



## SAE Gateway Overview

The Cisco® ASR 5500 provides wireless carriers with a flexible solution that functions as a System Architecture Evolution (SAE) Gateway with Packet Data Network (PDN) Gateway (P-GW) and Serving Gateway (S-GW) functions in LTE-SAE (3GPP2 Long Term Evolution-System Architecture Evolution) wireless data networks.

This overview provides general information about the SAEGW including:

- [SAEGW Product Description, on page 1](#)
- [S-GW Product Description, on page 3](#)
- [P-GW Product Description, on page 5](#)
- [S-GW Network Deployment\(s\), on page 8](#)
- [P-GW Network Deployment\(s\), on page 14](#)
- [S-GW Features and Functionality - Base Software, on page 29](#)
- [P-GW Features and Functionality - Base Software, on page 54](#)
- [P-GW Features and Functionality - Inline Service Support, on page 100](#)
- [S-GW Features and Functionality - Optional Enhanced Feature Software, on page 105](#)
- [P-GW Features and Functionality - Optional Enhanced Feature Software, on page 114](#)
- [How the Serving Gateway Works, on page 134](#)
- [How the PDN Gateway Works, on page 138](#)
- [S-GW Supported Standards, on page 147](#)
- [P-GW Supported Standards, on page 151](#)

## SAEGW Product Description

The SAEGW node is a combination of S-GW and P-GW nodes. SAEGW operates as a service on ASR5500 and requires existing S-GW and P-GW services to be configured and mentioned inside SAEGW service configuration. Existing standalone S-GW and P-GW services (when part of an SAEGW umbrella service) will work in tandem to present a single SAEGW node as a black-box view.

The SAEGW supports all of the interfaces that the standalone S-GW and P-GW products support, namely:

- S11/S4 – GTPv2 based control interface towards MME/S4-SGSN
- S1U/S12/S4U – GTPv1 based data interface towards eNodeB/RNC/S4-SGSN
- S5/S8 – GTPv2 based control interface between S-GW and P-GW
- Gi – Data interface towards packet data network

- Gx – Diameter based interface between P-GW and PCRF
- S6b – Diameter based interface between P-GW and HSS
- Rf – Diameter based offline charging interface between P-GW/S-GW and charging data function
- Gy – GTPP based online charging interface between P-GW and online charging system
- Gz – GTPP based offline charging interface between P-GW/S-GW and charging gateway function




---

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

---

Mode of operation is described as the functionality performed by SAEGW for a call. Granularity for mode of operation is per-PDN. The SAEGW service supports the following three modes of operation:

- S+P Collapsed: When a UE is using S-GW part of SAEGW and a PDN connection is terminating within the P-GW part of SAEGW.
- Pure-S: When a UE is using S-GW part of SAEGW and a PDN connection is terminating at an external P-GW not part of SAEGW.
- Pure-P: When a UE is using an external S-GW not part of SAEGW and a PDN connection is terminating within P-GW part of SAEGW.




---

**Important** For a given UE with multiple PDNs, SAEGW will be able to support S+P mode for some PDNs while Pure-S mode for others.

---




---

**Important** SAEGW supports change of operation-mode in life of a PDN. For example, a PDN initially doing S+P mode may change to doing Pure-P if S-GW gets relocated to external S-GW that is not part of SAEGW. Similarly, a PDN doing Pure-P mode may change to S+P mode if S-GW relocated so that new S-GW is part of SAEGW service.

---

An optimized SAEGW provides the following benefits:

- **Higher Capacity**

A UE with one PDN connection that passes through standalone S-GW and P-GW services consumes two license units because both S-GW and P-GW services account for it separately. SAEGW as a single node consumes only one license unit for the same, thus increasing the capacity. Contact your Cisco account representative for detailed information on product licensing.

- **Cohesive Configuration**

Configuration and management of SAEGW as a node is easier to follow than starting standalone S-GW and P-GW services.

## Platform Requirements

The SAEGW service runs on a Cisco® ASR 5500 Series chassis running StarOS. The chassis can be configured with a variety of components to meet specific network deployment requirements. For additional information, refer to the *Installation Guide* for the chassis and/or contact your Cisco account representative.

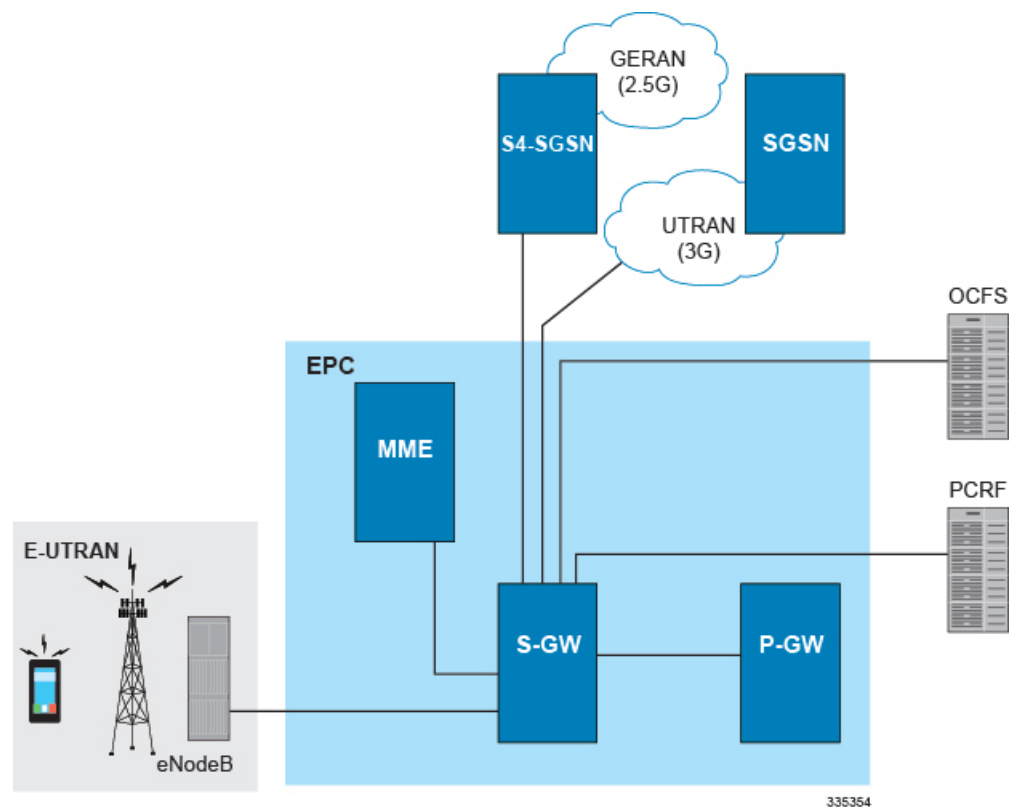
## Licenses

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

## S-GW Product Description

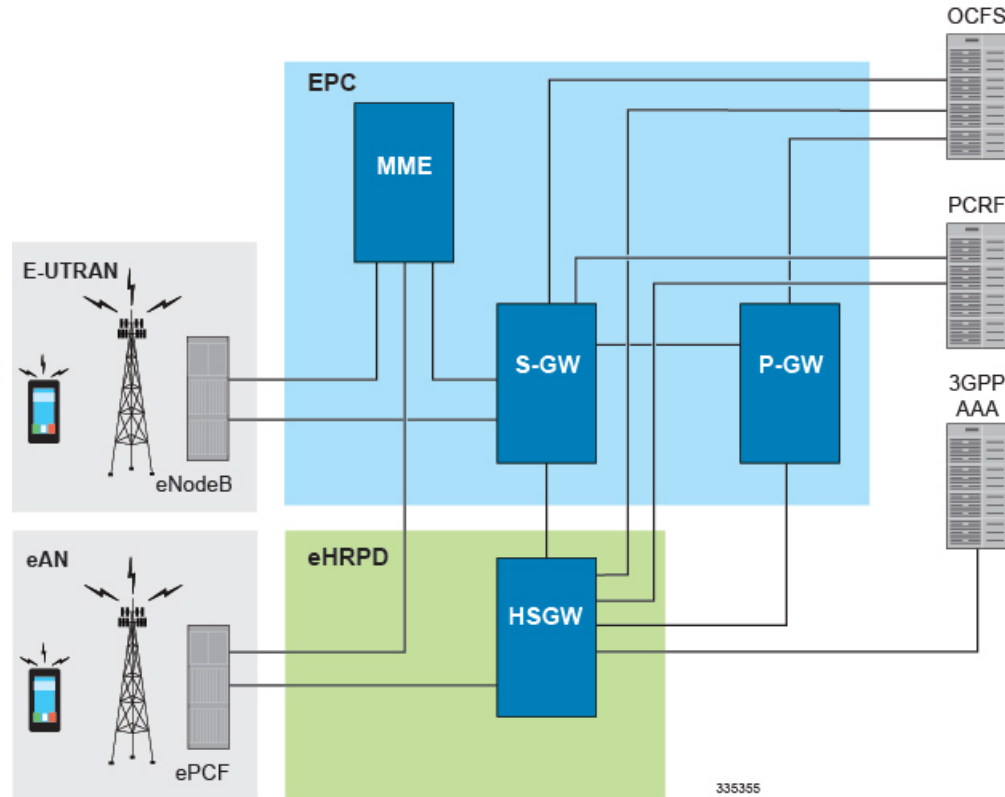
The Serving Gateway routes and forwards data packets from the UE and acts as the mobility anchor during inter-eNodeB handovers. Signals controlling the data traffic are received on the S-GW from the MME which determines the S-GW that will best serve the UE for the session. Every UE accessing the EPC is associated with a single S-GW.

**Figure 1: S-GW in the Basic E-UTRAN/EPC Network**



The S-GW is also involved in mobility by forwarding down link data during a handover from the E-UTRAN to the eHRPD network. An interface from the eAN/ePCF to an MME provides signaling that creates a GRE tunnel between the S-GW and the eHRPD Serving Gateway.

**Figure 2: S-GW in the Basic E-UTRAN/EPC and eHRPD Network**



The functions of the S-GW include:

- packet routing and forwarding.
- providing the local mobility anchor (LMA) point for inter-eNodeB handover and assisting the eNodeB reordering function by sending one or more "end marker" packets to the source eNodeB immediately after switching the path.
- mobility anchoring for inter-3GPP mobility (terminating the S4 interface from an SGSN and relaying the traffic between 2G/3G system and a PDN gateway).
- packet buffering for ECM-IDLE mode downlink and initiation of network triggered service request procedure.
- replicating user traffic in the event that Lawful Interception (LI) is required.
- transport level packet marking.
- user accounting and QoS class indicator (QCI) granularity for charging.
- uplink and downlink charging per UE, PDN, and QCI.
- reporting of user location information (ULI).

- support of circuit switched fallback (CSFB) for re-using deployed CS domain access for voice and other CS domain services.

## Platform Requirements

The S-GW service runs on a Cisco® ASR 5500 Series chassis running StarOS. The chassis can be configured with a variety of components to meet specific network deployment requirements. For additional information, refer to the *Installation Guide* for the chassis and/or contact your Cisco account representative.

## Licenses

The S-GW is a licensed Cisco product covered by the SAEGW license when part of an SAEGW umbrella service. Separate session and feature licenses may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

## P-GW Product Description

The P-GW is the node that terminates the SGi interface towards the PDN. If a UE is accessing multiple PDNs, there may be more than one P-GW for that UE. The P-GW provides connectivity to the UE to external packet data networks by being the point of exit and entry of traffic for the UE. A UE may have simultaneous connectivity with more than one P-GW for accessing multiple PDNs. The P-GW performs policy enforcement, packet filtering for each user, charging support, lawful interception and packet screening.

Figure 3: P-GW in the Basic E-UTRAN/EPC Network

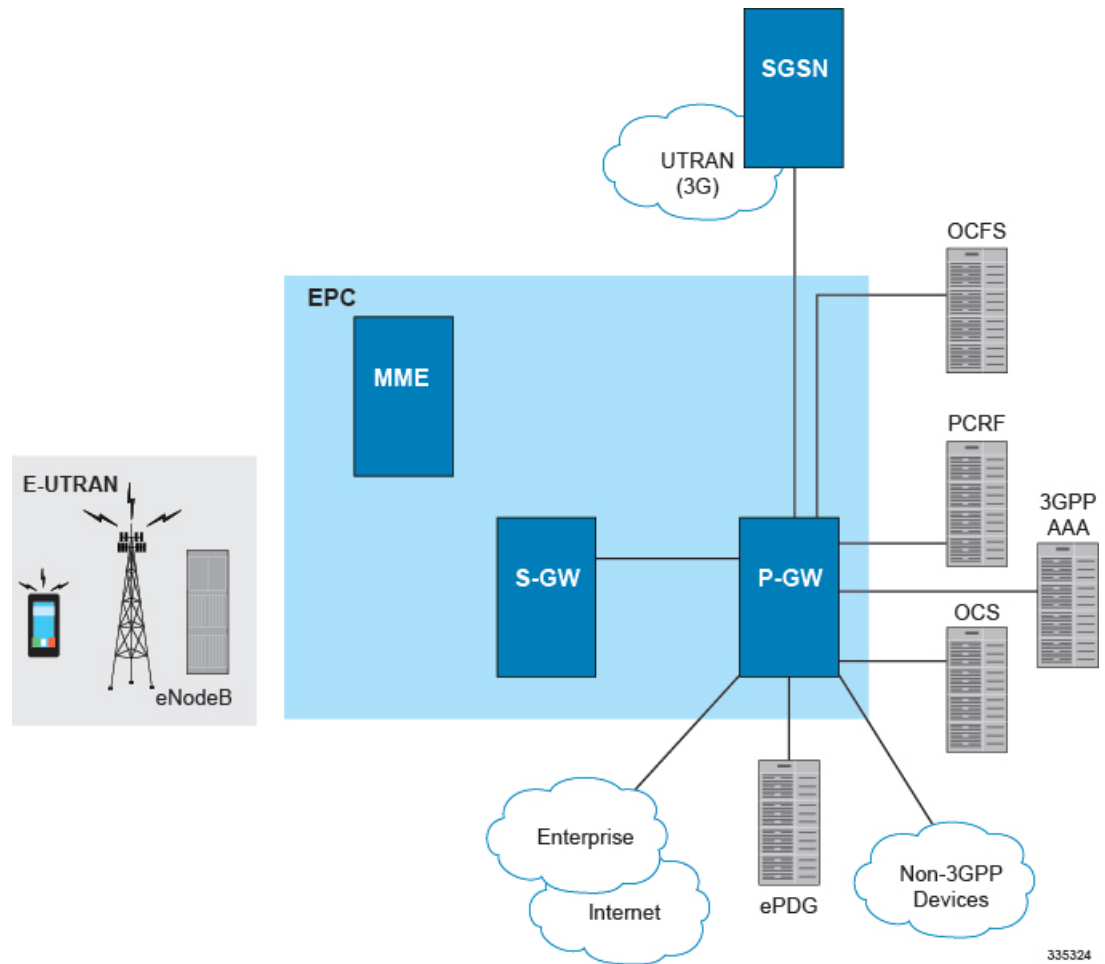
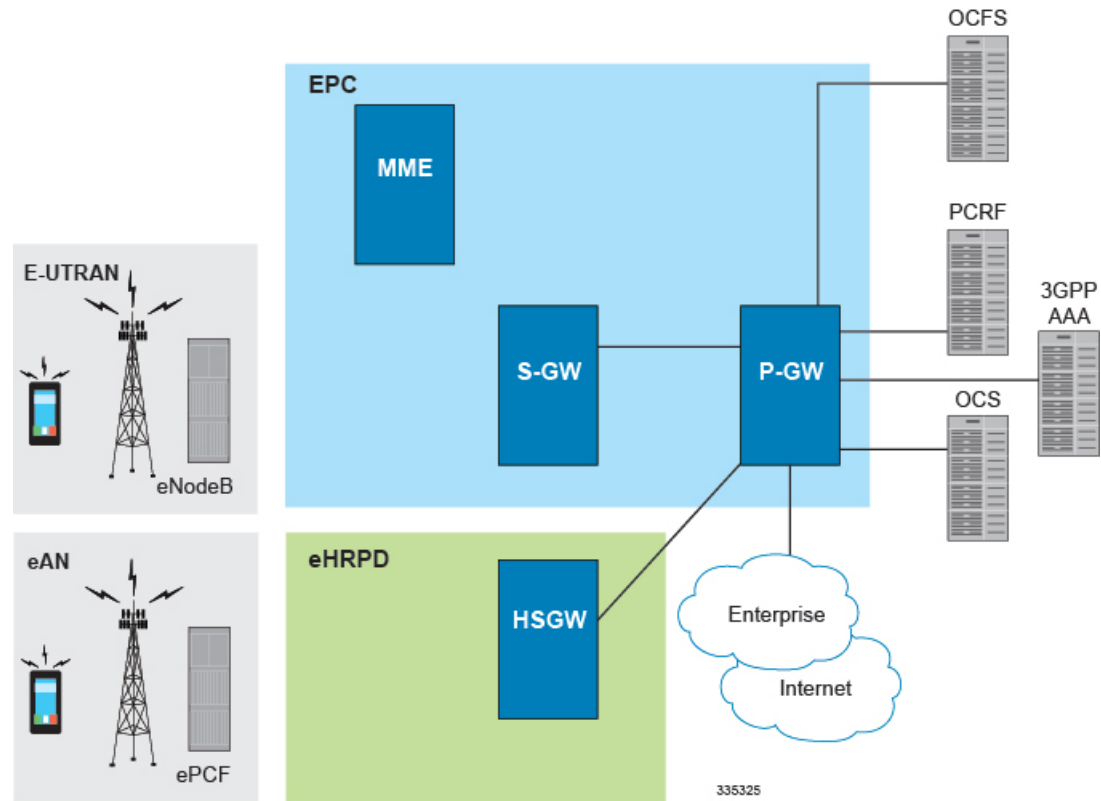


Figure 4: P-GW in the Basic E-UTRAN/EPC and eHRPD Network



Another key role of the P-GW is to act as the anchor for mobility between 3GPP and non-3GPP technologies such as WiMAX and 3GPP2 (CDMA 1X and EvDO).

P-GW functions include:

- Mobility anchor for mobility between 3GPP access systems and non-3GPP access systems. This is sometimes referred to as the SAE Anchor function.
- Policy enforcement (gating and rate enforcement)
- Per-user based packet filtering (deep packet inspection)
- Charging support
- Lawful Interception
- UE IP address allocation
- Packet screening
- Transport level packet marking in the downlink;
- Down link rate enforcement based on Aggregate Maximum Bit Rate (AMBR)

The following are additional P-GW functions when supporting non-3GPP access (eHRPD):

- P-GW includes the function of a Local Mobility Anchor (LMA) according to draft-ietf-netlmm-proxymip6, if PMIP-based S5 or S8 is used.

- The P-GW includes the function of a DSMIPv6 Home Agent, as described in draft-ietf-mip6-nemo-v4traversal, if S2c is used.

## Platform Requirements

The P-GW service runs on a Cisco® ASR 5500 chassis running StarOS. The chassis can be configured with a variety of components to meet specific network deployment requirements. For additional information, refer to the Installation Guide for the chassis and/or contact your Cisco account representative.

## Licenses

The P-GW is a licensed Cisco product covered by the SAEGW license when part of an SAEGW umbrella service. Separate session and feature licenses may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

## S-GW Network Deployment(s)

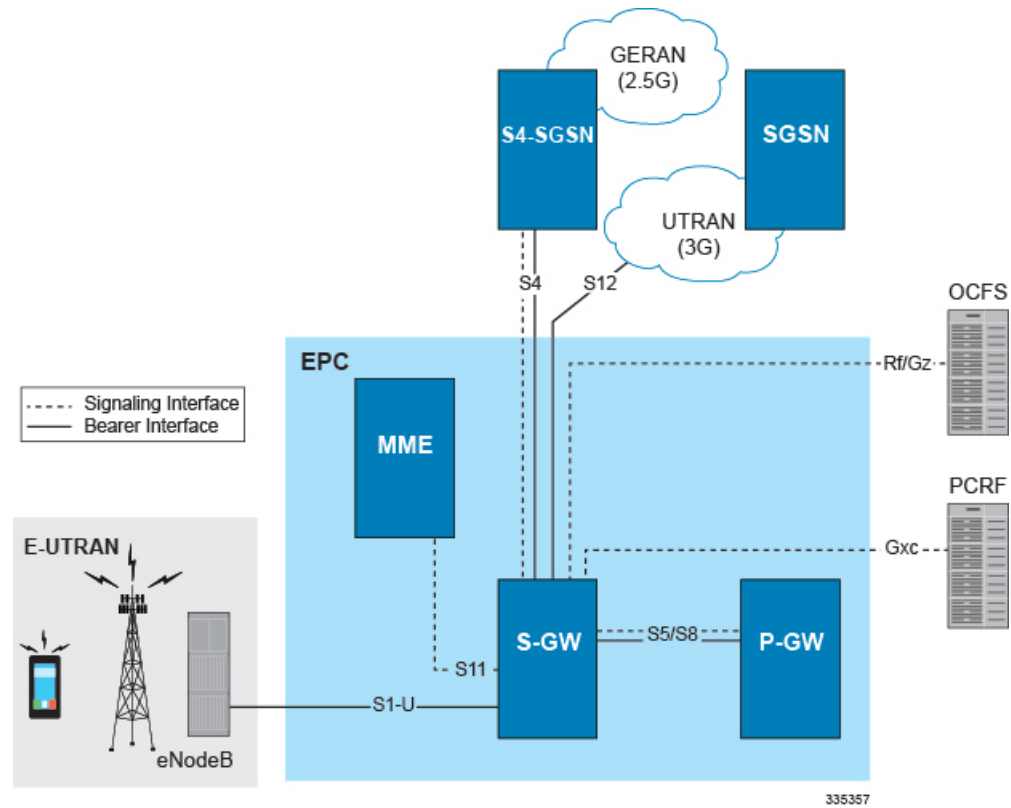
This section describes the supported interfaces and the deployment scenarios of a Serving Gateway.

## Serving Gateway in the E-UTRAN/EPC Network

The following figure displays the specific network interfaces supported by the S-GW. Refer to [Supported Logical Network Interfaces \(Reference Points\)](#), on page 10 for detailed information about each interface.



Figure 5: Supported S-GW Interfaces in the E-UTRAN/EPC Network



The following figure displays a sample network deployment of an S-GW, including all of the interface connections with other 3GPP Evolved-UTRAN/Evolved Packet Core network devices.

The diagram illustrates the 4G/LTE network architecture, centered around the Evolved Packet Core (EPC). The EPC contains the MME (Mobility Management Entity), S-GW (Serving Gateway), and P-GW (PDN Gateway). The EPC is connected to various external networks and devices through different interfaces.

- External Networks and Devices:**
  - GERAN (2.5G) and UTRAN (3G):** Connected to the EPC via S4 and S12 interfaces, respectively.
  - OCFS, HSS, PCRF, 3GPP AAA, OCS, and SWx:** These are part of the core network infrastructure, connected to the EPC via S6a, Gxc, Gx, S6b, and Gy interfaces.
  - Enterprise, Internet, ePDG, and Non-3GPP Devices:** These are external networks and devices connected to the EPC via SGi, S2b, and S2c interfaces.
- Internal EPC Components and Interfaces:**
  - MME:** The central control plane entity, connected to S-GW and P-GW via S11 and S1-MME interfaces.
  - S-GW:** The Serving Gateway, connected to P-GW via S5/S8 interface.
  - P-GW:** The PDN Gateway, connected to the external networks and devices.
- Other EPC Components:**
  - SGs/Sv:** Connected to the EPC via S13 interface.
  - MSC VLR and EIR:** These are legacy core network components connected to the EPC via S13 interface.
- Legend:**
  - Signaling Interface:** Represented by a dashed line.
  - Bearer Interface:** Represented by a solid line.

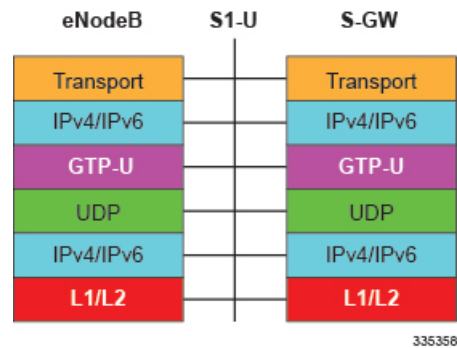
## S1-U Interface

This reference point provides bearer channel tunneling between the eNodeB and the S-GW. It also supports eNodeB path switching during handovers. The S-GW provides the local mobility anchor point for inter-eNodeB hand-overs. It provides inter-eNodeB path switching during hand-overs when the X2 handover interface between base stations cannot be used. The S1-U interface uses GPRS tunneling protocol for user plane (GTP-Uv1). GTP encapsulates all end user IP packets and it relies on UDP/IP transport. The S1-U interface also supports IPsec IKEv2. This interface is defined in 3GPP TS 23.401.

- Transport Layer: UDP, TCP
- Tunneling: IPv4 or IPv6 GTPv1-U (bearer channel)

- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

**Figure 7: Protocols Supported on the S1-U Interface**



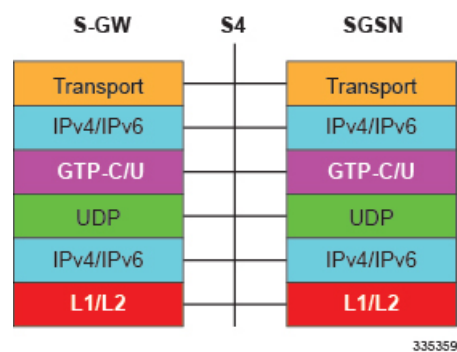
## S4 Interface

This reference point provides tunneling and management between the S-GW and a 3GPP S4 SGSN. The interface facilitates soft hand-offs with the EPC network by providing control and mobility support between the inter-3GPP anchor function of the S-GW. This interface is defined in 3GPP TS 23.401.

### Supported protocols:

- Transport Layer: UDP
- Tunneling:
  - GTP: IPv4 or IPv6 GTP-C (GTPv2 control/signaling channel) and GTP-U (GTPv1 user/bearer channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

**Figure 8: Protocols Supported on the S4 Interface**



## S5/S8 Interface

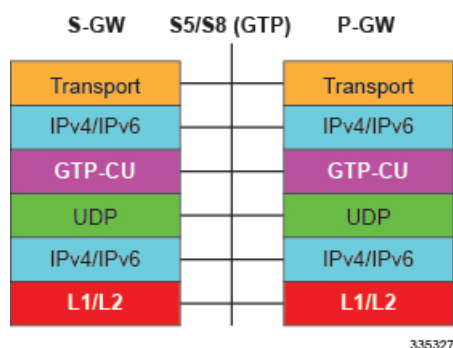
This reference point provides tunneling and management between the S-GW and the P-GW, as defined in 3GPP TS 23.401. The S8 interface is an inter-PLMN reference point between the S-GW and the P-GW used during roaming scenarios. The S5 interface is used between an S-GW and P-GW located within the same

administrative domain (non-roaming). It is used for S-GW relocation due to UE mobility and if the S-GW needs to connect to a non-located P-GW for the required PDN connectivity.

#### Supported protocols:

- Transport Layer: UDP, TCP
- Tunneling: GTP: GTPv2-C (signaling channel), GTPv1-U (bearer channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

**Figure 9: Supported Protocols on the S5/S8 Interface**



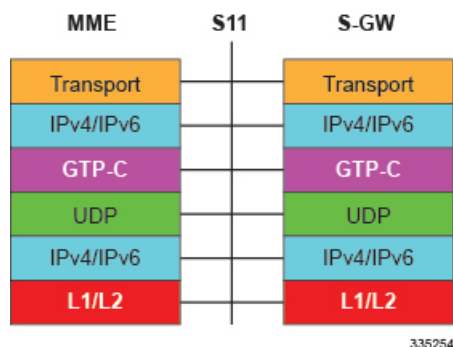
## S11 Interface

This reference point provides GTP-C control signal tunneling between the MME and the S-GW. One GTP-C tunnel is created for each mobile terminal between the MME and S-GW. This interface is defined in 3GPP TS 23.401.

#### Supported protocols:

- Transport Layer: UDP
- Tunneling: IPv4 or IPv6 GTPv2-C (signaling channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

**Figure 10: Supported Protocols on the S11 Interface**



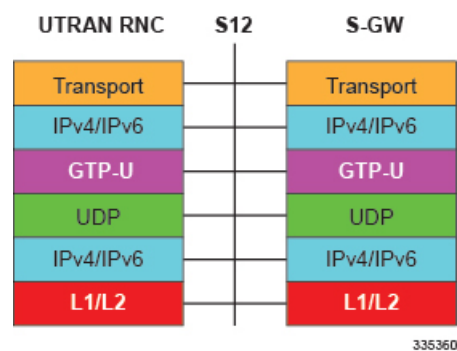
## S12 Interface

This reference point provides GTP-U bearer/user direct tunneling between the S-GW and a UTRAN Radio Network Controller (RNC), as defined in 3GPP TS 23.401. This interface provides support for inter-RAT handovers between the 3G RAN and EPC allowing a direct tunnel to be initiated between the RNC and S-GW, thus bypassing the S4 SGSN and reducing latency.

### Supported protocols:

- Transport Layer: UDP
- Tunneling: IPv4 or IPv6 GTP-U (GTPv1 bearer/user channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

**Figure 11: Supported Protocols on the S12 Interface**



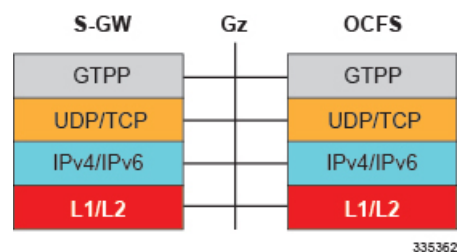
## Gz Interface

The Gz reference interface enables offline accounting functions on the S-GW. The S-GW collects charging information for each mobile subscriber UE pertaining to the radio network usage. The Gz interface and offline accounting functions are used primarily in roaming scenarios where the foreign P-GW does not support offline charging.

### Supported protocols:

- Transport Layer: TCP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

**Figure 12: Protocols Supported on the Gz Interface**



Rf Interface



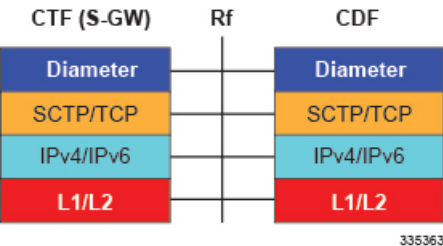
**Important** In StarOS releases 19 and later, the Rf interface is not supported on the S-GW.

The Diameter Rf interface (3GPP 32.240) is used for offline (post-paid) charging between the Charging Trigger Function (CTF, S-GW) and the Charging Data Function (CDF). It follows the Diameter base protocol state machine for accounting (RFC 3588) and includes support for IMS specific AVPs (3GPP TS 32.299)

**Supported protocols:**

- Transport Layer: TCP or SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

Figure 13: Protocols Supported on the Rf Interface



**Note** The Rf interface is not supported on the S-GW.

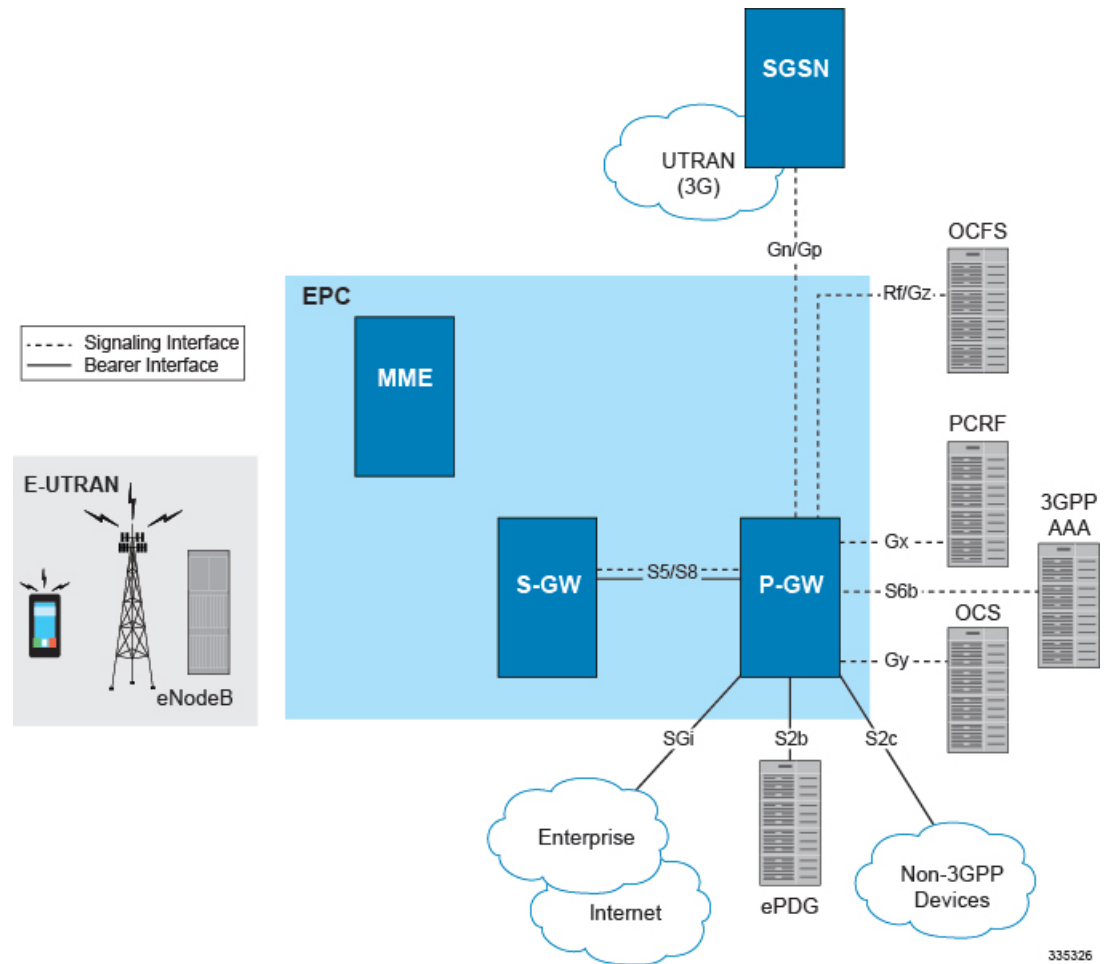
P-GW Network Deployment(s)

This section describes the supported interfaces and the deployment scenarios of a PDN Gateway.

PDN Gateway in the E-UTRAN/EPC Network

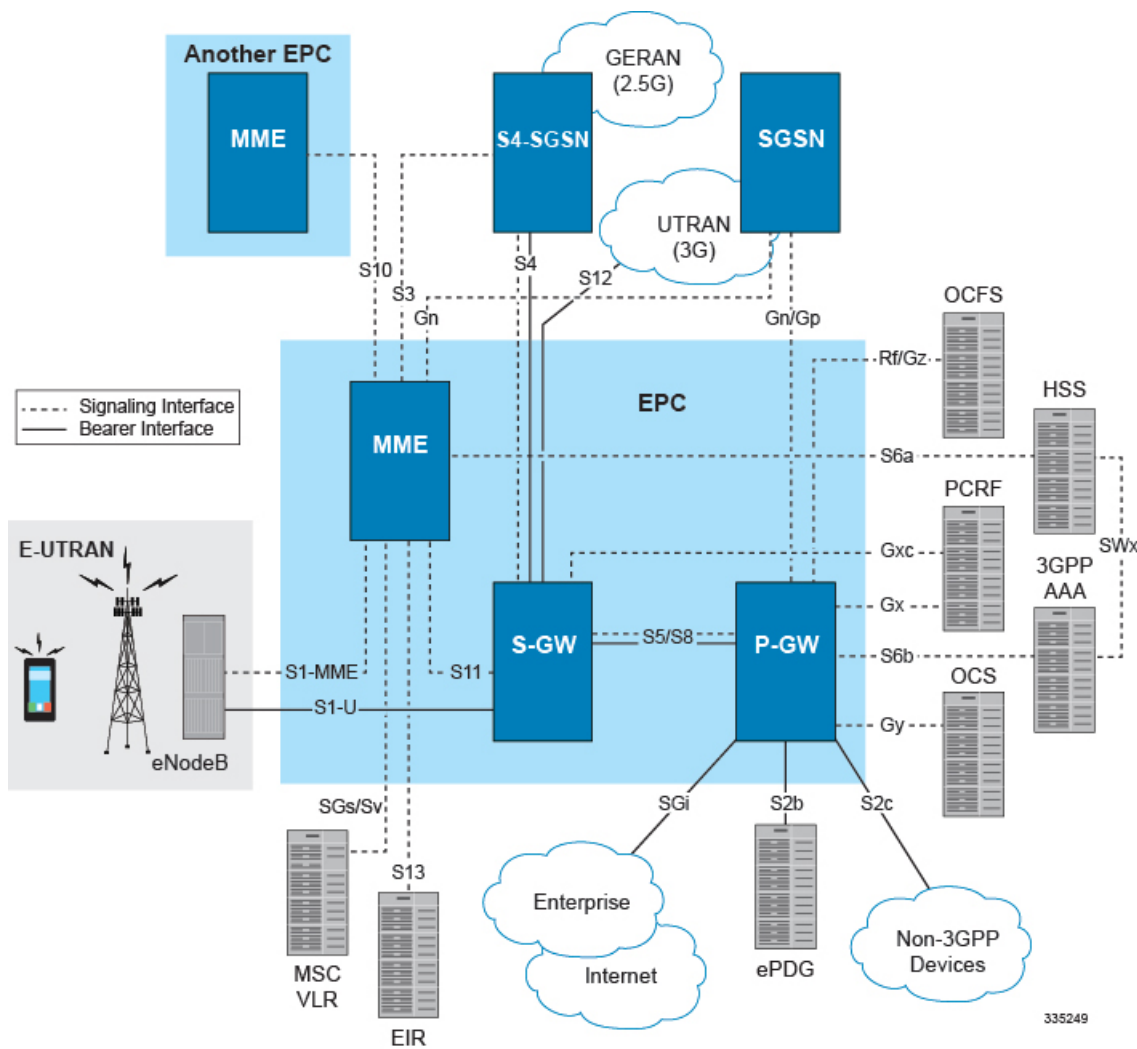
The following figure displays the specific network interfaces supported by the P-GW. Refer to [Supported Logical Network Interfaces \(Reference Points\)](#), on page 16 for detailed information about each interface.

Figure 14: Supported P-GW Interfaces in the E-UTRAN/EPC Network



The following figure displays a sample network deployment of a P-GW, including all of the interface connections with other 3GPP Evolved-UTRAN/Evolved Packet Core network devices.

Figure 15: P-GW in the E-UTRAN/EPC Network



## Supported Logical Network Interfaces (Reference Points)

The P-GW provides the following logical network interfaces in support of E-UTRAN/EPC network:

### S5/S8 Interface

This reference point provides tunneling and management between the S-GW and the P-GW, as defined in 3GPP TS 23.401 and TS 23.402. The S8 interface is an inter-PLMN reference point between the S-GW and the P-GW used during roaming scenarios. The S5 interface is used between an S-GW and P-GW located within the same administrative domain (non-roaming). It is used for S-GW relocation due to UE mobility and if the S-GW needs to connect to a non-collocated P-GW for the required PDN connectivity.

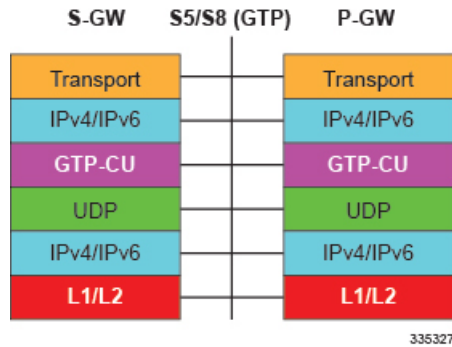
#### Supported protocols

- Transport Layer: UDP, TCP
- Tunneling:

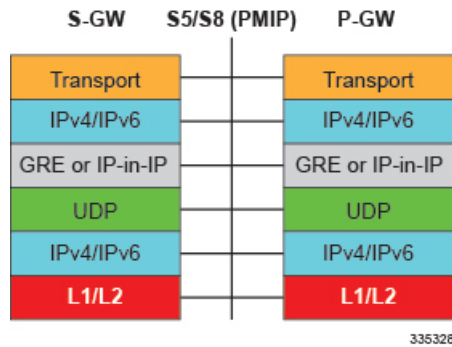


- GTP: GTPv2-C (signaling channel), GTPv1-U (bearer channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

**Figure 16: Supported GTP P-GW Protocols on the S5/S8 Interface**



**Figure 17: Supported PMIP P-GW Protocols on the S5/S8 Interface**



## S6b Interface

This reference point, between a P-GW and a 3GPP AAA server/proxy, is used for mobility-related authentication. It may also be used to retrieve and request parameters related to mobility and to retrieve static QoS profiles for UEs (for non-3GPP access) in the event that dynamic PCC is not supported.

The S6b interface is enhanced to pass on the UE assigned IPv6 address (IPv6 prefix and IPv6 interface ID) to the AAA server. S6b interface also has support for Framed-IPv6-Pool, Framed IP Pool, and served party IP address AVPs based IP allocation. With this support, based on the Pool name and APN name received from AAA server, the selection of a particular IP pool from the configuration is made for assigning the IP address.

The S6b interface on the P-GW or GGSN can be manually disabled to stop all message traffic to the 3GPP AAA during overload conditions. When the interface is disabled, the system uses locally configured APN-specific parameters including: Framed-Pool, Framed-IPv6-Pool, Idle-Timeout, Charging-Gateway-Function-Host, Server-Name (P-CSCF FQDN). This manual method is used when the HSS/3GPP AAA is in overload condition to allow the application to recover and mitigate the impact to subscribers.

The IPv6 address reporting through Authorization-Authentication-Request (AAR) towards the S6b interface is no longer a default feature. It is now configurable through the CLI.

Another enhancement on S6b interface support is the new S6b retry-and-continue functionality that creates an automatic trigger in the GGSN and P-GW to use the locally configured APN profile upon receipt of any uniquely defined Diameter error code on the S6b interface for an Authorization-Authentication-Request (AA-R) only. This procedure would be utilized in cases where a protocol, transient, or permanent error code is returned from the both the primary and secondary AAA to the GGSN or P-GW. In case of retry-and-continue functionality, P-GW should query from DNS server if it is configured in APN. S6b failure handling continues the data call. This behavior is only applicable to the aaa-custom15 Diameter dictionary.

P-GW supports receiving AVP "Restoration-Priority-Indicator" from AAA server over the S6b interface to distinguish between VoLTE enabled IMS PDN connections and non-VoLTE enabled IMS PDN connections. KPIs are also provided based on the AVP value.

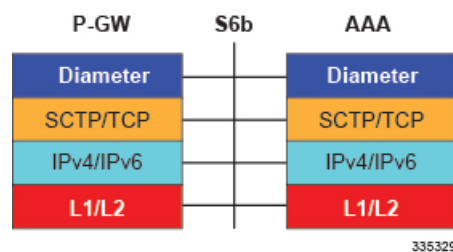


**Important** The S6b interface can be disabled via the CLI in the event of a long-term AAA outage.

#### Supported protocols:

- Transport Layer: TCP, SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

**Figure 18: Supported Protocols on the S6b Interface**

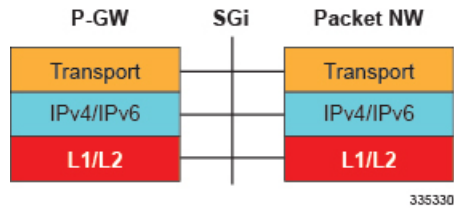


## SGi Interface

This reference point provides connectivity between the P-GW and a packet data network (3GPP TS 23.401). This interface can provide access to a variety of network types including an external public or private PDN and/or an internal IMS service provisioning network.

#### Supported protocols:

- Transport Layer: TCP, UDP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

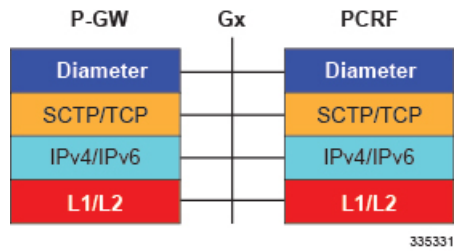
**Figure 19: Protocols Supported on the SGi Interface**

## Gx Interface

This signaling interface supports the transfer of policy control and charging rules information (QoS) between the Policy and Charging Enforcement Function (PCEF) on the P-GW and a Policy and Charging Rules Function (PCRF) server (3GPP TS 23.401).

### Supported protocols:

- Transport Layer: TCP, SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

**Figure 20: Protocols Supported on the Gx Interface**

For more information on the Gx interface, refer to the [Dynamic Policy Charging Control \(Gx Reference Interface\)](#), on page 66 in the *P-GW Features and Functionality - Base Software* section of this chapter.

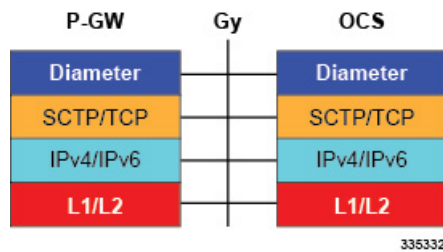
## Gy Interface

The Gy reference interface enables online accounting functions on the P-GW in accordance with 3GPP Release 8 and Release 9 specifications.

### Supported protocols:

- Transport Layer: TCP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

Figure 21: Protocols Supported on the Gy Interface



For more information on the Gy interface and online accounting, refer to [Gy Interface Support](#), on page 71 in the *P-GW Features and Functionality - Base Software* section of this chapter.

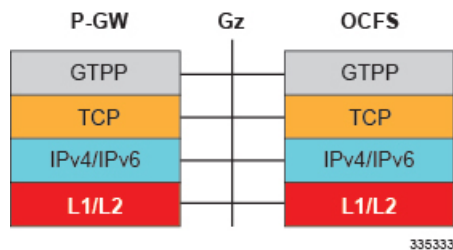
## Gz Interface

The Gz reference interface enables offline accounting functions on the P-GW. The P-GW collects charging information for each mobile subscriber UE pertaining to the radio network usage.

### Supported protocols:

- Transport Layer: TCP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

Figure 22: Protocols Supported on the Gz Interface

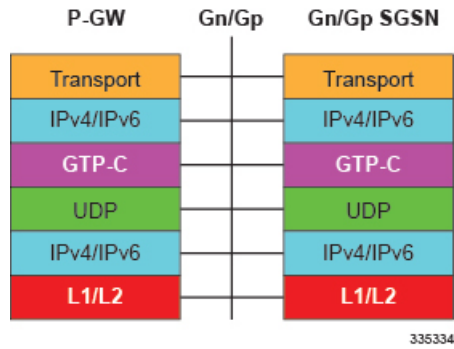


## Gn/Gp Interface

This reference point provides tunneling and management between the P-GW and the SGSN during handovers between the EPS and 3GPP 2G and/or 3G networks (3GPP TS 29.060). For more information on the Gn/Gp interface, refer to [Gn/Gp Handoff Support](#), on page 73 in the *P-GW Features and Functionality - Base Software* section of this chapter.

### Supported protocols

- Transport Layer: UDP, TCP
- Tunneling: GTP: GTP-C (signaling channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

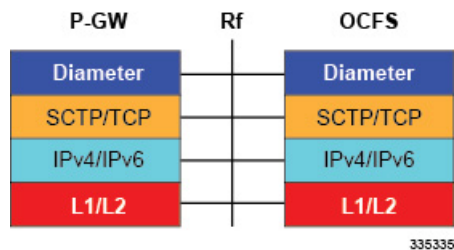
**Figure 23: Protocols Supported on the Gn/Gp Interface**

## Rf Interface

The Rf interface enables offline accounting functions on the P-GW in accordance with 3GPP Release 8 and Release 9 specifications. The P-GW collects charging information for each mobile subscriber UE pertaining to the radio network usage.

### Supported protocols:

- Transport Layer: TCP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

**Figure 24: Protocols Supported on the Rf Interface**

## PDN Gateway Supporting eHRPD to E-UTRAN/EPC Connectivity

The following figure displays the specific network interfaces supported by the P-GW in an eHRPD network. Refer to [Supported Logical Network Interfaces \(Reference Points\)](#), on page 25 for detailed information about each interface.

*Figure 25: P-GW Interfaces Supporting eHRPD to E-UTRAN/EPC Connectivity*

The following figure displays a sample network deployment of a P-GW in an eHRPD Network, including all of the interface connections with other 3GPP Evolved-UTRAN/Evolved Packet Core network devices.

*Figure 26: P-GW in the E-UTRAN/EPC Network Supporting the eHRPD Network*



## Supported Logical Network Interfaces (Reference Points)

The P-GW provides the following logical network interfaces in support of eHRPD to E-UTRAN/EPC connectivity:

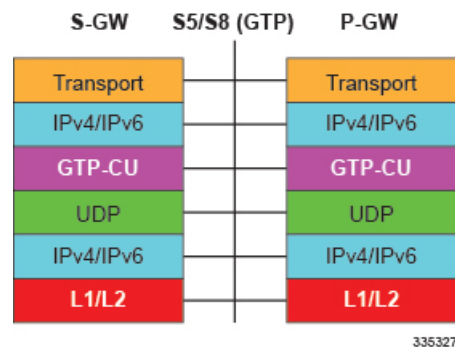
### S5/S8 Interface

This reference point provides tunneling and management between the S-GW and the P-GW, as defined in 3GPP TS 23.401. The S8 interface is an inter-PLMN reference point between the S-GW and the P-GW used during roaming scenarios. The S5 interface is used between an S-GW and P-GW located within the same administrative domain (non-roaming). It is used for S-GW relocation due to UE mobility and if the S-GW needs to connect to a non-collocated P-GW for the required PDN connectivity.

#### Supported protocols:

- Transport Layer: UDP, TCP
- Tunneling:
  - GTP: IPv4 or IPv6 GTP-C (signaling channel) and GTP-U (bearer channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

**Figure 27: Protocols Supported on the GTP P-GW S5/S8 Interface**



### S2a Interface

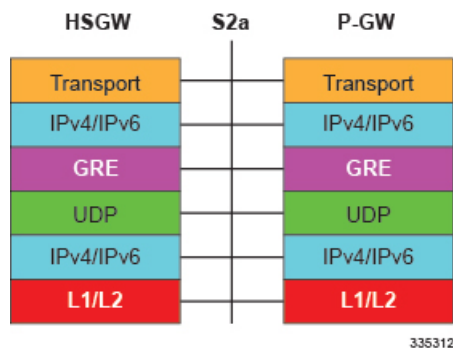
This reference point supports the bearer interface by providing signaling and mobility support between a trusted non-3GPP access point (HSGW) and the PDN Gateway. It is based on Proxy Mobile IP but also supports Client Mobile IPv4 FA mode which allows connectivity to trusted non-3GPP IP access points that do not support PMIP.

#### Supported protocols:

- Transport Layer: UDP, TCP
- Tunneling: GRE IPv6
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP

- Physical Layer: Ethernet

**Figure 28: Protocols Supported on the S2a Interface**



## S6b Interface

This reference point, between a P-GW and a 3GPP AAA server/proxy, is used for mobility-related authentication. It may also be used to retrieve and request parameters related to mobility and to retrieve static QoS profiles for UEs (for non-3GPP access) in the event that dynamic PCC is not supported.

From Release 12.2 onwards, the S6b interface has been enhanced to pass on the UE assigned IPv6 address (IPv6 prefix and IPv6 interface ID) to the AAA server. S6b interface also has support for Framed-IPv6-Pool, Framed IP Pool, and served party IP address AVPs based IP allocation. With this support, based on the Pool name and APN name received from AAA server, the selection of a particular IP pool from the configuration is made for assigning the IP address.

The S6b interface on the P-GW or GGSN can be manually disabled to stop all message traffic to the 3GPP AAA during overload conditions. When the interface is disabled, the system uses locally configured APN-specific parameters including: Framed-Pool, Framed-IPv6-Pool, Idle-Timeout, Charging-Gateway-Function-Host, Server-Name (P-CSCF FQDN). This manual method is used when the HSS/3GPP AAA is in overload condition to allow the application to recover and mitigate the impact to subscribers.

Release 12.3 onwards, the IPv6 address reporting through Authorization-Authentication-Request (AAR) towards the S6b interface is no longer a default feature. It is now configurable through the CLI.

Another enhancement on S6b interface support is the new S6b retry-and-continue functionality that creates an automatic trigger in the GGSN and P-GW to use the locally configured APN profile upon receipt of any uniquely defined Diameter error code on the S6b interface for an Authorization-Authentication-Request (AA-R) only. This procedure would be utilized in cases where a protocol, transient, or permanent error code is returned from the both the primary and secondary AAA to the GGSN or P-GW. In case of retry-and-continue functionality, P-GW should query from DNS server if it is configured in APN. S6b failure handling continues the data call. This behavior is only applicable to the aaa-custom15 Diameter dictionary.



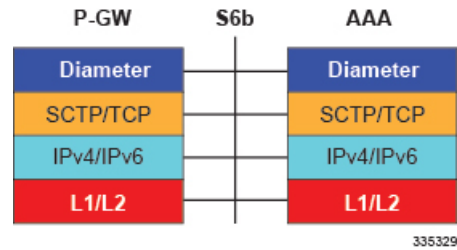
**Important** The S6b interface can be disabled via the CLI in the event of a long-term AAA outage.

### Supported protocols:

- Transport Layer: TCP, SCTP
- Network Layer: IPv4, IPv6

- Data Link Layer: ARP
- Physical Layer: Ethernet

**Figure 29: Protocols Supported on the S6b Interface**



## SGi Interface

This reference point provides connectivity between the P-GW and a packet data network. This interface can provide access to a variety of network types including an external public or private PDN and/or an internal IMS service provisioning network.

### Supported protocols:

- Transport Layer: TCP, UDP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

**Figure 30: Protocols Supported on the SGi Interface**

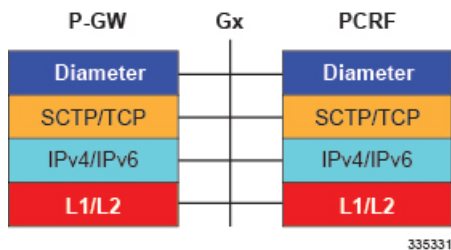


## Gx Interface

This signaling interface supports the transfer of policy control and charging rules information (QoS) between the Policy and Charging Enforcement Function (PCEF) on the P-GW and a Policy and Charging Rules Function (PCRF) server (3GPP TS 23.401).

### Supported protocols:

- Transport Layer: TCP, SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

**Figure 31: Protocols Supported on the Gx Interface**

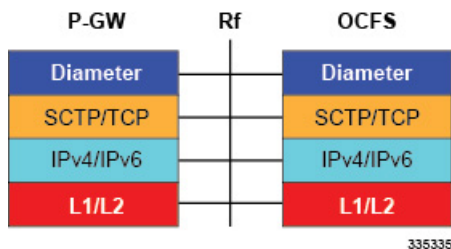
For more information on the Gx interface, refer to [Dynamic Policy Charging Control \(Gx Reference Interface\)](#), on page 66 in the *P-GW Features and Functionality - Base Software* section of this chapter.

## Rf Interface

The Rf reference interface enables offline accounting functions on the P-GW in accordance with 3GPP Release 8 and Release 9 specifications. The P-GW collects charging information for each mobile subscriber UE pertaining to the radio network usage.

### Supported protocols:

- Transport Layer: TCP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

**Figure 32: Protocols Supported on the Rf Interface**

For more information on Rf accounting, refer to [Rf Diameter Accounting](#), on page 50 in the *P-GW Features and Functionality - Base Software* section of this chapter.

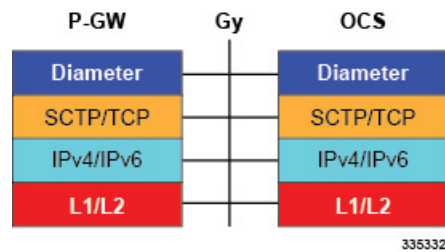
## Gy Interface

The Gy reference interface enables online accounting functions on the P-GW in accordance with 3GPP Release 8 and Release 9 specifications.

### Supported protocols:

- Transport Layer: TCP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

Figure 33: Protocols Supported on the Gy Interface



For more information on the Gy interface and online accounting, refer to [Gy Interface Support](#), on page 71 in the *P-GW Features and Functionality - Base Software* section of this chapter.

## S-GW Features and Functionality - Base Software



**Important** The SAEGW supports all of these features if an S-GW service is assigned to the SAEGW service.

This section describes the features and functions supported by default in the base software for the S-GW service and do not require any additional licenses to implement the functionality.

### 3GPP Release 12 Cause-Code IE Support

When an ERAB or a data session is dropped, an operator may need to get, beyond the ULI information, detailed RAN and/or NAS release cause codes information from the access network to be included in the S-GW and P-GW CDRs for call performance analysis, User QoE analysis and proper billing reconciliation. Also, for IMS sessions, the operator may need to get the above information available at P-CSCF.

'Per E-RAB Cause' is received in ERAB Release Command and ER AB Release Indication messages over S1. However RAN and NAS causes are not forwarded to the SGW and PGW, nor provided by the PGW to PCRF.

To resolve this issue a "RAN/NAS Release Cause" information element (IE), which indicates AS and/or NAS causes, has been added to the Session Deletion Request and Delete Bearer Command. The "RAN/NAS Release Cause" provided by the MME is transmitted transparently by the S-GW to the P-GW (if there exists signaling towards P-GW) for further propagation towards the PCRF.

For backward compatibility, the S-GW can still receive the cause code from the CC IE in the S4/S11 messages and/or receive the cause code from some customers' private extension.

### Abnormal Bearer Termination Cause in CDR

This feature provides additional information in a S-GW/P-GW CDR for a VoLTE call drop. A dropped bearer was previously reported as a 'abnormalrelease' in the CDR. This feature has the S-GW / P-GW CDRs indicate the proper bearer release for all failure cases identified in the VoLTE Retainability formula. This will provide the customer with the ability to perform gateway/network wide analysis for failures in the network.

New Disconnect reasons are added for GTPC/GTPU path failure and local purge GTPU error indications.

New field abnormalTerminationCause enum 83 is added in the S-GW CDR for a specific customer dictionary.

## ANSI T1.276 Compliance

ANSI T1.276 specifies security measures for Network Elements (NE). In particular it specifies guidelines for password strength, storage, and maintenance security measures.

ANSI T1.276 specifies several measures for password security. These measures include:

- Password strength guidelines
- Password storage guidelines for network elements
- Password maintenance, e.g. periodic forced password changes

These measures are applicable to the ASR 5500 Platform and an element management system since both require password authentication. A subset of these guidelines where applicable to each platform will be implemented. A known subset of guidelines, such as certificate authentication, are not applicable to either product. Furthermore, the platforms support a variety of authentication methods such as RADIUS and SSH which are dependent on external elements. ANSI T1.276 compliance in such cases will be the domain of the external element. ANSI T1.276 guidelines will only be implemented for locally configured operators.

## APN-level Traffic Policing

The S-GW now supports traffic policing for roaming scenarios where the foreign P-GW does not enforce traffic classes. Traffic policing is used to enforce bandwidth limitations on subscriber data traffic. It caps packet bursts and data rates at configured burst size and data rate limits respectively for given class of traffic.

Traffic Policing is based on RFC2698- A Two Rate Three Color Marker (trTCM) algorithm. The trTCM meters an IP packet stream and marks its packets green, yellow, or red. A packet is marked red if it exceeds the Peak Information Rate (PIR). Otherwise it is marked either yellow or green depending on whether it exceeds or doesn't exceed the Committed Information Rate (CIR). The trTCM is useful, for example, for ingress policing of a service, where a peak rate needs to be enforced separately from a committed rate.

## Backup and Recovery of Key KPI Statistics

Before the Backup and Recovery of Key KPI Statistics feature was implemented, statistics were not backed up and could not be recovered after a SessMgr task restart. Due to this limitation, monitoring the KPI was a problem as the GGSN, P-GW, SAEGW, and S-GW would lose statistical information whenever task restarts occurred.

KPI calculation involves taking a delta between counter values from two time intervals and then determines the percentage of successful processing of a particular procedure in that time interval. When a SessMgr crashes and then recovers, the GGSN, P-GW, SAEGW, and S-GW lose the counter values - they are reset to zero. So, the KPI calculation in the next interval will result in negative values for that interval. This results in a dip in the graphs plotted using the KPI values, making it difficult for operations team to get a consistent view of the network performance to determine if there is a genuine issue or not.

This feature makes it possible to perform reliable KPI calculations even if a SessMgr restart occurs.



---

**Important**

For more information on Backup and Recovery of Key KPI Statistics, refer to the *Backup and Recovery of Key KPI Statistics* chapter in this guide.

---

## Bulk Statistics Support

The system's support for bulk statistics allows operators to choose to view not only statistics that are of importance to them, but also to configure the format in which it is presented. This simplifies the post-processing of statistical data since it can be formatted to be parsed by external, back-end processors.

When used in conjunction with an element management system (EMS), the data can be parsed, archived, and graphed.

The system can be configured to collect bulk statistics (performance data) and send them to a collection server (called a receiver). Bulk statistics are statistics that are collected in a group. The individual statistics are grouped by schema. Following is a partial list of supported schemas:

- **System:** Provides system-level statistics
- **Card:** Provides card-level statistics
- **Port:** Provides port-level statistics
- **MAG:** Provides MAG service statistics
- **S-GW:** Provides S-GW node-level service statistics
- **IP Pool:** Provides IP pool statistics
- **APN:** Provides Access Point Name statistics

The system supports the configuration of up to four sets (primary/secondary) of receivers. Each set can be configured with to collect specific sets of statistics from the various schemas. Statistics can be pulled manually from the system or sent at configured intervals. The bulk statistics are stored on the receiver(s) in files.

The format of the bulk statistic data files can be configured by the user. Users can specify the format of the file name, file headers, and/or footers to include information such as the date, system host name, system uptime, the IP address of the system generating the statistics (available for only for headers and footers), and/or the time that the file was generated.

An EMS is capable of further processing the statistics data through XML parsing, archiving, and graphing.

The Bulk Statistics Server component of an EMS parses collected statistics and stores the information in its PostgreSQL database. It can also generate XML output and can send it to a Northbound NMS or an alternate bulk statistics server for further processing.

Additionally, the Bulk Statistics server can archive files to an alternative directory on the server. The directory can be on a local file system or on an NFS-mounted file system on an EMS server.



---

**Important**

For more information on bulk statistic configuration, refer to the *Configuring and Maintaining Bulk Statistics* chapter in the *System Administration Guide*.

---

## CDR Support for Including LAPI (Signaling Priority)

This feature is related to M2M support. 3GPP has added the LAPI (signaling priority) indication being sent in the GTP messages, to indicate that the PDN is a low priority bearer and thus can be treated accordingly. APN backoff timer support based on LAPI indication is not yet supported.

3GPP has also added a new AVP in CDR defined in TS 32.298 named "lowPriorityIndicator". If the S-GW receives the LAPI indicator in GTP, the SGW-CDR and generated will contain LAPI indication.

This benefit of this feature is that it provides support for carrying then LAPI attribute in SGW-CDR and PGW-CDR, so that billing system can then accordingly bill for that PDN.

## Circuit Switched Fall Back (CSFB) Support

Circuit Switched Fall Back (CSFB) enables the UE to camp on an EUTRAN cell and originate or terminate voice calls through a forced switchover to the circuit switched (CS) domain or other CS-domain services (for example, Location Services (LCS) or supplementary services). Additionally, SMS delivery via the CS core network is realized without CSFB. Since LTE EPC networks were not meant to directly anchor CS connections, when any CS voice services are initiated, any PS based data activities on the EUTRAN network will be temporarily suspended (either the data transfer is suspended or the packet switched connection is handed over to the 2G/3G network).

CSFB provides an interim solution for enabling telephony and SMS services for LTE operators that do not plan to deploy IMS packet switched services at initial service launch.

The S-GW supports CSFB messaging over the S11 interface over GTP-C. Supported messages are:

- Suspend Notification
- Suspend Acknowledge
- Resume Notification
- Resume Acknowledgment

The S-GW forwards Suspend Notification messages towards the P-GW to suspend downlink data for non-GBR traffic; the P-GW then drops all downlink packets. Later, when the UE finishes with CS services and moves back to E-UTRAN, the MME sends a Resume Notification message to the S-GW which forwards the message to the P-GW. The downlink data traffic then resumes.

## Closed Subscriber Group Support

The S-GW supports the following Closed Subscriber Group (CSG) Information Elements (IEs) and Call Detail Record:

- User CSG Information (UCI) IE in S5/S8
- CSG Information Reporting Action IE and functionality in S5/S8
- An SGW-CDR that includes a CSG record

## Collision Counter Support in the GTP Layer

GTPv2 message collisions occur in the network when a node is expecting a particular procedure message from a peer node but instead receives a different procedure message from the peer. The SAEGW software has been enhanced so that these collisions are now tracked by statistics and handled based on a pre-defined action for each message collision type.

If the SAEGW is configured as a pure P-GW or a pure S-GW, operators will still see the respective collision statistics if they occur.



The output of the **show egtpc statistics verbose** command has been enhanced to provide information on GTPv2 message collisions, including:

- **Interface:** The interface on which the collision occurred: SGW (S4/S11), SGW (S5), or PGW (S5).
- **Old Proc (Msg Type):** Indicates the ongoing procedure at eGTP-C when a new message arrived at the interface which caused the collision. The Msg Type in brackets specifies which message triggered this ongoing procedure.
- **New Proc (Msg Type):** The new procedure and message type.
- **Action:** The pre-defined action taken to handle the collision. The action can be one of:
  - **No Collision Detected**
  - **Suspend Old:** Suspend processing of the original (old) message, process the new message, then resume old message handling.
  - **Abort Old:** Abort the original message handling and processes the new message.
  - **Reject New:** The new message is rejected, and the original (old) message is processed.
  - **Silent Drop New:** Drop the new incoming message, and the old message is processed.
  - **Parallel Hndl:** Both the original (old) and new messages are handled in parallel.
  - **Buffer New:** The new message is buffered and processed once the original (old) message processing is done.
- **Counter:** The number of times each collision type has occurred.



**Important** The Message Collision Statistics section of the command output only appears if any of the collision statistics have a counter total that is greater than zero.

#### Sample output:

```

Message Collision Statistics
  Interface      Old Proc (Msg Type)      New Proc (Msg Type)      Action
Counter
  SGW(S5)      NW Init Bearer Create (95)  NW Init PDN Delete (99)  Abort Old      1

```

In this instance, the output states that at the S-GW egress interface (S5) a Bearer creation procedure is going on due to a CREATE BEARER REQUEST(95) message from the P-GW. Before its response comes to the S-GW from the MME, a new procedure PDN Delete is triggered due to a DELETE BEARER REQUEST(99) message from the P-GW.

The action that is carried out due to this collision at eGTP-C is to abort (Abort Old) the Bearer Creation procedure and carry on normally with the PDN Delete procedure. The Counter total of 1 indicates that this collision happened only once.

## Congestion Control

The congestion control feature allows you to set policies and thresholds and specify how the system reacts when faced with a heavy load condition.

Congestion control monitors the system for conditions that could potentially degrade performance when the system is under heavy load. Typically, these conditions are temporary (for example, high CPU or memory utilization) and are quickly resolved. However, continuous or large numbers of these conditions within a specific time interval may have an impact the system's ability to service subscriber sessions. Congestion control helps identify such conditions and invokes policies for addressing the situation.

Congestion control operation is based on configuring the following:

- **Congestion Condition Thresholds:** Thresholds dictate the conditions for which congestion control is enabled and establish limits for defining the state of the system (congested or clear). These thresholds function in a way similar to operational thresholds that are configured for the system as described in the *Thresholding Configuration Guide*. The primary difference is that when congestion thresholds are reached, a service congestion policy and an SNMP trap, starCongestion, are generated.

A threshold tolerance dictates the percentage under the configured threshold that must be reached in order for the condition to be cleared. An SNMP trap, starCongestionClear, is then triggered.

- **Port Utilization Thresholds:** If you set a port utilization threshold, when the average utilization of all ports in the system reaches the specified threshold, congestion control is enabled.
- **Port-specific Thresholds:** If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is enabled system-wide.
- **Service Congestion Policies:** Congestion policies are configurable for each service. These policies dictate how services respond when the system detects that a congestion condition threshold has been crossed.



#### Important

For more information on congestion control, refer to the *Congestion Control* chapter in the *System Administration Guide*.

## Dedicated Bearer Timeout Support on the S-GW

The SAE-GW has been enhanced to support a bearer inactivity timeout for GBR and non-GBR S-GW bearer type sessions per QoS Class Identifier (QCI). This enables the deletion of bearers experiencing less data traffic than the configured threshold value. Operators now can configure a bearer inactivity timeout for GBR and non-GBR bearers for more efficient use of system resources.

## Downlink Delay Notification

This feature is divided between the following:

- Value Handling
- Throttling
- EPS Bearer ID and ARP Support

### Value Handling

This feature provides for the handling of delay value information elements (IEs) at the S-GW. When a delay value is received at the S-GW from a particular MME, the S-GW delays sending data notification requests for all idle calls belonging to that particular MME. Once the timer expires, requests can be sent. The delay value at the S-GW is determined by the factor received in the delay value IE (as a part of either a Modify Bearer Request or a Data Downlink Notification Request) and a hard-coded base factor of 50 ms at the S-GW.

## Throttling

This feature provides additional controls allowing the S-GW to set factors that "throttle" the continuous sending and receiving of DDN messages. A single command configures the throttling parameters supporting this feature,

A description of the **ddn throttle** command is located in the S-GW Service Configuration Mode Commands chapter in the *Command Line Interface Reference*.

## EPS Bearer ID and ARP Support

This feature allows support for Priority Paging support in the network. This is mainly needed for MPS subscriber support. The paging priority in the paging message is set by MME based on ARP received in Downlink Data Notification message.

In order to support MPS requirement for Priority Paging in the network for MPS subscriber, DDN message has been enhanced to support passing ARP and EBI information. When the S-GW sends a Downlink Data Notification message, it shall include both EPS Bearer ID and ARP. If the Downlink Data Notification is triggered by the arrival of downlink data packets at the S-GW, the S-GW shall include the EPS Bearer ID and ARP associated with the bearer on which the downlink data packet was received. If the Downlink Data Notification is triggered by the arrival of control signaling, the S-GW shall include the EPS Bearer ID and ARP, if present in the control signaling. If the ARP is not present in the control signaling, the S-GW shall include the ARP in the stored EPS bearer context. If multiple EPS Bearers IDs are reported in the Downlink Data Notification message, the S-GW shall include all the EBI values and the ARP associated with the bearer with the highest priority (lowest ARP value). For more information, see TS 23.401 (section 5.3.4.3) and 29.274 (section 7.2.11). Details are discussed in CR-859 of 3GPP specifications.

## DSCP Ingress and Egress and DSCP Marking at the APN Profile

This feature provides operators with a configuration to set the DSCP value per APN profile, so different APNs can have different DSCP markings as per QOS requirements for traffic carried by the APN. In addition, the **qci-qos mapping** table is updated with the addition of a **copy-outer** for copying the DSCP value coming in the encapsulation header from the S1u interface to the S5 interface and vice-versa.

## Dynamic GTP Echo Timer

The Dynamic GTP Echo Timer enables the eGTP and GTP-U services to better manage GTP paths during network congestion. As opposed to the default echo timer which uses fixed intervals and retransmission timers, the dynamic echo timer adds a calculated round trip timer (RTT) that is generated once a full request/response procedure has completed. A multiplier can be added to the calculation for additional support during congestion periods.

## Event Reporting

The S-GW can be configured to send a stream of user event data to an external server. As users attach, detach, and move throughout the network, they trigger signaling events, which are recorded and sent to an external server for processing. Reported data includes failure reasons, nodes selected, user information (IMSI, IMEI, MSISDN), APN, failure codes (if any) and other information on a per PDN-connection level. Event data is used to track the user status via near real time monitoring tools and for historical analysis of major network events.

The *S-GW Event Reporting* chapter in this guide describes the trigger mechanisms and event record elements used for event reporting.

The SGW sends each event record in comma separated values (CSV) format. The record for each event is sent to the external server within 60 seconds of its occurrence. The **session-event-module** command in the Context Configuration mode allows an operator to set the method and destination for transferring event files, as well as the format and handling characteristics of event files. For a detailed description of this command, refer to the *Command Line Interface Reference*.

## GTP-C Path Failure Enhancements and Improved Debugging Tools

In StarOS release 20.0, 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.

The following enhancements are added as 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.

### Support to Avoid False Path Failure Detection

Several enhancements have been made to facilitate the node's ability to avoid false path failure detection:

- The software has been enhanced to avoid path failure detection due to spurious/incorrect messages from a peer. These messages can cause a large burst in network traffic due to the number of service deactivations and activations, resulting in network congestion. The **gtpc** command in *eGTP-C Service Configuration Mode* has been enhanced to resolve this issue. The **max-remote-restart-counter-change** keyword has been added to ensure false path failure detections are not detected as GTP-C path failures. For example, if the **max-remote-restart-counter-change** is set to 10 and the current peer restart counter is 251, eGTP will detect a peer restart only if the new restart counter is 252 through 255 or 0 through 5. Similarly, if the stored restart counter is 1, eGTP will detect a peer restart only if the new restart counter is 2 through 11.
- Also as part of this enhancement, new keywords have been added to the **path-failure detection-policy** command in *eGTP-C Service Configuration Mode* to enable or disable path failure detection.
- The **show egtp-service all** command in Exec Mode has been enhanced to indicate whether Echo Request/Echo Response Restart Counter Change and Control Message Restart Counter Change are enabled/disabled on the node.

### Improved GTP-C Path Failure Statistics

Several improvements have been made to improve the quality of the GTP-C path failures so that operators/engineers can more quickly identify the cause of the failure.

- The output of the **show egtpc statistics path-failure-reasons** has been enhanced to show the number and type of control message restart counter changes at the demuxmgr and sessmgr. This command output has also been enhanced to track the number of path failures detected that were ignored at the eGTP-C layer.
- The **show egtpc peers path-failure-history** command output has been added to provide detailed information on the last five path failures per peer.
- The output of the **show egtpc-service all name** and **show configuration** commands has been enhanced to show the current configuration settings specific to path GTP-C path failure detection policy.

## Idle-mode Signaling Reduction Support

The S-GW supports Idle-mode Signaling Reduction (ISR) allowing for a control connection to exist between an S-GW and an MME and S4-SGSN. The S-GW stores mobility management parameters from both nodes while the UE stores session management contexts for both the EUTRAN and GERAN/UTRAN. This allows a UE, in idle mode, to move between the two network types without needing to perform racking area update procedures, thus reducing the signaling previously required. ISR support on the S-GW is embedded and no configuration is required however, an optional feature license is required to enable this feature.

ISR support on the S-GW is embedded and no configuration is required, however, an optional feature license must be purchased to enable this feature.

## IMSI/IMEI Available in System Event Logs of Type Error and Critical

The GGSN/P-GW/SAEGW/S-GW can be configured to provide the IMSI/IMEI in the event log details for the following system event logs of type error and critical, if available.



#### Important

Note that the GGSN/P-GW/SAEGW/S-GW will make a best effort attempt to include the IMSI/IMEI in system event logs of type error and critical. However, there still may be cases where the IMSI is not seen which are not mentioned in the following table.

**Table 1: New and Modified System Event Logs with IMSI/IMEI in System Event Log Details**

Event Log #	Description
<b>New Events</b>	
12225	Represents misc_error3 in format "[IMSI <IMSI>] Misc Error3: %s, error code %d"
12226	Represents recover_call_from_crr_failed1 error in format "[IMSI <IMSI>]Sessmgr-%d Recover call from CRR failed for callid:0x%x reason=%s"
12227	Represents aaa_create_session_failed_no_more_sessions1 error in format "[IMSI <IMSI>] Sessmgr-%d Ran out of session handles"

Event Log #	Description
140075	Represents error_log1 in format "[IMSI <IMSI>]%s"
<b>Modified Events</b>	
139001	To print miscellaneous PGW error log.
191006	To print miscellaneous SAEGW error log.
10034	Represents FSM error in format "[IMSI <IMSI>] default call fsm error: ostate=%s(%d) state=%s(%d) event=%s(%d)"
10035	Represents FSM INVALID event in format "[IMSI <IMSI>] default call fsm invalid event: state=%s(%d) event=%s(%d)"
12382	Represents SN_LE_SESSMGR_PGW_REJECT_BEARER_OP in format "[IMSI <IMSI>] Sessmgr-%d: Request to %s bearer rejected. Reason: %s". For example "[IMSI 112233445566778 Sessmgr-1: Request to Create bearer rejected. Reason: Create Bearer Request denied as session recovery is in progress"
12668	Represents fsm_event_error in format "[IMSI <IMSI>] Misc Error: Bad event in sessmgr fsm, event code %d"
12774	Represents pgw_purge_invalid_err in format "[IMSI <IMSI>] Local %s TEID [%lu] Collision: Clp Connect Time: %lu, Old Clp Callid: %d, Old Clp Connect Time: %lu %s"
12855	Represents ncqos_nrspca_trig_err in format "[IMSI <IMSI>] NCQOS NRSPCA trig rcvd in invalid bcm mode."
12857	Represents ncqos_nrupc_tft_err in format "[IMSI <IMSI>] NCQOS NRUPC Trig : TFT validation failed for nsapi <%u>."
12858	Represents ncqos_nrxx_trig_already in format "[IMSI <IMSI>] NCQOS NRSPCA/NRUPC is already triggered on sess with nsapi <%u>."
12859	Represents ncqos_nrxx_tft_check_fail in format "[IMSI <IMSI>] NCQOS TFT check failed as TFT has invalid opcode for nsapi <%u>:pf_id_bitmap 0x%x and tft_opcode: %d"
12860	Represents ncqos_sec_rej in format "[IMSI <IMSI>] NCQOS Secondary ctxt with nsapi <%u> rejected, due to <%s>."
12861	Represents ncqos_upc_rej in format "[IMSI <IMSI>] UPC Rejected for ctxt with nsapi <%u>, due to <%s>."
12862	Represents ggsn_subsession_invalid_state in format "[IMSI <IMSI>] GGSN subsession invalid state state:<%s>,[event:<%s>]"
11830	Represents gngp_handoff_rejected_for_pdn_ipv4v6 in format "[IMSI <IMSI>] Sessmgr-%d Handoff from PGW-to-GGSN rejected, as GGSN doesn't support Deferred allocation for IPv4v6, dropping the call."

Event Log #	Description
11832	Represents gngp_handoff_rejected_no_non_gbr_bearer_for_def_bearer_selection in format "[IMSI <IMSI>] Sessmgr-%d Handoff from PGW-to-GGSN rejected, as GGSN Callline has no non-GBR bearer to be selected as Default bearer."
11834	Represents gngp_handoff_from_ggsn_rejected_no_ggsn_call in format "[IMSI <IMSI>] Sessmgr-%d Handoff from GGSN-to-PGW rejected, as GGSN call with TEIDC <0x%x> not found."
12960	Represents gtp_pdp_type_mismatch in format "[IMSI <IMSI>] Mismatch between PDP type of APN %s and in create req. Rejecting call"
11282	Represents pcc_intf_error_info in format "[IMSI <IMSI>] %s"
11293	Represents collision_error in format "[IMSI <IMSI>] Collision Error: Temp Failure Handling Delayed Pending Active Transaction: , error code %d"
11917	Represents rcvd_invalid_bearer_binding_req_from_acs in format "[IMSI <IMSI>] Sessmgr %d: Received invalid bearer binding request from ACS."
11978	Represents saegw_uid_error in format "[IMSI <IMSI>] %s"
11994	Represents unwanted_pcc_intf_setup_req error in format "[IMSI <IMSI>] GGSN_INITIATE_SESS_SETUP_REQ is already fwded to PCC interface "
140005	Represents ue_fsm_illegal_event in format "[IMSI <IMSI>] Invalid/unhandled UE event <%s> in state <%s>"
140006	Represents pdn_fsm_illegal_event in format "[IMSI <IMSI>] Invalid/unhandled PDN event <%s> in state <%s>"
140007	Represents epsb_fsm_illegal_event in format "[IMSI <IMSI>] Invalid/unhandled EPSB event <%s> in state <%s>"
10726	Represents saegwdrv_generic_error "[IMSI <IMSI>] %s"

The **include-ueid** keyword has been added to the **logging** command in *Global Configuration Mode*. When enabled, the previously mentioned system events of type error and critical will provide the IMSI/IMEI in the logging details, if available.

## IP Access Control Lists

IP access control lists allow you to set up rules that control the flow of packets into and out of the system based on a variety of IP packet parameters.

IP access lists, or Access Control Lists (ACLs) as they are commonly referred to, control the flow of packets into and out of the system. They are configured on a per-context basis and consist of "rules" (ACL rules) or filters that control the action taken on packets that match the filter criteria. Once configured, an ACL can be applied to any of the following:

- An individual interface
- All traffic facilitated by a context (known as a policy ACL)

- An individual subscriber
- All subscriber sessions facilitated by a specific context



**Important** The S-GW supports interface-based ACLs only. For more information on IP access control lists, refer to the *IP Access Control Lists* chapter in the *System Administration Guide*.

## IPv6 Capabilities

IPv6 enables increased address efficiency and relieves pressures caused by rapidly approaching IPv4 address exhaustion problem.

The S-GW platform offers the following IPv6 capabilities:

### IPv6 Connections to Attached Elements

IPv6 transport and interfaces are supported on all of the following connections:

- Diameter Gxc policy signaling interface
- Diameter Rf offline charging interface
- Lawful Intercept (X1, X2 interfaces)

### Routing and Miscellaneous Features

- OSPFv3
- MP-BGP v6 extensions
- IPv6 flows (Supported on all Diameter QoS and Charging interfaces as well as Inline Services (for example, ECS, P2P detection, Stateful Firewall, etc.)

## LIPA Support

A LIPA (Local IP Access) PDN is a PDN Connection for local IP access for a UE connected to a HeNB. The LIPA architecture includes a Local Gateway (LGW) acting as an S-GW GTPv2 peer. The LGW is collocated with HeNB in the operator network behaves as a PGW from SGW perspective. Once the default bearer for the LIPA PDN is established, then data flows directly to the LGW and from there into the local network without traversing the core network of the network operator.

In order to support millions of LIPA GTPC peers, S-GW memory management has been enhanced with regards to GTPv2 procedures and as well as to support the maintenance of statistics per peer node.

Establishment of LIPA PDN follows a normal call flow similar to that of a normal PDN as per 23.401; the specification does not distinguish between a LGW and a PGW call. As a result, the S-GW supports a new configuration option to detect a LIPA peer. As a fallback mechanism, heuristic detection of LIPA peer based on data flow characteristics of a LIPA call is also supported.

Whenever a peer is detected as a LIPA peer, the S-GW will disable GTPC echo mechanism towards that particular peer and stop maintaining some statistics for that peer.



A configuration option in APN profile explicitly indicates that all the PDN's for that APN are LIPA PDN's, so all GTPC peers on S5 for that APN are treated as LGW, and thus no any detection algorithm is applied to detect LGW.

## Location Reporting

Location reporting can be used to support a variety of applications including emergency calls, lawful intercept, and charging. This feature reports both user location information (ULI).

ULI data reported in GTPv2 messages includes:

- **TAI-ID:** Tracking Area Identity
- **MCC: MNC:** Mobile Country Code, Mobile Network Code
- **TAC:** Tracking Area Code

The S-GW stores the ULI and also reports the information to the accounting framework. This may lead to generation of Gz and Rf Interim records. The S-GW also forwards the received ULI to the P-GW. If the S-GW receives the UE time zone IE from the MME, it forwards this IE towards the P-GW across the S5/S8 interface.

## Mapping High Throughput Sessions on Session Managers

Session managers are upgraded to manage several high throughput sessions without sharing the core and without creating a bottleneck on the CPU load.

The gateway – S-GW, SAEGW or P-GW, classifies a session as a high throughput session based on a DCNR flag present in the IE: FLAGS FOR USER PLANE FUNCTION (UPF) SELECTION INDICATION, in the Create Session Request. This DCNR flag is checkpointed and recovered by the gateway.

A high throughput session is placed on a session manager that has no other high throughput session. If all session manager are handling a high throughput session then these sessions are allocated using the Round-Robbin method.



### Note

- The selection of session managers for non-high throughput sessions remains the same in the existing setup.
- Non-high throughput sessions are placed along with the high throughput sessions on the same session manager.

### Limitations

Managing high throughput sessions on a session manager has the following limitations:

- The following scenarios may result in placing two high throughput sessions on a session manager:
  - Initial attach from eHRPD/2G/3G sessions.
  - IP addresses – both IPv4 and IPv6, are placed on the same session manager.
  - For an S-GW, the second Create Session Request (PDN) from a UE lands directly on a session manager which has the first PDN of the same UE.

- For a collapsed call, the second Create Session Request (PDN) from a UE lands directly on a session manager which has the first PDN of the same UE.
- In a Multi-PDN call from a UE that is capable of DCNR. For example: VoLTE and Internet capable of DCN will be placed on the same session manager.
- The DCNR flag is not defined by 3GPP for Wi-Fi. Therefore, a session cannot be assigned to a session manager during a Wi-Fi to LTE handover with the DCNR flag set.
- This feature manages and supports distribution of high throughput sessions on a session manager but does not guarantee high throughput for a subscriber.
- In some cases, the round robin mechanism could place a high throughput session on a session manager that was already loaded with other high throughput sessions.

## MME Restoration Support

MME restoration is a 3GPP specification-based feature designed to gracefully handle the sessions at S-GW once S-GW detects that the MME has failed or restarted. If the S-GW detects an MME failure based on a different restart counter in the Recovery IE in any GTP Signaling message or Echo Request / Response, it will terminate sessions and not maintain any PDN connections.

### MME Restoration Standards Extension

The solution to recover from MME node failures proposed in the 3GPP standards rely on the deployment of MME pools where each pool services a coverage area. Following an MME failure, the S-GW and MSC/VLR nodes may select the same MME that used to service a UE, if it has restarted, or an alternate MME in the same pool to process Network-initiated signaling that it received in accordance with the NTSR procedures defined in 3GPP TS 23.007 Release 11.

For a failed MME, the S-GW will select an alternate MME from the associated NTSR pool in the round robin fashion in each sessmgr instance.

## S-GW NTSR Enhancement

CDETS=CSCuv99767 - [SGW] NTSR Enhancement

Applicable Products: S-GW

## Multiple PDN Support

Enables an APN-based user experience that enables separate connections to be allocated for different services including IMS, Internet, walled garden services, or offdeck content services.

The Mobile Access Gateway (MAG) function on the S-GW can maintain multiple PDN or APN connections for the same user session. The MAG runs a single node level Proxy Mobile IPv6 (PMIP) tunnel for all user sessions toward the Local Mobility Anchor (LMA) function of the P-GW.

When a user wants to establish multiple PDN connections, the MAG brings up the multiple PDN connections over the same PMIPv6 session to one or more P-GW LMAs. The P-GW in turn allocates separate IP addresses (Home Network Prefixes) for each PDN connection and each one can run one or multiple EPC default and dedicated bearers. To request the various PDN connections, the MAG includes a common MN-ID and separate Home Network Prefixes, APNs and a Handover Indication Value equal to one in the PMIPv6 Binding Updates.



---

**Important** Up to 11 multiple PDN connections are supported.

---

## Node Functionality GTP Echo

This feature helps exchange capabilities of two communicating GTP nodes, and uses the feature based on whether it is supported by the other node.

This feature allows S-GW to exchange its capabilities (MABR, PRN, NTSR) with the peer entities through ECHO messages. By this, if both the peer nodes support some common features, then they can make use of new messages to communicate with each other.

With new "node features" IE support in ECHO request/response message, each node can send its supported features (MABR, PRN, NTSR). This way, S-GW can learn the peer node's supported features. S-GW's supported features can be configured by having some configuration at the service level.

If S-GW wants to use new message, such as P-GW Restart Notification, then S-GW should check if the peer node supports this new feature or not. If the peer does not support it, then S-GW should fall back to old behavior.

If S-GW receives a new message from the peer node, and if S-GW does not support this new message, then S-GW should ignore it. If S-GW supports the particular feature, then it should handle the new message as per the specification.

## Online/Offline Charging

The Cisco EPC platforms support offline charging interactions with external OCS and CGF/CDF servers. To provide subscriber level accounting, the Cisco EPC platform supports integrated Charging Transfer Function (CTF) and Charging Data Function (CDF) / Charging Gateway Function (CGF). Each gateway uses Charging-IDs to distinguish between default and dedicated bearers within subscriber sessions.

The ASR 5500 platform offers a local directory to enable temporary file storage and buffer charging records in persistent memory located on a pair of dual redundant RAID hard disks. Each drive includes 147GB of storage and up to 100GB of capacity is dedicated to storing charging records. For increased efficiency it also possible to enable file compression using protocols such as GZIP.

The offline charging implementation offers built-in heart beat monitoring of adjacent CGFs. If the Cisco P-GW has not heard from the neighboring CGF within the configurable polling interval, it will automatically buffer the charging records on the local drives until the CGF reactivates itself and is able to begin pulling the cached charging records.



---

**Note** Online Charging is not supported on the S-GW.

---

## Online: Gy Reference Interface

The P-GW supports a Policy Charging Enforcement Function (PCEF) to enable Flow Based Bearer Charging (FBC) via the Gy reference interface to adjunct Online Charging System (OCS) servers. The Gy interface provides a standardized Diameter interface for real-time content-based charging of data services. It is based on the 3GPP standards and relies on quota allocation. The Gy interface provides an online charging interface

that works with the ECS Deep Packet Inspection feature. With Gy, customer traffic can be gated and billed. Both time- and volume-based charging models are supported.

## Offline: Gz Reference Interface

The Cisco P-GW and S-GW support 3GPP Release 8 compliant offline charging as defined in TS 32.251, TS 32.297 and 32.298. Whereas the S-GW generates SGW-CDRs to record subscriber level access to PLMN resources, the P-GW creates PGW-CDRs to record user access to external networks. Additionally when Gn/Gp interworking with SGSNs is enabled, the GGSN service on the P-GW records G-CDRs to record user access to external networks.

To provide subscriber level accounting, the Cisco S-GW supports integrated Charging Transfer Function (CTF) and Charging Data Function (CDF). Each gateway uses Charging-IDs to distinguish between default and dedicated bearers within subscriber sessions.

The Gz reference interface between the CDF and CGF is used to transfer charging records via the GTPP protocol. In a standards based implementation, the CGF consolidates the charging records and transfers them via an FTP or SFTP connection over the Bm reference interface to a back-end billing mediation server. The Cisco EPC gateways also offer the ability to transfer charging records between the CDF and CGF serve via FTP or SFTP. CDR records include information such as Record Type, Served IMSI, ChargingID, APN Name, TimeStamp, Call Duration, Served MSISDN, PLMN-ID, etc.

## Offline: Rf Reference Interface



**Important** Offline Charging via the RF Reference Interface is not supported in StarOS releases 19 and later.

Cisco EPC platforms also support the Rf reference interface to enable direct transfer of charging files from the CTF function of the S-GW to external CDF or CGF servers. This interface uses Diameter Accounting Requests (Start, Stop, Interim, and Event) to transfer charging records to the CDF/CGF. Each gateway relies on triggering conditions for reporting chargeable events to the CDF/CGF. Typically as EPS bearers are activated, modified or deleted, charging records are generated. The EPC platforms include information such as Subscription-ID (IMSI), Charging-ID (EPS bearer identifier) and separate volume counts for the uplink and downlink traffic.

## Operator Policy Support

The operator policy provides mechanisms to fine tune the behavior of subsets of subscribers above and beyond the behaviors described in the user profile. It also can be used to control the behavior of visiting subscribers in roaming scenarios, enforcing roaming agreements and providing a measure of local protection against foreign subscribers.

An operator policy associates APNs, APN profiles, an APN remap table, and a call-control profile to ranges of IMSIs. These profiles and tables are created and defined within their own configuration modes to generate sets of rules and instructions that can be reused and assigned to multiple policies. In this manner, an operator policy manages the application of rules governing the services, facilities, and privileges available to subscribers. These policies can override standard behaviors and provide mechanisms for an operator to get around the limitations of other infrastructure elements, such as DNS servers and HSSs.

The operator policy configuration to be applied to a subscriber is selected on the basis of the selection criteria in the subscriber mapping at attach time. A maximum of 1,024 operator policies can be configured. If a UE

was associated with a specific operator policy and that policy is deleted, the next time the UE attempts to access the policy, it will attempt to find another policy with which to be associated.

A default operator policy can be configured and applied to all subscribers that do not match any of the per-PLMN or IMSI range policies.

The S-GW uses operator policy to set the Accounting Mode - GTPP (default), RADIUS/Diameter or none. However, the accounting mode configured for the call-control profile will override this setting.

Changes to the operator policy take effect when the subscriber re-attaches and subsequent EPS Bearer activations.

## Optimization for egtpinmgr Recovery

Restarting the egtpinmgr task took a significant amount of time for recovery. Hence, the outage time when the GGSN, P-GW, SAEGW, and S-GW were unable to accept any new calls during egtpinmgr recovery was high.

The software is 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.

## Peer GTP Node Profile Configuration Support

Provides flexibility to the operators to have different configuration for GTP-C and Lawful Intercept, based on the type of peer or the IP address of the peer.

Peer profile feature allows flexible profile based configuration to accommodate growing requirements of customizable parameters with default values and actions for peer nodes of S-GW. With this feature, configuration of GTP-C parameters and disabling/enabling of Lawful Intercept per MCC/MNC or IP address based on rules defined.

A new framework of peer-profile and peer-map is introduced. Peer-profile configuration captures the GTP-C specific configuration and/or Lawful Intercept enable/disable configuration. GTP-C configuration covers GTP-C retransmission (maximum number of retries and retransmission timeout) and GTP echo configuration. Peer-map configuration matches the peer-profile to be applied to a particular criteria. Peer-map supports criteria like MCC/MNC (PLMN-ID) of the peer or IP-address of the peer. Peer-map can then be associated with S-GW service.

Intent of this feature is to provide flexibility to operators to configure a profile which can be applied to a specific set of peers. For example, have a different retransmission timeout for foreign peers as compared to home peers.

## P-GW Restart Notification Support

This procedure optimizes the amount of signaling involved on the S11/S4 interface when a P-GW failure is detected.

P-GW Restart Notification Procedure is a standards-based procedure supported on S-GW to notify detection of P-GW failure to MME/S4-SGSN. P-GW failure detection will be done at S-GW when it detects that the P-GW has restarted (based on restart counter received from the restarted P-GW) or when it detects that P-GW has failed but not restarted (based on path failure detection). When an S-GW detects that a peer P-GW has

restarted, it shall locally delete all PDN connection table data and bearer contexts associated with the failed P-GW and notify the MME via P-GW Restart Notification. S-GW will indicate in the echo request/response on S11/S4 interface that the P-GW Restart Notification procedure is supported.

P-GW Restart Notification Procedure is an optional procedure and is invoked only if both the peers, MME/S4-SGSN and S-GW, support it. This procedure optimizes the amount of signaling involved on S11/S4 interface when P-GW failure is detected. In the absence of this procedure, S-GW will initiate the Delete procedure to clean up all the PDNs anchored at that failed P-GW, which can lead to flooding of GTP messages on S11/S4 if there are multiple PDNs using that S-GW and P-GW.

## QoS Bearer Management

Provides a foundation for contributing towards improved Quality of User Experience (QoE) by enabling deterministic end-to-end forwarding and scheduling treatments for different services or classes of applications pursuant to their requirements for committed bandwidth resources, jitter and delay. In this way, each application receives the service treatment that users expect.

An EPS bearer is a logical aggregate of one or more Service Data Flows (SDFs), running between a UE and a P-GW in case of GTP-based S5/S8, and between a UE and HSGW in case of PMIP-based S2a connection. An EPS bearer is the level of granularity for bearer level QoS control in the EPC/E-UTRAN. The Cisco P-GW maintains one or more Traffic Flow Templates (TFTs) in the downlink direction for mapping inbound Service Data Flows (SDFs) to EPS bearers. The P-GW maps the traffic based on the downlink TFT to the S5/S8 bearer. The Cisco P-GW offers all of the following bearer-level aggregate constructs:

**QoS Class Identifier (QCI):** An operator provisioned value that controls bearer level packet forwarding treatments (for example, scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc). Cisco EPC gateways also support the ability to map the QCI values to DiffServ codepoints in the outer GTP tunnel header of the S5/S8 connection. Additionally, the platform also provides configurable parameters to copy the DSCP marking from the encapsulated payload to the outer GTP tunnel header.




---

**Important** The SAEGW does not support non-standard QCI values. QCI values 1 through 9 are standard values defined in 3GPP TS 23.203; the SAEGW supports these standard values.

---

**Guaranteed Bit Rate (GBR):** A GBR bearer is associated with a dedicated EPS bearer and provides a guaranteed minimum transmission rate in order to offer constant bit rate services for applications such as interactive voice that require deterministic low delay service treatment.

**Maximum Bit Rate (MBR):** The MBR attribute provides a configurable burst rate that limits the bit rate that can be expected to be provided by a GBR bearer (e.g. excess traffic may get discarded by a rate shaping function). The MBR may be greater than or equal to the GBR for a given dedicated EPS bearer.

**Aggregate Maximum Bit Rate (AMBR):** AMBR denotes a bit rate of traffic for a group of bearers destined for a particular PDN. The Aggregate Maximum Bit Rate is typically assigned to a group of Best Effort service data flows over the Default EPS bearer. That is, each of those EPS bearers could potentially utilize the entire AMBR, e.g. when the other EPS bearers do not carry any traffic. The AMBR limits the aggregate bit rate that can be expected to be provided by the EPS bearers sharing the AMBR (e.g. excess traffic may get discarded by a rate shaping function). AMBR applies to all Non-GBR bearers belonging to the same PDN connection. GBR bearers are outside the scope of AMBR.

**Policing:** The Cisco P-GW offers a variety of traffic conditioning and bandwidth management capabilities. These tools enable usage controls to be applied on a per-subscriber, per-EPS bearer or per-PDN/APN basis.

It is also possible to apply bandwidth controls on a per-APN AMBR capacity. These applications provide the ability to inspect and maintain state for user sessions or Service Data Flows (SDFs) within them using shallow L3/L4 analysis or high touch deep packet inspection at L7. Metering of out-of-profile flows or sessions can result in packet discards or reducing the DSCP marking to Best Effort priority.

## Removal of Private Extension-based Overcharging Feature

Prior to StarOS release 21.0, the Cisco P-GW and S-GW supported the sending and receiving of overcharging protection data via both a non-3GPP Private Extension Information Element (IE), and a 3GPP Indication IE.

However, since 3GPP support to exchange overcharging protection data exists, no operators were using the Overcharging Private Extension (OCP) based solution. It was also reported by some operators that the Private Extension IE carrying overcharging protection data sent by the P-GW was leading to issues at S-GWs of other vendors.

As a result, support for Private Extension-based Overcharging Support is being removed from the Cisco P-GW and S-GW. This has the benefit of preventing unexpected scenarios occurring due to the decoding of a Private Extension ID carrying overcharging protection data at the P-GW/S-GW of other vendors.

### Previous and New Behavior for the P-GW

The following table describes the previous and new behavior at the P-GW for Create Session Request (CSReq) and Create Session Response (CSRsp) messages due to the removal of Private Extension Overcharging Support.

**Table 2: Previous and New Behavior: CSReq and CSRsp Messages at P-GW Due to Removal of Private Extension Overcharging Support**

Scenario No.	IE Carrying OCP Capability Received from S-GW in CSReq	Old Behavior: IE carrying OCP Capability Sent to S-GW in CSRsp	New Behavior: IE Carrying OCP Capability Sent to S-GW in CSRsp
1	Indication IE	Indication IE	No change. Indication IE will be sent in CSRsp.
2	Private Extension IE	Both Private Extension and Indication IEs.	Private Extension IE received from S-GW is ignored. Indication IE is sent in CSRsp.
3	None	Both Private Extension and Indication IEs.	Only Indication IE is sent in CSRsp.
4	Both Private Extension and Indication IEs.	Indication IE	Private Extension IE received from S-GW is ignored. Only Indication IE is sent in CSRsp.

The following table describes the previous and new behavior in Modify Bearer Request (MBReq) and Modify Bearer Response (MBRsp) messages due to the removal of Private Extension Overcharging Support.

**Table 3: Previous and New Behavior: MBRreq and MBRsp Messages at P-GW Due to Removal of Private Extension Overcharging Support**

Scenario No.	IE carrying OCP Capability Received from S-GW in MBRreq	Old Behavior: IE Carrying OCP Capability Sent to S-GW in MBRsp	New Behavior: IE Carrying OCP Capability Sent to S-GW in MBRsp
1	Indication IE	Indication IE	No Change. Indication IE is sent in MBRsp messages.
2	Private Extension IE	Private Extension IE	Private Extension IE received from S-GW is ignored. Indication IE is sent in MBRsp message.
3	None	Both Private Extension and Indication IEs.	Only the Indication IE is sent in MBRsp message.
4	Both Private Extension and Indication IEs.	Indication IE	Private Extension IE received from the S-GW is ignored. Only the Indication IE is sent in the MBRsp message.

**Previous and New Behavior for the S-GW**

The following table describes the previous and new behavior in Create Session Response (CSRsp) messages at the S-GW due to the removal of Private Extension Overcharging Support.

**Table 4: Previous and New Behavior: CSRsp Messages at the S-GW Due to the Removal of Private Extension Overcharging Support**

Scenario No.	Old Behavior: IE Carrying OCP Capability Received from P-GW in CSRsp	New Behavior: IE Carrying OCP Capability Received from PGW in CSRsp	Old Behavior: IE Carrying OCP Capability Sent to MME in CSRsp	New Behavior: IE Carrying OCP Capability Sent to MME in CSRsp
12	Indication IE	No change. OCP capability received as part of the Indication IE is accepted.	Indication IE	No change. Indication IE is sent in CSRsp.
2	Private Extension IE	OCP capability received as part of Private Extension IE is ignored.	If gtpc private-extension overcharge-protection is disabled at egtpc service level: <b>Private Extension IE</b> .  If gtpc private-extension overcharge-protection is enabled at egtpc service level: <b>Indication IE</b> .	Since the CLI command is deprecated, then the Private Extension IE is forwarded to the MME in CSRsp as would be done for any unknown Private Extension IE.



Scenario No.	Old Behavior: IE Carrying OCP Capability Received from P-GW in CSRsp	New Behavior: IE Carrying OCP Capability Received from PGW in CSRsp	Old Behavior: IE Carrying OCP Capability Sent to MME in CSRsp	New Behavior: IE Carrying OCP Capability Sent to MME in CSRsp
3	Both Private Extension IE and Indication IE	OCP capability received as part of the Private Extension IE is ignored. Only OCP capability received as a part of the Indication IE is accepted.	If gtpc private-extension overcharge-protection is disabled at egtpc service level: <b>Private Extension IE and Indication IE</b> . If gtpc private-extension overcharge-protection is enabled at egtpc service level: <b>Indication IE</b> .	Since the CLI command is deprecated, then the Private Extension IE is forwarded to the MME in CSRsp as would be done for any unknown Private Extension IE.
4	None	No change.	None	No change.

The following table describes the previous and new behavior in Modify Bearer Response (MBRsp) messages at the S-GW due to the removal of Private Extension Overcharging Support.

**Table 5: Previous Behavior and New Behavior: MBRsp Messages at the S-GW Due to the Removal of Private Extension Overcharging Support**

Scenario No.	Old Behavior: IE Carrying OCP Capability Received from P-GW in MBRsp	New Behavior: IE Carrying OCP Capability Received from P-GW in MBRsp	Old Behavior: IE Carrying OCP Capability Sent to MME in MBRsp	New Behavior: IE Carrying OCP Capability Sent to MME in MBRsp
1	Indication IE	No change. OCP capability received as part of Indication IE is accepted.	Indication IE	No change. Indication IE is sent in MBRsp.
2	Private Extension IE	OCP capability received as part of Private Extension IE is ignored.	If gtpc private-extension overcharge-protection is disabled at egtpc service level: <b>None</b> . If gtpc private-extension overcharge-protection is enabled at egtpc service level: <b>Indication IE</b> .	Since the CLI command is deprecated, neither one of the two IEs is sent in the MBRsp to the MME for the OCP capability.
3	Both Private Extension ID and Indication IE	OCP capability received as part of the Private Extension IE is ignored. Only the OCP capability received as part of the Indication IE is accepted.	Indication IE	No change. Indication IE is sent in MBRsp.

Scenario No.	Old Behavior: IE Carrying OCP Capability Received from P-GW in MBRsp	New Behavior: IE Carrying OCP Capability Received from P-GW in MBRsp	Old Behavior: IE Carrying OCP Capability Sent to MME in MBRsp	New Behavior: IE Carrying OCP Capability Sent to MME in MBRsp
4	None	None	None	No change.



**Important** In the current release, the S-GW will send a MBReq message with only the indication IE for the Pause/Start Charging procedure. The private extension IE is not sent.



**Important** If the S-GW receives only the private extension IE from the P-GW in the CSRsp/MBRsp message, then the S-GW ignores the private extension IE. As a result, the S-GW assumes that Overcharging Protection is NOT enabled for the P-GW. So, in this scenario, even if the overcharging condition is met at the S-GW, the S-GW will not send a MBReq message for Charging pause to the P-GW.

## Rf Diameter Accounting



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

Provides the framework for offline charging in a packet switched domain. The gateway support nodes use the Rf interface to convey session related, bearer related or service specific charging records to the CGF and billing domain for enabling charging plans.

The Rf reference interface enables offline accounting functions on the HSGW in accordance with 3GPP Release 8 specifications. In an LTE application the same reference interface is also supported on the S-GW and P-GW platforms. The Cisco gateways use the Charging Trigger Function (CTF) to transfer offline accounting records via a Diameter interface to an adjunct Charging Data Function (CDF) / Charging Gateway Function (CGF). The HSGW and Serving Gateway collect charging information for each mobile subscriber UE pertaining to the radio network usage while the P-GW collects charging information for each mobile subscriber related to the external data network usage.

The S-GW collects information per-user, per IP CAN bearer or per service. Bearer charging is used to collect charging information related to data volumes sent to and received from the UE and categorized by QoS traffic class. Users can be identified by MSISDN or IMSI.

Flow Data Records (FDRs) are used to correlate application charging data with EPC bearer usage information. The FDRs contain application level charging information like service identifiers, rating groups, IMS charging identifiers that can be used to identify the application. The FDRs also contain the authorized QoS information (QCI) that was assigned to a given flow. This information is used correlate charging records with EPC bearers.

## S-GW Collision Handling

GTPv2 message collisions occur in the network when a node is expecting a particular procedure message from a peer node but instead receives a different procedure message from the peer. The S-GW has been enhanced to process collisions at the S-GW ingress interface for:

1. Create Bearer Request or Update Bearer Request messages with Inter-MME/Inter-RAT Modify Bearer Request messages (with and without a ULI change).
2. Downlink Data Notification(DDN) message with Create Bearer Request or Update Bearer Request.

An UBReq and MBReq [(Inter MME/Inter RAT (with or without a ULI change))] collision at the SGW ingress interface is handled with a suspend and resume procedure. The UBReq would be suspended and the MBReq would be processed. Once the MBRsp is sent to the peer from the SGW ingress interface, the UBReq procedure is resumed.

An UBReq and MBReq [(Inter MME/Inter RAT (with or without a ULI change))] collision at the SGW ingress interface is handled with a suspend and resume procedure. The UBReq would be suspended and the MBReq would be processed. Once the MBRsp is sent to the peer from the SGW ingress interface, the UBReq procedure is resumed.

The Downlink Data Notification (DDN) message transaction is dis-associated from bearers. So Create Bearer Request (CBR) or Update Bearer Request (UBR) with Downlink Data Notification (DDN) messages are handled parallel.

No S-GW initiated Cause Code message 110 (Temporarily rejected due to handover procedure in progress) will be seen as a part of such collisions. Collisions will be handled in parallel.

## Viewing S-GW Collision Handling Statistics

The output of the **show egtp statistics verbose** command has been enhanced to provide information on GTPv2 message collisions at the S-GW ingress interface, including:

- **Interface:** The interface on which the collision occurred: SGW (S4/S11), SGW (S5).
- **Old Proc (Msg Type):** Indicates the ongoing procedure at eGTP-C when a new message arrived at the interface which caused the collision. The Msg Type in brackets specifies which message triggered this ongoing procedure.
- **New Proc (Msg Type):** The new procedure and message type.
- **Action:** The pre-defined action taken to handle the collision. The action can be one of:
  - **No Collision Detected**
  - **Suspend Old:** Suspend processing of the original (old) message, process the new message, then resume old message handling.
  - **Abort Old:** Abort the original message handling and processes the new message.
  - **Reject New:** The new message is rejected, and the original (old) message is processed.
  - **Silent Drop New:** Drop the new incoming message, and the old message is processed.
  - **Parallel Hndl:** Both the original (old) and new messages are handled in parallel.
  - **Buffer New:** The new message is buffered and processed once the original (old) message processing is done.
- **Counter:** The number of times each collision type has occurred.

**Important**

The *Message Collision Statistics* section of the command output appears only if any of the collision statistics have a counter total that is greater than zero.

For more information on this feature, refer to the *Collision Handling on the P-GW/SAEGW/S-GW* chapter in this document.

## S-GW Session Idle Timer

A session idle timer has been implemented on the S-GW to remove stale session in those cases where the session is removed on the other nodes but due to some issue remains on the S-GW. Once configured, the session idle timer will tear down those sessions that remain idle for longer than the configured time limit. The implementation of the session idle timer allows the S-GW to more effectively utilize system capacity.

**Important**

The session idle timer feature will not work if the Fast Data Path feature is enabled.

## Subscriber Level Trace

Provides a 3GPP standards-based session level trace function for call debugging and testing new functions and access terminals in an LTE environment.

As a complement to Cisco's protocol monitoring function, the S-GW supports 3GPP standards based session level trace capabilities to monitor all call control events on the respective monitored interfaces including S1-U, S11, S5/S8, and Gxc. The trace can be initiated using multiple methods:

- Management initiation via direct CLI configuration
- Management initiation at HSS with trace activation via authentication response messages over S6a reference interface
- Signaling based activation through signaling from subscriber access terminal

Note: Once the trace is provisioned it can be provisioned through the access cloud via various signaling interfaces.

The session level trace function consists of trace activation followed by triggers. The EPC network element buffers the trace activation instructions for the provisioned subscriber in memory using camp-on monitoring. Trace files for active calls are buffered as XML files using non-volatile memory on the local dual redundant hard drives on the ASR 5500 platform. The Trace Depth defines the granularity of data to be traced. Six levels are defined including Maximum, Minimum and Medium with ability to configure additional levels based on vendor extensions.

All call control activity for active and recorded sessions is sent to an off-line Trace Collection Entity (TCE) using a standards-based XML format over an FTP or secure FTP (SFTP) connection. In the current release the IPv4 interfaces are used to provide connectivity to the TCE. Trace activation is based on IMSI or IMEI.

Once a subscriber level trace request is activated it can be propagated via the S5/S8 signaling to provision the corresponding trace for the same subscriber call on the P-GW. The trace configuration will only be propagated if the P-GW is specified in the list of configured Network Element types received by the S-GW. Trace configuration can be specified or transferred in any of the following message types:

- S11: Create Session Request
- S11: Trace Session Activation
- S11: Modify Bearer Request

As subscriber level trace is a CPU intensive activity the maximum number of concurrently monitored trace sessions per Cisco P-GW or S-GW is 32. Use in a production network should be restricted to minimize the impact on existing services.

## Threshold Crossing Alerts (TCA) Support

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e high CPU utilization, or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

The system supports Threshold Crossing Alerts for certain key resources such as CPU, memory, IP pool addresses, etc. With this capability, the operator can configure threshold on these resources whereby, should the resource depletion cross the configured threshold, a SNMP Trap would be sent.

The following thresholding models are supported by the system:

- **Alert:** A value is monitored and an alert condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.
- **Alarm:** Both high and low threshold are defined for a value. An alarm condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps:** SNMP traps have been created that indicate the condition (high threshold crossing and clear) of each of the monitored values.

Generation of specific traps can be enabled or disabled on the chassis. Ensuring that only important faults get displayed. SNMP traps are supported in both Alert and Alarm modes.

- **Logs:** The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.

Logs are supported in both the Alert and the Alarm models.

- **Alarm System:** High threshold alarms generated within the specified polling interval are considered outstanding until a the condition no longer exists or a condition clear alarm is generated. Outstanding alarms are reported to the system's alarm subsystem and are viewable through the Alarm Management menu in an element management system.

The Alarm System is used only in conjunction with the Alarm model.

**Important**

For more information on threshold crossing alert configuration, refer to the *Thresholding Configuration Guide*.

## ULI Enhancements

VoLTE carriers need the last cell/sector updates within the IMS CDRs to assist in troubleshooting customer complaints due to dropped calls as well as LTE network analysis, performance, fraud detection, and operational maintenance. The ultimate objective is to get the last cell sector data in the IMS CDR records in addition to the ULI reporting for session establishment.

To address this issue, the S-GW now supports the following:

- RAN/NAS Cause IE within bearer context of Delete Bearer Command message.
- The S-GW ignores the ULI received as call is going down so there is no point in updating the CDR.

This feature provides support for ULI and ULI Timestamp in Delete Bearer Command message.

Now, when a new ULI is received in the Delete Bearer Command message, a S-GW CDR is initiated.

## P-GW Features and Functionality - Base Software

**Important**

The SAEGW supports all of these features if a P-GW service is assigned to the SAEGW service.

This section describes the features and functions supported by default in the base software for the P-GW service and do not require any additional licenses to implement the functionality.

**Important**

To configure the basic service and functionality on the system for the P-GW service, refer to the configuration examples provided in this guide.

## 3GPP R9 Volume Charging Over Gx

Also known as accumulated usage tracking over Gx, this 3GPP R9 enhancement provides a subset of the volume and charging control functions defined in TS 29.212 based on usage quotas between a P-GW and PCRF. The quotas can be assigned to the default bearer or any of the dedicated bearers for the PDN connection.

This feature enables volume reporting over Gx, which entails usage monitoring and reporting of the accumulated usage of network resources on an IP-CAN session or service data flow basis. PCRF subscribes to the usage monitoring at session level or at flow level by providing the necessary information to PCEF. PCEF in turn reports the usage to the PCRF when the conditions are met. Based on the total network usage in real-time, the PCRF will have the information to enforce dynamic policy decisions.

When usage monitoring is enabled, the PCEF can monitor the usage volume for the IP-CAN session, or applicable service data flows, and report accumulated usage to the PCRF based on any of the following conditions:

- When a usage threshold is reached,

- When all PCC rules for which usage monitoring is enabled for a particular usage monitoring key are removed or deactivated,
- When usage monitoring is explicitly disabled by the PCRF,
- When an IP-CAN session is terminated or,
- When requested by the PCRF.

Accumulated volume reporting can be measured by total volume, the uplink volume, or the downlink volume as requested by the PCRF. When receiving the reported usage from the PCEF, the PCRF deducts the value of the usage report from the total allowed usage for that IP-CAN session, usage monitoring key, or both as applicable.

## AAA Server Groups

Value-added feature to enable VPN service provisioning for enterprise or MVNO customers. Enables each corporate customer to maintain its own AAA servers with its own unique configurable parameters and custom dictionaries.

This feature provides support for up to 800 AAA server groups and 800 NAS IP addresses that can be provisioned within a single context or across the entire chassis. A total of 128 servers can be assigned to an individual server group. Up to 1,600 accounting, authentication and/or mediation servers are supported per chassis.

## ANSI T1.276 Compliance

ANSI T1.276 specifies security measures for Network Elements (NE). In particular it specifies guidelines for password strength, storage, and maintenance security measures.

ANSI T1.276 specifies several measures for password security. These measures include:

- Password strength guidelines
- Password storage guidelines for network elements
- Password maintenance, e.g. periodic forced password changes

These measures are applicable to the ASR 5500 and an element management system since both require password authentication. A subset of these guidelines where applicable to each platform will be implemented. A known subset of guidelines, such as certificate authentication, are not applicable to either product. Furthermore, the platforms support a variety of authentication methods such as RADIUS and SSH which are dependent on external elements. ANSI T1.276 compliance in such cases will be the domain of the external element. ANSI T1.276 guidelines will only be implemented for locally configured operators.

## APN Support

The P-GW's Access Point Name (APN) support offers several benefits:

- Extensive parameter configuration flexibility for the APN.
- Creation of subscriber tiers for individual subscribers or sets of subscribers within the APN.
- Virtual APNs to allow differentiated services within a single APN.

In StarOS v12.x and earlier, up to 1024 APNs can be configured in the P-GW. In StarOS v14.0 and later, up to 2048 APNs can be configured in the P-GW. An APN may be configured for any type of PDP context, i.e., PPP, IPv4, IPv6 or both IPv4 and IPv6. Many dozens of parameters may be configured independently for each APN.

Here are a few highlights of what may be configured:

- **Accounting:** RADIUS, GTPP or none. Server group to use. Charging characteristics. Interface with mediation servers.
- **Authentication:** Protocol, such as, CHAP or PAP or none. Default username/password. Server group to use. Limit for number of PDP contexts.
- **Enhanced Charging:** Name of rulebase to use, which holds the enhanced charging configuration (e.g., eG-CDR variations, charging rules, prepaid/postpaid options, etc.).
- **IP:** Method for IP address allocation (e.g., local allocation by P-GW, Mobile IP, DHCP, etc.). IP address ranges, with or without overlapping ranges across APNs.
- **Tunneling:** PPP may be tunneled with L2TP. IPv4 may be tunneled with GRE, IP-in-IP or L2TP. Load-balancing across multiple tunnels. IPv6 is tunneled in IPv4. Additional tunneling techniques, such as, IPsec and VLAN tagging may be selected by the APN, but are configured in the P-GW independently from the APN.
- **QoS:** IPv4 header ToS handling. Traffic rate limits for different 3GPP traffic classes. Mapping of R98 QoS attributes to work around particular handset defections. Dynamic QoS renegotiation (described elsewhere).

After an APN is determined by the P-GW, the subscriber may be authenticated/authorized with an AAA server. The P-GW allows the AAA server to return VSAs (Vendor Specific Attributes) that override any/all of the APN configuration. This allows different subscriber tier profiles to be configured in the AAA server, and passed to the P-GW during subscriber authentication/authorization.

## Assume Positive for Gy-based Quota Tracking

In the current implementation, the PCEF uses a Diameter based Gy interface to interact with the OCS and obtain quota for each subscriber's data session. Now, the PCEF can retry the OCS after a configured amount of quota has been utilized or after a configured amount of time. The quota value would be part of the dcca-service configuration, and would apply to all subscribers using this dcca-service. The temporary quota will be specified in volume (MB) and/or time (minutes) to allow for enforcement of both quota tracking mechanisms, individually or simultaneously.

When a user consumes the interim total quota or time configured for use during failure handling scenarios, the PCEF shall retry the OCS server to determine if functionality has been restored. In the event that services have been restored, quota assignment and tracking will proceed as per standard usage reporting procedures. Data used during the outage will be reported to the OCS. In the event that the OCS services have not been restored, the PCEF should reallocate with the configured amount of quota and time assigned to the user. The PCEF should report all accumulated used data back to OCS when OCS is back online. If multiple retries and interim allocations occur, the PCEF shall report quota used during all allocation intervals.

When the Gy interface is unavailable, the P-GW shall enter "assume positive" mode. Unique treatment is provided to each subscriber type. Each functional application shall be assigned unique temporary quota volume amounts and time periods based on a command-level AVP from the PCRF on the Gx interface. In addition, a configurable option has been added to disable assume positive functionality for a subscriber group identified by a command-level AVP sent on the Gx interface by the PCRF.



## Bit Rate Mapping Across Gx and GTP-based Interfaces

This feature provides for more consistent behavior and ensures correct bandwidth is allocated for bearers.

Bit rate granularity provided by different interfaces was not aligned in 3GPP specifications. For example, the PCRF provided bits per second on the Gx and the GTP utilized kilobits per second. Due to the conversion of bps to kbps, there were scenarios where the rounding off could have resulted in the incorrect allocation of MBR/GBR values.

With this feature, a bitrate value sent on GTP interface will be rounded up if the conversion from bps (received from Gx) to kbps results in a fractional value. However, the enforcement of bitrate value (AMBR, MBR, GBR) values will remain the same. Once the value (in kbps) that is sent towards the Access side, it needs to be rounded up.

This feature (rounding up the bitrate in kbps) will be enabled by default. However, a CLI command under P-GW service, **[ no ] egtp bitrates-rounded-down-kbps**, controls the behavior of rounding-up. The CLI command enables/disables the old behavior of rounding down. By default, this CLI command is configured to use rounded-up bitrate values. Depending on how the CLI is configured, either rounded-up (Ceil) or rounded-down bitrate value will be sent on GTP interface towards the Access side. If the CLI command is enabled, then it will result in the old behavior. In addition, **show subscribers pgw-only full all** shows the APN-AMBR in terms of bps. Previously, **show subscribers pgw-only full all** used to show in terms of kbps.

CR - C4-132189 - is defined for TS 29.274 for GTP conversion by P-GW.

## Backup and Recovery of Key KPI Statistics

Before the Backup and Recovery of Key KPI Statistics feature was implemented, statistics were not backed up and could not be recovered after a SessMgr task restart. Due to this limitation, monitoring the KPI was a problem as the GGSN, P-GW, SAEGW, and S-GW would lose statistical information whenever task restarts occurred.

KPI calculation involves taking a delta between counter values from two time intervals and then determines the percentage of successful processing of a particular procedure in that time interval. When a SessMgr crashes and then recovers, the GGSN, P-GW, SAEGW, and S-GW lose the counter values - they are reset to zero. So, the KPI calculation in the next interval will result in negative values for that interval. This results in a dip in the graphs plotted using the KPI values, making it difficult for operations team to get a consistent view of the network performance to determine if there is a genuine issue or not.

This feature makes it possible to perform reliable KPI calculations even if a SessMgr restart occurs.



### Important

For more information on Backup and Recovery of Key KPI Statistics, refer to the *Backup and Recovery of Key KPI Statistics* chapter in this guide.

## Bulk Statistics Support

The system's support for bulk statistics allows operators to choose to view not only statistics that are of importance to them, but also to configure the format in which it is presented. This simplifies the post-processing of statistical data since it can be formatted to be parsed by external, back-end processors.

When used in conjunction with an element management system (EMS), the data can be parsed, archived, and graphed.

The system can be configured to collect bulk statistics (performance data) and send them to a collection server (called a receiver). Bulk statistics are statistics that are collected in a group. The individual statistics are grouped by schema. Following is a list of supported schemas for P-GW:

- **APN**: Provides Access Point Name statistics
- **APN Expansion**: Provides more granular GTP-C statistics on a per-APN and per-QCI level
- **Card**: Provides card-level statistics
- **Context**: Provides context service statistics
- **Diameter-acct**: Provides Diameter Accounting statistics
- **Diameter-auth**: Provides Diameter Authentication statistics
- **ECS**: Provides Enhanced Charging Service statistics
- **EGTPC**: Provides Evolved GPRS Tunneling Protocol - Control message statistics
- **FA**: Provides FA service statistics
- **GTPC**: Provides GPRS Tunneling Protocol - Control message statistics
- **GTPP**: Provides GPRS Tunneling Protocol - Prime message statistics
- **GTPU**: Provides GPRS Tunneling Protocol - User message statistics
- **HA**: Provides HA service statistics
- **IMSA**: Provides IMS Authorization service statistics
- **IP Pool**: Provides IP pool statistics
- **LMA**: Provides Local Mobility Anchor service statistics
- **P-GW**: Provides P-GW node-level service statistics
- **P-GW eGTP-C S2a**: Provides eGTP-C S2a interface statistics.
- **P-GW eGTP-C S2b**: Provides eGTP-C S2b interface statistics.
- **P-GW eGTP-C S5/S8**: Provides eGTP-C S5/S8 interface statistics.
- **Port**: Provides port-level statistics
- **PPP**: Provides Point-to-Point Protocol statistics
- **RADIUS**: Provides per-RADIUS server statistics
- **System**: Provides system-level statistics

The system supports the configuration of up to 4 sets (primary/secondary) of receivers. Each set can be configured with to collect specific sets of statistics from the various schemas. Statistics can be pulled manually from the system or sent at configured intervals. The bulk statistics are stored on the receiver(s) in files.

The format of the bulk statistic data files can be configured by the user. Users can specify the format of the file name, file headers, and/or footers to include information such as the date, system host name, system uptime, the IP address of the system generating the statistics (available for only for headers and footers), and/or the time that the file was generated.

When an EMS is used as the receiver, it is capable of further processing the statistics data through XML parsing, archiving, and graphing.

The Bulk Statistics Server component of an EMS parses collected statistics and stores the information in the PostgreSQL database. If XML file generation and transfer is required, this element generates the XML output and can send it to a Northbound NMS or an alternate bulk statistics server for further processing.

Additionally, if archiving of the collected statistics is desired, the Bulk Statistics server writes the files to an alternative directory on the server. A specific directory can be configured by the administrative user or the default directory can be used. Regardless, the directory can be on a local file system or on an NFS-mounted file system on an EMS server.



**Important** For more information on bulk statistic configuration, refer to the *Configuring and Maintaining Bulk Statistics* chapter in the *System Administration Guide*.

## Collision Counter Support in GTP Layer

GTPv2 message collisions occur in the network when a node is expecting a particular procedure message from a peer node but instead receives a different procedure message from the peer. The SAEGW software has been enhanced so that these collisions are now tracked by statistics and handled based on a pre-defined action for each message collision type.

If the SAEGW is configured as a pure P-GW or a pure S-GW, operators will still see the respective collision statistics if they occur.

The output of the **show egtpc statistics verbose** command has been enhanced to provide information on GTPv2 message collisions, including:

- **Interface:** The interface on which the collision occurred: SGW (S4/S11), SGW (S5), or PGW (S5).
- **Old Proc (Msg Type):** Indicates the ongoing procedure at eGTP-C when a new message arrived at the interface which caused the collision. The Msg Type in brackets specifies which message triggered this ongoing procedure.
- **New Proc (Msg Type):** The new procedure and message type.
- **Action:** The pre-defined action taken to handle the collision. The action can be one of:
  - **No Collision Detected**
  - **Suspend Old:** Suspend processing of the original (old) message, process the new message, then resume old message handling.
  - **Abort Old:** Abort the original message handling and processes the new message.
  - **Reject New:** The new message is rejected, and the original (old) message is processed.
  - **Silent Drop New:** Drop the new incoming message, and the old message is processed.
  - **Parallel Hndl:** Both the original (old) and new messages are handled in parallel.
  - **Buffer New:** The new message is buffered and processed once the original (old) message processing is done.
- **Counter:** The number of times each collision type has occurred.



**Important** The Message Collision Statistics section of the command output only appears if any of the collision statistics have a counter total that is greater than zero.

**Sample output:**

```

Message Collision Statistics
Interface      Old Proc (Msg Type)      New Proc (Msg Type)      Action
Counter
SGW(S5)        NW Init Bearer Create (95)  NW Init PDN Delete (99)  Abort Old      1

```

In this instance, the output states that at the S-GW egress interface (S5) a Bearer creation procedure is going on due to a CREATE BEARER REQUEST(95) message from the P-GW. Before its response comes to the S-GW from the MME, a new procedure PDN Delete is triggered due to a DELETE BEARER REQUEST(99) message from the P-GW.

The action that is carried out due to this collision at eGTP-C is to abort (Abort Old) the Bearer Creation procedure and carry on normally with the PDN Delete procedure. The Counter total of 1 indicates that this collision happened only once.

## Congestion Control

The congestion control feature allows you to set policies and thresholds and specify how the system reacts when faced with a heavy load condition.

Congestion control monitors the system for conditions that could potentially degrade performance when the system is under heavy load. Typically, these conditions are temporary (for example, high CPU or memory utilization) and are quickly resolved. However, continuous or large numbers of these conditions within a specific time interval may have an impact the system's ability to service subscriber sessions. Congestion control helps identify such conditions and invokes policies for addressing the situation.

Congestion control operation is based on configuring the following:

- **Congestion Condition Thresholds:** Thresholds dictate the conditions for which congestion control is enabled and establishes limits for defining the state of the system (congested or clear). These thresholds function in a way similar to operation thresholds that are configured for the system as described in the Thresholding Configuration Guide. The primary difference is that when congestion thresholds are reached, a service congestion policy and an SNMP trap, starCongestion, are generated.

A threshold tolerance dictates the percentage under the configured threshold that must be reached in order for the condition to be cleared. An SNMP trap, starCongestionClear, is then triggered.

- **Port Utilization Thresholds:** If you set a port utilization threshold, when the average utilization of all ports in the system reaches the specified threshold, congestion control is enabled.
- **Port-specific Thresholds:** If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is enabled system-wide.
- **Service Congestion Policies:** Congestion policies are configurable for each service. These policies dictate how services respond when the system detects that a congestion condition threshold has been crossed.

**Important**

For more information on congestion control, refer to the *Congestion Control* chapter in the *System Administration Guide*.

## Default and Dedicated EPC Bearers

Provides a foundation for contributing towards improved Quality of User Experience (QoE) by enabling deterministic end-to-end forwarding and scheduling treatments for different services or classes of applications pursuant to their requirements for committed bandwidth resources, jitter and delay. In this way, each application receives the service treatment that users expect.

In the StarOS 9.0 release, the Cisco EPC core platforms support one or more EPS bearers (default plus dedicated). An EPS bearer is a logical aggregate of one or more Service Data Flows (SDFs), running between a UE and a P-GW in the case of a GTP-based S5/S8 interface, and between a UE and HSGW (HRPD Serving Gateway) in case of a PMIP-based S2a interface. In networks where GTP is used as the S5/S8 protocol, the EPS bearer constitutes a concatenation of a radio bearer, S1-U bearer and an S5/S8 bearer anchored on the P-GW. In cases where PMIPv6 is used the EPS bearer is concatenated between the UE and HSGW with IP connectivity between the HSGW and P-GW.

Note: This release supports only GTP-based S5/S8 and PMIPv6 S2a capabilities with no commercial support for PMIPv6 S5/S8.

An EPS bearer uniquely identifies traffic flows that receive a common QoS treatment between a UE and P-GW in the GTP-based S5/S8 design, and between a UE and HSGW in the PMIPv6 S2a approach. If different QoS scheduling priorities are required between Service Data Flows, they should be assigned to separate EPS bearers. Packet filters are signaled in the NAS procedures and associated with a unique packet filter identifier on a per-PDN connection basis.

One EPS bearer is established when the UE connects to a PDN, and that remains established throughout the lifetime of the PDN connection to provide the UE with always-on IP connectivity to that PDN. That bearer is referred to as the default bearer. A PDN connection represents a traffic flow aggregate between a mobile access terminal and an external Packet Data Network (PDN) such as an IMS network, a walled garden application cloud or a back-end enterprise network. Any additional EPS bearer that is established to the same PDN is referred to as a dedicated bearer. The EPS bearer Traffic Flow Template (TFT) is the set of all 5-tuple packet filters associated with a given EPS bearer. The EPC core elements assign a separate bearer ID for each established EPS bearer. At a given time a UE may have multiple PDN connections on one or more P-GWs.

## DHCP Support

The P-GW supports dynamic IP address assignment to subscriber IP PDN contexts using the Dynamic Host Control Protocol (DHCP), as defined by the following standards:

- RFC 2131, Dynamic Host Configuration Protocol
- RFC 2132, DHCP Options and BOOTP Vendor Extensions

The method by which IP addresses are assigned to a PDN context is configured on an APN-by-APN basis. Each APN template dictates whether it will support static or dynamic addresses. Dynamically assigned IP addresses for subscriber PDN contexts can be assigned through the use of DHCP.

The P-GW acts as a DHCP server toward the UE and a DHCP client toward the external DHCP server. The DHCP server function and DHCP client function on the P-GW are completely independent of each other; one can exist without the other.

DHCP supports both IPv4 and IPv6 addresses.

The P-GW does not support DHCP-relay.

### Deferred IPv4 Address Allocation

Apart from obtaining IP addresses during initial access signaling, a UE can indicate via PCO options that it prefers to obtain IP address and related configuration via DHCP after default bearer has been established. This is also known as Deferred Address Allocation.

IPv4 addresses are becoming an increasingly scarce resource. Since 4G networks like LTE are always on, scarce resources such as IPv4 addresses cannot/should not be monopolized by UEs when they are in an ECM-IDLE state.

PDN-type IPv4v6 allows a dual stack implementing. The P-GW allocates an IPv6 address only by default for an IPv4v6 PDN type. The UE defers the allocation of IPv4 addresses based upon its needs, and relinquishes any IPv4 addresses to the global pool once it is done. The P-GW may employ any IPv4 address scheme (local pool or external DHCP server) when providing an IPv4 address on demand.

## Support for Option 26 in DHCP

While fetching IPv4 address for the UE, P-GW acts as an independent DHCP server and client at the same time. It acts as a DHCP server towards the UE and as DHCP client towards the external DHCP server. In earlier release, support for exchange of certain DHCP options between the UE and the external DHCP server through the P-GW was added. This included support for relaying certain external DHCP server provided options (1, 3, 6, 28, and 43) to the UE along with the IPv4 address when deferred address allocation was configured with IP-Addralloc Proxy mode.

This feature adds support for Option 26 received in DHCP OFFER message from the DHCP server.

P-GW preserved the exchanged DHCP option 26 between the UE and the external DHCP server. P-GW relays this option for any future message exchanges between the UE and the external DHCP server. The external DHCP server component of the P-GW reserves and maintains the external DHCP server provided DHCP option so that when the UE renews or rebinds the DHCP lease, P-GW responds with the preserved value.

This feature introduces a behavior change with respect to renewal request. Earlier, when the ASR5500 was configured in DHCP proxy mode and when the DHCP server did not respond to a renewal request, a retransmission at time T2 (.85 \* lease time) did not include both of the configured DHCP servers. DHCP lease got expired after retries exhaustion in the RENEW state.

With this feature, suppose the number of retransmission is configured as 2, then in RENEW state maximum 2 retries are done for the DHCP request messages. If no response is received from the DHCP server and state is changed to REBIND then also DHCP request messages is retried 2 times.

**Old Behavior:** Earlier, for lower values of "number of retransmission" (example  $\geq 2$ ), DHCP request message was not retried in the REBIND state.

**New Behavior:** Now, DHCP request message is retried for the number of times it is configured in both RENEW and REBIND state.

## DHCPv6 Support

The Dynamic Host Configuration Protocol (DHCP) for IPv6 enables the DHCP servers to pass the configuration parameters, such as IPv6 network addresses to IPv6 nodes. It offers the capability of allocating the reusable network addresses and additional configuration functionality automatically.

The DHCPv6 support does not just feature the address allocation, but also fulfills the requirements of Network Layer IP parameters. Apart from these canonical usage modes, DHCPv6's Prefix-Delegation (DHCP-PD) has also been standardized by 3GPP (Rel 10) for "network-behind-ue" scenarios.

P-GW manages IPv6 prefix life-cycle just like it manages IPv4 addresses, thus it is responsible for allocation, renew, and release of these prefixes during the lifetime of a session. IPv6 Prefix is mainly for the UE's session attached to P-GW, where as delegated prefix is for network/devices behind UE. For IPv6 prefixes, P-GW may be obtained from either local-pool, AAA (RADIUS/DIAMETER) or external DHCPv6 servers based on respective configuration. For Delegated IPv6 Prefix allocation, P-GW obtained it from external DHCPv6 servers based on configuration.

**Unicast Address Support Feature:** The IPv6 prefix delegation for the requested UE is either allocated locally or from an external DHCPv6 server by P-GW, GGSN, SAEGW based on configuration at these nodes. These DHCP messages are sent to the external DHCPv6 server using multicast address as destination address. In networks where there are large number of P-GW servers, but less number of DHCP servers, the DHCPv6 messages with multicast address have to travel through the entire network, increasing load on the network. The Unicast address support feature enables the operator to send all DHCPv6 messages on unicast address towards external server using configured address of DHCPv6 server in a DHCP service. This feature is CLI controlled and the operator needs to configure a CLI to support for client unicast operation to the DHCP Server.

DHCPv6 support for P-GW covers the following requirements:

- RFC 3315, Dynamic Host Configuration Protocol for IPv6 (Basic DHCPv6)
- RFC 3633, prefix delegation mechanism

## Direct Tunnel Support

When Gn/Gp interworking with pre-release SGSNs is enabled, the GGSN service on the P-GW supports direct tunnel functionality.

Direct tunnel improves the user experience (e.g. expedited web page delivery, reduced round trip delay for conversational services, etc.) by eliminating SGSN tunnel "switching" latency from the user plane. An additional advantage of direct tunnel from an operational and capital expenditure perspective is that direct tunnel optimizes the usage of user plane resources by removing the requirement for user plane processing on the SGSN.

The direct tunnel architecture allows the establishment of a direct user plane tunnel between the RAN and the GGSN, bypassing the SGSN. The SGSN continues to handle the control plane signaling and typically makes the decision to establish direct tunnel at PDP Context Activation. A direct tunnel is achieved at PDP context activation by the SGSN establishing a user plane (GTP-U) tunnel directly between RNC and GGSN (using an Update PDP Context Request toward the GGSN).

A major consequence of deploying direct tunnel is that it produces a significant increase in control plane load on both the SGSN and GGSN components of the packet core. It is therefore of paramount importance to a wireless operator to ensure that the deployed GGSNs are capable of handling the additional control plane loads introduced of part of direct tunnel deployment. The Cisco GGSN and SGSN offer massive control plane transaction capabilities, ensuring system control plane capacity will not be a capacity limiting factor once direct tunnel is deployed.



### Important

For more information on direct tunnel support, refer to the *Direct Tunnel for 4G (LTE) Networks* chapter in this guide.

## DNS Support for IPv4/IPv6 PDP Contexts

This feature adds functionality in P-GW for PDN type IPv4v6. in StarOS Release 15.0. Previously, if an MS requested an IPv4 DNS address, P-GW did not send the IPv4 DNS address.

MS may request for DNS server IPv4 or IPv6 addresses using the Protocol Configurations Options IE (as a container or as part of IPCP protocol configuration request) in PDP Context Activation procedure for PDP Type IPv4, IPv6, or IPv4v6. In that case, the P-GW may return the IP address of one or more DNS servers in the PCO IE in the PDP Context Activation Response message. The DNS address(es) shall be coded in the PCO as specified in 3GPP TS 24.008.

For PDP Type IPv4v6, if MS requested DNS server IPv4 address, it did not return an IPv4 address. Support is now added to respond with address requested by MS.

AAA server may also provide DNS Server IP Address in Access-Accept Auth Response. In such cases, AAA provided DNS server IPs takes priority over the one configured under APN.

When DNS server address is requested in PCO configuration, the following preference would be followed:

1. DNS values received from RADIUS Server.
2. DNS values locally configured with APN.
3. DNS values configured at context level with **ip name-servers** CLI.

## Domain Based Flow Definitions

This solution provides improved flexibility and granularity in obtaining geographically correct exact IP entries of the servers by snooping DNS responses.

Currently, it is possible to configure L7 rules to filter based on domain (m.google.com). Sometimes multiple servers may serve a domain, each with its own IP address. Using an IP-rule instead of an http rule will result in multiple IP-rules; one IP-rule for each server "behind" the domain, and it might get cumbersome to maintain a list of IP addresses for domain-based filters.

In this solution, you can create ruledefs specifying hostnames (domain names) and parts of hostnames (domain names). Upon the definition of the hostnames/domain names or parts of them, the P-GW will monitor all the DNS responses sent towards the UE and will snoop only the DNS response, which has q-name or a-name as specified in the rules, and identify all the IP addresses resulted from the DNS responses. DNS snooping will be done on live traffic for every subscriber.

## DSCP Marking

Provides support for more granular configuration of DSCP marking.

For Interactive Traffic class, the P-GW supports per-gateway service and per-APN configurable DSCP marking for Uplink and Downlink direction based on Allocation/Retention Priority in addition to the current priorities.

The following matrix may be used to determine the Diffserv markings used based on the configured traffic class and Allocation/Retention Priority:

**Table 6: Default DSCP Value Matrix**

Allocation Priority	1	2	3
Traffic Handling Priority			



Allocation Priority	1	2	3
1	ef	ef	ef
2	af21	af21	af21
3	af21	af21	af21

In addition, the P-GW allows configuration of diameter packets and GTP-C/GTP-U echo with DSCP values.

### RAT-Type based DSCP Marking

With 21.6 and later releases, operators can perform DSCP marking on gateways such as GGSN, P-GW, and SAE-GW, based on RAT-Type. It allows the operator to configure different QoS services and to optimize traffic based on the RAT-Type: EUTRAN, GERAN, and UTRAN.

RAT-Type based DSCP marking includes the following:

- Support for all QCI and ARP values.
- Support for Standard and non-Standard QCIs.
- If a particular RAT-Type is not configured, the DSCP marking functionality is applied to all RAT-Type.
- Applicable for Virtual APNs.
- During Inter-RAT hand-offs, DSCP marking is based on the RAT-Type of the current hand-off.
- DSCP marking per RAT-Type is only applicable for user data traffic and not for control traffic (GTP-C packets).



**Important** Backward compatibility is maintained for existing DSCP marking and IP-ToS functionalities.

## GTP-U on per APN Basis

This feature provides the flexibility to have a different DSCP marking table on per APN basis so that traffic on each of the APNs can be marked differently, depending on the needs of the APN.

The S-GW/P-GW supports configurable DSCP marking of the outer header of a GTP-U tunnel packet based on a QCI/THP table for the S5/S8 and Gn/Gp interfaces. This feature allows configuring DSCP marking table on a per APN basis.

Previously, DSCP marking table was configured on P-GW service level. As part of this requirement, CLI was added to associate the qos-qci-mapping table in APN.



**Important** The SAEGW does not support non-standard QCI values. QCI values 1 through 9 are standard values and are defined in 3GPP TS 23.203; the SAEGW supports these standard values.

In order to be backward compatible with older configurations, if a DSCP marking table is associated with P-GW service and not with the APN, then the one in P-GW service will be used. If table is associated in both P-GW service and APN, then the one on APN will take precedence.

## Dynamic GTP Echo Timer

The Dynamic GTP Echo Timer enables the eGTP and GTP-U services to better manage GTP paths during network congestion. As opposed to the default echo timer, which uses fixed intervals and retransmission timers, the dynamic echo timer adds a calculated round trip timer (RTT) that is generated once a full request/response procedure has completed. A multiplier can be added to the calculation for additional support during congestion periods.



### Important

For more information, refer to the *Configuring the GTP Echo Timer* section located in the *Configuring Optional Features on the P-GW* section of the *PDN Gateway Configuration* chapter.

## Dynamic Policy Charging Control (Gx Reference Interface)

Dynamic policy and charging control provides a primary building block toward the realization of IMS multimedia applications. In contrast to statically provisioned architectures, the dynamic policy framework provides a centralized service control layer with global awareness of all access-side network elements. The centralized policy decision elements simplify the process of provisioning global policies to multiple access gateways. Dynamic policy is especially useful in an Always-On deployment model as the usage paradigm transitions from a short lived to a lengthier online session in which the volume of data consumed can be extensive. Under these conditions dynamic policy management enables dynamic just in-time resource allocation to more efficiently protect the capacity and resources of the network.

Dynamic Policy Control represents the ability to dynamically authorize and control services and application flows between a Policy Charging Enforcement Function (PCEF) on the P-GW and the PCRF. Policy control enables a centralized and decoupled service control architecture to regulate the way in which services are provisioned and allocated at the bearer resource layer.

The StarOS 9.0 release included enhancements to conform with 3GPP TS 29.212 and 29.230 functions. The Gx reference interface uses Diameter transport and IPv6 addressing. The subscriber is identified to the PCRF at session establishment using IMSI based NAIs within the Subscription-ID AVP. Additionally the IMEI within the Equipment-Info AVP is used to identify the subscriber access terminal to the policy server. The Gx reference interface supports the following capabilities:

- Authorize the bearer establishment for a packet flow
- Dynamic L3/L4 transfer of service data flow filters within PCC rules for selection and policy enforcement of downlink/uplink IP CAN bearers
- Support static pre-provisioned L7 rulebase name attribute as trigger for activating Inline Services such as Peer-to-Peer Detection
- Authorize the modification of a service data flow
- Revoke the authorization of a packet flow
- Provision PCC rules for service data flows mapped to default or dedicated EPS bearers
- Support P-GW initiated event triggers based on change of access network gateway or IP CAN
- Provide the ability to set or modify APN-AMBR for a default EPS bearer
- Create or modify QoS service priority by including QCI values in PCC rules transmitted from PCRF to PCEF functions

## Enhanced Charging Service (ECS)

The Enhanced Charging Service provides an integrated in-line service for inspecting subscriber data packets and generating detail records to enable billing based on usage and traffic patterns. Other features include:

- [Content Analysis Support, on page 68](#)
- [Content Service Steering, on page 69](#)
- [Support for Multiple Detail Record Types, on page 70](#)
- [Diameter Credit Control Application, on page 70](#)
- [Accept TCP Connections from DCCA Server, on page 71](#)
- [Gy Interface Support, on page 71](#)

The Enhanced Charging Service (ECS) is an in-line service feature that is integrated within the system. ECS enhances the mobile carrier's ability to provide flexible, differentiated, and detailed billing to subscribers by using Layer 3 through Layer 7 deep packet inspection with the ability to integrate with back-end billing mediation systems.

ECS interacts with active mediation systems to provide full real-time prepaid and active charging capabilities. Here the active mediation system provides the rating and charging function for different applications.

In addition, ECS also includes extensive record generation capabilities for post-paid charging with in-depth understanding of the user session. Refer to the Support for Multiple Detail Record Types section for more information.

The major components include:

- **Service Steering:** Directs subscriber traffic into the ECS subsystem. Service Steering is used to direct selective subscriber traffic flows via an Access Control List (ACL). It is used for other redirection applications as well for both internal and external services and servers.
- **Protocol Analyzer:** The software stack responsible for analyzing the individual protocol fields and states during packet inspection. It performs two types of packet inspection:
  - **Shallow Packet Inspection:** inspection of the layer 3 (IP header) and layer 4 (e.g. UDP or TCP header) information.
  - **Deep Packet Inspection:** inspection of layer 7 and 7+ information. Deep packet inspection functionality includes:
    - Detection of URI (Uniform Resource Identifier) information at level 7 (e.g., HTTP, WTP, RTSP Uniform Resource Locators (URLs)).
    - Identification of true destination in the case of terminating proxies, where shallow packet inspection would only reveal the destination IP address / port number of a terminating proxy.
    - De-encapsulation of upper layer protocol headers, such as MMS-over-WTP, WSP-over-UDP, and IP-over GPRS.
    - Verification that traffic actually conforms to the protocol the layer 4 port number suggests.
- **Rule Definitions:** User-defined expressions, based on protocol fields and/or protocol-states, which define what actions to take when specific field values are true. Expressions may contain a number of operator types (string, =, >, etc.) based on the data type of the operand. Each Ruledef configuration is consisting of multiple expressions applicable to any of the fields or states supported by the respective analyzers.

- **Rule Bases:** a collection of rule definitions and their associated billing policy. The rule base determines the action to be taken when a rule is matched. It is possible to define a rule definition with different actions.

### Mediation and Charging Methods

To provide maximum flexibility when integrating with billing mediation systems, ECS supports a full range of charging and authorization interfaces.

- **Pre-paid:** In a pre-paid environment, the subscribers pay for service prior to use. While the subscriber is using the service, credit is deducted from subscriber's account until it is exhausted or call ends. The pre-paid accounting server is responsible for authorizing network nodes (GGSNs) to grant access to the user, as well as grant quotas for either time connected or volume used. It is up to the network node to track the quota use, and when these use quotas run low, the network node sends a request to the pre-paid server for more quota.

If the user has not used up the purchased credit, the server grants quota and if no credit is available to the subscriber the call will be disconnected. ECS and DCCA manage this functionality by providing the ability to setup quotas for different services.

Pre-paid quota in ECS is implemented using DIAMETER Credit Control Application (DCCA). DCCA supports the implementation of real-time credit control for a variety of services, such as networks access, messaging services, and download services.

In addition to being a general solution for real-time cost and credit control, DCCA includes these features:

- **Real-time Rate Service Information** - DCCA can verify when end subscribers' accounts are exhausted or expired; or deny additional chargeable events.
- **Support for Multiple Services** - DCCA supports the usage of multiple services within one subscriber session. Multiple Service support includes; 1) ability to identify and process the service or group of services that are subject to different cost structures 2) independent credit control of multiple services in a single credit control sub-session.

Refer to [Diameter Credit Control Application](#), on page 70 for more information.

- **Post-paid:** In a post-paid environment, the subscribers pay after use of the service. A AAA server is responsible for authorizing network nodes (GGSNs) to grant access to the user and a CDR system generates G-CDRs/eG-CDRs/EDRs/UDRs or Comma Separated Values (CSVs) for billing information on pre-defined intervals of volume or per time.



#### Important

Support for the Enhanced Charging Service requires a service license; the ECS license is included in the P-GW session use license. For more information on ECS, refer to the *Enhanced Charging Service Administration Guide*.

## Content Analysis Support

The Enhanced Charging Service is capable of performing content analysis on packets of many different protocols at different layers of the OSI model.

The ECS content analyzers are able to inspect and maintain state across various protocols at all layers of the OSI stack. ECS system supports, inspects, and analyzes the following protocols:

- IP
- TCP
- UDP
- DNS
- FTP
- TFTP
- SMTP
- POP3
- HTTP
- ICMP
- WAP: WTP and WSP
- Real-Time Streaming: RTP and RTSP
- MMS
- SIP and SDP
- File analysis: examination of downloaded file characteristics (e.g. file size, chunks transferred, etc.) from file transfer protocols such as HTTP and FTP.

Traffic analyzers in enhanced charging subsystem are based on configured rules. Rules used for Traffic analysis analyze packet flows and form usage records. Usage records are created per content type and forwarded to a pre-paid server or to a mediation/billing system. A traffic analyzer performs shallow (Layer 3 and Layer 4) and deep (above Layer 4) packet inspection of the IP packet flows.

The Traffic Analyzer function is able to do a shallow (layer 3 and layer 4) and deep (above layer 4) packet inspection of IP Packet Flows.

It is able to correlate all layer 3 packets (and bytes) with higher layer trigger criteria (e.g. URL detected in a HTTP header) and it is also perform stateful packet inspection to complex protocols like FTP, RTSP, SIP that dynamically open ports for the data path and by this way, user plane payload is differentiated into "categories".

The Traffic Analyzer works on the application level as well and performs event based charging without the interference of the service platforms.

**Important**

This functionality is available for use with the Enhanced Charging Service which requires a session-use license. For more information on ECS, refer to the *Enhanced Charging Service Administration Guide*.

## Content Service Steering

Content Service Steering (CSS) directs selective subscriber traffic into the ECS subsystem (In-line services internal to the system) based on the content of the data presented by mobile subscribers.

CSS uses Access Control Lists (ACLs) to redirect selective subscriber traffic flows. ACLs control the flow of packets into and out of the system. ACLs consist of "rules" (ACL rules) or filters that control the action taken on packets matching the filter criteria.

ACLs are configurable on a per-context basis and applies to a subscriber through either a subscriber profile or an APN profile in the destination context.



**Important** For more information on CSS, refer to the *Content Service Steering* chapter of the *System Administration Guide*.



**Important** For more information on ACLs, refer to the *IP Access Control Lists* chapter of the *System Administration Guide*.

## Support for Multiple Detail Record Types

To meet the requirements of standard solutions and at the same time, provide flexible and detailed information on service usage, the Enhanced Charging Service (ECS) provides the following type of usage records:

- Event Detail Records (EDRs)
- Usage Detail Records (UDRs)

ECS provides for the generation of charging data files, which can be periodically retrieved from the system and used as input to a billing mediation system for post-processing. These files are provided in a standard format, so that the impact on the existing billing/mediation system is minimal and at the same time, these records contain all the information required for billing based on the content.

GTPP accounting in ECS allows the collection of counters for different types of data traffic into detail records. The following types of detail records are supported:

- **Event Detail Records (EDRs):** An alternative to standard G-CDRs when the information provided by the G-CDRs is not sufficient to do the content billing. EDRs are generated according to explicit action statements in rule commands that are user-configurable. The EDRs are generated in comma separated values (CSV) format, generated as defined in traffic analysis rules.
- **User Detail Records (UDRs):** Contain accounting information related to a specific mobile subscriber. The fields to be reported in them are user-configurable and are generated on any trigger of time threshold, volume threshold, handoffs, and call termination. The UDRs are generated in comma separated values (CSV) format, generated as defined in traffic analysis rules.



**Important** This functionality is available for use with the Enhanced Charging Service which requires a session-use license. For more information on ECS, refer to the *Enhanced Charging Service Administration Guide*.

## Diameter Credit Control Application

Provides a pre-paid billing mechanism for real-time cost and credit control based on the following **standards**:

- RFC 3588, Diameter Base Protocol, September 2003
- RFC 4006, Diameter Credit-Control Application, August 2005

The Diameter Credit Control Application (DCCA) is used to implement real-time credit-control for a variety of end user services such as network access, Session Initiation Protocol (SIP) services, messaging services, download services etc.

Used in conjunction with ECS, the DCCA interface uses a mechanism to allow the user to be informed of the charges to be levied for a requested service. In addition, there are services such as gaming and advertising that may credit as well as debit from a user account.

DCCA also supports the following:

- **Real-time Rate Service Information:** The ability to verify when end subscribers' accounts are exhausted or expired; or deny additional chargeable events.
- **Support for Multiple Services:** The usage of multiple services within one subscriber session is supported. Multiple Service support includes:
  - The ability to identify and process the service or group of services that are subject to different cost structures.
  - Independent credit control of multiple services in a single credit control sub-session.



---

**Important**

This functionality is available for use with the Enhanced Charging Service, which requires a session-use license. For more information on ECS, refer to the *Enhanced Charging Service Administration Guide*.

---

## Accept TCP Connections from DCCA Server

This feature allows for peer Diameter Credit Control Application servers to initiate a connection the NGME.

This feature allows peer diameter nodes to connect to the NGME on TCP port 3868 when the diameter server is incapable of receiving diameter incoming diameter requests.



---

**Important**

For more information on Diameter support, if you are using StarOS 12.3 or an earlier release, refer to the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

---

## Gy Interface Support

The Gy interface enables the wireless operator to implement a standardized interface for real time content based charging with differentiated rates for time based and volume based charging.

As it is based on a quota mechanism, the Gy interface enables the wireless operator to spare expensive Prepaid System resources.

As it enables time-, volume-, and event-based charging models, the Gy interface flexibly enables the operator to implement charging models tailored to their service strategies.

The Gy interface provides a standardized Diameter interface for real time content based charging of data services. It is based on the 3GPP standards and relies on quota allocation.

It provides an online charging interface that works with the ECS deep packet inspection feature. With Gy, customer traffic can be gated and billed in an "online" or "prepaid" style. Both time- and volume-based

charging models are supported. In all of these models, differentiated rates can be applied to different services based on shallow or deep packet inspection.

Gy is a Diameter interface. As such, it is implemented atop, and inherits features from, the Diameter Base Protocol. The system supports the applicable Base network and application features, including directly connected, relayed or proxied DCCA servers using TLS or plaintext TCP.

In the simplest possible installation, the system exchanges Gy Diameter messages over Diameter TCP links between itself and one "prepay" server. For a more robust installation, multiple servers would be used. These servers may optionally share or mirror a single quota database so as to support Gy session failover from one server to the other. For a more scalable installation, a layer of proxies or other Diameter agents can be introduced to provide features such as multi-path message routing or message and session redirection features.

The Cisco implementation is based on the following standards:

- RFC 4006 generic DCCA, including:
  - CCR Initial, Update, and Final signaling
  - ASR and RAR asynchronous DCCA server messages
  - Time, Total-Octets, and Service-Specific-Units quota management
  - Multiple independent quotas using Multiple-Services-Credit-Control
  - Rating-Group for quota-to-traffic association
  - CC-Failure-Handling and CC-Session-Failover features
  - Final-Unit-Action TERMINATE behavior
  - Tariff-Time-Change feature.
- 3GPP TS 32.299 online mode "Gy" DCCA, including:
  - Final-Unit-Action REDIRECT behavior
  - Quota-Holding-Time: This defines a user traffic idle time, on a per category basis, after which the usage is returned and no new quota is explicitly requested
  - Quota-Thresholds: These AVPs define a low value watermark at which new quota will be sought before the quota is entirely gone; the intent is to limit interruption of user traffic.  
 These AVPs exist for all quota flavors, for example "Time-Quota-Threshold".
  - Trigger-Type: This AVP defines a set of events which will induce a re-authentication of the current session and its quota categories.

## Enhancement to New Call Setup after Sessmgr or DPC Failure

This enhancement is used to address some specific failure scenarios where either the sessmgr or the corresponding aaa manager restarts, and the P-GW service/sessmgr is unable to bring new calls up or establish a connection with all other dependent services. In these failure scenarios if a call landed on this particular P-GW service/sessmgr, the call establishment is significantly delayed and would fail until all the dependent services come up. This resulted in the possibility that the S-GW might time out and report that the peer P-GW is not responding to the Create Session Request (CSReq) message.



Prior to StarOS release 20, the demux did not prevent a sessmgr from accepting new calls even after a sessmgr restart had occurred, which then placed the sessmgr in a state where it was unable to accept new calls.

Although the issue is usually self-correcting and takes between 10 to 25 seconds to complete, if operators see too many call rejects due to a peer not responding to the Create Session Response (CSResp) message, and this is happening after a aaa manager restart or a sessmgr restart, the SAEGW can be configured via the CLI to temporarily stop seeing the peer not responding error. By enabling this new CLI-controlled feature, the demuxmgr will prevent the sessmgr from accepting new calls for a configured amount of time, after which the sessmgrs will restart.

Use the **require demux smgr-suspension interval** command in Global Configuration Mode to address these scenarios when they occur.

## Framed-Route Attribute Support

The Framed-Route attribute provides routing information to be configured for the user on the network access server (NAS). The Framed-Route information is returned to the RADIUS server in the Access-Accept message.

Mobile Router enables a router to create a PDN Session which the P-GW authorizes using RADIUS server. The RADIUS server authenticates this router and includes a Framed-Route attribute in the access-accept response packet. Framed-Route attribute also specifies the subnet routing information to be installed in the P-GW for the "mobile router." If the P-GW receives a packet with a destination address matching the Framed-Route, the packet is forwarded to the mobile router through the associated PDN Session. For more information, see *Routing Behind the Mobile Station on an APN* chapter.

## Gn/Gp Handoff Support

Integrated support of this feature requires that a valid session use license key be installed for both P-GW and GGSN. Contact your local Sales or Support representative for information on how to obtain a license.

In LTE deployments, smooth handover support is required between 3G/2G and LTE networks, and Evolved Packet Core (EPC) is designed to be a common packet core for different access technologies. P-GW supports handovers as user equipment (UE) moves across different access technologies.

Cisco's P-GW supports inter-technology mobility handover between 4G and 3G/2G access. Interworking is supported between the 4G and 2G/3G SGSNs, which provide only Gn and Gp interfaces but no S3, S4 or S5/S8 interfaces. These Gn/Gp SGSNs provide no functionality introduced specifically for the evolved packet system (EPS) or for interoperation with the E-UTRAN. These handovers are supported only with a GTP-based S5/S8 and P-GW supports handoffs between GTPv2 based S5/S8 and GTPv1 based Gn/Gp tunneled connections. In this scenario, the P-GW works as an IP anchor for the EPC.



### Important

To support the seamless handover of a session between GGSN and P-GW, the two independent services must be co-located on the same node and configured within the same context for optimum interoperation.



### Important

For more information on Gn/GP handoffs, refer to *Gn/Gp GGSN/SGSN (GERAN/UTRAN)* in the *Supported Logical Network Interfaces (Reference Points)* section in this chapter.

## GTP-C Path Failure Enhancements and Improved Debugging Tools

In StarOS release 20.0, 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.

The following enhancements are added as 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.

### Support to Avoid False Path Failure Detection

Several enhancements have been made to facilitate the node's ability to avoid false path failure detection:

- The software has been enhanced to avoid path failure detection due to spurious/incorrect messages from a peer. These messages can cause a large burst in network traffic due to the number of service deactivations and activations, resulting in network congestion. The **gtpc** command in *eGTP-C Service Configuration Mode* has been enhanced to resolve this issue. The **max-remote-restart-counter-change** keyword has been added to ensure false path failure detections are not detected as GTP-C path failures. For example, if the **max-remote-restart-counter-change** is set to 10 and the current peer restart counter is 251, eGTP will detect a peer restart only if the new restart counter is 252 through 255 or 0 through 5. Similarly, if the stored restart counter is 1, eGTP will detect a peer restart only if the new restart counter is 2 through 11.
- Also as part of this enhancement, new keywords have been added to the **path-failure detection-policy** command in *eGTP-C Service Configuration Mode* to enable or disable path failure detection.
- The **show egtp-service all** command in Exec Mode has been enhanced to indicate whether Echo Request/Echo Response Restart Counter Change and Control Message Restart Counter Change are enabled/disabled on the node.

### Improved GTP-C Path Failure Statistics

Several improvements have been made to improve the quality of the GTP-C path failures so that operators/engineers can more quickly identify the cause of the failure.

- The output of the **show egtpc statistics path-failure-reasons** has been enhanced to show the number and type of control message restart counter changes at the demuxmgr and sessmgr. This command output has also been enhanced to track the number of path failures detected that were ignored at the eGTP-C layer.

- The **show egtpc peers path-failure-history** command output has been added to provide detailed information on the last five path failures per peer.
- The output of the **show egtp-service all name** and **show configuration** commands has been enhanced to show the current configuration settings specific to path GTP-C path failure detection policy.

## IMS Emergency Bearer Handling

With this support, a UE is able to connect to an emergency PDN and make Enhanced 911 (E911) calls while providing the required location information to the Public Safety Access Point (PSAP).

E911 is a telecommunications-based system that is designed to link people who are experiencing an emergency with the public resources that can help. This feature supports E911-based calls across the LTE and IMS networks. In a voice over LTE scenario, the subscriber attaches to a dedicated packet data network (PDN) called EPDN (Emergency PDN) in order to establish a voice over IP connection to the PSAP. Signaling either happens on the default emergency bearer, or signaling and RTP media flow over separate dedicated emergency bearers. Additionally, different than normal PDN attachment that relies on AAA and PCRF components for call establishment, the EPDN attributes are configured locally on the P-GW, which eliminates the potential for emergency call failure if either of these systems is not available.

Emergency bearer services are provided to support IMS emergency sessions. Emergency bearer services are functionalities provided by the serving network when the network is configured to support emergency services. Emergency bearer services are provided to normally attached UEs and to UEs that are in a limited service state (depending on local service regulations, policies, and restrictions). Receiving emergency services in limited service state does not require a subscription.

The standard (refer to 3GPP TS 23.401) has identified four behaviors that are supported:

- Valid UEs only
- Authenticated UEs only
- MSI required, authentication optional
- All UEs

To request emergency services, the UE has the following two options:

- UEs that are in a limited service state (due to attach reject from the network, or since no SIM is present), initiate an ATTACH indicating that the ATTACH is for receiving emergency bearer services. After a successful attach, the services that the network provides the UE is solely in the context of Emergency Bearer Services.
- UEs that camp normally on a cell initiates a normal ATTACH if it requires emergency services. Normal attached UEs initiated a UE Requested PDN Connectivity procedure to request Emergency Bearer Services.

## IMSI/IMEI Available in System Event Logs of Type Error and Critical

The SAEGW can be configured to provide the IMSI/IMEI in the event log details for the following system event logs of type error and critical, if available. If the IMSI is not available, the SAEGW will make a best effort to obtain the IMEI.

Use the **logging include-ueid** command in Global Configuration Mode to enable this functionality.

Table 7: New and Modified System Event Logs with IMSI/IMEI in System Event Log Details 20

Event Log #	Description
<b>New Events</b>	
12225	Represents misc_error3 in format "[IMSI <IMSI>] Misc Error3: %s, error code %d"
12226	Represents recover_call_from_crr_failed1 error in format "[IMSI <IMSI>] Sessmgr-%d Recover call from CRR failed for callid:0x%x reason=%s"
12227	Represents aaa_create_session_failed_no_more_sessions1 error in format "[IMSI <IMSI>] Sessmgr-%d Ran out of session handles"
140075	Represents error_log1 in format "[IMSI <IMSI>]%s"
<b>Modified Events</b>	
139001	To print miscellaneous PGW error log.
191006	To print miscellaneous SAEGW error log.
10034	Represents FSM error in format "[IMSI <IMSI>] default call fsm error: ostate=%s(%d) state=%s(%d) event=%s(%d)"
10035	Represents FSM INVALID event in format "[IMSI <IMSI>] default call fsm invalid event: state=%s(%d) event=%s(%d)"
12382	Represents SN_LE_SESSMGR_PGW_REJECT_BEARER_OP in format "[IMSI <IMSI>] Sessmgr-%d: Request to %s bearer rejected. Reason: %s". For example "[IMSI 112233445566778 Sessmgr-1: Request to Create bearer rejected. Reason: Create Bearer Request denied as session recovery is in progress"
12668	Represents fsm_event_error in format "[IMSI <IMSI>] Misc Error: Bad event in sessmgr fsm, event code %d"
12774	Represents pgw_purge_invalid_crr in format "[IMSI <IMSI>] Local %s TEID [%lu] Collision: Clp Connect Time: %lu, Old Clp Callid: %d, Old Clp Connect Time: %lu %s"
12855	Represents ncqos_nrspca_trig_err in format "[IMSI <IMSI>] NCQOS NRSPCA trig rcvd in invalid bcm mode."
12857	Represents ncqos_nrupc_tft_err in format "[IMSI <IMSI>] NCQOS NRUPC Trig : TFT validation failed for nsapi <%u>."
12858	Represents ncqos_nrxx_trig_already in format "[IMSI <IMSI>] NCQOS NRSPCA/NRUPC is already triggered on sess with nsapi <%u>."
12859	Represents ncqos_nrxx_tft_check_fail in format "[IMSI <IMSI>] NCQOS TFT check failed as TFT has invalid opcode for nsapi <%u>:pf_id_bitmap 0x%x and tft_opcode: %d"
12860	Represents ncqos_sec_rej in format "[IMSI <IMSI>] NCQOS Secondary ctxt with nsapi <%u> rejected, due to <%s>."

Event Log #	Description
12861	Represents ncqos_upc_rej in format "[IMSI <IMSI>] UPC Rejected for ctxt with nsapi <%u>, due to <%s>."
12862	Represents ggsn_subsession_invalid_state in format "[IMSI <IMSI>] GGSN subsession invalid state state:<%s>,[event:<%s>]"
11830	Represents gngp_handoff_rejected_for_pdn_ipv4v6 in format "[IMSI <IMSI>] Sessmgr-%d Handoff from PGW-to-GGSN rejected, as GGSN doesnt support Deferred allocation for IPv4v6, dropping the call."
11832	Represents gngp_handoff_rejected_no_non_gbr_bearer_for_def_bearer_selection in format "[IMSI <IMSI>] Sessmgr-%d Handoff from PGW-to-GGSN rejected, as GGSN Callline has no non-GBR bearer to be selected as Default bearer."
11834	Represents gngp_handoff_from_ggsn_rejected_no_ggsn_call in format "[IMSI <IMSI>] Sessmgr-%d Handoff from GGSN-to-PGW rejected, as GGSN call with TEIDC <0x%x> not found."
12960	Represents gtp_pdp_type_mismatch in format "[IMSI <IMSI>] Mismatch between PDP type of APN %s and in create req. Rejecting call"
11282	Represents pcc_intf_error_info in format "[IMSI <IMSI>] %s"
11293	Represents collision_error in format "[IMSI <IMSI>] Collision Error: Temp Failure Handling Delayed Pending Active Transaction: , error code %d"
11917	Represents rcvd_invalid_bearer_binding_req_from_acs in format "[IMSI <IMSI>] Sessmgr %d: Received invalid bearer binding request from ACS."
11978	Represents saegw_uid_error in format "[IMSI <IMSI>] %s"
11994	Represents unwanted_pcc_intf_setup_req error in format "[IMSI <IMSI>] GGSN_INITIATE_SESS_SETUP_REQ is already fwded to PCC interface "
140005	Represents ue_fsm_illegal_event in format "[IMSI <IMSI>] Invalid/unhandled UE event <%s> in state <%s>"
140006	Represents pdn_fsm_illegal_event in format "[IMSI <IMSI>] Invalid/unhandled PDN event <%s> in state <%s>"
140007	Represents epsb_fsm_illegal_event in format "[IMSI <IMSI>] Invalid/unhandled EPSB event <%s> in state <%s>"
10726	Represents saegwdrv_generic_error "[IMSI <IMSI>] %s"

## IP Access Control Lists

IP access control lists allow you to set up rules that control the flow of packets into and out of the system based on a variety of IP packet parameters.

IP access lists, or access control lists (ACLs) as they are commonly referred to, are used to control the flow of packets into and out of the system. They are configured on a per-context basis and consist of "rules" (ACL

rules) or filters that control the action taken on packets that match the filter criteria. Once configured, an ACL can be applied to any of the following:

- An individual interface
- All traffic facilitated by a context (known as a policy ACL)
- An individual subscriber
- All subscriber sessions facilitated by a specific context

**Important**

For more information on IP access control lists, refer to the *IP Access Control Lists* chapter in the *System Administration Guide*.

## IP Address Hold Timers

Also known as address quarantining, this subscriber-level CLI introduces an address hold timer to temporarily buffer a previously assigned IP address from an IP address pool to prevent it from being recycled and reassigned to a new subscriber session. It is especially useful during inter-RAT handovers that sometimes lead to temporary loss of the mobile data session.

This feature provides a higher quality user experience for location-based services where the remote host server needs to reach the mobile device.

**Important**

Currently, the P-GW only supports an address hold timer with IPv4 addresses.

## IPv6 Capabilities

Enables increased address efficiency and relieves pressures caused by rapidly approaching IPv4 address exhaustion problem.

The P-GW offers the following IPv6 capabilities:

**Native IPv6 and IPv6 transport**

- Support for any combination of IPv4, IPv6 or dual stack IPv4/v6 address assignment from dynamic or static address pools on the P-GW.
- Support for native IPv6 transport and service addresses on PMIPv6 S2a interface. Note that transport on GTP S5/S8 connections in this release is IPv4 based.
- Support for IPv6 transport for outbound traffic over the SGi reference interface to external Packet Data Networks.

**IPv6 Connections to Attached Elements**

IPv6 transport and interfaces are supported on all of the following connections:

- Diameter Gx policy signaling interface
- Diameter Gy online charging reference interface

- S6b authentication interface to external 3GPP AAA server
- Diameter Rf offline charging interface
- Lawful Intercept (X1, X2 interfaces)

#### Routing and Miscellaneous Features

- OSPFv3
- MP-BGP v6 extensions
- IPv6 flows (Supported on all Diameter QoS and Charging interfaces as well as Inline Services (e.g. ECS))

## IPv6 MTU Option Support in RA Message

In RFC-4861, there is a provision to send the Maximum Transmission Unit (MTU) in Router Advertisement (RA) messages. The P-GW now supports the sending of the IPv6 MTU option in RAs for IPv6 and IPv4v6 PDN types towards the UE. As a result, the UE can now send uplink data packets based on the configured MTU and perform data fragmentation at the source, if required. This feature also reduces the number of ICMPv6 *Packet Too Big Error* messages in the customer's network.

The MTU size is configurable via the Command Line Interface (CLI) on the GGSN and P-GW.

#### Supported Functionality

To support the IPv6 MTU Option in RA Message feature, the P-GW/GGSN supports the following functionality and behavior:

- The **ipv6 initial-router-advt option mtu value** command in *APN Configuration Mode* is available to enable/disable this feature per APN. By default, this feature is enabled for all APNs.
  - For the P-GW and SAEGW, IPv6 initial router advertisement option MTU value must be configured in *octets -integer 1280-2000*. The configured value is sent in the RA packet rather than the data tunnel MTU.



#### Important

This value is used only for advertisement in RA packet and the gateway need not enforce this value. The behaviour of 'default' and 'no' options of this CLI remains the same.

- For the P-GW and SAEGW, the session manager sends the MTU value that is configured via the CLI command **data-tunnel mtu 1280-2000** in *APN Configuration Mode*.
- For the GGSN, the RADIUS-returned value in the Framed-MTU Attribute Value Pair (AVP) takes precedence over the value configured via the **ppp mtu 100-2000** CLI command in *APN Configuration Mode*.
- For the GGSN, if the RADIUS-returned MTU value is less than the minimum IPv6 MTU, then the minimum IPv6 MTU value of 1280 is sent in the IPv6 MTU option field in RA messages.
- For the GGSN, if the **ppp mtu 100-2000** CLI command is configured with an MTU value of less than 1280, then the minimum IPv6 MTU value is sent in the IPv6 MTU option field in RA messages.

- When no MTU value comes from the RADIUS server and both the above mentioned CLI commands are not configured, the default value of 1500 is used for the MTU.
- Support for the MTU option in RA messages is available in the GGSN/P-GW/SAEGW.
- This feature is supported on the P-GW independent of interfaces such as s2a/s2b/s5/s8.
- The MTU option in RA messages is supported for both IPv6 and IPv4v6 PDN types.
- The MTU option in RA messages is available in the output of the **monitor protocol** command.
- The same MTU value is sent by the gateway in initial and periodic RA messages for a calling.
- The behavior of sending the IPv6 MTU option in RA for a PDN call is persistent across session recovery and ICSR switchover.
- Existing MTU-related data path behavior for the GGSN/P-GW/SAEGW is not changed.

### Restrictions/Limitations

Note the following restrictions/limitations for this feature:

- The GGSN/P-GW/SAEGW does not consider the GTP-U tunnel overhead while calculating the MTU value to be sent in the IPv6 MTU option in RAs. Therefore, the operator has to configure the **data-tunnel mtu** by considering the tunnel overhead. Refer to the *Link MTU Considerations* section in *Annex-C of 3GPP TS 23.060*.
- Existing MTU-related data path behavior for the GGSN/P-GW/SAEGW is unchanged.
- If there is a Gn/Gp Handover followed by session recovery, operators will see the following behavior: The stateless IPv6 session is recovered with the MTU value configured for the current GGSN/P-GW service after the handover. This is existing behavior if the feature is not configured. With this feature enabled, the same recovered MTU value will be sent in periodic RA messages after such a handover occurs when followed by session recovery.
- This feature is not supported for eHRPD. As a result, in scenarios where an LTE-to-eHRPD to LTE-Handover or eHRPD-to-LTE Handover occurs, a new stateless IPv6 session is re-created using the latest APN configuration.
- With this feature enabled, there is no support for an MTU value received by the gateway via the S6b interface.

## IPv6 Prefix-Based Search Support for LTE-WiFi Handoff

LTE-to-WiFi handoffs were failing for some UE devices for a specific customer during Inter-RAT testing for WiFi. The UE devices were using Stateless Address Auto Configuration. This issue was only seen from specific UE devices when the UE is sending the changed IPv6 address on Create Session Response (CSResp) messages during handoffs. Another vendor device had no issues for the LTE-to-WiFi handoff since it was sending the IPv6 address assigned initially during the Create Session Response (CSResp) from P-GW.

When the P-GW performed an IPv6 lookup of the existing LTE session based on the complete IPv6 128-bit address (Prefix + Intf ID), the handover would fail with the error EGTP\_CONTEXT\_NOT\_FOUND.

Now, the P-GW performs the IPv6 lookup of the existing LTE session during an LTE-WiFi handoff using only the IPv6 prefix (64-bit). Operators now will see seamless handovers on these calls for UE devices with



Stateless Address Auto Configuration. The P-GW will not reject the handoff request if the UE uses a different interface-ID from the one provided during call creation during handoffs for PDN types IPv6 and IPv4v6.



**Important** There are no changes on external interfaces. The only change as part of this feature is that the internal search to find the existing session is performed using the 64-bit IPv6 prefix during handoff.

### Restrictions/Limitations

With Stateless Auto Configuration, when the UE uses a different interface-ID from the one provided by P-GW. The UE then later moves to another location that results in an S1/X2 handover with an S-GW change. As result, the S-GW may have a different IPv6 address for a PDN from the one maintained by the P-GW (that is, the IP Address provided during initial attach) for the same UE. This can result in a difference in the servedPDPPDNAddress element in the CDR from the P-GW and S-GW.

This restriction is due to an existing limitation in the 3GPP Modify procedure, such as Modify Bearer Request/Modify Bearer Response, where an exchange of the changed UE IPv6 address is not supported between the P-GW and S-GW during the S1/X2 handover.

It is assumed that the mediation devices will look into the 64-bit prefix of the IPv6 address in CDRs for Stateless Auto Configuration devices.

## Local Break-Out

Provides a standards-based procedure to enable LTE operators to generate additional revenues by accepting traffic from visited subscribers based on roaming agreements with other mobile operators.

Local Breakout is a policy-based forwarding function that plays an important role in inter-provider roaming between LTE service provider networks. Local Breakout is determined by the SLAs for handling roaming calls between visited and home networks. In some cases, it is more beneficial to locally breakout a roaming call on a foreign network to the visited P-W rather than incur the additional transport costs to backhaul the traffic to the Home network.

If two mobile operators have a roaming agreement in place, Local Break-Out enables the visited user to attach to the V-PLMN network and be anchored by the local P-GW in the visited network. The roaming architecture relies on the HSS in the home network and also introduces the concept of the S9 policy signaling interface between the H-PCRF in the H-PLMN and the V-PCRF in the V-PLMN. When the user attaches to the EUTRAN cell and MME (Mobility Management Entity) in the visited network, the requested APN name in the S6a NAS signaling is used by the HSS in the H-PLMN to select the local S-GW (Serving Gateway) and P-GWs in the visited EPC network.

## Mapping High Throughput Sessions on Session Managers

Session managers are upgraded to manage several high throughput sessions without sharing the core and without creating a bottleneck on the CPU load.

The gateway – S-GW, SAEGW or P-GW, classifies a session as a high throughput session based on a DCNR flag present in the IE: FLAGS FOR USER PLANE FUNCTION (UPF) SELECTION INDICATION, in the Create Session Request. This DCNR flag is checkpointed and recovered by the gateway.

A high throughput session is placed on a session manager that has no other high throughput session. If all session manager are handling a high throughput session then these sessions are allocated using the Round-Robbin method.

**Note**

- The selection of session managers for non-high throughput sessions remains the same in the existing setup.
- Non-high throughput sessions are placed along with the high throughput sessions on the same session manager.

**Limitations**

Managing high throughput sessions on a session manager has the following limitations:

- The following scenarios may result in placing two high throughput sessions on a session manager:
  - Initial attach from eHRPD/2G/3G sessions.
  - IP addresses – both IPv4 and IPv6, are placed on the same session manager.
  - For an S-GW, the second Create Session Request (PDN) from a UE lands directly on a session manager which has the first PDN of the same UE.
  - For a collapsed call, the second Create Session Request (PDN) from a UE lands directly on a session manager which has the first PDN of the same UE.
  - In a Multi-PDN call from a UE that is capable of DCNR. For example: VoLTE and Internet capable of DCN will be placed on the same session manager.
- The DCNR flag is not defined by 3GPP for Wi-Fi. Therefore, a session cannot be assigned to a session manager during a Wi-Fi to LTE handover with the DCNR flag set.
- This feature manages and supports distribution of high throughput sessions on a session manager but does not guarantee high throughput for a subscriber.
- In some cases, the round robin mechanism could place a high throughput session on a session manager that was already loaded with other high throughput sessions.

## MPLS EXP Marking of User Plane Traffic

Similar to 802.1p marking, MPLS EXP bit marking is supported for Enterprise APNs that use MPLS tunneling on the SGi interface on the P-GW. The QoS marking used in the LTE/EPC network (QCI per EPS bearer) is mapped to the 802.1p and MPLS EXP bit marking between the P-GW and L2/EPC switch and MPLS/PE routers (this is applicable to the upstream direction, from the P-GW to the Network). MPLS EXP marking related configuration is available as part of the QCI-QOS configuration table. MPLS EXP marking is selected based on QCI of the bearer to which that packet belongs.

**Important**

The SAEGW does not support non-standard QCI values. QCI values 1 through 9 are standard values and are defined in 3GPP TS 23.203; the SAEGW supports these standard values.

## Mobile IP Registration Revocation

Mobile IP registration revocation functionality provides the following benefits:

- Timely release of Mobile IP resources at the HSGW and/or P-GW
- Accurate accounting
- Timely notification to mobile node of change in service

Registration Revocation is a general mechanism whereby either the P-GW or the HSGW providing Mobile IP functionality to the same mobile node can notify the other mobility agent of the termination of a binding. Mobile IP Registration Revocation can be triggered at the HSGW by any of the following:

- Session terminated with mobile node for whatever reason
- Session renegotiation
- Administrative clearing of calls
- Session Manager software task outage resulting in the loss of HSGW sessions (sessions that could not be recovered)



---

**Important**

Registration Revocation functionality is also supported for Proxy Mobile IP. However, only the P-GW can initiate the revocation for Proxy-MIP calls.

---



---

**Important**

For more information on MIP registration revocation support, refer to the *Mobile IP Registration Revocation* chapter in this guide.

---

## MTU Size PCO

UEs usually use a hardcoded MTU size for IP communication. If this hardcoded value is not in sync with the network supported value, it can lead to unnecessary fragmentation of packets sent by the UE. Thus, in order to avoid unnecessary fragmentation, this feature helps in using the network-provided MTU size instead of the hardcoded MTU in UE.

3GPP defined a new PCO option in Release 10 specifications for the network to be able to provide an IPv4 MTU size to the UE. P-GW supports an option to configure a IPv4 Link MTU size in the APN profile.

If the UE requests IPv4 Link MTU size in the PCO options during Initial Attach or PDN connectivity request, the P-GW will provide the preconfigured value based on the APN.

If the MTU size configuration on APN is changed, the new MTU size will take effect only for new PDN connections and initial attaches. P-GW will not update for the existing PDN connections.

If the UE does not request IPv4 Link MTU size, P-GW will not include the IPv4 Link MTU size.

## Multiple PDN Support

Enables an APN-based user experience that enables separate connections to be allocated for different services including IMS, Internet, walled garden services, or off-deck content services.

The MAG function on the S-GW can maintain multiple PDN or APN connections for the same user session. The MAG runs a single node level Proxy Mobile IPv6 tunnel for all user sessions toward the LMA function of the P-GW. When a user wants to establish multiple PDN connections, the MAG brings up the multiple PDN connections over the same PMIPv6 session to one or more P-GW LMA's. The P-GW in turn allocates separate IP addresses (Home Network Prefixes) for each PDN connection and each one can run one or multiple EPC default & dedicated bearers. To request the various PDN connections, the MAG includes a common MN-ID and separate Home Network Prefixes, APNs and a Handover Indication Value equal to one in the PMIPv6 Binding Updates.



---

**Important** Up to 11 multiple PDN connections are supported.

---

## Node Functionality GTP Echo

This feature helps exchange capabilities of two communicating GTP nodes, and uses the new feature based on whether it is supported by the other node.

This feature allows S-GW to exchange its capabilities (MABR, PRN, NTSR) with the peer entities through ECHO messages. By this, if both the peer nodes support some common features, then they can make use of new messages to communicate with each other.

With new "node features" IE support in ECHO request/response message, each node can send its supported features (MABR, PRN, NTSR). This way, S-GW can learn the peer node's supported features. S-GW's supported features can be configured by having some configuration at the service level.

If the S-GW wants to use new message, such as P-GW Restart Notification, then the S-GW should check if the peer node supports this new feature or not. If the peer does not support it, then the S-GW should fall back to old behavior.

If the S-GW receives a new message from the peer node, and if S-GW does not support this new message, then the S-GW should ignore it. If the S-GW supports the particular feature, then it should handle the new message as per the specification.

## Non-Optimized e-HRPD to Native LTE (E-UTRAN) Mobility Handover

This feature enables a seamless inter-technology roaming capability in support of dual mode e-HRPD/e-UTRAN access terminals.

The non-optimized inter-technology mobility procedure is rooted at the P-GW as the mobility anchor point for supporting handovers for dual radio technology e-HRPD/E-UTRAN access terminals. To support this type of call handover, the P-GW supports handoffs between the GTP-based S5/S8 (GTPv2-C / GTPv1-U) and PMIPv6 S2a tunneled connections. It also provisions IPv4, IPv6, or dual stack IPv4/IPv6 PDN connections from a common address pool and preserves IP addresses assigned to the UE during inter-technology handover. In the current release, the native LTE (GTP-based) P-GW service address is IPv4-based, while the e-HRPD (PMIP) address is an IPv6 service address.

During the initial network attachment for each APN that the UE connects to, the HSS returns the FQDN of the P-GW for the APN. The MME uses DNS to resolve the P-GW address. When the PDN connection is established in the P-GW, the P-GW updates the HSS with the IP address of the P-GW on PDN establishment through the S6b authentication process. When the mobile user roams to the e-HRPD network, the HSS returns the IP address of the P-GW in the P-GW Identifier through the STa interface and the call ends up in the same P-GW. The P-GW is also responsible for initiating the session termination on the serving access connection after the call handover to the target network.

During the handover procedure, all dedicated EPS bearers must be re-established. On LTE- handovers to a target e-HRPD access network, the dedicated bearers are initiated by the mobile access terminal. In contrast, on handovers in the opposite direction from e-HRPD to LTE access networks, the dedicated bearers are network initiated through Gx policy interactions with the PCRF server.

Finally, in order to support the inter-technology handovers, the P-GW uses common interfaces and Diameter endpoint addresses for the various reference points:

- S6b: Non-3GPP authentication
- Gx: QoS Policy and Charging
- Rf: Offline Charging

All three types of sessions are maintained during call handovers. The bearer binding will be performed by the HSGW during e-HRPD access and by the P-GW during LTE access. Thus, the Bearer Binding Event Reporting (BBERF) function needs to migrate between the P-GW and the HSGW during the handover. The HSGW establishes a Gxa session during e-HRPD access for bearer binding and releases the session during LTE access. The HSGW also maintains a limited context during the e-HRPD <->LTE handover to reduce latency in the event of a quick handover from the LTE RAN back to the e-HRPD network.



#### Important

For more information on handoff interfaces, refer to the *Supported Logical Network Interfaces (Reference Points)* section in this chapter.

## Online/Offline Charging

The Cisco EPC platform offers support for online and offline charging interactions with external OCS and CGF/CDF servers.

### Online Charging

#### Gy/Ro Reference Interfaces

The StarOS 9.0 online prepaid reference interface provides compatibility with the 3GPP TS 23.203, TS 32.240, TS 32.251 and TS 32.299 specifications. The Gy/Ro reference interface uses Diameter transport and IPv6 addressing. Online charging is a process whereby charging information for network resource usage must be obtained by the network in order for resource usage to occur. This authorization is granted by the Online Charging System (OCS) upon request from the network. The P-GW uses a charging characteristics profile to determine whether to activate or deactivate online charging. Establishment, modification or termination of EPS bearers is generally used as the event trigger on the PCRF to activate online charging PCC rules on the P-GW.

When receiving a network resource usage request, the network assembles the relevant charging information and generates a charging event towards the OCS in real-time. The OCS then returns an appropriate resource

usage authorization that may be limited in its scope (e.g. volume of data or duration based). The OCS assigns quotas for rating groups and instructs the P-GW whether to continue or terminate service data flows or IP CAN bearers.

The following Online Charging models and functions are supported:

- Time based charging
- Volume based charging
- Volume and time based charging
- Final Unit Indication and termination or redirection of service data flows when quota is consumed
- Reauthorization triggers to rearm quotas for one or more rating groups using multi-service credit control (MSCC) instances
- Event based charging
- Billing cycle bandwidth rate limiting: Charging policy is enforced through interactions between the PDN GW and Online Charging Server. The charging enforcement point periodically conveys accounting information for subscriber sessions to the OCS and it is debited against the threshold that is established for the charging policy. Subscribers can be assigned a max usage for their tier (gold, silver, bronze for example), the usage can be tracked over a month, week, day, or peak time within a day. When the subscriber exceeds the usage limit, bandwidth is either restricted for a specific time period, or dropped depending on their tier of service.
- Fair usage controls

## Offline Charging

### Ga/Gz Reference Interfaces

The Cisco P-GW supports 3GPP-compliant offline charging as defined in TS 32.251, TS 32.297 and 32.298. Whereas the S-GW generates SGW-CDRs to record subscriber level access to PLMN resources, the P-GW creates PGW-CDRs to record user access to external networks. Additionally, when Gn/Gp interworking with pre-release SGSNs is enabled, the GGSN service on the P-GW records G-CDRs to record user access to external networks.

To provide subscriber level accounting, the Cisco S-GW and P-GWs support integrated Charging Transfer Functions (CTF) and Charging Data Functions (CDF). Each gateway uses Charging-ID's to distinguish between default and dedicated bearers within subscriber sessions. The Ga/Gz reference interface between the CDF and CGF is used to transfer charging records via the GTPP protocol. In a standards based implementation, the CGF consolidates the charging records and transfers them via an FTP/S-FTP connection over the Bm reference interface to a back-end billing mediation server. The Cisco EPC gateways also offer the ability to FTP/S-FTP charging records between the CDF and CGF server. CDR records include information such as Record Type, Served IMSI, ChargingID, APN Name, TimeStamp, Call Duration, Served MSISDN, PLMN-ID, etc. The ASR 5x00 platform offers a local directory to enable temporary file storage and buffer charging records in persistent memory located on a pair of dual redundant RAID hard disks. Each drive includes 147GB of storage and up to 100GB of capacity is dedicated to storing charging records. For increased efficiency it is also possible to enable file compression using protocols such as GZIP. The Offline Charging implementation offers built-in heart beat monitoring of adjacent CGFs. If the Cisco P-GW has not heard from the neighbor CGF within the configurable polling interval, they will automatically buffer the charging records on the local drives until the CGF reactivates itself and is able to begin pulling the cached charging records.

The P-GW supports a Policy Charging Enforcement Function (PCEF) to enable Flow Based Bearer Charging (FBC) via the Gy reference interface to adjunct OCS servers (See Online Charging description above).

#### **Rf Reference Interface**

The Cisco EPC platforms also support the Rf reference interface to enable direct transfer of charging files from the CTF function of the P-GW to external CDF/CGF servers. This interface uses Diameter Accounting Requests (Start, Stop, Interim, and Event) to transfer charging records to the CDF/CGF. Each gateway relies on triggering conditions for reporting chargeable events to the CDF/CGF. Typically as EPS bearers are activated, modified or deleted, charging records are generated. The EPC platforms include information such as Subscription-ID (IMSI), Charging-ID (EPS bearer identifier) and separate volume counts for the uplink and downlink traffic.

## **Optimization for egtpinmgr Recovery**

Restarting the egtpinmgr task took a significant amount of time for recovery. Hence, the outage time when the GGSN, P-GW, SAEGW, and S-GW were unable to accept any new calls during egtpinmgr recovery was high.

The software is 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.

## **P-CSCF Recovery**

Supports spec-based mechanism to support P-CSCF discovery for GTP-based S2b interface for WiFi integration. This is required for Voice over WiFi service.

The P-GW can store the P-CSCF FQDN received during the initial registration with the AAA. Upon receiving the P-CSCF restoration flag from the MME/S-GW, the P-GW performs a new DNS query using the existing P-CSCF FQDN to provide the updated list of three P-CSCF IP addresses using PCO.

## **Peer GTP Node Profile Configuration Support**

Provides flexibility to the operators to have different configuration for GTP-C and Lawful Intercept, based on the type of peer or the IP address of the peer.

Peer profile feature allows flexible profile based configuration to accommodate growing requirements of customizable parameters with default values and actions for peer nodes of P-GW. With this feature, configuration of GTP-C parameters and disabling/enabling of Lawful Intercept per MCC/MNC or IP address based on rules defined.

A new framework of peer-profile and peer-map is introduced. Peer-profile configuration captures the GTP-C specific configuration and/or Lawful Intercept enable/disable configuration. GTP-C configuration covers GTP-C retransmission (maximum number of retries and retransmission timeout) and GTP echo configuration. Peer-map configuration matches the peer-profile to be applied to a particular criteria. Peer-map supports criteria like MCC/MNC (PLMN-ID) of the peer or IP-address of the peer. Peer-map can then be associated with P-GW service.

Intent of this feature is to provide flexibility to operators to configure a profile which can be applied to a specific set of peers. For example, have a different retransmission timeout for foreign peers as compared to home peers.

## Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters

### Support for QCI and ARP Visibility

As of StarOS release 20.2, the software has been enhanced to support the viewing of QoS statistics on a Quality of Service Class Index (QCI) and Allocation and Retention Priority (ARP) basis.

ARP is a 3GPP mechanism for dropping or downgrading lower-priority bearers in situations where the network becomes congested. The network looks at the ARP when determining if new dedicated bearers can be established through the radio base station. QCI is an operator provisioned value that controls bearer level packet forwarding treatments.

This enhancement enables operators to monitor QoS statistics that identify multiple services running with the same QCI value. In addition, packet drop counters have been introduced to provide the specific reason the Enhanced Charging Service (ECS) dropped a packet. The packet drop counters provide output on a per ARP basis. This provides additional information that operators can use to troubleshoot and identify network issues that may be affecting service.




---

**Important** For the ARP value only the priority level value in the Allocation/Retention Priority (ARP) Information Element (IE) is considered. Pre-emption Vulnerability (PVI) and Pre-emption Capability (PCI) flags in the ARP IE are not considered.

---

The existing **show apn statistics name** *apn-name* and **show apn statistics Exec Mode** CLI commands have been enhanced. The output of these commands now provides visibility for QoS statistics on a QCI/ARP basis.




---

**Important** For more detailed information, refer to the *Extended QCI Options* chapter in this guide.

---

### Licensing

ARP Granularity for QCI Level Counters is a license-controlled feature. Per QCI Packet Drop Counters functionality does not require a license. Contact your Cisco account or support representative for licensing details.

## PMIPv6 Heartbeat

Proxy Mobile IPv6 (PMIPv6) is a network-based mobility management protocol to provide mobility without requiring the participation of the mobile node in any PMIPv6 mobility related signaling. The core functional entities Mobile Access Gateway (MAG) and the Local Mobility Anchor (LMA) set up tunnels dynamically to manage mobility for a mobile node.

Path management mechanism through Heartbeat messages between the MAG and LMA is important to know the reachability of the peers, to detect failures, quickly inform peers in the event of a recovery from node failures, and allow a peer to take appropriate action.

PMIP heartbeats from the HSGW to the P-GW are supported per RFC 5847. Refer to the **heartbeat** command in the LMA Service mode or MAG Service mode respectively to enable this heartbeat and configure the heartbeat variables.



## Proxy Mobile IPv6 (S2a)

Provides a mobility management protocol to enable a single LTE-EPC core network to provide the call anchor point for user sessions as the subscriber roams between native EUTRAN and non-native e-HRPD access networks

S2a represents the trusted non-3GPP interface between the LTE-EPC core network and the evolved HRPD network anchored on the HSGW. In the e-HRPD network, network-based mobility provides mobility for IPv6 nodes without host involvement. Proxy Mobile IPv6 extends Mobile IPv6 signaling messages and reuses the HA function (now known as LMA) on the P-GW. This approach does not require the mobile node to be involved in the exchange of signaling messages between itself and the Home Agent. A proxy mobility agent (e.g. MAG function on HSGW) in the network performs the signaling with the home agent and does the mobility management on behalf of the mobile node attached to the network.

The S2a interface uses IPv6 for both control and data. During the PDN connection establishment procedures the P-GW allocates the IPv6 Home Network Prefix (HNP) via Proxy Mobile IPv6 signaling to the HSGW. The HSGW returns the HNP in router advertisement or based on a router solicitation request from the UE. PDN connection release events can be triggered by either the UE, the HSGW or the P-GW.

In Proxy Mobile IPv6 applications the HSGW (MAG function) and P-GW (LMA function) maintain a single shared tunnel and separate GRE keys are allocated in the PMIP Binding Update and Acknowledgment messages to distinguish between individual subscriber sessions. If the Proxy Mobile IP signaling contains Protocol Configuration Options (PCOs) it can also be used to transfer P-CSCF or DNS server addresses.

## QoS Bearer Management

Provides a foundation for contributing towards improved Quality of User Experience (QoE) by enabling deterministic end-to-end forwarding and scheduling treatments for different services or classes of applications pursuant to their requirements for committed bandwidth resources, jitter and delay. In this way, each application receives the service treatment that users expect.

An EPS bearer is a logical aggregate of one or more Service Data Flows (SDFs), running between a UE and a P-GW in case of GTP-based S5/S8, and between a UE and HSGW in case of PMIP-based S2a connection. An EPS bearer is the level of granularity for bearer level QoS control in the EPC/E-UTRAN. The Cisco P-GW maintains one or more Traffic Flow Templates (TFT's) in the downlink direction for mapping inbound Service Data Flows (SDFs) to EPS bearers. The P-GW maps the traffic based on the downlink TFT to the S5/S8 bearer. The Cisco PDN GW offers all of the following bearer-level aggregate constructs:

**QoS Class Identifier (QCI):** An operator provisioned value that controls bearer level packet forwarding treatments (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc). The Cisco EPC gateways also support the ability to map the QCI values to DiffServ code points in the outer GTP tunnel header of the S5/S8 connection. Additionally, the platform also provides configurable parameters to copy the DSCP marking from the encapsulated payload to the outer GTP tunnel header.



### Important

The SAEGW does not support non-standard QCI values. QCI values 1 through 9 are standard values and are defined in 3GPP TS 23.203; the SAEGW supports these standard values.

**Guaranteed Bit Rate (GBR):** A GBR bearer is associated with a dedicated EPS bearer and provides a guaranteed minimum transmission rate in order to offer constant bit rate services for applications such as interactive voice that require deterministic low delay service treatment.

**Maximum Bit Rate (MBR):** The MBR attribute provides a configurable burst rate that limits the bit rate that can be expected to be provided by a GBR bearer (e.g. excess traffic may get discarded by a rate shaping function). The MBR may be greater than or equal to the GBR for a given Dedicated EPS bearer.

**Aggregate Maximum Bit Rate (AMBR):** AMBR denotes a bit rate of traffic for a group of bearers destined for a particular PDN. The Aggregate Maximum Bit Rate is typically assigned to a group of Best Effort service data flows over the Default EPS bearer. That is, each of those EPS bearers could potentially utilize the entire AMBR, e.g. when the other EPS bearers do not carry any traffic. The AMBR limits the aggregate bit rate that can be expected to be provided by the EPS bearers sharing the AMBR (e.g. excess traffic may get discarded by a rate shaping function). AMBR applies to all Non-GBR bearers belonging to the same PDN connection. GBR bearers are outside the scope of AMBR.

**Policing:** The Cisco P-GW offers a variety of traffic conditioning and bandwidth management capabilities. These tools enable usage controls to be applied on a per-subscriber, per-EPS bearer or per-PDN/APN basis. It is also possible to apply bandwidth controls on a per-APN AMBR capacity. These applications provide the ability to inspect and maintain state for user sessions or Service Data Flows (SDFs) within them using shallow L3/L4 analysis or high touch deep packet inspection at L7. Metering of out-of-profile flows or sessions can result in packet discards or reducing the DSCP marking to Best Effort priority.

## RADIUS Support

Provides a mechanism for performing authorization, authentication, and accounting (AAA) for subscriber PDP contexts based on the following standards:

- RFC-2618, RADIUS Authentication Client MIB, June 1999
- RFC-2620, RADIUS Accounting Client MIB, June 1999
- RFC-2865, Remote Authentication Dial In User Service (RADIUS), June 2000
- RFC-2866, RADIUS Accounting, June 2000
- RFC-2867, RADIUS Accounting Modifications for Tunnel Protocol Support, June 2000
- RFC-2868, RADIUS Attributes for Tunnel Protocol Support, June 2000
- RFC-2869, RADIUS Extensions, June 2000

The Remote Authentication Dial-In User Service (RADIUS) protocol is used to provide AAA functionality for subscriber PDP contexts. (RADIUS accounting is optional since GTPP can also be used.)

Within contexts configured on the system, there are AAA and RADIUS protocol-specific parameters that can be configured. The RADIUS protocol-specific parameters are further differentiated between RADIUS Authentication server RADIUS Accounting server interaction.

Among the RADIUS parameters that can be configured are:

- **Priority:** Dictates the order in which the servers are used allowing for multiple servers to be configured in a single context.
- **Routing Algorithm:** Dictate the method for selecting among configured servers. The specified algorithm dictates how the system distributes AAA messages across the configured AAA servers for new sessions. Once a session is established and an AAA server has been selected, all subsequent AAA messages for the session will be delivered to the same server.

In the event that a single server becomes unreachable, the system attempts to communicate with the other servers that are configured. The system also provides configurable parameters that specify how it should behave should all of the RADIUS AAA servers become unreachable.

The system provides an additional level of flexibility by supporting the configuration RADIUS server groups. This functionality allows operators to differentiate AAA services for subscribers based on the APN used to facilitate their PDP context.

In general, 128 AAA Server IP address/port per context can be configured on the system and it selects servers from this list depending on the server selection algorithm (round robin, first server). Instead of having a single list of servers per context, this feature provides the ability to configure multiple server groups. Each server group, in turn, consists of a list of servers.

This feature works in following way:

- All RADIUS authentication/accounting servers configured at the context-level are treated as part of a server group named "default". This default server group is available to all subscribers in that context through the realm (domain) without any configuration.
- It provides a facility to create "user defined" RADIUS server groups, as many as 399 (excluding "default" server group), within a context. Any of the user defined RADIUS server groups are available for assignment to a subscriber through the APN configuration within that context.

Since the configuration of the APN can specify the RADIUS server group to use as well as IP address pools from which to assign addresses, the system implements a mechanism to support some in-band RADIUS server implementations (i.e. RADIUS servers which are located in the corporate network, and not in the operator's network) where the NAS-IP address is part of the subscriber pool. In these scenarios, the P-GW supports the configuration of the first IP address of the subscriber pool for use as the RADIUS NAS-IP address.



#### Important

For more information on RADIUS AAA configuration, if you are using StarOS 12.3 or an earlier release, refer to the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

## Removal of Private Extension-based Overcharging Support

Prior to StarOS release 21.0, the Cisco P-GW and S-GW supported the sending and receiving of overcharging protection data via both a non-3GPP Private Extension Information Element (IE), and a 3GPP Indication IE.

However, since 3GPP support to exchange overcharging protection data exists, no operators were using the Overcharging Private Extension (OCP) based solution. It was also reported by some operators that the Private Extension IE carrying overcharging protection data sent by the P-GW was leading to issues at S-GWs of other vendors.

As a result, support for Private Extension-based Overcharging Support is being removed from the Cisco P-GW and S-GW. This has the benefit of preventing unexpected scenarios occurring due to the decoding of a Private Extension ID carrying overcharging protection data at the P-GW/S-GW of other vendors.

### Previous and New Behavior for the P-GW

The following table describes the previous and new behavior at the P-GW for Create Session Request (CSReq) and Create Session Response (CSRsp) messages due to the removal of Private Extension Overcharging Support.

**Table 8: Previous and New Behavior: CSReq and CSRsp Messages at P-GW Due to Removal of Private Extension Overcharging Support**

<b>Scenario No.</b>	<b>IE Carrying OCP Capability Received from S-GW in CSReq</b>	<b>Old Behavior: IE carrying OCP Capability Sent to S-GW in CSRsp</b>	<b>New Behavior: IE Carrying OCP Capability Sent to S-GW in CSRsp</b>
1	Indication IE	Indication IE	No change. Indication IE will be sent in CSRsp.
2	Private Extension IE	Both Private Extension and Indication IEs.	Private Extension IE received from S-GW is ignored. Indication IE is sent in CSRsp.
3	None	Both Private Extension and Indication IEs.	Only Indication IE is sent in CSRsp.
4	Both Private Extension and Indication IEs.	Indication IE	Private Extension IE received from S-GW is ignored. Only Indication IE is sent in CSRsp.

The following table describes the previous and new behavior in Modify Bearer Request (MBReq) and Modify Bearer Response (MBRsp) messages due to the removal of Private Extension Overcharging Support.

**Table 9: Previous and New Behavior: MBReq and MBRsp Messages at P-GW Due to Removal of Private Extension Overcharging Support**

<b>Scenario No.</b>	<b>IE carrying OCP Capability Received from S-GW in MBReq</b>	<b>Old Behavior: IE Carrying OCP Capability Sent to S-GW in MBRsp</b>	<b>New Behavior: IE Carrying OCP Capability Sent to S-GW in MBRsp</b>
1	Indication IE	Indication IE	No Change. Indication IE is sent in MBRsp messages.
2	Private Extension IE	Private Extension IE	Private Extension IE received from S-GW is ignored. Indication IE is sent in MBRsp message.
3	None	Both Private Extension and Indication IEs.	Only the Indication IE is sent in MBRsp message.
4	Both Private Extension and Indication IEs.	Indication IE	Private Extension IE received from the S-GW is ignored. Only the Indication IE is sent in the MBRsp message.

### Previous and New Behavior for the S-GW

The following table describes the previous and new behavior in Create Session Response (CSRsp) messages at the S-GW due to the removal of Private Extension Overcharging Support.

**Table 10: Previous and New Behavior: CSRsp Messages at the S-GW Due to the Removal of Private Extension Overcharging Support**

Scenario No.	Old Behavior: IE Carrying OCP Capability Received from P-GW in CSRsp	New Behavior: IE Carrying OCP Capability Received from PGW in CSRsp	Old Behavior: IE Carrying OCP Capability Sent to MME in CSRsp	New Behavior: IE Carrying OCP Capability Sent to MME in CSRsp
12	Indication IE	No change. OCP capability received as part of the Indication IE is accepted.	Indication IE	No change. Indication IE is sent in CSRsp.
2	Private Extension IE	OCP capability received as part of Private Extension IE is ignored.	If gtpc private-extension overcharge-protection is disabled at egtpc service level: <b>Private Extension IE</b> .  If gtpc private-extension overcharge-protection is enabled at egtpc service level: <b>Indication IE</b> .	Since the CLI command is deprecated, then the Private Extension IE is forwarded to the MME in CSRsp as would be done for any unknown Private Extension IE.
3	Both Private Extension IE and Indication IE	OCP capability received as part of the Private Extension IE is ignored. Only OCP capability received as a part of the Indication IE is accepted.	If gtpc private-extension overcharge-protection is disabled at egtpc service level: <b>Private Extension IE and Indication IE</b> .  If gtpc private-extension overcharge-protection is enabled at egtpc service level: <b>Indication IE</b> .	Since the CLI command is deprecated, then the Private Extension IE is forwarded to the MME in CSRsp as would be done for any unknown Private Extension IE.
4	None	No change.	None	No change.

The following table describes the previous and new behavior in Modify Bearer Response (MBRsp) messages at the S-GW due to the removal of Private Extension Overcharging Support.

**Table 11: Previous Behavior and New Behavior: MBRsp Messages at the S-GW Due to the Removal of Private Extension Overcharging Support**

Scenario No.	Old Behavior: IE Carrying OCP Capability Received from P-GW in MBRsp	New Behavior: IE Carrying OCP Capability Received from P-GW in MBRsp	Old Behavior: IE Carrying OCP Capability Sent to MME in MBRsp	New Behavior: IE Carrying OCP Capability Sent to MME in MBRsp
1	Indication IE	No change. OCP capability received as part of Indication IE is accepted.	Indication IE	No change. Indication IE is sent in MBRsp.

Scenario No.	Old Behavior: IE Carrying OCP Capability Received from P-GW in MBRsp	New Behavior: IE Carrying OCP Capability Received from P-GW in MBRsp	Old Behavior: IE Carrying OCP Capability Sent to MME in MBRsp	New Behavior: IE Carrying OCP Capability Sent to MME in MBRsp
2	Private Extension IE	OCP capability received as part of Private Extension IE is ignored.	If gtpc private-extension overcharge-protection is disabled at egtpc service level: <b>None</b> .  If gtpc private-extension overcharge-protection is enabled at egtpc service level: <b>Indication IE</b> .	Since the CLI command is deprecated, neither one of the two IEs is sent in the MBRsp to the MME for the OCP capability.
3	Both Private Extension ID and Indication IE	OCP capability received as part of the Private Extension IE is ignored. Only the OCP capability received as part of the Indication IE is accepted.	Indication IE	No change. Indication IE is sent in MBRsp.
4	None	None	None	No change.

**Important**

In StarOS releases 21.0 and later, the S-GW will send a MBReq message with only the indication IE for the Pause/Start Charging procedure. The private extension IE is not sent.

**Important**

If the S-GW receives only the private extension IE from the P-GW in the CSRsp/MBRsp message, then the S-GW ignores the private extension IE. As a result, the S-GW assumes that Overcharging Protection is NOT enabled for the P-GW. So, in this scenario, even if the overcharging condition is met at the S-GW, the S-GW will not send a MBReq message for Charging pause to the P-GW.

## S-GW Restoration Support

S-GW Restoration helps in handling the S-GW failure in the EPC network in a graceful manner. It allows affected PDNs due to S-GW failure to be restored by selecting another S-GW to serve the affected PDNs, thus avoiding unnecessary flooding of signaling for PDN cleanup.

S-GW Restoration is based on 3GPP Release 11. It requires enhancements at P-GW for maintaining the sessions in case path failure is detected or when S-GW restart is detected via recovery IE on GTP-C signaling. P-GW shall ensure that any dropped packets in this scenario are not charged and P-GW shall reject any bearer addition/modification request received for the PDN connection maintained after the S-GW failure detection, till the time that PDN is restored again.



**Important** If the S-GW Restoration feature is configured and enabled for a P-GW that is associated with an SAE GW service, the feature supports Pure-P calls only.

Once the session has been restored by the MME (i.e., P-GW receives a Modify Bearer Request from the restarted S-GW or a different S-GW), P-GW shall resume forwarding any received downlink data and start charging them.

When subscriber is in S-GW restoration phase, all RARs (except for Session Termination) will be rejected by PCEF. P-GW will reject all internal updates which can trigger CCR-U towards PCRF. P-GW shall trigger a CCR U with AN-GW-Change for the PDNs that are restored if the S-GW has changed on restoration.



**Important** Only the MME/S4-SGSN triggered S-GW restoration procedure is supported.

S-GW restoration detection based on GTP-U path failure shall not be considered for this release. GTP-C path failure detection should be enabled for enabling this feature.

MME/S4-SGSN is locally configured to know that P-GW in the same PLMN supports the S-GW restoration feature. When this feature is enabled at P-GW, it shall support it for all S-GWs/MMEs.

For more details on this feature, refer to the *S-GW Restoration Support* chapter in this guide.

## Source IP Address Validation

Insures integrity between the attached subscriber terminal and the P-GW by mitigating the potential for unwanted spoofing or man-in-the-middle attacks.

The P-GW includes local IPv4/IPv6 address pools for assigning IP addresses to UEs on a per-PDN basis. The P-GW defends its provisioned address bindings by insuring that traffic is received from the host address that it has awareness of. In the event that traffic is received from a non-authorized host, the P-GW includes the ability to block the non-authorized traffic. The P-GW uses the IPv4 source address to verify the sender and the IPv6 source prefix in the case of IPv6.

## SRVCC PS-to-CS Handover Indication Support

This feature helps in notifying the PCRF about the exact reason for PCC rule deactivation on Voice bearer deletion. This exact cause will help the PCRF to then take further action appropriately.

This feature ensures complete compliance for SRVCC, including support for PS-to-CS handover indication when voice bearers are released. The support for SRVCC feature was first added in StarOS Release 12.2.

SRVCC service for LTE comes into the picture when a single radio User Equipment (UE) accessing IMS-anchored voice call services switches from the LTE network to the Circuit Switched domain while it is able to transmit or receive on only one of these access networks at a given time. This removes the need for a UE to have multiple Radio Access Technology (RAT) capability.

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

If the IP-CAN bearer termination is caused by the PS to CS handover, the PCEF may report 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, which indicates if the bearer is selected for PS to CS continuity, is not added.

## Subscriber Level Trace

Provides a 3GPP standards-based session level trace function for call debugging and testing new functions and access terminals in an LTE environment.

As a complement to Cisco's protocol monitoring function, the P-GW supports 3GPP standards based session level trace capabilities to monitor all call control events on the respective monitored interfaces including S5/S8, S2a, SGi, and Gx. The trace can be initiated using multiple methods:

- Management initiation via direct CLI configuration
- Management initiation at HSS with trace activation via authentication response messages over S6a reference interface
- Signaling based activation through signaling from subscriber access terminal



### Important

Once the trace is provisioned, it can be provisioned through the access cloud via various signaling interfaces.

The session level trace function consists of trace activation followed by triggers. The time between the two events is treated much like Lawful Intercept where the EPC network element buffers the trace activation instructions for the provisioned subscriber in memory using camp-on monitoring. Trace files for active calls are buffered as XML files using non-volatile memory on the local dual redundant hard drives on the ASR 5500 platform. The Trace Depth defines the granularity of data to be traced. Six levels are defined including Maximum, Minimum and Medium with ability to configure additional levels based on vendor extensions.

All call control activity for active and recorded sessions is sent to an off-line Trace Collection Entity (TCE) using a standards-based XML format over a FTP or secure FTP (SFTP) connection. In the current release the IPv4 interfaces are used to provide connectivity to the TCE. Trace activation is based on IMSI or IMEI. Once a subscriber level trace request is activated it can be propagated via the S5/S8 signaling to provision the corresponding trace for the same subscriber call on the P-GW. The trace configuration will only be propagated if the P-GW is specified in the list of configured Network Element types received by the S-GW. Trace configuration can be specified or transferred in any of the following message types:

- S5/S8: Create Session Request
- S5/S8: Modify Bearer Request
- S5/S8: Trace Session Activation (New message defined in TS 32.422)

**Performance Goals:** As subscriber level trace is a CPU intensive activity the max number of concurrently monitored trace sessions per Cisco P-GW is 32. Use in a production network should be restricted to minimize the impact on existing services.

3GPP tracing was enhanced in StarOS Release 15.0 to increase the number of simultaneous traces to 1000. The generated trace files are forwarded to external trace collection entity at regular intervals through (S)FTP



if "push" mode is enabled. If the push mode is not used, the files are stored on the local hard drive and must be pulled off by the TCE using FTP or SFTP.



**Important** The number of session trace files generated would be limited by the total available hard disk capacity.

## 3GPP Tracing to Intercept Random Subscriber

Previously, a subscriber identifier like IMSI was required in order to enable trace. Sometimes operators want to enable a trace without knowing the subscriber ID. For example, an operator may want to monitor the next "n" number of calls, or monitor subscribers in a particular IMSI range.

3GPP tracing was enhanced in StarOS Release 15.0 to intercept random subscribers with this feature. The current session trace feature is either signaling or management based, which is very specific to a particular subscriber. The requirement is to trace random subscribers which are not explicitly linked or identified by IMSI in GTP messages or configured through CLI.

The random subscribers could be in an IMSI range, context activation in particular time intervals, etc.

The session trace is activated on demand for a limited period of time for specific analysis purposes. The maximum limit would restrict the number of random subscriber tracing. Random session trace will be given priority over signaling and management-based session trace.

## Support for One Million S1-U Peers on the S-GW

Due to customer business requirements and production forecasts, support has been added to the StarOS for one million S1-U connections on a single S-GW.

The S1-U interface is the user plane interface carrying user data between an eNodeB and an S-GW received from the terminal. The StarOS now has the capability to scale the number of S1-U peers to one million per VPN context.

A new CLI command has been added to enable operators to set the number of S1-U peers for which statistics should be collected. The limit is restricted to less than one million peers (128k) due to StarOS memory limitations.

### How it Works

The gtpumgr uses the following guidelines while allocating peers:

- When a session installation comes from the Session Manager, a peer is created. If statistics are maintained at the Session Manager, the gtpumgr also creates the peer record with the statistics.
- Peer records are maintained per service.
- The number of peers is maintained at the gtpumgr instance level. The limit is one million S1-U peers per gtpumgr instance.
- If the limit of one million peers is exceeded, then peer creation fails. It causes a call installation failure in the gtpumgr, which leads to an audit failure if an audit is triggered.

The feature changes impact all the interfaces/services using the gtpu-service including GGSN/S4-SGSN/SGW/PGW/SAEGW/ePDG/SaMOG/HNB-GW/HeNB-GW for:

- The Gn and Gp interfaces of the General Packet Radio Service (GPRS)

- The Iu, Gn, and Gp interfaces of the UMTS system
- The S1-U, S2a, S2b, S4, S5, S8, and S12 interfaces of the Evolved Packet System (EPS)

### Recovery/ICSR Considerations

- After a session manager/gtpumgr recovery or after an ICSR switchover, the same set of peers configured for statistics collection is recovered.
  - Peers with 0 sessions and without statistics are not recovered.
  - Peers with 0 sessions and with statistics are recovered.
  - Peers with Extension Header Support disabled are recovered.
- While upgrading from a previous release, ensure the newer release chassis **gtpu peer statistics threshold** is equal to or greater than the previous release. This ensures that the GTPU peer statistics are preserved during the upgrade. For example, if you are upgrading from release 19.0 to 20.2, and the 19.0 system has 17,000 GTPU sessions, then configure the threshold on the 20.2 chassis to 17,000 as well.

### Configuration/Restrictions

- Due to the large number of GTP-U entities connecting to the StarOS, Cisco recommends disabling the GTP-U Path Management feature.
- The configured threshold is not the hard upper limit for statistics allocation because of the distributed nature of system. It is possible that total GTP-U peers with statistics exceeds the configured threshold value to some extent.
- It is assumed that all 1,000,000 peers are not connected to the node in a point-to-point manner. They are connected through routers.
- There will not be any ARP table size change for the StarOS to support this feature.

## TCP Window Size



### Important

This feature is not fully qualified in this release. It is available only for testing purposes. For more information, contact your Cisco Accounts representative.

The operator can restrict the effective window size of all downlink TCP packets. A new CLI command **window-size** is added in the Rulebase Configuration mode to enable this feature.

The P-GW updates the TCP packets with the configured value if the effective window size is greater than the configured window size. Otherwise, the P-GW does not modify the window size of the packet.

The newly updated window size might not be the same as the configured window size because the P-GW does not have control over the Window Scale option (sent with SYN flag). Therefore, the updated window size is rounded off to the nearest value calculated by the Window Scale option.

This feature is not applicable on non-SYN flows as they do not have the Window Scale option is not available.

When TCP Window Size is enabled, Rulebase changes and configuration changes are applicable to both newly created flows and existing flows. The changes will not be applicable if TCP Window Size feature is not enabled for these flows.



**Note** There will be a performance impact as PGW updates every downlink packet for a specified Rulebase where the configured window size is lesser than the effective windows size in the packet.

## Threshold Crossing Alerts (TCA) Support

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e high CPU utilization, or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

The system supports Threshold Crossing Alerts for certain key resources such as CPU, memory, IP pool addresses, etc. With this capability, the operator can configure threshold on these resources whereby, should the resource depletion cross the configured threshold, a SNMP Trap would be sent.

The following thresholding models are supported by the system:

- **Alert:** A value is monitored and an alert condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.
- **Alarm:** Both high and low threshold are defined for a value. An alarm condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps:** SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values.

Generation of specific traps can be enabled or disabled on the chassis. Ensuring that only important faults get displayed. SNMP traps are supported in both Alert and Alarm modes.

- **Logs:** The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.

Logs are supported in both the Alert and the Alarm models.

- **Alarm System:** High threshold alarms generated within the specified polling interval are considered "outstanding" until a the condition no longer exists or a condition clear alarm is generated. "Outstanding" alarms are reported to the system's alarm subsystem and are viewable through an element management system.

The Alarm System is used only in conjunction with the Alarm model.

**Important**

For more information on threshold crossing alert configuration, refer to the *Thresholding Configuration Guide*.

## UE Time Zone Reporting

This feature enables time-based charging for specialized service tariffs, such as super off-peak billing plans

Time Zone of the UE is associated with UE location (Tracking Area/Routing Area). The UE Time Zone Information Element is an attribute the MME tracks on a Tracking Area List basis and propagates over S11 and S5/S8 signaling to the P-GW.

Time zone reporting can be included in billing records or conveyed in Gx/Gy signaling to external PCRF and OCS servers.

## Virtual APN Support

Virtual APNs allow differentiated services within a single APN.

The Virtual APN feature allows a carrier to use a single APN to configure differentiated services. The APN that is supplied by the MME is evaluated by the P-GW in conjunction with multiple configurable parameters. Then, the P-GW selects an APN configuration based on the supplied APN and those configurable parameters.

APN configuration dictates all aspects of a session at the P-GW. Different policies imply different APNs. After basic APN selection, however, internal re-selection can occur based on the following parameters:

- Service name
- Subscriber type
- MCC-MNC of IMSI
- Domain name part of username (user@domain)
- S-GW address

**Important**

For more information, refer to the **virtual-apn preference** command in *APN Configuration Mode Commands* in the *Command Line Interface Reference*.

## P-GW Features and Functionality - Inline Service Support

This section describes the features and functions of inline services supported on the P-GW. These services require additional licenses to implement the functionality.

**Important**

The SAEGW supports all of these features if a P-GW service is assigned to the SAEGW service.

## Content Filtering

The Cisco P-GW offers two variants of network-controlled content filtering / parental control services. Each approach leverages the native DPI capabilities of the platform to detect and filter events of interest from mobile subscribers based on HTTP URL or WAP/MMS URI requests:

- **Integrated Content Filtering:** A turnkey solution featuring a policy enforcement point and category based rating database on the Cisco P-GW. An offboard AAA or PCRF provides the per-subscriber content filtering information as subscriber sessions are established. The content filtering service uses DPI to extract URLs or URIs in HTTP request messages and compares them against a static rating database to determine the category match. The provisioned policy determines whether individual subscribers are entitled to view the content.
- **Content Filtering ICAP Interface:** This solution is appropriate for mobile operators with existing installations of Active Content Filtering external servers. The service continues to harness the DPI functions of the ASR 5500 platform to extract events of interest. However in this case, the extracted requests are transferred via the Integrated Content Adaptation Protocol (ICAP) with subscriber identification information to the external ACF server which provides the category rating database and content decision functions.

## Integrated Adult Content Filter

Provides a value-added service to prevent unintended viewing of objectionable content that exploits underage children. Content Filtering offers mobile operators a way to increase data ARPU and subscriber retention through a network-based solution for parental controls and content filtering. The integrated solution enables a single policy decision and enforcement point thereby streamlining the number of signaling interactions with external AAA/Policy Manager servers. When used in parallel with other services such as Enhanced Content Charging (ECS) it increases billing accuracy of charging records by insuring that mobile subscribers are only charged for visited sites they are allowed to access.

The Integrated Adult Content Filter is a subscriber-aware inline service provisioned on an ASR 5500 running P-GW services. Integrated Content Filtering utilizes the local DPI engine and harnesses a distributed software architecture that scales with the number of active P-GW sessions on the system.

Content Filtering policy enforcement is the process of deciding if a subscriber should be able to receive some content. Typical options are to allow, block, or replace/redirect the content based on the rating of the content and the policy defined for that content and subscriber. The policy definition is transferred in an authentication response from a AAA server or Diameter policy message via the Gx reference interface from an adjunct PCRF. The policy is applied to subscribers through rulebase or APN/Subscriber configuration. The policy determines the action to be taken on the content request on the basis of its category. A maximum of one policy can be associated with a rulebase.

## ICAP Interface

Provides a value-added service to prevent unintended viewing of objectionable content that exploits underage children. Content Filtering offers mobile operators a way to increase data ARPU and subscriber retention through a network-based solution for parental controls and content filtering. The Content Filtering ICAP solution is appropriate for operators with existing installations of Active Content Filtering servers in their networks.

The Enhanced Charging Service (ECS) for the P-GW provides a streamlined Internet Content Adaptation Protocol (ICAP) interface to leverage the Deep Packet Inspection (DPI) to enable external Application Servers to provide their services without performing the DPI functionality and without being inserted in the data flow.

The ICAP interface may be attractive to mobile operators that prefer to use an external Active Content Filtering (ACF) Platform. If a subscriber initiates a WAP (WAP1.x or WAP2.0) or Web session, the subsequent GET/POST request is detected by the deep packet inspection function. The URL of the GET/POST request is extracted by the local DPI engine on the ASR 5500 platform and passed, along with subscriber identification information and the subscriber request, in an ICAP message to the Application Server (AS). The AS checks the URL on the basis of its category and other classifications like, type, access level, content category and decides if the request should be authorized, blocked or redirected by answering the GET/POST message. Depending upon the response received from the ACF server, the P-GW either passes the request unmodified or discards the message and responds to the subscriber with the appropriate redirection or block message.

## Header Enrichment: Header Insertion and Encryption

Header enrichment provides a value-added capability for mobile operators to monetize subscriber intelligence to include subscriber-specific information in the HTTP requests to application servers.

Extension header fields (x-header) are the fields that can be added to headers of a protocol for a specific purpose. The enriched header allows additional entity-header fields to be defined without changing the protocol, but these fields cannot be assumed to be recognizable by the recipient. Unrecognized fields should be ignored by the recipient and must be forwarded by transparent proxies.

Extension headers can be supported in HTTP/WSP GET and POST request packets. The Enhanced Charging Service (ECS) for the P-GW offers APN-based configuration and rules to insert x-headers in HTTP/WSP GET and POST request packets. The charging action associated with the rules will contain the list of x-headers to be inserted in the packets. Protocols supported are HTTP, WAP 1.0 and WAP 2.0 GET, and POST messages.




---

**Important** For more information on ECS, see the *Enhanced Charging Service Administration Guide*.

---

The data passed in the inserted HTTP header attributes is used by end application servers (also known as Upsell Servers) to identify subscribers and session information. These servers provide information customized to that specific subscriber.

The Cisco P-GW can include the following information in the http header:

- User-customizable, arbitrary text string
- Subscriber's MSISDN (the RADIUS calling-station-id, in clear text)
- Subscriber's IMSI
- Subscriber's IP address
- S-GW IP address (in clear text)

X-Header encryption enhances the header enrichment feature by increasing the number of fields that can be supported and through encryption of the fields before inserting them.

The following limitations to insertion of x-header fields in WSP headers apply:

- x-header fields are not inserted in IP fragmented packets before StarOS v14.0.
- In case of concatenated request, x-header fields are only inserted in first GET or POST request (if rule matches for the same). X-header fields are not inserted in the second or later GET/POST requests in the concatenated requests. For example, if there is ACK+GET in packet, x-header is inserted in the GET

packet. However, if GET1+GET2 is present in the packet and rule matches for GET2 and not GET1 x-header is still inserted in GET2. In case of GET+POST also, x-header is not inserted in POST.

- In case of CO, x-header fields are not inserted if the WTP packets are received out of order (even after proper reordering).
- If route to MMS is present, x-headers are not inserted.
- x-headers are not inserted in WSP POST packet when header is segmented. This is because POST contains header length field which needs to be modified after addition of x-headers. In segmented WSP headers, header length field may be present in one packet and header may complete in another packet.

## Network Address Translation (NAT)

NAT translates non-routable private IP address(es) to routable public IP address(es) from a pool of public IP addresses that have been designated for NAT. This enables to conserve on the number of public IP addresses required to communicate with external networks, and ensures security as the IP address scheme for the internal network is masked from external hosts, and each outgoing and incoming packet goes through the translation process.

NAT works by inspecting both incoming and outgoing IP datagrams and, as needed, modifying the source IP address and port number in the IP header to reflect the configured NAT address mapping for outgoing datagrams. The reverse NAT translation is applied to incoming datagrams.

NAT can be used to perform address translation for simple IP and mobile IP. NAT can be selectively applied/denied to different flows (5-tuple connections) originating from subscribers based on the flows' L3/L4 characteristics—Source-IP, Source-Port, Destination-IP, Destination-Port, and Protocol.

NAT supports the following mappings:

- One-to-One
- Many-to-One



### Important

For more information on NAT, refer to the *Network Address Translation Administration Guide*.

## NAT64 Support

This feature helps facilitate the co-existence and gradual transition to IPv6 addressing scheme in the networks. Use of NAT64 requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

With the dwindling IPv4 public address space and the growing need for more routable addresses, service providers and enterprises will continue to build and roll out IPv6 networks. However, because of the broad scale IPv4 deployment, it is not practical that the world changes to IPv6 overnight. There is need to protect the IPv4 investment combined with the need to expand and grow the network will force IPv4 and IPv6 networks to co-exist together for a considerable period of time and keep end-user experience seamless.

The preferred approaches are to run dual stacks (both IPv4 and IPv6) on the end hosts, dual stack routing protocols, and dual stack friendly applications. If all of the above is available, then the end hosts will communicate natively using IPv6 or IPv4 (using NAT). Tunneling through the IPv4 or IPv6 is the next

preferred method to achieve communication wherever possible. When all these options fail, translation is recommended.

Stateful NAT64 is a mechanism for translating IPv6 packets to IPv4 packets and vice-versa. The system supports a Stateful NAT64 translator based on IETF Behave WG drafts whose framework is described in draft-ietf-behave-v6v4-framework-10. Stateful NAT64 is available as part of the existing NAT licenses from the current system implementation. The NAT44 and NAT64 will co-exist on the chassis and share the resources needed for NATing.

## Peer-to-Peer Detection

Enables operators to identify P2P traffic in the network and applying appropriate controlling functions to ensure fair distribution of bandwidth to all subscribers.

Peer-to-Peer (P2P) is a term used in two slightly different contexts. At a functional level, it means protocols that interact in a peering manner, in contrast to client-server manner. There is no clear differentiation between the function of one node or another. Any node can function as a client, a server, or both—a protocol may not clearly differentiate between the two. For example, peering exchanges may simultaneously include client and server functionality, sending and receiving information.

Detecting peer-to-peer protocols requires recognizing, in real time, some uniquely identifying characteristic of the protocols. Typical packet classification only requires information uniquely typed in the packet header of packets of the stream(s) running the particular protocol to be identified. In fact, many peer-to-peer protocols can be detected by simple packet header inspection. However, some P2P protocols are different, preventing detection in the traditional manner. This is designed into some P2P protocols to purposely avoid detection. The creators of these protocols purposely do not publish specifications. A small class of P2P protocols is stealthier and more challenging to detect. For some protocols no set of fixed markers can be identified with confidence as unique to the protocol.

Operators care about P2P traffic because of the behavior of some P2P applications (for example, Bittorrent, Skype, and eDonkey). Most P2P applications can hog the network bandwidth such that 20% P2P users can generate as much as traffic generated by the rest 80% non-P2P users. This can result into a situation where non-P2P users may not get enough network bandwidth for their legitimate use because of excess usage of bandwidth by the P2P users. Network operators need to have dynamic network bandwidth / traffic management functions in place to ensure fair distributions of the network bandwidth among all the users. And this would include identifying P2P traffic in the network and applying appropriate controlling functions to the same (for example, content-based premium billing, QoS modifications, and other similar treatments).

Cisco's P2P detection technology makes use of innovative and highly accurate protocol behavioral detection techniques.



### Important

For more information on peer-to-peer detection, refer to the *Application Detection and Control Administration Guide*.

## Personal Stateful Firewall

The Personal Stateful Firewall is an in-line service feature that inspects subscriber traffic and performs IP session-based access control of individual subscriber sessions to protect the subscribers from malicious security attacks.

The Personal Stateful Firewall supports stateless and stateful inspection and filtering based on the configuration.



In stateless inspection, the firewall inspects a packet to determine the 5-tuple—source and destination IP addresses and ports, and protocol—information contained in the packet. This static information is then compared against configurable rules to determine whether to allow or drop the packet. In stateless inspection the firewall examines each packet individually, it is unaware of the packets that have passed through before it, and has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is a rogue packet.

In stateful inspection, the firewall not only inspects packets up through the application layer / layer 7 determining a packet's header information and data content, but also monitors and keeps track of the connection's state. For all active connections traversing the firewall, the state information, which may include IP addresses and ports involved, the sequence numbers and acknowledgment numbers of the packets traversing the connection, TCP packet flags, etc. is maintained in a state table. Filtering decisions are based not only on rules but also on the connection state established by prior packets on that connection. This enables to prevent a variety of DoS, DDoS, and other security violations. Once a connection is torn down, or is timed out, its entry in the state table is discarded.

The Enhanced Charging Service (ECS) / Active Charging Service (ACS) in-line service is the primary vehicle that performs packet inspection and charging. For more information on ECS, see the *Enhanced Charging Service Administration Guide*.

**Important**

For more information on Personal Stateful Firewall, refer to the *Personal Stateful Firewall Administration Guide*.

## S-GW Features and Functionality - Optional Enhanced Feature Software

This section describes the optional enhanced features and functions for the S-GW service.

**Important**

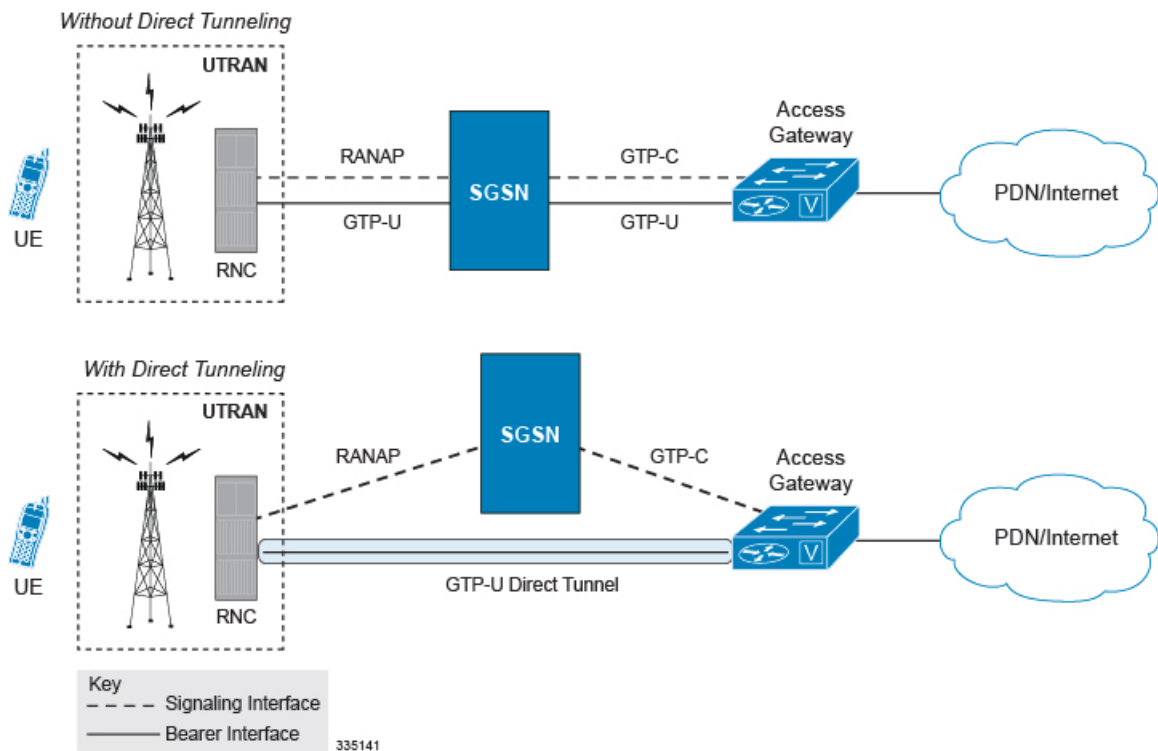
The SAEGW supports all of these features if an S-GW service is assigned to the SAEGW service.

Each of the features described in this section requires the purchase of an additional license to implement the functionality with the S-GW service.

### Direct Tunnel

In accordance with standards, one tunnel functionality enables the SGSN to establish a direct tunnel at the user plane level - a GTP-U tunnel, directly between the RAN and the S-GW.

Figure 34: GTP-U with Direct Tunnel



In effect, a direct tunnel reduces data plane latency as the tunnel functionality acts to remove the SGSN from the data plane and limit the SGSN to the control plane for processing. This improves the user experience (for example, expedites web page delivery, reduces round trip delay for conversational services). Additionally, direct tunnel functionality implements the standard SGSN optimization to improve the usage of user plane resources (and hardware) by removing the requirement from the SGSN to handle the user plane processing.

Typically, the SGSN establishes a direct tunnel at PDP context activation using an Update PDP Context Request towards the S-GW. This means a significant increase in control plane load on both the SGSN and S-GW components of the packet core. Hence, deployment requires highly scalable S-GWs since the volume and frequency of Update PDP Context messages to the S-GW will increase substantially. The ASR 5500 platform capabilities ensure control plane capacity will not be a limiting factor with direct tunnel deployment.



#### Important

For more information on direct tunnel support, refer to the *Direct Tunnel for 4G (LTE) Networks* chapter in this guide.

## Intelligent Paging for ISR

In case of when Idle-mode Signaling Reduction (ISR) active and the UE is idle, the S-GW will send Downlink Data Notification (DDN) Message to both the MME and the S4-SGSN if it receives the downlink data or network initiated control message for this UE. In turn, the MME and the S4-SGSN would do paging in parallel consuming radio resources.

To optimize the radio resource, the S-GW will now perform intelligent paging. When configured at the S-GW service level for each APN, the S-GW will page in a semi-sequential fashion (one by one to peer MME or S4-SGSN based on last known RAT type) or parallel to both the MME and S4-SGSN.

## Inter-Chassis Session Recovery

The ASR 5500 platform provide industry leading carrier class redundancy. The systems protects against all single points of failure (hardware and software) and attempts to recover to an operational state when multiple simultaneous failures occur.

The system provides several levels of system redundancy:

- Under normal N+1 packet processing card hardware redundancy, if a catastrophic packet processing card failure occurs all affected calls are migrated to the standby packet processing card if possible. Calls which cannot be migrated are gracefully terminated with proper call-termination signaling and accounting records are generated with statistics accurate to the last internal checkpoint
- If the Session Recovery feature is enabled, any total packet processing card failure will cause a packet processing card switchover and all established sessions for supported call-types are recovered without any loss of session.

Even though Cisco provides excellent intra-chassis redundancy with these two schemes, certain catastrophic failures which can cause total chassis outages, such as IP routing failures, line-cuts, loss of power, or physical destruction of the chassis, cannot be protected by this scheme. In such cases, the MME Inter-Chassis Session Recovery (ICSR) feature provides geographic redundancy between sites. This has the benefit of not only providing enhanced subscriber experience even during catastrophic outages, but can also protect other systems such as the RAN from subscriber re-activation storms.

ICSR allows for continuous call processing without interrupting subscriber services. This is accomplished through the use of redundant chassis. The chassis are configured as primary and backup with one being active and one in recovery mode. A checkpoint duration timer is used to control when subscriber data is sent from the active chassis to the inactive chassis. If the active chassis handling the call traffic goes out of service, the inactive chassis transitions to the active state and continues processing the call traffic without interrupting the subscriber session. The chassis determines which is active through a propriety TCP-based connection called a redundancy link. This link is used to exchange Hello messages between the primary and backup chassis and must be maintained for proper system operation.

### Interchassis Communication

Chassis configured to support ICSR communicate using periodic Hello messages. These messages are sent by each chassis to notify the peer of its current state. The Hello message contains information about the chassis such as its configuration and priority. A dead interval is used to set a time limit for a Hello message to be received from the chassis' peer. If the standby chassis does not receive a Hello message from the active chassis within the dead interval, the standby chassis transitions to the active state. In situations where the redundancy link goes out of service, a priority scheme is used to determine which chassis processes the session. The following priority scheme is used:

- router identifier
- chassis priority
- SPIO MAC address

### Checkpoint Messages

Checkpoint messages are sent from the active chassis to the inactive chassis. Checkpoint messages are sent at specific intervals and contain all the information needed to recreate the sessions on the standby chassis, if that chassis were to become active. Once a session exceeds the checkpoint duration, checkpoint data is collected on the session. The checkpoint parameter determines the amount of time a session must be active before it is included in the checkpoint message.



---

**Important** For more information on inter-chassis session recovery support, refer to the *Interchassis Session Recovery* chapter in *System Administration Guide*.

---

## IP Security (IPSec) Encryption

Enables network domain security for all IP packet switched LTE-EPC networks in order to provide confidentiality, integrity, authentication, and anti-replay protection. These capabilities are insured through use of cryptographic techniques.

The Cisco S-GW supports IKEv1 and IPSec encryption using IPv4 addressing. IPSec enables the following two use cases:

- Encryption of S8 sessions and EPS bearers in roaming applications where the P-GW is located in a separate administrative domain from the S-GW
- IPSec ESP security in accordance with 3GPP TS 33.210 is provided for S1 control plane, S1 bearer plane and S1 management plane traffic. Encryption of traffic over the S1 reference interface is desirable in cases where the EPC core operator leases radio capacity from a roaming partner's network.



---

**Important** You must purchase an IPSec license to enable IPSec. For more information on IPSec support, refer to the *IP Security (IPSec) Reference*.

---

## Lawful Intercept

The Cisco Lawful Intercept feature is supported on the S-GW. 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 documentation on the Lawful Intercept feature, contact your Cisco account or support representative.

## Layer 2 Traffic Management (VLANs)

Virtual LANs (VLANs) provide greater flexibility in the configuration and use of contexts and services.

VLANs are configured as tags on a per-port basis and allow more complex configurations to be implemented. The VLAN tag allows a single physical port to be bound to multiple logical interfaces that can be configured in different contexts. Therefore, each Ethernet port can be viewed as containing many logical ports when VLAN tags are employed.



---

**Important** For more information on VLAN support, refer to the VLANs chapter in the *System Administration Guide*.

---

## New Call Policy for Stale Sessions

Use of new call policy for stale sessions requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

If the newcall policy is set to **reject release-existing-session** and there are pre-existing sessions for the IMSI/IMEI received in Create Session Req, they will be deleted. This allows for no hung sessions on a node with newcall policy reject release configured. When GGSN/P-GW/SAEGW/S-GW releases the existing call, it follows a proper release process of sending Accounting Stop, sending CCR-T to PCRF/OCS, and generating CDR(s).

## New Standard QCI Support

New Standard QCI Support is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

The P-GW/SAEGW/S-GW support additional new 3GPP-defined standard QCIs. QCIs 65, 66, 69, and 70 are now supported for Mission Critical and Push-to-Talk (MC/PTT) applications. These new standard QCIs are supported in addition to the previously supported QCIs of 1 through 9, and operator-defined QCIs 128 through 254.

The StarOS will continue to reject QCIs 10 through 127 sent by the PCRF.

For detailed information on this feature, refer to the *New Standard QCI Support* chapter in this guide.

## Overcharging Protection Support

Use of Overcharging Protection requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

Overcharging Protection helps in avoiding charging the subscribers for dropped downlink packets while the UE is in idle mode. In some countries, it is a regulatory requirement to avoid such overcharging, so it becomes a mandatory feature for operators in such countries. Overall, this feature helps ensure subscriber are not overcharged while the subscriber is in idle mode.



---

**Important** This feature is supported on the P-GW, and S-GW. Overcharging Protection is supported on the SAEGW only if the SAEGW is configured for Pure P or Pure S functionality.

---

The P-GW will never be aware of UE state (idle or connected mode). Charging for downlink data is applicable at P-GW, even when UE is in idle mode. Downlink data for UE may be dropped at S-GW when UE is in idle mode due to buffer overflow or delay in paging. Thus, P-GW will charge the subscriber for the dropped packets, which isn't desired. To address this problem, with Overcharging Protection feature enabled, S-GW will inform P-GW to stop or resume charging based on packets dropped at S-GW and transition of UE from idle to active state.

If the S-GW supports the Overcharging Protection feature, then it will send a CSReq with the PDN Pause Support Indication flag set to 1 in an Indication IE to the P-GW.

If the PGW supports the Overcharging Protection feature then it will send a CSRsp with the PDN Pause Support Indication flag set to 1 in Indication IE and/or private extension IE to the S-GW.

Once the criterion to signal "stop charging" is met, S-GW will send Modify Bearer Request (MBReq) to P-GW. MBReq would be sent for the PDN to specify which packets will be dropped at S-GW. The MBReq will have an indication IE and/or a new private extension IE to send "stop charging" and "start charging" indication to P-GW. For Pause/Start Charging procedure (S-GW sends MBReq), MBRes from P-GW will have indication and/or private extension IE with Overcharging Protection information.

When the MBReq with stop charging is received from a S-GW for a PDN, P-GW will stop charging for downlink packets but will continue sending the packets to S-GW.

P-GW will resume charging downlink packets when either of these conditions is met:

- When the S-GW (which had earlier sent "stop charging" in MBReq) sends "start charging" in MBReq.
- When the S-GW changes (which indicates that maybe UE has relocated to new S-GW).

This feature aligns with the 3GPP TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C) specification.

For detailed information on this feature, refer to the *Overcharging Protection Support* chapter in this guide.

## Paging Policy Differentiation

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

S-GW/P-GW provide configuration control to change the DSCP value of the user-datagram packet and outer IP packet (GTP-U tunnel IP header). DSCP marking is done at various levels depending on the configuration. When the Paging Policy Differentiation (PPD) feature is enabled, however, the user-datagram packet DSCP (tunneled IP packet) marking does not change.

Currently, standards specify QCI to DSCP marking of outer GTP-U header only. All configurations present at ECS, P-GW, and S-GW to change the user-datagram packet DSCP value are non-standard. The standards-based PPD feature dictates that P-CSCF or similar Gi entity marks the DSCP of user-datagram packet. This user-datagram packet DSCP value is sent in DDN message by S-GW to MME/S4-SGSN. MME/S4-SGSN uses this DSCP value to give paging priority.



### Important

P-GW and S-GW should apply the PPD feature for both Default and Dedicated bearers. As per the specifications, P-GW transparently passes the user-datagram packet towards S-GW. This means, if PPD feature is enabled, operator can't apply different behavior for Default and Dedicated bearers.



### Important

For more information on paging policy differentiation, refer to the *Paging Policy Differentiation* chapter in this guide.

## R12 Load and Overload Support

Use of R12 Load and Overload Support requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

GTP-C Load Control feature is an optional feature which allows a GTP control plane node to send its Load Information to a peer GTP control plane node which the receiving GTP control plane peer node uses to augment existing GW selection procedure for the P-GW and S-GW. Load Information reflects the operating status of the resources of the originating GTP control plane node.

Nodes using GTP control plane signaling may support communication of Overload control Information in order to mitigate overload situation for the overloaded node through actions taken by the peer node(s). This feature is supported over the S5 and S8 interfaces via the GTPv2 control plane protocol.

A GTP-C node is considered to be in overload when it is operating over its nominal capacity resulting in diminished performance (including impacts to handling of incoming and outgoing traffic). Overload control Information reflects an indication of when the originating node has reached such a situation. This information, when transmitted between GTP-C nodes may be used to reduce and/or throttle the amount of GTP-C signaling traffic between these nodes. As such, the Overload control Information provides guidance to the receiving node to decide actions, which leads to mitigation towards the sender of the information.

In brief, load control and overload control can be described in this manner:

- Load control enables a GTP-C entity (for example, an S-GW/P-GW) to send its load information to a GTP-C peer (e.g. an MME/SGSN, ePDG, TWAN) to adaptively balance the session load across entities supporting the same function (for example, an S-GW cluster) according to their effective load. The load information reflects the operating status of the resources of the GTP-C entity.
- Overload control enables a GTP-C entity becoming or being overloaded to gracefully reduce its incoming signaling load by instructing its GTP-C peers to reduce sending traffic according to its available signaling capacity to successfully process the traffic. A GTP-C entity is in overload when it operates over its signaling capacity, which results in diminished performance (including impacts to handling of incoming and outgoing traffic).

A maximum of 64 different load and overload profiles can be configured.



---

**Important**

R12 Load and Overload Support is a license-controlled feature. Contact your Cisco representative for more information on licensing requirements.

---

### R12 Load and Overload Factor Calculation Enhancement

In capacity testing and also in customer deployments it was observed that the chassis load factor for the R12 Load and Overload Support feature was providing incorrect values even when the sessmgr card CPU utilization was high. The root cause is that when the load factor was calculated by taking an average of CPU utilization of sessmgr and demux cards, the demux card CPU utilization never increased more than the sessmgr card CPU utilization. As a result, the system did not go into the overload state even when the sessmgr card CPU utilization was high.

The R12 Load/Overload Control Profile feature has been enhanced to calculate the load factor based on the higher value of similar types of cards for CPU load and memory. If the demux card's CPU utilization value is higher than the sessmgr card's CPU utilization value, then the demux card CPU utilization value is used for the load factor calculation.

A new CLI command is introduced to configure different polling intervals for the resource manager so that the demuxmgr can calculate the load factor based on different system requirements.



**Important** For more information on this feature, refer to the *GTP-C Load and Overload Control Support on the P-GW, SAEGW, and S-GW* chapter in this guide.

## Operation

The node periodically fetches various parameters (for example, License-Session-Utilization, System-CPU-Utilization and System-Memory-Utilization), which are required for Node level load control information. The node then calculates the load control information itself either based on the weighted factor provided by the user or using the default weighted factor.

Node level load control information is calculated every 30 seconds. The resource manager calculates the system-CPU-utilization and System-Memory-Utilization at a systems level.

For each configured service, load control information can be different. This can be achieved by providing a weightage to the number of active session counts per service license, for example,  $((\text{number of active sessions per service} / \text{max session allowed for the service license}) * 100)$ .

The node's resource manager calculates the system-CPU-utilization and System-Memory-Utilization at a systems level by averaging CPU and Memory usage for all cards and which might be different from that calculated at the individual card level.

## Separate Paging for IMS Service Inspection

Use of Separate Paging for IMS Service Inspection requires that a valid license key be installed. Contact your Cisco account or support representative for information on how to obtain a license.

When some operators add an additional IMS service besides VoLTE such as RCS, they can use the same IMS bearer between the two services. In this case, separate paging is supported at the MME using an ID which can be assigned from the S-GW according to the services, where the S-GW distinguishes IMS services using a small DPI function to inspect where the traffic comes from using an ID which is assigned from SGW according to the services. The S-GW distinguishes IMS services using a small DPI function to inspect where the traffic comes from (for example IP, Port and so on). After the MME receives this ID from the S-GW after IMS service inspection, the MME will do classified separate paging for each of the services as usual.

## Session Recovery Support

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.

In the telecommunications industry, over 90 percent of all equipment failures are software-related. With robust hardware failover and redundancy protection, any card-level hardware failures on the system can quickly be corrected. However, software failures can occur for numerous reasons, many times without prior indication. The StarOS has the ability to support stateful intra-chassis session recovery (ICSR) for S-GW sessions.

When session recovery occurs, the system reconstructs the following subscriber information:

- Data and control state information required to maintain correct call behavior
- Subscriber data statistics that are required to ensure that accounting information is maintained



- A best-effort attempt to recover various timer values such as call duration, absolute time, and others

Session recovery is also useful for in-service software patch upgrade activities. If session recovery is enabled during the software patch upgrade, it helps to preserve existing sessions on the active packet services card during the upgrade process.



---

**Important** For more information on session recovery support, refer to the *Session Recovery* chapter in the *System Administration Guide*.

---

## S-GW Paging Enhancements

Use of S-GW Paging requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

S-GW Paging includes the following scenarios:

**Scenario 1:** S-GW sends a 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 does not 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 have been added to the DDN functionality:

- 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 is not lost.
- MBR guard timer, which is started when DDN Ack with temporary HO is received. A new 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 the above functionality, 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.



---

**Important** For more information on this functionality, refer to the *S-GW Paging Enhancements* chapter in this guide.

---

# P-GW Features and Functionality - Optional Enhanced Feature Software

This section describes the optional enhanced features and functions for the P-GW service.



**Important** The SAEGW supports all of these features if a P-GW service is assigned to the SAEGW service.

Each of the following features requires the purchase of an additional license to implement the functionality with the P-GW service.



**Important** For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

## AAA and Prefix Delegation DHCP Correlation

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

Currently at the DHCP server, DHCPv6 does not provide any mechanism to correlate allocated IPv6 (/64) prefix to a particular subscriber. This feature correlates the default prefix allocated from AAA server with the delegated prefix allocated from external DHCPv6 server during the PDN connection setup.

Options are available in DHCP Client Profile Configuration Mode to enable P-GW to send USER\_CLASS\_OPTION in DHCPv6 messages to external DHCPv6 server during delegated prefix setup.

## APN Backoff Timer Support

Previously, the P-GW did not distinguish signaling traffic from Delay Tolerant or Low Priority devices such as low priority machine-to-machine traffic.

The UE was able to indicate its device profile to the MME via NAS and Attach Request messages. The MME was able to pass this information to the P-GW via the Signaling Priority Indication Information Element (IE) on the S5 interface. Some UEs may not have supported providing the Signaling Priority Indication IE on S5 interface to the P-GW. As a result, the P-GW could not distinguish between the signaling types. the current release, the P-GW can distinguish between these signaling types.

Also, during overload situations, the P-GW previously allowed new sessions from LAPI devices and treated the traffic from Low Access Priority Indicator (LAPI) devices with the same priority as the normal UEs. With the current StarOS release, during overload conditions, the P-GW can be configured to backoff the traffic that is identified as LAPI. The identification is based on either the APN configuration or the signaling priority indicator IE.

The backoff timer algorithm and the R12 GTP-C Load/Overload Control algorithm now work together. This feature provides the benefit of rejecting low priority calls, which, in turn allows for more bandwidth for high priority calls.

For additional information, refer to the *APN Backoff Timer Support* chapter in this guide.

## Cause IE Enhancement for Delete Bearer Request

Use of Cause IE Enhancement for Delete Bearer Request requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

The cause value in the Delete Bearer Request previously had been limited. The behavior impacted by this feature is:

- Delete Bearer Request/Delete PDP Context due to idle-timer/session-timer expiration
- Delete Bearer Request due to bearer inactivity of default bearer
- Delete PDP Context due to bearer inactivity of the last PDP context of PDN connection
- Delete Bearer Request/Delete PDP Context triggered by **clear subscriber** CLI command

Configuration now is available to set cause values and cause inclusion in the following scenarios:

- CLI-based trigger to disconnect
- per APN when P-GW initiated disconnection for above mentioned timer expiry



### Important

This feature allows operator to override existing behavior. Such overridden behavior may not be compliant with standards.

## Dynamic RADIUS Extensions (Change of Authorization)

Use of Dynamic RADIUS Extensions (CoA and PoD) requires that a valid license key be installed. Contact your Cisco account or support representative for information on how to obtain a license.

Dynamic RADIUS extension support provides operators with greater control over subscriber PDP contexts by providing the ability to dynamically redirect data traffic, and or disconnect the PDP context.

This functionality is based on the RFC 3576, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), July 2003 standard.

The system supports the configuration and use of the following dynamic RADIUS extensions:

- **Change of Authorization:** The system supports CoA messages from the AAA server to change data filters associated with a subscriber session. The CoA request message from the AAA server must contain attributes to identify NAS and the subscriber session and a data filter ID for the data filter to apply to the subscriber session.
- **Disconnect Message:** The DM message is used to disconnect subscriber sessions in the system from a RADIUS server. The DM request message should contain necessary attributes to identify the subscriber session.

The above extensions can be used to dynamically re-direct subscriber PDP contexts to an alternate address for performing functions such as provisioning and/or account set up. This functionality is referred to as Session Redirection, or Hotlining.

Session redirection provides a means to redirect subscriber traffic to an external server by applying ACL rules to the traffic of an existing or a new subscriber session. The destination address and optionally the destination

port of TCP/IP or UDP/IP packets from the subscriber are rewritten so the packet is forwarded to the designated redirected address.

Return traffic to the subscriber has the source address and port rewritten to the original values. The redirect ACL may be applied dynamically by means of the Radius Change of Authorization (CoA) extension.



---

**Important** For more information on dynamic RADIUS extensions support, refer to the *CoA, RADIUS, And Session Redirection (Hotlining)* chapter in this guide.

---

## GRE Protocol Interface Support

Use of GRE Interface Tunneling requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The P-GW supports GRE generic tunnel interfaces in accordance with RFC 2784, Generic Routing Encapsulation (GRE). The GRE protocol allows mobile users to connect to their enterprise networks through GRE tunnels.

GRE tunnels can be used by the enterprise customers of a carrier 1) To transport AAA packets corresponding to an APN over a GRE tunnel to the corporate AAA servers and, 2) To transport the enterprise subscriber packets over the GRE tunnel to the corporation gateway.

The corporate servers may have private IP addresses and hence the addresses belonging to different enterprises may be overlapping. Each enterprise needs to be in a unique virtual routing domain, known as VRF. To differentiate the tunnels between same set of local and remote ends, GRE Key will be used as a differentiation.

GRE tunneling is a common technique to enable multi-protocol local networks over a single-protocol backbone, to connect non-contiguous networks and allow virtual private networks across WANs. This mechanism encapsulates data packets from one protocol inside a different protocol and transports the data packets unchanged across a foreign network. It is important to note that GRE tunneling does not provide security to the encapsulated protocol, as there is no encryption involved (like IPSec offers, for example).

GRE tunneling consists of three main components:

- Passenger protocol-protocol being encapsulated. For example: CLNS, IPv4 and IPv6.
- Carrier protocol-protocol that does the encapsulating. For example: GRE, IP-in-IP, L2TP, MPLS and IPSec.
- Transport protocol-protocol used to carry the encapsulated protocol. The main transport protocol is IP.



---

**Important** For more information on GRE protocol interface support, refer to the *GRE Protocol Interface* chapter in this guide.

---

## GTP-Based S2a Interface Support on the SAEGW



**Important** GTP-Based S2a Interface Support on the SAEGW is a licensed controlled feature. Contact your Cisco account or support representative for detailed licensing information.

GTP-based S2a interface support is also supported on the SAEGW. When the WLAN is considered as trusted by the operator, the Trusted WLAN Access Network (TWAN) is interfaced with the EPC as a trusted non-3GPP access via the S2a interface to the P-GW. Support has been extended for WiFi-to-LTE handovers using Make and Break for the SAEGW service. Multi-PDN handovers are also supported as part of this feature.

Supported functionality includes:

- Initial Attach
- WiFi-to-LTE handover
- LTE-to-WiFi handover
- Multi-PDN handovers

Operators deploying StarOS release 20.0 on the SAEGW are now able to integrate Trusted WiFi network functionality using this feature.

## GTP-based S2b Interface Support on the Standalone P-GW and SAEGW

Use of GTP-based S2b Interface Support on the Standalone P-GW and SAEGW requires that a valid license key be installed. Contact your Cisco account or support representative for information on how to obtain a license.

The S2b interface connects the standalone P-GW with the ePDG and the P-GW of the SAEGW with the ePDG. The UE tries to simultaneously connect to different APNs through different access networks only if the home network supports such simultaneous connectivity. The UE determines that the network supports such simultaneous connectivity over multiple accesses if the UE is provisioned with or has received per-APN inter-system routing policies. So the UE can have independent PDN connections via multiple access types. The access types supported are 4G and WiFi.

The S2b interface implementation on the P-GW and SAEGW supports the following:

- UE connecting to PDN via WiFi access
- UE multiple PDN connections
- Initial Attach
- LTE to WiFi Handoff
- WiFi to LTE Handoff



**Note** For more information on the S2a/S2b interface capability, refer to the *GTP-based S2b Interface Support on the P-GW and SAEGW* chapter in this guide.

## GTP Throttling

Use of GTP and Diameter Interface Throttling requires that a valid license key be installed. Contact your Cisco account or support representative for information on how to obtain a license.

This feature will help control the rate of incoming/outgoing messages on P-GW/GGSN. This will help in ensuring P-GW/GGSN doesn't get overwhelmed by the GTP control plan messages. In addition, it will help in ensuring the P-GW/GGSN will not overwhelm the peer GTP-C peer with GTP Control plane messages.

This feature requires shaping/policing of GTP (v1 and v2) control messages over Gn/Gp and S5/S8 interfaces. Feature will cover overload protection of P-GW/GGSN nodes and other external nodes with which it communicates. Throttling would be done only for session level control messages. Path management messages would not be rate limited at all.

External node overload can happen in a scenario where P-GW/GGSN generates signaling requests at a higher rate than other nodes can handle. If the incoming message rate is higher than the configured message rate, extra messages will get silently dropped. Also the actual call setup rate can be lower than the msg-rate configured, which could be due to delays in setting up the session due to many reasons like slow peer nodes or overloaded sm. Also the drops done as part of this throttling are silent drops, hence if path failure is configured for non-echo messages, path failure can be observed.

For protecting external nodes from getting overloaded from P-GW/GGSN control signaling, a framework will be used to handle shaping/policing of outbound control messages to external interfaces.

## Bypass Rate Limit Function

The Bypass Rate Limit Function is an enhancement to the existing GTP Throttling feature.

This enhancement requires no additional license. Existing licenses for the GTP-Throttling Feature (RLF License) and the VoLTE Prioritized Handling feature have been applied and used as follows:

- **RLF License:** The GTP-Throttling feature license has been enhanced to accommodate the message-types based RLF throttling bypass.
- **VoLTE Prioritized Handling Feature License:** This license has been enhanced to accommodate the emergency call, priority call, and apn-names based RLF throttling bypass.

The GTP Throttling feature helps control the rate of incoming/outgoing messages on P-GW/GGSN. It prevents the message flood from P-GW towards S-GW and MME. Currently, following outgoing messages are throttled by P-GW and GGSN using the RLF framework:

- Create Bearer Request (CBR)
- Delete Bearer Request (DBR)
- Update Bearer Request (UBR)
- NRUPC
- IPCA
- NRDPC

Once throttling is enabled for outgoing messages, all outgoing messages are throttled except the Create Bearer Request (CBR) message, which is piggybacked with Create Session Response message.

This feature has been enhanced to control the bypassing of some messages being throttled.

Operator can configure Overload Protection/RLF Throttling-override (Bypass RLF) on P-GW along with Overload Control feature at the egress side. In this scenario, the Overload Control based on peer's reduction metrics will take higher precedence and messages will be throttled based on Overload Control feature first.

If the message is passed to RLF throttling after Overload control feature processing then the Throttling override (Bypass RLF) will be applied after that according to the configuration. If the overload control feature is not configured and RLF throttling and Bypass RLF throttling is configured, then messages would be throttled based on RLF and throttling override (Bypass RLF) feature.

A new command option **throttling-override-policy** has been added to the existing CLI command **gtpc overload-protection egress rlf-template rlf-temp** which allows you to selectively by-pass throttling for a configured message type or for all messages in emergency call or priority call or call for the configured APN. A new CLI command mode **throttling-override-policy** has been also been introduced for Generic syntax for throttling override policy.



---

**Important** For more information on these commands, refer to the CLI Reference Guide.

---

## HSS and PCRF Based P-CSCF Restoration Support

Use of P-CSCF Restoration requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

This feature enables support for P-CSCF restoration. The P-CSCF restoration procedures were standardized to minimize the time a UE is unreachable for terminating calls after a P-CSCF failure. In compliance with 3GPP standard Release 13, this feature includes the following P-CSCF restoration mechanisms:

- HSS-based P-CSCF Restoration for Trusted/Untrusted WLAN Access (S2a/S2b)
- PCRF-based P-CSCF Restoration for LTE (S5/S8) and Trusted/Untrusted WLAN Access (S2a/S2b)



---

**Important** For more information on this feature, refer to the *HSS and PCRF Based P-CSCF Restoration Support* chapter in this guide.

---

## Inter-Chassis Session Recovery

Use of Interchassis Session Recovery requires that a valid license key be installed. Contact your local sales or support representative for information on how to obtain a license.

The ASR 5500 provides industry leading carrier class redundancy. The systems protects against all single points of failure (hardware and software) and attempts to recover to an operational state when multiple simultaneous failures occur.

The system provides several levels of system redundancy:

- Under normal N+1 packet processing card hardware redundancy, if a catastrophic packet processing card failure occurs all affected calls are migrated to the standby packet processing card if possible. Calls which cannot be migrated are gracefully terminated with proper call-termination signaling and accounting records are generated with statistics accurate to the last internal checkpoint
- If the Session Recovery feature is enabled, any total packet processing card failure will cause a packet processing card switchover and all established sessions for supported call-types are recovered without any loss of session.

Even though Cisco provides excellent intra-chassis redundancy with these two schemes, certain catastrophic failures which can cause total chassis outages, such as IP routing failures, line-cuts, loss of power, or physical destruction of the chassis, cannot be protected by this scheme. In such cases, the MME Inter-Chassis Session Recovery feature provides geographic redundancy between sites. This has the benefit of not only providing enhanced subscriber experience even during catastrophic outages, but can also protect other systems such as the RAN from subscriber re-activation storms.

The Interchassis Session Recovery feature allows for continuous call processing without interrupting subscriber services. This is accomplished through the use of redundant chassis. The chassis are configured as primary and backup with one being active and one in recovery mode. A checkpoint duration timer is used to control when subscriber data is sent from the active chassis to the inactive chassis. If the active chassis handling the call traffic goes out of service, the inactive chassis transitions to the active state and continues processing the call traffic without interrupting the subscriber session. The chassis determines which is active through a propriety TCP-based connection called a redundancy link. This link is used to exchange Hello messages between the primary and backup chassis and must be maintained for proper system operation.

#### • Interchassis Communication

Chassis configured to support Interchassis Session Recovery communicate using periodic Hello messages. These messages are sent by each chassis to notify the peer of its current state. The Hello message contains information about the chassis such as its configuration and priority. A dead interval is used to set a time limit for a Hello message to be received from the chassis' peer. If the standby chassis does not receive a Hello message from the active chassis within the dead interval, the standby chassis transitions to the active state. In situations where the redundancy link goes out of service, a priority scheme is used to determine which chassis processes the session. The following priority scheme is used:

- router identifier
- chassis priority
- SPIO MAC address

#### • Checkpoint Messages

Checkpoint messages are sent from the active chassis to the inactive chassis. Checkpoint messages are sent at specific intervals and contain all the information needed to recreate the sessions on the standby chassis, if that chassis were to become active. Once a session exceeds the checkpoint duration, checkpoint data is collected on the session. The checkpoint parameter determines the amount of time a session must be active before it is included in the checkpoint message.



#### Important

For more information on inter-chassis session recovery support, refer to the *Interchassis Session Recovery* chapter in the *System Administration Guide*.

## IP Security (IPSec) Encryption

Use of Network Domain Security requires that a valid license key be installed. Contact your local sales or support representative for information on how to obtain a license.

IPSec encryption enables network domain security for all IP packet switched LTE-EPC networks in order to provide confidentiality, integrity, authentication, and anti-replay protection. These capabilities are insured through use of cryptographic techniques.



The Cisco P-GW supports IKEv1 and IPSec encryption using IPv4 addressing. IPSec enables the following two use cases:

- Encryption of S8 sessions and EPS bearers in roaming applications where the P-GW is located in a separate administrative domain from the S-GW.
- IPSec ESP security in accordance with 3GPP TS 33.210 is provided for S1 control plane, S1 bearer plane and S1 management plane traffic. Encryption of traffic over the S1 reference interface is desirable in cases where the EPC core operator leases radio capacity from a roaming partner's network.



---

**Important** For more information on IPSec support, refer to the *IP Security (IPSec) Reference*.

---

## IPv6 Prefix Delegation from the RADIUS Server and the Local Pool

This feature adds support to obtain the DHCPv6 Prefix Delegation from the RADIUS server or a local pool configured on the GGSN/P-GW/SAEGW. Interface-ID allocation from RADIUS Server is also supported along with this feature.

A User Equipment (UE) or a Customer Premises Equipment (CPE) requests Prefix-Delegation. The P-GW or the GGSN then obtains this prefix from the RADIUS server or the local pool. P-GW and GGSN then advertise the prefix obtained by either RADIUS server or the local pool toward the UE client or the CPE.

This feature is divided into following three features:

- IPv6 Prefix Delegation from the RADIUS Server
- IPv6 Prefix Delegation from the Local Pool
- IPv6 Interface ID from the RADIUS Server



---

**Important** For more information on IPv6 Prefix Delegation, refer *IPv6 Prefix Delegation from the RADIUS Server and the Local Pool* chapter.

---

## L2TP LAC Support

Use of L2TP LAC requires that a valid license key be installed. Contact your local sales or support representative for information on how to obtain a license.

The system configured as a Layer 2 Tunneling Protocol Access Concentrator (LAC) enables communication with L2TP Network Servers (LNSs) for the establishment of secure Virtual Private Network (VPN) tunnels between the operator and a subscriber's corporate or home network.

The use of L2TP in VPN networks is often used as it allows the corporation to have more control over authentication and IP address assignment. An operator may do a first level of authentication, however use PPP to exchange user name and password, and use IPCP to request an address. To support PPP negotiation between the P-GW and the corporation, an L2TP tunnel must be setup in the P-GW running a LAC service.

L2TP establishes L2TP control tunnels between LAC and LNS before tunneling the subscriber PPP connections as L2TP sessions. The LAC service is based on the same architecture as the P-GW and benefits from dynamic resource allocation and distributed message and data processing.

The LAC sessions can also be configured to be redundant, thereby mitigating any impact of hardware or software issues. Tunnel state is preserved by copying the information across processor cards.



---

**Important** For more information on this feature support, refer to the *L2TP Access Concentrator* chapter in this guide.

---

## Lawful Intercept

The feature use license for Lawful Intercept on the P-GW is included in the P-GW session use license.

The Cisco Lawful Intercept feature is supported on the P-GW. 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 documentation on the Lawful Intercept feature, contact your Cisco account representative.

## Layer 2 Traffic Management (VLANs)

Use of Layer 2 Traffic Management requires that a valid license key be installed. Contact your Cisco sales or support representative for information on how to obtain a license.

Virtual LANs (VLANs) provide greater flexibility in the configuration and use of contexts and services.

VLANs are configured as "tags" on a per-port basis and allow more complex configurations to be implemented. The VLAN tag allows a single physical port to be bound to multiple logical interfaces that can be configured in different contexts; therefore, each Ethernet port can be viewed as containing many logical ports when VLAN tags are employed.



---

**Important** For more information on VLAN support, refer to the *VLANs* chapter in the *System Administration Guide*.

---

## Local Policy Decision Engine

Use of the Local Policy Decision Engine requires that a valid license key be installed. Contact your local Cisco sales or support representative for information on how to obtain a license.

The Local Policy Engine is an event-driven rules engine that offers Gx-like QoS and policy controls to enable user or application entitlements. As the name suggests, it is designed to provide a subset of a PCRF in cases where an operator elects not to use a PCRF or scenarios where connections to an external PCRF are disrupted. Local policies are used to control different aspects of a session like QoS, data usage, subscription profiles, and server usage by means of locally defined policies. A maximum of 1,024 local policies can be provisioned on a P-GW system.

Local policies are triggered when certain events occur and the associated conditions are satisfied. For example, when a new call is initiated, the QoS to be applied for the call could be decided based on the IMSI, MSISDN, and APN.

Potential use cases for the Local Policy Decision Engine include:

- Disaster recovery data backup solution in the event of a loss of PCRF in a mobile core network.
- Dedicated bearer establishment for emergency voice calls.
- Network-initiated bearer establishment on LTE to non-3GPP inter-domain handovers.

## MPLS Forwarding with LDP

Use of MPLS requires that a valid license key be installed. Contact your local Cisco sales or support representative for information on how to obtain a license.

Multi Protocol Label Switching (MPLS) is an operating scheme or a mechanism that is used to speed up the flow of traffic on a network by making better use of available network paths. It works with the routing protocols like BGP and OSPF, and therefore it is not a routing protocol.

MPLS generates a fixed-length label to attach or bind with the IP packet's header to control the flow and destination of data. The binding of the labels to the IP packets is done by the label distribution protocol (LDP). All the packets in a forwarding equivalence class (FEC) are forwarded by a label-switching router (LSR), which is also called an MPLS node. The LSR uses the LDP in order to signal its forwarding neighbors and distribute its labels for establishing a label switching path (LSP).

In order to support the increasing number of corporate APNs, which have a number of different addressing models and requirements, MPLS is deployed to fulfill at least the following two requirements:

- The corporate APN traffic must remain segregated from other APNs for security reasons.
- Overlapping of IP addresses in different APNs.

When deployed, the MPLS backbone automatically negotiates routes using the labels binded with the IP packets. Cisco P-GW as an LSR learns the default route from the connected provider edge (PE), while the PE populates its routing table with the routes provided by the P-GW.

## NEMO Service Supported

Use of NEMO requires that a valid license key be installed. Contact your local sales or support representative for information on how to obtain a license.

The P-GW may be configured to enable or disable Network Mobility (NEMO) service.

When enabled, the system includes NEMO support for a Mobile IPv4 Network Mobility (NEMO-HA) on the P-GW platform to terminate Mobile IPv4 based NEMO connections from Mobile Routers (MRs) that attach to an Enterprise PDN. The NEMO functionality allows bi-directional communication that is application-agnostic between users behind the MR and users or resources on Fixed Network sites.

The same NEMO4G-HA service and its bound Loopback IP address supports NEMO connections whose underlying PDN connection comes through GTP S5 (4G access) or PMIPv6 S2a (eHRPD access).



---

**Important**

For more information on NEMO support, refer to the *Network Mobility (NEMO)* chapter in this guide.

---

## NEMO Support in GGSN

Use of Dynamic Network Mobile Routing (NEMO) for GGSN requires that a valid license key be installed. Contact your Cisco account or support representative for information on how to obtain a license.

This feature now supports standards-based NEMO feature on GGSN, which allows operators to support Enterprise VPN service with the advantage of faster deployment and flexible bandwidth arrangement for customers.

NEMO (Network MObility) provides wireless connectivity between enterprise core network and remote sites over 3G/4G network. The wireless connection can be used as either primary link or backup link. All the hosts in the remote site can directly communicate with hosts in the core network without using NAT.

Enterprise VPN service is one of the main use case for this feature. Fast deployment and flexible bandwidth arrangement for customers are some of the advantages of this service. Customers include banks, financial institutions, multi-sited enterprises, city public safety departments, transportation fleet, etc.

NEMO is supported for subscribers roaming out on 3G (UMTS/GERAN) networks.

## Network Provided Location Information for IMS

Use of NPLI requires that a valid license key be installed. Contact your Cisco account or support representative for information on how to obtain a license.

This feature enables the P-GW to provide the required access network information to the PCRF within the 3GPP-User-Location-Info AVP, User-Location-Info-Time AVP (if available), and/or 3GPP-MS-TimeZone AVP as requested by the PCRF. The P-GW will also provide the ACCESS\_NETWORK\_INFO\_REPORT event trigger within Event-Trigger AVP.

During bearer deactivation or UE detach procedure, the P-GW will provide the access network information to the PCRF within the 3GPP-User-Location-Info AVP and information on when the UE was last known to be in that location within User-Location-Info-Time AVP. If the PCRF requested User location info as part of the Required-Access-Info AVP and it is not available in the P-GW, then the P-GW will provide the serving PLMN identifier within the 3GPP-SGSN-MCC-MNC AVP.

Previously, the P-GW notified ULI/MS-TimeZone/PLMN-ID to ECS/IMS/PCRF only when their value changed. With this feature, the P-GW receives NetLoc indication in the rules sent by ECS regardless of whether the values changed and it sends this to the ECS/IMS/PCRF. If the P-GW receives NetLoc as '1', then it will inform MS-Timezone. If the P-GW receives NetLoc as '0', then it will inform ULI and ULI Timestamp. If ULI is not available in that case, then the PLMN-ID is sent. If NetLoc indication is received for an update, then the P-GW will indicate this information to the access side in the UBReq using the RetLoc Indication flag.

This is required for VoLTE and aids in charging and LI functionality in IMS domain. This feature allows EPC core to support an efficient way of reporting ULI and Time-Zone information of the subscriber to the IMS core network.

## New Call Policy for Stale Sessions

Use of new call policy for stale sessions requires that a valid license key be installed. Contact your Cisco account or support representative for information on how to obtain a license.

If the newcall policy is set to **reject release-existing-session** and there are pre-existing sessions for the IMSI/IMEI received in Create Session Req, they will be deleted. This allows for no hung sessions on node with newcall policy reject release configured. When GGSN/P-GW/SAEGW/S-GW releases the existing call,

it follows a proper release process of sending Accounting Stop, sending CCR-T to PCRF/OCS, and generating CDR(s).

## Non-standard QCI Support

Use of non-standard QCIs require that a valid license key be installed. Contact your Cisco account or support representative for information on how to obtain a license.

Usually, only standards-based QCI values of 1 through 9 are supported on GGSN/P-GW/SAEGW/S-GW/ePDG. A special license, however, allows non-standard QCIs (128-254) to be used on P-GW/GGSN (not standalone GGSN).

QCI values 1 through 9 are defined in *3GPP Specification TS 23.203 "Policy and charging control architecture"*

From 3GPP Release 8 onwards, operator-specific/non-standard QCIs can be supported and carriers can define QCI 128-254. As per *3GPP Specification TS 29.212 "Policy and Charging Control over Gx reference point,"* QCI values 0 and 10 to 255 are defined as follows:

- 0: Reserved
- 10-127: Reserved
- 128-254: Operator-specific/Non-standard QCI
- 255: Reserved

Unique operator-specific QCIs (128-254) can be used to differentiate between various services/applications carriers provide to the end users in their network.

The **operator-defined-qci** command in the QCI-QoS Mapping Configuration Mode configures the non-standard QCIs in P-GW so that calls can be accepted when non-standard QCI values are received from UE or PCRF. Unique DSCP parameters (uplink and downlink) and GBR or Non-GBR can also be configured. Non-standard QCIs can only be supported with S5/S8/S2a/S2b interfaces; the Gn interface is not supported. As non-standard QCIs are not supported in GGSN, **pre-rel8-qos-mapping** is used as a reference for mapping the non-standard QCI values to pre-rel8 QoS values during 3G calls or GnGp handovers.



---

**Important** For more information on this command, refer to the *CLI Reference Guide*.

---

## Paging Policy Differentiation

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

S-GW/P-GW provide configuration control to change the DSCP value of the user-datagram packet and outer IP packet (GTP-U tunnel IP header). DSCP marking is done at various levels depending on the configuration. When the Paging Policy Differentiation (PPD) feature is enabled, however, the user-datagram packet DSCP (tunneled IP packet) marking does not change.

Currently, standards specify QCI to DSCP marking of outer GTP-U header only. All configurations present at ECS, P-GW, and S-GW to change the user-datagram packet DSCP value are non-standard. The standards-based PPD feature dictates that P-CSCF or similar Gi entity marks the DSCP of user-datagram packet. This user-datagram packet DSCP value is sent in DDN message by S-GW to MME/S4-SGSN. MME/S4-SGSN uses this DSCP value to give paging priority.




---

**Important** P-GW and S-GW should apply the PPD feature for both Default and Dedicated bearers. As per the specifications, P-GW transparently passes the user-datagram packet towards S-GW. This means, if PPD feature is enabled, operator can't apply different behavior for Default and Dedicated bearers.

---




---

**Important** For more information on paging policy differentiation, refer to the *Paging Policy Differentiation* chapter in this guide.

---

## Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters

### Support for QCI and ARP Visibility

As of StarOS release 20.2, the software has been enhanced to support the viewing of QoS statistics on a Quality of Service Class Index (QCI) and Allocation and Retention Priority (ARP) basis.

ARP is a 3GPP mechanism for dropping or downgrading lower-priority bearers in situations where the network becomes congested. The network looks at the ARP when determining if new dedicated bearers can be established through the radio base station. QCI is an operator provisioned value that controls bearer level packet forwarding treatments.

This enhancement enables operators to monitor QoS statistics that identify multiple services running with the same QCI value. In addition, packet drop counters have been introduced to provide the specific reason the Enhanced Charging Service (ECS) dropped a packet. The packet drop counters provide output on a per ARP basis. This provides additional information that operators can use to troubleshoot and identify network issues that may be affecting service.




---

**Important** For the ARP value only the priority level value in the Allocation/Retention Priority (ARP) Information Element (IE) is considered. Pre-emption Vulnerability (PVI) and Pre-emption Capability (PCI) flags in the ARP IE are not considered.

---

The existing **show apn statistics name** *apn-name* and **show apn statistics Exec Mode** CLI commands have been enhanced. The output of these commands now provides visibility for QoS statistics on a QCI/ARP basis.




---

**Important** For more detailed information, refer to the *Extended QCI Options* chapter in this guide.

---

### Licensing

ARP Granularity for QCI Level Counters is a license-controlled feature. Per QCI Packet Drop Counters functionality does not require a license. Contact your Cisco account or support representative for licensing details.

## Piggyback Support on S2b Interface

This feature supports piggybacking of "Create Session Response" and "Create Bearer Request" messages on ePDG and P-GW over the S2b interface. If piggybacking flag is set by the ePDG in the Create Session Request, P-GW can now send Create Session Response and Create Bearer Request together to the ePDG and eliminate the possibility of reordering of these messages.

## R12 Load and Overload Support

Use of R12 Load and Overload Support requires that a valid license key be installed. Contact your Cisco account or support representative for information on how to obtain a license.

GTP-C Load Control feature is an optional feature which allows a GTP control plane node to send its Load Information to a peer GTP control plane node which the receiving GTP control plane peer node uses to augment existing GW selection procedure for the P-GW and S-GW. Load Information reflects the operating status of the resources of the originating GTP control plane node.

Nodes using GTP control plane signaling may support communication of Overload control Information in order to mitigate overload situation for the overloaded node through actions taken by the peer node(s). This feature is supported over S4, S11, S5 and S8 interfaces via the GTPv2 control plane protocol.

A GTP-C node is considered to be in overload when it is operating over its nominal capacity resulting in diminished performance (including impacts to handling of incoming and outgoing traffic). Overload control Information reflects an indication of when the originating node has reached such a situation. This information, when transmitted between GTP-C nodes may be used to reduce and/or throttle the amount of GTP-C signaling traffic between these nodes. As such, the Overload control Information provides guidance to the receiving node to decide actions, which leads to mitigation towards the sender of the information.

In brief, load control and overload control can be described in this manner:

- Load control enables a GTP-C entity (for example, an S-GW/P-GW) to send its load information to a GTP-C peer (e.g. an MME/SGSN, ePDG, TWAN) to adaptively balance the session load across entities supporting the same function (for example, an S-GW cluster) according to their effective load. The load information reflects the operating status of the resources of the GTP-C entity.
- Overload control enables a GTP-C entity becoming or being overloaded to gracefully reduce its incoming signaling load by instructing its GTP-C peers to reduce sending traffic according to its available signaling capacity to successfully process the traffic. A GTP-C entity is in overload when it operates over its signaling capacity, which results in diminished performance (including impacts to handling of incoming and outgoing traffic).

A maximum of 64 different load and overload profiles can be configured.



---

**Important**

For more information on this feature, refer to the *GTP-C Load and Overload Control Support on the P-GW, SAEGW, and S-GW* chapter in this guide.

---

## Operation

The node periodically fetches various parameters (for example, License-Session-Utilization, System-CPU-Utilization and System-Memory-Utilization), which are required for Node level load control information. The node then calculates the load control information itself either based on the weighted factor provided by the user or using the default weighted factor.

Node level load control information is calculated every 30 seconds. The resource manager calculates the system-CPU-utilization and System-Memory-Utilization at a systems level.

For each configured service, load control information can be different. This can be achieved by providing a weightage to the number of active session counts per service license, for example,  $((\text{number of active sessions per service} / \text{max session allowed for the service license}) * 100)$ .

The node's resource manager calculates the system-CPU-utilization and System-Memory-Utilization at a systems level by averaging CPU and Memory usage for all cards and which might be different from that calculated at the individual card level.

## Session Recovery Support

The feature use license for Session Recovery on the P-GW is included in the P-GW session use license.

Session recovery 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.

In the telecommunications industry, over 90 percent of all equipment failures are software-related. With robust hardware failover and redundancy protection, any card-level hardware failures on the system can quickly be corrected. However, software failures can occur for numerous reasons, many times without prior indication. StarOS Release 9.0 adds the ability to support stateful intra-chassis session recovery for P-GW sessions.

When session recovery occurs, the system reconstructs the following subscriber information:

- Data and control state information required to maintain correct call behavior
- Subscriber data statistics that are required to ensure that accounting information is maintained
- A best-effort attempt to recover various timer values such as call duration, absolute time, and others

Session recovery is also useful for in-service software patch upgrade activities. If session recovery is enabled during the software patch upgrade, it helps to preserve existing sessions on the active packet processing cards during the upgrade process.



---

**Important**

For more information on session recovery support, refer to the *Session Recovery* chapter in the *System Administration Guide*.

---

## S-GW Paging Enhancements

Use of S-GW Paging requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

S-GW Paging includes the following scenarios:

**Scenario 1:** S-GW sends a 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 does not 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 have been added to the DDN functionality:

- 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 is not lost.
- MBR guard timer, which is started when DDN Ack with temporary HO is received. A new 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 the above functionality, 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.



---

**Important** For more information on this functionality, refer to the *S-GW Paging Enhancements* chapter in this guide.

---

## Smartphone Tethering Detection Support

Use of Smartphone Tethering Detection requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

On the P-GW, using the inline heuristic detection mechanism, it is now possible to detect and differentiate between the traffic from the mobile device and a tethered device connected to the mobile device.

## Traffic Policing

Use of Per-Subscriber Traffic Policing requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

Traffic policing allows you to manage bandwidth usage on the network and limit bandwidth allowances to subscribers.

Traffic policing enables the configuring and enforcing of bandwidth limitations on individual subscribers and/or APNs of a particular traffic class in 3GPP/3GPP2 service.

Bandwidth enforcement is configured and enforced independently on the downlink and the uplink directions.

A Token Bucket Algorithm (a modified trTCM) [RFC2698] is used to implement the Traffic-Policing feature. The algorithm used measures the following criteria when determining how to mark a packet:

- **Committed Data Rate (CDR):** The guaranteed rate (in bits per second) at which packets can be transmitted/received for the subscriber during the sampling interval.
- **Peak Data Rate (PDR):** The maximum rate (in bits per second) that subscriber packets can be transmitted/received for the subscriber during the sampling interval.
- **Burst-size:** The maximum number of bytes that can be transmitted/received for the subscriber during the sampling interval for both committed (CBS) and peak (PBS) rate conditions. This represents the maximum number of tokens that can be placed in the subscriber's "bucket". Note that the committed burst size (CBS) equals the peak burst size (PBS) for each subscriber.

The system can be configured to take any of the following actions on packets that are determined to be in excess or in violation:

- **Drop:** The offending packet is discarded.
- **Transmit:** The offending packet is passed.
- **Lower the IP Precedence:** The packet's ToS bit is set to "0", thus downgrading it to Best Effort, prior to passing the packet. Note that if the packet's ToS bit was already set to "0", this action is equivalent to "Transmit".



#### Important

For more information on traffic policing, refer to the *Traffic Policing and Shaping* chapter in this guide.

## Traffic Shaping

Traffic Shaping is a rate limiting method similar to Traffic Policing, but provides a buffer facility for packets exceeding the configured limit. Once packets exceed the data-rate, the packet is queued inside the buffer to be delivered at a later time.

The bandwidth enforcement can be done in the downlink and the uplink direction independently. If there is no more buffer space available for subscriber data, the system can be configured to either drop the packets or retain them for the next scheduled traffic session.

Traffic will be shaped to the configured APN-AMBR value. Previously, data carried on non-GBR bearers was policed at the configured APN-AMBR rate. APN-AMBR policing dropped the data that did not match the configured APN-AMBR. With APN-AMBR traffic shaping, non-GBR data that does not match the configured APN-AMBR rate will be buffered. When enough memory tokens are available, the data will be transmitted. In addition, operators still have the option to allow operators to drop or transmit the data when the buffer limit is reached.



#### Important

For more information on traffic shaping, refer to the *Traffic Policing and Shaping* chapter in this guide.

## UBR Suppression Feature

The Update Bearer Request (UBR) Suppression feature is a license controlled feature. Please contact your Cisco account or service representative for more information.

As the bit rate is expressed in bps on Gx and kbps on GTP, the P-GW does a round-off to convert a Gx request into a GTP request. When the P-GW receives RAR from PCRF with minimal bit rate changes (in bps), a UBR is sent, even if the same QoS (in Kbps) is already set for the bearer. The UBR suppression feature enables the P-GW to suppress such a UBR where there is no update for any of the bearer parameters.

A new CLI command, **suppress-ubr no-bitrate-change**, has been added to the P-GW Service Configuration Mode to enable UBR suppression. Once the CLI is configured, P-GW suppresses the UBR if the bit rate is the same after the round-off.

When UBR has multiple bearer contexts, the bearer context for which the bit rate change is less than 1 kbps after round-off is suppressed. If other parameters, such as QCI, ARP, and TFT, that might trigger UBR are changed and there is no change in bit rates after round-off, then UBR is not suppressed. Suppression of UBR is applicable for UBR triggered by CCA-I, RAR, and Modify Bearer Command.

To summarize, if the license is enabled and the CLI command is configured for UBR suppression, then UBR is suppressed if bit rates in kbps are the same after round-off and all other parameters, such as QCI, ARP, and TFT, that might trigger UBR are also unchanged.

## User Location Information Reporting

Use of User Location Information (ULI) Reporting requires that a valid license key be installed. Contact your local sales or support representative for information on how to obtain a license.

ULI Reporting allows the eNodeB to report the location of a UE to the MME, when requested by a P-GW.

The following procedures are used over the S1-MME interface to initiate and stop location reporting between the MME and eNodeB:

- **Location Reporting Control:** The purpose of Location Reporting Control procedure is to allow the MME to request that the eNodeB report where the UE is currently located. This procedure uses UE-associated signaling.
- **Location Report Failure Indication:** The Location Report Failure Indication procedure is initiated by an eNodeB in order to inform the MME that a Location Reporting Control procedure has failed. This procedure uses UE-associated signaling.
- **Location Report:** The purpose of Location Report procedure is to provide the UE's current location to the MME. This procedure uses UE-associated signaling.

The start/stop trigger for location reporting for a UE is reported to the MME by the S-GW over the S11 interface. The Change Reporting Action (CRA) Information Element (IE) is used for this purpose. The MME updates the location to the S-GW using the User Location Information (ULI) IE.

The following S11 messages are used to transfer CRA and ULI information between the MME and S-GW:

- **Create Session Request:** The ULI IE is included for E-UTRAN Initial Attach and UE-requested PDN Connectivity procedures. It includes ECGI and TAI. The MME includes the ULI IE for TAU/ X2-Handover procedure if the P-GW has requested location information change reporting and the MME support location information change reporting. The S-GW includes the ULI IE on S5/S8 exchanges if it receives the ULI from the MME. If the MME supports change reporting, it sets the corresponding indication flag in the Create Session Request message.
- **Create Session Response:** The CRA IE in the Create Session Response message can be populated by the S-GW to indicate the type of reporting required.

- **Create Bearer Request:** The CRA IE is included with the appropriate Action field if the Location Change Reporting mechanism is to be started or stopped for the subscriber in the MME.
- **Modify Bearer Request:** The MME includes the ULI IE for TAU/Handover procedures and UE-initiated Service Request procedures if the P-GW has requested location information change reporting and the MME supports location information change reporting. The S-GW includes this IE on S5/S8 exchanges if it receives the ULI from the MME.
- **Modify Bearer Response:** The CRA IE is included with the appropriate Action field if the Location Change Reporting mechanism is to be started or stopped for the subscriber in the MME.
- **Delete Session Request:** The MME includes the ULI IE for the Detach procedure if the P-GW has requested location information change reporting and MME supports location information change reporting. The S-GW includes this IE on S5/S8 exchanges if it receives the ULI from the MME.
- **Update Bearer Request:** The CRA IE is included with the appropriate Action field if the Location Change Reporting mechanism is to be started or stopped for the subscriber in the MME.
- **Change Notification Request:** If no existing procedure is running for a UE, a Change Notification Request is sent upon receipt of an S1-AP location report message. If an existing procedure is running, one of the following messages reports the ULI:
  - Create Session Request
  - Create Bearer Response
  - Modify Bearer Request
  - Update Bearer Response
  - Delete Bearer Response
  - Delete Session Request

If an existing Change Notification Request is pending, it is aborted and a new one is sent.



#### Important

Information on configuring User Location Information (ULI) Reporting support is located in the *Configuring Optional Features on the MME* section of the *Mobility Management Entity Configuration* chapter in the *Mobility Management Entity Administration Guide*.

## 3GPP ULI Reporting Support Enhanced

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

### Feature Change

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 any change is detected and same change has been requested by the PCRF as an event trigger then the ULI is reported to the PCRF.

SGSN reports ULI to the GGSN. GGSN determines the changes in the ULI with previously received ULI. If any change is detected and same change has been requested by the PCRF as an event trigger, then the ULI is

reported to the PCRF. Support has also been added to detect the change in RAI received as part of the ULI field at GGSN.

Following table summarizes the Change Reporting Action (CRA) values based on Event Triggers received from the PCRF, which the P-GW communicates with S4 SGSN.

Event Trigger From PCRF	CRA Sent to S4 SGSN
USER_LOCATION_CHANGE (13)	Start Reporting CGI/SAI and RAI (5)
RAI_CHANGE (12)	Start Reporting RAI (2)
USER_LOCATION_CHANGE + RAI_CHANGE	Start Reporting CGI/SAI and RAI (5)

Following table summarizes the MS Info Change Reporting Action values based on Event Triggers received from the PCRF which GGSN communicates to SGSN.

Event Trigger from PCRF	MS Info Change Reporting Action towards SGSN
USER_LOCATION_CHANGE (13)	Start Reporting CGI/SAI (1)
RAI_CHANGE (12)	Start Reporting RAI (2)
BOTH (12,13)	Start Reporting CGI/SAI (1)

P-GW/GGSN reports the CRA/MS Info Change Reporting Action immediately on receiving the Event Triggers without waiting for other events like APN/AMBR update or QoS update.

### Behavior Change

**Previous of Change Reporting Action:** Following table illustrates the old and new behavior of Change Reporting Action with respect to the Event Triggers received from PCRF, when the Access Node is S4SGSN.

Event Trigger From PCRF	CRA Sent to S4SGSN	CRA Sent to S4SGSN
ULI_CHANGE(13)	6 (START_REPORTING_TAI_ECGI)	5(START_REPORTING_CGI_RAI)
RAI_CHANGE(12)	No CRA Sent	2 (START_REPORTING_RAI)
BOTH (12,13)	6 (START_REPORTING_TAI_ECGI)	5 (START_REPORTING_CGI_RAI)

**Behavior of MS Info Change Reporting Action:** Following table illustrates the old and new behavior of MS Info CRA with respect to the Event Triggers received from PCRF, when the Access Node is SGSN.

Event Trigger From PCRF	CRA Sent to SGSN	CRA Sent to SGSN
ULI_CHANGE(13)	1 (START_REPORTING_CGI/SAI)	1 (START_REPORTING_CGI/SAI)
RAI_CHANGE(12)	No CRA Sent	2 (START_REPORTING_RAI)
BOTH (12,13)	1 (START_REPORTING_CGI/SAI)	1 (START_REPORTING_CGI/SAI)

**Limitations**

1. In GGSN, when a new ULI is received in the Network Request Updated PDP Context (NRUPC) Response, it is not reported to the PCRF.
2. In GGSN, when a dedicated bearer is deleted or call is dropped, ULI change is not detected.

## How the Serving Gateway Works

This section provides information on the function of the S-GW in an EPC E-UTRAN network and presents call procedure flows for different stages of session setup and disconnect.

The S-GW supports the following network flows:

- [GTP Serving Gateway Call/Session Procedures in an LTE-SAE Network, on page 134](#)

## GTP Serving Gateway Call/Session Procedures in an LTE-SAE Network

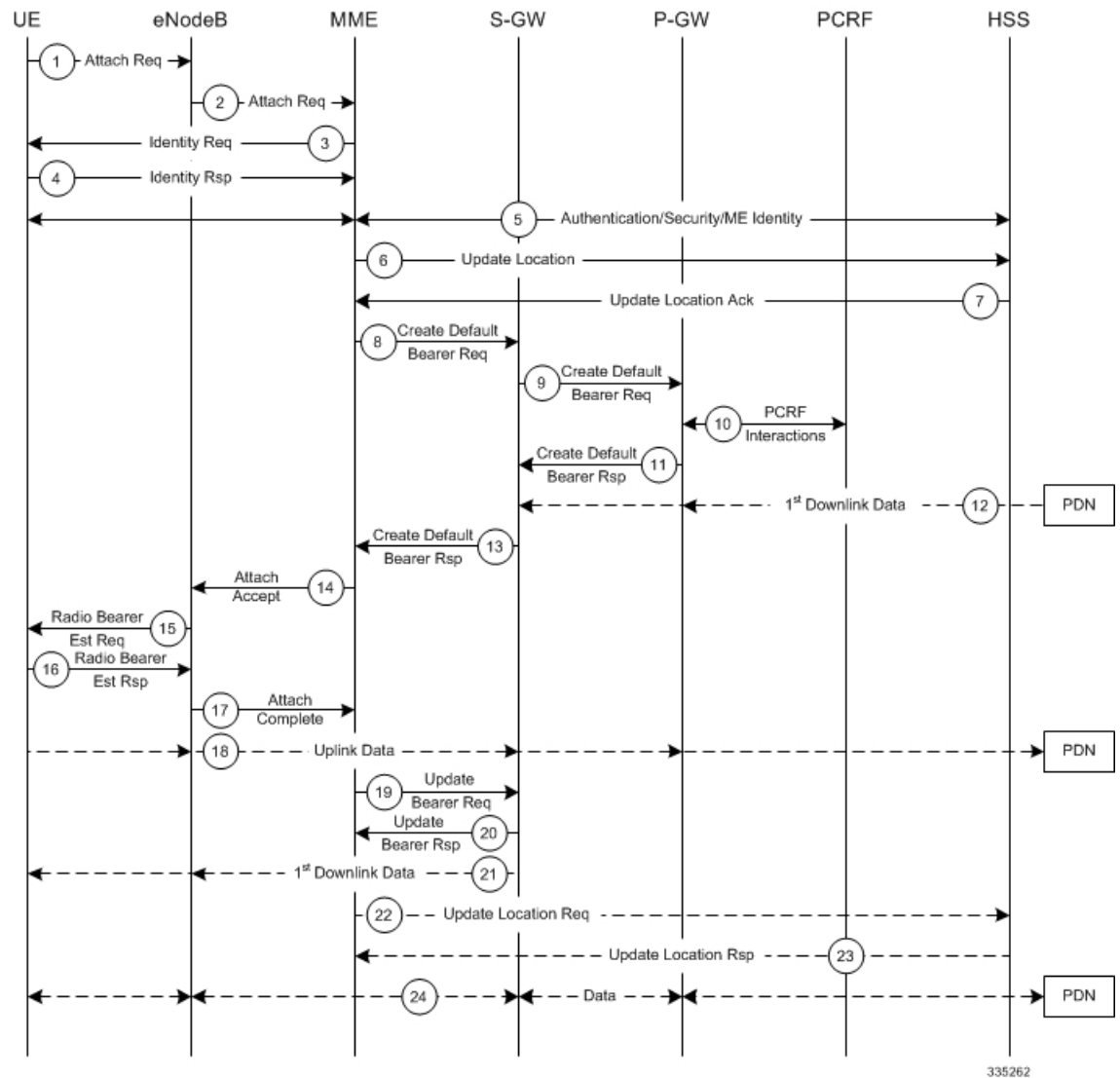
The following topics and procedure flows are included:

- [Subscriber-initiated Attach \(initial\), on page 134](#)
- [Subscriber-initiated Detach, on page 137](#)

### Subscriber-initiated Attach (initial)

This section describes the procedure of an initial attach to the EPC network by a subscriber.

Figure 35: Subscriber-initiated Attach (initial) Call Flow



335262

Table 12: Subscriber-initiated Attach (initial) Call Flow Description

Step	Description
1	The UE initiates the Attach procedure by the transmission of an Attach Request (IMSI or old GUTI, last visited TAI (if available), UE Network Capability, PDN Address Allocation, Protocol Configuration Options, Attach Type) message together with an indication of the Selected Network to the eNodeB. IMSI is included if the UE does not have a valid GUTI available. If the UE has a valid GUTI, it is included.
2	The eNodeB derives the MME from the GUTI and from the indicated Selected Network. If that MME is not associated with the eNodeB, the eNodeB selects an MME using an MME selection function. The eNodeB forwards the Attach Request message to the new MME contained in a S1-MME control message (Initial UE message) together with the Selected Network and an indication of the E-UTRAN Area identity, a globally unique E-UTRAN ID of the cell from where it received the message to the new MME.

Step	Description
3	If the UE is unknown in the MME, the MME sends an Identity Request to the UE to request the IMSI.
4	The UE responds with Identity Response (IMSI).
5	If no UE context for the UE exists anywhere in the network, authentication is mandatory. Otherwise this step is optional. However, at least integrity checking is started and the ME Identity is retrieved from the UE at Initial Attach. The authentication functions, if performed this step, involves AKA authentication and establishment of a NAS level security association with the UE in order to protect further NAS protocol messages.
6	The MME sends an Update Location (MME Identity, IMSI, ME Identity) to the HSS.
7	The HSS acknowledges the Update Location message by sending an Update Location Ack to the MME. This message also contains the Insert Subscriber Data (IMSI, Subscription Data) Request. The Subscription Data contains the list of all APNs that the UE is permitted to access, an indication about which of those APNs is the Default APN, and the EPS subscribed QoS profile for each permitted APN. If the Update Location is rejected by the HSS, the MME rejects the Attach Request from the UE with an appropriate cause.
8	The MME selects an S-GW using the Serving GW selection function and allocates an EPS Bearer Identity for the Default Bearer associated with the UE. If the PDN subscription context contains no P-GW address the MME selects a P-GW as described in clause PDN GW selection function. Then it sends a Create Default Bearer Request (IMSI, MME Context ID, APN, RAT type, Default Bearer QoS, PDN Address Allocation, AMBR, EPS Bearer Identity, Protocol Configuration Options, ME Identity, User Location Information) message to the selected S-GW.
9	The S-GW creates a new entry in its EPS Bearer table and sends a Create Default Bearer Request (IMSI, APN, S-GW Address for the user plane, S-GW TEID of the user plane, S-GW TEID of the control plane, RAT type, Default Bearer QoS, PDN Address Allocation, AMBR, EPS Bearer Identity, Protocol Configuration Options, ME Identity, User Location Information) message to the P-GW.
10	If dynamic PCC is deployed, the P-GW interacts with the PCRF to get the default PCC rules for the UE. The IMSI, UE IP address, User Location Information, RAT type, AMBR are provided to the PCRF by the P-GW if received by the previous message.
11	The P-GW returns a Create Default Bearer Response (P-GW Address for the user plane, P-GW TEID of the user plane, P-GW TEID of the control plane, PDN Address Information, EPS Bearer Identity, Protocol Configuration Options) message to the S-GW. PDN Address Information is included if the P-GW allocated a PDN address Based on PDN Address Allocation received in the Create Default Bearer Request. PDN Address Information contains an IPv4 address for IPv4 and/or an IPv6 prefix and an Interface Identifier for IPv6. The P-GW takes into account the UE IP version capability indicated in the PDN Address Allocation and the policies of operator when the P-GW allocates the PDN Address Information. Whether the IP address is negotiated by the UE after completion of the Attach procedure, this is indicated in the Create Default Bearer Response.
12	The Downlink (DL) Data can start flowing towards S-GW. The S-GW buffers the data.
13	The S-GW returns a Create Default Bearer Response (PDN Address Information, S-GW address for User Plane, S-GW TEID for User Plane, S-GW Context ID, EPS Bearer Identity, Protocol Configuration Options) message to the new MME. PDN Address Information is included if it was provided by the P-GW.
14	The new MME sends an Attach Accept (APN, GUTI, PDN Address Information, TAI List, EPS Bearer Identity, Session Management Configuration IE, Protocol Configuration Options) message to the eNodeB.
15	The eNodeB sends Radio Bearer Establishment Request including the EPS Radio Bearer Identity to the UE. The Attach Accept message is also sent along to the UE.

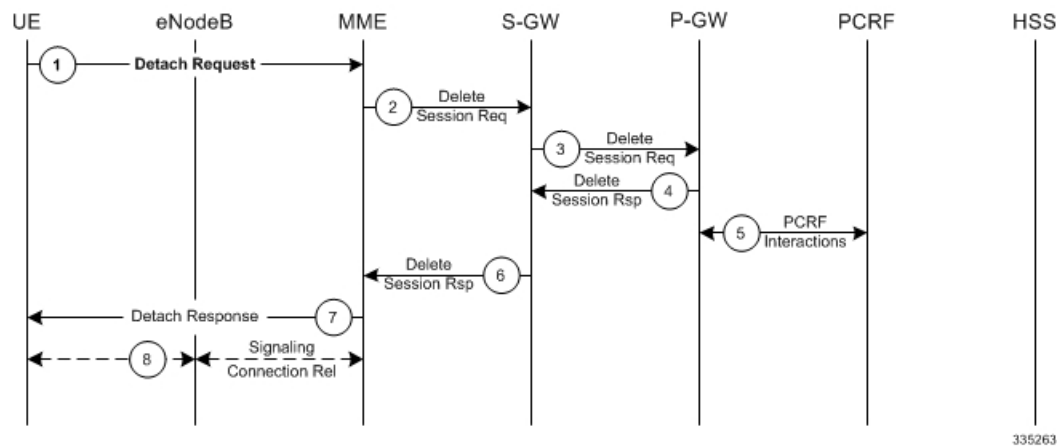


Step	Description
16	The UE sends the Radio Bearer Establishment Response to the eNodeB. In this message, the Attach Complete message (EPS Bearer Identity) is included.
17	The eNodeB forwards the Attach Complete (EPS Bearer Identity) message to the MME.
18	The Attach is complete and UE sends data over the default bearer. At this time the UE can send uplink packets towards the eNodeB which are then tunneled to the S-GW and P-GW.
19	The MME sends an Update Bearer Request (eNodeB address, eNodeB TEID) message to the S-GW.
20	The S-GW acknowledges by sending Update Bearer Response (EPS Bearer Identity) message to the MME.
21	The S-GW sends its buffered downlink packets.
22	After the MME receives Update Bearer Response (EPS Bearer Identity) message, if an EPS bearer was established and the subscription data indicates that the user is allowed to perform handover to non-3GPP accesses, and if the MME selected a P-GW that is different from the P-GW address which was indicated by the HSS in the PDN subscription context, the MME sends an Update Location Request including the APN and P-GW address to the HSS for mobility with non-3GPP accesses.
23	The HSS stores the APN and P-GW address pair and sends an Update Location Response to the MME.
24	Bidirectional data is passed between the UE and PDN.

## Subscriber-initiated Detach

This section describes the procedure of detachment from the EPC network by a subscriber.

**Figure 36: Subscriber-initiated Detach Call Flow**



**Table 13: Subscriber-initiated Detach Call Flow Description**

Step	Description
1	The UE sends NAS message Detach Request (GUTI, Switch Off) to the MME. Switch Off indicates whether detach is due to a switch off situation or not.
2	The active EPS Bearers in the S-GW regarding this particular UE are deactivated by the MME sending a Delete Bearer Request (TEID) message to the S-GW.

Step	Description
3	The S-GW sends a Delete Bearer Request (TEID) message to the P-GW.
4	The P-GW acknowledges with a Delete Bearer Response (TEID) message.
5	The P-GW may interact with the PCRF to indicate to the PCRF that EPS Bearer is released if PCRF is applied in the network.
6	The S-GW acknowledges with a Delete Bearer Response (TEID) message.
7	If Switch Off indicates that the detach is not due to a switch off situation, the MME sends a Detach Accept message to the UE.
8	The MME releases the S1-MME signaling connection for the UE by sending an S1 Release command to the eNodeB with Cause = Detach.

## How the PDN Gateway Works

This section provides information on the function of the P-GW in an EPC E-UTRAN network and presents call procedure flows for different stages of session setup and disconnect.

The P-GW supports the following network flows:

- [PMIPv6 PDN Gateway Call/Session Procedures in an eHRPD Network, on page 138](#)
- [GTP PDN Gateway Call/Session Procedures in an LTE-SAE Network, on page 144](#)

### PMIPv6 PDN Gateway Call/Session Procedures in an eHRPD Network

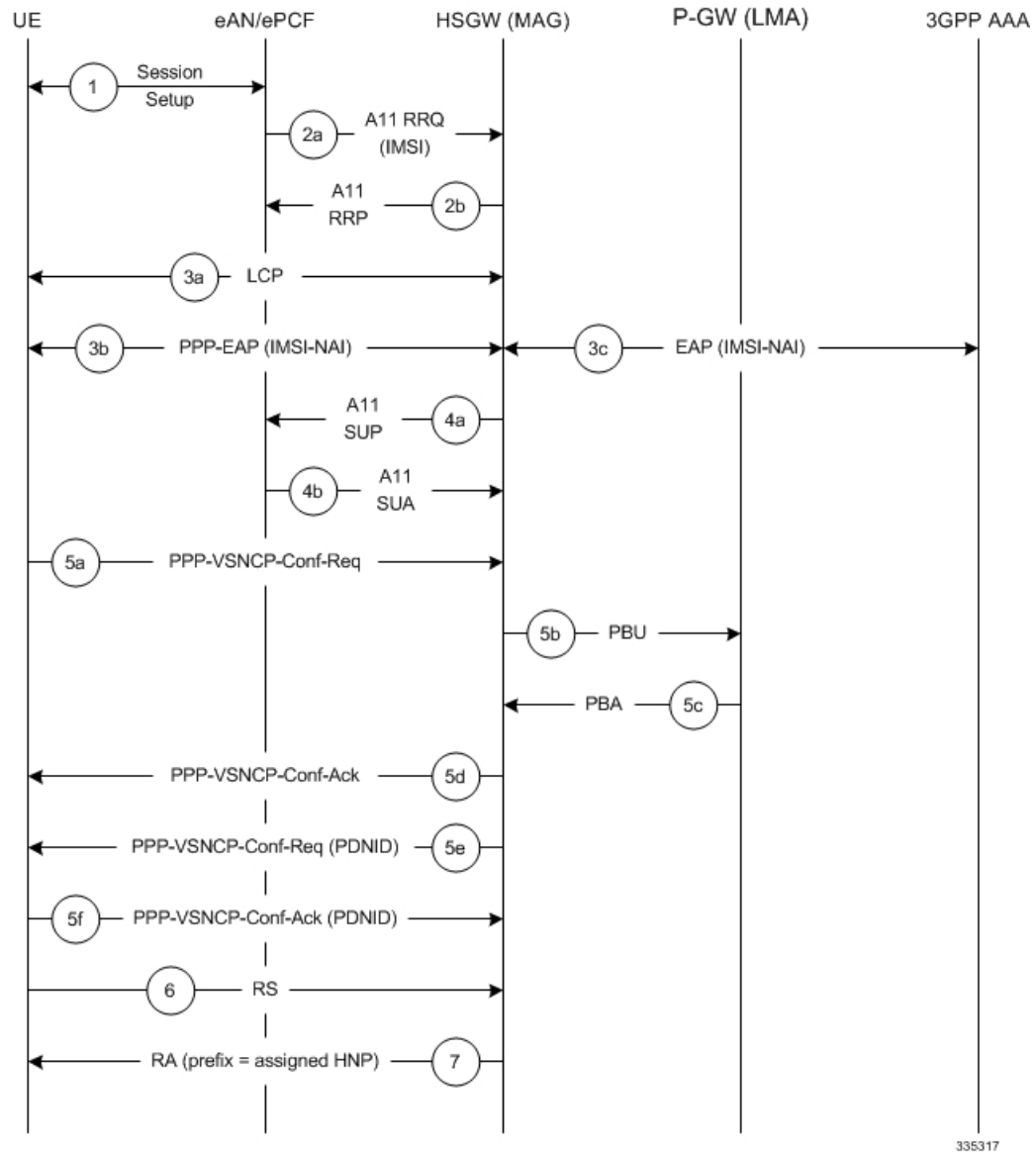
The following topics and procedure flows are included:

- [Initial Attach with IPv6/IPv4 Access, on page 138](#)
- [PMIPv6 Lifetime Extension without Handover, on page 140](#)
- [PDN Connection Release Initiated by UE, on page 141](#)
- [PDN Connection Release Initiated by HSGW, on page 142](#)
- [PDN Connection Release Initiated by P-GW, on page 143](#)

#### Initial Attach with IPv6/IPv4 Access

This section describes the procedure of initial attach and session establishment for a subscriber (UE).

Figure 37: Initial Attach with IPv6/IPv4 Access Call Flow



335317

Table 14: Initial Attach with IPv6/IPv4 Access Call Flow Description

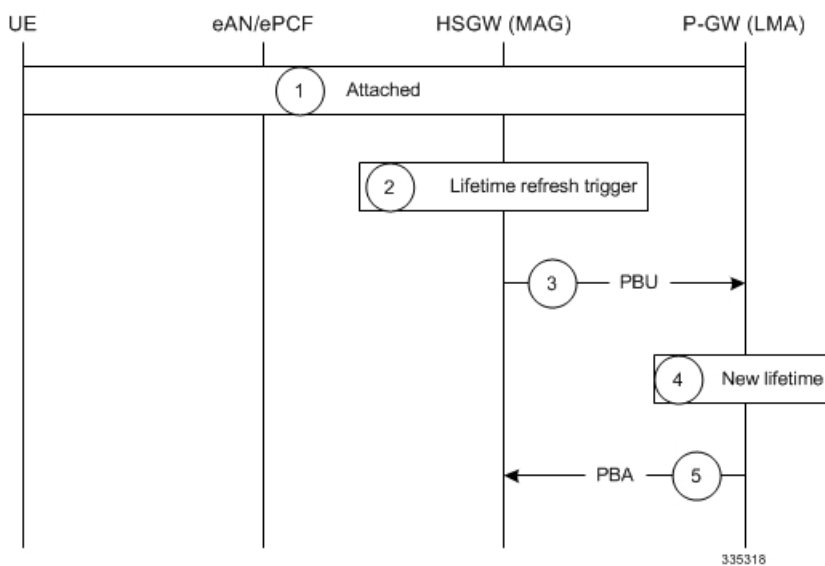
Step	Description
1	The subscriber (UE) attaches to the eHRPD network.
2a	The eAN/PCF sends an A11 RRQ to the HSGW. The eAN/PCF includes the true IMSI of the UE in the A11 RRQ.
2b	The HSGW establishes A10s and respond back to the eAN/PCF with an A11 RRP.
3a	The UE performs LCP negotiation with the HSGW over the established main A10.
3b	The UE performs EAP over PPP.

Step	Description
3c	EAP authentication is completed between the UE and the 3GPP AAA. During this transaction, the HSGW receives the subscriber profile from the AAA server.
4a	After receiving the subscriber profile, the HSGW sends the QoS profile in A11 Session Update Message to the eAN/PCF.
4b	The eAN/PCF responds with an A11 Session Update Acknowledgment (SUA).
5a	The UE initiates a PDN connection by sending a PPP-VSNCP-Conf-Req message to the HSGW. The message includes the PDNID of the PDN, APN, PDN-Type=IPv6/[IPv4], PDSN-Address and, optionally, PCO options the UE is expecting from the network.
5b	The HSGW sends a PBU to the P-GW.
5c	The P-GW processes the PBU from the HSGW, assigns an HNP for the connection and responds back to the HSGW with PBA.
5d	The HSGW responds to the VSNCP Conf Req with a VSNCP Conf Ack.
5e	The HSGW sends a PPP-VSNCP-Conf-Req to the UE to complete PPP VSNCP negotiation.
5f	The UE completes VSNCP negotiation by returning a PPP-VSNCP-Conf-Ack.
6	The UE optionally sends a Router Solicitation (RS) message.
7	The HSGW sends a Router Advertisement (RA) message with the assigned Prefix.

## PMIPv6 Lifetime Extension without Handover

This section describes the procedure of a session registration lifetime extension by the P-GW without the occurrence of a handover.

**Figure 38: PMIPv6 Lifetime Extension (without handover) Call Flow**

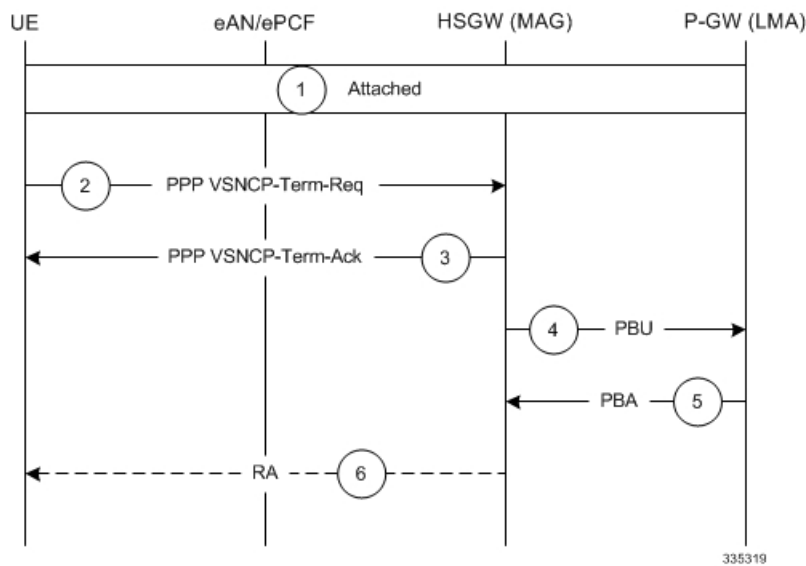


**Table 15: PMIPv6 Lifetime Extension (without handover) Call Flow Description**

Step	Description
1	The UE is attached to the EPC and has a PDN connection with the P-GW where PDNID=x and an APN with assigned HNP.
2	The HSGW MAG service registration lifetime nears expiration and triggers a renewal request for the LMA.
3	The MAG service sends a Proxy Binding Update (PBU) to the P-GW LMA service with the following attributes: Lifetime, MNID, APN, ATT=HRPD, HNP.
4	The P-GW LMA service updates the Binding Cache Entry (BCE) with the new granted lifetime.
5	The P-GW responds with a Proxy Binding Acknowledgment (PBA) with the following attributes: Lifetime, MNID, APN.

## PDN Connection Release Initiated by UE

This section describes the procedure of a session release by the UE.

**Figure 39: PDN Connection Release by the UE Call Flow****Table 16: PDN Connection Release by the UE Call Flow Description**

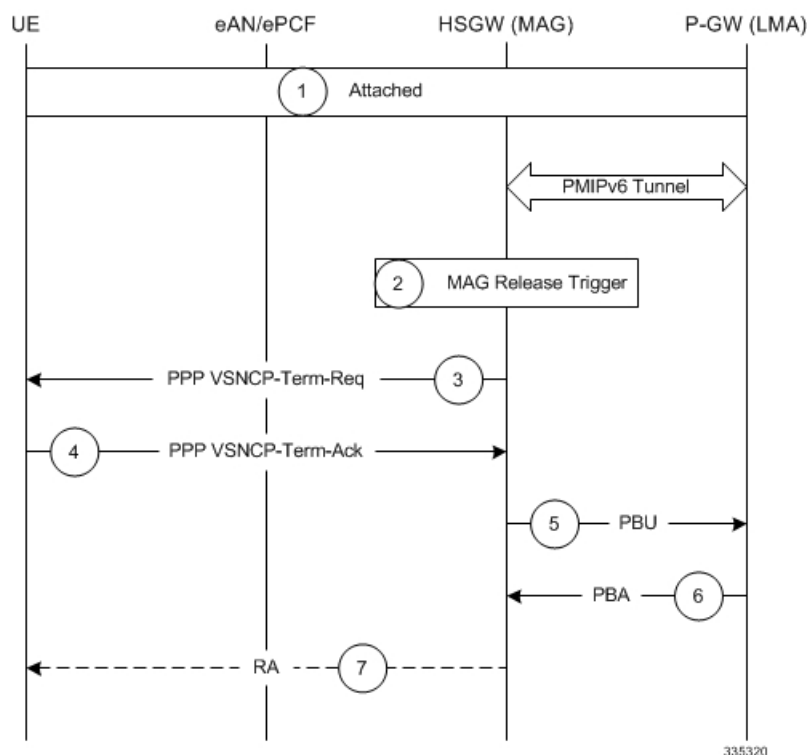
Step	Description
1	The UE is attached to the EPC and has a PDN connection with the P-GW for PDN-ID=x and APN with assigned HNP.
2	The UE decides to disconnect from the PDN and sends a PPP VSNCP-Term-Req with PDNID=x.
3	The HSGW starts disconnecting the PDN connection and sends a PPP-VSNCP-Term-Ack to the UE (also with PDNID=x).
4	The HSGW begins the tear down of the PMIP session by sending a PBU Deregistration to the P-GW with the following attributes: Lifetime=0, MNID, APN, ATT=HRPD, HNP. The PBU Deregistration message should contain all the mobility options that were present in the initial PBU that created the binding.

Step	Description
5	The P-GW looks up the Binding Cache Entry (BCE) based on the HNP, deletes the binding, and responds to the HSGW with a Deregistration PBA with the same attributes (Lifetime=0, MNID, APN, ATT=HRPD, HNP).
6	The HSGW optionally sends a Router Advertisement (RA) with assigned HNP and prefix lifetime=0.

## PDN Connection Release Initiated by HSGW

This section describes the procedure of a session release by the HSGW.

**Figure 40: PDN Connection Release by the HSGW Call Flow**



**Table 17: PDN Connection Release by the HSGW Call Flow Description**

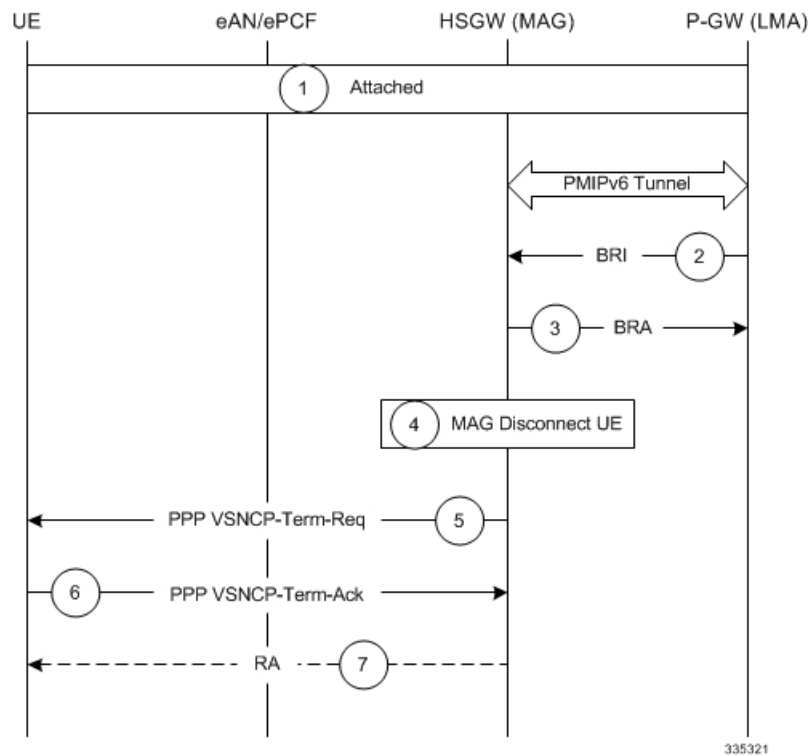
Step	Description
1	The UE is attached to the EPC and has a PDN connection with the P-GW for PDN-ID=x and APN with assigned HNP.
2	The HSGW MAG service triggers a disconnect of the PDN connection for PDNID=x.
3	The HSGW sends a PPP VSNCP-Term-Req with PDNID=x to the UE.
4	The UE acknowledges the receipt of the request with a VSNCP-Term-Ack (PDNID=x).
5	The HSGW begins the tear down of the PMIP session by sending a PBU Deregistration to the P-GW with the following attributes: Lifetime=0, MNID, APN, HNP. The PBU Deregistration message should contain all the mobility options that were present in the initial PBU that created the binding.

Step	Description
6	The P-GW looks up the BCE based on the HNP, deletes the binding, and responds to the HSGW with a Deregistration PBA with the same attributes (Lifetime=0, MNID, APN, ATT=HRPD, HNP).
7	The HSGW optionally sends a Router Advertisement (RA) with assigned HNP and prefix lifetime=0.

## PDN Connection Release Initiated by P-GW

This section describes the procedure of a session release by the P-GW.

**Figure 41: PDN Connection Release by the P-GW Call Flow**



**Table 18: PDN Connection Release by the P-GW Call Flow Description**

Step	Description
1	The UE is attached to the EPC and has a PDN connection with the P-GW for PDN-ID=x and APN with assigned HNP.
2	A PGW trigger causes a disconnect of the PDN connection for PDNID=x and the PGW sends a Binding Revocation Indication (BRI) message to the HSGW with the following attributes: MNID, APN, HNP.
3	The HSGW responds to the BRI message with a Binding Revocation Acknowledgment (BRA) message with the same attributes (MNID, APN, HNP).
4	The HSGW MAG service triggers a disconnect of the UE PDN connection for PDNID=x.
5	The HSGW sends a PPP VSNCP-Term-Req with PDNID=x to the UE.
6	The UE acknowledges the receipt of the request with a VSNCP-Term-Ack (PDNID=x).

Step	Description
7	The HSGW optionally sends a Router Advertisement (RA) with assigned HNP and prefix lifetime=0.

## GTP PDN Gateway Call/Session Procedures in an LTE-SAE Network

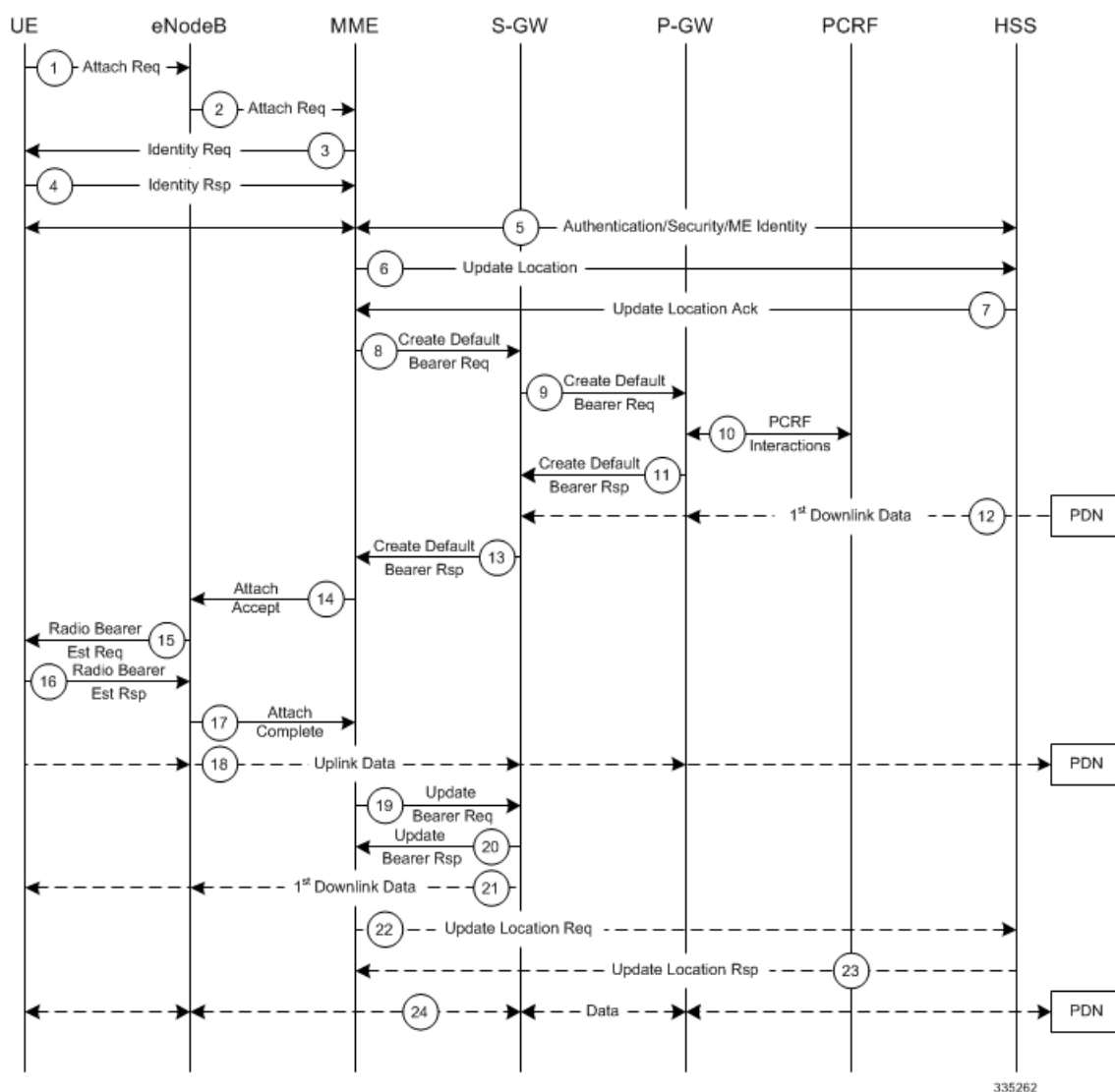
The following topics and procedure flows are included:

- [Subscriber-initiated Attach \(initial\)](#), on page 144
- [Subscriber-initiated Detach](#), on page 146

### Subscriber-initiated Attach (initial)

This section describes the procedure of an initial attach to the EPC network by a subscriber.

**Figure 42: Subscriber-initiated Attach (initial) Call Flow**



335262



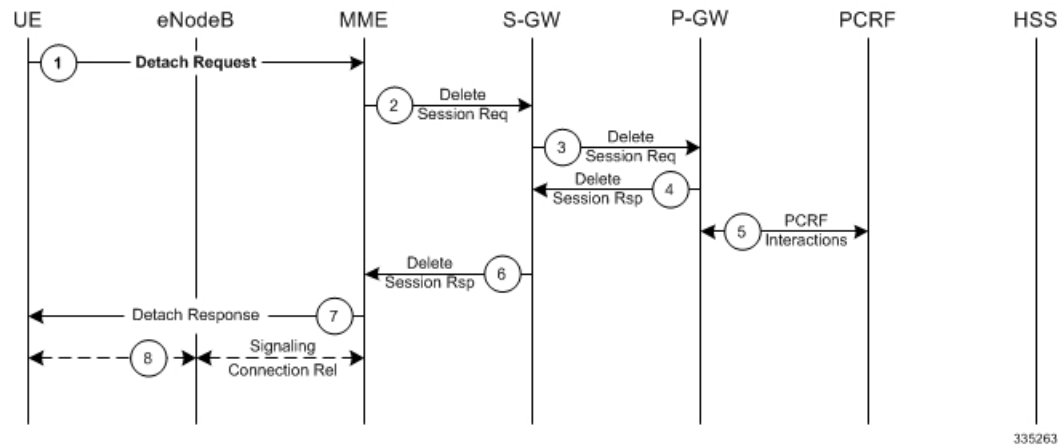
Table 19: Subscriber-initiated Attach (initial) Call Flow Description 44

Step	Description
1	The UE initiates the Attach procedure by the transmission of an Attach Request (IMSI or old GUTI, last visited TAI (if available), UE Network Capability, PDN Address Allocation, Protocol Configuration Options, Attach Type) message together with an indication of the Selected Network to the eNodeB. IMSI is included if the UE does not have a valid GUTI available. If the UE has a valid GUTI, it is included.
2	The eNodeB derives the MME from the GUTI and from the indicated Selected Network. If that MME is not associated with the eNodeB, the eNodeB selects an MME using an "MME selection function". The eNodeB forwards the Attach Request message to the new MME contained in a S1-MME control message (Initial UE message) together with the Selected Network and an indication of the E-UTRAN Area identity, a globally unique E-UTRAN ID of the cell from where it received the message to the new MME.
3	If the UE is unknown in the MME, the MME sends an Identity Request to the UE to request the IMSI.
4	The UE responds with Identity Response (IMSI).
5	If no UE context for the UE exists anywhere in the network, authentication is mandatory. Otherwise this step is optional. However, at least integrity checking is started and the ME Identity is retrieved from the UE at Initial Attach. The authentication functions, if performed this step, involves AKA authentication and establishment of a NAS level security association with the UE in order to protect further NAS protocol messages.
6	The MME sends an Update Location (MME Identity, IMSI, ME Identity) to the HSS.
7	The HSS acknowledges the Update Location message by sending an Update Location Ack to the MME. This message also contains the Insert Subscriber Data (IMSI, Subscription Data) Request. The Subscription Data contains the list of all APNs that the UE is permitted to access, an indication about which of those APNs is the Default APN, and the 'EPS subscribed QoS profile' for each permitted APN. If the Update Location is rejected by the HSS, the MME rejects the Attach Request from the UE with an appropriate cause.
8	The MME selects an S-GW using "Serving GW selection function" and allocates an EPS Bearer Identity for the Default Bearer associated with the UE. If the PDN subscription context contains no P-GW address the MME selects a P-GW as described in clause "PDN GW selection function". Then it sends a Create Default Bearer Request (IMSI, MME Context ID, APN, RAT type, Default Bearer QoS, PDN Address Allocation, AMBR, EPS Bearer Identity, Protocol Configuration Options, ME Identity, User Location Information) message to the selected S-GW.
9	The S-GW creates a new entry in its EPS Bearer table and sends a Create Default Bearer Request (IMSI, APN, S-GW Address for the user plane, S-GW TEID of the user plane, S-GW TEID of the control plane, RAT type, Default Bearer QoS, PDN Address Allocation, AMBR, EPS Bearer Identity, Protocol Configuration Options, ME Identity, User Location Information) message to the P-GW.
10	If dynamic PCC is deployed, the P-GW interacts with the PCRF to get the default PCC rules for the UE. The IMSI, UE IP address, User Location Information, RAT type, AMBR are provided to the PCRF by the P-GW if received by the previous message.

Step	Description
11	The P-GW returns a Create Default Bearer Response (P-GW Address for the user plane, P-GW TEID of the user plane, P-GW TEID of the control plane, PDN Address Information, EPS Bearer Identity, Protocol Configuration Options) message to the S-GW. PDN Address Information is included if the P-GW allocated a PDN address Based on PDN Address Allocation received in the Create Default Bearer Request. PDN Address Information contains an IPv4 address for IPv4 and/or an IPv6 prefix and an Interface Identifier for IPv6. The P-GW takes into account the UE IP version capability indicated in the PDN Address Allocation and the policies of operator when the P-GW allocates the PDN Address Information. Whether the IP address is negotiated by the UE after completion of the Attach procedure, this is indicated in the Create Default Bearer Response.
12	The Downlink (DL) Data can start flowing towards S-GW. The S-GW buffers the data.
13	The S-GW returns a Create Default Bearer Response (PDN Address Information, S-GW address for User Plane, S-GW TEID for User Plane, S-GW Context ID, EPS Bearer Identity, Protocol Configuration Options) message to the new MME. PDN Address Information is included if it was provided by the P-GW.
14	The new MME sends an Attach Accept (APN, GUTI, PDN Address Information, TAI List, EPS Bearer Identity, Session Management Configuration IE, Protocol Configuration Options) message to the eNodeB.
15	The eNodeB sends Radio Bearer Establishment Request including the EPS Radio Bearer Identity to the UE. The Attach Accept message is also sent along to the UE.
16	The UE sends the Radio Bearer Establishment Response to the eNodeB. In this message, the Attach Complete message (EPS Bearer Identity) is included.
17	The eNodeB forwards the Attach Complete (EPS Bearer Identity) message to the MME.
18	The Attach is complete and UE sends data over the default bearer. At this time the UE can send uplink packets towards the eNodeB which are then tunneled to the S-GW and P-GW.
19	The MME sends an Update Bearer Request (eNodeB address, eNodeB TEID) message to the S-GW.
20	The S-GW acknowledges by sending Update Bearer Response (EPS Bearer Identity) message to the MME.
21	The S-GW sends its buffered downlink packets.
22	After the MME receives Update Bearer Response (EPS Bearer Identity) message, if an EPS bearer was established and the subscription data indicates that the user is allowed to perform handover to non-3GPP accesses, and if the MME selected a P-GW that is different from the P-GW address which was indicated by the HSS in the PDN subscription context, the MME sends an Update Location Request including the APN and P-GW address to the HSS for mobility with non-3GPP accesses.
23	The HSS stores the APN and P-GW address pair and sends an Update Location Response to the MME.
24	Bidirectional data is passed between the UE and PDN.

## Subscriber-initiated Detach

This section describes the procedure of detachment from the EPC network by a subscriber.

**Figure 43: Subscriber-initiated Detach Call Flow****Table 20: Subscriber-initiated Detach Call Flow Description**

Step	Description
1	The UE sends NAS message Detach Request (GUTI, Switch Off) to the MME. Switch Off indicates whether detach is due to a switch off situation or not.
2	The active EPS Bearers in the S-GW regarding this particular UE are deactivated by the MME sending a Delete Bearer Request (TEID) message to the S-GW.
3	The S-GW sends a Delete Bearer Request (TEID) message to the P-GW.
4	The P-GW acknowledges with a Delete Bearer Response (TEID) message.
5	The P-GW may interact with the PCRF to indicate to the PCRF that EPS Bearer is released if PCRF is applied in the network.
6	The S-GW acknowledges with a Delete Bearer Response (TEID) message.
7	If Switch Off indicates that the detach is not due to a switch off situation, the MME sends a Detach Accept message to the UE.
8	The MME releases the S1-MME signaling connection for the UE by sending an S1 Release command to the eNodeB with Cause = Detach.

## S-GW Supported Standards

The S-GW service complies with the following standards.

- [3GPP References, on page 148](#)
- [3GPP2 References, on page 150](#)
- [IETF References, on page 150](#)
- [Object Management Group \(OMG\) Standards, on page 151](#)

## 3GPP References

### Release 12 3GPP References



#### Important

The S-GW currently supports the following Release 12 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 are listed under *3GPP2 References*.

- 3GPP TS 23.007: Restoration procedures
- 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) Tunneling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 29.281: General Packet Radio System (GPRS) Tunneling Protocol User Plane (GTPv1-U)

### Release 11 3GPP References



#### Important

The S-GW currently supports the following Release 11 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 are listed under *3GPP2 References*.

- 3GPP TS 23.007: Restoration procedures
- 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) Tunneling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 29.281: General Packet Radio System (GPRS) Tunneling Protocol User Plane (GTPv1-U)
- 3GPP TS 32.423: Telecommunication management; Subscriber and equipment trace; Trace data definition and management.
- 3GPP TS 36.414: Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 data transport

### Release 10 3GPP References



#### Important

The S-GW currently supports the following Release 10 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 are listed under *3GPP2 References*.

- 3GPP TS 23.007: Restoration procedures
- 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 29.281: General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)

## Release 9 Supported Standards

- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 23.060: General Packet Radio Service (GPRS); Service description; Stage 2
- 3GPP TS 23.216: Single Radio Voice Call Continuity (SRVCC); Stage 2 (Release 9)
- 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 (Release 9)
- 3GPP TS 29.281: General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)
- 3GPP TS 33.106: 3G Security; Lawful Interception Requirements
- 3GPP TS 36.414: Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 data transport

## Release 8 Supported Standards

- 3GPP TR 21.905: Vocabulary for 3GPP Specifications
- 3GPP TS 23.003: Numbering, addressing and identification
- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 23.107: Quality of Service (QoS) concept and architecture
- 3GPP TS 23.203: Policy and charging control architecture
- 3GPP TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402: Architecture Enhancements for non-3GPP accesses
- 3GPP TS 23.060: General Packet Radio Service (GPRS); Service description; Stage 2
- 3GPP TS 24.008: Mobile radio interface Layer 3 specification; Core network protocols
- 3GPP TS 24.229: IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3
- 3GPP TS 29.210: Gx application
- 3GPP TS 29.212: Policy and Charging Control over Gx reference point
- 3GPP TS 29.213: Policy and Charging Control signaling flows and QoS
- 3GPP TS 29.214: Policy and Charging Control over Rx reference point
- 3GPP TS 29.274 V8.1.1 (2009-03): 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3 (Release 8)

- 3GPP TS 29.274: Evolved GPRS Tunnelling Protocol for Control plane (GTPv2-C), version 8.2.0 (both versions are intentional)
- 3GPP TS 29.275: Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols, version 8.1.0
- 3GPP TS 29.281: GPRS Tunnelling Protocol User Plane (GTPv1-U)
- 3GPP TS 32.251: Telecommunication management; Charging management; Packet Switched (PS) domain charging
- 3GPP TS 32.295: Charging management; Charging Data Record (CDR) transfer
- 3GPP TS 32.298: Telecommunication management; Charging management; Charging Data Record (CDR) encoding rules description
- 3GPP TS 32.299: Charging management; Diameter charging applications
- 3GPP TS 33.106: 3G Security; Lawful Interception Requirements
- 3GPP TS 36.107: 3G security; Lawful interception architecture and functions
- 3GPP TS 36.300: Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description
- 3GPP TS 36.412: EUTRAN S1 signaling transport
- 3GPP TS 36.413: Evolved Universal Terrestrial Radio Access (E-UTRA); S1 Application Protocol (S1AP)
- 3GPP TS 36.414: Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 data transport

## 3GPP2 References

- X.P0057-0 v0.11.0 E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects

## IETF References

- RFC 768: User Datagram Protocol (STD 6).
- RFC 791: Internet Protocol (STD 5).
- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2460: Internet Protocol, Version 6 (IPv6) Specification
- RFC 2698: A Two Rate Three Color Marker
- RFC 2784: Generic Routing Encapsulation (GRE)
- RFC 2890: Key and Sequence Number Extensions to GRE
- RFC 3319: Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers
- RFC 3588: Diameter Base Protocol
- RFC 3775: Mobility Support in IPv6

- RFC 3646: DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 4006: Diameter Credit-Control Application
- RFC 4282: The Network Access Identifier
- RFC 4283: Mobile Node Identifier Option for Mobile IPv6 (MIPv6)
- RFC 4861: Neighbor Discovery for IP Version 6 (IPv6)
- RFC 4862: IPv6 Stateless Address Autoconfiguration
- RFC 5094: Mobile IPv6 Vendor Specific Option
- RFC 5213: Proxy Mobile IPv6
- Internet-Draft: Proxy Mobile IPv6
- Internet-Draft: GRE Key Option for Proxy Mobile IPv6, work in progress
- Internet-Draft: Binding Revocation for IPv6 Mobility, work in progress

## Object Management Group (OMG) Standards

- CORBA 2.6 Specification 01-09-35, Object Management Group

## P-GW Supported Standards

The P-GW service complies with the following standards.

- [Release 12 3GPP References, on page 151](#)
- [Release 11 3GPP References, on page 152](#)
- [Release 10 3GPP References, on page 152](#)
- [Release 9 3GPP References, on page 153](#)
- [Release 8 3GPP References, on page 154](#)
- [3GPP2 References, on page 155](#)
- [IETF References, on page 155](#)
- [Object Management Group \(OMG\) Standards, on page 156](#)

## Release 12 3GPP References



### Important

The P-GW currently supports the following Release 12 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 are listed under *3GPP2 References*.

- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402: Architecture enhancements for non-3GPP accesses

- 3GPP TS 29.060: General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface
- 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 29.281: General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)

## Release 11 3GPP References



### Important

The P-GW currently supports the following Release 11 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 are listed under *3GPP2 References*.

- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C)
- 3GPP TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402: Architecture enhancements for non-3GPP accesses
- 3GPP TS 29.060: General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface
- 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 29.281: General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)

## Release 10 3GPP References



### Important

The P-GW currently supports the following Release 10 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 are listed under *3GPP2 References*.

- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 23.203: Policy and charging control architecture; Stage 2
- 3GPP TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402: Architecture enhancements for non-3GPP accesses
- 3GPP TS 29.212: Policy and Charging Control over Gx reference point
- 3GPP TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C)
- 3GPP TS 29.281: GPRS Tunnelling Protocol User Plane (GTPv1-U)



## Release 9 3GPP References

**Important**

The P-GW currently supports the following Release 9 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 are listed under *3GPP2 References*.

- 3GPP TR 21.905: Vocabulary for 3GPP Specifications
- 3GPP TS 22.115: Service aspects; Charging and billing
- 3GPP TS 23.003: Numbering, addressing and identification
- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 23.060: General Packet Radio Service (GPRS); Service description; Stage 2
- 3GPP TS 23.203: Policy and charging control architecture
- 3GPP TS 23.207: End-to-end Quality of Service (QoS) concept and architecture
- 3GPP TS 23.216: Single Radio Voice Call Continuity (SRVCC); Stage 2
- 3GPP TS 23.228: IP Multimedia Subsystem (IMS); Stage 2
- 3GPP TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402: Architecture enhancements for non-3GPP accesses
- 3GPP TS 24.008: Mobile radio interface Layer 3 specification; Core network protocols
- 3GPP TS 29.060: General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface
- 3GPP TS 29.061: Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)
- 3GPP TS 29.212: Policy and Charging Control over Gx reference point
- 3GPP TS 29.214: Policy and Charging control over Rx reference point
- 3GPP TS 29.229: Cx and Dx interfaces based on Diameter protocol
- 3GPP TS 29.230: Diameter applications; 3GPP specific codes and identifiers
- 3GPP TS 29.272: Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol
- 3GPP TS 29.273: 3GPP EPS AAA Interfaces
- 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 29.275: Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols; Stage 3
- 3GPP TS 29.281: General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)
- 3GPP TS 29.282: Mobile IPv6 vendor specific option format and usage within 3GPP

- 3GPP TS 32.240: Telecommunication management; Charging management; Charging architecture and principles
- 3GPP TS 32.251: Telecommunication management; Charging management; Packet Switched (PS) domain charging
- 3GPP TS 32.298: Telecommunication management; Charging management; Charging Data Record (CDR) parameter description
- 3GPP TS 32.299: Telecommunication management; Charging management; Diameter charging application

## Release 8 3GPP References



### Important

The P-GW currently supports the following Release 8 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 are listed under *3GPP2 References*.

- 3GPP TR 21.905: Vocabulary for 3GPP Specifications
- 3GPP TS 23.003: Numbering, addressing and identification
- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 23.060: General Packet Radio Service (GPRS); Service description; Stage 2
- 3GPP TS 23.107: Quality of Service (QoS) concept and architecture
- 3GPP TS 23.203: Policy and charging control architecture
- 3GPP TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402: Architecture enhancements for non-3GPP accesses
- 3GPP TS 23.869: Support for Internet Protocol (IP) based IP Multimedia Subsystem (IMS) Emergency calls over General Packet Radio Service (GPRS) and Evolved Packet Service (EPS)
- 3GPP TS 24.008: Mobile radio interface Layer 3 specification; Core network protocols
- 3GPP TS 24.229: IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3
- 3GPP TS 27.060: Mobile Station (MS) supporting Packet Switched Services
- 3GPP TS 29.061: Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)
- 3GPP TS 29.210: Charging rule provisioning over Gx interface
- 3GPP TS 29.212: Policy and Charging Control over Gx reference point
- 3GPP TS 29.213: Policy and Charging Control signaling flows and QoS
- 3GPP TS 29.273: 3GPP EPS AAA Interfaces
- 3GPP TS 29.274: Evolved GPRS Tunnelling Protocol for Control plane (GTPv2-C)
- 3GPP TS 29.275: Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols

- 3GPP TS 29.281: GPRS Tunnelling Protocol User Plane (GTPv1-U)
- 3GPP TS 29.282: Mobile IPv6 vendor specific option format and usage within 3GPP
- 3GPP TS 32.295: Charging management; Charging Data Record (CDR) transfer
- 3GPP TS 32.298: Telecommunication management; Charging management; Charging Data Record (CDR) encoding rules description
- 3GPP TS 32.299: Charging management; Diameter charging applications
- 3GPP TS 36.300. EUTRA and EUTRAN; Overall description Stage 2
- 3GPP TS 36.412. EUTRAN S1 signaling transport
- 3GPP TS 36.413. EUTRAN S1 Application Protocol (S1AP)

## 3GPP2 References

- X.S0057-0 v3.0 E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects

## IETF References

- RFC 768: User Datagram Protocol (STD 6).
- RFC 791: Internet Protocol (STD 5).
- RFC 1701, Generic Routing Encapsulation (GRE)
- RFC 1702, Generic Routing Encapsulation over IPv4 networks
- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2460: Internet Protocol, Version 6 (IPv6) Specification
- RFC 2473: Generic Packet Tunneling in IPv6 Specification
- RFC 2698: A Two Rate Three Color Marker
- RFC 2784: Generic Routing Encapsulation (GRE)
- RFC 2890: Key and Sequence Number Extensions to GRE
- RFC 3162: RADIUS and IPv6
- RFC 3266: Support for IPv6 in Session Description Protocol (SDP)
- RFC 3319: Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers
- RFC 3588: Diameter Base Protocol
- RFC 3589: Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5
- RFC 3646: DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 3775: Mobility Support in IPv6

- RFC 4004: Diameter Mobile IPv4 Application
- RFC 4005: Diameter Network Access Server Application
- RFC 4006: Diameter Credit-Control Application
- RFC 4282: The Network Access Identifier
- RFC 4283: Mobile Node Identifier Option for Mobile IPv6 (MIPv6)
- RFC 4861: Neighbor Discovery for IP Version 6 (IPv6)
- RFC 4862: IPv6 Stateless Address Autoconfiguration
- RFC 5094: Mobile IPv6 Vendor Specific Option
- RFC 5149: Service Selection for Mobile IPv6
- RFC 5213: Proxy Mobile IPv6
- RFC 5447: Diameter Mobile IPv6: Support for NAS to Diameter Server Interaction
- RFC 5555: Mobile IPv6 Support for Dual Stack Hosts and Routers
- RFC 5844: IPv4 Support for Proxy Mobile IPv6
- RFC 5845: Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6
- RFC 5846: Binding Revocation for IPv6 Mobility
- Internet-Draft (draft-ietf-dime-qos-attributes-07): QoS Attributes for Diameter
- Internet-Draft (draft-ietf-mip6-nemo-v4traversal-06.txt): Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)
- Internet-Draft (draft-ietf-netlmm-grekey-option-01.txt): GRE Key Option for Proxy Mobile IPv6, work in progress
- Internet-Draft (draft-ietf-netlmm-pmip6-ipv4-support-02.txt) IPv4 Support for Proxy Mobile IPv6
- Internet-Draft (draft-ietf-netlmm-proxymip6-07.txt): Proxy Mobile IPv6
- Internet-Draft (draft-ietf-mext-binding-revocation-02.txt): Binding Revocation for IPv6 Mobility, work in progress
- Internet-Draft (draft-meghana-netlmm-pmip6-mip4-00.txt) Proxy Mobile IPv6 and Mobile IPv4 interworking

## Object Management Group (OMG) Standards

- CORBA 2.6 Specification 01-09-35, Object Management Group