# Release Change Reference, StarOS Release 21.13/Ultra Services Platform Release 6.7

**First Published:** 2019-03-28

**Last Modified:** 2020-07-14

**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

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

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

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

CHAPTER 1

# Release 21.13/6.7 Features and Changes Quick Reference

## Release 21.13/6.7 Features and Changes

| Features / Behavior Changes | Applicable Product(s) / Functional Area | Release Introduced / Modified |
|---|---|---|
| Automate RHEL Version Locking Mechanism, on page 13 | OSPD | 6.7 |
| Controlling the Inclusion of Extended Bitrate in PGW-CDRs, on page 15 | P-GW, SAEGW | 21.13 |
| Deprecation of Manual Scaling, on page 17 | UAS | 6.0 |
| Flow-based QoS, on page 19 | P-GW | 21.13.2 |
| IPSec Manager Support on Demux DPC2 cards, on page 23 | IPSec (IKEv1/IKEv2 ACL Mode) | 21.13 |
| MAC Algorithm Configuration, on page 27 | All | 21.13 |
| NB-IOT EDRX Supported values in ATTACH/TAU Accept, on page 29 | MME | 21.13.11 |
| Network Access Identifier Field Removal from MSISDN, on page 31 | P-GW | 21.13 |
| New Attribute in P-GW CDR for Custom GTPP Dictionary, on page 33 | P-GW | 21.13.2 |
| Paging eDRX H-SFN Changed to 10 Bits Counter, on page 35 | MME | 21.13.11 |
| Password Generation Support, on page 37 | All | 21.13 |

| Features / Behavior Changes | Applicable Product(s) / Functional Area | Release Introduced / Modified |
|---|---|---|
| PRA and Multi PRA Support, on page 41 | P-GW | 21.13.15 |
| Random Number Generator Support for OS and Platforms, on page 43 | All | 21.13 |
| S-GW CDR Support for Non-IP PDN Subscribers, on page 45 | C-SGN, S-GW | 21.13 |
| Target MME Load Balancing During Handover, on page 47 | MME | 21.13 |
| Tethering Block for Downlink Packets, on page 49 | P-GW | 21.13.2 |

CHAPTER 2

# Feature Defaults Quick Reference

## Feature Defaults

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

| Feature | Default |
|---|---|
| Automate RHEL Version Locking Mechanism | Disabled - Configuration required |
| Controlling the Inclusion of Extended-Bitrate in P-GW CDRs | Disabled - Configuration Required |
| Deprecation of Manual Scaling | Disabled - Configuration Required |
| Flow-based QoS | Disabled - Configuration Required |
| IPSec Manager Support on Demux DPC2 cards | Disabled - Configuration Required |
| MAC Algorithm Configuration | Disabled - Configuration Required |
| NB-IOT EDRX Supported values in ATTACH/TAU Accept | Enabled - Configuration Required |
| Network Access Identifier Field Removal from MSISDN | Enabled - Always-on |
| New Attribute in P-GW CDR for Custom GTPP Dictionary | Enabled - Always-on (for a customer-specific GTPP dictionary) |
| Paging eDRX H-SFN Changed to 10 Bits Counter | This feature is enabled/disabled, when the eDRX feature is enabled/disabled. |
| Password Generation Support | Enabled - Configuration Required |
| PRA and Multi PRA Support | Enabled - Always-on (for a customer-specific Gx dictionary) |
| Random Number Generator Support for OS and Platform | Disabled - Configuration Required |
| S-GW CDR Support for Non-IP PDN Subscribers | Enabled - Always-on |
| Target MME Load Balancing During Handover | Enabled - Always on |

| Feature | Default |
|---|---|
| Tethering Block for Downlink Packets | Disabled - Configuration Required |

CHAPTER 3

# Bulk Statistics Changes Quick Reference

This chapter identifies bulk statistics changes added to, modified for, or deprecated from the StarOS 21.13 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 21.13 include:

- New Bulk Statistics, on page 5
- Modified Bulk Statistics, on page 8
- Deprecated Bulk Statistics, on page 8

## New Bulk Statistics

This section identifies new bulk statistics and new bulk statistic schemas introduced in release 21.13.

**SAE-GW Schema**

The following bulk statistics are added in the SAE-GW schema in support of Transactional Rate KPI Statistics.

| Bulk Statistics | Description |
|---|---|
| pgw-transrate-sessevt-cumlt | Cumulative count: Indicates the number of new PDN Session Create or Delete requests received/sent. |
| pgw-transrate-sessevt-bkt1 | Indicates the number of new PDN Session Create or Delete Requests received in a given interval. |
| pgw-transrate-sessevt-bkt2 | Indicates the number of new PDN session creation or deletion requests received in a given interval. |
| pgw-transrate-sessevt-bkt3 | Indicates the number of new PDN session creation or deletion requests received in a given interval. |
| pgw-transrate-sessevt-bkt4 | Indicates the number of new PDN session creation or deletion requests received in a given interval. |

| | |
|---|---|
| pgw-transrate-sessevt-bkt5 | Indicates the number of new PDN session creation or deletion requests received in a given interval. |
| pgw-transrate-sessevt-bkt6 | Indicates the number of new PDN session creation or deletion requests received in a given interval. |
| pgw-transrate-sessevt-bkt7 | Indicates the number of new PDN session creation or deletion requests received in a given interval. |
| pgw-transrate-sessevt-bkt8 | Indicates the number of new PDN session creation or deletion requests received in a given interval. |
| pgw-transrate-succ-sessevt-cumlt | Cumulative count: Indicates the number of successful PDN session creation or deletion responses |
| pgw-transrate-succ-sessevt-bkt1 | Indicates the number of successful PDN session creation or deletion responses in a given interval. |
| pgw-transrate-succ-sessevt-bkt2 | Indicates the number of successful PDN session creation or deletion responses in a given interval. |
| pgw-transrate-succ-sessevt-bkt3 | Indicates the number of successful PDN session creation or deletion responses in a given interval. |
| pgw-transrate-succ-sessevt-bkt4 | Indicates the number of successful PDN session creation or deletion responses in a given interval. |
| pgw-transrate-succ-sessevt-bkt5 | Indicates the number of successful PDN session creation or deletion responses in a given interval. |
| pgw-transrate-succ-sessevt-bkt6 | Indicates the number of successful PDN session creation or deletion responses in a given interval. |
| pgw-transrate-succ-sessevt-bkt7 | Indicates the number of successful PDN session creation or deletion responses in a given interval. |
| pgw-transrate-succ-sessevt-bkt8 | Indicates the number of successful PDN session creation or deletion responses in a given interval. |
| pgw-transrate-unsucc-sessevt-cumlt | Cumulative count: Indicates the number of unsuccessful PDN session creation or deletion responses |
| pgw-transrate-unsucc-sessevt-bkt1 | Indicates the number of unsuccessful PDN session creation or deletion responses in a given interval. |
| pgw-transrate-unsucc-sessevt-bkt2 | Indicates the number of unsuccessful PDN session creation or deletion responses in a given interval. |
| pgw-transrate-unsucc-sessevt-bkt3 | Indicates the number of unsuccessful PDN session creation or deletion responses in a given interval. |
| pgw-transrate-unsucc-sessevt-bkt4 | Indicates the number of unsuccessful PDN session creation or deletion responses in a given interval. |

| | |
|---|---|
| pgw-transrate-unsucc-sessevt-bkt5 | Indicates the number of unsuccessful PDN session creation or deletion responses in a given interval. |
| pgw-transrate-unsucc-sessevt-bkt6 | Indicates the number of unsuccessful PDN session creation or deletion responses in a given interval. |
| pgw-transrate-unsucc-sessevt-bkt7 | Indicates the number of unsuccessful PDN session creation or deletion responses in a given interval. |
| pgw-transrate-unsucc-sessevt-bkt8 | Indicates the number of unsuccessful PDN session creation or deletion responses in a given interval. |
| pgw-transrate-nwinit-setupteardown-evt-cumlt | Cumulative count: Indicates the number of bearer creation or deletion requests sent |
| pgw-transrate-nwinit-setupteardown-evt-bkt1 | Indicates the number of bearer creation or deletion requests sent per second in a given interval. |
| pgw-transrate-nwinit-setupteardown-evt-bkt2 | Indicates the number of bearer creation or deletion requests sent per second in a given interval. |
| pgw-transrate-nwinit-setupteardown-evt-bkt3 | Indicates the number of bearer creation or deletion requests sent per second in a given interval. |
| pgw-transrate-nwinit-setupteardown-evt-bkt4 | Indicates the number of bearer creation or deletion requests sent per second in a given interval. |
| pgw-transrate-nwinit-setupteardown-evt-bkt5 | Indicates the number of bearer creation or deletion requests sent per second in a given interval. |
| pgw-transrate-nwinit-setupteardown-evt-bkt6 | Indicates the number of bearer creation or deletion requests sent per second in a given interval. |
| pgw-transrate-nwinit-setupteardown-evt-bkt7 | Indicates the number of bearer creation or deletion requests sent per second in a given interval. |
| pgw-transrate-nwinit-setupteardown-evt-bkt8 | Indicates the number of bearer creation or deletion requests sent per second in a given interval. |
| pgw-transrate-succ-nwinit-setupteardown-evt-cumlt | Cumulative count: Indicates the number of successful bearer Creation or deletion responses. |
| pgw-transrate-succ-nwinit-setupteardown-evt-bkt1 | Indicates the number of successful bearer creation or deletion responses sent per second in a given interval. |
| pgw-transrate-succ-nwinit-setupteardown-evt-bkt2 | Indicates the number of successful bearer creation or deletion responses sent per second in a given interval. |
| pgw-transrate-succ-nwinit-setupteardown-evt-bkt3 | Indicates the number of successful bearer creation or deletion responses sent per second in a given interval. |
| pgw-transrate-succ-nwinit-setupteardown-evt-bkt4 | Indicates the number of successful bearer creation or deletion responses sent per second in a given interval. |

| | |
|---|---|
| pgw-transrate-succ-nwinit-setupteardown-evt-bkt5 | Indicates the number of successful bearer creation or deletion responses sent per second in a given interval. |
| pgw-transrate-succ-nwinit-setupteardown-evt-bkt6 | Indicates the number of successful bearer creation or deletion responses sent per second in a given interval. |
| pgw-transrate-succ-nwinit-setupteardown-evt-bkt7 | Indicates the number of successful bearer creation or deletion responses sent per second in a given interval. |
| pgw-transrate-succ-nwinit-setupteardown-evt-bkt8 | Indicates the number of successful bearer creation or deletion responses sent per second in a given interval. |
| pgw-transrate-unsucc-nwinit-setupteardown-evt-cumlt | Cumulative count: Indicates the number of unsuccessful bearer creation or deletion responses |
| pgw-transrate-unsucc-nwinit-setupteardown-evt-bkt1 | Indicates the number of unsuccessful bearer creation or deletion responses sent per second in a given interval. |
| pgw-transrate-unsucc-nwinit-setupteardown-evt-bkt2 | Indicates the number of unsuccessful bearer creation or deletion responses sent per second in a given interval. |
| pgw-transrate-unsucc-nwinit-setupteardown-evt-bkt3 | Indicates the number of unsuccessful bearer creation or deletion responses sent per second in a given interval. |
| pgw-transrate-unsucc-nwinit-setupteardown-evt-bkt4 | Indicates the number of unsuccessful bearer creation or deletion responses sent per second in a given interval. |
| pgw-transrate-unsucc-nwinit-setupteardown-evt-bkt5 | Indicates the number of unsuccessful bearer creation or deletion responses sent per second in a given interval. |
| pgw-transrate-unsucc-nwinit-setupteardown-evt-bkt6 | Indicates the number of unsuccessful bearer creation or deletion responses sent per second in a given interval. |
| pgw-transrate-unsucc-nwinit-setupteardown-evt-bkt7 | Indicates the number of unsuccessful bearer creation or deletion responses sent per second in a given interval. |
| pgw-transrate-unsucc-nwinit-setupteardown-evt-bkt8 | Indicates the number of unsuccessful bearer creation or deletion responses sent per second in a given interval. |

# Modified Bulk Statistics

None in this release.

# Deprecated Bulk Statistics

None in this release.

CHAPTER 4

# SNMP MIB Changes in StarOS 21.13 and USP 6.7

This chapter identifies SNMP MIB objects, alarms and conformance statements added to, modified for, or deprecated from the StarOS 21.13 and Ultra Services Platform (USP) 6.7 software releases.

## SNMP MIB Object Changes for 21.13

This section provides information on SNMP MIB alarm changes in release 21.13.

**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 21.13.

The following alarms are new in this release:

- starIPAddressType
- starServiceLossCause
- starServiceLossDetected

### Modified SNMP MIB Object

This section identifies SNMP MIB alarms modified in release 21.13.

The following alarms have been modified in this release:

- starSRPIpAddress

- starSRPActive
- starSRPStandby
- starBGPPeerReachable
- starBGPPeerUnreachable
- starSRPAAAReachable
- starSRPAAAUnreachable
- starSRPSwitchoverInitiated
- starSRPCheckpointFailure
- starSRPConfigOutOfSync
- starSRPConfigInSync
- starSRPConnDown
- starSRPConnUp
- starUplaneServiceStop
- starDisabledEventIDs

### Deprecated SNMP MIB Object

None in this release.

# SNMP MIB Alarm Changes for 21.13

This section provides information on SNMP MIB alarm changes in release 21.13.

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

### New SNMP MIB Alarms

None in this release.

### Modified SNMP MIB Alarms

None in this release.

### Deprecated SNMP MIB Alarms

None in this release.

# SNMP MIB Conformance Changes for 21.13

This section provides information on SNMP MIB alarm changes in release 21.13.

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

### New SNMP MIB Conformance

None in the release.

### Modified SNMP MIB Conformance

None in the release.

### Deprecated SNMP MIB Conformance

None in the release.

# SNMP MIB Object Changes for 6.7

This section provides information on SNMP MIB object changes in the Ultra M MIB corresponding to release 6.7.

**Important** For more information regarding SNMP MIB objects in this section, see the *Ultra M Solutions Guide* for this release.

### New SNMP MIB Objects

None in this release.

### Modified SNMP MIB Objects

None in this release.

### Deprecated SNMP MIB Objects

None in this release.

# SNMP MIB Alarm Changes for 6.7

This section provides information on SNMP MIB alarm changes in the Ultra M MIB corresponding to release 6.7.

**Important** For more information regarding SNMP MIB alarms in this section, see the *Ultra M Solutions Guide* for this release.

### New SNMP MIB Alarms

None in this release.

### Modified SNMP MIB Alarms

None in this release.

### Deprecated SNMP MIB Alarms

None in this release.

## SNMP MIB Conformance Changes for 6.7

This section provides information on SNMP MIB conformance statement changes in the Ultra M MIB corresponding to release 6.7.

**Important** For more information regarding SNMP MIB conformance statements in this section, see the *Ultra M Solutions Guide* for this release.

### New SNMP MIB Conformance Statements

None in this release.

### Modified SNMP MIB Conformance Statements

None in this release.

### Deprecated SNMP MIB Conformance Statements

None in this release.

CHAPTER 5

# Automate RHEL Version Locking Mechanism

# Feature Summary and Revision History

### Summary Data

| | |
|---|---|
| Applicable Product(s) or Functional Area | OSPD |
| Applicable Platform(s) | UGP |
| Feature Default | Disabled - Configuration required |
| Related Features in this Release | Not Applicable |
| Related Documentation | • *Ultra M Solutions Guide*<br>• *Ultra Services Platform Deployment Automation Guide*<br>• *Ultra Services Platform NETCONF API Guide* |

### Revision History

| **Revision Details** | **Release** |
|---|---|
| First introduced. | 6.7 |

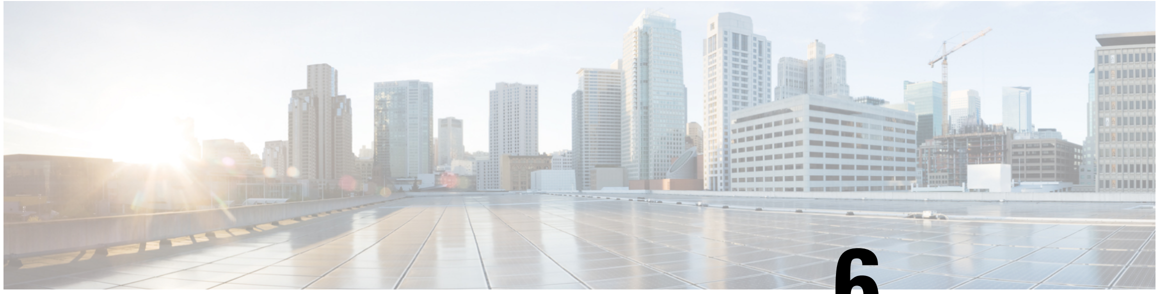
# Feature Description

This release introduces new configuration parameters to automate the RHEL version locking process.

**Note** The configuration commands to enable the version lock depends on the RHEL version.

As a prerequisite, the OpenStack Platform Director (OSPD) server must be registered with the RHEL satellite server using the appropriate activation key for the OSP and RHEL versions. Depending on the RHEL version, use the commands as shown in the following table.

| RHEL Version | Configuration Command | Example Command |
|---|---|---|
| RHEL version < 7.4 | **echo "**<*release-version*>**" \| sudo tee -a /etc/yum/vars/releasever**<br>**subscription-manager register --org="**<*organization*>**" --activationkey="**<*activation key*>**"** | **echo "7.3" \| sudo tee -a /etc/yum/vars/releasever**<br>**subscription-manager register --org="MCBU" --activationkey="osp9"** |
| RHEL version = or > 7.4 | **subscription-manager register --org="**<*organization*>**" --activationkey="**<*activation key*>**" --release="**<*release version*>**"**<br>**IMPORTANT**: The yum configuration is not required as the default value is used. | **subscription-manager register --org="MCBU" --activationkey="rhel75-osp10" --release="7.5"** |



CHAPTER 6

# Controlling the Inclusion of Extended Bitrate in PGW-CDRs

## Feature Summary and Revision History

### Summary Data

| | |
|---|---|
| Applicable Product(s) or Functional Area | • P-GW<br>• SAEGW |
| 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* |

### Revision History

| **Revision Details** | **Release** |
|---|---|
| A new CLI keyword is introduced to exclude 5G NSA specific extended-bitrate information from PGW-CDRs. | 21.13 |
| First introduced. | 21.9 |

# Feature Changes

P-GW/SAEGW controls the inclusion of extended-bitrate information in CDR over Gz interface even though the bandwidth is greater than 4.2 Gbps. Inclusion of extended-bitrate information in CDRs in P-GW/SAEGW is CLI controlled.

**Previous Behavior**: 5G NSA specific extended-bitrate information is included always in PGW CDRs whenever the APN-AMBR, MBR or GBR is greater than 4.2Gbps.

**New Behavior**: 5G NSA specific extended-bitrate information can be configured to exclude from PGW CDRs even though APN-AMBR, MBR or GBR is greater than 4.2Gbps. By default the extended bitrate information is included if the APN-AMBR, MBR or GBR is greater than 4.2Gbps

# Command Changes

This section describes the CLI configuration required to configure controlling the inclusion of Extended Bitrates in PGW CDRs.

## extended-bitrate

Use the following configuration to control the inclusion of Extended-Bitrates in PGW-CDRs.

```
configure
  context context_name
    [ no ] gtpp attribute extended-bitrate
    end
```

**NOTES:**

- **extended-bitrate**: Includes the extended bit-rate information in PGW-CDRs when the APN-AMBR, MBR or GBR is greater than 4.2 Gbps

- **no**: Does not include the extended bit-rate information in PGW-CDRs even though the APN-AMBR, MBR or GBR is greater than 4.2 Gbps.

CHAPTER 7

# Deprecation of Manual Scaling

## Feature Summary and Revision History

### Summary Data

| | |
|---|---|
| Applicable Product(s) or Functional Area | UAS |
| Applicable Platform(s) | UGP |
| Feature Default | Disabled - Configuration Required |
| Related Changes in This Release | Not applicable |
| Related Documentation | • *Ultra M Solutions Guide*<br>• *Ultra Services Platform Deployment Automation Guide* |

### Revision History

| **Revision Details** | **Release** |
|---|---|
| The support for manual scale-in and scale-out functionality has been deprecated in this release. | 6.0 through 6.14 |
| First introduced | 6.0 |

## Feature Changes

**Previous Behavior**: In previous releases, the Service Function (SF) scaling (including the manual scale-in and scale-out) feature was supported.

**New Behavior**: In this release, the manual scale-out and scale-in functionalities have been deprecated. For more information, contact your Cisco account representative.

CHAPTER 8

# Flow-based QoS

## 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 | • *Command Line Interface Reference*<br>• *P-GW Administration Guide* |

### Revision History

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

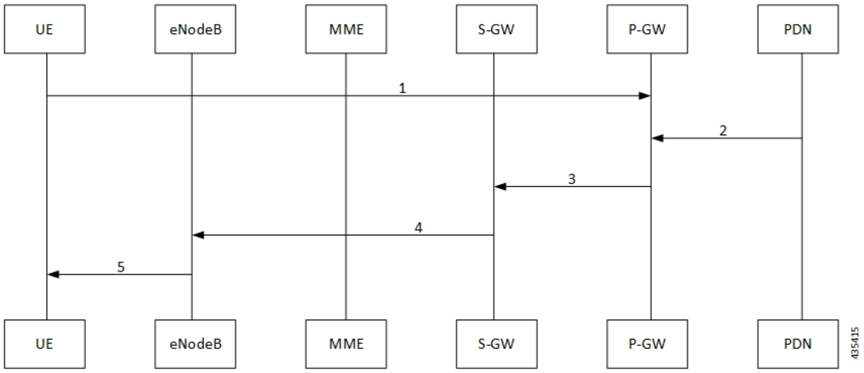
| **Revision Details** | **Release** |
|---|---|
| P-GW supports prioritization of downlink traffic with the same bearer, based on a configured DSCP value in the outer-IP header | 21.13.2 |

| Revision Details | Release |
|---|---|
| First introduced. | Pre 21.2 |

# Feature Changes

Traffic for a set of application flows can be prioritized based on the combination of the subscription value and the intended application. To support this, the P-GW provisions a configuration where the downlink traffic within the same bearer can be prioritized based on a configurable DSCP value in the outer-IP header.

The following call flow, at a high-level, illustrates the DSCP marking on the outer-IP header in a downlink traffic for a selected application.



| Steps | Description |
|---|---|
| 1 | UE Attach Procedure and Session establishment on all the EPC Nodes (UE, eNodeB, MME, S-GW, and P-GW). |
| 2 | Downlink traffic sent to the UE from the PDN. |
| 3 | On receiving the data in the downlink direction from specific applications flows, the P-GW encodes the dscp-marking of the outer-IP header with the configured **tos-value** of the **charging-action** present under **active-charging**. |
| 4 | Based on the S-GW policies, the data is processed further and forwarded towards the UE through eNodeB. |
| 5 | UE received data from the eNodeB. |

# Command Changes

A new CLI command – **outer-packet-only**, is added to the **charging-action** profile of the Active Charging Service mode. The DSCP value is configured under Charging-Action.

On configuring this command, the combination of Ruledef and the Charging-Action under the Rulebase ensures that a specific flow is selected for further processing. The configured DSCP value is encoded to the outer-IP DSCP field.

Use the following configuration to encode DSCP value in the outer-IP header for specific flows:

```
configure
   require active-charging
   active-charging-service
      charging-action action_name
         ip tos tos_valuedownlink outer-packet-only
         no ip tos downlink
         end
```

**Important** When the above CLI is configured, the outer-packet-only functionality takes precedence over other CLI configurations, which affects DSCP marking of outer-IP header.

**NOTES**:

- **ip**: Specifies the IP related configuration.
- **tos**: Specifies the type of service. *tos_value* specifies the ToS or DSCP value to be configured.
- **downlink**: Specifies downlink packets only.
- **outer-packet-only**: Copies the configured ToS value to the outer packet header.

# Performance Indicator Changes

## show active-charging charging-action statistics name

The output of this command includes the following field in support of this functionality:

- Outer IP header dscp marked Pkts: This field specifies the count of all the packets that are marked with the DSCP value in the outer-IP header for the corresponding charging-action.

CHAPTER 9

# IPSec Manager Support on Demux DPC2 cards

## Feature Summary and Revision History

### Summary Data

| | |
|---|---|
| Applicable Product(s) or Functional Area | IPSec (IKEv1/IKEv2 ACL Mode) |
| Applicable Platform(s) | ASR 5500 (DPC2) |
| Default Setting | Disabled - Configuration Required |
| Related Changes in This Release | Not Applicable |
| Related Documentation | *Command Line Interface Reference* |

### Revision History

| **Revision Details** | **Release** |
|---|---|
| First introduced. | 21.13 |

## Feature Description

With 21.13 release, Crypto processing for Crypto map has moved to demux card. As there is no session manager spawned in it, the under-utilized cores are used for IPSec traffic processing without affecting user data processing on non-Demux DPC2 cards. A CLI command is available to control the spawning of IPSec manager in the Demux card.

# How it Works

## Limitations

This section describes the known limitations for IPSec Manager Support on Demux DPC2 cards.

- This feature is supported only for DPC2.
- This feature is applicable for ACL mode for IKEv1, IKEv2-v4, and IKEv2-v6.
- **ipsec-on-demux** CLI command does not work when Demux on MIO is enabled.
- Each IPSec manager will serve only eight Crypto maps.
- Maximum IPSec managers supported per CPU is one, and maximum of three at card level for IKEv1 and IKEv2 separately.
- If more than 24 active Crypto maps are configured, then the fourth IPSec manager and subsequent IPSec managers are spawned on the non-Demux DPC2 card. New IPSec manager handles original number of Crypto maps (that is, 150).
- If a new Crypto map without the CLI is configured, then it spawns or reuse IPSec managers present on a non-Demux DPC2 card. New IPSec manager does not reuse or spawn IPSec managers already running on the demux card.
- If a new Crypto map with the CLI is configured, then it will spawn or re-use IPSec managers present on the Demux DPC2 card. It does not reuse or spawn IPSec managers already running on the non Demux card.
- When the limit of 24 Crypto maps that is configured is exceeded, then the subsequent new Crypto map (whether configured or not) is served by IPSec managers present in the Demux DPC2 cards.
- If any of the Crypto maps with CLI that are served by IPSec managers in Demux is removed and then any new or same map is added with CLI again, it will serve the IPSec manager in Demux.
- When the context is removed, IPSec managers are also removed. This creates room for new crypto maps with CLI and IPSec managers with the limit of 24 maps and 3 IPSec managers on demux card.
- Only one IPSec manager is spawned in each core of the Demux Card, due to this maximum of three IPSec manager are spawned in Demux DPC2 card.
- Each IPSec manager running on Demux card serve as a maximum of eight active Crypto maps.
- Demux on MIO card is not supported.
- To spawn IPSec managers on Demux, **ipsec-on-demux** must be configured before associating it with the interface.
- Every new context spawns new IPSec manager if a new Crypto Map is added under it. If there are 3 contexts, then individual contexts must not have more than 8 Crypto maps to utilize optimum resources. If an individual context have more than 8 Crypto maps then not all the 24 Crypto maps will serve by IPSec managers running on Demux card.
- IKEv1 and IKEv2 spawn IPSec managers independently, IPSec managers share the same resources if it is used in combination. Therefore it is recommended to use either IKEv1 or IKEv2 for Demux card.

- The CLI is visible in DPC1 platform, but it is not be supported.
- Because each Crypto group spawns two IPSec managers as peers are different in primary and secondary IKEv1 maps, only 8 sets of Crypto groups are allowed.
- Not more than eight Crypto maps can be used with same SRC and DST IP address, as they are served by the same IPSec manager and each IPSec manager on demux has limitation of 8 Crypto maps.

# Configuring IPSec Manager Support on Demux DPC2 cards

This section provides information on the CLI commands to configure IPSec Manager on Demux of DPC2.

## Enabling IPSec Manager Spawning

Use the following configuration to enable spawning of IPSec manager for a Crypto map on the Demux Card.

**Important** It is mandatory to configure **require demux processing-card** and **require session recovery** commands before configuring **ipsec-on-demux**command.

```
configure
   context context_name
      crypto map  policy_name ipsec-ikev1
         ipsec-on-demux
         end
```

**NOTES:**

- **no**: Disables the spawning of IPSec manager for Crypto map on Demux Card.

  **Important** If the configuration is removed using **no ipsec-on-demux** option, then this Crypto map must be removed and added again for this configuration to work.

- **ipsec-on-demux**: Enables the spawning of IPSec manager for a Crypto map on Demux Card.

# Monitoring and Troubleshooting

This section provides information regarding show commands available to monitor and troubleshoot the IPSec Manager Support on Demux DPC2 cards.

## Show Commands and Outputs

### show crypto managers *ipsec_manager_instance*

The output of this command includes the "Demux Card" field.

CHAPTER 10

# MAC Algorithm Configuration

## Feature Summary and Revision History

### Summary Data

| | |
|---|---|
| Applicable Product(s) or Functional Area | All |
| 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 | • *ASR 5500 System Administration Guide*<br>• *Command Line Interface Reference*<br>• *VPC-DI System Administration Guide*<br>• *VPC-SI System Administration Guide* |

### Revision History

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

| Revision Details | Release |
|---|---|
| First introduced. | 21.13 |

# Feature Description

The MAC Algorithm Configuration feature allows to configure or change the priority of MAC algorithms of internal SSHD servers.

A new CLI **MACs** CLI command is introduced in SSH Configuration Mode in support of this feature.

# Configuring MAC Algorithms

This section describes how to configure the MAC alogrithims.

Use the following configuration to specify the priority of the MAC algorithms.

```
configure
  context context_name
    server sshd
      macs algorithms
      end
```

```
default macs
```

**NOTES**:

- *algorithms*: Refers to a string of 1 through 511 alphanumeric characters that specifies the algorithms to be used as a single string of comma-separated variables (no spaces) in priority order (left to right) from those listed as follows:
  - HMAC = hash-based message authentication code
  - SHA2 = Secure Hash Algorithm 2
  - SHA1 = Secure Hash Algorithm 1
  - ETM = Encrypt-Then-MAC
  - UMAC = message authentication code based on universal hashing
- The help string and list of algorithms in a Normal build are:

  ```
  hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha2-512,
  hmac-sha2-256,hmac-sha1,umac-128-etm@openssh.com,umac-128@openssh.com,umac-64-etm@openssh.com,umac-64@openssh.com
  ```

- The help string and list of algorithms in a Trusted build are:

  ```
  hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha2-512,
  hmac-sha2-256,hmac-sha1
  ```

- The default value string is:

  ```
  hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha2-512,
  hmac-sha2-256,hmac-sha1
  ```

CHAPTER 11

# NB-IOT EDRX Supported values in ATTACH/TAU Accept

This chapter describes the following topics:

## 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 |
| Default Setting | Enabled - Configuration Required |
| Related Changes in This Release | Not Applicable |
| Related Documentation | *MME Administration Guide* |

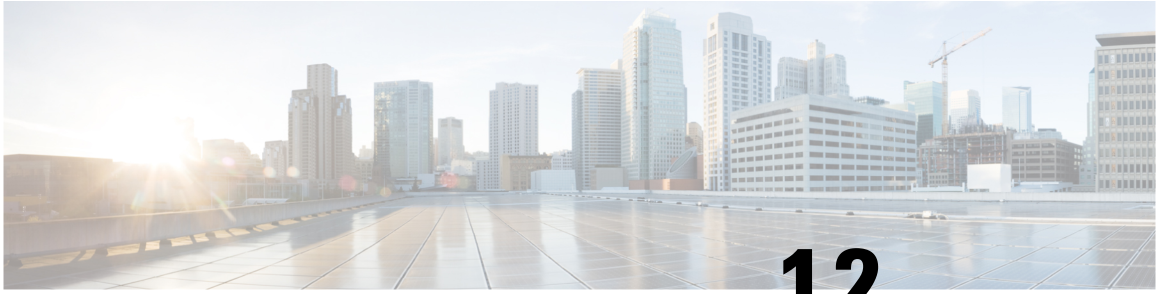
### Revision History

| **Revision Details** | **Release** |
|---|---|
| NB-IOT EDRX Supported values in ATTACH/TAU Accept is Introduced to 21.12 release. | 21.12.11 |
| NB-IOT EDRX Supported values in ATTACH/TAU Accept is Introduced to 21.13 release. | 21.13.11 |
| First introduced. | 21.14 |

# Feature Changes

**Previous Behavior:** UE requests the EDRX value in the Extended DRX parameters IE in the Attach-Request or in the TAU-Request. In the Attach-Accept or in the TAU-Accepts, the requested value is sent.

**New Behavior:** For the NBIOT device, If the Extended DRX parameter values are 4, 6, 7 or 8, it is interpreted as 2 and sent in the Attach-Accept or in the TAU Accept.



CHAPTER 12

# Network Access Identifier Field Removal from MSISDN

## 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 | Not Applicable |

### Revision History

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

| Revision Details | Release |
|---|---|
| The change in behavior is also applicable to this release. | 21.12.12 |
| With this release, the P-GW does not add an extra character "19", that is Network Access Identifier (NAI) field in MSISDN, which is sent in Protocol Configuration Option (PCO) IE in CSRsp message. | 21.13 |

| Revision Details | Release |
|---|---|
| First introduced. | Pre 21.2 |

# Feature Changes

**Previous Behavior**: When MSISDN was sent in PCO in Create Session Response (CSRsp), the P-GW added an extra character "19" in MSISDN that was present in PCO.

**New Behavior**: While sending MSISDN in PCO in CSRsp, the P-GW does not send NAI, that is to say, the extra character "19".

**Customer Impact**: None

CHAPTER 13

# New Attribute in P-GW CDR for Custom GTPP Dictionary

## 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 (for customer-specific GTPP dictionary) |
| Related Changes in This Release | Not Applicable |
| Related Documentation | Not Applicable |

### Revision History

| Revision Details | Release |
|---|---|
| In this release, new 5G NSA attributes are included in customer-specific P-GW GTPP dictionary. | 21.13.2 |
| First introduced. | Pre 21.2 |

# Feature Changes

To support 5G NSA NR usage reporting functionality, Cisco has introduced additional containers for secondary RAT usage reports in P-GW CDR for a customer-specific GTPP dictionary.

**Important** This feature is customer-specific, requiring a custom GTPP dictionary. For more information, contact your Cisco Account representative.

The following fields are now included in P-GW CDR for a custom GTPP dictionary.

| Field | Tag Number | Category | Description | Format | Size (in bytes) | ASN1 Code |
|---|---|---|---|---|---|---|
| List of RAN Secondary RAT Usage Reports | 73 | OC | This field includes one or more containers reported from the RAN for a secondary RAT. | Sequence of RAN Secondary RAT Usage Report | Variable | 0xbf49 |
| RAN Secondary RAT Usage Report | 73-0 | M | This field includes one or more containers reported from the RAN for a secondary RAT. | Sequence | Variable | 0x30 |
| Data Volume Uplink | 73-0-1 | M | This field includes the number of octets transmitted during the use of the packet data services in the uplink direction reported from RAN. The counting and reporting from RAN of uplink data volumes is optional. | Unsigned Integer | 9 | 0x81 |
| Data Volume Downlink | 73-0-2 | M | This field includes the number of octets transmitted during the use of the packet data services in the downlink direction reported from RAN. The counting and reporting from RAN of downlink data volumes is optional. | Unsigned Integer | 9 | 0x82 |
| RAN Start Time | 73-0-3 | M | This field is a time stamp, which defines the moment when the volume container is opened by the RAN. | Timestamp | 9 | 0x83 |
| RAN End Time | 73-0-4 | M | This field is a time stamp, which defines the moment when the volume container is closed by the RAN. | Timestamp | 9 | 0x84 |

CHAPTER 14

# Paging eDRX H-SFN Changed to 10 Bits Counter

## 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 | This feature is enabled/disabled, when the eDRX feature is enabled/disabled. |
| Related Changes in This Release | Not applicable |
| Related Documentation | *MME Administration Guide* |

### Revision History

| **Revision Details** | **Release** |
|---|---|
| Paging eDRX H-SFN changed to 10 bits counter introduced in release 21.13. | 21.13.11 |
| Paging eDRX H-SFN changed to 10 bits counter introduced in release 21.11. | 21.11.3 |
| Paging eDRX H-SFN changed to 10 bits counter introduced in release 21.12. | 21.12.5 |
| First introduced. | 21.0 |

# Feature Changes

**Previous Behavior**: Paging eDRX H-SFN is 32 bits counter.

**New Behavior**: Paging eDRX H-SFN changed to 10 bits counter to allow values between 0 to 1023 as per 3GPP TS 36.331 V13.13.0.

**Customer Impact**: Customer can see the change in the paging timings.

CHAPTER 15

# Password Generation Support

## Feature Summary and Revision History

### Summary Data

| | |
|---|---|
| Applicable Product(s) or Functional Area | All |
| Applicable Platform(s) | • ASR 5500<br>• VPC-DI<br>• VPC-SI |
| Default Setting | Enabled - Always-on |
| Related Changes in This Release | Not Applicable |
| Related Documentation | *Command Line Interface Reference* |

### Revision History

| **Revision Details** | **Release** |
|---|---|
| With this release, the user can select an auto-generated random password or specify a password of choice. These options are provided when the user password expires or is found weak. | 21.13 |
| First introduced. | Pre 21.2 |

# Feature Changes

In the current deployment of StarOS, when the user password expires or is found weak, the local or context user must enter a new password. This is the only option available.

**Previous Behavior**: In releases earlier to 21.13, for local and context users, when a user password expires or is found weak, at the next login attempt, the user was presented with an option to enter a new password and reconfirm it.

**New Behavior**: In this release, a new auto-generation of password functionality is added.

- **For Local Users**: When a user password expires or is found weak, an option is provided to the user to select an auto-generated, random password. If accepted, the user is expected to use the auto-generated password at the next login. If rejected, the user is presented with an option to enter their own password of choice.

  **Note** This auto-generated random password is also presented when the user tries to change the password using the **password change** CLI command in EXEC Mode after login.

- **For Context Users**: When a user password is found weak, an option is provided to the user to select an auto-generated, random password. If accepted, the user is expected to use the auto-generated password at the next login. If rejected, the user is presented with an option to enter their own password of choice.

This auto-generation of password functionality can be enabled or disabled. This functionality is supported with the new **auto-generate [ none | length** *password-length***]** keyword, which is added to the **local-user password** CLI command in Global Configuration Mode and to the **password** CLI command in Context Configuration Mode. When the functionality is enabled, the auto-generated random password length can be configured.

**Customer Impact**:

The user can now select auto-generated random password or specify a password of choice at login.

# Command Changes

## local-user password

Use the following configuration to configure an automatically generated password at login when password has expired or is found weak.

```
configure
   local-user password auto-generate length password_length
   end
```

```
default local-user password auto-generate
```

**NOTES**:

- **[ auto-generate [ none | length** *password-length***]**: Presents an option to automatically generate a password at login when password is expired or found weak.

  **none**: Specifies that the user must not be presented with the option to automatically generate a password.

  **length** *password-length*: Specifies the length of the automatically-generated password for the user. The length of the automatically-generated password must be an integer between 6 to 127.

- **default**: This CLI is enabled by default with the password length of 8.

# password

Use the following configuration to configure an automatically generated password at login when the password is found weak.

```
configure
  context context_name
    password auto-generate length password_length
    end
```

```
default password auto-generate
```

**NOTES**:

- **auto-generate [ none | length** *password-length***]**: Presents an option to automatically generate a password at login when password is found weak.

  **none**: Specifies that the user must not be presented with the option to automatically generate a password.

  **length** *password-length*: Specifies the length of the automatically-generated password for the user. The length of the automatically-generated password must be an integer between 6 to 127.

- **default**: This CLI is enabled by default with the password length of 8.

CHAPTER 16

# PRA and Multi PRA Support

## 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 (for a customer-specific Gx dictionary) |
| Related Changes in This Release | Not Applicable |
| Related Documentation | Not Applicable |

### Revision History

| Revision Details | Release |
|---|---|
| With this release, support is added for PRA and MPRA features to report an Event-Trigger. | 21.13.15 |
| First introduced. | 21.9 |

# Feature Changes

**Important** This change in behavior is applicable to a customer-specific Gx dictionary. Contact your Cisco Account representative for more information.

**Previous Behavior**: A customer-specific Gx dictionary did not support Presence Reporting Area (PRA) and Multiple PRA (MPRA) features to report an Event-Trigger, which is CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT (48).

**New Behavior**: The customer-specific Gx dictionary supports Presence Reporting Area (PRA) and Multiple PRA (MPRA) features to report an Event-Trigger, which is CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT (48).

**Customer Impact**: CCR-U for CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT is reported to the PCRF when the same is enabled from PCRF in CCA/RAR, and respective supported feature is negotiated during initial CCR-I/CCA-I negotiation.

CHAPTER 17

# Random Number Generator Support for OS and Platforms

## Feature Summary and Revision History

### Summary Data

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

### Revision History

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

| Revision Details | Release |
|---|---|
| First introduced. | 21.13 |

# Feature Description

A few of the features deployed on the ASR 5500 and VPC platforms require random numbers for performing certain tasks. While it uses the kernel random number generator for these tasks, the numbers generated may or may not be sufficiently random as per the security standards. However, hardware or host-provided random numbers are considered reliable and meet security standards.

The Random Number Generator Support for OS and Platforms feature addresses this security compliance requirement. It enables the system administrator to configure hardware random number generator (HWRNG) on their host machines.

When configured, the system uses the the hardware random number generators.

**Note** This feature works only when HWRNG support is available on the host.

When HWRNG support is available, add the following configuration to the `libvirt xml` file on the host. This adds `virtio_rng` support to the client (StarOS).

```
<rng model='virtio'>
      <backend model='random'>/dev/random</backend>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x07' function='0x0'/>
</rng>
```

**Note** If there is a conflict in using slot number 7 (as shown in the preceding configuration) in the configuration, use the next available slot.

This configuration must be applied on the supported platforms based on the respective deployment configurations.

No configuration changes are required on the client. The client (StarOS) picks up `virtio_rng` automatically if the support is enabled on the host.

CHAPTER 18

# S-GW CDR Support for Non-IP PDN Subscribers

## Feature Summary and Revision History

### Summary Data

| | |
|---|---|
| Applicable Product(s) or Functional Area | • C-SGN<br>• S-GW |
| Applicable Platform(s) | • ASR 5500<br>• UGP<br>• VPC-DI<br>• VPC-SI |
| Default Setting | Enabled - Always-on |
| Related Changes in This Release | Not Applicable |
| Related Documentation | • *GTPP Interface Administration and Reference*<br>• *Ultra IoT C-SGN Administration Guide* |

### Revision History

| **Revision Details** | **Release** |
|---|---|
| With this release, S-GW CDR support is added for Non-IP PDN subscribers. | 21.13 |
| First introduced. | 21.3 |

# Feature Changes

A new PDP Type, Non-IP, is introduced along with the existing IPv4, IPv6, and IPv4v6 in S-GW CDR. The Volume traffic fields are also updated for Non-IP PDN subscribers.

**Previous Behavior**: The PDP Type field supported values that were IPv4, IPv6, or IPv4v6.

**New Behavior**: The PDP Type field supports Non-IP, in addition to IPv4, IPv6, or IPv4v6, value.

**Customer Impact**: Helps to charge Non-IP PDN subscribers.

CHAPTER 19

# Target MME Load Balancing During Handover

## 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 |
| Default Setting | Enabled - Always on |
| Related Changes in This Release | Not Applicable |
| Related Documentation | *MME Administration Guide* |

### Revision History

| **Revision Details** | **Release** |
|---|---|
| With this release, this feature is fully qualified. | 21.13 |
| First introduced.<br>**Important** Target MME Load Balancing During Handover feature is not fully qualified in this release. It is available only for testing purposes. | 21.12.2 |

# Feature Description

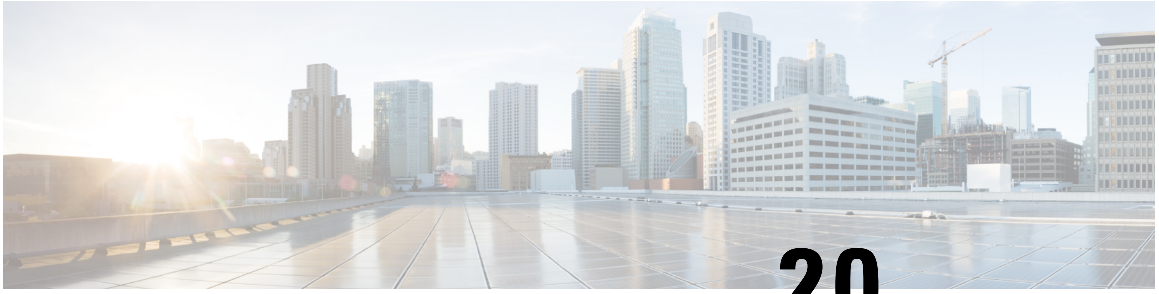
MME can now configure multiple MME addresses for the same Tracking Area Identity (TAI) with the same priority. During the S1 handover procedure, MME selects the target MME based on the static configuration. If more than one MME is configured for the same TAI and priority then the round robin logic of selecting MMEs is used.

With this release, the limitation in configuring multiple MME addresses for the same TAI and priority is removed.

Consider an example where target MMEs with ip-address1, ip-address2 and ip-address3 are configured for the same TAI and priority. For the first handover to target TAI, the MME with address1 is used, for the second handover the MME address2 is used, and for the third handover the MME address3 is used. This sequence is repeated upon successive handovers to the same TAI.

```
peer-mme tai-match  priority <val> mcc <val> mnc <val> tac <val> address <ip-address1>
peer-mme tai-match  priority <val> mcc <val> mnc <val> tac <val> address <ip-address2>
peer-mme tai-match  priority <val> mcc <val> mnc <val> tac <val> address <ip-address3>
```

**Note** Each Session Manager independently load balances between the target MMEs.



CHAPTER 20

# Tethering Block for Downlink Packets

## 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 | • *Command Line Interface Reference*<br>• *ECS Administration Guide* |

### Revision History

| **Revision Details** | **Release** |
|---|---|
| First introduced. | 21.13.2 |

# Feature Description

Tethered devices can connect, browse, and download from the internet although the devices are not charged for it. This feature allows rewriting of TTL/Hop-limit as "1" on all downlink packets for the particular subscriber. By doing this, all the downlink packets are consumed at the UE-level. The downlink packets are not forwarded to the next-hop/Tethered devices since the TTL/Hop-limit is "1", and the UE decrements it by "1", resulting in TTL as "0". As a result, tethered devices will not be able to download and/or browse unless they are subscribed for this.

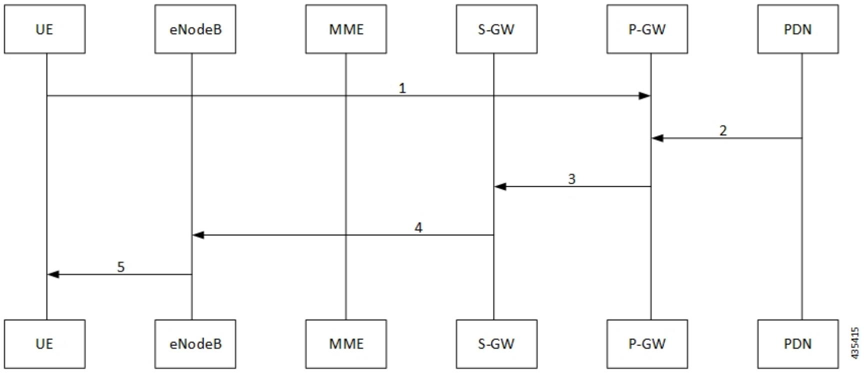
# How It Works

This feature is CLI-controlled wherein TTL/Hop-limit value can be configured under ACS Rulebase configuration mode, and the feature is enabled for all the subscribers under this rule base. As per the configured CLI value, the TTL is rewritten in all the downlink packets under that rule-base, irrespective of service and access technology.

The feature supports Flow Aware Packet Acceleration (FAPA), fragmentation, and buffering.

## Call Flows

The following call flow provides the details for setting TTL as "1" in the IP header.



| Step | Description |
|---|---|
| 1 | UE Attach Procedure and Session establishment on all the EPC Nodes (UE, eNodeB, MME, S-GW, and P-GW). |
| 2 | Downlink traffic is sent for the UE from the PDN. |
| 3 | On receiving the data from the PDN, the P-GW rewrites the TTL/Hop-limit of the IP header with the configured “TTL value” of the “rulebase” profile present in the “active-charging”. |
| 4 | S-GW forwards data toward the UE through eNodeB. |
| 5 | The UE receives the data (downlink packets with TTL=1) from the eNodeB. |

# Configuring the Tethering Block for Downlink Packets Feature

This section describes how to configure the Tethering Block for Downlink Packets feature.

## Enabling Tethering Block for Downlink Packets

Use the following CLI commands to rewrite the TTL/Hop-limit value in the IP header downlink packets.

```
configure
   active-charging service service_name
      rulebase rulebase_name
         ip ttl ttl_value downlink
         end
```

**NOTES**:

- **ip**: Specifies the IP related to a user session.
- **ttl** *ttl_value*: Rewrites the TTL value for an IP packet. The *ttl_value* specifies the value to be configured.
- **downlink**: Modifies the IP header TTL on downlink packets.
- If previously configured, use the **no ip ttl** CLI command to disable the feature.
- By default, the CLI is disabled.

# Monitoring and Troubleshooting the Tethering Block for Downlink Packet Feature

This section provides the CLI commands available to monitor and troubleshoot the feature.

## Show Commands

### show active-charging rulebase name <rulebase_name>

The output of this show CLI command has been modified to display whether the feature is enabled or disabled along with the configured TTL value.

- Tethering Block Feature
  - TTL Value

### show active-charging rulebase statistics name <rulebase_name>

The output of this show CLI command has been modified to display the number of downlink packets which are modified by rewriting TTL/Hop-limit as per the CLI-configured value.

- Tethering Blocking Statistics

- TTL Modified downlink packets