

Overview

The Evolved Packet Core (EPC) network is evolving and moving toward Control User Plane Separation (CUPS) based architecture where User Plane and Control Plane are separate nodes for P-GW, S-GW, and TDF products. The User Plane and Control Plane combined together provide functionality of a node for other elements in the EPC network. However, keeping it separate has numerous advantages from the network point of view – support different scaling for Control Plane and User Plane, support more capacity on per session level in User Plane, and so on.

This chapter highlights high-level details, call flows, and configurations related to Control Plane implementation for P-GW, S-GW, and SAEGW products.

- Product Description, on page 1
- Supported Features and Functionality, on page 2
- How It Works, on page 20

Product Description

The existing non-CUPS SAEGW service is reused to provide Control Plane functionality for Sxa, Sxb, and Sxab (combined Sxa and Sxb) interfaces. The differences are:

1. The respective EGTPC services of P-GW and S-GW are not associated with GTP-U service.
2. Sx service, which is the interface toward the User Plane, is associated with the SAEGW service.
3. The GTP-U service is associated with an SAEGW service for receiving GTP-U packets (for Router Advertisement/Router Solicitation or any data buffering required at Control Plane).

Sx Interface

As part of the CUPS architecture, the Sx interface is used for communication between Control Plane and User Plane.

At Control Plane, the SAE-GW service is associated with Sx service for communication with the User Plane. Also, a single Sx service is capable of handling all interfaces like Sxa, Sxb, and Sxab, which is required for Pure-S, Pure-P and Collapsed PDN respectively.

Licensing Information

The Cisco UPC CUPS supports Cisco Smart Licensing, a cloud-based licensing model that simplifies the purchase, deployment, and management of Cisco software assets. For more information, refer to the Smart Licensing collection page.

Supported Features and Functionality

3GPP ULI Enhanced Reporting Support

This feature enhancement covers ULI-related gaps in P-GW and GGSN as per 3GPP standards.

S4SGSN reports ULI to the P-GW through S-GW. P-GW determines the changes in the ULI with previously received ULI. If P-GW detects any change and the change request is from the PCRF as an event trigger, then the P-GW reports the ULI to the PCRF.

SGSN reports ULI to the GGSN. GGSN determines the changes in the ULI with previously received ULI. If GGSN detects any change and the change request is from the PCRF as an event trigger, then the GGSN reports the ULI to the PCRF. This feature also supports the detection of the change in RAI received as part of the ULI field at GGSN.

For more information on 3GPP ULI Reporting Support Enhancement, refer the *3GPP ULI Reporting Support Enhanced* section in the *StarOS P-GW Administration Guide*.

AAA Server Group

The AAA Server Group feature is used to create and manage the Diameter/RADIUS server groups within the context or system. The AAA server group facilitates management of group (list) of servers at per subscriber/APN/realm-level for AAA functionality.

APN Configuration Support

Note Revision history details are not provided for features introduced before release 21.24.

Revision Details	Release
First introduced	Pre 21.24

The CLI commands **radius-group**, **cc-home behaviour 0x10 profile 2** and **mediation-device** are qualified and validated in the CUPS architecture to support APN configuration.

radius-group

Under this functionality validation the CUPS architecture supports 800 Radius Server Groups each group configured with RADIUS Authentication and Accounting server.

cc-home { behavior *bits* | profile *index* }

Configures the home subscriber charging characteristics (CC) used by the GGSN when those from the SGSN will not be accepted. The values configured in the CLI are taken into precedence by CUPS SAEGW service and populated appropriately in the GTPP CDR records.

NOTES:

- **behavior** *bits*: Specifies the behavior bit for the home subscriber charging characteristic. bits can be configured to any unique bit from 001H to FFFH (0001 to 1111 1111 1111 bin) where the least-significant bit corresponds to B1 and the most-significant bit corresponds to B12.
- **profile** *index*: Specifies the profile index for the home subscriber charging characteristic. index can be configured to any integer value between 0 and 15. Default: 8
- For more information, refer to the **cc-home** command under *APN Configuration Mode Commands* chapter in the *Command Line Interface Reference A-B* document

mediation-device [context-name *context_name*] [delay-GTP-response] [no-early-PDUs] [no interims] +

This command and all associated sub section CLIs are supported in CUPS. This CLI enables use of **mediation device** and all associated configuration that can be used for a given APN by CUPS SAEGW service.

NOTES:

- **context-name** *context_name*: Configures the mediation VPN context for this APN as an alphanumeric string of 1 through 79 characters that is case sensitive. If not specified, the mediation context is the same as the destination context of the subscriber. Default: The subscribers destination context.
- **delay-GTP-response**: When enabled, delays the CPC response until an Accounting Start response is received from the mediation device. Default: Disabled.
- **no-early-pdus**: Specifies that the system delays PDUs from the MS until a response to the GGSN accounting start request is received from the mediation device. The PDUs are queued, not discarded. Default: Disabled.
- **no-interim**: Disables sending interims to the mediation server. Default: Disabled.
- For more information, refer to the **mediation-device** command under *APN Configuration Mode Commands* chapter in the *Command Line Interface Reference A-B* document

Asynchronous Core Transfer Support for egtpinmgr

Asynchronous core transfer support for egtpinmgr has been added in CUPS to optimize outage time during an egtpinmgr restart.

Previously, when the egtpinmgr restarted, the recovery process began only after a core dump file was created and transferred. However, the time taken to transfer the core file was significant. The outage time during an egtpinmgr restart was equal to the egtpinmgr recovery time plus the core file transfer time.

Support for Asynchronous Core Transfer has been added in CUPS to include the egtpinmgr during the recovery process. Now, recovery begins when the egtpinmgr process crashes without waiting for the kernel to complete a core dump file transfer and release its resources. As a result, the outage time during an egtpinmgr restart is equal to the egtpinmgr recovery time only.

With this enhancement, outage time during an egtpinmgr restart is reduced. The outage time consists only of the time required to recover the egtpinmgr. The time taken to create and transfer the core file no longer contributes to the outage time.

Note The Asynchronous Core Transfer Support for egtpinmgr is an existing feature that is supported in non-CUPS architecture. With this release, the feature is qualified in CUPS architecture.

Bit Rate Mapping Support

P-GW converts the bit rate value that it receives from PCRF from bps to kbps. This conversion may lead to truncation of fractional value to nearest integer (floor) value and lead to loss of information. 3GPP suggested that if the conversion from bps to kbps leads to a fractional value, then it should be rounded up to the nearest integer value (ceil) value and sent to the access side.

Note Design changes are done to ensure rounded down (floor) value from bps to kbps is sent on the PFCP interface.

Standards Compliance

The bit rate mapping feature complies with 3GPP TS 29.274 release 12.

Configuring the Bit Rate Mapping Feature

To configure the rounded up (ceil) value for bit rate from bps to kbps in APN-AMBR, GBR, and MBR on P-GW, perform the following steps:

```
configure
  context context_name
    pgw-service service_name
      [ no ] egtp bitrates-rounded-down-kbps
      end
```

To configure the rounded down (floor) value for bit rate from bps to kbps in APN-AMBR, GBR, and MBR on P-GW, perform the following steps:

```
configure
  context context_name
    pgw-service service_name
      egtp bitrates-rounded-down-kbps
      end
```

New Behavior in CUPS

By default, the rounded up value of bit rate in kbps for APN-AMBR, MBR, and GBR will be sent on the Sx and GTP interfaces. To enable the rounding down behavior, CLI must be configured.

Call Log Summary

Call Log Summary (CLS) is a mechanism by which subscriber activities like Session Creation or Deletion, Bearer Creation or Update or Deletion is reported to external server.

When CLS is enabled on the CUPS CP node, it generates events records. These records can be stored in chassis hard disk in CSV file format.The files can be stored in *.gz* compressed format as well. These files are later SFTPed to external server for further analysis from network operator in order to maintain and troubleshoot the network.

In CUPS mode the feature can be enabled in Control Plane node, where SGW, PGW records are generated depending upon SAEGW call type.

Note For more details on Call Log Summary (CLS), refer to the StarOS SAEGW Administration Guide.

Charging Data Records to HDD

A Charging Data Record (CDR) is a formatted collection of information about a chargeable event. The GTPP accounting CDRs that are generated are sent to an external node for storage. The CDRs are written to files in formats supported by the external node and stored on the hard disk (HDD). From the HDD, CDR files can be pushed or pulled using FTP or SFTP protocols.

Note It is strongly recommended that you do not use the system directories created by StarOS under */hd-raid/records/* for deployment use cases such as backups. If such directories are used, this could impact the normal functioning of the product.

CDR is an existing feature that is supported in the non-CUPS architecture, and qualified in the CUPS architecture. For additional information, see the *HDD Storage* chapter in the *GTPP Interface Administration and Reference*.

GTP-C Path Failure Enhancements and Improved Debugging Tools

In CUPS architecture, enhancements have been added to optimize GTP-C path failure functionality, and to improve the debug capability of the system for GTP-C path failure problems. These features will help Operators and Engineers to debug different aspects of the system that will help in identifying the root cause of GTP-C path failures in the network. These enhancements affect path failure detection via the S5, S8, S2b, and S2a interfaces.

These enhancements are part of this feature:

- The node can be configured so that it does not detect a path failure if a low restart counter is received due to incorrect or spurious messages. This prevents call loss. The option to disable path failure due to Echo Request/Response and Control Message Request/Response messages is also available so that call loss is prevented in the event of a false path failure detection.
- More granularity has been added to GTP-C path failure statistics so that the root cause of issues in the network can be diagnosed more quickly.

- A path failure history for the last five path failures per peer is available to assist in debugging path failures in the network.
- Seamless path failure handling is implemented so that call loss is avoided during redundancy events.

Note The GTP-C Path Failure Enhancements and Improved Debugging Tools is an existing feature that is supported in non-CUPS architecture. With this release, the feature is qualified in CUPS architecture. For additional information, refer the *GTP-C Path Failure Enhancements and Improved Debugging Tools* section in the *P-GW Administration Guide*.

GTPP Suppress-CDR No Zero Volume

This feature allows suppression of CDRs with zero byte data count, so that the OCG node is not overloaded with a flood of CDRs. The CDRs can be categorized as follows:

- Final-cdrs: These CDRs are generated at the end of a context.
- Internal-trigger-cdrs: These CDRs are generated due to internal triggers such as volume limit, time limit, tariff change, or user-generated interims through the CLI commands.
- External-trigger-cdrs: These CDRs are generated due to external triggers such as QoS Change, RAT change and so on. All triggers which are not considered as final-cdrs or internal-trigger-cdrs are considered as external-trigger-cdrs.

The customers can select the CDRs they want to suppress.

The CLI command mentioned below helps suppress CDRs on different CDR triggers supported in CUPS:

- **[default | no] gtpp suppress-cdrs zero-volume { external-trigger-cdr | final-cdr | internal-trigger-cdr }**

Lawful Intercept

The Cisco Lawful Intercept feature is supported on CUPS. Lawful Intercept is a licensed-enabled, standards-based feature that provides telecommunications service providers with a mechanism to assist law enforcement agencies in monitoring suspicious individuals for potential illegal activity.

For additional information and/or to obtain documentation for Lawful Intercept feature, contact your Cisco Account representative.

Location Based DNS and PCSCF IP Address Selection

Location-based DNS and P-CSCF Selection provides an option to the operator to manage the DNS server address and P-CSCF IP address according to location information.

P-GW gathers the DNS server address and P-CSCF IP address information by Tracking Area Identifier (TAI), which is achieved through the TAC-based Virtual APN (VAPN) selection.

When UE sends the PCO request in session creation, P-GW selects the Virtual APN (VAPN) with the received location information. The selected VAPN (with DNS server address and P-CSCF IP address configured in it) with PCO IE is sent in the Create session response.

Following are the CLI commands for enabling the Location-based DNS and PCSCF IP address selection:

Command	Description
Tracking-area-code-range from <*start value*> **to** <*end value*>	Provides the tracking area code range, starting from 0 through 65536. The end value is always greater than the start value.
P-cscf priority <*priority*> **ip/ipv6** <*IPv4/Ipv6 address*>	Specifies the priority for P-CSCF address for the APN. Address_ priority is an integer 1–3. One is the maximum priority. IPv4_address is in IPv4 dotted-decimal notation. IPv6_address is in IPv6 colon-separated-hexadecimal notation.
Show apn name <*APN Name*>	To show PCSCF IP address at APN
dns primary <*IPv4 address*> **Dns secondary** <*IPv4 address*> **ipv6 dns primary** <*IPv6 address*> **ipv6 dns secondary** <*IPv6 address*>	Primary: Configures the primary DNS server for the APN. Secondary: Configures the secondary DNS server for the APN. Only one secondary DNS server is configurable. Address: Configures the IP address of the DNS server expressed in IPv4 dotted-decimal notation. Default: primary = 0.0.0.0, secondary = 0.0.0.0 dns_address: Specifies the IP address of the DNS server to remove, expressed in IPv4 dotted-decimal notation.
Show apn name <*APN Name*>	To show DNS IP address at APN

MPRA Support

P-GW supports negotiation of Multiple-Presence Reporting Area feature in Feature-List-ID 2 over Gx interface with PCRF. The CNO-ULI feature works only when the P-GW and/or the PCRF doesn't support Multiple-PRA and both P-GW and PCRF support CNO-ULI.

For Multiple-PRA feature support during the lifetime of the IP-CAN session, P-GW handles the change of UE Presence in Reporting Areas request from PCRF in PRA-Install AVP including the Presence-Reporting-Area-Information AVPs. Each AVP contains the Presence Reporting Area Identifier within the Presence-Reporting-Area-Identifier AVP

For more information on Presence Reporting Area (PRA) and Multiple PRA, refer the *Presence Reporting Area* chapter in the *StarOS P-GW Administration Guide*.

Fallback to default rulebase during movement from 5G Area to 4G Area

Feature Name	Release Information	Description
Fallback to default rule during 5G to 4G movement with PRA	2025.02.0	This feature enables the session to fallback to the default rulebase when the call moves from 5G area to 4G area. This allows the call to be continued with the default rule configured under APN, even when the PCRF removes the only installed rulebase when the call moves from 5G to 4G. **Commands Introduced:** **active-charging fallback-to-apn-rulebase**: This CLI is configured under APN to make the session fallback to its default rulebase. **Default Settings:** Disabled—Configuration Required to Enable.

When the call is initially attached to 4G, the default rulebase confgured under APN is the 4G rulebase. If the session transitions from 4G to 5G, the PCRF overwrites the 4G rulebase and installs the 5G rulebase.

However, if the session moves back from 5G to 4G again, as a default behvior, the PCRF removes the 5G rulebase and does not install the 4G rulebase. As a result, the session gets disconnected.

To solve this issue, this feature allows the network operator to configure the session to fallback to the default rulebase configured under APN. This allows the session to be continued, even when the PCRF removes the only installed rulebase after the session moves back from 5G to 4G.



Note This functionality is applicable to all other scenarios of hand-offs where the rulebase is removed without installing the new rulebase from the call.

Enable fallback to default rulebase during 5G area to 4G area movement

Follow these steps to enable Fallback to Default Rulebase during 5G to 4G movement:

Procedure

Step 1 Use the command **context** *context_name* to create an instance of the context profile after entering the Global configuration mode.

Example:

```
[local]qvpc-si# configure
[local]qvpc-si(config)# context ingress
[ingress]qvpc-si(config-ctx)#
```

Step 2 Use the command **apn** *apn_name* to enter into the APN configuration mode.

Example:

```
[ingress]qvpc-si(config-ctx)# apn intershat
[ingress]qvpc-si(config-apn)#
```

Step 3 Use the command **active-charging fallback-to-apn-rulebase** to enable fallback to the default rulebase configured under APN.

Example:

```
[ingress]qvpc-si(config-apn)# [no] active-charging fallback-to-apn-rulebase
```

Note

- By default, this CLI is disabled.
- This CLI configuration will be applicable for the new incoming calls only. The existing calls will not have any impact on the ongoing calls.

Once this CLI is configured with **[no]** and the PCRF removes the rulebase, session will not fall back to default rulebase configured under APN. This will result in the termination of the call.

Step 4 Use the command **show apn name intershat** to verify if the fallback functionality is enabled under the APN.

Example:

```
[local]qvpc-si# show apn name intershat
access point name (APN):  intershat
authentication context:  ingress
pdp type:  ipv4 and ipv6
emergency: no
delay tolerant pdn: no
PCO Options:
    custom1      Mode: disabled
    custom2      Mode: disabled        PCO Value: n/a
    custom3      Mode: disabled        PCO Value: n/a
    custom4      Mode: disabled        PCO Value: n/a
    custom5      Mode: disabled        PCO Value: n/a
    custom6      Mode: disabled        PCO Value: n/a
    custom7      Mode: disabled        PCO Value: n/a
    custom8      Mode: disabled        PCO Value: n/a
    custom9      Mode: disabled        PCO Value: n/a
    custom10     Mode: disabled        PCO Value: n/a
    Link MTU: 1500
    Non-IP Link MTU: 1358
    Roamer Link MTU: 1500
    ePDG Selection FQDN: N/A
ehrpd access: N/A
.
.
.
.
Fallback To APN Rule Base : Disabled
```

No udp-checksum Support

This feature supports **no udp-checksum** CLI command for CUPS under GTPU service where **udp-checksum** is disabled in the outer GTPU header for the downlink subscriber packet. When downlink packet arrives from internet, the GTPU header is added on top of the packet and is sent to the access side. The "checksum" value is zero in the outer UDP layer of this packet enabling optimization and therefore, improving the performance throughput.

Use the following configuration to enable the feature.

```
configure
  context context_name
    gtpu-service gtpu_service_name
    [ no ] udp-checksum
    end
```

Show Commands and Outputs

This section provides information about the show CLI commands available in support of the feature.

Use the following command to determine if **GTPU UDP Checksum** is enabled or disabled.

- **show gtpu-service all**—Displays all GTPU services.
- **show gtpu-service name** *service_name*—Displays information for the specific GTPU service name.

Optimization for egtpinmgr Recovery

Previously, when the egtpinmgr task restarted, it took a significant amount of time for it to recover. As a result, the outage time when the SAEGW were unable to accept any new calls during egtpinmgr recovery was high.

The software has been enhanced to optimize the recovery outage window in the event of an egtpinmgr task restart; this has been achieved by optimizing the internal algorithms of egtpinmgr recovery and the data structures required. In addition, recovery time now is dependent only on the number of unique IMSIs and not on the number of sessions for an IMSI.



Note The Optimization for egtpinmgr Recovery is an existing feature that is supported in non-CUPS architecture. With this release, the feature is qualified in CUPS architecture.

QUIC IETF Implementation

In the current framework, Deep Packet Inspection (DPI) is done for every packet in a flow when it reaches the plugin. The DPI is done by analyzing the packets and extracting deterministic patterns. The DPI is done in-order to detect the application and to classify its subtype. Plugin excludes the flow after the DPI. The flow is offloaded after the detection. As part of QUIC IETF, the initial QUIC handshake packets (Client/Server Hello) are encrypted over the network. Hence, there are no deterministic patterns available for detection of the application. Support is added in p2p plugin to decrypt and obtain the SNI (Server Name Indication) for detection.

Configuring QUIC IETF

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

```
configure
  active-charging service acs_service_name
    p2p-detection debug-param protocol-param p2p_quic_ietf_decrypt 1
    end
```

Note By default, the CLI is disabled and there's minimal impact on the performance due to TLS decryption.

Quota Hold Time Support

Quota-Hold-Time (QHT) is an inactivity time duration, after which the Gateway(Diameter client) returns the Charging-Bucket with its usage and reaches a clean-state.

The QHT value is provided by the OCS per Category - Multiple-Services-Credit-Control (MSCC), or the gateway provides an option to configure the default value of the QHT - for enabling the default QHT value for the MSCCs for which the OCS has not provided any QHT AVP.

The QHT timer runs per MSCC bucket. If the QHT timer expires without a packet during run-time, then the usage is reported with the Reporting-Reason: QHT as per 3GPP specification.

The QHT value received in the CP from the OCS, is sent in the "Quota Holding Time" IE defined in the CUPS specification 3GPP TS 29.244. Also along with provisioning the Quota-Holding-Time IE to the UP, the Reporting-Triggers will be sent with the bit corresponding to Quota-Holding-Time SET, so that on QHT expiry the reporting takes place.

The UP on receiving the Quota-Holding-Time IE along with the QHT Reporting-Triggers enabled, starts the timer per URR to monitor the inactivity period. Once the inactivity period exceeds the QHT time, the Usage-Reporting is initiated from the UP for the Trigger : Quota-Holding-Time.

The CP on receiving the QHT event from UP, triggers the QHT reporting to the OCS after updating the usage in the MSCC bucket.

Configuring Quota Hold Time

Use the following configuration to enable Quota Hold Time in CUPS:

```
configure
  require active-charging
  active-charging service service_name
    credit-control group group_name
      quota-hold-time timer_value
      end
```

NOTES:

- **quota-hold-time**: configures the inactivity duration after which the charging bucket reports its usage and have a clean state.

Limitation

The QHT (inactivity-timer) usually is a larger value compared to the flow-idle timer. If the flow-idle timer is larger than QHT, then there is a possibility for the flows present even after the QHT expiry, and is processed by VPP as per the NoQuota Pending-Traffic-Treatment configuration.

S-GW Paging Enhancement

S-GW Paging includes the following scenarios:

Scenario 1: S-GW sends a Downlink Data Notification (DDN) message to the MME/S4-SGSN nodes. MME/S4-SGSN responds to the S-GW with a DDN Ack message. While waiting for the DDN Ack message from the MME/S4-SGSN, if the S-GW receives a high priority downlink data, it does not resend a DDN to the MME/S4-SGSN.

Scenario 2: If a DDN is sent to an MME/S4-SGSN and TAU/RAU MBR is received from another MME/S4-SGSN, S-GW doesn't send DDN.

Scenario 3: DDN is sent to an MME/S4-SGSN and DDN Ack with Cause #110 is received. DDN Ack with cause 110 is treated as DDN failure and standard DDN failure action procedure is initiated.

To handle these scenarios, the following two enhancements are added to the DDN functionality in CUPS architecture:

- High Priority DDN at S-GW
- MBR-DDN Collision Handling

These enhancements support the following:

- Higher priority DDN on S-GW and SAEGW, which helps MME/S4-SGSN to prioritize paging.
- Enhanced paging KPI and VoLTE services.
- DDN message and mobility procedure so that DDN isn't lost.
- MBR guard timer, which is started when DDN Ack with temporary HO is received. A CLI command **ddn temp-ho-rejection mbr-guard-timer** has been introduced to enable the guard timer to wait for MBR once the DDN Ack with cause #110 (Temporary Handover In Progress) is received.
- TAU/RAU with control node change triggered DDNs.

In addition, to be compliant with 3GPP standards, support has been enhanced for Downlink Data Notification message and Mobility procedures. As a result, DDN message and downlink data which triggers DDN is not lost. This helps improve paging KPI and VoLTE success rates in scenarios where DDN is initiated because of SIP invite data.



Note For information on Downlink Data Notification (DDN) messages with support for DDN Delay and DDN Throttling, refer the *SAEGW Idle Buffering with DDN Delay and DDN Throttling* chapter in this guide.

For more information on how S-GW Paging Enhancement feature works, configuration, monitoring and troubleshooting, refer the *S-GW Paging Enhancements* chapter in the StarOS *S-GW Administration Guide*.

Session Recovery and ICSR at Control Plane

The Session Recovery (SR) feature provides seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault within the system preventing a fully connected user session from being disconnected.

The Interchassis Session Recovery (ICSR) feature provides the highest possible availability for continuous call processing without interrupting subscriber services. ICSR allows the operator to configure gateways for redundancy purposes. In the event of a gateway failure, ICSR allows sessions to be transparently routed around the failure, thus maintaining the user experience. ICSR also preserves session information and state.

The existing non-CUPS framework is extended to support CUPS Control Plane SR and ICSR. At Control Plane, complete session/PDN state is recovered in case of SR/ICSR.

For more information on SR and ICSR, refer the *Session Recovery* and *Interchassis Session Recovery* feature chapter in the *VPC-SI System Administration Guide*.



Important In this release, if ICSR switchover is performed on Control Plane (CP), then the **show sx peers** CLI command doesn't show any associated peers on new active chassis. However, there's no impact to the functionality.

SRP over IPsec on the Active CP and Standby CP

IPSec is a suite of protocols that interact with one another to provide secure private communications across IP networks. These protocols allow the system to establish and maintain secure tunnels with peer security gateways. IPSec provides confidentiality, data integrity, access control, and data source authentication to IP datagrams.

The CUPS architecture leverages the IPSec protocol to encrypt the packets sent over the Interchassis Session Recovery (ICSR) connection between the active and standby CPs. This encryption is done by defining an access-list to match all traffic between Service Redundancy Protocol (SRP) peers and associating it with a crypto map. This crypto map is used to establish Security Association between IPSec peers residing in CPs.

For more information on IPSec, its features/functionality, and applicable CLI configurations, refer the StarOS *IPSec Reference*.

Example Configurations

1. **IKEv1 – Tunnel Mode**

   The following is an example configuration of IKEv1 in tunnel mode.

```
ACL:
   ip access-list acl_name
      permit ip host ipv4_address host ipv4_address
Transform Set:
crypto ipsec transform-set transform_name esp hmac sha1-96 cipher
aes-cbc-128
     mode tunnel
Policy:
ikev1 policy priority
     encryption aes-cbc-256
     group 5
     lifetime time
Crypto-Map:
crypto map map_name ipsec-ikev1
     match address acl_name
     set peer ipv4_address
     set ikev1 preshared-key ikev1_key
     set pfs group2
     set security-association lifetime seconds seconds
     set transform-set transform_name
Interface Association:
    interface interface_name
       ip address ipv4address_range
```

```
      crypto-map map_name
   interface interface_name loopback
      ip address address_range
!
ip route ipv4address_range interface_name
```

2. **IKEv1 – Transport Mode**

   The following is an example configuration of IKEv1 in transport mode.

```
ACL:
   ip access-list acl_name
     permit ip host ipv4_address host ipv4_address
Transform Set:
crypto ipsec transform-set transform_name esp hmac sha1-96 cipher
aes-cbc-128
     mode transport
Policy:
ikev1 policy priority
     encryption aes-cbc-256
     group 5
     lifetime time
Crypto-Map:
crypto map map_name ipsec-ikev1
     match address acl_name
     set peer ipv4_address
     set ikev1 preshared-key ikev1_key
     set pfs group2
     set security-association lifetime seconds seconds
     set transform-set transform_name
Interface Association:
   interface interface_name
      ip address ipv4address_range
!
   interface interface_name loopback
      ip address address_range
      crypto-map map_name
!
ip route ipv4address_range interface_name
```

Note IKEv1 - Transport mode with Authentication Header (AH) protocol isn't supported. Only Tunnel mode is supported. Encapsulating Security Payload (ESP) is recommended as ESP performs both Authentication and Encryption.

3. **IKEv2 – IPv4**

   The following is an example configuration of IKEv1 for IPv4 address.

```
ACL:
   ip access-list acl_name
     permit ip host ipv4_address host ipv4_address
Transform Set:
ipsec transform-set transform_name
```

```
!
ikev2-ikesa transform-set transform_name
Crypto-Map:
crypto map map_name ikev2-ipv4
     match address name
     authentication local pre-shared-key key key_name
     authentication remote pre-shared-key key key_name
     ikev2-ikesa max-retransmission mt_value
     ikev2-ikesa retransmission-timeout rt_seconds
     ikev2-ikesa transform-set list name
     payload payload match ipv4
       ipsec transform-set list name
     peer ipv4_address
     ikev2-ikesa policy error-notification
Interface Association:
    interface interface_name
      ip address ipv4address_range
      crypto-map map_name
!
    interface interface_name loopback
      ip address ipv4address_range
!
 ip route ipv4address_range interface_name
```

4. **IKEv2 – IPv6**

   The following is an example configuration of IKEv1 for IPv6 address.

```
ACL:
   ip access-list acl_name
     permit ip host ipv6_address host ipv6_address
Transform Set:
ipsec transform-set transform_name
!
ikev2-ikesa transform-set transform_name
Crypto-Map:
crypto map map_name ikev2-ipv6
     match address name
     authentication local pre-shared-key key key_name
     authentication remote pre-shared-key key key_name
     ikev2-ikesa transform-set list name
     payload payload match ipv6
       ipsec transform-set list name
!
     peer ipv6_address
Interface Association:
    interface interface_name
      ipv6 address ipv6_address
      crypto-map map_name
!
    interface interface_name loopback
      ipv6 address ipv6_address
!
 ipv6 route ipv6address_range interface_name
```

NOTES:

- MTU must be configured to maximum limit of loopback interface. For example:

```
configure
   context SRP
      ip path-mtu-max 1300
```

- IKEv1 - Transport mode with Authentication Header (AH) protocol isn't supported. Only Tunnel mode is supported. Encapsulating Security Payload (ESP) is recommended as ESP performs both Authentication and Encryption.
- Auto-delete Existing IKEv1/IKEv2 ACL Tunnels: Critical (Authentication, Encryption, Hash, and DH group) parameter changes inside the IKEv1 policy deletes all the established tunnels within that context.

  Refer *Auto-delete Existing IKEv1/IKEv2 ACL Tunnels* section in the StarOS *IPSec Reference* for more information.

SRVCC PS to CS Handover Indication and the QoS Class Index IMS Media Configuration Support

This feature notifies the PCRF about the cause for PCC rule deactivation on Voice bearer deletion. This notification helps the PCRF to take further action appropriately.

This feature ensures the compliance for SRVCC. This feature also supports the PS-to-CS handover indication after release of the voice bearers.

SRVCC service for LTE lets a single radio User Equipment (UE) accessing IMS-anchored voice call services to switch from LTE network to Circuit Switched domain. The UE switches the network while it can transmit or receive on only one of the access networks then. The SRVCC service removes the need for a UE to have multiple Radio Access Technology (RAT) capabilities.

After handing over the PS sessions to the target, the source MME removes the Voice Bearers (VB). The MME removes the VB by deactivating the voice bearers. The MME bars the VB towards S-GW/P-GW and sets the VB flag of Bearer Flags IE in the Delete Bearer Command message (TS 29.274 v9.5.0).

If the IP-CAN bearer termination happens due to PS to CS handover. The PCEF reports the related PCC rules for this IP-CAN bearer by including the Rule-Failure-Code AVP set to the value: PS_TO_CS_HANDOVER (TS 29.212 v10.2.0 and TS 23.203 v10.3.0).

Support for new AVP PS-to-CS-Session-Continuity (added in 3GPP Release 11) inside Charging Rule Install indicates the bearer support for PS to CS continuity.

QCI IMS-Media Configuration Support

Specifies the QoS Class Index (QCI) value to mark the IMS media bearers for preferential treatment during session recovery and ICSR switchover.

Mode

Exec > Global Configuration > Context Configuration > APN Configuration

configure > context <*context_name* > **apn** <*apn_name*>

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

qci *value_bytes* **ims-media**

no qci *value_bytes* **ims-media**

Note

- *no*: Disables this IMS QCI feature.
- *ims_media*: Marks bearers classified as IMS media for preferential treatment during session recovery and ICSR switchover.
- *value_bytes*: Specifies the QCI value an integer from 1 through 254.

Usage Guidelines

Use this command to specify the QCI value to be used to mark bearers classified as IMS media for preferential treatment during session recovery and ICSR switchover.

The following prerequisites apply to the implementation of this feature:

- A dedicated APN must be reserved for VoLTE traffic.
- A call connected to this APN will not be classified as Active VoLTE unless there is a dedicated bearer matching the VoLTE-configured QCI.
- Preferential treatment would be given to only those calls which are active VoLTE.
- A GGSN call connected to this APN will not be classified as Active VoLTE unless there is network initiated bearer matching the VoLTE-configured QCI.
- VoLTE marking is preserved across a Gn-Gp handoff.

When this feature is enabled via a CLI command, the actions are taken:

- During bearer creation
  - New bearer QCI is matched against APN configuration.
  - If the QCI matches an APN configuration, the bearer is marked for preferential treatment.
  - Flow_entries are modified with this information (if this is first VoLTE bearer).
  - Egtpu_session is updated with the VoLTE tag during a rx_setup request.
  - An indication message informs ECS about the VoLTE tagging.
- During bearer deletion
  - Flow_entry is updated with VoLTE information if this is the last VoLTE bearer.
  - ECS is informed of the deletion via an indication message.

The following command enables preferential treatment for IMS bearers with a QCI of 9:

qci 9 ims-media

Support for ip hide-service-address CLI Command

The **ip hide-service-address** CLI command is supported in CUPS.

When enabled, this CLI renders the IP address of the GGSN unreachable from mobile stations (MSs) using this APN. This command is configured on a per-APN basis.

Use the following configuration to enable or disable the feature.

```
configure
  context context_name
    apn apn_name
      [ default | no ] ip hide-service-address
      end
```

- **default**: Does not allow the mobile station to reach the GGSN IP address using this APN.
- **no**: Allows the mobile station to reach the GGSN IP address using this APN.
- Use this command to prevent subscribers from using traceroute to discover the network addresses that are in the public domain and configured on services.

Support for regardless-of-other-triggers CLI Command

This feature supports **regardless-of-other-triggers** option in CLI for CUPS. **regardless-of-other-triggers** option enables eG-CDR or P-GW-CDR generation at the fixed time interval irrespective of any other eG-CDR or P-GW-CDR triggers that may occur in between. Therefore, when you enable this option although other CDR triggers occur, the Time Limit CDR gets triggered dynamically at every *interval* in seconds, that is, the Time Threshold calculation is based on the sum of the last threshold time and the interval. This option supports session recovery and ICSR.

Use the following configuration to enable the feature.

```
configure
  active-charging service service_name
    rulebase rulebase_name
      egcdr threshold interval interval regardless-of-other-triggers
      end
```

The following steps are carried out when a new call comes in:

- When you enable, **regardless-of-other-triggers** even if any other usage report triggers in between, timer will not be reset, and the session usage report for the time threshold occurs for every interval time configured.

Show Commands and Outputs

This section provides information about the show CLI commands available in support of the feature.

- **show active-charging rulebase name** *name*
- **show active-charging rulebase all**

The output of these CLI commands includes the following fields to support this feature.

- Interval Threshold: <seconds> (secs) Regardless of Other Triggers

TFT Suppression for Default Bearer

Feature Description

TFT Suppression for default bearer is supported in the UPC CUPS architecture. Following CLI commands are added in support of this feature.

- **policy-control update-default-bearer**
- **no tft-notify-ue-def-bearer**

The preceding CLI commands are used to bind all the predefined rules received from PCRF without QoS and ARP or with the same QoS and ARP as that of the default bearer, to the default bearer.



Important This CLI is applicable to all the rulebases in the chassis configuration. If the rulebase is changed to some other rulebase in the interim period or anytime later, this CLI will continue to apply to the current new rulebase too.

Configuring TFT Suppression

Configuring TFT Suppression in Default Bearer for Predefined Rules

Use the following commands to configure TFT Suppression for default bearers.

```
configure
  require active-charging
  require active-charging service_name
    [ default | no ] policy-control update-default-bearer
    end
```



Caution Upon executing this CLI command "**no policy-control update-default-bearer**", system crash is likely to occur if the TFT information is not added to the charging-action.

Configuring TFT Suppression in Default Bearer

Use the following commands to configure TFT Suppression for default bearers.

```
configure
  require active-charging
  require active-charging service_name
    rulebase rulebase_name
      [ default | no ] tft-notify-ue-def-bearer
    end
```

Note

- **default:** Configures this command with its default setting.

  Disables only binding those rules having QoS of default bearer to the default bearer and specifies to not ignore other rules. Rules having respective QoS gets attached to the relevant bearers. Also, TFT updates towards UE (access side) is not suppressed.

- **no:** Enables binding rules having QoS of default bearer to the default bearer and specifies to ignore other rules.

  In case no QoS is specified the rule gets attached to default bearer. Also, TFT updates towards UE (access side) is suppressed for default bearer. So only one default-bearer is ever be created.

Zero-byte EDR Suppression

The Zero-byte Event Data Record (EDR) Suppression, a CLI-controlled feature, enables or disables creation of EDRs when there is no data for the flow. A zero-byte EDR is typically possible when two successive EDRs are generated for a flow. The CLI command suppresses the second such EDR for the flow.

Use the following configuration to enable or disable the suppression of zero-byte EDRs.

```
configure
  active-charging service service_name
    rulebase rulebase_name
      [ default | no ] edr suppress-zero-byte-records
      end
```

NOTES:

- **default**: Configures this command with its default setting.

  Default: Disabled; same as **no edr suppress-zero-byte-records**

- **no**: Disables the suppression of zero-byte EDRs.
- **edr suppress-zero-byte-records**: Suppresses zero-byte EDRs.
- The "Total zero-byte EDRs suppressed" field in the output of the following CLI command can be used to verify if the zero-byte EDRs are suppressed: **show user-plane-service statistics rulebase name** *rulebase_name*.

How It Works

Architecture

User Plane Selection

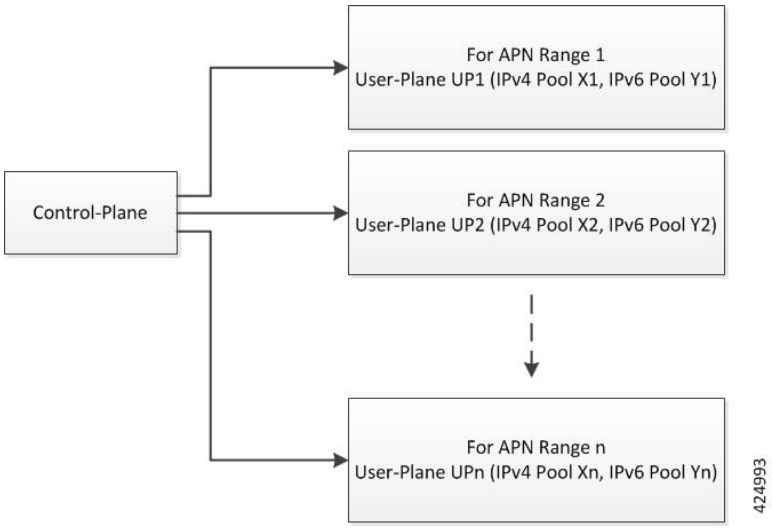
This section describes how Control Plane selects a particular User Plane for communicating through the Sx interface. The current mechanism uses APN information associated with that PDN, as a key for selecting the User Plane Profile.

Pure-P/ Collapsed PDN

The following flow describes how APN is used as a key for selecting a particular User Plane group.

APN → Associated IP Pool → Associated User Plane Profile ID → User Plane Profile

Every APN is configured with both the associated IPv4 and IPv6 pools. Also, all configured IP pools under APN configuration are associated with the same User Plane group, which contains information related to User Plane IP address and User Plane capabilities. In case Control Plane has to communicate with the same User Plane for all APNs, the IPv4 and IPv6 Pool configuration under APN configuration is not required.



NOTES:

- Control Plane can be configured to communicate with multiple User Planes.
- There is 1-n mapping between the User Plane and APN.
- Multiple APNs can be reached through the same User Plane but for every APN, there can be only one associated User Plane.

Pure-S PDN

The following flow describes how APN is used as key for selecting a particular User Plane group. The APN profile must be configured with associated User Plane group, which contains information related to User Plane IP address and User Plane capabilities.

APN Profile → Associated User Plane Profile ID → User Plane Group

Call Flows

Following is a high-level description of the Control Plane flow in CUPS architecture:

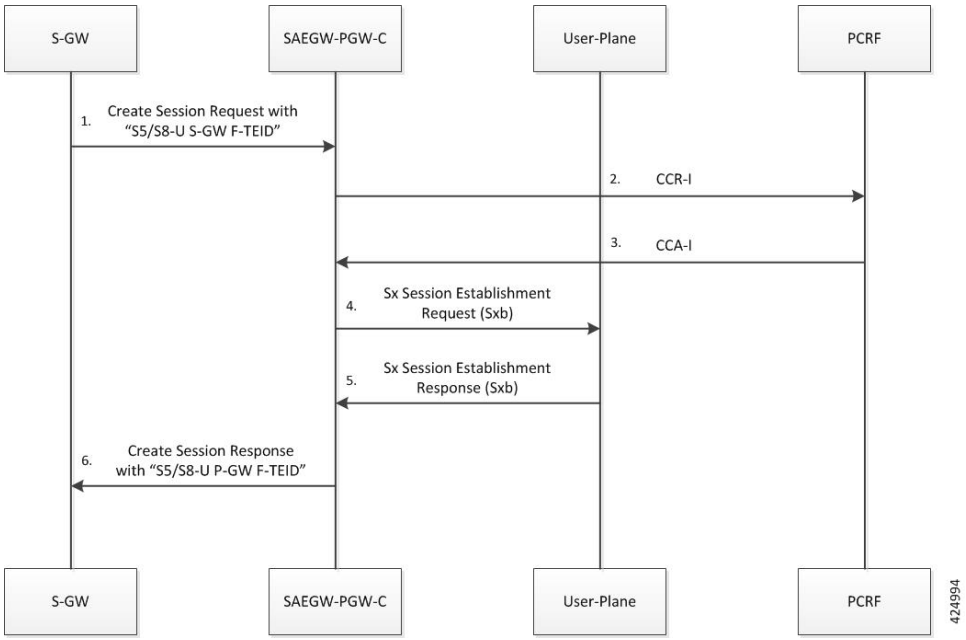
- On receipt of the Create Session Request, the S-GW first makes Sx communication (Sx Session Establishment Request/Response) before sending Create Session Request toward the P-GW.
- On receipt of Create Session Request, the P-GW does the following in sequence:
  - Gx Communication (IP-CAN Session Establishment procedure),

- Sx Communication (Sx Session Establishment Request/Response), followed by
- Create Session Response toward S-GW.

- On receipt of the Create Session Response from P-GW, the S-GW first makes Sx communication (Sx Session Modification Request/Response) before sending Create Session Response toward the MME.

Initial Attach Procedure (Pure-P)

The following call flow illustrates, at a high-level, the initial attach procedure for a Pure-P PDN.



1. For CUPS SAEGW Pure-P call, SAEGW-PGW-C does the following:
   - After Gx interaction, performs Gx communication (CCR-I and CCA-I).
   - Performs User Plane selection based on **user-plane-profile** configured with IP Pool (APN associated with IP Pool).
   - Establishes GTP-U session (required for RA/RS, in case of IPv6/IPv4v6 PDN).
   - Performs Sxb interaction with selected User Plane.
2. Sx Establishment Request contains the following information:
   - Create PDR/FAR/URR information for Uplink and Downlink data path: For dynamic/pre-defined/static rules.
   - Create PDR/FAR for RA/RS: Required for IPv6/IPv4v6 PDN Type.

Important

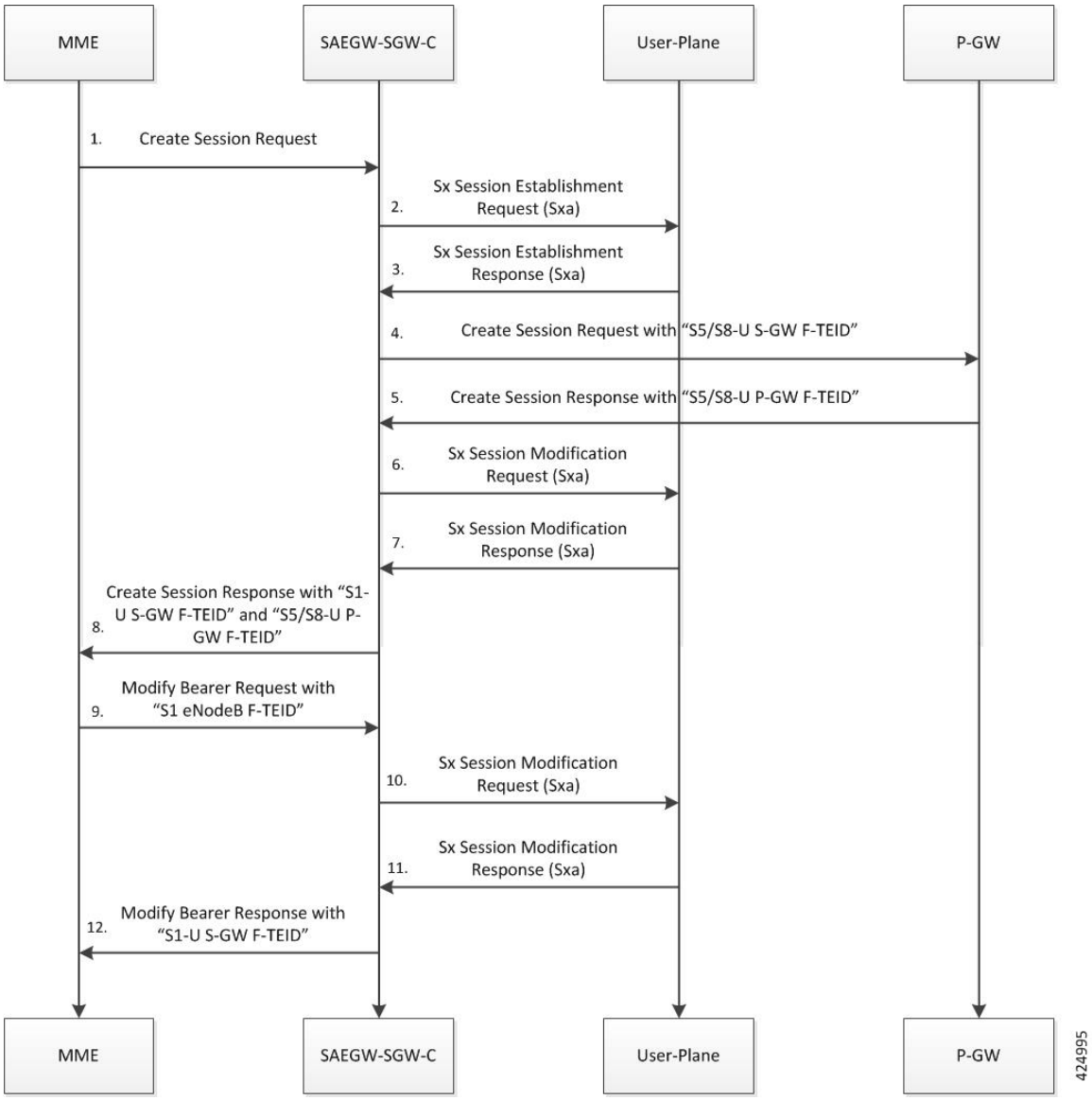
- Create Uplink PDR is sent with "Outer Header Removal" based on IP address information in "S5/S8-U S-GW F-TEID".
- Create Downlink FAR is sent with "Outer Header Creation" as "S5/S8-U S-GW F-TEID".

- Additionally, Control Plane requests User Plane to allocate F-TEID for P-GW Ingress PDR "S5/S8-U P-GW F-TEID"

3. User Plane provides following information as part of Sx Session Establishment Response:
   - Created PDR: P-GW Ingress PDR "S5/S8-U P-GW F-TEID"
4. On receipt of Sx Session Establishment Response, the SAEGW-PGW-C sends Create Session Response toward S-GW with "S5/S8-U P-GW F-TEID"

Initial Attach Procedure (Pure-S)

Following call flow illustrates, at a high-level, the initial attach procedure for a Pure-S PDN.

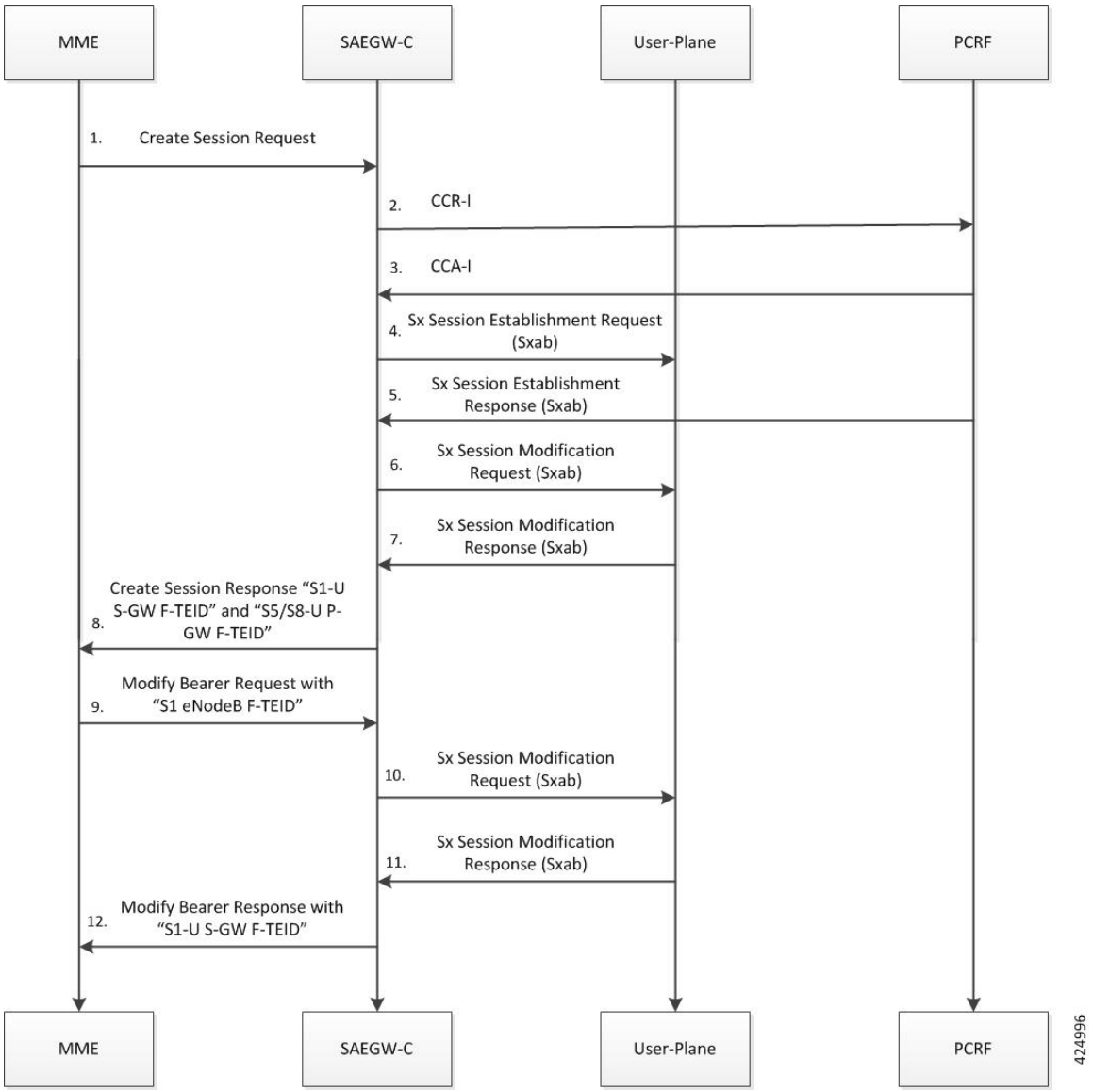


1. For CUPS SAEGW Pure-S call, the SAEGW-SGW-C does the following:
   - Performs User Plane selection based on APN profile.
   - Performs Sxa interaction with selected User Plane.
   - No GTP-U interaction (Note that it is required for non-CUPS behavior).
2. Sx Session Establishment Request contains following information:
   - Create PDR/FAR for S-GW Uplink and Downlink data path.
   - Aditionally, Control Plane requests User Plane to allocate F-TEID for:
     - S-GW Ingress PDR "S1-U S-GW F-TEID"
     - S-GW Egress PDR "S5/S8-U S-GW F-TEID"

3. User Plane provides following information as part of Sx Session Establishment Response:
   - Created PDR: S-GW Ingress PDR "S1-U S-GW F-TEID"
   - Created PDR: S-GW Egress PDR "S5/S8-U S-GW F-TEID"
4. On receipt of Sx Session Establishment Response, the SAEGW-SGW-C sends Create Session Request toward P-GW with "S5/S8-U S-GW F-TEID"
5. On receipt of Create Session Response, the SAEGW-SGW-C does the following:
   - Trigger Sx Session Modification Request:
     - To update Uplink FAR with "Outer Header Creation" as "S5/S8-U P-GW F-TEID".
     - To update Downlink PDR with "Outer Header Removal" based on IP address information in "S5/S8-U P-GW F-TEID".
6. On receipt of Sx Session Modification Response, the SAEGW-SGW-C sends Create Session Response toward MME with "S1-U S-GW F-TEID" and "S5/S8-U P-GW F-TEID".
7. On receipt of Modify Bearer Request (MBR), the SAEGW-SGW-C does the following:
   - MBR is consumed by S-GW node. No GTP signaling toward P-GW node.
   - Trigger Sx Session Modification Request:
     - To update Downlink FAR with "Outer Header Creation" as "S1 eNodeB F-TEID".
     - To update Uplink PDR with "Outer Header Removal" based on IP address information in "S1 eNodeB F-TEID".
8. On receipt of Sx Session Modification Response, the SAEGW-SGW-C sends MBR with "S1-U S-GW F-TEID".

Initial Attach Procedure (Collapsed PDN)

The following call flow illustrates, at a high-level, the initial attach procedure for Collapsed PDN.



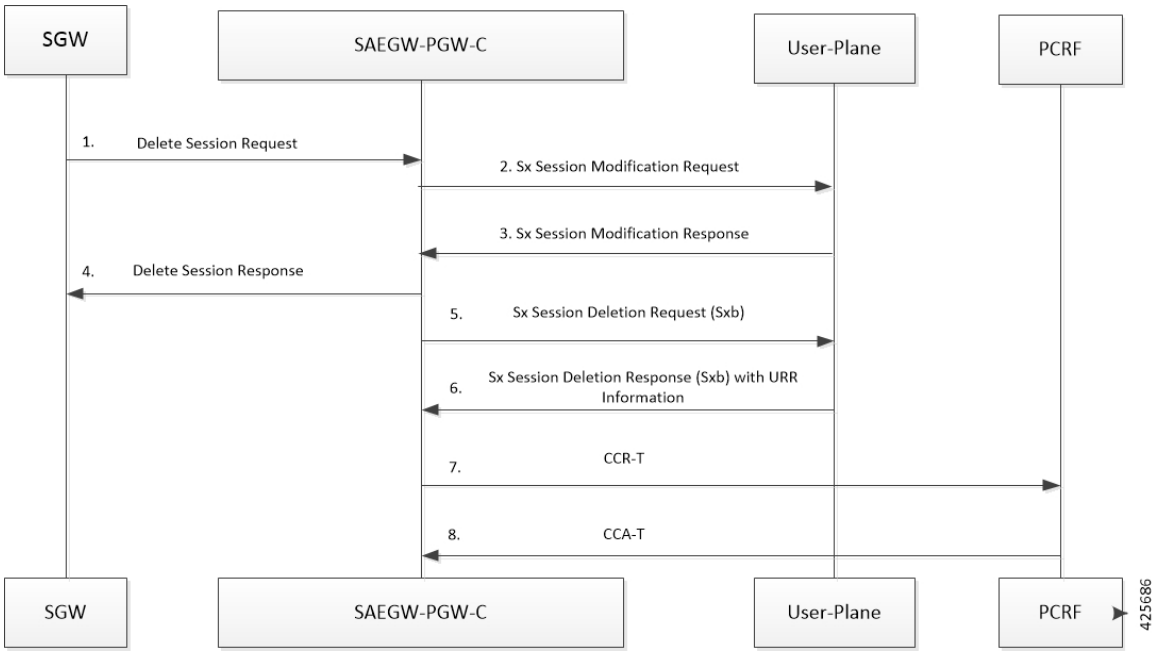
1. For CUPS SAEGW collapsed call, SAEGW-C does the following:
   - After Gx interaction, performs Gx communication (CCR-I and CCA-I).
   - Performs User Plane selection based on **user-plane-profile** configured with IP Pool (APN associated with IP Pool).
   - Establishes GTP-U session (required for RA/RS, in case of IPv6/IPv4v6 PDN).
   - Performs Sxab interaction with selected User Plane.
2. Sx Establishment Request contains the following information:
   - Create PDR/FAR information for S-GW Uplink and Downlink data path (Sxa Type PDR).
   - Create PDR/FAR/URR information for Uplink and Downlink data path (Sxb Type PDR): For dynamic/pre-defined/static rules.

- Create PDR/FAR for RA/RS (Sxb Type PDR): Required for IPv6/IPv4v6 PDN Type.
- Additionally, Control Plane requests User Plane to allocate F-TEID for:
  - S-GW Ingress "S1-U S-GW F-TEID",
  - S-GW Egress "S5/S8-U S-GW F-TEID", and
  - P-GW Ingress PDR "S5/S8-U P-GW F-TEID"

3. User Plane provides following information as part of Sx Session Establishment Response:
   - Created PDR: S-GW Ingress PDR "S1-U S-GW F-TEID",
   - Created PDR: S-GW Egress PDR "S5/S8-U S-GW F-TEID", and
   - Created PDR: P-GW Ingress PDR "S5/S8-U P-GW F-TEID"
4. On receipt of successful Sx Session Establishment Response, the Control Plane triggers Sx Modification Request with the following information:
   - To update P-GW (Sxb) "Uplink PDR" with "Outer Header Removal" based on IP address information in "S5/S8-U S-GW F-TEID"
   - To update P-GW (Sxb) "Downlink FAR" with "Outer Header Creation" as "S5/S8-U S-GW F-TEID"
   - To update S-GW (Sxa) "Uplink FAR" with "Outer Header Creation" as "S5/S8-U P-GW F-TEID"
   - To update S-GW (Sxa) "Downlink PDR" with "Outer Header Removal" based on IP address information in "S5/S8-U P-GW F-TEID"
5. On receipt of Sx Session Modification Response, the SAEGW-C sends Create Session Response toward MME with "S1-U S-GW F-TEID" and "S5/S8-U P-GW F-TEID".
6. On receipt of Modify Bearer Request (MBR), the SAEGW-C does the following:
   - Trigger Sx Session Modification Request:
     - To update Downlink FAR with "Outer Header Creation" as "S1 eNodeB F-TEID".
     - To update Uplink PDR with "Outer Header Removal" based on IP address information in "S1 eNodeB F-TEID".
7. On receipt of Sx Session Modification Response, the SAEGW-SGW-C sends MBR with "S1-U S-GW F-TEID".

Detach Procedure (Pure-P): UE Initiated

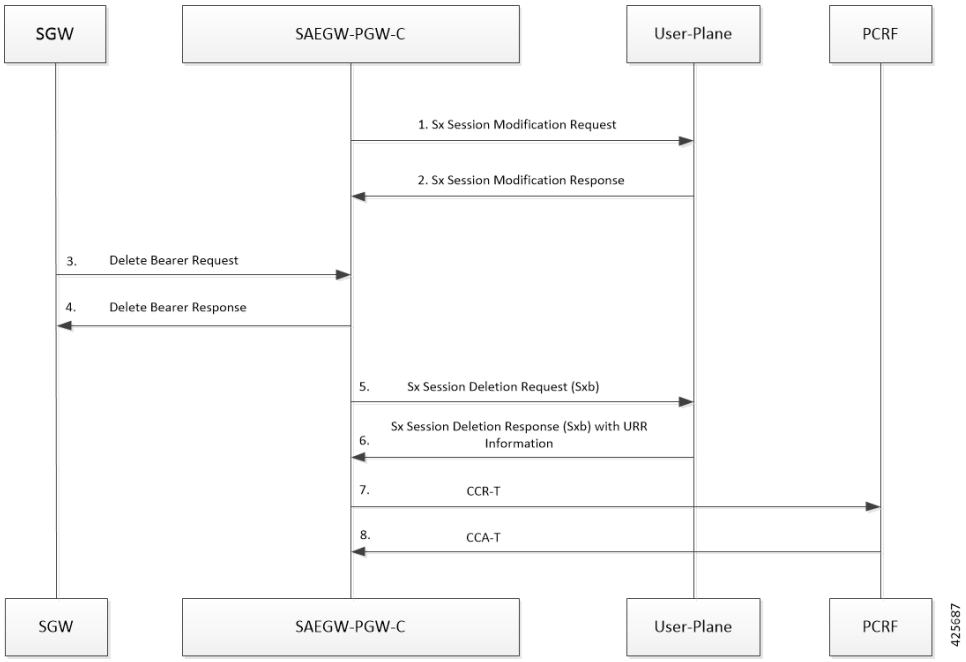
Following call flow illustrates, at a high-level, the detach procedure for UE initiated Pure-P PDN.



1. On receipt of Delete Session Request , the SAE-GW-C performs Sxab interaction to update FAR with the Apply Action as "DROP" for both Uplink and Downlink data path.
2. On receipt of Sx Session Modification Response, SAE-GW-C sends Delete Session Response towards MME.
3. For CUPS SAEGW Pure-P call, the SAEGW-PGW-C does the following:
   - Removes GTP-U session (required for RA/RS in case of IPv6/IPv4v6 PDN).
   - Performs Sxb interaction with the selected User Plane.
4. On receipt of Sx Session Deletion Response, the SAEGW-PGW-C does the following:
   - Performs Gx communication (CCR-T and CCA-T).
   - Generates CDR (Gz) based on URR information received.

Detach Procedure (Pure-P): Network Initiated

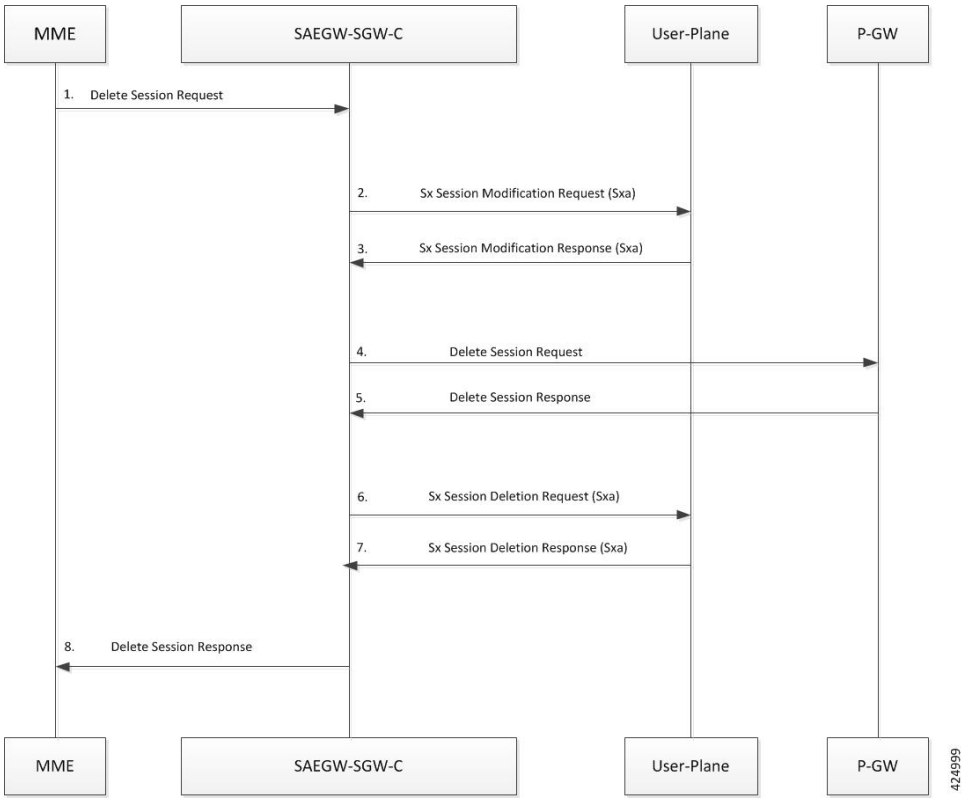
Following call flow illustrates, at a high-level, the detach procedure for network initiated Pure-P PDN.



1. On receipt of the Delete Bearer Request (RAR initiated or by the **clear sub all** CLI, the SAEGW-PGW-C performs Sxb interaction to update FAR with the Apply Action as "DROP" for both Uplink and Downlink data path.
2. On receipt of Sx Session Modification Response, SAEGW-PGW-C sends the Delete Bearer Request toward SGW.
3. For CUPS SAEGW Pure-P call, the SAEGW-PGW-C does the following:
   - Removes GTP-U session (required for RA/RS in case of IPv6/IPv4v6 PDN).
   - Performs Sxb interaction with the selected User Plane.
4. On receipt of Sx Session Deletion Response, the SAEGW-PGW-C does the following:
   - Performs Gx communication (CCR-T and CCA-T).
   - Generates CDR (Gz) based on URR information received.

Detach Procedure (Pure-S): UE Initiated

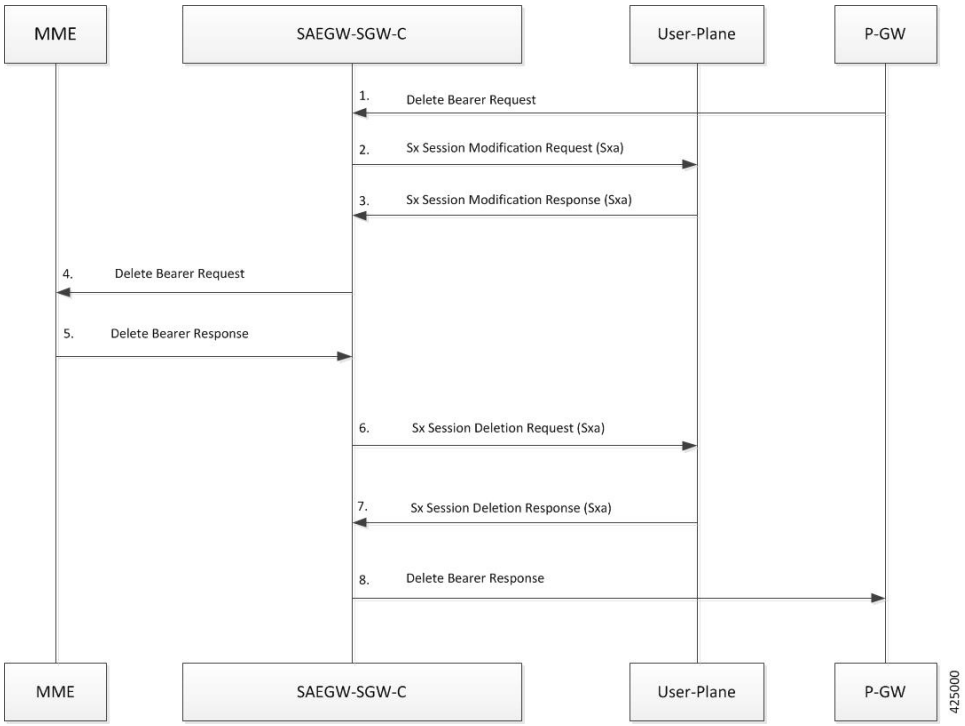
Following call flow illustrates, at a high-level, the detach procedure for UE initiated Pure-S PDN.



1. On receipt of Delete Session Request, the SAEGW-SGW-C performs Sxa interaction to "Update FAR" with Apply Action as "DROP" for both Uplink and Downlink data path.
2. On receipt of Sx Session Modification Response, the SAEGW-SGW-C sends Delete Session Request toward the P-GW.
3. On receipt of Delete Session Response, the SAEGW-SGW-C performs Sxa interaction to delete Sx session.
4. On receipt of Sx Session Deletion Response, the SAEGW-SGW-C sends Delete Session Response toward the MME.

Detach Procedure (Pure-S): Network Initiated

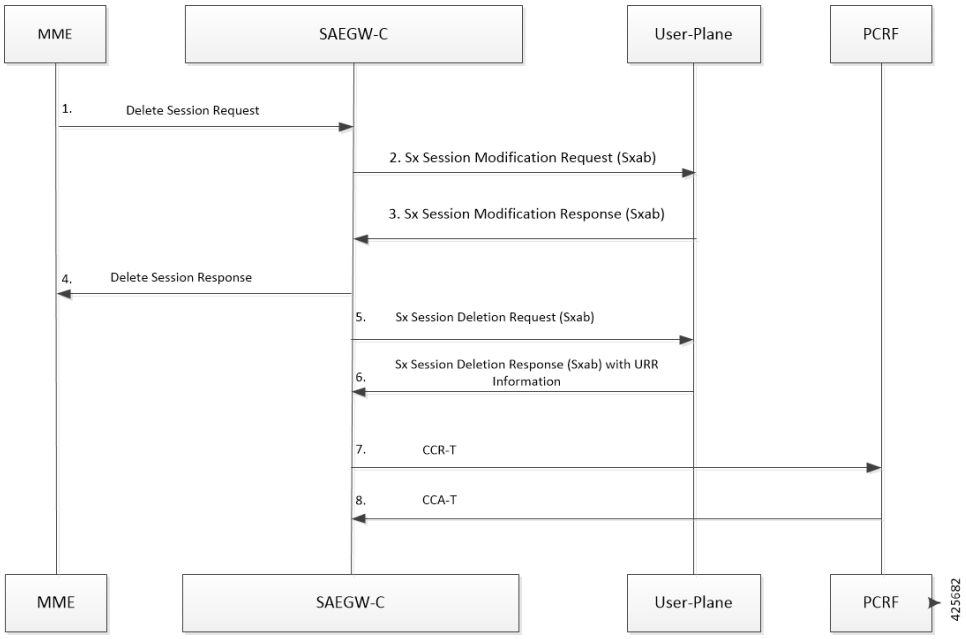
Following call flow illustrates, at a high-level, the detach procedure for network initiated Pure-S PDN.



1. On receipt of Delete Bearer Request, the SAEGW-SGW-C performs Sxa interaction to "Update FAR" with Apply Action as "DROP" for both Uplink and Downlink data path.
2. On receipt of Sx Session Modification Response, the SAEGW-SGW-C sends Delete Bearer Request toward the MME.
3. On receipt of Delete Session Response from MME, the SAEGW-SGW-C performs Sxa interaction to delete Sx session.
4. On receipt of Sx Session Deletion Response, the SAEGW-SGW-C sends Delete Bearer Response toward the P-GW.

Detach Procedure (Collapsed): UE Initiated

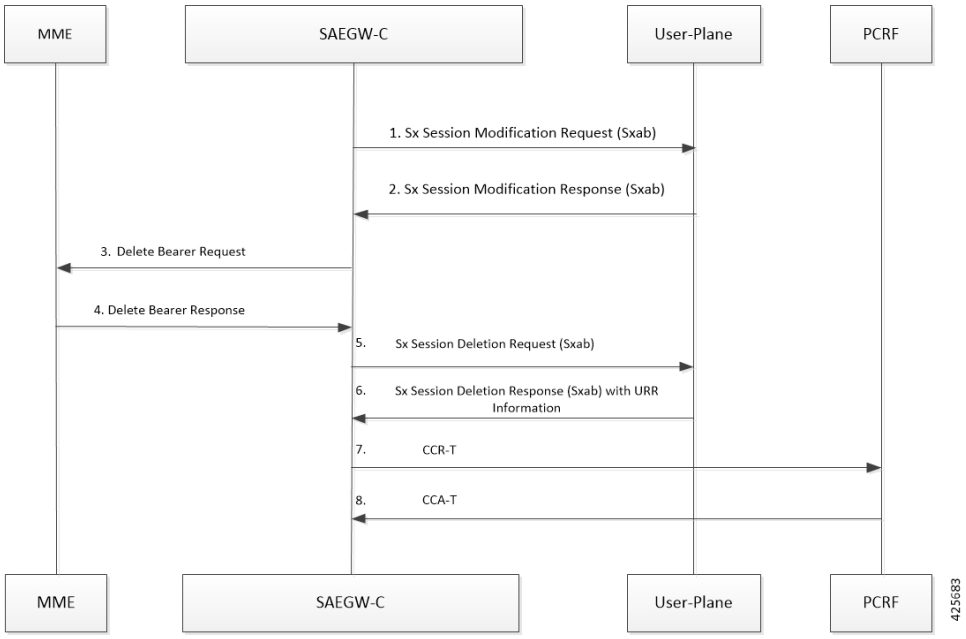
Following call flow illustrates, at a high-level, the detach procedure for UE initiated Collapsed PDN.



1. On receipt of Delete Session Request, the SAEGW-C performs Sxab interaction to update FAR with Apply Action as "DROP" for both Uplink and Downlink data path.
2. On receipt of Sx Session modification Response, SAEGW-C sends Delete Session Response towards MME.
3. For CUPS SAEGW Collapsed call, the SAEGW-C does the following:
   - Removes GTP-U session (required for RA/RS in case of IPv6/IPv4v6 PDN).
   - Performs Sxab interaction with the selected User Plane.
4. On receipt of Sx Session Deletion Response, the SAEGW-C does the following:
   - Performs Gx communication (CCR-T and CCA-T).
   - Generates CDR (Gz) based on URR information received.

Detach Procedure (Collapsed): Network Initiated

Following call flow illustrates, at a high-level, the detach procedure for network initiated Collapsed PDN.

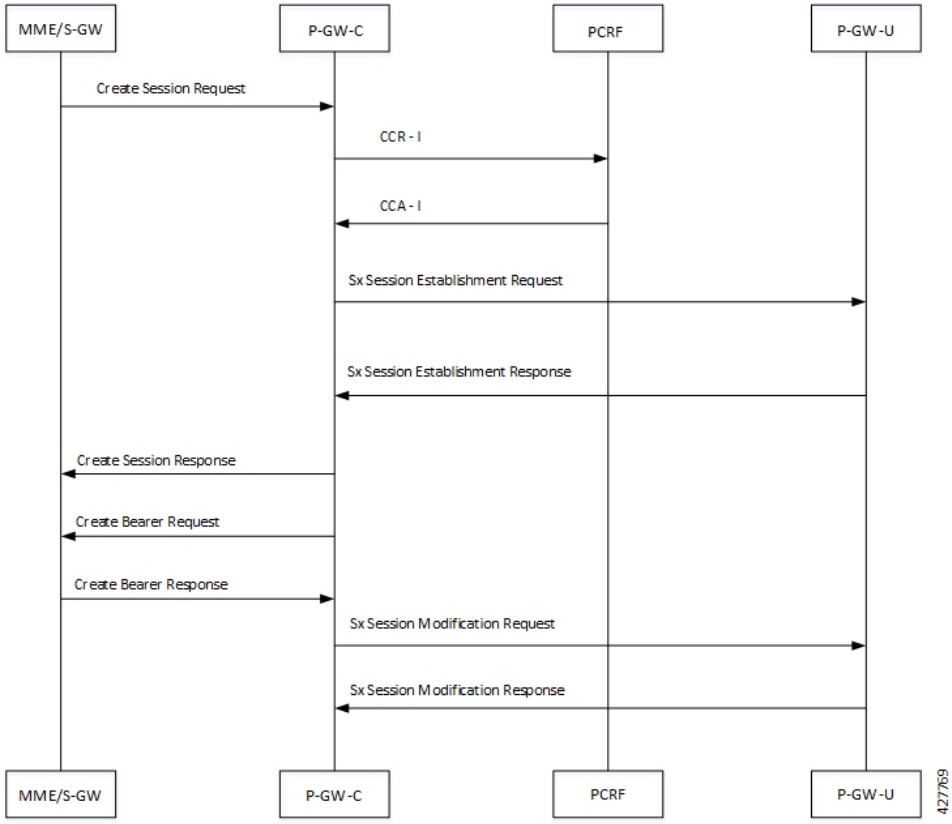


1. On receipt of Delete Bearer Request (RAR initiated or by the **clear sub all** CLI), SAEGW-C performs Sxab interaction to update FAR with Apply Action as "DROP" for both Uplink and Downlink data path.
2. On receipt of Sx Session Modification Response, SAEGW-C sends Delete Bearer Request toward MME.
3. For CUPS SAEGW Collapsed call, the SAEGW-C does the following:
   - Removes GTP-U session (required for RA/RS in case of IPv6/IPv4v6 PDN).
   - Performs Sxab interaction with the selected User Plane.
4. On receipt of Sx Session Deletion Response, the SAEGW-C does the following:
   - Performs Gx communication (CCR-T and CCA-T).
   - Generates CDR (Gz) based on URR information received.

Dedicated Bearer Creation, Modification (Update) and Deletion

Creating, updating and deleting dedicated bearers is only qualified for P-GW and SAEGW.

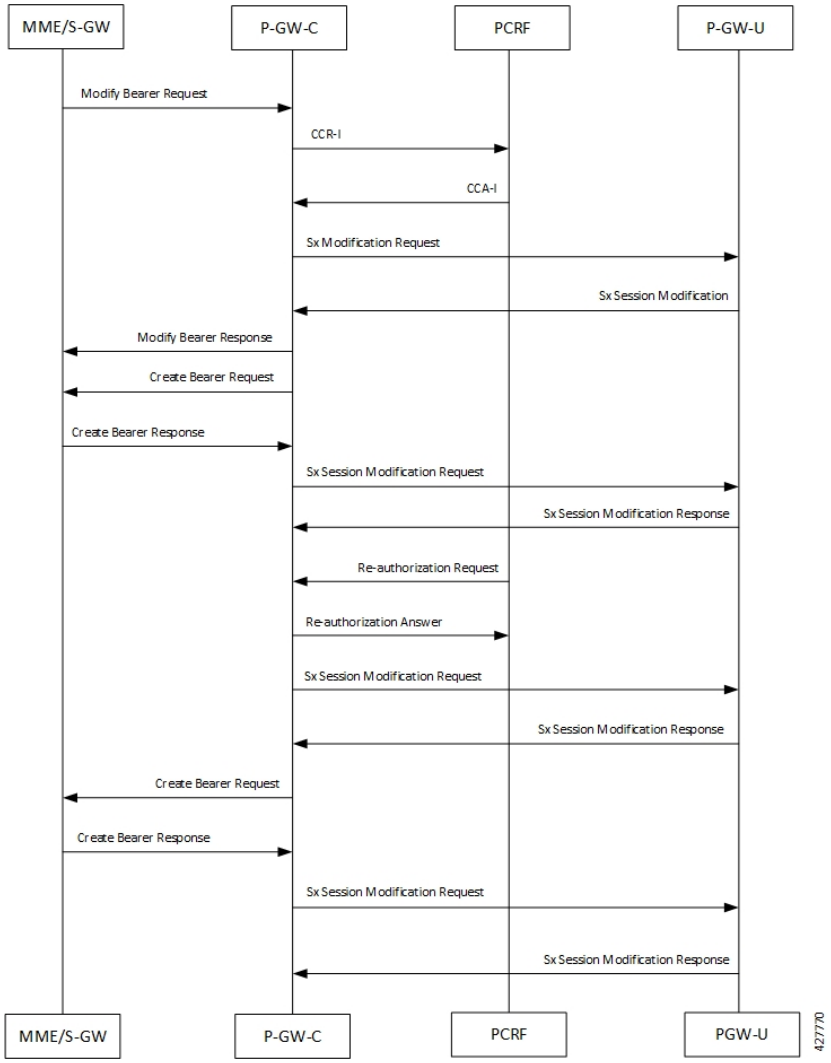
Bearer Creation in CCA-I (Pure-P)



1. UE initiates an attach procedure through the first PDN. S-GW forwards the Create Session Request with IMSI, APN, EBI, and APN AMBR UL/DL along with other mandatory parameters to PGW-C to establish a PDN connection.
2. PGW-C sends a Credit-Control-Request (Initial) to PCRF.
3. PCRF responds with Credit-Control-Answer (Initial) to PGW-C with APN AMBR UL/DL and install dynamic/predefined rule with QCI ARP different from default QoS.
4. On receiving Credit-Control-Answer (Initial) from PCRF, PGW-C initiates a Sx Session Establishment Request to PGW-U with Create PDR for default bearers with choose ID - x, and Create PDR for dedicated bearer with choose ID - y.
5. P-GW-U responds with Sx Session Establishment Response to PGW-C with list of created PDR's and the PGW-U local FTEID's.
6. P-GW-C sends Create Session Response to S-GW for first PDN connection setup.
7. P-GW sends Create Bearer Request to S-GW with the P-GW's Data FTEID filled in the bearer Context.
8. S-GW sends Create Bearer Response with Remote data FTEID. On receiving the same, Sx modify request is initiated towards UP function, to send update FAR for all downlink FAR's, with the remote F-TEID's.
9. P-GW-U responds with an Sx Session Modification Response to P-GW-C.

Bearer Creation due to MBR/MCmd/CCA-U and RAR

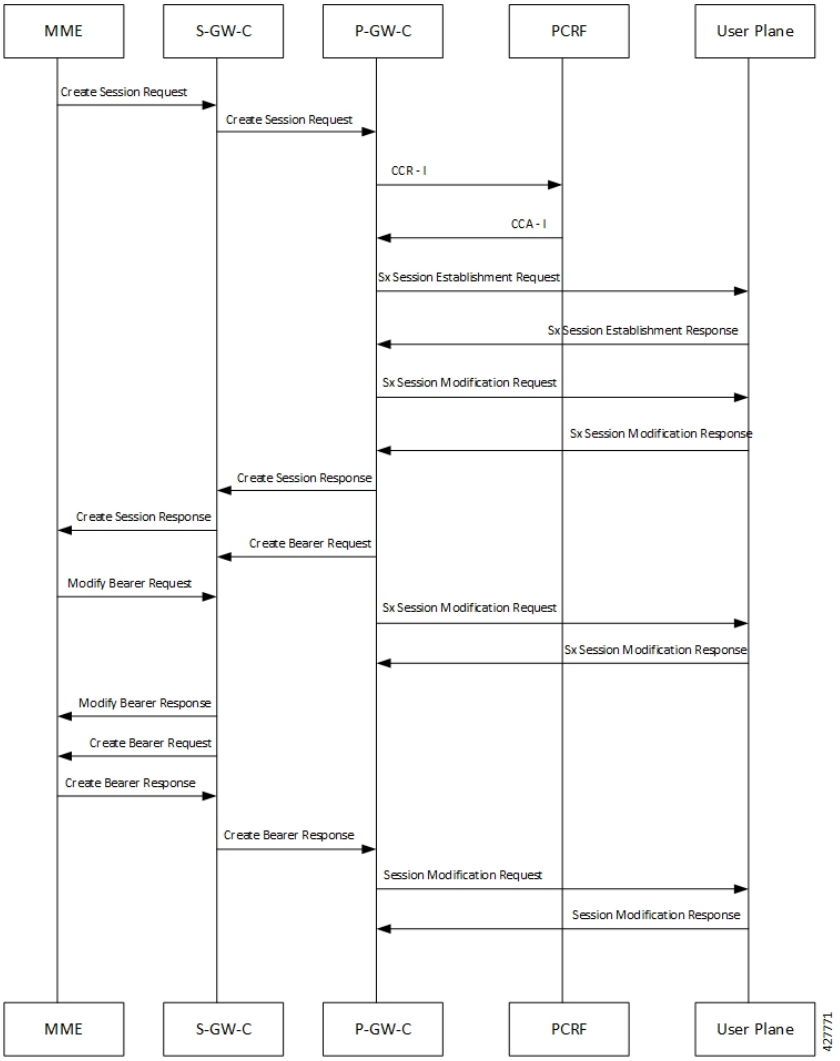
Following call flow illustrates, at a high level, bearer creation due to MBR/MCmd/CCA-U and RAR:



1. On receiving Credit-Control-Answer (Update) or Re-Authorization Request from PCRF, P-GW-C initiates Sx Session Modification Request to P-GW-U with Create PDR for default bearer with choose ID - x, and Create PDR for dedicated bearer with choose ID - y.
2. P-GW-U responds with Sx Session Modification Response to P-GW-C with list of created PDR's and the P-GW-U local FTEID's.
3. P-GW sends Create Bearer Request to S-GW with the P-GW's Data FTEID filled in bearer Context.
4. S-GW sends Create Bearer Response with Remote data FTEID. On receiving the same, Sx modify request is initiated towards UP function, to send update FAR for all downlink FAR's, with the remote F-TEID's.
5. P-GW-U responds with an Sx Modification Response to P-GW-C.

Dedicated Bearer Creation for a Collapsed Call

Following call flow illustrates, at a high level, bearer creation for collapsed call:

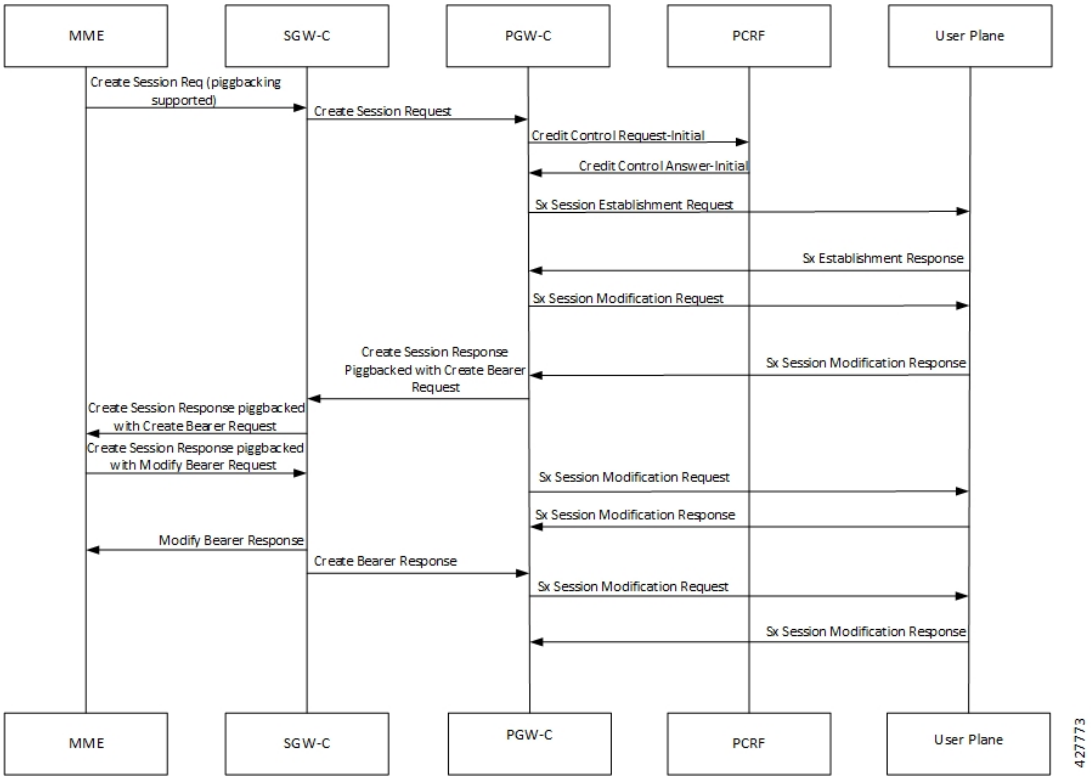


1. UE initiates attach procedure through first PDN.SGW-C forwards the Create Session Request with IMSI, APN, EBI, and APNAMBR UL/DL along with other mandatory parameters to PGW-C to establish a PDN connection.
2. PGW-C sends Credit-Control-Request (Initial) to PCRF.
3. PCRF responds with Credit-Control-Answer (Initial) to PGW-C with APN AMBR UL/DL and install dynamic/predefined rule with QCI ARP different from default QoS.
4. On receiving Credit-Control-Answer (Initial) from PCRF, PGW-C initiates Sx Session Establishment Request to SAEGW-U with Create PDR for default bearer with choose ID x and Create PDR for dedicated bearer with choose ID y.
5. SAEGW-U responds with Sx Session Establishment Response to PGW-C with list of created PDR's and the PGW-U local FTEID's.

6. SAEGW-U responds with Sx Session Establishment Response to PGW-C with list of created PDR's and the PGW-U local FTEID's.
7. PGW-C sends Create Session Response to SGW-C for first PDN connection setup.
8. PGW-C sends Create Bearer Request to SGW-C with the PGW's Data FTEID filled in bearer Context.
9. SGW-C receives Modify bearer request with eNodeB TEID's for which Sx transaction is initiated.
10. SGW-C receives Create Bearer Response with Remote data FTEID. On receiving the same, Sx modify request is initiated towards UP function, to send update FAR for all downlink FAR's, with the remote F-TEID's.
11. SAEGW-U responds with Sx Session Modification Response to PGW-C.

Bearer Creation with Piggybacking Enabled for Collapsed Call

Following call flow illustrates, at a high level, bearer creation with piggybacking enabled for a collapsed call:

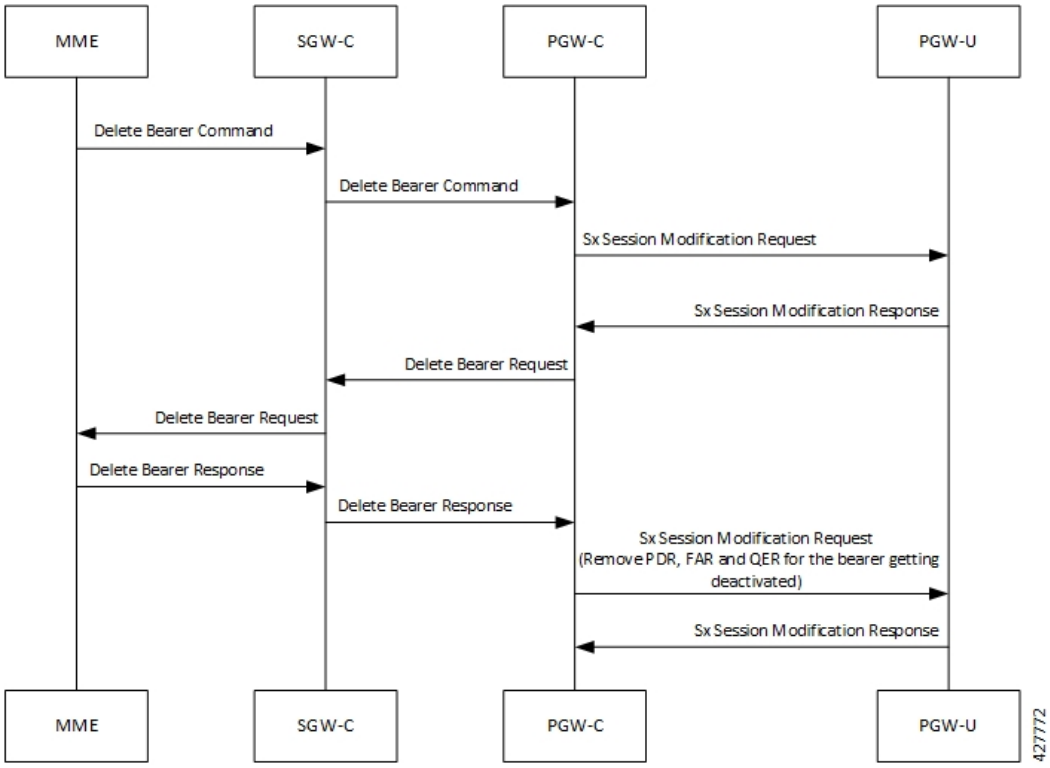


1. UE initiates attach procedure through first PDN.SGW-C forwards the Create Session Request with IMSI, APN, EBI, and APNAMBR UL/DL along with other mandatory parameters to PGW-C to establish a PDN connection.
2. PGW-C sends Credit-Control-Request (Initial) to PCRF.
3. PCRF responds with Credit-Control-Answer (Initial) to PGW-C with APN AMBR UL/DL and install dynamic/predefined rule with QCI ARP different from default QoS.

4. On receiving Credit-Control-Answer (Initial) from PCRF, PGW-C initiates Sx Session Establishment Request to SAEGW-U with Create PDR for default bearer with choose ID x and Create PDR for dedicated bearer with choose ID y.
5. SAEGW-U responds with Sx Session Establishment Response to PGW-C with list of created PDR's and the PGW-U local FTEID's.
6. Sx modification request is triggered to update the PDR and FAR for both default and dedicated bearers.
7. PGW-C sends Create Session Response to SGW-C for first PDN connection setup.
8. PGW-C sends Create Bearer Request to SGW-C with the PGW's Data FTEID filled in bearer Context, which is buffered at SGW-C until PDN is fully connected.
9. SGW-C receives Modify bearer request with eNodeB TEID's for which Sx transaction is initiated.
10. SGW-C received Create Bearer Response with Remote data FTEID. On receiving the same, Sx modify request is initiated towards UP function, to send update FAR for all downlink FAR's, with the remote F-TEID's.
11. SAEGW-U responds with Sx Session Establishment Response to PGW-C.

Delete Bearer Command Call Flow for Pure P Call

Following call flow illustrates, at a high level, command call flow for a Pure P call:

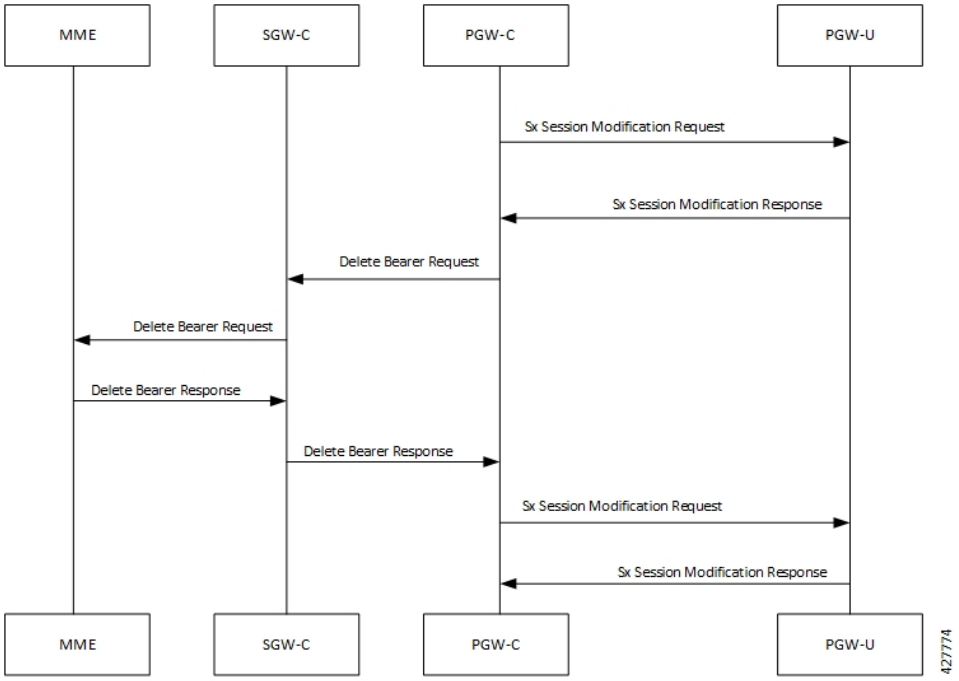


1. UE initiates detach procedure through first PDN.SGW-C forwards the Delete Bearer Command to PGW-C to delete set of dedicated bearers.

2. PGW-C sends an Sx modification Request with All Update FAR for dedicated bearer's with apply action as DROP.
3. PGW-U responds with Sx Session modification Response to PGW-C.
4. PGW-C Sends Delete Bearer Request to access side and on receiving Delete Bearer Response, Sx modification request is triggered to remove the PDR and FAR for dedicated bearers.

Clear Subscriber EBI for Pure P Call

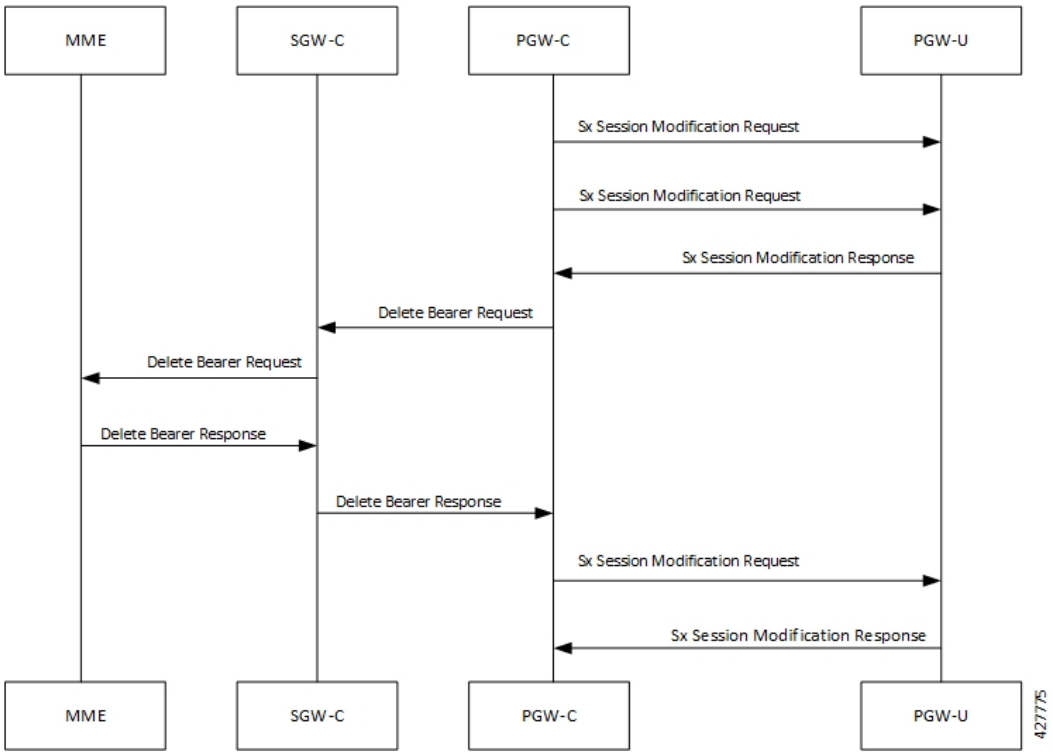
Following call flow illustrates, at a high level, Clear Subscriber EBI for a Pure P call:



1. PGW-C initiates detach procedure through first PDN.
2. PGW-C sends a Sx modification Request with All Update FAR for dedicated bearer's with apply action as DROP.
3. PGW-U responds with Sx Session modification Response to PGW-C.
4. PGW-C Sends Delete Bearer Request to access side and on receiving Delete Bearer Response, Sx modification request is triggered to remove the PDR and FAR for dedicated bearers.

PCRF Initiated Delete for Pure P Call

Following call flow illustrates, at a high level, PCRF initiated delete for a Pure P call:



1. PCRF performs Rule-removal, which leads to dedicated bearer deletion.
2. PGW-C initiates Sx modification Request with All Update FAR for dedicated bearer's with apply action as DROP.
3. PGW-U responds with Sx Session modification Response to PGW-C.
4. PGW-C Sends Delete Bearer Request to access side and on receiving Delete Bearer Response, Sx modification request is triggered to remove the PDR and FAR for dedicated bearers.

Limitations

Dedicated Bearer Creation and Deletion and Modification (updating) has the following limitations:

- Dedicated bearer creation for Pure S call is not supported.
- During collision scenarios session clean-up is triggered when events/operations are requested for a bearer, for which deletion is already in progress. For example, a CCA-U/RAR (EBI = 6) is received during an on going DELETE_BEARER_COMMAND (EBI = 6).

Support for Addition, Deletion and Updation of Dedicated Bearers for S-GW

Feature Description

Addition, Deletion and Updation of Dedicated Bearers for Pure-S calls is supported in the CUPS architecture.

The following functionality is added in support of this feature:

- SAEGW-CP supports Create Bearer Request for dedicated bearer for Pure-S Call.

- SAEGW -CP supports multiple bearer contexts in single Create Bearer Request.
- SAEGW-CP supports multiple Create Bearer request in parallel for different PDN; these PDN can be Pure-S PDN or Collapsed and Pure-S combinations.
- SAEGW-UP creates uplink and downlink bearer stream at VPP for Pure-S call per bearer. Number of streams per direction depends on the GTP-U Service IP address.
- SAEGW-CP supports Release Access Bearer Request (RAB) with dedicated bearer, all FAR corresponding to all bearer is modified.
- SAEGW-CP supports Modify Bearer Request (Idle mode, Connected mode) with dedicated bearer.
- SAEGW-CP supports Create Bearer Response Failure handling from MME.
- SAEGW-CP and SAEGW-UP supports DSCP marking for default and dedicated bearer with VPP.
- SAEGW-CP and SAEGW-UP supports Delete Bearer Request for dedicated bearer. SAEGW-UP removes bearer stream and TEP entries belonging to those bearers.
- SAEGW-CP supports Pure-S Dedicated Bearer Creation when call is in IDLE state.
- SAEGW-CP supports Pure-S Dedicated Bearer S-GW Relocation (both X2 and S1-based).
- SAEGW-CP supports Pure-S Dedicated Bearer Update success scenarios.
- SAEGW-CP supports Piggybacking of Create Bearer Request for dedicated bearer for Pure-S call along with Create Session Response.
- SAEGW-CP supports Piggybacking of Create Bearer Response for dedicated bearer for Pure-S call with Modify Bearer Request.
- SAEGW-CP supports Pure-S Dedicated Bearer Creation if P-GW receives bearer creation as part of CCA-I, where P-GW does not send Piggyback request, which results in Create Session Response followed by Create Bearer Request.
- SAEGW-CP supports Session Recovery and ICSR with Pure-S dedicated bearer.
- SAEGW-CP supports Create Bearer Request and Delete Bearer Request (default bearer) collision.
- SAEGW-CP supports Create Bearer Request and Delete Session Request collision.
- SAEGW-CP supports Create Bearer Response and Delete Bearer Request (default bearer) collision.
- SAEGW-CP supports Create Bearer Response and Delete Session Request collision.
- SAEGW-CP supports End Marker with Pure-S default and dedicated bearer.
- SAEGW-UP supports Session Recovery with Pure-S default and dedicated bearer.
- SAEGW-UP supports movement of IP transport from IPv4 to IPv6, or IPv6 to IPv4, during IDLE->Active and Handover procedure on S1U interface. Transport selected on S1U at the time of Attach is supported. For example, eNode handover from IPv4 eNodeB to IPv6 eNodeB will work.
- SAEGW-CP supports CBRsp with Cause Partially Accepted and Context Not Found.
- SAEGW-CP supports Downlink Data Notification for Pure-S Call, so when UE moves to IDLE state for Pure-S call, FAR action is set as BUFFER.

- SAEGW-CP supports Update Bearer Response with cause PARTIALLY_ACCEPTED and context not Found.
- SAEGW-CP supports the Error and Failure handling from other peer nodes including User Plane node.

LTE Handoff with S-GW Relocation Call Flows

In SAEGW deployment, S-GW handles the 'S-GW Relocation Handoff Create Session' request when the subscriber is in the active mode or in the idle mode. In SAEGW deployment, P-GW handles the 'S-GW Relocation Handoff Modify Bearer' request.

In case of Idle Mode TAU, when OI is set to 1, the eNodeB FTEID is not sent in 'Create Session Request' sent from the MME.

In case of Tracking Area Update procedure with the S-GW change call flow is same is X2 based handover with the S-GW change.

In case of Active Subscriber with X2 based handoff, when OI is set to 1, eNodeB FTEID is present in 'Create Session Request' sent from the MME.

In case of S1 based handover, when OI is set to 0, the 'Create Session Request' from MME does not contain the eNodeB FTEID. 'Create Session Request' is followed by 'Modify Bearere Request' from MME, which contains the eNodeB FTEID.

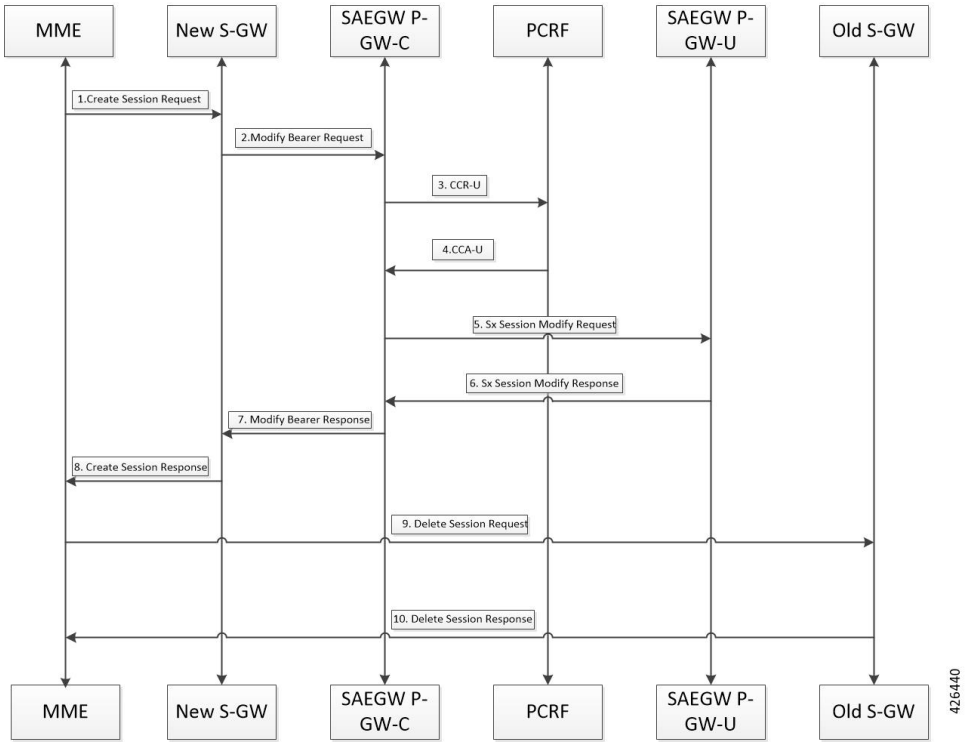
Following sections illustrate the S-GW relocation call flows for X2 and S1 based handover where eNodeB FTEID is present in the 'Create Session Request' of an Active Subscriber.

S-GW Relocation Call Flows for X2 Based Handover

This section covers S-GW relocation call flows for X2 based handover, when OI is set to 1.

S-GW Relocation Procedure (Pure-P)

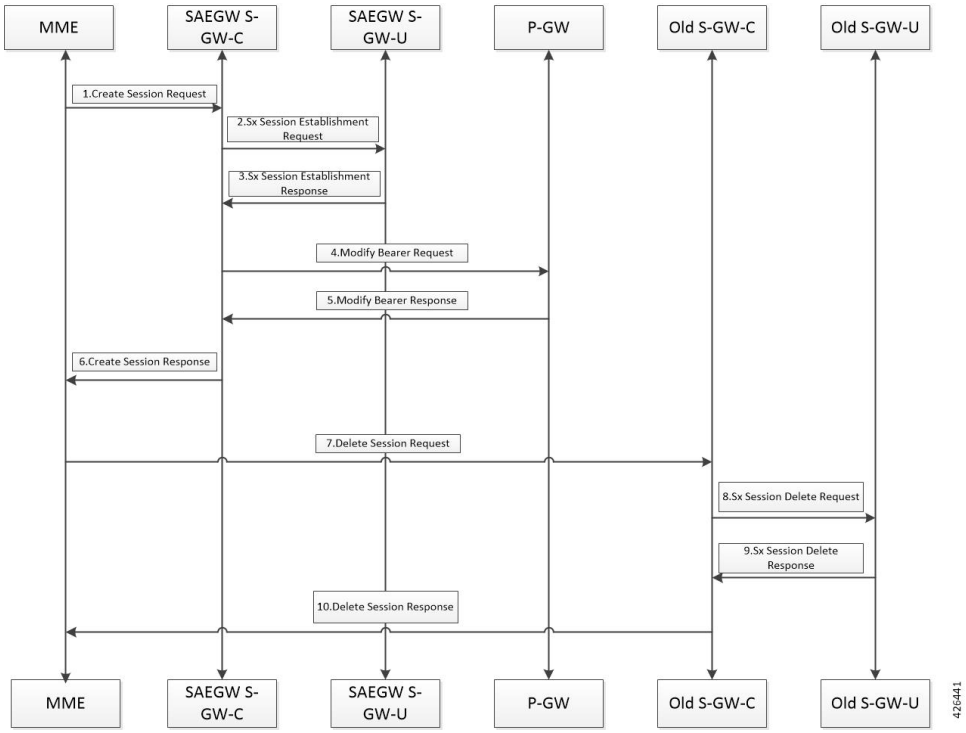
Following call flow illustrates, the initial attach procedure for a S-GW Relocation Pure-P PDN at a high-level.



1. On S-GW handover, when the 'Create Session Request' is sent to new S-GW from MME.
2. 'Modify Bearer Request' is sent to SAEGW-P-GW-C from the new S-GW with S-GW S5/S8-U Data FTEID.
3. SAEGW-PGW-C performs Gx communication (CCR-U).
4. SAEGW-PGW-C performs Gx communication (CCA-U).
5. After Gx interaction, SAEGW-P-GW-C triggers 'Sx Modification Request' towards SAEGW-PGW-U. 'Sx Modify Request' contains the following:
   - 'Update PDR (Uplink PDR)' with 'Outer Header Removal' set based on IP address information in S5/S8-U S-GW DATA FTEID.
   - 'Update FAR (Downlink FAR)' with 'Outer Header Creation' set with S5/S8-U S-GW DATA FTEID.
6. SAEGW-P-GW-U sends 'Sx Modification Response'.
7. On receipt of 'Sx Modification Response', SAEGW-P-GW-C sends 'Modify Bearer Response' to the new S-GW.
8. The new S-GW then sends 'Create Session Response' back to the MME.
9. MME sends 'Delete Session Request' to the old S-GW.
10. The old S-GW responds with 'Delete Session Response' to the MME.

S-GW Relocation Procedure (Pure-S)

The following call flow, at a high-level, illustrates the procedure for an S-GW Relocation Pure-S PDN.

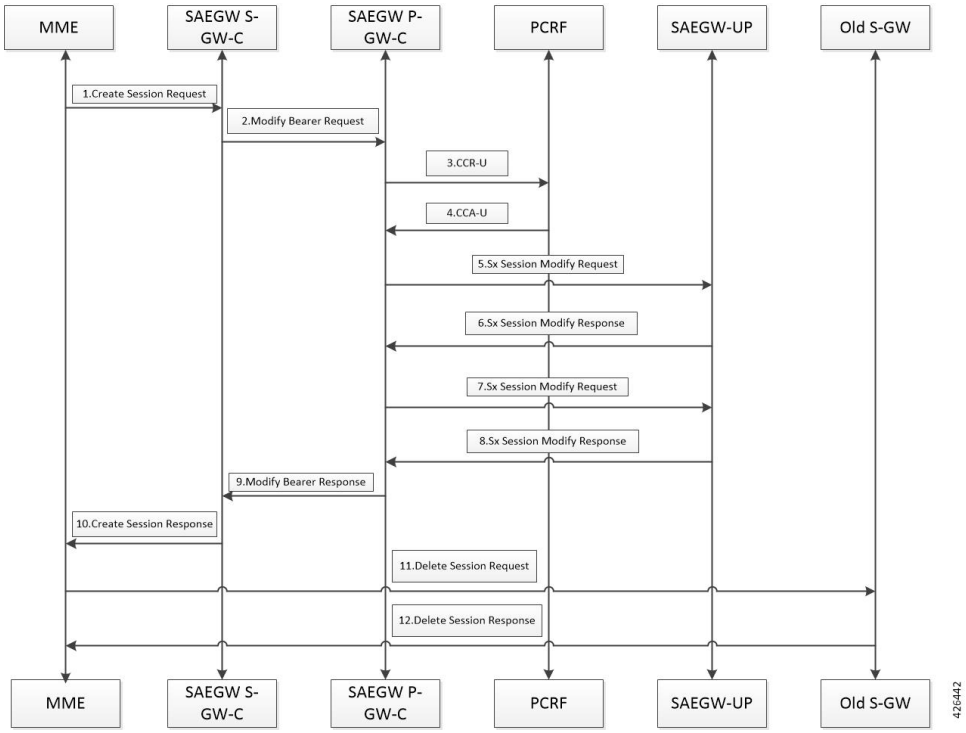


1. On S-GW handover, the MME sends 'Create Session Request' with enodeB FTEID, P-GW S5/S8-U DATA FTEID and P-GW S5/S8-C Ctrl FTEID to the new S-GW-C.
2. The new S-GW-C sends 'Sx Establishment Request' to the new S-GW-U. 'Sx Establishment Request' contains the following:
   - 'Create S-GW Ingress PDR' with 'Outer Header Removal' set based on eNodeB FTEID.
   - 'Create S-GW Egress PDR' with 'Outer Header Removal' set based on P-GW S5/S8-U Data FTEID.
   - 'Create S-GW Ingress FAR' with 'Outer Header Creation' set to P-GW S5/S8-U Data FTEID.
   - 'Create S-GW Egress FAR' with 'Outer Header Creation' set to eNodeB FTEID.
   - 'Create S-GW Egress FAR' with 'Outer Header Creation' set to eNodeB FTEID for X2/In case of TAU S-GW Egress FAR will not contain Outer Header Creation and Apply Action will be set to drop.
3. 'Sx Establishment Response' is received at the S-GW-C with the S-GW S1-U and the S5/S8-U DATA FTEIDs.
4. Once 'Sx Establishment Response' is received from the S-GW-U, the 'Modify Bearer Request' with S-GW S5/S8-U DATA FTEID is sent to the P-GW.
5. When the P-GW responds with the 'Modify Bearer Response'.
6. The new S-GW-C then sends a 'Create Session Response' with S-GW ctrl S11C FTEID and S-GW S1-U DATA FTEID to the MME.

7. On receipt of the 'Create Session Response', the MME sends 'Delete Session Request' to the old S-GW-C.
8. Old S-GW-C sends 'Sx Delete Session Request' to the old S-GW-U.
9. Old S-GW-U responds with the 'Sx Delete Session Response' to the old S-GW-C.
10. Old S-GW-C responds with the 'Delete Session Response' to the MME.

S-GW Relocation Pure-P Call to Collapsed Call

Following call flow illustrates, at a high-level, the procedure for an S-GW Relocation Pure-P call to Collapsed Call.



1. On S-GW handover, MME sends 'Create Session Request' to the new SAEGW-SGW-C which is part of the SAEGW anchoring P-GW call of that subscriber.
2. SAEGW-S-GW-C does the following:
   - S-GW-C does not perform any Sx Communication after detecting that it is a collapsed call.
   - S-GW-C triggers 'Modify bearer Request' to the P-GW-C with zero S-GW S5/S8-U Data FTEID.
3. SAEGW-P-GW-C performs Gx communication with PCRF CCR-U.
4. SAEGW-P-GW-C performs Gx communication with PCRF CCA-U.
5. After the Gx interaction is complete, the SAEGW-P-GW-C triggers 'Sx Modification Request' to SAEGW-P-GW-U. Sx Modification Request contains the following:
   - 'Create PDR' and 'Create FAR' (with apply action as DROP) for an S-GW Ingress.
   - 'Create PDR' and 'Create FAR' (with apply action as DROP) for an S-GW Egress.

Control Plane requests User Plane to allocate following S-GW DATA FTEIDS for both uplink and downlink path:

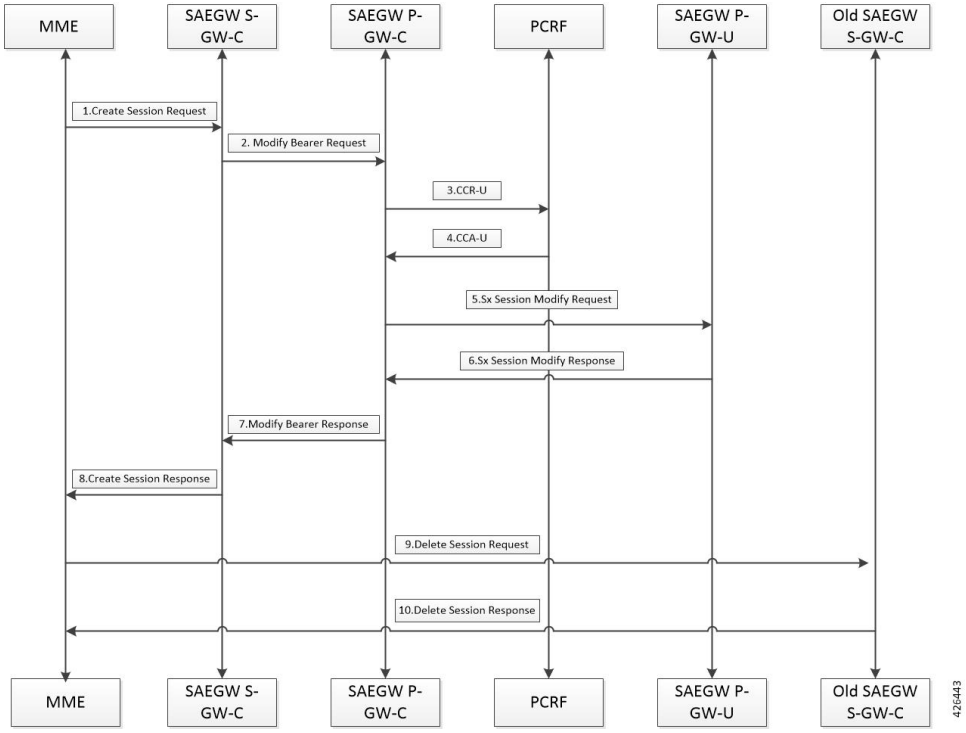
- S-GW S1-U DATA FTEID
- S-GW S5/S8-U DATA FTEID

Interface type changes from Sxb to Sxab, that is, Pure P call to Collapsed call.

6. SAEGW-P-GW-U responds with 'Sx Modification Response' to SAEGW-P-GW-C over Sxab interface.
7. SAEGW-P-GW-C triggers second 'Sx Modification Request' to SAEGW-P-GW-U. The 'Sx Modification Request' contains the following:
   - Update S-GW Ingress PDR with 'Outer Header Removal' set based on eNodeB S1-U DATA FTEID.
   - Update S-GW Egress PDR with 'Outer Header Removal' set based on P-GW S5/S8-U DATA FTEID.
   - Update S-GW Ingress FAR with 'Outer Header Creation' set to P-GW S5/S8-U DATA FTEID and apply action as FORWARD.
   - Update S-GW Egress FAR with 'Outer Header Creation' set to eNodeB S1-U DATA FTEID and apply action as FORWARD. In case of TAU, S-GW Egress FAR will not contain 'Outer Header Creation' and apply action is set to DROP.
   - Update P-GW Egress FAR with 'Outer Header Creation' set to S-GW S5/S8-U DATA FTEID and apply action as FORWARD.
8. SAEGW-P-GW-U sends 'Sx Modification Response' to SAEGW-P-GW-C.
9. On receipt of 'Sx Modification Response', SAEGW-PGW-C sends 'Modify Bearer Response' to SAEGW-S-GW-C.
10. SAEGW-S-GW-C sends 'Create Session Response' with S-GW ctrl S11c FTEID and S-GW S1-U DATA FTEID.
11. MME sends 'Delete Session Request' to the old S-GW.
12. Old S-GW responds with 'Delete Session Response' to the MME.

S-GW Relocation Collapsed Call to Pure-P Call

Following call flow illustrates, the procedure for an S-GW Relocation Collapsed call to a Pure-P Call at a high-level.



1. On S-GW handover, MME sends 'Create Session Request' to the new S-GW.
2. The new S-GW sends 'Modify Bearer Request' to the SAEGW-P-GW-C with S-GW S5/S8-U DATA FTEID.
3. SAEGW-P-GW-C performs the Gx communication CCR-U.
4. SAEGW-P-GW-C performs the Gx communication CCA-U.
5. After the Gx interaction, SAEGW-P-GW-C sends 'Sx Modification Request' to the SAEGW-P-GW-U.
   - Interface type changes from Sxab to Sxb, that is, Collapsed call to Pure P call.
   - Remove the 'S-GW Ingress PDR' and the Egress PDR (Sxa type PDRs).
   - Remove the 'S-GW Ingress FAR' and the Egress FAR set for the uplink and the downlink data path.
   - Update the 'P-GW Ingress PDR' with 'Outer Header Removal' set based on S-GW S5/S8-U DATA FTEID.
   - Update the 'P-GW Egress FAR' with 'Outer Header Creation' set to S-GW S5/S8-U DATA FTEID.

Note SAEGW/PGW-C retains the Sxa tunnel of source SGW-U until Delete Session Request (DSR) is sent from MME. This tunnel retention enables uplink data to flow over SGW-U till the path switches. Use the **sxa-tunnel-del-at-dsr-on-sgw-change** command in the SAEGW-Service configuration mode to enable or disable Sxa tunnel deletion at DSR. See the *Configuring the Sxa Tunnel Deletion* section for more information.

6. SAEGW-P-GW-U responds with the 'Sx Session Modification Response'.
7. SAEGW-P-GW-C responds with the 'Modify Bearer Response' to the new S-GW.
8. New S-GW responds with the 'Create Session Response' to the MME.
9. On receipt of the 'Create Session Response', MME sends the 'Delete Session Request' to SAEGW-S-GW-C (old S-GW). SAEGW-S-GW-C(old S-GW) does not perform any Sx communication.
10. SAEGW-S-GW-C (old S-GW) responds with the 'Delete Session Response' to the MME.

Configuring the Sxa Tunnel Deletion

To enable or disable Sxa tunnel deletion, use the following command.

```
configure
  context context_name
    saegw-service service_name
      [ no ] sxa-tunnel-del-at-dsr-on-sgw-change
      end
```

NOTES:

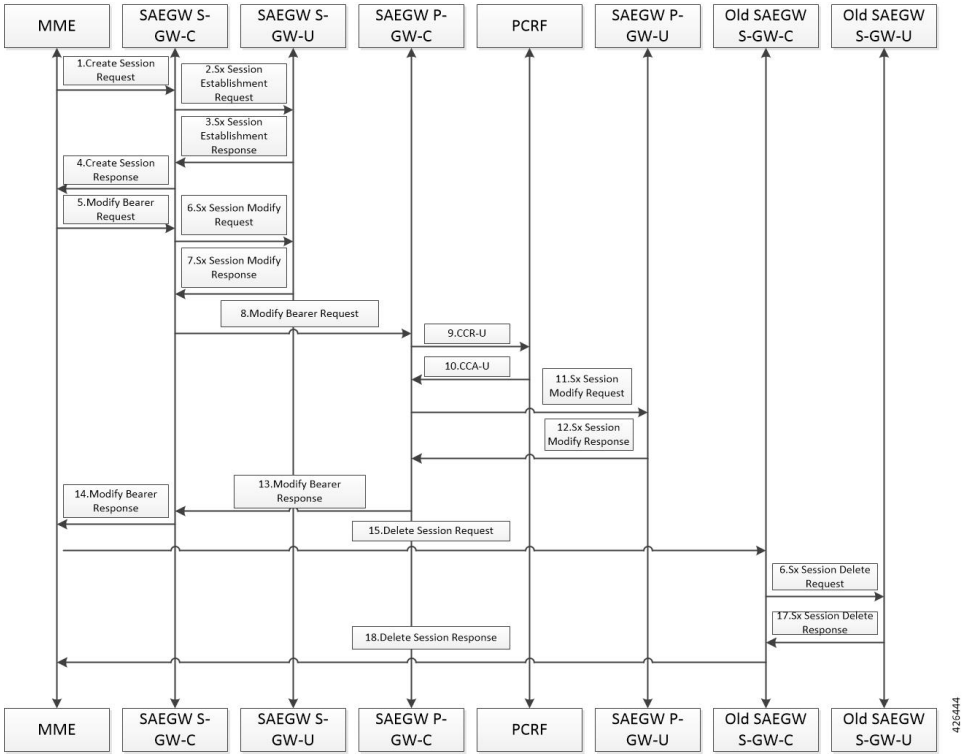
- **sxa-tunnel-del-at-dsr-on-sgw-change** : Enable the Sxa tunnel deletion at DSR during X2/S1 based handover with SGW relocation.
- **no sxa-tunnel-del-at-dsr-on-sgw-change** : Disable the Sxa tunnel deletion at DSR during X2/S1 based handover.
- The configuration is disabled by default.
- The configuration will be applied to all current and new sessions.

S-GW Relocation Call Flows for S1 Based Handover

This section covers S-GW relocation call flows for S1 based handover, when OI is set to 0.

Pure-P and Pure-S Call Flows

Following call flow illustrates, at a high-level, the procedure for an S-GW Relocation Pure-P and Pure-S PDN with OI set to 0.

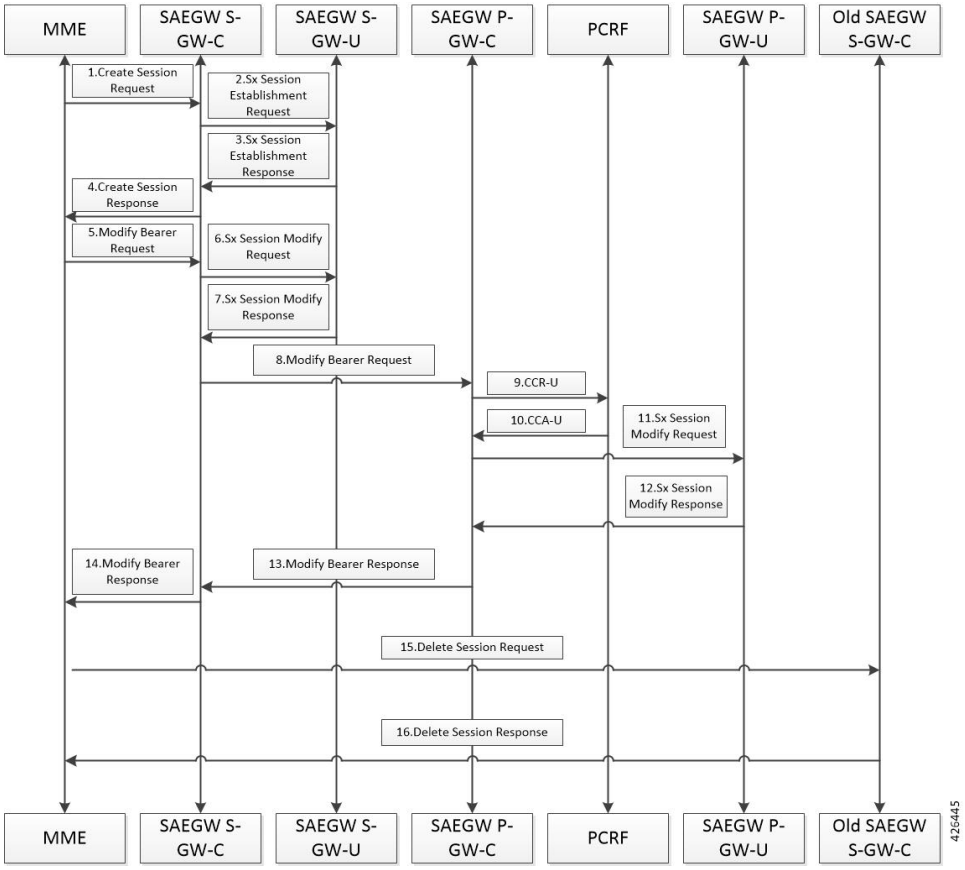


1. On S1 based handover with S-GW change, MME sends the 'Create Session Request' with P-GW S5/S8-U DATA FTEID and P-GW S5/S8-C Ctrl FTEID to the new S-GW-C.
2. The new S-GW-C sends the 'Sx Establishment Request' to the new S-GW-U. 'Sx Establishment Request' contains the following:
   - 'Create S-GW Ingress PDR'.
   - 'Create S-GW Egress PDR' with 'Outer Header Removal' set based on P-GW S5/S8-U Data FTEID.
   - 'Create S-GW Ingress FAR' with 'Outer Header Creation' set to P-GW S5/S8-U Data FTEID.
   - 'Create S-GW Egress FAR' with apply action as DROP.
3. 'Sx Establishment Response' is received at S-GW-C with S-GW S1-U and S5/S8-U DATA FTEIDs allocated at the User Plane.
4. Once 'Sx Establishment Response' is received from S-GW-U, S-GW-C sends 'Create Session Response' to MME.
5. On receiving 'Create Session Response' from S-GW-C, MME sends 'Modify Bearer Request' with eNodeB FTEID to S-GW-C.
6. S-GW-C sends 'Sx Modify Request' to S-GW-U.
   - Updates 'S-GW Ingress PDR' with 'Outer Header Removal' set based on eNodeB FTEID.
   - Updates 'S-GW Egress FAR' with 'Outer Header Creation' set based on eNodeB FTEID.
7. S-GW-U sends 'Sx Modify Response' to S-GW-C.

8. S-GW-C sends 'Modify Bearer Request' with S-GW S5/S8-U DATA FTEID to P-GW-C.
9. On receiving 'Modify Bearer Request' from S-GW-C, P-GW-C performs Gx communication with the PCRF CCR-U.
10. On receiving 'Modify Bearer Request' from S-GW-C, P-GW-C performs Gx communication with the PCRF CCA-U.
11. After the Gx interaction, P-GW-C sends the 'Sx Modification Request' to the P-GW-U. 'Sx Modification Request' contains the following:
    - Updates P-GW Ingress PDR with 'Outer Header Removal' based on the S-GW S5/S8U DATA FTEID.
    - Updates P-GW Egress FAR with 'Outer Header Creation' based on the S-GW S5/S8U DATA FTEID.
12. P-GW-U sends 'Sx Modification Response' back to the P-GW-C.
13. P-GW-C sends the 'Modify Bearer Response' to the S-GW-C.
14. When P-GW responds with the 'Modify Bearer Response', SGW-C then sends the 'Modify Bearer Response' with the S-GW ctrl S11C FTEID and the S-GW S1-U DATA FTEID to the MME.
15. On receipt of the 'Modify Bearer Response', MME sends the 'Delete Session Request' to the old S-GW-C.
16. The old S-GW-C sends the 'Sx Delete Session Request' to the old S-GW-U.
17. The old S-GW-U responds with the 'Sx Delete Session Response' to the old S-GW-C.
18. The old S-GW-C responds with the 'Delete Session Response' to the MME.

S-GW Relocation Collapsed Call to Pure-P Call

Following call flow illustrates, at a high-level, the procedure for an S-GW Relocation Collapsed call to a Pure-P Call.



1. On S1 based handover with S-GW change, MME sends 'Create Session Request' with P-GW S5/S8-U DATA FTEID and P-GW S5/S8-C Ctrl FTEID to the new S-GW-C.
2. The new S-GW-C sends 'Sx Establishment Request' to the new S-GW-U. Sx Establishment Request contains the following:
   - 'Create S-GW Ingress PDR'.
   - 'Create S-GW Egress PDR' with 'Outer Header Removal' set based on P-GW S5/S8-U Data FTEID.
   - 'Create S-GW Ingress FAR' with 'Outer Header Creation' set to P-GW S5/S8-U Data FTEID.
   - 'Create S-GW Egress FAR' with apply action action as DROP.
3. 'Sx Establishment Response' is received at S-GW-C with S-GW S1-U and S5/S8-U DATA FTEIDs allocated at UP.
4. Once 'Sx Establishment Response' is received from S-GW-U, S-GW-C sends 'Create Session Response' to the MME.
5. On receiving 'Create Session Response' from S-GW-C, MME sends 'Modify Bearer Request' with eNodeB FTEID to S-GW-C.
6. S-GW-C sends 'Sx Modification Request' to the S-GW-U. 'Sx Modification Request' contains the following:
   - 'Update S-GW Ingress PDR' with 'Outer Header Removal' based on eNodeB FTEID.

- 'Update S-GW Egress FAR' with 'Outer Header Creation' based on eNodeB FTEID.

7. S-GW-U sends 'Sx Modification Response' to S-GW-C.
8. S-GW-C sends 'Modify Bearer Request' with S-GW S5/S8-U DATA FTEID to P-GW-C.
9. On receiving 'Modify Bearer Request' from S-GW-C, P-GW-C performs Gx communication with the PCRF CCR-U.
10. On receiving 'Modify Bearer Request' from S-GW-C, P-GW-C performs Gx communication with the PCRF CCA-U.
11. After Gx interaction, P-GW-C sends 'Sx Modification Request' to the P-GW-U. 'Sx Modification Request' contains the following:
    - Interface type changes from Sxab to Sxb, that is, Collapsed call to Pure P call.
    - 'Remove S-GW Ingress' and 'Egress PDR'.
    - 'Remove S-GW Ingress' and 'Egress FAR'.
    - 'Update P-GW Ingress PDR' with 'Outer Header Removal' based on S-GW S5/S8U DATA FTEID.
    - 'Update P-GW Egress FAR' with 'Outer Header Creation' based on S-GW S5/S8U DATA FTEID.

Note SAEGW/PGW-C retains the Sxa tunnel of source SGW-U until Delete Session Request (DSR) is sent from MME. This tunnel retention enables uplink data to flow over SGW-U till the path switches. Use the **sxa-tunnel-del-at-dsr-on-sgw-change** command in the SAEGW-Service configuration mode to enable or disable Sxa tunnel deletion at DSR. See the *Configuring the Sxa Tunnel Deletion* section for more information.

12. P-GW-U sends 'Sx Modification Response' back to P-GW-C.
13. P-GW-C sends 'Modify Bearer Response' to S-GW-C.
14. When P-GW responds with 'Modify Bearer Response', S-GW-C then sends 'Modify Bearer Response' with S-GW ctrl S11C FTEID and S-GW S1-U DATA FTEID to MME.
15. On receipt of 'Modify Bearer Response', MME sends 'Delete Session Request' to the the old S-GW-C. Old S-GW-C does not perform any Sx communication.
16. Old S-GW-C responds with 'Delete Session Response' to MME.

Configuring the Sxa Tunnel Deletion

To enable or disable Sxa tunnel deletion, use the following command.

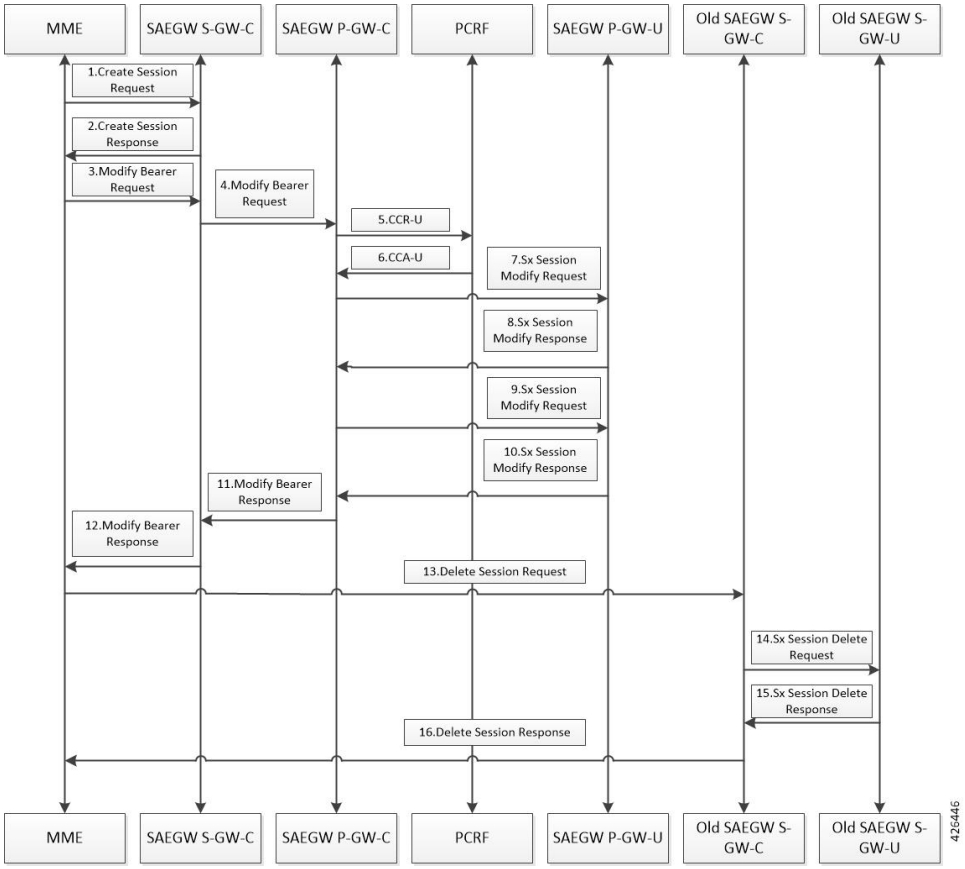
```
configure
  context context_name
    saegw-service service_name
      [ no ] sxa-tunnel-del-at-dsr-on-sgw-change
      end
```

NOTES:

- **sxa-tunnel-del-at-dsr-on-sgw-change** : Enable the Sxa tunnel deletion at DSR during X2/S1 based handover with SGW relocation.
- **no sxa-tunnel-del-at-dsr-on-sgw-change** : Disable the Sxa tunnel deletion at DSR during X2/S1 based handover.
- The configuration is disabled by default.
- The configuration will be applied to all current and new sessions.

S-GW Relocation Pure-P Call to Collapsed Call

Following call flow illustrates, the procedure for an S-GW Relocation Pure-P call to Collapsed call at a high-level.



1. On S-GW handover, MME sends 'Create Session Request' to new SAEGW-S-GW-C which is part of SAEGW anchoring P-GW call of that subscriber. SGW-C does not perform any Sx communication after detecting that it is a collapsed call.
2. SGW-C sends 'Create Session Response' back to the MME.
3. On receiving 'Create Session Response', MME sends 'Modify Bearer Request' with eNodeB FTEID to S-GW-C.
4. S-GW-C triggers 'Modify Bearer Request' to P-GW-C with zero S-GW S5/S8-U Data FTEID. Allows zero S5/S8-U SGW DATA FTEID in 'Modify Bearer Request' for the collapsed calls.

5. Performs Gx commuincation with PCRF CCR-U.
6. Performs Gx commuincation with PCRF CCA-U.
7. After Gx interaction is complete, the SAEGW-P-GW-C triggers 'Sx Modification Request' to SAEGW-P-GW-U. Sx Modification Request contains the following:
   - 'Create PDR' and 'Create FAR' (with apply action as DROP) for S-GW Ingress.
   - 'Create PDR' and 'Create FAR' (with apply action as DROP) for S-GW Egress.

   Control Plane requests User Plane to allocate following S-GW DATA FTEIDS for both uplink and downlink path:
   - S-GW S1-U DATA FTEID
   - S-GW S5/S8-U DATA FTEID

   Interface type changes from Sxb to Sxab, that is, Pure P to Collapsed call.
8. SAEGW-P-GW-U responds with 'Sx Modification Response' to SAEGW-PGW-C over Sxab interface.
9. SAEGW-P-GW-C triggers second 'Sx Modification Request' to SAEGW-P-GW-U. The 'Sx Modification Request' contains the following:
   - 'Update S-GW Ingress PDR' with 'Outer Header Removal' set based on eNodeB S1-U DATA FTEID.
   - 'Update S-GW Egress PDR' with 'Outer Header Removal' set based on P-GW S5/S8-U DATA FTEID.
   - 'Update S-GW Ingress FAR' with 'Outer Header Creation' set to P-GW S5/S8-U DATA FTEID and apply action as FORWARD.
   - 'Update S-GW Egress FAR' with 'Outer Header Creation' set to eNodeB S1-U DATA FTEID and apply action as FORWARD.
   - 'Update P-GW Ingress PDR' with 'Outer Header Removal' based on S-GW S5/S8-U DATA FTEID.
   - 'Update P-GW Egress FAR' with 'Outer Header Creation' set to S-GW S5/S8-U DATA FTEID and apply action as FORWARD.
   - Update the 'P-GW Ingress PDR' with 'Outer Header Removal' set based on S-GW S5/S8-UDATA FTEID.
10. SAEGW-P-GW-U sends 'Sx Modification Response' to SAEGW-P-GW-C.
11. On receipt of 'Sx Modification Response', SAEGW-PGW-C sends 'Modify Bearer Response' to SAEGW-SGW-C.
12. SAEGW-S-GW-C sends 'Modify Bearer Response' with S-GW ctrl S11c FTEID and S-GW S1-U DATA FTEID.
13. On receipt of 'Modify Bearer Response', MME sends 'Delete Session Request' to the old SGW-C.
14. Old SGW-C sends 'Sx Delete Session Request' to the old SGW-U.
15. Old SGW-U responds with 'Sx Delete Session Response' to the old SGW-C.

16. Old SGW-C responds with 'Delete Session Response' to the MME.

PDN Update Procedures

This section highlights the following PDN Update Procedures supported over CUPS architecture.

- UE Initiated Procedures
  - Modify Bearer Command
  - Modify Bearer Request
- Network Initiated Procedures
  - RAR
  - CCA-U (Triggered as part of UE Initiated Procedures or any internal trigger)

The above scenarios are supported for both SAEGW Pure-P and SAEGW Collapsed Call type.

All possible network failure scenarios are also supported, which includes:

- Sx Failures (Sx Modification Response)
- GTP Failures (Update Bearer Response)
- Gx Failures
- Create Bearer Response failure

Failure Handling and Call Drop Scenarios

Following table highlights the various possible Sx/GTP failures scenarios and the resultant P-GW behavior. It also highlights the conditions where the P-GW initiates call termination to avoid inconsistency between Control Plane and User Plane.

Sx Modification Failure Scenarios	P-GW Behaviour
Sx Modification Request is carrying - Query URR **NOTE**: Sx Modification may or may not carry additional IE's along with Query URR (apart from Revert Scenario) - Dynamic Rule Addition (Create PDR/FAR/URR/QER) - Predefine Rule Addition (Create PDR/URR) - Rule Updation (Update PDR/FAR/URR/QER) - Dynamic Rule Removal (Remove PDR/QER) - Predefine Dynamic Rule Removal (Remove PDR) - APN-AMBR QER Change - DSCP Change (QoS Change)	Call Drop: Yes **Disconnect Reason:** sxfail-opr-get-usagereport

Sx Modification Failure Scenarios	P-GW Behaviour
a) Sx Modification Request is carrying - Query URR b) Sx Modification Response is received with Cause: Failure + Usage Information	The Usage Information is not processed.
a) Sx Modification Request is carrying 1) Dynamic Rule Addition (Create PDR/FAR/URR/QER) 2) Predefine Rule Addition (Create PDR/URR) 3) Rule Updation (Update PDR/FAR/URR/QER) 4) Dynamic Rule Removal (Remove PDR/QER) 5) Predefine Rule Removal (Remove PDR) 6) APN-AMBR QER Change 7) DSCP Change (QoS Change) 8) Query URR b) Sx Modification Response is received with Cause: Failure	Control Plane sends another "Sx Modification Request" 1) No Action (CP and UP are in sync) 2) No Action (CP and UP are in sync) 3) Remove Rule (Remove "PDR/FAR/URR/QER") so that CP and UP will be in sync. 4) Call Drop (Conditional) a) Remove PDR/URR: Call Drop b) Remove QER/FAR: Retain Call, Error Log 5) Call Drop (Conditional) a) Remove PDR : Call Drop b) Remove QER : Retain Call, Error Log 6) APN-AMBR QER Change: No Action (CP and UP are in sync) 7) DSCP Change (QoS Change): No Action (CP and UP are in sync) 8) Call Drop **NOTE**: As of now, CP does not send "Remove URR and Remove FAR" as part of Rule Removal event. **Disconnect Reason (In priority order) :** sxfail-opr-get-usagereport sxfail-opr-create-rulebase-pdr sxfail-opr-remove-pdr

Sx Modification Failure Scenarios	P-GW Behaviour
a) Sx Modification Request is carrying 1) Dynamic Rule Addition (Create PDR/FAR/URR/QER) 2) Predefine Rule Addition (Create PDR/URR) 3) Rule Updation (Update PDR/FAR/URR/QER) 4) Dynamic Rule Removal (Remove PDR/QER) 5) Predefine Rule Removal (Remove PDR) 6) APN-AMBR QER Change 7) DSCP Change (QoS Change) 8) Query URR b) Sx Modification Response is received with "Cause : Success", followed by c) Update Bearer Request d) Update Bearer Response (Cause = Failure)	Control Plane send another "Sx Modification Request" to revert back to older state. 1) Remove Rule (Remove "PDR/FAR/URR/QER"), So that CP and UP will be in sync. 2) Remove Rule (Remove "PDR/QER"), So that CP and UP will be in sync. 3) Remove Rule (Remove "PDR/FAR/URR/QER") so that CP and UP will be in sync. 4) No Action (CP and UP are in sync) 5) No Action (CP and UP are in sync) 6) Send Retained (Old) APN-AMBR so that CP and UP will be in sync. 7) Send Retained (Old QoS) DSCP so that CP and UP will be in sync. 8) No Action **NOTE**: As of now, CP does not send "Remove URR and Remove FAR" as part of Rule Removal event.
a) When Sx Modification Request is initiated as part of Update Bearer Response (Failure) : To keep CP and UP in Sync 1) Remove PDR/FAR/URR/QER 2) Remove PDR/QER (Predef Rule) 3) Retained(Old) APN-AMBR QER 4) Retained(Old) DSCP 5) Query URR b) Sx Modification Response is received with "Cause : Failure"	1) Call Drop a) Remove PDR/**URR** : Call Drop b) Remove QER/**FAR** : Retain Call, Error Log 2) Call Drop (Conditional) a) Remove PDR : Call Drop b) Remove QER : Retain Call, Error Log 3) Call Drop 4) Call Drop 5) Query URR : Call Drop **Disconnect Reason :**sxfail-opr-revert-info
When Sx Modification Request is sent and fails because of: - Sx Modification Response (Context Not Found) - No Sx Modification Response (Sx Retransmission Timeout)	Call Drop: Yes **Disconnect Reason :**sx-cntxt-not-found sx-no-response

Scenario's	Call Drop
Context Not Found (GTP/Sx)	Yes
Retransmission Timeout (GTP/Sx)	Yes
GTP Cause : Temp fail Temp Failure CLI is not configured	No, Sx Mod (Revert to old APN-AMBR/Default QoS values or Remove Rules)
GTP Cause : Temp fail (Retry Exhausted) Temp Failure CLI is configured	No, Sx Mod (Revert to old APN-AMBR/Default QoS values or Remove Rules)
MBC -> UBReq -> UBRsp (No Resouce Available)	Call drop behaviour should be inline with non-cups
MBR/RAR ->UBReq -> UBRsp (No Resouce Available)	No, Sx Mod (Revert to old APN-AMBR/Default QoS values or Remove Rules)
Other cause (GTP/Sx)	No, Sx Mod (Revert to old APN-AMBR/Default QoS values or Remove Rules)

PDN Update Procedures - eNodeB F-TEIDu

Feature Description

As a part of the CUPS architecture, a procedure to initiate an Sx Modification Request has been implemented for an eNodeB F-TEIDu update or a Release Access Bearer (RAB) Request for an eNodeB release for an S-GW or SAE-GW.

How It Works

The PDN update procedures includes the following events for an eNodeB F-TEIDu Update/Release:

- For eNodeB F-TEIDu Update
  1. The SGW-C initiates an Sx Session Modification Request towards SGW-U on receiving a Modify Bearer Request for eNodeB F-TEIDu Update from the MME.
  2. The Sx Modification Request for eNodeB F-TEIDu update contains Update FAR with Apply Action as “Forward” and the updated eNodeB IPv4/IPv6 address in Outer Header Creation, which are a part of the Update Forwarding Parameters IE.

- For eNodeB F-TEIDu Release
  1. The SGW-C initiates an Sx Modification Request towards SGW-U on receiving a RAB Request from the MME.
  2. RAB is a UE-level message. If the UE has multiple PDN connections then the Sx Modification Request is sent to each PDN connection separately.
  3. SGW-C initiates Sx Session Modification Request towards SGW-U for the Sx session with Update FAR with destination interface as ACCESS. Update FAR contains: FAR ID and Apply Action as Drop. FAR with the destination interface as CORE is not updated.

Standards Compliance

The PDN Update procedure 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 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 of EPC ".
- 3GPP TS 23.214: "Architecture enhancements for control and user plane separation of EPC nodes; Stage 2"
- 3GPP TS 23.714: "Study on control and user plane separation of EPC nodes"

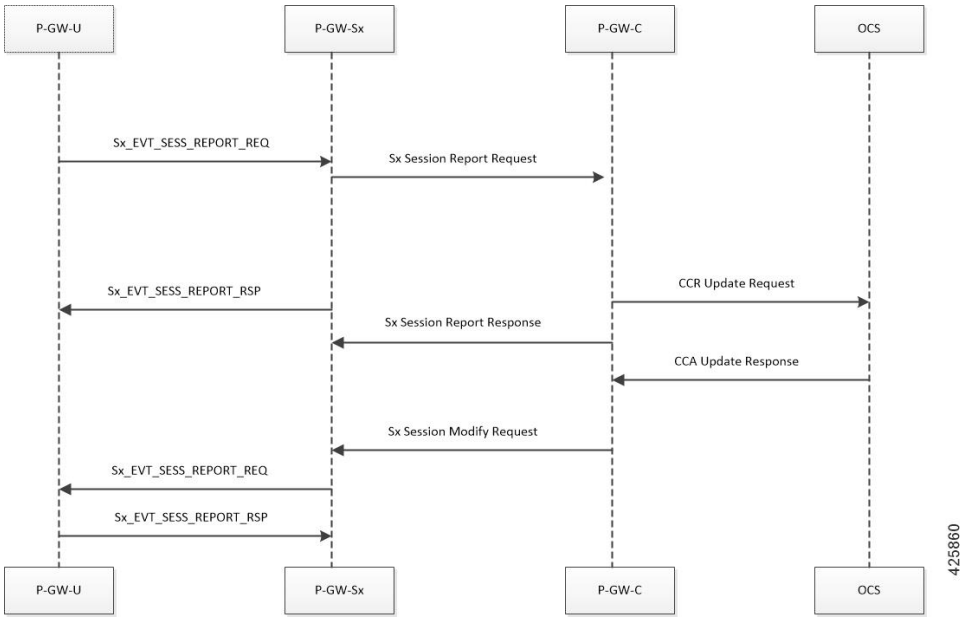
Gx Update Procedures

Following is the behavior of Gx update procedure:

- Common FAR is used for the PDRs if FAR attributes are the same.
- In case of update of (only) flow status/rating group, Update QER/URR is sent. That is to say, no Update PDR is sent in such cases.
- Rule installation triggers Create PDR and Create QER (SDF level), and may or may not have Create FAR and Create URR (rule can reuse FAR and URR of other rules).
- Rule modification for a flow status/rating group triggers Update QER/Update URR and may or may not have Update PDR (that is, no TFT/QoS change).
- Rule modification for TFT/QoS triggers Update PDR and may or may not have Update QER/Update URR (no QER/URR change).
- Rule removal is triggered in case of Update QER, Update URR, Update FAR, or Update PDR failure as part of Sx modify.
- Call drop is initiated if failure happens for Remove PDR and Create PDR (of rule base).
- APN-AMBR change received from PCRF triggers Update QER.
- The default-eps-bearer-qos change, received from PCRF, triggers Update FAR if there is a change in DSCP marking corresponding to the new QoS.

P-GW Session Reporting with Gy Interface

This section describes P-GW session reporting with Gy interface.



URR Creation During Session Setup

- Control Plane function sends a list of URRs in the Sx Session Establishment request, along with their references in corresponding PDRs.
- The CCR/CCA-I message exchange happenes by the time the Sx-Session-Establishment request is generated by the CP, and the quota for the Dynamic-Rules and Pre-emptive MSCCs is received from the OCS.

URR Creation during Session-Modification/Mid-Session

- When a Rule-Modification/install occurs from PCRF in mid-session, then the Sx Session Modification request is used to provision the PDRs and URRs. When creating the URR in the mid-session, if the Quota information is not present in the OCS, then the “Start-of-Packet” trigger is set along with the Measurement Methods: Time & Volume.
- On the arrival of the first packet, the "Start-of-Packet" trigger is sent to the Control Plane for packet-detection, and the Control Plane initiates the Quota negotiation with the OCS server.

URR Processing in Session Disconnect

- The P-GW User Plane sends the URR information as part of Sx Session Delete Response.
- The P-GW Control Plane does the mapping of these URRs to corresponding MSCC buckets and uses existing framework to send the Credit-Control-Messages on the Gy/Ro interface.

Session Delete Response

- P-GW User Plane sends the URR information as part of the Sx Delete Response.
- PGW Control Plane maps these URRs to the corresponding MSCC buckets and use the existing framework to send the Credit-Control-Messages on the Gy/Ro interface.

Sx Session Report Request Handling

P-GW User Plane sends the Usage report for triggers like volume, time-quota, threshold, validity-time, quota-hold-time and so on. P-GW Control Plane maps the URRs to the corresponding charging buckets (MSCC). It initiates the Credit-Control-Request Update for the respective MSCCs.

URR Reporting Handling for Gy

The URR reporting results in Credit-Control-Request-Update generation, depending on the trigger that is sent by the P-GW User Plane.

- When User Plane reports a URR for any trigger, it is first mapped to the MSCC bucket at the Control Plane. The values are updated in the MSCC data-structure.
- After the URR buckets are processed in the current reporting, the Control Plane analyzes the MSCC buckets that are being updated. It initiates the Credit-Control-Request Update request containing all the MSCC-buckets.



Important For this release, the single MSCC-per-update feature is not supported.

Failure Handling Support for Gy

The Failure-Handling configuration is to specify the action to be taken when a failure occurs during communication with the OCS server. The possible Failure-Handling configurations are Continue, Terminate, Retry, and Terminate. The Terminate and Retry-Terminate are solely at the Control Plane. For Continue, the following actions are performed:

- When the CCFH Continue action is applied, all the Gy URRs are disassociated and removed from the PDRs, so that no further reporting/charging occurs for the Online Charging.
- The "removeURR" IE is provisioned for all the Gy URRs to the User Plane, and the User Plane clears all the references to the URR and does the removal internally.
- Handling of MSCC level Error-Result-Codes is supported excluding the following mscc-result-codes: 4010, 4012, 5003, 5012, and 5031.

How failure handling on Gy with session disconnects works

Summary

This process describes how the Policy and Charging Enforcement Function (PCEF) handles update requests, especially in situations of communication failures with the Online Charging System (OCS).

The key components involved in the process are:

- PCEF (Policy and Charging Enforcement Function): Initiates Credit Control session with OCS (CCR-I/U/T) and manages the session's state and quota consumption,
- OCS (Online Charging System): Receives and processes Credit Control requests, manages charging information, and provides responses,
- Secondary Server: A backup OCS server used by the PCEF in case of primary server communication failure, and

- SU Mechanism (Service Ureachability Mechanism): A quota allocation mechanism at the PCEF triggered when communication with both the Primary and Secondary OCS fails, allowing the session to continue with an interim quota assignment, if configured. A quota allocation mechanism at the PCEF, triggered when communication with both the Primary and Secondary OCS fails. This mechanism allows the session to continue with an interim quota assignment, if configured.

Workflow

The process involves these stages:

1. The PCEF sends a Credit Control Request (CCR-I / CCR-U) to the OCS.
2. The PCEF detects communication issues with the primary OCS.

If...	Then...
Transport failure detected	PCEF immediately retries with the secondary server.
Timeout detected	Tx expiry is triggered. **Note** The Service Unreachability(SU) is triggered only after the detecting server failure i.e. post the Tx timer expiry at secondary OCS server as well. If the reply is received before the Tx expiry then PCEF does not activate SU.

3. The PCEF activates SU and assigns Interim Quota only when the communication with the secondary OCS server also fails

If...	Then...
Interim volume and or time or both, are configured	Interim quota is assigned to the session.

4. The PCEF retries CCR request (CCR-I / CCR-U) to the last attempted OCS server after Interim Quota exhaustion (time or volume quota), if the server retries value is greater than zero. PCEF sends another CCR-I or CCR-U to the server that triggered the SU mechanism. If this attempt also fails, the PCEF sends a CCR-U to another server, containing the entire consumed unreported quota (only CCR-U based retry, in case of CCR-I based retry it doesn't include the consumed quota).
5. PCEF repeats this failure mechanism and then disconnects the session or continues the session depending on SU action configured (continue/terminate).

   PCEF continues to attempt communication until a successful response is received or retry limit is met.

If...	Then...
Transport failure or Tx-timeout again detected	Steps 2 through 4 are repeated.
Server retries value is exhausted	The session is disconnected, if SU configured action is terminate. **Note** The session remains but not retried to any OCS server, if SU configured action is continue.

If...	Then...
Successful response from OCS is received	The PCEF exits the SU state and reports all interim usage to OCS.

6. When the session is disconnected due to exceeding maximum retries for CCR-U message, the PCRF sends a Credit Control Request Terminate (CCR-T) to the OCS with the entire consumed quota used in the SU state. If the session is disconnected due to exceeding maximum CCR-I failure, then the CCR-T is not sent as the session is not established with respect to the OCS.
7. The OCS responds to the final report with Result Code 2002, and no futher CCR is triggered by the PCEF as session is terminated.

Result

This process ensures robust handling of update requests under communication failure conditions, allowing the system to manage session state, assign interim quotas during outages, attempt re-establishment of communication, and ultimately ensure accurate reporting of consumed quota even if a session must be disconnected due to persistent server unreachability.

Re-Authorization-Request Handling

When the RAR request comes from the OCS server, the Control Plane sends the "QueryURR" for the required Charging-Buckets to the User Plane. When the User Plane sends back the URR report to the Control Plane, the Control Plane sends the CCR-Update for the FORCED_REAUTHORIZATION trigger.

Quota-Validity-Time Handling

When the Quota-Validity-Time is received for an MSCC bucket, the same is sent to the User Plane. Since there is no specific IE that can be used directly, the QVT value is filled in the Time-Quota IE, and URR is sent to the User Plane. The lesser QVT or Time-Quota is set in the Time-Quota IE. And, the Usage-Reporting from the User Plane for the Time-Quota trigger, the interpretation is made and the CCR-Update for the Validity-Timeout is generated.

Re-Authorization of the Blacklisted Content

The category Multiple-Services-Credit-Control (MSCC) gets blacklisted when it recieves the 4012/4010 result codes at the MSCC level. It indicates that no further packets passes for this category but instead it drops. In CUPS, FAR is created with the DROP action, and is linked to the URR and sent it to the UP as part of the QuotaFAR along with the 0 quota, so that the UP starts applying the DROP action.

In non-CUPS architecture, there is a provision to re-authorize these blacklisted contents, on the next packets after the timer expiry (the timer is either locally configured – quota-retry-timer, or ocs provided – gating-expire-timer). After this timer expires, on the arrival of the next packets, it triggers the quota-allocation-request to the OCS. To implement this in the CUPS mode, run the timer in the CP (new timer – in case of the non-CUPS architecture it accomplishes by comparing the timestamps).

On expiry of the timer (either GET of QRT timer), the FAR is removed from the URR, and URR is modified with the Start-of-Traffic trigger. On the next packets arrival, there is a URR reporting to CP for the Start-of-Traffic. This information can be used at CP to request the quota to OCS and get the new quota allocation.

The variation of this feature is the configuration of the CLI, **diameter reauth-blacklisted-content**. It says that the OCS can send the RAR for requesting the re-enabling of the blacklisted categories.

Server-Unreachable Support for Gy

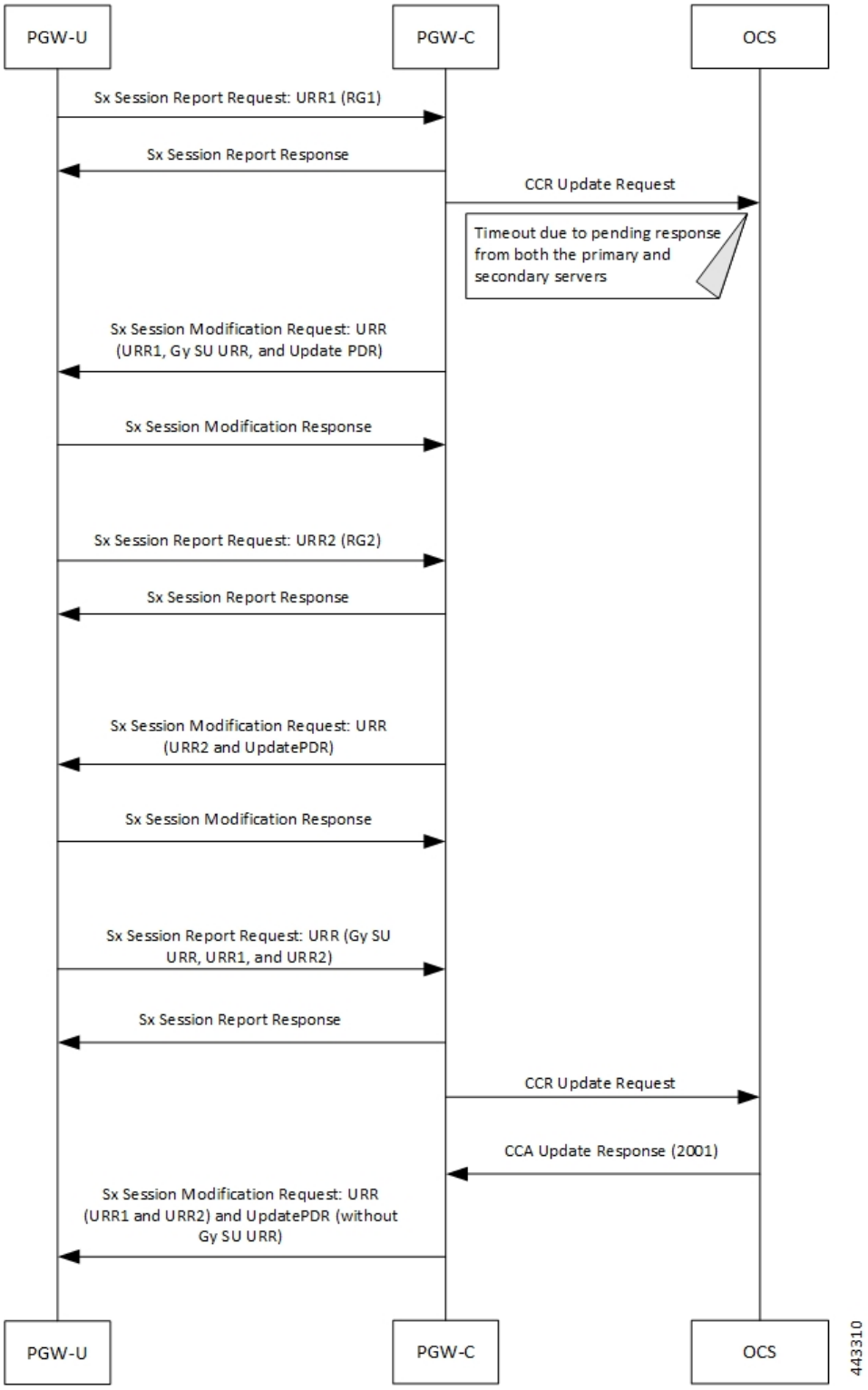
The Server-Unreachable (SU) mechanism is configured on the Control-Plane (CP), for the Gy interface in order to resolve issues that are encountered on the Online Charging System (OCS) or with the connectivity between Policy and Charging Enforcement Function (PCEF) and OCS. The SU configuration provides the options to continue the session even after a failure by providing the option to use configurable interim quota (volume and/or time) and configurable server retries before a session is converted to offline or terminated.

A new Usage Reporting Rule (URR) bucket is created, which contains the SU quota when a Gy session goes into the SU state. The ID for the new URR is generated dynamically when the SU URR is allocated.

In a CUPS User Plane (UP) node, the existing Vector Packet Processor (VPP) streams are modified with a new LC record, which contains the updated SU URR bucket along with the existing set of charging buckets.

When the VPP streams are in the SU state, two quota rows are available, GyURR and SU URR. When GyURR is in the SU state with linked-usage-reporting trigger set, the quota row for the SU URR is linked to the VPP streams.

The following diagram describes the SU call flow in CUPS.


PGW-U
PGW-C
OCS
Sx Session Report Request: URR1 (RG1)
Sx Session Report Response
CCR Update Request
Timeout due to pending response from both the primary and secondary servers
Sx Session Modification Request: URR (URR1, Gy SU URR, and Update PDR)
Sx Session Modification Response
Sx Session Report Request: URR2 (RG2)
Sx Session Report Response
Sx Session Modification Request: URR (URR2 and UpdatePDR)
Sx Session Modification Response
Sx Session Report Request: URR (Gy SU URR, URR1, and URR2)
Sx Session Report Response
CCR Update Request
CCA Update Response (2001)
Sx Session Modification Request: URR (URR1 and URR2) and UpdatePDR (without Gy SU URR)
PGW-U
PGW-C
OCS
443310

Step	Description
1	PGW-U sends a Sx Session Report Request message with URR1 (RG-1) to PGW-C due to internal triggers like Time and Volume or Quota and Threshold.
2	PGW-C acknowledges the request and sends a Sx Session Report Response message to PGW-U.
3	PGW-C sends CCR Update (CCR-U) Request message to both the primary and secondary OCS.
4	When the CCR-U Request messages fail at both primary and secondary OCS, the Gy session enters an SU state. The SU URR is created for the Gy session, and it's linked to the relevant PDRs. PGW-C sends an Sx Session Modification Request message to PGW-U with UpdatePDR, which includes Gy SU URR in the PDR URR list.
5	PGW-U starts updating the usage in both the Gy buckets (URR1 and Gy SU URR1) and sends an Sx Session Modification Response message to PGW-C.
6	PGW-U sends another Sx Session Report Request message with URR2 (RG-2) to PGW-C after the Gy URR bucket exhausts the quota .
7	PGW-C acknowledges the request sends a Sx Session Report Response message to PGW-U.
8	PGW-C sends an Sx Session Modification Request message to PGW-U with UpdatePDR and Update RR2. The UpdatePDR has a modified URR list, which contains both URR2 and Gy SU URR.
9	PGW-U sends an Sx Session Modification Response message to PGW-C.
10	PGW-U sends a Sx Session Report Request message with URR1 (RG-1) and URR2 (RG-2) to PGW-C after the Gy SU URR quota is exhausted.
11	PGW-C acknowledges the request and sends a Sx Session Report Response.
12	PGW-C sends CCR Update (CCR-U) Request message to OCS after an SU retry.
13	OCS sends a CCA Update Response message with the Result-Code as 2001.
14	PGW-C sends an Sx Modification Request message with URR1 (RG-1), URR2 (RG-2), and UpdatePDR (without Gy SU URR) to PGW-U.

New Behavior in CUPS

The new SU mechanism in CUPS, are as follows:

- In a non CUPS architecture, where a single node (P-GW) processes the Gy session state and the data-traffic, an SU URR is created without any messaging delay. However, in the CUPS mode, the CP forms an additional node, which maintains information about the session state and handles any URR requests from the User Plane (UP). Only the CP can associate a Gy session with an SU URR. This messaging between UP and CP causes a delay and the data packets are treated according to the Pending-Traffic-Treatment configuration to complete the communication.
- In a non CUPS architecture, the SU state timer is processed in a different manner compared to the Time-Quota timer. After an SU quota is exhausted, the retry attempt to OCS occurs and a new next-interim-time-quota is started. However, in the CUPS mode, when the SU Time Quota is used and it is reported to CP for the Quota Exhaust, and if the session goes into Server-Unreachable state again, the time elapsed from the last Usage-Report is accounted in the usage.

- It's not recommended to use the **servers-unreachable after-timer-expiry** *timeout_period* CLI command in CUPS. Instead, use the **servers-unreachable after-interim-time** *timeout_period* **server-retries** *retry_count* to achieve similar behavior but with a single retry (set *retry_count* to 1).

Limit-Reached Postprocessing

Limit-reached-post-processing is a non-3GPP, proprietary behavior supported in both CUPS and non-CUPS architecture. This feature allows redirection or restriction operation implemented when the quota is exhausted for the charging-bucket, however, the OCS server is unable to grant the FUI-Redirect or FUI-Restrict. When using this feature, the operator can combine all the rule-matching criteria that are available—for example, to enable IMSI-based matching criteria, and so on—to selectively apply different handling for different subscribers/traffic. Use the following CLI commands to enable the feature.

```
configure
  active-charging service service_name
    rulebase rulebase_name
      post-processing policy always
      end
```

Also, **rule-application post-processing** CLI command must be configured as limit-reached under ACS Ruledef configuration mode.

PTT no-quota Limited Pass

This feature allows the subscriber to use the network while waiting for the response from OCS. The Limited-Pass configuration allows to specify the Volume which the subscriber can consume while waiting for the quota-response from OCS. The usage is accounted in the respective charging bucket and are adjusted against the next-quota allocation.

Use the following CLI commands to enable the feature:

```
configure
  active-charging service service_name
    credit-control
      pending-traffic-treatment noquota limited-pass volume volume
      end
```

Limited Pass Volume is used only for **noquota** case (Rating Group (RG) seeking quota for the first time) and not for **quota-exhausted**. Limited Pass Volume isn't used for subsequent credit requests.

The traffic is allowed to pass until the Limited-Pass Volume gets exhausted. The usage is counted in the respected charging-bucket and adjusted against the "Quota" granted. If the "Quota" allocation is less than the actual usage, immediate reporting towards OCS with the usage-report occurs requesting for more quota allocation. The subsequent incoming packets are handled as per the "quota-exhausted" PTT configuration.

If the Limited Pass Volume is NOT exhausted before the OCS responds with denial of quota, traffic is blocked after the OCS response. The gateway reports usage on Limited-Pass Volume even in for CCR-U (FINAL) (in non-CUPS) or CCR-T (for CUPS) until the OCS responds.

If the Limited Pass Volume is exhausted before the OCS responds, then the subsequent incoming packets for the session are dropped until quota is granted from OCS.

The default pending-traffic-treatment for **noquota** is Drop. The **default pending-traffic-treatment noquota** command removes any Limited Pass Volume size configured.

PTT Quota-Exhausted Limited Pass

Pending-Traffic-Treatment (PTT) Quota-Exhausted Limited-Pass in CUPS architecture is an alternative to the Buffering option. The Buffering option has practical limitations in the high-speed network. Buffering requires packet buffering for large number of packets at the gateway, causing the risk to run out of memory and affecting the bandwidth speed. The PTT Quota-Exhausted Limited Pass allows the traffic to pass through until it reaches the configured limit on the Quota-Exhaust scenarios.

The PTT allows the traffic until the Limited-Pass volume exhausts. The PTT counts and adjusts the usage in the respected charging-bucket against the granted "Quota". If the "Quota" allocation is less than the actual usage, there's immediate reporting towards OCS with the usage-report and asking for more quota allocation.

If the Limited-Pass Volume doesn't exhaust before the OCS responds with denial of quota, there's traffic blockage after the OCS response. Gateway reports the usage in CCR-U (FINAL).

If the Limited-Pass Volume exhausts before the OCS responds, then further incoming packets for the session are dropped until quota is granted from OCS.

The default behavior of pending-traffic-treatment for quota-exhausted is Drop. The default pending-traffic-treatment quota-exhausted CLI command removes any configured Limited-Pass Volume size.

Use the following CLI command to enable the feature:

```
configure
  active-charging service service_name
    credit-control
     pending-traffic-treatment quota-exhausted limited-pass volume volume

       end
```



Note The above CLI command is applicable only in CUPS architecture.

NOTES:

- **limited-pass**: Enables limited access to subscriber when OCS is unreachable.
- **volume** *volume*: Enables limited volume access to subscriber when OCS is unreachable. *volume* specifies the Default Quota size (in bytes) and must be an integer from 1 through 4294967295

Supported Functionality and Limitations

Basic call flow with Volume-Quota mechanism is supported with the following limitations on P-GW session reporting for Gy interface:

- Only CCR/CCA-I , CCR/CCA-U and CCR/CCA-T, RAR/RAA messages are supported.
- Dynamic Rules with Online Enabled is supported; both at Session-Setup and Mid-Session.
- Predefined Rules (dynamic-only) is supported; both at Session-Setup and Mid-Session. No restriction on configuring the "preemptively request".
- Static-rules with Online Charging are supported.
- Ignore-service-id is supported.
- Volume-Quota/Volume-Threshold mechanisms are supported.

- Event-Triggers (through which the Query URR occurs), and sending of usage information to the OCS is supported.

Important RAT-change functionality is not validated for this release.

- The "updateURR" procedure, through the Sx-Session-Modification procedure where the OCS grants a fresh Quota, is supported.
- Bearer-Level Gy and Subscriber-Level Gy is supported.
- Pending-Traffic-Treatment (PTT) Drop/Pass is supported with following limitations:
  - The scenarios supported for now are no-quota and quota-exhausted.
  - The trigger/re-authorization scenarios are not supported.
  - The PTT action (Forward/Drop) is considered after the quota-get is exhausted.
- Failure scenarios are qualified, which includes:
  - Failure-Handling Terminate, Continue and Retry, and Terminate: With CC-Group/FHT
  - Handling for the Error-Result-Codes (both at MSCC and Command level) is supported.
- Wall-Clock time-quota mechanism is supported.
- Other Time Quota Mechanisms (Discrete Time Period and Continuous-Time-Period) are not supported.
- Final-Unit-Indication Terminate mechanism is supported.
- FUI-Restrict is not supported.
- Mid-Session Rule Installation/Removal/Modification is supported.
- RAR mechanism is supported.
- Server-Unreachable (SU) mechanism is now supported with minor change in behavior compared to non-CUPS P-GW.
  - When an URR needs quota at UP, the usage-report is generated to CP and until the CP responds with the linked SU_URR, the packets matching this URR are treated with Pending-Traffic-Treatment configuration.
  - When the SU Time Quota is used and it's reported to CP for the Quota Exhaust, and if the session goes into Server-Unreachable state again, the time elapsed from the last Usage-Report is accounted in the usage.
- Pending-Traffic-Treatment Buffer mechanism is not supported.
- The “send-ccri on traffic-start” is supported.
- Quota-Hold-Time is supported.
- Quota-Consumption-Time mechanism is not supported.
- Quota-Validity-Time is supported.

- Triggering Gz records from Gy, when any event in Gy occurs, is supported; Gy-Gz sync is not supported.
- Triggering Rf records from Gy, when any event in Gy occurs, is not supported.
- Configuring different "rating-group" value other than the "content-id" is supported.
  - The RG 0 is not supported.
- Trigger to PCRF for the Out-of-Credit, Reallocation-of-Credit events are not qualified.

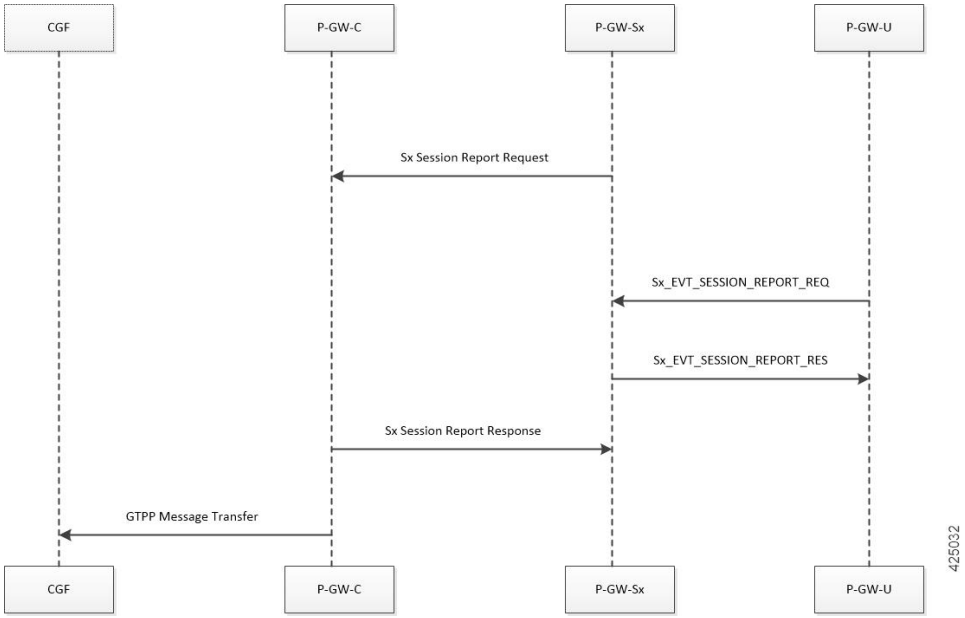


Important Event-trigger Out-of-Credit towards PCRF is validated with a limitation of having only one time Grant-Quota (Keeping Total Volume and Granted Volume at same value).

- The delayed response from OCS for the CCR-I is supported.
- Service-Specific-Units are not supported.
- Tariff-Time change is supported as per 3GPP specification.
- Quota-Retry Timer is supported.
- The **diameter mscc-final-unit-action terminate session** CLI command under Credit Control Configuration mode is supported.
- FUI-Redirect is supported with following limitations:
  - Redirection for HTTPs is not supported.
  - The FUI-Redirect with Filter-IDs/Filter-Rules are not supported.
  - The WSP Protocol is not supported.
  - In accordance with 3GPP specification, the Redirected-Traffic also gets redirected if it hits the rule that is in FUI-Redirect. There is no provision to allow the redirected-traffic to pass through.
    - In accordance with 3GPP specification, the CUPS architecture adheres to **no diameter fui-redirected-flow allow** CLI command behavior.
  - The **redirect-require-user-agent** CLI command is not supported; the redirection continues to work even if the user-agent is not present.
  - Appending the original URL is not supported.
  - The **diameter redirect-validity-timer immediate** CLI command is supported. However, **diameter redirect-validity-timer traffic-start** CLI command is not supported.
  - Token based mechanism, to come out of Redirection, is not supported. To end the redirection in CUPS, OCS sends Redirect Validity-Time or RAR.
  - FUI-Redirection is supported only for the URL, similar to the behavior in non-CUPS architecture.
- Rulebase change from PCRF/OCS is supported.

P-GW Session Reporting with Gz Interface

This section describes P-GW session reporting with Gz interface.



URR Processing in Detach Request

- The URR information will be sent by PGW User-Plane as part of Sx Session Delete Response.
- P-GW Control Plane maps these URRs to the corresponding charging buckets and then use the existing framework to send the charging records on the respective interfaces like Gz, Gy, and so on.

Sx Session Report Request Handling

P-GW User plane sends the Usage Report for triggers like Volume or Time-Threshold. P-GW Control Plane maps the URRs to the corresponding charging buckets.

URR Reporting Handling for Gz

URR reporting results in LOSDV bucket creation and P-GW CDR generation depending on the trigger sent by the P-GW User-Plane.

- If the bearer level URR is received, it results in generating the P-GW CDR for corresponding sub-session/bearer, along with reporting any existing LOSDV containers and the ones getting created as part of current report request. It is assumed that, when bearer level URR is received, User-Plane has sent all the SDF level URRs as well.
- When the SDF level URRs are received, they are stored as LOSDV containers. In this case the fbc_bucket is created with necessary counts or timestamps from the URR.

Standards Compliance

The Control Plane in CUPS complies with the following standards:

- 3GPP specification 23.214 release 14.0: Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancements for control and user plane separation of EPC nodes.
- 3GPP specification 29.244 release 14.0: LTE; Interface between the Control Plane and the User Plane of EPC Nodes.
- 3GPP specification 23.401 release 14.0: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access.