of DIAMETER_LOOP_DETECTED result code value (3005), when an agent detected a loop while trying to get the message to the intended recipient. The message may be sent to an alternate peer, if one is available, but the peer reporting the error has identified a configuration problem. |
| Result Code 3008 | Shows the aggregate total count of DIAMETER_INVALID_HDR_BITS result code value (3008), if a request was received whose bits in the Diameter header were set either to an invalid combination or to a value that is inconsistent with the Command Code definition. |
| Result Code 3009 | Shows the aggregate total count of DIAMETER_INVALID_AVP_BITS result code value (3009), if a request was received that included an AVP whose flag bits are set to an unrecognized value or that is inconsistent with the AVP definition. |
| Result Code Others | Total number of aggregate count results for 3xxx result codes. This Result Code Others does not match with any of the other specific result codes counter. |
| **Transient Failures (4xxx)** | |
| Result Code 4001 | Shows the aggregate total count of DIAMETER_AUTHENTICATION_REJECTED result code value (4001), when the authentication process fails, due to an invalid password used by the user. Further attempts must only be allowed after prompting the user for a new password. |
| Result Code 4002 | Shows the aggregate total couunt of DIAMETER_OUT_OF_SPACE Result code value (4002), when a Diameter node receives the accounting request but was unable to commit it to stable storage due to a temporary lack of space. |

| Field | Description |
|---|---|
| Result Code Others | Total number of aggregate count result for 4xxx result codes. This Result Code Others does not match with any of the other specific result codes counter. |
| **Permanent Failures (5xxx]** | |
| Result Code 5002 | Displays the aggregate total count of DIAMETER_UNKNOWN_SESSION_ID result code value (5002), if the request contains an unknown Session-Id. |
| Result Code 5003 | Displays the aggregate total count of DIAMETER_AUTHORIZATION_REJECTED (5003) result code value, if a request was received for which the user could not be authorized. This error occurs if the requested service is not permitted to the user. |
| Result Code 5005 | Displays the aggregate total count of DIAMETER_MISSING_AVP (5005) result code value, if a request did not contain an AVP that is required by the Command Code definition.<br>**Important** If this value is sent in the Result-Code AVP, a Failed-AVP should be included in the message. The Failed-AVP must contain an example of the missing AVP complete with the Vendor-Id if applicable. The value field of the missing AVP should be of correct minimum length and contain zeroes. |
| Result Code 5006 | Displays the aggregate total count of DIAMETER_RESOURCES_EXCEEDED (5006) result code value, when a request was received that cannot be authorized because the user has already used the allowed resources. For example, error occurs when a user is restricted to one dial-up PPP port, attempts to establish a second PPP connection. |
| Result Code 5012 | Displays the aggregate total count of DIAMETER_UNABLE_TO_COMPLY (5012) result code value, if an error is returned when a request is rejected for unspecified reasons. |
| Result Code 5030 | Displays the aggregate total count of DIAMETER_USER_UNKNOWN (5030) result code value. |
| Result Code Others | Total number of aggregate count result for 5xxx result codes. This Result Code Others does not match with any of the other specific result codes counter. |
| **Experimental Result Code Stats** | |
| Exp Result Code 5001 | Total number of times the Experimental-Result-Code DIAMETER_ERROR_USER_UNKNOWN (5001) is received in the authentication response message. |

| Field | Description |
|---|---|
| Exp Result Code 5004 | Total number of times the Experimental-Result-Code DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004) is received in the authentication response message. |
| **Accounting Servers Summary** | |
| **Protocol Errors (3xxx]** | |
| Result Code 3002 | Shows the aggregate total count of DIAMETER_UNABLE_TO_DELIVER result code value (3002), if Diameter cannot deliver the message to the destination, either because no host within the realm supporting the required application was available to process the request or because the Destination-Host AVP was specified without the associated Destination-Realm AVP. |
| Result Code 3004 | Displays the aggregate total count of DIAMETER_TOO_BUSY error result code value (3004) only when a specific server is requested and it cannot provide the requested service. |
| Result Code 3005 | Shows the aggregate total count of DIAMETER_LOOP_DETECTED result code value (3005), when an agent detected a loop while trying to get the message to the intended recipient. The message may be sent to an alternate peer, if one is available, but the peer reporting the error has identified a configuration problem. |
| Result Code 3008 | Shows the aggregate total count of DIAMETER_INVALID_HDR_BITS result code value (3008), if a request was received whose bits in the Diameter header were set either to an invalid combination or to a value that is inconsistent with the Command Code definition. |
| Result Code 3009 | Shows the aggregate total count of DIAMETER_INVALID_AVP_BITS result code value (3009), if a request was received that included an AVP whose flag bits are set to an unrecognized value or that is inconsistent with the AVP definition. |
| Result Code Others | Total number of aggregate count results for 3xxx result codes. This Result Code Others does not match with any of the other specific result codes counter. |
| **Transient Failures (4xxx)** | |
| Result Code 4001 | Shows the aggregate total count of DIAMETER_AUTHENTICATION_REJECTED result code value (4001), when the authentication process fails, due to an invalid password used by the user. Further attempts must only be allowed after prompting the user for a new password. |

| Field | Description |
|---|---|
| Result Code 4002 | Shows the aggregate total count of DIAMETER_OUT_OF_SPACE Result code value (4002), when a Diameter node receives the accounting request but was unable to commit it to stable storage due to a temporary lack of space. |
| Result Code Others | Total number of aggregate count results for 4xxx result codes. This Result Code Others does not match with any of the other specific result codes counter. |
| **Permanent Failures (5xxx]** | |
| Result Code 5002 | Displays the aggregate total count of DIAMETER_UNKNOWN_SESSION_ID result code value (5002), if the request contains an unknown Session-Id. |
| Result Code 5003 | Displays the aggregate total count of DIAMETER_AUTHORIZATION_REJECTED (5003) result code value, if a request was received for which the user could not be authorized. This error occurs if the requested service is not permitted to the user. |
| Result Code 5005 | Displays the aggregate total count of DIAMETER_MISSING_AVP (5005) result code value, if a request did not contain an AVP that is required by the Command Code definition.<br>**Important** If this value is sent in the Result-Code AVP, a Failed-AVP should be included in the message. The Failed-AVP must contain an example of the missing AVP complete with the Vendor-Id if applicable. The value field of the missing AVP should be of correct minimum length and contain zeroes. |
| Result Code 5006 | Displays the aggregate total count of DIAMETER_RESOURCES_EXCEEDED (5006) result code value, when a request was received that cannot be authorized because the user has already expended allowed resources. For example, error occurs when a user is restricted to one dial-up PPP port, attempts to establish a second PPP connection. |
| Result Code 5012 | Displays the aggregate total count of DIAMETER_UNABLE_TO_COMPLY (5012) result code value, if an error is returned when a request is rejected for unspecified reasons. |
| Result Code 5030 | Displays the aggregate total count of DIAMETER_USER_UNKNOWN (5030) result code value. |
| Result Code Others | Total number of aggregate count results for 5xxx result codes. This Result Code Others does not match with any of the other specific result codes counter. |

| Field | Description |
|---|---|
| **Experimental Result Code Stats** | |
| Exp Result Code 5001 | Total number of times the Experimental-Result-Code DIAMETER_ERROR_USER_UNKNOWN (5001) is received in the authentication response message. |
| Exp Result Code 5004 | Total number of times the Experimental-Result-Code DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004) is received in the authentication response message. |

# Bulk Statistics

This section provides bulkstats related to diameter-auth and diameter-acct schemas for ePDG and SaMOG services.

## diameter-acct Schema

The following counters are available in the Diameter Accounting schema for the following error codes.

| Bulk Statistics | Description |
|---|---|
| acct-result-unable-to-deliver | Shows the total number of Diameter account results with a result code 3002 that cannot be delivered to the destination. |
| acct-result-too-busy | Shows the total number of Diameter account results with a result code 3004 that cannot be allowed for the requested service, when specific servers are requested for. |
| acct-result-loop-detected | Shows the total number of Diameter account results with a result code 3005 that an agent detected a loop while trying to get the message to the inteded recipient. |
| acct-result-invld-hdr-bits | Shows the total number of Diameter account results with a result code 3008 for an invalid header bits request received. A request received could be related to bits in the diameter header , which is set either to an invalid combination or to a value that is inconsistent with the definition of the Command Code. |
| acct-result-invld-avp-bits | Shows the total number of Diameter account results with a result code 3009 for a request received. The diameter code includes an AVP whose flag bits are set to an unrecognized value or that is inconsistent with the AVP definition. |

| Bulk Statistics | Description |
|---|---|
| acct-result-authen-rej | Shows the total number of Diameter account results with a result code 4001 for the user authentication failure due to an invalid password used by the user. |
| acct-result-out-of-space | Shows the total number of Diameter account results with a result code 4002 for a Diameter node received but was unable to commit due to a temporary lack of space. |
| acct-exp-result-user-unknown | Shows the total number of Diameter account expected results with a result code 5001 for the unknown user error. |
| acct-result-unk-sess-id | Shows the total number of Diameter account results with a result code 5002 that contains unknown session Identifiers. |
| acct-result-author-rej | Shows the total number of Diameter account results with a result code 5003 where the user requests could not be authorized. |
| acct-exp-result-roaming-not-allowed | Shows the total number of Diameter expected account results with a result code 5004 for which roaming calls are not allowed. |
| acct-result-missing-avp | Shows the total number of Diameter account results with a result code 5005 that does not contain an AVP. |
| acct-result-resrc-exceed | Shows the total number of account results with a result code 5006 that cannot be authorized because the user has already used allowed resources. |
| acct-result-unable-to-comply | Shows the total number of account results with a result code 5012 rejected for unspecified reasons. |
| acct-result-user-unknown | Shows the total number of account results with a result code 5030 that contains unknown users. |
| acct-exp-result-no-wlan-subs | Shows the total number of expected account results with a result code 5041 for no VLAN sub band. |

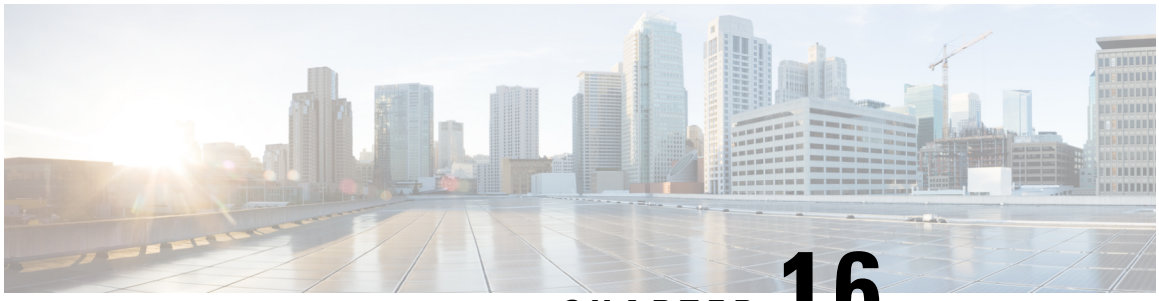
## diameter-auth Schema

The following counters are available in the Diameter Authentication/Authorization schema for the following error codes.

| Bulk Statistics | Description |
|---|---|
| auth-result-unable-to-deliver | Shows the total number of diameter authentiction/authroization results with a result code 3002 that cannot be delivered to the destination. |

| Bulk Statistics | Description |
|---|---|
| auth-result-too-busy | Shows the total number of Diameter authentication/authorization results with a result code 3004 that cannot be allowed for the requested service, when specific servers are requested for. |
| auth-result-loop-detected | Shows the total number of Diameter authentication/authorization results with a result code 3005 that an agent detected a loop while trying to get the message to the inteded recipient. |
| auth-result-invld-hdr-bits | Shows the total number of Diameter authentication/authorization results with a result code 3008 for an invalid header bits request received. A request received could be related to bits in the diameter header that is set either to an invalid combination or to a value that is inconsistent with the definition of the Command Code. |
| auth-result-invld-avp-bits | Shows the total number of Diameter authentication/authorization results with a result code 3009 for a request received. This Diameter authentication/authorization results includs an AVP whose flag bits are set to an unrecognized value or that is inconsistent with the AVP definition. |
| auth-result-authen-rej | Shows the total number of Diameter authentication/authorization results with a result code 4001 for the user authentication failure due to an invalid password used by the user. |
| auth-result-out-of-space | Shows the total number of Diameter authentication/authorization results with a result code 4002 for a Diameter node received but was unable to perform stable commit due to a temporary lack of space. |
| auth-exp-result-user-unknown | Shows the total number of Diameter authentication/authorization expected results with a result code 5001 for the unknown user error. |
| auth-result-unk-sess-id | Shows the total number of Diameter authentication/authorization results with a result code 5002 that contains unknown session Identifiers. |
| auth-result-author-rej | Shows the total number of Diameter authentication/authorization results with a result code 5003 where the user requests could not be authorized. |

| Bulk Statistics | Description |
|---|---|
| auth-exp-result-roaming-not-allowed | Shows the total number of Diameter authentication/authorization expected results with a result code 5004 for which roaming calls are not allowed. |
| auth-result-missing-avp | Shows the total number of Diameter authentication/authorization results with a result code 5005 that does not contain an AVP. |
| auth-result-resrc-exceed | Shows the total number of Diameter authentication/authorization results with a result code 5006 that cannot be authorized because the user has already used allowed resources. |
| auth-result-unable-to-comply | Shows the total number of Diameter authentication/authorization results with a result code 5012 rejected for unspecified reasons. |
| auth-result-user-unknown | Shows the total number of Diameter authentication/authorization results with a result code 5030 that contains unknown users. |
| auth-exp-result-no-wlan-subs | Shows the total number of expected diameter authentication/authorization results with a result code 5041 for no VLAN sub band. |



CHAPTER 16

# Support to List Non-Fatal Snaps and Fatal Crashes in StarOS



## Feature Summary and Revision History

### Summary Data

| | |
|---|---|
| Applicable Product(s) or Functional Area | StarOS |
| Applicable Platform(s) | • ASR 5500<br>• VPC-DI<br>• VPC-SI |
| Feature Default | Enabled - Configuration Required |
| Related Changes in This Release | Not Applicable |
| Related Documentation | *Statistics and Counters Reference* |

### Revision History

| Revision Details | Release |
|---|---|
| First introduced. | 21.21 |

## Feature Description

In StarOS, crashes are classified into two types: Fatal and non-fatal. The following existing crash CLI commands are used to retrieve both Fatal crashes and Non-fatal snaps:

- **show crash all**
- **show crash number <no>**
- **crash copy number <no> url <location>**
- **clear crash list**
- **clear crash number <no>**

In the StarOS 21.20 and later releases, the ‘crash' CLI commands lists only fatal crashes and the following new CLIs lists only non-fatal snaps. Also, support to show that snap records from standby cards are added:

- **show snap list**
- **show snap all**
- **show snap number <no>**
- **snap copy number <no> url <location>**
- **clear snap list**
- **clear snap number <no>**

# Monitoring and Troubleshooting

## Show Commands and Outputs

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

### show crash commands

The following commands shows list of fatal crashes.

- **show crash list** : Shows list of fatal crash records.

  To clear all fatal crash records, use **clear crash list**.

- **show crash all** : Shows all fatal crash records.
- **show crash number**: Shows a particular fatal crash record.

  To view a particular Fatal crash record that is copied to a location , use the **snap copy number** *no.* **url** *location*.

  To clear all fatal crash records, use **clear crash number** *no.*

### show snap commands

The following list of show snap commands shows non-fatal snap records:

- **show snap list**:Shows list of non-fatal snaps.

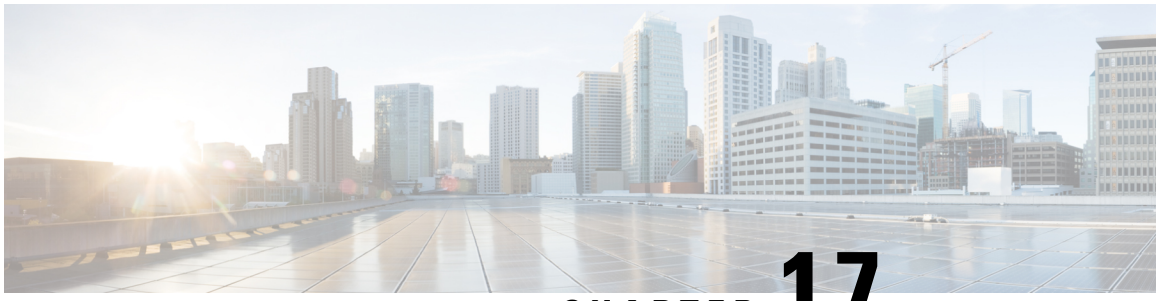
  To clear all non- fatal snap records, use **clear snap list**.

- **show snap number**:Shows a particular Non-Fatal snap record.

  To view a particular Non-Fatal snap record that is copied to a location , use the **snap copy number** *no.* **url** *location*.

  To clear all non-fatal snap records, use **clear snap number** *no.*

- **show snap all**: Shows all non-fatal snap records.
- **show snap list standby**: Shows list of Non-Fatal snaps from standby card.
- **show snap all standby**: Shows all non-fatal snap records from a standby card.
- **show snap number # standby**: Shows a particular non-fatal snap record from a standby card.



CHAPTER 17

# TCP Information Fields in EDR



## Feature Summary and Revision History

### Summary Data

| | |
|---|---|
| Applicable Product(s) or Functional Area | ECS |
| Applicable Platform(s) | • ASR 5500<br>• VPC-DI<br>• VPC-SI |
| Feature Default | Disabled - Configuration Required |
| Related Changes in This Release | Not applicable |
| Related Documentation | • *ECS Administration Guide* |

### Revision History

| Revision Details | Release |
|---|---|
| First Introduced. | 21.21 |

## Feature Description

When the data traffic with TCP starts for a subscriber attached to LTE network. Need to calculate and record time difference between control packets of TCP flow in EDR. Need to record the difference between following packets:

- SYN and SYN-ACK packet

- SYN-ACK and ACK packet

# TCP Fast Open

TCP Fast Open (TFO) is an extension to speed up the opening of successive TCP connections between two endpoints. It works by using a TFO cookie (a TCP option), which is a cryptographic cookie stored on the client and set upon the initial connection with the server. When the client later reconnects, it sends the initial SYN packet along with the TFO cookie data to authenticate itself. If successful, the server may start sending data to the client even before the reception of the final ACK packet of the three-way handshake. Due to this RTT between SYN-ACK and ACK is calculated based on difference between SYN-ACK packet and first uplink ACK packet.

# Configuring and Removing the TCP Information Fields

### Configuring the TCP info Fields

Use the following CLI commands to configure the additional fields in the EDR. Make sure that all other EDR related configurations are present.

```
configure
  active-charging service service_name
    edr-format format_name
      rule-variable tcp syn_synack_rtt priority 3
      rule-variable tcp syn_synack_ack_rtt priority 4
      exit
```

### Removing the TCP info fields

Use the following CLI commands to remove the additional fields in the EDR.

```
configure
  active-charging service service_name
    edr-format format_name
      no rule-variable tcp syn_synack_rtt priority 3
      no rule-variable tcp syn_synack_ack_rtt priority 4
      exit
```