Cisco Ultra Cloud Serving Gateway Control Plane Function, Release 2021.02 - Configuration and Administration Guide

First Published: 2021-06-06

Last Modified: 2021-11-12

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

About this Guide

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

This preface describes the *Ultra Cloud Core Serving Gateway Control Plane Function - Configuration and Administration Guide*, the document conventions, and the customer support details.

Conventions Used

The following tables describe the conventions used throughout this documentation.

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

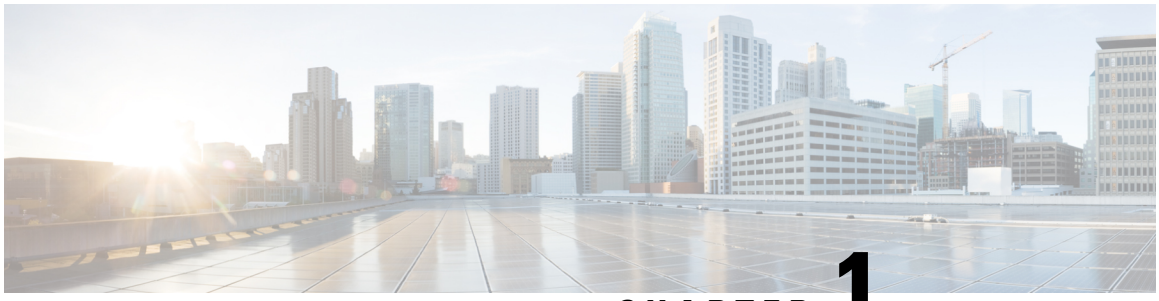
Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`

Typeface Conventions	Description
Text represented as **commands**	This typeface represents commands that you enter, for example: **show ip access-list** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **command** *variable*	This typeface represents a variable that is part of a command, for example: **show card** *slot_number* *slot_number* is a variable representing the applicable chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**

Contacting Customer Support

Use the information in this section to contact customer support.

Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password are required to access this site. Please contact your Cisco sales or service representative for additional information.



CHAPTER 1

5G Architecture

Overview

The Ultra Cloud Core is Cisco's solution supporting 3GPP's standards for 5G new radio (NR) standalone (SA) mode. These standards define various network functions (NFs) based on the separation of control plane (CP) and user plane (UP) (for example CUPS) functionality for increased network performance and capabilities.

Control Plane Network Functions

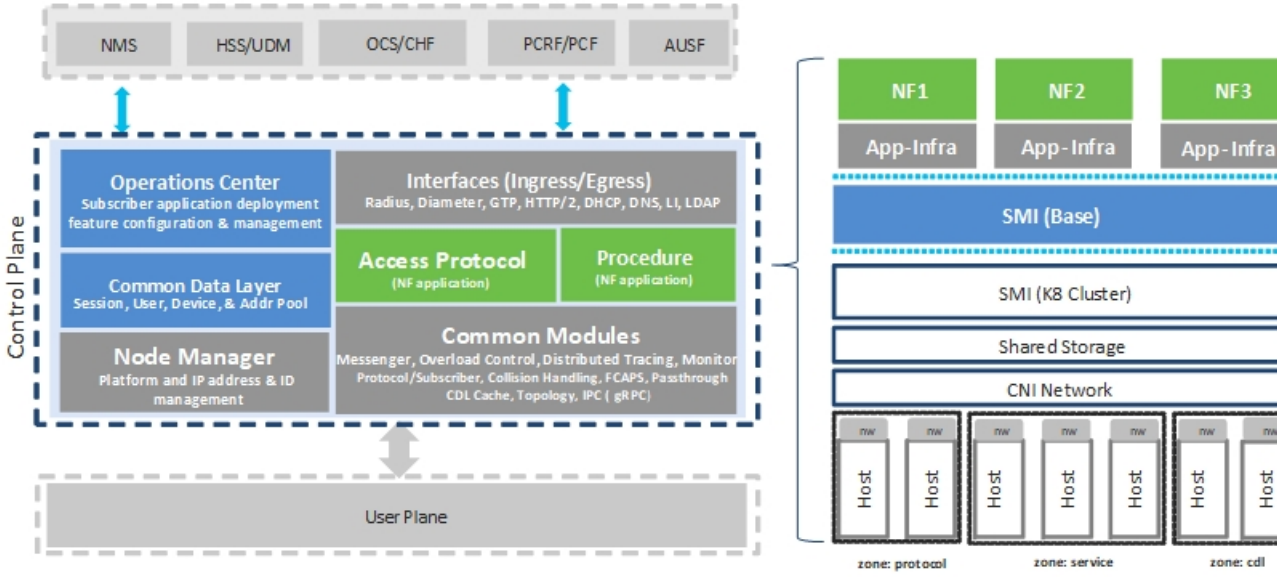
The CP-related NFs that comprise the Ultra Cloud Core are based on a common architecture that is designed around the following tenants:

- Cloud-scale—Fully virtualized for simplicity, speed, and flexibility.
- Automation and orchestration—Optimized operations, service creation, and infrastructure.
- Security—Multiple layers of security across the deployment stack from the infrastructure through the NF applications.
- API exposure—Open and extensive for greater visibility, control, and service enablement.
- Access agnostic—Support for heterogeneous network types (for example 5G, 4G, 3G, Wi-Fi, and so on).

These control plane NFs are each designed as containerized applications (for example microservices) for deployment through the Subscriber Microservices Infrastructure (SMI).

The SMI defines the common application layers for functional aspects of the NF such as life-cycle management (LCM), operations and management (OAM), and packaging.

Figure 1: Ultra Cloud Core CP Architectural Components



User Plane Network Function

The 5G UP NF within the Ultra Cloud Core is the User Plane Function (UPF). Unlike the CP-related NFs, the 5G UPF leverages the same Vector Packet Processing (VPP) technology currently in use by the user plane component within Cisco 4G CUPS architecture. This commonality ensures the delivery of a consistent set of capabilities between 4G and 5G such as:

- Ultrafast packet forwarding.
- Extensive integrated IP Services such as Subscriber Firewall, Tethering, Deep-Packet Inspection (DPI), Internet Content Adaption Protocol (ICAP), Application Detection and Control (ADC), and header enrichment (HE).
- Integrated third-party applications for traffic and TCP optimization.

Subscriber Microservices Infrastructure Architecture

The Ultra Cloud Core (UCC) Subscriber Microservices Infrastructure (SMI) is a layered stack of cloud technologies that enable the rapid deployment of, and seamless life-cycle operations for microservices-based applications.

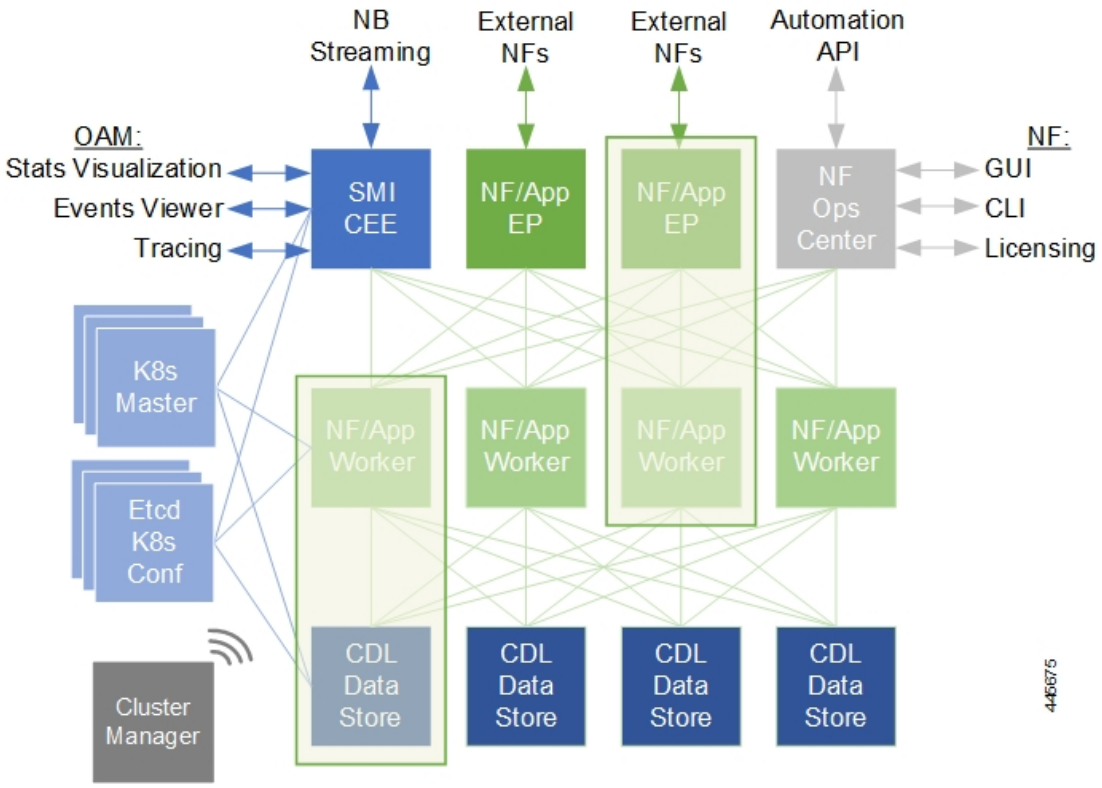
The SMI stack consists of the following:

- SMI Cluster Manager—Creates the Kubernetes (K8s) cluster, creates the software repository, and provides ongoing LCM for the cluster including deployment, upgrades, and expansion.

- Kubernetes Management—Includes the K8s primary and etcd functions, which provide LCM for the NF applications that are deployed in the cluster. This component also provides cluster health monitoring and resources scheduling.
- Common Execution Environment (CEE)—Provides common utilities and OAM functionalities for Cisco Cloud native NFs and applications, including licensing and entitlement functions, configuration management, telemetry and alarm visualization, logging management, and troubleshooting utilities. Also, it provides consistent interaction and experience for all customer touch points and integration points in relation to these tools and deployed applications.
- Common Data Layer (CDL)—Provides a high performance, low latency, stateful data store, designed specifically for 5G and subscriber applications. This next generation data store offers high availability in local or geo-redundant deployments.
- Service Mesh—Provides sophisticated message routing between application containers, enabling managed interconnectivity, extra security, and the ability to deploy new code and new configurations in low risk manner.
- NB Streaming—Provides Northbound Data Streaming service for billing and charging systems.
- NF or Application Worker Nodes—The containers that comprise an NF application pod.
- NF or Application Endpoints (EPs)—The NFs or applications and their interfaces to other entities on the network
- Application Programming Interfaces (APIs)—Provides various APIs for deployment, configuration, and management automation.

The following figure depicts how these components interconnect to comprise a microservice-based NF or application.

Figure 2: SMI Components



For more information on SMI components, see Ultra Cloud Core Subscriber Microservices Infrastructure and the related-documentation at *Deployment Guide* > *Overview* chapter.

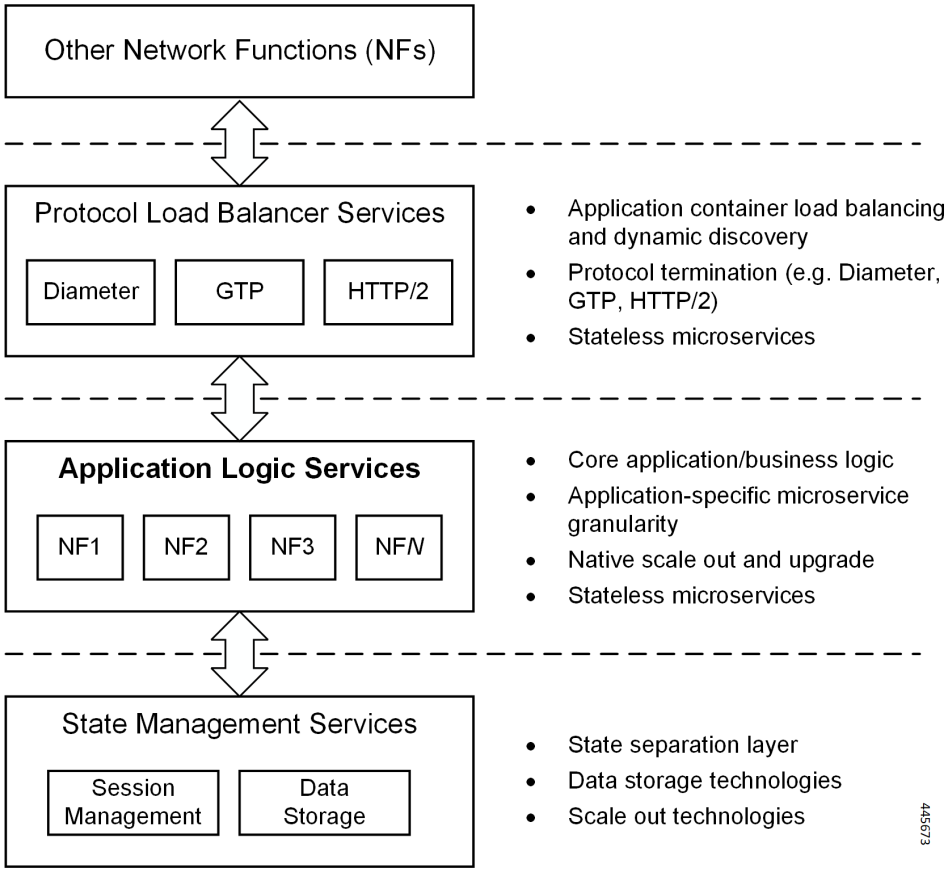
Control Plane Network Function Architecture

Control plane (CP) NFs are designed around a three-tiered architecture that take advantage of the stateful or stateless capabilities that are afforded within cloud native environments.

The architectural tiers are as follows:

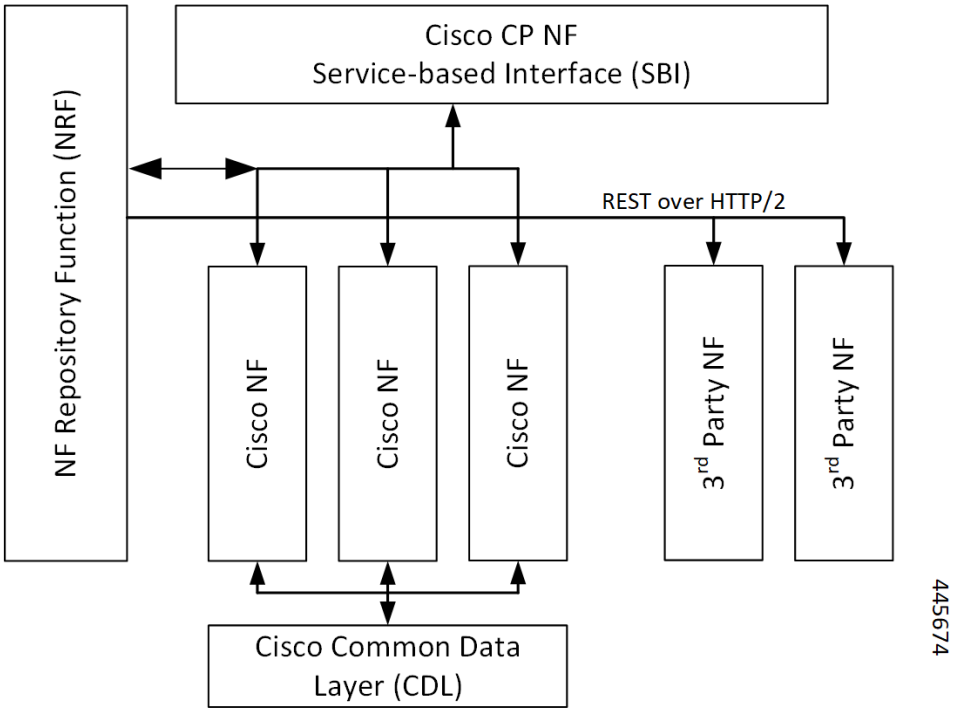
- Protocol Load Balancer Services—These are stateless microservices that are primarily responsible for dynamic discovery of application containers as well as for protocol proxy and termination. These include traditional 3GPP protocols and new protocols that are introduced with 5G.
- Applications Services—Responsible for implementing the core application or business logic, these are the stateless services that render the actual application based on the received information. This layer may contain varying degrees of microservice granularity. Application services are stateless.
- State management services—Enable stateless application services by providing a common data layer (CDL) to store or cache state information (for example session and subscriber data). This layer supports various data storage technologies from in-memory caches to full-fledge databases.

Figure 3: Control Plan Network Function Tiered Architecture

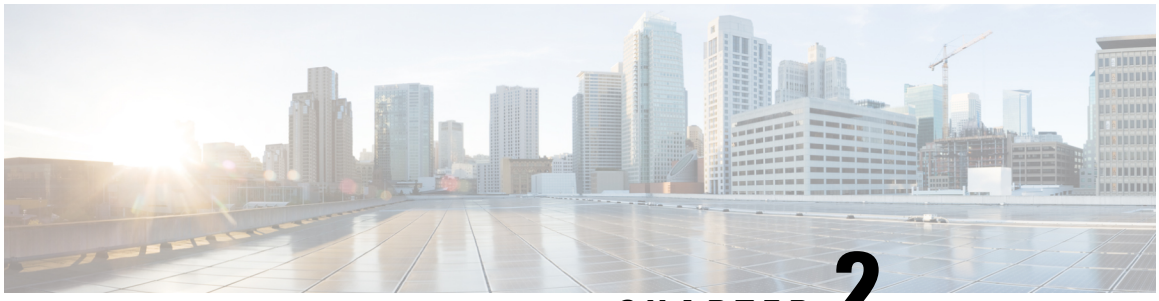


The three-tiered architecture on which Cisco CP NFs are designed fully support the 5G core (5GC) Service-based Architecture (SBA) defined by 3GPP. These NFs communicate with each other and with third-party NFs over the Service-based Interface (SBI) using HTTP/2 over TCP as defined by 3GPP.

Figure 4: Cisco CP NF Service-based Architecture Support



For more information on the Cisco network functions, see their corresponding network function documentation.



CHAPTER 2

cnSGW-C Overview

Product Description

cnSGW-C is a Control Plane Network Function (NF) of the converged core network (4G-5GC). The Serving Gateway Control Plane Function (cnSGW-C) is built on top of the SMI architecture. cnSGW-C acts as a UE anchor and supports mobility procedures, along with session setup and termination procedures, as specified in *3GPP TS 23.401* and *3GPP TS 23.214*.

The Serving Gateway Control Plane Function (cnSGW-C) provides the functionality of the S-GW as defined by *TS 23.401 [2]*, except for the functions that are performed by the SGW-U, as described in *3GPP Spec 23.214 Table 4.3.2-1*. In addition, the cnSGW-C is responsible for selecting the SGW-U (as described in 3*GPP Spec 23.214 clause 4.3.3*) and for controlling the SGW-U with respect to the functions described in *TS 23.214 Table 4.3.2-1*.

With SMF (IWF) support based on Cisco Cloud Native Platform, it is recommended to support cnSGW-C functionality on Cloud Native Platform for better hardware utilization and O&M activities.

Converged Core Overview

The converged core solution provides an advanced, cloud-native, converged control plane with the capability to support 4G and 5G devices, and use cases.

Important This release supports only the cloud-native integrated S-GW and SMF instance with S5C and cnSGW-C functionalities.

The converged core solution removes the operational complexity by providing a unified core network to handle all types of subscribers and use cases.

The operator has the following benefits:

- Improves the overall network efficiency by reducing signaling between cnSGW-C and SMF while handling a 4G subscriber or handoff from 5G to 4G coverage area.
- Reduces latency introduced due to the extra hop SGW-U for a subscriber in 4G coverage area, by collapsing the data path in the Converged UPF, thus improving the overall user experience.
- Provides ability to use a unified subscriber policy and billing infrastructure using SBA interfaces for 4G and 5G devices.

The solution supports the following converged control plane and user plane functions:

- Converged Control Plane Functions
  - Integrates S-GW and SMF network functions as a single deployment, under a single Kubernetes namespace, to support 4G and 5G devices from E-UTRAN/NR (converged core gateway)
  - Supports logical network functions (data)
- Converged User Plane Functions
  - Integrates UPF and SGW-U functionalities as a single network function
  - Provides simultaneous support for N4 and Sxa interfaces
  - Terminates multiple control planes in a single deployment

Use Cases

This section describes the use cases that cnSGW-C supports:

- **cnSGW-C Configuration**

  The cnSGW-C base configuration provides a detailed view of configurations required for the cnSGW-C to be operational. The configuration includes setting up the infrastructure to deploy the cnSGW-C, deploying the cnSGW-C through SMI, and configuring the Ops Center for exploiting the cnSGW-C capabilities over time. For more information on SMI, see the *Ultra Cloud Core SMI Cluster Deployer Operations Guide*.

  The following features are related to this use case:

  - APN Profile Support, on page 95
  - Service Configuration Enhancements, on page 367
  - UPF Selection Support, on page 453

  For Converged Core deployment, cnSGW-C is deployed using Converged Ops Center.

- **Session Management**

  Every UE accessing the EPC is associated with a single S-GW. cnSGW-C supports multiple PDN for given UE. As a part of Session Management, cnSGW-C supports the following:

- Default and dedicated bearer establishment
- Bearer modification
- Bearer deactivation

The following features are related to this use case:

- 3GPP RAN/NAS Cause Codes Support, on page 83
- Change Notification Request Handling, on page 99
- Context Replacement Support, on page 111
- Dedicated Bearer Support, on page 119
- Delete Bearer and Delete Session Request, on page 131
- DSCP Marking for CP Signaling Messages, on page 162
- eMPS/WPS Support, on page 171
- Emergency Call Support, on page 167
- Idle Session Timeout Settings, on page 247
- Initial Attach Support, on page 255
- Multiple PDN Attach or Detach Procedures, on page 357
- Update Bearer Request and Response, on page 447
- VoLTE Call Prioritization, on page 475

- **Support for UE Mobility**

  cnSGW-C is a mobility anchor point for UE. In LTE Network, there can be mobility between eNodeB to eNodeB, with or without MME change. UE can also move from one cnSGW-C to another cnSGW-C with different modes, S1-based Relocation, X2-based Relocation, and 5G-4G interworking.

  The following features are related to this use case:

  - IDFT Support, on page 231
  - Intra-MME and Inter-MME Handover Procedures, on page 269
  - Modify Bearer Request Support, on page 319
  - SGW Relocation Support, on page 423

- **S1-Release/Buffering/Downlink Data Notification**

  cnSGW-C handles releasing S1-U bearer between eNodeB and SGW-U. When cnSGW-C receives Radio Access Bearers (RAB) message indicating that S1-U bearers are released, it updates User Plane and moves UE to IDLE state. When in IDLE state, if UE receives downlink data packet, cnSGW-C generates DDN message towards MME to page UE.

  cnSGW-C also supports DDN Throttling, DDN Delay, and High Priority feature for DDN.

  The following features are related to this use case:

- Access Bearer Release Support, on page 91
- Downlink Data Notification, on page 137
- DDN Advance Features, on page 148

- **Retransmission and Timeout**

  For all procedures, as per *3GPP TS 23.401/29.274*, cnSGW-C supports N3-Retransmission, and T3-Timeout Support. These are supported for S11, S5, and Sx interfaces.

  The following feature is related to this use case:

  - GTPv2 and Sx Messages Retransmission and Timeout Handling, on page 209

- **Failure and Error Handling**

  cnSGW-C supports handling of:

  - Failure response for Create Session Request as part of initial attach procedure and additional PDN setup procedure
  - PGW-initiated Dedicated Bearer Creation (DBC) procedure failure scenario
  - Radio Access Bearers (RAB), Modify Bearer Request and Response (MBR) from PGW and User Plane

  The following feature is related to this use case:

  - Failure and Error Handling Support, on page 181

- **Load/overload Control Functions**

  cnSGW-C supports:

  - Exchange of load/overload control information and actions during peer node overload over Sx interface.
  - Handling load/overload information on GTPv2 interface.

  The following features are related to this use case:

  - GTPv2 Load/Overload Support, on page 215
  - Sx Load/Overload Control Handling, on page 441

- **cnSGW-C Charging Support**

  cnSGW-C supports:

  - Offline Charging (Gz).
  - Writing CDR to local disk storage. The CDR files are pushed to SFTP server periodically.
  - CDR generation for selected subscribers. This is achieved by enabling CDR generation per Operator Policy through call control profile.

  The following feature is related to this use case:

  - SGW Charging Support, on page 375

- **Peer and Path Management for GTPC and Sx**

  cnSGW-C supports:

  - Peer management for MME (S11 peers), PGW (S5 Peers), and User Plane.
  - Peer monitoring through ECHO Request/Response and Heartbeat Request/Response.
  - Handling of path failure events for S11 and S5 peers.

  The following features are related to this use case:

  - GTPC and Sx Path Management, on page 194
  - GTPC Path Failure, on page 199
  - Customization of Path Failure Detection, on page 204
  - Sx Path Failure, on page 202

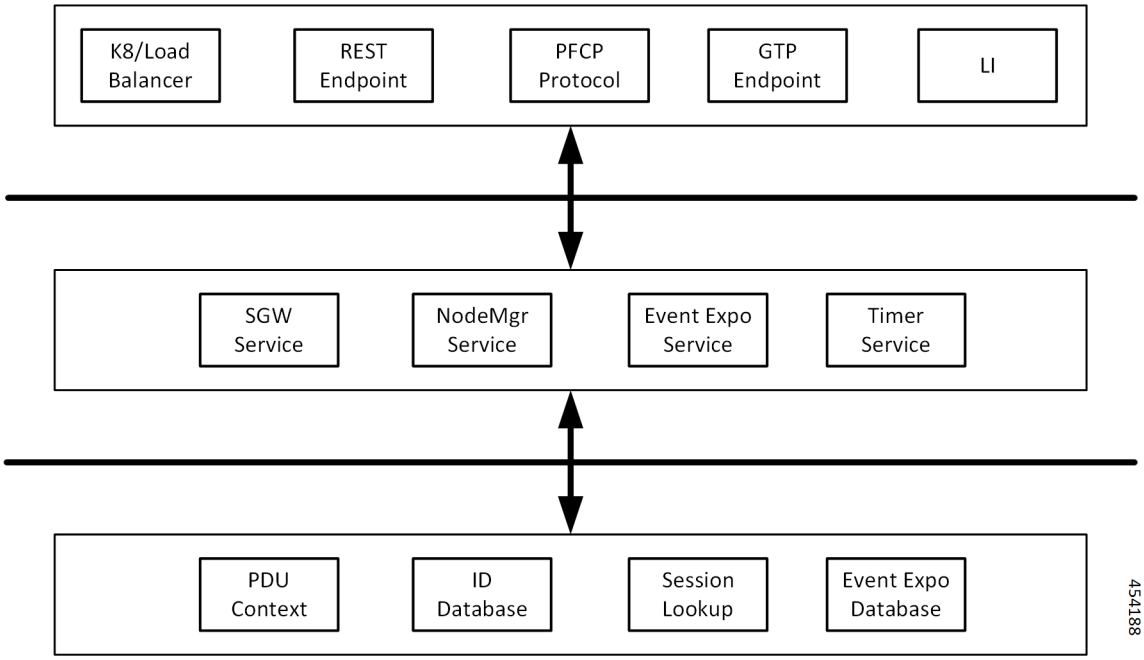
Deployment Architecture and Interfaces

cnSGW-C is a part of the converged core network functions portfolio with a common mobile core platform architecture. The core network functions include Access and Mobility Management Function (AMF), Policy Control Function (PCF), Session Management Function (SMF), and User Plane Function (UPF).

cnSGW-C Architecture

cnSGW-C network function consists of loosely coupled microservices. The microservice decomposition is based on a three-layered architecture, as illustrated in the following figure:

Figure 5: cnSGW-C Architecture



The following are the three layers of the cnSGW-C architecture:

- Layer 1 - Protocol and Load Balancer services (Stateless)
- Layer 2 - Application services (Stateless)
- Layer 3 - Database services (Stateful)

cnSGW-C Deployment

cnSGW-C NF is deployed in a separate namespace as an independent NF.

Figure 6: cnSGW-C Deployment

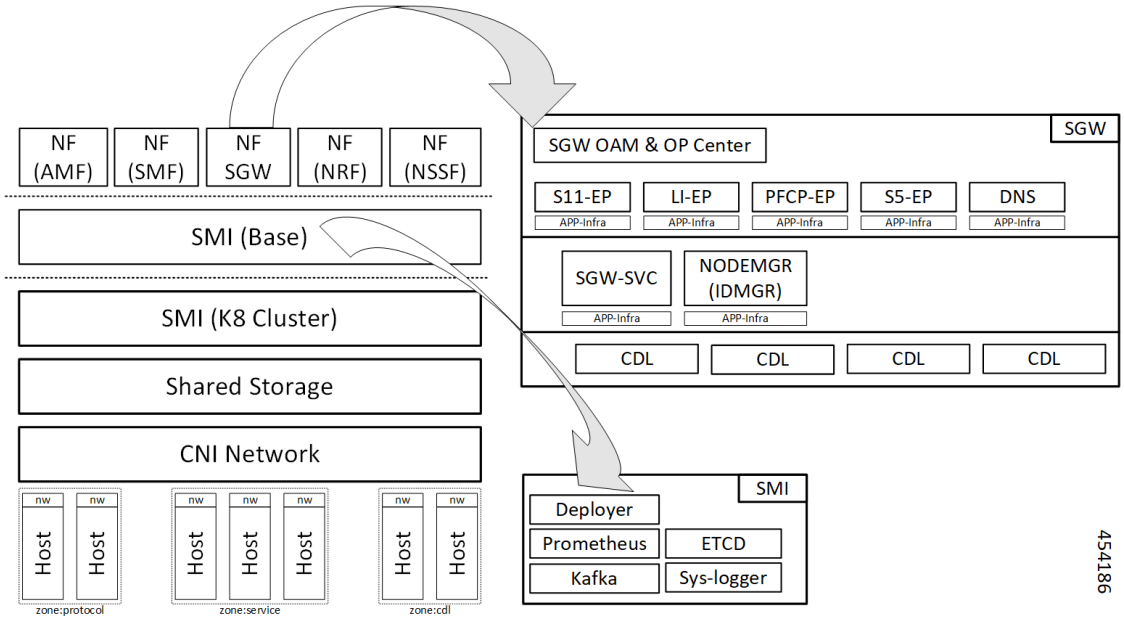
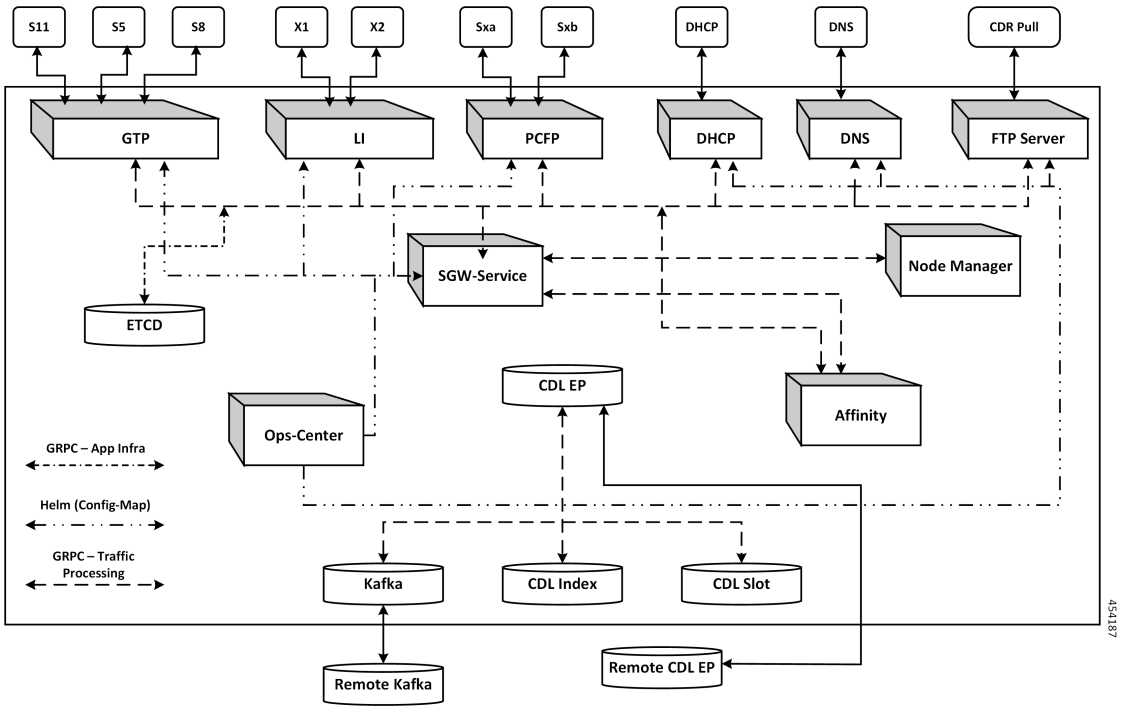


Figure 7: cnSGW-C HELM Chart



Converged Core Architecture

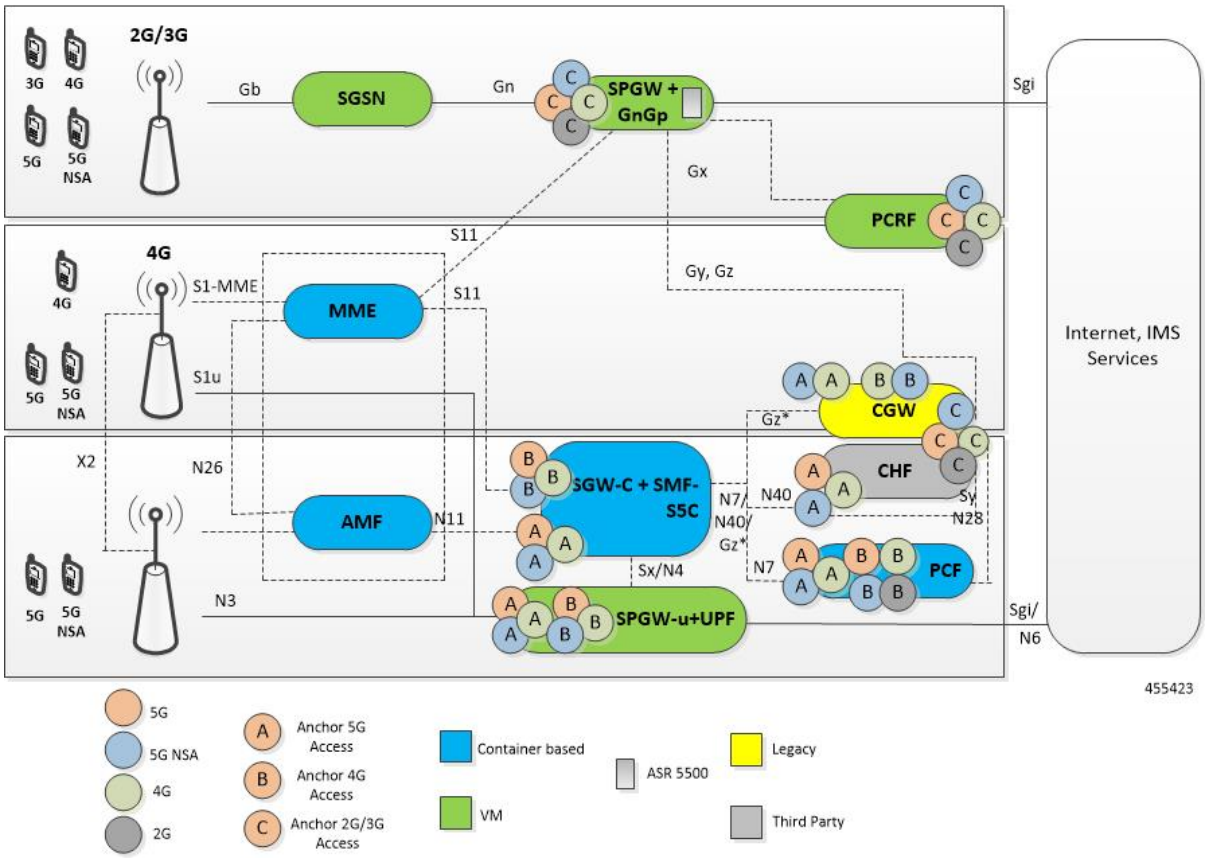
The converged core solution provides a single unified platform which is based on SMI architecture. The supporting architecture integrates the cloud-native S-GW and SMF deployment with 5GC and cnSGW-C functionalities. The solution uses 3GPP-defined SBA interfaces for policy and charging functions.

In the converged core architecture, the 4G and 5G capable UEs are anchored on the same control plane instance. The control plane instance provides the SMF, 5GC, and cnSGW-C functionalities.

The handoffs between 4G and 5G access types are seamless for 5G capable devices. The handoffs from LTE to UTRAN (bi-directional communication between 4G/5G and 3G/2G) are not seamless for 4G capable devices.

The following figure illustrates the supported network architecture.

Figure 8: Converged Core Architecture



The UPF deployed as a part of this solution is a VPC-SI VM. The UPF deployment is VM-based, and supports:

- SGW-U, PGW-U, and UPF functionalities in the same instance, and exposes the Sxa, Sxb, Sxab, or N4 interface towards the control plane.
- Multiple CP instances (up to 4) simultaneously.

Converged Core Deployment

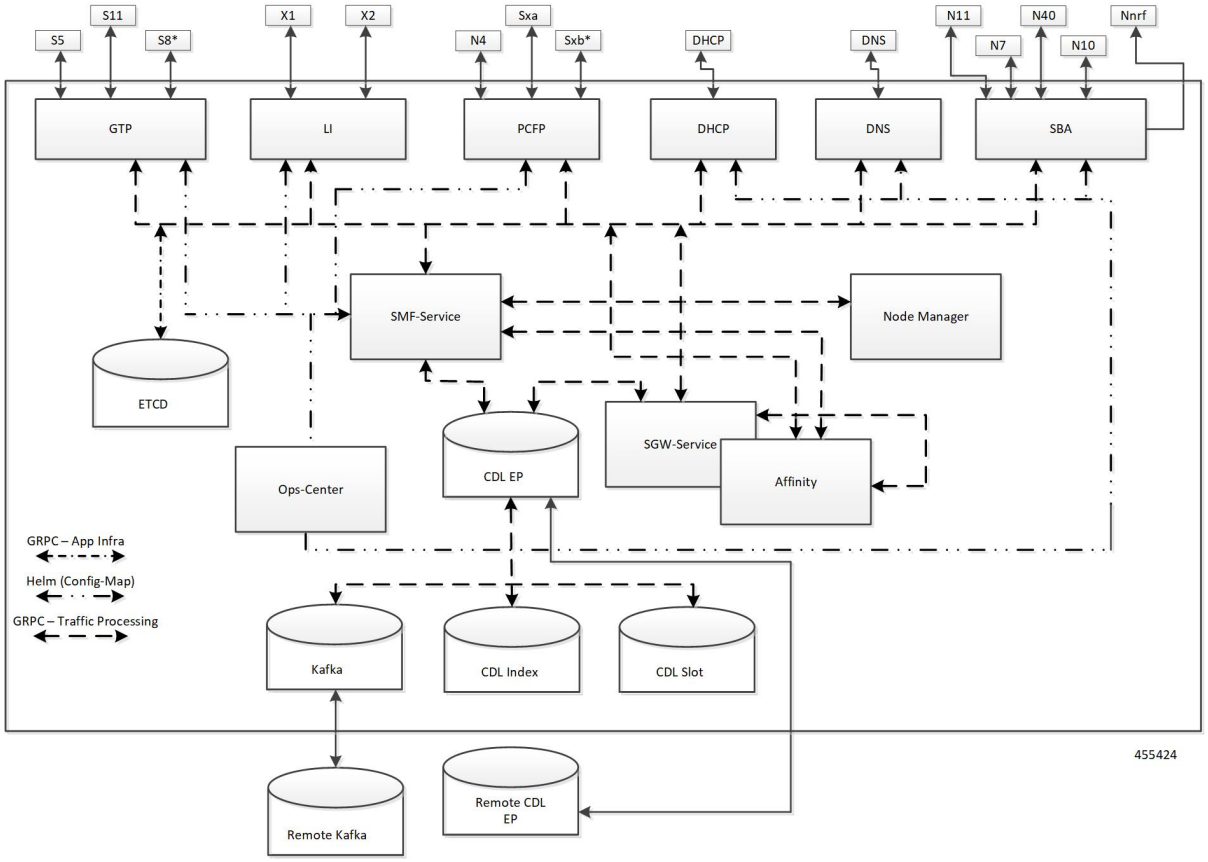
The converged core deployment is based on the converged control plane and unified user plane infrastructure for all use cases.

In the converged core deployment, all 4G and 5G-capable UEs are anchored on the 5G core (SMF) with SBA interfaces towards PCF.

The converged core deployment has a converged Ops Center that allows the configuration of cnSGW-C and SMF services along with other microservices. A single product helm chart is used to install components.

The following figure illustrates the Kubernetes deployment for the converged S-GW and SMF network function.

Figure 9: Kubernetes Deployment



The protocol layer services are shared across SMF and S-GW. The GTP endpoint terminates the S11 interface and S5/S8 interface. Similarly, the PFCP (protocol) endpoint terminates the N4 and Sxa interfaces.

The SMF and S-GW services are deployed as distinct pods and the session processing is segregated. Both the service pods use CDL for storing subscriber sessions.

Supported Interfaces

This section describes the interfaces supported between cnSGW-C and other network functions in the 5GC.

- S11—Reference point between the SGW and the MME
- S5/S8—Reference point between the SGW and the PGW/SMF
- Sxa—Reference point between the SGW-C and the SGW-U
- Gz—Reference point between the SGW-C and the Charging Server

Life Cycle of Data Packet

For information on life cycle of a data packet, see Initial Attach Support, on page 255.

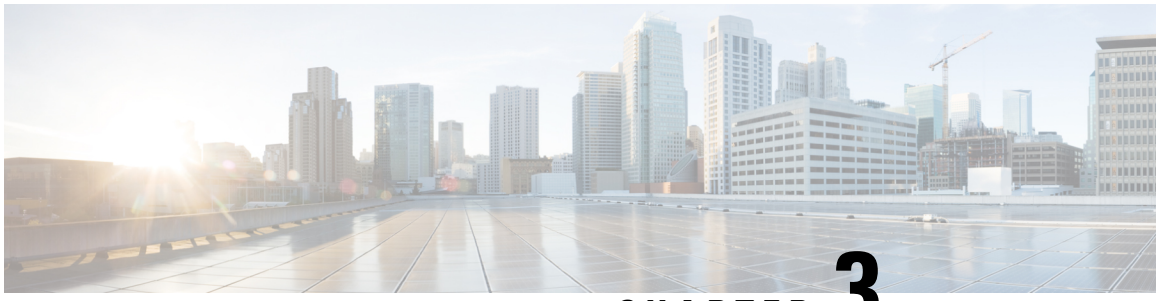
License Information

cnSGW-C supports Cisco Smart Licensing. For more information, see Smart Licensing Support, on page 41.

Standards Compliance

cnSGW-C complies with the following 3GPP standards:

- *3GPP TS 23.401 "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access"*
- *3GPP TS 23.402 "Architecture enhancements for non-3GPP accesses"*
- *3GPP TS 29.274 "Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C);"*
- *3GPP TS 23.214 "Architecture enhancements for control and user plane separation of EPC nodes"*
- *3GPP TS 29.244 "Interface between the Control Plane and the User Plane nodes"*
- *3GPP TS 24.008 "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3"*
- *3GPP TS 23.007 "Restoration procedures"*
- *3GPP TS 22.153 "Multimedia priority service"*
- *3GPP TS 33.107 "3G security; Lawful interception architecture and functions"*



CHAPTER 3

Deploying and Configuring cnSGW-C through Operations Center

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
The following enhancements were introduced: • Multiple entitlement tags • cnSGW-C deployment on bare metal server	2021.02.0

Revision Details	Release
First introduced.	2020.07.0

Feature Description

cnSGW-C deployment process involves deploying cnSGW-C through Subscriber Microservices Infrastructure (SMI) Cluster Deployer. You can perform configurations or customizations through the cnSGW-C Ops Center which is based on the Confd CLI.

cnSGW-C Ops Center

The Ops Center is a system-level infrastructure that provides the following user interface to:

- Trigger the deployment of microservices by providing variable helm chart parameters. These chart parameters control the scale and properties of Kubernetes objects (deployment, pod, services, and so on) associated with the deployment.
- Push application specific configuration to one or more micro-services through Kubernetes configuration maps.
- Issue application-specific execution commands (such as show commands and clear). These commands:
  - Invoke APIs in application-specific pods
  - Display the information returned by the application on the user interface

The following screenshot is a sample of the web-based CLI.

Figure 10: Web-based Ops Center

The cnSGW-C Ops Center allows you to configure the features, such as licensing, cnSGW-C engine, EGPT and PFCP endpoint, and CDL.

Prerequisites

Before deploying cnSGW-C on the SMI layer:

- Ensure that all the virtual network functions (VNFs) are deployed.
- Run the SMI synchronization operation for the cnSGW-C Ops Center and Cloud Native Common Execution Environment (CN-CEE).

cnSGW-C Service Configuration

The cnSGW-C service requires the basic configuration to process Call Setup, Modify, and Delete Request.

Mapping Pods with Node Labels

Prerequisites

- Ensure that the node labels are according to the pod deployment layout.
- Ensure that the external VIPs are according to the requirement of NF.
- Enable Istio for pod to pod traffic load balancing.

Node Labels are key and value pairs that are attached to nodes at cluster synchronization. Each node can have a set of key and value labels defined. Each key must be unique for a node. With labels, users can map their NF pods onto nodes in a loosely coupled manner.

Important

- The pod-level labeling configuration is applicable only when the cnSGW-C is deployed on a bare metal server.
- Ensure to configure the node label on the SMI cluster deployer before mapping the pods. Following is the sample command for master-1 labeling:

```
[cndp-clpnc-cm-cm-primary] SMI Cluster Deployer (config-nodes-master-1)# k8s node-labels
smi.cisco.com/svc-type smf-node
```

To map the pods with node labels, use the following sample configuration:

```
config
   k8 label protocol-layer key label_key value label_value
   k8 label service-layer key label_key value label_value
   k8 label cdl-layer key label_key value label_value
   k8 label oam-layer key label_key value label_value
   end
```

Following is an example configuration of pod to node-label mapping:

```
k8 label protocol-layer key smi.cisco.com/node-type value smf-proto
exit
k8 label service-layer key vm-type value smf-svc
exit
k8 label cdl-layer key smi.cisco.com/node-type value smf-cdl
exit
k8 label oam-layer key smi.cisco.com/node-type value oam
exit
```

Deploying and Accessing cnSGW-C

This section describes how to deploy cnSGW-C and access the cnSGW-C Ops Center.

Deploying cnSGW-C

The Subscriber Microservices Infrastructure (SMI) platform is responsible for deploying and managing the cnSGW-C application and other network functions.

For information on how to deploy cnSGW-C Ops Center on bare metal servers (currently Cisco UCS-C servers) environment, see *Operating the SMI Cluster Manager on Bare Metal* section in the *Ultra Cloud Core Subscriber Microservices Infrastructure — Operations Guide*.

Accessing the cnSGW-C Ops Center

You can connect to the cnSGW-C Ops Center through SSH or the web-based CLI console.

- SSH:

  ssh admin*@ops_center_pod_ip* **-p 2024**

- Web-based console:

  1. Log in to the Kubernetes master node.
  2. Run the following command:

     kubectl get ingress <*namespace*>

     The available ingress connections get listed.
  3. Select the appropriate ingress and access the Ops Center.
  4. Access the following URL from your web browser:

     cli.<*namespace*>**-ops-center**.<*ip_address*>.**nip.io**

By default, the Day 0 configuration is loaded into the cnSGW-C.

Day 0 Configuration

To view the Day 0 configuration, run the following command.

show running-config

The following is a sample Day 0 configuration:

```
system mode shutdown
helm default-repository base-repos
helm repository base-repos
 url https://charts.209.165.201.1.nip.io/ccg.2021.01.0.i60
exit
k8s name          2nd-a18-kub-cluster
k8s namespace     cn-cn3
k8s nf-name       smf
k8s registry      docker.209.165.201.1.nip.io/ccg.2021.01.0.i60
```

```
k8s single-node   false
k8s use-volume-claims false
k8s ingress-host-name 209.165.201.2.nip.io
k8s nodes 2nd-a18-kub-cluster-master-11
 node-type   master
 worker-type master
exit
k8s nodes 2nd-a18-kub-cluster-master-22
 node-type   master
 worker-type master
exit
k8s nodes 2nd-a18-kub-cluster-master-33
 node-type   master
 worker-type master
exit
aaa authentication users user admin
 uid        1117
 gid        1117
 password   $1$XNGJOr.C$iZZvQbNfmPN15qG4GpQa8/
 ssh_keydir /tmp/admin/.ssh
 homedir    /tmp/admin
exit
aaa ios level 0
 prompt "\h> "
exit
aaa ios level 15
 prompt "\h# "
exit
aaa ios privilege exec
 level 0
  command action
  exit
  command autowizard
  exit
  command enable
  exit
  command exit
  exit
  command help
  exit
  command startup
  exit
 exit
 level 15
  command configure
  exit
 exit
exit
nacm write-default deny
nacm groups group LI
 user-name [ liadmin ]
exit
nacm groups group admin
 user-name [ admin ]
exit
nacm rule-list admin
 group [ admin ]
 rule li-deny-tap
  module-name       lawful-intercept
  path              /lawful-intercept
  access-operations *
  action            deny
 exit
 rule li-deny-clear
```

```
  module-name       tailf-mobile-smf
  path              /clear/lawful-intercept
  access-operations *
  action            deny
 exit
 rule any-access
  action permit
 exit
exit
nacm rule-list confd-api-manager
 group [ confd-api-manager ]
 rule any-access
  action permit
 exit
exit
nacm rule-list ops-center-security
 group [ * ]
 rule change-self-password
  module-name       ops-center-security
  path              /smiuser/change-self-password
  access-operations exec
  action            permit
 exit
 rule smiuser
  module-name       ops-center-security
  path              /smiuser
  access-operations exec
  action            deny
 exit
exit
nacm rule-list lawful-intercept
 group [ LI ]
 rule li-accept-tap
  module-name       lawful-intercept
  path              /lawful-intercept
  access-operations *
  action            permit
 exit
 rule li-accept-clear
  module-name       tailf-mobile-smf
  path              /clear/lawful-intercept
  access-operations *
  action            permit
 exit
exit
nacm rule-list any-group
 group [ * ]
 rule li-deny-tap
  module-name       lawful-intercept
  path              /lawful-intercept
  access-operations *
  action            deny
 exit
 rule li-deny-clear
  module-name       tailf-mobile-smf
  path              /clear/lawful-intercept
  access-operations *
  action            deny
 exit
exit
```

Loading Day 1 Configuration

The cnSGW-C configuration is provided using the Ops Center infrastructure. To load the Day 1 configuration, run the following command:

```
ssh admin@ops_center_pod_ip -p 2024 Day1config.cli
```

Note The Day1config.cli, on page 23 file contains the necessary parameters required for the Day 1 configuration.

Alternatively, you can copy the configuration and paste it in the cnSGW-C Ops Center CLI to load the Day 1 configuration.

```
config
  <Paste the Day 1 configuration here>
  commit
  end
```

Day1config.cli

The following is a sample `Day1config.cli` file, which contains the Day 1 configuration for the cnSGW-C.

```
ipam
instance 1
source local
address-pool poolv4
vrf-name ISP
tags
dnn intershat
dnn starent.com
exit
ipv4
split-size
per-cache 1024
per-dp    256
exit
address-range 209.165.200 209.165.200.224
exit
exit
address-pool poolv4DNN2
vrf-name ISP
tags
dnn intershat1
exit
ipv4
split-size
per-cache 1024
per-dp    256
exit
address-range 209.165.100 209.165.201.0
exit
exit
address-pool poolv4DNN3
static
vrf-name ISP
tags
dnn intershat2
```

```
exit
ipv4
split-size
per-cache 512
per-dp    512
exit
address-range 209.165.202 209.165.202.128
exit
ipv6
prefix-ranges
split-size
per-cache 8192
per-dp    8192
exit
prefix-range 2002:db0:: length 48
exit
exit
exit
address-pool poolv4vDNN
vrf-name ISP
tags
dnn intershat1
exit
ipv4
split-size
per-cache 1024
per-dp    256
exit
address-range 209.165.200 209.165.202.128
exit
exit
address-pool poolv6
vrf-name ISP
tags
dnn intershat
exit
ipv6
prefix-ranges
split-size
per-cache 8192
per-dp    1024
exit
prefix-range 2001:db0:: length 48
exit
exit
exit
address-pool poolv6DNN2
vrf-name ISP
tags
dnn intershat1
exit
ipv6
prefix-ranges
split-size
per-cache 8192
per-dp    1024
exit
prefix-range 2001:ef0:: length 48
exit
exit
exit
address-pool poolv6vDNN
vrf-name ISP
tags
```

```
dnn intershat1
exit
ipv6
prefix-ranges
split-size
per-cache 8192
per-dp    1024
exit
prefix-range 2001:ab0:: length 48
exit
exit
exit
exit
cdl deployment-model small
cdl zookeeper replica 1
cdl datastore session
 slice-names 1
index map    1
index write-factor 1
slot replica 1
slot map     1
slot write-factor 1
exit
cdl kafka replica 1
etcd replicas 1
instances instance 1
 slice-name 1
 system-id  DCNAME001
 cluster-id CLUSTER0001
exit
local-instance instance 1
instance instance-id 1
endpoint sbi
replicas 1
vip-ip 209.165.201.3 vip-port 1234

  interface nrf
   loopbackPort 9001
   sla response 1000
   sla procedure 1000
   vip-ip 209.165.201.3 vip-port 9002 offline
  exit
  interface n11
   loopbackPort 9011
   sla response 1000
   sla procedure 1000
   vip-ip 209.165.201.3 vip-port 8090
  exit
  interface n7
   loopbackPort 9007
   sla response 1000
   sla procedure 1000
   vip-ip 209.165.201.3 vip-port 8090
  exit
  interface n10
   loopbackPort 9010
   sla response 1000
   sla procedure 1000
   vip-ip 209.165.201.3 vip-port 8090
  exit
  interface n40
   loopbackPort 9040
   sla response 1000
   sla procedure 1000
```

```
   vip-ip 209.165.201.3 vip-port 8090
  exit


exit
endpoint li
replicas 1
vip-ip 209.165.201.3
exit
endpoint nodemgr
replicas 1
nodes    1
exit
endpoint gtp
replicas 1
interface s5
vip-ip 209.165.200.225
exit
interface s2b
vip-ip 209.165.200.225
exit
interface s5e
vip-ip 209.165.201.3
exit
interface s11
vip-ip 209.165.200.226
exit
exit
endpoint pfcp
replicas 1
enable-cpu-optimization true
interface sxa
heartbeat
interval               5
retransmission-timeout 3
max-retransmissions    5
exit
interface n4
heartbeat
interval               0
retransmission-timeout 3
max-retransmissions    5
exit
exit
exit
#endpoint radius-dns
#replicas 1
#vip-ip 209.165.201.3
#interface radius-client
#vip-ip 209.165.201.3
#exit
#exit
endpoint service
replicas 1
nodes 1
exit
endpoint protocol
vip-ip 209.165.201.3
replicas 1
interface n4
vip-ip 209.165.200.225
exit
interface sxa
vip-ip 209.165.201.3
```

```
exit
exit
endpoint sgw-service
replicas 1
node 1
exit
exit
logging level application debug
logging level transaction debug
logging level tracing debug
logging name infra.config.core level application trace
logging name infra.config.core level transaction trace
logging name infra.config.core level tracing off
logging name infra.message_log.core level transaction trace
deployment
 model small
 app-name     SMF
 cluster-name Local
 dc-name      DC
exit
k8 label protocol-layer key disktype value ssd
#k8 label service-layer key radnaik_key value mine
#k8 label service-layer key smi.cisco.com/node-type value oam
exit
system mode running
helm default-repository cn
helm repository cn
#access-token smf-deployer.gen:Mitg_123
#access-token dev-deployer.gen:Mitg_123
#access-token
dev-deployer.gen:AKCp5ekcXA7TknM9DbLASNBw4jwVEsx9Z9WpQwEvCvCQ2mJhLymcz6BfbH38YJiWC6fn1cKmw
access-token
smf-deployer.gen:AKCp5ekcX7DcBhuAmMZYfGLaHvH3E4Syr9TQDp1gjzcSjYrqsrGbXSYs5X2XYij3d9n9VfWQe
#url
https://engci-maven-master.cisco.com/artifactory/smi-fuse-internal-snapshot/mobile-cnat-cn/cn-products/dev-cn-stage
url
https://engci-maven-master.cisco.com/artifactory/smi-fuse-internal-snapshot/mobile-cnat-cn/cn-products/dev-cn-stage
exit
profile nf-client nf-type udm
udm-profile UP1
locality LOC1
priority 30
service name type nudm-sdm
endpoint-profile EP1
capacity   30
uri-scheme http
version
uri-version v2
exit
exit
endpoint-name EP1
primary ip-address ipv4 209.165.201.3
primary ip-address port 8001
exit
exit
exit
service name type nudm-uecm
endpoint-profile EP1
capacity   30
uri-scheme http
endpoint-name EP1
primary ip-address ipv4 209.165.201.3
primary ip-address port 8001
exit
```

```
exit
exit
service name type nudm-ee
endpoint-profile EP1
capacity       30
api-uri-prefix PREFIX
api-root       ROOT
uri-scheme     http
endpoint-name EP1
priority 56
primary ip-address ipv4 209.165.201.3
primary ip-address port 8001
exit
exit
exit
exit
exit
exit
profile nf-client nf-type pcf
pcf-profile PP1
locality LOC1
priority 30
service name type npcf-am-policy-control
endpoint-profile EP1
capacity   30
uri-scheme http
endpoint-name EP1
priority 56
primary ip-address ipv4 209.165.201.3
primary ip-address port 8003
exit
exit
exit
service name type npcf-smpolicycontrol
endpoint-profile EP1
capacity   30
uri-scheme http
endpoint-name EP1
priority 56
primary ip-address ipv4 209.165.201.3
primary ip-address port 8003
exit
exit
exit
exit
exit
exit
profile nf-client nf-type amf
amf-profile AP1
locality LOC1
priority 30
service name type namf-comm
endpoint-profile EP2
capacity   30
uri-scheme http
endpoint-name EP1
priority 56
primary ip-address ipv4 209.165.201.3
primary ip-address port 8002
exit
exit
exit
exit
exit
```

```
exit
profile nf-client nf-type chf
chf-profile CP1
locality LOC1
priority 30
service name type nchf-convergedcharging
endpoint-profile EP1
capacity   30
uri-scheme http
version
uri-version v2
exit
exit
endpoint-name EP1
priority 56
primary ip-address ipv4 209.165.201.3
primary ip-address port 8004
exit
exit
exit
exit
exit
chf-profile CP2
locality LOC1
priority 31
service name type nchf-convergedcharging
endpoint-profile EP1
capacity   30
uri-scheme http
version
uri-version v2
exit
exit
endpoint-name EP1
priority 56
primary ip-address ipv4 209.165.201.3
primary ip-address port 9040
exit
exit
exit
exit
exit
exit
profile nf-pair nf-type UDM
nrf-discovery-group udmdiscovery
locality client  LOC1
locality preferred-server LOC1
locality geo-server GEO
exit
profile nf-pair nf-type AMF
nrf-discovery-group udmdiscovery
locality client  LOC1
locality preferred-server LOC1
locality geo-server GEO
exit
profile nf-pair nf-type PCF
nrf-discovery-group udmdiscovery
locality client  LOC1
locality preferred-server LOC1
locality geo-server GEO
exit
profile nf-pair nf-type UPF
nrf-discovery-group udmdiscovery
locality client  LOC1
```

```
locality preferred-server LOC1
locality geo-server GEO
exit
profile nf-pair nf-type CHF
nrf-discovery-group udmdiscovery
locality client  LOC1
locality preferred-server LOC1
locality geo-server GEO
exit
profile nf-client-failure nf-type udm
profile failure-handling FH4
service name type nudm-sdm
message type UdmSdmGetUESMSubscriptionData
status-code httpv2 403
retry  3
action retry-and-ignore
exit
status-code httpv2 404
action continue
exit
status-code httpv2 413
retry  3
action retry-and-continue
exit
status-code httpv2 501
retry  3
action retry-and-terminate
exit
status-code httpv2 503
action terminate
exit
status-code httpv2 504
retry  3
action retry-and-terminate
exit
exit
message type UdmSdmSubscribeToNotification
status-code httpv2 403
retry  3
action retry-and-ignore
exit
status-code httpv2 404
action continue
exit
status-code httpv2 413
retry  3
action retry-and-continue
exit
status-code httpv2 501
retry  3
action retry-and-terminate
exit
status-code httpv2 503
action terminate
exit
status-code httpv2 504
retry  3
action retry-and-terminate
exit
exit
exit
service name type nudm-uecm
message type UdmUecmRegisterSMF
status-code httpv2 403
```

```
retry  3
action retry-and-ignore
exit
status-code httpv2 404
action continue
exit
status-code httpv2 413
retry  3
action retry-and-continue
exit
status-code httpv2 501
retry  3
action retry-and-terminate
exit
status-code httpv2 503
action terminate
exit
status-code httpv2 504
retry  3
action retry-and-terminate
exit
exit
exit
exit
exit
profile nf-client-failure nf-type pcf
profile failure-handling FH1
service name type npcf-smpolicycontrol
message type PcfSmpolicycontrolCreate
status-code httpv2 0
action retry-and-ignore
exit
status-code httpv2 400
action continue
exit
status-code httpv2 403
action retry-and-ignore
exit
status-code httpv2 404
action terminate
exit
status-code httpv2 500
retry  2
action retry-and-ignore
exit
status-code httpv2 503
retry  2
action retry-and-continue
exit
exit
message type PcfSmpolicycontrolUpdate
status-code httpv2 0
action retry-and-ignore
exit
status-code httpv2 400
action continue
exit
status-code httpv2 403
action retry-and-ignore
exit
status-code httpv2 404
action terminate
exit
status-code httpv2 500
```

```
retry  2
action retry-and-ignore
exit
status-code httpv2 503
retry  2
action retry-and-continue
exit
exit
message type PcfSmpolicycontrolDelete
status-code httpv2 0
action retry-and-ignore
exit
status-code httpv2 400
action continue
exit
status-code httpv2 403
action retry-and-ignore
exit
status-code httpv2 404
action terminate
exit
status-code httpv2 500
retry  2
action retry-and-ignore
exit
status-code httpv2 503
retry  2
action retry-and-continue
exit
exit
exit
exit
exit
profile nf-client-failure nf-type chf
profile failure-handling FH2
service name type nchf-convergedcharging
message type ChfConvergedchargingCreate
status-code httpv2 0
action continue
exit
status-code httpv2 400
retry  3
action retry-and-terminate
exit
status-code httpv2 403
retry  3
action retry-and-ignore
exit
status-code httpv2 404
retry  3
action retry-and-terminate
exit
status-code httpv2 500
action continue
exit
status-code httpv2 503
action terminate
exit
status-code httpv2 504
action continue
exit
exit
message type ChfConvergedchargingUpdate
status-code httpv2 0
```

```
action continue
exit
status-code httpv2 400
retry  3
action retry-and-terminate
exit
status-code httpv2 403
retry  3
action retry-and-ignore
exit
status-code httpv2 404
retry  3
action retry-and-terminate
exit
status-code httpv2 500
action continue
exit
status-code httpv2 503
action terminate
exit
status-code httpv2 504
action continue
exit
exit
message type ChfConvergedchargingDelete
status-code httpv2 0
action continue
exit
status-code httpv2 400
retry  3
action retry-and-terminate
exit
status-code httpv2 403
retry  3
action retry-and-ignore
exit
status-code httpv2 404
retry  3
action retry-and-terminate
exit
status-code httpv2 500
action continue
exit
status-code httpv2 503
action terminate
exit
status-code httpv2 504
action continue
exit
exit
exit
exit
exit
profile sgw sgw1
 locality          LOC2
 fqdn              cisco.com.apn.epc.mnc456.mcc123
 #subscriber-policy polSub
exit
profile smf smf1
node-id       abcdef
locality      LOC1
fqdn          cisco.com.apn.epc.mnc456.mcc123
allowed-nssai [ slice1 ]
plmn-id mcc 123
```

```
plmn-id mnc 456
service name nsmf-pdu
type               pdu-session
schema             http
service-id         1
version            1.Rn.0.0
http-endpoint base-url http://smf-service
icmpv6-profile     icmpprf1
compliance-profile comp1
access-profile     access1
subscriber-policy  polSub
exit
exit
profile sgw sgw1
locality      LOC2
fqdn          cisco.com.apn.epc.mnc456.mcc123
plmn-id mcc 123
plmn-id mnc 456
#subscriber-policy  polSub
exit
profile dnn starent.com
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 charging-profile chgprf1
 virtual-mac      b6:6d:47:47:47:47
 ssc-mode 2 allowed [ 3 ]
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 upf apn starent.com
 #dcnr true
exit

profile dnn default-profile
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 charging-profile chgprf1
 virtual-mac      b6:6d:47:47:47:47
 ssc-mode 2 allowed [ 3 ]
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 upf apn starent.com
 #dcnr true
exit

profile dnn intershat
network-element-profiles chf chf1
network-element-profiles amf amf1
network-element-profiles pcf pcf1
network-element-profiles udm udm1
charging-profile chgprf1
virtual-mac      b6:6d:47:47:47:47
ssc-mode 2 allowed [ 3 ]
session type IPV4 allowed [ IPV6 IPV4V6 ]
upf apn intershat
dcnr             true
exit
profile dnn intershat1
network-element-profiles chf chf1
network-element-profiles amf amf1
network-element-profiles pcf pcf1
network-element-profiles udm udm1
charging-profile chgprf1
```

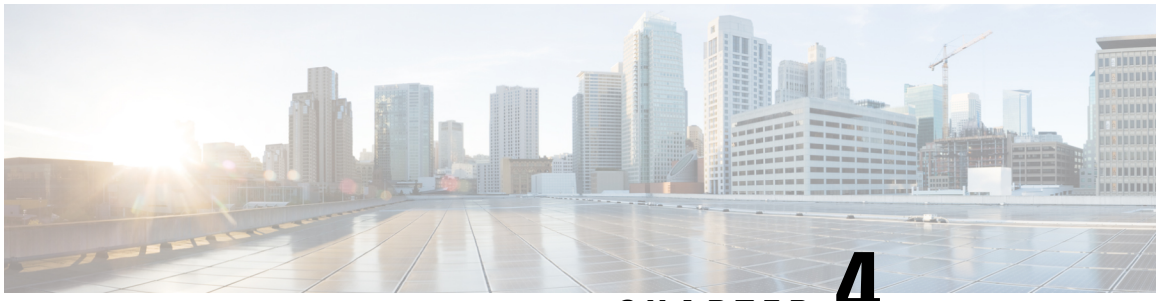
```
virtual-mac      b6:6d:47:47:47:48
pcscf-profile    PCSCF_Prof_2
ssc-mode 1
session type IPV4
exit
profile dnn intershat2
network-element-profiles chf chf
network-element-profiles amf amf
network-element-profiles pcf pcf
network-element-profiles udm udm
charging-profile chgprf1
virtual-mac      b6:6d:47:47:47:49
ssc-mode 2 allowed [ 3 ]
session type IPV4 allowed [ IPV6 IPV4V6 ]
upf apn intershat2
exit
profile qos abc
ambr ul "250 Kbps"
ambr dl "500 Kbps"
qi5      7
arp priority-level 14
arp preempt-cap NOT_PREEMPT
arp preempt-vuln PREEMPTABLE
priority 120
max data-burst 2000
exit
profile failure-handling FH1
interface pfcp message N4SessionEstablishmentReq
cause-code pfcp-entity-in-congestion action retry-terminate max-retry 2
cause-code system-failure action terminate
cause-code service-not-supported action terminate
cause-code no-resource-available action retry-terminate max-retry 3
cause-code no-response-received action retry-terminate max-retry 1
cause-code reject action terminate
exit
interface pfcp message N4SessionModificationReq
cause-code mandatory-ie-incorrect action terminate
cause-code session-ctx-not-found action terminate
cause-code reject action terminate
exit
exit
profile failure-handling gtp1
interface gtpc message S5S8CreateBearerReq
cause-code temp-fail
action retry timeout 1000 max-retry 2
exit
exit
interface gtpc message S5S8UpdateBearerReq
cause-code temp-fail
action retry timeout 1000 max-retry 2
exit
exit
interface gtpc message S5S8DeleteBearerReq
cause-code temp-fail
action retry timeout 1000 max-retry 2
exit
exit
exit
profile network-element amf amf1
nf-client-profile        AP1
failure-handling-profile FH3
query-params [ dnn ]
exit
profile network-element pcf pcf1
```

```
nf-client-profile        PP1
failure-handling-profile FH1
query-params [ dnn ]
rulebase-prefix          cbn#
predefined-rule-prefix   crn#
exit
profile network-element udm udm1
nf-client-profile        UP1
failure-handling-profile FH4
query-params [ dnn ]
exit
profile network-element upf upf226
node-id upf226@sgw.com
n4-peer-address ipv4 209.165.201.4
n4-peer-port 8805
dnn-list     [ intershat intershat1 intershat2 cisco.com starent.com ]
capacity     2000
priority     10
exit
profile network-element upf upf1
node-id upf1@sgw.com
n4-peer-address ipv4 209.165.201.5
n4-peer-port 8805
dnn-list     [ intershat intershat1 intershat2 cisco.com starent.com ]
capacity     2000
priority     10
exit
profile network-element upf upf2
node-id upf2@sgw.com
n4-peer-address ipv4 209.165.201.6
n4-peer-port 8805
dnn-list     [ intershat1 intershat2 cisco.com starent.com ]
capacity     2000
priority     1
exit
profile network-element upf upf76
node-id upf3@sgw.com
n4-peer-address ipv4 209.165.201.7
n4-peer-port 8805
dnn-list     [ intershat1 intershat2 starent.com cisco.com ]
capacity     1000
priority     10
exit
profile network-element upf upf70
node-id upf4@sgw.com
n4-peer-address ipv4 209.165.201.8
n4-peer-port 8805
dnn-list     [ intershat1 intershat2 starent.com cisco.com ]
capacity     1000
priority     10
exit
profile network-element upf upf71
node-id upf5@sgw.com
n4-peer-address ipv4 209.165.201.9
n4-peer-port 8805
dnn-list     [ intershat1 intershat2 starent.com cisco.com ]
capacity     1000
priority     10
exit
profile network-element upf upf72
n4-peer-address ipv4 209.165.201.10
n4-peer-port 8805
dnn-list     [ intershat1 intershat2 starent.com cisco.com ]
capacity     2000
```

```
priority     10
exit
profile network-element upf upf79
n4-peer-address ipv4 209.165.201.11
n4-peer-port 8805
dnn-list     [ intershat1 intershat2 starent.com cisco.com ]
capacity     2000
priority     10
exit
profile network-element upf upf131
n4-peer-address ipv4 209.165.201.12
n4-peer-port 8805
dnn-list     [ intershat1 intershat2 starent.com cisco.com ]
capacity     2000
priority     10
exit
profile network-element upf upf132
n4-peer-address ipv4 209.165.201.13
n4-peer-port 8805
dnn-list     [ intershat1 intershat2 starent.com cisco.com ]
capacity     2000
priority     10
exit
profile network-element upf upf133
n4-peer-address ipv4 209.165.201.14
n4-peer-port 8805
dnn-list     [ intershat1 intershat2 starent.com cisco.com ]
capacity     2000
priority     10
exit
profile network-element upf upf134
n4-peer-address ipv4 209.165.201.15
n4-peer-port 8805
dnn-list     [ intershat1 intershat2 starent.com cisco.com ]
capacity     2000
priority     10
exit
profile network-element upf upf135
n4-peer-address ipv4 209.165.201.16
n4-peer-port 8805
dnn-list     [ intershat1 intershat2 starent.com cisco.com ]
capacity     2000
priority     10
exit
profile network-element upf upf136
n4-peer-address ipv4 209.165.201.17
n4-peer-port 8805
dnn-list     [ intershat1 intershat2 starent.com cisco.com ]
capacity     2000
priority     10
exit
profile network-element chf chf1
nf-client-profile         CP1
failure-handling-profile  FH2
query-params [ dnn ]
nf-client-profile-offline CP2
exit
profile network-element chf chgser1
exit
profile compliance comp1
service nsmf-pdusession
version uri v1
version full 1.0.0
version spec 15.4.0
```

```
exit
service namf-comm
version uri v1
version full 1.0.0
version spec 15.4.0
exit
service n1
version uri v1
version full 1.0.0
version spec 15.4.0
exit
service n2
version uri v1
version full 1.0.0
version spec 15.4.0
exit
service nudm-sdm
version uri v1
version full 1.0.0
version spec 15.4.0
exit
service nudm-uecm
version uri v1
version full 1.0.0
version spec 15.4.0
exit
service nnrf-disc
version uri v1
version full 1.0.0
version spec 15.4.0
exit
service nnrf-nfm
version uri v1
version full 1.0.0
version spec 15.4.0
exit
service npcf-smpolicycontrol
version uri v1
version full 1.0.0
version spec 15.4.0
exit
service nchf-convergedcharging
version uri v1
version full 1.0.0
version spec 15.3.0
exit
exit
profile upf-group group1
failure-profile FH1
exit
profile access access1
n26 idft enable timeout 15
n2 idft enable timeout 15
gtpc gtpc-failure-profile gtp1
exit
profile icmpv6 icmpprf1
options virtual-mac b6:6d:57:45:45:45
exit
profile charging chgprf1
method [ offline ]
exit
profile charging-characteristics 1
charging-profile chgprf1
exit
```

```
nssai name slice1
sst 2
sdt Abf123
dnn [ dnn1 intershat intershat1 intershat2 ]
exit
policy subscriber polSub
precedence 1
sst              02
sdt              Abf123
serving-plmn mcc 123
serving-plmn mnc 456
supi-start-range 100000000000001
supi-stop-range  999999999999999
gpsi-start-range 1000000000
gpsi-stop-range  9999999999
operator-policy  opPol1
exit
precedence 511
operator-policy defOprPol1
exit
exit
policy operator defOprPol1
policy dnn         defPolDnn
policy network-capability nc1
exit
policy operator opPol1
policy dnn         polDnn
policy network-capability nc1
exit
policy dnn defPolDnn
profile default-profile
dnn dnn2 profile profile2
dnn intershat profile intershat
dnn intershat1 profile intershat1
dnn starent.com profile starent.com
exit
policy dnn polDnn
profile default-profile
dnn dnn2 profile profile2
dnn intershat profile intershat
dnn intershat1 profile intershat1
dnn intershat2 profile intershat2
dnn starent.com profile starent.com
exit
policy network-capability nc1
nw-support-local-address-tft true
exit
nacm groups group LI2
user-name [ liadmin2 ]
exit
nacm groups group LI3
user-name [ liadmin3 ]
exit
nacm groups group admin
user-name [ admin ]
exit
commit
end
```



CHAPTER 4

Smart Licensing Support

Feature Summary and Revision History

Summary Data

Table 3: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration required
Related Documentation	Not Applicable

Revision History

Table 4: Revision History

Revision Details	Release
Enhancement introduced. Multiple Entitlement Tags - cnSGW-C supports a REST service that returns Software License entitlements information based on the installed service profile.	2021.02.0
First introduced.	2020.03.0

Smart Software Licensing

Cisco employs two types of license models - Legacy Licensing and Smart Software Licensing. Legacy Licensing consists of software activation by installing Product Activation Keys (PAK) on to the Cisco product. A Product Activation Key is a purchasable item, ordered in the same manner as other Cisco equipment and used to obtain license files for feature set on Cisco Products. This traditional licensing does not need any online communication with the Cisco licensing server.

Smart Software Licensing is a cloud-based licensing of the end-to-end platform through the use of a few tools that authorize and deliver license reporting. Smart Software Licensing functionality incorporated into the NFs complete the product registration and authorization. cnSGW-C supports the Smart Software Licensing model.

Smart Licensing simplifies the purchase, deployment, and management of Cisco software assets. Entitlements are purchased through your Cisco account through Cisco Commerce Workspace (CCW) and immediately available in your Virtual Account for usage. This approach eliminates the need to install license files on every device. Smart-enabled products communicate directly to Cisco to report consumption. A single location—Cisco Software Central—is available for customers to manage Cisco software licenses. License ownership and consumption are readily available to help make a better purchase decision that is based on consumption or business need.

For more information on Cisco Smart Licensing, see https://www.cisco.com/c/en/us/buy/smart-accounts/software-licensing.html.

Cisco Software Central

Cisco Software Central (CSC) enables the management of software licenses and the smart account from a single portal. The CSC interface allows you to enable your product, manage entitlements, renew, and upgrade software. You need a functioning smart account to complete the registration process.

To access Cisco Software Central, see https://software.cisco.com.

Smart Accounts and Virtual Accounts

A Smart Account provides a single location for all smart-enabled products and entitlements. It helps in procurement, deployment, and maintenance of Cisco Software. When creating a smart account, you must have the authority to represent the requesting organization. After submission, the request goes through approval process.

A Virtual Account exists as a sub-account within the smart account. Virtual Accounts are customer-defined based on the organizational layout, business function, geography, or any defined hierarchy. Smart account administrator creates and maintains the virtual accounts.

For information on setting up or managing the Smart Accounts, see https://software.cisco.com.

Requesting a Cisco Smart Account

A Cisco Smart Account is an account where smart licensing-enabled products are available. A Cisco smart account allows you to manage and activate your licenses to devices, monitor license use, and track Cisco license purchases. Through transparent access, you have a real-time view into your smart licensing products. IT administrators can manage licenses and account users within the organization's smart account through Cisco Software Central. To create a Cisco Smart Account, perform the following steps:

Step 1 Visit the following URL:

`https://software.cisco.com`

Step 2 Log in using your credentials, and click **Request a Smart Account** in the **Administration** area.

The **Smart Account Request** window appears.

Step 3 Under **Create Account**, select one of the following options:

- **Yes, I have authority to represent my company and want to create the Smart Account**. If you select this option, you agree to authorize to create and manage product and service entitlements, users, and roles, on behalf of the organization.
- **No, the person specified below will create the account**. If you select this option, you must enter the email address of the person who creates the smart account.

Step 4 Under **Account Information**,

a) Click **Edit** beside **Account Domain Identifier**.
b) In the **Edit Account Identifier** dialog box, enter the domain, and click **OK**. By default, the domain is based on the email address of the person creating the account, and must belong to the company that will own this account.
c) Enter the **Account Name** (typically, the company name).

Step 5 Click **Continue**.

The Smart Account request will be in pending status until it is approved by the Account Domain Identifier. After the approval, you will receive an email confirmation with instructions for completing the setup process.

cnSGW-C Smart Licensing

The Smart Licensing feature supports application entitlement for online and offline licensing for all 5G applications. The application usage is unrestricted during all stages of licensing, including Out of Compliance (OOC) and expired stages.

Note A 90 day evaluation period is granted for all licenses in use. Currently, the functionality and operation of the 5G applications is unrestricted even after the end of the evaluation period.

Software Tags and Entitlement Tags

The following sections provide information on software and entitlement tags that are created to identify, report, and enforce licenses.

Software Tags

A Software tag or a Product tag is a unique identifier that helps Smart Licensing system identify the software product family. During the addition of Smart product instance in Cisco Smart Software Manager, the Smart client uses the software/product tag for identification.

The following software tags exist for the cnSGW-C.

Product Type / Description	Software Tag
Ultra Cloud Core - Serving Gateway Function (cnSGWc), Base Minimum	regid.2020-07.com.cisco.cnSGWc,1.0_ff0b64f1-f54d-46d3-afc7-052d41870b59

Entitlement Tags

An Entitlement tag is a part of the software that identifies the features that are being used in a software image. These tags underlay the communication on usage and entitlements of the software products that are installed on the devices. The entitlement tags map to both the PID license and the Software image. Every Smart-enabled PID may contain one or more entitlement tags.

The following entitlement tags identify licenses in use:

Product Type / Description	Entitlement Tag
Ultra Cloud Core - Serving Gateway Function (cnSGWc), 1K Sessions	regid.2020-07.com.cisco.cnSGWc_1K,1.0_6ce36c73-26dd-4607-ab9b-077fbb2e0f54

Note The license information is retained during software upgrades and rollback.

Multiple Entitlement Tags

Feature Description

cnSGW-C supports configuring REST endpoint. This REST endpoint supports a REST service that returns Software License entitlements information based on the installed service profile. For example:

- Standalone SMF
- Standalone cnSGW-C
- A combination of SMF and cnSGW-C

Note This feature is applicable only for Converged Core products.

How it Works

This section describes how this feature works.

To configure multiple entitlement tags, use the GET service added in NF's (cnSGW-C/SMF) rest-ep pod on the internal port 8000. The REST service name is 'entitlements'.

Note As `localhost:8000` is already occupied by entitlements service, it's recommended not to create a new service on port 8000 and localhost inside REST-EP.

Ops Center's `values.yaml` registers this service as a part of product configuration.

The following is a sample configuration:

```
ops-center:
  product:
    id: <product_id>, e.g. SMF
    softwareID: <s/w id>, e.g.
regid.2020-04.com.cisco.SMF,1.0_37ffdc21-3e95-4192-bcda-d3225b6590ce
    entitlementsURL: http://entitlements:8000/entitlements.json
```

After `values.yaml` is populated with entitlementsURL, Ops Center installs all the available licenses received from entitlements service.

The entitlements service looks up for entitlements in `rest-ep-entitlements-cm` configmap and returns all the available entitlements back as a JSON response.

Entitlements in `rest-ep-entitlements-cm` are registered based on the following flags:

- restep.smfProfile
- restep.sgwProfile

Note The flags are configured in **cn-ops-center** > **confd_init** > **render** > **rest-ep** > **pod.yaml**.

If entitlements service has no entitlement information, Ops Center doesn't send any request to the smart license server or doesn't install any license.

SNMP Traps

If the product is not in compliance with the contract (the product has used too many licenses/entitlements or not authorized to use a particular entitlement tag), a notification is sent to all the applications using the entitlement tag. An SNMP trap is sent indicating the entitlements that are not in compliance. This SNMP trap is seen in smart agent syslogs, with the trap name as `SMART_LIC-3-OUT_OF_COMPLIANCE`.

Limitations

Converged Core has two service profiles—SMF and cnSGW-C, with each service having a specific product ID. When registering with Software License server, the SMF and the cnSGW-C send respective product ID with their entitlements.

Smart agent doesn't support processing multiple product IDs. It is recommended to use SMF product ID for processing by the smart agent.

Sample Configuration

The following is an example configuration of `rest-ep-entitlements-cm` configmap.

```
Name:         rest-ep-entitlements-cm
Namespace:    smf
Labels:       app=rest-ep
```

```
              app.kubernetes.io/managed-by=Helm
              chart=rest-ep-0.5.2-dev-multi-entitlement-7600-210225084534-a5b5b67
              component=rest-ep
              heritage=Helm
              release=smf-rest-ep
Annotations:  meta.helm.sh/release-name: smf-rest-ep
              meta.helm.sh/release-namespace: smf

Data
====
nf-profiles:
----
configuredProfiles:
- name: "smf"
  entitlement:
    displayName: "UCC 5G SMF BASE"
   entitlementTag: regid.2020-04.com.cisco.SMF_BASE,1.0_b49f5997-21aa-4d15-9606-0cff88729f69

    entitlementVersion: "1.0"
- name: "sgw"
  entitlement:
    displayName: "UCC cnSGWc 1K"
   entitlementTag: regid.2020-07.com.cisco.cnSGWc_1K,1.0_6ce36c73-26dd-4607-ab9b-077fbb2e0f54

    entitlementVersion: "1.0"
Events:  <none>

JSON response format from REST API http://entitlements:8000/entitlemens.json

[
{
  "displayName" : "SMF_BASE",
  "entitlementTag" : "
regid.2020-04.com.cisco.SMF_BASE,1.0_b49f5997-21aa-4d15-9606-0cff88729f69",
  "entitlementVersion" : "1.0"

},
{
  "displayName" : "cnSGW_BASE",
  "entitlementTag" :
"regid.2020-02.com.cisco.cnSGW_BASE,1.0_a61f0740-ef15-4ac2-916f-77257902b22",
  "entitlementVersion" : "1.0"

}
]
```

Configuration Checks

This section describes the configuration checks.

- The following checks must be done after you configure multiple entitlement tags:
  - Make sure that NF's Ops Center is deployed successfully.
  - Post new deployment and configuration, make sure that all pods are up and in ready state (primarily, the service, nodemgr, cachepod, udp-proxy, rest-ep, and protocol pods).
  - If SMF service is configured with profile, then `rest-ep-entitlements-cm` must be populated with SMF entitlement.
  - If the cnSGW-C service is configured with profile, then `rest-ep-entitlements-cm` must be populated with cnSGW-C entitlement.

- If both—the SMF and the cnSGW-C services—are configured with the profile, then `rest-ep-entitlements-cm` must be populated with SMF and cnSGW-C entitlements.

- The following checks must be done after you remove multiple entitlement tag configurations:
  - Make sure all pods are terminated and removed (and SMF deregisters with NRF).
  - Make sure all security-related items (except for security items used by Ops Center) are removed.

Troubleshooting

This section describes troubleshooting information.

- To troubleshoot entitlements service, check rest-ep pod logs.

  kubectl logs rest-ep-n0-0 -n *<namespace>* **-f**
- To debug the issue with the entitlement service, you can also check the output data from the following commands.
  - **show license tech-support**
  - **show license status**
  - **show license summary**
- To troubleshoot smart-agent and Ops Center pods, you can use the following commands.
  - **kubectl logs** *<smart_agent_pod>* **-n namespace**
  - **kubectl logs** *<ops_center_pod>* **-n namespace**

Configuring Smart Licensing

You can configure Smart Licensing after a new cnSGW-C deployment.

Users with Access to Cisco Software Central

This section describes how to configure Smart Licensing if you have access to Cisco Software Central (CSC) portal from your environment.

Setting Up the Product and Entitlement in CSC

To set up your product and entitlement in CSC:

1. Log in to your CSC account.
2. Click **Add Product** and enter the following details.
   - **Product name**—Specify the name of the deployed product. Example: SGW.
   - **Primary PM CEC ID**—Specify the primary Project Manager's CEC ID for the deployed product.
   - **Dev Manager CEC ID**—Specify the Development Manager's CEC ID for the deployed product.

- **Description**—(Optional) Specify a brief description of the deployed product.
- **Product Type**—Specify the product type.
- **Software ID Tag**—Specify the software ID Tag provided by the Cisco Accounts team.

3. Click **Create**.
4. Select your product from the **Product/Entitlement Setup** grid.
5. Click **Entitlement** drop-down and select **Create New Entitlement**.
6. Select **New Entitlement** in **Add Entitlement** and enter the following details:
   - **Entitlement Name**—Specify the license entitlement name. Example: SGW_BASE.
   - **Description**—(Optional) Specify a brief description about the license entitlement.
   - **Entitlement Tag**—Specify the entitlement tag provided by the Cisco Accounts team.
   - **Entitlement Type**—Specify the type of license entitlement.
   - **Vendor String**—Specify the vendor name.
7. Click **Entitlement Allocation**.
8. Click **Add Entitlement Allocation**.
9. In **New License Allocation**, provide the following details:
   - **Product**—Select your product from the drop-down list.
   - **Entitlement**—Select your entitlement from the drop-down list.
10. Click **Continue**.
11. In **New License Allocation**, enter the following details:
    - **Quantity**—Specify the number of licenses.
    - **License Type**—Specify the type of license.
    - **Expiring Date**—Specify the date of expiry for the license purchased.
12. Click **Create**.

Registering Smart Licensing

You must register the product entitled to the license with the CSC. To register the product, you must generate an ID token from the CSC.

1. Log in to your CSC account.
2. Click **General > New Token** and enter the following details:
   - **Description**—Specify a brief description for the ID token.
   - **Expires After**—Specify the number of days for the token to expire.
   - **Max. Number Users**—Specify the maximum number of users.

3. Click **Create Token**.
4. Select **new ID token** in **Product Instance Registration Token**.
5. Click **Actions > Copy**.
6. Log in to cnSGW-C Ops Center CLI and paste the **ID token** using the following command:

   `license smart register` *`idtoken`*

   NOTES:

   - **license smart register** —Registers Smart Licensing with the CSC.
   - *idtoken* —Specify the ID token generated from CSC.

   Example:

   ```
   license smart register
   Value for 'idtoken' (<string>): MTI2Y2FlNTAtOThkMi00YTAxLWE4M2QtOTNhNzNjNjY4ZmFiLTE2MTc4N
   Tky%0AMTA5MDh8ck1jUHNwc3k1ZC9nWFFCSnVEcUp4QU1jTFoxOGxDTU5kQ3lpa25E%0Ab04wST0%3D%0A
   ```

7. Verify the Smart Licensing status using the following command:

   `show license all`

   Example:

   ```
   show license all

   Smart Licensing Status
   ======================
   Smart Licensing is ENABLED

   Registration:
     Status: REGISTERED
     Smart Account: CN-5G-NF
     Virtual Account: Default
     Export-Controlled Functionality: Allowed
     Initial Registration: SUCCEEDED on Jul 12 19:46:04 2020 GMT
     Last Renewal Attempt: SUCCEEDED on Jul 12 19:46:04 2020 GMT
     Next Renewal Attempt: Jan 8 19:46:04 2021 GMT
     Registration Expires: Jul 12 19:39:10 2021 GMT

   License Authorization:
     Status: AUTHORIZED on Jul 12 19:46:06 2020 GMT
     Last Communication Attempt: SUCCEEDED on Jul 12 19:46:06 2020 GMT
     Next Communication Attempt: Aug 11 19:46:06 2020 GMT
     Communication Deadline: Oct 10 19:43:32 2020 GMT

   License Conversion:
    Automatic Conversion Enabled: true
    Status: NOT STARTED

   Utility:
     Status: DISABLED

   Transport:
     Type: CALLHOME

   Evaluation Period:
     Evaluation Mode: Not In Use
     Evaluation Period Remaining: 89 days, 1 hr, 20 min, 55 sec

   License Usage
   ```

```
=============
License Authorization Status: AUTHORIZED as of Jul 12 19:46:06 2020 GMT

cnSGWc_1K (cnSGWc_1K)
  Description: Ultra Cloud Core - Serving Gateway Function (cnSGWc), 1K Sessions
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
===================
UDI: PID:cnSGWc,SN:JC5LXHI-2KVPPIQ

Agent Version
=============
Smart Agent for Licensing: 3.0.13
```

Deregistering Smart Licensing

To deregister Smart Licensing:

1. Log in to cnSGW-C Ops Center CLI and use the following command:

   `license smart deregister`

   NOTES:

   - **license smart deregister** —Deregisters Smart Licensing from CSC.

2. Verify the Smart Licensing status using the following command:

   `show license all`

   Example:

```
show license all

Smart Licensing Status
======================
Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 89 days, 1 hr, 18 min, 55 sec
  Last Communication Attempt: NONE

License Conversion:
 Automatic Conversion Enabled: true
 Status: NOT STARTED

Utility:
  Status: DISABLED

Transport:
  Type: CALLHOME
```

```
Evaluation Period:
  Evaluation Mode: In Use
  Evaluation Period Remaining: 89 days, 1 hr, 18 min, 55 sec

License Usage
=============
License Authorization Status: EVALUATION MODE
  Evaluation Period Remaining: 89 days, 1 hr, 18 min, 55 sec

cnSGWc_1K (cnSGWc_1K)
  Description: Ultra Cloud Core - Serving Gateway Function (cnSGWc), 1K Sessions
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: NOT RESTRICTED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
===================
UDI: PID:cnSGWc,SN:JC5LXHI-2KVPPIQ

Agent Version
=============
Smart Agent for Licensing: 3.0.13
```

Users without Access to Cisco Software Central

The Smart License Reservation feature—Perpetual Reservation—is reserved for customers without access to CSC from their internal environments. Cisco allows customers to reserve licenses from their virtual account and tie them to their devices' Unique Device Identifier (UDI). This enables customers to use their devices with reserved licenses in a disconnected mode.

The subsequent section describes the procedure involved in reserving Smart License for users without access to CSC from their internal environment.

Enabling and Generating Smart License Reservation Request Code

To enable and generate the Smart License reservation request code:

1. Log in to cnSGW-C Ops Center CLI.
2. To enable reservation, use the following configuration:

   ```
   config terminal
     license smart reservation
     end
   ```

   NOTES:

   - **license smart reservation** —Enables license reservation.

3. To request for a reservation code, use the following command:

   ```
   license smart reservation request
   ```

   NOTES:

   - **license smart reservation request** —Generates the license reservation request code.

Important Copy the generated license request code from the SGW Ops Center CLI to your local machine for further use.

Example:

```
license smart reservation request
reservation-request-code CE-ZcnSGWc:JC5LXHI-2KVPPIQ-AwjEHYoEo-F8
Message from confd-api-manager at 2020-07-13 08:27:27...
Global license change NotifyReservationInProgress reason code Success - Successful.
```

Generating an Authorization Code from CSC

To generate an authorization code from CSC using the license reservation request code:

1. Log in to your CSC account.
2. Click **License Reservation**.
3. Enter the Request Code: Paste the license reservation request code copied from the SGW Ops Center CLI in the **Reservation Request Code** text-box.
4. Select the Licenses: Click **Reserve a Specific License** radio button and select *UCC 5G SGW BASE*.

Note In the **Reserve** text box, enter the value *1*.

5. Review your selection.
6. Click **Generate Authorization Code**.
7. Download the response file: The authorization code is generated and displayed on-screen. Click **Download as File** to download the authorization code.
8. Click **Close**.

Reserving Smart Licensing

To reserve Smart License for the deployed product using the authorization code generated in CSC:

1. Log in to cnSGW-C Ops Center CLI and use the following command:

   `license smart reservation install` *`authorization_code`*

   NOTES:

   - **license smart reservation install** *authorization_code* —Installs a Smart License Authorization code.

   Example:

   ```
   license smart reservation install
   Value for 'key' (<string>): CAAAsJ-iwTYvW-puASse-nLGbcj-NJwnCo-EpxZ
   Message from confd-api-manager at 2020-07-13 08:30:00...
   Global license change NotifyReservationInstalled reason code Success - Successful.
   Message from confd-api-manager at 2020-07-13 08:30:01...
   Global license change NotifyRegisterSuccess reason code Success - Successful
   ```

2. Verify the smart licensing status using the following command:

   show license all

   Example:

```
show license all

Smart Licensing Status
======================
Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Mon Jul 13 08:29:59 GMT 2020
  Last Renewal Attempt: None

License Authorization:
  Status: AUTHORIZED - RESERVED on Mon Jul 13 08:29:59 GMT 2020

Utility:
  Status: DISABLED

Transport:
  Type: CALLHOME

Evaluation Period:
  Evaluation Mode: Not In Use
  Evaluation Period Remaining: 88 days, 23 hr, 28 min, 54 sec

License Usage
=============
License Authorization Status:
  Status: AUTHORIZED - RESERVED on Mon Jul 13 08:29:59 GMT 2020
  Last Communication Attempt: SUCCEEDED on Jul 13 08:29:59 2020 GMT
  Next Communication Attempt: NONE
  Communication Deadline: NONE

cnSGWc_1K (cnSGWc_1K)
  Description: Ultra Cloud Core - Serving Gateway Function (cnSGWc), 1K Sessions
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: RESTRICTED_ALLOWED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
===================
UDI: PID:cnSGWc,SN:JC5LXHI-2KVPPIQ

Agent Version
=============
Smart Agent for Licensing: 3.0.13
```

Returning the Reserved License

To return the reserved license, use the following procedure:

1. When the license reservation authorization code is installed in the SGW Ops Center:
   a. Log in to the cnSGW-C Ops Center CLI and use the following command:

license smart reservation return

NOTES:

- **license smart reservation return**—Returns a reserved Smart License.

Example:

```
license smart reservation return
reservation-return-code CAAsJA-vNGQbQ-YmwMTz-ZnN4Kb-eekEy7-jeo
Message from confd-api-manager at 2020-07-13 08:32:37...
Global license change NotifyReservationReturned reason code Success - Successful.
```

b. Copy the license reservation return code generated in SGW Ops Center CLI to your local machine for further use.

c. Log in to your CSC account.

d. Select your product instance from the list.

e. Click **Actions** > **Remove**.

f. Paste the license reservation return code in the **Return Code** text box.

2. When the license reservation authorization code is not installed in the SGW Ops Center:

a. Log in to the cnSGW-C Ops Center CLI and use the following command to generate the return code:

license smart reservation return
authorization_code

Important Paste the license reservation authorization code generated in CSC to generate the return code.

b. Log in to your CSC account.

c. Select your product instance from the list.

d. Click **Actions** > **Remove**.

e. Paste the license reservation return code in the **Return Code** text box.

3. Verify the smart licensing status using the following command:

show license all

Example:

```
show license all

Smart Licensing Status
======================
Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed

License Authorization:
  Status: EVAL MODE
```

```
  Evaluation Period Remaining: 88 days, 23 hr, 23 min, 54 sec
  Last Communication Attempt: SUCCEEDED on Jul 13 08:29:59 2020 GMT
  Next Communication Attempt: NONE
  Communication Deadline: NONE

License Conversion:
 Automatic Conversion Enabled: true
 Status: NOT STARTED

Utility:
  Status: DISABLED

Transport:
  Type: CALLHOME

Evaluation Period:
  Evaluation Mode: In Use
  Evaluation Period Remaining: 88 days, 23 hr, 23 min, 54 sec

License Usage
=============
License Authorization Status: EVALUATION MODE
  Evaluation Period Remaining: 88 days, 23 hr, 23 min, 54 sec

cnSGWc_1K (cnSGWc_1K)
  Description: Ultra Cloud Core - Serving Gateway Function (cnSGWc), 1K Sessions
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: RESTRICTED_NOTALLOWED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
===================
UDI: PID:cnSGWc,SN:JC5LXHI-2KVPPIQ

Agent Version
=============
Smart Agent for Licensing: 3.0.13
```

Viewing the Smart Licensing information

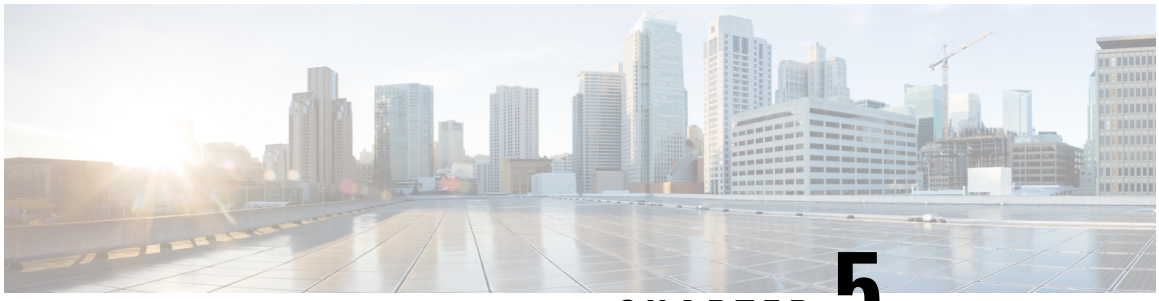
Use the following **show license** command to view the Smart Licensing information in the cnSGW-C Ops Center:

show license [all | UDI | displaylevel | reservation | smart | status | summary | tech-support | usage]

NOTES:

- **all**—Displays an overview of Smart Licensing information that includes license status, usage, product information, and Smart Agent version.
- **UDI**—Displays Unique Device Identifiers (UDI) details.
- **displaylevel**—Depth to display information.
- **reservation**—Displays Smart Licensing reservation information.

- **smart**—Displays Smart Licensing information.
- **status**—Displays the overall status of Smart Licensing.
- **summary**—Displays a summary of Smart Licensing.
- **tech-support**—Displays Smart Licensing debugging information.
- **usage**—Displays the license usage information for all the entitlements that are currently in use.



CHAPTER 5

cnSGW-C Rolling Software Update

Feature Summary and Revision History

Summary Data

Table 5: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 6: Revision History

Revision Details	Release
First introduced.	2021.02.0

Introduction

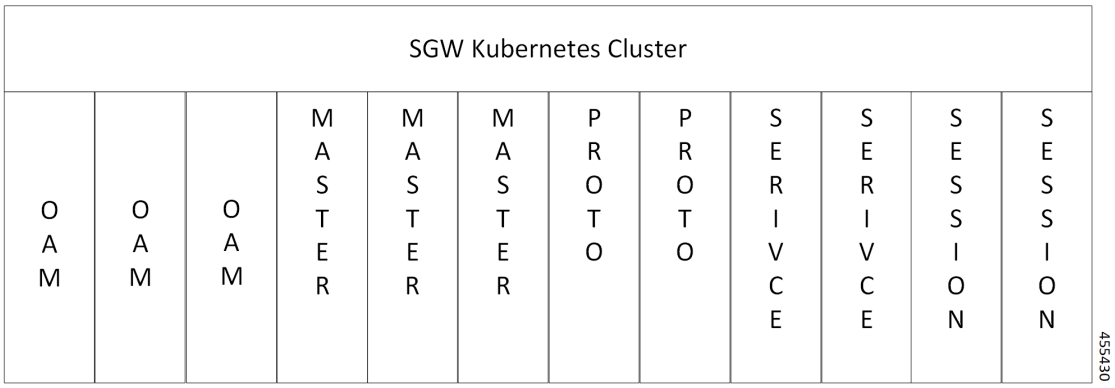
The cnSGW-C has a three-tier architecture consisting of Protocol, Service, and Session. Each tier includes a set of microservices (pods) for a specific functionality. Within these tiers, there exists a Kubernetes Cluster comprising of Kubernetes (K8s) master, and worker nodes (including Operation and Management (OAM) nodes).

For high availability and fault tolerance, a minimum of two K8s worker nodes are configured for each tier. You can have multiple replicas for each worker node. Kubernetes orchestrates the pods using the StatefulSets controller. The pods require a minimum of two replicas for fault tolerance.

The following figure depicts cnSGW-C K8s cluster with 12 nodes.

- Three master nodes
- Three OAM worker nodes
- Two Protocol worker nodes
- Two Service worker nodes
- Two Session (data store) worker nodes

Figure 11: cnSGW-C Kubernetes Cluster



The cnSGW-C Kubernetes cluster comprises of the following nodes:

- The OAM worker nodes host the Ops Center pods for configuration management and metrics pods for statistics and Key Performance Indicators (KPIs).
- The Protocol worker nodes host the cnSGW-C protocol-related pods for service-based interfaces (N11, N7, N10, N40) and UDP-based protocol interfaces (N4, S5/S8).
- The Service worker nodes host the cnSGW-C application-related pods that perform session management processing.
- The Session worker nodes host the database-related pods that store subscriber session data.

Updating cnSGW-C

The rolling software update is a process of updating or migrating the build from an older to a newer version or updating the patch for the prescribed deployment set of application pods.

Rolling update takes place with zero downtime by incrementally updating the pod instances with the new ones.

Note The applications must be available when new versions are expected to be deployed with the new build versions or patches.

Update Scope

The rolling update feature is supported from an older to the newer versions within the same major release.

- **Assumptions:** When updating, it is assumed that the following has not been changed between the versions:
  - Features supported in the old and the new versions.
  - Configuration addition, deletion, or modification of the existing CLI behavior.
  - Interface change within the peer or across the pods.
- **Recommendations:**
  - Configuration changes are not recommended during the update process.
  - All configuration changes should be done after the update process is complete.
- **Failure Handling:** The system should be downgraded manually to an older healthy build following the downgrade process for:
  - Failure during the process such as crash, and pods deployment failures.
  - Failure after the successful update such as new events or procedures.

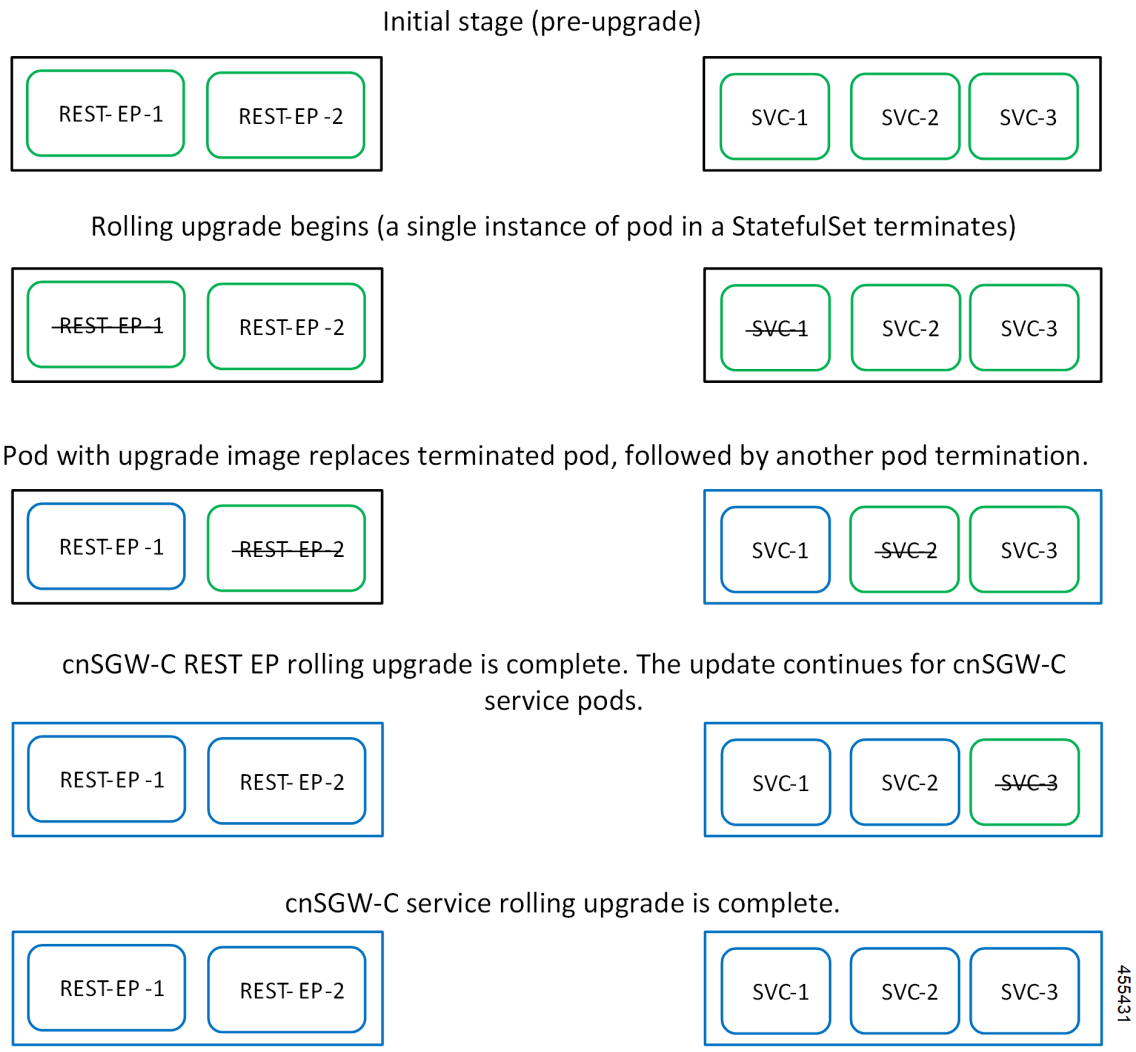
Rolling Software Update Using the SMI Cluster Manager

The cnSGW-C software update or in-service update procedure utilizes the K8s rolling strategy to update the pod images. In this strategy, the pods of a StatefulSet are updated sequentially to ensure that the ongoing process remains unaffected. Initially, a rolling update on a StatefulSet causes a single pod instance to terminate. A pod with an updated image replaces the terminated pod. This process continues until all the replicas of the StatefulSet are updated. The terminating pods exit gracefully after competing all the ongoing processes. Other in-service pods continue to receive and process the traffic to provide a seamless software update. You can control the software update process through the Ops Center CLI.

Note Each pod needs a minimum of two pods for high availability. In a worst-case scenario, the processing capacity of the pod may briefly reduce to 50% while the software update is in-progress.

The following figure illustrates a cnSGW-C rolling update for cnSGW-C REST endpoint pods (two replicas) on Protocol worker nodes along with cnSGW-C Service pods (three replicas) on Service worker nodes.

Figure 12: cnSGW-C Rolling Update



Prerequisites

The prerequisites for upgrading cnSGW-C are:

- All the nodes that include all the pods in the node that are up and running.
- A patch version of the cnSGW-C software.

Note Major versions do not support rolling update.

Important Trigger rolling update only when the CPU usage of the nodes is less than 50%.

- Intra-site HA support.

cnSGW-C Health Check

Perform a health check to ensure that all the services are running and the nodes are in the ready state.

To perform health check, use the following configuration:

- Log in to the master node and use the following configuration:

```
kubectl get pods -n smi
kubectl get nodes
kubectl get pod --all-namespaces -o wide
kubectl get pods -n cnsgw-wsp -o wide
kubectl get pods -n cee-wsp -o wide
kubectl get pods -n smi-vips -o wide
helm list
kubectl get pods -A | wc -l
```

Important Make sure that all the services are running and nodes are in the ready state before you proceed.

Backing Up the Deployment File

To create a backup configuration, logs, and deployment files, use the following configuration:

1. Log in to the SMI Cluster Manager Node as an Ubuntu user.
2. Create a new directory for deployment.

   Example:

   ```
   test@smicnsgw-cm01:~$ mkdir -p "temp_$(date +'%m%d%Y_T%H%M')" && cd "$_"
   ```

3. Back up the working files into the newly created deployment directory.
4. Untar the `cnsgw` deployment file.

   Example:

   ```
   test@smi1cnsgw01-cm01:~/temp_08072019_T1651$ tar -xzvf cnsgw.2020.01.0-1.SPA.tgz
   ./
   ./cnsgw_REL_KEY-CCO_RELEASE.cer
   ./cisco_x509_verify_release.py
   ./cnsgw.2020.01.0-1.tar
   ./cnsgw.2020.01.0-1.tar.signature.SPA
   ./cnsgw.2020.01.0-1.tar.SPA.README
   ```

5. Verify the downloaded image.

   Example:

   ```
   test@smi1cnsgw01-cm01:~/temp_08072019_T1651$ cat cnsgw.2020.01.0-1.tar.SPA.README
   ```

Important Follow the procedure mentioned in the *SPA.README* file to verify the build before proceeding to the next step.

Backing Up the Ops Center Configuration

To back up the Ops Center configurations, use the following configuration:

1. Log in to the SMI Cluster Manager node as an Ubuntu user.
2. Back up the SMI Ops Center configuration to the **/home/ubuntu/smiops.backup** file, using the following configuration:

   ```
   ssh -p <port_number> admin@$(kubectl get svc -n smi | grep
   '.*netconf.*<port_number>' | awk '{ print $4 }') "show run | nomore"
   > smiops.backup_$(date +'%m%d%Y_T%H%M')
   ```

3. Back up the CEE Ops Center configuration to the **/home/ubuntu/ceeops.backup** file, using the following configuration:

   ```
   ssh admin@<cee-vip> "show run | nomore" > ceeops.backup_$(date
   +'%m%d%Y_T%H%M')
   ```

4. Back up the cnSGW-C Ops Center configuration to the **/home/ubuntu/cnSGWops.backup** file, using the following configuration:

   ```
   ssh admin@<cnSGW-vip> "show run | nomore" > cnSGWops.backup_$(date
   +'%m%d%Y_T%H%M')
   ```

Back Up CEE and cnSGW-C Ops Center Configuration

To back up the CEE and Ops Center configuration from the master node, use the following configuration:

1. Log in to the master node as an Ubuntu user.
2. Create a directory to backup the configuration files, using the following configuration:

   ```
   mkdir backups_$(date +'%m%d%Y_T%H%M') && cd "$_"
   ```

3. Back up the cnSGW-C Ops Center configuration and verify the line count of the backup files, using the following configuration:

   ```
   ssh -p <port_number> admin@$(kubectl get svc -n $(kubectl get namespaces
    | grep -oP 'cnSGW-(\d+|\w+)') | grep <port_number> | awk '{ print $3
    }') "show run | nomore" > cnSGWops.backup_$(date +'%m%d%Y_T%H%M') &&
    wc -l cnSGWops.backup_$(date +'%m%d%Y_T%H%M')
   ```

   Example:

   ```
   ubuntu@pocnSGW-mas01:~/backups_09182019_T2141$ ssh -p 2024 admin@$(kubectl get svc -n
   $(kubectl get namespaces | grep -oP 'cnSGW-(\d+|\w+)') | grep <port_number> | awk '{
   print $3 }') "show run | nomore" > cnSGWops.backup_$(date +'%m%d%Y_T%H%M') && wc -l
   cnSGWops.backup_$(date +'%m%d%Y_T%H%M')
   admin@<ipv4address>'s password: cnSGW-OPS-PASSWORD
   334 cnSGWops.backup
   ```

4. Back up the CEE Ops Center configuration and verify the line count of the backup files, using the following configuration:

   ```
   ssh -p <port_number> admin@$(kubectl get svc -n $(kubectl get namespaces
    | grep -oP 'cee-(\d+|\w+)') | grep <port_number> | awk '{ print $3
   }') "show run | nomore" > ceeops.backup_$(date +'%m%d%Y_T%H%M') && wc
    -l ceeops.backup_$(date +'%m%d%Y_T%H%M')
   ```

   Example:

```
ubuntu@pocnSGW-mas01:~/backups_09182019_T2141$ ssh -p <port_number> admin@$(kubectl get
 svc -n $(kubectl get namespaces | grep -oP 'cee-(\d+|\w+)') | grep <port_number> | awk
 '{ print $3 }') "show run | nomore" > ceeops.backup_$(date +'%m%d%Y_T%H%M') && wc -l
ceeops.backup_$(date +'%m%d%Y_T%H%M')
admin@<ipv4address>'s password: CEE-OPS-PASSWORD
233 ceeops.backup
```

5. Move the SMI Ops Center backup file (from the SMI Cluster Manager) to the backup directory, using the following configuration:

   scp $(grep cm01 /etc/hosts | awk '{ print $1 }'):/home/ubuntu/smiops.backup_$(date +'%m%d%Y_T%H%M') .

   Example:

   ```
   ubuntu@pocnSGW-mas01:~/backups_09182019_T2141$ scp $(grep cm01 /etc/hosts | awk '{ print
    $1 }'):/home/ubuntu/smiops.backup_$(date +'%m%d%Y_T%H%M') .
   ubuntu@<ipv4address>'s password: SMI-CM-PASSWORD
   smiops.backup                                                 100% 9346    22.3MB/s
      00:00
   ```

6. Verify the line count of the backup files.

   Example:

   ```
   ubuntu@pocnSGW-mas01:~/backups_09182019_T2141$ wc -l *
     233 ceeops.backup
     334 cnSGWops.backup
     361 smiops.backup
     928 total
   ```

Staging a New cnSGW-C Image

To stage a new cnSGW-C image before initiating the update, use the following configuration:

1. Download and verify the new cnSGW-C image.
2. Log in to the SMI Cluster Manager node as an Ubuntu user.
3. Copy the image to the **uploads** directory.

   sudo mv <cnSGW_new_image.tar> /data/software/uploads

Note The SMI uses the new image present in the **uploads** directory to update.

4. Verify whether the image is picked up by the SMI for processing from the **uploads** directory.

   sleep 30; ls /data/software/uploads

   Example:

   ```
   ubuntu@pocnSGW-cm01:~/temp_08072019_T1651$ sleep 30; ls /data/software/uploads
   ubuntu@pocnSGW-cm01:~/temp_08072019_T1651$
   ```

5. Verify whether the images were successfully picked up and processed.

   Example:

   ```
   auser@unknown:$ sudo du -sh /data/software/packages/*
   1.6G /data/software/packages/cee.2019.07
   5.3G /data/software/packages/cnSGW.2019.08-04
   16K /data/software/packages/sample
   ```

Note The SMI must unpack the images into the **packages** directory successfully to complete the staging.

Triggering the Rolling Software Upgrade

cnSGW-C utilizes the SMI Cluster Manager to perform a rolling software update.

To update cnSGW-C using SMI Cluster Manager, use the following configurations:

Important Before you begin, ensure that cnSGW-C is up and running with the current version of the software.

1. Log in to the SMI Cluster Manager Ops Center.
2. Download the latest tarall from the URL.

   software-packages download *url*

   NOTES:

   - **software-packages download** *url*—Specifies the software packages to be downloaded through HTTP/HTTPS.

   Example:

   ```
   SMI Cluster Manager# software-packages download <url>
   ```

3. Verify whether the tarall is loaded.

   software-packages list

   NOTES:

   - **software-packages list** —Specifies the list of available software packages.

   Example:

   ```
   SMI Cluster Manager# software-packages list
   [ cnSGW-2019-08-21 ]
   [ sample ]
   ```

4. Update the product repository URL with the latest version of the product chart.

   Note If the repository URL contains multiple versions, the Ops Center automatically selects the latest version.

   ```
   configure
     cluster cluster_name
      ops-centers app_name cnSGW_instance_name
           repository url
            exit
          exit
   ```

   Example:

```
SMI Cluster Manager# config
SMI Cluster Manager(config)# clusters test2
SMI Cluster Manager(config-clusters-test2)# ops-centers cnSGW data
SMI Cluster Manager(config-ops-centers-cnSGW/data)# repository <url>
SMI Cluster Manager(config-ops-centers-cnSGW/data)# exit
SMI Cluster Manager(config-clusters-test2)# exit
```

5. To update to the latest version of the product chart, run the **cluster sync** command using the following command:

   clusters *cluster_name* **actions sync run**

   Example:

   ```
   SMI Cluster Manager# clusters test2 actions sync run
   ```

NOTES:

- **cluster** —Specifies the K8s cluster.
- *cluster_name* —Specifies the name of the cluster.
- **ops-centers** *app_name instance_name* —Specifies the product Ops Center and instance. *app_name* is the application name. *instance_name* is the name of the instance.
- **repository** *url*—Specifies the local registry URL for downloading the charts.
- **actions** —Specifies the actions performed on the cluster.
- **sync run** —Triggers the cluster synchronization.

Important

- The cluster synchronization updates the cnSGW-C Ops Center, which in turn updates the application pods (through **helm sync** command) one at a time automatically.
- When you trigger rolling upgrade on a specific pod, the cnSGW-C avoids routing new calls to that pod.
- The cnSGW-C honors in-progress call by waiting for 30 seconds before restarting the pod where rolling upgrade is initiated. Also, the cnSGW-C establishes all the in-progress calls completely within 30 seconds during the upgrade period (maximum call-setup time is 10 seconds).

Monitoring the Update Procedure

To monitor the status update through SMI Cluster Manager Ops Center, use the following configurations:

config
clusters *cluster_name* **actions sync run debug true**
clusters *cluster_name* **actions sync logs**
monitor sync-logs *cluster_name*
clusters *cluster_name* **actions sync status**
exit

Example:

```
SMI Cluster Manager# clusters test1 actions sync run
SMI Cluster Manager# clusters test1 actions sync run debug true
SMI Cluster Manager# clusters test1 actions sync logs
```

```
SMI Cluster Manager# monitor sync-logs test1
SMI Cluster Manager# clusters test1 actions sync status
```

NOTES:

- **clusters** *cluster_name*—Specifies the information about the nodes to be deployed. *cluster_name* is the name of the cluster.
- **actions**—Specifies the actions performed on the cluster.
- **sync run**—Triggers the cluster synchronization.
- **sync logs**—Shows the current cluster synchronization logs.
- **sync status** —Shows the current status of the cluster synchronization.
- **debug true**—Enters the debug mode.
- **monitor sync logs**—Monitors the cluster synchronization process.

Important You can view the pod details after the upgrade through the CEE Ops Center. For more information on pod details, see Viewing the Pod Details, on page 66 section.

Viewing the Pod Details

To view the details of the current pods through CEE Ops Center, use the following command in the CEE Ops Center CLI:

`cluster pods` *`instance_name pod_name`* **`detail`**

NOTES:

- **cluster pods**—Specifies the current pods in the cluster.
- *instance_name*—Specifies the name of the instance.
- *pod_name*—Specifies the name of the pod.
- **detail**—Displays the details of the specified pod.

The following example displays the details of the pod named *alertmanager-0* in the *cnSGW-data* instance.

Example:

```
cee# cluster pods cnSGW-data alertmanager-0 detail
details apiVersion: "v1"
kind: "Pod"
metadata:
  annotations:
    alermanager.io/scrape: "true"
    cni.projectcalico.org/podIP: "<ipv4address/subnet>"
    config-hash: "5532425ef5fd02add051cb759730047390b1bce51da862d13597dbb38dfbde86"
  creationTimestamp: "2020-02-26T06:09:13Z"
  generateName: "alertmanager-"
  labels:
    component: "alertmanager"
    controller-revision-hash: "alertmanager-67cdb95f8b"
    statefulset.kubernetes.io/pod-name: "alertmanager-0"
  name: "alertmanager-0"
```

```
  namespace: "cnSGW"
  ownerReferences:
  - apiVersion: "apps/v1"
    kind: "StatefulSet"
    blockOwnerDeletion: true
    controller: true
    name: "alertmanager"
    uid: "82a11da4-585e-11ea-bc06-0050569ca70e"
  resourceVersion: "1654031"
  selfLink: "/api/v1/namespaces/cnSGW/pods/alertmanager-0"
  uid: "82aee5d0-585e-11ea-bc06-0050569ca70e"
spec:
  containers:
  - args:
    - "/alertmanager/alertmanager"
    - "--config.file=/etc/alertmanager/alertmanager.yml"
    - "--storage.path=/alertmanager/data"
    - "--cluster.advertise-address=$(POD_IP):6783"
    env:
    - name: "POD_IP"
      valueFrom:
        fieldRef:
          apiVersion: "v1"
          fieldPath: "status.podIP"
    image: "<path_to_docker_image>"
    imagePullPolicy: "IfNotPresent"
    name: "alertmanager"
    ports:
    - containerPort: 9093
      name: "web"
      protocol: "TCP"
    resources: {}
    terminationMessagePath: "/dev/termination-log"
    terminationMessagePolicy: "File"
    volumeMounts:
    - mountPath: "/etc/alertmanager/"
      name: "alertmanager-config"
    - mountPath: "/alertmanager/data/"
      name: "alertmanager-store"
    - mountPath: "/var/run/secrets/kubernetes.io/serviceaccount"
      name: "default-token-kbjnx"
      readOnly: true
  dnsPolicy: "ClusterFirst"
  enableServiceLinks: true
  hostname: "alertmanager-0"
  nodeName: "for-smi-cdl-1b-worker94d84de255"
  priority: 0
  restartPolicy: "Always"
  schedulerName: "default-scheduler"
  securityContext:
    fsGroup: 0
    runAsUser: 0
  serviceAccount: "default"
  serviceAccountName: "default"
  subdomain: "alertmanager-service"
  terminationGracePeriodSeconds: 30
  tolerations:
  - effect: "NoExecute"
    key: "node-role.kubernetes.io/oam"
    operator: "Equal"
    value: "true"
  - effect: "NoExecute"
    key: "node.kubernetes.io/not-ready"
    operator: "Exists"
```

```
    tolerationSeconds: 300
  - effect: "NoExecute"
    key: "node.kubernetes.io/unreachable"
    operator: "Exists"
    tolerationSeconds: 300
  volumes:
  - configMap:
      defaultMode: 420
      name: "alertmanager"
    name: "alertmanager-config"
  - emptyDir: {}
    name: "alertmanager-store"
  - name: "default-token-kbjnx"
    secret:
      defaultMode: 420
      secretName: "default-token-kbjnx"
status:
  conditions:
  - lastTransitionTime: "2020-02-26T06:09:02Z"
    status: "True"
    type: "Initialized"
  - lastTransitionTime: "2020-02-26T06:09:06Z"
    status: "True"
    type: "Ready"
  - lastTransitionTime: "2020-02-26T06:09:06Z"
    status: "True"
    type: "ContainersReady"
  - lastTransitionTime: "2020-02-26T06:09:13Z"
    status: "True"
    type: "PodScheduled"
  containerStatuses:
  - containerID: "docker://821ed1a272d37e3b4c4c9c1ec69b671a3c3fe6eb4b42108edf44709b9c698ccd"

    image: "<path_to_docker_image>"
    imageID: "docker-pullable://<path_to_docker_image>"
    lastState: {}
    name: "alertmanager"
    ready: true
    restartCount: 0
    state:
      running:
        startedAt: "2020-02-26T06:09:05Z"
  hostIP: "<host_ipv4address>"
  phase: "Running"
  podIP: "<pod_ipv4address>"
  qosClass: "BestEffort"
  startTime: "2020-02-26T06:09:02Z"
cee#
```

Rolling Software Update on Non-SMI Cluster

To configure the helm repository, use the following configuration:

- Log in to cnSGW-C Ops Center and use the following configuration:

```
config
 helm default-repository cn
 helm repository cn
 access-token
smf-deployer.gen:AKCp5ekcX7DcBhuAmMZYfGLaHvH3E4Syr9TQDp1gjzcSjYrqsrGbXSYs5X2XYij3d9n9VfWQe

 url <old-build/new-build>
exit
```

Validating the Update

The health check, current helm charts, and subscriber/peer/session information help in understanding whether the rolling update process is successful.

To validate the update, use the following steps:

1. All pods that are deployed should be in the running state before and after an update.

   ```
   kubectl get pods -n cn
   ```

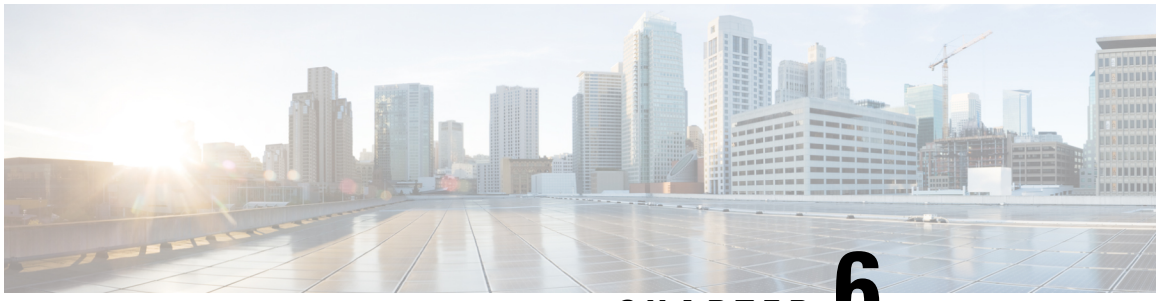
2. Helm charts should reflect charts from the appropriate build.

   To check the helm charts currently deployed, use the following command in the cnSGW-C Ops Center.

   ```
   show helm charts
   show running-config helm repository
   ```

3. Check subscriber, session, or peer information for retention validation, using the following configuration:

   ```
   show subscriber namespace sgw count all
   show peers all
   ```



CHAPTER 6

Pods and Services Reference

Feature Summary and Revision History

Summary Data

Table 7: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Revision Details	Release
First introduced	2020.07

Feature Description

cnSGW-C is built on the Kubernetes cluster strategy, adopting the native concepts of containerization, high availability, scalability, modularity, and ease of deployment. cnSGW-C uses the components, such as pods and services offered by Kubernetes.

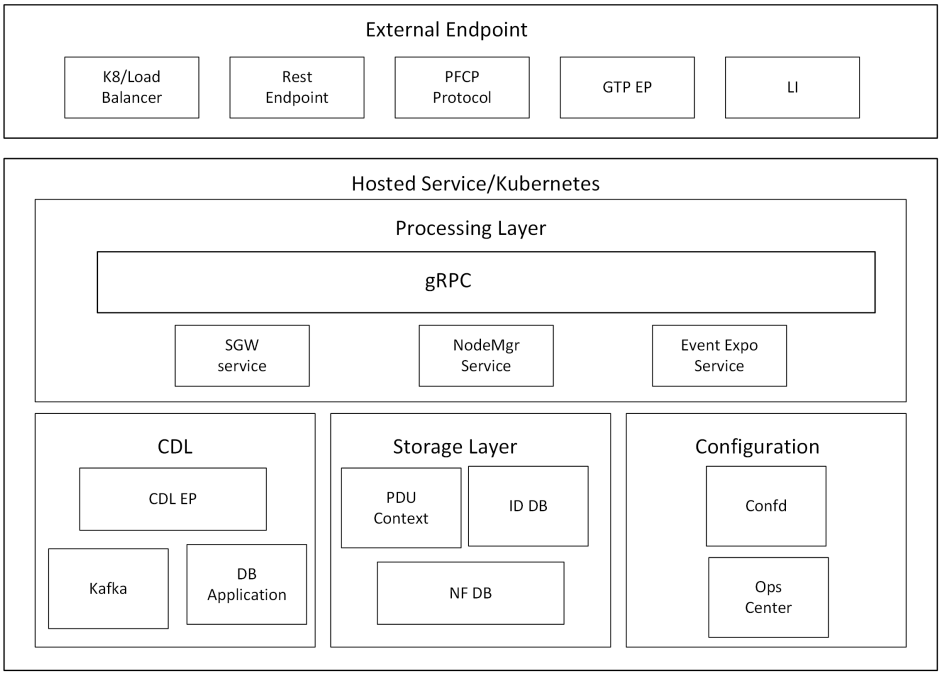
Depending on your deployment environment, the cnSGW-C deploys the pods on the configured virtual machines(VM) that you have configured. Pods operate through the services that are responsible for the intrapod communications. If the machine hosting the pods fail or experiences network disruption, the pods are terminated or deleted. However, this situation is transient and k8s, create new pods to replace the invalid pods.

The following workflow provides high-level information about:

- Host machines
- Associated pods and services
- Interaction among pods

The representation might defer based on your deployment infrastructure.

Figure 13: Communication Workflow of Pods



Kubernetes deployment includes the kubectl command-line tool to manage the Kubernetes resources in the cluster. You can manage the pods, nodes, and services.

For generic information on the Kubernetes concepts, see the Kubernetes documentation.

Pods

A pod is a process that runs on Kubernetes cluster. Pod encapsulates a granular unit known as a container. A pod can contains one or more containers.

Kubernetes deploys one or multiple pods on a single node which can be a physical or a virtual machine. Each pod has a discrete identity with an internal IP address and port number. The containers within the pod shares the storage and network resources.

The following tables list the cnSGW-C and Common Execution Environment (CEE) pod names and the hosts on which they are deployed depending on the labels that you assign. See the following table for information on how to assign the labels.

Table 8: cnSGW-C Pods

Pod Name	Description	Host Name
api-sgw-ops-center	Functions as *confD* API pod for the cnSGW-C Ops Center.	OAM
base-entitlement-sgw	Operates to support smart licensing feature.	OAM **Note** Currently no
bgpspeaker	Operates to support dynamic routing for L3 route management and BFD monitoring.	Protocol
cache-pod	Operates to support cache system information that is used by other pods as applicable.	Protocol
cdl-ep-session-c1	Provides an interface to the CDL.	Session
cdl-index-session-c1	Preserves the mapping of keys to the session pods.	Session
cdl-slot-session-c1	Operates as the CDL session pod to store the session data.	Session
documentation	Contains the documentation.	OAM
etcd-sgw-etcd-cluster	Hosts the etcd for the cnSGW-C OAM application to store information such as pod instances, leader information, endpoints.	OAM
georeplication	Operates to support cache, ETCD replication across sites, and site role management.	Protocol
grafana-dashboard-app-infra	Contains the default dashboard of app-infra metrics in Grafana.	OAM
grafana-dashboard-cdl	Contains the default dashboard of CDL metrics in Grafana.	OAM
grafana-dashboard-sgw	Contains the default dashboard of cnSGW-C service metrics in Grafana.	OAM
gtpc-ep-n0	Operates as GTPC endpoint of cnSGW-C.	Protocol
kafka	Hosts the Kafka details for the CDL replication.	Protocol
li-ep-n0	Operates as Lawful Intercept endpoint of cnSGW-C.	Protocol
oam-pod	Operates as the pod to facilitate Ops Center actions, such as show commands, configuration commands, monitor protocol monitor subscriber.	OAM

Pod Name	Description	Host Name
ops-center-sgw-ops-center	Acts as the cnSGW-C Ops Center.	OAM
smart-agent-sgw-ops-center	Operates as the utility pod for the cnSGW-C Ops Center.	OAM
nodemgr-n0	Performs node level interactions, such as Sxa link establishment and management (heartbeat). It generates unique identifiers, such as UE IP address and SEID.	Service
protocol-n0	Operates as encoder and decoder of application protocols (PFCP, whose underlying transport protocol is UDP).	Protocol
rest-ep-n0	cnSGW-C uses REST-EP as Notification client.	Protocol
service-n0	Contains main business logic of cnSGW-C.	Service
udp-proxy	Operates as proxy for all UDP messages. Owns UDP client and server functionalities.	Protocol
swift-sgw-ops-center	Operates as the utility pod for the cnSGW-C Ops Center.	OAM
zookeeper	Assists Kafka for topology management.	OAM

CEE Pods

For details, see the "CEE pods" topic from the UCC Common Execution Environment - Configuration and Administration Guide.

UDP Proxy Pod

Feature Description

The cnSGW-C has UDP interfaces towards the UP (Sxa), MME (S11), and PGW (S5 or S8). With the help of the protocol layer pods, the messages are encoded, decoded, and exchanged on these UDP interfaces.

For achieving the functionalities mentioned on the 3GPP specifications:

- It is mandatory for the protocol layer pods to receive the original source and destination IP address and port number. But the original IP and UDP header is not preserved when the incoming packets arrive at the UDP service in the Kubernetes (K8s) cluster.
- Similarly, for the outgoing messages, the source IP set to the external IP address of the UDP service (published to the peer node) is mandatory. But the source IP is selected as per the egress interface when different instances of protocol layer pods send outgoing messages from different nodes of the K8s cluster.

The protocol layer pod spawns on the node, which has the physical interface configured with the external IP address to achieve the conditions mentioned earlier. However, spawning the protocol layer pods has the following consequences:

- It is not possible to achieve the node level HA (High Availability) as the protocol pods are spawned on the same node of the K8s cluster. Any failure to that node may result in loss of service.
- The protocol pods must include their own UDP client and server functionalities. In addition, each protocol layer pod may require labeling of the K8s nodes with the affinity rules. This restricts the scaling requirements of the protocol layer pods.

The cnSGW-C addresses these issues with the introduction of a new K8s pod called udp-proxy. The primary objectives of this pod are:

- The udp-proxy pod acts as a proxy for all kinds of UDP messages. It also owns the UDP client and server functionalities.
- The protocol pods perform the individual protocol (PFCP, GTP, Radius) encoding and decoding, and provide the UDP payload to the udp-proxy pod. The udp-proxy pod sends the UDP payload out after it receives the payload from the protocol pods.
- The udp-proxy pod opens the UDP sockets on a virtual IP (VIP) instead of a physical IP. This ensures that the udp-proxy pod does not have any strict affinity to a specific K8s node (VM), thus enabling node level HA for the UDP proxy.

Note One instance of the udp-proxy pod is spawned by default in all the worker nodes in the K8s cluster.

The UDP proxy for cnSGW-C feature has functional relationship with the Virtual IP Address feature.

Architecture

The udp-proxy pod is placed in the worker nodes in the K8s cluster.

1. Each of the K8s worker node contains one instance of the udp-proxy pod. However, only one of the K8s worker node owns the virtual IP at any time. The worker node that owns the virtual IP remains in the active mode while all the other worker nodes remain in the standby mode.
2. The active udp-proxy pod binds to the virtual IP and the designated ports for listening to the UDP messages from the peer nodes (UPF and SGW).
3. The UDP payload received from the peer nodes are forwarded to one instance of the protocol, gtp-ep, or radius-ep pods. The payload is forwarded either on the same node or different node for further processing.
4. The response message from the protocol, gtp-ep, or radius-ep pods is forwarded back to the active instance of the udp-proxy pod. The udp-proxy pod sends the response message back to the corresponding peer nodes.
5. The cnSGW-C-initiated messages are encoded at the protocol, gtp-ep, or radius-ep pods. In addition, the UDP payload is sent to the udp-proxy pod. Eventually, the udp-proxy pod comprises of the complete IP payload and sends the message to the peer. When the response from the peer is received, the UDP payload is sent back to the same protocol pod from which the message originated.

Protocol Pod Selection for Peer-Initiated Messages

When the udp-proxy pod receives the peer node (for instance UPF) initiated messages, it is load-balanced across the protocol instances to select any instance of the protocol pod. An entry of this instance number is

stored along with the source IP and source port number of the peer node. This ensures that the messages form the same source IP and source port are sent to the same instance that was selected earlier.

High Availability for the UDP Proxy

The UDP proxy's HA model is based on the keepalived virtual IP concepts. A VIP is designated to the N4 interface during the deployment. Also, a keepalived instance manages the VIP and ensures that the IP address of the VIP is created as the secondary address of an interface in one of the worker nodes of the K8s cluster.

The udp-proxy instance on this worker node binds to the VIP and assumes the role of the active udp-proxy pod. All udp-proxy instances in the other worker nodes remain in the standby mode.

Services

The cnSGW-C configuration is composed of several microservices that run on a set of discrete pods. These Microservices are deployed during the cnSGW-C deployment. cnSGW-C uses these services to enable communication between the pods. When interacting with another pod, the service identifies the pod's IP address to initiate the transaction and acts as an endpoint for the pod.

The following table describes the cnSGW-C services and the pod on which they run.

Table 9: cnSGW-C Services and Pods

Service Name	Pod Name	Description
base-entitlement-sgw	base-entitlement-sgw	Operates to support sma
bgpspeaker-pod	bgpspeaker	Operates to support dyn route management and
datastore-ep-session	cdl-ep-session-c1	Responsible for the CDL
datastore-notification-ep	smf-rest-ep	Responsible for sending the CDL to the *sgw-servi* **Note** cnSGW-C uses notification clie
datastore-tls-ep-session	cdl-ep-session-c1	Responsible for the secu
documentation	documentation	Responsible for the cnS
etcd	etcd-sgw-etcd-cluster-0, etcd-sgw-etcd-cluster-1, etcd-sgw-etcd-cluster-2	Responsible for pod dis namespace.
etcd-sgw-etcd-cluster-0	etcd-sgw-etcd-cluster-0	Responsible for synchro the *etcd* cluster.
etcd-sgw-etcd-cluster-1	etcd-sgw-etcd-cluster-1	Responsible for synchro the *etcd* cluster.
etcd-sgw-etcd-cluster-2	etcd-sgw-etcd-cluster-2	Responsible for synchro the *etcd* cluster.

Service Name	Pod Name	Description
grafana-dashboard-app-infra	grafana-dashboard-app-infra	Responsible for the app-infra metrics in
grafana-dashboard-cdl	grafana-dashboard-cdl	Responsible for the metrics in Grafana.
grafana-dashboard-sgw	grafana-dashboard-sgw	Responsible for the cnSGW-C service m
gtpc-ep	gtpc-ep-n0	Responsible for inter GTP-C pod.
helm-api-sgw-ops-center	api-sgw-ops-center	Manages the Ops Ce
kafka	kafka	Processes the Kafka
li-ep	li-ep-n0	Responsible for lawf
local-ldap-proxy-sgw-ops-center	ops-center-sgw-ops-center	Responsible for leve credentials by other
oam-pod	oam-pod	Responsible to facili Ops Center.
ops-center-sgw-ops-center	ops-center-sgw-ops-center	Manages the cnSGW
ops-center-sgw-ops-center-expose-cli	ops-center-sgw-ops-center	To access cnSGW-C IP address.
smart-agent-sgw-ops-center	smart-agent-sgw-ops-center	Responsible for the c
smf-nodemgr	smf-nodemgr	Responsible for inter *smf-nodemgr* pod.
smf-protocol	smf-protocol	Responsible for inter smf-protocol pod.
sgw-service	sgw-service	Responsible for inter cnSGW-C service po
swift-sgw-ops-center	swift	Operates as the utilit Ops Center.
zookeeper	zookeeper	Assists Kafka for top
zookeeper-service	zookeeper	Assists Kafka for top

Open Ports and Services

The cnSGW-C uses different ports for communication. The following table describes the default open ports and the associated services.

Table 10: Open Ports and Services

Port	Type	Service	Usage
22	tcp	SSH	SMI uses TCP port to communicate with the virtual machines.

Port	Type	Service	Usage
53	tcp	domain	DNS port.
80	tcp	HTTP	SMI uses TCP port for providing Web access to CLI, Documentation, and TAC.
111	tcp	rpcbind	Open Network Computing Remote Procedure Call.
179	tcp	bgp	Border Gateway Protocol (BGP)
443	tcp	SSL/HTTP	SMI uses TCP port for providing Web access to CLI, Documentation, and TAC.
2379	tcp	etcd-client	CoreOS etcd client communication.
6443	tcp	http	SMI uses port to communicate with the Kubernetes API server.
7472	tcp	unknown	speaker, used by Grafana.
8083	tcp	us-srv	Kafka connects REST interface.
8850	tcp	unknown	udp-proxy
8879	tcp	unknown	udp-proxy
9100	tcp	jetdirect	SMI uses TCP port to communicate with the Node Exporter. Node Exporter is a Prometheus exporter for hardware and OS metrics with pluggable metric collectors. It allows you to measure various machine resources, such as memory, disk, and CPU utilization.
10250	tcp	SSL/HTTP	SMI uses TCP port to communicate with Kubelet. Kubelet is the lowest level component in Kubernetes. It is responsible for what is running on an individual machine. It is a process watcher or supervisor focused on active container. It ensures the specified containers are up and running.
10251	tcp	-	SMI uses TCP port to interact with the Kube scheduler. Kube scheduler is the default scheduler for Kubernetes and runs as part of the control plane. A scheduler watches for newly created pods that have no node assigned. For every pod that the scheduler discovers, the scheduler becomes responsible for finding the best node for that pod to run on.
10252	tcp	apollo-relay	SMI uses this TCP port to interact with the Kube controller. The Kubernetes controller manager is a daemon that embeds the core control loops shipped with Kubernetes. The controller is a control loop that watches the shared state of the cluster through the API server and makes changes to move the current state to the desired state.

Port	Type	Service	Usage
10256	-	HTTP	SMI uses TCP port to interact with the Kube proxy. Kube proxy is a network proxy that runs on each node in your cluster. Kube proxy maintains network rules on nodes. These network rules allow network communication to your pods from network sessions inside or outside of your cluster.
50051	tcp	unknown	gRPC service listen port.
53	udp	domain ISC BIND (Fake version: 9.11.3- 1ubuntu1.9- Ubuntu)	DNS port
111	udp	rpcbin	Open Network Computing Remote Procedure Call
2123	udp	gtpc	GTP control
8805	udp	pfcp	Packet Forwarding Control Protocol (PFCP)

Associating Pods to the Nodes

This section describes how to associate a pod to the node.

After configuring a cluster, you can associate the pods to the nodes through labels. This association enables the pods to get deployed on the appropriate node, based on the key-value pair.

Labels are required for the pods to identify the nodes where they must be deployed and to run the services. For example, when you configure the protocol-layer label with the required key-value pair, the pods are deployed on the nodes that match the key-value pair.

1. To associate pods to the nodes through the labels, use the following configuration:

```
config
 k8
   label
     cdl-layer
       key key_value
       value value
     oam-layer
       key key_value
       value value
     protocol-layer
       key key_value
       value value
     service-layer
       key key_value
```

```
value value
end
```

NOTES:

- If you don't configure the labels, cnSGW-C assumes the labels with the default key-value pair.
  - **label { cdl-layer { key** *key_value* **| value** *value* **}**—Configures the key value pair for CDL.
  - **oam-layer { key** *key_value* **| value** *value* **}**—Configures the key value pair for OAM layer.
  - **protocol-layer { key** *key_value* **| value** *value* **}**—Configures the key value pair for protocol layer.
  - **service-layer { key** *key_value* **| value** *value* **}**—Configures the key value pair for the service layer.

Viewing the Pod Details and Status

If the service requires additional pods, cnSGW-C creates and deploys the pods. You can view the list of available pods in your deployment through the cnSGW-C Ops Center.

You can run the kubectl command from the master node to manage the Kubernetes resources.

Pod Details

1. To view the comprehensive pod details, use the following command.

   kubectl get pods -n sgw *pod_name* **-o yaml**

The output of this command provides the pod details in YAML format with the following information:

- The IP address of the host where the pod is deployed.
- The service and the application that is running on the pod.
- The ID and the name of the container within the pod.
- The IP address of the pod.
- The present state and phase of the pod.
- The start time from which pod is in the present state.

Use the following command to view the summary of the pod details.

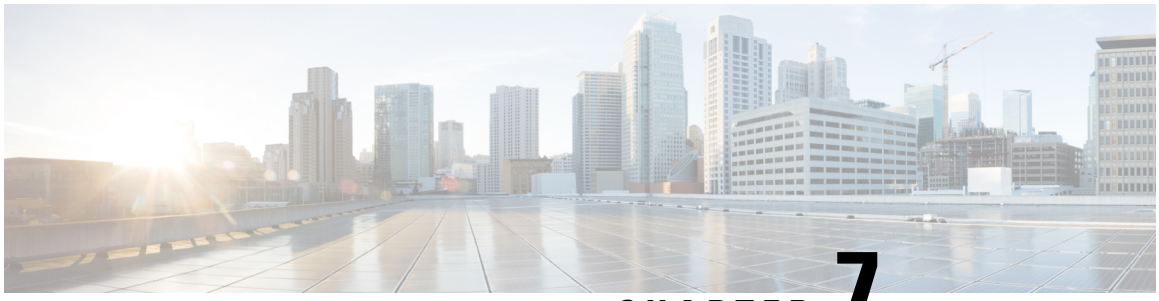
kubectl get pods -n *sgw_namespace* **-o wide**

States

The following table describes the state of a pod.

Table 11: Pod States

State	Description
Running	The pod is healthy and deployed on a node. It contains one or more containers.
Pending	The application is in the process of creating the container images for the pod.
Succeeded	Indicates that all the containers in the pod are successfully terminated. These pods cann't be restarted.
Failed	One ore more containers in the pod have failed the termination process. The failure occurred as the container either exited with non-zero status or the system terminated the container.



CHAPTER 7

3GPP RAN/NAS Cause Codes Support

Feature Summary and Revision History

Summary Data

Table 12: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 13: Revision History

Revision Details	Release
First introduced.	2021.02.0

Feature Description

cnSGW-C supports RAN/NAS cause codes as defined in *3GPP TS 29.274*, *version 15.4.0*, *section 8.103*, *RAN/NAS Cause*.

cnSGW-C transparently transmits the RAN/NAS Release Cause IE provided by the MME to the PGW for further propagation towards the PCRF.

Note GTP-based S5/S8 and S11 are supported.

The following table lists the RAN/NAS Cause codes.

Table 14: RAN/NAS Cause Codes

Octets	Bits							
	8	7	6	5	4	3	2	1
1	Type = 172 (decimal)							
2–3	Length = n							
4	Spare				Instance			
5	Protocol Type				Cause Type			
6 to m	Cause Value							
(m+1) to (n+4)	One or more octets from these octets are present, only if explicitly specified							

The Protocol Type field is encoded with the specified values for the RAN/NAS Cause as follows:

Table 15: Protocol Type

Protocol Type	Values (Decimal)
S1AP Cause	1
EMM Cause	2
ESM Cause	3
<spare>	4–15

The Cause Value field (and the associated RAN cause subcategory) is transferred over the S1-AP interface. The field is encoded in one octet as a binary integer.

Table 16: Cause Type

Cause Type	Values (Decimal)
Radio Network Layer	0
Transport Layer	1
NAS	2
Protocol	3
Miscellaneous	4

Cause Type	Values (Decimal)
<spare>	5–15

For EMM and ESM Causes, the Cause Value field contains the cause value as specified in *3GPP TS 24.301*. If the Protocol is S1AP, the cause value contains the specified value as in *3GPP TS 36.413*.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for the RAN/NAS Cause Codes feature.

Create Bearer Procedure Call Flow

This section describes the create bearer procedure call flow.

Figure 14: Create Bearer Procedure Call Flow

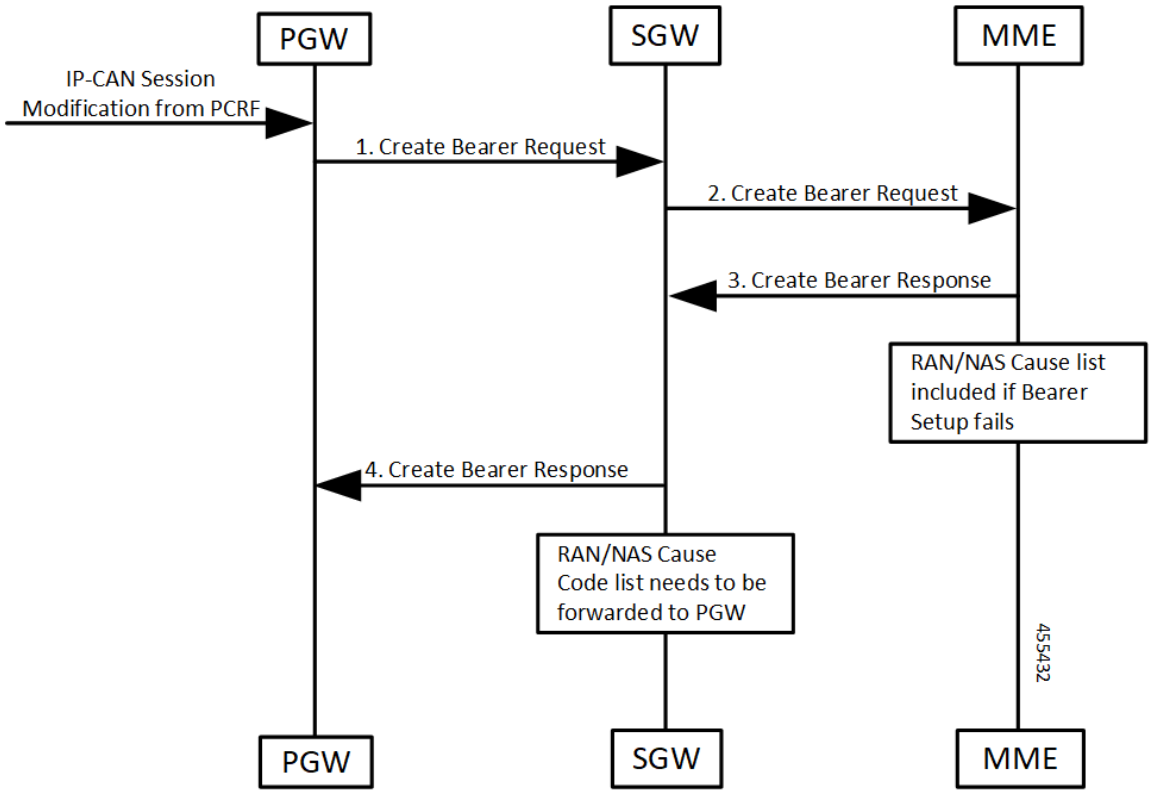


Table 17: Create Bearer Procedure Call Flow Description

Step	Description
1	PGW receives IP-CAN session modification request from PCRF. PGW creates the Create Bearer Request message and sends it to SGW (cnSGW-C).
2	SGW (cnSGW-C) forwards the Create Bearer Request message request to MME.
3	MME generates a Create Bearer Response message towards SGW (cnSGW-C). If bearer setup fails, then the RAN/Cause list included in the response.
4	SGW (cnSGW-C) forwards the Create Bearer Response message to PGW. It includes RAN/NAS Cause Code list.

Update Bearer Procedure Call Flow

This section describes the update bearer procedure call flow.

Figure 15: Update Bearer Procedure Call Flow

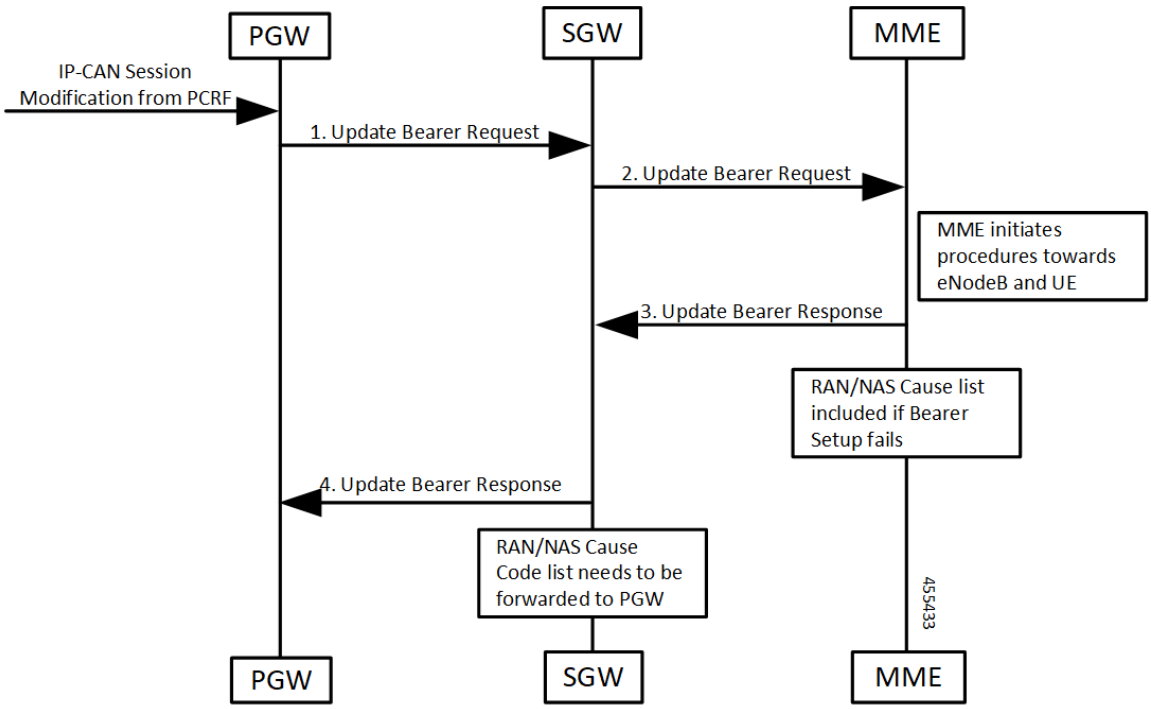


Table 18: Update Bearer Procedure Call Flow Description

Step	Description
1	PGW receives IP-CAN session modification request from PCRF. PGW creates the Update Bearer Request message to SGW (cnSGW-C).

Step	Description
2	SGW (cnSGW-C) forwards the Update Bearer Request message to MME.
3	MME generates an Update Bearer Response message towards SGW (cnSGW-C). If this bearer modification fails, then the RAN/NAS list included in the response.
4	SGW (cnSGW-C) forwards the Update Bearer Response message to PGW.

Delete Bearer Command Procedure Call Flow

This section describes the delete bearer command procedure call flow.

Figure 16: Delete Bearer Command Procedure Call Flow

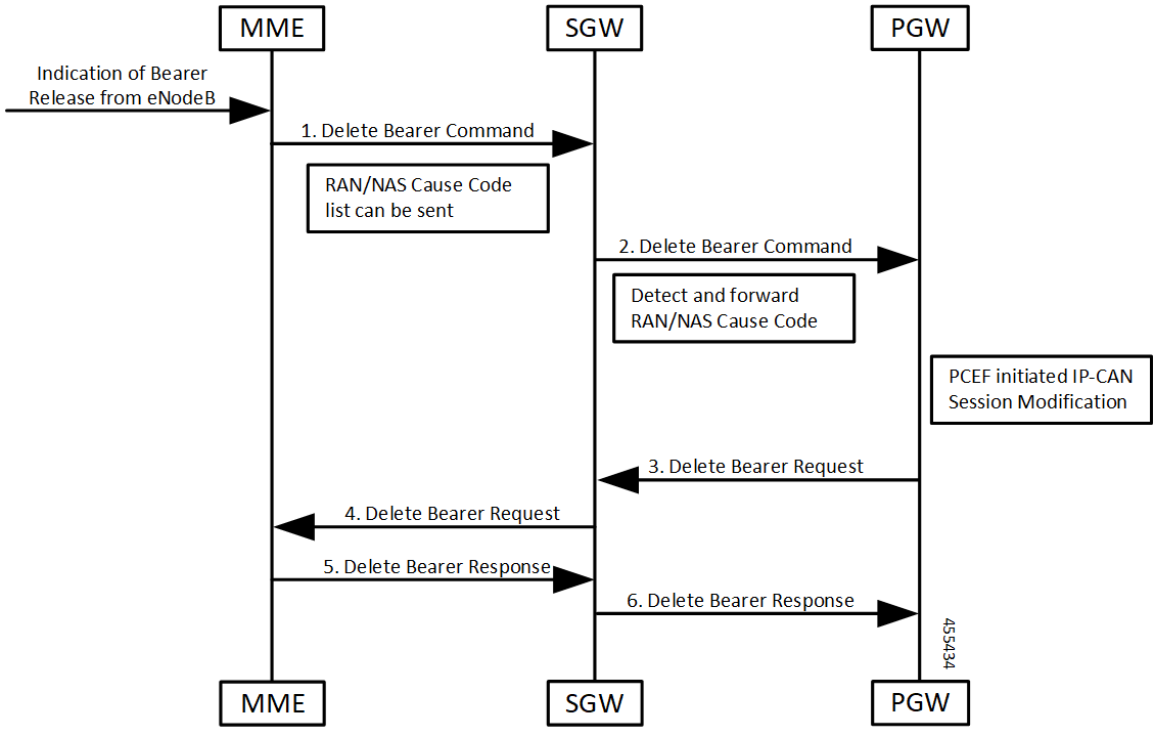


Table 19: Delete Bearer Command Procedure Call Flow Description

Step	Description
1	MME receives an indication of Bearer Release from eNodeB request. MME creates Delete Bearer Command message to SGW (cnSGW-C). It includes RAN/NAS cause code list.
2	SGW (cnSGW-C) forwards the Delete Bearer Command message request to PGW. It detects and forwards RAN/NAS cause code list.

Step	Description
3	PGW sends the Delete Bearer Request message to SGW (cnSGW-C). PGW receives IP-CAN session modification request from PCEF.
4	SGW (cnSGW-C) generates a Delete Bearer Request message towards MME.
5	MME generates a Delete Bearer Response message towards SGW (cnSGW-C).
6	SGW (cnSGW-C) further sends the Delete Bearer Response message to PGW.

Delete Session Procedure Call Flow

This section describes the delete session procedure call flow.

Figure 17: Delete Session Procedure Call Flow

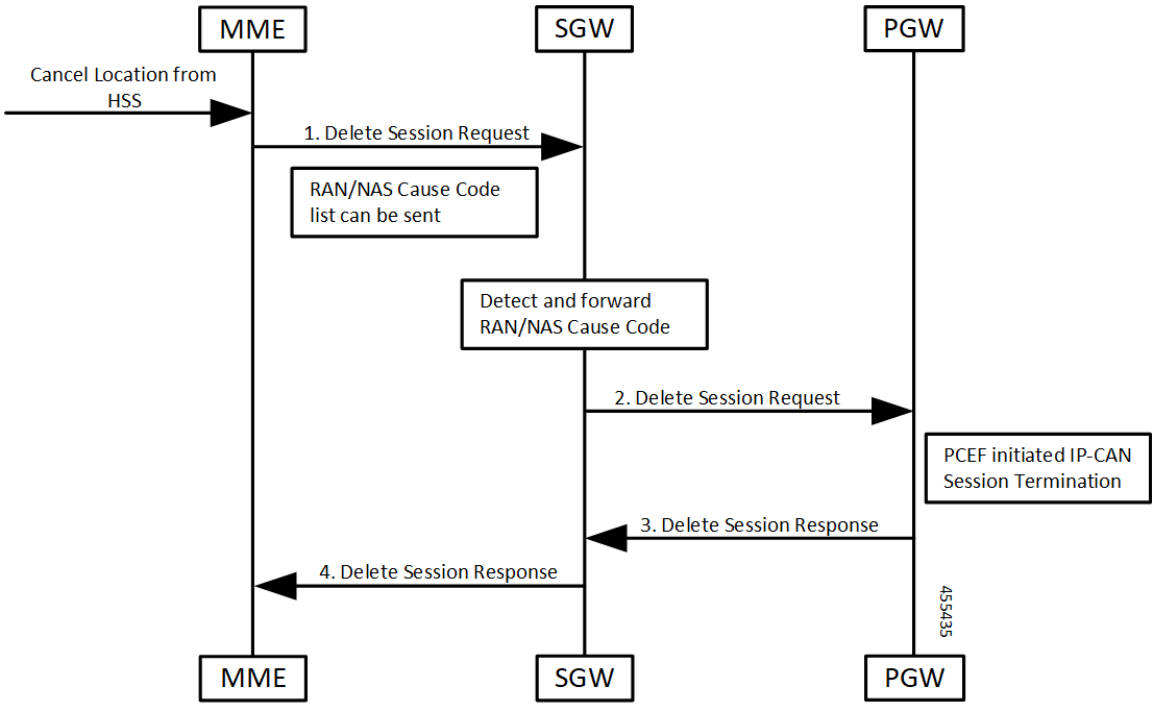
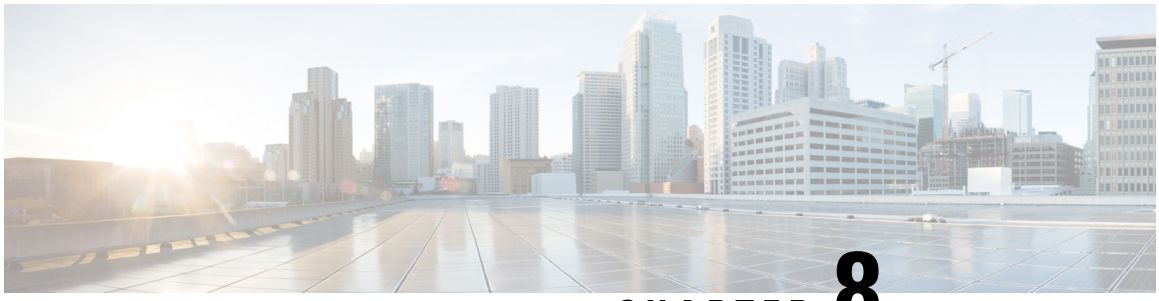


Table 20: Delete Session Procedure Call Flow Description

Step	Description
1	MME receives an indication of Cancel Location from HSS. MME creates Delete Session Request message to SGW (cnSGW-C). It includes RAN/NAS cause code list.
2	SGW (cnSGW-C) forwards the Delete Session Request message request to PGW. It detects and forwards RAN/NAS cause code list.

Step	Description
3	PGW sends the Delete Session Response message to SGW (cnSGW-C). PGW receives IP-CAN session modification request from PCEF.
4	SGW (cnSGW-C) generates a Delete Session Response message towards MME.



CHAPTER 8

Access Bearer Release Support

Feature Summary and Revision History

Summary Data

Table 21: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 22: Revision History

Revision Details	Release
First introduced.	2020.03.0

Feature Description

cnSGW-C supports the handling of the Release Access Bearer (RAB) request procedure. It's a UE-level message. In multiple PDN scenarios, the MME sends only one RAB message, which applies to all the PDNs.

cnSGW-C brings all the bearers of all the PDNs to the IDLE state.

How it Works

This section describes how this feature works.

cnSGW-C sends the Sx Modification Request message per PDN to the corresponding User Plane. After receiving the Sx Modification response message from all user planes (for all PDNs), cnSGW-C sends the response message to MME.

cnSGW-C updates the state as IDLE for all the bearers in CDL.

Call Flows

This section describes the key call flow for the Access Bearer Release Support feature.

Release Access Bearer (Active to IDLE Transaction) Call Flow

This section describes the Release Access Bearer call flow.

Figure 18: Release Access Bearer (Active to IDLE Transaction) Call Flow

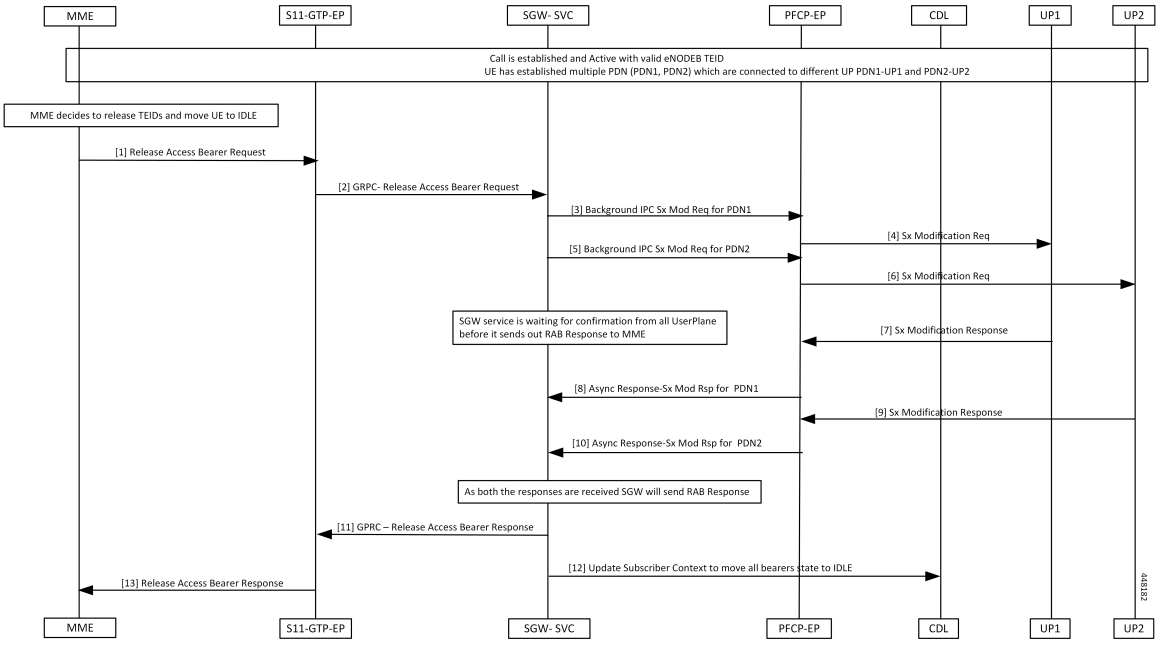
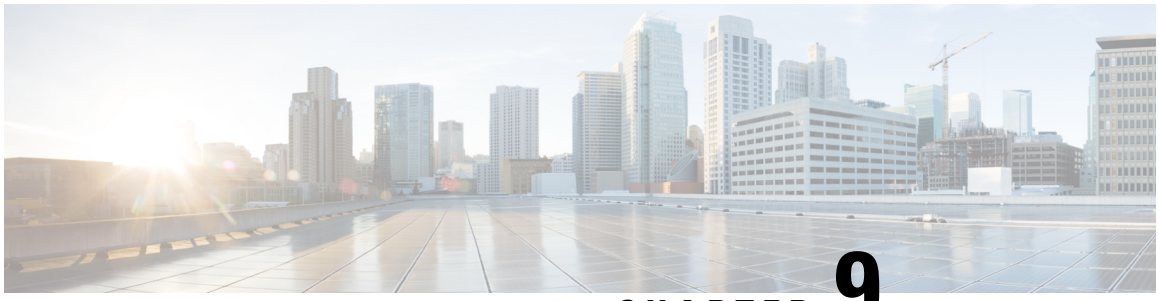


Table 23: Release Access Bearer (Active to IDLE Transaction) Call Flow Description

Step	Description
1	MME sends Release Access Bearer (RAB) request to S11-GTP-EP to release all S1-U bearers for the UE.

Step	Description
2	S11-GTP EP decodes the received UDP message and converts it into gRPC. The converted gRPC message then sent to the SGW-Service pod, using the TEID value, which can handle this UE session. SGW-Service pod performs the following activities: • Finds out Subscriber Context using local ingress TEID • Validates the RAB request content • Moves UE to the IDLE state • Builds the Sx Modify request message with the downlink apply action as DROP, to drop all downlink packets at SGW-U
3	SGW-Service pod sends the Sx Mod request message using the background IPC async call for PDN1 to PFCP-EP.
4	PFCP-EP forwards the Sx Modify Request (PDN1) message to UPF1 through the UDP proxy. UPF1 processes the Sx Modify Request (PDN1) message.
5	SGW-Service pod sends the Sx Modify Request message using the background IPC async call for PDN2. PFCP-EP forwards the Sx Modify Request (PDN2) message to UPF2 through the UDP proxy.
6	UPF2 processes the Sx Modify Request (PDN2) message.
7	UPF1 sends the Sx Modify response (PDN1) message to PFCP-EP.
8	PFCP-EP sends the Async Sx Modify response message to cnSGW-C service for PDN1. SGW-Service pod waits for the PDN2 Sx Modify response message.
9	UPF2 sends the Sx Modify response (PDN2) message to PFCP-EP.
10	PFCP-EP sends the Async Sx Modify response message to cnSGW-C service for PDN2.
11	The SGW-Service pod sends the following, after receiving the PDN (PDN1, PDN2) responses: • RAB response message to S11-GTP-EP using the gRPC protocol. • Updates to the CDL module
12	SGW-Service pod sends Update Subscriber Context state to CDL, which moves all the bearers to the IDLE state. CDL module updates the information in the database.
13	S11-GTP-EP forwards the RAB response message to MME. MME process the RAB response message.



CHAPTER 9

APN Profile Support

Feature Summary and Revision History

Summary Data

Table 24: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Configuration Required
Related Documentation	Not Applicable

Revision History

Table 25: Revision History

Revision Details	Release
First introduced.	2021.01.0

Feature Description

This feature supports Access Point Name (APN) or Data Network Name (DNN) profile for the SGW (cnSGW-C) service. DNN is equivalent to APN in Evolved Packet System (EPS).

Using the Operator Policy and the Subscriber map, you can determine the DNN Profile for the cnSGW-C service.

Feature Configuration

Configuring this feature involves the following steps:

- Configure DNN Profile. For more information, refer to Configuring DNN Profile, on page 96.
- Configure Network Element Profile. For more information, refer to Configuring Network Element Profile, on page 96.

Configuring DNN Profile

To configure this feature, use the following configuration:

```
config
  profile dnn dnn_name
    upf-selection-policy upf_select_name
      dnn dnn_name network-function-list network_function_list
      end
```

NOTES:

- **dnn** *dnn_name*—Specify the DNN profile name. Must be a string.
- **upf-selection-policy** *upf_select_name*—Specify the UPF selection policy name. Must be a string.
- **network-function-list** *network_function_list*—Specify the list of network functions to which the selected DNN profile is sent. Must be a string.

Configuring Network Element Profile

Network element profile represents peer IP (UPF) profile and has the following configurations:

- Peer address and Port configuration
- Peer-supported DNNs or APNs. This configuration helps in UPF selection.

UPF selection considers priority and capacity parameters.

upf-group-profile indicates the UPF group to which it belongs.

To configure this feature, use the following configuration:

```
config
  profile network-element upf upf_name
    node-id  node_id_value

    n4-peer-address ipv4 ipv4_address
    n4-peer-port port_number

    dnn-list dnn_list
    capacity capacity_value
```

```
priority priority_value
upf-group-profile upf_group_name
end
```

NOTES:

- **network-element**—Specify the peer network element.
- **upf** *upf_name*—Specify the UPF peer name.
- **node-id** *node_id_value*—Specify the Node ID of the UPF node.
-
-
-
- **dnn-list** *dnn_list*—Specify the DNN list supported by UPF node.
- **capacity** *capacity_value*—Specify the capacity relative to other UPFs. This is used for load balancing. Must be an integer in the range of 0-65535. Default value is 10.
- **priority** *priority_value*—Specify the static priority relative to other UPFs. This is used for load balancing. Must be an integer in the range of 0-65535. Default value is 1.
- **upf-group-profile** *upf_group_name*—Specify the UPF group profile name. Must be a string.

Configuration Modification Impact

The following table indicates the impact or the configuration change behavior on an existing call, a new PDN, or a new subscriber.

Modification	cnSGW-C Existing Call	cnSGW-C New PDN or New subscriber
Delete the apn-profile	No impact	Applied new configuration based on the changes for the following: • subscriber policy • operator policy • dnn policy • dnn profile
Modify the apn profile name in the operator policy	No impact	Applied new configuration based on the changes for the following: • subscriber policy • operator policy • dnn policy • dnn profile

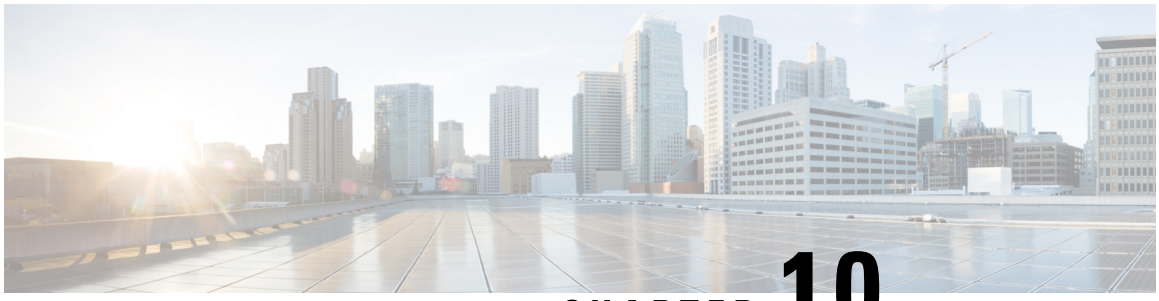
Troubleshooting Information

This section describes troubleshooting information for this feature.

Configuration Errors

This section describes the errors that cnSGW-C might report during the APN profile configuration.

```
show config-error | tab
ERROR COMPONENT   ERROR DESCRIPTION
--------------------------------------------------------------------------------------------------
SGWProfile        Subscriber policy name : sub_policy in profile sgw1 is not configured
SubscriberPolicy  Operator policy : op_policy1 under subscriber policy sub_policy2 is not
configured
OperatorPolicy    Dnn policy name : dnn_policy1 in operator policy op_policy2 is not
configured
DnnPolicy        Dnn profile name : dnn_profile1 in dnn policy dnn_policy2 is not configured
DnnProfile        UPF selection policy name : upf_sel_policy1 in dnn profile dnn_profile2
is not configured
```



CHAPTER 10

Change Notification Request Handling

Feature Summary and Revision History

Summary Data

Table 26: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 27: Revision History

Revision Details	Release
First introduced.	2021.02.0

Feature Description

A change notification message is initiated in cnSGW-C to indicate modifications for the User Location Information (ULI) and User CSG Information (UCI) updates. If these updates are valid, the cnSGW-C CDR is initiated. The change notifications may contain the secondary RAT usage IE which is specific to the

cnSGW-C and the ISGW. The cnSGW-C saves the RAT usage information and transmits the usage information in the subsequent CDR message.

Standards Compliance

This feature complies with the following standards specifications:

- *3GPP TS 29.274 "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3"*

How it Works

This section describes how this feature works.

The cnSGW-C network function handles the change notification request using the following approach:

- If the ULI or the UCI changes are valid in the connection request (CNREQ), the associated packet data network (PDN) is updated.
- cnSGW-C initiates a Query URR to get the latest usage information and generates cnSGW-C CDR when:
  - ULI is modified.
  - Charging and ULI trigger is enabled.

For information on configuring charging, see SGW Charging Support chapter.

Call Flows

This section describes the key call flow for this feature.

Change Notification Request Call Flow

This section describes the change notification request and the response call flow.

Figure 19: Change Notification Request Call Flow

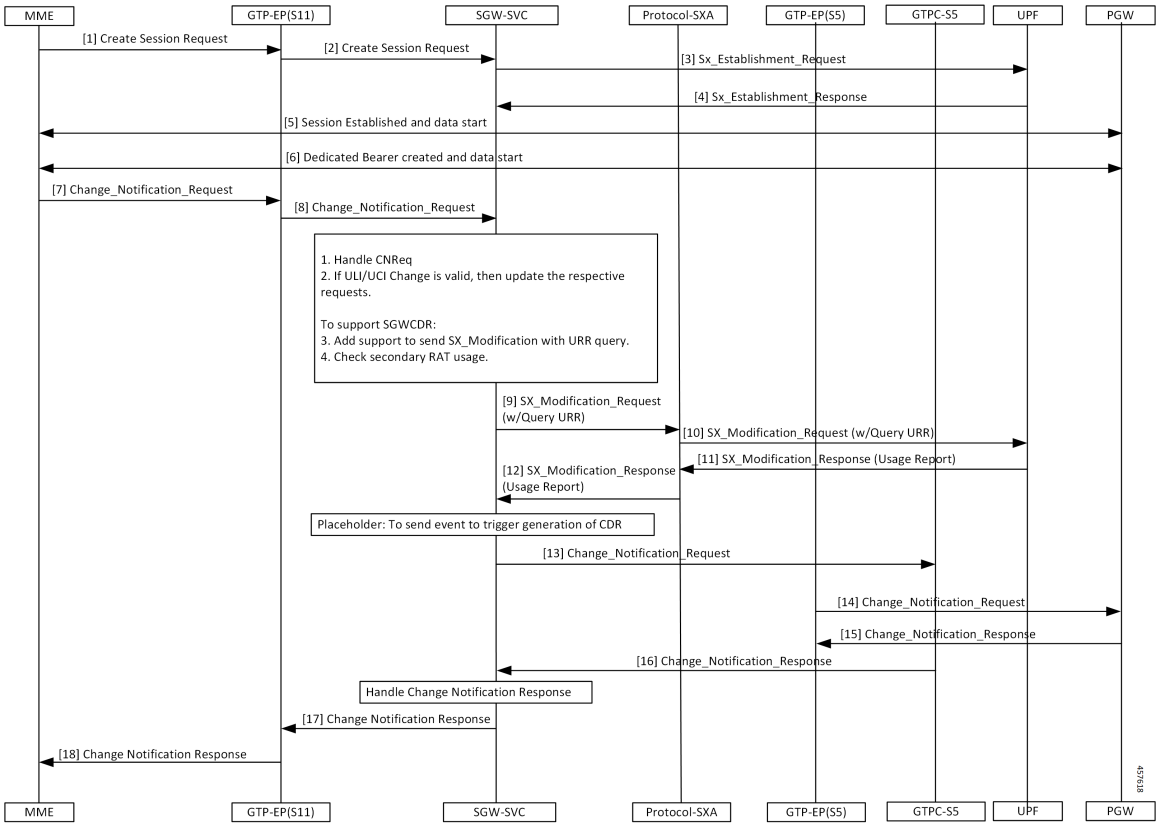


Table 28: Change Notification Request Call Flow Description

Step	Description
1	The MME sends a Create Session Request towards GTP-EP(S11).
2	The GTP-EP(S11) forwards the Create Session Request to the SGW-SVC.
3	The SGW-SVC sends the Sx Establishment Request to the UPF.
4	The UPF responds to the request with the SX Establishment Response directed towards the SGW-SVC.
5	The MME and the PGW establish the sessions and start exchanging data.
6	The MME and the PGW create the dedicated bearer and start exchanging data.
7	The MME sends the Change Notification Request to the GTP-EP.
8	The GTP-EP forwards the Change Notification Request to the SGW-SVC. If ULI or UCI changes are valid in the connection request (CNREQ), the PDN is updated. The GTP-EP sends the Sx Modification Request with the URR query after checking the secondary RAT usage.

Step	Description
9	The SGW-SVC sends the Sx Modification Request with the URR query to the Proto-SXA.
10	The Proto-SXA forwards the Sx Modification Request with the URR query to the UPF.
11	The UPF responds to the request with the Sx Modification Response, with the usage report to the Proto-SXA.
12	The Proto-SXA forwards the Sx Modification Response with the usage report to the SGW-SVC.
13	The SGW-SVC sends the Change Notification Request to the GTPC-S5.
14	The GTPC-S5 forwards the Change Notification Request to the PGW.
15	The PGW responds with the Change Notification Response to the GTPC-S5.
16	The GTPC-S5 forwards the Change Notification Response to the SGW-SVC.
17	The SGW-SVC sends the Change Notification Response to the GTP-EP(S11).
18	The GTP-EP(S11) forwards the Change Notification Response to the MME.

OAM Support

This section describes operations, administration, and maintenance information for this feature.

Bulk Statistics Support

The change notification filter displays the status of the change requests for which the notification is invoked. The following are the sample statistics and are provided for reference purposes only.

```
sgw_service_stats{app_name="smf",cluster="Local",data_center="DC",fail_reason="",
instance_id="0",interface="interface_sgw_egress",reject_cause="",service_name="sgw-service",
sgw_procedure_type="change_notification",status="attempted",sub_fail_reason=""}
1
```

```
sgw_service_stats{app_name="smf",cluster="Local",data_center="DC",fail_reason="",
instance_id="0",interface="interface_sgw_egress",reject_cause="",service_name="sgw-service",
sgw_procedure_type="change_notification",status="success",sub_fail_reason=""} 1
```

```
sgw_service_stats{app_name="smf",cluster="Local",data_center="DC",fail_reason="",
instance_id="0",interface="interface_sgw_egress",reject_cause="",service_name="sgw-service",
sgw_procedure_type="initial_attach",status="attempted",sub_fail_reason=""} 1
```

```
sgw_service_stats{app_name="smf",cluster="Local",data_center="DC",fail_reason="",
instance_id="0",interface="interface_sgw_egress",reject_cause="",service_name="sgw-service",
sgw_procedure_type="initial_attach",status="success",sub_fail_reason=""} 1
```

```
sgw_service_stats{app_name="smf",cluster="Local",data_center="DC",fail_reason="",
instance_id="0",interface="interface_sgw_ingress",reject_cause="",service_name="sgw-service",
sgw_procedure_type="change_notification",status="attempted",sub_fail_reason=""}
1
```

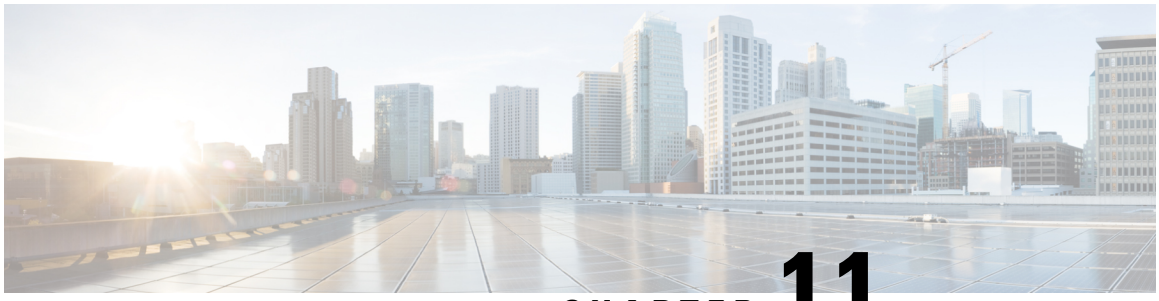
```
sgw_service_stats{app_name="smf",cluster="Local",data_center="DC",fail_reason="",
instance_id="0",interface="interface_sgw_ingress",reject_cause="",service_name="sgw-service",
sgw_procedure_type="change_notification",status="success",sub_fail_reason=""} 1
```

```
sgw_service_stats{app_name="smf",cluster="Local",data_center="DC",fail_reason="",
instance_id="0",interface="interface_sgw_ingress",reject_cause="",service_name="sgw-service",
sgw_procedure_type="initial_attach",status="attempted",sub_fail_reason=""} 1
```

```
sgw_service_stats{app_name="smf",cluster="Local",data_center="DC",fail_reason="",
instance_id="0",interface="interface_sgw_ingress",reject_cause="",service_name="sgw-service",
sgw_procedure_type="initial_attach",status="success",sub_fail_reason=""} 1
```

```
sgw_service_stats{app_name="smf",cluster="Local",data_center="DC",fail_reason="",
instance_id="0",interface="interface_sgw_ingress",reject_cause="",service_name="sgw-service",
sgw_procedure_type="modify_bearer_req_initial_attach",status="attempted",sub_fail_reason=""}
 1
```

```
sgw_service_stats{app_name="smf",cluster="Local",data_center="DC",fail_reason="",
instance_id="0",interface="interface_sgw_ingress",reject_cause="",service_name="sgw-service"
,sgw_procedure_type="modify_bearer_req_initial_attach",status="success",sub_fail_reason=""}
 1
```



CHAPTER 11

Clear Subscriber Request

Feature Summary and Revision History

Summary Data

Table 29: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 30: Revision History

Revision Details	Release
First introduced.	2020.04

Feature Description

cnSGW-C handles the Clear Subscriber or the PDN Request from the Ops Center.

The Clear Subscriber Request initiates the administrative clearing of subscribers for a specific IMSI or all IMSIs using the local purge and remote signaling procedures.

Based on the OAM query, the cnSGW-C receives the Subscriber Notification message at REST-EP and triggers the Clear Subscriber Request message towards the SGW-Service.

Standards Compliance

This feature complies with the following standards specifications:

- *3GPP TS 23.401 "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access"*
- *3GPP TS 23.214 "Architecture enhancements for control and user plane separation of EPC nodes"*
- *3GPP TS 29.274 "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3"*
- *3GPP TS 29.244 "Interface between the Control Plane and the User Plane nodes"*

How it Works

This section describes how this feature works.

When the cnSGW-C receives the admin-initiated Deletion Request with the purge option as “true”, it initiates Sx signaling towards User Plane and exchanges following messages:

1. SGW sends a Sx Session Deletion Request to User Plane.
2. User Plane sends a Sx Session Deletion Response SGW.

When cnSGW-C receives the Deletion Request with the purge option as “false”, it performs the Sx signaling towards User Plane and GTP-C signaling towards MME and PGW. The cnSGW-C exchanges the following messages with User Plane, MME, and PGW:

1. SGW sends the Sx Session Modification Request to the User Plane.
2. User Plane sends the Sx Session Modification Response to SGW.
3. SGW sends the Delete Bearer Request to MME.
4. SGW sends the Delete Session Request to PGW.
5. MME sends the Delete Bearer Response to SGW.
6. PGW sends the Delete Session Response to SGW.
7. SGW sends the Sx Session Deletion Request to User Plane.
8. User Plane sends the Sx Session Deletion Response to SGW.

cnSGW-C sends the Delete Session Request towards PGW and Delete Bearer Request towards MME. After receiving the response from both remote peers, the cnSGW-C sends Sx Session Deletion Request towards User Plane to clear the sessions.

Supported Clear Command

cnSGW-C supports the following clear commands:

Table 31: Supported Clear Commands

Supported Clear Command Options	GTP-C Signalling (Towards MME/PGW)	Sx Signalling (Towards UP)	Impact (Subscriber/PDN)
clear sub all **clear sub all purge false**	Yes	Yes	All subscribers
clear sub all purge true	No	Yes	All subscribers
• **clear sub namespace sgw imsi** *imsi_val* • **clear sub namespace sgw imsi***imsi_val***purge false**	Yes	Yes	Subscriber with IMSI as *imsi_val*
clear sub namespace sgw imsi*imsi_val***purge true**	No	Yes	Subscriber with IMSI as *imsi_val*
clear sub namespace sgw imsi*imsi_val***ebi***ebi_value*	Yes	Yes	PDN with IMSI as *imsi_val* and default ebi as *ebi_value*

Call Flows

This section describes the key call flows for this feature.

Clear PDN Call Flow

This section describes the Clear PDN call flow.

Figure 20: Clear PDN Call Flow

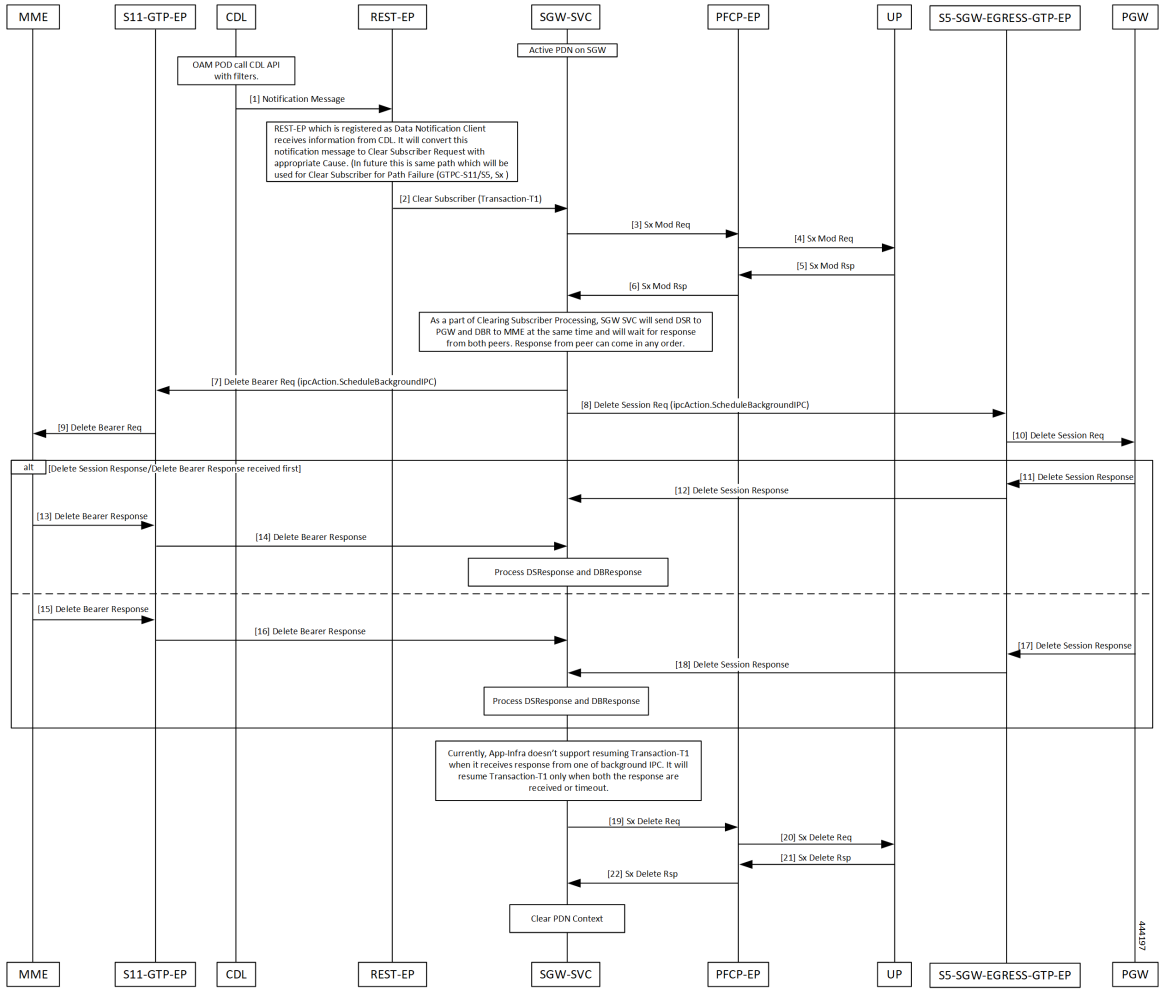
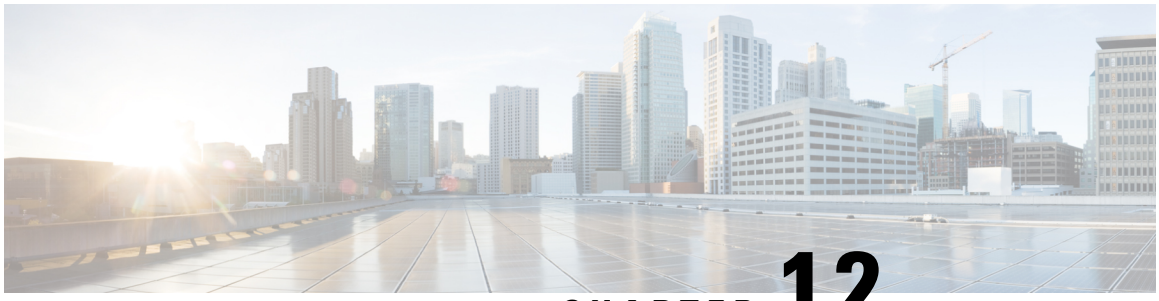


Table 32: Clear PDN Call Flow Description

Step	Description
1	The OAM pod calls the CDL API with the filters. CDL sends the notification message to REST EP.
2	The REST-EP converts this message to Clear Subscriber Request with a cause and sends Clear Subscriber to the SGW-Service pod. Transaction-T1 started.
3-6	The SGW-Service pod sends Sx Modification Request to UPF through PFCP-EP. The SGW-Service pod receives Sx Modification Response from UPF through PFCP-EP.
7	The SGW-Service pod sends the Delete Bearer Request to the S11-GTP-EP.
8	The SGW-Service pod sends the Delete Session Request to the S5-SGW-EGRESS-GTP-EP.

Step	Description
9	The S11-GTP-EP sends the Delete Bearer Request to MME.
10-12	The S5-SGW-EGRESS-GTP-EP sends the Delete Session Request to PGW. The PGW sends the Delete Session Response to S5-SGW-EGRESS-GTP-EP. The S5-SGW-EGRESS-GTP-EP forwards this request to the SGW-Service pod.
13-16	MME sends the Delete Bearer Response to S11-GTP-EP. S11-GTP-EP forwards to the SGW-Service pod.
17, 18	PGW sends the Delete Session Response to S5-SGW-EGRESS-GTP-EP. S5-SGW-EGRESS-GTP-EP forwards this request to the SGW-Service pod.
19-22	The SGW-Service pod sends the Sx Delete Request to PFCP-EP. The PFCP-EP forwards the request to UPF. UPF sends the Sx Delete Response to PFCP-EP, which it forwards it to the SGW-Service pod.



CHAPTER 12

Context Replacement Support

Feature Summary and Revision History

Summary Data

Table 33: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 34: Revision History

Revision Details	Release
Introduced support for partial context replacement.	2021.02.0
First introduced.	2020.01.0

Feature Description

The cnSGW-C supports context replacement when it receives Create Session Request (CSReq) with the existing EBI. When the MME node and cnSGW-C are not synchronized, the session gets locally terminated on the MME. The MME sends a CSReq with the EBI that is already present in the cnSGW-C. If the CSReq contains a TEID with value as non-ZERO, then cnSGW-C partially replaces the context. When TEID is zero, cnSGW-C performs full context replacement.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

Full Context Replacement Call Flow

This section describes the full context replacement call flow.

Create Session Request Call Flow

This section describes the Create Session Request call flow.

Figure 21: Create Session Request (Context Replacement – Single or Multi-PDN subscriber) Call Flow

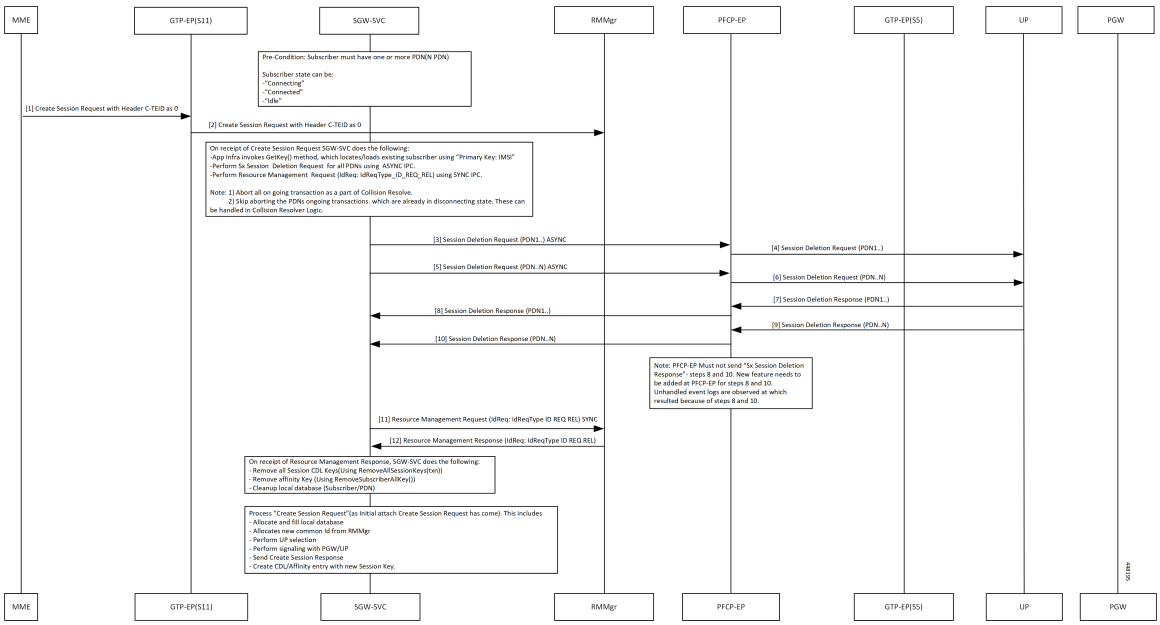


Table 35: Create Session Request (Context Replacement – Single or Multi-PDN subscriber) Call Flow Description

Step	Description
1	MME sends Create Session Request with C-TEID as zero to GTPC-EP ingress.
2	GTPC-EP ingress forwards the Create Session Request to SGW-SVC. Following actions takes place: • App Infra invokes the GetKey() method, which locates and loads the existing subscribers using Primary Key: IMSI. • Performs Sx Session Deletion Request for all PDNs using ASYNC IPC • Performs Resource Management Request (IdReq: IdReqType_ID_REQ_REL) using SYNC IPC
3, 5	The SGW service pod sends the Delete Session Request for PDN 1 - N to PFCP-EP.
4, 6	PFCP-EP forwards Delete Session Request for PDN 1 - N to UPF.
7, 9	PFCP-EP receives Delete Session Response for PDN 1 to N from UPF.
8, 10	PFCP-EP forwards Delete Session Response for PDN 1 - N to SGW service pod.
11	SGW service pod sends Resource Management Request to RMMgr with request ID-type as Request REL.
12	SGW service pod receives Resource Management Response from RMMgr with Req ID-type as REQ REL. The SGW service pod performs following: • Removes all session CDL keys (Using RemoveAllSessionKeys(txn)) • Removes affinity Key (Using RemoveSubscriberAllKey()) • Cleans up the local database (Subscriber/PDN)

Note You can ignore unhandled events for the Deletion Response from UPF.

Partial Context Replacement Call Flow

This section describes the partial context replacement call flow.

When cnSGW-C receives a CSReq with the existing EBI and TEID as non-ZERO, then cnSGW-C performs a partial context replacement by invoking the following call flows:

- EBI received in CSReq is for the existing default bearer.
- EBI received in CSReq is for the existing dedicated bearer.

Create Session Request with Default Bearer EBI Call Flow

This section describes the Create Session Request with Default Bearer EBI call flow.

Figure 22: CSReq with Default Bearer EBI Call Flow

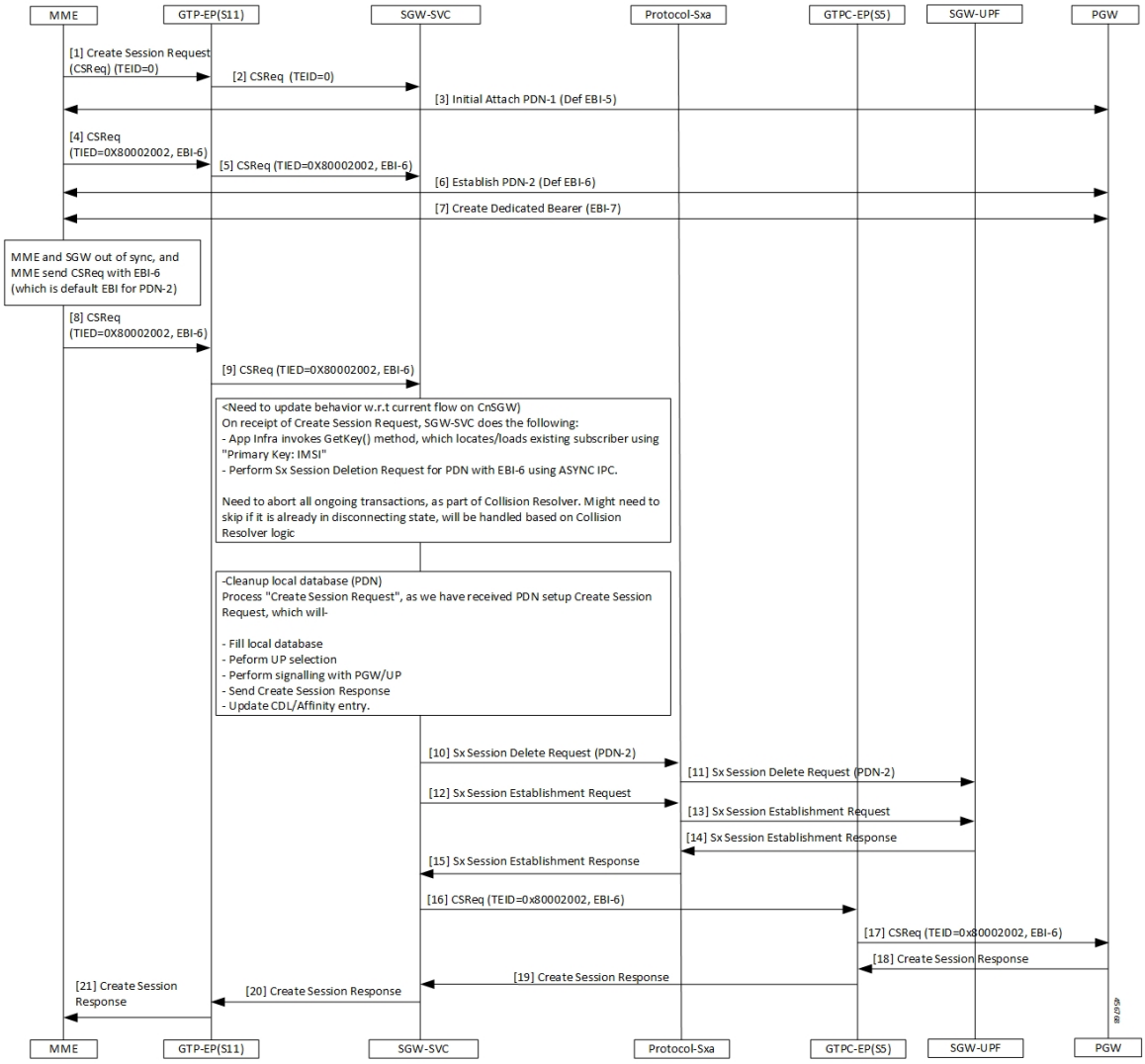


Table 36: CSReq with Default Bearer EBI Call Flow Description

Step	Description
1	The MME sends a Create Session Request with TIED value as 0 to the GTPC-EP(S11).
2	The GTPC-EP(S11) forwards the Create Session Request with TIED value as 0 to the SGW-SVC.
3	The MME and the PGW process the Initial Attach PDN-1 with the default EBI-5 process.
4	The MME sends a Create Session Request TIED=0x80002002 with EBI-6 to the GTPC-EP.

Step	Description
5	The GTPC-EP forwards the Create Session Request TIED=0x80002002 with EBI-6 to the SGW-SVC.
6	The MME and the PGW establish the PDN-2 with default EBI-6 connection.
7	The MME and PGW complete the Create Dedicated Bearer with EBI-7 process.
8	If the SGW and MME are not in sync, the MME sends a Create Session Request with EBI-6 present in the SGW.
9	The GTPC-EP sends a CSReq TIED= 0x80002002 with EBI-6 to SGW.
10	After receiving the Create Session Request, the SGW-SVC performs the following- • Cleans up the PDN with default EBI=6. • Sends the Sx signalling to UPF to clear the session. • Performs the Create Session Request as a new PDN-Setup. The SGW sends an Sx Session Delete Request on PDN-2 to Protocol-SXA.
11	The Protocol-SXA forwards a Sx Session Delete Request to SGW-UPF.
12	The SGW sends a Session Establishment Request to the Protocol-SXA.
13	The Protocol-SXA forwards a Sx Session Establishment Request to SGW-UPF.
14	The SGW-UPF responds to the Protocol-SXA with the Sx Session Establishment Response.
15	The Protocol-SXA sends the Sx Session Establishment Response to the SGW-SVC.
16	The SGW-SVC sends the Create Session Request TIED= 0x80002002 with EBI-6 to the GTPC-EP.
17	The GTPC-EP sends the Create Session Request TIED= 0x80002002 with EBI-6 to the PGW.
18	The PGW sends a Create Session Response to the GTPC-EP.
19	The GTPC-EP responds to the SGW-SVC with the Create Session Response.
20	The SGW-SVC forwards the response to the GTPC-EP.
21	The GTPC-EP sends the Create Session Response to the MME.

Create Session Request with Dedicated Bearer EBI Call Flow

This section describes the Create Session Request with the Dedicated EBI call flow.

Figure 23: CSReq with Dedicated Bearer EBI Call Flow

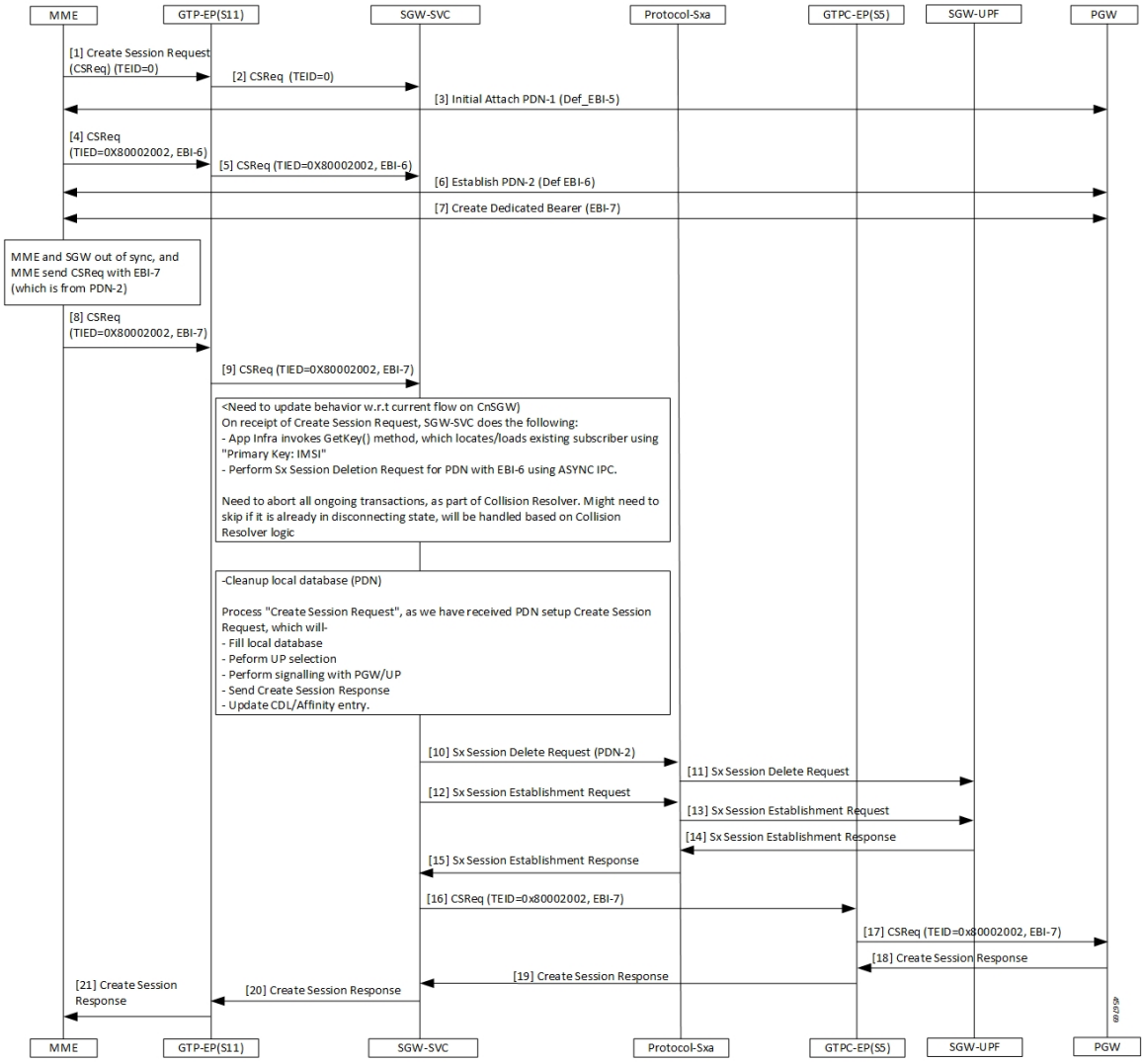


Table 37: CSReq with Dedicated Bearer EBI Call Flow Description

Step	Description
1	The MME sends a Create Session Request with the TIED value as zero to the GTPC-EP(S11).
2	The GTPC-EP(S11) forwards the Create Session Request with TIED value as zero to the SGW-SVC.
3	The MME and the PGW process the Initial Attach PDN with the EBI-5 process.
4	The MME sends the Create Session Request with EBI-6 to the GTPC-EP.
5	The GTPC-EP forwards the Create Session Request with EBI-6 to the SGW-SVC.
6	The MME and PGW establish the PDN with the EBI-6 connection.

Step	Description
7	The MME and PGW complete the Create Dedicated Bearer with EBI-7 process.
8	If the SGW and MME are not in sync, then MME sends a Create Session Request with EBI-6 present in SGW.
9	The GTPC-EP sends a CSReq with EBI-7 to SGW.
10	After receiving the Create Session Request, the SGW-SVC: • Cleans up the PDN with default EBI=6. • Sends the Sx signalling to UPF to clear the session. • Performs the Create Session Request as new PDN-Setup. The SGW sends a Sx Session Delete Request on PDN-2 to Protocol-SXA.
11	The Protocol-SXA forwards the Sx Session Delete Request to SGW-UPF.
12	The SGW sends a Session Establishment Request to the Protocol-SXA.
13	The Protocol-SXA forwards a Sx Session Establishment Request to SGW-UPF.
14	The SGW-UPF responds to the Protocol-SXA with the Sx Session Establishment Response.
15	The Protocol-SXA sends the Sx Session Establishment Response to the SGW-SVC.
16	The SGW-SVC sends the Create Session Request containing TIED=0x80002002, EBI-7 to the GTPC-EP.
17	The GTPC-EP sends the Create Session Request containing TIED=0x80002002, EBI-7 to the PGW.
18	The PGW sends a Create Session Response to the GTPC-EP.
19	The GTPC-EP responds to the SGW-SVC with the Create Session Response.
20	The SGW-SVC forwards the response to the GTPC-EP.
21	The GTPC-EP sends the Create Session Response to the MME.

OAM Support

This section describes operations, administration, and maintenance support for this feature.

Bulk Statistics

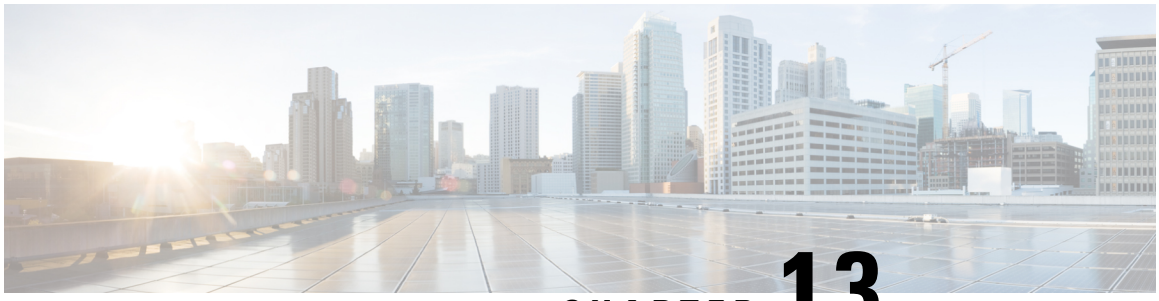
The following statistics are supported for the partial context replacement feature.

- sgw_pdn_disconnect_stats: Captures the total number of SGW PDN in the disconnected status.

  An example of the Prometheus query:

```
sgw_pdn_disconnect_stats{app_name="smf",cluster="cn",data_center=\

"cn",instance_id="0",pdn_type="ipv4",rat_type="EUTRAN",reason="context_replacement",\
service_name="sgw-service"} 1
```



CHAPTER 13

Dedicated Bearer Support

Feature Summary and Revision History

Summary Data

Table 38: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 39: Revision History

Revision Details	Release
First introduced.	2021.01.0

Feature Description

Setup and Update Dedicated Bearers

cnSGW-C supports creating and updating single/multiple dedicated bearers.

Delete Dedicated Bearers

cnSGW-C supports deletion of single/multiple dedicated bearers.

Setup and Update Dedicated Bearers

Feature Description

cnSGW-C supports creating and updating dedicated bearers for both single and multiple PDN subscribers. It also supports multiple bearer contexts as part of single create bearer procedure.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

Dedicated Bearer Setup – Request Accepted Call Flow

This section describes the Dedicated Bearer Setup – Request Accepted call flow.

Figure 24: Dedicated Bearer Setup – Request Accepted Call Flow

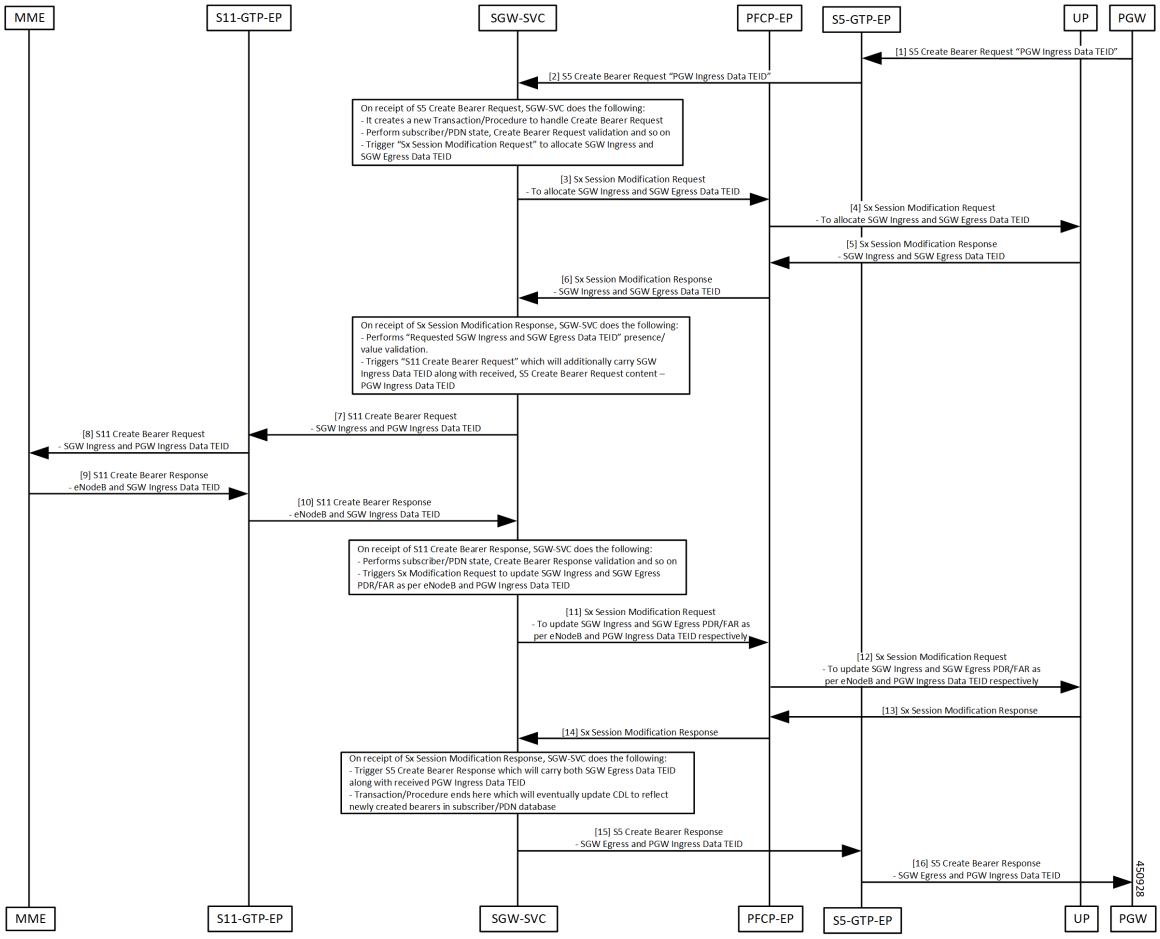


Table 40: Dedicated Bearer Setup – Request Accepted Call Flow Description

Step	Description
1	The PGW sends the S5 Create Bearer Request to the S5-GTPC-EP pod.
2	The S5-GTPC-EP pod forwards the S5 Create Bearer Request to the SGW-SVC pod.
3	The SGW-SVC receives the S5 Create Bearer request and performs the following: • Creates a new transaction • Performs GTP validations • Triggers the Sx Modification Request to the PFCP-EP pod
4	The PFCP-EP pod forwards the Sx Modification Request to the UP for allocating SGW Ingress and SGW Egress TEIDs.
5	The PFCP-EP pod receives the Sx Modification Response with SGW Ingress and SGW Egress TEIDs, from the UP.

Step	Description
6	The PFCP-EP pod forwards the Sx Modification Response with SGW Ingress and SGW Egress TEIDs, to the SGW-SVC.
7	The SGW-SVC receives the Sx Modification response and performs the following: • Validates the received SGW Ingress and SGW Egress TEIDs • Triggers the S11 Create Bearer Request with the SGW Ingress TEID to the S11-GTPC-EP pod
8	The S11-GTPC-EP pod forwards the S11 Create Bearer Request with the SGW Ingress TEID, to the MME.
9	The MME sends the S11 Create Bearer Response to the S11-GTPC-EP pod.
10	The S11-GTPC-EP pod forwards the S11 Create Bearer Response to the SGW-SVC.
11	The SGW-SVC receives the S11 Create Bearer response and performs the following: • GTP validations • Triggers the Sx Modification Request to the PFCP-EP pod to update SGW Ingress and SGW Egress PDR/FAR, with the MME and the PGW GTPU-TEID
12	The PFCP-EP pod forwards the Sx Modification Request to the UP.
13	The UP sends the Sx Modification Response to the PFCP-EP pod.
14	The PFCP-EP pod forwards the Sx Modification Response to the SGW-SVC pod.
15, 16	The SGW-SVC pod receives the Sx Modification Response and performs the following: • Ends the transaction/procedure • Updates the CDL • Sends the S5 Create Bearer Response with SGW Egress TEIDs with matching PGW GTPU TEIDs, and with the cause as Accepted.

Dedicated Bearer Setup – Request Accepted Partially Call Flow

This section describes the Dedicated Bearer set up call flow. In this procedure, the MME sends the Create Bearer Response with the GTP cause as Request Accepted Partially.

Prerequisite: Create Bearer Procedure with two bearer contexts.

Figure 25: Dedicated Bearer Setup – Request Accepted Partially Call Flow

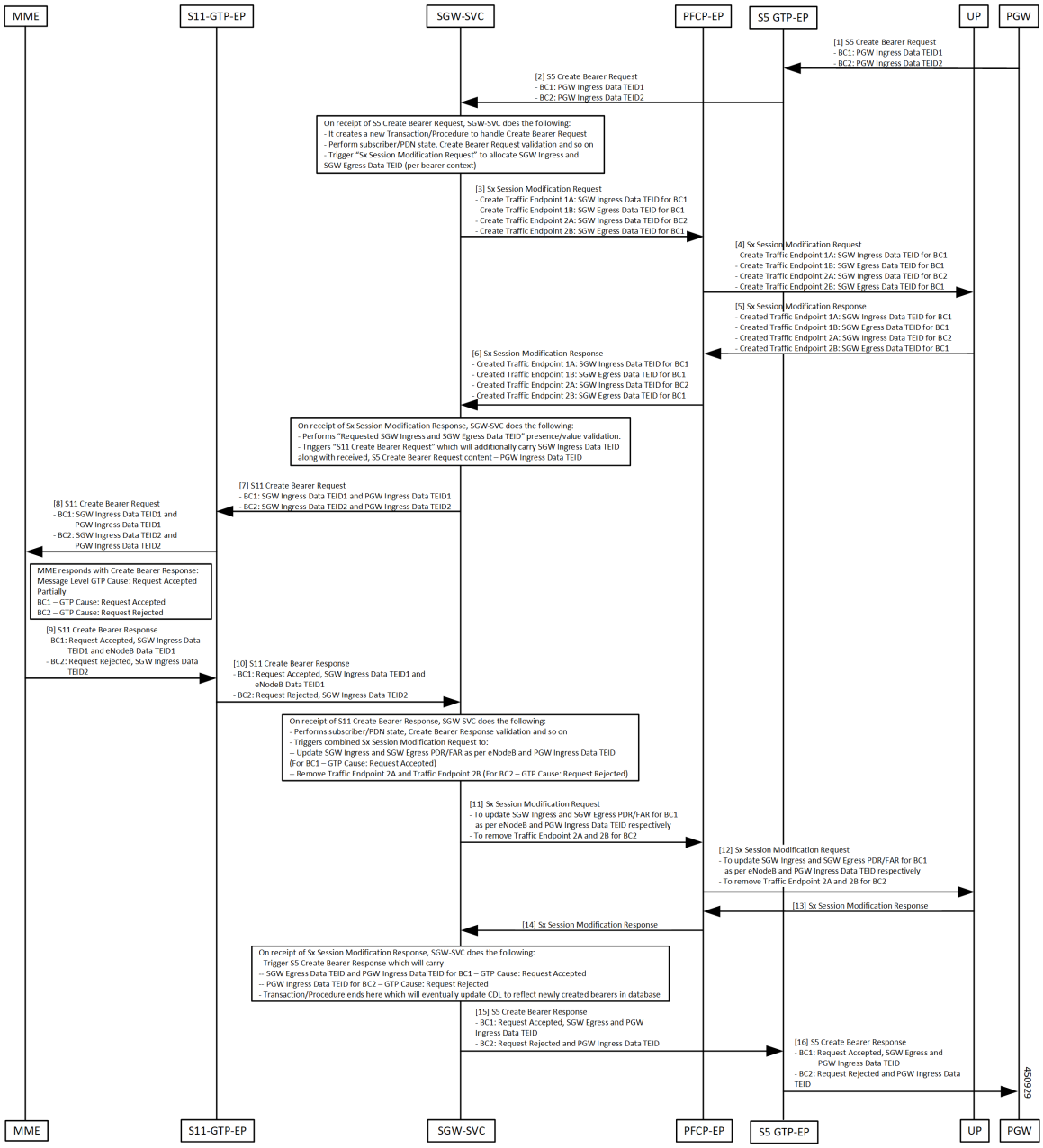


Table 41: Dedicated Bearer Setup – Request Accepted Partially Call Flow Description

Step	Description
1	The PGW sends the S5 Create Bearer Request with multiple bearer contexts to the S5-GTPC-EP pod.
2	The S5-GTPC-EP pod forwards the S5 Create Bearer Request to the SGW-SVC pod.

Step	Description
3	The SGW-SVC pod receives the S5 Create Bearer request and performs the following: • Creates a new transaction • Performs GTP validations • Triggers the Sx Modification Request to allocate SGW Ingress and SGW Egress TEIDs to the PFCP-EP pod.
4	The PFCP-EP pod forwards the Sx Modification Request to the UP.
5	The UP sends the Sx Modification Response to the PFCP-EP pod.
6	The PFCP-EP pod forwards the Sx Modification Response to the SGW-SVC pod.
7	The SGW-SVC receives the Sx Modification Response and performs the following: • Validates the received SGW Ingress and SGW Egress TEIDs • Triggers an S11 Create Bearer Request with the SGW Ingress TEID to the S11-GTPC-EP pod
8	The S11-GTPC-EP pod forwards the S11 Create Bearer Request to the MME.
9	The S11-GTPC-EP receives the S11 Create Bearer Response from the MME, with the Message Level GTP cause as Request Accepted Partially: • For some Bearer Contexts, GTP cause is Request Accepted • For some Bearer Contexts, GTP cause is Request Rejected
10	The S11-GTPC-EP pod forwards the S11 Create Bearer Response to the SGW-SVC pod.
11	The SGW-SVC pod receives the S11 Create Bearer response and performs the following: • GTP validations • For successful bearers: Triggers the Sx Modification Request to the PFCP-EP pod for updating SGW Ingress and SGW Egress PDR/FAR with the MME and the PGW GTPU-TEID • For failed bearers: Removes the traffic endpoints
12	The PFCP-EP pod forwards the Sx Modification Request to the UP.
13	The UP sends the Sx Modification Response to the PFCP-EP pod.
14	The PFCP-EP pod forwards the Sx Modification Response to the SGW-SVC pod.

Step	Description
15, 16	The SGW-SVC pod receives the Sx Modification Response and performs the following: • Ends the transaction/procedure • Updates the CDL • For successful bearers: Sends the S5 Create Bearer Response with SGW Egress TEIDs with matching PGW GTPU TEIDs. • For failed bearers: Sends the bearer contexts as is with the message level cause as Partially Accepted.

Dedicated Bearer Update – Request Accepted Call Flow

This section describes the Default/Dedicated Bearer Update Procedure call flow.

Single Update Bearer Procedure supports:

- Default bearer QoS/TFT change
- Single/Multiple dedicated bearer QoS/TFT change
- APN-AMBR change

Note The call flow doesn't contain Sx Communication Messages related to the Default/Dedicated Bearer Update procedure.

Figure 26: Default/Dedicated Bearer Update (Single/Multiple Bearers) Support Call Flow

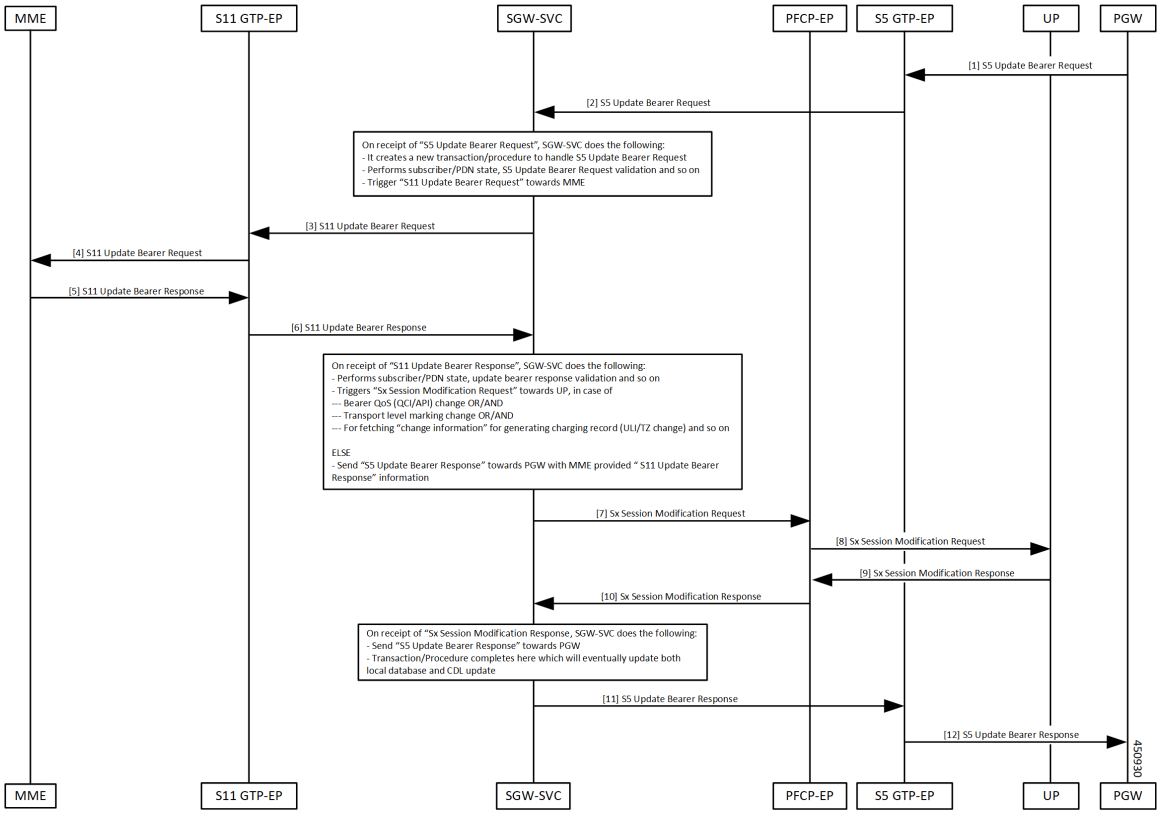


Table 42: Default/Dedicated Bearer Update (Single/Multiple Bearers) Support Call Flow Description

Step	Description
1	The PGW sends the S5 Update Bearer Request with multiple bearer contexts to the GTPC-EP pod.
2	The GTPC-EP pod forwards the S5 Update Bearer request to the SGW-SVC pod.
3	SGW-SVC receives the S5 Update Bearer request and performs the following: • Creates a new transaction • Performs GTP validations • Triggers the S11 Update Bearer Request to the GTPC-EP pod
4	The GTPC-EP pod forwards the S11 Update Bearer Request to the MME.
5	The MME sends the S11 Update Bearer Response to the GTPC-EP pod.
6	The GTPC-EP pod forwards the S11 Update Bearer Response to the SGW-SVC pod.

Step	Description
7	SGW-SVC receives the S11 Update Bearer Response and performs GTP validations. • If: Any of the following is true, the SGW-SVC triggers Sx Modification Request to the PFCP-EP pod: • Bearer QoS (QCI/ARP) change • Transport Level Marking change • Fetch charging information for generating charging record ULI/TZ change • Else: The SGW-SVC sends the S11 Update Bearer Response to the PGW with the MME-provided S11 Update Bearer Response information.
8	The PFCP-EP pod forwards the Sx Session Modification Request to the UP.
9	The UP sends the Sx Session Modification Response to the PFCP-EP pod.
10	The PFCP-EP pod forwards the Sx Session Modification Response to the SGW-SVC. The SGW-SVC receives the Sx Modification Response and performs the following: • Ends the transaction/procedure • Updates the CDL • Sends the S5 Update Bearer Response with cause as Accepted
11	The SGW-SVC sends the S5 Update Bearer Response to the PFCP-EP pod. The PFCP-EP pod forwards the S5 Update Bearer Response to the GTP-EP pod.
12	The GTP-EP pod forwards the S5 Update Bearer Response to the UP. The UP forwards the S5 Update Bearer Response to the PGW.

Delete Dedicated Bearers

Feature Description

cnSGW-C supports single/multiple dedicated bearer deletion as part of single delete bearer procedure.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

Dedicated Bearer Deletion Procedure Call Flow

This section describes the Dedicated Bearer Delete Procedure call flow.

Figure 27: Dedicated Bearer Deletion Procedure (Single/Multiple Bearer) Call Flow

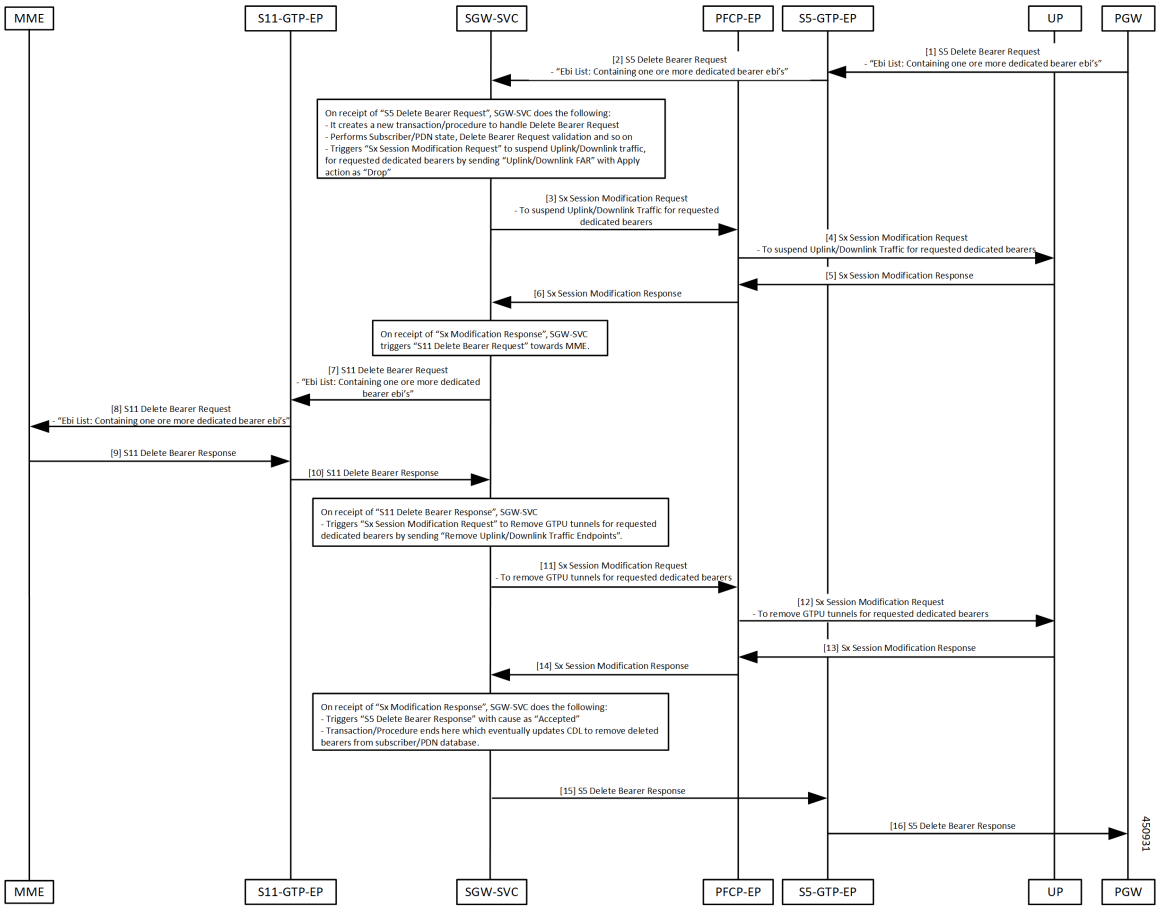
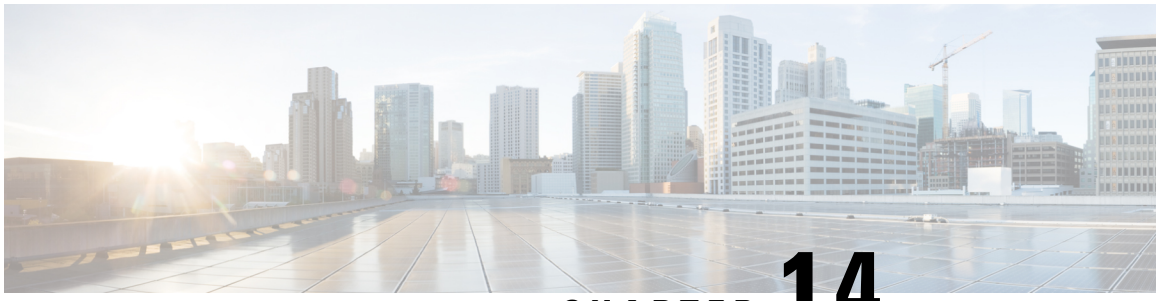


Table 43: Dedicated Bearer Deletion Procedure (Single/Multiple Bearer) Call Flow Description

Step	Description
1	The PGW sends the S5 Delete Bearer Request with EBI list containing one or more dedicated bearer EBIs, to the GTPC-EP pod.
2	The GTPC-EP pod forwards the S5 Delete Bearer Request to the SGW-SVC pod.
3	The SGW-SVC pod receives the S5 Delete Bearer request and performs the following: • Creates a new transaction • Performs GTP validations • Triggers the Sx Modification Request to the PFCP-EP pod to suspend uplink/downlink traffic for the requested bearers
4	The PFCP-EP pod forwards the Sx Modification Request to the UP.

Step	Description
5	The UP sends the Sx Modification Response to the PFCP-EP pod.
6	The PFCP-EP pod forwards the Sx Modification Response to the SGW-SVC pod.
7	The SGW-SVC pod receives the Sx Modification Response and triggers the S11 Delete Bearer Request to the GTPC-EP pod.
8	The GTPC-EP pod forwards the S11 Delete Bearer Request to the MME.
9	The MME sends the S11 Delete Bearer Response to the GTPC-EP pod.
10	The GTPC-EP pod forwards the S11 Delete Bearer Response to the SGW-SVC pod.
11	The SGW-SVC receives the S11 Delete Bearer Response and triggers the Sx Modification Request to the PFCP-EP pod, to remove traffic endpoints for removal of the GTPU tunnels for the requested dedicated bearers.
12	The PFCP-EP pod forwards the Sx Modification Request to the UP to remove GTP tunnels for the requested dedicated bearers.
13	The UP sends the Sx Modification Response to the PFCP-EP pod.
14	The PFCP-EP forwards the Sx Modification Response to the SGW-SVC pod.
15	The SGW-SVC receives the Sx Modification Response and performs the following: • Ends the transaction/procedure • Updates the CDL • Sends the S5 Delete Bearer Response with cause as Accepted, to the GTP-EP pod
16	The GTP-EP pod forwards the S5 Delete Bearer Response to the PGW.



CHAPTER 14

Delete Bearer and Delete Session Request

Feature Summary and Revision History

Summary Data

Table 44: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 45: Revision History

Revision Details	Release
First introduced.	2020.04

Feature Description

This feature supports the following:

- Deletion of Session Request from the MME
- Deletion of Bearer Request from the PGW

This deletion helps in clearing the PDN connection at the SGW, which in turn clears resources at the cnSGW-C, and releases all the relevant TEIDs.

Delete from MME

1. cnSGW-C sends the Sx Modification Request to the User Plane (UP) to mark the forwarding action as DROP so that all uplink or downlink packets are dropped at the SGW-U.
2. cnSGW-C sends the Delete Session Request to the PGW/SMF.
3. After SGW receives the Delete Session Response from the PGW/SMF, cnSGW-C sends the Sx Terminate Request to the UP to clear the session.
4. After UP confirms the deletion of the SGW-U session, cnSGW-C releases the allocated ID by sending request to the Node Manager, and the Delete Session Response to the MME.

Delete from PGW

1. cnSGW-C sends the Sx Modification Request to the UP to mark the forwarding action as DROP so that all the uplink and downlink packets are dropped at the SGW-U.
2. cnSGW-C sends the Delete Bearer Request to the MME.
3. After SGW receives the Delete Bearer Response from the MME, the cnSGW-C sends the Sx Terminate Request to the UP to clear the session.
4. After UP confirms the deletion of the SGW-U session, cnSGW-C releases the allocated ID by sending request to the Node Manager, and the Delete Bearer Response to the PGW.

Standard Compliance

The Delete Bearer and Delete Session Request Support feature complies with the following standards:

- *3GPP TS 23.401 "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access"*
- *3GPP TS 23.214 "Architecture enhancements for control and user plane separation of EPC nodes"*
- *3GPP TS 29.274 "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3"*
- *3GPP TS 29.244 "Interface between the Control Plane and the User Plane nodes"*

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

Figure 28: Delete from MME Call Flow

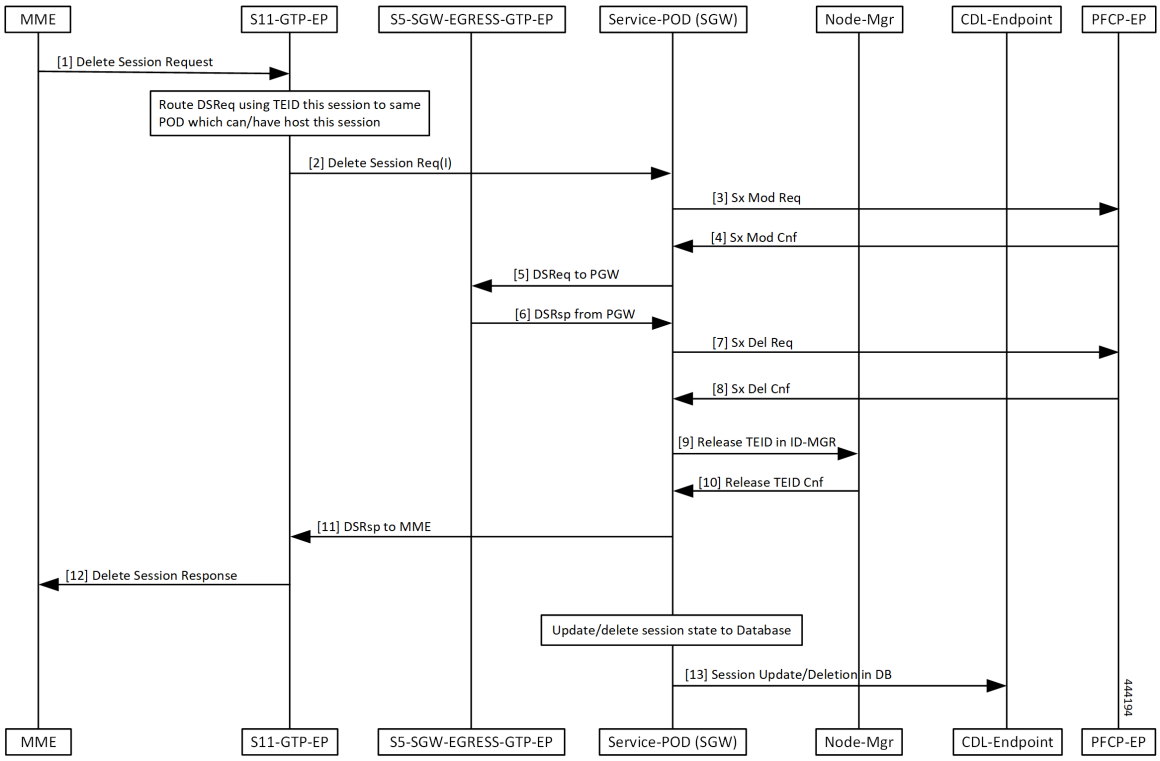


Table 46: Delete from MME Call Flow Description

Step	Description
1	The MME sends the Delete Session Request to the S11-GTP-EP.
2	The S11-GTP-EP routes this message with TEID value to the Service-POD (SGW) which handles this session.
3	The Service-POD (SGW) sends the Sx Modification Request to PFCP-EP.
4	The PFCP-EP sends the Sx Modification Confirmation to the Service-POD (SGW).
5	The Service-POD (SGW) sends the Delete Session Request to the PGW through the S5-SGW-EGRESS-GTP-EP.
6	The Service-POD (SGW) receives the Delete Session Request from the PGW through the S5-SGW-EGRESS-GTP-EP.
7	The Service-POD (SGW) sends the Sx Delete Request to PFCP-EP.
8	The Service-POD (SGW) receives the Sx Delete Confirmation from PFCP-EP.
9	The Service-POD (SGW) sends Release TEID in ID-MGR to Node-Mgr.
10	The Service-POD (SGW) receives the Release TEID Confirmation from the Node-Mgr.

Step	Description
11	The Service-POD (SGW) sends the Delete Session Response to S11-GTP-EP.
12	The S11-GTP-EP sends the Delete Session Response to the MME.
13	The Service-POD (SGW) sends the Session Update or Delete in database message to the CDL.

Figure 29: Delete from PGW Call Flow

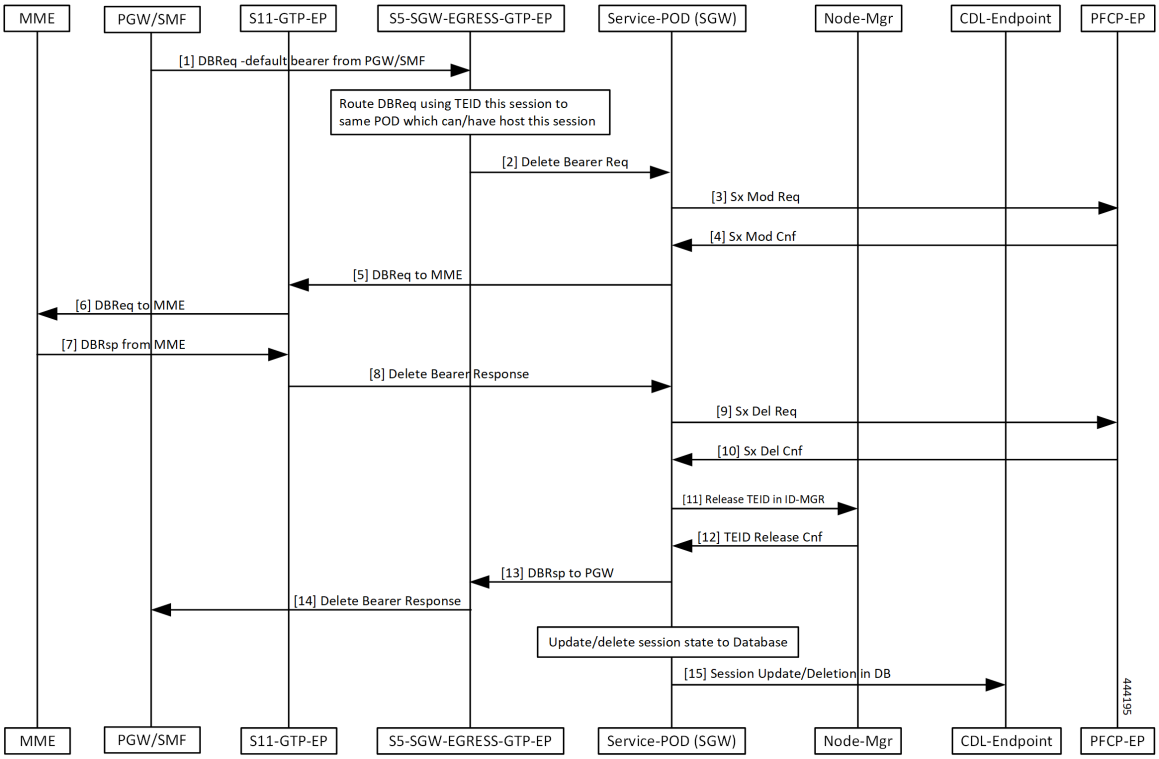
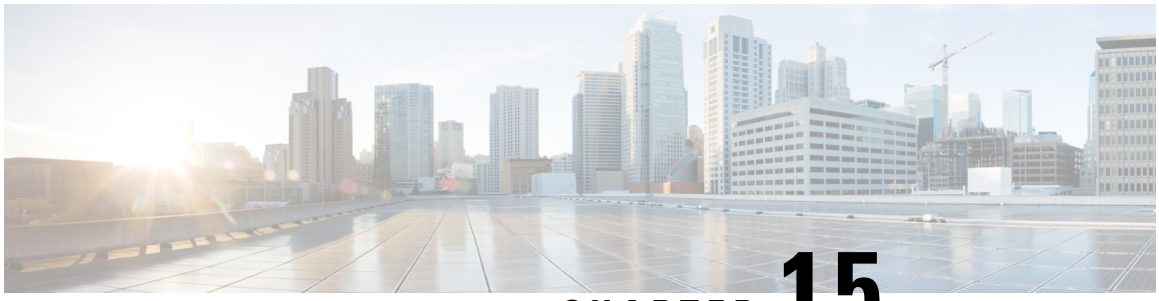


Table 47: Delete from PGW Call Flow Description

Step	Description
1	The PGW/SMF sends the Delete Bearer Request to the S5-SGW-EGRESS-GTP-EP.
2	The S5-SGW-EGRESS-GTP-EP performs routing of this message with TEID value to the same pod that has hosted this session. The S5-SGW-EGRESS-GTP-EP sends the Delete Bearer Request to the Service-POD (SGW).
3	The Service-POD (SGW) sends the Sx Modification Request to PFCP-EP and receives Sx Mod Cnf from it.
4	The PFCP-EP sends the Sx Modification Confirmation to the Service-POD (SGW).
5	The Service-POD (SGW) sends the Delete Bearer Request to the MME through the S11-GTP-EP.
6	The S11-GTP-EP forwards the Delete Bearer Request to the MME.

Step	Description
7	The MME sends the Delete Bearer Response to the S11-GTP-EP.
8	The S11-GTP-EP forwards the Delete Bearer Response to the Service-POD (SGW).
9	The Service-POD (SGW) sends the Sx Delete Request to the PFCP-EP.
10	The Service-POD (SGW) receives the Sx Delete Confirmation from the PFCP-EP.
11	The Service-POD (SGW) sends the Release TEID in ID-MGR to the Node-Mgr.
12	The Service-POD (SGW) receives the Release TEID Confirmation from the Node-Mgr.
13	The S11-GTP-EP sends the Delete Bearer Response to the PGW through S5-SGW-EGRESS-GTP-EP.
14	The S5-SGW-EGRESS-GTP-EP sends the Delete Bearer Response to the PGW/SMF.
15	The Service-POD (SGW) sends the Session Update or Delete in database message to the CDL.



CHAPTER 15

Downlink Data Notification

Feature Summary and Revision History

Summary Data

Table 48: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	DDN Message Handling Support: Enabled - Always-on Control Messages Triggered DDN Support: Disabled - Configuration required to enable DDN Advance Features: Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 49: Revision History

Revision Details	Release
Enhancement introduced. Added support for DDN Advance Features.	2021.02.0

Revision Details	Release
First introduced.	2021.01.0

Feature Description

The following sub-features are associated with this feature:

- DDN Message Handling
- Control Messages Triggered DDN
- Downlink Data Notification Delay
- High Priority Downlink Data Notification
- DDN Throttling

DDN Message Handling

Feature Description

cnSGW-C supports handling of the Downlink Data Notification (DDN) functionality that includes:

- Generating a DDN message towards the MME to page the UE on arrival of downlink data when UE is in IDLE state.
- Handling DDN ACK/DDN failure indication.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

Downlink Data Notification Success Call Flow

This section describes the Downlink Data Notification Success call flow.

Figure 30: Downlink Data Notification Success Procedure Call Flow

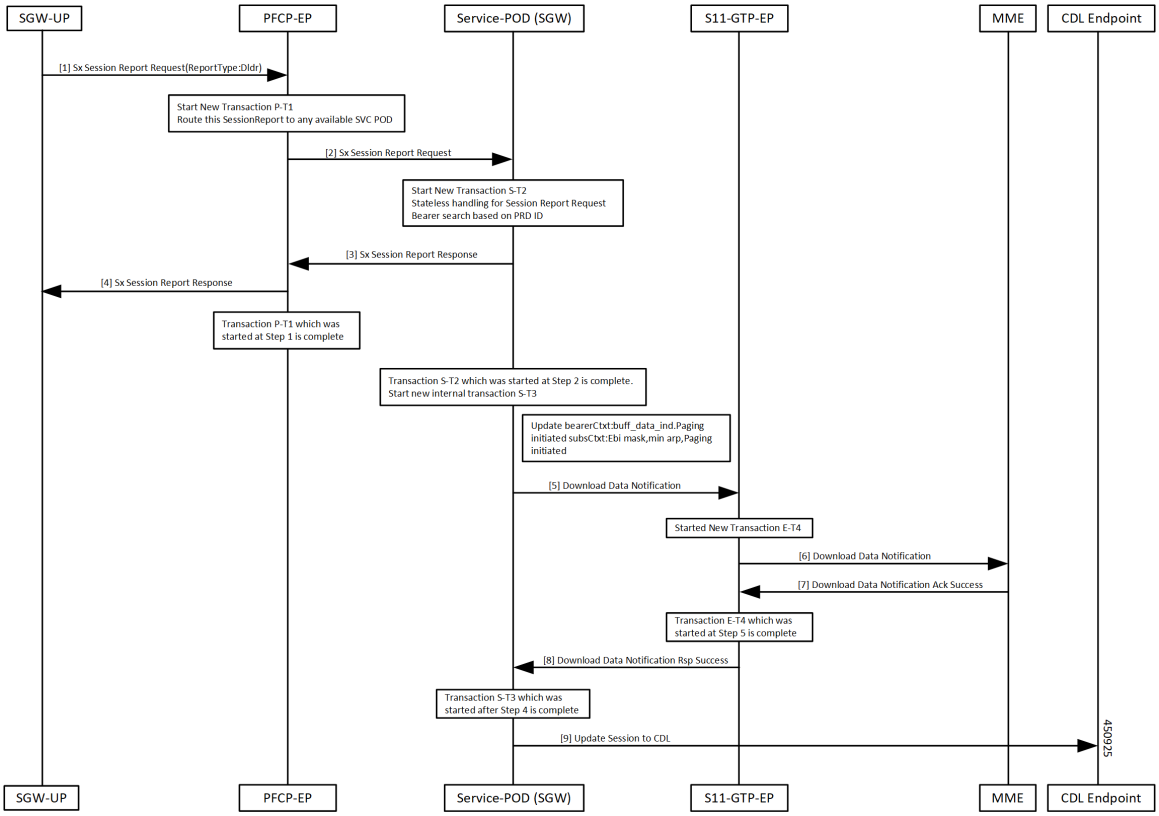


Table 50: Downlink Data Notification Success Procedure Call Flow Description

Step	Description
1	SGW-UP sends the Session Report Request to the PFCP-EP pod.
2	After receiving the Session Report Request, the PFCP-EP performs the following: • Starts a new P-T1 transaction. • Checks for the interface type. If its Sxa interface, it finds the available SGW-service pod and routes the request accordingly. • Sends the Sx Session Report Request to the SGW-service pod.

Step	Description
3	Upon reception of the Sx Session Report Request, SGW-service pod: • Creates a new S-T2 transaction. • Based on the message type received, updates the state processing not required for this message. • Handles the non-state processing transaction. (High priority is given to handle such messages). • Searches for the bearer based on PDR ID. If the bearer isn't found, the SGW-service pod fills the cause as **request rejected** in the Session Report Response. • If the received report type in the request isn't valid/supported, SGW-service pod fills the cause as **request rejected** and sends the Sx Session Report Response.
4	PFCP-EP forwards the Sx Session Report Response to the SGW-UP.
5	P-T1 transaction which is started at step one is completed. At SGW-service pod: • S-T2 transaction which is started at step two is completed. • If the Sx Session Report Response is success, a new internal transaction S-T3 is started with the same buffer as of the Session Report Request. • A DDN procedure for DLDR report type is initiated. • Bearer information is extracted from the received PDR ID. • Bearer context is updated with buffer-data_ind. • Initiated the DDN with EBI of bearers, which has downlink data, and minimum ARP among these bearers. • Sends the DDN to the S11-GTP-EP pod.
6	After receiving the DDN, S11-GTP-EP: • Creates a new E-T4 transaction. • Sends the DDN to the MME.
7	MME sends the DDN ACK Success to the S11-GTP-EP.
8	The transaction S-T3 which is started after step four is complete. S11-GTP-EP sends the DDN Response success to SGW-service pod.
9	SGW-service pod updates the CDL.

Downlink Data Notification Failure Call Flow

This section describes the Downlink Data Notification Failure call flow.

Figure 31: Downlink Data Notification Failure Call Flow

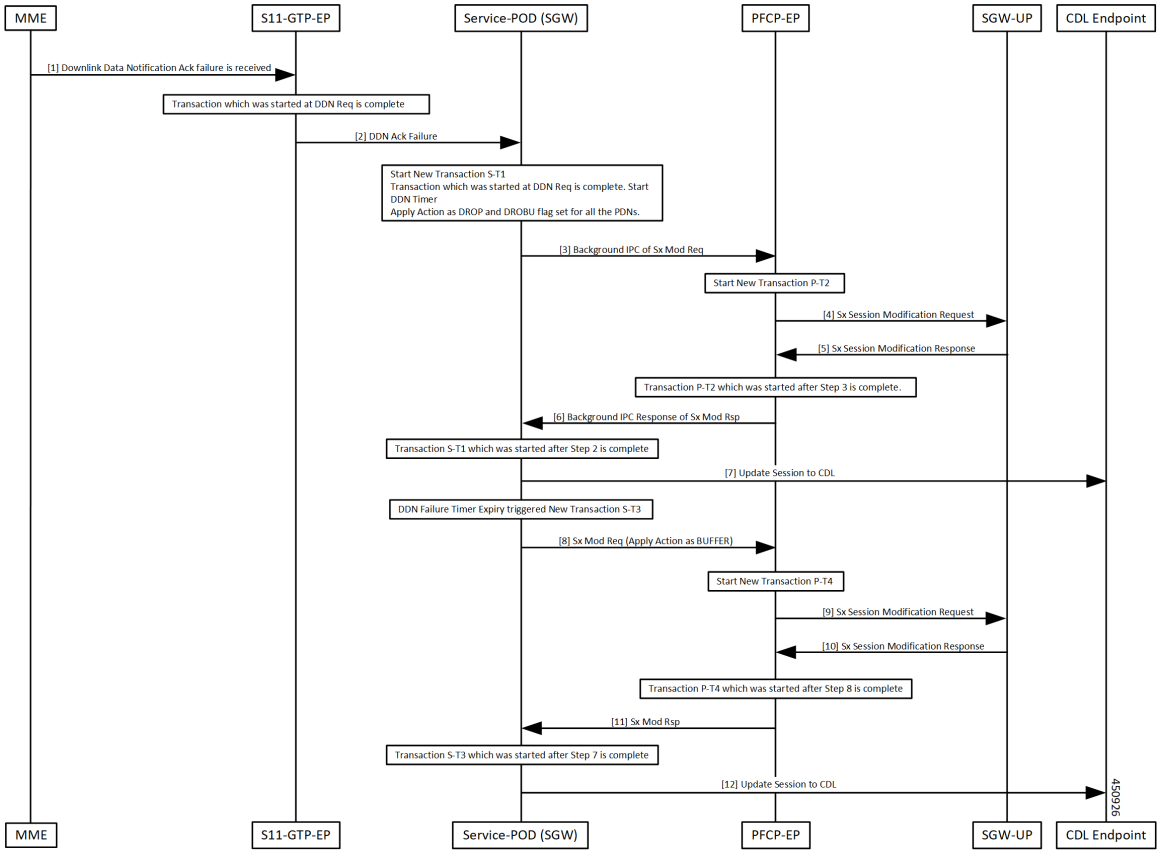


Table 51: Downlink Data Notification Failure Procedure Call Flow Description

Step	Description
1	S11-GTP-EP pod receives DDN ACK Failure.
2	The transaction started while sending the DDN Request ends. S11-GTP-EP forwards the DDN ACK Failure to the SGW-service pod.

Step	Description
3	After receiving the DDN ACK Failure at the SGW-service pod: • Decides the paging state based on the cause received: • EGTP_CAUSE_CONTEXT_NOT_FOUND: Submit internal transaction for call deletion. • EGTP_CAUSE_UNABLE_TO_PAGE_UE • EGTP_CAUSE_UNABLE_TO_PAGE_UE_DUE_TO_SUSPENSION • EGTP_CAUSE_UE_ALREADY_REATTACHED • EGTP_CAUSE_TEMP_REJECTED_DUE_TO_HANDOVER_IN_PROGRESS • Checks if the PDNs are in connected state to initiate the Sx Modify Request. Minimum one one PDN should be in the CONNECTED state. • Submits internal transactions to handle these paging failure causes. • Ends the current procedure and transaction. • In the new transaction of handling paging failures, derives all the PDNs for which you want to send Sx Modify request. • Based on the paging state, derives paging action and send Sx Modify Request based on the action required. Sends background IPC request for Sx Modification Request to PFCP-EP pod. Create a new transaction P-T2.
4	After receiving background IPC request for Sx Modification request, PFCP-EP: • Starts a new P-12 transaction. • Sends the o the SGW-UP.
5	PFCP-EP receives the Sx Modification Response from the SGW-UP.
6	The transaction P-T2 started at step three is complete. PFCP-EP pod sends background IPC response to the SGW-service pod.
7	The transaction S-T1 started at step two is complete. SGW-service pod updated the CDL with buff_data_ind at bearer level flag.
8	On DDN Failure timer expiry, a new transaction S-T3 is started. SGW-service pod sends background IPC request for the Sx Modification Request to the PFCP-EP pod with Apply Action as BUFFER.
9	A new P-T4 transaction is created. PFCP-EP pod sends the Sx Modification Request to the SGW-UP.
10	SGW-UP sends the Sx Modification Response to the PFCP-EP pod.

Step	Description
11	The transaction P-T4 started at step eight is complete. PFCP-EP pod forwards the Sx Modification Response to the SGW-service pod.
12	The transaction S-T3 started at step seven is complete. SGW-service pod updates the CDL.

No User Connect Retry Timer Call Flow

This section describes the No User Connect Retry Timer call flow.

Figure 32: No User Connect Retry Timer Call Flow

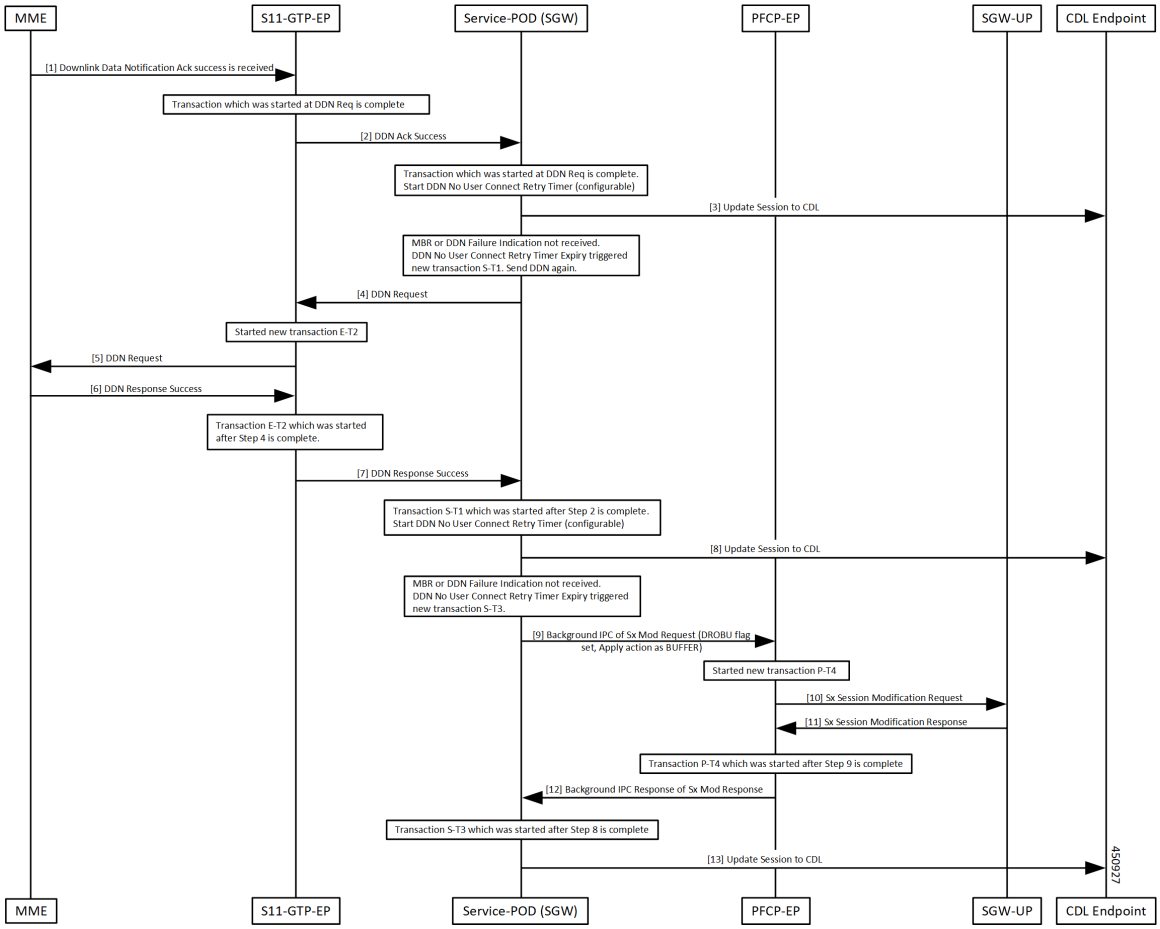


Table 52: No User Connect Retry Timer Call Flow Description

Step	Description
1	Received DDN ACK success at the S11-GTP-EP pod.

Step	Description
2	The transaction started while sending the DDN ends here. S11-GTP-EP sends the DDN ACK success to the SGW-service pod.
3	No User Connect Retry timer is started at the SGW-C pod. This timer is configurable. SGW-service pod updates the CDL.
4	SGW-service pod sends the DDN Request to the S11-GTP-EP pod, when: • The DDN Failure Indication/MBR is not received • No User Connect Retry timer expires. A new transaction S-T1 is created.
5	A new E-T2 transaction is created. S11-GTP-EP pod forwards the DDN Request to MME.
6	MME sends the DDN Response to the S11-GTP-EP.
7	The transaction E-T2 started at step four is complete. S11-GTP-EP forwards the DDN Response Success to the SGW-service pod.
8	S-T1 transaction started at step two is completed. No User Connect Retry timer is started at the SGW-C pod. This timer is configurable. SGW-service pod updates the CDL.
9	If DDN Failure Indication/MBR is not received, No User Connect Retry expiry triggered. A new transaction S-T3 is created. SGW-service pod sends the background IPC request for Sx Modification request to the PFCP-EP pod (DROBU flag and Apply Action as BUFFER).
10	A new transaction P-T4 is created. PFCP-EP pod sends the Sx Modification Request to the SGW-U pod.
11	PFCP-PE pod receives the Sx Modification Response.
12	The transaction P-T4 started at step nine is complete. PFCP-EP pod sends the background IPC response to the SGW-service pod.
13	The transaction S-T3 started at step eight is complete. CDL is updated.

Feature Configuration

Configuring this feature involves the following steps:

Configuring the DDN Failure Timer

DDN Failure Timer is configured under the `sgw-profile`.

To configure this feature, use the following configuration:

```
config
   profile sgw sgw_name
       ddn failure-action-drop-timer timer_value
       ddn timeout-purge-session { true | false }
       end
```

NOTES:

- **ddn failure-action-drop-timer** *timer_value*—Specify the duration of the DDN packet drop timer. During this specified timeframe, the DDN is not sent to the UE. This timer is used, when a notification of DDN ACK Failure or DDN Failure Indication is received. The default value is 300 seconds.

Note To disable the timer, set the timer value to zero.

- **ddn timeout-purge-session { true | false }**—Specify the option to enable or disable the DDN timeout purge session. The default value is false.

Configuration Example

The following is an example configuration.

```
config
profile sgw sgw1
ddn failure-action-drop-timer 60
ddn timeout-purge-session false
end
```

Configuration Verification

To verify the configuration:

```
show running-config profile sgw
profile sgw sgw1
locality LOC1
fqdn 209.165.201.1
ddn failure-action-drop-timer 60
ddn timeout-purge-session false
end
```

Configuring DDN No User Connect Retry Timer

This section describes how to configure the DDN No User Connect Retry Timer.

DDN No User Connect Retry Timer can be configured under sgw-profile.

To configure this feature, use the following configuration:

```
config
  profile sgw sgw_name
   ddn no-user-connect-retry-timer timer_value
   end
```

NOTES:

- **ddn no-user-connect-retry-timer** *timer_value* - Specify the DDN retry timer used when DDN Ack is received with Success and MBR is not received. Default value is 60 seconds.

  To disable the timer, set the value to 0.

Configuration Example

The following is the sample configuration.

```
config
 profile sgw sgw1
  ddn no-user-connect-retry-timer 120
  end
```

Configuration Verification

To verify the configuration:

```
show running-config profile sgw
profile sgw sgw1
locality LOC1
fqdn cisco.com.apn.epc.mnc456.mcc123
ddn failure-action-drop-timer 60
ddn no-user-connect-retry-timer 120
```

Control Messages Triggered DDN Support

Feature Description

This feature supports paging the UE for the PGW-initiated control procedures when the UE is in IDLE mode.

Note This feature is CLI controlled.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

Downlink Data Notification for PGW-initiated procedure with Cloud Native Call Flow

This section describes the DDN for the PGW-initiated procedure with Cloud Native call flow.

Figure 33: Downlink Data Notification for PGW initiated Procedure with Cloud Native Call Flow

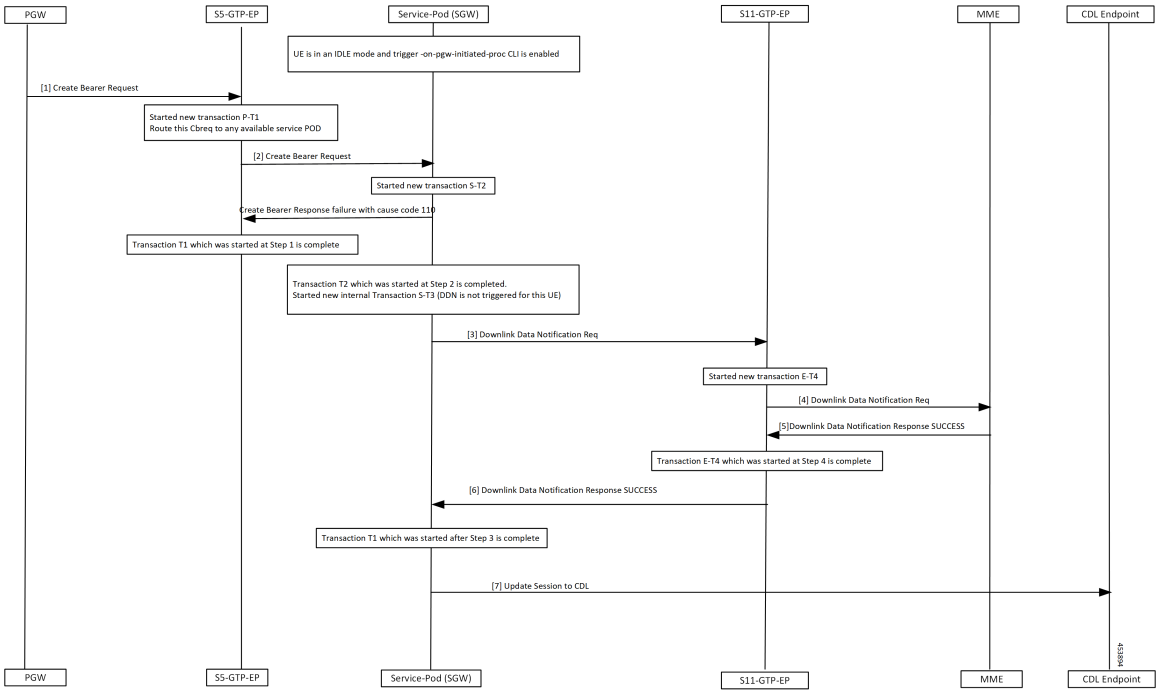


Table 53: Downlink Data Notification for PGW initiated procedure (CBR) with Cloud Native Call Flow Description

Step	Description
1, 2	Enabled trigger-on-pgw-initiated-proc CLI and state of the UE is in IDLE mode. S5-GTP-EP receives the CBR from the PGW and forwards it to the SGW-service pod. SGW-service pod starts a new S-T2 transaction. SGW-service pod sends failure response to the S5-GTP-EP with cause code 110.
3	The T2 transaction which started in step two is completed. A new S-T3 transaction is started for the UE for which DDN is not triggered. SGW-service pod initiates the DDN Request to the theS11-GTP-EP.
4	A new E-T4 transaction is started. S11-GTP-EP forwards the DDN Request to the MME.
5	S11-GTP-EP receives the DDN Response success from the MME.
6	Transaction E-T4 which started in step four is completed. S11-GTP-EP sends the DDN Response success to the SGW-service pod.
7	Transaction T1 which is started in step three is completed. SGW-service pod updates the session to CDL.

Feature Configuration

To configure this feature, use the following configuration:

```
config
 profile sgw sgw_name
  ddn trigger-on-pgw-initiated-proc
  end
```

NOTES:

- **ddn trigger-on-pgw-initiated-proc**—When UE is in IDLE mode, the DDN triggers paging for PGW-initiated procedures. SGW sends failure response to the PGW with cause code 110.

Configuration Example

The following is an example configuration.

```
config
 profile sgw sgw1
  ddn trigger-on-pgw-initiated-proc
  end
```

Configuration Verification

To verify the configuration:

```
show running-config profile sgw
profile sgw sgw1
locality LOC1
fqdn 209.165.201.1
ddn failure-action-drop-timer 60
ddn no-user-connect-retry-timer 120
ddn trigger-on-pgw-initiated-proc
exit
```

Disabling the DDN Control Procedure

Use `no ddn trigger-on-pgw-initiated-proc` to disable DDN Control Procedure feature.

DDN Advance Features

Feature Description

This feature supports the following:

- Downlink Data Notification Delay
- High Priority Downlink Data Notification
- DDN Throttling

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

DDN Delay Call Flow

This section describes DDN Delay call flow.

Figure 34: DDN Delay Call Flow

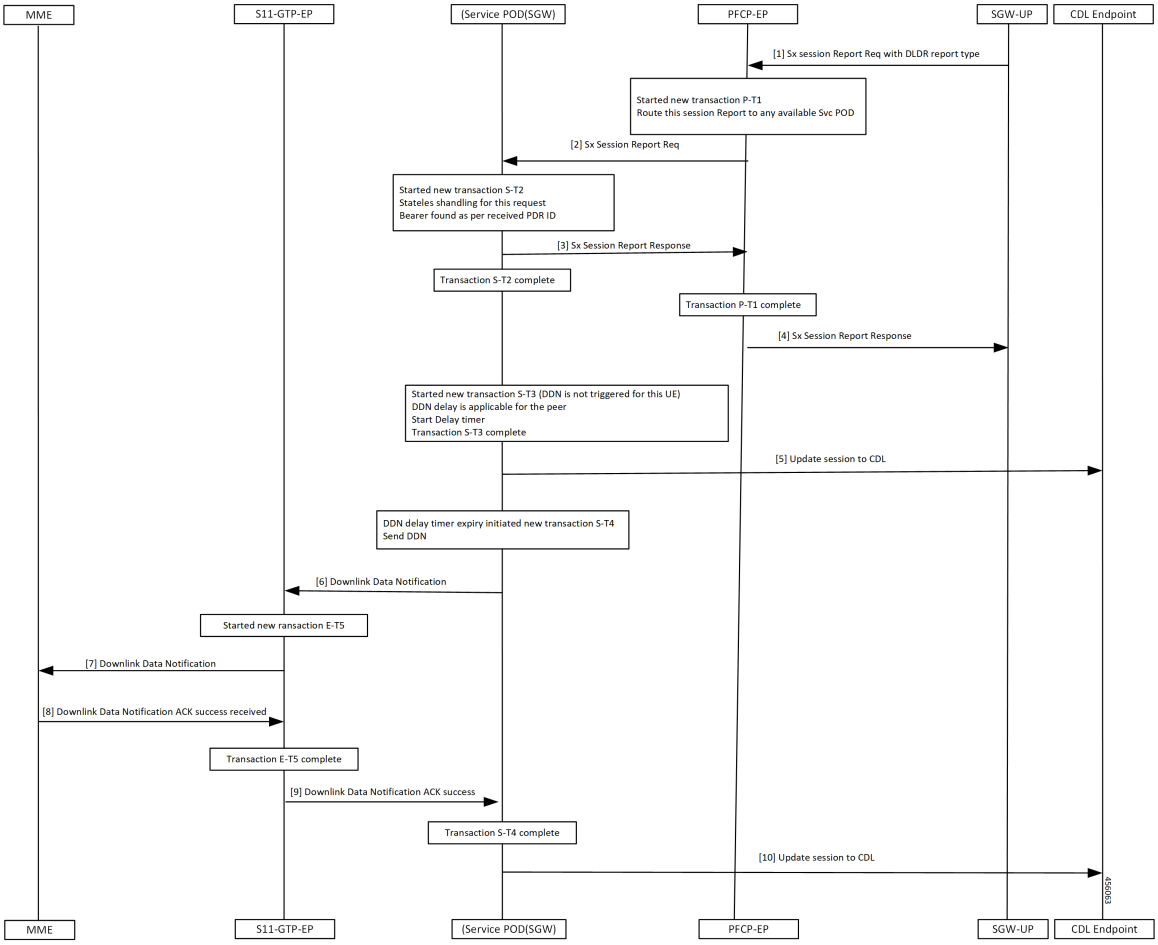


Table 54: DDN Delay Call Flow Description

Step	Description
1	Received downlink data when UE is in IDLE state. SGW-UP sends the Sx Report Request with report type as DLDR with corresponding PDR ID to the PFCP-EP.

Step	Description
2	Started a new P-T1 transaction. PFCP-EP pod: • Checks the available service pod. • Sends the Sx Session Report to the the SGW-service pod.
3	A new transaction S-T2 is stared. SGW-CP sends success response to the SGW-UP, when a bearer found at CP for this PDR-ID.
4	The S-T2, P-T1 transactions are completed. PFCP-EP sends the Sx Session Report Response to the SGW-UP.
5	A new transaction S-T3 is started when DDN is not triggered for this UE. Sgw-service pod gets the peer information to check if the peer configured with the DDN delay value. DDN delay timer is triggered, if DDN delay configured. S-T3 transaction is completed. SGW-service pod sends the CDL update.
6, 7	A new S-T4 transaction started. SGW-service pod sends the DDN to the S11-GTP-EP. A new E-T5 transaction is started. S11-GTP-EP forwards the DDN to the MME.
8, 9	MME sends the DDN ACK success to the S11-GTP-EP. Transaction E-T5 started in step seven is completed. S11-GTP-EP forwards the DDN ACK success towards the SGW-service pod.
10	Transaction S-T4 started in step six is completed. SGW-service pod updates session information to CDL.

High Priority DDN Call Flow

This section describes High Priority DDN call flow.

Figure 35: High Priority DDN Call Flow

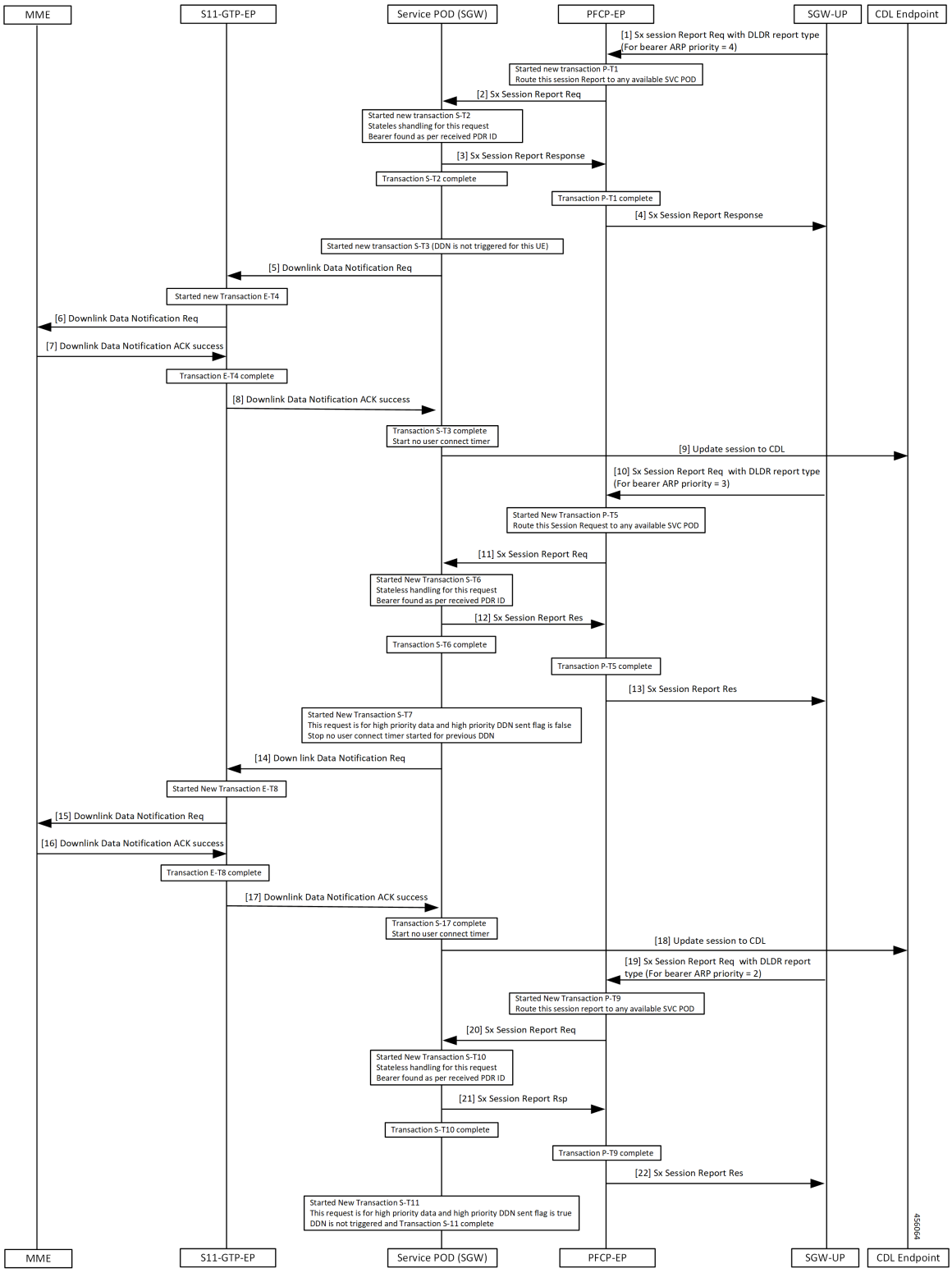


Table 55: High Priority DDN Call Flow Description

Step	Description
1	Bearer received downlink data with ARP priority value as four, when UE is in IDLE state. SGW-UP sends the Sx Report Request to the PFCP-EP with report type as DLDR with corresponding PDR ID.
2	New P-T1 transaction is started and routed the session report to all available service pods. PFCP-EP sends the Sx Session Report Request to the SGW-service pod.
3	New S-T2 transaction is started and the SGW-service pod sends Sx Session Report Response to the PFCP-EP.
4	Transaction P-T1 and S-T2 completed and the PFCP-EP forwards the Sx Session Report Response to the SGW-UP.
5	New S-T3 transaction is started for which the DDN isn't triggered. SGW-service pod sends the DDN Request to the S11-GTP-EP.
6	New E-T4 transaction is started and the S11-GTP-EP forwards the DDN Request to the MME.
7	MME sends the DDN ACK success to the S11-GTP-EP.
8	Transaction E-T4 is completed. S11-GTP-EP forwards the DDN ACK success to the SGW-service pod.
9	Transaction S-T3 completed. SGW-service pod triggers No User Connect timer and updates session to CDL.
10	SGW-UP sends the Sx Session Report Request to the PFCP-EP with report type as DLDR for bearer whose ARP priority value is three.
11	New P-T5 transaction is started and routed the session report to all the available service pods. PFCP-EP sends the Sx Session Report Request to the SGW-service pod.
12	New transaction S-T6 started SGW-service pod sends the Sx Session Report Response to the PFCP-EP when bearer found as per the received PDR ID.
13	Transaction S-T6 and P-T5 completed and PFCP-EP forwards the Sx Session Report Response to the SGW-UP.
14	New transaction S-T7 started and data, high priority DDN sent with the flag value as False. No User Connect timer is topped. SGW-service pod sends the DDN Request to the S11-GTP-EP.
15	New E-T8 transaction is started and the S11-GTP-EP forwards the DDN Request to the MME.
16	MME sends the DDN ACK success to the S11-GTP-EP.

Step	Description
17	S11-GTP-EP forwards the DDN ACK success to the SGW-service pod for this PDR ID.
18	Transaction S-17 completed. SGW-service pod triggers the No User Connect timer when received DDN ACK success and updated the session to CDL.
19	Bearer received the downlink data with ARP priority value as two. SGW-UP sends the Sx Report Request to the PFCP-EP with report type as DLDR with corresponding PDR ID.
20	New transaction P-T9 started and routed the session report to all the available service pods. PFCP-EP sends the Sx Session Report Request to the SGW-service pod.
21	New transaction S-T10 started and the SGW-service pod sends the Sx Session Report Response to the PFCP-EP when the bearer found as per the received PDR ID.
22	Transaction S-T10 and P-T9 completed and the PFCP-EP forwards the Sx Session Report Response to the SGW-UP. At SGW-service pod: • New transaction S-T11 started and data, high priority DDN sent with the flag value as True. SGW-service pod stops No User Connect timer. • SGW-service pod doesn't trigger DDN when high priority DDN already initiated. Transaction S-11 is completed.

DDN Throttling Call Flow

This section describes DDN Throttling call flow.

Figure 36: DDN Throttling Call Flow

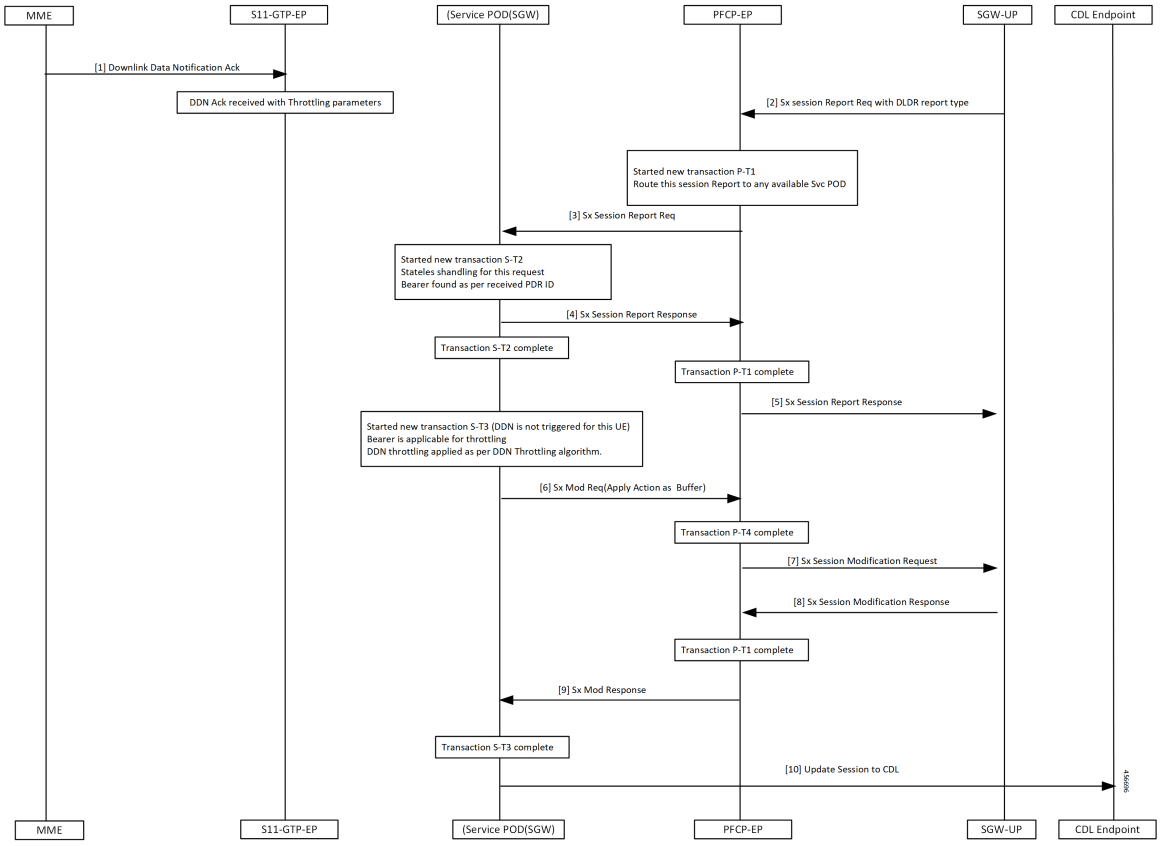


Table 56: DDN Throttling Call Flow Description

Step	Description
1	Received DDN with throttling parameters when UE is in IDLE state. MME sends the DDN ACK to the S11-GTP-EP.
2	SGW-UP sends the Sx Report Request with report type as DLDR with corresponding PDR ID to PFCP-EP.
3	PFCP-EP triggers a new P-T1 transaction and routes the Sx Report Request to available service pod. PFCP-EP sends the Sx Session Report Request to the SGW-service pod.
4	Started a new S-T2 transaction. Get peer information to check if DDN Throttle is active for this peer. Check if priority of this bearer is more than the configured ARP watermark SGW-service pod sends the Sx session Report Response to the PFCP-EP.

Step	Description
5	S-T2 transaction started in step four is completed. P-T1 transaction started in step threee is completed. When a bearer found at CP for this PDR ID, the PFCP-EP sends success response to the SGW-UP.
6	A new S-T3 transaction is started for the UE for which DDN is not triggered. Apply DDN algorithm to check if the DDN must be throttled. If DDN throttled, SGW-service pod sends the Sx Modification Request with Apply Action as BUFFER towards PFCP-EP.
7, 8	P-T4 transaction is completed. PFCP-EP sends the Sx Session Modification Request to the SGW-UP and receives the Sx Session Modification Response from the SGW-UP.
9	P-T1 transaction started in step five is completed. PFCP-EP sends Sx Modification Response to the SGW-service pod.
10	S-T3 transaction started in step six is completed. SGW-service pod updates the session to CDL.

Standards Compliance

The Downlink Data Notification Support feature complies with the following standards:

- *3GPP TS 23.401, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access"*
- *3GPP TS 23.402, "Architecture enhancements for non-3GPP accesses"*
- *3GPP TS 29.274, "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3"*
- *3GPP TS 23.214, "Architecture enhancements for control and user plane separation of EPC nodes"*
- *3GPP TS 29.244, "Interface between the Control Plane and the User Plane nodes"*
- *3GPP TS 24.008, "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3"*

Feature Configuration

By default, the DDN throttling is always enabled.

Note cnSGW-C handles DDN throttling parameters sent from the MME.

To configure this feature, use the following configuration:

```
config
 profile sgw sgw_name
  ddn throttle-arp-watermark arp_value
  end
```

NOTES:

- **ddn throttle-arp-watermark***arp_ value*—Specify the lowest priority ARP for DDN throttle.

  Throttling is applicable only for bearer having ARP PL value greater than the configured *value*. Must be an integer in the range of 0-15.

  By default, throttling is applicable for all bearers.

Configuration Example

The following is an example configuration.

```
config
 profile sgw sgw1
  ddn throttle-arp-watermark 3
  end
```

OAM Support

This section describes operations, administration, and maintenance information for this feature.

Bulk Statistics

The following statistics are supported for the DDN Advance feature.

```
sgw_ddn_stats{app_name="smf",cluster="cn",data_center="cn",
ddn_stats_type="control_proc_triggered",instance_id="0",service_name="sgw-service"}2
```

```
sgw_ddn_stats{app_name="smf",cluster="cn",data_center="cn",ddn_stats_type="data_triggered",
instance_id="0",service_name="sgw-service"} 18
```

```
sgw_ddn_stats{app_name="smf",cluster="cn",data_center="cn",ddn_stats_type="delayed",
instance_id="0",service_name="sgw-service"} 7
```

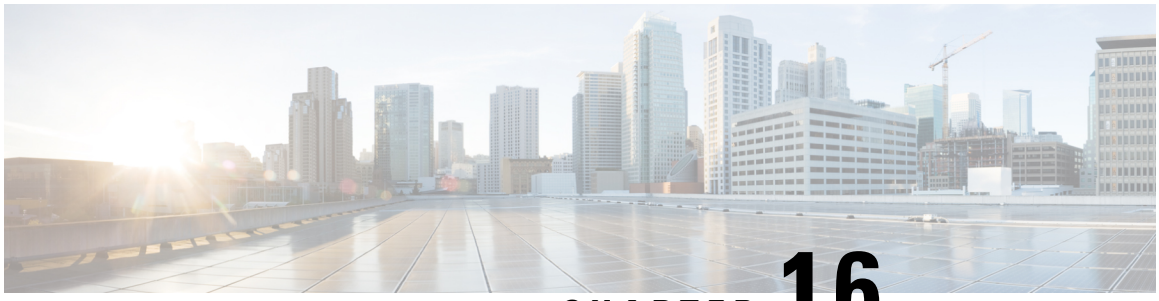
```
sgw_ddn_stats{app_name="smf",cluster="cn",data_center="cn",ddn_stats_type="high_priority_initiated",
instance_id="0",service_name="sgw-service"} 3
```

```
sgw_ddn_stats{app_name="smf",cluster="cn",data_center="cn",ddn_stats_type="high_priority_suppressed",
instance_id="0",service_name="sgw-service"} 1
```

```
sgw_ddn_stats{app_name="smf",cluster="cn",data_center="cn",ddn_stats_type="throttled",
instance_id="0",service_name="sgw-service"} 6
```

- high_priority_initiated - DDN initiated count, due to high priority paging trigger.

- high_priority_suppressed - DDN high priority count which is suppressed. When a UE is already working on the high priority DDN-initiated paging request. It suppresses the incoming high priority paging request.
- throttled - DDN throttled count.
- delayed - DDN initiated count after the DDN delay timer.
- control_proc_triggered - The received count of paging triggers from control procedure when UE is in IDLE state.
- data_triggered - The received count of paging triggers from UPF for downlink data when UE is in IDLE state.



CHAPTER 16

DSCP Marking Support

Feature Summary and Revision History

Summary Data

Table 57: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	DSCP Marking for Data packets: Disabled – Configuration required to enable DSCP Marking for CP Signaling Messages: Enabled – Always-on
Related Documentation	Not Applicable

Revision History

Table 58: Revision History

Revision Details	Release
Added support for DSCP Marking for CP Signaling Messages.	2021.02.0
First introduced.	2021.01.0

Feature Description

Differentiated Services Code Point (DSCP) is a means of classifying and managing network traffic. It provides quality of service (QoS) in modern Layer 3 IP networks.

This feature supports the following:

- DSCP Marking for Data Packets
- DSCP Marking for CP Signaling Messages

DSCP Marking for Data Packets

Feature Description

This feature supports marking of DSCP with the combination of QCI and ARP.

It also supports the programming of the DSCP marking value to the User Plane (UP) for data packets.

How it Works

This section describes how this feature works.

DSCP Marking IEs

DSCP marking IEs are sent in the Sx Establishment Request or the Sx Modification Request message. These IEs are a part of Forwarding Action Rule (FAR) IE. The following are the supported IEs and their functions:

- Inner Packet Marking (Private Extension IE): Sends the user-datagram DSCP marking values to the UP.
- Transport Packet Marking (3GPP Spec-defined IE): Sends the encaps-header DSCP values to the UP.
- Transport Packet Marking Options (Private Extension IE): Sends copy-inner and copy-outer options of encaps-header marking to the UP.

Feature Configuration

To configure this feature, use the following configuration:

```
config
   profile
      sgw-qos-profile qos_profile_name
         dscp-map
            operator-defined-qci non_standard_qos_class_id
            qci qci_value
               downlink downlink_value
                  user-datagram
                     dscp-marking dscp_marking_value
                  encaps-header
```

```
                dscp-marking dscp_marking_value
            encsp-header enscp_header_value
                dscp-marking dscp_marking_value
        uplink uplink_value
            user-datagram
                dscp-marking dscp_marking_value
            encaps-header
                dscp-marking dscp_marking_value
            encsp-header enscp_header_value
    arp-priority-level arp_priority_level_value
        uplink
            user-datagram
                dscp-marking dscp_marking_value
            encaps-header
                dscp-marking dscp_marking_value
        downlink
            user-datagram
                dscp-marking dscp_marking_value
            encaps-header
                dscp-marking dscp_marking_value
                end
```

NOTES:

- **sgw-qos-profile** *qos_profile_name*—Specify the QoS profile configuration name for SGW.
- **dscp-map**—Configures QCI to DSCP-Marking mapping.
- **operator-defined-qci** *non_standard_qos_class_id*—Specify the non-standard QoS class identifier. Must be an integer in the range of 128-254.
- **qci** *qci_value*—Specify the standard QCI value. Must be an integer from the following options: 1-9, 65, 66, 69, 70, 80, 82, 83.
- **arp-priority-level** *arp_priority_value*—Specify the ARP Priority Level. Must be an integer in the range of 1-15.
- **uplink** *uplink_value*—Specify the uplink QCI value.
- **downlink** *downlink_value*—Specify the downlink QCI value.
- **gbr**—Specify the type of the QCI to GBR.
- **non-gbr**—Specify the type of the QCI to non-GBR.
- **encaps-header**—Specify the DSCP value to be applied to the encaps header.
- **user-datagram**—Specify the DSCP value to be applied to the user datagram.
- **copy-inner**—Starts copying the inner DSCP to outer value.
- **copy-outer**—Starts copying the outer DSCP to inner value.
- **dscp-marking** *dscp_marking_value*—Specify the DSCP value to be applied to packets. (A hexadecimal string value, starting with 0x. For example: 0x3F)

- **qci**—The QCI uplink and downlink options are the same. Similarly, the commands for **operator-defined-qci** and standard QCI are the same, the only difference is the mandatory selection of *bearer-type* in **operator-defined-qci**. You can also specify ARP along with the type of the bearer.

Configuration Example

The following is an example configuration.

```
config
  profile sgw-qos-profile q
    dscp-map qci 1 uplink encaps-header copy-inner user-datagram dscp-marking 0x1
    dscp-map qci 1 downlink user-datagram dscp-marking 0x2 encaps-header dscp-marking 0x3
    dscp-map qci 2 gbr uplink user-datagram dscp-marking 0x5 encaps-header dscp-marking 0x6

    dscp-map operator-defined-qci 128 gbr arp-priority-level 1 uplink user-datagram
dscp-marking 0x7
    end
```

Configuration Verification

To verify the configuration:

```
show running-config profile sgw-qos-profile q
  profile sgw-qos-profile q
    dscp-map qci 1 uplink encaps-header copy-inner user-datagram dscp-marking 0x1
    dscp-map qci 1 downlink user-datagram dscp-marking 0x2 encaps-header dscp-marking 0x3
    dscp-map qci 2 gbr uplink user-datagram dscp-marking 0x5 encaps-header dscp-marking 0x6

    dscp-map operator-defined-qci 128 gbr arp-priority-level 1 uplink user-datagram
dscp-marking 0x7
    end
```

DSCP Marking for CP Signaling Messages

Feature Description

This feature supports the marking of DSCP values to control packets as per the configuration at the following interfaces:

- GTPC: S11, S5
- PFCP: Sxa

Feature Configuration

Configuring this feature involves the following steps:

- Configuring DSCP under the S11 Interface for the GTP Endpoint. For more information, refer to Configuring DSCP under S11 Interface for GTP Endpoint, on page 163.
- Configuring DSCP under the S5e Interface for the GTP Endpoint. For more information, refer to Configuring DSCP under S5e Interface for GTP Endpoint, on page 163.

- Configuring DSCP under the Sxa Interface for the Protocol Endpoint. For more information, refer to Configuring DSCP under Sxa Interface for Protocol Endpoint, on page 164.

Configuring DSCP under S11 Interface for GTP Endpoint

To configure this feature, use the following configuration:

```
config
    instance instance-id instance_id
        endpoint endpoint_name
        interface interface_name
        dscp dscp_value
        end
```

NOTES:

- **endpoint** *endpoint_name*—Specify the endpoint name.
- **interface** *interface_name*—Specify the endpoint interface name.
- **dscp** *dscp_value*—Specify the DSCP value. Must be a hexadecimal string starting with 0x (for example, 0x3F), or a decimal value (for example, 12). The decimal value must be in the range of 0-63.

Configuration Example

The following is an example configuration.

```
config
    instance instance-id 1
        endpoint gtp
        interface s11
        dscp 0x2
        end
```

Configuration Verification

To verify the configuration:

```
show running-config instance instance-id 1 endpoint
    endpoint gtp
    interface s11
    dscp 0x2
    end
```

Configuring DSCP under S5e Interface for GTP Endpoint

To configure this feature, use the following configuration:

```
config
    instance instance-id instance_id
        endpoint endpoint_name
        interface interface_name
        dscp dscp_value
        end
```

Configuration Example

The following is an example configuration.

```
config
    instance instance-id 1
        endpoint gtp
        interface s5e
        dscp 0x2
        end
```

Configuration Verification

To verify the configuration:

```
show running-config instance instance-id 1 endpoint
    endpoint gtp
    interface s5e
    dscp 0x2
    end
```

Configuring DSCP under Sxa Interface for Protocol Endpoint

To configure this feature, use the following configuration:

```
config
    instance instance-id instance_id
        endpoint endpoint_name
        interface interface_name
        dscp dscp_value
        end
```

Configuration Example

The following is an example configuration.

```
config
    instance instance-id 1
        endpoint gtp
        interface sxa
        dscp 0x2
        end
```

Configuration Verification

To verify the configuration:

```
show running-config instance instance-id 1 endpoint
    endpoint gtp
    interface sxa
    dscp 0x2
    end
```

Removing DSCP Configuration

When you remove the DSCP signaling configuration from the interface or endpoint, it uses the default marking. The default value is 10 or 0xa (in Hexadecimal).

To clear the DSCP configuration:

```
config
    instance instance-id instance_id
        endpoint endpoint_name
        interface interface_name
```

```
no dscp
end
```

Configuration Example

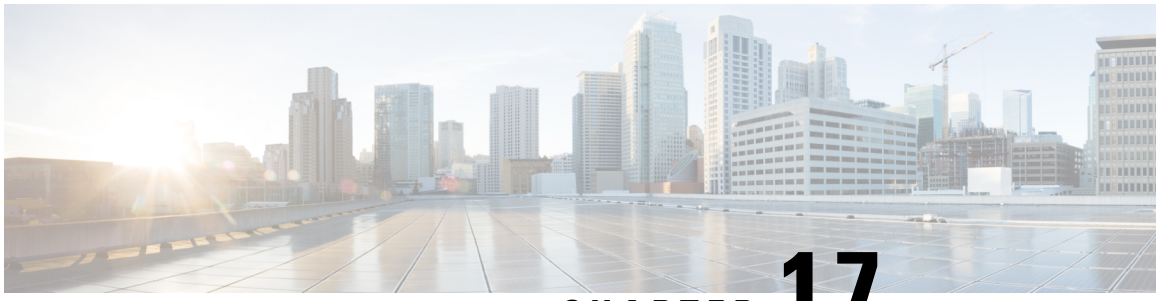
The following is an example configuration for the removal of the DSCP configuration.

```
config
    instance instance-id 1
        endpoint gtp
        interface s11
        no dscp
        end
```

Configuration Verification

To verify the DSCP configuration removal:

```
show running-config instance instance-id 1 endpoint
    instance instance-id 1
    endpoint gtp
    interface s5e
    dscp 0x4
    exit
    interface s11
    exit
    exit
    endpoint protocol
    interface sxa
    dscp 8
    end
```



CHAPTER 17

Emergency Call Support

Feature Summary and Revision History

Summary Data

Table 59: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 60: Revision History

Revision Details	Release
First introduced.	2021.02.0

Feature Description

Emergency services refer to the functionalities provided by the serving network when the network is configured to support emergency services. These are provided to support IMS emergency sessions.

The MME Emergency Configuration Data contains the Emergency APN which is used for deriving a PDN GW. The MME Emergency Configuration Data can also contain the statically configured PDN GW for the Emergency APN.

cnSGW-C considers calls as emergency when:

- Create Session request has IMEI only.
- The Indication flag indicates unauthenticated IMSI and there's a valid IMSI and IMEI in the Create Session Request.

Note With an emergency session setup, cnSGW-C rejects any additional PDN request (Create Session Request) sent by the MME.

Limitations

This feature has the following limitations in 2021.02.0 and later releases:

- IMEI with 15 digits or 16 digits is supported only for the following procedures—show subscriber, clear subscriber, and monitor subscriber.

How it Works

This section describes how this feature works.

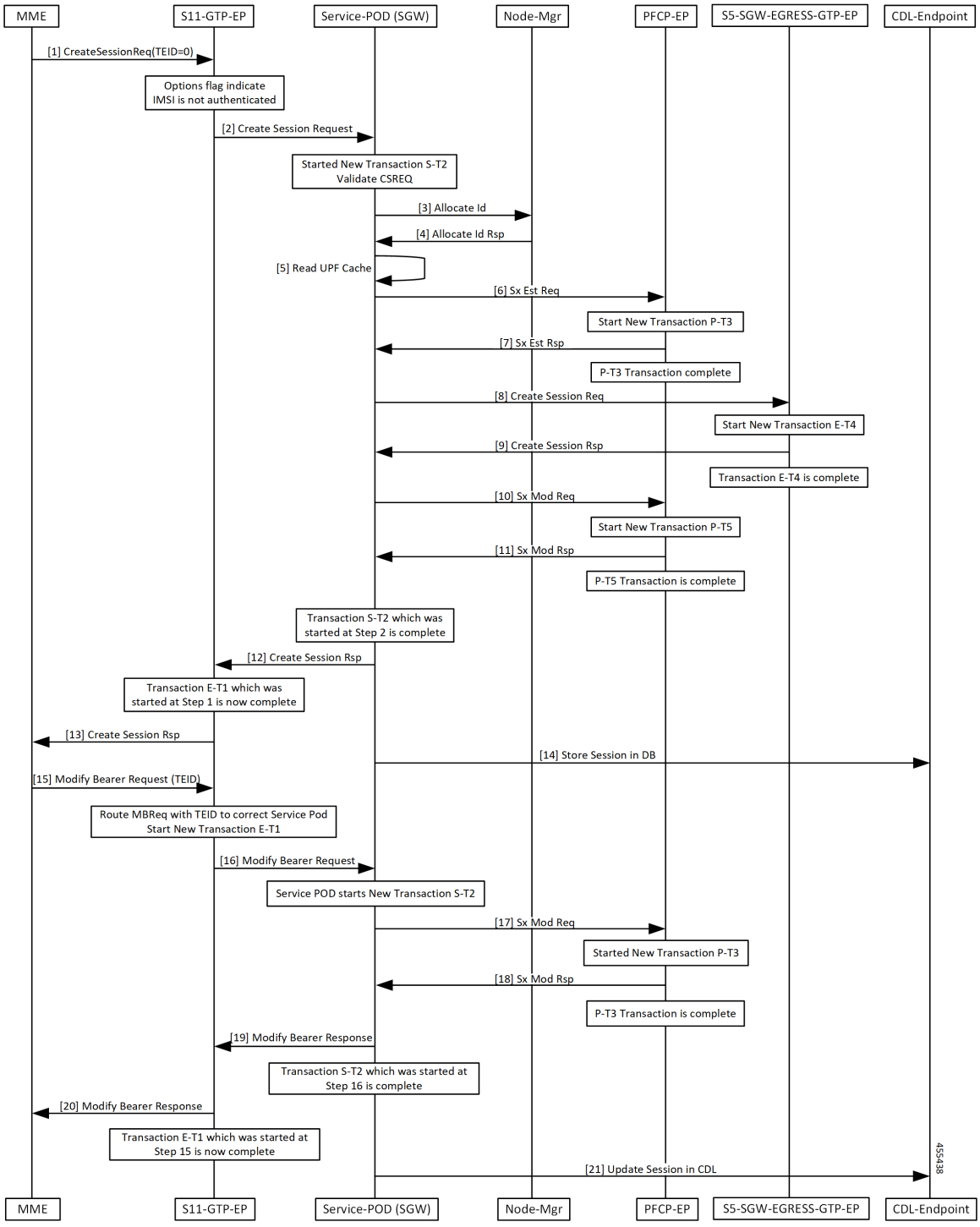
Call Flows

This section describes the key call flows for the feature.

Create Emergency Session Call Flow

This section describes the create emergency session (IMEI, Unauthenticated IMSI) call flow.

Figure 37: Create Emergency Session Call Flow



For an Emergency call, cnSGW-C receives an Initial Attach Request in CSR with an UnAuthenticated IMSI, or with an IMEI only. cnSGW-C allocates TEID and SEID from the Node Manager and sends the Sx Establishment Request with local SEID to the UP to establish the session.

Once cnSGW-C receives the Sx Establishment Response from the UP with the UP SEID and the local GTPU TEID for S5 and S1 GTPU FTEID, cnSGW-C sends the Create Session Request to the PGW using EGTP EP. After receiving response from the PGW for Create Session Response, cnSGW-C sends the Sx Modification Request to connect S5-GTPU tunnel between PGW-U and SGW-U. On successful reception of Sx Modification Response, cnSGW-C sends the Create Session Response to the MME and the session is created in CDL.

With Initial attach procedure, cnSGW-C supports handling of Modify Bearer Request which connects S1 GTPU tunnel between eNodeB and SGW-U. When cnSGW-C receives MBR, it sends Sx Modification Request to connect S1 GTPU tunnel between eNodeB and SGW-U. After receiving Sx Modification Response, cnSGW-C sends Modify Bearer Response to the MME. Session is updated in CDL as the end of transaction.

OAM Support

This section describes operations, administration, and maintenance information for this feature.

Bulk Statistics Support

Emergency Counters

```
sgw_ue_stats{app_name="SMF",cluster="Local",data_center="DC",gr_instance_id="1",
instance_id="0",rat_type="EUTRAN",service_name="sgw-service",status="emergency_release"}
 9
```

```
sgw_ue_stats{app_name="SMF",cluster="Local",data_center="DC",gr_instance_id="1",
instance_id="0",rat_type="EUTRAN",service_name="sgw-service",status="emergency_setup"}
 9
```

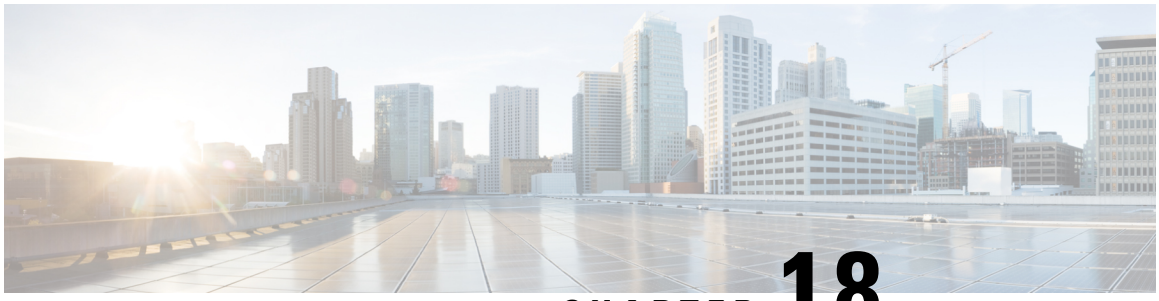
Emergency Statistics

```
db_records_total{app_name="datastore-ep",cluster="session",data_center="test",db=
"session",instance_id="3232257055",service_name="datastore-ep",session_type="SGW:
emergency_call:true",sliceName="1",systemId=""} 1
```

```
db_records_total{app_name="datastore-ep",cluster="session",data_center="test",db=
"session",instance_id="3232257055",service_name="datastore-ep",session_type="SGW:
rat_type:EUTRAN",sliceName="1",systemId=""} 3
```

```
db_records_total{app_name="datastore-ep",cluster="session",data_center="test",db=
"session",instance_id="3232257055",service_name="datastore-ep",session_type="SGW:
state:active",sliceName="1",systemId=""} 3
```

```
db_records_total{app_name="datastore-ep",cluster="session",data_center="test",db=
"session",instance_id="3232257055",service_name="datastore-ep",session_type="total",
sliceName="1",systemId="1"} 3
```



CHAPTER 18

eMPS/WPS Support

Feature Summary and Revision History

Summary Data

Table 61: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration required to enable
Related Documentation	Not Applicable

Revision History

Table 62: Revision History

Revision Details	Release
First introduced.	2021.02.0

Feature Description

This feature supports the following:

- Enhanced Multimedia Priority Service (eMPS) or Wireless Priority Service (WPS)
- eMPS GTPv2 Load/Overload Self Protection Exclusion
- Message Priority Profiles to define priority either at global level or at each interface level (PFCP, GTP).

eMPS/WPS Support

Feature Description

This feature supports identifying the eMPS subscriber. The feature sets the message priority bit for:

- PFCP interface towards the UP.
- GTPC interface towards the MME and PGW.

This feature includes DSCP marking for request messages in control messages as per the configured value in the profile for eMPS subscriber.

eMPS GTPv2 Load/Overload Self Protection Exclusion Support

Feature Description

cnSGW-C supports interaction of eMPS with GTPv2 load or overload feature. It supports excluding eARPs /APNs/Emergency call during self-protection mode in GTPv2 load or overload feature.

cnSGW-C can exclude the dnn-list, arp-list, and qci-list from the rejection for incoming request messages in self-protection mode. cnSGW-C excludes this rejection in the following manner:

- Excludes the dnn-list from rejection for any call level procedure when subscriber APN name (NI+OI) matches with *overload-exclude-profile*
- Excludes bearer modification or creation from rejection for any new or existing ARP (Priority-Level) value
- Excludes bearer modification or creation from rejection for any new or existing QCI value.
- Excludes the delete bearer or the session operations, such as Delete Bearer Request, Delete Session Request, Delete Bearer command from rejection irrespective of the overload-exclude-profile configuration

Note cnSGW-C does not support message throttling.

Feature Configuration

Configuring this feature involves the following steps:

- Configure WPS-Profile. For more information, refer to Configuring WPS Profile, on page 173.

- Configure SGW-Profile, and enable WPS-Profile and SGW-Profile association. For more information, refer to Configuring WPS-Profile and SGW-Profile Association, on page 173.
- Configure DNN-Profile, and enable WPS-Profile and DNN-Profile association. For more information, refer to Configuring WPS-Profile and DNN-Profile Association, on page 174.

Configuring WPS Profile

To configure this feature, use the following configuration:

```
config
  profile wps wps_name
    arp arp_value message-priority-profile msg_priority_profile_name
    dscp dscp_value
    message-priority [ pfcp | gtpc ]
    end
```

NOTES:

- **wps** *wps_name*—Specify the WPS service name. Must be a string.
- **arp** *arp_value*—Specify the range of ARP levels (separated by , or -). Must be an integer or a string. WPS session is decided based on ARP.
- **message-priority-profile** *msg_priority_profile_name*— Specifies that a message-priority profile is added in ARP list within WPS profile. WPS session is decided based on the configured ARP and the associated message priority profile inside the WPS profile.
- **dscp** *dscp_value*—Specify the DSCP marking value in the decimal range 0-63 or hex range 0x0-0x3F. Must be a string.

Configuration Example

The following is an example configuration.

```
config
   profile wps wp1
     arp 2 message-priority-profile message_priority_name
   end
```

Configuration Verification

To verify the configuration:

```
show full-configuration profile wps wps1
profile wps wps1
arp 2 message-priority-profile mp1
exit
```

Configuring WPS-Profile and SGW-Profile Association

To configure WPS-Profile and SGW-Profile association, use the following configuration:

```
config
 profile sgw sgw_name
```

```
wps-profile wps_name
end
```

NOTES:

- **wps-profile** *wps_name*—Specify the Wireless Priority Service (WPS) name. Must be a string.

Configuration Example

The following is an example configuration.

```
config
   profile sgw sgw1
     wps-profile wp1
     end
```

Configuration Verification

To verify the configuration:

```
show running-config profile sgw
profile sgw sgw1
wps-profile wp1
```

Configuring WPS-Profile and DNN-Profile Association

This section describes how to configure WPS-Profile and DNN-Profile association.

Note If WPS profile is associated with SGW profile and DNN profile, DNN profile takes the priority.

To configure WPS-Profile and DNN-Profile association, use the following configuration:

```
config
 profile dnn dnn_name
   wps-profile wps_name
   end
```

Configuration Example

The following is an example configuration.

```
config
  profile dnn dnn1
  wps-profile wps1
  end
```

Configuration Verification

To verify the configuration:

```
show running-config profile dnn
profile dnn dnn1
wps-profile wps1
```

Feature Configuration

Configuring this feature involves the following steps:

- Configure Overload Exclude Profile. For more information, refer to Configuring Overload Exclude Profile, on page 175.
- Configure Overload-Profile, and enable Overload Exclude Profile and SGW-Profile Association. For more information, refer to Associating the Overload-Profile with SGW-Profile Association, on page 175.

Configuring Overload Exclude Profile

To configure the Overload Exclude profile, use the following configuration:

```
config
  profile overload-exclude overload_exclude_profile_name
    dnn-list list_of_dnn
    arp-list list_of_arp

    end
```

NOTES:

- **overload-exclude** *overload_exclude_profile_name*— Specify the exclude overload profile name.
- **dnn-list** *list_of_dnn*—Specify the list of DNNs that needs to be excluded from throttling decision. Maximum three entries are allowed.
- **arp-list** *list_of_arp*—Specify the ARP list that needs to be excluded from throttling decisions. Must be an integer in the range of 1-15. Maximum eight entries are allowed.

Configuration Example

The following is an example configuration.

```
config
   profile overload-exclude oe1
     dnn-list  starent.com
     arp-list  1
     qci-list  1
     end
```

Configuration Verification

To verify the configuration:

```
show running-config profile overload-exclude
profile overload-exclude oe1
dnn-list  starent.com
arp-list  1 2
qci-list 3 4 5 6
end
```

Associating the Overload-Profile with SGW-Profile Association

The association of the Overload-Profile and the SGW-Profile, can be configured.

To configure this feature use the following configuration:

```
config
   profile overload overload_profile_name
      overload-exclude-profile self-protection self_protection_profile_name
   node-level
      tolerance
         minimum min_percentage
         maximum max_percentage
      reduction-metric
         minimum min_percentage
         maximum max_percentage
         advertise
         interval interval_value
         change-factor
         exit
      interface gtpc
         overloaded-action [ advertise ]
         exit
      exit
   exit
   profile load load_name
   load-calc-frequency load_calc_frequency_value
   load-fetch-frequency load_fetch_frequency_value
   advertise
   interval interval_value
   change-factor change_factor_value
```

```
   exit
   interface gtpc
   action advertise
   exit
exit
profile sgw sgw_name
load-profile profile_name
overload-profile overload_profile_name
end
```

NOTES:

- **overload** *overload_name*—Specify the overload protection profile name. Must be a string.
- **overload-exclude-profile**—Excludes profiles for overload scenarios.
- **self-protection** *overload_value*—Specify the profile to be excluded for self-protection. Must be a string.
- **tolerance minimum** *min_percentage*—Specify the minimum tolerance level below which the system is in a normal state. Must be an integer in the range of 1-100. The default value is 80.
- **tolerance maximum** *max_percentage*—Specify the maximum tolerance level above which the system is in a self-protection state. Must be an integer in the range of 1-100. The default value is 95.

- **reduction-metric minimum** *min_percentage*—Specify the percentage of reduction along with minimum tolerance-level for configuration. Must be an integer in the range of 1-100. The default value is 10.
- **reduction-metric maximum** *max_percentage*—Specify the percentage of reduction along with maximum tolerance-level for configuration. Must be an integer in the range of 1-100. The default value is 100.
- **interval** *interval_value*—Specify the advertising interval in seconds. Must be an integer in the range of 0-3600. The default value is 300 seconds.
- **validity** *validity_value*—Specify the validity period of the advertised OCI value in seconds. Must be an integer in the range of 1-3600. The default value is 600 seconds.
- **change-factor** *change_factor_value*—Specify the minimum change between current OCI and last indicated OCI, after which the advertising should happen. Must be an integer in the range of 1-20. The default value is five.
- **profile load** *load_name*—Specify the name of the load profile. Must be a string.
- **load-calc-frequency** *load_calc_frequency_value*—Specify the system load calculation interval in seconds. Must be an integer in the range of 5-3600. The default value is 10 seconds.
- **load-fetch-frequency** *load_fetch_frequency_value*—Specify the time interval in seconds at which the service pods fetch load from the cache pod. Must be an integer in the range of 5-3600. The default value is 10 seconds.
- **load-profile** *profile_name*—Specify the name of the load profile.
- **overload-profile** *overload_profile_name*—Specify the name of the overload profile.
- : Specify the exclude overload profile name:
  - : Specify the ARP list that needs to be excluded from throttling decisions. Must be an integer in the range of 1-15. Maximum eight entries are allowed.
  - : Specify the list of DNNs that needs to be excluded from throttling decision. Maximum three entries are allowed.
  - **message-priority**: Specify upto which message periority to be excluded from throttling decisions.
  - **procedure-list**: Procedures to be excluded from throttling decisions. This parameter is applicable only for Self-Protection.
  - : Specify the QoS Class Identifier to be excluded from throttling decisions. Must be an integer in the range of 1-.254. Maximum 8 entries are allowed. For example, range values can be 1-9,65,66,69,70,80,82,83,128-254.

Configuration Example

The following is an example configuration.

```
config
profile overload op
overload-exclude-profile self-protection <overload-exclude-profile-name>
node-level
tolerance minimum 5
tolerance maximum 50
reduction-metric minimum 50
reduction-metric maximum 100
advertise
```

```
interval 0
change-factor 1
exit
interface gtpc
overloaded-action [ advertise ]
exit
exit
exit
profile load lp
load-calc-frequency 120
load-fetch-frequency 15
advertise
interval 0
change-factor 1
exit
interface gtpc
action advertise
exit
exit
profile sgw <sgw_name>
load-profile <profile_name>
overload-profile <overload_profile_name>
end
```

Configuration Verification

To verify the configuration:

```
show running-config profile
profile sgw sgw1
load lp1
overload op1
end
```

OAM Support

This section describes operations, administration, and maintenance information for this feature

Bulk Statistics Support

The following are the examples for eMPS messages:

```
sgw_pdn_emps_counters{app_name="smf",cluster="cn",data_center="cn",instance_id="0",
service_name="sgw-service",status="active"} 1
```

```
sgw_pdn_emps_stats{app_name="smf",cluster="cn",data_center="cn",instance_id="0",
service_name="sgw-service",status="release"} 7
```

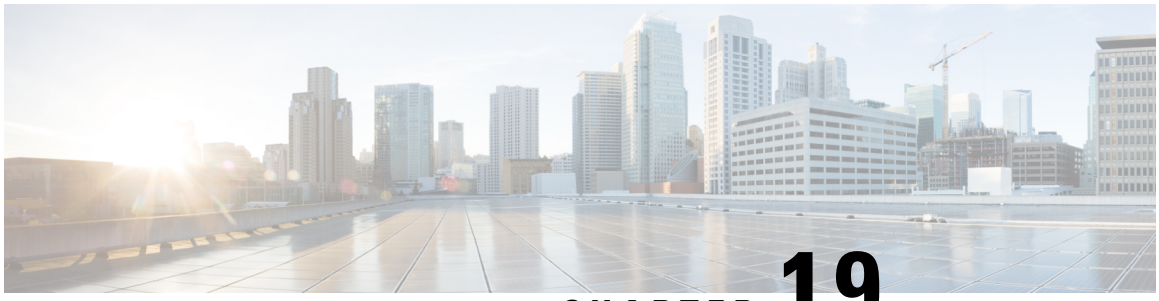
```
sgw_pdn_emps_stats{app_name="smf",cluster="cn",data_center="cn",instance_id="0",
service_name="sgw-service",status="setup"} 8
```

```
gtpc_app_priority_events{app_name="smf",cluster="smf",data_center="smf",event_type=
"NumRxModifyBearerResFrmSerSuccess",instance_id="0",
interface_type="S11",priority_msg="true",service_name="gtpc-ep"} 3
```

```
gtpc_app_priority_events{app_name="smf",cluster="smf",data_center="smf",event_type=
"RxCreateSessionRes",instance_id="0",interface_type="S5E",
priority_msg="true",service_name="gtpc-ep"} 2
```

```
proto_pfcp_msg_total{app_name="smf",cluster="smf",data_center="smf",instance_id="0",
interface_type="SXA",message_direction="outbound",
message_name="N4_MSG_SESSION_ESTABLISHMENT_REQUEST",msgpriority="True",service_name=
"protocol",status="accepted",transport_type="origin"} 2
```

```
proto_pfcp_msg_total{app_name="smf",cluster="smf",data_center="smf",instance_id="0",
interface_type="SXA",message_direction="outbound",
message_name="N4_MSG_SESSION_MODIFICATION_REQUEST",msgpriority="True",service_name="protocol",
status="accepted",transport_type="origin"} 6
```



CHAPTER 19

Failure and Error Handling Support

Feature Summary and Revision History

Summary Data

Table 63: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 64: Revision History

Revision Details	Release
First introduced.	2021.01.0

Overview

cnSGW-C supports:

- Attach and Detach failure and error handling.
- Create, Update, Delete Bearer Request and Response failure and error handling.
- Radio Access Bearer or Modify Beare Request failure and error handling.

The different types of failures that can occur during the call processing are as follows, except for Session Setup timer:

- Advance validation failure on request and response.
- Retransmission timeout.
- Transaction service level agreement (SLA).
- Failure reported from peer (UP, PGW, or MME depending on the stage of message process).

For Session Setup timer during attach procedure, following failures can happen:

- Ongoing PDN establishment and Modify Bearer Request from MME isn't received for Initial Attach and multi-PDN.

Attach and Detach Failure and Error Handling

cnSGW-C supports the following:

- Setup timeout functionlaity
- Failure response handling for:
  - Clear Session Request as a part of the Initial Attach and additional PDN setup procedures
  - Delete Beare Request and Delete Session Request processing for the PGW and UPF

Create Session Request Failure Handling

This section covers the Create Session Request procedure failure scenarios.

When failure occurs during Initial Attach procedure, subscriber context isn't created,

When another PDN setup fails, PDN isn't created in subscriber context.

The following table summarizes cnSGW-C behavior during different stages in the call processing for various failure types:

Table 65: cnSGW-C Behavior for Create Session Request Proceudure Failure Scenarios

Scenarios	Sx Signaling (Revert)	S11 Signaling (Revert)	S5 Signaling
• Create Session Request advance validation failure • Sx Session Establishment Response failure from User Plane (UP)	No	Negative - Create Session Response	No
• Create Session Response failure	Yes Delete traffic endpoint for newly created bearers	Negative - Create Session Response	No
• Sx Modify Response process failure	Yes Delete traffic endpoint for newly created bearers	Negative - Create Session Response	Delete Session Request to delete newly created session

Delete Default Bearer Procedure Failure Handling

This section covers the PGW-initiated default bearer deletion procedure failure scenarios.

The following table summarizes cnSGW-C behavior during different stages of call processing for various failure types:

Table 66: cnSGW-C Behavior for Delete Default Bearer Procedure Failure Scenarios

Scenarios	SGW-service Behavior	Signaling	Output
Delete Bearer Request advance validation failure	Send failure/No signaling over Sx/PGW	Negative - S5 Delete Bearer Response	Session/PDN is not deleted
Sx Session Modify failure	Skip failure and continue	Send S11 Delete Bearer Request towards MME S5 Delete Bearer Response (Cause = Accepted) Sx Delete Request (to Delete traffic endpoint) depends upon Sx Session Modify Response	Session/PDN is deleted
S11 Delete Bearer Request failure	Skip failure and continue	Send Delete Bearer Response (Cause = Accepted) to PGW Sx Delete Request (to Delete traffic endpoint)	Session/PDN is deleted

Scenarios	SGW-service Behavior	Signaling	Output
Sx Session Delete Request failure	Skip failure and continue	Send Delete Bearer Response (Cause = Accepted) to PGW	Session/PDN is deleted

Delete Session Procedure Failure Handling

This section covers the MME-initiated Deletion Session procedure failure scenarios.

The following table represents cnSGW-C behavior for the failure scenarios:

Table 67: cnSGW-C Behavior for Delete Session Procedure Failure Scenarios

Scenarios	SGW-service Behavior	Signaling	Output
Delete Session Request advance validation failure	Send failure/No signaling over Sx/MME	Negative - S11 Delete Session Response	Session/PDN is not deleted
Sx Session Modify Request failure	Skip failure and continue	Send Delete Session Request towards PGW Send Delete Session Response (Cause = Accepted) to MME Sx Delete Request (to Delete traffic endpoint) depends upon Sx Session Modify Response	Session/PDN is deleted
S5 Delete Session Request failure	Skip failure and continue	Send Delete Session Response (Cause = Accepted) to MME Sx Delete Request (to Delete traffic endpoint)	Session/PDN is deleted
Sx Session Delete Request failure	Skip failure and continue	Send Delete Session Response (Cause = Accepted) to MME	Session/PDN is deleted

Session Setup Timer during Attach Procedure

This section covers the session setup timer during attach procedure.

The following table represents cnSGW-C behavior for the session timeout scenarios:

Table 68: cnSGW-C Behavior for Session Timeout Failure Scenarios

Scenarios	Sx Signaling (Revert)	S11 Signaling (Revert)	S5 Signaling	Output
Session setup timeout expired after SGW sends Create Session Response to MME and waits for the Modify Bearer Request from MME.	Sx Delete Request (To delete traffic endpoint for newly created bearers)	Delete Session Request	Delete Bearer Request	Session/PDN is deleted

Create-Update-Delete Bearer Request and Response Failure and Error Handling

This section describes create, update, and deletge bearer request and response failure and error handling scenarios.

Create Bearer Procedure Failure Handling

This section covers the PGW-initiated dedicated bearer creation procedure failure scenarios.

The following table summarizes cnSGW-C behavior during different stages of call processing for various failure types:

Note During processing of create dedicated Bearer Request and Response, if SGW receives Context Not Found from peer (MME/UP) it deletes the PDN without performing any signaling towards the peer which sent this cause.

Table 69: cnSGW-C Behavior for Create Bearer Procedure Failure Scenarios

Scenarios	Sx Signaling (Revert)	S11 Signaling (Revert)	S5 Signaling	Output
• Create Bearer Request advance validation failure • Sx Session Modify Request failure (request sent to UP to allocate tunnel endpoint and GTPU TEIDs).	No	No	Negative - Create Bearer Response to PGW	New Bearer Context is not created.

Scenarios	Sx Signaling (Revert)	S11 Signaling (Revert)	S5 Signaling	Output
Create Bearer Request is sent to MME and SGW is waiting for the Response.	Yes To remove traffic endpoint for newly created bearers.	No	Negative - Create Bearer Response to PGW	New Bearer Context is not created. Optional parameters of Create Bearer Response are ignored.
SGW receives Create Bearer Resposne from MME and sends Sx Modify to UP to connect GTPU tunnel between eNodeB and SGW-U.	Yes To remove traffic endpoint for newly created bearers.	Yes To delete newly created bearers.	Negative - Create Bearer Response to PGW	New Bearer Context is not created. Optional parameters of Create Bearer Response are ignored.
Failure in Revert handling for the Delete Bearer Request or Sx Modify Request.	No	No	Negative - Create Bearer Response	Bearer Context is not created. Optional parameters of Create Bearer Response are ignored.

Delete Dedicated Bearer Procedure Failure Handling

This section covers the PGW-initiated dedicated bearer deletion procedure failure scenarios.

The following table summarizes cnSGW-C behavior during different stages of the call processing for various failure types:

Note During processing of delete dedicated Bearer Request and Response if SGW receives Context Not Found from peer (MME/UP), it deletes the PDN without performing any signaling towards the peer which sent this cause.

Table 70: cnSGW-C Behavior for Delete Dedicated Bearer Procedure Failure Scenarios

Scenarios	SGW-Service Behavior	Signaling	Output
Delete Bearer Request advance validation failure	Send failure/No Signaling over Sx/MME	Negative - Delete Bearer Response to PGW	Dedicated Bearer is not deleted.

Scenarios	SGW-Service Behavior	Signaling	Output
Partial Accepted: Delete Bearer Request received with multiple EBI's, where: • Some EBIs belong to PDN • Some EBIs don't belong to PDN/Invalid EBIs	Continue DBR Procedure and delete all existing bearers for which Delete Bearer Request is received. S11 Delete Bearer Request should carry only existing EBIs information Sx Session Modification Request should carry existing EBIs information (Remove Traffic Endpoint)	S5 Delete Bearer Response (Cause = Partially Accepted)	S5 Delete Bearer Response where message level cause is Partially Accepted and bearer level cause is: • **Some EBIs belong to PDN:** S11 Delete Bearer Response • **Some EBIs does not belong to PDN/Invalid EBIs:** Context Not Found CDL is updated (Remove all existing bearers)
Sx Session Modify to set action as DROP	Skip failure and continue	S5 Delete Bearer Response (Cause = Accepted)	Skip failure and continue with DBR Procedure Call Flow: Yes S5 Delete Bearer Response (Cause = Accepted) CDL is updated
S11 Delete Bearer Request Failure	Skip failure and continue	S5 Delete Bearer Response (Cause) = Accepted	Skip failure and continue with DBR Procedure Call Flow: Yes CDL is updated
Sx Session Modify Request failure (Request to remove traffic endpoint on UP)	Skip failure and continue	S5 Delete Bearer Response (Cause = Accepted)	Skip failure and continue with DBR Procedure Call Flow: Yes CDL is updated

Update Bearer Procedure Failure Handling

This section covers the PGW-initiated update bearer procedure failure scenarios.

The following table summarizes cnSGW-C behavior during different stages in call processing for various failure types:

Table 71: cnSGW-C Behavior for Update Bearer Procedure Failure Scenarios

Scenarios	S5/Sx Signaling	Output
Update Bearer Request advance validation failure	Negative - Update Bearer Response	No change in Bearer/PDN context.

Scenarios	S5/Sx Signaling	Output
Update Bearer Request with non-existing EBIs	Update Bearer Response with message level cause as REQ_PARTIALLY_ACCEPTED. Bearer level cause for non-existing EBIs as Context Not Found. (Normal handling for existing EBIs)	Update Bearer Response with message level cause as REQ_PARTIALLY_ACCEPTED. Bearer level cause for non-existing EBIs as CONTEXT_NOT_FOUND. Normal handling for existing EBIs. CDL is updated for existing EBIs only.
Update Bearer Request is sent to MME and waiting for the response	Negative - Update Bearer Response	Negative - Update Bearer Response CDL is not updated.
S11 Update Bearer Response (Message level Cause == CONTEXT_NOT_FOUND) and S5 Update Bearer Req/Rsp had default bearer in the bearer context list	Sx Delete Req/Rsp Negative - Update Bearer Response	Negative - Update Bearer Response CDL is not updated. Statistics/Transactional Logs PDN Key Release + PDN deallocation If this is the last PDN, then resource manager is released, all subscriber keys are released and subscriber deallocation is done.
S11 Update Bearer Response (Message level Cause == CONTEXT_NOT_FOUND) and S5 Update Bearer Req/Rsp didn't have default bearer in the bearer context list	Sx Modify Req/Rsp Negative - Update Bearer Response	CDL is not updated.
S11 Update Bearer Response (Message level Cause == REQ_PARTIALLY_ACCEPTED, Bearer Context Cause == Any failure for dedicated bearer)	Sx Modify Req/Rsp Update Bearer Response with message level cause as REQ_PARTIALLY_ACCEPTED	Update Bearer Response with message level cause as REQ_PARTIALLY_ACCEPTED CDL is updated for successful bearers.

Scenarios	S5/Sx Signaling	Output
S11 Update Bearer Response (Message level Cause == REQ_PARTIALLY_ACCEPTED, Bearer Context Cause == CONTEXT_NOT_FOUND for default bearer)	Sx Delete Req/Rsp Negative - Update Bearer Response	Negative - Update Bearer Response CDL is not updated. PDN Key Release and PDN deallocation If this is the last PDN, then resource manager is released, all subscriber keys are released and subscriber deallocation is done.
If Sx modify is triggered after Update Bearer Response: • Sx Session Modify Request (IPC/Retransmission Timeout/Internal Failure and so on) • Sx Session Modify Response (Cause != ACCEPTED except CONTEXT_NOT_FOUND)	Ignore failure and continue	Ignore failure and continue
If Sx Modify is triggered after Update Bearer Response: • Sx Session Modify Response (Cause == CONTEXT_NOT_FOUND)	[1]	[2]
If Sx Delete is triggered after Update Bearer Response: • Sx Session Delete Request (IPC/Retransmission Timeout/Internal Failure and so on) • Sx Session Delete Response (Cause != ACCEPTED) • Resource manager release (Internal Error)	Ignore failure and continue	Ignore failure and continue

[1] As part of Update Bearer Procedure handling, SGW-service triggers new transaction for PDN deletion:

- Sx Failure Cause received as part of Sx Session Modification Response
  - Context Not Found

SGW Behavior (New Transaction):

- SGW triggers S11 Delete Bearer Request and S5 Delete Session Request to delete that PDN
- No Sx Signaling

SGW Behavior (Update Bearer Transaction): SGW sends S5 Update Bearer Response with Cause as No Resource Available, as part of Update Bearer Procedure Transaction. Also, SGW doesn't initiate any signaling towards UP as soon as it receives Sx Session Modification Response with cause as Context Not Found.

2 As part of Update Bearer Procedure handling, SGW-SVC additionally triggers new transaction for PDN deletion:

- Sx Failure Cause received as part of Sx Session Modification Response
  - Context Not Found

SGW Behavior (New Transaction):

- SGW triggers S11 Delete Bearer Request and S5 Delete Session Request to delete that PDN
- No Sx Signaling

SGW Behavior (Update Bearer Transaction): SGW sends S5 Update Bearer Response with Cause as No Resource Available, as part of Update Bearer Procedure Transaction. Also, SGW doesn't initiate any signaling towards UP as soon as it receives Sx Session Modification Response with cause as Context Not Found.

Radio Access Bearer/Modify Bearer Request Failure and Error Handling

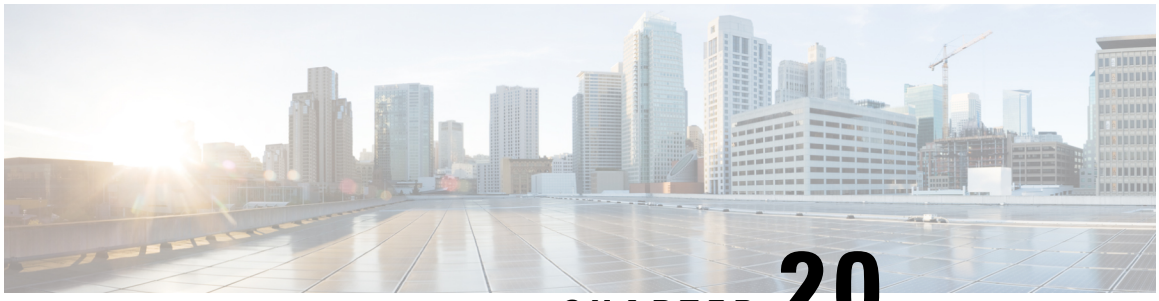
This section covers the Radio Access Bearers (RAB), Modify Bearer Request and Response (MBR) from PGW and User Plane (UP) failure scenarios.

The following table summarizes cnSGW-C behavior during different stages of call processing for various failure types:

Table 72: cnSGW-C Behavior for Radio access Bearer and Modify Bearer Response Procedure Failure Scenarios

Message Type	Failure Interface	Failure Response Recevied	Failure Response to be sent	Handling
MBR initial attach	Sx	CONTEXT_NOT_FOUND	EGTP_CAUSE_ NO_RESOURCES_ AVAILABLE	Cleanup PDN with DSR towards PGW and DBR towards MME
		Other Failure Response	EGTP_CAUSE_ NO_RESOURCES_ AVAILABLE	Cleanup PDN with DSR towards PGW and DBR towards MME. Sx_Modification_Req/ Sx_Session_Delete to cleanup resource on UP
	Timeout	Timeout on PFCP	EGTP_CAUSE_ NO_RESOURCES_ AVAILABLE	Cleanup PDN with DSR towards PGW and DBR towards MME. Sx_Modification_Req/ Sx_Session_Delete to cleanup resource on UP
MBR Service Request	Sx	CONTEXT_NOT_FOUND	EGTP_CAUSE_ NO_RESOURCES_ AVAILABLE	Cleanup PDN with DSR towards PGW and DBR towards MME
		Other Failure Responses	EGTP_CAUSE_ NO_RESOURCES_ AVAILABLE	Do not update anything in PDN, Ignore S5 Signaling
		Timeout	EGTP_CAUSE_ NO_RESOURCES_ AVAILABLE	Do not update anything in PDN, Ignore S5 Signaling
	S5	EGTP_CAUSE_ CONTEXT_NOT_ FOUND	EGTP_CAUSE_ CONTEXT_NOT_ FOUND	Sx_Session_Delete send to UP MBRsp failure to MME (No DBR/DSR)
		Other Failure Responses	Failure Response received from PGW	Do not update PDN/DB
	Timeout	Timeout from PGW	EGTP_CAUSE_ PEER_NOT_ RESPONDING	Do not update PDN/DB

Message Type	Failure Interface	Failure Response Recevied	Failure Response to be sent	Handling
RAB	Sx	CONTEXT_ NOT_FOUND (Single PDN call)	EGTP_CAUSE_ REQ_ACCEPTED	Cleanup PDN with DSR towards PGW and DBR towards MME
		CONTEXT_ NOT_FOUND (Multi PDN call and context not found for one PDN)	Send RAB Resp (EGTP_CAUSE_ REQ_ACCEPTED)	Cleanup the PDN for which context not found received with DSR towards PGW and DBR towards MME Move other PDN/UE to IDLE
		Other Failure Response	EGTP_CAUSE_ REQ_ACCEPTED	Move PDN/UE to IDLE
		Timeout	EGTP_CAUSE_ REQ_ACCEPTED	Move PDN/UE to IDLE



CHAPTER 20

GTPC and Sx Path Management

Feature Summary and Revision History

Summary Data

Table 73: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	GTPC and Sx Path Management: Disabled – Configuration required to enable GTPC Path Failure: Enabled – Always-on Sx Path Failure: Enabled – Always-on Path Failure Detection Customization: Disabled – Configuration required to enable
Related Documentation	Not Applicable

Revision History

Table 74: Revision History

Revision Details	Release
First introduced.	2021.02.0

Feature Description

The GTPC and Sx Path Management feature supports the following:

- GTPC path management using Echo Request and Echo Response messages.
- Sx path management using PFCP Heartbeat Request and Heartbeat Response. Node-level heartbeat procedures between the SGW-C and UPF.
- Detection of the GTPC path failure on S11 and S5 interface.
- Detection of the Sx path failure on the Sx interface.
- Configuration of the path failure detection policy to configure the path failure detection capability.

GTPC and Sx Path Management

Feature Description

GTPC and Sx Path Management supports the following:

- GTPC path management using Echo Request and Echo Response exchange over S5 and S11 interface to check peer aliveness.
- Sx path management using Packet Forwarding Control Protocol (PFCP) Heartbeat Request and Heartbeat Response exchange over Sx interface to check peer aliveness.

Feature Configuration

Configuring this feature involves the following steps:

- Configure the echo parameters. For more information, refer to Configuring the Echo Parameters, on page 195.
- Configure the heartbeat parameters. For more information, refer to Configuring Heartbeat, on page 195.
- Verify the peer configuration. For more information, refer to Viewing the Peer Configuration, on page 196.

Configuring the Echo Parameters

To configure the Echo parameters, use the following configuration:

Enabling the Echo Request

To enable the Echo Request, use the following configuration:

```
config
   instance instance-id instance_id
      endpoint endpoint_name
         interface [ s11 | s5e ]
           echo interval interval_value
           echo max-retransmissions max_retransmissions_count
           echo retransmission-timeout retransmission_timeout_count
           end
```

NOTES:

- **interval** *interval_value*—Specify the echo interval in seconds. Must be an integer in the range of 60-3600. Default value is 60 seconds.
- **max-retransmissions** *max_retransmissions_count*—Specify the maximum number of retries for GTP Echo Request. Must be an integer in the range of 0-15. Default value is 3.
- **retransmission-timeout** *retransmission_timeout_count*—Specify the Echo Request retransmission timeout period in seconds. Must be an integer in the range of 1-20. Default value is 5.

Disabling the Echo Request

To disable the Echo Request, use the following configuration:

```
config
   instance instance-id instance_id
      endpoint endpoint_name
         replicas replicas_count
         interface interface_name
            no echo
            end
```

Configuring Heartbeat

To configure the heartbeat parameters, use the following configuration:

Enabling Heartbeat

To enable a heartbeat, use the following configuration:

```
config
   instance instance-id instance_id
      endpoint pfcp
         interface sxa
            heartbeat
            interval interval
            retransmission-timeout timeout
```

```
max-retransmissions retransmission_count
end
```

NOTES:

- **interval** *heartbeat_interval*—Specify the heartbeat interval in seconds. Must be an integer in the range of 0-3600. To disable, set to 0.
- **max-retransmissions** *max_retransmissions*—Specify the maximum number of retries for the PFCP Heartbeat Request. Must be an integer in the range of 0-15. Default value is 4.
- **retransmission-timeout** *retransmission_timeout*—Specify the heartbeat retransmission timeout period in seconds. Must be an integer in the range of 1-20. Default value is 5.

Disabling Heartbeat

To disable a heartbeat, use the following configuration:

```
config
   instance instance-id instance_id
      endpoint pfcp
         interface sxa
            heartbeat
            interval interval
            end
```

NOTES:

- **interval** *heartbeat_interval*—Specify the heartbeat interval as 0 to disable the heartbeat.

Viewing the Peer Configuration

To view the peer restart counter, use the following configuration:

The following command displays the peer configuration:

show peers all [endpoint] [local addr] [peer addr]

```
show peers all SXA 209.165.201.12:8805 209.165.201.18:8805 POD CONNECTED
ENDPOINT LOCAL ADDRESS PEER ADDRESS DIRECTION INSTANCE TYPE TIME RPC ADDITIONAL DETAILS
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
SXA 209.165.201.12:8805 209.165.201.18:8805 Inbound nodemgr-0 Udp 4 hours SGW-U Capacity:
65535,
LoadMetric: 0,LoadSeqNo: 0,Mode: Online,OverloadMetric: 0,OverloadSeqNo: 0,Priority: 65535

show peers all S11 209.165.201.4:2123 209.165.201.7:2123 LOCAL POD CONNECTED
ADDITIONAL ENDPOINT ADDRESS PEER ADDRESS DIRECTION INSTANCE TYPE TIME RPC DETAILS
-------------------------------------------------------------------------------------
-----------------
S11 209.165.201.4:2123 209.165.201.7:2123 Inbound nodemgr-0 Udp 25 seconds MME Recovery:
10

show peers all S5E 209.165.201.4:2123 209.165.201.21:2123 LOCAL POD CONNECTED
ADDITIONAL ENDPOINT ADDRESS PEER ADDRESS DIRECTION INSTANCE TYPE TIME RPC DETAILS
-------------------------------------------------------------------------------------
----------------
S5E 209.165.201.4:2123 209.165.201.21:2123 Inbound nodemgr-0 Udp 25 seconds PGW Recovery:
10
```

```
show peers all POD CONNECTED
ENDPOINT LOCAL ADDRESS PEER ADDRESS DIRECTION INSTANCE TYPE TIME RPC ADDITIONAL DETAILS
--------------------------------------------------------------------------------------------------------------------------------
<none> 209.165.201.29 209.165.201.18:8001 Outbound rest-ep-0 Rest 17 hours UDM <none>
<none> 209.165.201.29 209.165.201.18:8002 Outbound rest-ep-0 Rest 17 hours AMF <none>
<none> 209.165.201.29 209.165.201.18:8003 Outbound rest-ep-0 Rest 17 hours PCF <none>
<none> 209.165.201.29 209.165.201.18:8004 Outbound rest-ep-0 Rest 17 hours CHF <none>
<none> 209.165.201.29 209.165.201.18:9040 Outbound rest-ep-0 Rest 17 hours CHF <none>
S11 209.165.201.4:2123 209.165.201.6:2123 Inbound nodemgr-1 Udp 18 minutes MME Recovery:
10
S5E 209.165.201.12:2123 209.165.201.24:2123 Inbound nodemgr-1 Udp 5 hours PGW Recovery:
65535
SXA 209.165.201.12:8805 209.165.201.18:8805 Inbound nodemgr-0 Udp 22 minutes SGW-U Capacity:
 65535,LoadMetric: 0,LoadSeqNo: 0,Mode: Online,OverloadMetric: 0,OverloadSeqNo: 0,Priority:
 65535
```

Configuration Example

The following is an example configuration to enable the echo.

```
config
   instance instance-id 1
      endpoint gtp
         interface s11
            echo interval 60
            echo max-retransmissions 5
            echo retransmission-timeout 4
            end
```

The following is an example configuration to disable the echo.

```
config
   instance instance-id 1
      endpoint gtp
         replicas 1
         interface s5e
            no echo
            exit
         interface s11
            no echo
            end
```

OAM Support

This section describes operations, administration, and maintenance support for this feature.

Alerts

To configure Alerts for Peer Up and Peer Down, see *Key Performance Indicators* chapter in *Cisco Ultra Cloud Serving Gateway Control Plane Function - Metrics Reference*.

Bulk Statistics Support

Node Manager

The following are examples of Echo Transmitted and Echo Retransmitted messages:

```
nodemgr_gtpc_msg_stats{app_name="smf",cluster="cn",data_center="cn",gtpc_msg_type="gtpc_echo_req_retx",
gtpc_peer_ip="209.165.201.11",instance_id="1",interface_type="S5E",service_name="nodemgr"}
 3

nodemgr_gtpc_msg_stats{app_name="smf",cluster="cn",data_center="cn",gtpc_msg_type="gtpc_echo_req_tx",
gtpc_peer_ip="209.165.200.230",instance_id="1",interface_type="S11",service_name="nodemgr"}
 2

nodemgr_gtpc_msg_stats{app_name="smf",cluster="cn",data_center="cn",gtpc_msg_type="gtpc_echo_req_tx",
gtpc_peer_ip="209.165.201.11",instance_id="1",interface_type="S5E",service_name="nodemgr"}
 4

nodemgr_gtpc_msg_stats{app_name="smf",cluster="cn",data_center="cn",gtpc_msg_type="gtpc_echo_req_tx_initial",
gtpc_peer_ip="209.165.200.230",instance_id="1",interface_type="S11",service_name="nodemgr"}
 2

nodemgr_gtpc_msg_stats{app_name="smf",cluster="cn",data_center="cn",gtpc_msg_type="gtpc_echo_req_tx_initial",
gtpc_peer_ip="209.165.201.11",instance_id="1",interface_type="S5E",service_name="nodemgr"}
 1

nodemgr_gtpc_msg_stats{app_name="smf",cluster="cn",data_center="cn",gtpc_msg_type="gtpc_echo_res_rx",
gtpc_peer_ip="209.165.200.230",instance_id="1",interface_type="S11",service_name="nodemgr"}
 2
```

GTPC-EP Pod

The following are examples of Echo Request received and Echo Response sent messages:

```
gtpc_echo_msg_stats{app_name="smf",cluster="cn",data_center="cn",gtpc_msg_type="gtpc_echo_req_rx",
gtpc_peer_ip="209.165.200.230",instance_id="0",service_name="gtpc-ep"} 1

gtpc_echo_msg_stats{app_name="smf",cluster="cn",data_center="cn",gtpc_msg_type="gtpc_echo_req_rx",
gtpc_peer_ip="209.165.200.231",instance_id="0",service_name="gtpc-ep"} 1

gtpc_echo_msg_stats{app_name="smf",cluster="cn",data_center="cn",gtpc_msg_type="gtpc_echo_req_rx",
gtpc_peer_ip="209.165.201.11",instance_id="0",service_name="gtpc-ep"} 1

gtpc_echo_msg_stats{app_name="smf",cluster="cn",data_center="cn",gtpc_msg_type="gtpc_echo_res_tx",
gtpc_peer_ip="209.165.200.230",instance_id="0",service_name="gtpc-ep"} 1

gtpc_echo_msg_stats{app_name="smf",cluster="cn",data_center="cn",gtpc_msg_type="gtpc_echo_res_tx",
gtpc_peer_ip="209.165.200.231",instance_id="0",service_name="gtpc-ep"} 1

gtpc_echo_msg_stats{app_name="smf",cluster="cn",data_center="cn",gtpc_msg_type="gtpc_echo_res_tx",
gtpc_peer_ip="209.165.201.11",instance_id="0",service_name="gtpc-ep"} 1
```

Procedure-Level

The following are examples of how to check the incremented values of Heartbeat Request, Heartbeat Response, and Heartbeat Request retry.

```
nodemgr_up_hb_msg_stats{app_name="smf",cluster="Local",current_nodemgr_id="0",data_center="DC",
instance_id="0",interface_type="SXA",primary_nodemgr_id="0",service_name="nodemgr",up_ep_key=
"209.165.201.1:209.165.201.21",up_msg_type="up_heartbeat_req_retx"} 3
```

```
nodemgr_up_hb_msg_stats{app_name="smf",cluster="Local",current_nodemgr_id="0",data_center="DC",
instance_id="0",interface_type="SXA",primary_nodemgr_id="0",service_name="nodemgr",up_ep_key=
"209.165.201.1:209.165.201.21",up_msg_type="up_heartbeat_req_tx"} 5
```

```
nodemgr_up_hb_msg_stats{app_name="smf",cluster="Local",current_nodemgr_id="0",data_center="DC",
instance_id="0",interface_type="SXA",primary_nodemgr_id="0",service_name="nodemgr",up_ep_key=
"209.165.201.1:209.165.201.21",up_msg_type="up_heartbeat_rsp_rx"} 5
```

GTPC Path Failure

Feature Description

GTPC path failure detects peer-level GTPC path failure on the S11 and the S5 interface when:

- Echo Response contains a new restart counter value.
- Echo Request contains a new restart counter value.
- Echo Response is not received.
- Create Session Request or Modify Bearer Request contains a new restart counter value.
- Create Session Response or Modify Bearer Response contains a new restart counter value.

The connections may get disconnected due to different path failure is as follows:

- s11_path_failure
- s5e_path-failure
- s11_path_failure_local_purge
- s5e_ path_failure_local_purge
- s5e_recovery
- s11_recovery
- s5e_recovery_local_purge
- s11_recovery_local_purge

How it Works

This section describes how this feature works.

GTPC Path Failure Detection

Path failure is detected in the following conditions:

- Echo Failure: Echo failure occurs when the peer doesn't respond to the Echo Request or the retries.
- Restart Counter in Echo Response or Control Messages: The GTPC entity receives Recovery IE either in an Echo Response or from the peer GTPC message. GTPC entity compares the received the restart counter value with the previously stored restart counter value for that peer entity and performs the following:
  - Stores the received restart counter value for the peer when previously stored value isn't available.
  - When the max-remote-rc-change parameter is not configured, GTPC detects the change in the restart counter.
  - When max-remote-rc-change is configured, calculate the difference in the restart counter value considering restart counter rollover. Detects path failure when the difference between new and old restart counter is less than the value of max-remote-rc-change.

Note For more information on max-remote-rc-change, refer to Customization of Path Failure Detection, on page 204.

Path Failure Handling

Upon detecting a path failure, the network node notifies the failure through the Operation and Maintenance system and performs the following:

- Deletes the PDN connections (EPS bearer contexts) or the associated PDP contexts with peer IP address.
- Specifies the following actions for the selected interface:
  - **Local Purge:** The cnSGW-C clears the affected bearer (or PDN if the default bearer receives the path failure) locally without informing the peer. This action is default for all interfaces.

Note cnSGW-C sends the Sx Session Delete Request to UPF to clear session on path failure detection.

  - **Signal-Peer:** The cnSGW-C sends control signal towards the peer MME and P-GW.

    When signaling:

    - For PDN deletion, the SGW sends a Delete Session Request message to the PGW and a Delete Bearer Request (with LBI) message to the MME.
    - SGW sends a Delete Request on the S11 or the S5 interface to notify the peer.

Note Echo Request exchange is stopped when the peer is deleted.

Feature Configuration

Configuring this feature involves the following steps:

- Configure the action that must be taken on path failure detection. For more information, refer to Configuring Action on Path Failure Detection, on page 201.
- Configure the notification to update the peer node. For more information, refer to Configuring Notification to Update the Peer Node, on page 201.
- Verify the configuration. For more information, refer to Configuration Example, on page 201.

Configuring Action on Path Failure Detection

To configure the action for path failure detection, use the following configuration:

```
config
  profile sgw sgw_name
   path-failure [ s11 | s5e ] [ local-purge | signal-peer ]
   end
```

Configuring Notification to Update the Peer Node

Whenever cnSGW-C is restarted, the restart counter needs to be updated. For implementing this functionality, verify the Kubernetes use-volume-claims parameter value is set as true in Ops Center.

This configuration updates the restart counter when cnSGW-C restarts with the CLI system mode shutdown and system mode running.

Configuration Example

The following is an example configuration of path failure detection:

```
config
profile sgw sgw1
 path-failure s11 local-purge
 path-failure s5e local-purge
exit
```

OAM Support

This section describes operations, administration, and maintenance information for this feature.

Bulk Statistics Support

The following are examples of the GTPC path failure:

```
nodemgr_gtpc_pathfail_reasons{app_name="smf",cluster="cn",
data_center="cn",instance_id="1",pathfail_reason="pathfail_no_echo_rcv",
service_name="nodemgr"} 2
```

```
nodemgr_gtpc_pathfail_reasons{app_name="smf",cluster="cn",data_center="cn",
instance_id="0",pathfail_reason="pathfail_echo_res_rc_change",
service_name="nodemgr"} 1
```

Sx Path Failure

Feature Description

Sx path failure detects the path failure on the Sx interface when:

- Heartbeat Request contains a higher value of recovery timestamp.
- Heartbeat Response contains a higher value of recovery timestamp.
- Heartbeat Response is not received.
- Sx Association Request is received.
- cnSGW-C receives the Sx Association Update Request to release the peer.

How it Works

This section describes how this feature works.

Heartbeat Request

The cnSGW-C or UPF sends the Heartbeat Request on a path to the peer node to find out if the node is alive. The Heartbeat Request messages are sent for each peer with which a PFCP control association is established. cnSGW-C or UPF is prepared to receive the Heartbeat Request and it responds with a Heartbeat Response. The Heartbeat Request starts with the peer when a new session is established with the peer and it's stopped when the last session is released from the peer.

cnSGW-C and UPF send the Heartbeat Request based on the configured interval. If the peer doesn't respond, the message is retried for the configured number of times within the retry interval. After the response is received the defined action is taken for the calls associated with the corresponding peer.

Recovery Time Stamp is the IE which contains the start time of the peer node. The Heartbeat Request contains the selfrecovery timestamp value sent to the peer.

Note The heartbeat request is stopped only when the peer is deleted.

Heartbeat Response

The Heartbeat Response message is sent as a response to a received Heartbeat Request.

Recovery Timestamp is the IE which contains the start time of the node. Heartbeat Response contains the peer's Recovery Timestamp value.

Sx Path Failure Detection

Sx path failure is detected in the following conditions:

- **Heartbeat Failure:** When the peer doesn't respond to the heartbeat sent and also to the retries.
- **Recovery Timestamp Change in Heartbeat:** When the Heartbeat Response has a new Recovery Timestamp value then the previously received value. If the Recovery Timestamp value received is lower than the previously received value, the path failure isn't detected.
- **Sx Association Message:** When the Sx Association message is received again from the peer. In this case, all the calls are cleared and a notification is sent to eGTP peer.
- **Sx Association Release Message:** When the Sx Association release message is received. In this case, all the calls are cleared and a notification is sent to eGTP peer.

Path Failure Handling

When the recovery timestamp value received is more than the previously received value, the peer restart is detected. If the timestamp is lower than the previously received value, the value is ignored and peer restart isn't detected.

When the peer restart is detected to indicate the path failure for the peer, all the calls connected to that peer are cleared. The disconnection reason used for such calls is Sx path failure.

Sx association is also removed on detecting Sx path failure.

Heartbeat Handling

Whenever a PFCP entity receives a Heartbeat Request message (even from unknown peers), it responds with a Heartbeat Response message.

After a path failure is detected due to **No response to peer** error, no further Heartbeat Request is sent to that peer until the association is reestablished. Calls are cleared based on the path failure detection policy configuration.

Note After the Sx associations are removed, the heartbeat is stopped when Sx path failure is detected.

OAM Support

This section describes operations, administration, and maintenance support for this feature.

Bulk Statistics Support

The following are examples of the procedure-level statistics incremented for Heartbeat Request, Heartbeat Response, and Heartbeat Request retry:

```
nodemgr_up_hb_msg_stats{app_name="smf",cluster="Local",current_nodemgr_id="0",
data_center="DC",instance_id="0",interface_type="SXA",primary_nodemgr_id="0",service_name=
"nodemgr",up_ep_key="209.165.201.5:209.165.201.28",up_msg_type="up_heartbeat_req_retx"}
 3
```

```
nodemgr_up_hb_msg_stats{app_name="smf",cluster="Local",current_nodemgr_id="0",
data_center="DC",instance_id="0",interface_type="SXA",primary_nodemgr_id="0",service_name=
"nodemgr",up_ep_key="209.165.201.5:209.165.201.28",up_msg_type="up_heartbeat_req_tx"}
 5
```

```
nodemgr_up_hb_msg_stats{app_name="smf",cluster="Local",current_nodemgr_id="0",
data_center="DC",instance_id="0",interface_type="SXA",primary_nodemgr_id="0",service_name=
"nodemgr",up_ep_key="209.165.201.5:209.165.201.28",up_msg_type="up_heartbeat_rsp_rx"}
 5
```

Customization of Path Failure Detection

Feature Description

cnSGW-C lets you configure the path failure detection policy. By default, the path failure detection policy is enabled.

- **GTPC Path Failure Detection Customization:** GTPC path failure is detected when:
  - The Echo Request retries are exhausted.
  - The Echo Request or Response Restart counter is modified.
  - The control message Response Restart counter is modified.
  - If the absolute difference between the new and old restart counters is less than the value configured for max-remote-rc-change.

Note GTPC Path Failure Detection Customization allows user to ignore false peer restart with max remote restart counter (max-remote-rc-change) change functionality.

- **Sx Path Failure Detection Customization:** PFCP path failure is detected when:
  - The Heartbeat Request retries are exhausted.
  - The Heartbeat Request or Response recovery timestamps have modified.

Feature Configuration

Configuring this feature involves the following steps:

- Configure the GTPC path failure customization. For more information, refer to Configuring GTPC Path Failure Customization, on page 205.
- Configure the Sx path failure customization. For more information, refer to Configuring Sx Path Failure Customization, on page 205.

Configuring Sx Path Failure Customization

To configure the Sx path failure customization, use the following configuration:

```
config
  policy sx-path-failure-detection policy
   ignore heartbeat-retry-failure
   ignore heartbeat-recovery-timestamp-change
exit
 instance instance-id instance_id
   endpoint pfcp
     replicas replica_count
     sx-path-failure sx-detection-policy policy
     interface sxa
     sx-path-failure sx-detection-policy policy
     end
```

Configuring GTPC Path Failure Customization

To configure the GTPC path failure customization, use the following configuration:

```
config
   policy path-failure-detection policy_name
     max-remote-rc-change maximum_remote
     ignore echo-rc-change
     ignore control-rc-change
     ignore echo-failure
   exit
 exit
 instance instance-id instance_id
   endpoint gtp
     replicas replica_count


     path-failure detection-policy policy
     interface [ s11 | s5e ]
     end
```

NOTES:

- When GTPC path failure detection policy isn't configured at interface-level, endpoint-level path failure detection policy is applicable.
- The max-remote-rc-change configuration specifies the counter change after which the S11 or S5 detects a peer restart. A peer restart is detected only if the absolute difference between the new and old restart counter is less than the value configured. For example, if the max-remote-rc-change is 10 and current peer restart counter is 251, then eGTP detects a peer restart only if the new restart counter is 252 through

255 or 0 through 5. Similarly, if the stored restart counter is 1, eGTP detects a peer restart only if the new restart counter is 2 through 11.

- Valid settings are from 1 to 255. The recommended setting is 32.

OAM Support

This section describes operations, administration, and maintenance support for this feature.

Bulk Statistics Support

GTPC Path Failure

Maintain statistics indicating number of times path failure was detected due to restart counter change in echo request or response message or control request or response message.

```
nodemgr_gtpc_msg_stats{app_name="smf",cluster="Local",data_center="DC",
gtpc_msg_type="gtpc_false_peer_restart_cfg_ctrl_rc_change",gtpc_peer_ip=
"209.165.201.17",instance_id="0",interface_type="S11",service_name="nodemgr"} 1
```

```
nodemgr_gtpc_msg_stats{app_name="smf",cluster="Local",data_center="DC",
gtpc_msg_type="gtpc_false_peer_restart_cfg_echo_rc_change",gtpc_peer_ip=
"209.165.201.17",instance_id="0",interface_type="S11",service_name="nodemgr"} 1
```

```
nodemgr_gtpc_msg_stats{app_name="smf",cluster="Local",data_center="DC",
gtpc_msg_type="gtpc_false_peer_restart_cfg_echo_rc_change",gtpc_peer_ip=
"209.165.201.27",instance_id="0",interface_type="S5E",service_name="nodemgr"} 1
```

```
nodemgr_gtpc_msg_stats{app_name="smf",cluster="Local",data_center="DC",
gtpc_msg_type="gtpc_ignore_echo_timeout",gtpc_peer_ip="209.165.201.27",
instance_id="0",interface_type="S5E",service_name="nodemgr"} 1
```

```
nodemgr_gtpc_msg_stats{app_name="smf",cluster="Local",data_center="DC",
gtpc_msg_type="gtpc_false_peer_restart_ignore_echo_rc_cfg",gtpc_peer_ip=
"209.165.201.27",instance_id="0",interface_type="S5E",service_name="nodemgr"} 1
```

```
nodemgr_gtpc_msg_stats{app_name="smf",cluster="Local",data_center="DC",
gtpc_msg_type="gtpc_false_peer_restart_ignore_ctrl_rc_cfg",gtpc_peer_ip=
"209.165.201.27",instance_id="0",interface_type="S5E",service_name="nodemgr"} 1
```

Table 75: GTPC Path Failure Statistics Descriptions

Statistics	Description
gtpc_false_peer_restart_cfg_echo_rc_change	The number of GTPC path failures ignored because Echo Restart Counter Change isn't within max-remote-rc-change configured.

Statistics	Description
gtpc_false_peer_restart_ignore_echo_rc_cfg	The number of GTPC path failures ignored because of Echo Restart Counter Change.
gtpc_false_peer_restart_cfg_ctrl_rc_change	The number of GTPC path failures ignored because Control Message Restart Counter Change isn't within max-remote-rc-change configured.
gtpc_false_peer_restart_ignore_ctrl_rc_cfg	The number of GTPC path failures ignored because of Control message Restart Counter Change.
gtpc_ignore_echo_timeout	The number of GTPC path failures ignored because of Echo Request timeout.

Sx Path Failure

Maintain statistics indicating number of times path failure was detected due to recovery timestamp change in the following messages.

```
nodemgr_up_pathfail_reasons{app_name="smf",cluster="cn",data_center="cn",
instance_id="0",service_name="nodemgr",up_pathfail_reason="up_pathfail_ignored_hb_retry"}
 1
```

```
nodemgr_up_pathfail_reasons{app_name="smf",cluster="cn",data_center="cn",
instance_id="1",service_name="nodemgr",up_pathfail_reason="up_pathfail_ignored_hb_rt_change"}
 1
```

```
nodemgr_up_pathfail_reasons{app_name="smf",cluster="cn",data_center="cn",
instance_id="1",service_name="nodemgr",up_pathfail_reason="up_pathfail_reason_association_release"}
 1
```

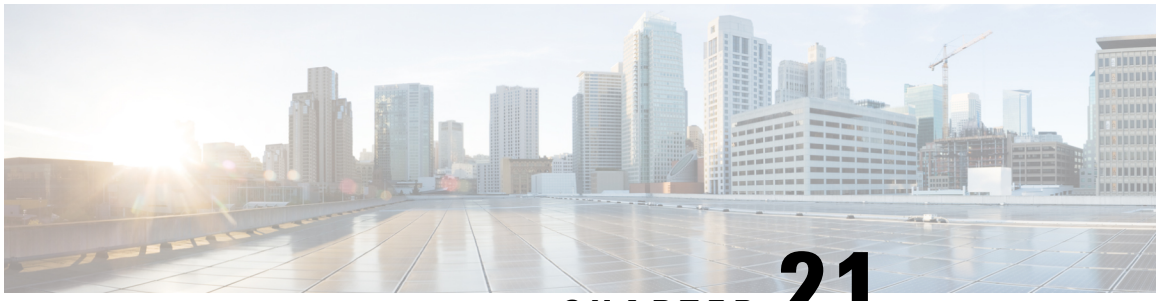
```
nodemgr_up_pathfail_reasons{app_name="smf",cluster="cn",data_center="cn",
instance_id="1",service_name="nodemgr",up_pathfail_reason="up_pathfail_reason_hb_retry"}
 8
```

```
nodemgr_up_pathfail_reasons{app_name="smf",cluster="cn",data_center="cn",
instance_id="1",service_name="nodemgr",up_pathfail_reason="up_pathfail_reason_hb_rt_change"}
 1
```

Table 76: Sx Path Failure Statistics Descriptions

Statistics	Description
up_pathfail_ignored_hb_retry	The number of Sx path failures ignored because of Heartbeat Request timeout.
up_pathfail_reason_hb_retry	The number of Sx path failures detected because of Heartbeat Request timeout.

Statistics	Description
up_pathfail_ignored_hb_rt_change	The number of Sx path failures ignored because of Heartbeat Request Recovery Timestamp Change Ignored.
up_pathfail_reason_hb_rt_change	The number of Sx path failures detected because of Heartbeat Request Recovery Timestamp Change.
up_pathfail_reason_association_release	The number of Sx path failures detected because of Sx Association Release.



CHAPTER 21

GTPv2 and Sx Messages Retransmission and Timeout Handling

Feature Summary and Revision History

Summary Data

Table 77: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 78: Revision History

Revision Details	Release
First introduced.	2021.01.0

Feature Description

cnSGW-C enables the retransmission and timeout handling for the parameters associated with outbound and inbound messages through CLI. The retransmission and timeout handling is applicable for the:

- Messages over a GTPC interface towards MME and PGW and
- Sx messages sent towards the User Plane (UP).

Note For handling the retransmission and timeout parameters, you must add the retransmission configuration (N3/T3) for the interface (S5e, S11, and Sxa).

How it Works

S-GW service, GTPC-EP, and SMF protocol are the primary nodes involved in the the retransmission and timeout handling.

The SGW-serice is responsible for:

- Handling the timeout event from GTPC-EP and SMF protocol
- Ignoring the inbound retransmitted message

The GTPC-EP and SMF protocol is responsible for:

- Retransmission and timeout handling
- Reading the N3/T3 configuration
- Updating the N3/T3 on configuration change

The retransmission and timeout handling is applicable for both outbound and inbound messages.

Outbound Message

To supports retransmission and timeout of outgoing GTP and PFCP messages, you must configure an interface specific N3 (maximum number of retries) and T3 (retransmission timeout) timer values in accordance to network response time/delay time.

The MME/S11 peers can have different retransmission timeout as compared to PGW/S5 or UPF/SXA.

The GTPC-EP/Protocol pod retries the outgoing request messages based on configured N3T3 values until the response is received or N3T3 is exhausted. In case of N3T3 gets exhausted, the GTPC-EP/Protocol pod sends the failure response with cause peer no response to service pod to indicate that no response has been received for outgoing request message.

Inbound Message

At each N4 and GTP endpoint, there's a set of queues for incoming and outgoing traffic. Each queue has a dispatcher thread running that pulls the message from the queue. It dispatches the message to the application for further processing.

Each dispatcher references a retransmission cache to check if the incoming request is already in service. It further performs the following actions:

- If it's a retry request, the dispatcher drops the incoming request.
- If the retransmission cache reaches the threshold for outstanding requests, the incoming request is dropped.

Each dispatcher has a separate retransmission cache. This cache is also updated with the response of the request sent. It's for the retransmission request received after the response is sent.

Configuring the Retransmission and Timeout Values

This section includes the CLI commands to configure the retransmission and timeout values for the outbound and inbound messages.

Following is the CLI configuration for the outbound messages:

```
config
  instance instance-id instance_id
    endpoint endpoint_name
      interface interface_name
        retransmission timeout timeout_intervalmax-retry retry_value
        end
```

NOTES:

- **instance instance-id** *instance_id*—Specify the instance ID.
- **endpoint** *endpoint_name*—Specify the endpoint name.
- **interface** *interface_name*—Specify the interface name.
- **retransmission timeout** *timeout_interval*—Configure the timeout interval value.

Following is the CLI configuration for the inbound messages:

```
config
    instance instance-id 1
    endpoint protocol
    interface n4
        dispatcher
            count 5
            outbound true
        threshold 5000
        end
```

NOTES:

- **capacity** *capacity_value*—Specify the queue size for each dispatcher queue. The default value is 5000.
- **count** *value*—Specify the number of supported dispatcher queues for the interface or the endpoint.

- **expiry** *expiry_duration*—Specify the duration for which the cache entry with response is held in the cache. The default value is 60 seconds.
- **nonresponsive** *nonresponsive_duration*—Specify the duration for which the cache entry without response is held in the cache.
- **outbound** *true | false*—Disable dispatcher queue support for outgoing messages. The default value is true. When set to false, the queue support is enabled for outgoing messages.

  It means by default, the queue support is enabled for the outgoing messages. Must be one of the following:

  - *true*—Disable dispatcher queue support for outgoing messages, set the **outbound** to true.
  - *false*—Enable dispatcher queue support for outgoing messages, set the **outbound** to false.

- **rate-limit** *rate_limit*—Specify the rate limit for each queue.
- **threshold** *threshold*—Specify the outstanding limit for non-responsive cache entries. When the threshold is reached, the incoming requests are dropped. It must be an integer. The default value is 30000 milliseconds.

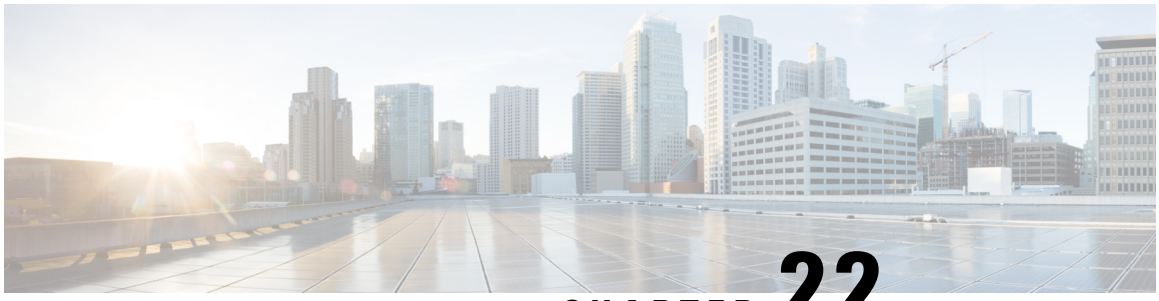
Configuration Verification

Following is the sample configuration to verify the retrnasmission and timeout handling configuration for the outbound and inbound messages:

```
show running-config instance instance-id 1 endpoint gtp
instance instance-id 1
endpoint gtp
replicas 1
interface s5e
retransmission timeout 2 max-retry 2
sla response 7000
dispatcher
count 1
capacity 1000
outbound true
threshold 10000
expiry 40000
nonresponsive 20000
exit
vip-ip 209.165.201.25
exit
interface s11
retransmission timeout 2 max-retry 2
sla response 7000
dispatcher
count 1
capacity 1000
outbound true
threshold 10000
expiry 40000
nonresponsive 20000
exit
vip-ip 209.165.201.2
exit
exit

show running-config instance instance-id 1 endpoint pfcp
instance instance-id 1
```

```
endpoint pfcp
replicas 1
interface sxa
retransmission timeout 2 max-retry 2
dispatcher
count 1
capacity 1000
outbound true
threshold 10000
expiry 40000
nonresponsive 20000
exit
heartbeat
interval 0
retransmission-timeout 3
max-retransmissions 5
exit
retransmission timeout 5 max-retry 1
exit
interface n4
heartbeat
interval 0
retransmission-timeout 3
max-retransmissions 5
exit
exit
exit
```



CHAPTER 22

GTPv2 Load/Overload Support

Feature Summary and Revision History

Summary Data

Table 79: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration required to enable
Related Documentation	Not Applicable

Revision History

Table 80: Revision History

Revision Details	Release
First introduced.	2021.02.0

Feature Description

The following are the details for the load control and the overload control features.

Load Control

The load control enables a GTPC entity, such as SGW or PGW, to send its load information to a GTPC peer, such as MME, ePDG, and TWAN. This information is used to balance the session load across all the nodes supporting the same function, such as SGW cluster, as per their effective loads. The load information reflects the operational status of the GTPC entity resources.

cnSGW-C load control behavior is as follows:

- Activate or deactivate the load control support in cnSGW-C, using the CLI.
- When the load control feature is activated, cnSGW-C signals its load control information to the MME for the following reasons:
  - Optimum GW selection procedures
  - Enhanced load balancing across cnSGW-C in the network
- The calculation of the load control information is based on the deployment scenarios.
- The applicable GTPC request or the response message contains piggybacked load control information.
- cnSGW-C includes only the single instance of LCI (Load Control Information) IE as per the SGW load control information. cnSGW-C sends the LCI IE received from the PGW to the MME, along with its LCI information.
- The frequency of load control information inclusion at SGW is based on the deployment scenario. The SGW ensures the propagation of the new or the updated load control information to the target receivers is within the acceptable delay. This acceptable delay helps in achieving the effective load balancing act in the network.

Overload Control

The overload control enables a GTPC entity to reduce gracefully its own incoming signaling load by instructing its GTPC peers to send the reduced traffic. The GTPC entity reaches overload, when it operates above the signaling capacity. This overload results in a diminished performance, resulting in to impacts on the incoming and the outgoing traffic handling. The GTPC node uses the load information to reduce, or throttle, or reduce and throttle, the amount of GTPC signaling traffic between these nodes.

cnSGW-C overload control behavior is as follows:

- Activate or deactivate overload control support in cnSGW-C using the CLI.
- When the overload control feature is activated, cnSGW-C signals its overload control information to the MME or the PGW. This helps in controlling the GTPC signaling traffic towards itself.
- SGW supports the handling of the overload control information in all the applicable messages.
- The applicable GTPC request or the response message contains piggybacked overload control information.
- cnSGW-C includes only the single instance of OCI (Overload Control Information) IE as per the SGW overload control information. cnSGW-C sends the OCI IE received from the PGW to the MME, along with its OCI information.
- The calculation of the overload control information is based on the deployment scenario.
- cnSGW-C rejects with the cause as GTPC entity congestion, when the SGW is in self-protection mode.

- SGW doesn't store the MME or the PGW overload control information.
- SGW doesn't perform throttling towards the MME and the PGW.

Note The load control and the overload control are optional features.

Configuring the GTPv2 Load and Overload Feature

This section describes how to configure the GTPv2 load or overload conditions.

Configuring this feature involves the following steps:

- Configuring the Load Profile: This section describes how to configure the load profile and the parameters required to calculate the load of cnSGW-C.
- Configuring the Exclude Profile, on page 218: This section describes how to make an exclusion and configure the exclude profile in overload conditions.
  - This profile determines the session-related messages to exclude from the throttling decisions.
  - Both self-protection and peer overload control, use this configuration.
- Configuring the Overload Condition Profile, on page 219: This section describes how to configure the profile in overload conditions.
  - The profile determines the various conditions for overload control and the resulting throttling decisions.
  - It supports only one overload profile.
  - The load profile supports overload profile functionality.
- Configuring the Maximum Session Count, on page 220: This section describes how to configure the maximum session count that contributes to the session percent load factor in LCI/OCI calculation.
- Associating the Overload-Profile with SGW-Profile Association, on page 175: The association of the Overload-Profile and the SGW-Profile, can be configured.

Configuring the Load Profile

To configure this feature use the following configuration:

```
config
   profile load profile_name
      load-calc-frequency load_calc_frequency_value
      load-fetch-frequency load_fetch_frequency_value
      advertise
      interval interval_value
      change-factor change_factor_value
      exit
```

```
    interface gtpc
       action advertise
end
```

NOTES:

- **profile load** *profile_name*—Specify the load profile name.
- **load-calc-frequency** *load_calc_frequency_value*—Specify the system load calculation time in seconds. Must be an integer in the range of 5-3600. The default value is 10 seconds.
- **load-fetch-frequency** *load_fetch_frequency_value*—Specify the time interval in seconds at which protocol pods fetch load from the cache POD. Must be an integer in the range of 5-3600. The default value is 10 seconds.
- **advertise interval** *interval_value*—Specify the time interval of sending LCI to the peers in seconds. Must be an integer in the range of 0-3600. The default value is 300 seconds.
- **advertise change-factor** *change_factor_value*—Specify the LCI value to corresponding peers, if the difference between the current load value and the last indicated load value is greater than the change-factor. Must be an integer in the range of 1-20. The default value is five.
- **interface gtpc action advertise**—Enables LCI publishing on the GTPC interface.

Configuration Example

The following is an example configuration.

```
config
profile load pl
load-calc-frequency 30
load-fetch-frequency 60
advertise
interval 300
change-factor 1
exit
interface gtpc
action advertise
end
```

Configuring the Exclude Profile

To configure this feature use the following configuration:

```
config
   profile overload-exclude overload_exclude_profile_name
       dnn-list dnn_list
       arp-list arp_list
       end
```

NOTES:

- **profile overload-exclude** *overload_exclude_profile_name*—Specify the name of the exclude profile. You can configure multiple exclude profiles.
- **dnn-list** *dnn_list*—Specify the list of DNNs that needs to be excluded from throttling decisions. The maximum limit is three.

- **arp-list** *arp_list*—Specify the list of 5G allocation and retention priorities and exclusion of throttling decision messages. Must be an integer in the range of 1-15. The maximum limit is eight.

Configuration Example

The following is an example configuration.

```
config
profile overload-exclude ol-excl-prof1
dnn-list emergency-dnn1 wps-dnn2
arp-list 1 2 3
end
```

Configuring the Overload Condition Profile

To configure this feature use the following configuration:

```
config
   profile overload overload_profile_name
      overload-exclude-profile self-protection self_protection_profile_name
         node-level
         tolerance
            minimum min_percentage
            maximum max_percentage
         reduction-metric
            minimum min_percentage
            maximum max_percentage
         interface gtpc
            overloaded-action advertise
               advertise
                  interval interval_value
                  change-factor change_factor_value
                  validity-period validity_period_value
                  end
```

NOTES:

- **profile overload** *overload_profile_name*—Specify the overload profile name.
- **overload-exclude-profile self-protection** *self_protection_profile_name*—(This is an optional configuration) Exclude messages from throttling decisions in self-protection condition.
- **tolerance minimum** *min_percentage* **maximum** *max_percentage*—Specify the system overload limits. Refer the following scenarios:
  - When the system load is less than *min_percentage*, the system is in a normal state.
  - When the system load is in between *min_percentage* and *max_percentage*, the system is in an overloaded state. In this scenario, the node overload control action is triggered.
  - When the system load is greater than *max_percentage*, the system is in a self-protection state. In this scenario, the self-protection action is triggered.
  - *max_percentage* must be an integer in the range of 1-100. The default value is 95.
  - *min_percentage* must be an integer in the range of 1-100. The default value is 80.

- **reduction-metric minimum** *min_percentage* **maximum** *max_percentage*—Specify the reduction metric limits. Refer the following scenarios:
  - Both percentage values, *min_percentage* and *max_percentage* work along with the **tolerance** configuration.
  - The percentage value *max_percentage* must be an integer in the range of 1-100. The default value is 100.
  - The percentage value *min_percentage* must be an integer in the range of 1-100. The default value is 10.

  Example: Send 10 percent OCI to peer nodes, when the load is 80 percent, and 30 percent, when the load is 95 percent, during the following conditions:
  - **tolerance** *min_percentage* is 80 and *max_percentage* is 95.
  - **reduction-metric** *min_percentage* is 10 and *max_percentage* is 30.
- **interface gtpc overloaded-action advertise**—Configures the action on GTPC interface when a node gets overloaded. GTPC includes S5/S8/S11/S2b interfaces. Certain actions apply only to specific interfaces.
- **advertise interval** *interval_value*—Specify the periodicity of sending LCI to the peers in seconds. Must be an integer in the range of 0-3600. The default value is 300 seconds.
- **advertise change-factor** *change_factor_value*—Specify the change-factor value. GTPC sends the LCI to corresponding peers, if the difference between the current load value and the lastly indicated load value is greater than the change-factor value. Must be an integer in the range of 1-20. The default value is five.
- **advertise validity-period** *validity_period_value*— Specify the validity period of the advertised OCI value in seconds. Must be an integer in the range of 1-3600. The default value is 600 seconds.

Configuring the Maximum Session Count

To configure this feature use the following configuration:

```
config
   profile converged-core profile_name
      max-session-count max_session_count_value
      end
```

NOTES:

- **profile converged-core** *profile_name*—Specify the name of the converged core profile.
- **max-session-count** *max_session_count_value*—Specify the maximum number of sessions supported. Must be an integer in the range of 1-12000000.

Configuration Example

The following is an example configuration.

```
config
profile converged-core convergedCoreProfile
```

```
max-session-count 12000000
exit
```

Associating the Overload-Profile with SGW-Profile Association

The association of the Overload-Profile and the SGW-Profile, can be configured.

To configure this feature use the following configuration:

```
config
   profile overload overload_profile_name
      overload-exclude-profile self-protection self_protection_profile_name
   node-level
      tolerance
         minimum min_percentage
         maximum max_percentage
      reduction-metric
         minimum min_percentage
         maximum max_percentage
         advertise
         interval interval_value
         change-factor
         exit
      interface gtpc
         overloaded-action [ advertise ]
         exit
      exit
   exit
   profile load load_name
   load-calc-frequency load_calc_frequency_value
   load-fetch-frequency load_fetch_frequency_value
   advertise
   interval interval_value
   change-factor change_factor_value
   exit
   interface gtpc
   action advertise
   exit
exit
profile sgw sgw_name
load-profile profile_name
overload-profile overload_profile_name
end
```

NOTES:

- **overload** *overload_name*—Specify the overload protection profile name. Must be a string.

- **overload-exclude-profile**—Excludes profiles for overload scenarios.
- **self-protection** *overload_value*—Specify the profile to be excluded for self-protection. Must be a string.
- **tolerance minimum** *min_percentage*—Specify the minimum tolerance level below which the system is in a normal state. Must be an integer in the range of 1-100. The default value is 80.
- **tolerance maximum** *max_percentage*—Specify the maximum tolerance level above which the system is in a self-protection state. Must be an integer in the range of 1-100. The default value is 95.
- **reduction-metric minimum** *min_percentage*—Specify the percentage of reduction along with minimum tolerance-level for configuration. Must be an integer in the range of 1-100. The default value is 10.
- **reduction-metric maximum** *max_percentage*—Specify the percentage of reduction along with maximum tolerance-level for configuration. Must be an integer in the range of 1-100. The default value is 100.
- **interval** *interval_value*—Specify the advertising interval in seconds. Must be an integer in the range of 0-3600. The default value is 300 seconds.
- **validity** *validity_value*—Specify the validity period of the advertised OCI value in seconds. Must be an integer in the range of 1-3600. The default value is 600 seconds.
- **change-factor** *change_factor_value*—Specify the minimum change between current OCI and last indicated OCI, after which the advertising should happen. Must be an integer in the range of 1-20. The default value is five.
- **profile load** *load_name*—Specify the name of the load profile. Must be a string.
- **load-calc-frequency** *load_calc_frequency_value*—Specify the system load calculation interval in seconds. Must be an integer in the range of 5-3600. The default value is 10 seconds.
- **load-fetch-frequency** *load_fetch_frequency_value*—Specify the time interval in seconds at which the service pods fetch load from the cache pod. Must be an integer in the range of 5-3600. The default value is 10 seconds.
- **load-profile** *profile_name*—Specify the name of the load profile.
- **overload-profile** *overload_profile_name*—Specify the name of the overload profile.
- : Specify the exclude overload profile name:
  - : Specify the ARP list that needs to be excluded from throttling decisions. Must be an integer in the range of 1-15. Maximum eight entries are allowed.
  - : Specify the list of DNNs that needs to be excluded from throttling decision. Maximum three entries are allowed.
  - **message-priority**: Specify upto which message periority to be excluded from throttling decisions.
  - **procedure-list**: Procedures to be excluded from throttling decisions. This parameter is applicable only for Self-Protection.
  - : Specify the QoS Class Identifier to be excluded from throttling decisions. Must be an integer in the range of 1-.254. Maximum 8 entries are allowed. For example, range values can be 1-9,65,66,69,70,80,82,83,128-254.

Configuration Example

The following is an example configuration.

```
config
profile overload op
overload-exclude-profile self-protection <overload-exclude-profile-name>
node-level
tolerance minimum 5
tolerance maximum 50
reduction-metric minimum 50
reduction-metric maximum 100
advertise
interval 0
change-factor 1
exit
interface gtpc
overloaded-action [ advertise ]
exit
exit
exit
profile load lp
load-calc-frequency 120
load-fetch-frequency 15
advertise
interval 0
change-factor 1
exit
interface gtpc
action advertise
exit
exit
profile sgw <sgw_name>
load-profile <profile_name>
overload-profile <overload_profile_name>
end
```

Configuration Verification

To verify the configuration:

```
show running-config profile
profile sgw sgw1
load lp1
overload op1
end
```

GTPv2 Load and Overload OAM Support

This section describes operations, administration, and maintenance information for this feature.

Bulk Statistics

Normal

```
node_overload_status{app_name="smf", cluster="cn", data_center="cn",
instance_id="0", service_name="oam-pod"} 0
```

Overload

```
node_overload_status{app_name="smf", cluster="cn", data_center="cn",
instance_id="0", service_name="oam-pod"} 1
```

Self-Protection

```
node_overload_status{app_name="smf", cluster="cn", data_center="cn",
instance_id="0", service_name="oam-pod"} 2
```

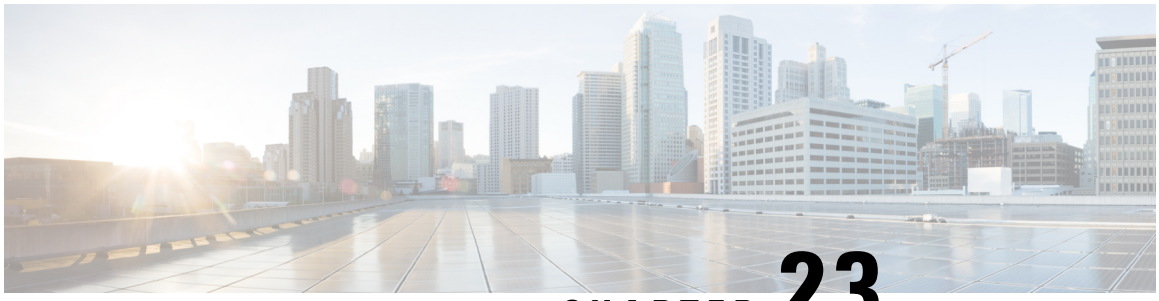
SGW Service Statistics

```
sgw_service_stats{app_name="smf", cluster="cn", data_center="cn",
fail_reason="gtp_entity_in_congestion", instance_id="0",
interface="interface_sgw_ingress", reject_cause="entity_in_congestion",
service_name="sgw-service", sgw_procedure_type="initial_attach",
status="rejected", sub_fail_reason=""}
```

LCI/OCI Metric Values

```
node_lci_metric{app_name="SGW", cluster="cn", component="oam-pod",
data_center="DC", namespace="cn", instance_id="0", service_name="oam-pod"}
```

```
node_oci_metric{app_name="SGW", cluster="cn", component="oam-pod",
data_center="DC", namespace="cn", instance_id="0", service_name="oam-pod"}
```



CHAPTER 23

GTPv2 Message Validation

Feature Summary and Revision History

Summary Data

Table 81: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 82: Revision History

Revision Details	Release
First introduced.	2021.01.0

Feature Description

cnSGW-C supports basic GTPv2 message validation of IEs (values, mandatory IE, and service-dependent IE), and sends responses from the SGW-Service/GTPC-EP pod.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

Basic and Advance Validation on SGW-Ingress (S11) Call Flow

The following section describes the Basic and Advance Validation on SGW-Ingress (S11) call flow.

Figure 38: Basic and Advance Validation - S11 Call Flow

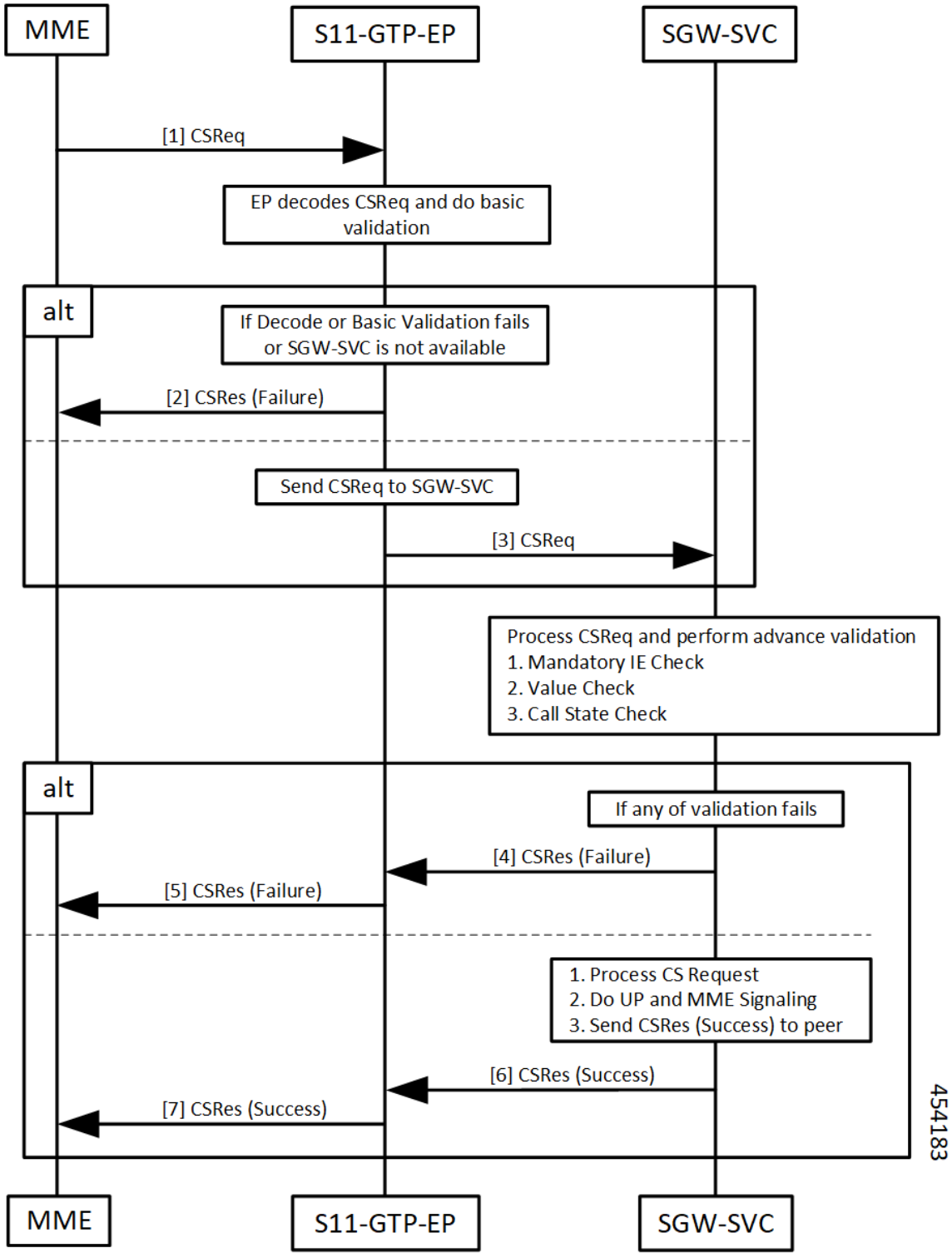


Table 83: Basic and Advance Validation - S11 Call Flow Description

Step	Description
1	The MME sends the Create Session Request to the S11-GTP-EP pod. The S11-GTP-EP pod decodes the Create Session Request and performs basic validation.
2	If decoding or basic validation fails, or if SGW-SVC is not available, the S11-GTP-EP pod sends Create Session Response failure message to the MME.
3	If Create Session Request basic validation is successful, the S11-GTP-EP pod forwards the Create Session Request to the SGW-SVC pod. SGW-SVC processes the Create Session Request and performs the following: • Mandatory IE check • Value check • Call State check
4, 5	If validation from Step 3 fails: • The SGW-SVC sends the Create Session Response failure message to the S11-GTP-EP pod. • The S11-GTP-EP pod forwards the Create Session Response failure message to the MME.
6, 7	If validation from Step 3 is successful, the SGW-SVC performs the following: • Processes Create Session Request • Performs UP and MME signaling • Sends Create Session Response success message to the S11-GTP-EP pod The S11-GTP-EP pod forwards the Create Session Response success message to the MME.

Basic and Advance Validation on SGW-Egress (S5) Call Flow

The following section describes the Basic and Advance Validation on SGW-Egress (S5) call flow.

Figure 39: Basic and Advance Validation - S5 Call Flow

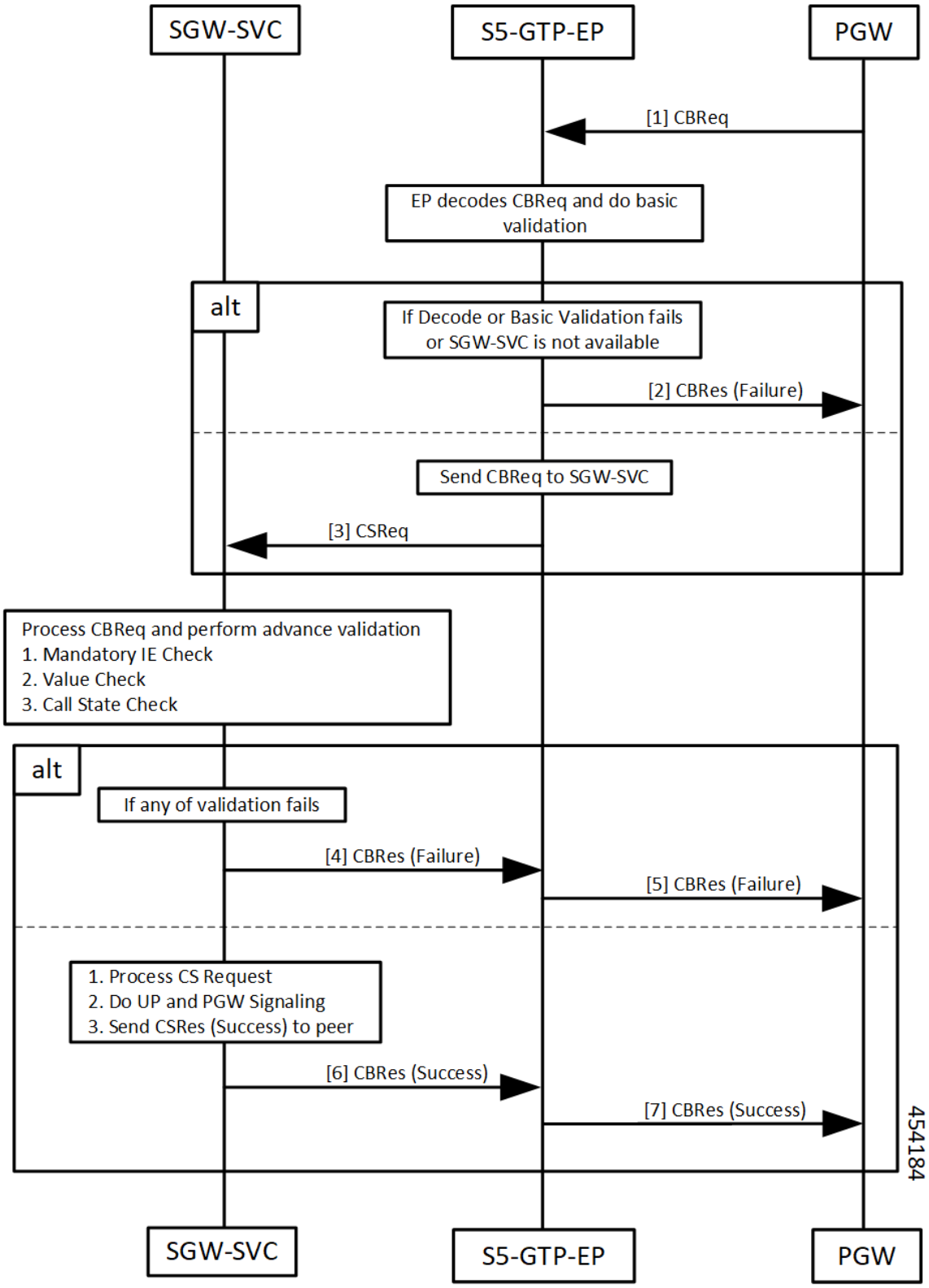
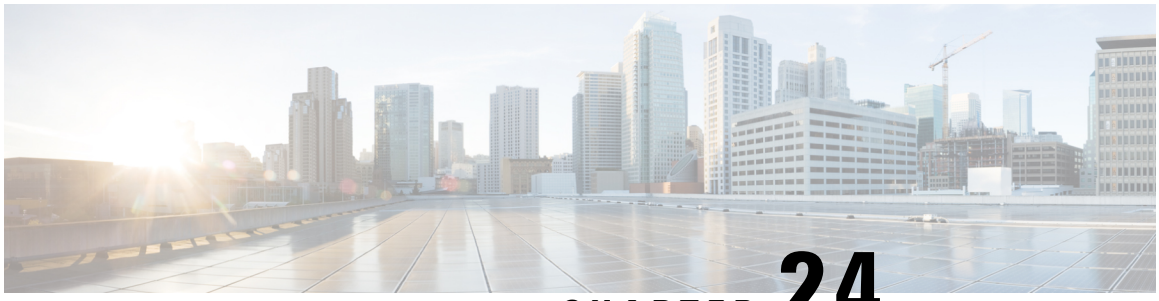


Table 84: Basic and Advance Validation - S5 Call Flow Description

Step	Description
1	The PGW sends the Create Bearer Request to the S5-GTPC-EP pod. The S5-GTPC-EP pod decodes the Create Bearer Request and performs basic validation.
2	If decoding or basic validation fails, or if SGW-SVC is not available, the S5-GTP-EP pod sends the Create Bearer Response failure message to the PGW.
3	If Create Bearer Request basic validation is successful, the S5-GTP-EP pod forwards the Create Bearer Request to the SGW-SVC pod. SGW-SVC processes the Create Bearer Request and performs the following: • Mandatory IE check • Value check • Call State check
4, 5	If validation from Step 3 fails: • The SGW-SVC sends the Create Bearer Response failure message to the S5-GTP-EP pod. • The S5-GTP-EP pod forwards the Create Bearer Response failure message to the PGW.
6, 7	If validation from Step 3 is successful, the SGW-SVC performs the following: • Processes Create Bearer Request • Performs UP and PGW signaling • Sends Create Bearer Response success message to the S5-GTP-EP pod The S5-GTP-EP pod forwards the Create Bearer Response success message to the PGW.



CHAPTER 24

IDFT Support

Feature Summary and Revision History

Summary Data

Table 85: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 86: Revision History

Revision Details	Release
First introduced.	2021.02.0

Feature Description

cnSGW-C supports Indirect Forwarding Tunnel (IDFT) Creation and Deletion for Pure-S call with dedicated bearers, with and without SGW relocation.

Standards Compliance

This feature complies with the following standards specifications:

- *3GPP TS 23.401 "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access"*
- *3GPP TS 23.402 "Architecture enhancements for non-3GPP accesses"*
- *3GPP TS 29.274 "Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C)"*
- *3GPP TS 23.214 "Architecture enhancements for control and user plane separation of EPC nodes"*
- *3GPP TS 29.244 "Interface between the Control Plane and the User Plane nodes"*
- *3GPP TS 24.008 "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3"*

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

IDFT Support without SGW Relocation Call Flow

This section describes the IDFT Support without SGW Relocation call flow.

Figure 40: IDFT Support without SGW Relocation Call Flow

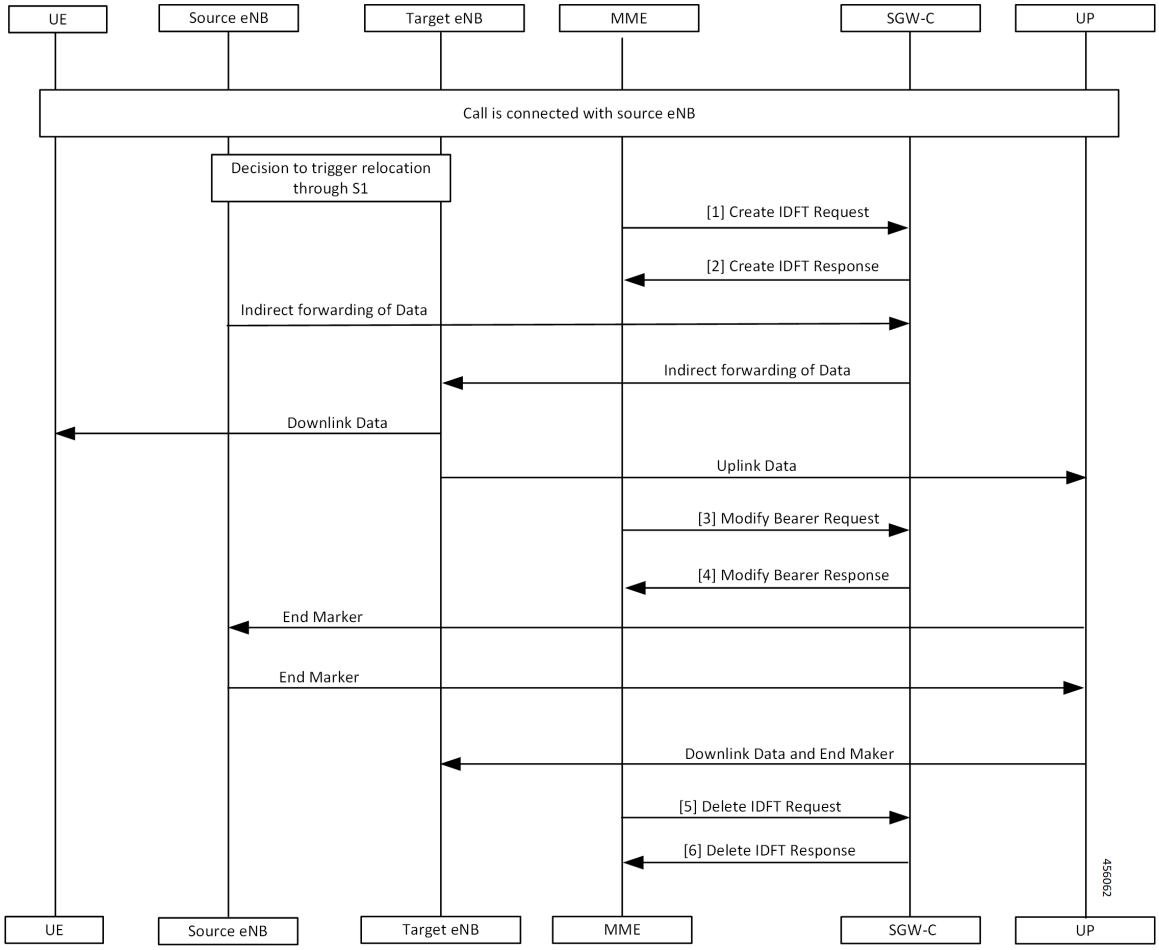


Table 87: IDFT Support without SGW Relocation Call Flow Description

Step	Description
1	Call is connected with the Source eNodeB and there's a decision to trigger relocation via S1. The MME sends the Create IDFT Request to the SGW-C.
2	The MME receives the Create IDFT Response from the SGW-C.
3	The indirect forwarding of the data starts from the Source eNodeB to the SGW-C. The indirect forwarding of the data starts from the SGW-C to the eNodeB. The Target eNodeB sends the Downlink Data to the UE. The Target eNodeB sends the Uplink Data to the UP. The MME sends the Modify Bearer Request to the SGW-C.

Step	Description
4	The SGW-C sends the Modify Bearer Response to the MME. The UP sends the End Marker to the Source eNodeB, and the Source eNodeB forwards the End Marker to the UP. The UP sends the Downlink Data and the End Marker to the Target eNodeB.
5	The MME sends the Delete IDFT Request to the SGW-C.
6	The MME receives the Delete IDFT Response from the SGW-C.

IDFT Support with SGW Relocation Call Flow

This section describes the IDFT Support with SGW Relocation call flow.

Figure 41: IDFT Support with SGW Relocation Call Flow

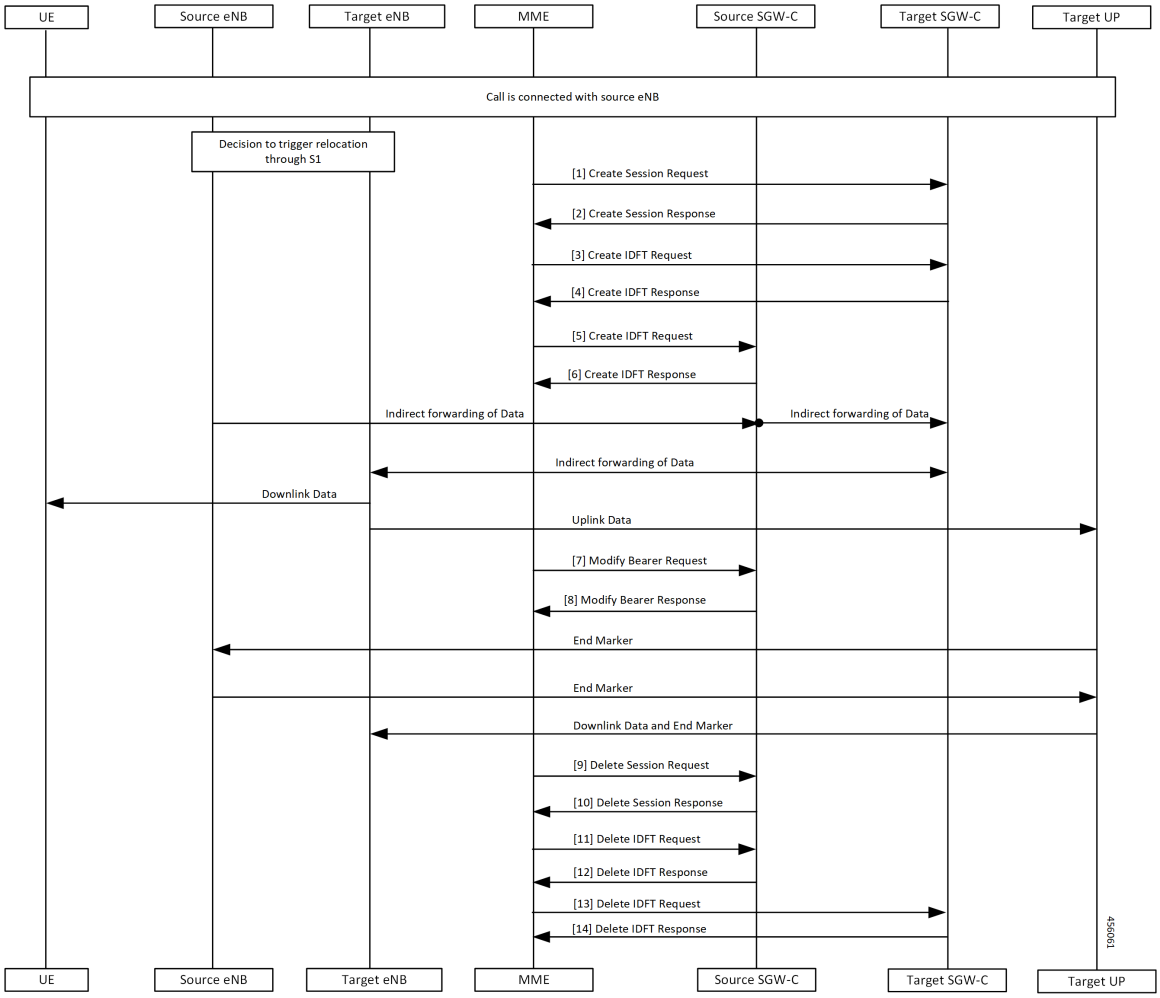


Table 88: IDFT Support with SGW Relocation Call Flow Description

Step	Description
1	Call is connected with the Source eNodeB and there's a decision to trigger relocation via S1. The MME sends the Create Session Request to the Target SGW-C.
2	The MME receives the Create Session Response from the Target SGW-C.
3	The MME sends the Create IDFT Request to the Target SGW-C.
4	The MME receives the Create IDFT Response from the Target SGW-C.
5	The MME sends the Create IDFT Request to the Source SGW-C.
6	The MME receives the Create IDFT Response from the Source SGW-C. The indirect forwarding of the data starts from the Source eNodeB to the Source SGW-C. The indirect forwarding of the data starts from the Source SGW-C to the Target SGW-C. The indirect forwarding of the data starts from the Target SGW-C to the Target eNodeB. The Target eNodeB sends the Downlink Data to the UE. The Target eNodeB sends the Uplink Data to the Target UP.
7	The MME sends the Modify Bearer Request to the Target SGW-C.
8	The Source SGW-C sends the Modify Bearer Response to the MME. The Target UP sends the End Marker to the Source eNodeB, and the Source eNodeB forwards the End Marker to the Target UP. The Target UP sends the Downlink Data and the End Marker to the Target eNodeB.
9	The MME sends the Delete Session Request to the Source SGW-C.
10	The MME receives the Delete Session Response from the Source SGW-C.
11	The MME sends the Delete IDFT Request to the Source SGW-C.
12	The MME receives the Delete IDFT Response from the Target SGW-C.
13	The MME sends the Delete IDFT Request to the Target SGW-C.
14	The MME receives the Delete IDFT Response from the Target SGW-C.

5G to 4G Handover Flow for Pure-S Call Flow

This section describes the 5G to 4G Handover flow for Pure-S call flow.

Figure 42: 5G to 4G Handover Flow for Pure-S Call Flow

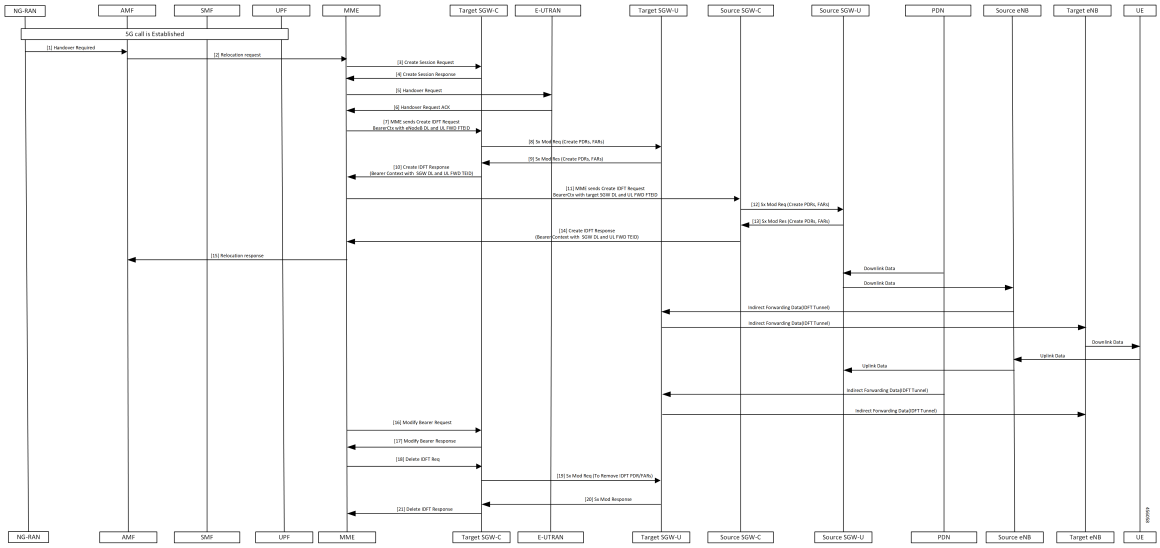


Table 89: 5G to 4G Handover Flow for Pure-S Call Flow Description

Step	Description
1	5G call is established. The NG-RAN sends the Handover Required message to the AMF.
2	The AMF sends the Relocation Request to the MME.
3	The MME sends the Create Session Request to the Target SGW-C.
4	The MME receives the Create Session Response from the Target SGW-C.
5	The MME sends the Handover Request to the E-UTRAN.
6	The MME receives the Handover Request ACK from the E-UTRAN.
7	The MME sends the Create IDFT Request with the Bearer Context with the eNodeB DL and UL FWD FTEID, to the Target SGW-C.
8	The Target SGW-C sends the Sx Modification Request with the Create PDRs and FARs to the Target SGW-U.
9	The Target SGW-U sends the Sx Modification Response with the Create PDRs and FARs to the Target SGW-C.
10	The Target SGW-C sends the Create IDFT Response with the Bearer Context with the SGW DL and UL FWD TEID, to the MME.
11	The MME sends Create IDFT Request with the Bearer Context, along with SGW DL and UL FWD FTEID, to the Source SGW-C.
12	The Source SGW-C sends the Sx Modification Request with Create PDRs and FARs, to the Source SGW-U.

Step	Description
13	The Source SGW-C receives the Sx Modification Response with Create PDRs and FARs, from the Source SGW-U.
14	The MME receives the Create IDFT Response with the Bearer Context, with the SGW DL and UL FWD TEID, from the Source SGW-C.
15	The MME sends the Relocation Response to the AMF. The PDN sends the Downlink Data to the Source SGW-U, and the Source SGW-U sends the Downlink Data to the Source eNodeB. The indirect forwarding data (IDFT Tunnel) starts from the Source eNodeB to the Target SGW-U, and from the Target SGW-U to the Target eNodeB. The Target eNodeB sends the Downlink Data to the UE. The UE sends the Uplink Data to the Source eNodeB, and the Source eNodeB sends the Uplink Data to the Source SGW-U. The PDN sends the indirect forwarding data to the Target SGW-U, and the Target SGW-U sends the indirect forwarding data to the Target eNodeB.
16	The MME sends the Modify Bearer Request to the Target SGW-C.
17	The MME receives the Modify Bearer Response from the Target SGW-C.
18	The MME sends the Delete IDFT Request to the Target SGW-C.
19	The Target SGW-C sends the Sx Modification Request with PDRs and FARs (to remove), to the Target SGW-U.
20	The Target SGW-C receives the Sx Modification Response from the Target SGW-U.
21	The MME receives the Delete IDFT Response from the Target SGW-C.

4G to 5G Handover Flow for Pure-S Call Flow

This section describes the 4G to 5G Handover flow for Pure-S call flow.

Figure 43: 4G to 5G Handover Flow for Pure-S Call Flow

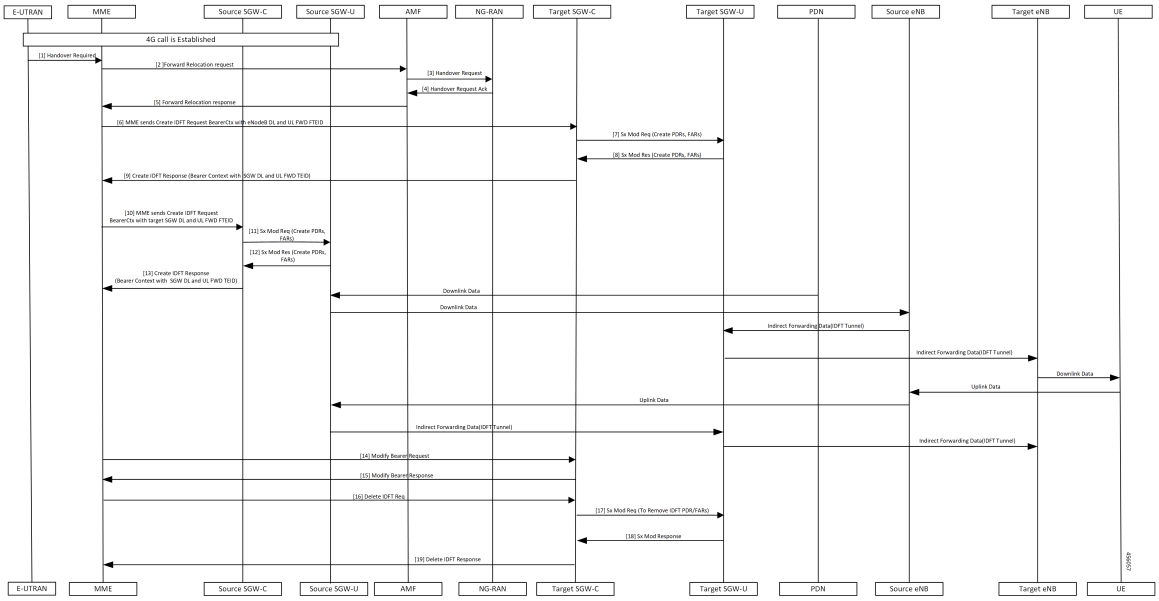


Table 90: 4G to 5G Handover Flow for Pure-S Call Flow Description

Step	Description
1	4G call is established. The E-UTRAN sends the Handover Required message to the MME.
2	The MME sends the Forward Relocation Request to the AMF.
3	The AMF sends the Handover Request message to the NG-RAN.
4	The AMF receives Handover Request ACK message.
5	The MME receives the Forward Relocation Response from the AMF.
6	The MME sends the Create IDFT Request with the Bearer Context with the eNodeB DL and UL FWD FTEID, to the Target SGW-C.
7	The Target SGW-C sends the Sx Modification Request with Create PDRs and FARs to the Target SGW-U.
8	The Target SGW-U sends the Sx Modification Response with Create PDRs and FARs to the Target SGW-C.
9	The Target SGW-C sends the Create IDFT Request with the Bearer Context along with eNodeB DL and UL FWD FTEID to the MME.
10	The MME sends the Create IDFT Request with the Bearer Context along with target SGW DL and UL FWD FTEID to the Source SGW-C.
11	The Source SGW-C sends the Sx Modification Request with Create PDRs and FARs to the Source SGW-U.

Step	Description
12	The Source SGW-C receives the Sx Modification Response with Create PDRs and FARs from the Source SGW-U.
13	The MME receives the Create IDFT Response with the Bearer Context along with SGW DL and UL FWD FTEID, from the Source SGW-C. The PDN sends the Downlink Data to the Source SGW-U, and the Source SGW-U sends the Downlink Data to the Source eNodeB. The indirect forwarding data (IDFT Tunnel) starts from the Source eNodeB to the Target SGW-U, and from the Target SGW-U to the Target eNodeB. The Target eNodeB sends the Downlink Data to the UE. The UE sends Uplink Data to the Source eNodeB, and the Source eNodeB sends the Uplink Data to the Source SGW-U. The Source SGW-U sends the indirect forwarding data to the Target SGW-U, and the Target SGW-U sends the indirect forwarding data to the Target eNodeB.
14	The MME sends the Modify Bearer Request to the Target SGW-C.
15	The MME receives the Modify Bearer Response from the Target SGW-C.
16	The MME sends the Delete IDFT Request to the Target SGW-C.
17	The Target SGW-C sends the Sx Modification Request to the Target SGW-U, to remove the PDRs and FARs.
18	The Target SGW-C receives the Sx Modification Response from the Target SGW-U.
19	The MME receives the Delete IDFT Response from the Target SGW-C.

Create IDFT (System-level) Call Flow

This section describes the Create IDFT (System-level) call flow.

Figure 44: Create IDFT (System-level) Call Flow

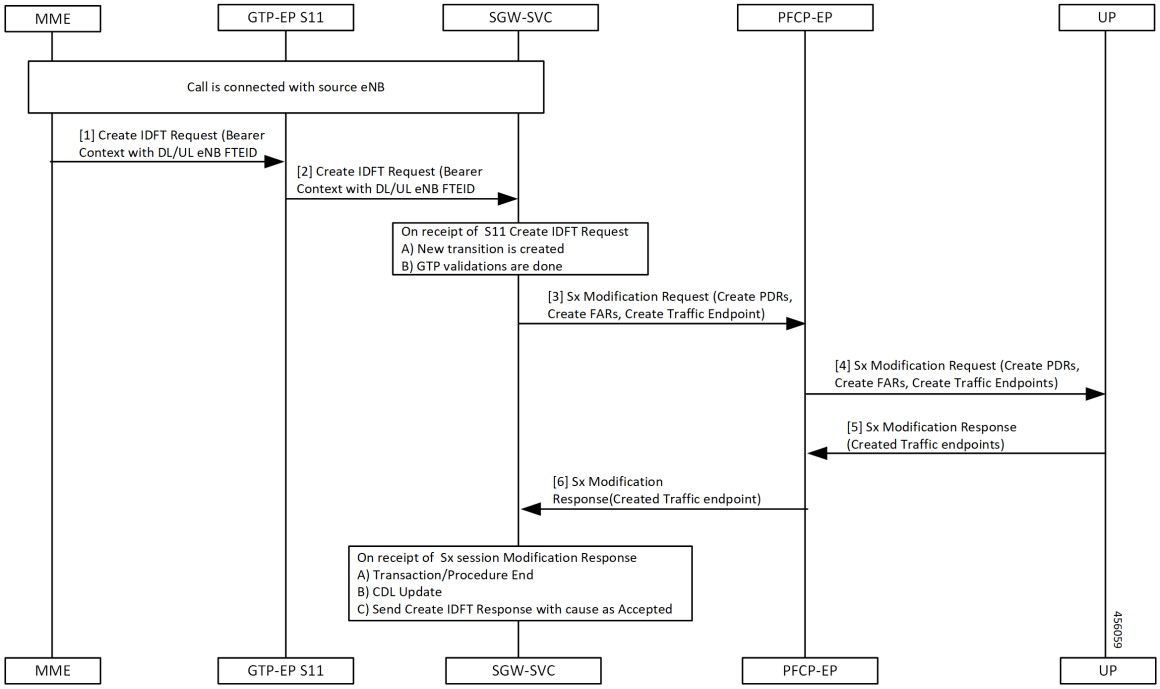


Table 91: Create IDFT (System-level) Call Flow Description

Step	Description
1	Call is connected with the Source eNodeB. The MME sends the S11 Create IDFT Request with the Bearer Context with a DL/UL enB FTEID, to the GTP-EP S11.
2	The GTP-EP S11 sends the S11 Create IDFT Request with the Bearer Context with a DL/UL enB FTEID, to the SGW-SVC. The SGW-SVC receives the S11 Create IDFT Request and performs the following: • Creates a new transaction • Completes GTP validations
3	The SGW-SVC sends the Sx Modification Request with Create PDRs, Create FARs, and Create Traffic Endpoints, to the PFCP-EP.
4	The PFCP-EP sends the Sx Modification Request with Create PDRs, Create FARs, and Create Traffic Endpoints, to the UP.
5	The UPF sends the Sx Session Modification Response with Created Traffic endpoints, to the PFCP-EP.

Step	Description
6	The SGW-SVC receives the Sx Session Modification Response from the PFCP-EP and performs the following: • Ends the transaction/procedure • Updates the CDL • Sends the Create IDFT Response with cause as Accepted

Delete IDFT (System-level) Call Flow

This section describes the Delete IDFT (system-level) call flow.

Figure 45: Delete IDFT (System-level) Call Flow

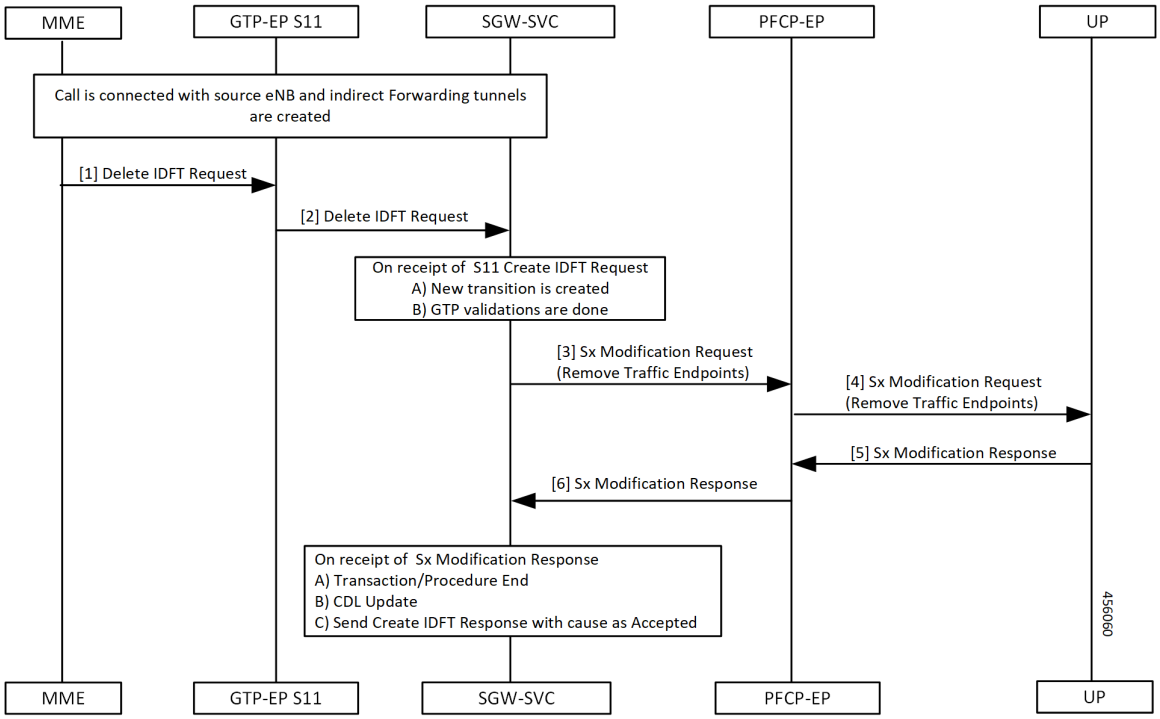


Table 92: Delete IDFT (System Level Flow) Call Flow Description

Step	Description
1	Call is connected with the Source eNodeB and indirect forwarding tunnels are created. MME sends the S11 Delete IDFT Request with Bearer Context with a DL/UL enB FTEID, to the GTP-EP S11.

Step	Description
2	The GTP-EP S11 forwards the S11 Delete IDFT Request with Bearer Context with a DL/UL enB FTEID, to the SGW-SVC. The SGW-SVC receives the S11 Delete IDFT Request and performs the following: • Creates a new transaction • Completes the GTP validations
3	The SGW-SVC sends the Sx Modification Request with Remove Traffic Endpoints, to the PFCP-EP.
4	The PFCP-EP sends the Sx Modification Request with Remove Traffic Endpoints, to the UP.
5	The UP sends the Sx Session Modification Response to the PFCP-EP.
6	The SGW-SVC receives the Sx Session Modification Response from the PFCP-EP and performs the following: • Ends the transaction/procedure • Updates the CDL • Sends the Delete IDFT Response with cause as Accepted

OAM Support

This section describes operations, administration, and maintenance information for this feature.

Viewing IDFT Configuration

This section describes the command to view IDFT configurations.

Non- active IDFT for the UE

Command: **show subscriber namespace sgw imsi 123456789012345**

Output:

```
{ "subResponses": [ { "status": true,
…
…
"pdnInfoList": { "totalPdn": 1,
"bearerInfoList": {
"totalBearer": 1, "bearerInfo": [ { "bearerId": "Bearer-1", "state": "Connected",
…
…
} }
]
}
```

Active IDFT for the UE with one PDN having one bearer

Command: **show subscriber namespace sgw imsi 123456789012345**

Output:

```
{ "subResponses": [ { "status": true,
…
…
"pdnInfoList": { "totalPdn": 1,
"bearerInfoList": {
"totalBearer": 1, "bearerInfo": [ { "bearerId": "Bearer-1", "state": "Connected",
…
…
"IndirectForwardingInfo": {
"UplinkInfo":{
"localTeid": "[0x1100000e] 285212686", "localIPv4Address": "209.165.201.8", "remoteTeid":
"[0x1100000f] 285212687", "remoteIPv4Address": "209.165.201.8",
}
"DownlinkInfo":{
"localTeid": "[0x1100000e] 285212686", "localIPv4Address": "209.165.201.8", "remoteTeid":
"[0x1100000f] 285212687", "remoteIPv4Address": "209.165.201.8",
}
}
}
]
}
```

Active IDFT for the UE with one PDN having one bearer in downlink direction

Command: **show subscriber namespace sgw imsi 123456789012345**

Output:

```
{ "subResponses": [ { "status": true,
…
…
"pdnInfoList": { "totalPdn": 1,
"bearerInfoList": {
"totalBearer": 1, "bearerInfo": [ { "bearerId": "Bearer-1", "state": "Connected",
…
…
"IndirectForwardingInfo": {
"DownlinkInfo":{
"localTeid": "[0x1100000e] 285212686",
"localIPv4Address": "209.165.201.8",
"remoteTeid": "[0x1100000f] 285212687",
"remoteIPv4Address": "209.165.201.8",
}
}
}
]
}
```

Active IDFT for one bearer for the UE with one PDN having two bearers

Command: **show subscriber namespace sgw imsi 123456789012345**

Output:

```
"subResponses": [ { "status": true,
…
…
"pdnInfoList": { "totalPdn": 1,
"bearerInfoList": {
"totalBearer": 2, "bearerInfo": [ { "bearerId": "Bearer-1", "state": "Connected",
…
…
```

```
"IndirectForwardingInfo": {
“UplinkInfo”:{
"localTeid": "[0x1100000e] 285212686", "localIPv4Address": "209.165.201.8", "remoteTeid":
"[0x1100000f] 285212687", "remoteIPv4Address": "209.165.201.8",
}
“DownlinkInfo”:{
"localTeid": "[0x1100000e] 285212686", "localIPv4Address": "209.165.201.8", "remoteTeid":
"[0x1100000f] 285212687", "remoteIPv4Address": "209.165.201.8",
}
}
"bearerInfo": [ { "bearerId": "Bearer-2", "state": "Connected",
…
}
}
]
}
```

Note The displayed IndirectForwardingInfo block is only for bearers having indirect forwarding tunnels.

Failure Handling

cnSGW-C supports failure handling for creating or deleting IDFT request procedure.

Following are the failure types that can occur during message processing:

- Advance validation failure on request and response
- Retransmissions timeout
- Transaction SLA
- Failure reported from peer (UP/PGW/MME), depending on the stage of message processing.

The following table depicts the behavior of cnSGW-C during different failure scenarios in call processing.

Failure Scenario	SGW-SVC behavior	Signaling (S11)
1. Create IDFT Request advance validation failure. 2. cnSGW doesn’t have a bearer context for any of the EBIs received in Create IDFT.	Sends failure or No signaling over Sx.	Negative Create IDFT response.

Failure Scenario	SGW-SVC behavior	Signaling (S11)
Single PDN **1.** Sx Session Modify Request (for example, IPC, Retransmission, Internal Failure) with single PDN **2.** Sx Session Modify Response (Cause!= ACCEPTED) with single PDN **3.** Sx Modification Response validation failure	Sends failure. Sends Context not found of nonexisting EBI. Clear the PDN if sxCause = Context Not Found.	Negative Create IDFT response. DBR and DSR over S11 and S5 when *sxCause = Context Not Found.*
Multi PDN (Partial Failure) **1.** Partial Existing PDN: Continue with existing PDN **2.** Sx Session Modify Request (for example, IPC, Retransmission Timeout, Internal Failure) for some PDNs **3.** Sx Session Modify Response (Cause!= ACCEPTED) for some PDN **4.** Sx Modification Response validation failure	Send Context Not Found for nonexisting PDNs. Send failure in Bearer Context for PDNs for which Sx Modification Request fails.	Partially Accepted Create IDFT Response. DBR and DSR over S11 and S5 for the PDN for which *sxCause = Context Not Found.*
Multi PDN (Complete Failure): **1.** Partial Existing PDN: Continue with existing PDN. **2.** Sx Session Modify Request (for example, IPC, Retransmission Timeout, Internal Failure) **3.** Sx Session Modify Response (Cause!= ACCEPTED) **4.** Sx Modification Response validation failure	Send Context Not Found for nonexisting PDNs. Send failure in Bearer Context for PDNs which has Sx Modification Request fails.	Negative Create IDFT Response. DBR and DSR over S11 and S5 for the PDN for which *sxCause = Context Not Found.*
Delete IDFT Request Advance validation failure.	Send failure or No signaling over Sx.	Negative Delete IDFT response.

Failure Scenario	SGW-SVC behavior	Signaling (S11)
1. Single and Multi-PDN 2. Sx Session Modify Request (for example, IPC, Retransmission Timeout, Internal Failure) 3. Sx Session Modify Response (Cause!= ACCEPTED)	Ignore Failure.	Positive Delete IDFT Response. DBR and DSR over S11 and S5 for the PDN for which *sxCause = Context Not Found.*

Bulk Statistics Support

The following statistics are supported for the IDFT Support feature.

```
sgw_service_stats{app_name="smf",cluster="cn",data_center="cn",fail_reason="",
instance_id="0",interface="interface_sgw_ingress",reject_cause="",service_name="sgw-service",
sgw_procedure_type="create_indirect_data_forwarding_tunnel",status="attempted",sub_fail_reason=""}
 3
```

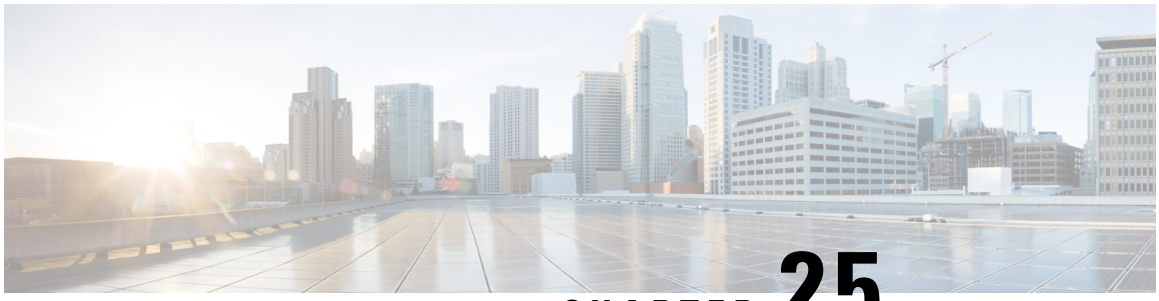
```
sgw_service_stats{app_name="smf",cluster="cn",data_center="cn",fail_reason="",instance_id="0",
interface="interface_sgw_ingress",reject_cause="",service_name="sgw-service",sgw_procedure_type=
"create_indirect_data_forwarding_tunnel",status="success",sub_fail_reason=""} 2
```

```
sgw_service_stats{app_name="smf",cluster="cn",data_center="cn",fail_reason="",instance_id="0",
interface="interface_sgw_ingress",reject_cause="",service_name="sgw-service",sgw_procedure_type=
"delete_indirect_data_forwarding_tunnel",status="attempted",sub_fail_reason=""}
1
```

```
sgw_service_stats{app_name="smf",cluster="cn",data_center="cn",fail_reason="",
instance_id="0",interface="interface_sgw_ingress",reject_cause="",service_name="sgw-service",
sgw_procedure_type="delete_indirect_data_forwarding_tunnel",status="success",sub_fail_reason=""}
 1
```

```
sgw_service_stats{app_name="smf",cluster="cn",data_center="cn",fail_reason="",instance_id="0",
interface="interface_sgw_ingress",reject_cause="",service_name="sgw-service",sgw_procedure_type=
"indirect_data_forwarding_tunnel_guard_timer_expiry",status="attempted",sub_fail_reason=""}
 1
```

```
sgw_service_stats{app_name="smf",cluster="cn",data_center="cn",fail_reason="",instance_id="0",
interface="interface_sgw_ingress",reject_cause="",service_name="sgw-service",sgw_procedure_type=
"indirect_data_forwarding_tunnel_guard_timer_expiry",status="success",sub_fail_reason=""}
 1
```



CHAPTER 25

Idle Session Timeout Settings

Feature Summary and Revision History

Summary Data

Table 93: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration required to enable
Related Documentation	Not Applicable

Revision History

Table 94: Revision History

Revision Details	Release
First introduced.	2021.02.0

Feature Description

The stale session timeout determines the duration for which the SGW-U sessions can remain inactive before they are terminated. On the cnSGW-C platform, the SubscribeCtx represents the subscriber session. The SGW-U establishes a connection with peers, such as:

- MME and PGW using the S11 or S4 interface
- PGW on the S5 or S8 interface

When the peers delete the peer session, the SGW-U doesn't receive the deletion message or inadvertently misses them. In such situations, the SGW-U sessions remain idle and continue to receive the calls but do not process or respond to the request. To prevent the stale sessions from using the resources, the idle timeout feature enables the SGW-U to receive new subscriber session requests after deleting the old or stale sessions.

How it Works

This section describes how this feature works.

A subscriber session is idle when data traffic activity is not steered towards it as it is inactive for a stipulated time.

The session manager on the user plane tracks the state of the call line. Sessions for which the session manager does not record the call line data traffic are determined as idle. Using the idle session timeout configuration, you can set the time interval for which the session can remain idle before it times out. The idle timeout configuration is set when the session is established. The SGW-U sends the timeout configuration to the user plane in the Sx Session Establishment Request. In case of multi-PDN calls, the calls directed towards a stale session are cleared after the inactivity report is generated for all PDNs.

Every second, the SGW-U monitors the data traffic activity to determine the session's idleness status. On identifying a stale session, the user plane updates the User Plane Inactivity Report in the Sx Session Usage Report and sends it to cnSGW-C to convey that the session is idle. Further, the cnSGW-C initiates a session deletion request towards its peers.

Based on the network environment, configure the idle timeout configuration in seconds. The accepted range of the timeout value is 1–4294967295 seconds. The timeout configuration is applicable at the SGW-U service profile level enabling the idle timeout handling for the set of subscribers handled by the SGW-U service.

Call Flows

This section describes the key call flows for this feature.

Inactivity Report Call Flow

This section describes the Inactivity Report call flow.

Figure 46: Inactivity Report Call Flow

Table 95: Inactivity Report Call Flow Description

Step	Description
1	The MME sends the Create Session Request to the GTP-EP (S11).
2	The GTP-EP (S11) forwards the Create Session Request to the SGW.
3	The SGW-SVC sends the Session Idle Timer in IE = USER INACTIVITY as part of Sx Session Establishment Request to the Protocol.
4	The SGW-U reads the Session Idle Timer from USER INACTIVITY and stores it at the CLP level. The UPF sends the Sx Session Report Request to the Protocol.
5	The Protocol sends the Sx Session Report Request to the SGW-SVC.
6	The SGW-SVC sends the Sx Session Report Response to the Protocol.
7	The Protocol sends the Sx Session Report Response to the UPF.

Step	Description
8	The SGW-SVC sends the Delete Session Request to the GTPC-EP.
9	The GTPC-EP sends the Delete Session Request to the PGW.
10	The SGW-SVC sends the Delete Bearer Request to the GTP-EP.
11	The GTP-EP sends the Delete Bearer Request to the MME.
12	The MME sends the Delete Bearer Response to the GTP-EP.
13	The GTP-EP sends the Delete Bearer Response to the SGW-SVC.
14	The PGW sends the Delete Session Response to the GTPC-EP.
15	The GTPC-EP sends the EGTP Delete Session Response to the SGW-SVC.
16	The SGW-SVC sends the Sx Session Deletion Request to the Protocol.
17	The Protocol sends the Sx Session Deletion Request to the UPF.
18	The UPF sends the Sx Session Deletion Response to the Protocol.
19	The Protocol sends the Sx Session Deletion Response to the SGW-SVC.

Idle Timer Handling on UPF Call Flow

This section describes the call flow when the idle timer is received in the Create Session Request on the UPF.

Figure 47: Idle Timer Handling on UPF Call Flow

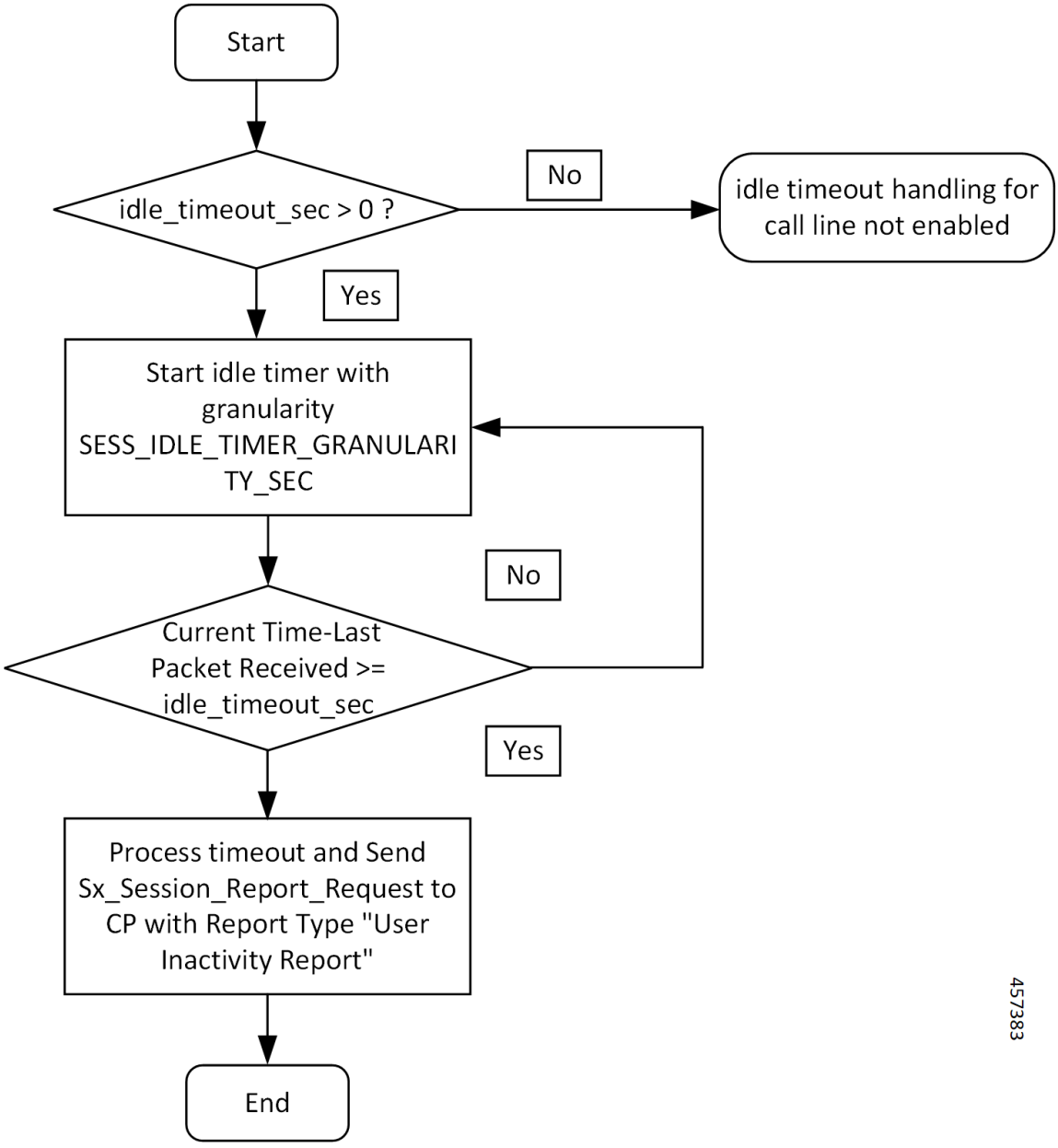


Table 96: Idle Timer Handling on UPF Call Flow Description

Step	Description
1	If the value of idle_timeout_sec is greater than zero, the timer is started on UPF with granularity of one second. Else, idle timeout is disabled.

Step	Description
2	The timer timeouts every second. Checks if the difference in current time and last packet received is greater than idle_timeout_sec or not. If the time difference is greater than idle_timeout_sec, then UP sends the Sx Session Report Request with Report Type = UPIR (Inactivity Report) to CP (cnSGW-C).

Reactivity Report Call Flow

This section describes the Reactivity Report call flow.

Figure 48: Reactivity Report Call Flow

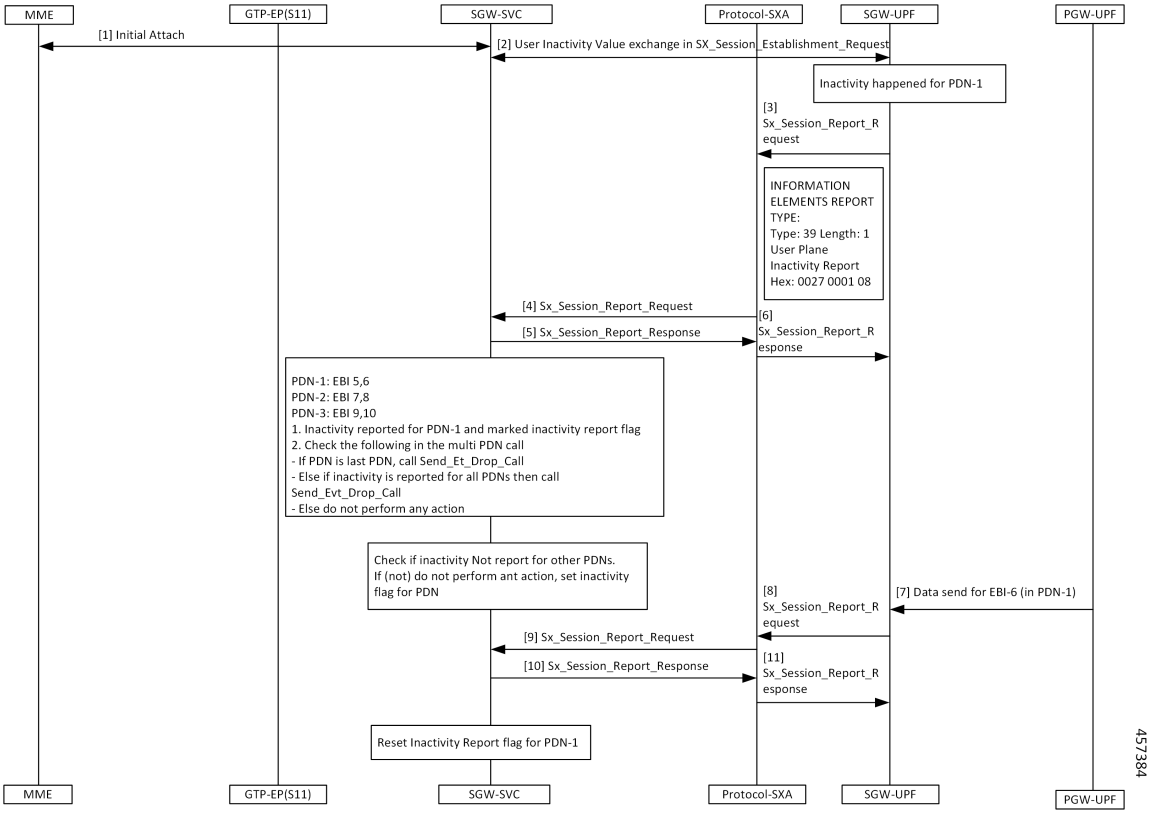


Table 97: Reactivity Report Call Flow Description

Step	Description
1	The MME and the SGW-SVC process the initial attach request.
2	The Protocol-SXA and the SGW-UPF perform the user inactivity exchange in the Sx Session Establishment Request.
3	If the inactivity is observed in PDN-1, the SGW-UPF sends the Sx_Session_Report_Request with type User Plane Inactivity Report to the Protocol-SXA.

Step	Description
4	The Protocol-SXA sends the Sx_Session_Report_Request to the SGW-SVC.
5	The SGW-SVC sends the Sx_Session_Report_Response to the Protocol-SXA.
6	The Protocol-SXA forwards the Sx_Session_Report_Response to the SGW-UPF.
7	The PGW-UPF sends the data for the EBI-6 (in PDN-1) to the SGW-UPF.
8	The SGW-UPF sends the Sx_Session_Report_Request with IE Report-Type = User Plane Re-Activity Report to the Protocol-SXA.
9	The Protocol-SXA sends the Sx_Session_Report_Request with IE Report-Type = User Plane Re-Activity Report to the SGW-SVC.
10	The SGW-SVC responds with the Sx_Session_Report_Response to the Protocol-SXA.
11	The Protocol-SXA sends the Sx_Session_Report_Response to the SGW-UPF. After receiving the Sx_Session_Report_Response on the control plane, SGW-SVC clears the Inactivity Report Flag for the PDN.

Clear Call Handling Call Flow

This section describes the Clear Call Handling call flow.

Figure 49: Clear Call Handling Call Flow

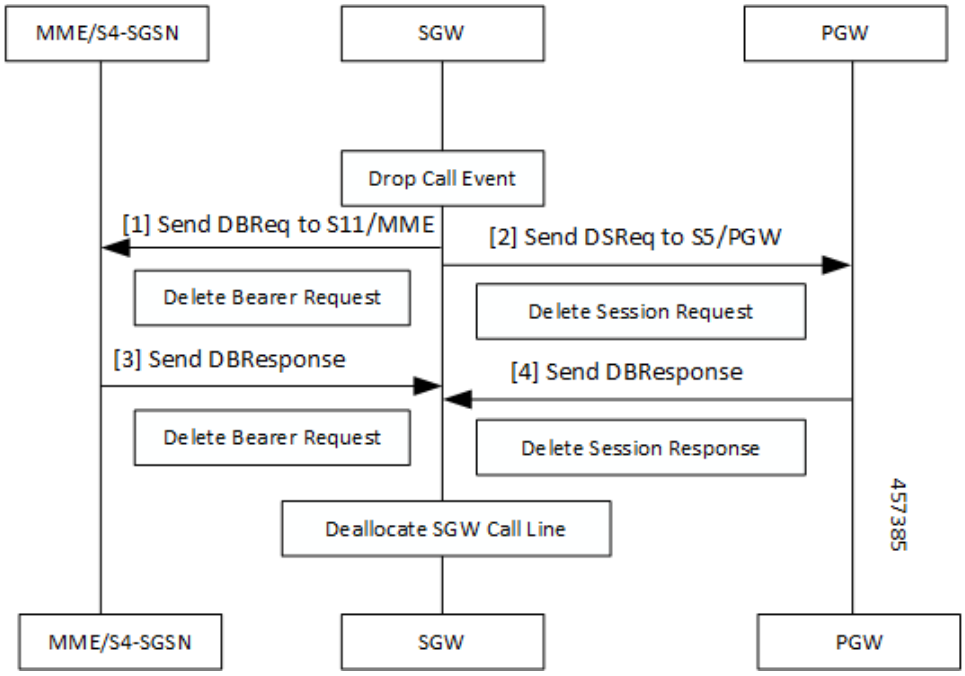


Table 98: Clear Call Handling Call Flow Description

Step	Description
1	On the SGW, the control plane receives the User Plane Inactivity Report in Sx Session Report Request. The control plane evaluates if PDN in the request is the latest PDN, or the inactivity report has already reported other PDNs. The control plane initiates the ClearCall procedure.
2	After receiving the ClearCall message, the cnSGW-C triggers a Session Deletion Request to its peers.
3	The SGW sends the Delete Bearer Request to the S11/MME.
4	The SGW sends the Delete Session Request to the S5/PGW.
5	On receiving the Delete Session Request, SGW clears resources on the UPF by sending a Sx Session Delete Request.

Feature Configuration

To configure this feature, use the following configuration:

```
config
  profile sgw sgw_group_name
    session-idle-timer session_idle_timer
    end
```

NOTES:

- **session-idle-timer** *session_idle_timer*—Specify the maximum duration in seconds for which a session remains idle. After the configured time is reached, the system automatically terminates the session. The accepted range contains integers in the range of 1–4294967295. The default value is zero indicating that the idle session is disabled.

Configuration Example

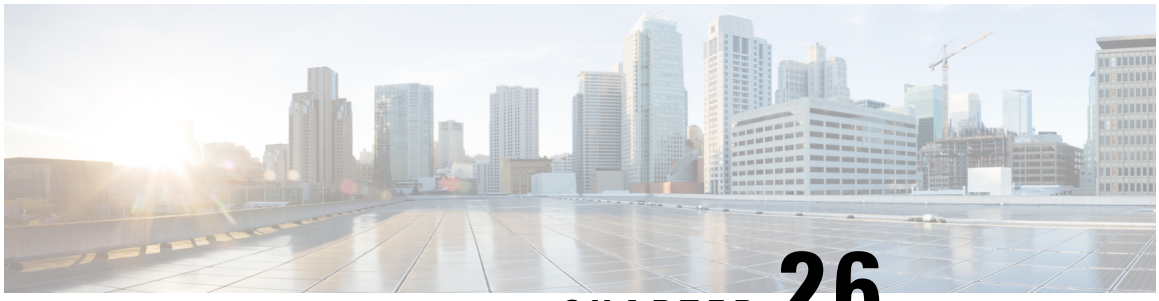
The following is an example configuration.

```
config
   profile sgw sgw1
     session-idle-timer 1000
     end
```

Configuration Verification

To verify the configuration:

```
show running-config profile sgw sgw1 session-idle-timer
profile sgw sgw1
session-idle-timer 1000
```



CHAPTER 26

Initial Attach Support

Feature Summary and Revision History

Summary Data

Table 99: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 100: Revision History

Revision Details	Release
First introduced.	2020.04

Feature Description

cnSGW-C supports handling of Initial Attach Create Session Request. As a part of this feature, cnSGW-C supports receiving Create Session Request from the MME through the EGTP endpoint. Further, cnSGW-C decodes the UDP message and converts the message into gRPC message for internal message processing.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flow for this feature.

Initial Attach Call Flow

This section describes the Initial Attach call flow.

Figure 50: Initial Attach Call Flow

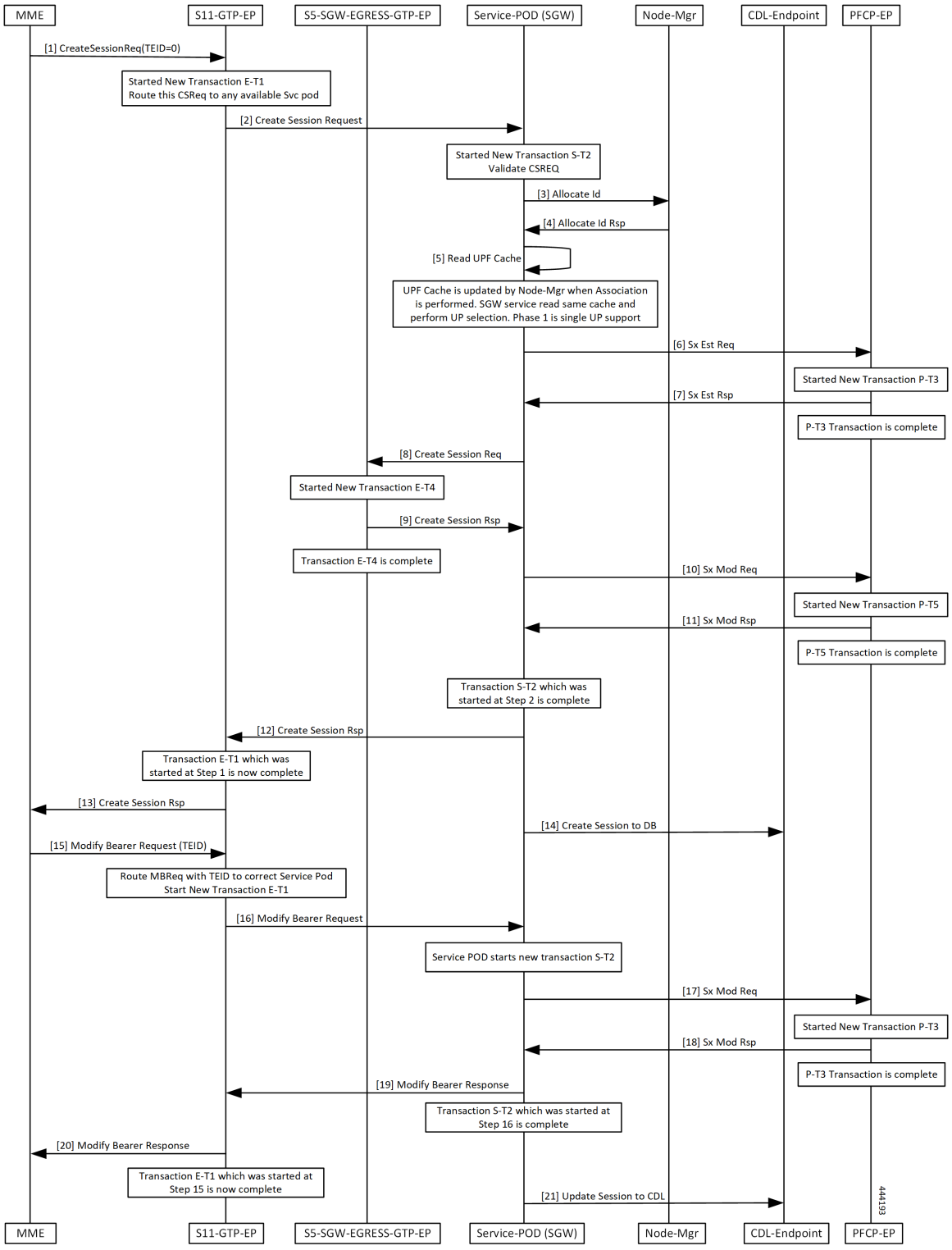


Table 101: Initial Attach Call flow Description

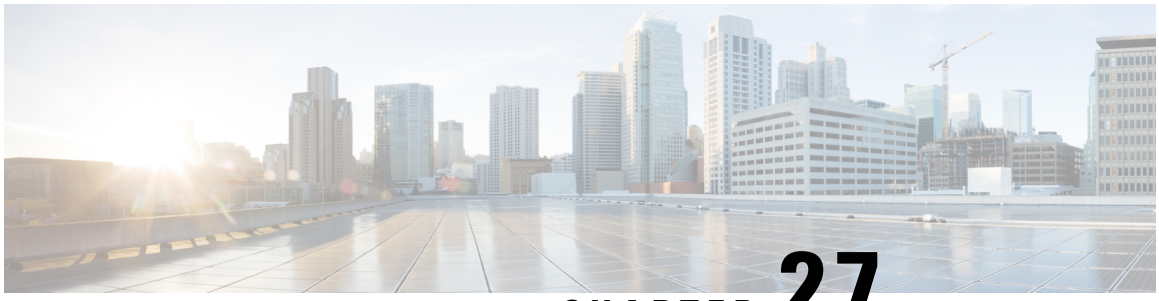
Step	Description
1	The MME sends the Create Session Request with TEID value zero to the S11-GTP-EP.
2	Transaction E-T1 is started. The S11-GTP-EP forwards the Create Session Request to the Service-POD (SGW).
3	Transaction S-T2 is started to validate the Create Session Request. The Service-POD (SGW) sends the Allocate Id Request to the Node-Mgr.
4	The Node-Mgr sends the Allocate Id Response to the Service-POD (SGW).
5	The Service-POD (SGW) reads the cache to perform the UPF selection.
6	The Service-POD (SGW) sends the Sx Establishment Request to the PFCP-EP.
7	Transaction P-T3 is started. The PFCP-EP sends the Sx Establishment Response to the Service-POD (SGW).
8	Transaction P-T3 is completed. The Service-POD (SGW) sends the Create Session Request to the S5-SGW-EGRESS-GTP-EP.
9	Transaction E-T4 is started. The S5-SGW-EGRESS-GTP-EP sends the Create Session Response to the Service-POD (SGW).
10	Transaction E-T4 is completed. The Service-POD (SGW) sends the Sx Modification Request to the PFCP-EP.
11	Transaction P-T5 is started. The PFCP-EP sends the Sx Modification Response to the Service-POD (SGW).
12	Transactions P-T5 and S-T2 are completed. The Service-POD (SGW) sends the Create Session Response to the S11-GPT-EP.
13	Transaction E-T1 is completed. The S11-GPT-EP forwards the Create Session Response to the MME.
14	The Service-POD (SGW) sends the Create Session to DB message to the CDL-Endpoint.
15	The MME sends the Modify Bearer Request with TEID to the S11-GTP-EP.
16	Transaction E-T1 is started. The S11-GTP-EP sends the Modify Bearer Request to the Service-POD (SGW).
17	Transaction S-T2 is started. The Service-POD (SGW) sends the Sx Modification Request to the PFCP-EP.

Step	Description
18	Transaction P-T3 is started. The PFCP-EP sends the Sx Modification Response to the Service-POD (SGW).
19	Transaction P-T3 is completed. The Service-POD (SGW) sends the Modify Bearer Response to the S11-GTP-EP.
20	Transaction S-T2 is completed. The S11-GPT-EP forwards the Modify Bearer Response to the MME.
21	Transaction E-T1 is completed. The Service-POD (SGW) sends the Update Session to CDL message to the CDL-Endpoint. The session is updated in CDL.

Standards Compliance

This feature complies with the following standards specifications:

- *3GPP TS 29.274 "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3"*



CHAPTER 27

Inter System RAT Handover

Feature Summary and Revision History

Summary Data

Table 102: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 103: Revision History

Revision Details	Release
First introduced.	2021.01.0

Feature Description

cnSGW-C is the Control Plane Network Functions (NF) of the Converged Core Network (4G-5GC).

cnSGW-C NF is built on top of SMI architecture. cnSGW-C acts as the UE anchor and supports mobility procedures along with session setup and termination procedures as specified in 3GPP TS 23.401, 23.214.

cnSGW-C User Plane (UP) is used to create UP sessions and bearers to carry data traffic.

This feature supports the following procedures in cnSGW-C:

- Wi-Fi to LTE
- GnGp to LTE Hand Over

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows of this feature.

Wi-Fi to LTE Success Call Flow

This section describes the Wi-Fi to LTE success call flow.

Figure 51: Wi-Fi to LTE Success Call Flow

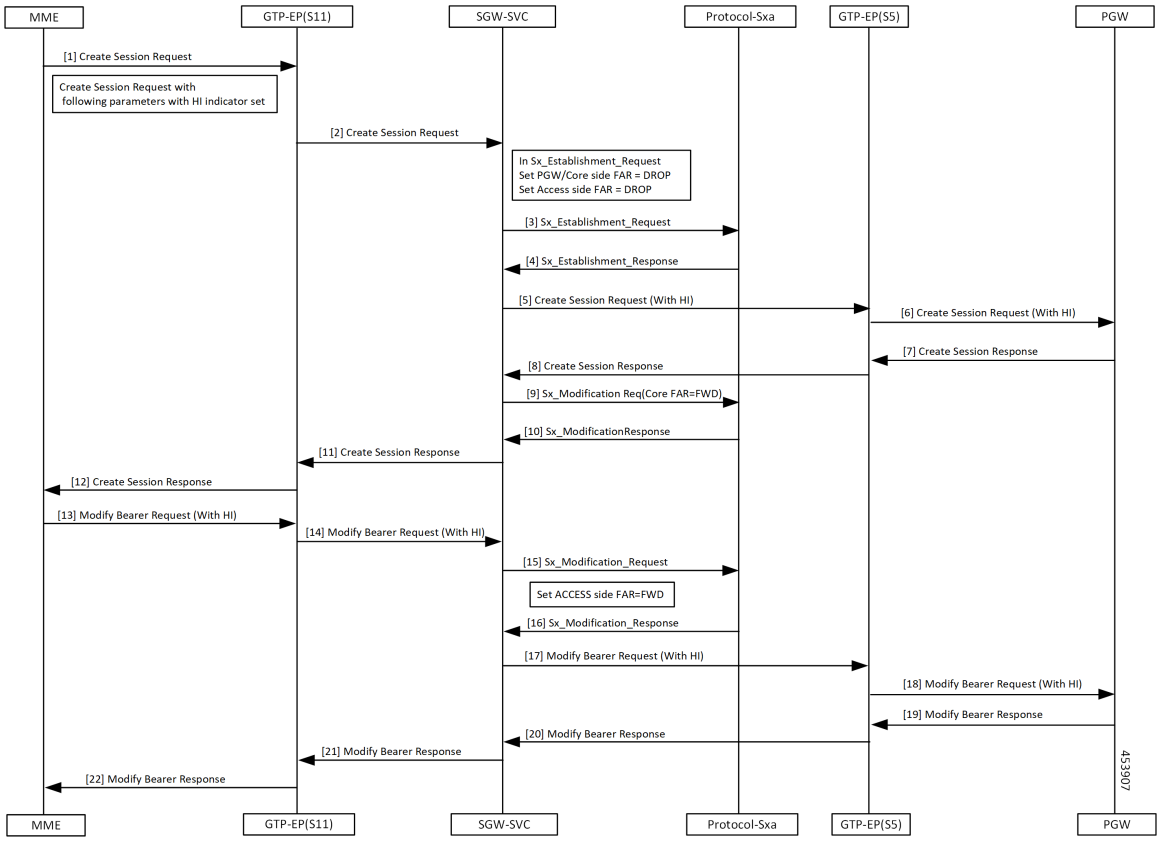


Table 104: Wi-Fi to LTE Success Call Flow Description

Step	Description
1	The MME sends the Create Session Request to the GTP-EP(S11) with: • RAT as EUTRAN • The handoff indicator set to TRUE.
2	The GTP-EP(S11) forwards the Create Session Request to the SGW-SVC.
3	The SGW-SVC sends the Sx Establishment Request to the Protocol-Sxa.
4	The Protocol-Sxa sends the Sx Establishment Response to the SGW-SVC.
5	The SGW-SVC sends the Create Session Request (with HI) to the GTP-EP(S5).
6	The GTP-EP(S5) forwards the Create Session Request (with HI) to the PGW.
7	The PGW sends the Create Session Response to the GTP-EP(S5). The PGW provides IPv6 Prefix.
8	The GTP-EP(S5) forwards the Create Session Response to the SGW-SVC.
9	The SGW-SVC sends the Sx Modification Request to the Protocol-Sxa.
10	The Protocol-Sxa sends the Sx Modification Response to the SGW-SVC.
11	The SGW-SVC sends the Create Session Response to the GTP-EP(S11).
12	The GTP-EP(S11) sends the Create Session Response to the MME.
13	The MME sends the Modify Bearer Request (with HI) to the GTP-EP(S11).
14	The GTP-EP forwards the Modify Bearer Request (with HI) to the SGW-SVC.
15	The SGW-SVC sends the Sx Modification Request to the Protocol-Sxa.
16	The Protocol-Sxa sends the Sx Modification Response to the SGW-SVC.
17	The SGW-SVC forwards the Modify Bearer Request (with HI) to the GTP-EP(S5).
18	The GTP-EP(S5) forwards the Modify Bearer Request (with HI) to the PGW.
19	The PGW sends the Modify Bearer Response to the GTP-EP(S5).
20	The GTP-EP(S5) forwards the Modify Bearer Response to the SGW-SVC.
21	The SGW-SVC forwards the Modify Bearer Response to the GTP-EP(S11).

Step	Description
22	The GTP-EP(S11) forwards the Modify Bearer Response to the MME. The S1 SGW FTEID is the same as the S1-U SGW FTEID sent in Create Session Response from the SGW-SVC to the MME. The SGW-SVC can now send the downlink packets to the eNodeB, and the switching of the data path from Wi-Fi to LTE occurs after the Modify Bearer Response.

GnGp to LTE Handover with OI Indicator Set Call Flow

This section describes the GnGp to LTE Handover with Operation Indication (OI) Indicator Set call flow.

Figure 52: GnGp to LTE Handover with OI Indicator Set Call Flow

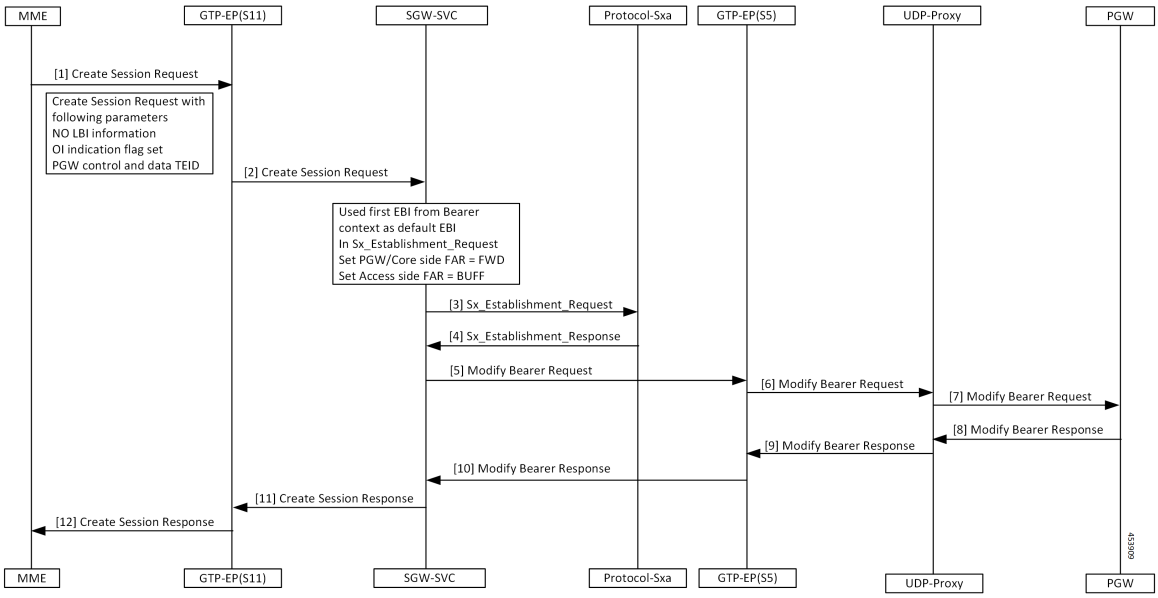


Table 105: GnGp to LTE Handover with OI Indicator Set Call Flow Description

Step	Description
1	The MME sends the Create Session Request to the GTP-EP(S11) with the following information: • EBI List (No LBI Information) • PGW control and data TEID • OI Indicator flag set
2	The GTP-EP(S11) forwards the Create Session Request to the SGW-SVC.
3	The SGW-SVC sends the Sx Session Establishment Request to the Protocol-Sxa.
4	The Protocol-Sxa sends the Sx Establishment Response to the SGW-SVC.
5	The SGW-SVC sends the Modify Bearer Request to GTP-EP(S5).

Step	Description
6	The GTP-EP(S5) forwards the Modify Bearer Request to the UDP-proxy.
7	The UDP-proxy forwards the Modify Bearer Request to the PGW.
8	The PGW sends the Modify Bearer Response with the default EBI information to the UDP-Proxy.
9	The UDP-proxy forwards the Modify Bearer Response to the GTP-EP(S5).
10	The GTP-EP(S5) forwards the Modify Bearer Response to the SGW-SVC.
11	The SGW-SVC sends the Create Session Response with the default EBI information to the GTP-EP(S11).
12	The GTP-EP(S11) forwards the Create Session Response to the MME.

GnGp to LTE Handover with OI Indicator Unset Call Flow

This section describes the GnGp to LTE Handover with Operation Indication (OI) Indicator Unset call flow.

Figure 53: GnGp to LTE Handover with OI Indicator Unset Call Flow

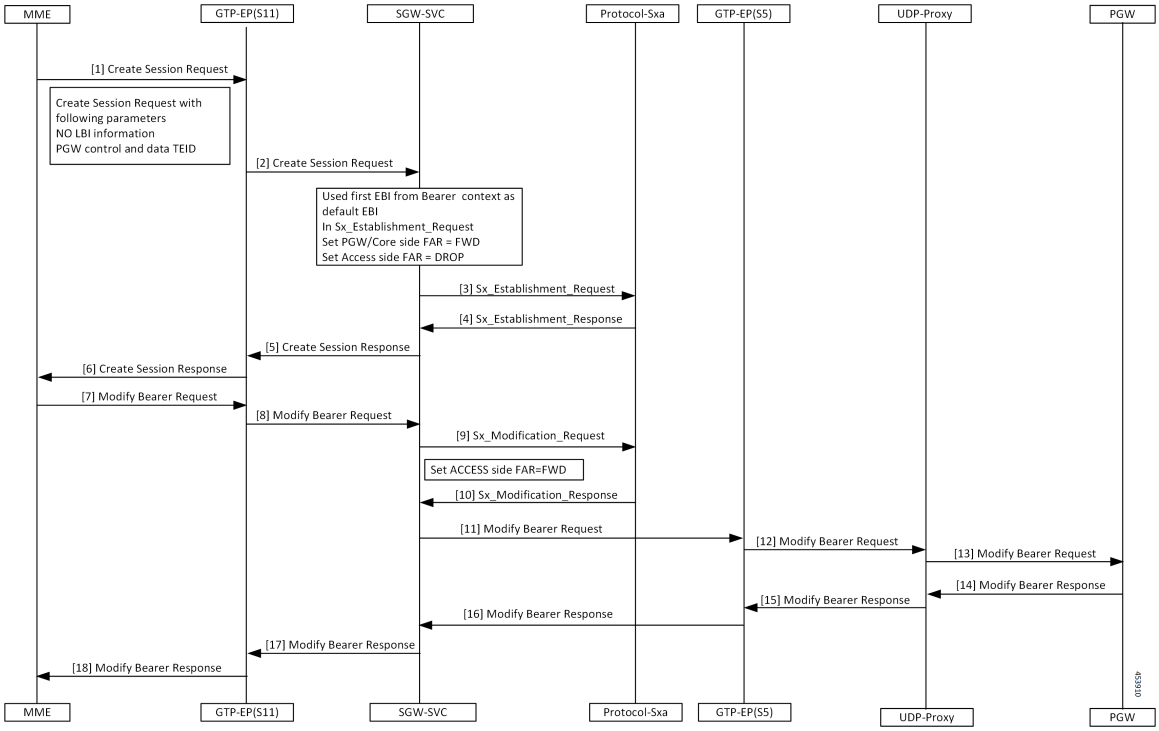


Table 106: GnGp to LTE HO with OI Indicator Unset Call Flow Description

Step	Description
1	The MME sends the Create Session Request to the GTP-EP(S11) with the following information: • EBI List (No LBI Information) • PGW control and data TEID • OI Indicator flag unset
2	The GTP-EP(S11) forwards the Create Session Request to the SGW-SVC.
3	The SGW-SVC sends the Sx Session Establishment Request to the Protocol-Sxa.
4	The Protocol-Sxa sends the Sx Establishment Response to the SGW-SVC.
5	The SGW-SVC sends the Create Session Response to the GTP-EP(S11).
6	The GTP-EP(S11) forwards the Create Session Response to the MME.
7	The MME sends the Modify Bearer Request to the GTP-EP(S11).
8	The GTP-EP(S11) forwards the Modify Bearer Request to the SGW-SVC.
9	The SGW-SVC sends the Sx Modification Request to the Protocol-Sxa.
10	The Protocol-Sxa sends the Sx Modification Response to the SGW-SVC.
11	The SGW-SVC sends the Modify Bearer Request to the GTP-EP(S5).
12	The GTP-EP(S5) forwards the Modify Bearer Request to the UDP-Proxy.
13	The UDP-proxy forwards the Modify Bearer Request to the PGW.
14	The PGW sends the Modify Bearer Response with the default EBI information to the UDP-Proxy.
15	The UDP-Proxy forwards the Modify Bearer Response to the GTP-EP(S5).
16	The GTP-EP(S5) forwards the Modify Bearer Response to the SGW-SVC.
17	The SGW-SVC forwards the Modify Bearer Response to the GTP-EP(S11).
18	The GTP-EP(S11) forwards the Modify Bearer Response to the MME. The S1 SGW FTEID is the same as the S1-U SGW FTEID sent in Create Session Response from the SGW-SVC to the MME. The SGW-SVC can now send the downlink packets to the eNodeB, and the switching of the data path from Wi-Fi to LTE occurs after the Modify Bearer Response.

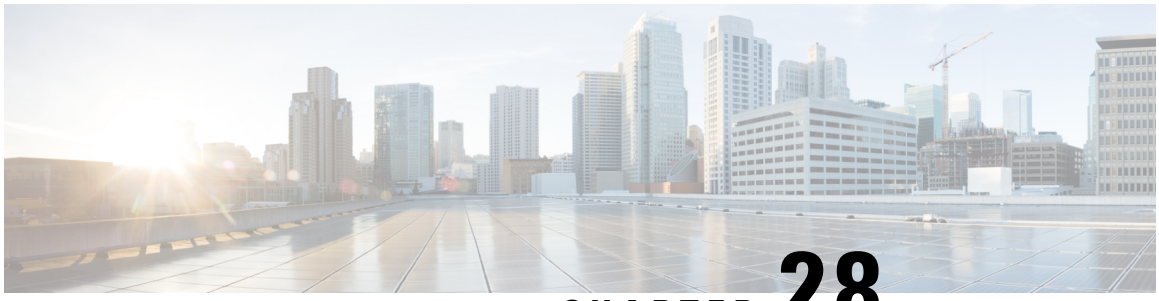
Note cnSGW-C clears the call when the received default EBI in the Modify Bearer Response differs with the first EBI in the following scenarios:

- GnGp to LTE HO with OI Indicator Set
- GnGp to LTE HO with OI Indicator Unset

Standards Compliance

This feature complies with the following standards specifications:

- *3GPP TS 23.401 "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access"*
- *3GPP TS 23.214 "Architecture enhancements for control and user plane separation of EPC nodes"*



CHAPTER 28

Intra-MME and Inter-MME Handover Procedures

Feature Summary and Revision History

Summary Data

Table 107: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 108: Revision History

Revision Details	Release
First introduced.	2021.01.0

Feature Description

cnSGW-C supports Intra-MME Intra-SGW, and Inter-MME Intra-SGW handover.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

Inter-MME Handover Active-Active Transition Call Flow

This section describes the Inter-MME Handover Active-Active Transition call flow.

Figure 54: Inter-MME Handover Active-Active Transition Call Flow

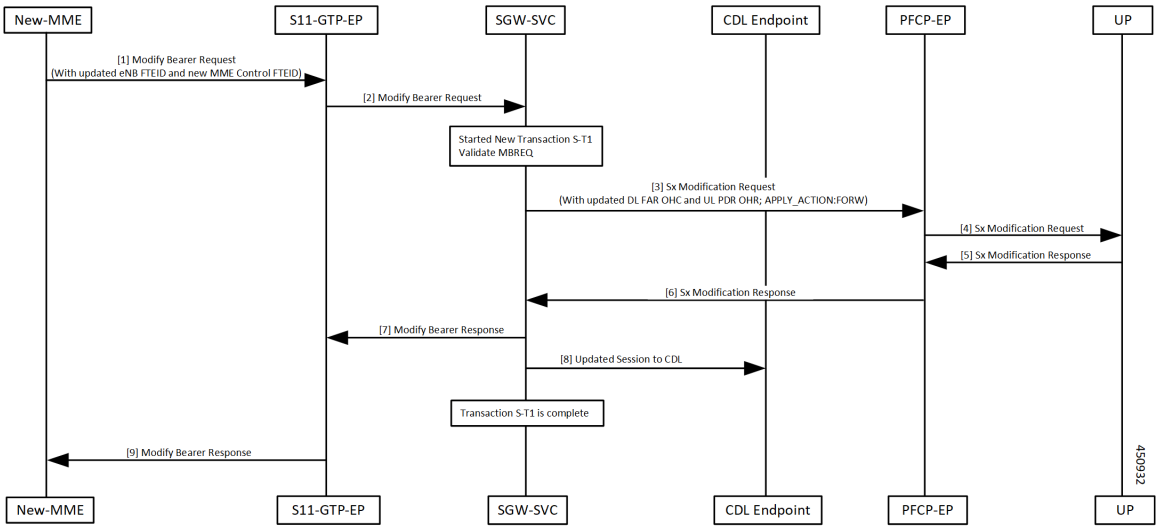


Table 109: Inter-MME Handover Active-Active Transition Call Flow Description

Step	Description
1	New-MME sends the Modify Bearer Request to the S11-GTP-EP pod, with updated eNodeB F-TEID and new MME control F-TEID.
2	S11-GTP-EP pod forwards the Modify Bearer Request to the SGW-SVC. SGW-SVC performs the following: • Creates a new transaction S-T1 • Validates the Modify Bearer Request
3	SGW-SVC sends the the Sx Modification Request with downlink FAR OHC, uplink PDR OHR, and APPLY ACTION as FORWARD, to the PFCP-EP pod.
4	PFCP-EP pod sends the Sx Modification Request to the UP.
5	UP sends the Sx Modification Response to the PFCP-EP pod.

Step	Description
6	PFCP-EP pod sends the Sx Modification Response to the SGW-SVC.
7	SGW-Service pod sends the Modify Bearer response to the S11-GTP-EP pod.
8	SGW-SVC sends the Updated Session to the CDL Endpoint. Transaction S-T1 is complete.
9	S11-GTP-EP pod sends the Modify Bearer Response to the New-MME.

Intra-MME Handover Active-Active Transition Call Flow

This section describes the Inear-MME Handover Active-Active Transition call flow.

Figure 55: Intra-MME Handover Active-Active Transition Call Flow

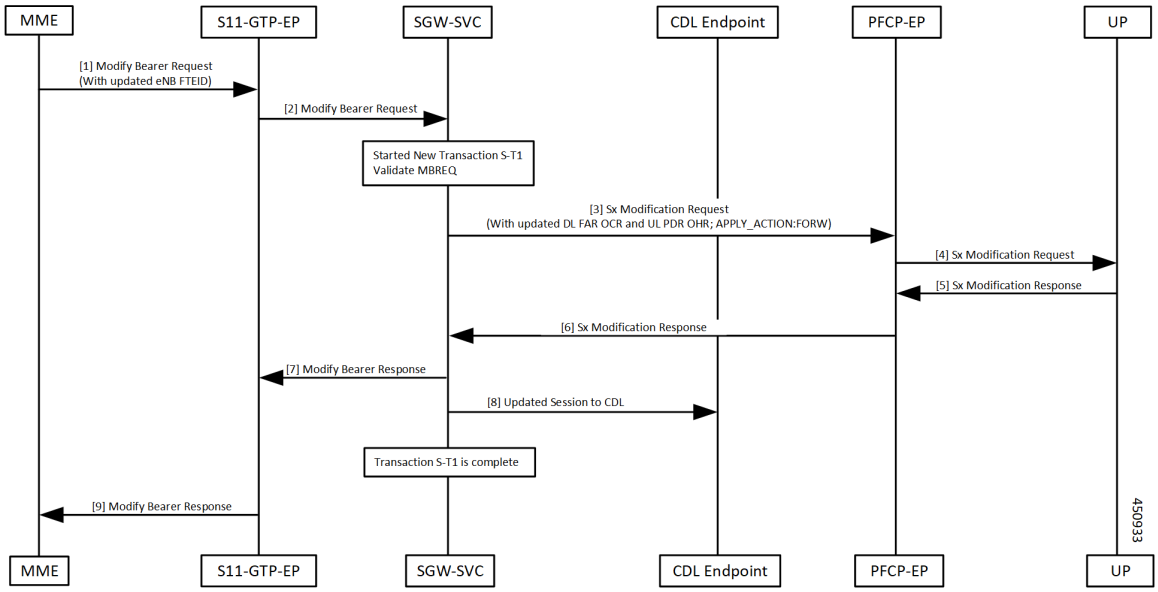


Table 110: Intra-MME Handover Active-Active Transition Call Flow Description

Step	Description
1	MME sends the Modify Bearer Request to the S11-GTP-EP pod, with the updated eNodeB F-TEID.
2	S11-GTP-EP pod sends the Modify Bearer Request to the SGW-SVC. SGW-SVC performs the following: • Creates a new transaction S-T1 • Validates Modify Bearer Request
3	SGW-SVC sends the the Sx Modification Request with downlink FAR OCR, uplink PDR OHR, and APPLY ACTION as FORWARD, to the PFCP-EP pod.

Step	Description
4	PFCP-EP pod forwards the Sx Modification Request to the UP.
5	UP sends the Sx Modification Response to the PFCP-EP pod.
6	PFCP-EP pod sends the Sx Modification Response to the SGW-SVC.
7	SGW-SVC sends the Modify Bearer Response to the S11-GTP-EP pod.
8	SGW-SVC sends the Updated Session to the CDL Endpoint. Transaction S-T1 is complete.
9	S11-GTP-EP pod sends the Modify Bearer Response to the MME.

Inter/Intra-MME Handover Idle-Idle Transition Call Flow

This section describes the Inter/Intra-MME Handover Idle-Idle Transition call flow.

Figure 56: Inter/Intra-MME Handover Idle-Idle Transition Call Flow

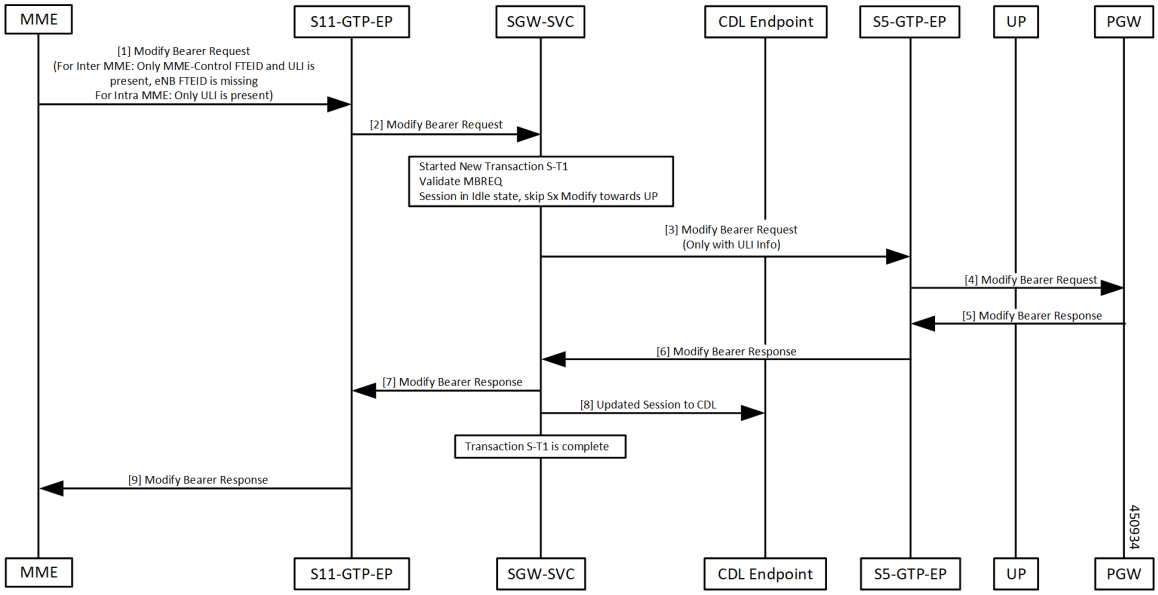


Table 111: Inter/Intra-MME Handover Idle-Idle Transition Call Flow Description

Step	Description
1, 2	For inter-MME, received Modify Bearer request at SGW-Service POD via S11-GTPC-EP POD with MME control F-TEID and ULI. There is no eNodeB F-TEID. For intra-MME, received Modify Bearer request at SGW-Service POD with only ULI present: • Create a new transaction S-T1. • Validate Modify Bearer request. • Skip Sx modification as session is in idle state.

Step	Description
3, 4	Received Modify Bearer request at S5 GTPC-EP POD from SGW-Service POD with ULI. Modify Bearer request is forwarded to PGW.
5, 6	Received Modify Bearer response at S5 GTPC-EP POD from PGW. Modify Bearer response received at SGW-Service POD.
7	SGW-Service POD forwards Modify Bearer response to S11 GTPC-EP POD ingress.
8, 9	Session updated at CDL. Transaction S-T1 is complete. S11 GTPC-EP POD forwards Modify Bearer response to MME.

Inter/Intra-MME Handover Active-Idle Transition Call Flow

This section describes the Inter/Intra-MME Handover Active-Idle transition call flow.

Figure 57: Inter/Intra-MME Handover Active-Idle Transition Call Flow

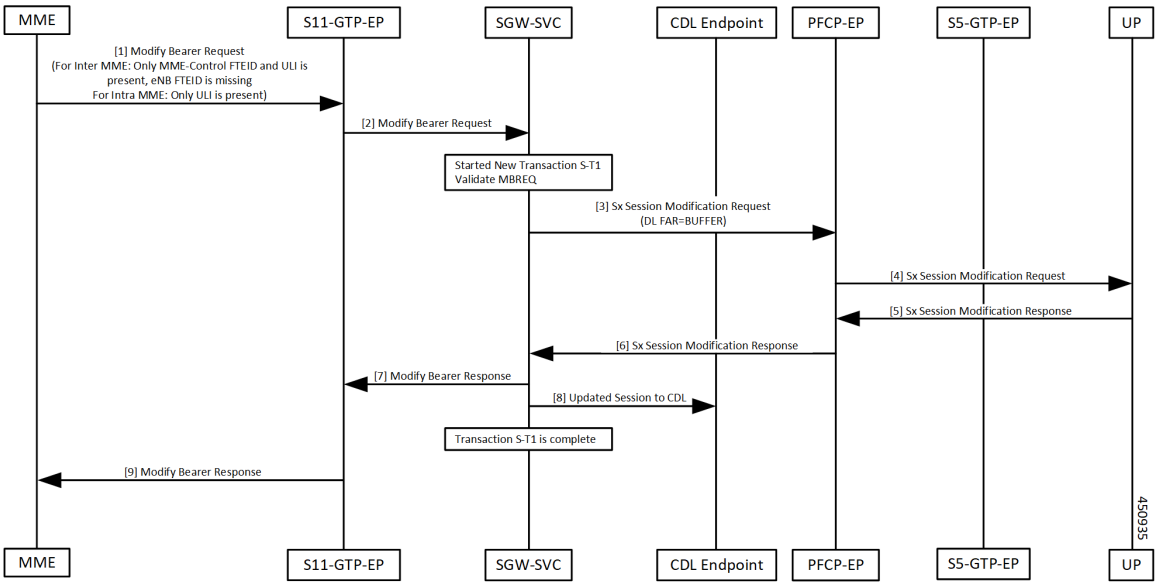


Table 112: Inter/Intra-MME Handover Active-Idle Transition Call Flow Description

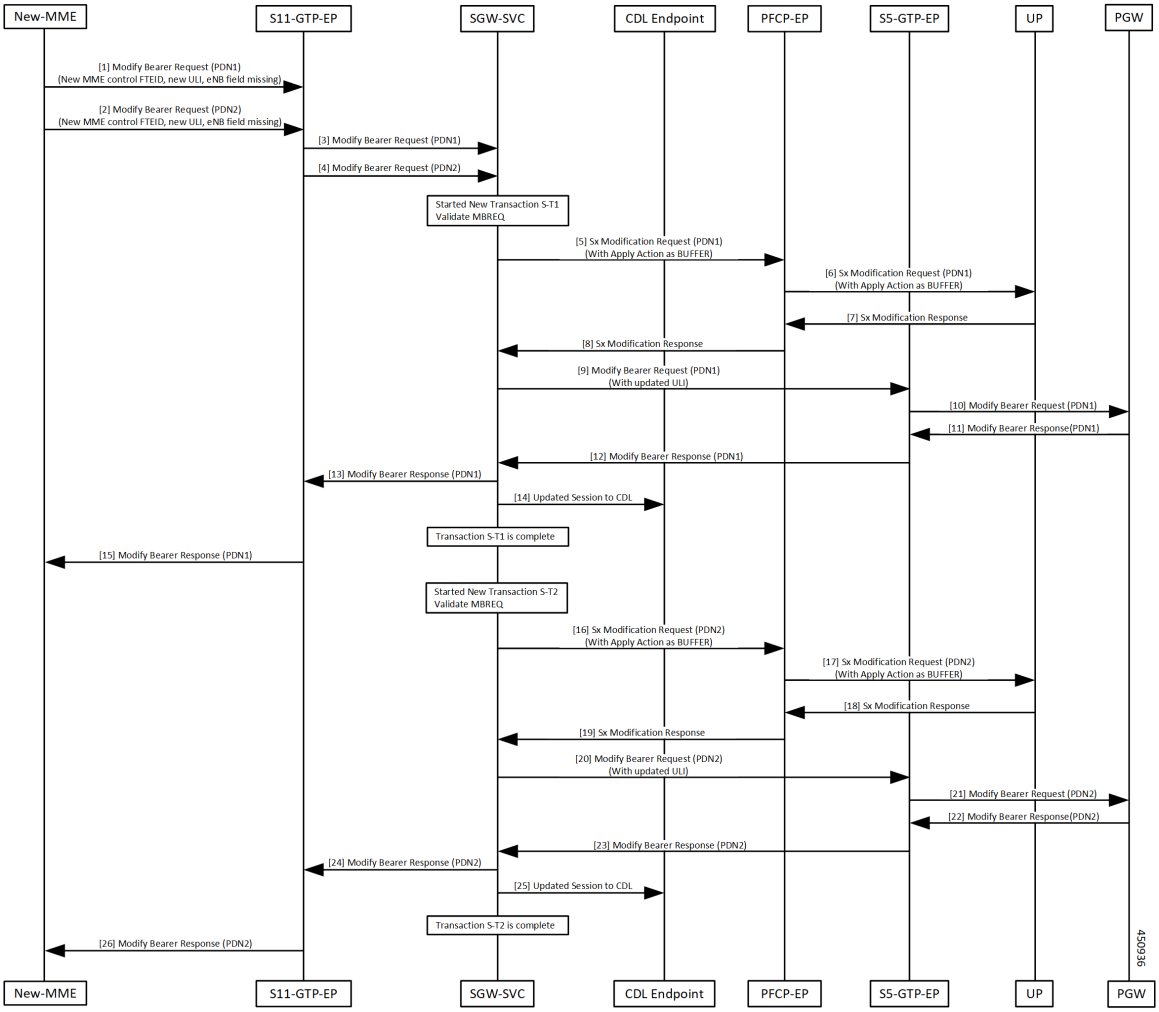
Step	Description
1, 2	For inter-MME, received Modify Bearer request at SGW-Service POD via S11-GTPC-EP POD with MME control F-TEID and ULI. There is no eNodeB F-TEID. For intra-MME, received Modify Bearer request at SGW-Service POD with only ULI present: • Create a new transaction S-T1. • Validate Modify Bearer request.
3, 4	Received Sx Modification request at PFCP-EP POD from SGW-Service POD with downlink FAR as BUFFER. Sx Modification request is forwarded to UP.

Step	Description
5, 6	Received Sx Modification response at at PFCP-EP POD from UP. Sx Modification response received at SGW-Service POD.
7	SGW-Service POD forwards Modify Bearer response to GTPC-EP POD ingress.
8, 9	Session updated at CDL. Transaction S-T1 is complete. GTPC-EP POD forwards Modify Bearer response to MME.

Inter-MME Handover and Multi-PDN Handling Active-Idle Transition with ULI Change Call Flow

This section describes the Inter-MME Handover and Multi-PDN Handling Active-Idle transition with ULI change call flow.

Figure 58: Inter-MME Handover and Multi-PDN Handling Active-Idle Transition with ULI Change Call Flow



Repeat the steps provided in the Table 113: Inter-MME Handover and Multi-PDN Handling Active-Idle Transition with ULI Change Call Flow Description, on page 275 for PDN1 and PDN2 with respective transaction S-T1 and S-T2.

Table 113: Inter-MME Handover and Multi-PDN Handling Active-Idle Transition with ULI Change Call Flow Description

Step	Description
1, 2, 3, 4	Received Modify Bearer request for both the PDNs (PDN1 and PDN2) at SGW-Service POD with new MME control F-TEID and new ULI. There is no eNodeB F-TEID present in Modify Bearer request. • Create a new transaction S-T1. • Validate Modify Bearer request.
5, 6	Received Sx Modification request from SGW-Service POD > PFCP-EP POD with APPLY ACTION as BUFFER. Sx Modification request is forwarded to UP.
7, 8	Received Sx Modification response from UP > PFCP-EP POD. Sx Modification response received at SGW-Service POD.
9, 10	Received Modify Bearer request from SGW-Service POD > S5 GTPC-EP POD with updated ULI. Modify Bearer request is received at PGW.
11, 12	Received Modify Bearer response from PGW > S5 GTPC-EP POD. Modify Bearer response received from S5 GTPC-EP POD > SGW-Service POD.
13	SGW-Service POD forwards Modify Bearer response to GTPC-EP POD ingress.
14, 15	Session updated at CDL. Transaction S-T1 is complete. GTPC-EP POD forwards Modify Bearer response to MME.

Inter-MME Handover with Bearer Context Marked for Removal Call Flow

This section describes the Inter-MME Handover with Bearer Context Marked for Removal call flow.

Figure 59: Inter-MME Handover with Bearer Context Marked for Removal Call Flow

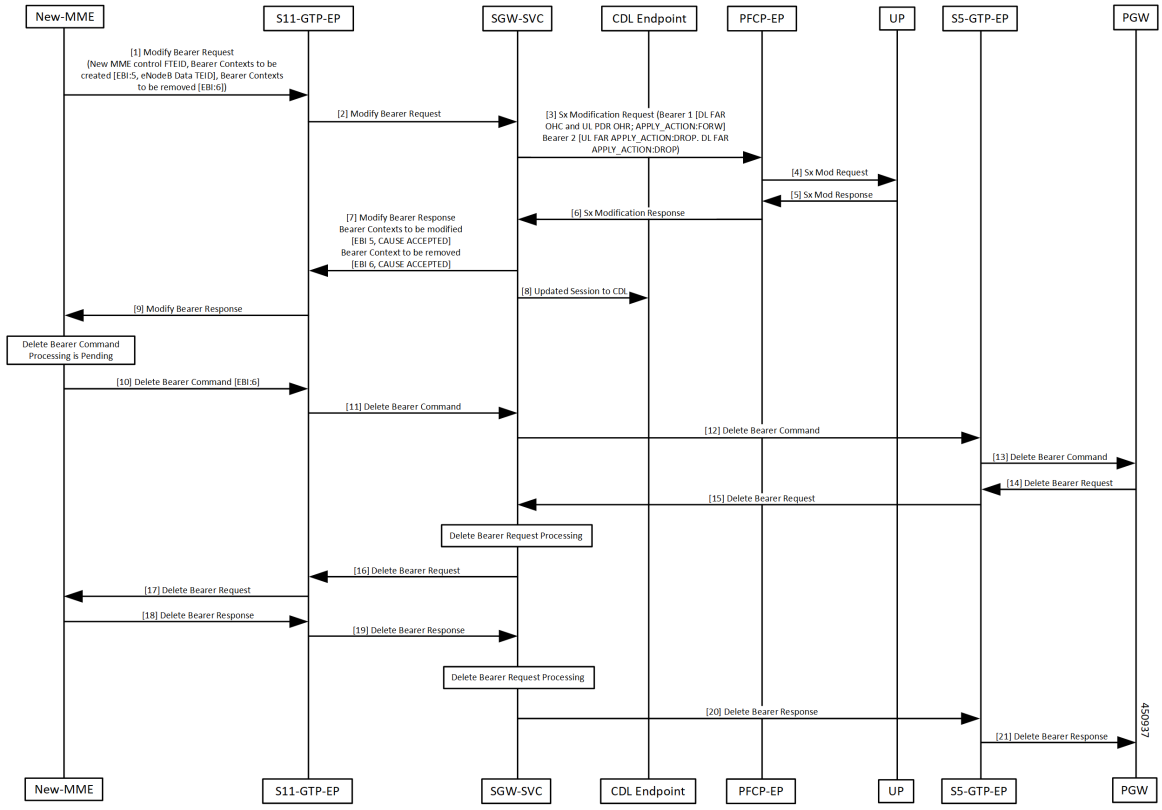


Table 114: Inter-MME Handover with Bearer Context Marked for Removal Call Flow Description

Step	Description
1, 2	Received Modify Bearer request at SGW-Service POD with new MME control F-TEID, bearer-context-1 to be created with EBI:5, eNodeB data TEID, bearer-context-2 to be removed with EBI:6. • Create a new transaction S-T1. • Validate Modify Bearer request.
3, 4	Received Sx Modification request from SGW-Service POD to PFCP-EP POD for: • bearer-context-1: downlink FAR OHC, uplink PDR OHR and APPLY ACTION as FORWARD • bearer-context-2: uplink FAR APPLY ACTION as DROP and downlink FAR APPLY ACTION as DROP Sx Modification request is forwarded to UP.
5, 6	Received Sx Modification response from UP > PFCP-EP POD. Sx Modification response is received at SGW-Service POD.

Step	Description
7	SGW-Service POD forwards Modify Bearer response to GTPC-EP POD ingress with bearer context to be modified (EBI:5, cause as ACCEPTED) and bearer context to be removed (EBI:6, cause as ACCEPTED).
8, 9	Session updated at CDL. GTPC-EP POD forwards Modify Bearer response to MME.
10, 11	Received delete bearer command at SGW-Service POD with EBI:6.
12, 13	SGW-Service POD forwards delete bearer command to S5 GTPC-EP POD. Delete bearer command received at PGW.
14, 15	Received Delete Bearer request from PGW > S5 GTPC-EP POD. Delete Bearer request received at SGW-Service POD.
16, 17	SGW-Service POD processes Delete Bearer request and forwards it to GTPC-EP POD ingress.
18, 19	Delete Bearer response received at SGW-Service POD and processed.
20, 21	Delete Bearer response received at S5 GTPC-EP POD. Delete Bearer response is received at PGW.

Intra-MME and Inter-MME Handover Procedures OAM Support

This section describes operations, administration, and maintenance information for this feature.

Bulk Statistics

The following statistics are supported for the Intra-MME and Inter-MME Handover Procedures feature.

Intra-MME Handover

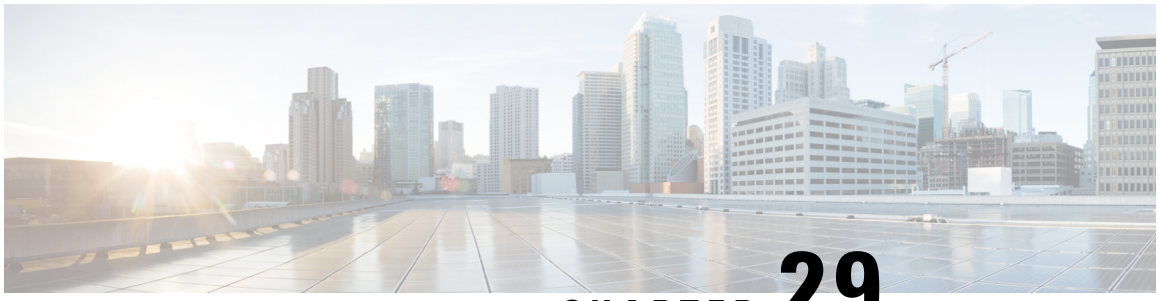
```
sgw_service_stats{app_name="smf",cluster="cn",data_center="cn",fail_reason="",
instance_id="0",interface="interface_sgw_ingress",reject_cause="",service_name="sgw-service",
sgw_procedure_type="intra_mme_handover",status="attempted",sub_fail_reason=""} 2
```

```
sgw_service_stats{app_name="smf",cluster="cn",data_center="cn",fail_reason="",
instance_id="0",interface="interface_sgw_ingress",reject_cause="",service_name="sgw-service",
sgw_procedure_type="intra_mme_handover",status="success",sub_fail_reason=""} 2
```

Inter-MME Handover

```
sgw_service_stats{app_name="smf",cluster="cn",data_center="cn",fail_reason="",
instance_id="0",interface="interface_sgw_ingress",reject_cause="",service_name="sgw-service",
sgw_procedure_type="inter_mme_handover",status="attempted",sub_fail_reason=""} 2
```

```
sgw_service_stats{app_name="smf",cluster="cn",data_center="cn",fail_reason="",
instance_id="0",interface="interface_sgw_ingress",reject_cause="",service_name="sgw-service",
sgw_procedure_type="inter_mme_handover",status="success",sub_fail_reason=""} 2
Perform S1 Based SGW handover (with OI=0)
```



CHAPTER 29

MCC/MNC Configuration in the SGW Service

Feature Summary and Revision History

Summary Data

Table 115: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration required to enable
Related Documentation	Not Applicable

Revision History

Table 116: Revision History

Revision Details	Release
First introduced.	2021.01.0

Feature Description

This feature supports the list of MCC and MNC configuration as a PLMN-list in the SGW profile.

As per the PLMN-list configuration in the SGW profile, the PLMN-type is identified as one of the following:

- Homer
- Roamer
- Visitor

Note If this feature is not enabled, the PLMN-type subscriber is marked as a Visitor, by default.

How it Works

This section describes how the feature works.

Call Flows

This section describes the key call flows for this feature.

PLMN-type Detection Call Flow

This section describes the PLMN-type Detection call flow.

Figure 60: PLMN-type Detection Call Flow

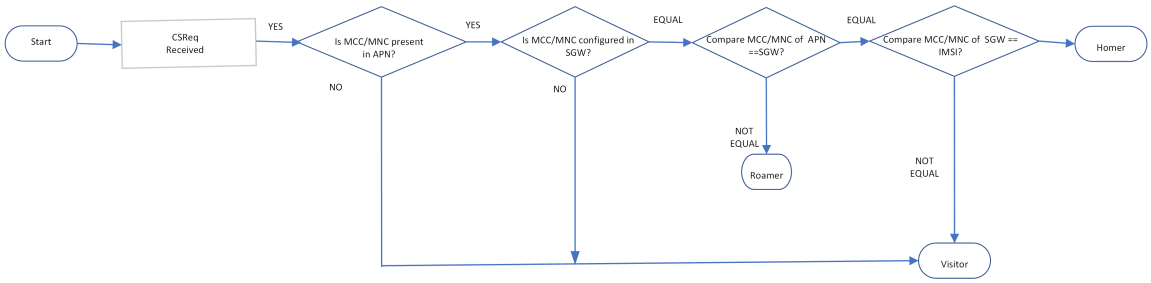


Table 117: PLMN-type Detection Call Flow Description

Step	Description
1	The PLMN-type detection process begins.
2	The Create Session Request is received.
3	The MCC or the MNC presence in the APN is verified: • If YES, the next step is executed. • If NO, the PLMN-type subscriber is concluded as Visitor.

Step	Description
4	The MCC or the MNC presence in the SGW is verified: • If YES, the next step is executed. • If NO, the PLMN-type subscriber is concluded as Visitor.
5	The values of the MCC or the MNC in the APN and the SGW are compared: • If EQUAL, it proceeds to the next step. • If NOT EQUAL, the PLMN-type subscriber is concluded as Roamer.
6	The values of the MCC or the MNC in the SGW and the IMSI are compared: • If EQUAL, the PLMN-type subscriber is concluded as Homer. • If NOT EQUAL, the PLMN-type subscriber is concluded as Visitor.

Configuring the MCC or the MNC in the SGW Service

This section describes how to configure the MCC or the MNC in the SGW service.

Use the following commands to configure the MCC or the MNC in the SGW service.

```
config
   profile sgw sgw_name
      plmn-list
         mcc mcc_value
         mnc mnc_value
         end
```

NOTES:

- **plmn-list**—List of MCC and MNC values.
- **mcc** *mcc_value*—Specify the MCC value. Must be a three-digit number. Example: 123
- **mnc** *mnc_value*—Specify the MNC value. Must be a two or three-digit number. Example: 23 or 456

Configuration Example

The following is an example configuration.

```
config
   profile sgw sgw_1
      plmn-list
         mcc 123
         mnc 456
         end
```

OAM Support

This section describes operations, administration, and maintenance support for this feature.

Bulk Statistics Support

The following statistics are supported for the MCC and MNC Configuration in the SGW Service feature.

Active PDN Counters

```
sgw_pdn_counters{app_name="smf",cluster="cn",data_center="cn",
instance_id="0",pdn_plmn_type="homer",pdn_type="ipv6",rat_type="EUTRAN",
service_name="sgw-service"} 12
```

```
sgw_pdn_counters{app_name="smf",cluster="cn",data_center="cn",
instance_id="0",pdn_plmn_type="roamer",pdn_type="ipv4v6",rat_type="EUTRAN",
service_name="sgw-service"} 3
```

```
sgw_pdn_counters{app_name="smf",cluster="cn",data_center="cn",
instance_id="0",pdn_plmn_type="visitor",pdn_type="ipv4",rat_type="EUTRAN",
service_name="sgw-service"} 2
```

Setup or Released PDN Statistics

```
sgw_pdn_stats{app_name="smf",cluster="cn",data_center="cn",
instance_id="0",pdn_plmn_type="homer",pdn_type="ipv6",rat_type="EUTRAN",
service_name="sgw-service",status="release"} 1
```

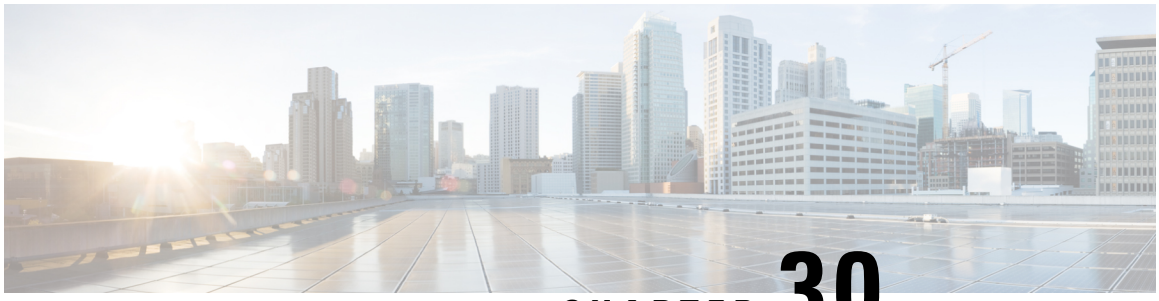
```
sgw_pdn_stats{app_name="smf",cluster="cn",data_center="cn",
instance_id="0",pdn_plmn_type="homer",pdn_type="ipv6",rat_type="EUTRAN",
service_name="sgw-service",status="setup"} 13
```

```
sgw_pdn_stats{app_name="smf",cluster="cn",data_center="cn",
instance_id="0",pdn_plmn_type="roamer",pdn_type="ipv4v6"rat_type="EUTRAN",
service_name="sgw-service",status="release"} 1
```

```
sgw_pdn_stats{app_name="smf",cluster="cn",data_center="cn",
instance_id="0",pdn_plmn_type="roamer",pdn_type="ipv4v6",rat_type="EUTRAN",
service_name="sgw-service",status="setup"} 4
```

```
sgw_pdn_stats{app_name="smf",cluster="cn",data_center="cn",
instance_id="0",pdn_plmn_type="visitor",pdn_type="ipv4",rat_type="EUTRAN",
service_name="sgw-service",status="release"} 1
```

```
sgw_pdn_stats{app_name="smf",cluster="cn",data_center="cn",
instance_id="0",pdn_plmn_type="visitor"pdn_type="ipv4",rat_type="EUTRAN",
service_name="sgw-service",status="setup"} 3
```



CHAPTER 30

Message Interactions Support

Feature Summary and Revision History

Summary Data

Table 118: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Documentation	Not Applicable

Revision History

Table 119: Revision History

Revision Details	Release
Procedures added for: • Collision Resolver • Multiple CBR • Double Delete Optimized • Abort Handling of Low priority and Handling Suspension	2021.02.0

Revision Details	Release
First introduced.	2021.01.0

Feature Description

The Message Interactions feature provides the capability to receive and process the messages from different peers (UPF, MME, and PGW), and performs the priority resolution.

The following are the examples of message interaction scenarios and priorities:

- The Modify Bearer Request (MBR) and Update Bearer Request (UBR) received for the same PDN1 waits for the Sx Modify Response from UPF. The UBR is processed after the MBR is completed. In this scenario, the UBR process is suspended until the MBR is processed.
- The UBR1 received for the PDN1 while processing a Release Access Bearer (RAB) for the same PDN1. The UBR is processed after the RAB is completed. In this scenario, the UBR1 process is suspended when the RAB procedure is in progress.
- The existing PDN procedure is stopped when the disconnect procedure (Delete Session Request (DSR), Delete Bearer Request (DBR), or Clear Sub) is sent for the same PDN. For example, cnSGW-C receives the DSR for the PDN when the CBR1 and UBR1 procedures are in progress for the same PDN1. The DSR processing is started, and CBR1 and UBR1 processing is stalled. For more information, see the Graceful Stop the Existing PDN Procedure Call Flow, on page 290 call flow.
- The existing UE procedure (RAB or DDN) is stopped when the disconnect procedure (DSR, DBR, or Clear Sub) for the PDN is received. For example, cnSGW-C receives the DBR for the PDN while processing the RAB or DDN. The DBR procedure is started, and the RAB or DDN procedure is stopped.
- The incoming procedure for the PDN is stopped when the disconnect procedure (DSR, DBR, or Clear Sub) for the same PDN is in progress. For example, the UBR receives the PDN when sending the DSR for the same PDN. The UBR procedure is stopped, and the DSR procedure continues.
- The new incoming UE procedure is stopped when processing the disconnect procedure (DSR, DBR, or Clear Sub) for the same PDN. For example, the RAB received for the PDN1 when processing the multi-PDN call DSR for the same PDN1. The RAB procedure is stopped and rescheduled after the DSR for PDN1 gets completed.
- The CBR and the UBR message handling are stopped when the initial attach procedure is in progress.
- Optimization of the double delete handling. For example, the cnSGW-C receives the DSR from MME and DBR in the PGW, for which the DBR Sx modify step is pending toward the UPF. The DBR signaling is not initiated toward the S11 interface.
- The processing of the low priority procedures is stopped when the high priority procedure is received on the same bearer. For example, cnSGW-C receives the DBR for the PDN on a dedicated bearer while processing UBR on the same bearer. The DBR handling procedure is started, and the processing of the existing UBR procedure on the same bearer is stopped.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

CBR Multi-PDN Call Flow

This section describes the CBR Multi-PDN call flow.

Figure 61: CBR Multi-PDN Call Flow

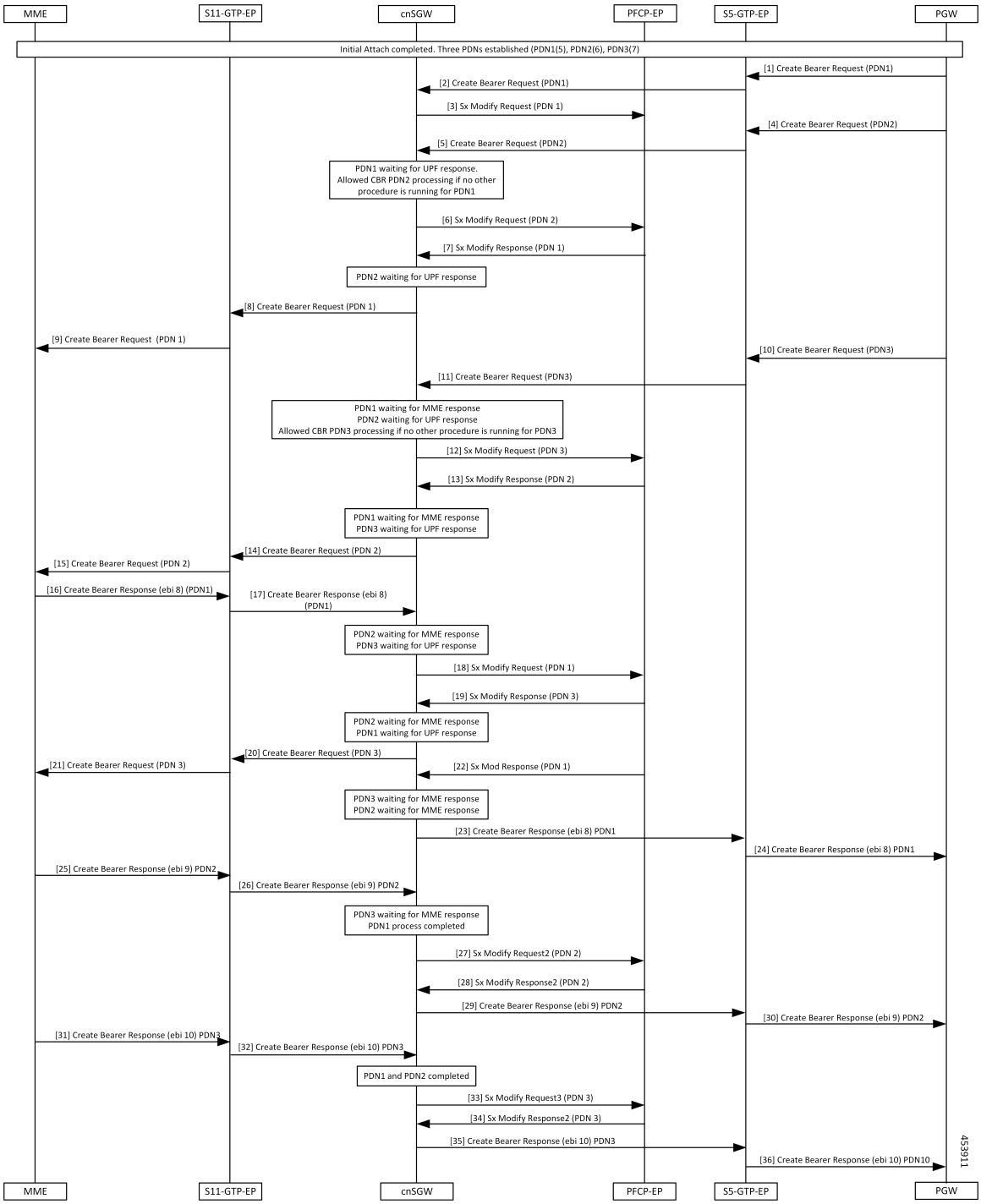


Table 120: CBR Multi-PDN Call Flow Description

Step	Description
1	The Initial Attach process is completed with the three established PDNs. The PGW sends a Create Bearer Request for PDN1 to the S5-GTP-EP.
2	The S5-GTP-EP sends the Create Bearer Request for PDN1 to the cnSGW.
3	The cnSGW sends a Sx Modify Request for PDN1 to the PFCP-EP.
4	The PGW sends a Create Bearer Request for PDN2 to the S5-GTP-EP.
5	The S5-GTP-EP sends the Create Bearer Request PDN2 to the cnSGW.
6	The cnSGW sends a Sx Modify Request to PFCP-EP for PDN2.
7	The PFCP-EP sends the Sx Modify Response for PDN1 to the cnSGW.
8	The cnSGW sends the Create Bearer Request for PDN1 to the S11-GTP-EP.
9	The S11-GTP-EP sends the Create Bearer Request for PDN1 to the MME.
10	The PGW sends the Create Bearer Request (PDN3) to the S5-GTP-EP.
11	The S5-GTP-EP sends the Create Bearer Request (PDN3) to the cnSGW.
12	The cnSGW sends the Sx Modify Request (PDN3) to the PFCP-EP.
13	The PFCP-EP sends the Sx Modify Response for PDN2 to the cnSGW.
14	The cnSGW sends the Create Bearer Request for PDN2 to the S11-GTP-EP.
15	The S11-GTP-EP sends the Create Bearer Request for PDN1 to the MME.
16	The MME sends the Create Bearer Response for PDN1 to the S11-GTP-EP.
17	The S11-GTP-EP sends the Create Bearer Response for PDN1 to the cnSGW.
18	The cnSGW sends the Sx Modify Request for PDN1 to the PFCP-EP.
19	The PFCP-EP sends the Sx Modify Response for PDN3 to the cnSGW.
20	The cnSGW sends the Create Bearer Request for PDN3 to the S11-GTPC-EP.
21	The S11-GTPC-EP sends the Create Bearer Request for PDN3 to the MME.
22	The PFCP-EP sends the Sx Modify Response2 for PDN1 to the cnSGW.
23	The cnSGW sends the Create Bearer Response for PDN1 to the S5-GTP-EP.
24	The S5-GTP-EP sends the Create Bearer Response for PDN1 to the PGW.
25	The MME sends the Create Bearer Response for PDN2 to the S11-GTPC-EP.
26	The S11-GTPC-EP sends the Create Bearer Response for PDN1 to the cnSGW.

Step	Description
27	The cnSGW sends the Sx Modify Request to the PFCP-EP for PDN2.
28	The PFCP-EP sends the Sx Modify Response for PDN2 to the cnSGW.
29	The cnSGW sends the Create Bearer Response for PDN2 to the S5-GTP-EP.
30	The S5-GTP-EP sends the Create Bearer Response for PDN2 to the PGW.
31	The MME sends the Create Bearer Response for PDN3 to the S11-GTPC-EP.
32	The S11-GTPC-EP sends the Create Bearer Response for PDN3 to the cnSGW.
33	The cnSGW sends the Sx Modify Request for PDN2 to the PFCP-EP.
34	The PFCP-EP sends the Sx Modify Response for PDN3 to the cnSGW.
35	The cnSGW sends the Create Bearer Response for PDN3 to the S5-GTP-EP.
36	The S5-GTP-EP sends the Create Bearer Response for PDN3 to the PGW.

Graceful Stop the Existing PDN Procedure Call Flow

This section describes the Graceful Stop the Existing PDN Procedure call flow.

Figure 62: Graceful Stop the Existing PDN Procedure Call Flow

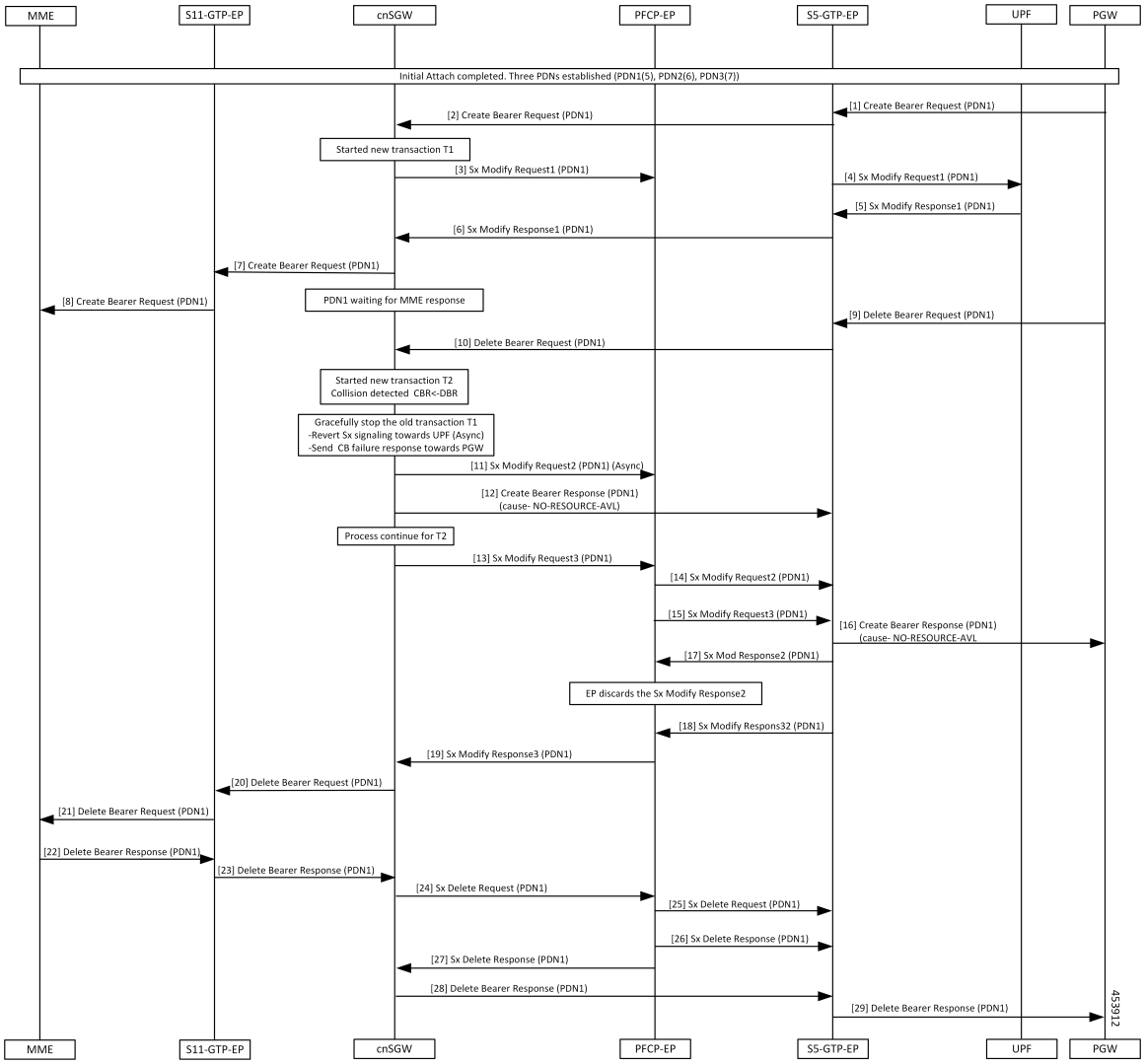


Table 121: Graceful Stop the Existing PDN Procedure Call Flow Description

Step	Description
1	The Initial Attach process is completed with the already established three PDNs. The PGW sends the Create Bearer Request to the S5-GTPC-EP.
2	The S5-GTCP-EP forwards the Create Bearer Request for PDN1 to the cnSGW.
3	The cnSGW forwards the Sx Modify Request for PDN1 to the PFCP-EP. The cnSGW waits for the Sx Modify Response for PDN1.
4	The PFCP-EP sends the Sx Modify Request for PDN1 to the UPF.
5	The UPF sends the Sx Modify Response for PDN1 to the PFCP-EP.

Step	Description
6	The PFCP-EP sends the Sx Modify Response for PDN1 to the cnSGW.
7	The cnSGW sends the Create Bearer Request for PDN1 to the S11-GTPC-EP.
8	The S11-GTPC-EP forwards the Create Bearer Request for PDN1 to the MME.
9	The PGW sends the Delete Bearer Request for PDN1 to the S5-GTPC-EP.
10	The S5-GTPC-EP forwards the Delete Bearer Request for PDN1 to the cnSGW. The cnSGW waits for the MME response and the cnSGW receives the Delete Bearer Request for PDN1. When collision is detected for PDN1, stop the old transaction T1 for PDN1.
11	The cnSGW sends the Sx Modify Request (async) to the PFCP-EP.
12	The cnSGWcnSGW sends the Create Bearer Response with cause No-Resource-Available for PDN1 to the S5-GTPC-EP.
13	The cnSGW sends the Sx Modify Request for DBR to the PFCP-EP.
14	The PFCP-EP forwards the Sx Modify Request for CBR to the UPF.
15	The PFCP-EP forwards the Sx Modify Request for DBR to the UPF.
16	The S5-GTPC-EP sends the Create Bearer Response with cause No.
17	The UPF sends the Sx Modify Response for CBR to the PFCP-EP. The PFCP-EP discards this response.
18	The UPF sends the Sx Modify Response for DBR to the PFCP-EP.
19	The PFCP-EP forwards the Sx Modify Response for DBR to the cnSGW.
20	The cnSGW sends the Delete Bearer Request for PDN1 to the S11-GTPC-EP.
21	The S11-GTPc-EP forwards the Delete Bearer Request for PDN1 to the MME.
22	The MME sends the Delete Bearer Response for PDN1 to the S11-GTPC-EP.
23	The S11-GTCP-EP forwards the Delete Bearer Response for PDN1 to the cnSGW.
24	The cnSGW sends the Sx Delete Request for PDN1 to the PFCP-EP.
25	The PFCP-EP forwards the Sx Delete Request for PDN1 to the UPF.
26	The UPF sends the Sx Delete Response for PDN1 to the PFCP-EP.
27	The PFCP-EP forwards the Sx Delete Response for PDN1 to the cnSGW.
28	The cnSGW sends the Delete Bearer Response for PDN1 to the S5-GTPC-EP.
29	The S5-GTPC-EP forwards the Delete Bearer Response for PDN1 to the PGW.

Inter MME Handover with Multi-PDN Handling (With PGW Interaction) Call Flow

This section describes the Inter MME Handover with Multi-PDN Handling (With PGW Interaction) call flow.

Figure 63: Inter MME Handover with Multi-PDN Handling (With PGW Interaction) Call Flow

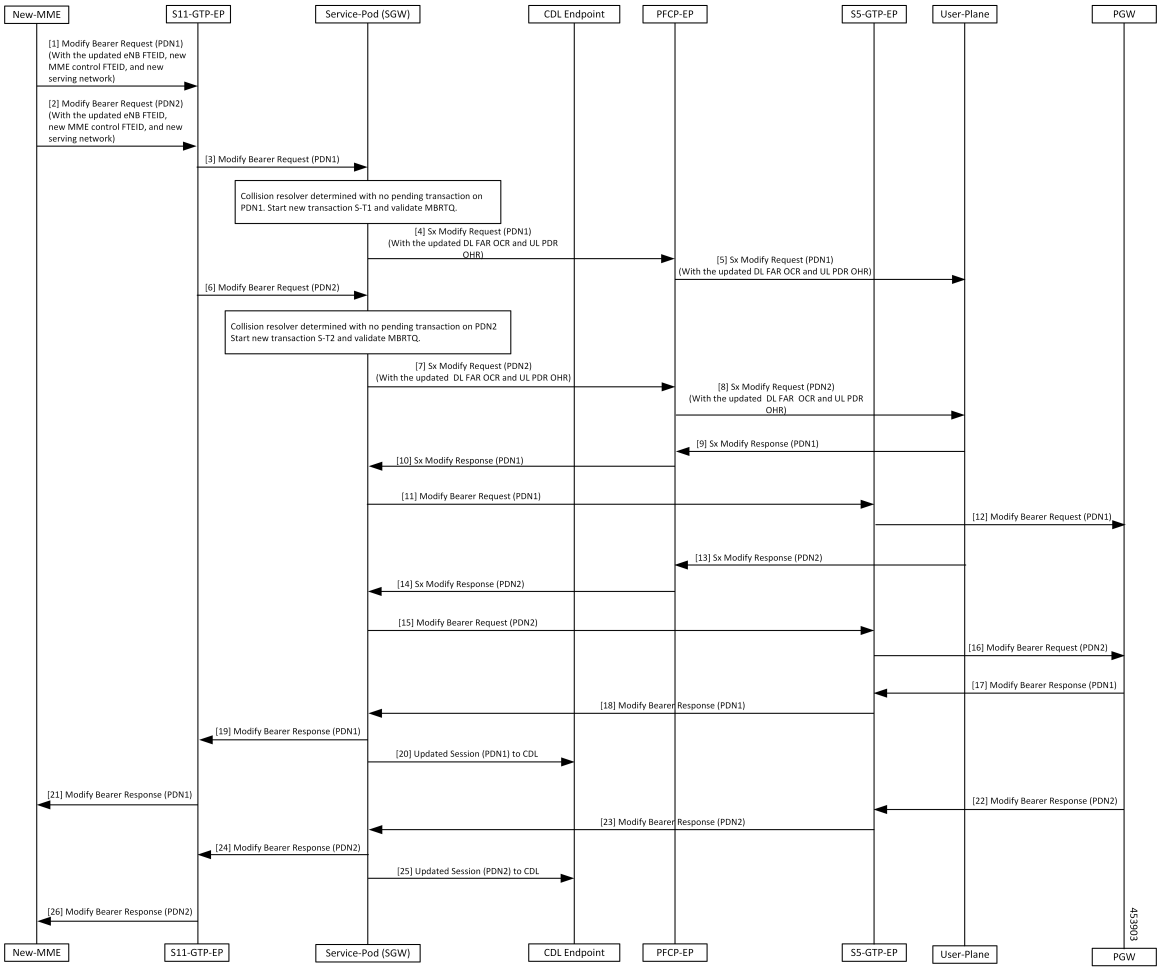


Table 122: Inter MME Handover with Multi-PDN Handling (With PGW Interaction) Call Flow Description

Step	Description
1	The New-MME sends the Modify Bearer Request for (PDN1) with the updated eNodeB FTEID, new MME control FTEID, and new serving network to the S11-GTP-EP.
2	The New-MME sends the Modify Bearer Request for (PDN2) with the updated eNodeB FTEID, new MME control FTEID, and new serving network to the S11-GTP-EP.
3	The S11-GTP-EP sends the Modify Bearer Request (PDN1) to the cnSGW-C.
4	The cnSGW-C sends the Sx Modify Request (PDN1) with the updated DL FAR OCR and UL PDR OHR to the PFCP-EP.
5	The PFCP-EP forwards the Sx Modify Request for (PDN1) to the User-Plane.

Step	Description
6	The S11-GTP-EP sends the Modify Bearer Request (PDN2).
7	The Service-Pod (SGW) sends Sx Modify Request (PDN2) with updated DL FAR OCR and UL PDR OHR to the PFCP-EP.
8	The PFCP-EP forwards the Sx Modify Request (PDN2) to User-Plane.
9	The User-Plane sends the Sx Modify Response (PDN1) to the PFCP-EP.
10	The PFPC-EP forwards the Sx Modify Response (PDN1) to the Service-Pod (SGW).
11	The Service-Pod (SGW) sends the Modify Bearer Request (PDN1) with updated serving network information to the S5-GTP-EP.
12	The S5-GTP-EP forwards the Modify Bearer Request (PDN1) to the PGW.
13	The User-Plane sends the Sx Modify Response (PDN2) to the PFCP-EP.
14	The PFCP-EP forwards the Sx Modify Response (PDN2) to the Service-Pod (SGW).
15	The Service-Pod (SGW) sends the Modify Bearer Request (PDN2) with the updated serving network information to S5-GTP-EP.
16	The S5-GTP-EP sends the Modify Bearer Request (PDN2) to the PGW.
17	The PGW sends the Modify Bearer Response (PDN1) to the S5-GTP-EP.
18	The S5-GPT-EP forwards the Modify Bearer Response (PDN1) to the Service-Pod (SGW).
19	The Service-Pod (SGW) forwards the Modify Bearer Response (PDN1) to the S11-GTP-EP.
20	The Service-Pod (SGW) updates the PDN1 session sent to the CDL Endpoint.
21	The S11-GTP-EP sends the Modify Bearer Response (PDN1) to the New-MME.
22	The PGW sends the Modify Bearer Response for (PDN2) to the S5-GTP-EP.
23	The S5-GPT-EP forwards the Modify Bearer Response (PDN2) to the Service-Pod (SGW).
24	The Service-Pod (SGW) forwards the Modify Bearer Response (PDN2) to the S11-GTP-EP.
25	The Service-Pod (SGW) marks Inter-MME as completed (PDN2) and updates PDN2 session sent to the CDL Endpoint.
26	The S11-GTP-EP sends the Modify Bearer Response (PDN2) to New-MME.

Multi PDN Call X2 Handover SGW Relocation to cnSGW-C Call Flow

This section describes the Multi PDN Call X2 Handover SGW Relocation to cnSGW-C call flow.

Figure 64: Multi PDN Call X2 Handover SGW Relocation to cnSGW-C Call Flow

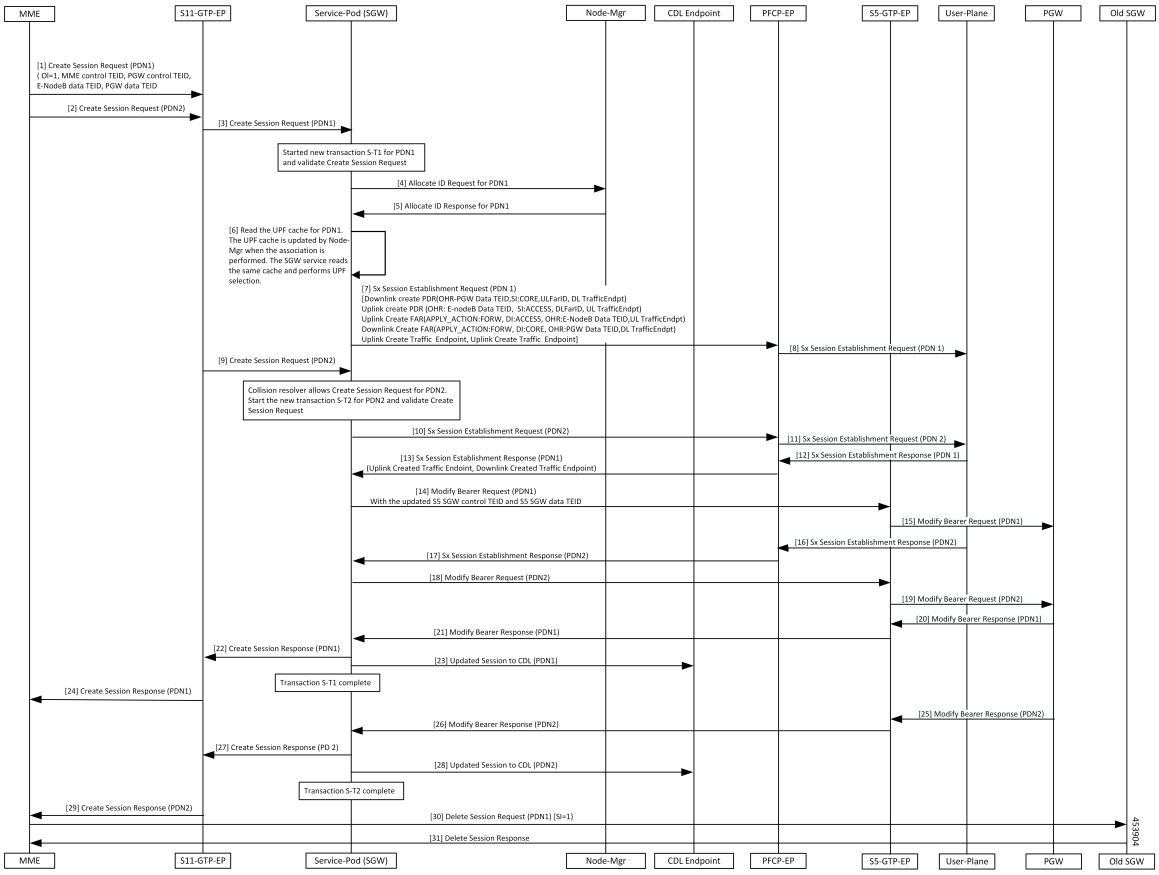


Table 123: Multi PDN call X2 Handover SGW Relocation to cnSGW-C Call Flow Description

Step	Description
1	The MME sends the Create Session Request for (PDN1) with (OI = 1, MME Control TEID, PGW Control TEID, eNodeB Data TEID, PGW Data TEID) to the S11-GTP-EP.
2	The MME sends the Create Session Request (PDN2) to the S11-GTP-EP.
3	The S11-GTP-EP forwards the Create Session Request (PDN1) to the Service-Pod (SGW).
4	The Service-Pod (SGW) requests for ID allocation (PDN1) to the Node-Mgr.
5	The Node-Mgr responds with the Allocate Id Response (PDN1).
6	The Service-Pod (SGW) performs the UPF selection.
7	The Service-Pod (SGW) sends the Sx Session Establishment Request (PDN1) to the PFCP-EP.
8	The PFCP-EP forwards the Sx Session Establishment Request (PDN1) to the User-Plane.
9	The S11-GTP-EP sends the Create Session Request (PDN2) to the Service-Pod (SGW).

Step	Description
10	The Service-Pod (SGW) sends the Sx Session Establishment Request (PDN2) to PFCP-EP.
11	The PFCP-EP forwards the Sx Session Establishment Request (PDN2) to the User-Plane.
12	The User-Plane sends the Sx Session Establishment Response (PDN1) to the PFCP-EP.
13	The PFCP-EP sends the Sx Session Establishment Response (PDN1) to the Service-Pod (SGW).
14	The Service-Pod (SGW) sends the Modify Bearer Request (PDN1) with the updated S5 SGW Control TEID and S5 SGW Data TEID to S5-GTP-EP.
15	The S5-GTP-EP forwards the Modify Bearer Request (PDN1) to the PGW.
16	The User-Plane sends the Sx Session Establishment Response (PDN2) to the PFCP-EP.
17	The PFCP-EP forwards the Sx Session Establishment Response (PDN2) to the Service-Pod (SGW).
18	The Service-Pod (SGW) sends the Modify Bearer Request (PDN2) with the updated S5 SGW Control TEID and S5 SGW Data TEID to the S5-GTP-EP.
19	The S5-GTP-EP forwards the Modify Bearer Request (PDN2) to the PGW.
20	The PGW sends the Modify Bearer Response (PDN1) to the S5-GTP-EP.
21	The S5-GTP-EP forwards the Modify Bearer Response (PDN1) to the Service-Pod (SGW).
22	The Service-Pod (SGW) sends the Create Session Response (PDN1) to the S11-GTP-EP.
23	The Service-Pod (SGW) updates the PDN1 session to the CDL Endpoint.
24	The S11-GTP-EP forwards the Create Session Response (PDN1) to the MME.
25	The PGW sends the Modify Bearer Response (PDN2) to the S5-GTP-EP.
26	The S5-GTP-EP forwards the Modify Bearer Response (PDN2) to the Service-Pod (SGW).
27	The Service-Pod (SGW) sends the Create Session Response (PDN2) to the S11-GTP-EP.
28	The Service-Pod (SGW) updates the PDN2 session to the CDL Endpoint.
29	The S11-GTP-EP forwards the Create Session Response (PDN2) to the MME.
30	The MME sends the Delete Session Request (PDN1) [SI=1] to the Old SGW.
31	The Old SGW responds with the Delete Session Response to the MME.

Multi-PDN S1 Handover SGW Relocation to Service-Pod (SGW) Call Fow

This section describes the Multi-PDN S1 Handover SGW Relocation to Service-Pod (SGW) call flow.

Figure 65: Multi-PDN S1 Handover SGW Relocation to Service-Pod (SGW) Call Flow

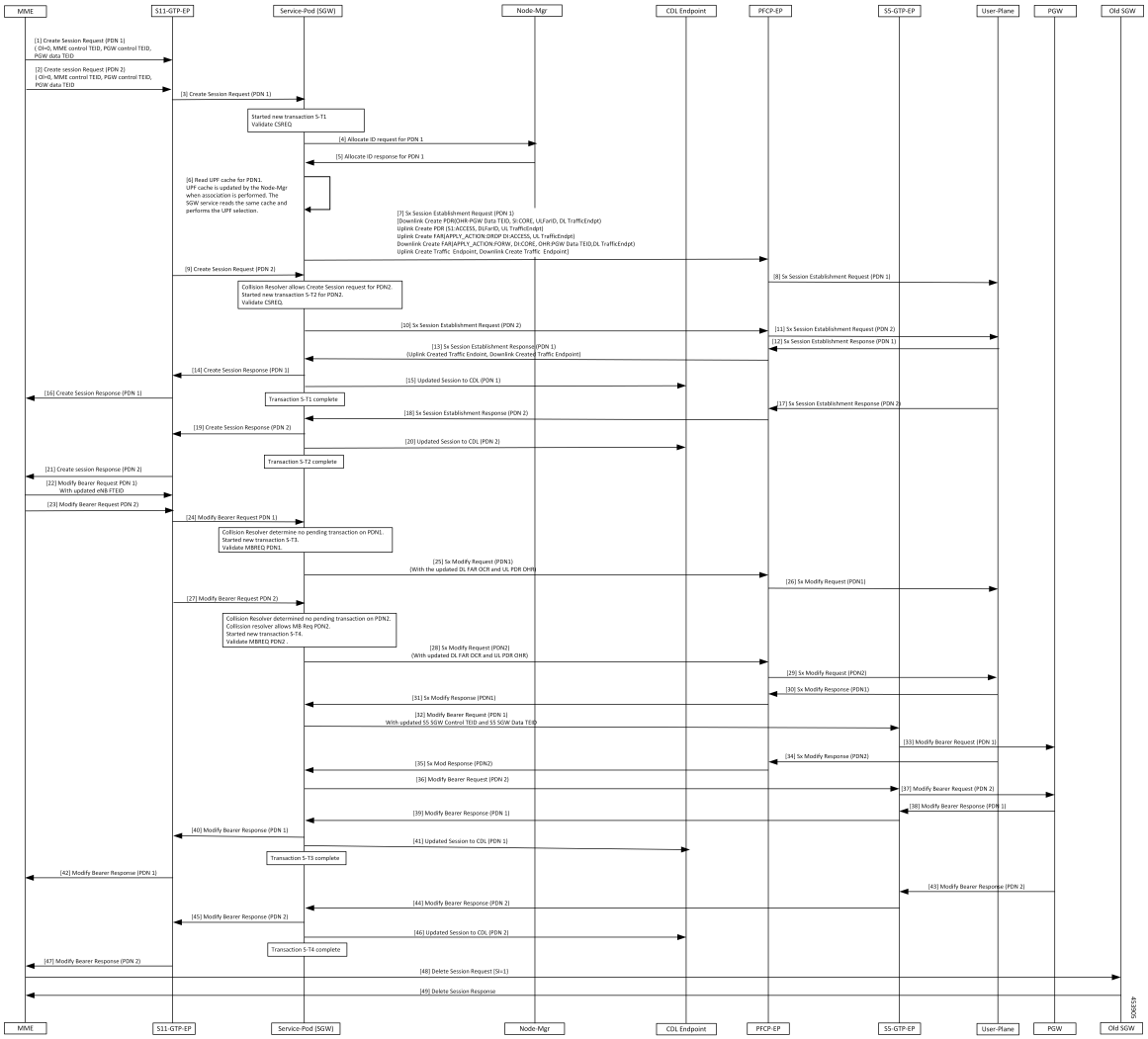


Table 124: Multi-PDN S1 Handover SGW Relocation to Service-Pod (SGW) Call Flow Description

Step	Description
1	The MME sends a Create Session Request (PDN1) with (OI = 0, MME Control TEID, PGW Control TEID, and PGW Data TEID) to the S11-GTP-EP.
2	The MME sends the Create Session Request (PDN2) with (OI = 0, MME Control TEID, PGW Control TEID, and PGW Data TEID) to the S11-GTP-EP.
3	The S11-GTP-EP sends the Create Session Request (PDN1) to the Service-Pod (SGW).
4	The Service-Pod (SGW) requests ID allocation (PDN1) to the Node-Mgr.
5	The Node-Mgr responds with the Allocate ID Response (PDN1) to the Service-Pod (SGW).
6	The Service-Pod (SGW) performs the UPF selection.

Step	Description
7	The Service-Pod (SGW) triggers the Sx Session Establishment Request (PDN1) to the PFCP-EP.
8	The PFCP-EP forwards a Sx Session Establishment Request (PDN1) to the User-Plane.
9	The Service-Pod (SGW) receives the Create Session Request (PDN2) from the S11-GTP-EP.
10	The Service-Pod (SGW) sends a Sx Session Establishment Request (PDN2) to the PFCP-EP.
11	The PFCP-EP forwards the Sx Session Establishment Request (PDN2) to the User-Plane.
12	The User-Plane responds with the Sx Session Establishment Response (PDN1) to the PFCP-EP.
13	The PFCP-EP forwards the Sx Session Establishment Response (PDN1) to the Service-Pod (SGW).
14	The Service-Pod (SGW) sends the Create Session Response (PDN1) to the S11-GTP-EP.
15	The Service-Pod (SGW) updates the PDN1 session to the CDL Endpoint.
16	The S11-GTP-EP forwards the Create Session Response (PDN1) to the MME.
17	The User-Plane responds with the Sx Session Establishment Response (PDN2) to the PFCP-EP.
18	The PFCP-EP forwards the Sx Session Establishment Response (PDN2) to the Service-Pod (SGW).
19	The Service-Pod (SGW) sends the Create Session Response (PDN2) to the S11-GTP-EP.
20	The Service-Pod (SGW) updates the PDN2 session to the CDL Endpoint.
21	The S11-GTP-EP forwards the Create Session Response (PDN2) to the MME.
22	The MME sends a Modify Bearer Request (PDN1) to the S11-GTP-EP.
23	The MME sends the Modify Bearer Request (PDN2) to the S11-GTP-EP.
24	The S11-GTP-EP forwards the Modify Bearer Request (PDN1) to the Service-Pod (SGW).
25	The Service-Pod (SGW) sends a Sx Modify Request (PDN1) to the PFCP-EP.
26	The PFCP-EP forwards the Sx Modify Request (PDN1) to the User-Plane.
27	The S11-GTP-EP sends the Modify Bearer Request (PDN2) to the Service-Pod (SGW).
28	The Service-Pod (SGW) sends a Sx Modify Request (PDN2) with the updated DL FAR OCR and UL PDR OHR to the PFCP-EP.
29	The PFCP-EP forwards the Sx Modify Request (PDN2) to the User-Plane.
30	The User-Plane responds with the Sx Modify Response (PDN1) to the PFCP-EP.
31	The PFCP-EP forwards the Sx Modify Response (PDN1) to the Service-Pod (SGW).
32	The Service-Pod (SGW) sends the Modify Bearer Request (PDN1) with the updated S5 SGW Control TEID and S5 SGW Data TEID to the S5-GTP-EP.
33	The S5-GTP-EP forwards the Modify Bearer Request (PDN1) to the PGW.

Step	Description
34	The User-Plane sends the Sx Modify Response (PDN2) to the PFCP-EP.
35	The PFCP-EP forwards the Sx Modify Response (PDN2) to the Service-Pod (SGW).
36	The Service-Pod (SGW) sends the Modify Bearer Request (PDN2) to the S5-GTP-EP.
37	The S5-GTP-EP forwards the Modify Bearer Request (PDN2) to the PGW.
38	The PGW responds with the Modify Bearer Response (PDN1) to the S5-GTP-EP.
39	The S5-GTP-EP forwards the Modify Bearer Response (PDN1) to the Service-Pod (SGW).
40	The Service-Pod (SGW) sends the Modify Bearer Response (PDN1) to the S11-GTP-EP.
41	The Service-Pod (SGW) updates the PDN1 session to the CDL Endpoint.
42	The S11-GTP-EP forwards the Modify Bearer Response (PDN1) to the MME.
43	The PGW responds with the Modify Bearer Response (PDN2) to the S11-GTP-EP.
44	The S5-GTP-EP forwards the Modify Bearer Response (PDN2) to the Service-Pod (SGW).
45	The Service-Pod (SGW) sends the Modify Bearer Response (PDN2) to the S11-GTP-EP.
46	The Service-Pod (SGW) updates the PDN2 session to the CDL Endpoint.
47	The S11-GTP-EP forwards the Modify Bearer Response (PDN2) to the MME.
48	The MME triggers the Delete Session Request [SI=1] to Old SGW.
49	The Old SGW deletes the session and responds with the Delete Session Response.

Multiple CBR for Same PDN Call Flow

This section describes the Multiple CBR for Same PDN call flow.

Figure 66: Multiple CBR for Same PDN Call Flow

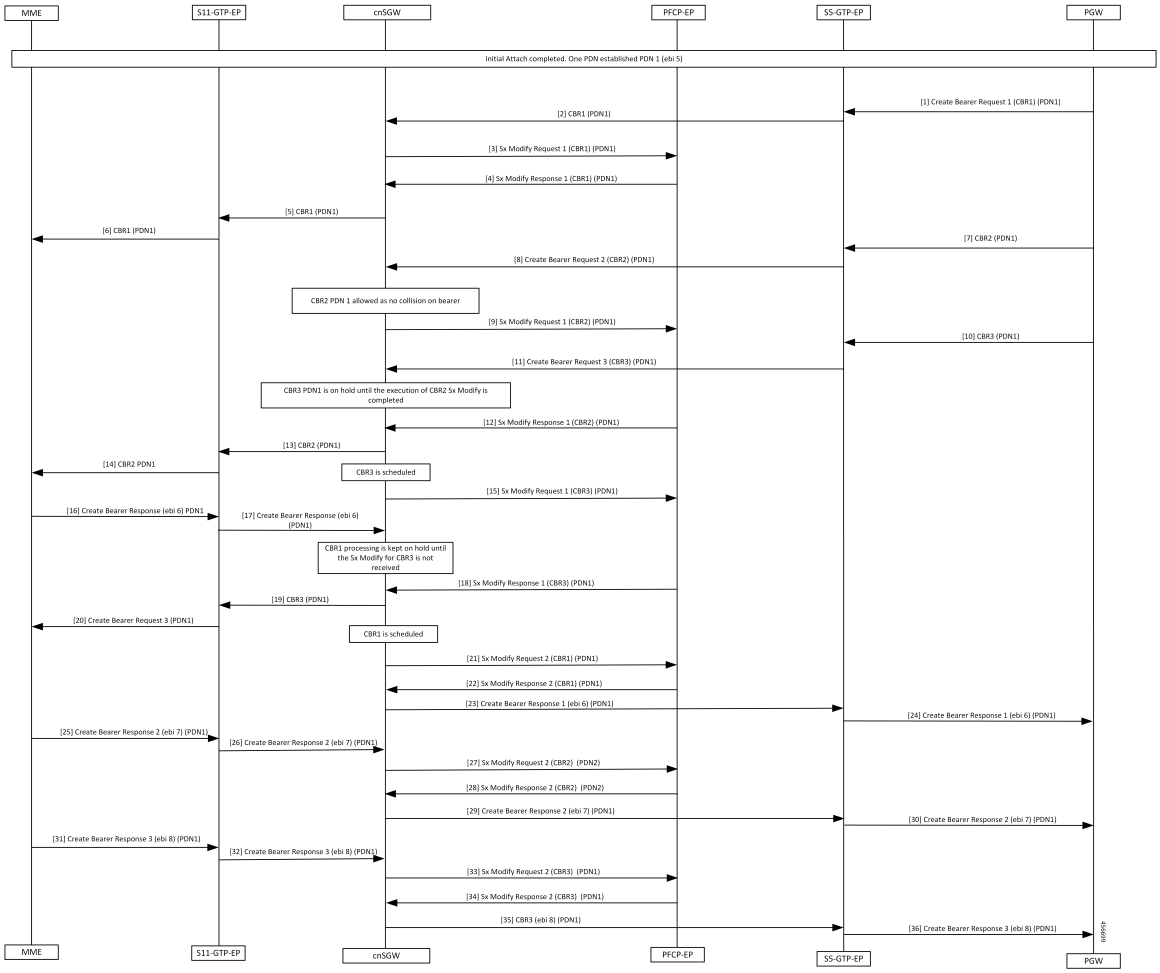


Table 125: Multiple CBR for Same PDN Call Flow Description

Step	Description
1	Initial Attach completed. One PDN has established PDN1 (ebi 5). The PGW sends the Create Bearer Request 1 for PDN1 to the S5-GTP-EP.
2	The S5-GTP-EP forwards the Create Bearer Request 1 for PDN1 to the cnSGW.
3	The cnSGW sends the Sx Modify Request 1 for PDN1 to the PFCP-EP.
4	The cnSGW receives the Sx Modify Response 1 for PDN1 from the PFCP-EP.
5	The cnSGW sends the Create Bearer Request 1 for PDN1 to the S11-GTP-EP.
6	The S11-GTP-EP sends the Create Bearer Request 1 for PDN1 to the MME.
7	The PGW sends the Create Bearer Request 2 to the S5-GTP-EP.

Step	Description
8	The S5-GTP-EP sends the Create Bearer Request 2 to the cnSGW.
9	The cnSGW sends the Sx Modify Request 1 (Create Bearer Request 2) for PDN1 to the PFCP-EP.
10	The PGW sends the Create Bearer Request 3 for PDN1 to the S5-GTP-EP.
11	The S5-GTP-EP sends the Create Bearer Request 3 for PDN1 to the cnSGW
12	The PFCP-EP sends the Sx Modify Response 1 (CBR2) for PDN1 to the cnSGW.
13	The cnSGW sends the Create Bearer Request 2 for PDN1 to the S11-GTP-EP.
14	The S11-GTP-EP sends the Create Bearer Request 2 for PDN1 to the MME.
15	The cnSGW sends the Sx Modify Request 1(CBR3) for PDN1 to the PFPC-EP.
16	The MME sends the Create Bearer Response 1 (ebi6) for PDN1 to the S11-GTP-EP.
17	The S11-GTP-EP sends the Create Bearer Response 1 (ebi6) for PDN1 to the cnSGW.
18	The cnSGW receives the Sx Modify Response 1 (CBR3) for PDN1 to the PFPC-EP.
19, 20	The cnSGW sends the Create Bearer Request 3 to the S11-GTP-EP.
20	The S11-GTP-EP sends the Create Bearer Request 3 to the MME.
21	The cnSGW sends the Sx Modify Request 2(CBR1) for PDN1 to the PFPC-EP.
22	The cnSGW receives the Sx Modify Response 2 (CBR1) for PDN1 to the PFPC-EP.
23	The cnSGW sends the Create Bearer Response 1 (ebi 6) for PDN1 to the S5-GTP-EP.
24	The S5-GTP-EP sends the Create Bearer Response 1 (ebi 6) for PDN1 to the PGW.
25	The MME sends the Create Bearer Response 2 (ebi 7) for PDN1 sent from MME to cnSGW.
26	The S11-GTP-EP sends the Create Bearer Response 2 (ebi 7) for PDN1 sent from MME to the cnSGW.
27	The cnSGW sends the Sx Modify Request 2 (CBR2) for PDN1 to PFCP-EP.
28	The PFCP-EP sends the Sx Modify Response 2 (CBR2) for PDN1 to the cnSGW.
29	The cnSGW sends the Create Bearer Response 2 (ebi 7) for PDN1 to the S5-GTP-EP.
30	The S5-GTP-EP sends the Create Bearer Response 2 (ebi 7) for PDN1 to the PGW.
31	The MME sends the Create Bearer Response 3 (ebi 8) for PDN1 to the S11-GTP-EP.
32	The S11-GTP-EP sends the Create Bearer Response 3 (ebi 8) for PDN1 to the cnSGW.
33	The cnSGW sends the Sx Modify Request 2 (CBR3) for PDN1 to the PFPC-EP.
34	The PFCP-EP send the Sx Modify Response 2 (CBR3) for PDN1 to the cnSGW.

Step	Description
35	The cnSGW sends the Create Bearer Response 3 (ebi 8) for PDN1 to the S5-GTP-EP.
36	The S5-GTP-EP sends the Create Bearer Response 3 (ebi 8) for PDN1 to the PGW.

Collision Resolver Discard Handling Call Flow

This section describes the Collision Resolver Discard Handling call flow.

Figure 67: Collision Resolver Discard Handling Call Flow

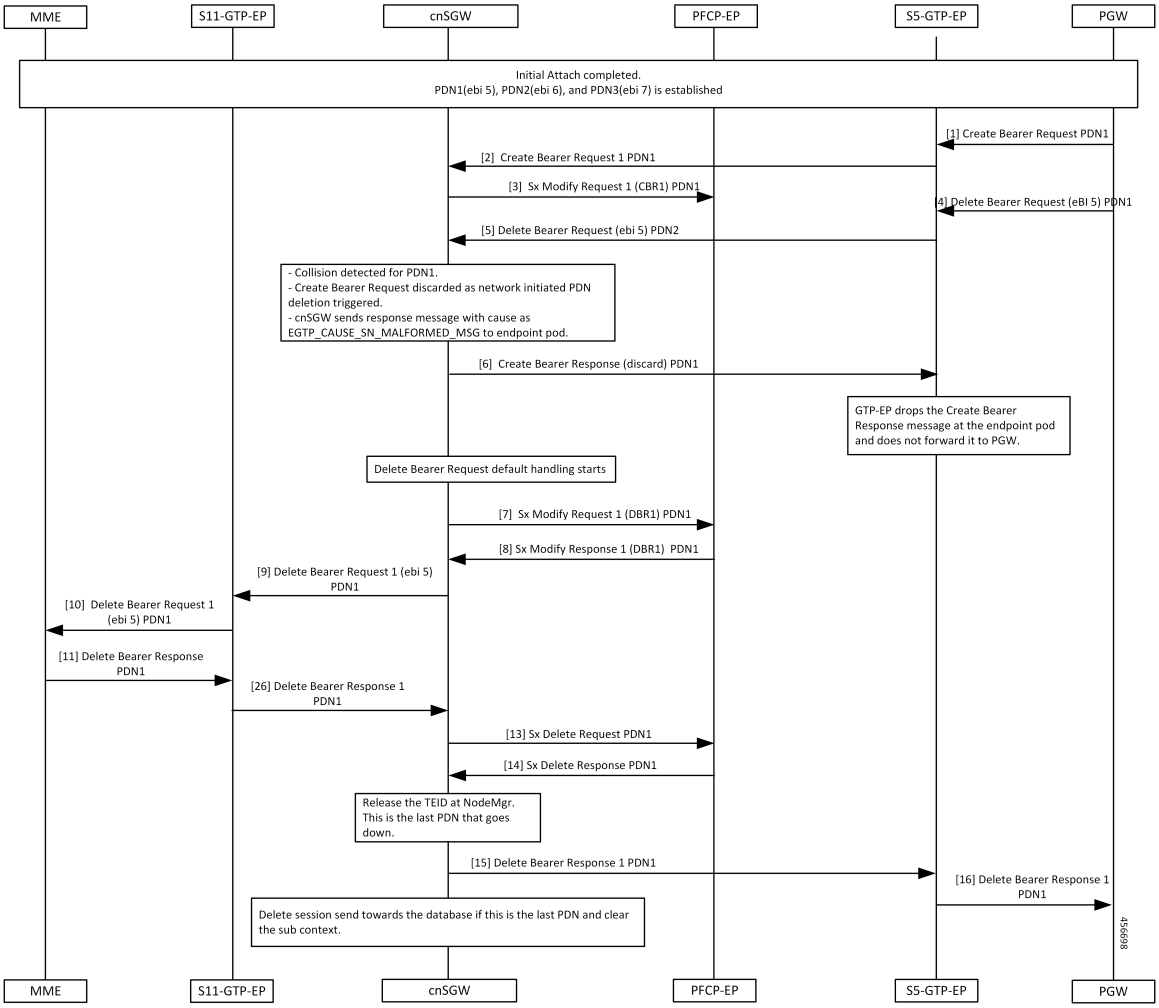


Table 126: Collision Resolver Discard Handling Call Flow Description

Step	Description
1	Initial Attach procedure is completed. The PDN1(ebi 5), PDN2(ebi 6), and PDN3(ebi 7) is established. The PGW sends the Create Bearer Request for PDN1 to the S5-GTP-EP.

Step	Description
2	The PFCP-EP sends the Create Bearer Request 1 for PDN1 to the cnSGW.
3	The cnSGW sends the Sx Modify Request 1 for PDN1 to the PFCP-EP.
4, 5	The PGW sends the Delete Bearer Request (ebi5) for PDN1 to the cnSGW.
6	Collision detected for PDN1. The Create Bearer Request is discarded as network initiated PDN deletion request is triggered. The cnSGW sends a response message with the cause as EGTP_CAUSE_SN_MALFORMED_MSG to the endpoint pod. The cnSGW sends Create Bearer Response (discard 1) for PDN1 to the S5-GTP-EP.
7	The cnSGW sends the Sx Modify Request 1 (DBR1) for PDN1 to the PFPC-EP.
8	The cnSGW receives the Sx Modify Response 1 (DBR1) for PDN1 from the PFPC-EP.
9	The cnSGW sends the Delete Bearer Request 1 to the S11-GTP-EP.
10	The S11-GTP-EP sends the Delete Bearer Request 1 to the MME.
11	The MME sends the Delete Bearer Response 1 to the S11-GTP-EP.
12	The S11-GTP-EP sends the Delete Bearer Response 1 to the cnSGW.
13	The cnSGW sends the Sx Delete Request for PDN1 to the PFCP-EP.
14	The PFPC-EP sends the Sx Delete Response for PDN1 to the cnSGW.
15	The cnSGW sends the Delete Bearer Response 1 for PDN1 to the PGW.
16	The S5-GTP-EP sends the Delete Bearer Response for PDN1 to the PGW.

Suspend Handling Call Flow

This section describes the Suspend Handling call flow.

Figure 68: Suspend Handling Call Flow

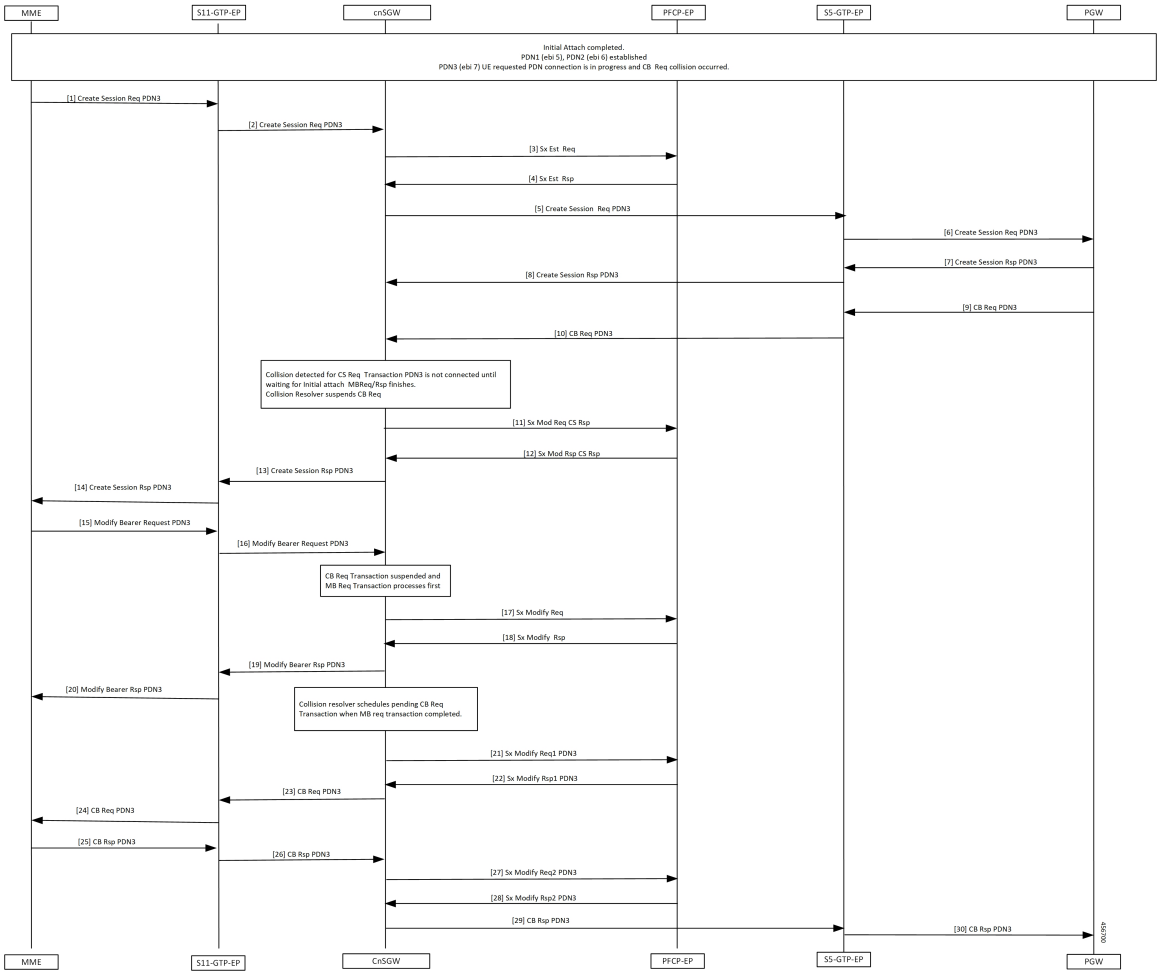


Table 127: Suspend Handling Call Flow Description

Step	Description
1	Initial Attach process is completed. The PDN1 (ebi 5) and PDN2 (ebi 6) is established. PDN3 (ebi 7) UE requested that PDN connection is in progress. The Create Bearer Request collision occurred. The MME sends Create Session Req for PDN3 to S11-GTP-EP.
2	The S11-GTP-EP sends the Create Session Request for PDN3 to the cnSGW.
3	The cnSGW sends the Sx Establishment Request to the PFCP-EP.
4	The PFCP-EP sends the Sx Establishment Response to the cnSGW.
5	The cnSGW sends the Create Session Request for PDN3 to the PGW.

Step	Description
6	The S5-GTP-EP sends the Create Session Request for PDN3 to the PGW.
7	The PGW sends the Create Session Rsppnse for PDN3 to the S5-GTP-EP.
8	The S5-GTP-EP sends the Create Session Response for PDN3 to the cnSGW.
9	The PGW sends the Create Bearer Request for PDN3 to the S5-GTP-EP.
10	The S5-GTP-EP sends the Create Bearer Request for PDN3 to the cnSGW.
11	Collision that is detected for Create Session Request transaction for PDN3 gets connected when waiting for the initial attach Modify Bearer Request or Response is complete. Collision Resolver suspends Create Bearer Request. The cnSGW sends Sx Modify Request and Create Session Request to the PFCP-EP.
12	The PFCP-EP sends the Sx Modify Response and Create Session Response to cnSGW.
13	The cnSGW sends the Create Session Response for PDN3 sent to the S11-GTP-EP.
14	The S11-GTP-EP sends the Create Session Response for PDN3 sent to the MME.
15	The MME sends the Modify Bearer Request for PDN3 to the S11-GTP-EP.
16	The S11-GTP-EP sends the Modify Bearer Request for PDN3 to the cnSGW.
17	The cnSGW sends the Modify Bearer Request for PDN3 to the PFCP-EP.
18	The PFCP-EP sends the Sx Modify Response to the cnSGW.
19	The cnSGW sends the Modify Bearer Response for PDN3 to the S11-GTP-EP.
20	The S11-GTP-EP sends the Modify Bearer Response for PDN3 to the MME.
21	The cnSGW sends Sx Modify Request 1 for PDN3 to the PFCP-EP.
22	The PFPC-EP sends the Sx Modify Response 1 for PDN3 to the PFPC-EP.
23	The cnSGW sends the Create Bearer Request for PDN3 sent to the S11-GTP-EP.
24	The S11-GTP-EP sends the Create Bearer Request for PDN3 sent to the MME.
25	The MME sends the Create Bearer Response for PDN3 to the S11-GTP-EP.
26	The S11-GTP-EP sends the Create Bearer Response for PDN3 to the cnSGW.
27	The cnSGW sends Sx Modify Request 2 for PDN3 to the PFCP-EP.
28	The PFCP-EP sends the Sx Modify Response 2 for PDN3 to the cnSGW.
29	The cnSGW sends the Create Bearer Response for PDN3 to the PGW.
30	The S5-GTP-EP sends the Create Bearer Response for PDN3 to the PGW.

Abort Handling of Low-Priority Procedure Call Flow

This section describes the Abort Handling of Low-Priority Procedure call flow.

Figure 69: Abort Handling of Low-Priority Procedure Call Flow

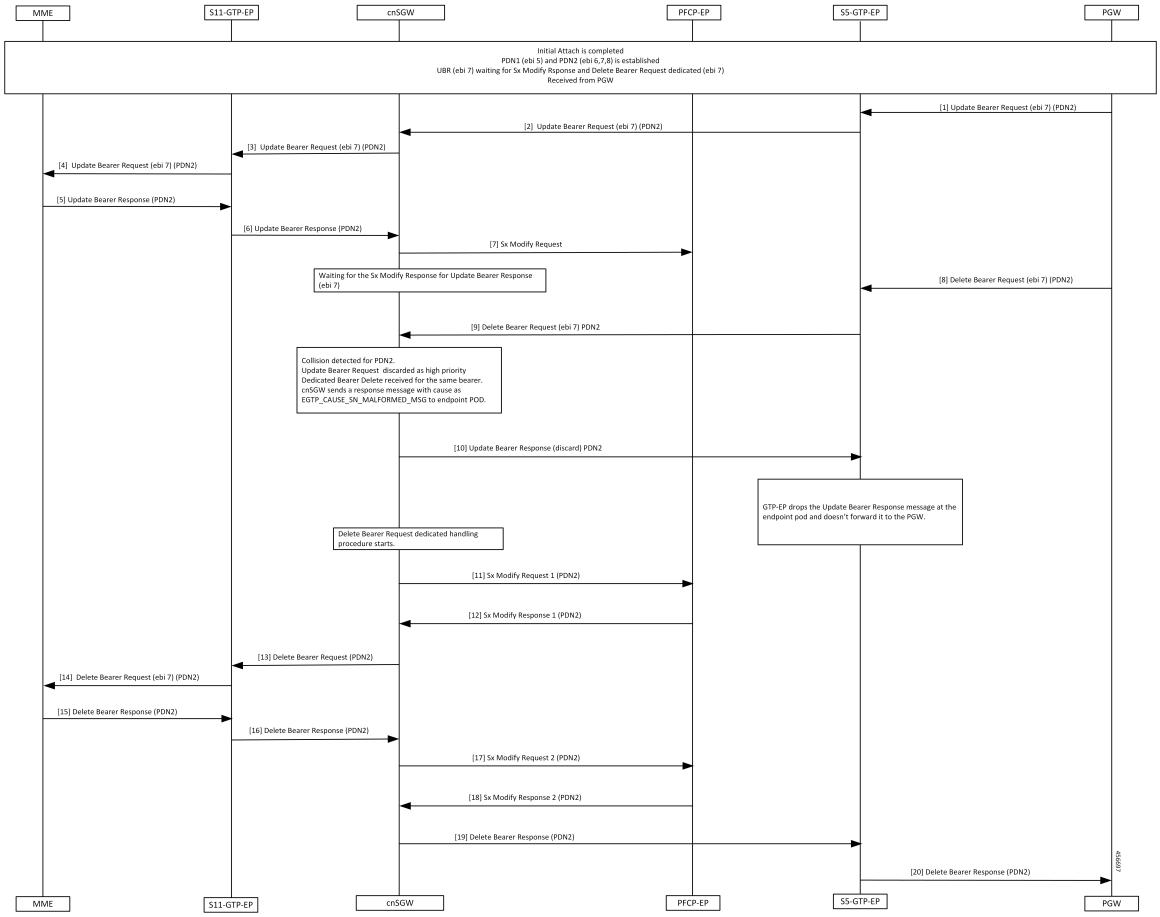


Table 128: Abort Handling of Low-Priority Procedure Call Flow Description

Step	Description
1	Initial Attach procedure is completed. The PDN1(ebi 5) and PDN2(ebi 6,7,8) is established. The Update Bearer Request (ebi 7) is waiting for the Sx Modify Response and Dedicated Bearer Request dedicated (ebi 7) received from the PGW. The PGW sends an Update Bearer Request (eBi 7) PDN2 to the S5-GTP-EP.
2	The PFCP-EP sends the Update Bearer Request (eBi 7) PDN2 to the cnSGW.
3	The cnSGW sends the Update Bearer Request (eBi 7) PDN2 to the S11-GTP-EP.
4	The S5-GTP-EP forwards the Update Bearer Request (eBi 7) PDN2 to the MME.

Step	Description
5	The MME sends an Update Bearer Response to the S11-GTP-EP.
6	The S11-GTP-EP sends a Update Bearer Response to the cnSGW.
7	The cnSGW sends Sx Modify Request to the PFCP-EP.
8	The PGW sends the Delete Bearer Request (eBi 7) for PDN2 to the S5-GTP-EP.
9	The S5-GTP-EP forwards Delete Bearer Request (eBi 7) for PDN2 to the cnSGW.
10	Collision is detected for PDN2. The Update Bearer Request is discarded as high priority-dedicated bearer delete received for the same bearer. The cnSGW sends a response message with cause as EGTP_CAUSE_SN_MALFORMED_MSG to endpoint POD. The cnSGW sends Update Bearer Response (Discard) for PDN2 to the S5-GTP-EP.
11	The GTP-EP drops the Update Bearer Response message at endpoint pod and not forwarded to the PGW. The cnSGW sends the Sx Modify Request 1 for PDN2 to the PFCP-EP.
12	The PFCP-EP sends the Sx Modify Response 1 for PDN2 to the cnSGW.
13	The cnSGW sends the Delete Bearer Request for PDN2 to the S11-GTP-EP.
14	The S11-GTP-EP sends the Delete Bearer Request (ebi 7) for PDN2 to the MME.
15	The MME sends the Delete Bearer Response for PDN2 to the S11-GTP-EP.
16	The S11-GTP-EP sends the Delete Bearer Response for PDN2 to the cnSGW.
17	The cnSGW sends the Sx Modify Request for PDN2 to the PFCP-EP.
18	The PFCP-EP sends Sx Modify Response for PDN2 to the cnSGW.
19	The cnSGW sends the Delete Bearer Response for PDN2 to the S5-GTP-EP.
20	The S5-GTP-EP sends the Delete Bearer Response for PDN2 to the PGW.

Double Delete Optimization Call Flow

This section describes the Double Delete Optimization call flow.

Figure 70: Double Delete Optimization Call Flow

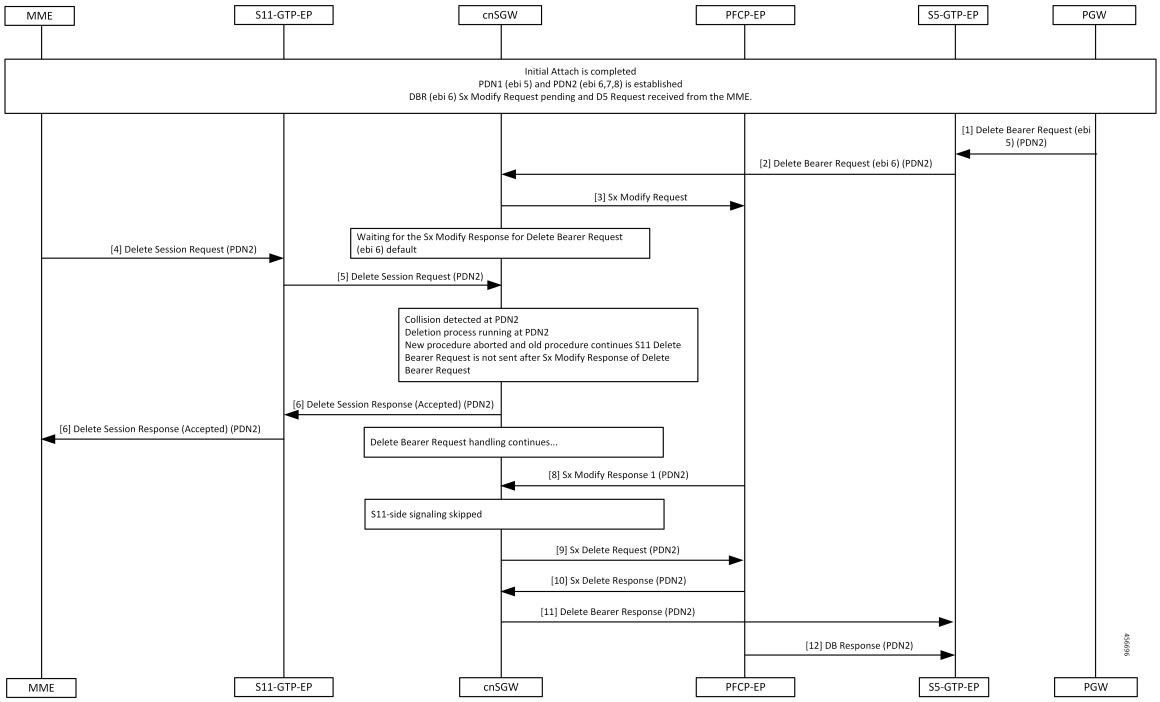
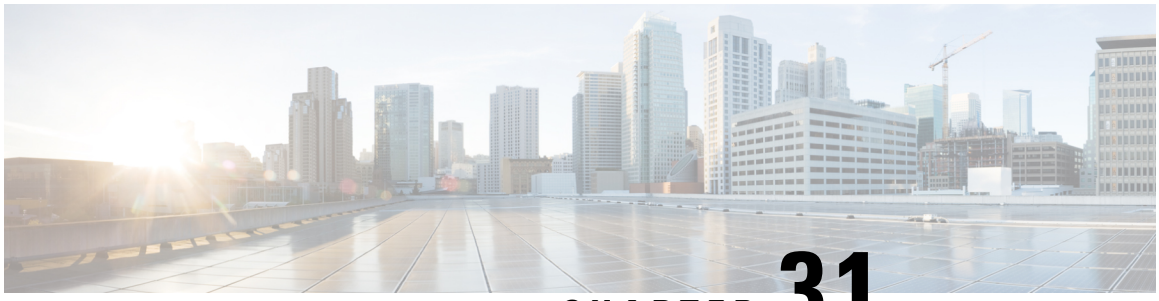


Table 129: Double Delete Optimization Call Flow Description

Step	Description
1	Initial Attach procedure is completed. The PDN1(ebi 5) and PDN2(ebi 6,7,8) is established. The Delete Bearer Request (ebi 6) and Sx Modify Request is pending and the Delete Session Request is received from the MME. The PGW sends the Delete Bearer Request (ebi 6) for PDN2 to the S5-GTP-EP.
2	The S5-GTP-EP forwards the Delete Bearer Request (ebi 6) for PDN2 to the cnSGW.
3	The cnSGW sends the Sx Modify Request to the PFCP-EP.
4	Waits for the Sx Modify Response for the Delete Bearer Request (ebi 6) default. The MME sends the Delete Session Request for PDN2 to the S11-GTP-EP.
5	The S11-GTP-EP forwards the Delete Session Request for PDN2 to the cnSGW.

Step	Description
6	Collision detected at PDN2. Deletion process running at PDN2. New procedure aborted and old procedure continue. The S11 Delete Bearer Request isn't send after an Sx Modify Response of the Delete Bearer Request. The cnSGW sends Delete Session Response (Accepted) for PDN2 to the S11-GTP-EP.
7	The S11-GTP-EP forwards the Delete Session Response (Accepted) for PDN2 to the MME.
8	While the Delete Bearer Request handling continues, the PFCP-EP sends Sx Modify Response 1 for PDN2 to the cnSGW.
9	The cnSGW sends the Sx Delete Request for PDN2 to the PFCP-EP.
10	The PFCP-EP sends the Sx Delete Response for PDN2 to the cnSGW.
11	The cnSGW sends Delete Bearer Response for PDN2 to the S5-GTP-EP.
12	The S5-GTP-EP forwards the Delete Bearer Response for PDN2 to the PGW.



CHAPTER 31

Modify and Delete Bearer Command Support

Feature Summary and Revision History

Summary Data

Table 130: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Documentation	Not Applicable

Revision History

Table 131: Revision History

Revision Details	Release
First introduced.	2021.01.0

Feature Description

cnSGW-C supports Modify Bearer Command (MBC) and Delete Bearer Command (DBC).

This feature is supported on the following pods—SGW-service, GTP-EP, and UDP-Proxy.

The SGW-service pod is responsible for handling the following:

- The MBC and DBC
- The MBC triggered Update Bearer Request
- The DBC triggered Delete Bearer Response

The GTPC-EP pod is responsible for sending the following:

- Modify Bearer Command Failure Indication (MBCFI) and Delete Bearer Command Failure Indication (DBCFI) if no response is received.
- MBCFI and DBCFI (success) on receiving Update Bearer Request and Delete Bearer Request respectively.
- Update Bearer Response and Delete Bearer Response back to PGW on receiving the respective message from the SGW-service pod.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

MBC Failure Handling Call Flow

This section describes the MBC Failure Handling call flow.

Figure 71: MBC Failure Handling Call Flow

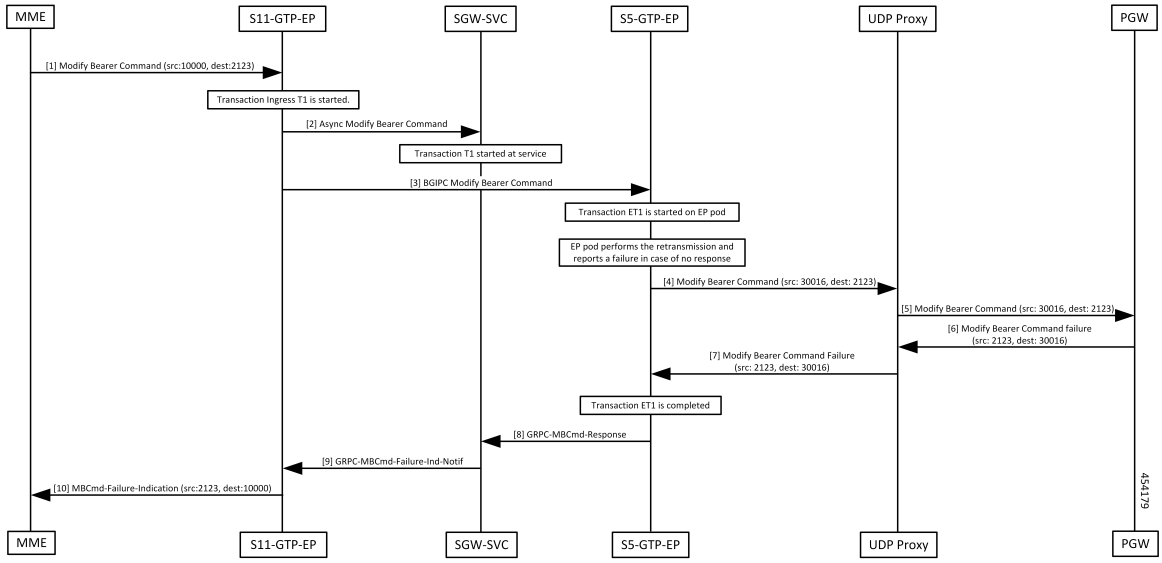


Table 132: MBC Failure Handling Call Flow Description

Step	Description
1	The MME sends the Modify Bearer Command to the S11 GTPC-EP pod.
2	The GTPC-EP pod sends the ASYNC Modify Bearer Command to the SGW-SVC pod.
3	The SGW-SVC pod forwards Modify Bearer Command to PGW. Save MBC_info in PDN for the response.
4	The GTPC-EP pod performs retransmission. If there is no response, the pod sends Modify Bearer Command Failure Indication (MBCFI) to SGW-SVC pod.
5	The UDP Proxy sends the Modify Bearer Command request to PGW.
6	The MBCFI is received on the S5 GTPC-EP pod and is forwarded to SGW-SVC pod.
7	The UDP Proxy sends the Modify Bearer Command failure details to the S5-GTP-EP.
8	The S5-GTP-EP sends the GRPC Modify Bearer Command Response to the SGW-SVC.
9	The SGW-SVC sends the GRPC Modify Bearer Command failure notification to the S11-GTP-EP.
10	The SGW-SVC pod processes MBCFI and forwards the response to MME with saved MBC_Info.

MBC Success Handling Call Flow

This section describes the MBC Success Handling call flow.

Figure 72: MBC Success Handling Call Flow

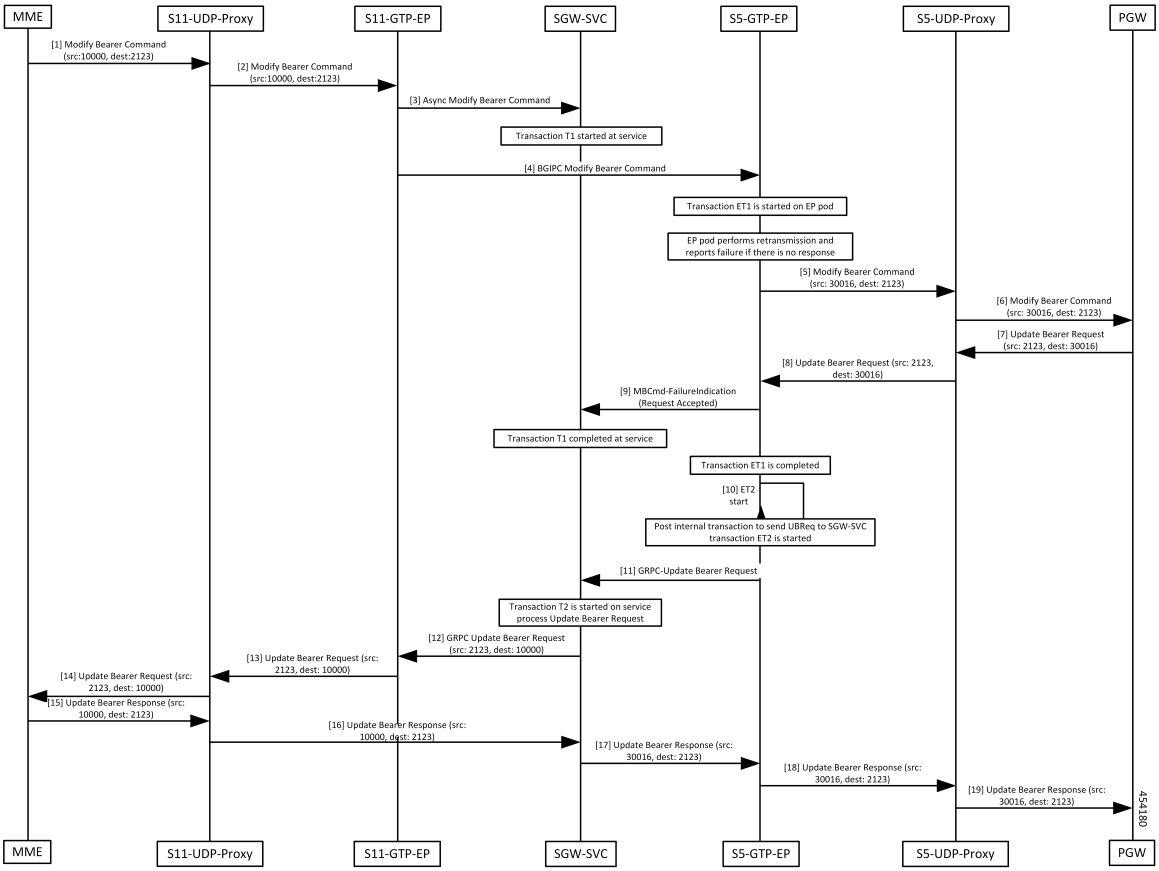


Table 133: MBC Success Handling Call Flow Description

Step	Description
1	The MME sends the Modify Bearer Command to the S11-UDP-Proxy.
2	The S11-UDP-Proxy forwards the Modify Bearer Command to the S11-GTP-EP pod.
3	The S11-GTP-EP pod sends the ASYNC Modify Bearer Command to the SGW-SVC pod. The SGW-SVC pod forwards the Modify Bearer Command to the PGW. Save MBC_info in PDN for response.
4	The S11-GTP-EP pod performs the retransmission. If there is no response, the pod sends the Modify Bearer Command Failure Indication (MBCFI) to the S5-GTP-EP pod.
5	The S5-GTP-EP sends the Modify Bearer Command to the S5-UDP-Proxy.
6	The S5-UDP-Proxy forwards the Modify Bearer Command to the PGW.
7	The PGW sends the Update Bearer Request to the S5-UDP-Proxy.
8	The S5-UDP-Proxy sends the Update Bearer Request (src: 2123, dest: 30016) to the S5-GTP-EP.

Step	Description
9	The S5-GTP-EP pod sends MBCmd-FailureIndication to SGW-SVC pod to end the transaction. Post internal transaction, the GRPC Update Bearer Request is sent to the SGW-SVC pod.
10	The S5-GTP-EP starts the ET2.
11	The S5-GTP-EP sends the GRPC Update Bearer Request to SGW-SVC pod.
12	The SGW-SVC pod processes the Update Bearer Request and consumes the saved MBC_Info to send Update Bearer Request to the S11-GTP-EP.
13	The S11-GTP-EP sends the Update Bearer Request to the S11-UDP-Proxy.
14	The S11-UDP-Proxy forwards the Update Bearer Request to the MME.
15	The MME sends Update Bearer Response to the SGW-SVC pod.
16	The S11-UDP-Proxy processes and sends the Update Bearer Response to the SGW-SVC pod.
17	The SGW-SVC pods forward the Update Bearer Response to the S5-GTP-EP pod.
18	The S5-GTP-EP pod sends the Update Bearer Response to the S5-UDP-Proxy.
19	The S5-UDP-Proxy sends the Update Bearer Response to the PGW.

DBC Failure Handling Call Flow

This section describes the DBC Failure Handling call flow.

Figure 73: DBC Failure Handling Call Flow

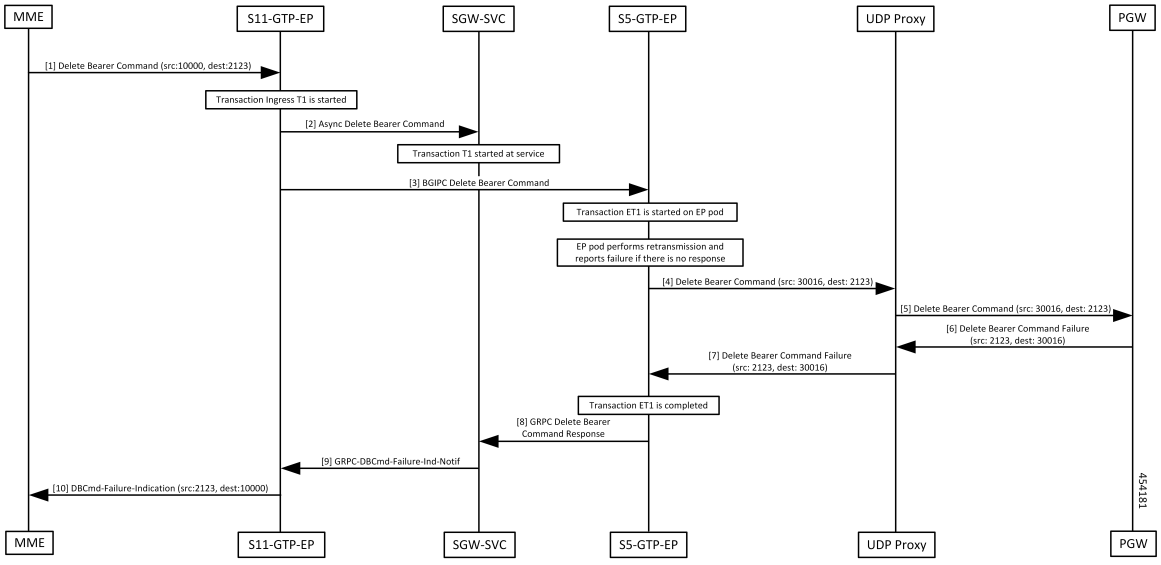


Table 134: DBC Failure Handling Call Flow Description

Step	Description
1	The MME sends the Delete Bearer Command to the S11-GTP-EP pod.
2	The S11-GTP-EP pod sends the ASYNC Delete Bearer Command to the SGW-SVC pod.
3	The SGW-SVC pod forwards Delete Bearer Command to the PGW. Save DBC_info in PDN for response. The EP pod performs retransmission. If there is no response, the pod sends the Delete Bearer Command Failure Indication (DBCFI) to the SGW-SVC pod.
4	The S5-GTP-EP sends the Delete Bearer Command to the UDP Proxy.
5	The UDP Proxy forwards the Delete Bearer Command to the PGW.
6	The PGW sends the Delete Bearer Command Failure to the UDP Proxy. DBCFI is received on S5 GTPC-EP pod and is forwarded to the SGW-SVC pod.
7	The UDP Proxy forwards the Delete Bearer Command Failure to the S5-GTP-EP.
8	The S5-GTP-EP sends the GRPC Delete Bearer Command Response to the SGW-SVC.
9	The SGW-SVC pod sends the GRPC-DBCmd-Failure-Ind-Notif to the S11-GTP-EP.
10	The S11-GTP-EP pod processes the DBCFI and forwards the response to MME with the saved DBC_Info.

DBC Success Handling Call Flow

This section describes the DBC Success Handling call flow.

Figure 74: DBC Success Handling Call Flow

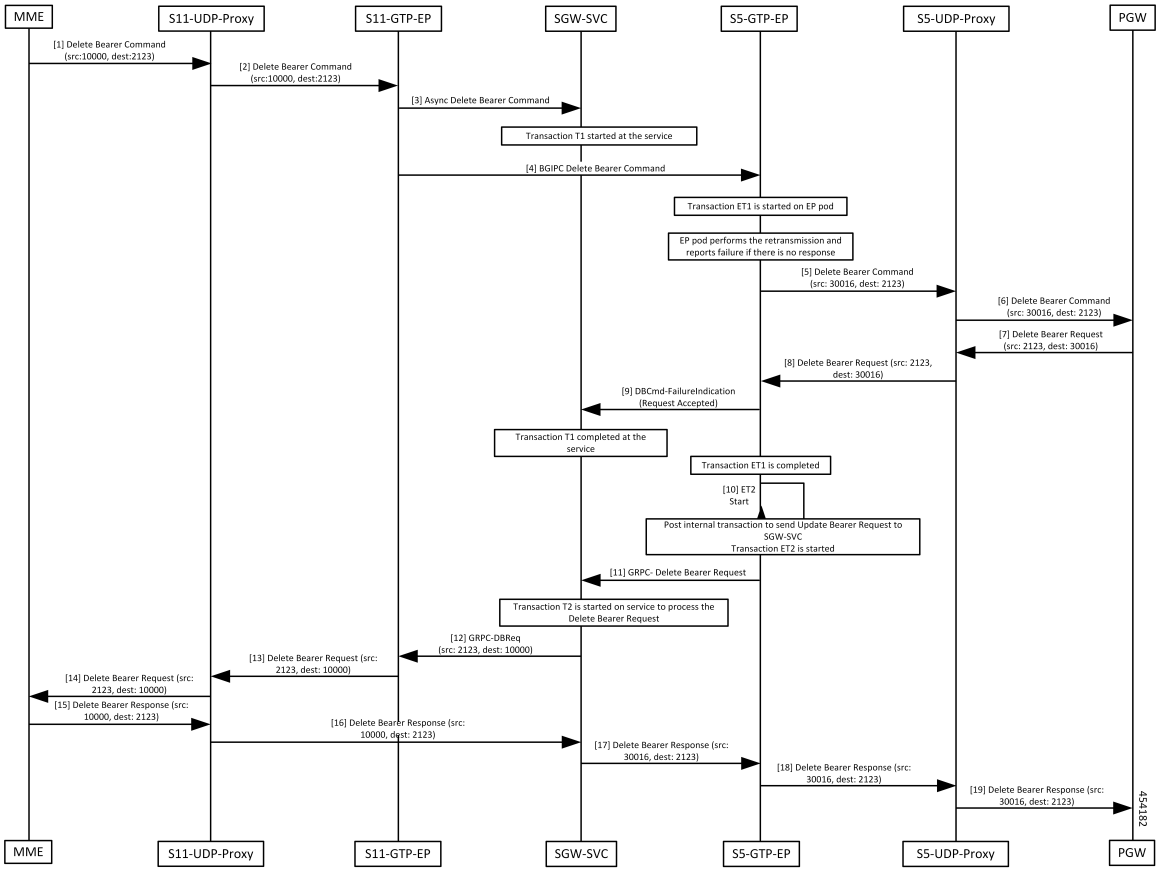
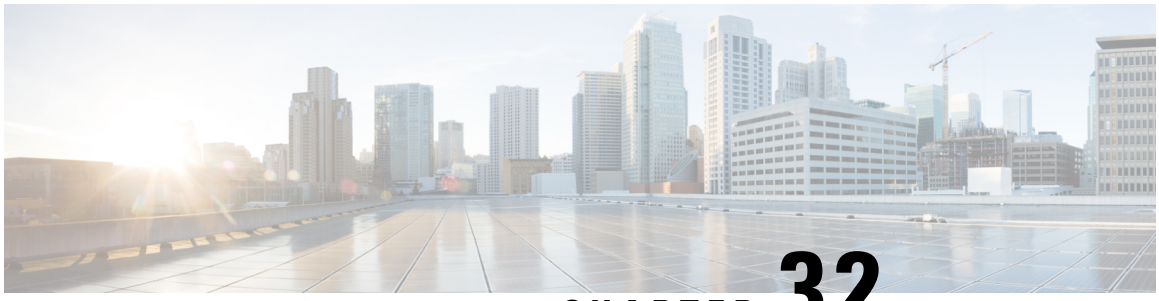


Table 135: DBC Success Handling Call Flow Description

Step	Description
1	The MME sends a Delete Bearer Command to the S11-UDP-Proxy.
2	The S11-UDP-Proxy forwards the Delete Bearer Command to the S11-GTP-EP.
3	The S11-UDP-Proxy sends the ASYNC Delete Bearer Command to the SGW-SVC pod.
4	The SGW-SVC pod sends the BGIPC Delete Bearer Command to the S5-GTP-EP. Save DBC_info in the PDN for response.
5	The EP pod performs the retransmission and reports a failure if there is no response. The pod sends the Delete Bearer Command Failure Indication (DBCFI) to the SGW-SVC pod. The S5-GTP-EP sends the Delete Bearer Command to the S5-UDP-Proxy.
6	The S5-UDP-Proxy send the Delete Bearer Command to the PGW.
7	The PGW sends the Delete Bearer Request to the S5-UDP-Proxy pod.
8	The S5-UDP-Proxy pod forwards the Delete Bearer Request to the S5-GTP-EP.

Step	Description
9	The S5-GTP-EP pod sends the DBCFI (with Request as ACCEPTED) to the SGW-SVC pod to end the transaction. The SGW-SVC pod ends the transaction and consumes this DBCFI. The post internal transaction sends the GRPCE_DBReq to SGW-SVC pod.
10	After the ET1 transaction is completed, the S5-GTP-EP starts.
11	The S5-GTP-EP pod sends the GRPC-DBRequest to the SGW-SVC.
12	The SGW-SVC pod processes the Delete Bearer Request and used saved DBC_Info to send the Updated Bearer Request to the MME.
13	The S11-GTP-EP pod sends the Delete Bearer Request to the S11-UDP-Proxy pod.
14	The S11-UDP-Proxy forwards the Delete Bearer Request to the MME.
15	The MME sends the Delete Bearer Response to the S11-UDP-Proxy pod.
16	The S11-UDP-Proxy processes the Delete Bearer Response to the SGW-SVC.
17	The SGW-SVC forwards the Delete Bearer Response to the S5-GTP-EP.
18	The S5-GTP-EP pod sends the Delete Bearer Response to the S5-UDP-Proxy.
19	The S5-UDP-Proxy sends the Delete Bearer Response to the PGW.



CHAPTER 32

Modify Bearer Request Support

Feature Summary and Revision History

Summary Data

Table 136: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Revision Details	Release
First introduced.	2020.03.0

Feature Description

cnSGW-C supports the MBR service request from MME to change the UE state from IDLE to ACTIVE. cnSGW-C supports the following service requests:

- UE-triggered service request without PGW interaction
- UE-triggered service request with PGW interaction

How it Works

This section describes how this feature works.

The cnSGW-C performs the following actions while processing the UE-triggered service request:

- Sends the Sx Modification Request message to the UPF to:
  - Mark downlink Forwarding Action Rule (FAR) as forward.
  - Update the S1 eNodeB-F TEID information to UPF sends the downlink packets to eNodeB.
- After receiving the Sx Modify Response message from the UPF, cnSGW-C:
  - Sends the Modify Bearer Response message to MME.
  - Checks User Location Information (ULI) or UE time zone. For any change in the time zone, it sends Modify Bearer Request to PGW to update the TAI. The UE-triggered service request with PGW interaction request only considers ULI or UE time zone check.

Call Flows

This section describes the key call flows for this feature.

UE-Triggered Service Request without PGW Interaction Call Flow

This section describes the UE-Triggered Service Request without PGW Interaction call flow.

Figure 75: UE Triggered Service Request without PGW Interaction Call Flow

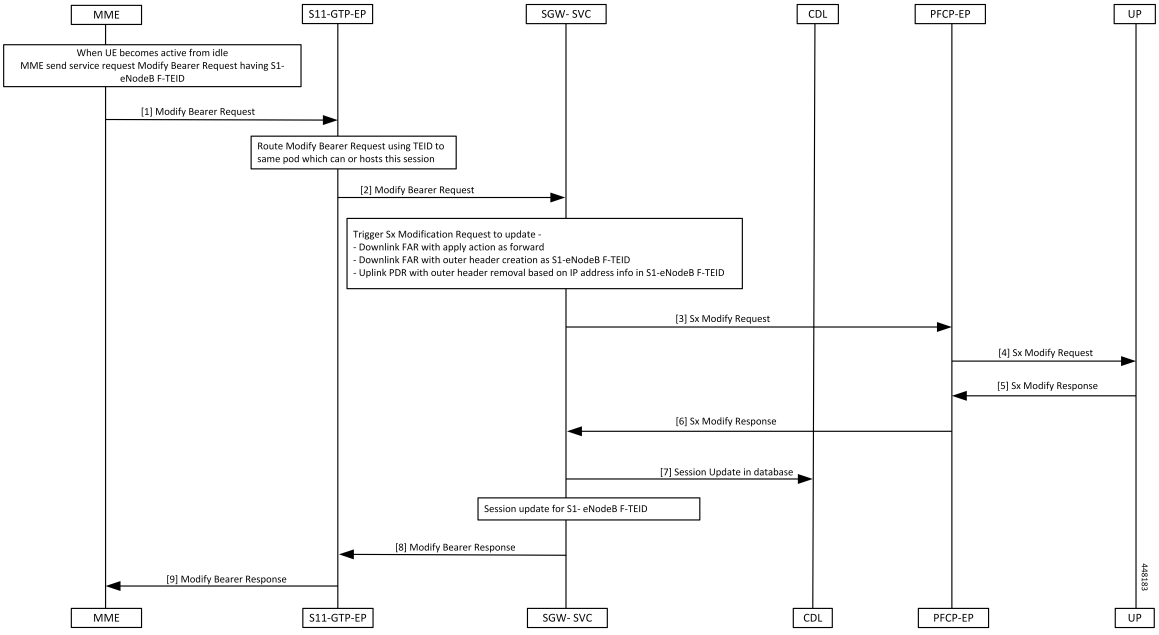


Table 137: UE Triggered Service Request without PGW Interaction Call Flow Description

Step	Description
1	The MME sends the Modify Bearer Request message with s1-eNodeB F-TEID to cnSGW-C when the UE changes from IDLE to ACTIVE state.
2	The S11-GTP-EP decodes the UDP message and converts it into gRPC message. This gRPC message is sent to the SGW-SVC pod (which can handle this UE session) using TEID.
3	The SGW-SVC pod finds the subscriber context using the local ingress TEID. The SGW-SVC pod sends the Modify Bearer Request content and sends Sx Modify Request to PFCP-EP.
4	The PFCP-EP sends Sx Modify Request message to UPF through the UDP proxy.
5	The UPF process the Sx Modify Request message and sends Sx Modify Response message to PFCP-EP.
6	The PFCP-EP sends the Sx Modify Response message to SGW-SVC pod.
7	The SGW-SVC pod chnages PDN into CONNECTED state and sends session update to CDL. The CDL module updates the information in the database.
8	The SGW-SVC pod sends the Modify Bearer Response message to the S11-GTP-EP.
9	The S11-GTP-EP sends the Modify Bearer Response message to MME. The MME processes the Modify Bearer Response message.

UE-Triggered Service Request with PGW Interaction Call Flow

This section describes the UE-Triggered Service Request with PGW Interaction call flow.

Figure 76: UE-Triggered Service Request with PGW Interaction Call Flow

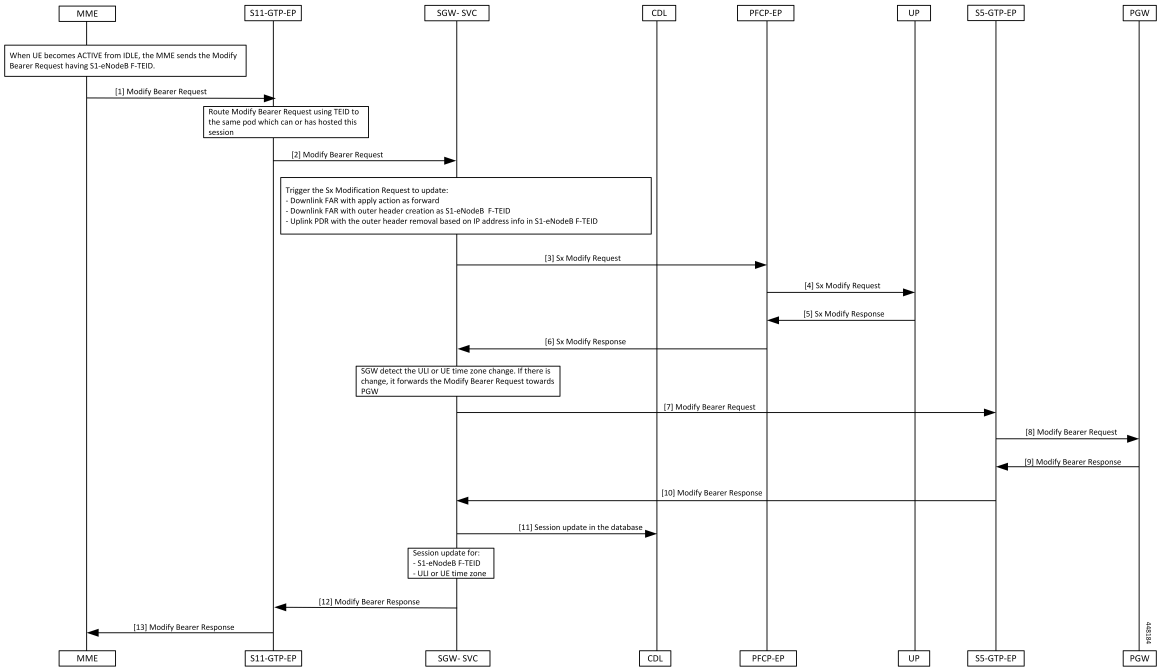
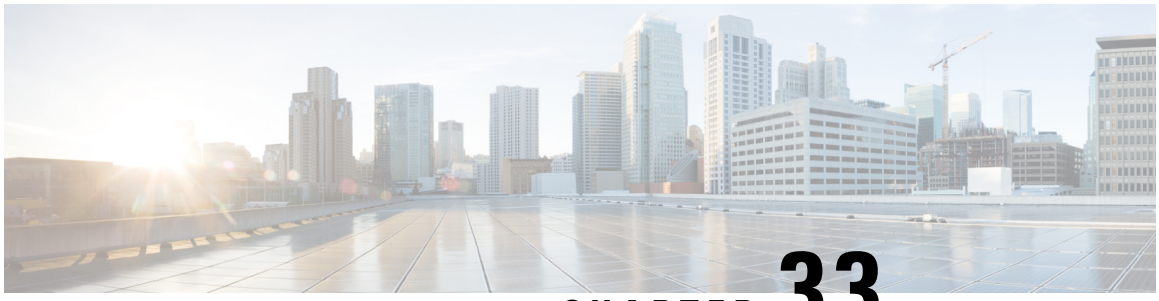


Table 138: UE-Triggered Service Request with PGW Interaction Call Flow description

Step	Description
1	The MME sends the Modify Bearer Request with s1-eNodeB F-TEID to cnSGW-C when the UE changes from the IDLE to ACTIVE state.
2	The S11-GTP-EP decodes the UDP message and converts it into the gRPC message. This gRPC message is sent to the SGW-Service pod, which handles the UE session using TEID.
3	The SGW-Service pod finds the subscriber context using the local ingress TEID. It validates the Modify Bearer Request content and sends the Sx Modify Request to PFCP-EP.
4	The PFCP-EP sends the Sx Modify Request to the UPF through the UDP proxy.
5	The UPF1 processes the Sx Modify Request and sends the Sx Modify Response message.
6	The PFCP-EP sends the Sx Modify Response message to the SGW-Service pod.
7	The SGW-Service pod detects ULI or UE time zone change and sends the Modify Bearer Request message to S5-GTP-EP.
8	The S5-GTP-EP sends the Modify Bearer Request message to the PGW.
9	The PGW processes the Modify Bearer Request message and sends the Modify Bearer Response message.
10	The S5-GTP-EP sends the Modify Bearer Response message to the SGW-Service pod.

Step	Description
11	The SGW-Service pod moves PDN into the CONNECTED state and sends the update to CDL. The CDL module updates the information in the database.
12	The SGW-Service pod sends the Modify Bearer Response message to the S11-GTP-EP.
13	The S11-GTP-EP sends the Modify Bearer Response message to the MME. The MME processes the Modify Bearer Response message.



CHAPTER 33

Monitor Subscriber and Protocol Support

Feature Summary and Revision History

Summary Data

Table 139: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Configuration required to disable
Related Documentation	Not Applicable

Revision History

Table 140: Revision History

Revision Details	Release
First introduced.	2021.01.0

Feature Description

The cnSGW-C service supports the subscriber map and the operator policy configurations for the SGW service parameters.

Configuring Monitor Subscriber

Monitor subscriber is an utility to trace messages related to a specified subscriber. The app-infra provides the following command to monitor subscriber:

```
monitor subscriber [ supi ] [ imsi ] [ imei ] (capture-duration)
(internal-messages) (transaction-logs) (nf-service) (gr-instance)
```

Note In 2021.02 and later releases, the **namespace** keyword is deprecated and replaced with the **nf-service** keyword.

NOTES:

- **supi** - Specify the subscriber identifier.

  Example: imsi-123456789, imsi-123*

- **imsi** - Specify the IMSI value.

  Example: 123456789, *

- **imei** - Specify the IMEI value.
- Example: 123456789012345, *
- **capture-duration** - (Optional) Used to specify the duration in seconds during which monitor subscriber is enabled. Default value is 300 secs.
- **internal-messages** - (Optional) When set to yes, it enables internal messaging. By default, it is disabled.
- **transaction-logs** - (Optional) When set to yes, it enables transaction logging. By default, it is disabled.

Note Messages and transaction logs are mutually exclusive.

- **namespace** - Deprecated option. Use nf-service instead.
- **nf-service** - (Optional) Specify the NF service. Possible values are sgw, smf. Default value is none.
- **gr-instance** - (Optional) Monitor subscriber for a given gr-instance only.

Accessing Logs: The monitor subscriber logs can be accessed from the oam-pod at path `/opt/workspace/logs/monsublogs`.

```
root@oam-pod-0:/opt/workspace/logs/monsublogs# ls
none.imsi-123456789_TS_2021-06-05T06:19:12.682444275.txt
sgw.imei-352099001761480_TS_2021-06-05T13:07:41.774214146.txt.sorted
 none.imsi-123456789_TS_2021-06-05T06:20:39.751939118.txt
sgw.imei-352099001761480_TS_2021-06-05T13:48:51.868279985.txt
 none.imsi-123456789_TS_2021-06-06T06:22:16.015635407.txt
sgw.imei-352099001761480_TS_2021-06-05T13:48:51.868279985.txt.sorted
 sgw.imei-352099001761480_TS_2021-06-04T19:09:24.863985017.txt
sgw.imei-352099001761480_TS_2021-06-05T14:50:09.330635953.txt
 sgw.imei-352099001761480_TS_2021-06-04T19:09:24.863985017.txt.sorted
sgw.imei-352099001761480_TS_2021-06-05T14:50:09.330635953.txt.sorted
 sgw.imei-352099001761480_TS_2021-06-05T08:44:25.889632126.txt
```

```
sgw.imei-352099001761480_TS_2021-06-05T17:36:17.238331396.txt
 sgw.imei-352099001761480_TS_2021-06-05T08:44:25.889632126.txt.sorted
sgw.imei-352099001761480_TS_2021-06-05T17:36:17.238331396.txt.sorted
 sgw.imei-352099001761480_TS_2021-06-05T10:26:23.529652777.txt
'sgw.imsi-*_TS_2021-06-05T06:23:19.865508390.txt'
 sgw.imei-352099001761480_TS_2021-06-05T10:26:23.529652777.txt.sorted
'sgw.imsi-*_TS_2021-06-05T06:25:18.219875282.txt'
 sgw.imei-352099001761480_TS_2021-06-05T13:07:41.774214146.txt
```

Example

The following is an example:

```
monitor subscriber imsi 123456789 capture-duration 100 internal-messages yes
monitor subscriber imsi 123456789 capture-duration 100 transaction-logs yes
```

Sample Output

Here is a sample ouput:

```
monitor subscriber imsi * namespace sgw
supi: imsi-*
captureDuraiton: 300
enableInternalMsg: false
enableTxnLog: false
namespace(deprecated. Use nf-service instead.): sgw
nf-service: none
gr-instance: 0
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   277  100    89  100   188   6846  14461 --:--:-- --:--:-- --:--:-- 21307
Command: --header Content-type:application/json --request POST --data
{"command":"mon_sub","parameters":{"supi":"imsi-*","duration":300,"enableTxnLog":false,"enableInternalMsg":false,"action":"start","namespace":"sgw","nf-service":"none","grInstance":0}}
 http://oam-pod:8879/commands
Result start mon_sub, fileName
->logs/monsublogs/sgw.imsi-*_TS_2021-06-06T06:38:23.892447899.txt
Starting to tail the monsub messages from file:
logs/monsublogs/sgw.imsi-*_TS_2021-06-06T06:38:23.892447899.txt
Defaulting container name to oam-pod.
Use 'kubectl describe pod/oam-pod-0 -n cn' to see all of the containers in this pod.
      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.158362
      Message: Sx Session Establishment Request
      Description: Sx Session Establishment Request Message from SGWC to SGWU
      Source: 10.1.2.156
      Destination: 10.1.2.155
      PAYLOAD:
        Sx Session Establishment Request:
            Sx Session Establishment Request:
                FSeid:
                    Seid: 1297037239519281279
                    IPv4Address: 10.1.2.156
                CreatePdr:
                    CreatePdr[0]:
                        PdrId: 1
                        Precedence: 0
                        Pdi:
                            SrcIf: CORE
                            UeIp:
                                Src: false
                                Dst: false
                                IPv4Addr: 0.0.0.0
                            TEndpointId: 1
                            Valid: true
```

```
                OuterHdrRem: 0
                FarId:
                    FarId[0]: 1
                UrrId:
                    UrrId[0]: 1
                Qfi: 0
                OuterHdrRemValid: false
            CreatePdr[1]:
                PdrId: 2
                Precedence: 0
                Pdi:
                    SrcIf: ACCESS
                    UeIp:
                        Src: false
                        Dst: false
                        IPv4Addr: 0.0.0.0
                    TEndpointId: 2
                    Valid: true
                OuterHdrRem: 0
                FarId:
                    FarId[0]: 2
                UrrId:
                    UrrId[0]: 1
                Qfi: 0
                OuterHdrRemValid: false
        CreateFar:
            CreateFar[0]:
                FarId: 1
                ApplyAction:
                    Drop: true
                    Frwd: false
                    Buff: false
                    Nocp: false
                    Dupl: false
                    Valid: true
                FwdParams:
                    DestIf: ACCESS
                    RedirectInfo:
                        AddrType: 0
                        Valid: false
                    OuterHdr:
                        OuterHdrDesc: 0
                        Teid: 0
                        IPv4Address: 0.0.0.0
                        Port: 0
                        Valid: false
                    TEndptId: 2
                    OuterPktTos: 255
                    InnerPktTos: 255
                    TosOpt:
                        CopyInner: false
                        CopyOuter: false
                    SendTos: 0
                    PfcpSmFlags:
                        Drobu: false
                        Qaurr: false
                        Sndem: false
                        Valid: false
                    Valid: true
                    NextHopId: 0
                DuplParams:
                    DestIf: ACCESS
                    OuterHdr:
                        OuterHdrDesc: 0
```

```
                Teid: 0
                IPv4Address: 0.0.0.0
                Port: 0
                Valid: false
            InterceptInfo:
                InterceptId: 0
                ChargingId: 0
                SmfLiNodeId:
                    IpDesc: 0
                    IPv4Address: 0.0.0.0
                    Valid: false
                PduSessionId: 0
                Valid: false
            Valid: false
        BarId: 0
    CreateFar[1]:
        FarId: 2
        ApplyAction:
            Drop: true
            Frwd: false
            Buff: false
            Nocp: false
            Dupl: false
            Valid: true
        FwdParams:
            DestIf: CORE
            RedirectInfo:
                AddrType: 0
                Valid: false
            OuterHdr:
                OuterHdrDesc: 0
                Teid: 0
                IPv4Address: 0.0.0.0
                Port: 0
                Valid: false
            TEndptId: 1
            OuterPktTos: 255
            InnerPktTos: 255
            TosOpt:
                CopyInner: false
                CopyOuter: false
            SendTos: 0
            PfcpSmFlags:
                Drobu: false
                Qaurr: false
                Sndem: false
                Valid: false
            Valid: true
            NextHopId: 0
        DuplParams:
            DestIf: ACCESS
            OuterHdr:
                OuterHdrDesc: 0
                Teid: 0
                IPv4Address: 0.0.0.0
                Port: 0
                Valid: false
            InterceptInfo:
                InterceptId: 0
                ChargingId: 0
                SmfLiNodeId:
                    IpDesc: 0
                    IPv4Address: 0.0.0.0
                    Valid: false
```

```
                PduSessionId: 0
                Valid: false
            Valid: false
        BarId: 0
CreateTEndpt:
    CreateTEndpt[0]:
        EndpointId: 1
        FTeid:
            Teid: 0
            IPv4Address: 0.0.0.0
            ChooseId: 0
        BearerLvlInfo:
            Valid: 1
            Qci: 6
    CreateTEndpt[1]:
        EndpointId: 2
        FTeid:
            Teid: 0
            IPv4Address: 0.0.0.0
            ChooseId: 0
        BearerLvlInfo:
            Valid: 1
            Qci: 6
PdnType: 0
UplaneInacTimer: 0
MetaData: From:10.1.2.156:12002->To:10.1.2.155:8805
Supi:
Seid: 1297037239519281279
Seqno: 918
Version: 0
MsgPriority: false
MsgPriorityVal: 0
Cmnid: 0
Rseid: 0
IntfType: 0
HdrLen: 0
MsgLen: 0
CreateUrr:
    CreateUrr[0]:
        UrrId: 1
        MeasurementType:
            Duration: false
            Volume: true
            Event: false
        ReportingTriggers:
            PERIO: false
            VOLTH: true
            TIMTH: false
            QUHTI: false
            START: false
            STOPT: false
            DROTH: false
            LIUSA: false
            VOLQU: false
            TIMQU: false
            ENVCL: false
            MACAR: false
        VolumeThresh:
            TotVol_Valid: false
            ULVol_Valid: true
            DLVol_Valid: true
            TotVolumeThreshold: 0
            UlVolumeThreshold: 1000000
            DlVolumeThreshold: 2000000
```

```
                    UserIDInfo:
                        Imsi: 123456789012348
                        Imei: 123456786666660
                        Msisdn: 223310101010101
                        Valid: true
                    XHeaderInfo:
                        RatType:
                        Valid: false
                    CfPolicyId:
                        PolicyId: 0
                        Valid: false
                    ChargingDisabled:
                        Valid: false
                        Value: false
                    ChargingParams:
                        Valid: 0
                        GyOfflineChargingEnabled: 0
                    NextHopIPv4: 0

------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.204469
      Message: Sx Session Establishment Response
      Description: Sx Session Establishment Response Message from SGWU to SGWC
      Source: 10.1.2.155
      Destination: 10.1.2.156
      PAYLOAD:
        Sx Session Establishment Response:
            Sx Session Establishment Response:
                Cause: 1
                OffendingIe: 0
                FSeid:
                    Seid: 10002
                    IPv4Address: 10.1.2.155
                CreatedTEndpt:
                    CreatedTEndpt[0]:
                        EndpointId: 1
                        FTeid:
                            Teid: 2287
                            IPv4Address: 192.168.131.1
                            ChooseId: 0
                    CreatedTEndpt[1]:
                        EndpointId: 2
                        FTeid:
                            Teid: 2288
                            IPv4Address: 1.1.1.83
                            ChooseId: 0
                MetaData: From:10.1.2.155:8805->To:10.1.2.156:12002
                Supi:
                Seid: 1297037239519281279
                Seqno: 918
                Version: 0
                MsgPriority: false
                MsgPriorityVal: 0
                Cmnid: 0
                Rseid: 0
                IntfType: 0
                HdrLen: 0
                MsgLen: 0
                LoadControlInfo:
                    SeqNum: 0
                    Metric: 0
                    Valid: false
```

```
                OverloadControlInfo:
                    SeqNum: 0
                    Metric: 0
                    Ociflag: 0
                    Valid: false

-------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.208740
      Message: GtpEpDecodeRPCResponse
      Description:  2071
      Source:
      Destination:
      PAYLOAD:

-------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.209227
      Message: S5 S8 Create Session Request
      Description: S5 S8 Create Session Request Message
      Source: 10.1.2.156
      Destination: 10.1.2.154
      PAYLOAD:
        S5 S8 Create Session Request:
            S5 S8 Create Session Request:
                Version: 2
                Pflag: false
                TEIDflag: true
                MsgPriority: false
                MsgLength: 221
                TIED: 0
                Seq: 65970
                MsgTypeId: 32
                MsgPriorityValue: 0
                Peer_IPv4_Flag: false
                Peer_IPv6_Flag: false
                MetaData: From:10.1.2.156:15001->To:10.1.2.154:2123
                Seid: 0
                Rseid: 0
                Cmnid: 0
                MsgType:
                    Create_Session_Request:
                        IMSI: 123456789012348
                        Recovery:
                            Value: 0
                        APN: intershat
                        AMBR:  UL: 232323 kbps, DL: 232323 kbps
                        MEI: 123456786666660
                        MSISDN: 223310101010101
                        Indication:
                            DAF: false
                            DTF: false
                            HI: true
                            DFI: false
                            OI: false
                            ISRSI: false
                            ISRAI: false
                            SGWCI: false
                            SQCI: false
                            UIMSI: false
                            CFSI: false
                            CRSI: false
```

```
    P: false
    PT: false
    SI: false
    MSV: false
    RetLoc: false
    PBIC: false
    SRNI: false
    S6AF: false
    S4AF: false
    MBMDT: false
    ISRAU: false
    CCRSI: false
    CPRAI: false
    ARRL: false
    PPOF: false
    PPON_PPEI: false
    PPSI: false
    CSFBI: false
    CLII: false
    CPSR: false
    NSI: false
    UASI: false
    DTCI: false
    BDWI: false
    PSCI: false
    PCRI: false
    AOSI: false
    AOPI: false
    ROAAI: false
    EPCOSI: false
    CPOPCI: false
    PMTSMI: false
    S11TF: false
    PNSI: false
    UNACCSI: false
    WPMSI: false
    5GSIWK: false
    EEVRSI: false
    LTEMUI: false
    LTEMPI: false
    ENBCRSI: false
    TSPCMI: false
    PGBK: false
    PCPSI: false
    PCP: false
    PCPU: false
    N26_5GS: false
    RI_5GCN: false
    RS_5GCN: false
PAA:
    PDN_Type: 1
    IPv4: 12.0.0.173
    IPv6_Prefix: 0
RAT_Type:
    Value: 6
Serving_Network:
    MCC: 123
    MNC: 456
ULI:
    UliTai:  Mcc: 123, Mnc: 456, TAC: 2346
    UliEcgi:
        Mcc: 123
        Mnc: 456
        Eci: 1234567
```

```
                                FQ_TEID:
                                    SgwCntrl:
                                        IFace: 6
                                        TEID: 1375731839
                                        IPv4: 10.1.2.156
                                Bearer_Context_List:
                                    NumBearerCtxt: 1
                                    PbBearerCxt:
                                        PbBearerCxt[0]:
                                            BearerCtxType: 0
                                            EBI: 5
                                            Fqteid:
                                                SgwData:
                                                    IFace: 0
                                                    TEID: 2287
                                                    IPv4: 192.168.131.1
                                            BearerQos:
                                                PCI: true
                                                PL: 12
                                                PVI: true
                                                QCI: 6
                                                UL_MBR: 0 kbps
                                                DL_MBR: 0 kbps
                                                UL_GBR: 0 kbps
                                                DL_GBR: 0 kbps
                                                Arp: 113
                                                QciType: 0
                                Charging_Characteristics:
                                    Value:
                                        Value[0]: 210
                                        Value[1]: 4
                                        Value[2]: 0
                                        Value[3]: 0
                                PDN_Type:
                                    Value: 1
                                UE_Time_Zone:
                                    Time_Zone: 16
                                    Daylight_Saving_Time: 1
                                APN_Restriction:
                                    Value: 0
                                Selection_Mode:
                                    Value: 0
                                EPCO:
                                    Len: 5
                                    Value:
                                        Value[0]: 128
                                        Value[1]: 0
                                        Value[2]: 26
                                        Value[3]: 1
                                        Value[4]: 5

------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2020/09/25 05:22:36.739932
      Message: GtpEpDecodeRPCResponse
      Description:  2071
      Source:
      Destination:
      PAYLOAD:

------------------------------------------------

      Subscriber Id: imsi-123456789012348
```

```
      Timestamp: 2020/09/25 05:22:36.739932
      Message: GtpEpDecodeRPCIPCResponse
      Description:  2071
      Source:
      Destination:
      PAYLOAD:

-------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.252214
      Message: GtpEpDecodeRPCResponse
      Description:  2071
      Source:
      Destination:
      PAYLOAD:

-------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.252767
      Message: S5 S8 Create Session Response
      Description: S5 S8 Create Session Response Message
      Source: 10.1.2.154
      Destination: 10.1.2.156
      PAYLOAD:
        S5 S8 Create Session Response:
            S5 S8 Create Session Response:
                Version: 2
                Pflag: false
                TEIDflag: true
                MsgPriority: false
                MsgLength: 107
                TIED: 1375731839
                Seq: 65970
                MsgTypeId: 33
                MsgPriorityValue: 0
                Peer_IPv4_Flag: false
                Peer_IPv6_Flag: false
                MetaData: From:10.1.2.154:0->To:10.1.2.156:0
                Seid: 0
                Rseid: 0
                Cmnid: 0
                MsgType:
                    Create_Session_Response:
                        Cause:
                            Cause_Value: 16
                            PCE: false
                            BCE: false
                            OrigInd: false
                        Recovery:
                            Value: 100
                        AMBR:  UL: 10 kbps, DL: 20 kbps
                        PAA:
                            PDN_Type: 1
                            IPv4: 12.0.0.173
                            IPv6_Prefix: 0
                        FQ_TEID:
                            PgwCntrl:
                                IFace: 7
                                TEID: 1885
                                IPv4: 10.1.2.154
                        Bearer_Context_List:
                            NumBearerCtxt: 1
```

```
                                PbBearerCxt:
                                    PbBearerCxt[0]:
                                        BearerCtxType: 0
                                        EBI: 5
                                        Cause:
                                            Cause_Value: 16
                                            PCE: false
                                            BCE: false
                                            OrigInd: false
                                        Fqteid:
                                            PgwData:
                                                IFace: 5
                                                TEID: 1886
                                                IPv4: 10.1.2.154
                                        ChrgId:
                                            Value: 303174163
                            APN_Restriction:
                                Value: 1

------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.256786
      Message: Sx Session Modification Request
      Description: Sx Session Modification Request Message from SGWC to SGWU
      Source: 10.1.2.156
      Destination: 10.1.2.155
      PAYLOAD:
        Sx Session Modification Request:
            Sx Session Modification Request:
                UpdatePdr:
                    UpdatePdr[0]:
                        PdrId: 1
                        OuterHdrRem: 0
                        Precedence: 0
                        Pdi:
                            SrcIf: ACCESS
                            UeIp:
                                Src: false
                                Dst: false
                                IPv4Addr: 0.0.0.0
                            TEndpointId: 0
                            Valid: false
                        Qfi: 0
                UpdateFar:
                    UpdateFar[0]:
                        FarId: 2
                        ApplyAction:
                            Drop: false
                            Frwd: true
                            Buff: false
                            Nocp: false
                            Dupl: false
                            Valid: true
                        UpdateFwdParams:
                            DestIf: ACCESS
                            RedirectInfo:
                                AddrType: 0
                                Valid: false
                            OuterHdr:
                                OuterHdrDesc: 256
                                Teid: 1886
                                IPv4Address: 10.1.2.154
                                Port: 0
```

```
                    Valid: true
                TEndptId: 0
                OuterPktTos: 0
                InnerPktTos: 0
                TosOpt:
                    CopyInner: false
                    CopyOuter: false
                SendTos: 0
                PfcpSmFlags:
                    Drobu: false
                    Qaurr: false
                    Sndem: false
                    Valid: false
                Valid: true
                NextHopId: 0
            UpdateDuplParams:
                DestIf: ACCESS
                OuterHdr:
                    OuterHdrDesc: 0
                    Teid: 0
                    IPv4Address: 0.0.0.0
                    Port: 0
                    Valid: false
                InterceptInfo:
                    InterceptId: 0
                    ChargingId: 0
                    SmfLiNodeId:
                        IpDesc: 0
                        IPv4Address: 0.0.0.0
                        Valid: false
                    PduSessionId: 0
                    Valid: false
                Valid: false
            BarId: 0
    UplaneInacTimer: 0
    MetaData: From:10.1.2.156:11001->To:10.1.2.155:8805
    Supi:
    Seid: 1297037239519281279
    Seqno: 917
    Version: 0
    MsgPriority: false
    MsgPriorityVal: 0
    Cmnid: 0
    Rseid: 10002
    IntfType: 0
    HdrLen: 0
    MsgLen: 0
    PfcpSmFlags:
        Drobu: false
        Qaurr: false
        Sndem: false
        Valid: false
    UserIDInfo:
        Valid: false
    XHeaderInfo:
        RatType:
        Valid: false
    CfPolicyId:
        PolicyId: 0
        Valid: false
    GyStatus:
        Valid: false
        Value: false
    ChargingDisabled:
```

```
                    Valid: false
                    Value: false
                QueryInterface:
                    Valid: false
                    OfflineUrr: false
                    OnlineUrr: false
                    RadiusUrr: false
                    BearerUrr: false
                    SessUrr: false

-------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.290097
      Message: Sx Session Modification Response
      Description: Sx Session Modification Response Message from SGWU to SGWC
      Source: 10.1.2.155
      Destination: 10.1.2.156
      PAYLOAD:
        Sx Session Modification Response:
            Sx Session Modification Response:
                Cause: 1
                OffendingIe: 0
                LoadControlInfo:
                    SeqNum: 0
                    Metric: 0
                    Valid: false
                OverloadControlInfo:
                    SeqNum: 0
                    Metric: 0
                    Ociflag: 0
                    Valid: false
                MetaData: From:10.1.2.155:8805->To:10.1.2.156:11001
                Supi:
                Seid: 1297037239519281279
                Seqno: 917
                Version: 1
                MsgPriority: false
                MsgPriorityVal: 0
                Cmnid: 0
                Rseid: 0
                IntfType: 0
                HdrLen: 17
                MsgLen: 0

-------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.140860
      Message: S11 Create Session Request
      Description: S11 Create Session Request Message
      Source: 10.1.2.155
      Destination: 10.1.2.156
      PAYLOAD:
        S11 Create Session Request:
            S11 Create Session Request:
                Version: 2
                Pflag: false
                TEIDflag: false
                MsgPriority: false
                MsgLength: 219
                TIED: 0
                Seq: 511
                MsgTypeId: 32
```

```
MsgPriorityValue: 0
Peer_IPv4_Flag: false
Peer_IPv6_Flag: false
MetaData: From:10.1.2.155:2123->To:10.1.2.156:2123
Seid: 0
Rseid: 0
Cmnid: 0
MsgType:
    Create_Session_Request:
        IMSI: 123456789012348
        Recovery:
            Value: 100
        APN: intershat
        AMBR:  UL: 232323 kbps, DL: 232323 kbps
        MEI: 123456786666660
        MSISDN: 223310101010101
        Indication:
            DAF: false
            DTF: false
            HI: true
            DFI: false
            OI: false
            ISRSI: false
            ISRAI: false
            SGWCI: false
            SQCI: false
            UIMSI: false
            CFSI: false
            CRSI: false
            P: false
            PT: false
            SI: false
            MSV: false
            RetLoc: false
            PBIC: false
            SRNI: false
            S6AF: false
            S4AF: false
            MBMDT: false
            ISRAU: false
            CCRSI: false
            CPRAI: false
            ARRL: false
            PPOF: false
            PPON_PPEI: false
            PPSI: false
            CSFBI: false
            CLII: false
            CPSR: false
            NSI: false
            UASI: false
            DTCI: false
            BDWI: false
            PSCI: false
            PCRI: false
            AOSI: false
            AOPI: false
            ROAAI: false
            EPCOSI: false
            CPOPCI: false
            PMTSMI: false
            S11TF: false
            PNSI: false
            UNACCSI: false
```

```
    WPMSI: false
    5GSIWK: false
    EEVRSI: false
    LTEMUI: false
    LTEMPI: false
    ENBCRSI: false
    TSPCMI: false
    PGBK: false
    PCPSI: false
    PCP: false
    PCPU: false
    N26_5GS: false
    RI_5GCN: false
    RS_5GCN: false
PAA:
    PDN_Type: 1
    IPv4: 12.0.0.173
    IPv6_Prefix: 0
RAT_Type:
    Value: 6
Serving_Network:
    MCC: 123
    MNC: 456
ULI:
    UliTai:  Mcc: 123, Mnc: 456, TAC: 2346
    UliEcgi:
        Mcc: 123
        Mnc: 456
        Eci: 1234567
FQ_TEID:
    MmeCntrl:
        IFace: 10
        TEID: 2286
        IPv4: 10.1.2.155
    PgwCntrl:
        IFace: 7
        TEID: 0
        IPv4: 10.1.2.154
Bearer_Context_List:
    NumBearerCtxt: 1
    PbBearerCxt:
        PbBearerCxt[0]:
            BearerCtxType: 0
            EBI: 5
            Fqteid:
            BearerQos:
                PCI: true
                PL: 12
                PVI: true
                QCI: 6
                UL_MBR: 0 kbps
                DL_MBR: 0 kbps
                UL_GBR: 0 kbps
                DL_GBR: 0 kbps
                Arp: 113
                QciType: 0
Charging_Characteristics:
    Value:
        Value[0]: 210
        Value[1]: 4
        Value[2]: 0
        Value[3]: 0
PDN_Type:
    Value: 1
```

```
                            UE_Time_Zone:
                                Time_Zone: 16
                                Daylight_Saving_Time: 1
                            APN_Restriction:
                                Value: 0
                            Selection_Mode:
                                Value: 0
                            EPCO:
                                Len: 5
                                Value:
                                    Value[0]: 128
                                    Value[1]: 0
                                    Value[2]: 26
                                    Value[3]: 1
                                    Value[4]: 5

-------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.297373
      Message: GtpEpDecodeRPCResponse
      Description:  258
      Source:
      Destination:
      PAYLOAD:

-------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.297913
      Message: GtpEpDecodeRPCResponse
      Description:  258
      Source:
      Destination:
      PAYLOAD:

-------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.298354
      Message: S11 Create Session Response
      Description: S11 Create Session Response Message
      Source: 10.1.2.156
      Destination: 10.1.2.155
      PAYLOAD:
        S11 Create Session Response:
            S11 Create Session Response:
                Version: 2
                Pflag: false
                TEIDflag: true
                MsgPriority: false
                MsgLength: 120
                TIED: 2286
                Seq: 511
                MsgTypeId: 33
                MsgPriorityValue: 0
                Peer_IPv4_Flag: false
                Peer_IPv6_Flag: false
                MetaData: From:10.1.2.156:2123->To:10.1.2.155:2123
                Seid: 0
                Rseid: 0
                Cmnid: 0
                MsgType:
                    Create_Session_Response:
```

```
                        Cause:
                            Cause_Value: 16
                            PCE: false
                            BCE: false
                            OrigInd: false
                        Recovery:
                            Value: 0
                        AMBR:  UL: 10 kbps, DL: 20 kbps
                        PAA:
                            PDN_Type: 1
                            IPv4: 12.0.0.173
                            IPv6_Prefix: 0
                        FQ_TEID:
                            PgwCntrl:
                                IFace: 7
                                TEID: 1885
                                IPv4: 10.1.2.154
                            SgwCntrl:
                                IFace: 11
                                TEID: 301990015
                                IPv4: 10.1.2.156
                        Bearer_Context_List:
                            NumBearerCtxt: 1
                            PbBearerCxt:
                                PbBearerCxt[0]:
                                    BearerCtxType: 0
                                    EBI: 5
                                    Cause:
                                        Cause_Value: 16
                                        PCE: false
                                        BCE: false
                                        OrigInd: false
                                    Fqteid:
                                        PgwData:
                                            IFace: 5
                                            TEID: 1886
                                            IPv4: 10.1.2.154
                                        SgwData:
                                            IFace: 1
                                            TEID: 2288
                                            IPv4: 1.1.1.83
                                    ChrgId:
                                        Value: 303174163
                        APN_Restriction:
                            Value: 1

-----------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.298524
      Message: S11 Create Session Response
      Description: S11 Create Session Response Message
      Source: 10.1.2.156
      Destination: 10.1.2.155
      PAYLOAD:
        S11 Create Session Response:
            S11 Create Session Response:
                Version: 2
                Pflag: false
                TEIDflag: true
                MsgPriority: false
                MsgLength: 120
                TIED: 2286
                Seq: 511
```

```
                    MsgTypeId: 33
                    MsgPriorityValue: 0
                    Peer_IPv4_Flag: false
                    Peer_IPv6_Flag: false
                    MetaData: From:10.1.2.156:2123->To:10.1.2.155:2123
                    Seid: 0
                    Rseid: 0
                    Cmnid: 0
                    MsgType:
                        Create_Session_Response:
                            Cause:
                                Cause_Value: 16
                                PCE: false
                                BCE: false
                                OrigInd: false
                            Recovery:
                                Value: 0
                            AMBR:  UL: 10 kbps, DL: 20 kbps
                            PAA:
                                PDN_Type: 1
                                IPv4: 12.0.0.173
                                IPv6_Prefix: 0
                            FQ_TEID:
                                PgwCntrl:
                                    IFace: 7
                                    TEID: 1885
                                    IPv4: 10.1.2.154
                                SgwCntrl:
                                    IFace: 11
                                    TEID: 301990015
                                    IPv4: 10.1.2.156
                            Bearer_Context_List:
                                NumBearerCtxt: 1
                                PbBearerCxt:
                                    PbBearerCxt[0]:
                                        BearerCtxType: 0
                                        EBI: 5
                                        Cause:
                                            Cause_Value: 16
                                            PCE: false
                                            BCE: false
                                            OrigInd: false
                                        Fqteid:
                                            PgwData:
                                                IFace: 5
                                                TEID: 1886
                                                IPv4: 10.1.2.154
                                            SgwData:
                                                IFace: 1
                                                TEID: 2288
                                                IPv4: 1.1.1.83
                                        ChrgId:
                                            Value: 303174163
                            APN_Restriction:
                                Value: 1

------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.358210
      Message: Sx Session Modification Request
      Description: Sx Session Modification Request Message from SGWC to SGWU
      Source: 10.1.2.156
      Destination: 10.1.2.155
```

```
PAYLOAD:
  Sx Session Modification Request:
      Sx Session Modification Request:
          UpdatePdr:
              UpdatePdr[0]:
                  PdrId: 2
                  OuterHdrRem: 0
                  Precedence: 0
                  Pdi:
                      SrcIf: ACCESS
                      UeIp:
                          Src: false
                          Dst: false
                          IPv4Addr: 0.0.0.0
                      TEndpointId: 0
                      Valid: false
                  Qfi: 0
          UpdateFar:
              UpdateFar[0]:
                  FarId: 1
                  ApplyAction:
                      Drop: false
                      Frwd: true
                      Buff: false
                      Nocp: false
                      Dupl: false
                      Valid: true
                  UpdateFwdParams:
                      DestIf: ACCESS
                      RedirectInfo:
                          AddrType: 0
                          Valid: false
                      OuterHdr:
                          OuterHdrDesc: 256
                          Teid: 2289
                          IPv4Address: 10.1.2.155
                          Port: 0
                          Valid: true
                      TEndptId: 0
                      OuterPktTos: 0
                      InnerPktTos: 0
                      TosOpt:
                          CopyInner: false
                          CopyOuter: false
                      SendTos: 0
                      PfcpSmFlags:
                          Drobu: false
                          Qaurr: false
                          Sndem: false
                          Valid: false
                      Valid: true
                      NextHopId: 0
                  UpdateDuplParams:
                      DestIf: ACCESS
                      OuterHdr:
                          OuterHdrDesc: 0
                          Teid: 0
                          IPv4Address: 0.0.0.0
                          Port: 0
                          Valid: false
                      InterceptInfo:
                          InterceptId: 0
                          ChargingId: 0
                          SmfLiNodeId:
```

```
                                    IpDesc: 0
                                    IPv4Address: 0.0.0.0
                                    Valid: false
                                PduSessionId: 0
                                Valid: false
                            Valid: false
                        BarId: 0
                UplaneInacTimer: 0
                MetaData: From:10.1.2.156:11000->To:10.1.2.155:8805
                Supi:
                Seid: 1297037239519281279
                Seqno: 917
                Version: 0
                MsgPriority: false
                MsgPriorityVal: 0
                Cmnid: 0
                Rseid: 10002
                IntfType: 0
                HdrLen: 0
                MsgLen: 0
                PfcpSmFlags:
                    Drobu: false
                    Qaurr: false
                    Sndem: false
                    Valid: false
                UserIDInfo:
                    Valid: false
                XHeaderInfo:
                    RatType:
                    Valid: false
                CfPolicyId:
                    PolicyId: 0
                    Valid: false
                GyStatus:
                    Valid: false
                    Value: false
                ChargingDisabled:
                    Valid: false
                    Value: false
                QueryInterface:
                    Valid: false
                    OfflineUrr: false
                    OnlineUrr: false
                    RadiusUrr: false
                    BearerUrr: false
                    SessUrr: false

------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.380172
      Message: Sx Session Modification Response
      Description: Sx Session Modification Response Message from SGWU to SGWC
      Source: 10.1.2.155
      Destination: 10.1.2.156
      PAYLOAD:
        Sx Session Modification Response:
            Sx Session Modification Response:
                Cause: 1
                OffendingIe: 0
                LoadControlInfo:
                    SeqNum: 0
                    Metric: 0
                    Valid: false
```

```
                    OverloadControlInfo:
                        SeqNum: 0
                        Metric: 0
                        Ociflag: 0
                        Valid: false
                    MetaData: From:10.1.2.155:8805->To:10.1.2.156:11000
                    Supi:
                    Seid: 1297037239519281279
                    Seqno: 917
                    Version: 1
                    MsgPriority: false
                    MsgPriorityVal: 0
                    Cmnid: 0
                    Rseid: 0
                    IntfType: 0
                    HdrLen: 17
                    MsgLen: 0

------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.383136
      Message: S5 S8 Modify Bearer Request
      Description: S5 S8 Modify Bearer Request Message
      Source: 10.1.2.156
      Destination: 10.1.2.154
      PAYLOAD:
        S5 S8 Modify Bearer Request:
            S5 S8 Modify Bearer Request:
                Version: 2
                Pflag: false
                TEIDflag: true
                MsgPriority: false
                MsgLength: 19
                TIED: 1885
                Seq: 131539
                MsgTypeId: 34
                MsgPriorityValue: 0
                Peer_IPv4_Flag: false
                Peer_IPv6_Flag: false
                MetaData: From:10.1.2.156:15002->To:10.1.2.154:2123
                Seid: 0
                Rseid: 0
                Cmnid: 0
                MsgType:
                    Modify_Bearer_Request:
                        Indication:
                            DAF: false
                            DTF: false
                            HI: true
                            DFI: false
                            OI: false
                            ISRSI: false
                            ISRAI: false
                            SGWCI: false
                            SQCI: false
                            UIMSI: false
                            CFSI: false
                            CRSI: false
                            P: false
                            PT: false
                            SI: false
                            MSV: false
                            RetLoc: false
```

```
                                PBIC: false
                                SRNI: false
                                S6AF: false
                                S4AF: false
                                MBMDT: false
                                ISRAU: false
                                CCRSI: false
                                CPRAI: false
                                ARRL: false
                                PPOF: false
                                PPON_PPEI: false
                                PPSI: false
                                CSFBI: false
                                CLII: false
                                CPSR: false
                                NSI: false
                                UASI: false
                                DTCI: false
                                BDWI: false
                                PSCI: false
                                PCRI: false
                                AOSI: false
                                AOPI: false
                                ROAAI: false
                                EPCOSI: false
                                CPOPCI: false
                                PMTSMI: false
                                S11TF: false
                                PNSI: false
                                UNACCSI: false
                                WPMSI: false
                                5GSIWK: false
                                EEVRSI: false
                                LTEMUI: false
                                LTEMPI: false
                                ENBCRSI: false
                                TSPCMI: false
                                PGBK: false
                                PCPSI: false
                                PCP: false
                                PCPU: false
                                N26_5GS: false
                                RI_5GCN: false
                                RS_5GCN: false
-------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2020/09/25 05:22:36.739932
      Message: GtpEpDecodeRPCResponse
      Description:  2075
      Source:
      Destination:
      PAYLOAD:

-------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2020/09/25 05:22:36.739932
      Message: GtpEpDecodeRPCIPCResponse
      Description:  2075
      Source:
      Destination:
      PAYLOAD:
```

```
-------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.405954
      Message: GtpEpDecodeRPCResponse
      Description:  2075
      Source:
      Destination:
      PAYLOAD:

-------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.406211
      Message: S5 S8 Modify Bearer Response
      Description: S5 S8 Modify Bearer Response Message
      Source: 10.1.2.154
      Destination: 10.1.2.156
      PAYLOAD:
        S5 S8 Modify Bearer Response:
            S5 S8 Modify Bearer Response:
                Version: 2
                Pflag: false
                TEIDflag: true
                MsgPriority: false
                MsgLength: 19
                TIED: 1375731839
                Seq: 131539
                MsgTypeId: 35
                MsgPriorityValue: 0
                Peer_IPv4_Flag: false
                Peer_IPv6_Flag: false
                MetaData: From:10.1.2.154:0->To:10.1.2.156:0
                Seid: 0
                Rseid: 0
                Cmnid: 0
                MsgType:
                    Modify_Bearer_Response:
                        Recovery:
                            Value: 100
                        Cause:
                            Cause_Value: 16
                            PCE: false
                            BCE: false
                            OrigInd: false

-------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.353146
      Message: S11 Modify Bearer Request
      Description: S11 Modify Bearer Request Message
      Source: 10.1.2.155
      Destination: 10.1.2.156
      PAYLOAD:
        S11 Modify Bearer Request:
            S11 Modify Bearer Request:
                Version: 2
                Pflag: false
                TEIDflag: true
                MsgPriority: false
                MsgLength: 48
                TIED: 301990015
```

```
Seq: 512
MsgTypeId: 34
MsgPriorityValue: 0
Peer_IPv4_Flag: false
Peer_IPv6_Flag: false
MetaData: From:10.1.2.155:2123->To:10.1.2.156:2123
Seid: 0
Rseid: 0
Cmnid: 0
MsgType:
    Modify_Bearer_Request:
        RAT_Type:
            Value: 6
        Indication:
            DAF: false
            DTF: false
            HI: true
            DFI: false
            OI: false
            ISRSI: false
            ISRAI: false
            SGWCI: false
            SQCI: false
            UIMSI: false
            CFSI: false
            CRSI: false
            P: false
            PT: false
            SI: false
            MSV: false
            RetLoc: false
            PBIC: false
            SRNI: false
            S6AF: false
            S4AF: false
            MBMDT: false
            ISRAU: false
            CCRSI: false
            CPRAI: false
            ARRL: false
            PPOF: false
            PPON_PPEI: false
            PPSI: false
            CSFBI: false
            CLII: false
            CPSR: false
            NSI: false
            UASI: false
            DTCI: false
            BDWI: false
            PSCI: false
            PCRI: false
            AOSI: false
            AOPI: false
            ROAAI: false
            EPCOSI: false
            CPOPCI: false
            PMTSMI: false
            S11TF: false
            PNSI: false
            UNACCSI: false
            WPMSI: false
            5GSIWK: false
            EEVRSI: false
```

```
                                LTEMUI: false
                                LTEMPI: false
                                ENBCRSI: false
                                TSPCMI: false
                                PGBK: false
                                PCPSI: false
                                PCP: false
                                PCPU: false
                                N26_5GS: false
                                RI_5GCN: false
                                RS_5GCN: false
                            FQ_TEID:
                            Bearer_Context_List:
                                NumBearerCtxt: 1
                                PbBearerCxt:
                                    PbBearerCxt[0]:
                                        BearerCtxType: 0
                                        EBI: 5
                                        Fqteid:
                                            ENbData:
                                                IFace: 0
                                                TEID: 2289
                                                IPv4: 10.1.2.155

-------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.412402
      Message: GtpEpDecodeRPCResponse
      Description:  258
      Source:
      Destination:
      PAYLOAD:

-------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.412598
      Message: GtpEpDecodeRPCResponse
      Description:  258
      Source:
      Destination:
      PAYLOAD:

-------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.412852
      Message: S11 Modify Bearer Response
      Description: S11 Modify Bearer Response Message
      Source: 10.1.2.156
      Destination: 10.1.2.155
      PAYLOAD:
        S11 Modify Bearer Response:
            S11 Modify Bearer Response:
                Version: 2
                Pflag: false
                TEIDflag: true
                MsgPriority: false
                MsgLength: 42
                TIED: 2286
                Seq: 512
                MsgTypeId: 35
                MsgPriorityValue: 0
```

```
                    Peer_IPv4_Flag: false
                    Peer_IPv6_Flag: false
                    MetaData: From:10.1.2.156:2123->To:10.1.2.155:2123
                    Seid: 0
                    Rseid: 0
                    Cmnid: 0
                    MsgType:
                        Modify_Bearer_Response:
                            Cause:
                                Cause_Value: 16
                                PCE: false
                                BCE: false
                                OrigInd: false
                            Bearer_Context_List:
                                NumBearerCtxt: 1
                                PbBearerCxt:
                                    PbBearerCxt[0]:
                                        BearerCtxType: 0
                                        EBI: 5
                                        Cause:
                                            Cause_Value: 16
                                            PCE: false
                                            BCE: false
                                            OrigInd: false
                                        Fqteid:
                                            SgwData:
                                                IFace: 1
                                                TEID: 2288
                                                IPv4: 1.1.1.83

-------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:47.412930
      Message: S11 Modify Bearer Response
      Description: S11 Modify Bearer Response Message
      Source: 10.1.2.156
      Destination: 10.1.2.155
      PAYLOAD:
        S11 Modify Bearer Response:
            S11 Modify Bearer Response:
                Version: 2
                Pflag: false
                TEIDflag: true
                MsgPriority: false
                MsgLength: 42
                TIED: 2286
                Seq: 512
                MsgTypeId: 35
                MsgPriorityValue: 0
                Peer_IPv4_Flag: false
                Peer_IPv6_Flag: false
                MetaData: From:10.1.2.156:2123->To:10.1.2.155:2123
                Seid: 0
                Rseid: 0
                Cmnid: 0
                MsgType:
                    Modify_Bearer_Response:
                        Cause:
                            Cause_Value: 16
                            PCE: false
                            BCE: false
                            OrigInd: false
                        Bearer_Context_List:
```

```
                                NumBearerCtxt: 1
                                PbBearerCxt:
                                    PbBearerCxt[0]:
                                        BearerCtxType: 0
                                        EBI: 5
                                        Cause:
                                            Cause_Value: 16
                                            PCE: false
                                            BCE: false
                                            OrigInd: false
                                        Fqteid:
                                            SgwData:
                                                IFace: 1
                                                TEID: 2288
                                                IPv4: 1.1.1.83

-------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:42:57.590559
      Message: Sx Session Modification Request
      Description: Sx Session Modification Request Message from SGWC to SGWU
      Source: 10.1.2.156
      Destination: 10.1.2.155
      PAYLOAD:
        Sx Session Modification Request:
            Sx Session Modification Request:
                UpdateFar:
                    UpdateFar[0]:
                        FarId: 1
                        ApplyAction:
                            Drop: false
                            Frwd: true
                            Buff: false
                            Nocp: false
                            Dupl: true
                            Valid: true
                        UpdateFwdParams:
                            DestIf: ACCESS
                            RedirectInfo:
                                AddrType: 0
                                Valid: false
                            OuterHdr:
                                OuterHdrDesc: 256
                                Teid: 2289
                                IPv4Address: 10.1.2.155
                                Port: 0
                                Valid: true
                            TEndptId: 0
                            OuterPktTos: 0
                            InnerPktTos: 0
                            TosOpt:
                                CopyInner: false
                                CopyOuter: false
                            SendTos: 0
                            PfcpSmFlags:
                                Drobu: false
                                Qaurr: false
                                Sndem: false
                                Valid: false
                            Valid: true
                            NextHopId: 0
                        UpdateDuplParams:
                            DestIf: LI
```

```
            OuterHdr:
                OuterHdrDesc: 1024
                Teid: 2289
                IPv4Address: 10.1.2.155
                Port: 9900
                Valid: true
            InterceptInfo:
                InterceptId: 1
                ChargingId: 303174163
                Licontext: LI
                SmfLiNodeId:
                    IpDesc: 0
                    IPv4Address: 10.1.2.156
                    Valid: true
                PduSessionId: 5
                Valid: true
            Valid: true
        BarId: 0
    UpdateFar[1]:
        FarId: 2
        ApplyAction:
            Drop: false
            Frwd: true
            Buff: false
            Nocp: false
            Dupl: true
            Valid: true
        UpdateFwdParams:
            DestIf: ACCESS
            RedirectInfo:
                AddrType: 0
                Valid: false
            OuterHdr:
                OuterHdrDesc: 256
                Teid: 1886
                IPv4Address: 10.1.2.154
                Port: 0
                Valid: true
            TEndptId: 0
            OuterPktTos: 0
            InnerPktTos: 0
            TosOpt:
                CopyInner: false
                CopyOuter: false
            SendTos: 0
            PfcpSmFlags:
                Drobu: false
                Qaurr: false
                Sndem: false
                Valid: false
            Valid: true
            NextHopId: 0
        UpdateDuplParams:
            DestIf: LI
            OuterHdr:
                OuterHdrDesc: 1024
                Teid: 1886
                IPv4Address: 10.1.2.155
                Port: 9900
                Valid: true
            InterceptInfo:
                InterceptId: 1
                ChargingId: 303174163
                Licontext: LI
```

```
                                    SmfLiNodeId:
                                        IpDesc: 0
                                        IPv4Address: 10.1.2.156
                                        Valid: true
                                    PduSessionId: 5
                                    Valid: true
                                Valid: true
                            BarId: 0
                        UplaneInacTimer: 0
                        MetaData: From:10.1.2.156:13002->To:10.1.2.155:8805
                        Supi: 123456789012348
                        Seid: 1297037239519281279
                        Seqno: 919
                        Version: 0
                        MsgPriority: false
                        MsgPriorityVal: 0
                        Cmnid: 0
                        Rseid: 10002
                        IntfType: 0
                        HdrLen: 0
                        MsgLen: 0
                        PfcpSmFlags:
                            Drobu: false
                            Qaurr: false
                            Sndem: false
                            Valid: false
                        UserIDInfo:
                            Valid: false
                        XHeaderInfo:
                            RatType:
                            Valid: false
                        CfPolicyId:
                            PolicyId: 0
                            Valid: false
                        GyStatus:
                            Valid: false
                            Value: false
                        ChargingDisabled:
                            Valid: false
                            Value: false
                        QueryInterface:
                            Valid: false
                            OfflineUrr: false
                            OnlineUrr: false
                            RadiusUrr: false
                            BearerUrr: false
                            SessUrr: false

-------------------------------------------------

      Subscriber Id: imsi-123456789012348
      Timestamp: 2021/06/06 06:43:00.597025
      Message: Sx Session Modification Response
      Description: Sx Session Modification Response Message from SGWU to SGWC
      Source: 10.1.2.155
      Destination: 10.1.2.156
      PAYLOAD:
        Sx Session Modification Response:
            Sx Session Modification Response:
                Cause: 1
                OffendingIe: 0
                LoadControlInfo:
                    SeqNum: 0
                    Metric: 0
```

```
                    Valid: false
                OverloadControlInfo:
                    SeqNum: 0
                    Metric: 0
                    Ociflag: 0
                    Valid: false
                MetaData: From:10.1.2.155:8805->To:10.1.2.156:13002
                Supi:
                Seid: 1297037239519281279
                Seqno: 919
                Version: 1
                MsgPriority: false
                MsgPriorityVal: 0
                Cmnid: 0
                Rseid: 0
                IntfType: 0
                HdrLen: 17
                MsgLen: 0

-------------------------------------------------

command terminated with exit code 124
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   222  100    35  100   187   7000  37400 --:--:-- --:--:-- --:--:-- 44400
Stop Response Disabled mon_sub as part of timeout for Cmd: --header
Content-type:application/json --request POST --data
{"command":"mon_sub","parameters":{"supi":"imsi-*","duration":30,"enableDiag":false,"enableInternalMsg":false,"action":"stop","namespace":"sgw","nf-service":"none","gInstance":0}}
 http://oam-pod:8879/commands
```

Limitation

When the monitor subscriber is run for extended duration, the `.sorted` file stores messages only for the 1024 messages.

Configuring the Transaction Messages

To configure the transaction logs, use the following configuration:

```
config
   logging transaction message [ disable | enable ]
   end
```

NOTES:

- **logging transaction message [disable | enable]**—Configure the messages in transaction logging. When set to enable, the transactional and internal logs are combined. By default, the logs are disabled.

Configuring the Monitor Protocol

To configure this feature, use the following configuration:

```
exec
   monitor protocol interface interface
      capture-duration capture_duration
      pcap [ Yes | No ]
```

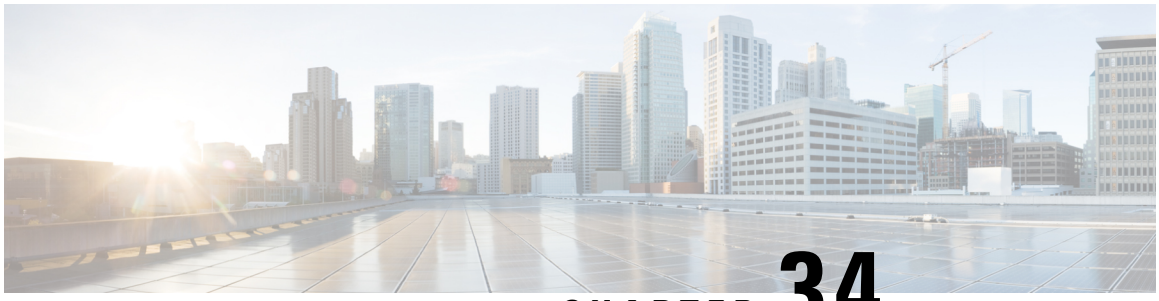
```
gr-instance gr_instance
end
```

NOTES:

- **monitor protocol interface** *interface*—Specify the interface on which PCAP is captured. For example, sbi, pfcp, gtpu, gtpc, gtp, and radius.
- **capture-duration** *capture_duration*—Specify the duration in seconds during which PCAP is captured. The default value is 300 seconds.
- **pcap [Yes | No]** —Configures the PCAP file generation. By default, the pcap feature is disabled.
- **gr-instance** *gr_instance*—Specify the GR instance that the cnSGW-C monitors the subscriber for.

Note If the GTP endpoint IPs are the same on S5e and S11 interfaces, the protocol output is inconsistent and displays S11 for the S5 interface on which the message is received. The following is a sample of an endpoint configuration:

```
instance instance-id 1 endpoint gtp replicas 3 interface s5e vip-ip 209.165.201.22
instance instance-id 1 endpoint gtp replicas 3 interface s11 vip-ip 209.165.201.22
```



CHAPTER 34

Multiple PDN Attach or Detach Procedures

Feature Summary and Revision History

Summary Data

Table 141: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 142: Revision History

Revision Details	Release
First introduced.	2020.03.0

Feature Description

cnSGW-C handles the following functionalities:

- UE-requested PDN connection
- UE-requested PDN disconnection

- PGW-initiated PDN disconnection
- Admin-initiated disconnection.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

UE-requested PDN Connection Call Flow

This section describes the UE-requested PDN connection call flow.

Figure 77: UE-requested PDN Connection Call Flow

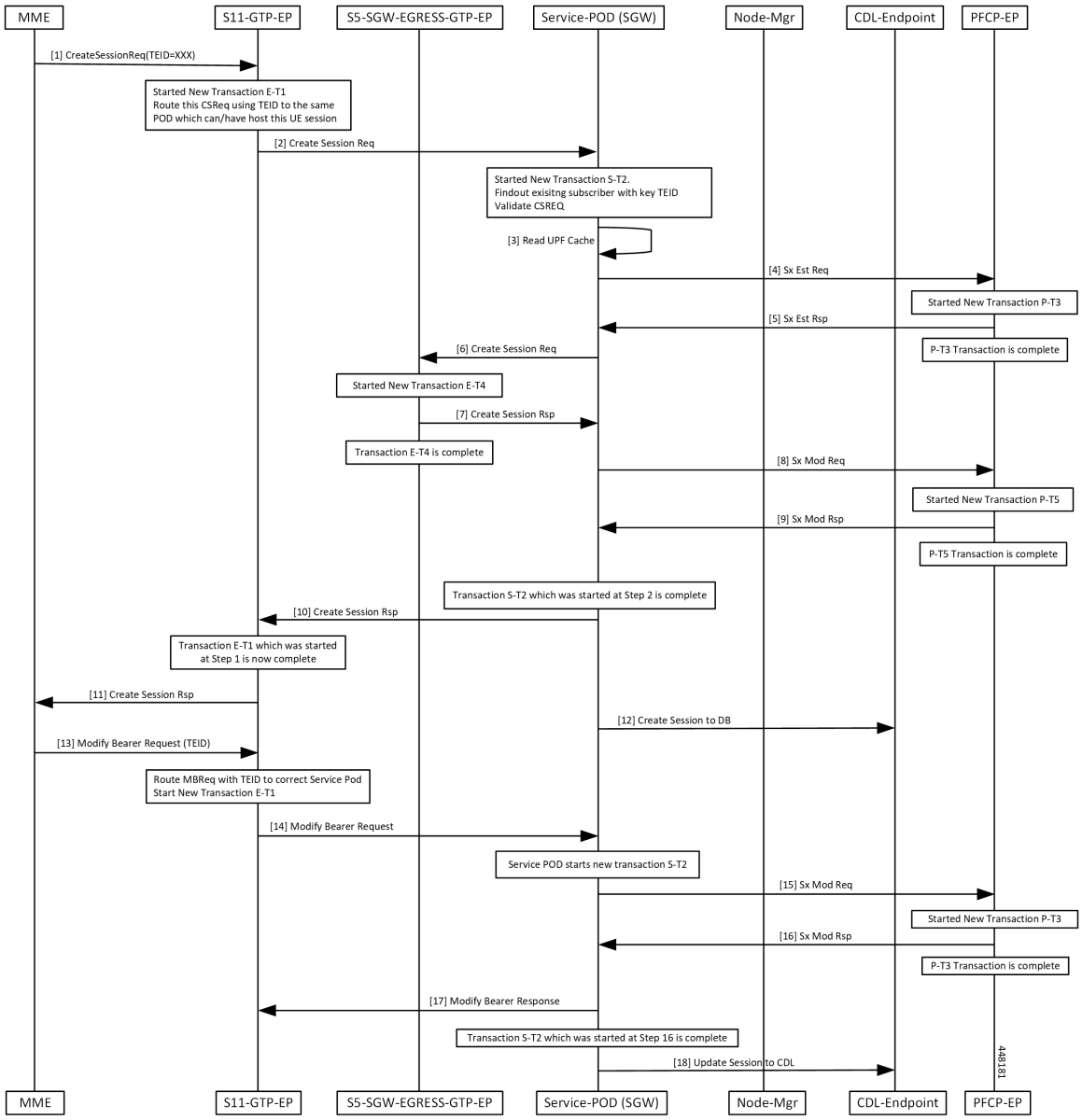


Table 143: UE-requested PDN Connection Call Flow Description

Step	Description
1	The MME sends the Create Session Request for a new PDN connection to the S11-GTP-EP with a nonzero TEID.

Step	Description
2	The E-T1 transaction is started. The S11-GTP-EP decodes the received UDP message and converts the message into the gGRPC message. Based on the IMSI value, the message is forwarded to the respective SGW-service pod which handles the UE session. The SGW-service pod receives the Create Session Request from the S11-GTP-EP.
3	The S-T2 transaction is started. The SGW-service pod finds the subscriber context based on the local ingress TEID, and validates the Create Session Request content and updates the PDN and subscriber information. The SGW-service pod reads the UPF cache to provide the selected UPF.
4	The SGW-service pod sends the Sx Establishment Request to the PFCP-EP.
5	The P-T3 transaction is started. The PFCP-EP sends the Sx Establishment Response to the SGW-service pod.
6	The P-T3 transaction is completed. The SGW-service pod sends the Create Session Request to the S5-SGW-EGRESS-GTP-EP with S11-U and S5-U TEID details.
7	The E-T4 transaction is started. The Create Session Response is validated and the S5-U remote TEID is updated in the PDN. The S5-SGW-EGRESS-GTP-EP sends the Create Session response to the SGW-service pod.
8	The E-T4 transaction is completed. The SGW-service pod sends the Sx Modify Request to the PFCP-EP.
9	The P-T5 transaction is started. The PFCP-EP sends the Sx Modify Response to the SGW-service pod on expiry of the timer T5.
10	The P-T5 and S-T2 transaction is completed. The GTP-EP receives the Create Session Response from the SGW-service pod.
11	The E-T1 transaction is completed. The MME receives the Create Session Response from the S11-GTP-EP.
12	The SGW-service pod updates the created session in CDL endpoint (database) with new PDN information.
13	The MME sends the Modify Bearer Request with TEID to the S11-GTP-EP.
14	The E-T1 transaction is started. The S11-GTP-EP routes the Modify Bearer Request to the SGW-service pod. The S11-GTP-EP sends the Modify Bearer Request to the SGW-service pod.

Step	Description
15	The S-T2 transaction is started. The SGW-service pod sends the Sx Modify Request to the PFCP-EP pod on expiry of the timer S-T2.
16	The P-T3 transaction is started. The PFCP-EP sends the Sx Modify Response to the SGW-service pod on expiry of the timer T3.
17	R-T3 transaction is completed. The SGW-service pod sends the Modify Bearer Response to the MME.
18	S-T2 transaction is completed The SGW-service pod sends the update session to the CDL endpoint.

UE-requested or the MME-requested PDN Disconnection Call Flow

This section describes the UE or the MME-requested PDN disconnection call flow.

Figure 78: UE-requested or the MME-requested PDN Disconnection Call Flow

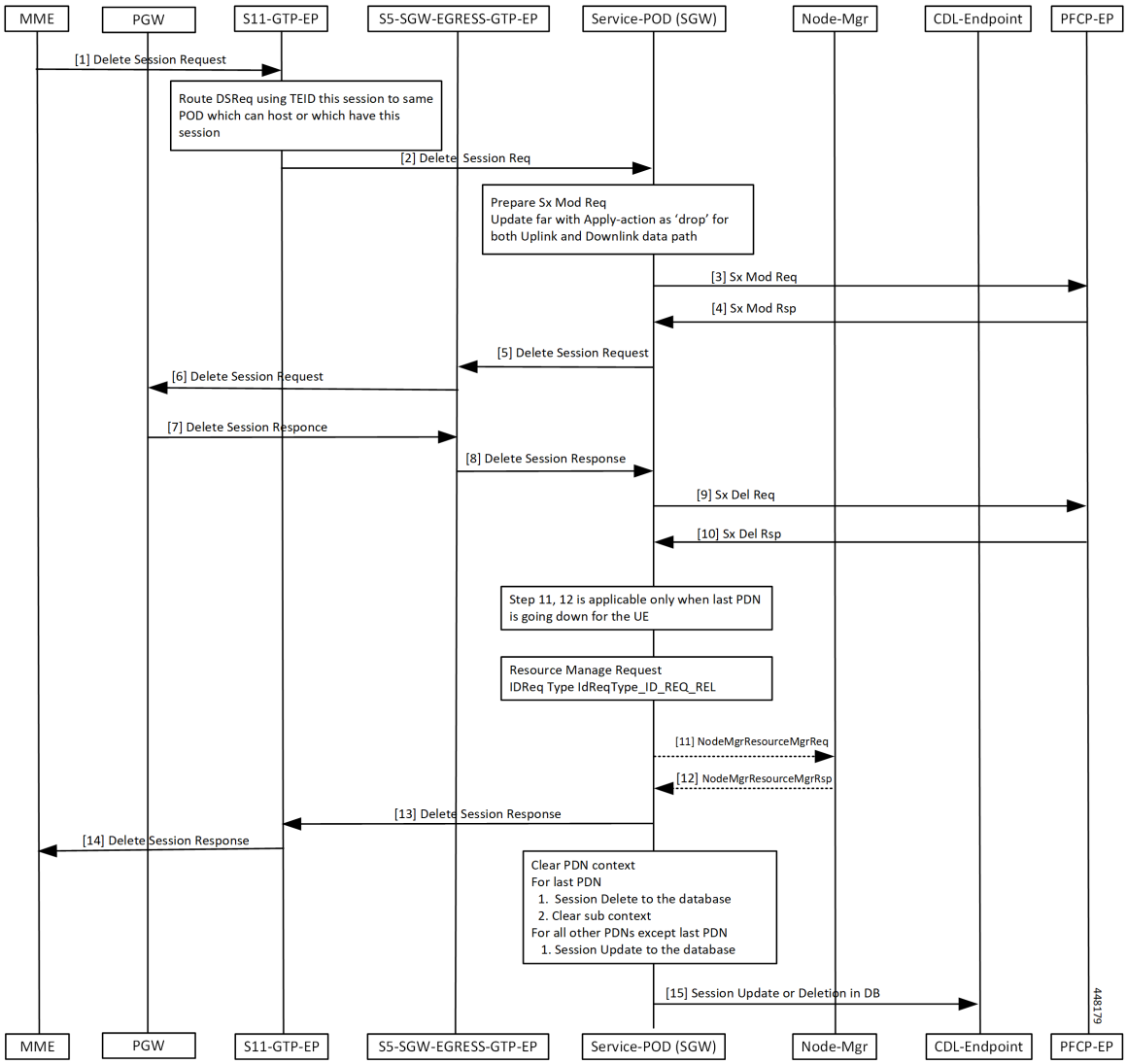


Table 144: UE-requested or the MME-requested PDN Disconnection Call Flow Description

Step	Description
1	The MME sends the Delete Session Request to the S11-GTP-EP for other PDN disconnection.
2	The GTP-EP decodes the received UDP message and converts the message into the gRPC message. Based on the TEID value, the gRPC message is forwarded to the SGW-service pod which can handle the UE session.
3	The SGW-service pod finds the subscriber context information as per the local ingress TEID. The SGW-service pod validates the Delete Session Request content. The SGW-service pod sends the Sx Modify Request to the PFCP-EP with apply action as DROP to drop the uplink or downlink packets at the SGW-U.

Step	Description
4	The PFCP-EP sends the Sx Modify Response to the SGW-service pod.
5	The SGW-service pod forwards the Delete Session Request to the S5-SGW-EGRESS-GTP-EP.
6	The S5-SGW-EGRESS-GTP-EP forwards the Delete Session Request to the PGW through the UDP proxy.
7	The PGW sends the Delete Session Response to the S5-SGW-EGRESS-GTP-EP.
8	The S5-SGW-EGRESS-GTP-EP forwards the Delete Session Response to the SGW-service pod.
9	The SGW-service pod validates the Delete Session Response, and sends the Sx Delete Request to the PFCP-EP.
10	The SGW-service pod receives the Sx Delete Session Response from the PFCP-EP.
11	For the last PDN, the SGW-service pod sends the NodeMgrResourceManager Request for the ID release to the NodeManager.
12	The Node Manager releasees the ID and sends the acknowledgment to the SGW-service pod.
13	The SGW-service pod sends the Delete Session Response to the S11-GTP-EP.
14	The S11-GTP-EP forwards the Delete Session Response to the MME.
15	The SGW-service pod • Updates the session in database for the delete PDN information for other than the last PDN • Sends the delete session message to the database for the last PDN

PGW-requested Disconnection Call Flow

This section describes the PGW-requested disconnection call flow.

Figure 79: PGW-requested Disconnection Call Flow

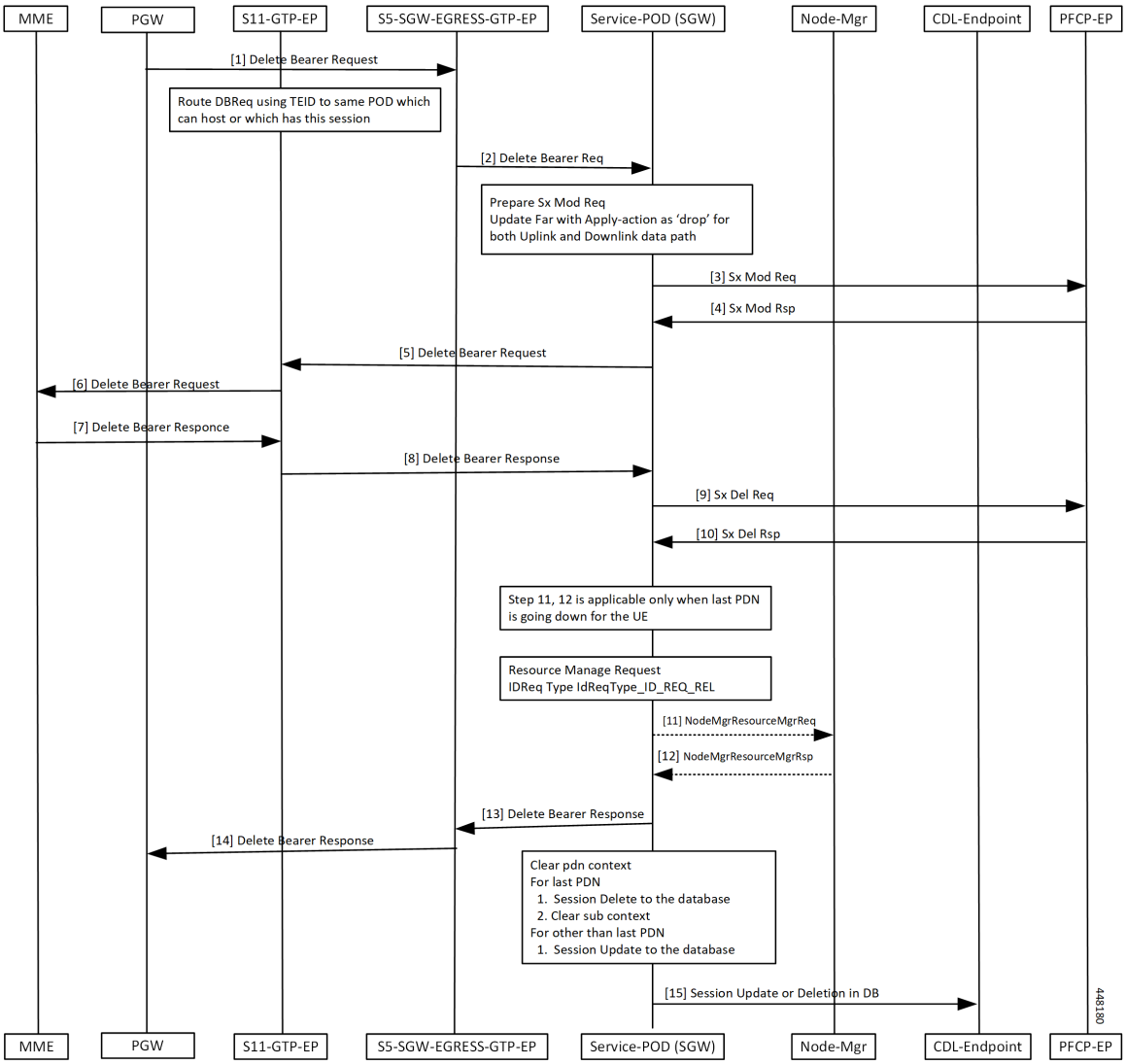
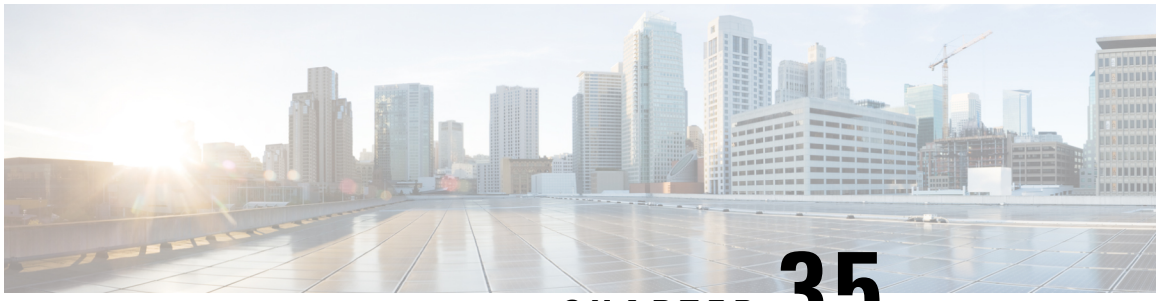


Table 145: PGW-requested Disconnection Call Flow Description

Step	Description
1	The PGW sends the Delete Bearer Request to the S11-GTP-EP for other PDN disconnection.
2	The GTP-EP decodes the received UDP message and converts the message into the gRPC message. Based on the TEID value, the gRPC message is forwarded to the SGW-service pod which can handle the UE session.
3	The SGW-service pod finds the subscriber context information as per the local ingress TEID. The SGW-service pod validates the Delete Bearer Request content. The SGW-service pod sends the Sx Modify Request to the PFCP-EP with apply action as DROP to drop the uplink or downlink packets at the SGW-U.

Step	Description
4	The PFCP-EP sends the Sx Modify Response to the SGW-service pod.
5	The SGW-service pod forwards the Delete Bearer Request to the S5-SGW-EGRESS-GTP-EP.
6	The S5-SGW-EGRESS-GTP-EP forwards the Delete Bearer Request to the PGW through the UDP proxy.
7	The PGW sends the Delete Bearer Response to the S5-SGW-EGRESS-GTP-EP.
8	The S5-SGW-EGRESS-GTP-EP forwards the Delete Bearer Response to the SGW-service pod.
9	The SGW-service pod validates the Delete Bearer Response, and sends the Sx Delete Request to the PFCP-EP.
10	The SGW-service pod receives the Sx Delete Bearer Response from the PFCP-EP.
11	For the last PDN, the SGW-service pod sends the NodeMgrResourceManager Request for the ID release to the NodeManager.
12	The Node Manager releasees the ID and sends the acknowledgment to the SGW-service pod.
13	The SGW-service pod sends the Delete Bearer Response to the S11-GTP-EP.
14	The S11-GTP-EP forwards the Delete Bearer Response to the MME.
15	The SGW-service pod • Updates the Bearer in database for the delete PDN information for other than the last PDN • Sends the delete Bearer message to the database for the last PDN



CHAPTER 35

Service Configuration Enhancements

Feature Summary and Revision History

Summary Data

Table 146: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 147: Revision History

Revision Details	Release
First introduced	2020.01.0

Feature Description

cnSGW-C supports Subscriber Map and Operator Policy configurations.

SGW profile represents SGW-service or node. The operator policy is decided based on subscriber policy association.

Feature Configuration

Configuring this feature involves the following steps:

- SGW profile. For more information, see Configuring the SGW Profile, on page 368.
- Subscriber policy. For more information, see Configuring the Subscriber Policy, on page 369.
- Operator policy. For more information, see Configuring the Operator Policy, on page 370.
- Policy DNN. For more information, see Configuring the Policy DNN, on page 370.

Configuring the SGW Profile

To configure this feature, use the following configuration:

```
config
   profile sgw sgw_name
      locality locality_code
      fqdn dnn_name
      subscriber-policy policy_name
      end
```

NOTES:

- **locality** *locality_code*—Specify the locality code. Must be a string.
- **fqdn** *dnn_name*—Specify the cnSGW-C FQDN.
- **subscriber-policy** *policy_name*—Specify the subscriber policy name. Must be a string.

Configuration Example

The following is an example configuration.

```
config
   profile sgw sgw-data
      locality LOC1
      fqdn 209.165.200.254
      subscriber-policy subpol1
      end
```

Configuration Verification

To verify the configuration:

```
show running-config profile sgw
profile sgw sgw-data
locality LOC1
fqdn 209.165.200.254
subscriber-policy subpol1
```

Configuring the Subscriber Policy

Note The maximum number of supported subscriber map profiles is 64.

To configure this feature, use the following configuration:

```
config
   policy subscriber subscriber_name
      precedence precedence_value
         imsi
            mcc mcc_value
            mnc mnc_value
            msin first_value last_value
         serving-plmn
            mcc mcc_value
            mnc mnc_value
         imsi-start-range range_value
         imsi-stop-range range_value
         supi-start-range range_value
         supi-stop-range range_value
         operator-policy policy_name
         end
```

Note All parameters are optional.

NOTES:

- **precedence** *precedence_value*—Specify the precedence for entry. Must be an integer in the range of 1-2048.
- **mcc** *mcc_value*—Specify the Mobile Country Code (MCC). Must be a three digit integer.
- **mnc** *mnc_value*—Specify the Mobile Network code (MNC). Must be a two or three digit integer.
- **msin** *first_value last_value*—Specify the mobile subscriber identification number (MSIN) range.

  first_value—Specify starting value of the MSIN range. Must be an integer in the range of 1-9999999999.

  last_value—Specify the ending value of the MSIN range. Must be an integer in the range of 1-9999999999.
- **operator-policy** *policy_name*—Specify the operator policy name. Must be a string.
- **imsi-start-range** *range_value*—Specify the IMSI start range. Must be an integer in the range of 100000000000000-9999999999999999.
- **imsi-stop-range** *range_value*—Specify the IMSI stop range. Must be an integer in the range of 100000000000000-9999999999999999.
- **supi-start-range** *range_value*—Specify the SUPI start range. Must be an integer in the range of 100000000000000-999999999999999.

- **supi-stop-range** *range_value*—Specify the SUPI stop range. Must be an integer in the range of 100000000000000-999999999999999.

Configuration Example

The following is an example configuration.

```
config
   policy subscriber sub1
      precedence 2
         imsi mcc 123 mnc 456
         imsi msin first 99 last 100
      serving-plmn mcc 404 mnc 678
      supi-start-range 100000000000001
      supi-stop-range  199999999999999
      imsi-start-range 200000000000001
      imsi-stop-range  299999999999999
      operator-policy op1
      end
```

Configuring the Operator Policy

Note The maximum number of supported operator policy profiles is 1000.

To configure this feature, use the following configuration:

```
config
  policy operator operator_name
  policy dnn dnn_policy_name
  end
```

NOTES:

- **policy operator** *operator_name*—Specify the operator policy name. Must be a string.
- **policy dnn** *dnn_policy_name*—Specify the DNN policy name. Must be a string.

Configuration Example

The following is an example configuration.

```
config
   policy operator op1
   policy dnn pol1
   end
```

Configuring the Policy DNN

This section describes how to configure Policy DNN and adding it to cnSGW-C. The DNN support enables you to determine the exact APN profile as per the APN name, APN network-identifier and APN operator-identifier.

Note The maximum number of supported DNN policies is 1000.

To configure this feature, use the following configuration:

```
config
   policy dnn dnn_policy_name
       dnn dnn_name

          profile profile_name
       dnn network-identifier network_identifier_name operator-identifier
operator_identifier_name profile profile_name
       dnn operator-identifier operator_identifier_name profile profile_name
       dnn operator-identifier profile profile_name
       end
```

NOTES:

- **dnn** *dnn_name*—Specify the DNN name.
- **network-identifier** *network_identifier_name*—Specify the network identifier. Must be a string.
- **profile** *profile_name*—Specify the profile name. Must be a string.
- **operator-identifier** *operator_identifier_name*—Specify the operator identifier. Must be a string.
- **profile** *default_dnn_profile*—Specify the default DNN profile name.

Note With present evaluation criteria, following is the matching order to select the associated profile:

- DNN
- NI+OI
- NI
- OI
- Default

Don’t configure overlapping criteria.

Configuration Example

The following is an example configuration.

```
config
   policy dnn polsub1
      dnn network-identifier ims profile ims1
      dnn network-identifier ims operator-identifier ims.com profile ims
      dnn network-identifier voice operator-identifier volte profile voiceprofile
      dnn operator-identifier data profile data-profile
   profile default-dnn-profile
   end
```

Configuration Modification Impact

This section describes the impact or behavior of configuration change on existing call, new PDN, or new subscriber.

Modification	cnSGW-C Existing Call	cnSGW-C New PDN or New subscriber
Define a new SGW-profile and delete the old profile (with or without the pod restart)	When the new transaction happens, the call gets loaded on cn-SGW-C from CDL. *Observation:* Change in the cnSGW-C profile configuration and termination of the call.	Rejects the new PDN and deletes the existing call. New subscriber uses new SGW profile.
Delete the subscriber map	No impact	Applies modified configuration for the following: • subscriber policy • operator policy • dnn policy • dnn profile
Modify the subscriber map in SGW-service	No impact	Applies modified configuration for the following: • subscriber policy • operator policy • dnn policy • dnn profile
Delete the operator policy	No impact	Applies modified configuration for the following: • subscriber policy • operator policy • dnn policy • dnn profile

Modification	cnSGW-C Existing Call	cnSGW-C New PDN or New subscriber
Add the deleted or new operator policy	No impact	Applies modified configuration for the following: • subscriber policy • operator policy • dnn policy • dnn profile
Modify the operator policy name in the subscriber map	No impact	Applies modified configuration for the following: • subscriber policy • operator policy • dnn policy • dnn profile

Troubleshooting Information

This section describes the troubleshooting information that enables you to resolve the service configuration issues.

Configuration Errors

This section describes the errors that cnSGW-C reports during the service configuration.

Subscriber Policy Configuration Errors

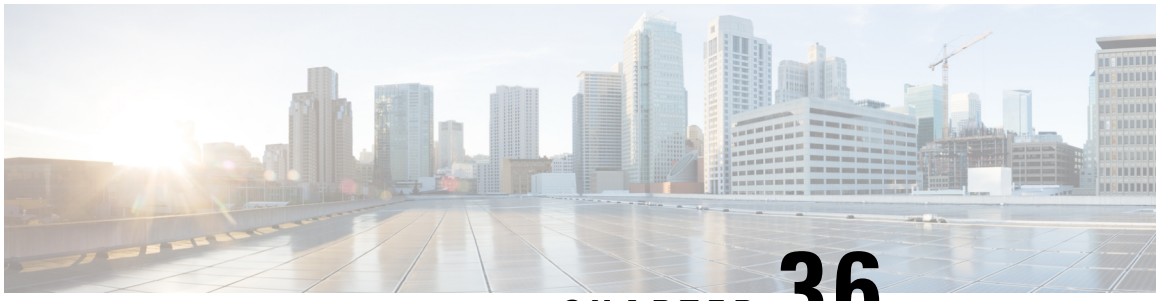
```
show config-error
ERROR
COMPONENT ERROR DESCRIPTION
------------------------------------------------------------------------
SGWProfile Subscriber policy name : polSubSgw in profile sgw1 is not configured
```

Operator Policy Configuration Errors

```
show config-error
ERROR COMPONENT ERROR DESCRIPTION
------------------------------------------------------------------------
SubscriberPolicy Operator policy : op2 under subscriber policy polSubSgw is not configured
```

DNN Policy Configuration Errors

```
show config-error
ERROR COMPONENT ERROR DESCRIPTION
------------------------------------------------------------------------
OperatorPolicy Dnn policy name : dnn_1 in operator policy op1 is not configured
```



CHAPTER 36

SGW Charging Support

Feature Summary and Revision History

Summary Data

Table 148: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 149: Revision History

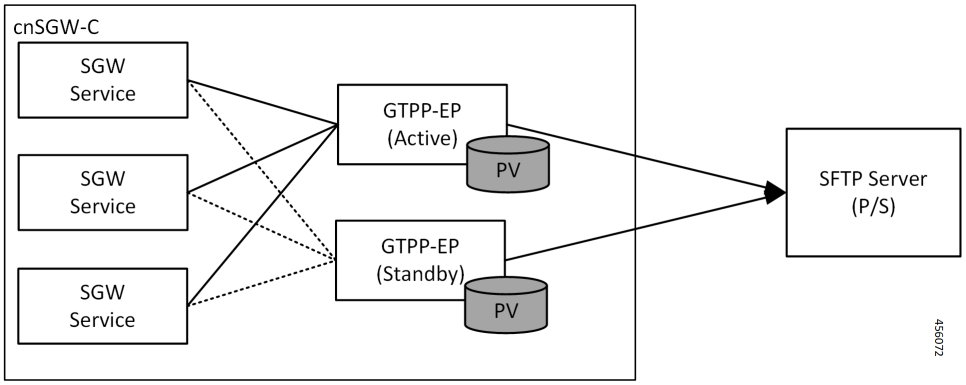
Revision Details	Release
First introduced.	2021.02.0

Feature Description

cnSGW-c supports the following:

- GTPP charging (Gz) interface
- Monitor subscriber for Charging Data Record (CDR)
- CDR dictionary: **custom24**
- Two custom file formats: **custom1** (default) and **custom5**
- One replica of GTPP-EP pod which is functional with active or standby mode (two pods get spawned when GTPP-EP pod configured with one instance)
- Writing CDR records to the local file system

Architecture



- GTP’ (GTP Prime) or GTPP-EP is the new endpoint pod and interfaces with mediation or CGF server over SFTP
- GTP’ attaches to the local disk (Persistent Volume). This attachment is with each server or virtual machine (VM)
- SGW-service generates CDRs and sends the records to the GTP' endpoint for the storage
- GTP' stores the CDRs in ASN.1 encoding in flat files in persistent storage
- GTP' pushes the flat files over SCTP towards the mediation server or CGF

The charging functionality is split into two parts.

- Accounting and CDR generation:
  - SGW-service generates usage reporting rule (URR) for each established bearer on the Sxa interface with SGW-U
  - SGW-service uses the reported usage information with the trigger event to generate accounting information
- CDR management and storage:
  - GTPP-EP microservice or K8 pod archives the CDRs and pushes the CDR files to the external storage server
  - GTPP-EP receives the proto-CDRs from SGW-service over the streaming GRPC IPC endpoint

- GTPP-EP encodes each received proto-CDR into ASN.1 format as specified in the dictionary (from CLI)
- The ASN.1 CDRs are written to flat files in the specified pattern as specified in the CLI configuration
- Transfers to the new CDR files to the configured external storage server using SFTP protocol periodically

Roaming Support

Roaming scenarios uses a Gz interface and offline accounting functions to match the CDR records with the foreign PGW.

The operator policy provides mechanisms to modify the behavior of subsets of subscribers described in the SGW profile. cnSGW-C supports call-control-profile under the operator-policy to control the accounting mode (enable or disable the charging) and define more charging configurations.

The default accounting mode is NONE which indicates charging is disabled.

The accounting mode value from the call control profile overrides the configured value in the SGW profile.

See the following configuration details:

- Call Control Profile Configuration
- Charging-Characteristics under Call-Control-Profile

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

URR Installation on Initial Attach Call Flow

This section describes URR Installation on Initial Attach call flow.

Figure 80: URR Installation on Initial Attach Call Flow

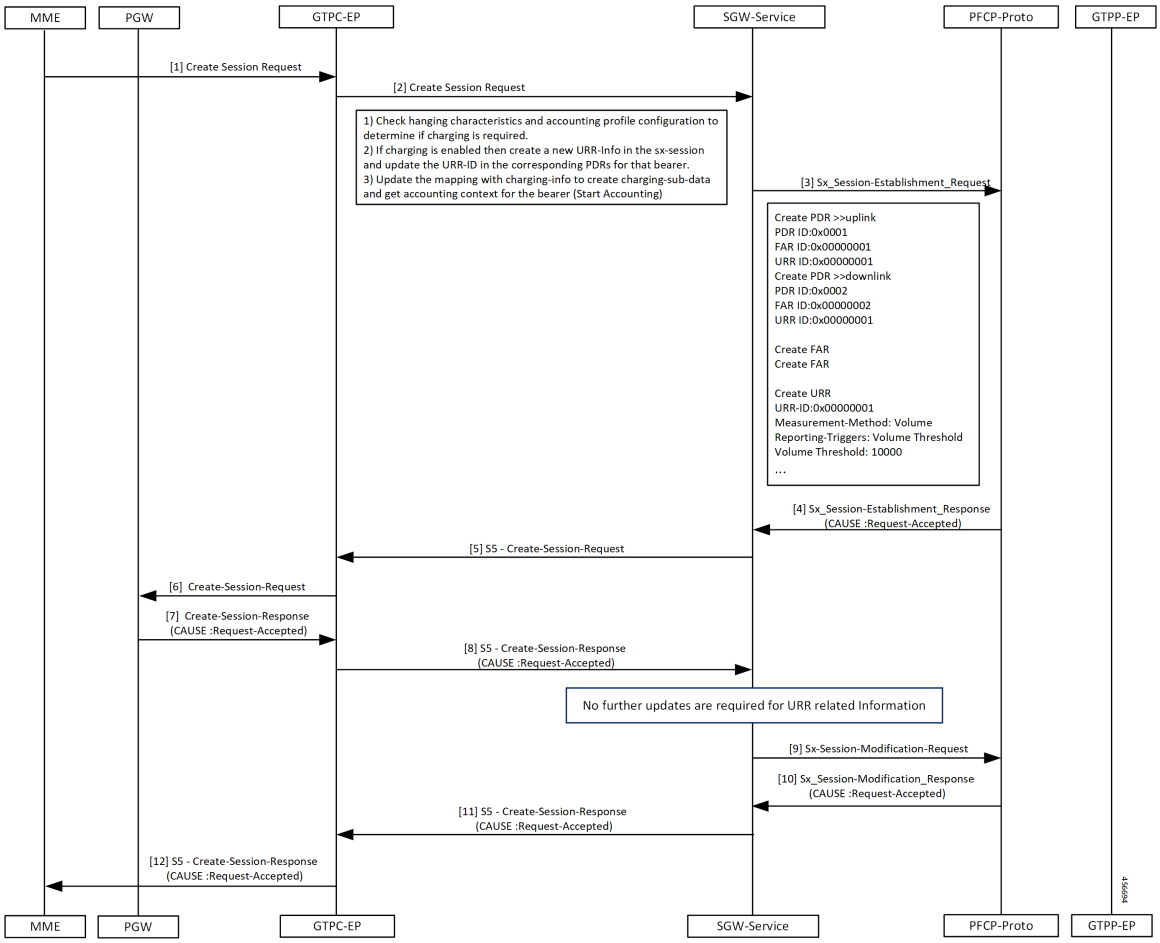


Table 150: URR Installation on Initial Attach Call Flow Description

Step	Description
1	The MME sends the Create Session Request to the GTPC-EP.
2	The GTPC-EP forwards the Create Session Request to the SGW-service pod.
3	The SGW-service pod sends the Sx Session Establishment Request to the PFCP proto
4	The PFCP proto sends the Sx Session Establishment Response to the SGW-service with the cause as Request-Accepted.
5	The SGW-service pod sends the S5 Create Session Request to the GTPC-EP.
6	The GTPC-EP sends the S5 Create Session Request to the PGW.
7	The PGW sends the Create Session Response to the GTPC-EP with the cause as Request-Accepted.
8	The GTPC-EP sends the S5 Create Session Response to the SGW-service with the cause as Request-Accepted.

Step	Description
9	The SGW-service pod sends the Sx Session Modification Request to the PFCP proto.
10	The SGW-service pod receives the Sx Session Modification Response from the PFCP proto with the cause as Request-Accepted.
11	The SGW-service pod sends the S5 Create Session Response to the GTPC-EP with the cause as Request-Accepted.
12	The GTPC-EP forwards the S5 Create Session Response to the MME with the cause as Request-Accepted.

SGW CDR Call Flow

This section describes the SGW CDR call flow.

Figure 81: SGW CDR Call Flow

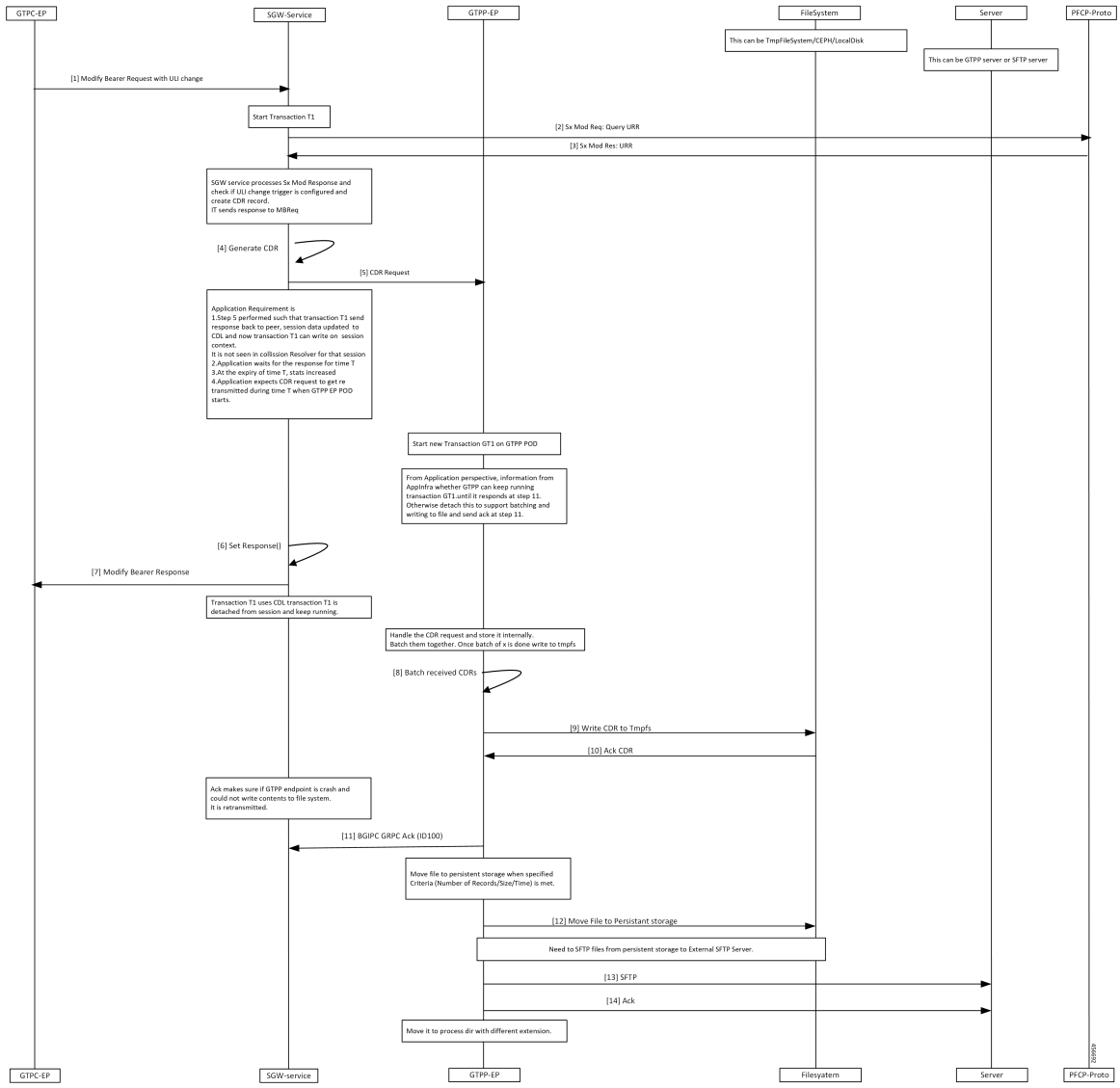


Table 151: SGW CDR Call Flow Description

Step	Description
1	The GTPC-EP sends the Modify Bearer Request with ULI to the SGW-service pod.
2	The SGW-service pod sends the Sx Mod Request with Query URR to the PFCP proto.
3	The SGW-service pod receives the Sx Mod Response with URR from the PFCP proto.
4	The SGW-service pod generate CDR.
5	The SGW-service pod sends the CDR request to the GTPP-EP.
6	The SGW-service pod triggers a set response () function.

Step	Description
7	The SGW-service pod sends the Modify Bearer Response to the GTPC-EP.
8	The GTPP-EP batches the received CDR requests .
9	The GTPP-EP sends the batched CDR requests to the TmpF5 file.
10	The GTPP-EP receives the CDR ACK from the file system.
11	The GTPP-EP sends GRPC ACK to the SGW-service.
12	The GTPP-EP moves the file to persistent storage when specified criteria (number of records or size or time) meets.
13	The GTPP-EP sends SFTP files from persistent storage to the server.
14	The GTPP-EP receives ACK from the server and moves it to the process directory with different extension.

URR Removal and CDR Reporting on Detach Call Flow

This section describes URR Removal and CDR Reporting on Detach call flow.

Figure 82: URR Removal and CDR Reporting on Detach Call Flow

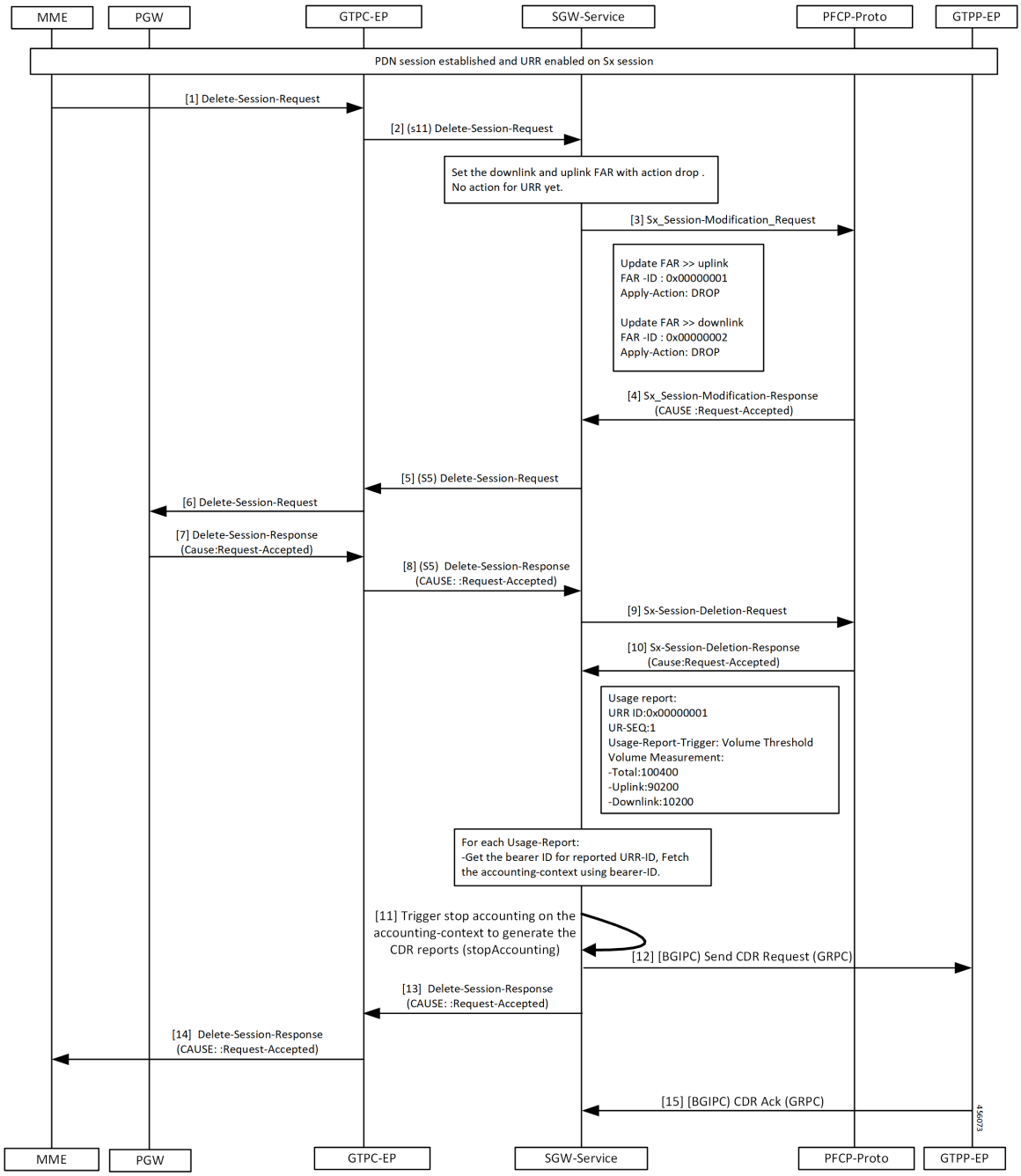


Table 152: URR Removal and CDR Reporting on Detach Call Flow Description

Step	Description
1	A PDN session is established and URR is enabled for Sx session. The MME sends the Delete Session Request to the GTPC-EP.

Step	Description
2	The GTPC-EP forwards the S11 Delete Bearer Request to the SGW-service pod.
3	The SGW-service pod sends the Sx Session Modification Request to the PFCP proto.
4	The PFCP proto sends the Sx Session Modification Response to the SGW-service pod with the cause as Request-Accepted.
5	The SGW-service pod sends the S5 Delete Session Request to the GTPC-EP.
6	The GTPC-EP sends the Delete Session Request to the PGW.
7	The PGW sends the Delete Session Response to the GTPC-EP with the cause as Request-Accepted.
8	The GTPC-EP sends the S5 Delete Session Response to the SGW-service pod with the cause as Request-Accepted.
9	The SGW-service pod sends the Sx Session Delete Request to the PFCP proto.
10	The SGW-service pod receives the Sx Session Delete Response from the PFCP proto with the cause as Request-Accepted.
11	The SGW-service pod triggers the CDR generation.
12	The SGW-service pod sends the CDR request to the GTPP-EP.
13	The SGW-service pod sends the Delete Session Response to the GTPC-EP with the cause as Request-Accepted.
14	The GTPC-EP pod forwards the Delete Session Response to the MME with the cause as Request-Accepted.
15	The GTPP-EP sends the CDR ACK to the SGW-service pod.

Usage Report on Hitting Threshold Call Flow

This section describes Usage Report on Hitting Threshold call flow.

Figure 83: Usage Report on Hitting Threshold Call Flow

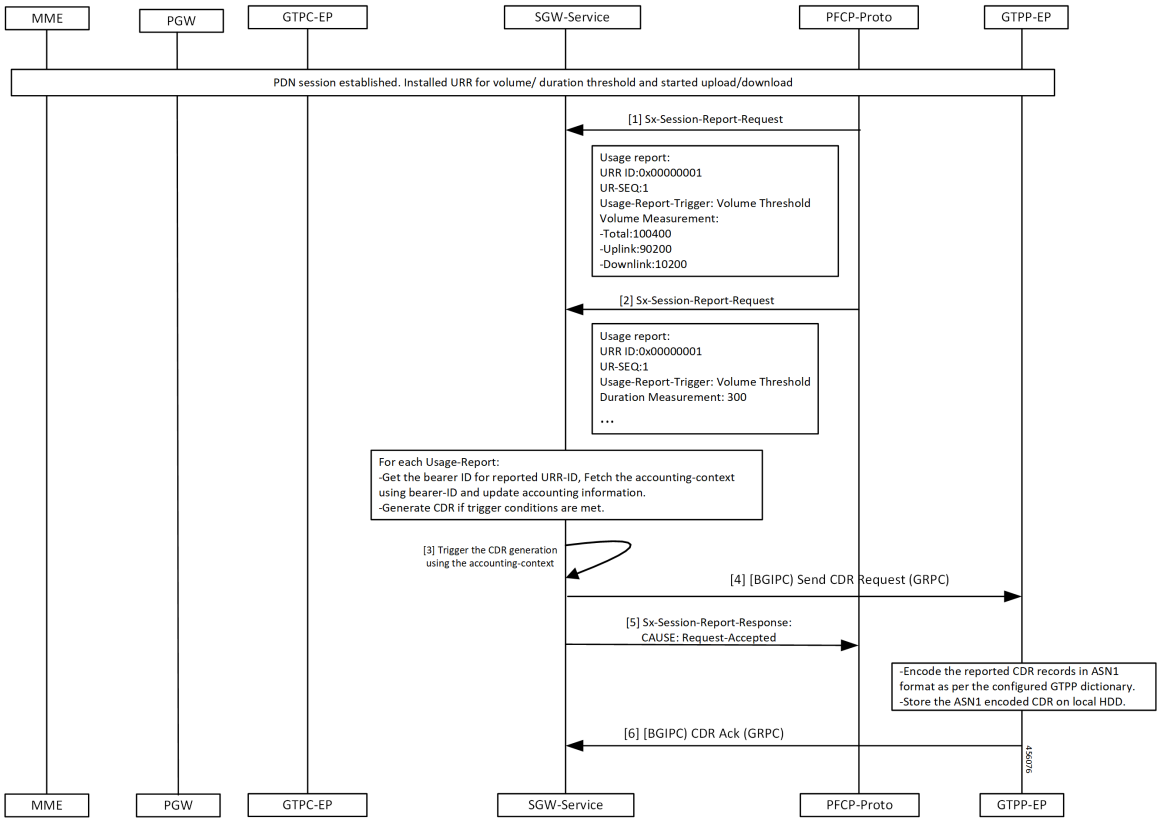


Table 153: Usage Report on Hitting Threshold Call Flow Description

Step	Description
1	Established a PDN session. Installed URR for the threshold duration. Trigger upload and download. The PFCP proto sends the Sx Session Report Request to the SGW-service pod.
2	The PFCP proto sends the Sx Session Report Request to the SGW-service pod until it reaches the threshold value of the User-plane.
3	The SGW-service pod triggers the CDR generation.
4	The SGW-service pod sends the CDR request to the GTPP-EP.
5	The SGW-service pod sends the Sx Session Report Response to the PFCP proto with the cause as Request-Accepted.
6	The GTPP-EP sends the CDR ACK to the SGW-service pod.

URR Installation for Dedicated Bearer Call Flow

This section describes the URR Installation for Dedicated Bearer call flow.

Figure 84: URR Installation for Dedicated Bearer Call Flow

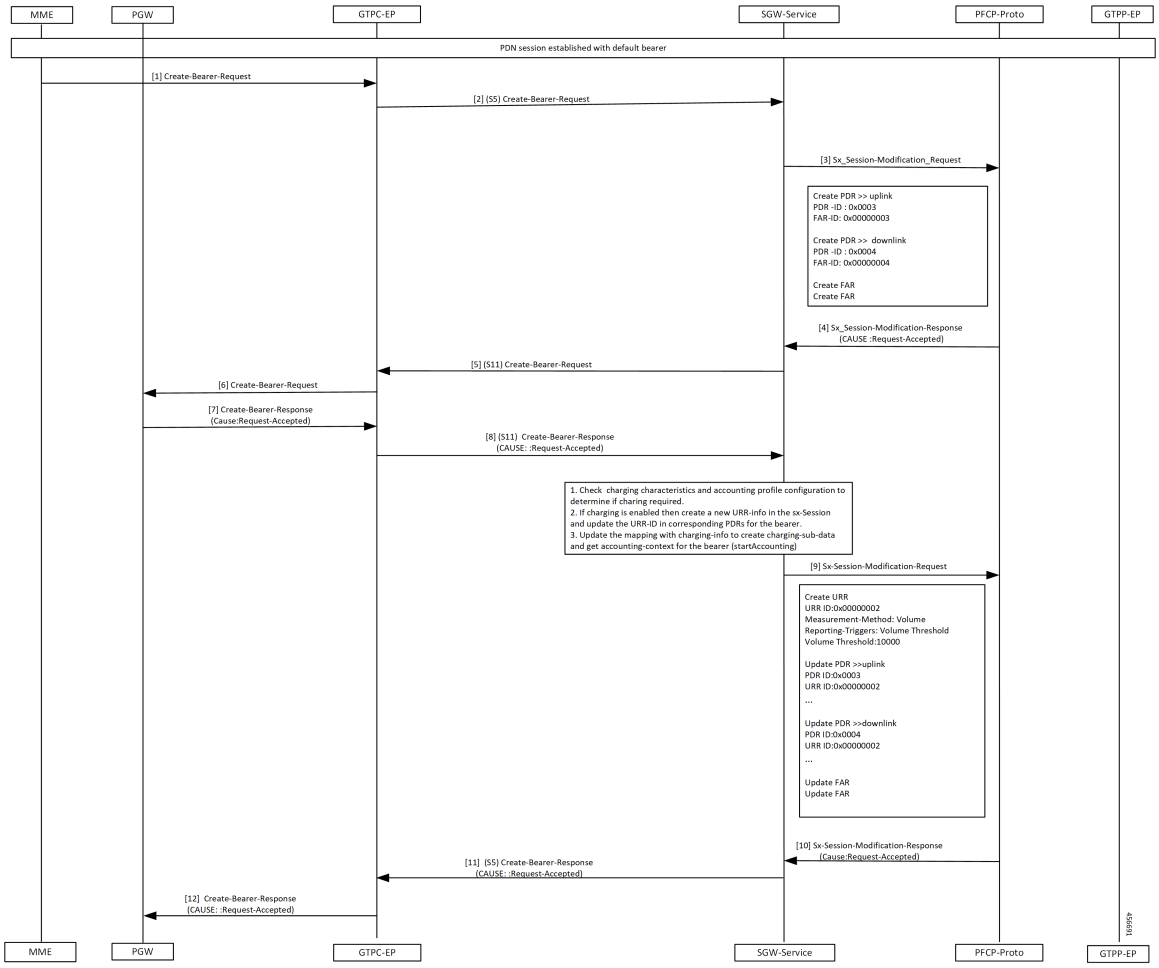


Table 154: URR Installation for Dedicated Bearer Call Flow Description

Step	Description
1	Established a PDN session with a default bearer. The PGW sends the Create Bearer Request to the GTPC-EP.
2	The GTPC-EP forwards the S5 Create Bearer Request to the SGW-service pod.
3	The SGW-service pod sends the Sx Session Modification Request to the PFCP proto.
4	The PFCP proto sends the Sx Session Modification Response to the SGW-service pod with the cause as Request-Accepted.
5	The SGW-service pod sends the S11 Create Bearer Request to the GTPC-EP.

Step	Description
6	The GTPC-EP forwards the S11 Create Bearer Request to the MME.
7	The GTPC-EP receives the Create Bearer Response to the GTPC-EP with the cause as Request-Accepted.
8	The GTPC-EP forwards the S11 Create Bearer Response to the SGW service with the cause as Request-Accepted.
9	The SGW-service pod sends the Sx Session Modification Request to the PFCP proto.
10,	The PFCP proto sends the Sx Session Modification Response to the SGW-service pod with the cause as Request-Accepted.
11	The SGW-service pod sends the S5 Create Bearer Response to the GTPC-EP with the cause as Request-Accepted.
12	The GTPC-EP sends the Create Bearer Response to the PGW with the cause as Request-Accepted.

URR Removal and CDR Generation on Deletion of Dedicated Bearer Call Flow

This section describes the URR Removal and CDR Generation on Deletion of Dedicated Bearer call flow.

Figure 85: URR Removal and CDR Generation on Deletion of Dedicated Bearer Call Flow

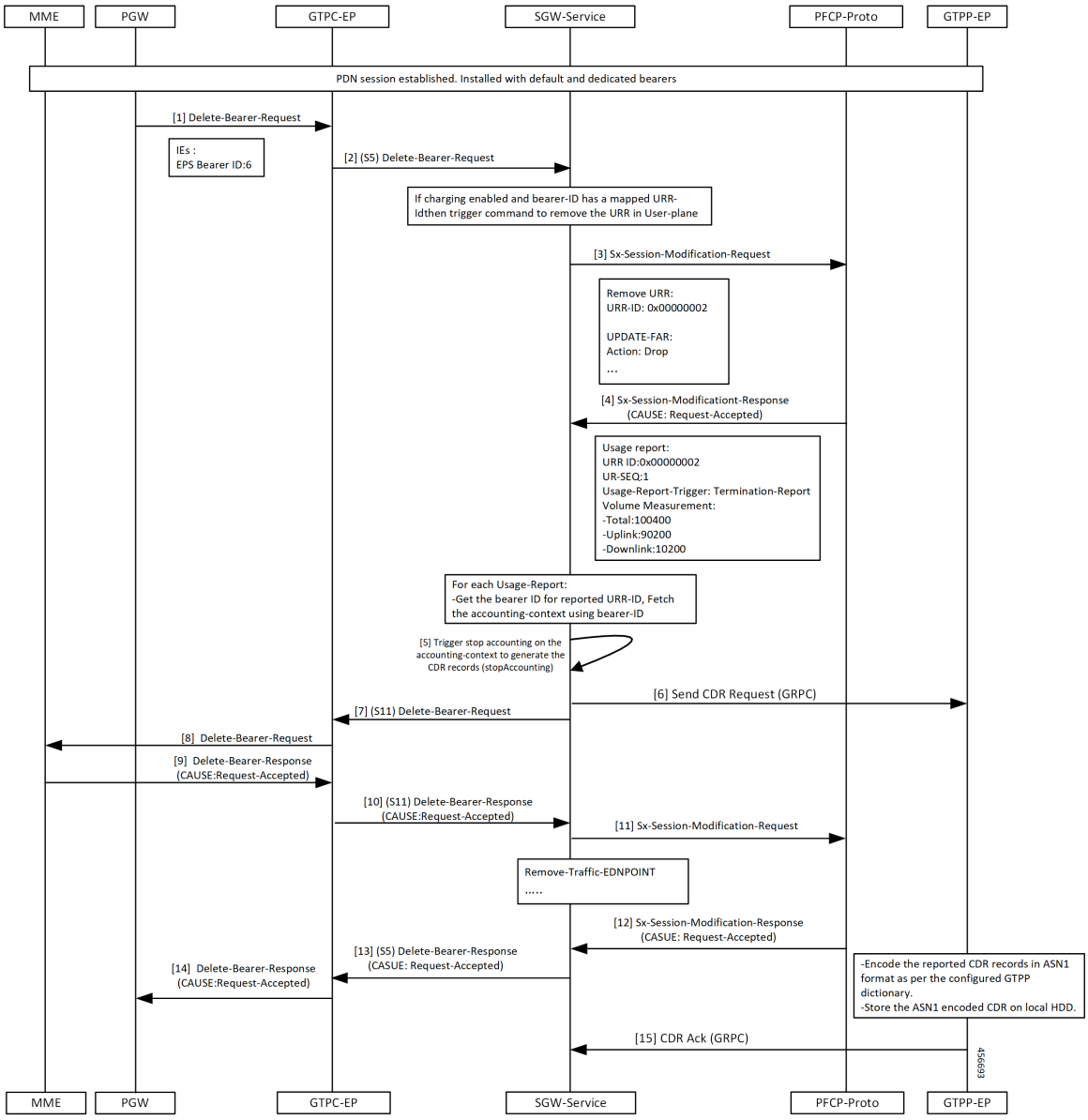


Table 155: URR Removal and CDR Generation on Deletion of Dedicated Bearer Call Flow Description

Step	Description
1	Established a PDN session with the default and dedicated bearer. The PGW sends the Delete Bearer Request to the GTPC-EP.
2	The GTPC-EP forwards the S5 Delete Bearer Request to the SGW-service pod.

Step	Description
3	The SGW-service pod requests a usage report query when charging enabled with QoS trigger and QoS change detected. The SGW-service pod sends the Sx Session Modification Request to the PFCP-Proto.
4	The PFCP proto sends the Sx Session Modification Response to the SGW-service pod with the cause as Request-Accepted.
5	The SGW-service pod triggers the CDR generation and sends CDR request to the GTPP-EP.
6	The SGW-service pod sends the S5 Sx Modify Bearer Request to the GTPP-EP.
7	The SGW-service pod sends the S11 Delete Bearer Request to the GTPC-EP.
8	The GTPC-EP forwards the Delete Bearer Request to the MME.
9	The GTPC-EP receives the Delete Barer Response from the MME with the cause as Request-Accepted.
10	The GTPC-EP forwards the S11 Delete Bearer Response to the SGW-service pod with the cause as Request-Accepted.
11	The SGW-service pod sends the Sx Session Modification Request to the PFCP proto.
12	The SGW-service pod receives the Sx Session Modification Response from the PFCP proto with the cause as Request-Accepted.
13	The SGW-service pod sends the S5 Delete Bearer Response to the GTPC-EP with the cause as Request-Accepted.
14	The GTPC-EP sends the Delete Bearer Response to the PGW with the cause as Request-Accepted.
15	The PFCP proto sends the CDR ACK to the SGW-service pod.

Volume Reporting on S11 Trigger Call Flow

This section describes Volume Reporting on S11 Trigger call flow.

Figure 86: Volume Reporting on S11 Trigger Call Flow

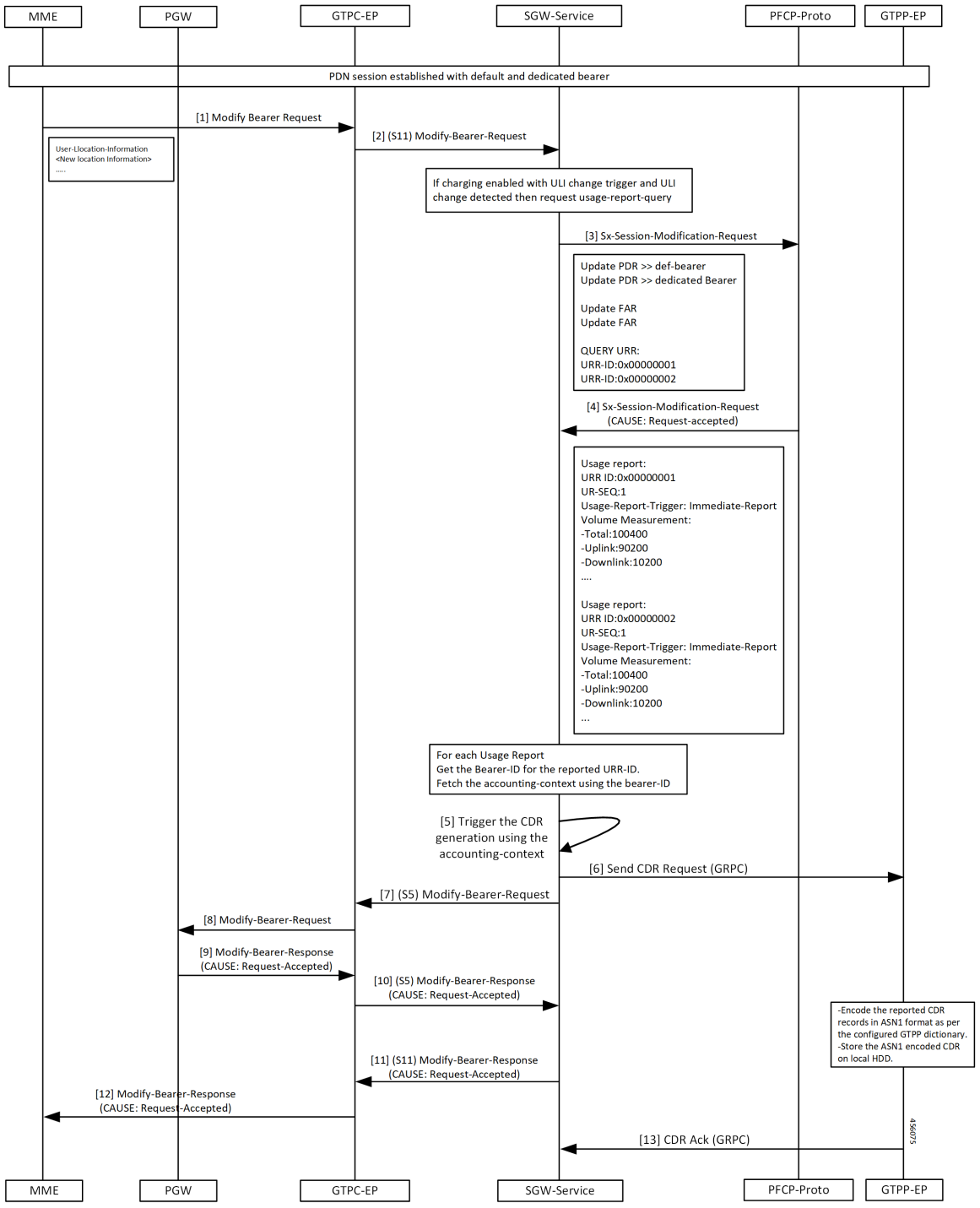


Table 156: Volume Reporting on S11 Trigger Call Flow Description

Step	Description
1	Established a PDN session with the default and dedicated bearers. The MME sends Modify Bearer Request to the GTPC-EP.
2	The GTPC-EP forwards the S11 Modify Bearer Request to the SGW-service pod.
3	The SGW-service pod requests the usage report query when charging enabled with QoS trigger and QoS change detected. The SGW-service pod sends the Sx session Modification Request to the PFCP proto.
4	The PFCP proto sends the Sx Session Modification Response to the SGW-service pod with the cause as Request-Accepted.
5	The SGW-service pod triggers the CDR generation.
6	The SGW-service pod sends the generated CDR request to the GTPP-EP.
7	The SGW-service pod sends the S5 Sx Modify Bearer Request to the GTPC-EP.
8	The GTPC-EP sends the Modify Bearer Request to the PGW.
9	The GTPC-EP receives the Modify Bearer Response from the PGW with the cause as Request-Accepted.
10	The GTPC-EP forwards the S5 Modify Bearer Response to the SGW-service pod with the cause as Request-Accepted.
11	The SGW-service pod sends the S11 Modify Bearer Response to the PGW with the cause as Request-Accepted.
12	The GTPC-EP sends the Modify Bearer Response to the MME with the cause as Request-Accepted.
13	The GTPP-EP sends the CDR ACK to the SGW-service pod.

Volume Reporting on S5 Trigger Call Flow

This section describes the Volume Reporting on S5 Trigger call flow.

Figure 87: Volume Reporting on S5 Trigger Call Flow

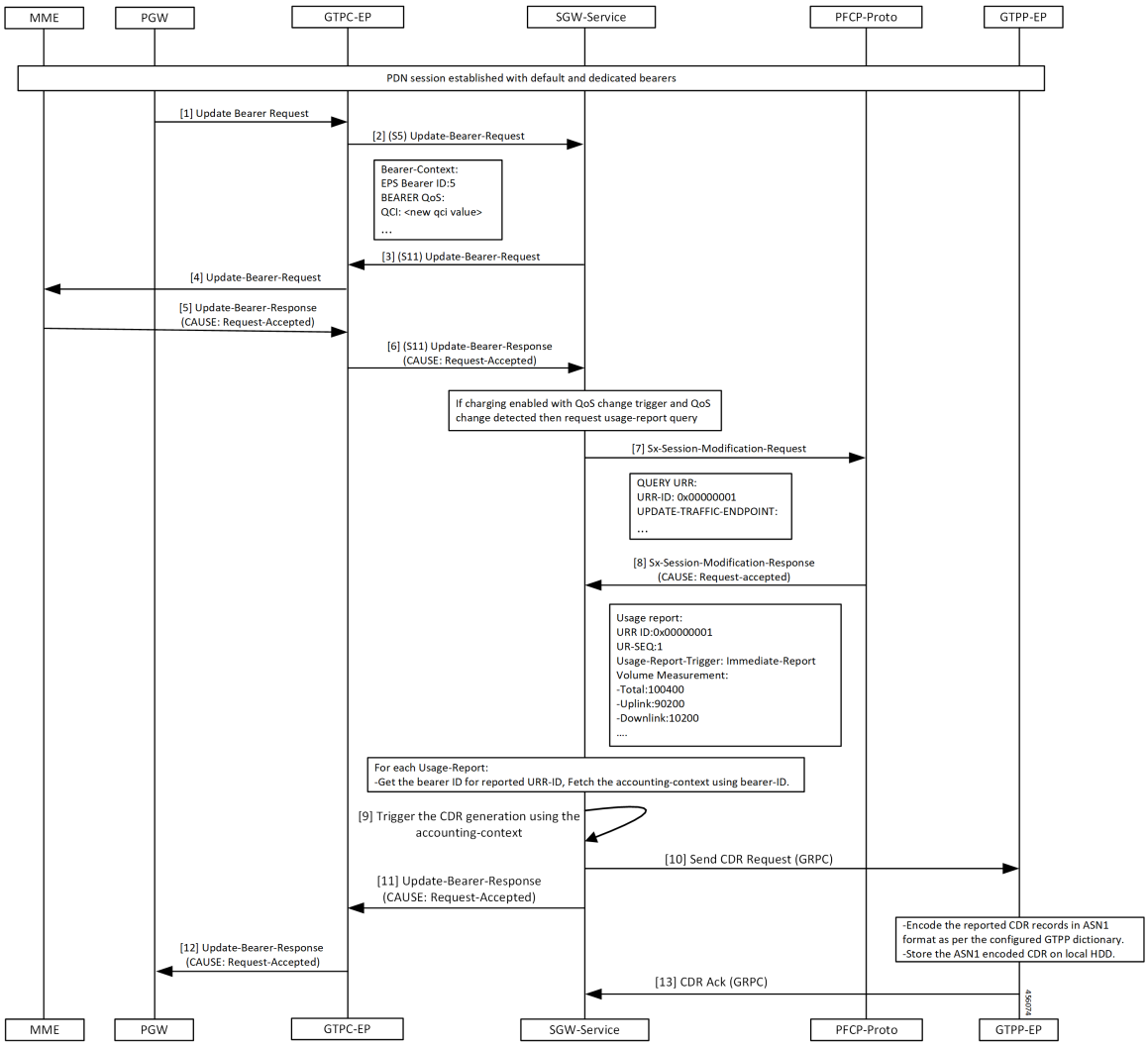


Table 157: Volume Reporting on S5 Trigger Call Flow Description

Step	Description
1	Established a PDN session with the default and dedicated bearers. The PGW sends the Update Bearer Request to the GTPC-EP.
2	The GTPC-EP forwards S5 Update Bearer Request to the SGW-service pod.
3	The SGW sends the Update Bearer request S11 to the GTPC-EP.
4	The GTPC-EP forwards the Update Bearer request to the MME.
5	The MME sends the Update Bearer Response to the GTPC-EP with the cause as Request-Accepted.

Step	Description
6	The GTPC-EP sends the S11 Update Bearer Response to the SGW-service pod with the cause as Request-Accepted.
7	The SGW-service pod requests the Usage report query when charging enabled with QoS trigger and QoS Change detected. The SGW-service pod sends the Sx Session Modification Request to the PFCP proto.
8	The SGW-service pod receives the Sx Session Modification Response from the PFCP proto with the cause as Request-Accepted.
9	The SGW-service pod triggers the CDR generation.
10	The SGW-service pod sends the CDR report to the GTPP-EP.
11	The GTPC-EP receives the Update Bearer response from the SGW-service pod with the cause as Request-Accepted.
12	The PGW forwards the S5 the Update Bearer response from the GTPC-EP with the cause as Request-Accepted.
13	The GTPP-EP sends the CDR ACK to the SGW-service pod.

Standards Compliance

The SGW Charging support complies with the following 3GPP standards:

- *3GPP TS 32.251 "Telecommunication management;Charging management;Packet Switched (PS) domain charging"*
- *3GPP TS 32.295 "Telecommunication management; Charging management; Charging Data Record (CDR) transfer"*
- *3GPP TS 32.297 "Telecommunication management; Charging management; Charging Data Record (CDR) file format and transfer"*
- *3GPP TS 32.298 "Telecommunication management; Charging management; Charging Data Record (CDR) parameter description"*

Limitations

This feature has the following limitations in this release:

- In 2021.02.0 release, cnSGW-C supports the following:
  - Enable or Disable of anp-mbr and node-id-prefix CDR attributes. Other cnSGW-C CDR attributes are enabled by default
  - Only encrypted-url configuration while performing push operation to a remote SFTP server
- In 2021.02.0 release, cnSGW-C does not support the following:

- Monitor protocol doesn't support CDR
- Served PDP or PDN Address Extension CDR attribute for the dual stack (IPv4v6) calls
- Behavior bit. Default value is zero
- Compression of CDR files
- Purging of CDR files using user provided regex

- For cnSGW-C Charging Profile dynamic configuration:
  - You cannot remove the Charging Profile configuration dynamically. Before removing the Charging Profile configuration, the existing subscriber must be cleared.

Feature Configuration

Configuring this feature involves the following steps:

- CLI Configuration-This configuration provides commands to configure cnSGW-C charging profile, mode, threshold, and its characteristics. For more information, refer to CLI Configuration, on page 393.
- Show CLI-This configuration provides the commands to display the SFTP push CLI. For more information, refer to Show CLI, on page 404.

CLI Configuration

cnSGW-C charging CLI configuration involves the following steps:

- Charging Profile or GTP Prime-This configuration provides commands to configure cnSGW-C GTPP profile. For more information, refer to Configuring the cnSGW-C Charging Profile or GTP Prime, on page 394.
- Charging Mode-This configuration provides commands to configure the cnSGW-C charging mode. For more information, refer to Configuring the Charging Mode, on page 399.
- Charging Threshold-This configuration provides commands to configure the cnSGW-C charging threshold. For more information, refer to Configuring the cnSGW-C Charging Threshold, on page 399.
- Charging Threshold and Charging Profile Association-This configuration provides commands to configure cnSGW-C charging threshold and cnSGW-C charging profile association. For more information, refer to Configuring cnSGW-C Charging Threshold and cnSGW-C Charging Profile Association, on page 401.
- Call Control Profile-This configuration provides commands to configure cnSGW-Ccall control profile. For more information, refer to Configuring Call Control Profile, on page 402.
- Charging Characteristics Under Call Control Profile-This configuration provides commands to configure cnSGW-C charging characteristics under call control profile. For more information, refer to Configuring Charging Characteristics Under Call Control Profile, on page 403.

Configuring the cnSGW-C Charging Profile or GTP Prime

Note

- cnSGW-C charging supports multiple replicas of GTP Prime.
- cnSGW-C switches from primary storage server to secondary storage server on four consecutive failures with the primary storage server. It switches back to primary storage server on four consecutive failures to secondary storage server or after 30 minutes of switchover from primary storage server to secondary storage server whichever is earlier.
- When CDR file storage reaches beyond 95% of its allocated size, then old CDR files are deleted.

Configuring cnSGW-C charging profile or GTP prime involves the following steps:

- GTPP profile-This configuration provides commands to configure cnSGW-C GTPP profile. For more information, refer to Configuring the GTPP Profile, on page 394.
- Existing endpoint-related CLI-This configuration provides commands to configure cnSGW-C existing endpoint-related CLI. For more information, refer to Configuring the GTPP Endpoint, on page 397.
- SGW charging profile--This configuration provides commands to configure cnSGW-C GTPP profile. For more information, refer to Configuring SGW Charging Profile, on page 397.

Configuring the GTPP Profile

You can configure server details, dictionary, timeout, and so on, to use by the GTPP-EP pod.

To configure the GTPP profile, use the following configuration:

```
config
  profile gtpp-profile profile_name gtpp
    local-storage
      file
        rotation
         volume volume_value
         cdr-count cdrcount_value
         time-interval interval_value
        exit
        name
         prefix prefix_value
         format format
         max-file-seq-num max_sequence_number
         start-file-seq-num start_sequence_number
         recover-file-seq-num { true | false }
        exit
        purge-processed-files purge-interval purgeinterval_value
       exit
       push
        encrypted-url url_name
        encrypted-secondary-url url_name
       exit
      exit
```

```
dictionary  custom_value
end
```

NOTES:

- **local-storage**—Local storage details.
- **file**—Specify the file details.
- **rotation**—Specify the file rotation details.
- **volume** *volume_value*—Specify the file volume in MiB for file rotation. Must be an integer in the range of 2-40. Default value is 4.
- **cdr-count** *cdrcount_value*—Specify the CDR count for file rotation. Must be an integer in the range of 1000-65000. Default value is 10000.
- **time-interval** *interval_value*—Specify the time interval in seconds for file rotation. Must be an integer in the range of 30-86400. Default value is 3600.
- **prefix** *prefix_value*—Specify the file name prefix to be used. If the prefix value isn't specified, the configuration takes default profile name.
- **format** *format*—Specify the file name format to be used to override the name format associated with the file format.
- **max-file-seq-num** *max_sequence_number*—Specify the maximum file sequence number to rollover. Default value is 4294967295.
- **start-file-seq-num** *start_sequence_number*—Specify the start sequence number during rollover. Default value is 1.
- **recover-file-seq-num { true | false }**—When set to true, file sequence number continues from the last sequence number on application restart. Default value is false.
- **purge-processed-files** —Enables periodic purging of processed files.
- **purge-processed-files purge-interval** *purgeinterval_value*—Specify the purging interval of processed files in minutes. Default value is 60.
- **encrypted-url**—Specify the primary SFTP URL to push CDR files to.
- **encrypted-secondary-url**—Specify the secondary SFTP URL to push when push fails on primary host.
- **dictionary** *custom_value*—Specify the dictionary to be used to ASN.1 encode a CDR.

Note

- The path in SFTP URL is by default a relative path to home directory of SFTP URL user specified in URL.

  Example: `encrypted-url sftp://user:pass@example.com:2020/upload/pf1`. It pushes files to `%USER_HOME/upload/pf1`

  Example: `encrypted-url sftp://user:pass@example.com:2020`. It pushes files to `%USER_HOME`

- To upload files to a folder outside the user's home directory, configure an absolute path by preceding the path with // at the beginning of the SFTP server path.

  Example: `encrypted-url sftp://user:pass@example.com:2020//var/opt`. It pushes the files to absolute path `/var/opt`

  SFTP user must have the write access to this path for the upload to be successful.

If password contains any special character outside the permissible URL character set, they must be percent coded as per the RFC 3986. For example, a URL with password `pass!word`, entered as `sftp://user:pass%21word@example.com/path/to/folder`

Configuration Example

The following is an example configuration.

```
config
   profile gtpp-profile pf1 gtpp
      local-storage
         file
            rotation
               volume   5
               cdr-count 1000
               time-interval 60
               exit
               name
                  prefix  NYPCF508
                  format  .%Y-%m-%d%H-%M-%S.%4Q
                  max-file-seq-num     4
                  start-file-seq-num   1
                  recover-file-seq-num false
                  exit
               purge-processed-files purge-interval 10
               exit
               push
                  encrypted-url sample.com sftp://user:pass@example.com//var/opt
                  encrypted-secondary-url sftp://user:pass@mirror.example.com//var/opt
                  exit
               exit
               dictionary custom24
               end
```

Configuring the GTPP Endpoint

Note

- GTPP-EP pod uses this configuration.
- GTPP-EP pod always ignores nodes configuration.
- When **k8s single-node** is set to **`false`**, it spawns two replicas of GTPP-EP pod in active or standby mode independent of replicas and nodes configuration.
- When **k8s single-node** is set to **`true`**, the configured replicas have its impact.
- When **k8s use-volume-claim** is set to **`true`**, endpoint GTP prime is used to set the storage size limit. Default value of storage size limit is one GB.
- When system is up and running, we can't change the storage size.

To configure GTPP endpoint, use the following commands:

```
config
 instance instance-id instance_id
   endpoint gtpprime
      replicas replicas_count
      nodes nodes_count
      storage storage_capacity
      end
```

NOTES:

- **replicas** *replicas_count*—Specify the number of replicas per node. Must be an integer.
- **nodes** *nodes_count*—This property is ignored. You may skip configuring it.
- **storage** *storage_capacity*—Specify the storage size of persistent volume in GB. Must be an integer in the range of 1-20.

Note CLI doesn't allow changing storage size while system is running. To change the storage size, bring the system down first.

Configuration Example

The following is an example configuration.

```
config
   instance instance-id 1
      endpoint gtpprime
         replicas 1
         storage  2
         end
```

Configuring SGW Charging Profile

This section describes how to configure SGW Charging profile.

You can configure the SGW charging profile for the following:

- Attribute details and adding them to the CDRs
- Different triggers in generating CDR

SGW service pod uses this configuration in cnSGW-C charging.

Use following commands to configure cnSGW-C charging profile.

```
config
  profile sgw-charging-profile profile_name
    gtpp-triggers
      volume-limit { enable | disable }
      time-limit { enable | disable }
      serving-node-change-limit { enable | disable }
      serving-node-plmn-change { enable | disable }
      uli-change { enable | disable }
      qos-change { enable | disable }
      ms-timezone-change { enable | disable }
    gtpp-attributes
      apn-ambr
        include-for-all-bearers
        include-for-default-bearer
        include-for-non-gbr-bearers
      node-id-suffix suffix_value
    gtpp-profile association_profile_name
    exit
```

Note The value of node-id-suffix is implementation-specific. However, it's recommended to give same value as prefix configured as a part of GTPP Profile.

NOTES:

- **apn-ambr**—Includes APN-AMBR value in CDR.
- **node-id-suffix** *suffix_value*—Specify the node ID suffix to include in NodeId field of CDR.
- **ms-timezone-change { enable | disable }**—Specify enable or disable the MS time zone change as a trigger for CDR generation. Default value is enable.
- **qos-change { enable | disable }**—Specify enable or disable the QoS change as a trigger for container addition to CDR. Default value is enable.
- **serving-node-change-limit { enable | disable }**—Specify enable or disable the serving node change (address) as a trigger for CDR generation. Default value is enable.
- **serving-node-plmn-change { enable | disable }**—Specify enable or disable the serving node PLMN change as a trigger for CDR generation.
- **time-limit { enable | disable }]**—Specify enable or disable the time limit breach as a trigger for CDR generation. Default value is enable.

- **uli-change { enable | disable }**—Specify enable or disable the ULI change as a trigger for container addition to CDR. Default value is enable.
- **volume-limit { enable | disable }**—Specify enable or disable the volume limit breach as a trigger for CDR generation. Default value is enable and that is included in NodeId field of CDR.

Configuration Example

The following is an example configuration.

```
config
   profile sgw-charging-profile ch1
      gtpp-triggers volume-limit enable
      gtpp-triggers time-limit  enable
      gtpp-triggers serving-node-change-limit disable
      gtpp-triggers uli-change  enable
      gtpp-triggers qos-change  disable
      gtpp-triggers ms-timezone-change disable
      gtpp-attributes apn-ambr include-for-all-bearers
      gtpp-attributes node-id-suffix test
      gtpp-profile pf1
      end
```

Configuring the Charging Mode

Charging mode configures the cnSGW-C service mode for accounting GTPP or none (default).

Note Enable offline charging when charging mode is set to GTPP.

To configure charging mode, use the following configuration:

```
config
  profile sgw sgw_srv_name
     charging-mode { gtpp | none }
     sgw-charging-threshold sgw_threshold_name
     sgw-charging-profile  sgw_charging-profile_name
     end
```

NOTES:

- **charging-mode { gtpp | none }**—Specify cnSGW-C charging mode.
- **sgw-charging-threshold** *sgw_threshold_name*—Specify the name of associated cnSGW-C charging threshold
- **sgw-charging-profile** *sgw_charging-profile_name*—Specify the name of associated cnSGW-C charging profile

Configuring the cnSGW-C Charging Threshold

cnSGW-C charging threshold configuration helps in configuring the thresholds or limits corresponding to volume or duration or buckets per CC (charging-characteristics).

Configuration of cnSGW-c charging threshold can be done in two ways.

Method - 1

```
config
   profile sgw-charging-threshold threshold_name
      cc profile value cc_profile_value
         volume total total_value
         buckets buckets_value
         duration duration_value
         end
```

Method - 2

```
config
   profile sgw-charging-threshold threshold_name
      cc profile value cc_profile_value
         volume
            total total_value
            uplink uplink_value
            downlink downlink_value
         volume total
         buckets buckets_value
         serving-node-changesnode_changes_value
         duration duration_value
         end
```

NOTES:

- **buckets** *buckets_value*—Specify the number of traffic volume container changes due to QoS change or other triggers before an accounting record must be closed. It ranges 1–20 and the default value is 4.
- **duration** *duration_value*—Specify the normal time duration that must elapse before closing an accounting record.
- **volume total**—Specify the CC volume details.

Configuration Example

The following is an example configuration:

```
config
   profile sgw-charging-threshold thre1
      cc profile value 1
         volume total 100000
         buckets  1
         duration 60
         end

config
   profile sgw-charging-threshold thre1
      cc profile value 2
         volume uplink 100000
         volume downlink 100000
         buckets  1
         serving-node-changes 4
         duration 120
         end
```

Note When **gtpp-triggers serving-node-change-limit** is enabled and **serving-node-changes** configured under SGW charging threshold, CDR gets generated after 4 times serving node changes (MME).

Configuring cnSGW-C Charging Threshold and cnSGW-C Charging Profile Association

This section describes how to configure the SGW Charging Threshold and SGW Charging profile association.

This configuration associate **sgw-charging-threshold** and **sgw-charging-profiles** to the SGW profile.

Configuration of cnSGW-c charging threshold and cnSGW-c charging profile association can be done in two ways.

Method - 1

To configure cnSGW-c charging threshold and cnSGW-c charging profile association, use the following commands.

```
config
  profile sgw sgw_srv_name
    locality location_code
    fqdn dnn_name
    plmn-id
      mcc mcc_value
      mnc mnc_value
    charging-mode { gtpp | none }
    sgw-charging-profile value
    sgw-charging-threshold limit_name
    end
```

Method - 2

Use the following commands to configure SGW Charging Threshold and SGW Charging Profile association.

```
config
  profile sgw sgw_srv_name
    sgw-charging-threshold threshold_value
    locality location_code
    fqdn dnn_name
    charging-mode mode_name
    subscriber-policy policy_name
    end
```

Configuration Example

The following is an example configuration.

```
config
  profile sgw sgw1
    locality LOC1
    fqdn 209.165.200.254
    allowed-nssai [ slice1 ]
    plmn-id mcc 123
    plmn-id mnc 456
    charging-mode gtpp
```

```
      sgw-charging-profile ch1
      sgw-charging-threshold limit1
      end

config
   profile sgw sgw1
      sgw-charging-threshold thre1
      locality  LOC1
      fqdn 209.165.200.254
      charging-mode none
      subscriber-policy polSub
      end
```

Configuring Call Control Profile

Call control profile configuration defines and applies the call handling rules through an operator policy.

The charging mode value from the call control profile overrides the configured value in cnSGW-C profile.

Note

- One call control profile is associated with one operator policy
- It's a standalone configuration

Configuring cnSGW-C call control profile involves the following steps:

- Call Control Profile Creation-This configuration provides commands to configure cnSGW-C call control profile Creation. For more information, refer to Configuring the Call Control Profile Creation, on page 402.
- Operator Policy Association-This configuration provides commands to configure cnSGW-operator policy association. For more information, refer to Configuring the Operator Policy Association, on page 402.

Configuring the Call Control Profile Creation

To configure the call control profile creation, use the following configuration:

```
config
   policy call-control-profile call_control_profile_name
      charging-mode sgw_charging_mode
      sgw-charging-profile assocaited_sgw_charging_profile
      end
```

Configuration Example

The following is an example configuration.

```
config
   policy call-control-profile ccp1
      charging-mode gtpp
      sgw-charging-profile ch1
      end
```

Configuring the Operator Policy Association

To configure the operator policy association, use following configuration:

```
config
   policy operator operator_name
   policy dnn  dnn_policy_name
   policy network-capability network_name
   call-control-profile value
   end
```

Configuration Example

The following is an example configuration.

```
config
   policy operator opPol1
   policy dnn polDnn
   policy network-capability nc1
   call-control-profile ccp1
   end
```

Configuring Charging Characteristics Under Call Control Profile

You can define local values and select the source of charging characteristics for charging decisions.

To configure charging characteristics under call control profile, use the following configuration:

```
config
   policy call-control-profile  call_control_profile_name
      sgw-charging-profile charging_type
      charging-mode mode_type
      cc prefer preference_type
      cc local-value profile index_bit
      end
```

NOTES:

- **cc prefer local-value** and **cc prefer hlr-hss-value** are optional parameters.
- **cc prefer { hlr-hss-value | local-value }**—Specify a preference to use in charging characteristics from the following:
  - When received from HLR or HSS through MME and preference set to hlr-hss.
  - When preference set to local-value. See the following CLI:

    ```
    cc prefer local-value
    cc local-value profile index-bit
    ```

- **cc local-value profile** —Specify the local-value parameter information as follows:
  - index_bit default value is 8
  - Sets the local value of the profile index for the charging characteristics, when the charging characteristics(CC) prefer value is set to local-value

Configuration Example

The following is an example configuration.

```
config
   policy call-control-profile CCP
```

```
      sgw-charging-profile test
      charging-mode gtpp
      cc prefer local-value
      cc local-value profile 4
      end
```

```
config
   policy call-control-profile CCP1
      sgw-charging-profile test
      charging-mode gtpp
      cc prefer hlr-hss-value
      end
```

Note Use the system default configured value as 8 otherwise use the value which comes in CSR.

```
config
   policy call-control-profile CCP2
      sgw-charging-profile test
      charging-mode gtpp
      cc prefer local-value
      end
```

Note Default value for cc profile is 8.

Show CLI

GTPP-EP SFTP Push CLI

- **show gtpp-ep endpoints**: Displays the list of running GTPP-EP pods and their corresponding IPs
- **show gtpp-ep files endpoint** *pod-name* **profile** *gtpp-profile_name*: Displays the archived files on specific GTPP-EP pod for the given gtpp
- **cdr push endpoint** *pod-name* **profile** *gtpp-profile* **filename** *file-to-be-uploaded*: Pushes the available file to archive folder on specific GTPP-EP pod for given GTPP profile.

CDR Fields Supported in cnSGW-CDRs

The tables in this section list the cnSGW-CDR fields present in the available dictionaries.

custom24 Dictionary

Table 158: custom24 Dictionary Description

Field Name	Tag Number	Category	Description
Record Type	0	M	SGW IP-CAN bearer record.

Field Name	Tag Number	Category	Description
Served IMSI	3	M	IMSI of the served party.
S-GW Address	4	M	The control plane IP address of the SGW used.
S-GW BINARY IPV4 ADDRESS	4-0	M	The octet string includes the Gn address of the GGSN service i binary coding.
S-GW BINARY IPV6 ADDRESS	4-0	M	The octet string included in the field described includes the Gn address of the GGSN service in binary coding.
Charging ID	5	M	IP-CAN bearer identifier. To identify IP-CAN bearers created b PCNs in different records
List of Serving Node Address	6	M	List of serving node control plane IP addresses (Example: SGS MME) used during this record.
Serving Node BINARY IPV4 ADDRESS	6-0	M	The octet string included in the field described above includes t IPv4 address of the MME.
Serving Node BINARY IPV6 ADDRESS	6-0	M	The octet string included in the Serving node binary IPv4 addre field includes the IPV6 address of the MME.
Access point name network identifier	7	M	The logical name of the connected access point to the external pa data network (network identifier part of APN).
PDP/PDN Type	8	M	This field indicates PDN type (Example IPv4, IPv6 or IPv4v6).
Served PDP/PDN Address	9	M	IP address allocated for the PDP context or PDN connection, if available. IPv4 when PDN type is IPv4 or IPv6 when PDN type is IPv6 o IPv4v6.
PDP IP Address	9-0	M	This field contains the IP address for the PDP context.
PDP IPv4 Address	9-0-0	M	The octet string included in the PDP IP address field includes th SGW assigned IPv4 address to the subscriber in binary format.
PDP IPv6 Address	9-0-0	M	The octet string included in the PDP IP address field includes t IPv6 address assigned to the subscriber by the SGW in binary coc
Dynamic Address Flag	11	O	Indicates whether served PDP/PDN address is dynamic, which allocated during IP-CAN bearer activation, initial attach (E-UTR or over S2x) and UE requested PDN connectivity. This field is missing if address is static.

Field Name	Tag Number	Category	Description
List of Traffic Data Volumes	12	M	A list of changes in charging conditions for QCI, ARP pair, each change is time stamped. Charging conditions categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are also listed.
Change of charging condition	12-0	M	Each traffic volume container contains details of a charging condition. A new container is usually created for a QoS change and for tariff changes.
Data Volume GPRS Uplink	12-0-3	M	This field is a part of the ChangeOf CharCondition element in the List of Traffic Volumes. It includes the number of octets received in the uplink direction during the timeframe specified by the container. For each new container, the counter is reset and does not accumulate.
Data Volume GPRS Downlink	12-0-4	M	This field is a part of the ChangeOf CharCondition element in the List of Traffic Volumes. It includes the number of octets transmitted in the downlink direction during the timeframe specified by the container. For each new container, the counter is reset and does not accumulate.
Change Condition	12-0-5	M	This field is part of the ChangeOf CharCondition element in the List of Traffic Volumes. It defines the change in user plane to UE.
Change Time	12-0-6	M	This field is part of the ChangeOf CharCondition element in the List of Traffic Volumes. It provides the local time when a change condition (example: record closure) occurred and the container is closed.
User Location Information	12-0-8	O	This field contains the User Location Information.
EPC QoS Information	12-0-9	O	In case of IP-CAN bearer specific container, this field contains authorized QoS for the IP-CAN bearer. First container for each QCI/ARP pair includes this field. In the following containers this field is present if previous change condition is "QoS change". This field is applicable only in SGW-CDR.
CP CIoT EPS Optimisation Indicator	12-0-19	O	The cPCIo TEPSOptimisation Indicator field indicates whether Control Plane CIoT EPS optimisation is used for the transfer of the data volume captured by the container. This is included in the Traffic data container only if previous container's change condition is "change in user plane to UE". Note, the CP CIoT EPS Optimisation indicator field in SGW-CDR main level contains the CP CIoT EPS optimisation indicator value when SGW-CDR was opened.

Field Name	Tag Number	Category	Description
QCI	12-9-1	M	—
Uplink MBR	12-9-2	O	—
Down link MBR	12-9-3	O	—
Uplink GBR	12-9-4	O	—
Down link GBR	12-9-5	O	—
arp	12-9-6	O	—
APN AMBR Uplink	12-9-7	O	—
APN AMBR Downlink	12-9-8	O	—
Extended Maximum Requested BW UL	12-9-9	O	—
Extended Maximum Requested BW DL	12-9-10	O	—
Extended GBR UL	12-9-11	O	—
extended GBRDL	12-9-12	0	—
Extended APN AMBR UL	12-9-13	O	—
Extended APN AMBR DL	12-9-14	O	—
Record Opening Time	13	M	Time stamp when IP-CAN bearer is activated in this S-GW or re opening time on subsequent partial records.
Duration	14	M	This field contains the duration in seconds for the record.
Cause for Record Closing	15	M	This field contains a reason for the closure of the CDR.
Diagnostics	16	O	This field is included in the CDR when the bearer context is rele and when the **gtpp attribute diagnostics** is configured.
gsm408cause	16-0	M	—
Record Sequence Number	17	O	Partial record sequence number, only present in case of partial rec
Node ID	18	O	Name of the recording entity.

Field Name	Tag Number	Category	Description
Record Extensions	19	O	A set of network operator or manufacturer specific extensions to the record. Conditioned when the extension is available.
Local Record Sequence Number	20	O	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode	21	M	An index indicating how the APN is selected.
Served MSISDN	22	M	The primary MSISDN of the subscriber.
Charging Characteristics	23	M	The charging characteristics that are applied to the IP-CAN bearer.
Charging Characteristics Selection Mode	24	O	Holds the information about how charging characteristics are selected
IMS Signaling Context	25	O	Included if the IM-CN Subsystem Signalling Flag is set, see [201] IP-CAN bearer is used for IMS signalling.
Serving Node PLMN Identifier	27	O	Serving node PLMN Identifier (MCC and MNC) used during this record, if available.
Served IMEISV	29	O	IMEISV of the ME, if available.
RAT Type	30	O	This field indicates the Radio Access Technology (RAT) type currently used by the Mobile Station, when available.
MS Time Zone	31	O	The Time Zone IE that the MME may provide to the SGW during the PDN context activation or modification procedure.
User Location Information	32	O	This field contains the user location information as described in TS 29.274 for eGTP case (Example: CGI, SAI, RAI TAI and ECGI). This field is provided by the SGSN or MME and transferred to the SGW or PGW during the IP-CAN bearer activation or modification
S-GW Change	34	O	This field is present only in the SGW-CDR to indicate that this is the first record after an SGW change. In this case, it is set to TRUE (FF)
Serving Node Type	35	M	These fields contain one or several serving node types in control plane of SGW or PGW, which is connected during the record. The serving node types listed here map to the serving node addresses listed in the field Serving node Address in sequence.
Serving Node Type enum	35-1	M	—
P-GW Address Used	36	M	This field is the PGW IP address for the control plane.

Field Name	Tag Number	Category	Description
P-GW Binary IPV4 Address	36-0	M	This field includes the PGW assigned IPv4 address to the subscr in binary format.
P-GW Binary IPV6 Address	36-0	M	This field includes the PGW assigned IPv6 address to the subscr in binary format.
P-GW PLMN Identifier	37	O	—
Start Time	38	O	This field holds the time when User IP-CAN session starts. It's available in the CDR for the first bearer in an IP-CAN session.
Stop Time	39	O	This field holds the time when User IP-CAN session is termina It's available in the CDR for the last bearer in an IP-CAN sessio
PDN Connection ID	40	O	This field holds the PDN connection (IP-CAN session) identifi identify different records belonging to same PDN connection.
iMSI unauthenticated Flag	41	O	This field indicates the provided served IMSI is not authenticat (emergency bearer service situation).
user CSG Information	42	O	This field contains the User CSG Information status of the user accessing a CSG cell. It comprises CSG ID within the PLMN, Ac mode and indication on CSG membership for the user when hy access applies, as defined in *TS 29.060* for GPRS case, and in *T 29.274* for EPC case.
cSGId	42-0	O	A CSG ID is a unique identifier within the scope of PLMN whi identifies a Closed Subscriber Group (CSG) in the PLMN associ with a CSG cell or group of CSG cells.
cSGAccess Mode	42-1	O	cSGAccessMode. It's either closed or hybrid.
cSG Membership Indication	42-2	O	This field provides an indication on CSG membership for the u
Served PDP PDN Address Extension	43	O	This field contains the IPv4 address for the PDN connection (P context, IP-CAN bearer) when dual-stack IPv4 IPv6 is used, and IPv6 adress is included in served PDP address or served PDP or P address.
PDP IP Address	43-0	M	This field contains the IP address for the PDP context.
PDP IPV4 Address	43-0-0	M	This field includes the IPv4 address assigned to the subscriber b SGW in binary coding.
lowAccess Priority Indicator	44	O	This field indicates if the PDN connection has a low priority, w is for machine type communication.

Field Name	Tag Number	Category	Description
dynamic Address FlagExt	47	O	This field indicates whether served IPv4 PDP or PDN address is dynamic, which is allocated during IP-CAN bearer activation, initia attach (E-UTRAN or over S2x) and UE requested PDN connectivity with PDP or PDN type IPv4v6. This field is missing if IPv4 addres is static.
s-GW iPv6 Address	48	O	The control plane IPv6 address, in case of IPv4v6 dual stack, of the S-GW.
SGW BINARY IPV6 ADDRESS	48-0	O	This field includes the Gn address of the GGSN service in binary format.
List of Serving Node IPv6Address	49	O	List of serving node control plane IPv6 addresses, in case of IPv4v6 dual stack, (Example: S4-SGSN, MME) used during this record.
Serving Node BINARY IPV6 ADDRESS	49-0	M	The octet string in this field includes the IPV6 address of the MME
p-GW iPv6 Address Used	50	O	This field is the PGW IPv6 Address, in case of IPv4v6 dual stack, for the control plane.
PGW BINARY IPV6 ADDRESS	50-0	O	The octet string in this field includes the IPV6 address assigned to the subscriber by of the P-GW in binary coding.
last User Location Information	55	O	Indicates the UE's last user location information during bearer deactivation or session release.
last MSTime Zone	56	O	Indicates the Latest timezone of UE while bearer deactivation or session release.
CP CIoT EPS Optimisation Indicator	59	O	This field indicates whether Control Plane CIoT EPS optimisation is used by the PDN connection during data transfer with the UE (tha is, Control Plane NAS PDU viaS11-U between S-GW and MME) o not (that is, User Plane via S1-U between S-GW and eNB).
UNI PDU CP Only Flag	60	O	The uNIPDUCP OnlyFlag field indicates whether this PDN connection is applied witl "Control Plane Only flag", that is, transferred using Control Plane NAS PDUs only, when Control Plane CIoT EPS Optimisation is enabled. This field is not flagged when both user plane and control plane UNI for PDU transfer (that is, S1-U and S11-U from S-GW) are allowed, when Control Plane CIoT EPS Optimisation is enabled
List of RAN Secondary RAT Usage Reports	64	OC	This field includes one or more containers reported from the RAN for a secondary RAT.
RAN Secondary RAT Usage Report	64-0	M	This field includes RAN reported containers for a secondary RAT.

Field Name	Tag Number	Category	Description
Data Volume Uplink	64-0-1	M	This field includes the number of octets transmitted during the u of the packet data services in the uplink direction reported from R The counting and reporting from RAN of uplink data volumes i optional.
Data Volume Downlink	64-0-2	M	This field includes the number of octets transmitted during the u of the packet data services in the downlink direction reported fr RAN. The counting and reporting from RAN of downlink data volumes is optional.
RAN Start Time	64-0-3	M	This field is a timestamp at which RAN opens the volume conta
RAN End Time	64-0-4	M	This field is a time stamp at which RAN closes the volume conta
Secondary RAT Type	64-0-5	OC	This field contains the RAT type for the secondary RAT.
UE Local IP Port Info	253	O	This field includes the S2b user local IP port information.
UE Local IP Address	253-0	O	This field includes the UWAN user IP address.
UDP Source Port	253-1	O	This field includes the UWAN user source port.

Note All IP addresses are encoded in binary format.

ASN.1 Definition for Fields in custom24

The following section provides the complete ASN.1 definition of all cnSGW-CDR related fields in the custom24 dictionary.

```
GPRS-SGW-Charging-DataTypes-REL8 DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-------------------------------------------------------------------------------
--
--    GPRS RECORDS
--
-------------------------------------------------------------------------------

GPRSRecord::= CHOICE
--
-- Record values 20, 22..27 are specific
-- Record values 76..77 are MBMS specific
-- Record values 78..79 are EPC specific
{
    sGWRecord[78] SGWRecord
}

SGWRecord    ::= SET
{
    recordType                                  [0] RecordType,
    servedIMSI                                  [3] IMSI,
    s-GWAddress                                 [4] GSNAddress,
```

```
    chargingID                                  [5] ChargingID,
    servingNodeAddress                          [6] SEQUENCE OF GSNAddress,
    accessPointNameNI                           [7] AccessPointNameNI OPTIONAL,
    pdpPDNType                                  [8] PDPType OPTIONAL,
    servedPDPPDNAddress                         [9] PDPAddress OPTIONAL,
    dynamicAddressFlag                          [11] DynamicAddressFlag OPTIONAL,
    listOfTrafficVolumes                        [12] SEQUENCE OF ChangeOfCharCondition
OPTIONAL,
    recordOpeningTime                           [13] TimeStamp,
    duration                                    [14] CallDuration,
    causeForRecClosing                          [15] CauseForRecClosing,
    diagnostics                                 [16] Diagnostics OPTIONAL,
    recordSequenceNumber                        [17] INTEGER OPTIONAL,
    nodeID                                      [18] NodeID OPTIONAL,
    recordExtensions                            [19] ManagementExtensions OPTIONAL,
    localSequenceNumber                         [20] LocalSequenceNumber OPTIONAL,
    apnSelectionMode                            [21] APNSelectionMode OPTIONAL,
    servedMSISDN                                [22] MSISDN OPTIONAL,
    chargingCharacteristics                     [23] ChargingCharacteristics,
    chChSelectionMode                           [24] ChChSelectionMode OPTIONAL,
    iMSsignalingContext                         [25] NULL OPTIONAL,
    servingNodePLMNIdentifier                   [27] PLMN-Id OPTIONAL,
    servedIMEISV                                [29] IMEI OPTIONAL,
    rATType                                     [30] RATType OPTIONAL,
    mSTimeZone                                  [31] MSTimeZone OPTIONAL,
    userLocationInformation                     [32] OCTET STRING OPTIONAL,
    sGWChange                                   [34] SGWChange OPTIONAL,
    servingNodeType                             [35] SEQUENCE OF ServingNodeType,
    p-GWAddressUsed                             [36] GSNAddress OPTIONAL,
    p-GWPLMNIdentifier                          [37] PLMN-Id OPTIONAL,
    startTime                                   [38] TimeStamp OPTIONAL,
    stopTime                                    [39] TimeStamp OPTIONAL,
    pDNConnectionID                             [40] ChargingID OPTIONAL,
    servedPDPPDNAddressExt                      [43] PDPAddress OPTIONAL,
    lowAccessPriorityIndicator                  [44] NULL OPTIONAL,
    dynamicAddressFlagExt                       [47] DynamicAddressFlag OPTIONAL,
    s-GWiPv6Address                             [48] GSNAddress OPTIONAL,
    servingNodeiPv6Address                      [49] SEQUENCE OF GSNAddress OPTIONAL,
    p-GWiPv6AddressUsed                         [50] GSNAddress OPTIONAL,
    lastUserLocationInformation                 [55] OCTET STRING OPTIONAL,
    lastMSTimeZone                              [56] MSTimeZone OPTIONAL,
    cPCIoTEPSOptimisationIndicator              [59] BOOLEAN OPTIONAL,
    uNIPDUCPOnlyFlag                            [60] BOOLEAN OPTIONAL,
    listOfRANSecondaryRATUsageReports           [64] SEQUENCE OF RANSecondaryRATUsageReport
 OPTIONAL,
    uELocalIPAddressPort                       [253] SEQUENCE OF UELocalIPPortInfo OPTIONAL

}

AccessPointNameNI::= IA5String (SIZE(1..63))
 --
 -- Network Identifier part of APN in dot representation.
 -- For example, if the complete APN is 'apn1a.apn1b.apn1c.mnc022.mcc111.gprs'
 -- NI is 'apn1a.apn1b.apn1c' and is presented in this form in the CDR.

APNSelectionMode::= ENUMERATED
{
 --
 -- See Information Elements TS 29.060, TS 29.274    or TS 29.275
 --
     mSorNetworkProvidedSubscriptionVerified    (0),
     mSProvidedSubscriptionNotVerified          (1),
     networkProvidedSubscriptionNotVerified     (2)
}
```

```
CallDuration::= INTEGER
                --
                -- The call duration is counted in seconds.
                -- For successful calls /sessions / PDP contexts, this is the chargeable
duration.
                -- For call attempts this is the call holding time.
                --


CauseForRecClosing ::= INTEGER
{
 --
 -- In PGW-CDR and SGW-CDR the value servingNodeChange is used for partial record
 -- generation due to Serving Node Address list Overflow
 -- In SGSN servingNodeChange indicates the SGSN change
 --
 -- LCS related causes belong to the MAP error causes acc. TS 29.002
 --
 -- cause codes 0 to 15 are defined 'CauseForTerm' (cause for termination)
 -- All cause values are not relevent to SGW. Refer the spec to find out the
          -- cause values for SGW.
     normalRelease                           (0),
     abnormalRelease                         (4),
     cAMELInitCallRelease                    (5),
     volumeLimit                             (16),
     timeLimit                               (17),
     servingNodeChange                       (18),
     maxChangeCond                           (19),
     managementIntervention                  (20),
     intraSGSNIntersystemChange              (21),
     rATChange                               (22),
     mSTimeZoneChange                        (23),
     sGSNPLMNIDChange                        (24),
     unauthorizedRequestingNetwork           (52),
     unauthorizedLCSClient                   (53),
     positionMethodFailure                   (54),
     unknownOrUnreachableLCSClient           (58),
     listofDownstreamNodeChange              (59)
}


ChangeCondition ::= ENUMERATED
{
     qoSChange                              (0),
     tariffTime                             (1),
     recordClosure                          (2),
     cGI-SAICHange                          (6),    -- bearer modification. CGI-SAI Change
     rAIChange                              (7),    -- bearer modification. RAI Change
     dT-Establishment                       (8),
     dT-Removal                             (9),
     eCGIChange                             (10),    -- bearer modification. ECGI Change
     tAIChange                              (11),    -- bearer modification. TAI Change
     apnAmbrChange                          (50)     -- apn-ambr change

}


ChangeOfCharCondition ::= SEQUENCE
{
        --
        -- qosRequested and qosNegotiated are used in S-CDR only
        -- ePCQoSInformation used in SGW-CDR,PGW-CDR, IPE-CDR, TWAG-CDR and ePDG-CDR only
        -- userLocationInformation is used only in S-CDR, SGW-CDR and PGW-CDR
```

```
        -- chargingID used in PGW-CDR only when Charging per IP-CAN session is active
        -- accessAvailabilityChangeReason and relatedChangeOfCharCondition applicable only
 in PGW-CDR
        -- cPCIoTOptimisationIndicator is used in SGW-CDR only
        --
        qosRequested                    [1] QoSInformation OPTIONAL,
        qosNegotiated                   [2] QoSInformation OPTIONAL,
        dataVolumeGPRSUplink            [3] DataVolumeGPRS OPTIONAL,
        dataVolumeGPRSDownlink          [4] DataVolumeGPRS OPTIONAL,
        changeCondition                 [5] ChangeCondition,
        changeTime                      [6] TimeStamp,
        userLocationInformation         [8] OCTET STRING OPTIONAL,
        ePCQoSInformation               [9] EPCQoSInformation OPTIONAL,
        chargingID                      [10] ChargingID OPTIONAL,
        userCSGInformation              [12] UserCSGInformation OPTIONAL,
        diagnostics                     [13] Diagnostics OPTIONAL,
        rATType                         [15] RATType OPTIONAL,
        uWANUserLocationInformation     [17] UWANUserLocationInfo OPTIONAL,
        cPCIoTEPSOptimisationIndicator [19] CPCIoTEPSOptimisationIndicator OPTIONAL


}

ChargingCharacteristics ::= OCTET STRING (SIZE(2))


ChargingID ::= INTEGER (0..4294967295)
 --
 -- Generated in P-GW, part of IP CAN bearer
 -- 0..4294967295 is equivalent to 0..2**32-1
 --

ChChSelectionMode    ::= ENUMERATED
{
     servingNodeSupplied        (0), -- For S-GW/P-GW
     subscriptionSpecific       (1), -- For SGSN only
     aPNSpecific                (2), -- For SGSN only
     homeDefault                (3), -- For SGSN, S-GW and P-GW
     roamingDefault             (4), -- For SGSN, S-GW and P-GW
     visitingDefault            (5) -- For SGSN, S-GW and P-GW
}

DataVolumeGPRS ::= INTEGER
 --
 -- The volume of data transferred in octets.
 --

DynamicAddressFlag ::= BOOLEAN


EPCQoSInformation ::= SEQUENCE
{
     --
     -- See TS 29.212 for more information
     --
     qCI                            [1] INTEGER,
     maxRequestedBandwithUL         [2] INTEGER OPTIONAL,
     maxRequestedBandwithDL         [3] INTEGER OPTIONAL,
     guaranteedBitrateUL            [4] INTEGER OPTIONAL,
     guaranteedBitrateDL            [5] INTEGER OPTIONAL,
     aRP                            [6] INTEGER OPTIONAL,
     apnAmbrUplink                  [7] INTEGER OPTIONAL,
     apnAmbrDownlink                [8] INTEGER OPTIONAL,
     extendedMaxRequestedBWUL       [9] INTEGER OPTIONAL,
```

```
     extendedMaxRequestedBWDL       [10] INTEGER OPTIONAL,
     extendedGBRUL                  [11] INTEGER OPTIONAL,
     extendedGBRDL                  [12] INTEGER OPTIONAL,
     extendedAPNAMBRUL              [13] INTEGER OPTIONAL ,
     extendedAPNAMBRDL              [14] INTEGER OPTIONAL
}

ETSIAddress::= AddressString
 --
 -- First octet for nature of address, and numbering plan indicator (3 for X.121)
 -- Other octets TBCD
 -- See TS 29.002
 --

GSNAddress::= IPAddress


MSNetworkCapability ::= OCTET STRING (SIZE(1..8))
 -- see TS 24.008

NetworkInitiatedPDPContext ::= BOOLEAN
 --
 -- Set to true if PDP context was initiated from network side
 --

NodeID ::= IA5String (SIZE(1..20))

NumberOfDPEncountered    ::= INTEGER


PDPAddress ::= CHOICE
{
     iPAddress         [0] IPAddress,
     eTSIAddress     [1] ETSIAddress
}

PDPType    ::= OCTET STRING (SIZE(2))
 --
 -- OCTET 1: PDP Type Organization
 -- OCTET 2: PDP Type Number
 -- See TS 29.060 for GTP, TS 29.274 for eGTP and TS 29.275 for PMIP
 --

PLMN-Id    ::= OCTET STRING (SIZE (3))
 --
 -- This is a 1:1 copy from the Routing Area Identity (RAI) IE specified in TS 29.060
 --            as follows:
 -- OCTET 1 of PLMN-Id = OCTET 2 of RAI
 -- OCTET 2 of PLMN-Id = OCTET 3 of RAI
 -- OCTET 3 of PLMN-Id = OCTET 4 of RAI
 --

QoSInformation ::= OCTET STRING (SIZE (4..255))
 --
 -- This    octet string
 -- is a 1:1 copy of the contents (i.e. starting with octet 5) of the "Bearer Quality of
 -- Service" information element specified in TS 29.274
 --

RANSecondaryRATUsageReport ::= SEQUENCE
                -- ]
{
                dataVolumeUplink              [1] DataVolumeGPRS,
                dataVolumeDownlink            [2] DataVolumeGPRS,
```

```
                rANStartTime                    [3] TimeStamp,
                rANEndTime                      [4] TimeStamp,
                secondaryRATType                [5] SecondaryRATType OPTIONAL
}

SecondaryRATType ::= INTEGER
{
                reserved (0),
                nR (1) -- New Radio 5G
}

RATType ::= INTEGER (0..255)
 --
 -- This integer is 1:1 copy of the RAT type value as defined in TS 29.060 for GTP,
 -- TS 29.274 for eGTP and TS 29.275 for PMIP.
 --

UWANUserLocationInfo ::= SEQUENCE
{
     uELocalIPAddress    [0] IPAddress,
     uDPSourcePort       [1] OCTET STRING (SIZE(2)) OPTIONAL,
    sSID               [2] OCTET STRING OPTIONAL,     -- see format in IEEE Std 802.11-2012
 [408]
    bSSID              [3] OCTET STRING OPTIONAL      -- see format in IEEE Std 802.11-2012
 [408]
}

RecordType    ::= INTEGER
{
    -- Record values 0..17 are CS specific.
    -- The contents are defined in TS 32.250

    sGWRecord         (84)
}

ResultCode ::= INTEGER
 -- charging protocol return value, range of 4 byte (0...4294967259)
 -- see Result-Code AVP as used in 3GPP 32.299
 --


ServingNodeType ::= ENUMERATED
{
     sGSN                (0),
     pMIPSGW             (1),
     gTPSGW              (2),
     ePDG                (3),
     hSGW                (4),
     mME                 (5)
}

SGWChange ::= BOOLEAN
 --
 -- present if first record after inter S-GW change
 --

Diagnostics            ::= CHOICE
{
     gsm0408Cause                                    [0] INTEGER,
     -- See TS 24.008
     gsm0902MapErrorValue                    [1] INTEGER,
     -- Note: The value to be stored here corresponds to
     -- the local values defined in the MAP-Errors and
     -- MAP-DialogueInformation modules, for full details
```

```
     -- see TS 29.002
               itu-tQ767Cause                      [2] INTEGER,
     -- See ITU-T Q.767
              networkSpecificCause                [3] ManagementExtension,
     -- To be defined by network operator
              manufacturerSpecificCause     [4] ManagementExtension,
 -- To be defined by manufacturer
              positionMethodFailureCause [5] PositionMethodFailure-Diagnostic,
     -- see TS 29.002
              unauthorizedLCSClientCause [6] UnauthorizedLCSClient-Diagnostic
     -- see TS 29.002
}

IPAddress::= CHOICE
{
     iPBinaryAddress                         IPBinaryAddress,
     iPTextRepresentedAddress    IPTextRepresentedAddress
}

CPCIoTEPSOptimisationIndicator ::= BOOLEAN

IPBinaryAddress::= CHOICE
{
     iPBinV4Address     [0] OCTET STRING (SIZE(4)),
     iPBinV6Address     [1] OCTET STRING (SIZE(16))
}

IPTextRepresentedAddress::= CHOICE
{
 --
 -- IP address in the familiar "dot" notation
 --
     iPTextV4Address     [2] IA5String (SIZE(7..15)),
     iPTextV6Address     [3] IA5String (SIZE(15..45))
}

PositionMethodFailure-Diagnostic ::= ENUMERATED
{
                congestion                                              (0),
                insufficientResources                                   (1),
                insufficientMeasurementData                             (2),
                inconsistentMeasurementData                             (3),
                locationProcedureNotCompleted                           (4),
                locationProcedureNotSupportedByTargetMS                 (5),
                qoSNotAttainable                                        (6),
                positionMethodNotAvailableInNetwork                     (7),
                positionMethodNotAvailableInLocationArea                (8)
}

LocalSequenceNumber ::= INTEGER (0..4294967295)
 --
 -- Sequence number of the record in this node
 -- 0.. 4294967295 is equivalent to 0..2**32-1, unsigned integer in four octets


ManagementExtension ::= SEQUENCE
{
     identifier OBJECT IDENTIFIER,
     significance        [1]         BOOLEAN DEFAULT FALSE,
     information         [2]         ANY DEFINED BY identifier
}

ManagementExtensions ::= SET OF ManagementExtension
```

```
MSISDN::= ISDN-AddressString
                --
 -- See TS 23.003

MSTimeZone::= OCTET STRING (SIZE (2))
 --
 -- 1.Octet: Time Zone and 2. Octet: Daylight saving time, see TS 29.060


TimeStamp::= OCTET STRING (SIZE(9))
                --
                -- The contents of this field are a compact form of the UTCTime format
                -- containing local time plus an offset to universal time. Binary coded
                -- decimal encoding is employed for the digits to reduce the storage and
                -- transmission overhead
                -- e.g. YYMMDDhhmmssShhmm
                -- where
                -- YY     =            Year 00 to 99                    BCD encoded
                -- MM     =            Month 01 to 12                   BCD encoded
                -- DD     =            Day 01 to 31                       BCD encoded
                -- hh     =            hour 00 to 23                    BCD encoded
                -- mm     =            minute 00 to 59                BCD encoded
                -- ss     =            second 00 to 59                BCD encoded
                -- S      =            Sign 0 = "+", "-"             ASCII encoded
                -- hh     =            hour 00 to 23                    BCD encoded
                -- mm     =            minute 00 to 59                BCD encoded
                --

UELocalIPPortInfo   ::= SEQUENCE
{
    --
    -- The S2b user Local IP Port Information
    --
    uELocalIPAddress                          [0] IPAddress OPTIONAL,
    uDPSourcePort                              [1] INTEGER OPTIONAL
}

UELocalIPAddress::= IPAddress
UDPSourcePort           ::= INTEGER


UnauthorizedLCSClient-Diagnostic ::= ENUMERATED
{
                noAdditionalInformation                                    (0),
                clientNotInMSPrivacyExceptionList                          (1),
                callToClientNotSetup                                       (2),
                privacyOverrideNotApplicable                               (3),
                disallowedByLocalRegulatoryRequirements                    (4),
                unauthorizedPrivacyClass                                   (5),
                unauthorizedCallSessionUnrelatedExternalClient             (6),
                unauthorizedCallSessionRelatedExternalClient               (7)
}

CSGAccessMode ::= ENUMERATED
{
                 closedMode  (0),
                 hybridMode  (1)
}
CSGId         ::= OCTET STRING (SIZE(4))
                --
                -- Defined in 23.003. Coded according to TS 29.060 for GTP, and in TS
29.274
                -- for eGTP.
                -- 24.008
```

```
                --
UserCSGInformation          ::= SEQUENCE
{
                cSGId                                           [0] CSGId,
                cSGAccessMode                                   [1] CSGAccessMode,
                cSGMembershipIndication                         [2] NULL OPTIONAL
}
TBCDSTRING ::= OCTET STRING
ISDN-AddressString ::= OCTET STRING
IMEI ::= TBCDSTRING (SIZE(8))
IMSI ::= TBCDSTRING (SIZE(3..8))
maxAddressLength    INTEGER ::= 20
AddressString ::= OCTET STRING (SIZE (1..maxAddressLength))
END
```

SGW Charging OAM Support

This section describes operations, administration, and maintenance information for this feature.

Bulk Statistics

SGW Charging CDR Statistics

sgw_charging_cdr counter

```
sgw_charging_cdr{action="close_final",app_name="SMF",cause="abnormalRelease",
cluster="Local",data_center="DC",event="AbnormalRelease",gr_instance_id="1",instance_id="0",
pdn_plmn_type="visitor",pdn_type="ipv4v6",service_name="sgw-service"} 1
sgw_charging_cdr{action="close_final",app_name="SMF",cause="normalRelease",
cluster="Local",data_center="DC",event="NormalRelease",gr_instance_id="1",instance_id="0",
pdn_plmn_type="visitor",pdn_type="ipv4v6",service_name="sgw-service"} 22
sgw_charging_cdr{action="close_final",app_name="SMF",cause="sGWChange",
cluster="Local",data_center="DC",event="SGWChange",gr_instance_id="1",instance_id="0",
pdn_plmn_type="visitor",pdn_type="ipv4v6",service_name="sgw-service"} 3
sgw_charging_cdr{action="close_interim",app_name="SMF",cause="maxChangeCond",
cluster="Local",data_center="DC",event="QoSChange",gr_instance_id="1",instance_id="0",
pdn_plmn_type="visitor",pdn_type="ipv4v6",service_name="sgw-service"} 3
sgw_charging_cdr{action="close_interim",app_name="SMF",cause="maxChangeCond",
cluster="Local",data_center="DC",event="ServingNodeChange",gr_instance_id="1",instance_id="0",
pdn_plmn_type="visitor",pdn_type="ipv4v6",service_name="sgw-service"} 5
sgw_charging_cdr{action="close_interim",app_name="SMF",cause="timeLimit",
cluster="Local",data_center="DC",event="TimeLimit",gr_instance_id="1",instance_id="0",
pdn_plmn_type="visitor",pdn_type="ipv4v6",service_name="sgw-service"} 56
sgw_charging_cdr{action="close_interim",app_name="SMF",cause="volumeLimit",
cluster="Local",data_center="DC",event="VolumeLimit",gr_instance_id="1",instance_id="0",
pdn_plmn_type="visitor",pdn_type="ipv4v6",service_name="sgw-service"} 3
sgw_charging_cdr{action="open",app_name="SMF",cause="",cluster="Local",
data_center="DC",event="QoSChange",gr_instance_id="1",instance_id="0",pdn_plmn_type="visitor",
pdn_type="ipv4v6",service_name="sgw-service"} 3
sgw_charging_cdr{action="open",app_name="SMF",cause="",cluster="Local",
data_center="DC",event="SGWChange",gr_instance_id="1",instance_id="0",pdn_plmn_type="visitor",
pdn_type="ipv4v6",service_name="sgw-service"} 3
sgw_charging_cdr{action="open",app_name="SMF",cause="",cluster="Local",
data_center="DC",event="ServingNodeChange",gr_instance_id="1",instance_id="0",pdn_plmn_type="visitor",
```

```
pdn_type="ipv4v6",service_name="sgw-service"} 5
sgw_charging_cdr{action="open",app_name="SMF",cause="",cluster="Local",
data_center="DC",event="StartAccounting",gr_instance_id="1",instance_id="0",pdn_plmn_type="visitor",
pdn_type="ipv4v6",service_name="sgw-service"} 26
sgw_charging_cdr{action="open",app_name="SMF",cause="",cluster="Local",
data_center="DC",event="TimeLimit",gr_instance_id="1",instance_id="0",pdn_plmn_type="visitor",
pdn_type="ipv4v6",service_name="sgw-service"} 56
sgw_charging_cdr{action="open",app_name="SMF",cause="",cluster="Local",
data_center="DC",event="VolumeLimit",gr_instance_id="1",instance_id="0",pdn_plmn_type="visitor",
pdn_type="ipv4v6",service_name="sgw-service"} 3
```

SGW Charging CDR Container Statistics

sgw_charging_cdr_container counter

```
sgw_charging_cdr_container{action="close",app_name="SMF",change_condition="qoSChange",
cluster="Local",data_center="DC",event="QoSChange",gr_instance_id="1",instance_id="0",
pdn_plmn_type="visitor",pdn_type="ipv4v6",service_name="sgw-service"} 6
sgw_charging_cdr_container{action="close",app_name="SMF",change_condition="recordClosure",
cluster="Local",data_center="DC",event="AbnormalRelease",gr_instance_id="1",instance_id="0",
pdn_plmn_type="visitor",pdn_type="ipv4v6",service_name="sgw-service"} 1
sgw_charging_cdr_container{action="close",app_name="SMF",change_condition="recordClosure",
cluster="Local",data_center="DC",event="NormalRelease",gr_instance_id="1",instance_id="0",
pdn_plmn_type="visitor",pdn_type="ipv4v6",service_name="sgw-service"} 22
sgw_charging_cdr_container{action="close",app_name="SMF",change_condition="recordClosure",
cluster="Local",data_center="DC",event="SGWChange",gr_instance_id="1",instance_id="0",
pdn_plmn_type="visitor",pdn_type="ipv4v6",service_name="sgw-service"} 3
sgw_charging_cdr_container{action="close",app_name="SMF",change_condition="recordClosure",
cluster="Local",data_center="DC",event="ServingNodeChange",gr_instance_id="1",instance_id="0",
pdn_plmn_type="visitor",pdn_type="ipv4v6",service_name="sgw-service"} 5
sgw_charging_cdr_container{action="close",app_name="SMF",change_condition="recordClosure",
cluster="Local",data_center="DC",event="TimeLimit",gr_instance_id="1",instance_id="0",
pdn_plmn_type="visitor",pdn_type="ipv4v6",service_name="sgw-service"} 56
sgw_charging_cdr_container{action="close",app_name="SMF",change_condition="recordClosure",
cluster="Local",data_center="DC",event="VolumeLimit",gr_instance_id="1",instance_id="0",
pdn_plmn_type="visitor",pdn_type="ipv4v6",service_name="sgw-service"} 3
sgw_charging_cdr_container{action="open",app_name="SMF",change_condition="",cluster="Local",
data_center="DC",event="QoSChange",gr_instance_id="1",instance_id="0",pdn_plmn_type="visitor",
pdn_type="ipv4v6",service_name="sgw-service"} 6
sgw_charging_cdr_container{action="open",app_name="SMF",change_condition="",cluster="Local",
data_center="DC",event="SGWChange",gr_instance_id="1",instance_id="0",pdn_plmn_type="visitor",
pdn_type="ipv4v6",service_name="sgw-service"} 3
sgw_charging_cdr_container{action="open",app_name="SMF",change_condition="",cluster="Local",
data_center="DC",event="ServingNodeChange",gr_instance_id="1",instance_id="0",pdn_plmn_type="visitor",
pdn_type="ipv4v6",service_name="sgw-service"} 5
sgw_charging_cdr_container{action="open",app_name="SMF",change_condition="",cluster="Local",
data_center="DC",event="StartAccounting",gr_instance_id="1",instance_id="0",pdn_plmn_type="visitor",
pdn_type="ipv4v6",service_name="sgw-service"} 26
sgw_charging_cdr_container{action="open",app_name="SMF",change_condition="",cluster="Local",
data_center="DC",event="TimeLimit",gr_instance_id="1",instance_id="0",pdn_plmn_type="visitor",
pdn_type="ipv4v6",service_name="sgw-service"} 56
sgw_charging_cdr_container{action="open",app_name="SMF",change_condition="",cluster="Local",
data_center="DC",event="VolumeLimit",gr_instance_id="1",instance_id="0",pdn_plmn_type="visitor",
pdn_type="ipv4v6",service_name="sgw-service"}
```

SGW Sx Report Statistics

sgw_sx_session_report_stats counter

```
sgw_sx_session_report_stats{app_name="SMF",cluster="Local",data_center="DC",
gr_instance_id="1",instance_id="0",service_name="sgw-service",status="success",
sx_session_report_type="USAR"} 55
```

sgw_sx_usage_report_stats counter

```
sgw_sx_usage_report_stats{app_name="SMF",cluster="Local",data_center="DC",
gr_instance_id="1",instance_id="0",service_name="sgw-service",status="success"}
95
```

GTPP-EP Statistics

gtpp_received_cdrs_total counter

```
gtpp_received_cdrs_total{app_name="SMF",cluster="Local",data_center="DC",dictionary="custom24",
gtpp_profile="pf1",instance_id="0",service_name="gtpp-ep"} 7
```

gtpp_processed_cdrs_total counter

```
gtpp_processed_cdrs_total{app_name="SMF",cluster="Local",data_center="DC",dictionary="custom24",
gtpp_profile="pf1",instance_id="0",service_name="gtpp-ep",status="success"} 7
```

gtpp_batched_cdrs_total gauge

```
gtpp_batched_cdrs_total{app_name="SMF",cluster="Local",data_center="DC",dictionary="custom24",
gtpp_profile="pf1",instance_id="0",service_name="gtpp-ep",status="batch_success"}
 2
```

gtpp_batch_flush_millis_total counter

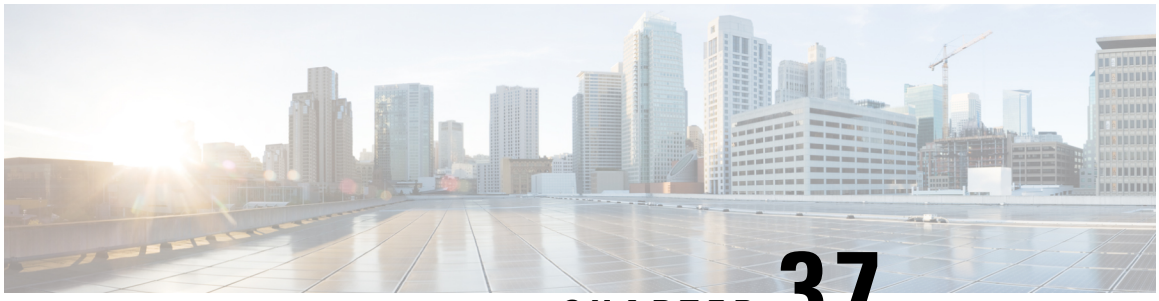
```
gtpp_batch_flush_millis_total{app_name="SMF",cluster="Local",data_center="DC",dictionary="custom24",
gtpp_profile="pf1",instance_id="0",service_name="gtpp-ep",status="batch_success"}
 1126.000588626
```

gtpp_batch_flush_duration_histogram_total counter

```
gtpp_batch_flush_duration_histogram_total{app_name="SMF",bin=">5000ms",cluster="Local",data_center="DC",
dictionary="custom24",gtpp_profile="pf1",instance_id="0",service_name="gtpp-ep",status="batch_success"}
 6
```

gtpp_asn1field_encoding_failures_total

```
gtpp_asn1field_encoding_failures_total{app_name="SMF",cluster="Local",data_center="DC",gtpp_profile="pf1",
dictionary="custom24",asn1_field="ServedIMSI",reason="Constraint
Violation",gr_instance_id="1",service_name="gtpp-ep"}1
```



CHAPTER 37

SGW Relocation Support

Feature Summary and Revision History

Summary Data

Table 159: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 160: Revision History

Revision Details	Release
First introduced.	2021.01.0

Feature Description

This feature supports following procedures:

- S1 based SGW Relocation

- X2 based SGW Relocation
- TAU SGW Relocation
- 5G to 4G SGW Relocation

This feature also supports ePCO Indication flag at the PDN level, if it receives this indication in CS Request during Initial attach or PDN connection or SGW relocation.

SGW triggers a Modify Bearer Request to PGW in the following scenario:

- The source MME supports ePCO and the target MME does not support it.
- The target MME supports ePCO and the source MME does not support it.

Note When 4G SGW relocation Create Session Request message receives 5GS Interworking Indication (5GSIWKI), then set SGW relocation type as 5G.

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for SGW relocation feature.

X2 Handover SGW Relocation to cnSGW-C Call Flow

This section describes the X2 handover SGW relocation to cnSGW-C call flow.

Figure 88: X2 Handover SGW Relocation to cnSGW-C Call Flow

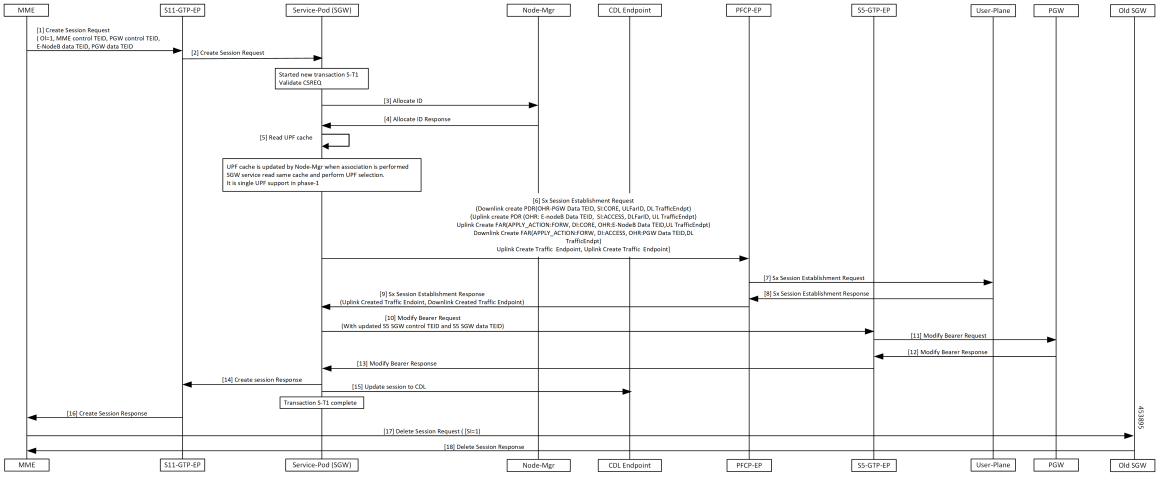


Table 161: X2 Handover SGW Relocation to cnSGW-C Call Flow Description

Step	Description
1	MME sends Create Session Request message to GTPC-EP ingress with the following: • OI flag set • MME Control TEID • PGW Control TEID • eNodeB Data TEID • PGW Data TEID Establishes new transaction at GTPC-EP ingress.
2	SGW service POD receives Create Session Request.
3	SGW service POD Create a new transaction S-T1.
4	Validate Create Session Req.
5	NodeMgr allocates TEID. SGW service POD reads the UPF cache and performs UPF selection.
6	PFCP-EP receives Sx Session Establishment Request from SGW service POD with the uplink and downlink Create PDRs/FARs (Apply Action as Forward)/CTEs.
7	PFCP-EP forwards Sx Session Establishment Request to UPF.
8	PFCP-EP receives Sx Session Establishment Response from UPF with Created CTEs.
9	SGW service POD receives Sx Session Establishment Response from PFCP-EP.
10	Modify Bearer Request with updated S5 SGW Control TEID and S5 SGW Data TEID sent from the SGW service POD to GTPC-EP.
11	PGW receives Modify Bearer Request message from GTPC-EP.
12	GTCP-EP receives Modify Bearer Response from PGW.
13	SGW service POD receives Modify Bearer Response from GTPC-EP.
14	SGW service POD forwards Create Session Response to GTPC-EP ingress.
15	Updated session at CDL. Transaction S-T1 completed.
16	GTPC-EP ingress forwards Create Session Response to MME.
17	MME sends Delete Session Request with SI=1 to old SGW and receives Delete Session Response. Call cleared in old SGW.

S1 Handover SGW Relocation to cnSGW-C Call Flow

This section describes the S1 handover SGW Relocation to cnSGW-C call flow.

Figure 89: S1 Handover SGW Relocation to cnSGW-C Call Flow

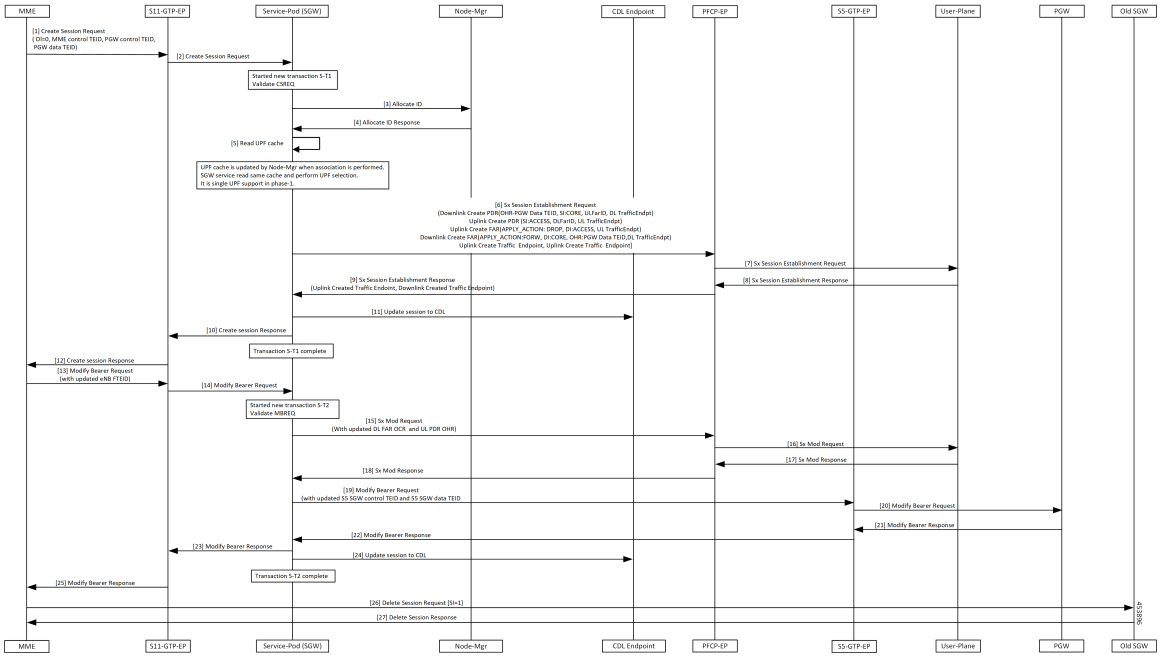


Table 162: S1 Handover SGW Relocation to cnSGW-C Call Flow Description

Step	Description
1	MME sends Create Session Request message to GTPC-EP ingress with the following: • OI flag unset • MME Control TEID • PGW Control TEID • PGW Data TEID Establishes new transaction at GTPC-EP ingress.
2	SGW service POD receives Create Session Request.
3	Create a new transaction S-T1.
4	Validate Create Session Req.
5	NodeMgr allocates TEID. SGW service reads the UPF cache and performs UPF selection.
6	PFCP-EP receives Sx Session Establishment Request from SGW service POD with the following: • Uplink and downlink Create PDRs/FARs (Apply Action as Forward)/CTEs

Step	Description
7	PFCP-EP forwards Sx Session Establishment Request to UPF
8	PFCP-EP receives Sx Session Establishment Response from UPF with Created CTEs.
9	SGW service POD receives Sx Session Establishment Response from PFCP-EP.
10	SGW service POD forwards Create Session Response to GTPC-EP ingress.
11	Updated session at CDL. Transaction S-T1 completed.
12	GTPC-EP ingress forwards Create Session Response to MME.
13	GTPC-EP ingress receives Modify Bearer Req with updated eNodB FTEID from MME.
14	GTPC-EP ingress forwards Modify Bearer Req to SGW service POD. Creates new transaction-T2.
15	PFCP-EP receives Sx Mod Req from SGW service POD with the updated downlink FAR and uplink PDR.
16	PFCP-EP forwards Sx Mod Req to UPF.
17	PFCP-EP receives Sx Mod Response from UPF.
18	SGW receives Sx Mod Response from PFCP-EP.
19	SGW service POD sends Modify Bearer Request with updated S5 SGW Control TEID and S5 SGW Data TEID to GTPC-EP.
20	GTPC-EP forwards Modify Bearer Request to PGW.
21	GTPC-EP receives Modify Bearer Response from PGW.
22	SGW service POD receives Modify Bearer Response from GTPC-EP.
23	GTPC-EP ingress receives Modify Bearer Response from SGW service POD.
24	Session updated at CDL. Transaction S-T2 completed.
25	GTPC-EP ingress forwards Modify Bearer Response to MME.
26	MME sends Delete Session Request with SI=1 to old SGW and receives Delete Session Response. Call cleared in old SGW.

TAU X2 Handover SGW Relocation to cnSGW-C Call Flow

This section describes the TAU X2 handover SGW telocation to cnSGW-C call flow.

Figure 90: TAU X2 Handover SGW Relocation to cnSGW-C Call Flow

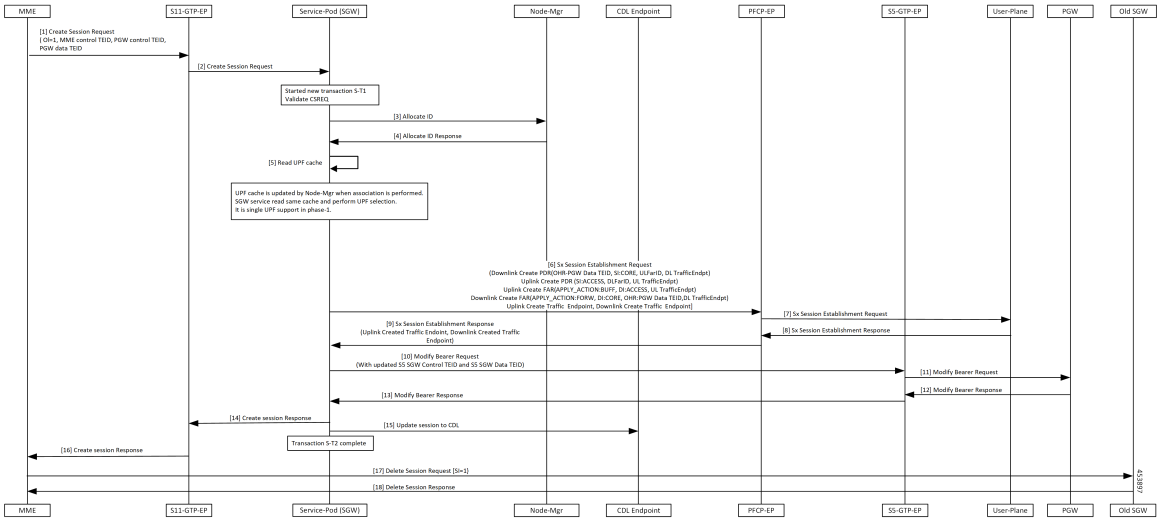


Table 163: TAU X2 Handover SGW Relocation to cnSGW-C Call Flow Description

Step	Description
1	MME sends Create session Req to GTPC-EP ingress with the following: • OI flag set • MME Control TEID • PGW Control TEID • PGW Data TEID Establishes new transaction at GTPC-EP ingress.
2	GTPC-EP ingress forwards Create Session req to SGW service POD.
3	SGW service POD receives Create Session Req. Create a new transaction S-T1.
4	Validate CSReq. NodeMgr performs TEID allocation.
5	SGW service reads UPF Cache and performs UPF selection.
6	PFCP-EP receives Sx Session Establishment Req from SGW service POD with the following: • Uplink and downlink Create PDRs/FARs(ApplyAction as Forward for the uplink FAR)/CTEs.
7	PFCP-EP forwards Sx Session Establishment Req to UPF.
8	PFCP-EP receives Sx Session Establishment Response from UPF.
9	SGW service POD receives Sx Session Establishment Response from PFCP-EP.

Step	Description
10	SGW service POD sends Modify Bearer Req with updated S5 SGW Control TEID and S5 SGW Data TEID to GTPC-EP.
11	GTPC-EP forwards Modify Bearer Request to PGW.
12	GTPC-EP receives Modify Bearer Response from PGW.
13	GTPC-EP forwards Modify Bearer Response to SGW service POD.
14	SGW service POD forwards Create Session Response to GTPC-EP ingress.
15	Session updated at CDL. Transaction S-T1 completed.
16	GTPC-EP ingress forwards Create Session Response to MME.
17	MME sends Delete Session Request with SI=1 sent to old SGW and receives Delete Session Response. Call cleared in old SGW.

X2 Handover SGW Relocation to CN-SGW (Multi PDN) Call Flow

This section describes the X2 handover SGW relocation to CN-SGW (Multi PDN) to cnSGW-C call flow.

Figure 91: X2 Handover SGW Relocation to CN-SGW (Multi PDN) Call Flow

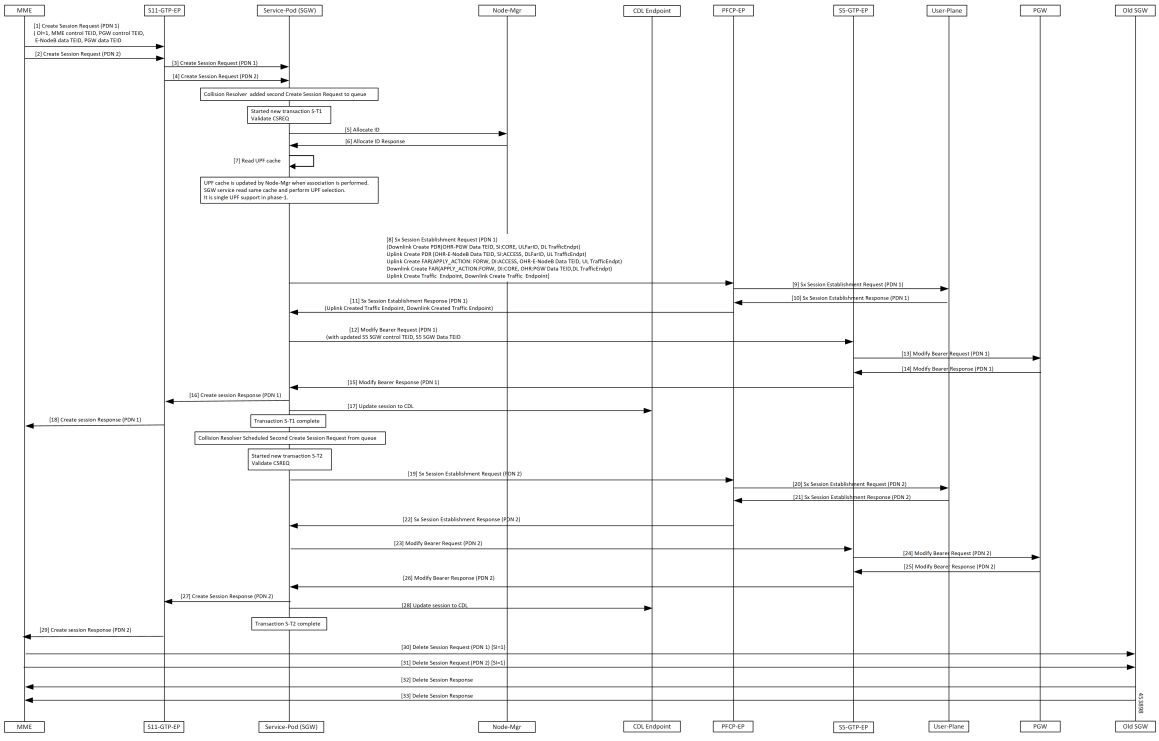


Table 164: X2 Handover SGW Relocation to CN-SGW (Multi PDN) Call Flow Description

Step	Description
1, 2	MME sends Create Session Req for both PDNs to GTPC-EP ingress with the following: • OI flag set • MME Control TEID • PGW Control TEID • eNodeB Data TEID • PGW Data TEID Establishes new transactions at GTPC-EP ingress.
3, 4	SGW service POD receives Create Session Req for both PDNs from PFCP-EP ingress. Collision resolver added Create Session Req for PDN 2 in queue.
5	Create a new transaction S-T1 for Create Session Req for PDN1 Validate CSReq.
6	NodeMgr allocates TEID.
7	SGW service POD reads UPF Cache and performs UPF selection.
8	PFCP-EP receives Sx Session Establishment Req from SGW service POD for PDN 1 with the following: • Uplink and downlink Create PDRs/FARs(ApplyAction as Forward)/CTEs.
9	PFCP-EP forwards Sx Session Establishment Req for PDN 1 to UPF.
10	UPF sends Sx Session Establishment Response for PDN 1 to PFCP-EP with Created CTEs.
11	PFCP-EP forwards Sx Session Establishment Response for PDN 1 to SGW service POD.
12	SGW service POD sends Modify Bearer Req for PDN 1 to GTPC-EP with the following: • Updated S5 SGW Control TEID • S5 SGW Data TEID
13	GTPC-EP forwards Modify Bearer Req for PDN 1 to PGW.
14	PGW sends Modify Bearer Response for PDN 1 to GTPC-EP.
15	GTPC-EP forwards Modify Bearer Response for PDN 1 to SGW service POD.
16	SGW service forwards Create Session Response for PDN 1 to GTPC-EP ingress.
17	Session updated at CDL. Transaction S-T1 completed. Collision resolver schedules Create Session Req for PDN 2 from queue.

Step	Description
18	GTPC-EP ingress forwards Create Session Response for PDN 1 to MME.
19 - 27	Repeat steps from 8 to 16 for PDN2.
28	Session updated at CDL. Transaction S-T2 completed.
29	GTPC-EP ingress forwards Create Session Response for PDN 2 to MME.
30 - 33	MME sends Delete Session Request for both PDNs with SI=1 to old SGW and receives Delete Session Response. Call cleared in old SGW.

S1 Handover SGW Relocation to CN-SGW (Multi PDN) Call Flow

This section describes the S1 handover SGW relocation to CN-SGW (Multi PDN) to CN-SGW call flow.

Figure 92: S1 Handover SGW Relocation to CN-SGW (Multi PDN) Call Flow

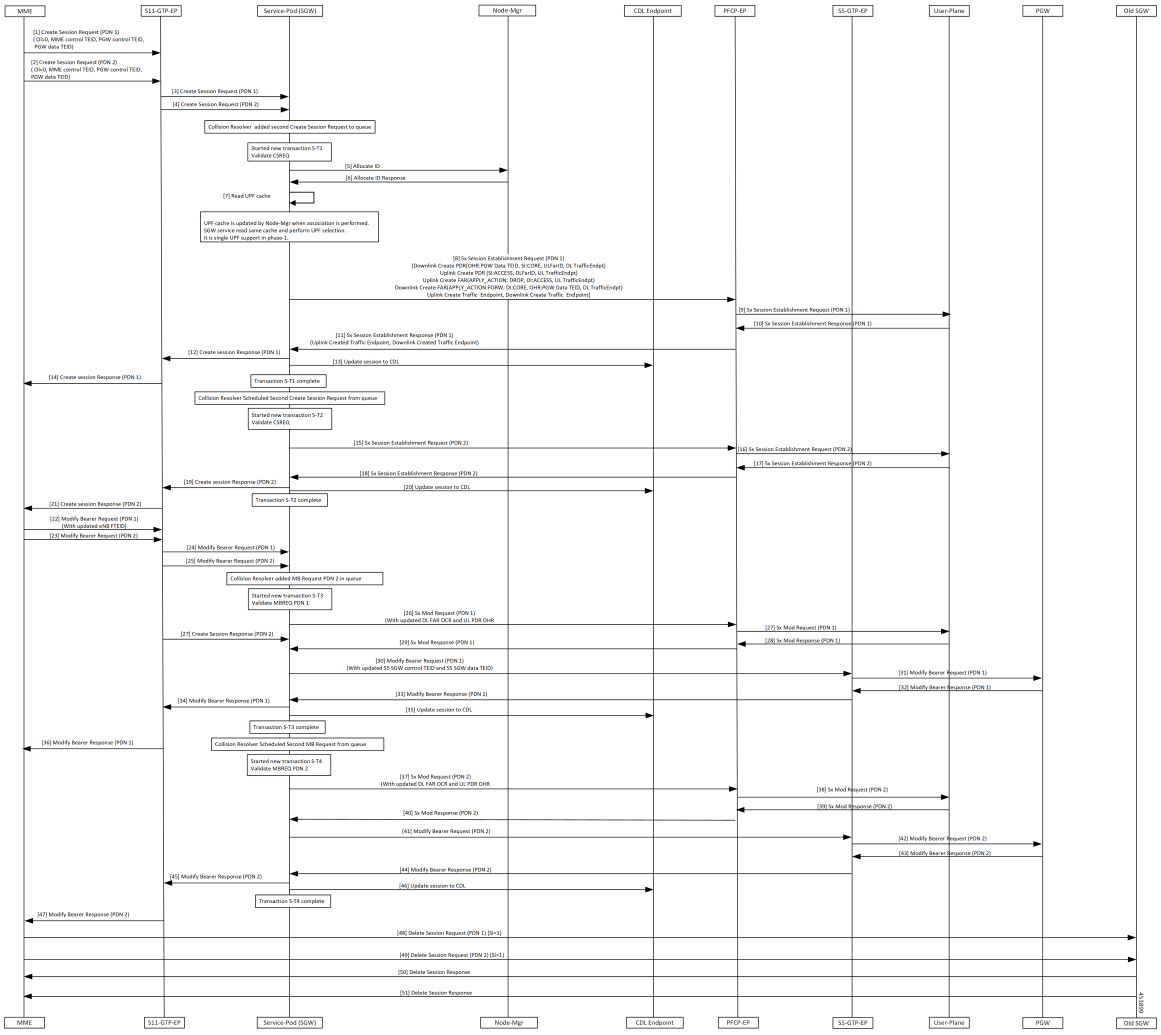


Table 165: S1 Handover SGW Relocation to CN-SGW (Multi PDN) Call Flow Description

Step	Description
1, 2	GTCP-EP ingress receives Create Session Req for both the PDNs with the following: • Ol flag unset • MME control TEID • PGW control TEID • PGW Data TEID Establishes new transaction at GTPC-EP ingress.
3, 4	SGW service POD receives Create Session Req for both the PDNs from GTPC-EP ingress. Collision resolver added Create Session Req for PDN 2 in queue. Create a new transaction S-T1.
5	Validate CSReq.
6	NodeMgr allocates TEID.
7	SGW service reads UPF Cache and performs UPF selection.
8	PFCP-EP receives Sx Session Establishment Req from SGW service POD for PDN 1 with the following: • Uplink and downlink Create PDRs/FARs/CTEs.
9	PFCP-EP forwards Sx Session Establishment Req for PDN 1 to UPF.
10	PFCP-PE receives Sx Session Establishment Response for PDN 1 from UPF with Created CTEs.
11	SGW service POD receives Sx Session Establishment Response for PDN 1 from PFCP-EP.
12	SGW service POD forwards Create Session Response for PDN 1 to GTPC-EP ingress.
13	Session updated at CDL. Transaction S-T1 completed. Collision resolver scheduled Create Session Req for PDN 2 from queue.
14	GTPC-EP ingress forwards Create Session Response for PDN 1 to MME.
15–21	Repeat steps 11–14 for PDN2(S-T2).
22, 23	GTPC-EP ingress receives Modify Bearer Req for both the PDNs with updated eNodB FTEID from MME.
24, 25	GTPC-EP ingress forwards Modify Bearer Req to both PDNs to SGW service POD. Collision resolver added Modify Bearer Req for PDN 2 in the queue. Create a new transaction S-T3.

Step	Description
26	PFCP-EP receives Sx Session Modification Req for PDN 1 from SGW service POD with the updated downlink FAR and uplink PDR.
27	PFCP-EP forwards Sx Session Modification Req for PDN 1 to UPF.
28	UPF sends Sx Session Modification Response for PDN 1 to PFCP-EP.
29	SGW service POD receives Sx Modify Response for PDN 1 from PFCP-EP.
30	GTPC-EP receives Modify Bearer Req for PDN 1 from SGW service POD with the following: • Updated S5 SGW Control TEID and S5 SGW Data TEID.
31	GTPC-EP forwards Modify Bearer Req for PDN 1 to PGW.
32	GTPC-EP receives Modify Bearer Response for PDN 1 from PGW.
33	GTPC-EP forwards Modify Bearer Response for PDN 1 to SGW service POD.
34	SGW service POD forwards Modify Bearer Response for PDN 1 to GTPC-EP ingress.
35	Session updated at CDL.
36	GTPC-EP ingress forwards Modify Bearer Response for PDN 1 to MME.
37	SGW service POD sends Modify Bearer Req for PDN 2 to PFCP-EP. Transaction S-T3 completed. Collision resolver schedules Modify Bearer Req to PDN 2.
38–40	Repeat steps 27,28, 29 for PDN 2.
41	SGW service POD sends Modify Bearer request for PDN 2 to GTPC-EP.
42–47	Repeat steps 31–36 for PDN 2.
48, 49	MME sends Delete Session Request for both the PDNs with SI=1 sent to old SGW.
50	MME receives Delete Session Response. Call cleared in old SGW.

X2 Handover SGW Relocation with Bearer Context Marked for Removal Call Flow

This section describes the X2 handover SGW relocation with bearer context marked for removal call flow.

Figure 93: X2 Handover SGW Relocation with Bearer Context Marked for Removal Call Flow

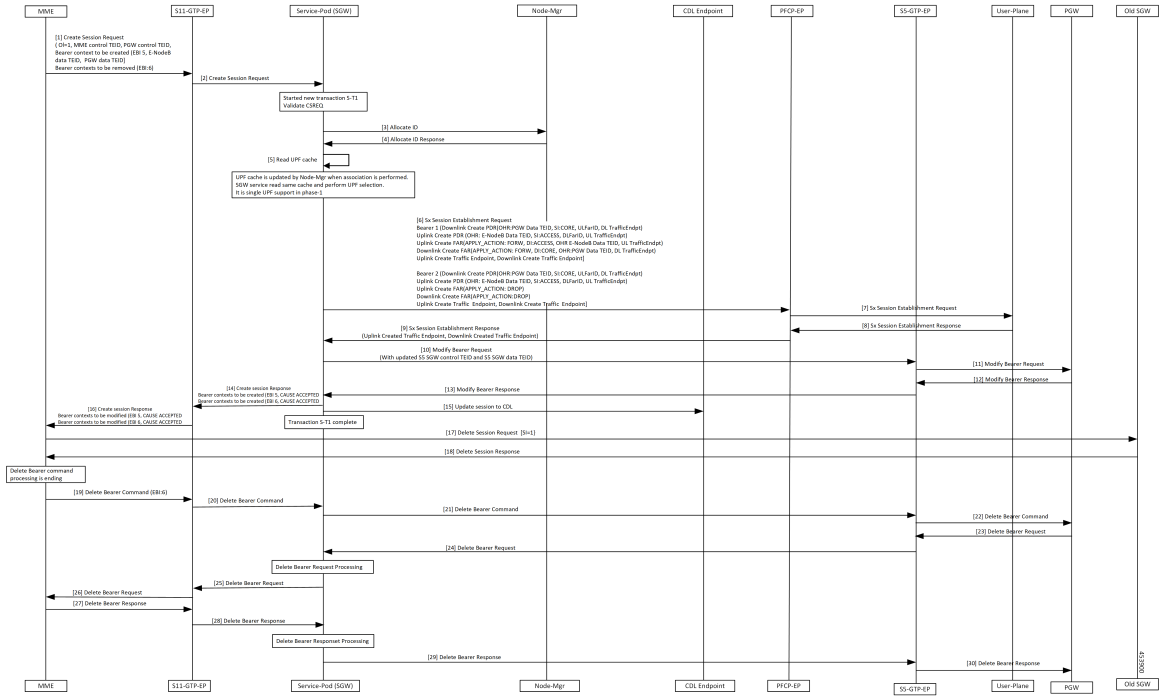


Table 166: X2 Handover SGW Relocation with Bearer Context Marked for Removal Call Flow Description

Step	Description
1	GTPC-EP ingress receives Create Session Req with the following: • OI flag set • MME Control TEID • PGW Control TEID • new Bearer Contexts to create (EBI:5, eNodeB Data TEID and PGW Data TEID) • Bearer context to delete (EBI: 6) Establishes new transaction at GTPC-EP.
2	GTPC-EP ingress forwards Create Session Req to SGW service POD.
3	SGW service POD receives Create Session Req. Create a new transaction S-T1.
4	Validate CSReq. NodeMgr allocates TEID.
5	SGW service POD reads UPF Cache and performs UPF selection.

Step	Description
6	PFCP-EP receives Sx Session Establishment Req from SGW service POD with the following: • Uplink and downlink Create PDRs/FARs (ApplyAction as Forward for EBI 5 and as Drop EBI 6)/CTEs.
7	PFCP-EP forwards Sx Session Establishment Req to UPF.
8	PFCP-EP receives Sx Session Establishment Response from UPF with Created CTEs.
9	SGW service POD receives Sx Session Establishment Response from PFCP-EP.
10	SGW service POD sends Modify Bearer Req with updated S5 SGW Control TEID and S5 SGW Data TEID to GTPC-EP.
11	GTPC-EP forwards Modify Bearer Request to PGW.
12	GTPC-EP receives Modify Bearer Response from PGW.
13	GTPC-EP forwards Modify Bearer Response to SGW service POD.
14	SGW service POD sends Create Session Response to GTPC-EP ingress with cause Accepted for both Bearer Contexts.
15	Session updated at CDL. Transaction S-T1 completed.
16	GTPC-EP ingress forwards Create Session Response to MME.
17	MME sends Delete Session Request with SI=1 sent to old SGW.
18	MME receives Delete Session Response. Call cleared in old SGW.
19	GTPC-EP ingress receives Delete Bearer Command for Bearer Context from MME to delete (EBI 6).
20	SGW service POD receives Delete Bearer Command from GTPC-EP ingress.
21	SGW service POD forwards Delete Bearer Command to GTPC-EP.
22	GTPC-EP forwards Delete Bearer Command to PGW.
23	PGW responds with Delete Bearer Request (EBI 6) to GTPC-EP.
24	GTPC-EP forwards Delete Bearer Request to SGW service POD.
25	SGW service POD processes Delete Bearer Request and sends to GTPC-EP.
26	GTPC-EP ingress forwards Delete Bearer request to MME.
27	MME responds with the Delete Bearer Response to GTPC-EP ingress.
28	GTPC-EP ingress forwards Delete Bearer Response to SGW service POD.
29	SGW service POD processes Delete Bearer Response and sends to GTPC-EP.

Step	Description
30	GTPC-EP forwards Delete Bearer Response to PGW.

S1 Handover SGW Relocation with Bearer Context Marked for Removal Call Flow

This section describes the S1 handover SGW relocation with bearer context marked for removal call flow.

Figure 94: S1 Handover SGW Relocation with Bearer Context Marked for Removal Call Flow

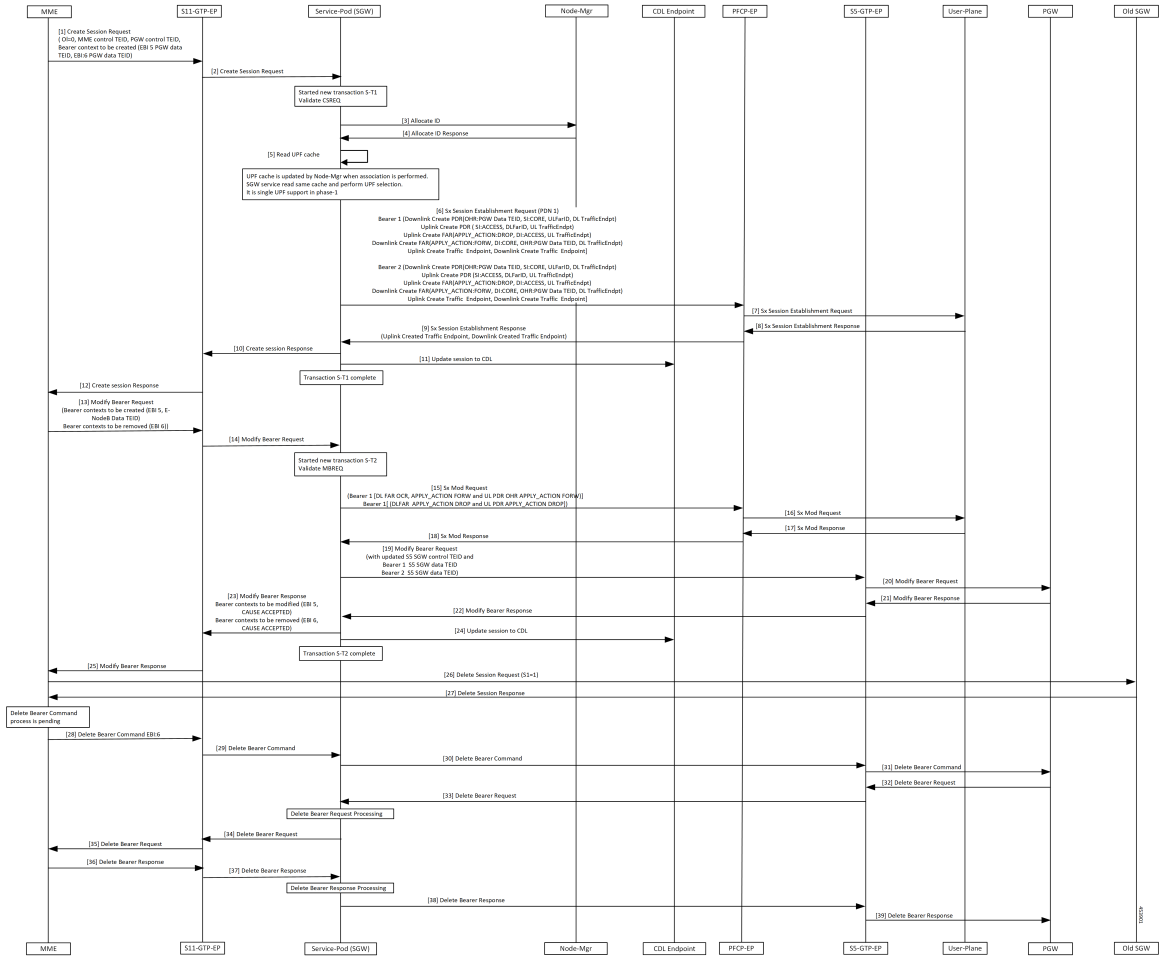


Table 167: S1 Handover SGW Relocation with Bearer Context Marked for Removal Call Flow Description

Step	Description
1	GTPC-EP ingress receives Create Session Request from MME with the following: • OI flag unset • MME Control TEID • PGW Control TEID • Bearer context to create (EBI:5, PGW Data TEID, EBI:6, PGW Data TEID) Establishes new transaction at GTPC-EP ingress.
2	GTPC-EP ingress forwards Create Session req to SGW service POD.
3	SGW service POD receives Create Session Req. Create a new transaction S-T1.
4	Validate CSReq. NodeMgr allocates TEID.
5	SGW service reads UPF cache and performs UPF selection.
6	PFCP-EP receives Sx Session Establishment Req from SGW service with the following: • Uplink and downlink Create PDRs/FARs(ApplyAction as Forward for EBI 5 and as Drop EBI 6)/CTEs.
7	PFCP-EP forwards Sx Session Establishment Req to UPF.
8	PFCP-EP receives Sx Session Establishment Response from UPF with Created CTEs.
9	SGW service receives Sx Session Establishment Response from PFCP-EP.
10	SGW forwards Sx Session Establishment Response to GTPC-EP ingress.
11	Session updated at CDL. Transaction S-T1 completed.
12	GTPC-EP ingress sends Create Session Response to MME.
13	GTPC-EP ingress receives Modify Bearer Req with the following: • Updated eNodeB FTEID with new Bearer Contexts (here EBI 5) and removed (here EBI 6).
14	GTPC-EP forwards Modify Bearer Req to SGW.
15	Create a new transaction S-T2. PFCP-EP receives Sx Session Modification Req from SGW service POD with the following: • Updated downlink FAR and uplink PDR (Apply Action as DROP for Bearer 2).
16	PFCP-EP forwards Sx Session Modification Req forwarded to UPF.

Step	Description
17	UPF sends Sx Modification Response to PFCP-EP
18	PFCP-EP forwards Sx Modification Response to SGW service POD.
19	SGW service POD sends Modify Bearer Req with updated S5 SGW Control TEID and S5 SGW Data TEID to GTPC-EP.
20	GTPC-EP forwards Modify Bearer Request to PGW.
21	GTPC-EP receives Modify Bearer Response from PGW.
22	GTPC-EP forwards Modify Bearer Response to SGW service POD.
23	SGW service POD forwards Create Session Response to GTPC-EP ingress with cause Accepted for both Bearer Contexts.
24	Session updated at CDL. Transaction S-T2 completed.
25	GTPC-EP ingress sends Modify Bearer Response to MME.
26	MME sends Delete Session Request with SI=1 to old SGW.
27	MME receives Delete Session Response. Call cleared in old SGW.
28	GTPC-EP ingress receives Delete Bearer Command from MME for BearerContext to delete (EBI 6).
29	SGW service POD receives Delete Bearer Command from GTPC-EP ingress.
30	SGW service POD forwards Delete Bearer Command to GTPC-EP.
31	GTPC-EP forwards Delete Bearer Command to PGW.
32	PGW responds with Delete Bearer Request (EBI 6) to GTPC-EP.
33	GTPC-EP sends Delete Bearer Request to SGW service POD.
34	SGW service POD processes Delete Bearer Request and sends to GTPC-EP ingress.
35	GTPC-EP ingress sends Delete Bearer request to MME.
36	MME responds with the Delete Bearer Response to GTPC-EP ingress.
37	GTPC-EP ingress receives Delete Bearer response and sends to SGW service POD.
38	SGW service POD processes Delete Bearer Response and forwards to GTPC-EP.
39	GTPC-EP forwards Delete Bearer Response to PGW.

Inter and Intra MME Handover and S1 SGW Relocation with Less Number of Bearer Context Call Flow

This section describes the inter and intra MME handover and S1 SGW relocation with less number of bearer context call flow.

Figure 95: Inter and Intra MME Handover and S1 SGW Relocation with Less Number of Bearer Context Call Flow

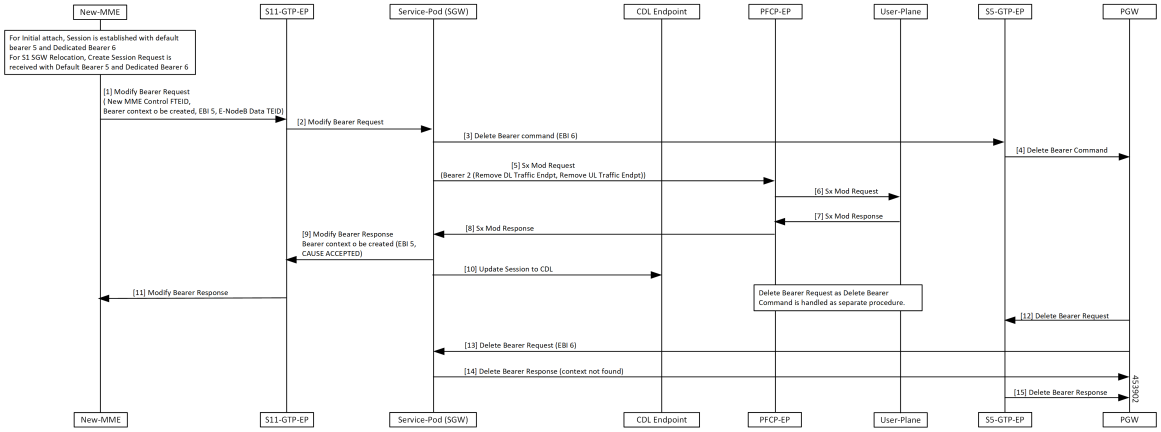


Table 168: Inter and Intra MME Handover and S1 SGW Relocation with Less Number of Bearer Context Call Flow Description

Step	Description
1	Established NEW MME session with the default bearer EBI 5 and dedicated bearer 6. New MME receives Create Session Request for S1 SGW Relocation with Default bearer EBI 5 and dedicated bearer 6. New MME sends Modify Bearer Request to GTPC-EP ingress with the following: • New MME Control TEID • New Bearer Contexts to create • EBI5 • eNodeB Data TEID
2	GTPC-EP ingress forwards Modify Bearer Request to SGW service POD.
3	SGW service POD sends Delete Bearer Command with EBI 6 to GTPC-EP.
4	GTPC-EP forwards Delete Bearer Command to PGW.
5	SGW service POD sends Sx Mod Req to PFCP-EP with Remove DL Traffic Endpoint and Remove UL Traffic Endpoint for Bearer 2.
6	PFCP-EP forwards Sx Mod Req to UPF.
7	UPF sends Sx Mod Response to PFCP-EP.
8	PFCP-EP forwards Sx Mod Response to SGW service POD.

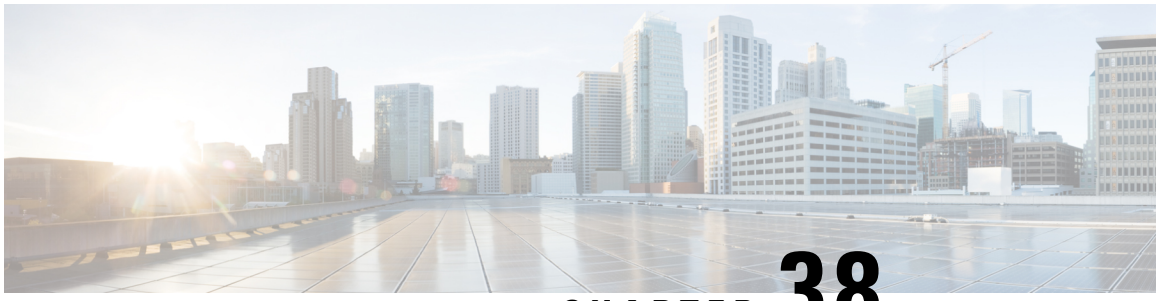
Step	Description
9	SGW service POD sends Modify Bearer Response to GTPC-EP ingress with the following: • Bearer Contexts EBI 5 to modify with cause as *Accepted*
10	Updated session to CDL.
11	GTPC-EP ingress sends Modify Bearer Response to New MME.
12	PGW sends Delete Bearer Request to GTPC-EP.
13	SGW service POD receives Delete Bearer Request with EBI6 from PGW as Delete Bearer Command handled as separate procedure.
14	SGW service POD responds with Delete Bearer Response with cause as *Context Not Found* to GTPC-EP.
15	GTPC-EP forwards Delete Bearer Response to PGW.

Note

- Sx Modify Request message along with Remove DL traffic Endpoint and Remove UL traffic Endpoint is sent as don't confirm message in Legacy CUPS. Sx Modify for MBReq message follows Sx Modify Request and sent to UPF.
- UPF receives the following messages in cnSGW-C.
  - Single Sx Modify Request message for MB Request
  - Remove DL traffic Endpoint
  - Remove UL traffic Endpoint

SGW Relocation OAM Support

This section describes operations, administration, and maintenance information for this feature.



CHAPTER 38

Sx Load/Overload Control Handling

Feature Summary and Revision History

Summary Data

Table 169: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration required to enable
Related Documentation	Not Applicable

Revision History

Table 170: Revision History

Revision Details	Release
First introduced.	2021.01.0

Feature Description

This feature supports enabling Sx load and overload for user-plane. UP selection takes place when the user-plane reports LCI (Load control information) and OCI (Overload Control Information).

Load control enables the user-plane function to send its load information to the control plane function. This load information is to balance the PFCP session load across the user-plane functions according to their effective loads.

Overload controls the information for throttling of new session requests towards specific user-plane.

How it Works

This section describes how this feature works.

Node Feature Support

As per 3GPP standard:

- CP informs load and overload feature to the user-plane.
- User-plane decides to send load or overload information towards the CP peer or not.

Configure load and overload feature at CP as a part of PFCP Sxa endpoint node feature. This configuration in turn communicates to UP during Sx Association Response message or Sx Association Update Request message when change in configuration occurs.

The CP Function Feature IE indicates the supported CP function features. This IE contains features which have (system-wide) UP function behavior impact.

Note If CP does not support load or overload feature through CLI then it ignores the user-plane reported load or overload information for the UP selection process.

UP Selection

UP selection occurs as per LCI value only whereas throttling occurs as per OCI value only (Specified in 3GPP standards).

Per Peer Level LCI and OCI display:

```
show peers | tab | exclude rest
                                                                    POD
ENDPOINT  LOCAL ADDRESS  PEER ADDRESS  DIRECTION  INSTANCE  TYPE  CONNECTED TIME  RPC
ADDITIONAL DETAILS
------------------------------------------------------------------------------------------------------------
S5/S8  <nil>:2123  209.165.202.143:2123  Inbound  nodemgr-0  Udp  6 minutes   SGW  Recovery:
 10
SXA  209.165.200.226:8805  209.165.202.143:8805  Inbound  nodemgr-0  Udp  About a minute
SGW-U  Capacity: 65535,
LoadMetric: 20,LoadSeqNo: 1,OverloadMetric: 0,OverloadSeqNo: 0,Priority: 10
SXA  209.165.200.226:8805  209.165.202.147:8805  Inbound  nodemgr-0  Udp  2 minutes  SGW-U
```

```
  Capacity: 10,
LoadMetric: 40,LoadSeqNo: 1,OverloadMetric: 100,OverloadSeqNo: 1,Priority: 20
SXA  209.165.200.226:8805  209.165.202.159:8805  Inbound  nodemgr-0  Udp  2 minutes  SGW-U
  Capacity: 10,
LoadMetric: 100,LoadSeqNo: 1,OverloadMetric: 77,OverloadSeqNo: 1,Priority: 1
```

Throttling Support for Sx Establishment

When user-plane is in overload situation, cnSGW-C establishes throttling the Sx Establishment request message toward user-plane. This throttling avoids new calls (Low priority or non-emergency) towards the overloaded user-plane.

Throttling takes place as per the reported OCI values in percentage. Following actions takes place when throttling happens:

- Random drop of percentage in reported Sx Establishment Request messages towards that user-plane.
- Call drop occurs at cnSGW-C with `sx_no_resource_available` disconnect reason.
- Respective statistics get incremented.

Session Termination Trigger From User-Plane in Self-Protection

User-plane triggers the session termination request towards cnSGW-C in pacing manner through Sx Report Request message. User-plane triggers session termination request when it is in self-protection mode and there is no improvement in load. This trigger happens with setting of SPTER (Self Protection Termination Request) bit.

cnSGW-C initiates Sx Termination Request for those PDNs and releases the PDN session with disconnect reason as `userplane_requested_termination`.

Failure-handling Profile Support for Congestion Cause

When the user-pane is in self-protection mode and rejects the new sessions with the cause `PFCP_ENTITY_IN_CONGESTION (74)`, cnSGW-C selects different user-plane as per the failure template profile configuration.

Failure-handling profile is associated with UPF-Group.

Reselection of UPF follows the UPF selection process and considers the retries count to different UPF from profile configuration.

Note Currently, only `PFCP_ENTITY_IN_CONGESTION(74)` is supported as cause code for retry and reselection of user-plane as part of this feature.

Configuring the Sx Load/Overload Feature

This section describes how to configure Sx Load/Overload.

Use the following commands to configure Sx Load/Overload configuration.

```
config
 instance instance-id instance_id
  endpoint endpoint_name
   interface interface_name
    supported-features [ load-control | overload-control ]
   exit
  exit
```

NOTES:

- **endpoint** *endpoint_name* - Specify the endpoint name.
- **interface** *interface_name* - Specify the interface name.
- **supported-features [load-control | overload-control]** - Enable load/overload control.

Sample Configuration

Following is a sample configuration.

```
configure
 instance instance-id 1
  endpoint pfcp
   interface sxa
    supported-features load-control overload-control
   exit
```

Verifying Sx Load/Overload Configuration

Use the following `show` command to view the Sx load/overload configuration.

```
show running-config instance instance-id 1 endpoint
instance instance-id 1
endpoint pfcp
interface sxa
supported-features load-control overload-control
exit
exit
```

Configuring Failure Handling Profile

This section describes how to configure failure handling profile.

Use the following commands to configure failure handling profile.

```
config
 profile failure-handling failure-handling_profile_name
  interface interface_name
   message message_type
    cause-code cause_code
     action action_type
      max-retry max_retry_count
    exit
   exit
  exit
 profile upf-group upf-group_profile_name
```

```
  failure-profile profile_name
 exit
```

NOTES:

- **profile failure-handling** *failure-handling_profile_name* - Specify the failure-handling profile name.
- **interface** *interface_name* - Specify the interface name.
- **message** *message_type* - Specify the message type.
- **cause-code** *cause_code* - Specify the cause ID (range of 2-255) or range of cause IDs (range of 2-255) separated by either '-' or ',' or both.

  -Or-

  Must be one of the following:

  - no-resource-available
  - no-response-received
  - pfcp-entity-in-congestion
  - reject
  - service-not-supported
  - system-failure

- **action** *action_type* - Specify the action type for the cause. Must be one of the following:
  - retry-terminate
  - terminate
- **max-retry** *max_retry_count* - Specify the maximum retry count for the retry-terminate action. Must be an integer in the range of 0-5. Default value is 1.
- **profile upf-group** *upf-group_profile_name* - Specify the UPF group profile name.
- **failure-profile** *profile_name* - Specify the UPF failure profile name.

Sample Configuration

Following is the sample configuration:

```
profile failure-handling fh1
 interface sxa
  message SessionEstablishmentReq
   cause-code pfcp-entity-in-congestion action terminate
  exit
 exit
exit
profile failure-handling fh2
 interface sxa
  message SessionEstablishmentReq
   cause-code 74 action retry-terminate max-retry 3
  exit
 exit
exit
```

```
profile upf-group g1
 failure-profile fh1
exit
profile upf-group g2
 failure-profile fh2
exit
```

Sx Load/Overload Control OAM Support

This section describes operations, administration, and maintenance information for this feature.

Bulk Statistics

UE Disconnect Statistics

```
sgw_ue_disconnect_stats{app_name="smf",cluster="cn",data_center="cn",instance_id=
"0",reason="sx_no_resource_available",service_name="sgw-service"} 1
```

```
sgw_ue_disconnect_stats{app_name="smf",cluster="cn",data_center="cn",instance_id=
"0",reason="userplane_requested_termination",service_name="sgw-service"} 1
```

PDN Disconnect Statistics

```
sgw_pdn_disconnect_stats{app_name="smf",cluster="cn",data_center="cn",instance_id=
"0",pdn_type="ipv4",rat_type="EUTRAN",reason="sx_no_resource_available",service_name="sgw-service"}
 1
```

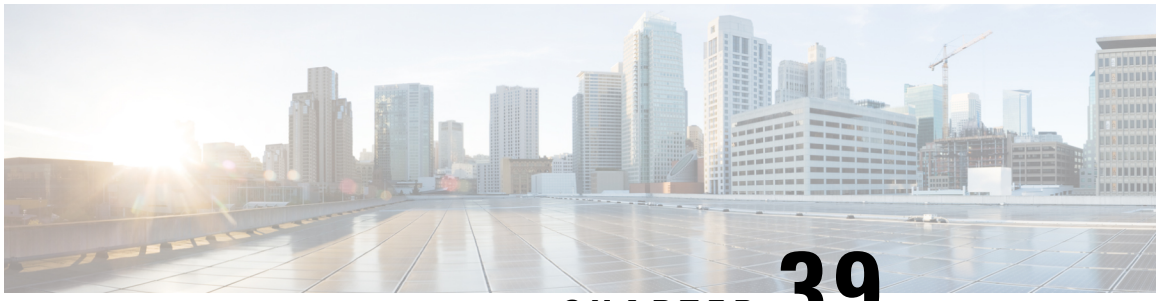
```
sgw_pdn_disconnect_stats{app_name="smf",cluster="cn",data_center="cn",instance_id=
"0",pdn_type="ipv4v6",rat_type="EUTRAN",reason="userplane_requested_termination",service_name="sgw-service"}
 1
```

SGW Service Statistics

```
sgw_service_stats{app_name="smf",cluster="cn",data_center="cn",fail_reason="sx_oci_throttling_reject",
instance_id="0",interface="interface_sgw_ingress",reject_cause="no_resources_available",service_name=
"sgw-service",sgw_procedure_type="initial_attach",status="rejected",sub_fail_reason=""}
 1
```

```
sgw_service_stats{app_name="smf",cluster="cn",data_center="cn",fail_reason="",instance_id="0",
interface="interface_sgw_egress",reject_cause="",service_name="sgwservice",sgw_procedure_type=
"upf_initiated_deletion",status="attempted",sub_fail_reason=""} 1
```

```
sgw_service_stats{fail_reason="sx_cause_fail",interface="interface_sgw_ingress",reject_cause=
"service_denied",sub_fail_reason="pfcp_entity_in_congestion",sgw_procedure_type="initial_attach",
status="rejected"}
```



CHAPTER 39

Update Bearer Request and Response

Feature Summary and Revision History

Summary Data

Table 171: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 172: Revision History

Revision Details	Release
First introduced.	2020.04

Feature Description

In this release, cnSGW-C supports only relay of update bearer request (which can contain TFT change, QCI change or APB – AMBR change) from PGW towards MME. When MME sends response to cnSGW-C, it relays update bearer response towards PGW.

This release doesnt support signaling towards User Plane.

Standards Compliance

The Update Bearer Request and Response Support feature complies with the following standards:

- *3GPP TS 23.401*
- *3GPP TS 23.214*
- *3GPP TS 29.274*
- *3GPP TS 29.244*

How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flow of Update Bearer Request and Response feature.

Figure 96: Bearer Request/Response without UP Signaling Call Flow

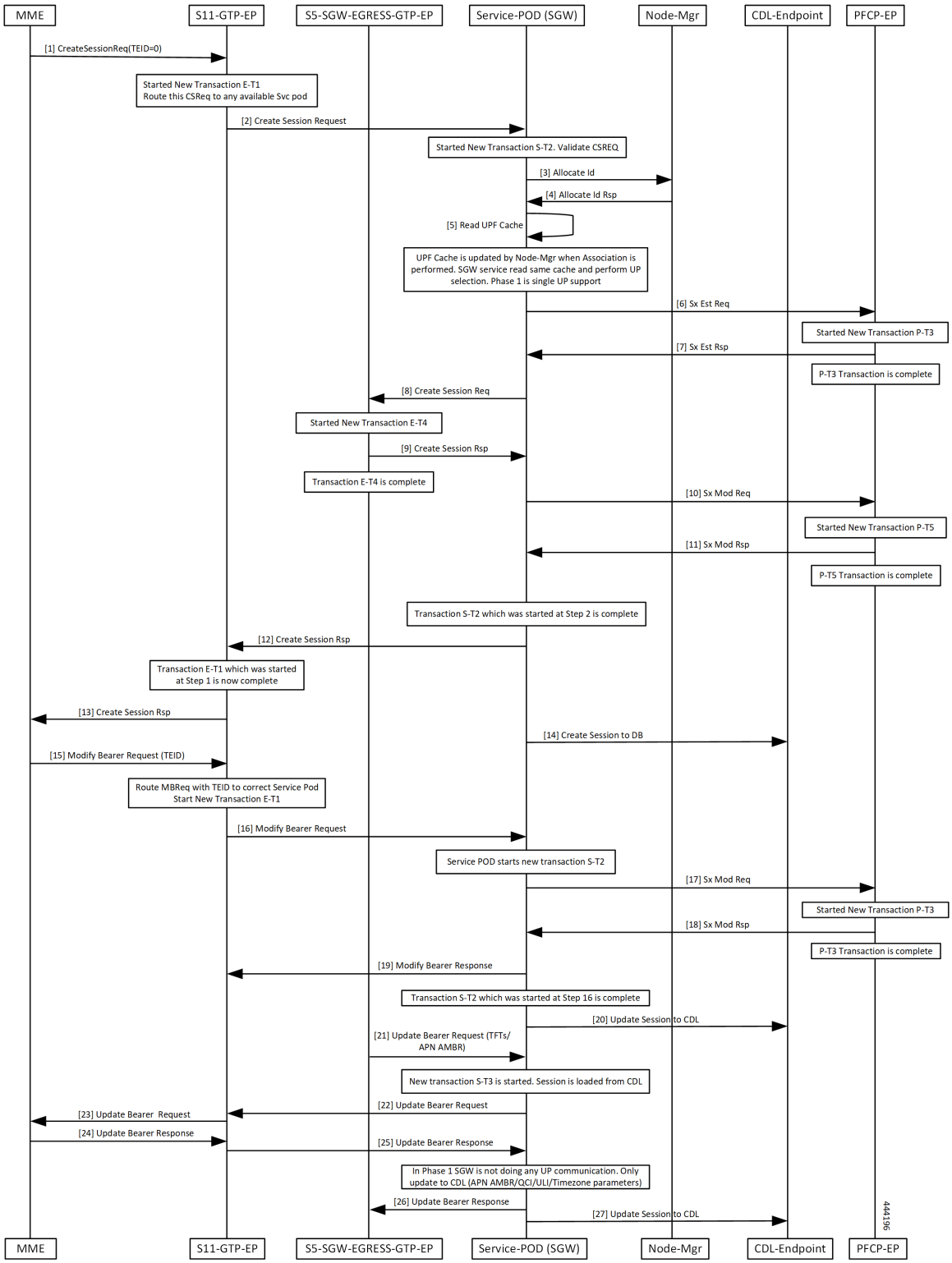
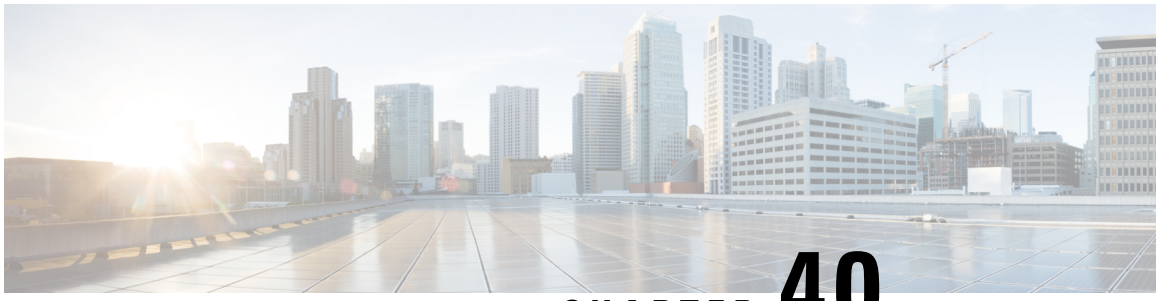


Table 173: Bearer Request/Response without UP Signaling Call Flow Description

Step	Description
1	MME sends Create Session Req to S11-GTP-EP with TEID value as zero.
2	Transaction E-T1 started. S11-GTP-EP sends Create Session Req to SGW-Service POD.
3, 4	Transaction S-T2 started. SGW-Service POD sends Allocate ID to Node-Mgr and receives response from it.
5, 6, 7	SGW-Service POD reads Node-Mgr updated UPF cache and performs UPF selection. SGW-Service POD sends Sx Est Req to PFCP-EP. Transaction P-T3 started. SGW-Service POD receives Sx Est Rsp from PFCP-EP.
8, 9	Transaction P-T3 completed. SGW-Service POD sends Create Session Req to S5-SGW-EGRESS-GTP-EP. Transaction E-T4 started. SGW-Service POD receives Create Session Rsp from S5-SGW-EGRESS-GTP-EP.
10, 11, 12	Transaction E-T4 completed. SGW-Service POD sends Sx Mod Req to PFCP-EP. Transaction P-T5 started. SGW-Service POD receives Sx Mod Rsp from PFCP-EP.
12	Transaction S-T2 ans P-T5 completed. SGW-Service POD sends Create Session Rsp to S11-GTP-EP.
13	Transaction E-T1 completed. S11-GTP-EP sends Create Session Rsp to MME.
14	SGW-Service POD sends Create Session to DB.
15	MME sends Modify Bearer Req with TEID value to S11-GTP-EP.
16	S11-GTP-EP routes MBReq with TEID to the exact SGW-Service POD. S11-GTP-EP sends Modify Bearer Request SGW-Service POD.
17	Transaction S-T2 completed. SGW-Service POD sends Sx Mod Req to PFCP-EP.
18	Transaction P-T3 started. SGW-Service POD receives Sx Mod Rsp from PFCP-EP.

Step	Description
19	Transaction P-T3 completed. SGW-Service POD sends Sx Mod Rsp to S11-GTP-EP.
20	Transaction S-T2 completed. SGW-Service POD sends Update Session to CDL.
21	S5-SGW-EGRESS-GTP-EP sends Update Bearer request with TFTs and APN AMBR to SGW-Service POD.
22, 23	Transaction S-T3 completed. SGW-Service POD sends Update Bearer Request to S11-GTP-EP. S11-GTP-EP forwards Update Bearer Request to MME.
24, 25	MME sends Update Bearer Rsp to S11-GTP-EP. S11-GTP-EP forwards Update Bearer Rsp to SGW-Service POD.
26	SGW-Service POD forwards Update Bearer Rsp to S5-SGW-EGRESS-GTP-EP.
27	SGW-Service POD sends Update Session to CDL.



CHAPTER 40

UPF Selection Support

Feature Summary and Revision History

Summary Data

Table 174: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	UPF Selection using DCNR Support: Disabled – Configuration required to enable UPF Selection using DNN Support: Enabled – Always-on UPF Selection using Location Support: Disabled – Configuration required to enable Combined UPF Selection for cnSGW-C and SMF: Disabled – Configuration required to enable
Related Documentation	Not Applicable

Revision History

Table 175: Revision History

Revision Details	Release
Added support for UPF selection using Location. Added support for Combined UPF selection for cnSGW-C and SMF.	2021.02.0
First introduced.	2021.01.0

Feature Description

This feature describes the following UPF selection methods.

- DNN and DCNR
- Location support
- cnSGW-C and SMF to select same UPF instance

UPF Selection using DNN and DCNR Support

Feature Description

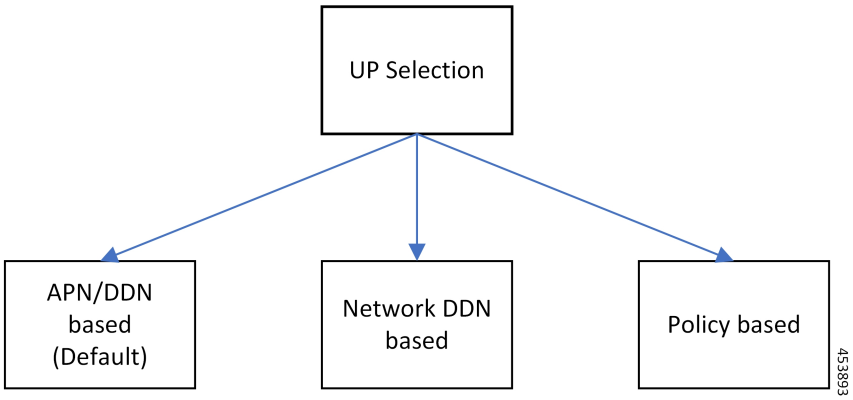
The following are the three UPF selection methods:

- DNN or APN based
- Network based
- Policy based

Note DNN is enabled when UPF selection policy isn't associated.

How it Works

This section describes how the feature works.



UPF Selection Methods

DNN or APN Based

- Create Session request message has APN information. This APN gets configured as part of DNN-list in the Network element profile for each user-plane.
- The PDN establishment considers these user-planes.
- UPF selection uses Capacity and Priority if many user-planes are available.

Network Based

- UPF selection considers DNN which got configured as part of the APN or DNN profile.
- This DNN is local SGW network specific DNN name.
- The same network DNN or APN name gets configured as part of DNN-list in the network element profile for each user-plane.
- Instead of using APN that comes in CSReq, local DNN is used for the UPF selection based on the DNN list.

  For example, in case of roaming scenario where APN is not known, this configuration helps in UPF selection.
- PDN establishment considers these user-planes.
- UPF selection uses Capacity and Priority if many user-planes are available.

UPF Selection Policy Based

- UPF selection profile configuration with parameters determines UPF for each precedence. The supported max number of precedencies are four.
- Each precedence parameter is a *Logical AND* condition. If DNN and DCNR are configured as precedence 1, then it searches for the DNN supported user-plane and enables DCNR based support. If this search criteria fails, it moves to the next (mostly 2) precedence and tries to evaluate that condition.
- UPF selection policy is associated with a DNN profile.

- UPF group provides characteristics to the network element profile which belongs to the same UPF group profile.
- UPF selection uses Capacity and Priority if many user-planes available.

Note

- cnSGW-C rejects the call with Create Session Response specifying cause as NO_RESOURCE_AVAILABLE when no UPF matches the precedence criteria.

Configuring UPF Selection Methods

This section describes how to configure the UPF selection methods.

Configuring UPF Group Profile-based UPF Selection

This section describes how to configure UPF group profile-based UPF selection.

Use the following commands to configure the UPF group profile-based UPF selection.

```
config
  profile upf-group upf_group_name
    dcnr [true | false]
    end
```

NOTES:

- **profile upf-group** *upf_group_name*—Specify the UPF group name. Must be a string.
- **dcnr [true | false]**—Specify to enable or disable support for dual connectivity with new radio. Default value is false.

Sample Configuration

Following is a sample configuration.

```
config
profile upf-group G1
 dcnr true
 end
```

Configuring Network-based UPF Selection

Use the following commands to configure the network-based UPF selection

```
config
   profile network-element upfupf_name
      node-id  node_id_value

 ipv6_address
 port_number

      upf-group-profile upf_group_profile_name
      dnn-list dnn_list
      priority priority_value
```

```
capacity capacity_value
end
```

NOTES:

- **network-element upf** *upf_name*—Specify the UPF profile name.
- **node-id** *node_id_value*—Specify the Node ID of the UPF node.
-
-
-
- **upf-group-profile** *upf_group_profile_name*—Specify the UPF group profile name.
- **dnn-list** *dnn_list*—Specify the DNN list supported by the UPF node.
- **priority** *priority_value*—Specify the static priority relative to other UPFs. This value is used for load balancing and must be an integer in the range of 0–65535. The default value is 1.
- **capacity** *capacity_value*—Specify the capacity relative to other UPFs. This value is used for load balancing and must be an integer in the range of 0–65535. The default value is 10.

Sample Configuration

The following is a sample configuration.

```
config
profile network-element upf UP1
 node-id      upf1@sgw.com
 upf-group-profile G1
 dnn-list [dnn1 dnn2]
 priority 20
 capacity 65535
 end
```

Configuring Policy based UPF Selection

This section describes how to configure Policy based UPF selection.

Use the following commands to configure the Policy based UPF Selection.

```
config
 policy upf-selection upf_selection_policyname
   precedence precedence_value location
   exit
   precedence precedence_value dnn
   exit
 exit
```

NOTES:

- **upf-selection** *upf_selection_policyname* - Specify the UPF selection policy name.
- **precedence** *precedence_value* - Specify the precedence for entry. Must be an integer in the range of 1-4.

Sample Configuration

Following is a sample configuration.

```
config
policy upf-selection upf_pol1
  precedence 1
    [ location ]
  exit
  precedence 2
    [ dnn ]
  exit
exit
```

Troubleshooting Information

This section describes the troubleshooting information that enables you to view the UPF selection using DNN and DCNR configuration issues.

Configuration Errors

```
show config-error | tab
ERROR COMPONENT   ERROR DESCRIPTION
-------------------------------------------------------------------------------------------------------
SGWProfile        Subscriber policy name : sub_policy in profile sgw1 is not configured
SubscriberPolicy  Operator policy : op_policy1 under subscriber policy sub_policy2 is not
configured
OperatorPolicy    Dnn policy name : dnn_policy1 in operator policy op_policy2 is not
configured
DnnPolicy        Dnn profile name : dnn_profile1 in dnn policy dnn_policy2 is not configured
DnnProfile        UPF selection policy name : upf_sel_policy1 in dnn profile dnn_profile2
is not configured
```

UPF Selection using Location Support

Feature Description

This feature supports Location-based UPF selection in Create Session Request message. It performs this selection as per the received TAI or ECGI or both TAI and ECGI values together.

Configuring the UPF Selection Feature

This section describes how to configure the UPF selection using location.

Configuring ECGI for EPS

This section describes how to configure ECGI for EPS.

New configuration and profile **ecgi-group** added to configure the list of individual ECGI values or the range of ECGI.

You can configure both ECGI list and ECGI range. ECGI range configuration is optional.

Use the following commands to configure the ECGI Configuration for EPS.

```
config
  profile ecgi-group ecgi_group_name
    mcc mcc_value
```

```
    mnc mnc_value
       ecgi list ecgi_list_name
       ecgi range start start_value end end_value
exit
```

NOTES:

- **ecgi-group** *ecgi_group_name* - Specify the ECGI group name.
- **mcc** *mcc_value* - Specify the MCC value. Must be a three digit number. For example, 123
- **mnc** *mnc_value* - Specify the MNC value. Must be a two or three digit number. For example, 23 or 456
- **ecgi list** *ecgi_list* - Specify the list of ECGI values - 7 digit hex string Eutra Cell ID. For example, A12345f. Must be a string.
- **ecgi range start** *start_value* **end** *end_value* - Specify the ECGI range start and end values. Must be a string.

Note

- You can configure multiple ECGI range values.
- You can configure multiple [PLMN and ECGI values] under **ecgi-group** configuration.
- You can configure maximum of 16 PLMNs under **ecgi-group** configuration.
- You can configure maximum of 64 ECGI values in the ECGI list under a PLMN.
- Maximum defined number of ECGI ranges under a PLMN is 64.

Sample Configuration

Following is the sample configuration.

```
config
profile ecgi-group e1 mcc 123 mnc 45
ecgi list [ 1234567 abcdef0 ]
ecgi range start 1111111 end fffffff
exit
```

Verifying ECGI for EPS Configuration

This section describes how to verify the ECGI Configuration for EPS.

Use the following `show` command to view the ECGI configuration for EPS.

```
show running-config profile ecgi-group
profile ecgi-group e1
mcc 123 mnc 45
ecgi list [ 1234567 abcdef0 ]
ecgi range start 1111111 end fffffff
exit
exit
exit
```

Configuring TAI-Group

This section describes how to configure TAI-Group.

You can enhance the following TAI-Group configuration to support multiple TAI-Group configurations with different names.

Use the following commands to configure the TAI-Group.

```
config
  profile tai-group tai_group_name
    mcc mcc_value
    mnc mcc_value
      tac list tac_list
      tac range start start_value end end_value
  exit
```

NOTES:

- **tai-group** *tai_group_name* - Specify the TAI group name.
- **mcc** *mcc_value* - Specify the MCC value. Must be a three digit number. For example, 123
- **mnc** *mnc_value* - Specify the MNC value. Must be a two or three digit number. For example, 23 or 456
- **tac list** *tac_list* - Specify the list of TAC values - [0-9a-fA-F]{4}|[0-9a-fA-F]{6} - 4 digit or 6 digit hex string - Example A123, 1a2B3F. Must be a string.
- **tac range start** *start_value* **end** *end_value* - Specify the TAC range start and end values. Must be a string.

Note

- You can configure maximum of 16 PLMNs under a TAI-Group.
- You can configure maximum of 64 TAC values in a TAC list under a PLMN.
- Maximum defined number of TAC ranges under a PLMN is 64.

Sample Configuration

Following is the sample configuration.

```
config
profile tai-group TAI-GRP1
  mcc 123 mnc 234
    tac list [ 1a25 A123 ]
    tac range start B234 end b999
    exit
    tac range start C213 end c999
    exit
  exit
  mcc 231 mnc 45
    tac list [ 2a2B B123 ]
    tac range start d111 end d999
    exit
  exit
exit
```

Configuring Location-area-group

This section describes how to configure Location-area-group.

You can add new configuration and profile location-area-group. Configuration of **ecgi-group** and **tai-group** are optional.

Use the following commands to configure the Location-area-group.

```
config
  profile location-area-group location_area_group_name
     tai-group tai_group_name
     ecgi-group ecgi_group_name
  exit
```

NOTES:

- **location-area-group** *location_area_group_name* - Specify the location area group name.
- **tai-group** *tai_group_name* - Specify the TAI group name.
- **ecgi-group** *ecgi_group_name* - Specify the ECGI group name.

Sample Configuration

Following is the sample configuration.

```
config
profile location-area-group LOC_AREA_GRP_1
  tai-group TAI-AUTO-GRP1
  ecgi-group ECGI-AUTO-GRP1
exit
profile location-area-group LOC_AREA_GRP_2
  tai-group TAI-AUTO-GRP2
exit
```

Configuring UPF Group and UPF Selection Policy Enhancement

This section describes how to configure UPF Group and UPF Selection Policy Enhancement.

You can add new configuration under upf-group-profile to configure location-area-group-list.

Use the following commands to configure the UPF group anf UPF selection policy enhancement.

```
config
  profile upf-group upf_group_name
     location-area-group-list [area_group_list]
  exit

config
  policy upf-selection selection_policy_name
   precedence value  [ selection_parameter_list ]
  exit
```

NOTES:

- **upf-group** *upf_group_name* - Specify the UPF group name.
- **location-area-group-list** *area_group_list* - Specify the list of Location Area Group supported by UPF node.
- **upf-selection** *selection_policy_name* - Specify the UPF selection policy name.

- **precedence** *value* **[** *selection_parameter_list* **]** - Specify the precedence for entry. Must be an integer in the range of 1-4.

Note If pdn-type-subscription and pdn-type-session both are configured, pdn-type-subscription is considered.

Sample Configuration

Following is the sample configuration.

```
config
profile upf-group G1
 location-area-group-list [ LOC_AUTO_GRP_1 ]
exit
profile upf-group G2
 location-area-group-list [ LOC_AUTO_GRP_2 ]
exit
profile upf-group G3
 location-area-group-list [LOC_AUTO_GRP_1 LOC_AUTO_GRP_2 ]
exit
```

```
config
policy upf-selection upf_pol1
  precedence 1
    [ location ]
  exit
  precedence 2
    [ dnn ]
  exit
exit
```

Combined UPF Selection for cnSGW-C and SMF

Feature Description

This feature supports cnSGW-C and SMF to select the same UPF instance when the UPF and SMF are deployed on same cluster and UPF instance is available. If the UPF instance is not available, the UPF selection is based on the existing configurations.

Standards Compliance

The Combined UPF Selection for cnSGW-C and SMF feature complies with the following standards:

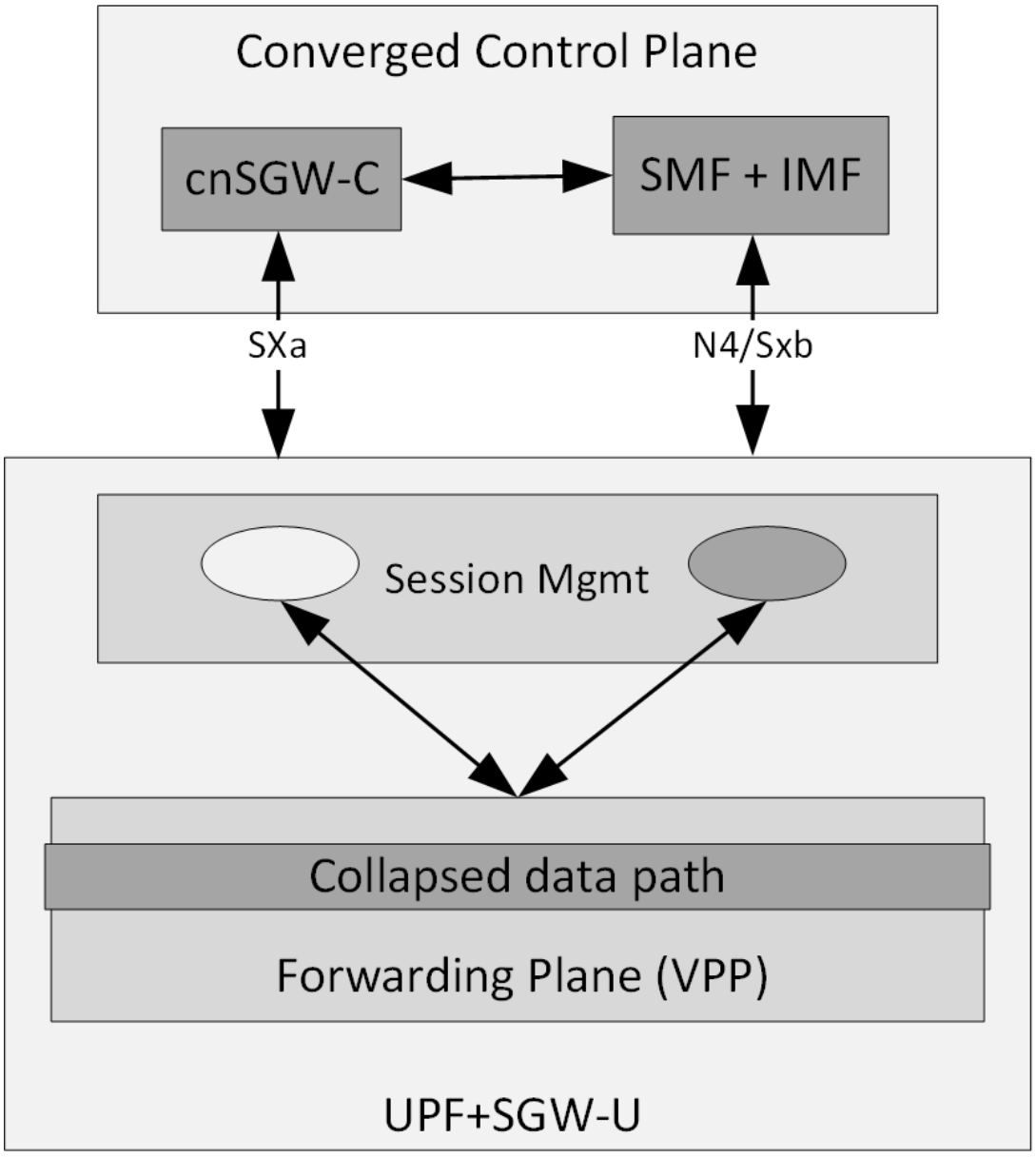
- *3GPP TS 23.401*
- *3GPP TS 23.402*
- *3GPP TS 29.274*
- *3GPP TS 23.214*
- *3GPP TS 29.244*

• *3GPP TS 24.008*

How it Works

This section describes how this feature works.

System Architecture



cnSGW-C and SMF/IWF uses the same UPF instance, so that UPF can use those sessions to the collapsed data path.

Control plane (cnSGW-C and SMF) selects the same User-plane in various scenarios (initial attach, handover, and so on).

Following actions takes place during Initial Attach:

- cnSGW-C passes the SGW-U FQDN information of selected UPF instance to SMF in Initial attach.
- SMF selects the UPF instance as per the received SGW-U FQDN.
- Same UPF FQDN is configured at cnSGW-C and at SMF to create a correlation as part of the network element profile.

Call Flows

This section describes the key call flows of Combined UPF Selection for cnSGW-C and SMF feature.

Initial Attach on 4G for 5G Capable Device Call Flow

This section describes the Initial Attach on 4G for 5G Capable Device call flow.

Figure 97: Initial Attach on 4G for 5G Capable Device Call Flow

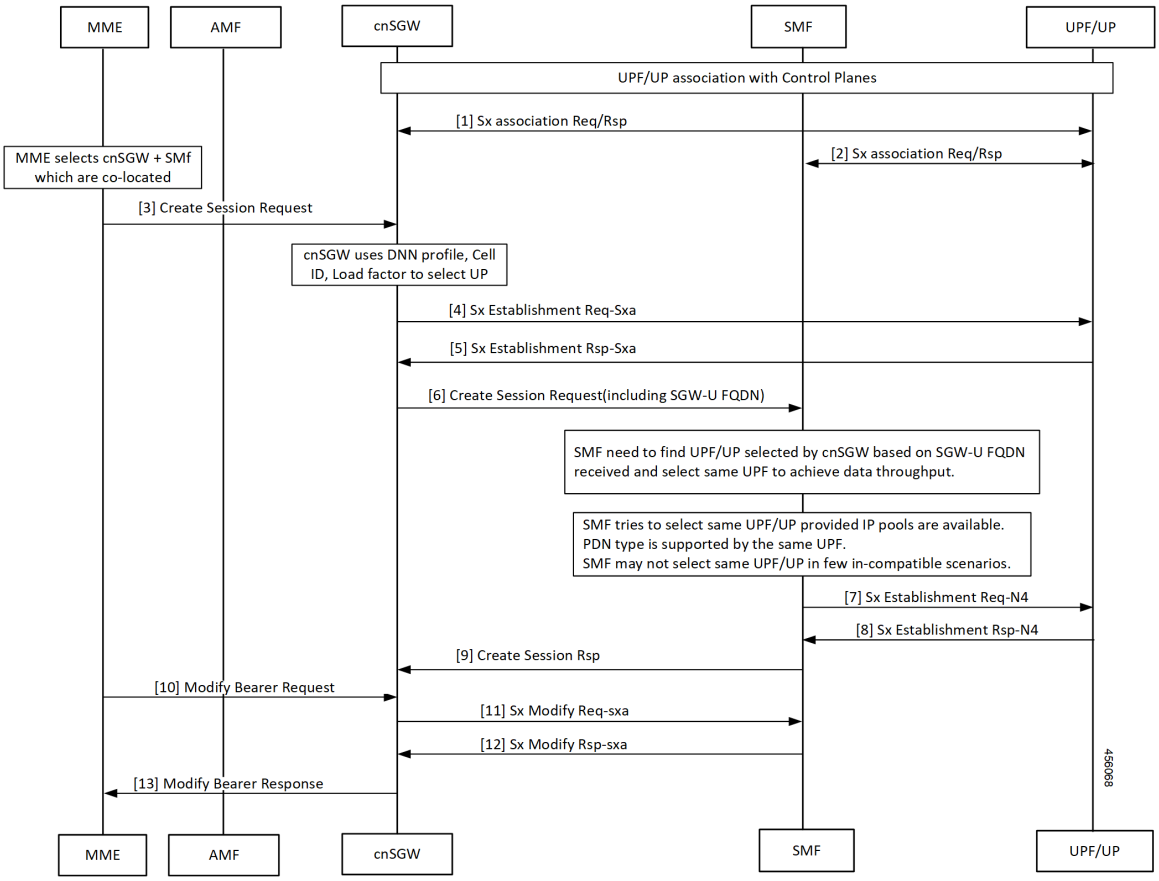


Table 176: Initial Attach on 4G for 5G Capable Device Call Flow Description

Step	Description
1	Established UPF association with control planes. cnSGW-C sends Sx Association Req/Rep to UPF.
2	SMF sends Sx Association Req/Rep to UPF.
3	MME sends Create Session Request to cnSGW-C after selecting co-located cnSGW-C and SMF.
4	cnSGW-C sends Sx Establishment Req (SXA) to UPF after selecting UPF using DNN profile, Cell ID, and local factors.
5	cnSGW-C receives Sx Establishment Res from UPF.
6	cnSGW-C sends Create Session Request to SMF including SGW-U FQDN.
7	SMF must find cnSGW-C selected UPF as per received SGW-U FQDN and select the same UPF to achieve data throughput. SMF tries to select same UPF when IP pools are available. Same UPF supports the PDN type. SMF may not select same UPF in few in-compatible scenarios. SMF send Sx Establishment Req N4 to UPF.
8	SMF receives Sx Establishment Res-N4 from UP.
9	cnSGW-C receives Create Session Response from SMF.
10	MME sends Modify Bearer Request to cnSGW-C.
11	cnSGW-C sends Sx Modify Req (SXA) to SMF.
12	cnSGW-C receives Sx Modify Res (SXA) to SMF.
13	cnSGW-C sends Modify Bearer Response to MME.

UPF Registration with User Plane ID Call Flow

This section describes the UPF Registration with User Plane ID call flow.

Figure 98: UPF Registration with User Plane ID Call Flow

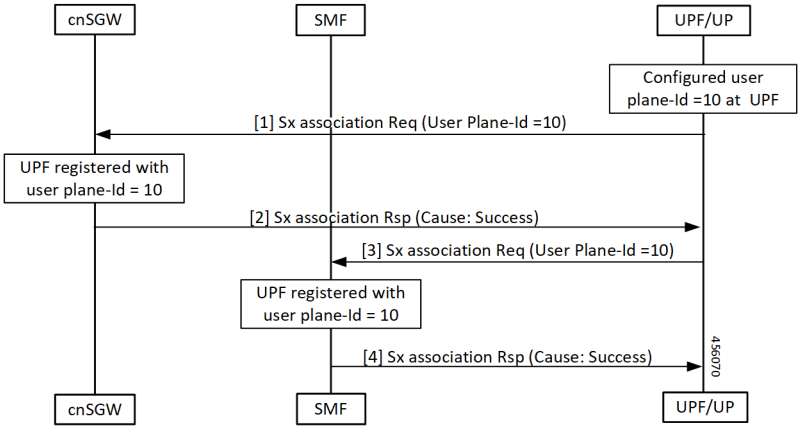


Table 177: UPF Registration with User Plane ID Call Flow Description

Step	Description
1	Configured User-plane ID at UPF cnSGW-C receives Sx association Request from UPF with configured User-plane ID.
2	UPF receives Sx association Response with Cause = SUCCESS from cnSGW-C.
3	SMF receives Sx association Request from UPF with configured User-plane ID.
4	UPF receives Sx association Response with Cause = SUCCESS from SMF.

Inter-SGW Handover on 4G RAT for 5G Capable Devices Call Flow

This section describes the Inter-SGW Handover on 4G RAT for 5G Capable Devices call flow.

Figure 99: Inter-SGW Handover on 4G RAT for 5G Capable Devices Call Flow

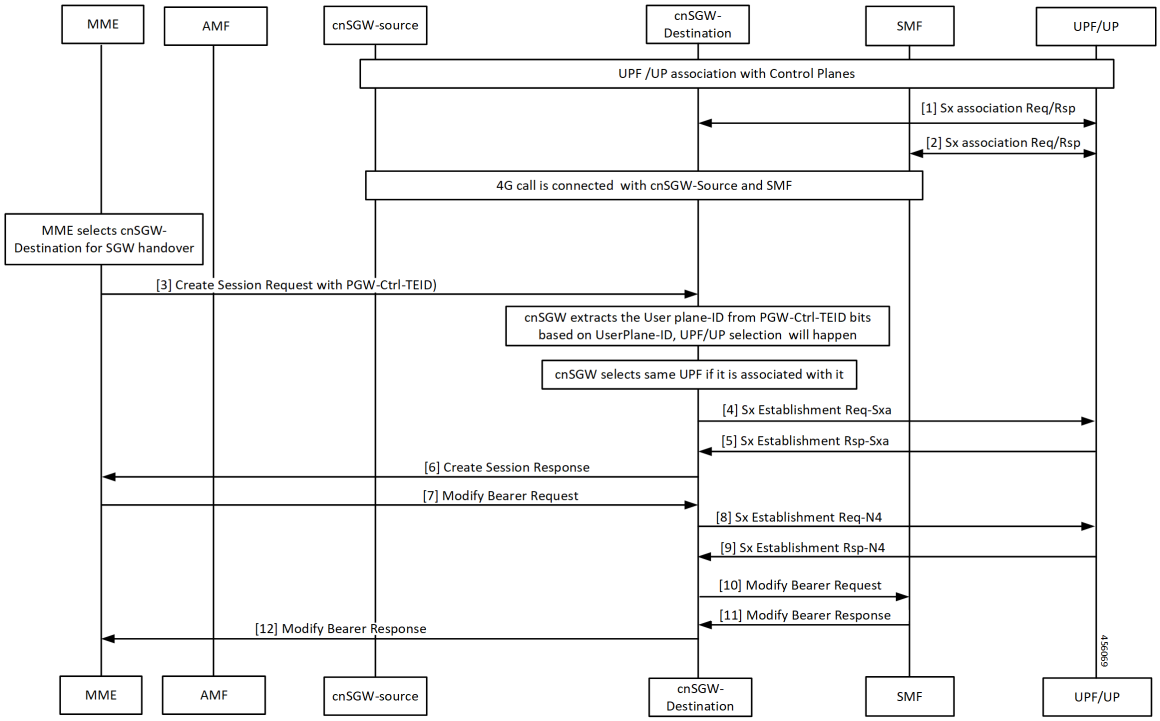


Table 178: Inter-SGW Handover on 4G RAT for 5G Capable Devices Call Flow Description

Step	Description
1	Established UPF association with control planes. UPF sends Sx Association Req/Rep to destination cnSGW-C.
2	UPF sends Sx Association Req/Rep to SMF.
3	4G call connected between cnSGW-C-source and SMF. MME selects cnSGW-C-Destination for the SGW handover. MME sends Create Session Req with PGW-Ctrl-TEID to cnSGW-C-Destination.
4	cnSGW-C extracts same associated UPF ID from PGW-Ctrl-TEID. cnSGW-C-Destination sends Sx Establishment Req (SXA) to UPF.
5	cnSGW-C-Destination receives Sx Establishment Rsp (SXA) from UPF.
6	cnSGW-C-Destination sends Create Session Response to MME.
7	cnSGW-C-Destination receives Modify Bearer Request from MME.
8	cnSGW-C-Destination sends Sx Establishment Req-N4 to UPF.
9	cnSGW-C-Destination receives Sx Establishment Rsp-N4 from UPF.

Step	Description
10	cnSGW-C-Destination sends Modify Bearer Request to SMF.
11	cnSGW-C-Destination receives Modify Bearer Response from SMF.
12	cnSGW-C-Destination forwards Modify Bearer Request to MME.

5G to EPS Handover Using N26 Interface – cnSGW-C and SMF Separate Node Call Flow

This section describes the 5G to EPS Handover Using N26 Interface – cnSGW-C and SMF Separate Node call flow.

Figure 100: 5G to EPS Handover Using N26 Interface – cnSGW-C and SMF Separate Node Call Flow

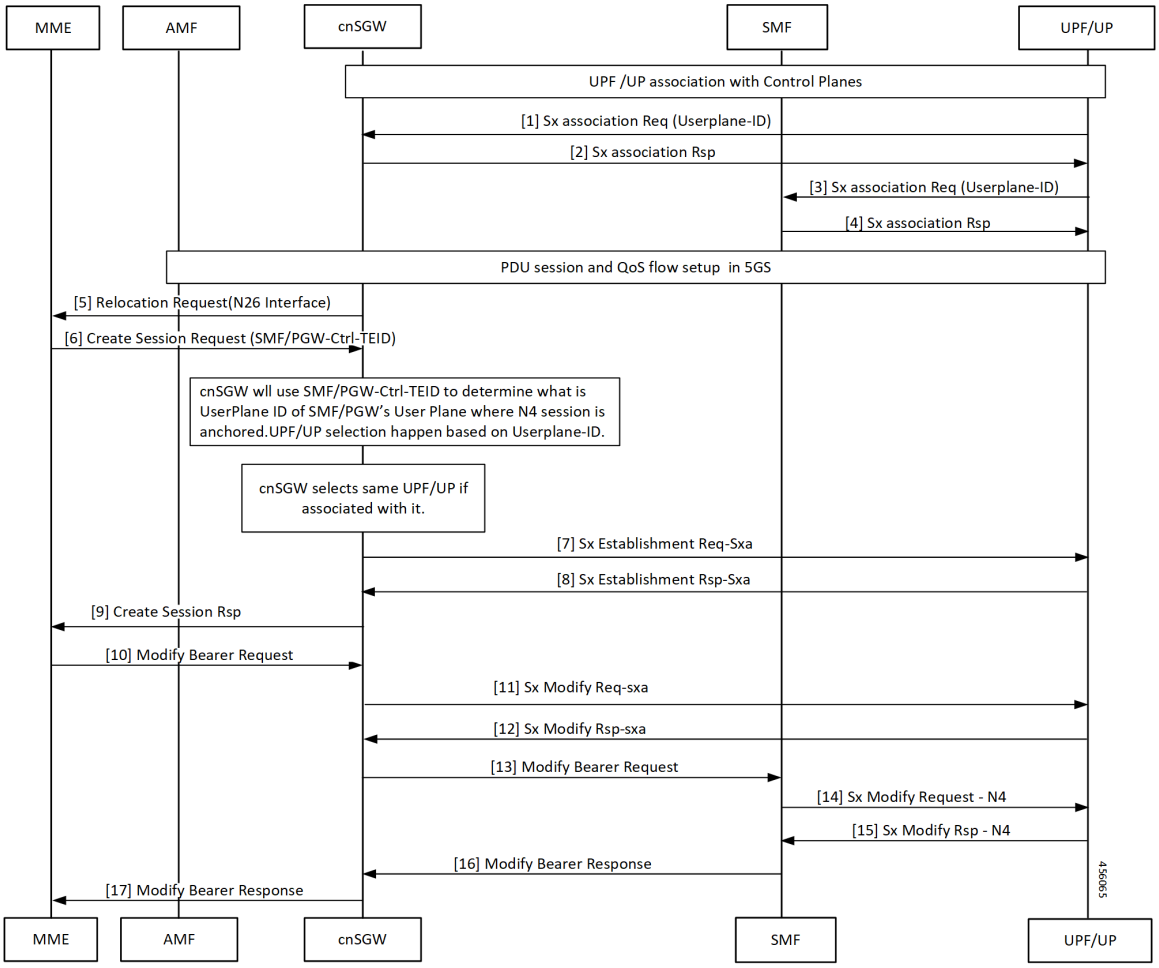


Table 179: 5G to EPS Handover Using N26 Interface – cnSGW-C and SMF Separate Node Call Flow Description

Step	Description
1	cnSGW-C selects associated same UPF. cnSGW-C receives Sx Establishment Request with User-plane ID from UPF/UP.

Step	Description
2	cnSGW-C sends Sx Establishment Response from UPF/UP.
3	UPF/UP sends Sx Association Request with User-plane ID to SMF.
4	SMF sends Sx Association Response to UPF/UP.
5	cnSGW-C sends Relocation Request to MME on interface N26.
6	MME sends Create Session Request to cnSGW-C with SMF and PGW-ctrl-TEID information.
7	cnSGW-C selects associated same UPF. cnSGW-C sends Sx Establishment Req (SXA) to UPF/UP.
8	cnSGW-C receives Sx Establishment Rsp (SXA) from UPF/UP.
9	cnSGW-C sends Create Session response to MME.
10	MME sends Modify Bearer Request to cnSGW-C.
11	cnSGW-C sends Sx Modify Req (SXA) to UPF/UP.
12	cnSGW-C receives Sx Modify Rsp (SXA) from UPF/UP.
13	cnSGW-C sends Modify Bearer Request to SMF.
14	SMF sends Sx Modify Request – N4 to UPF/UP.
15	SMF receives Sx Modify Response from UPF/UP.
16	cnSGW-C receives Modify Bearer Response to SMF.
17	cnSGW-C forwards Modify Bearer Response to MME.

Wi-Fi to LTE Handover Call Flow

This section describes the Wi-Fi to LTE Handover call flow.

Figure 101: Wi-Fi to LTE Handover Call Flow

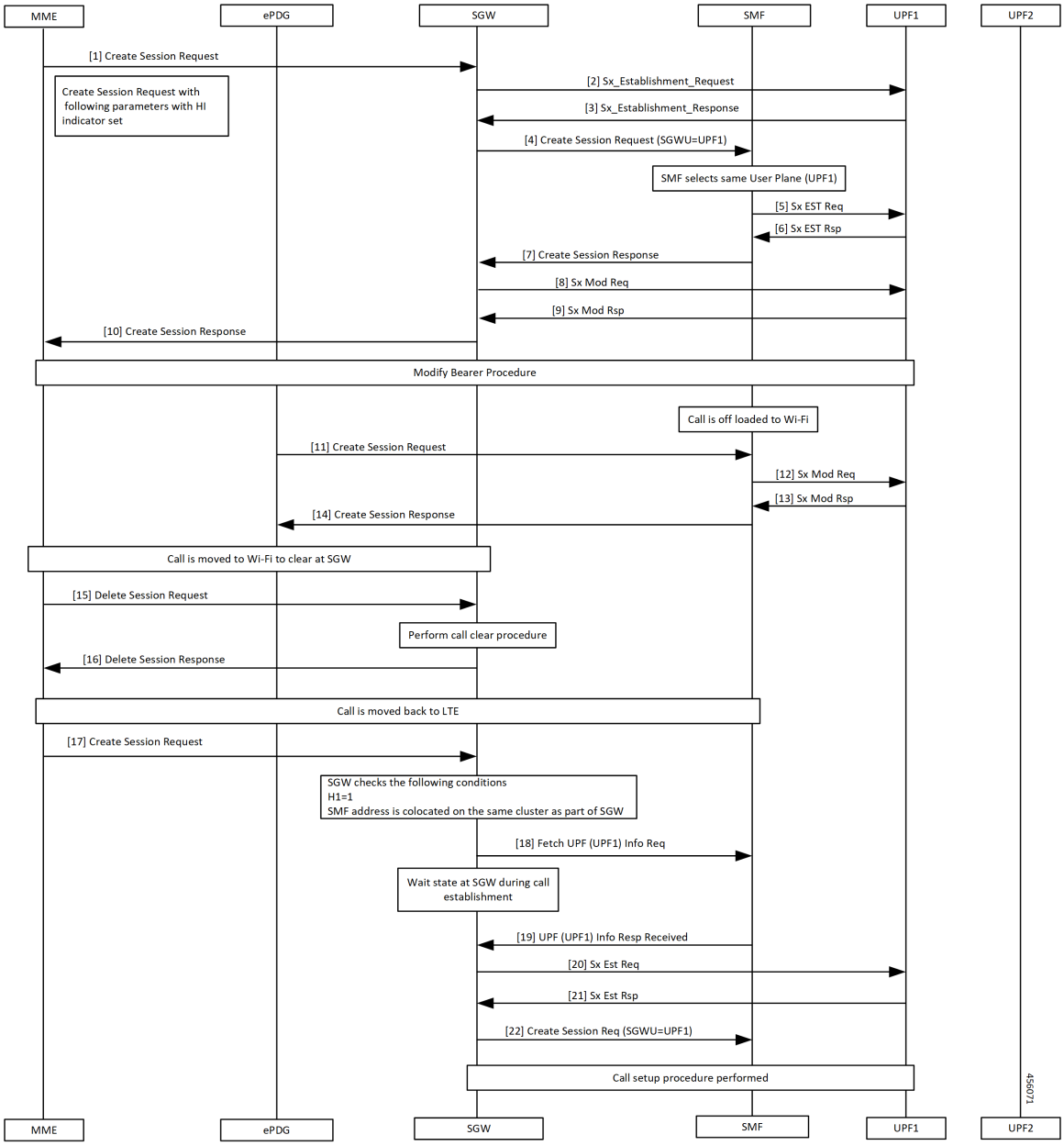


Table 180: Wi-Fi to LTE Handover Call Flow Description

Step	Description
1	MME sends create Session Request to SGW.
2	SGW sends Sx Establishment Request to UPF1.
3	SGW receives Sx Establishment Response from SMF.
4	SGW sends Create Session Request to SMF. SMF selects same UPF.

Step	Description
5	SMF sends Sx Establishment Request to UPF1.
6	SMF receives Sx Establishment Response from UPF1.
7	SMF sends Create Session Response to SGW.
8	SGW sends Sx Mod Request to UPF1.
9, 10	SGW receives Sx Mod Response from UPF1 and forwards to MME.
11	Modify Bearer procedure takes place and off-loaded call to Wi-Fi. ePDG sends Create Session Request to SGW.
12	SMF sends Sx Mod Request to UPF1.
13	SMF receives Sx Mod Response from UPF1.
14	ePDG receives Create Session Response from SGW.
15	Call moved to Wi-Fi to clear at SGW. MME sends Delete Session Request to SGW.
16	MME receives Delete Session Response from SGW after performing call clear procedure.
17	MME sends Create Session Request to SGW.
18	SGW sends fetch UPF (UPF1) info request to SMF after checking SMF as same cluster as cnSGW-C.
19	SGW receives UPF (UPF1) Info Response from SMF.
20	SGW sends Sx Establishment Request to UPF1.
21	SGW receives Sx Establishment Response from UPF1.
22	SGW sends Create Session Request with SGWU=UPF1 to UPF1 and performs call setup procedure.

Configuring the Combined UPF Selection for cnSGW-C and SMF

This section describes how to configure the Combined UPF Selection for cnSGW-C and SMF.

Configuring Converged-Core Profile

This section describes how to configure the Converged-Core Profile.

Use the following commands to configure the profile converged-core with UPF selection enabled.

```
config
  profile converged-core core_name
    max-upf-index value
    no upf-selection disable
  exit
```

Use the following commands to configure the profile converged-core with UPF selection disabled.

```
config
  profile converged-core core_name
    max-upf-index value
    upf-selection disable
  exit
```

NOTES:

- **converged-core** *core_name* - Specify the converged core prolile name.
- **max-upf-index** *value* - Specify the UPF index value. Must be an integer in the range of 1-1023.
- **no upf-selection disable** - Enable colocated UPF selection.
- **upf-selection disable**- Disable colocated UPF slection.

Sample configuration

Following is a sample configuration with UPF selection enabled.

```
config
profile converged-core cc1
max-upf-index 1023
no upf-selection disable
exit
```

Following is a sample configuration with UPF selection disabled.

```
config
profile converged-core cc1
max-upf-index 1023
upf-selection disable
exit
```

Verifying the Profile Converged-core Configuration

This section describes how to verify the Profile Converged-core configuration.

Use the following show command to view the Profile Converged-Core configuration with UPF selection enabled.

```
show running-config profile converged-core cc1
profile converged-core cc1
max-upf-index 1023
no upf-selection disable
exit
```

Use the following show command to view the Profile Converged-Core configuration with UPF selection disabled.

```
show running-config profile converged-core cc1
profile converged-core cc1
max-upf-index 1023
upf-selection disable
exit
```

Configuring Node-ID

This section describes how to configure the Node-ID.

Use the following commands to configure the Node-ID.

```
config
  profile network-element upf upf_name
    node-id node_id_value
  exit
```

NOTES:

- **network-element upf** *upf_name* - Specify the UPF peer network element name.
- **node-id** *node_id_value* - Specify the Node ID of the UPF node. Must be a string

Sample Configuration

Following is a sample configuration.

```
config
profile network-element upf upf1
node-id upf1@cn.com
exit
```

UPF Selection OAM Support

This section describes operations, administration, and maintenance information for this feature.

Bulk Statistics

UE Disconnect Statistics

```
sgw_ue_disconnect_stats{app_name="smf",cluster="cn",data_center="cn",instance_id="0",
reason="userplane_info_not_available",service_name="sgw-service"} 24
```

PDN Disconnect Statistics

```
sgw_pdn_disconnect_stats{app_name="smf",cluster="cn",data_center="cn",instance_id="0",
pdn_type="ipv4",rat_type="EUTRAN",reason="userplane_info_not_available",service_name="sgw-service"}
 8
```

```
sgw_pdn_disconnect_stats{app_name="smf",cluster="cn",data_center="cn",instance_id="0",
pdn_type="ipv4v6",rat_type="EUTRAN",reason="userplane_info_not_available",service_name="sgw-service"}
 15
```

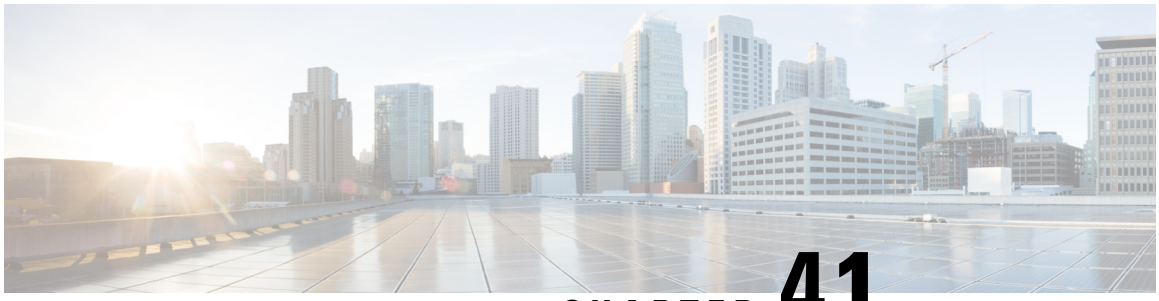
```
sgw_pdn_disconnect_stats{app_name="smf",cluster="cn",data_center="cn",instance_id="0",
pdn_type="ipv6",rat_type="EUTRAN",reason="userplane_info_not_available",service_name="sgw-service"}
 1
```

SGW Service Statistics

```
sgw_service_stats{app_name="smf",cluster="cn",data_center="cn",fail_reason="userplane_selection_fail",
instance_id="0",interface="interface_sgw_ingress",reject_cause="no_resources_available",service_name=
```

```
"sgw-service",sgw_procedure_type="initial_attach",status="failure",sub_fail_reason=""}
 22
```

```
sgw_service_stats{app_name="smf",cluster="cn",data_center="cn",fail_reason="userplane_selection_fail",
instance_id="0",interface="interface_sgw_ingress",reject_cause="no_resources_available",service_name="sgw-service",
sgw_procedure_type="secondary_pdn_creation",status="failure",sub_fail_reason=""}
 2
```



CHAPTER 41

VoLTE Call Prioritization

Feature Summary and Revision History

Summary Data

Table 181: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 182: Revision History

Revision Details	Release
First introduced.	2021.02.0

Feature Description

cnSGW-C provides:

- CLI support to mark QCI as IMS media.
- CLI support to display whether session/bearer is VoLTE or not in `show subscriber` output.
- Counter support to identify number of VoLTE subscribers in the system.
- Sx message priority configuration based on VoLTE marked session.

How it Works

This section describes how this feature works.

- SGW profile represents SGW service.
- SGW profile has associated subscriber policy, which helps to select the Operator Policy.
- Operator Policy has DNN policy associated with it.
- DNN policy has DNN profile associated with it which has the QCI mark for marking VoLTE subscriber for priority.

Based on the QCI marking as IMS, *volteBearer* and *volteSession* flags are set internally when you execute `show subscriber` command.

- *volteBearer* is a bearer level flag. If bearer QCI is present in marked QCI list, *volteBearer* flag is set as true and the bearer is considered as **volteBearer**.
- *volteSession* is a session level flag. This flag is set as **true** if there's a VoLTE bearer present in any PDN of that subscriber.

Feature Configuration

Configuring this feature involves the following steps:

- Configure the call priority. For more information, refer to Configuring the Priority, on page 476.
- Configure the message priority. For more information, refer to Sx Message Priority, on page 479.

Configuring the Priority

This section describes how to configure the priority.

CLI is used to mark the QCI level as VoLTE media under dnn profile. If requested QCI in the call matches with the marked QCI, SGW sets the *volteSession* and *volteBearer* flags. If a subscriber session has **volteSession**, then that subscriber has the highest priority compared to other subscribers.

`profile dnn` *`profile_name`* **`ims mark qci`** *`qci_value`*

NOTES:

- **profile dnn** *profile_name* - DNN profile name.
- **mark** - For marking standard QCI value as IMS media.

- **qci** *qci_value*: Specify the QCI value. The following QoS Class Identifiers are supported:

  Standard: 1-9

Sample Configuration

Following is the sample configuration.

```
profile dnn dnn1 ims mark qci [ 2 3 4 ]
```

Sample Output

This section provides sample output.

```
show full-configuration profile dnn dnn1
profile dnn dnn1
 ims mark qci [ 2 3 4 ]
exit
```

Based on the QCI marking as IMS, *volteSession* and *volteBearer* flags are set internally when you execute `show subscriber` command.

This section provides sample output.

```
show subscriber namespace sgw imsi 121100789012345
subscriber-details
{
  "subResponses": [
    {
      "status": true,
      "genericInfo": {
        "imsi": "imsi-121100789012345",
        "mei": "imei-000349526666660",
        "msisdn": "912010101010101",
        "accessType": "EUTRAN",
        "plmnId": {
          "mcc": "121",
          "mnc": "100"
        },
        "sgwProfileName": "sgw1",
        "volteSession": true
      },
      "s11cInterfaceInfo": {
        "sgwTeid": "[0x11000016] 285212694",
        "sgwIPv4Address": "10.1.5.170",
        "mmeTeid": "[0x4d3] 1235",
        "mmeIPv4Address": "10.1.5.169"
      },
      "pdnInfoList": {
        "totalPdn": 1,
        "pdnInfo": [
          {
            "pdnId": "PDN-1",
            "apn": "starent.com",
            "attachType": "Initial Attach",
            "sgwRelocState": "N/A",
            "operatorPolicyName": "N/A",
            "dnnProfileName": "N/A",
            "defaultEbi": 5,
            "pdnType": "IPv4",
            "allocatedIPv4": "12.0.0.1",
            "apnSelectionMode": "unknown",
            "ambrUplink": "232323 Kbps",
```

```
"ambrDownlink": "232323 Kbps",
"s5cInterfaceInfo": {
  "sgwTeid": "[0x51000016] 1358954518",
  "sgwIPv4Address": "10.1.5.170",
  "pgwTeid": "[0x4d4] 1236",
  "pgwIPv4Address": "10.1.5.171"
},
"sxaInterfaceInfo": {
  "selectedUP": "10.1.5.169",
  "upEpKey": "10.1.5.169:10.1.5.170",
  "cpSeid": "[0x1100001651000016] 1224979194493009942",
  "upSeid": "[0x2712] 10002"
},
"bearerInfoList": {
  "totalBearer": 2,
  "bearerInfo": [
    {
      "bearerId": "Bearer-1",
      "state": "Connected",
      "ebi": 5,
      "qci": 9,
      "arp": 68,
      "isDefaultBearer": true,
      "s1uInterfaceInfo": {
        "sgwTeid": "[0x4d5] 1237",
        "sgwIPv4Address": "1.1.1.83",
        "eNodeBTeid": "[0x4d6] 1238",
        "eNodeBIPv4Address": "10.1.5.169"
      },
      "s5uInterfaceInfo": {
        "sgwTeid": "[0x4d4] 1236",
        "sgwIPv4Address": "192.168.131.1",
        "pgwTeid": "[0x4d5] 1237",
        "pgwIPv4Address": "10.1.5.171"
      },
      "volteBearer": true
    },
    {
      "bearerId": "Bearer-2",
      "state": "Connected",
      "ebi": 6,
      "qci": 5,
      "arp": 68,
      "s1uInterfaceInfo": {
        "sgwTeid": "[0x4d8] 1240",
        "sgwIPv4Address": "1.1.1.83",
        "eNodeBTeid": "[0x4d9] 1241",
        "eNodeBIPv4Address": "10.1.5.169"
      },
      "s5uInterfaceInfo": {
        "sgwTeid": "[0x4d7] 1239",
        "sgwIPv4Address": "192.168.131.1",
        "pgwTeid": "[0x4d7] 1239",
        "pgwIPv4Address": "10.1.5.171"
      },
      "volteBearer": true
    }
  ]
},
"uli": {
  "mcc": "121",
  "mnc": "100",
  "tac": "0x8888"
},
```

```
            "plmnType": "VISITOR"
          }
        ]
      }
    }
  ]
}
```

Sx Message Priority

This section describes the Sx message priority.

Based on the VoLTE flags (volteSession and volteBearer), SGW sets the message priority in Sx request messages (Sx-Est, Sx-Mod, and so on) while processing the received requests/responses (for example, S5-CBReq, S11CBResp, S11-UBRes, S5DBReq, and so on).

Sx Message Priority is set when the session is marked for volteSession (or it has VoLTE QCI).

In Sx Req (Establishment or Modification) Message Header:

```
"HEADERS": {
      "length": 30,
      "msg_type": 52,
      "priority": 2,        <<< VOLTE Session priority value
      "priority_flag": 1,   <<< Priority flag is true i.e 1
      "retransmit": 0,
      "seid": 10002,
      "seid_flag": 1,
      "seq_number": 22,
      "version": 1
    },
```

OAM Support

This section describes operations, administration, and maintenance information for this feature.

Bulk Statistics

sgw_voltesession_counter is added based on the *volteSession* flag. This counter indicates how many VoLTE sessions are present in the system at a particular moment.

If *volteSession* flag is true, counter gets incremented.

If *volteSession* flag isn't present (no VoLTE bearer is present in any PDN), the counter gets decremented.

Counter Name: sgw_voltesession_counter

Description: Current active VoLTE sessions present in the system.

Label:

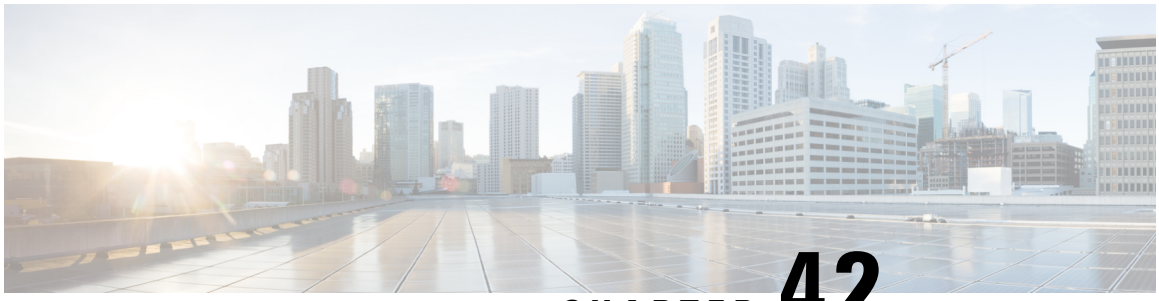
- LABEL_STAT: VolteSession

Sample Counter Output:

You can check the counter from the pod:

```
curl http://209.165.201.20:8080/metrics | grep "volte"
```

```
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0#
HELP sgw_voltesession_counter Current Active Volte Session
# TYPE sgw_voltesession_counter gauge
sgw_voltesession_counter{app_name="smf",cluster="cn",data_center="cn",instance_id="0",
service_name="sgw-service",state="VolteSession"} 1
100  246k    0  246k    0     0  16.0M      0 --:--:-- --:--:-- --:--:-- 17.1M
root@sgw-service-n0-0:/opt/workspace#
```



CHAPTER 42

cnSGW-C Troubleshooting

Description

This chapter provides information on using the command line interface (CLI) commands and logs for troubleshooting any issues that may arise during system operation.

Using CLI Data

This section describes the show and clear commands and the monitor commands that are used for troubleshooting

show subscriber and cdl show Commands

This section describes troubleshooting information.

- To display the SGW subscriber information, use the following commands:

  show subscriber namespace sgw imsi *imsi_value*

  show subscriber nf-service sgw imsi *imsi_value*

  show subscriber count { all }

```
show subscriber namespace sgw imsi 123456789012348
subscriber-details
{
  "subResponses": [
    {
      "status": true,
      "genericInfo": {
        "imsi": "imsi-123456789012348",
        "mei": "imei-123456786666660",
        "msisdn": "msisdn-223310101010101",
        "accessType": "EUTRAN",
        "plmnId": {
          "mcc": "123",
```

```
      "mnc": "456"
    },
    "sgwProfileName": "sgw1",
    "unAuthenticatedImsi": "No"
  },
  "s11cInterfaceInfo": {
    "sgwTeid": "[0x12000147] 301990215",
    "sgwIPv4Address": "209.165.201.19",
    "mmeTeid": "[0x62b5] 25269",
    "mmeIPv4Address": "209.165.201.20"
  },
  "pdnInfoList": {
    "totalPdn": 1,
    "pdnInfo": [
      {
        "pdnId": "PDN-1",
        "apn": "intershat",
        "attachType": "Initial Attach",
        "sgwRelocState": "N/A",
        "operatorPolicyName": "N/A",
        "dnnProfileName": "N/A",
        "defaultEbi": 5,
        "pdnType": "IPv4",
        "allocatedIPv4": "209.165.201.26",
        "apnSelectionMode": "Subscribed",
        "ambrUplink": "10 Kbps",
        "ambrDownlink": "20 Kbps",
        "s5cInterfaceInfo": {
          "sgwTeid": "[0x52000147] 1375732039",
          "sgwIPv4Address": "209.165.201.19",
          "pgwTeid": "[0x339a] 13210",
          "pgwIPv4Address": "209.165.201.18"
        },
        "sxaInterfaceInfo": {
          "selectedUP": "209.165.201.20",
          "upEpKey": "209.165.201.20:209.165.201.19",
          "cpSeid": "[0x1200014752000147] 1297038098512740679",
          "upSeid": "[0x2712] 10002"
        },
        "bearerInfoList": {
          "totalBearer": 1,
          "bearerInfo": [
            {
              "bearerId": "Bearer-1",
              "state": "Connected",
              "ebi": 5,
              "isDefaultBearer": true,
              "qosInfo": {
                "qci": 6,
                "arp": 113
              },
              "s1uInterfaceInfo": {
                "sgwTeid": "[0x62b7] 25271",
                "sgwIPv4Address": "209.165.200.226",
                "eNodeBTeid": "[0x62b8] 25272",
                "eNodeBIPv4Address": "209.165.201.20"
              },
              "s5uInterfaceInfo": {
                "sgwTeid": "[0x62b6] 25270",
                "sgwIPv4Address": "209.165.201.1",
                "pgwTeid": "[0x339b] 13211",
                "pgwIPv4Address": "209.165.201.18"
              },
              "chargingId": 303174163
```

```
                }
              ]
            },
            "uli": {
              "mcc": "123",
              "mnc": "456",
              "tac": "0x92a",
              "eci": "0x12d687"
            },
            "uetimeZone": {
              "timeZone": "+0:15",
              "dayLightSavingTime": "+1 hour"
            },
            "plmnType": "VISITOR"

          }
        ]
      }
    }
  ]
}
```

```
show subscriber count all
subscriber-details
{
   "sessionCount": 50
}
```

- To display the session summary information, use the following command:

  cdl show sessions summary

```
cdl show sessions summary
message params: {session-summary cli session {0 100 0 [] 0 0}}
session {
    primary-key imsi-146062234105885
    unique-key [ 16777218 ]
    map-id 1
    instance-id 1
    version 1
    create-time 2020-04-27 16:18:24.225646626 +0000 UTC
    last-updated-time 2020-04-27 16:18:24.87241245 +0000 UTC
    purge-on-eval false
    next-eval-time 2020-05-04 16:18:24 +0000 UTC
    data-size 406
}
```

- To clear subscriber information, use the following commands:

  clear subscriber all

  clear subscriber nf-service sgw all

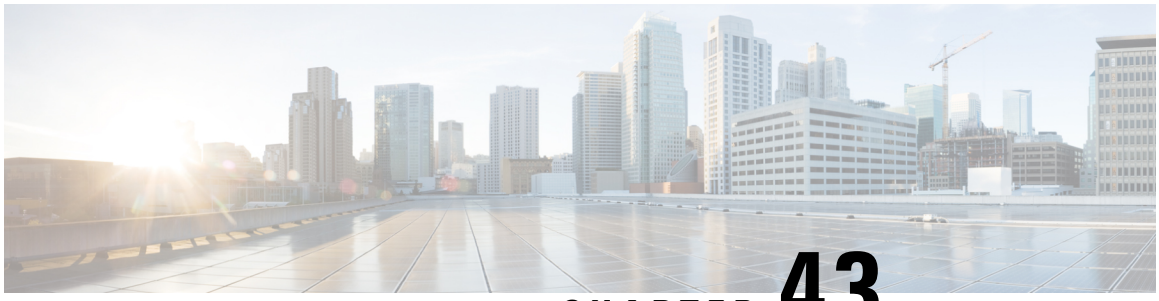
```
clear subscriber all
result
ClearSubscriber Request submitted
```

```
clear subscriber nf-service sgw all
result
ClearSubscriber Request submitted
```

Logs

The system logging feature provides a common way to log the log messages across applications. Each log consists of the following components:

- Timestamp—Shows the date and time of the log creation.
- Log message—Shows the message of a specific log.
- Log level—Shows the level of importance of log message.
- Log tag—Shows the details of module name, component name, and interface name. A log tag is pre-created and passes during logging.



CHAPTER 43

Sample cnSGW-C Configuration

Sample Configuration

The following is a sample configuration.

```
show running-config
profile compliance comp1
 service nsmf-pdusession
  version uri v1
  version full 1.0.0
  version spec 15.4.0
 exit
 service namf-comm
  version uri v1
  version full 1.0.0
  version spec 15.4.0
 exit
 service n1
  version uri v1
  version full 1.0.0
  version spec 15.4.0
 exit
 service n2
  version uri v1
  version full 1.0.0
  version spec 15.4.0
 exit
 service nudm-sdm
  version uri v1
  version full 1.0.0
  version spec 15.4.0
 exit
 service nudm-uecm
  version uri v1
  version full 1.0.0
  version spec 15.4.0
 exit
 service nnrf-disc
  version uri v1
  version full 1.0.0
  version spec 15.4.0
 exit
 service nnrf-nfm
  version uri v1
```

```
  version full 1.0.0
  version spec 15.4.0
 exit
 service npcf-smpolicycontrol
  version uri v1
  version full 1.0.0
  version spec 15.4.0
 exit
 service nchf-convergedcharging
  version uri v1
  version full 1.0.0
  version spec 15.3.0
 exit
exit
profile network-element amf amf1
 nf-client-profile        AP1
 failure-handling-profile FH3
 query-params [ dnn ]
exit
profile network-element udm udm1
 nf-client-profile        UP1
 failure-handling-profile FH4
 query-params [ dnn ]
exit
profile network-element pcf pcf1
 nf-client-profile        PP1
 failure-handling-profile FH1
 query-params [ dnn ]
 rulebase-prefix          cbn#
 predefined-rule-prefix   crn#
exit
profile network-element chf chf1
 nf-client-profile         CP1
 failure-handling-profile  FH2
 query-params [ dnn ]
 nf-client-profile-offline CP2
exit
profile network-element chf chgser1
exit
profile network-element upf upf1
 node-id      upf1@sgw.com
 n4-peer-address ipv4 209.165.200.234
 n4-peer-port 8805
 dnn-list     [ cisco.com intershat starent.com ]
 capacity     65535
 priority     65535
exit
profile upf-group group1
 failure-profile FH1
exit
profile icmpv6 icmpprf1
 options virtual-mac b6:6d:57:45:45:45
exit
profile charging chgprf1
 method [ offline ]
exit
profile charging-characteristics 1
 charging-profile chgprf1
exit
profile failure-handling FH1
 interface pfcp
  message N4SessionEstablishmentReq
   cause-code pfcp-entity-in-congestion action retry-terminate max-retry 2
   cause-code system-failure action terminate
```

```
    cause-code service-not-supported action terminate
    cause-code no-resource-available action retry-terminate max-retry 3
    cause-code no-response-received action retry-terminate max-retry 1
    cause-code reject action terminate
   exit
   message N4SessionModificationReq
    cause-code mandatory-ie-incorrect action terminate
    cause-code session-ctx-not-found action terminate
    cause-code reject action terminate
   exit
  exit
 exit
exit
profile failure-handling gtp1
 interface gtpc message S5S8CreateBearerReq
  cause-code temp-fail
   action retry timeout 1000 max-retry 2
  exit
 exit
 interface gtpc message S5S8UpdateBearerReq
  cause-code temp-fail
   action retry timeout 1000 max-retry 2
  exit
 exit
 interface gtpc message S5S8DeleteBearerReq
  cause-code temp-fail
   action retry timeout 1000 max-retry 2
  exit
 exit
exit
profile access access1
 n26 idft enable timeout 15
 n2 idft enable timeout 15
 gtpc gtpc-failure-profile gtp1
exit
profile dnn default-profile
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 charging-profile chgprf1
 virtual-mac      b6:6d:47:47:47:47
 ssc-mode 2 allowed [ 3 ]
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 upf apn starent.com
exit
profile dnn intershat
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 charging-profile chgprf1
 virtual-mac      b6:6d:47:47:47:47
 ssc-mode 2 allowed [ 3 ]
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 upf apn intershat
 dcnr             true
exit
profile dnn intershat1
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 charging-profile chgprf1
 virtual-mac      b6:6d:47:47:47:48
```

```
 pcscf-profile    PCSCF_Prof_2
 ssc-mode 1
 session type IPV4
exit
profile dnn intershat2
 network-element-profiles chf chf
 network-element-profiles amf amf
 network-element-profiles pcf pcf
 network-element-profiles udm udm
 charging-profile chgprf1
 virtual-mac      b6:6d:47:47:47:49
 ssc-mode 2 allowed [ 3 ]
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 upf apn intershat2
exit
profile dnn starent.com
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 charging-profile chgprf1
 virtual-mac      b6:6d:47:47:47:47
 ssc-mode 2 allowed [ 3 ]
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 upf apn starent.com
exit
profile qos abc
 ambr ul "250 Kbps"
 ambr dl "500 Kbps"
 qi5      7
 arp priority-level 14
 arp preempt-cap NOT_PREEMPT
 arp preempt-vuln PREEMPTABLE
 priority 120
 max data-burst 2000
exit
profile nf-client nf-type udm
 udm-profile UP1
  locality LOC1
   priority 30
   service name type nudm-sdm
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     version
      uri-version v2
      exit
     exit
     endpoint-name EP1
      primary ip-address ipv4 209.165.201.21
      primary ip-address port 8001
     exit
    exit
   exit
   service name type nudm-uecm
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      primary ip-address ipv4 209.165.201.21
      primary ip-address port 8001
     exit
    exit
   exit
```

```
   service name type nudm-ee
    endpoint-profile EP1
     capacity       30
     api-uri-prefix PREFIX
     api-root       ROOT
     uri-scheme     http
     endpoint-name EP1
      priority 56
      primary ip-address ipv4 209.165.201.21
      primary ip-address port 8001
     exit
    exit
   exit
  exit
 exit
exit
profile nf-client nf-type pcf
 pcf-profile PP1
  locality LOC1
   priority 30
   service name type npcf-am-policy-control
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      priority 56
      primary ip-address ipv4 209.165.201.21
      primary ip-address port 8003
     exit
    exit
   exit
   service name type npcf-smpolicycontrol
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      priority 56
      primary ip-address ipv4 209.165.201.21
      primary ip-address port 8003
     exit
    exit
   exit
  exit
 exit
exit
profile nf-client nf-type amf
 amf-profile AP1
  locality LOC1
   priority 30
   service name type namf-comm
    endpoint-profile EP2
     capacity   30
     uri-scheme http
     endpoint-name EP1
      priority 56
      primary ip-address ipv4 209.165.201.21
      primary ip-address port 8002
     exit
    exit
   exit
  exit
 exit
exit
profile nf-client nf-type chf
```

```
 chf-profile CP1
  locality LOC1
   priority 30
   service name type nchf-convergedcharging
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     version
      uri-version v2
      exit
     exit
     endpoint-name EP1
      priority 56
      primary ip-address ipv4 209.165.201.21
      primary ip-address port 8004
     exit
    exit
   exit
  exit
 exit
 chf-profile CP2
  locality LOC1
   priority 31
   service name type nchf-convergedcharging
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     version
      uri-version v2
      exit
     exit
     endpoint-name EP1
      priority 56
      primary ip-address ipv4 209.165.201.21
      primary ip-address port 9040
     exit
    exit
   exit
  exit
 exit
exit
profile nf-pair nf-type UDM
 nrf-discovery-group udmdiscovery
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
exit
profile nf-pair nf-type AMF
 nrf-discovery-group udmdiscovery
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
exit
profile nf-pair nf-type PCF
 nrf-discovery-group udmdiscovery
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
exit
profile nf-pair nf-type UPF
 nrf-discovery-group udmdiscovery
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
```

```
exit
profile nf-pair nf-type CHF
 nrf-discovery-group udmdiscovery
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
exit
profile nf-client-failure nf-type udm
 profile failure-handling FH4
  service name type nudm-sdm
   message type UdmSdmGetUESMSubscriptionData
    status-code httpv2 403
     retry  3
     action retry-and-ignore
    exit
    status-code httpv2 404
     action continue
    exit
    status-code httpv2 413
     retry  3
     action retry-and-continue
    exit
    status-code httpv2 501,504
     retry  3
     action retry-and-terminate
    exit
    status-code httpv2 503
     action terminate
    exit
   exit
   message type UdmSdmSubscribeToNotification
    status-code httpv2 403
     retry  3
     action retry-and-ignore
    exit
    status-code httpv2 404
     action continue
    exit
    status-code httpv2 413
     retry  3
     action retry-and-continue
    exit
    status-code httpv2 501,504
     retry  3
     action retry-and-terminate
    exit
    status-code httpv2 503
     action terminate
    exit
   exit
  exit
  service name type nudm-uecm
   message type UdmUecmRegisterSMF
    status-code httpv2 403
     retry  3
     action retry-and-ignore
    exit
    status-code httpv2 404
     action continue
    exit
    status-code httpv2 413
     retry  3
     action retry-and-continue
    exit
```

```
    status-code httpv2 501,504
     retry  3
     action retry-and-terminate
    exit
    status-code httpv2 503
     action terminate
    exit
   exit
  exit
 exit
exit
profile nf-client-failure nf-type pcf
 profile failure-handling FH1
  service name type npcf-smpolicycontrol
   message type PcfSmpolicycontrolCreate
    status-code httpv2 0,403
     action retry-and-ignore
    exit
    status-code httpv2 400
     action continue
    exit
    status-code httpv2 404
     action terminate
    exit
    status-code httpv2 500
     retry  2
     action retry-and-ignore
    exit
    status-code httpv2 503
     retry  2
     action retry-and-continue
    exit
   exit
   message type PcfSmpolicycontrolUpdate
    status-code httpv2 0,403
     action retry-and-ignore
    exit
    status-code httpv2 400
     action continue
    exit
    status-code httpv2 404
     action terminate
    exit
    status-code httpv2 500
     retry  2
     action retry-and-ignore
    exit
    status-code httpv2 503
     retry  2
     action retry-and-continue
    exit
   exit
   message type PcfSmpolicycontrolDelete
    status-code httpv2 0,403
     action retry-and-ignore
    exit
    status-code httpv2 400
     action continue
    exit
    status-code httpv2 404
     action terminate
    exit
    status-code httpv2 500
     retry  2
```

```
     action retry-and-ignore
    exit
    status-code httpv2 503
     retry  2
     action retry-and-continue
    exit
   exit
  exit
 exit
exit
profile nf-client-failure nf-type chf
 profile failure-handling FH2
  service name type nchf-convergedcharging
   message type ChfConvergedchargingCreate
    status-code httpv2 0,500,504
     action continue
    exit
    status-code httpv2 400,404
     retry  3
     action retry-and-terminate
    exit
    status-code httpv2 403
     retry  3
     action retry-and-ignore
    exit
    status-code httpv2 503
     action terminate
    exit
   exit
   message type ChfConvergedchargingUpdate
    status-code httpv2 0,500,504
     action continue
    exit
    status-code httpv2 400,404
     retry  3
     action retry-and-terminate
    exit
    status-code httpv2 403
     retry  3
     action retry-and-ignore
    exit
    status-code httpv2 503
     action terminate
    exit
   exit
   message type ChfConvergedchargingDelete
    status-code httpv2 0,500,504
     action continue
    exit
    status-code httpv2 400,404
     retry  3
     action retry-and-terminate
    exit
    status-code httpv2 403
     retry  3
     action retry-and-ignore
    exit
    status-code httpv2 503
     action terminate
    exit
   exit
  exit
 exit
exit
```

```
profile smf smf1
 locality      LOC1
 allowed-nssai [ slice1 ]
 plmn-id mcc 123
 plmn-id mnc 456
 service name nsmf-pdu
  type               pdu-session
  schema             http
  service-id         1
  version            1.Rn.0.0
  http-endpoint base-url http://smf-service
  icmpv6-profile     icmpprf1
  compliance-profile comp1
  access-profile     access1
  subscriber-policy  polSub
 exit
exit
profile sgw sgw1
 sgw-charging-threshold thre1
 sgw-charging-profile   ch1
 locality               LOC2
 fqdn                   cisco.com.apn.epc.mnc456.mcc123
 charging-mode          gtpp
exit
profile sgw-charging-threshold thre1
 cc profile value 1
  volume total 100000
  buckets  1
  duration 60
 exit
 cc profile value 2
  volume uplink 100000
  volume downlink 100000
  buckets  1
  duration 120
 exit
exit
profile sgw-charging-profile ch1
 gtpp-triggers volume-limit enable
 gtpp-triggers time-limit enable
 gtpp-profile pf1
exit
profile gtpp-profile pf1 gtpp
 local-storage
  file
   rotation
    volume        5
    cdr-count     1000
    time-interval 60
   exit
   name
    prefix               NYPCF508
    format               .%Y-%m-%d%H-%M-%S.%4Q
    max-file-seq-num     4
    start-file-seq-num   1
    recover-file-seq-num false
   exit
   purge-processed-files purge-interval 10
   format custom5
  exit
  push
   encrypted-url
"$8$6vhjkoHt8RL2noFs/ON6ZJavTDzwGS2KUn/YqlBzgkezFmx5SzvnARYzAdVacCSyCirYOvcC\nTFnHpBNim3QY3Q=="
```

```
  exit
 exit
 dictionary custom24
exit
policy subscriber polSub
 precedence 1
  sst              02
  sdt              Abf123
  serving-plmn mcc 123
  serving-plmn mnc 456
  supi-start-range 100000000000001
  supi-stop-range  999999999999999
  gpsi-start-range 1000000000
  gpsi-stop-range  9999999999
  operator-policy  opPol1
 exit
 precedence 511
  operator-policy defOprPol1
 exit
exit
policy operator defOprPol1
 policy dnn         defPolDnn
 policy network-capability nc1
exit
policy operator opPol1
 policy dnn         polDnn
 policy network-capability nc1
exit
policy dnn defPolDnn
 profile default-profile
 dnn dnn2 profile profile2
 dnn intershat profile intershat
 dnn intershat1 profile intershat1
 dnn starent.com profile starent.com
exit
policy dnn polDnn
 profile default-profile
 dnn dnn2 profile profile2
 dnn intershat profile intershat
 dnn intershat1 profile intershat1
 dnn intershat2 profile intershat2
 dnn starent.com profile starent.com
exit
policy network-capability nc1
 nw-support-local-address-tft true
exit
nssai name slice1
 sst 2
 sdt Abf123
 dnn [ dnn1 intershat intershat1 intershat2 ]
exit
ipam
 instance 1
  source local
  address-pool poolv4
   vrf-name ISP
   tags
    dnn starent.com
   exit
   ipv4
    split-size
     per-cache 1024
     per-dp    256
    exit
```

```
  address-range 209.165.202.129 209.165.200.253
 exit
exit
address-pool poolv4DNN2
 vrf-name ISP
 tags
  dnn intershat1
 exit
 ipv4
  split-size
   per-cache 1024
   per-dp    256
  exit
  address-range 209.165.200.241 209.165.200.244
 exit
exit
address-pool poolv4DNN3
 vrf-name ISP
 static
 tags
  dnn intershat2
 exit
 ipv4
  split-size
   per-cache 512
   per-dp    512
  exit
  address-range 209.165.200.247 209.165.200.248
 exit
 ipv6
  prefix-ranges
   split-size
    per-cache 8192
    per-dp    8192
   exit
   prefix-range 2002:db0:: length 48
  exit
 exit
exit
address-pool poolv4vDNN
 vrf-name ISP
 tags
  dnn intershat1
 exit
 ipv4
  split-size
   per-cache 1024
   per-dp    256
  exit
  address-range 209.165.200.245 209.165.200.244
 exit
exit
address-pool poolv6
 vrf-name ISP
 tags
  dnn intershat
 exit
 ipv6
  prefix-ranges
   split-size
    per-cache 8192
    per-dp    1024
   exit
   prefix-range 2001:db0:: length 48
```

```
    exit
   exit
  exit
  address-pool poolv6DNN2
   vrf-name ISP
   tags
    dnn intershat1
   exit
   ipv6
    prefix-ranges
     split-size
      per-cache 8192
      per-dp    1024
     exit
     prefix-range 2001:ef0:: length 48
    exit
   exit
  exit
  address-pool poolv6vDNN
   vrf-name ISP
   tags
    dnn intershat1
   exit
   ipv6
    prefix-ranges
     split-size
      per-cache 8192
      per-dp    1024
     exit
     prefix-range 2001:ab0:: length 48
    exit
   exit
  exit
 exit
exit
cdl system-id          1
cdl enable-geo-replication true
cdl deployment-model   small
cdl zookeeper replica 1
cdl remote-site 2
 db-endpoint host 209.165.202.157
 db-endpoint port 8882
 kafka-server 209.165.202.157 10001
 exit
exit
cdl datastore session
 geo-remote-site [ 2 ]
 slice-names     [ cnSGW1 cnSGW2 ]
 endpoint replica 1
 endpoint external-ip 209.165.202.156
 endpoint external-port 8882
 index map    1
 index write-factor 1
 slot replica 1
 slot map     1
 slot write-factor 1
 features instance-aware-notification enable true
 features instance-aware-notification system-id 1
  slice-names [ cnSGW1 ]
 exit
 features instance-aware-notification system-id 2
  slice-names [ cnSGW2 ]
 exit
exit
```

```
cdl kafka replica 1
cdl kafka external-ip 209.165.202.156 10001
exit
etcd replicas 1
instance instance-id 1
 endpoint li
  replicas 1
  vip-ip 209.165.200.237
 exit
 endpoint nodemgr
  replicas 1
  nodes    1
 exit
 endpoint gtp
  replicas 1
  interface s5
   vip-ip 209.165.201.11
  exit
  interface s5e
   vip-ip 209.165.201.21
  exit
  interface s11
   vip-ip 209.165.200.237
  exit
 exit
 endpoint pfcp
  replicas 1
  interface sxa
   heartbeat
    interval 0
   exit
  exit
  interface n4
   heartbeat
    interval               0
    retransmission-timeout 3
    max-retransmissions    5
   exit
  exit
 exit
 endpoint radius-dns
  replicas 1
  vip-ip 209.165.201.21
 exit
 endpoint service
  replicas 1
 exit
 endpoint protocol
  replicas     1
  internal-vip 209.165.201.11
  vip-ip 209.165.201.21
  interface sxa
   vip-ip 209.165.201.21
  exit
  interface n4
   vip-ip 209.165.201.11
  exit
 exit
 endpoint gtpprime
  replicas 2
  nodes    1
 exit
 endpoint sgw-service
  replicas 1
```

```
 exit
 endpoint geo
  replicas 1
  nodes    2
  interface geo-internal
   vip-ip 209.165.200.233 vip-port 7001
  exit
  interface geo-external
   vip-ip 209.165.200.234 vip-port 7002
  exit
 exit
 endpoint sbi
  replicas 1
  vip-ip 209.165.201.21
 exit
 endpoint bgpspeaker
  replicas 1
  nodes    2
 exit
exit
instance instance-id 2
 endpoint li
  replicas 1
  vip-ip 209.165.200.238
 exit
 endpoint nodemgr
  replicas 1
  nodes    1
 exit
 endpoint gtp
  replicas 1
  interface s5
   vip-ip 209.165.201.12
  exit
  interface s5e
   vip-ip 209.165.201.141
  exit
  interface s11
   vip-ip 209.165.200.238
  exit
 exit
 endpoint pfcp
  replicas 1
  interface sxa
   heartbeat
    interval 0
   exit
  exit
  interface n4
   heartbeat
    interval               0
    retransmission-timeout 3
    max-retransmissions    5
   exit
  exit
 exit
 endpoint radius-dns
  replicas 1
  vip-ip 209.165.201.141
 exit
 endpoint service
  replicas 1
 exit
 endpoint protocol
```

```
  replicas     1
  internal-vip 209.165.201.11
  vip-ip 209.165.201.141
  interface sxa
   vip-ip 209.165.201.141
  exit
  interface n4
   vip-ip 209.165.201.12
  exit
 exit
 endpoint gtpprime
  replicas 2
  nodes    1
 exit
 endpoint sgw-service
  replicas 1
 exit
 endpoint geo
  replicas 1
  nodes    2
  interface geo-internal
   vip-ip 209.165.200.235 vip-port 7001
  exit
  interface geo-external
   vip-ip 209.165.200.236 vip-port 7002
  exit
 exit
 endpoint sbi
  replicas 1
  vip-ip 209.165.201.141
 exit
 endpoint bgpspeaker
  replicas 1
  nodes    2
 exit
exit
logging level application debug
logging level transaction debug
logging level tracing debug
logging name gtpp-ep0.application.config level application debug
logging name gtpp-ep0.application.gen level application trace
logging name gtpp-ep1.application.config level application debug
logging name gtpp-ep1.application.gen level application trace
logging name infra.cdr.core level application debug
logging name infra.cdr_sftp.core level application debug
logging name infra.config.core level application trace
logging name infra.config.core level transaction trace
logging name infra.config.core level tracing off
logging name infra.message_log.core level transaction trace
router bgp 65061
 bfd interval 250000 min_rx 250000 multiplier 3
 interface v4001
  neighbor 209.165.202.131 remote-as 65060 fail-over bfd
 exit
 policy-name allow-all ip-prefix 209.165.201.30/0 mask-range 0..32
exit
deployment
 app-name     smf
 cluster-name Local
 dc-name      DC
 model        small
exit
k8 label protocol-layer key disktype value ssd
exit
```

```
geomonitor podmonitor pods bgpspeaker-pod
 retryCount            1
 retryInterval         200
 retryFailOverInterval 200
 failedReplicaPercent  40
exit
geomonitor podmonitor pods gtpp-ep
 retryCount            1
 retryInterval         200
 retryFailOverInterval 200
 failedReplicaPercent  40
exit
geomonitor podmonitor pods li-ep
 retryCount            1
 retryInterval         200
 retryFailOverInterval 200
 failedReplicaPercent  40
exit
geomonitor podmonitor pods sgw-service
 retryCount            1
 retryInterval         200
 retryFailOverInterval 200
 failedReplicaPercent  40
exit
instances instance 1
 system-id  DCNAME001
 cluster-id CLUSTER0001
 slice-name cnSGW1
exit
instances instance 2
 system-id  DCNAME002
 cluster-id CLUSTER0002
 slice-name cnSGW2
exit
local-instance instance 1
system mode running
helm default-repository cn
helm repository cn
 access-token
sgw-deployer.gen:AKCp8ihVrCfvm9puwTSt8oKGK6HxP1Fn8sLY5fzqWyR3NhrBmjjJrUHaxfZD3ziQpiLkAy1Q3
 url
https://engci-maven-master.cisco.com/artifactory/smi-fuse-internal-snapshot/mobile-cnat-cn/cn-products/rel-2021.02/
exit
k8s name           cn
k8s namespace      cn
k8s nf-name        smf
k8s registry       dockerhub.cisco.com/smi-fuse-docker-internal
k8s single-node    true
k8s use-volume-claims true
k8s image-pull-secrets regcred
k8s ingress-host-name 209.165.200.235.nip.io
aaa authentication users user admin
 uid        117
 gid        117
 password   $1$g8J36yTY$1g/tM5a9pdsGMnKcspnxD.
 ssh_keydir /tmp/admin/.ssh
 homedir    /tmp/admin
exit
aaa ios level 0
 prompt "\h> "
exit
aaa ios level 15
 prompt "\h# "
exit
```

```
aaa ios privilege exec
 level 0
  command action
  exit
  command autowizard
  exit
  command enable
  exit
  command exit
  exit
  command help
  exit
  command startup
  exit
 exit
 level 15
  command configure
  exit
 exit
exit
nacm write-default deny
nacm groups group LI
 user-name [ liadmin ]
exit
nacm groups group LI2
 user-name [ liadmin2 ]
exit
nacm groups group LI3
 user-name [ liadmin3 ]
exit
nacm groups group admin
 user-name [ admin ]
exit
nacm rule-list admin
 group [ admin ]
 rule li-deny-tap
  module-name       lawful-intercept
  path              /lawful-intercept
  access-operations *
  action            deny
 exit
 rule li-deny-clear
  module-name       tailf-mobile-smf
  path              /clear/lawful-intercept
  access-operations *
  action            deny
 exit
 rule any-access
  action permit
 exit
exit
nacm rule-list confd-api-manager
 group [ confd-api-manager ]
 rule any-access
  action permit
 exit
exit
nacm rule-list ops-center-security
 group [ * ]
 rule change-self-password
  module-name       ops-center-security
  path              /smiuser/change-self-password
  access-operations exec
  action            permit
```

```
 exit
 rule smiuser
  module-name       ops-center-security
  path              /smiuser
  access-operations exec
  action            deny
 exit
exit
nacm rule-list lawful-intercept
 group [ LI LI2 LI3 ]
 rule li-accept-tap
  module-name       lawful-intercept
  path              /lawful-intercept
  access-operations *
  action            permit
 exit
 rule li-accept-clear
  module-name       tailf-mobile-smf
  path              /clear/lawful-intercept
  access-operations *
  action            permit
 exit
exit
nacm rule-list any-group
 group [ * ]
 rule li-deny-tap
  module-name       lawful-intercept
  path              /lawful-intercept
  access-operations *
  action            deny
 exit
 rule li-deny-clear
  module-name       tailf-mobile-smf
  path              /clear/lawful-intercept
  access-operations *
  action            deny
 exit
exit
```