PDN Gateway Overview

The Cisco® Packet Data Network (PDN) Gateway (P-GW) is a critical network function for the 4G mobile core network, known as the evolved packet core (EPC). The P-GW acts as the interface between the 3GPP2 Long Term Evolution-System Architecture Evolution (LTE-SAE) network and other packet data networks, such as the Internet, SIP-based IP Multimedia Subsystem (IMS) networks, and evolved High Rate Packet Data (eHRPD) wireless data networks.

This overview provides general information about the P-GW including:

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

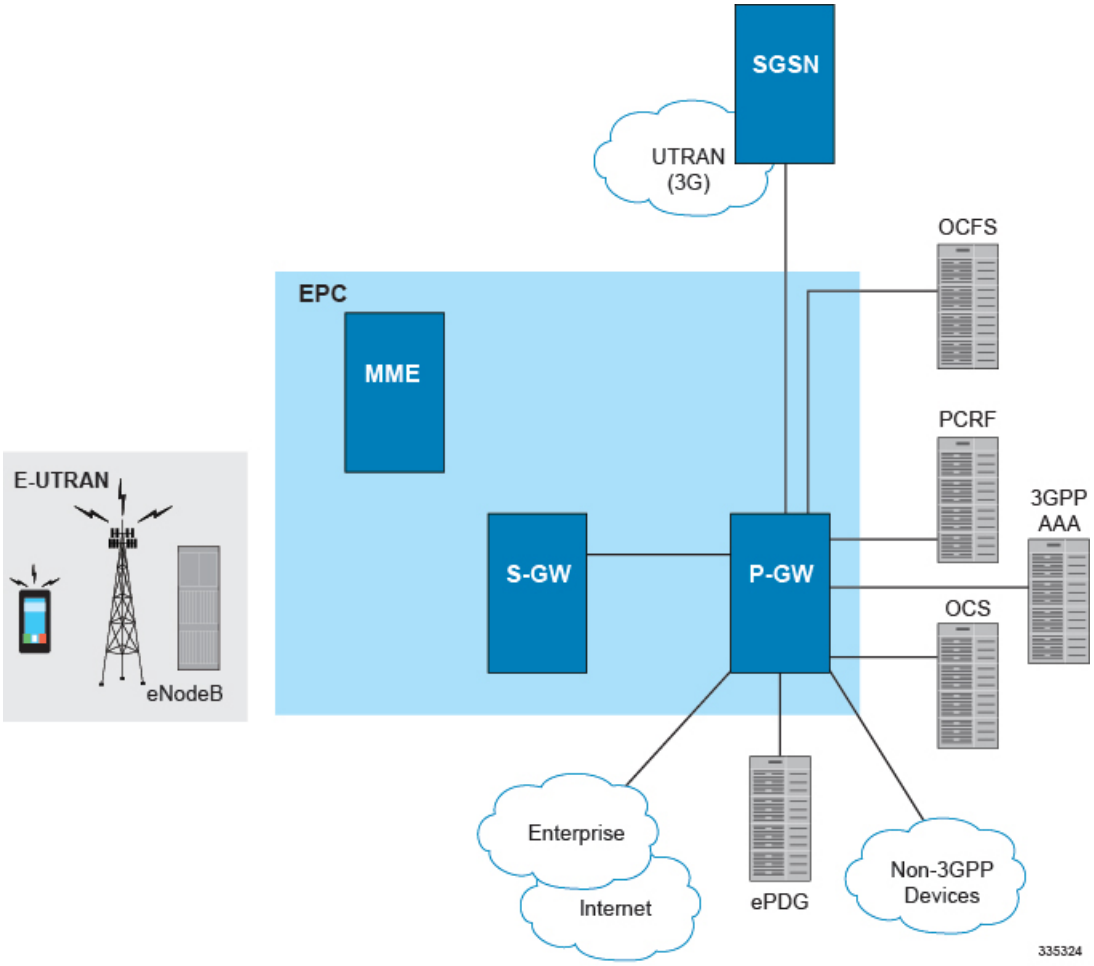
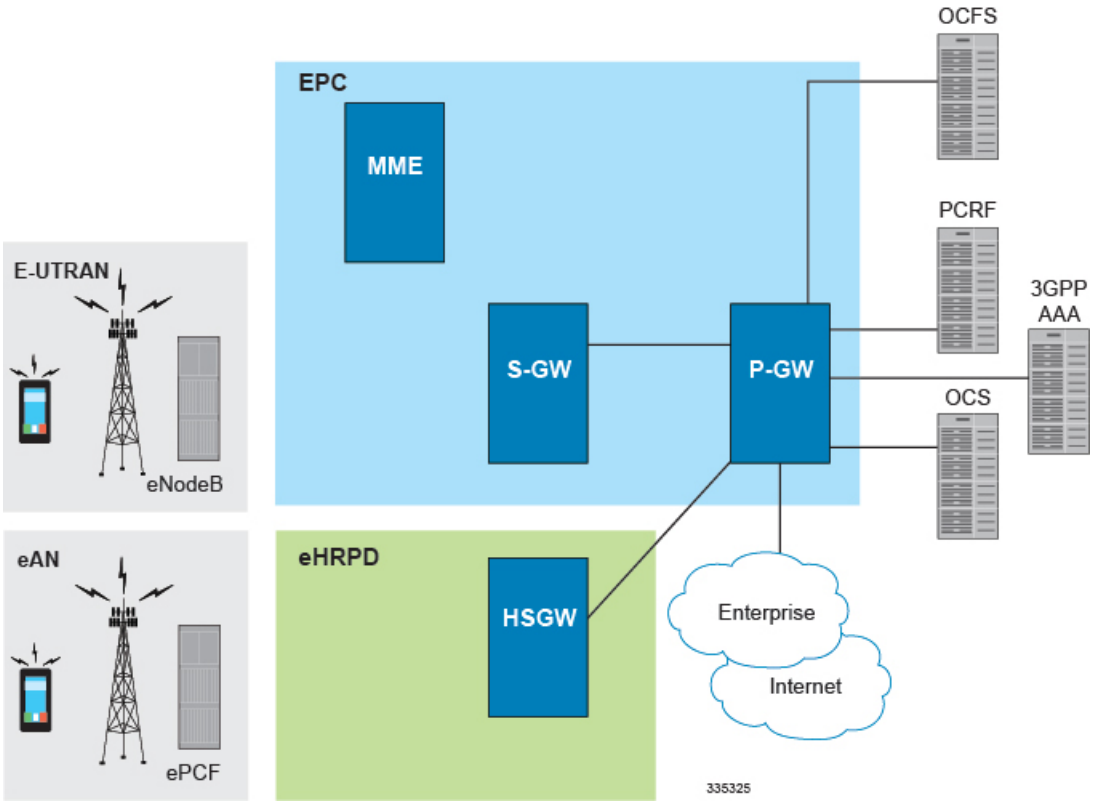


Figure 2: P-GW in the Basic E-UTRAN/EPC and eHRPD Network



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.

Qualified Platforms

P-GW is a StarOS application that runs on Cisco ASR 5500 and virtualized platforms. For additional platform information, refer to the appropriate *System Administration Guide* and/or contact your Cisco account representative.

Licenses

The P-GW 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*.

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - License Required
Related Changes in This Release	Not Applicable
Related Documentation	• *P-GW Administration Guide*

Revision History

Revision Details	Release
In this release, the S6b interface is enhanced to align with the 3GPP AAA with the allocation of static and dynamic through AVP.	21.22

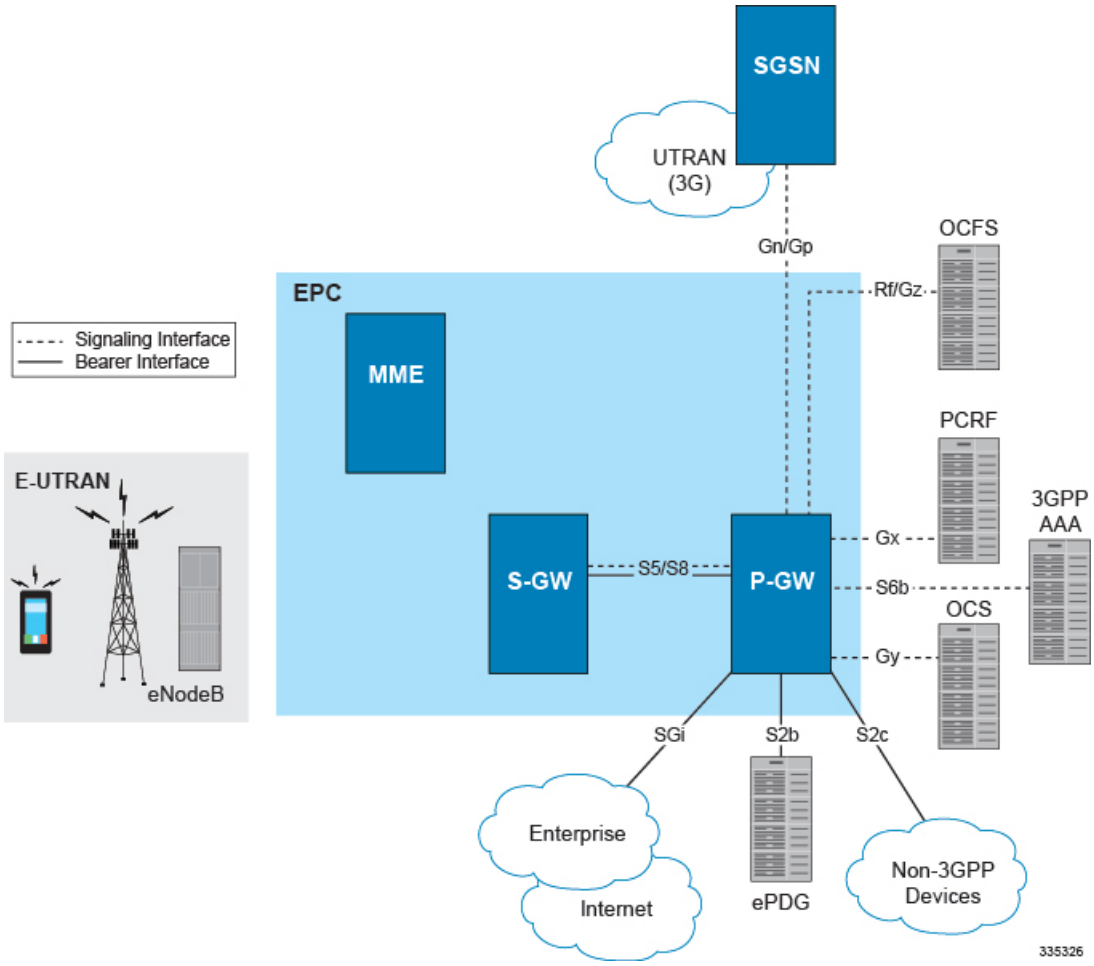
Network Deployment(s)

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

PDN Gateway in the E-UTRAN/EPC Network

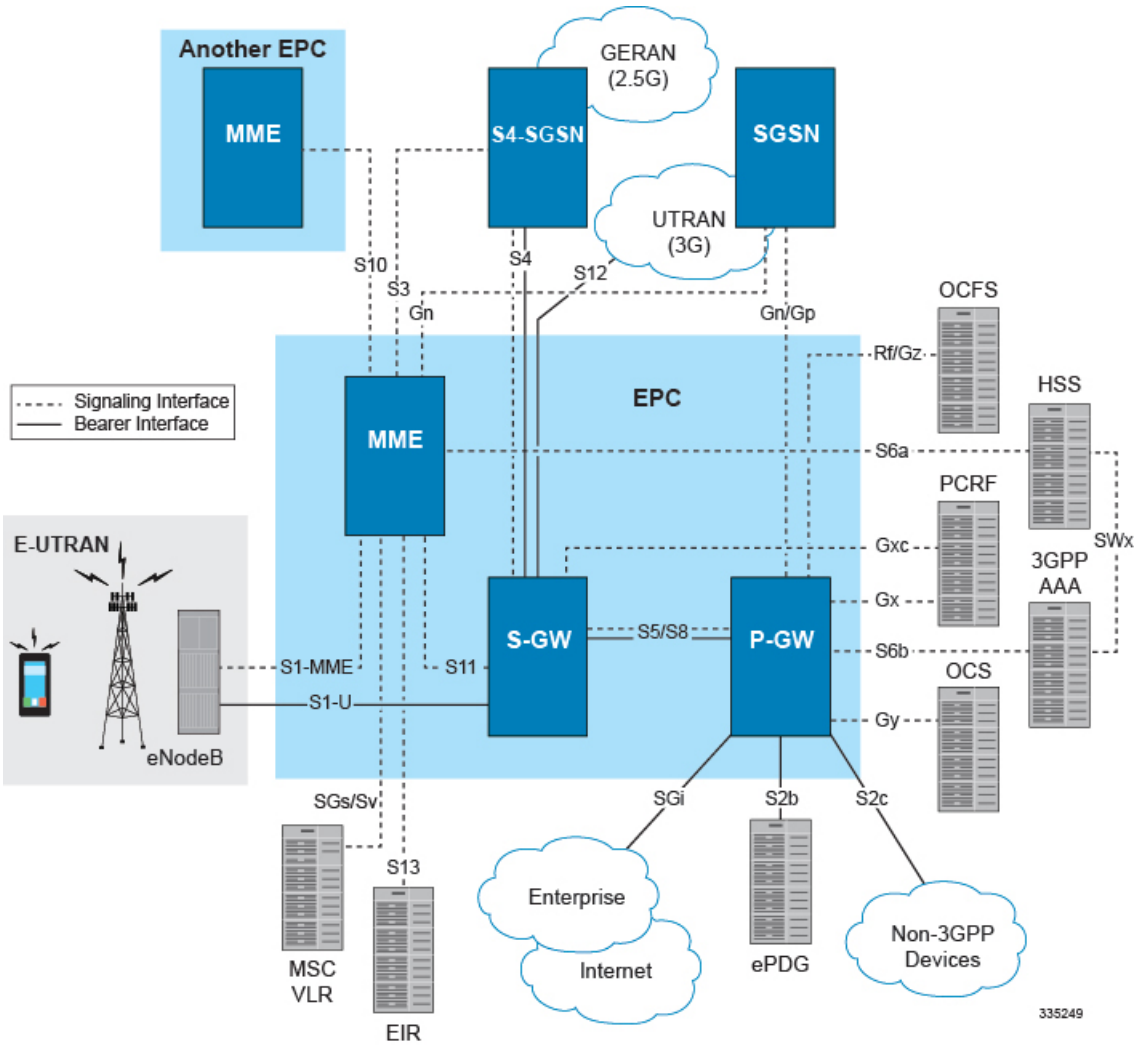
The following figure displays the specific network interfaces supported by the P-GW. Refer to Supported Logical Network Interfaces (Reference Points), on page 14 for detailed information about each interface.

Figure 3: 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 4: 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:

S2b Interface

The S2b interface reference point defined between the non-trusted non-3GPP ePDG (Evolved Packet Data Gateway) and the P-GW uses PMIPv6 (Proxy Mobile IP version 6) for providing access to the EPC. GTPv2-C is the signaling protocol used on the S2b. The S2b interface is based on 3GPP TS 29.274.

The S2b interface runs PMIPv6 protocol to establish WLAN UE sessions with the P-GW. It also supports the transport of P-CSCF attributes and DNS attributes in PBU (Proxy-MIP Binding Update) and PBA (Proxy-MIP Binding Acknowledgement) messages as part of the P-CSCF discovery performed by the WLAN UEs.

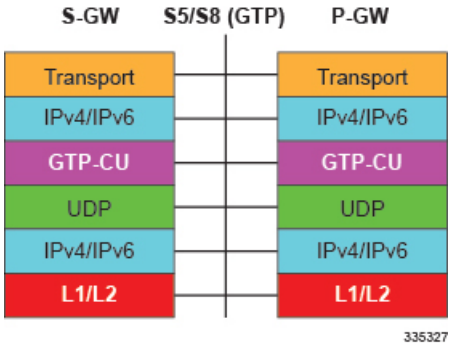
When the P-CSCF Address information is missing, P-CSCF Discovery is initiated upon S4-SGSN to LTE (and vice versa) handoff.If the P-CSCF Address information is already available, there is no need to explicitly trigger another P-CSCF Discovery upon S4-SGSN to LTE (and vice versa) handoff.

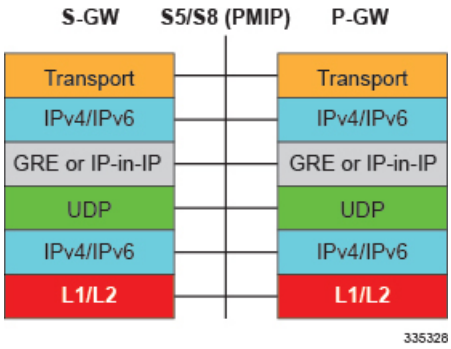
S5/S8 Interface

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)
  - PMIPv6: GRE or IP-in-IP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet





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.

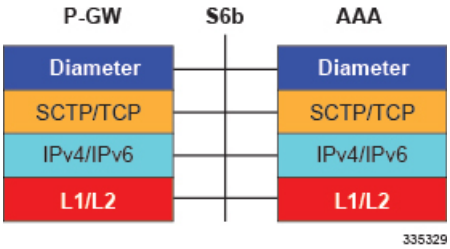
Another enhancement on S6b interface support is the new S6b retry-and-continue functionality that creates an automatic trigger in the GGSN and P-GW to use the locally configured APN profile upon receipt of any uniquely defined Diameter error code on the S6b interface for an Authorization-Authentication-Request (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.

StarOS Release 17 and onwards, 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



Enhancement for S6b Interface Update

In the StarOS 21.22 and the later releases, the S6b interface is enhanced to align with the 3GPP AAA with the allocation of static and dynamic through the following AVP:

- **Class AVP**

- **User-Name AVP**
- **Origination-Time-Stamp AVP**

Class AVP: The following enhancement is supported:

During the initial PDN connection request, PGW/GGSN receives the CLASS AVP, if available, in the AA Answer message from 3GPP AAA. Then, PGW/GGSN sends Answer to 3GPP AAA. While sending AA_request message to 3GPP AA, PGW/GGSN drops the CLASS AVP. PGW/GGSN has the option to initiate re-authorization. However, if PGW/GGSN has previously received the CLASS AVP from 3GPP AAA, it includes Class AVP in subsequent session termination requests but not re-authorization requests. It results in removal of Class AVP from all messages except AA Answer and Session-Termination messages (STR and STA messages).

If Auth-Session-State is negotiated as STATE_MAINTAINED, then on session termination, PGW initiates a Session-Termination-Request {Session-Id, Origin-Host, Origin-Realm, Destination-Realm, Auth-Application-Id=(16777999), Destination-Host, Termination-Cause, User-Name } to the 3GPP AAA.

Note The Class AVP can only be removed from the instances wherever `aaa-custom15` dictionary is used.

User-Name AVP: The following enhancement is supported.

When PGW/GGSN sends subsequent session termination (STR) requests to 3GPP AAA, it includes the mandatory parameter, **User-Name AVP**.

Note During backward compatibility, 3GPP AAA accepts STR without **User-Name AVP**.

Ensure that the User-Name doesn't include prefix.

For Example:

```
<IMSI>@nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org.
```

Origination-Time-Stamp AVP: The following enhancement is supported.

The **Origination-TimeStamp AVP** is replaced with the 3GPP standard Origination-Time-Stamp AVP.

Maximum-Wait-Time AVP: The following enhancement is supported.

The **Max-Wait-Time AVP** is replaced with 3GPP standard Maximum-Wait-Time AVP **Maximum-Wait-Time AVP**.

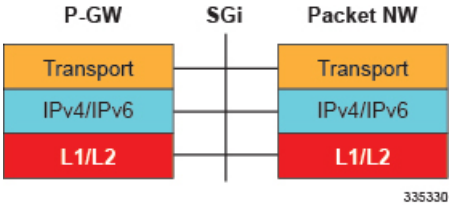
SGi Interface

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

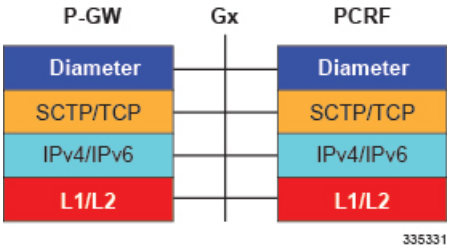


Gx Interface

This signalling 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



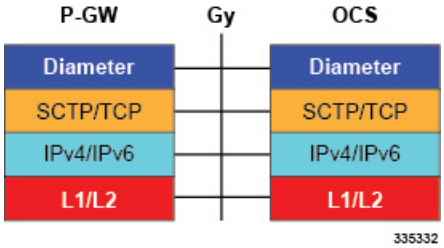
For more information on the Gx interface, refer to Dynamic Policy Charging Control (Gx Reference Interface), on page 32.

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



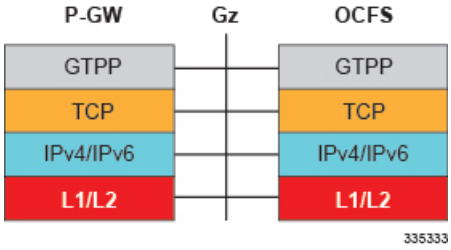
For more information on the Gy interface and online accounting, refer to Gy Interface Support, on page 38.

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

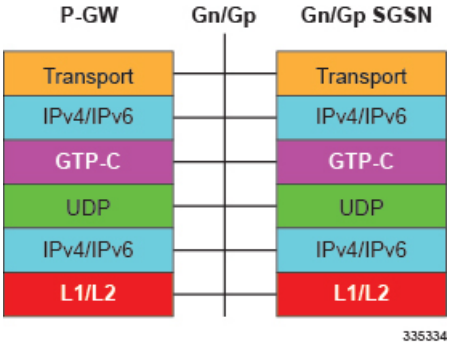


Gn/Gp Interface

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 39.

Supported protocols

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

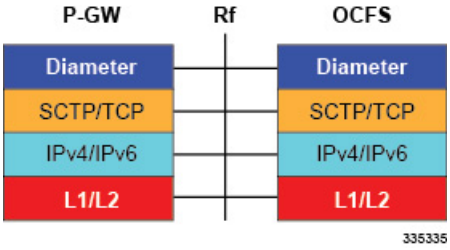


Rf Interface

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:

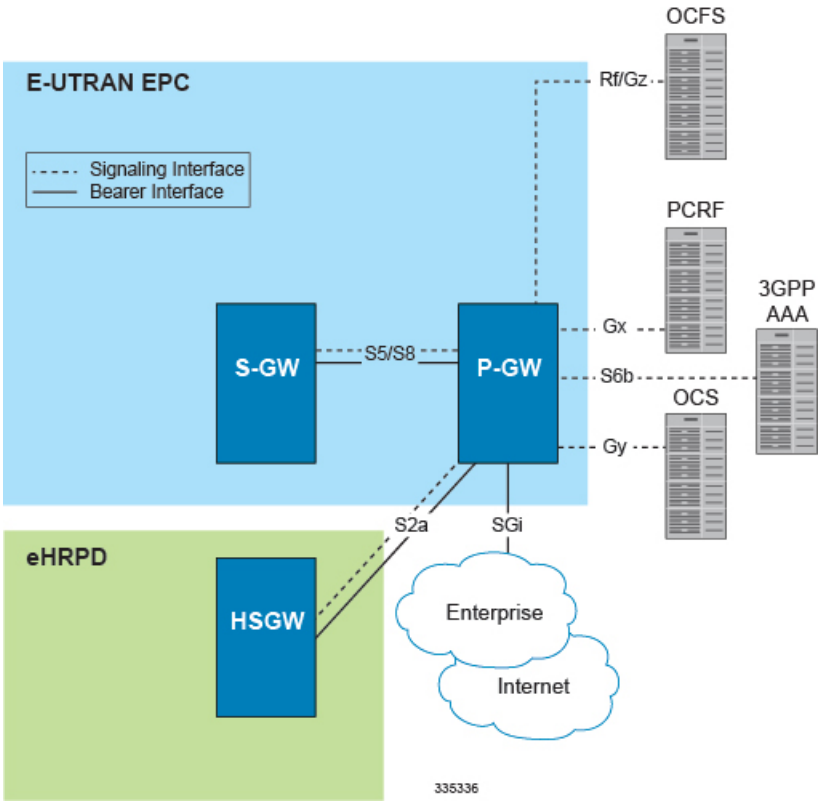
- Transport Layer: TCP, SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



PDN Gateway Supporting eHRPD to E-UTRAN/EPC Connectivity

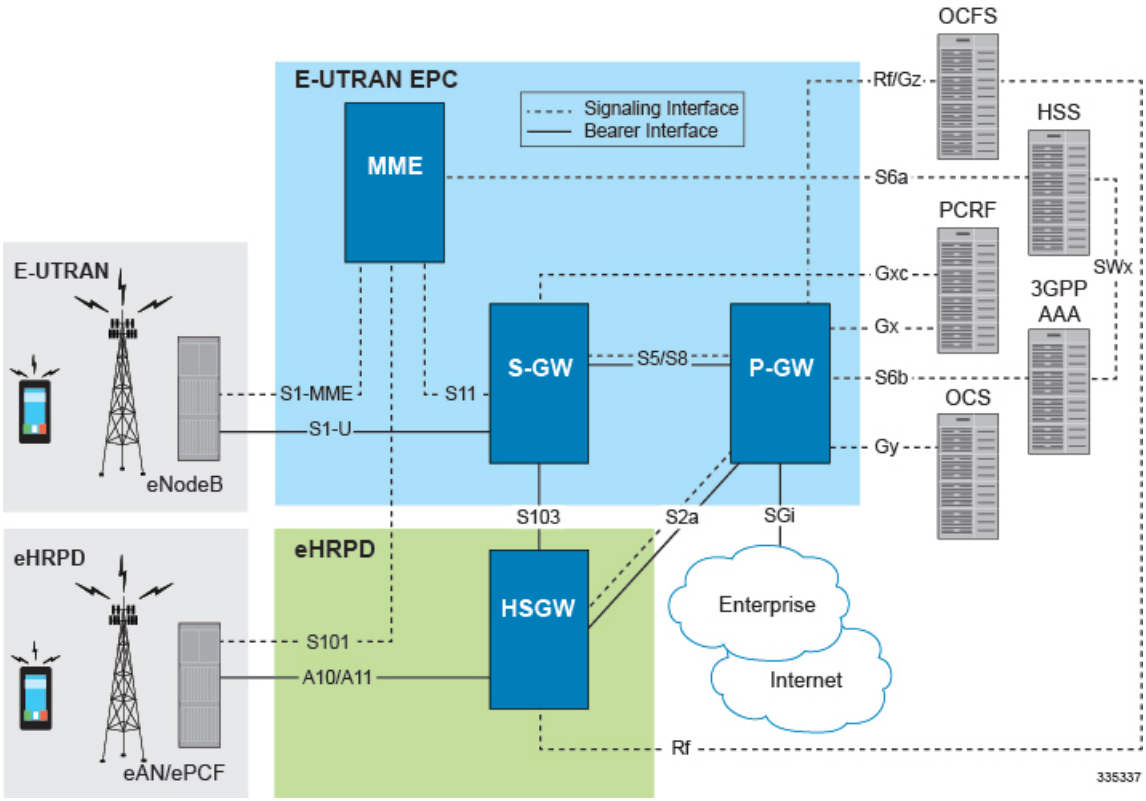
The following figure displays the specific network interfaces supported by the P-GW in an eHRPD network. Refer to Supported Logical Network Interfaces (Reference Points), on page 6 for detailed information about each interface.

Figure 5: 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 6: 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:

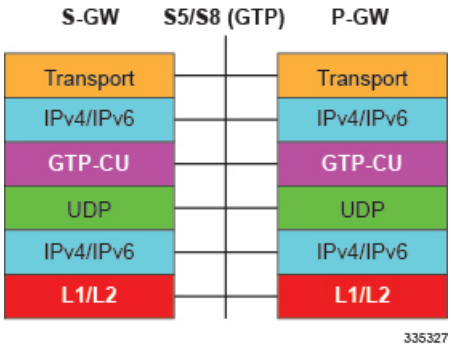
S5/S8 Interface

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)
  - PMIPv6: IPv6 GRE or IP-in-IP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP

- Physical Layer: Ethernet

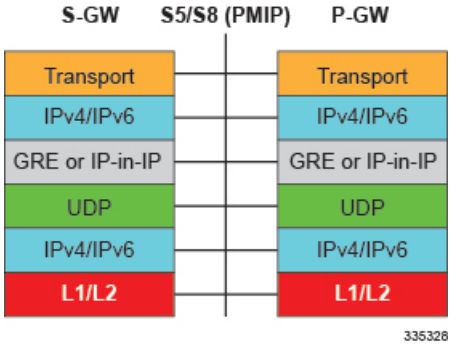


S2a Interface

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



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

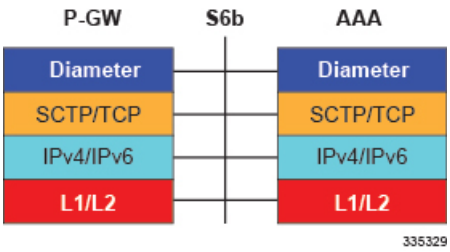
Release 12.3 onwards, the IPv6 address reporting through Authorization-Authentication-Request (AAR) towards the S6b interface is no longer a default feature. It is now configurable through the CLI.

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



Enhancement for S6b Interface Update

In the StarOS 21.22 and the later releases, the S6b interface is enhanced to align with the 3GPP AAA with the allocation of static and dynamic through the following AVP:

- **Class AVP**
- **User-Name AVP**
- **Origination-Time-Stamp AVP**

Class AVP: The following enhancement is supported:

During the initial PDN connection request, PGW/GGSN receives the CLASS AVP, if available, in the AA Answer message from 3GPP AAA. Then, PGW/GGSN sends Answer to 3GPP AAA. While sending AA_request message to 3GPP AA, PGW/GGSN drops the CLASS AVP. PGW/GGSN has the option to initiate re-authorization. However, if PGW/GGSN has previously received the CLASS AVP from 3GPP AAA, it includes Class AVP in subsequent session termination requests but not re-authorization requests. It results in removal of Class AVP from all messages except AA Answer and Session-Termination messages (STR and STA messages).

If Auth-Session-State is negotiated as STATE_MAINTAINED, then on session termination, PGW initiates a Session-Termination-Request {Session-Id, Origin-Host, Origin-Realm, Destination-Realm, Auth-Application-Id=(16777999), Destination-Host, Termination-Cause, User-Name } to the 3GPP AAA.

Note The Class AVP can only be removed from the instances wherever `aaa-custom15` dictionary is used.

User-Name AVP: The following enhancement is supported.

When PGW/GGSN sends subsequent session termination (STR) requests to 3GPP AAA, it includes the mandatory parameter, **User-Name AVP**.

Note During backward compatibility, 3GPP AAA accepts STR without **User-Name AVP**.

Ensure that the User-Name doesn't include prefix.

For Example:

```
<IMSI>@nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org.
```

Origination-Time-Stamp AVP: The following enhancement is supported.

The **Origination-TimeStamp AVP** is replaced with the 3GPP standard Origination-Time-Stamp AVP.

Maximum-Wait-Time AVP: The following enhancement is supported.

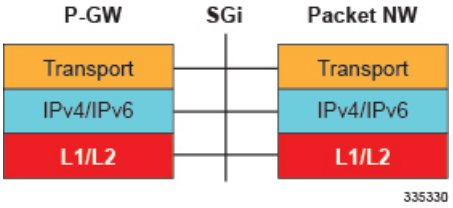
The **Max-Wait-Time AVP** is replaced with 3GPP standard Maximum-Wait-Time AVP **Maximum-Wait-Time AVP**.

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

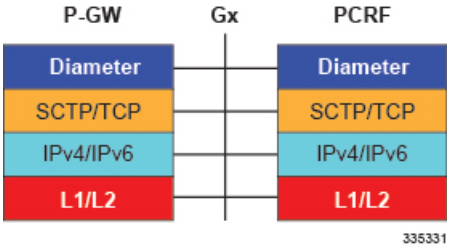


Gx Interface

This signalling 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



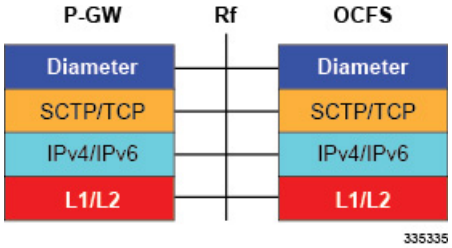
For more information on the Gx interface, refer to Dynamic Policy Charging Control (Gx Reference Interface), on page 32.

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



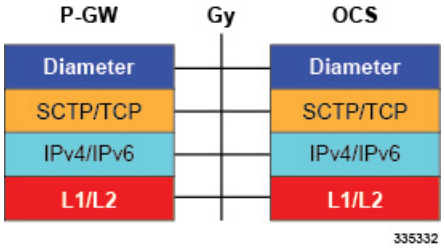
For more information on Rf accounting, refer to Features and Functionality - Base Software, on page 19.

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



For more information on the Gy interface and online accounting, refer to Gy Interface Support, on page 38.

Features and Functionality - Base Software

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.

3GPP Release 12 Cause Code IE Support

When an E-RAB or a data session is dropped, an operator may need to get detailed RAN and/or NAS release cause code information as well as ULI information from the access network to be included in P-GW and S-GW CDRs for call performance analysis, user QoE analysis and proper billing reconciliation. The operator may also need to retrieve the above information at the P-CSCF for IMS sessions.

"Per E-RAB Cause" was received in a E-RAB Release command and a E-RAB Release Indication messages over S1. However RAN and NAS causes were not forwarded to the P-GW and the S-GW and they were not provided by the P-GW to the PCRF.

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 is signaling towards the 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.

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.

Important As AAA applications do not support the indirectly connected hosts, configure only the directly connected host.

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.

Important For more information on APN configuration, refer to the *PDN Gateway Configuration* chapter this guide.

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.

Asynchronous Core Transfer Support for egtpinmgr

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

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

Support for Asynchronous Core Transfer has been added to include the egtpinmgr during the recovery process. Now, recovery begins when the egtpinmgr process crashes without waiting for the kernel to complete a core

dump file transfer and release its resources. As a result, the outage time during an egtpinmgr restart is equal to the egtpinmgr recovery time only.

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

Availability of SSID Information in Gx, Gy, Gz, and LI Interface

On the S2a interface P-GW receives the identity of the Wifi access point in the TWAN-IDENTIFIER attribute in the CREATE SESSION REQUEST message. This information consists of AP MAC address, SSID, and CIVIC Address (which may contain information like AP Group name).

For location tracking and location based policy purpose, the above information needs to be propagated to the Policy Server (Gx), Quota Server(Gy), Charging Gateway(Gz) and LI Server. This new feature enhances the P-GW to propagate the AP SSID, BSSID and Civic Address on all these interfaces whenever received on the S2a interface.

Gx Interface

On the Gx interface this information is sent to PCRF in CCR-I/CCR-U and CCR-T messages in TWAN IDENTIFIER attribute. The standard Gx dictionary configuration is sufficient for this.

Gy Interface

On the Gy interface this information is sent to quota server in CCR-I/CCR-U and CCR-T messages in a Cisco Vendor specific attribute named "Civic-Addr" whenever dcca_custom33 dictionary is configured for this interface.

Gz Interface

On the Gz interface this information is sent to charging gateway in the CDR (Charging Data Records) in TWANUserLocationInformation attribute whenever custom53 dictionary is configured on this interface.

LI Interface

On the LI interface the information is sent to the LI server in the IRI events in "twan_identifier" field. No specific dictionary change is needed for this.

Important The PGW receives this SSID/BSSID/Civic Address information on s2a interface from a Trusted WLAN network (via SaMOG). If Cisco SaMOG is used then the functionality of sending this information from SaMOG to PGW can be controlled via a configuration (refer the SaMOG functionality for this). This feature will lead to 3-4% increase in baseline AAAmgr memory usage.

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.

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 kpbs) 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 kpbs.

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

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
- **eGTP-C**: 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*.

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 and later, 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.

Important The P-GW supports 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 signalled 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 signalling, 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 know 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 >= 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

Important For more information on DHCPv6 service configuration, refer to the *DHCPv6 Configuration* section of the *PDN Gateway Configuration* chapter.

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 signalling 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 anIPv4 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 1: Default DSCP Value Matrix

Allocation Priority	1	2	3
Traffic Handling Priority			
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

Operators can perform DSCP marking on gateways such as P-GW, SAE-GW and GGSN, 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 P-GW does not support non-standard QCI values unless a valid license key is installed.

QCI values 1 through 9 are standard values defined in 3GPP TS 23.203; the P-GW supports these standard values.

From 3GPP Release 8 onwards, operator-specific/non-standard QCIs can be supported and carriers can define QCI 128- 254. For more information, see Non-standard QCI Support, on page 87.

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 35
- Content Service Steering, on page 36
- Support for Multiple Detail Record Types, on page 36
- Diameter Credit Control Application, on page 37
- Accept TCP Connections from DCCA Server, on page 37
- Gy Interface Support, on page 38

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 Support for Multiple Detail Record Types, on page 36 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 37*Diameter Credit Control Application* 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 *ECS 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".

Important In release 20.0 and higher Trusted StarOS builds, the FTP option is no longer available.

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 *ECS 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 *ECS 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 *ECS 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.

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 Interface, on page 11.

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.

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 and IPv4 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/IPv4 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 mobility packets wrapped with UDP and IPv4 headers.
- Support for native IPv6/IPv4 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.
- Support for downlink IPv4 data packets received from the SGi forwarded/redirected to a configured next-hop address if the subscriber session does not exist in the P-GW. If the next-hop is not ARP resolvable, then the packet will be dropped. The appropriate interface stats will be updated with the packets forward/dropped counts.

Important The **unconnected-address next-system** *ip address* keyword must be enabled to support the downlink IPv4 data packets forwarding/redirection.

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. Prior to StarOS release 20.0, the Cisco P-GW did not support the IPv6 MTU option in RA messages. In StarOS release 20.0 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

Prior to StarOS release 20.0, 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.

With StarOS release 20.0, 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.

LTE Video Calling

In a Voice over LTE (VoLTE) scenario, the P-GW provides support for LTE Video Calling (LVC). No additional configuration is required to support this functionality.

The P-GW checks the data usage quota for a subscriber at video call setup and periodically during an active video call. The following functionality applies to post paid subscribers with data usage control:

Quota Check - Call Setup

If the P-GW determines that the subscriber has reached their data usage quota during the call setup:

- The audio bearer portion of the call is activated.The video bearer portion of the call is NOT activated.The P-GW sends the PCRF a Credit Control Request update (CCR-U) with "OUT_OF_CREDIT" event trigger and the Final-Unit-Action (FUA) received from the OCS.The PCRF removes the Service Data Flow (SDF) from the P-GW, and sends the P-CSCF indication of the failure of the video bearer channel setup.

Quota Check - During Active Video Call

If the subscriber exhausts their data usage during a video call:

- The audio bearer portion of the call is preserved.The video bearer portion of the call is terminated.The P-GW sends the PCRF CCR-U with "OUT_OF_CREDIT" event trigger and the Final-Unit-Action (FUA) received from the OCS.The PCRF removes the SDF from the P-GW, and sends the P-CSCF indication of the failure of the video bearer channel setup.

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 P-GW does not support non-standard QCI values unless a valid license key is installed.

QCI values 1 through 9 are standard values defined in 3GPP TS 23.203; the P-GW supports these standard values.

From 3GPP Release 8 onwards, operator-specific/non-standard QCIs can be supported and carriers can define QCI 128- 254. For more information, see Non-standard QCI Support, on page 87.

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 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 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 & 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 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.

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 Supported Logical Network Interfaces (Reference Points), on page 6.

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 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 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.

Important In release 20.0 and higher Trusted StarOS builds, the FTP option is no longer available.

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

Prior to StarOS release 20, when the egtpinmgr task restarted it took a significant amount of time for it to recover. As a result, the outage time for which the GGSN, P-GW, SAEGW, and S-GW were unable to accept any new calls during egtpinmgr recovery was high.

In StarOS release 20, the software has been enhanced to optimize the recovery outage window in the event of an egtpinmgr task restart. The optimization has been achieved by optimizing the internal algorithms of egtpinmgr recovery as well as optimizing 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 needed 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.

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.

Important For more information on PMIPv6 Heartbeat support, refer to the *PMIPv6 Heartbeat* chapter in this guide.

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 Acknowledgement 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.

To support 802.1p network traffic prioritization for use in grouping packets into various traffic classes, the P-GW enables operators to map QCI values to 802.1p priorities for uplink and downlink packets.

Important The P-GW does not support non-standard QCI values unless a valid license key is installed.

QCI values 1 through 9 are standard values defined in 3GPP TS 23.203; the P-GW supports these standard values.

From 3GPP Release 8 onwards, operator-specific/non-standard QCIs can be supported and carriers can define QCI 128- 254. For more information, see Non-standard QCI Support, on page 87.

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 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 MBReq	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.

Scenario No.	IE carrying OCP Capability Received from S-GW in MBReq	Old Behavior: IE Carrying OCP Capability Sent to S-GW in MBRsp	New Behavior: IE Carrying OCP Capability Sent to S-GW in MBRsp
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: **Private Extension IE**. If gtpc private-extension overcharge-protection is enabled at egtpc service level: **Indication IE**.	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: **Private Extension IE and Indication IE**. If gtpc private-extension overcharge-protection is enabled at egtpc service level: **Indication IE**.	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: **None**. If gtpc private-extension overcharge-protection is enabled at egtpc service level: **Indication IE**.	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.

S-GW Restoration Support

S-GW Restoration helps in handling the S-GW failure in the EPC network. It allows affected PDNs that fail due to S-GW to be restored by selecting another S-GW to serve the affected PDNs. This avoids unnecessary flooding of signaling for PDN cleanup.

The P-GW maintains the sessions in case path failure is detected or if S-GW restart is detected during recovery IE on GTP-C signaling. The P-GW will ensure that any dropped packets in this scenario are not charged. The P-GW also rejects any bearer additions or modification requests received for the PDN connection maintained after the S-GW failure detection. This occurs until the PDN is restored.

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

When a subscriber is in S-GW restoration phase, all RARs (expect for Session Termination) reject the PCEF. The P-GW rejects all internal updates which can trigger CCR-U towards the PCRF. The P-GW triggers a CCR-U with AN-GW changes for the PDNs that are restored if the S-GW has changed on restoration.

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

Important Only MME/S4-SGSN triggered S-GW restoration procedure will be 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.

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.

The P-GW Restart Notification may also be used to signal that the peer P-GW has failed and not restarted. In this case, the P-GW Restart Notification contains a cause value: P-GW not responding. While sending the PRN, the S-GW includes the cause with this new cause value depending on the echo response.

Important 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 PDN 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 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 signalling 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.

Important In release 20.0 and higher Trusted StarOS builds, the FTP option is no longer available.

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 signalling 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*.

Transaction Rate KPIs - Session Events Per Second

Prior to StarOS release 20, key performance indicators (KPIs) did not differentiate between successful or unsuccessful PDN session activations and deactivations. In addition, the KPIs did not provide any information related to the Voice-over-LTE (VoLTE) service.

In StarOS release 20, Session Events Per Second (SEPS) KPIs have been implemented to address these issues. These KPIs measure the signaling load on the P-GW/ePDG. Further, network initiated setup/tear down KPIs have been added to measure the event rate for VoLTE call setup and tear down. Together, these measurements assist operators in performing network dimensioning/planning for the P-GW/ePDG node.

For the P-GW, both types of KPIs are supported on the S5, S8, S2a, and S2b Interfaces. Also for the P-GW, SEPS KPIs are supported for any associated eHRPD/PMIP service.

Specifically, the following KPIs have been implemented:

Session Events Per Second (SEPS)

Session Events per Second KPIs have been implemented to assist operators in measuring the signaling load on the P-GW/ePDG. These SEPS KPIs include the following:

- Total session events (session setup and tear down) per second.
- Successful Session Events (session setup and tear down) per second.
- Unsuccessful Session Events (session setup and tear down) per second.

N/w Initiated Setup/Tear down Events Per Second

Network initiated setup/tear down event KPIs have been implemented to assist operators in measuring Voice-over-LTE (VoLTE) call setup and tear down events rate at the P-GW/ePDG. Both Create Bearer Requests (CBReqs) and Delete Bearer Requests (DBReqs) originally initiated by the P-GW and CBReqs and DBReqs initiated by the P-GW as a result of Home Subscriber Server (HSS)- and User Equipment (UE)-initiated events will be accounted for in these KPIs. The N/w Initiated Setup/Tear down Events Per Second KPIs include the following:

- Total N/w Initiated Setup/Teardown Events (VoLTE bearer setup and tear down) per second.
- Successful N/w Initiated Setup/Teardown Events (VoLTE bearer setup and tear down) per second.
- Unsuccessful N/w Initiated Setup/Teardown Events (VoLTE bearer setup and tear down) per second

Operation

The P-GW/ePDG contains 8 buckets for transaction rate statistics collection for both session events per second KPIs and N/w Initiated Setup/Tear down Events per Second KPIs. The buckets are based on a configurable bucket interval that is from 1 to 20 minutes in length. During the configured time interval, an average is computed and stored for the entire bucket interval.

After the first 8 bucket intervals have elapsed and statistics collected, the P-GW continues sequentially through the 8 bucket intervals and eventually overwrites the original 8 bucket-intervals with more recent data. In short, the 8 bucket intervals provide a running value for the last eight bucket-intervals for which the KPIs have been computed. While the statistics are eventually overwritten with new values, all statistic totals are added to the historical statistics, which are not overwritten.

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 signalling 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.

User Location Change Reporting Support

The user information change reporting is enabled on GGSN via PCRF using GPRS specific event triggers and GPRS specific credit re-authorization triggers. The user information to be reported include Location Change Reporting (ULI) and Closed Subscriber Group Information Change reporting (UCI)

For Location change reporting for a subscriber session requested by GGSN, the SGSN includes the User Location Information (ULI) if the MS is located in a RAT Type of GERAN, UTRAN or GAN. It also includes the CGI, SAI or RAI depending on whether the MS is in a cell, a service or a routing area respectively. The SGSN may optionally include the User Location Information for other RAT Types.

Closed Subscriber Group (CSG) identifies a group of subscribers who are permitted to access one or more CSG cells of the PLMN as a member of the CSG. A CSG ID is a unique identifier within the scope of PLMN which identifies a CSG in the PLMN associated with a CSG cell or group of CSG cells. For CSG info change reporting for a subscriber session requested by GGSN, the SGSN includes the User CSG Information if the MS is located in the CSG cell or the hybrid cell.

Release 20.0 and later, support has been added to process and handle a MS Info Change notification received with valid information to identify a PDN (non-zero TEID and/or IMSI+NSAPI) and with appropriate ULI and/or UCI information. In case of collision between MS-Info-change message and NRUPC, GGSN will process MS-info-change request first and send out its MS-info-change response. Then the NRUPC will be retried again.

Important CSG reporting is not yet supported on GGSN, P-GW, or SAEGW.

Limitations

Following are the limitations of this feature:

- UCI trigger from PCRF is not supported.
- The MS Info Change reporting action trigger will not be recovered if trigger if:
  - trigger is changed
  - MS reporting action has not gone in CPC/UPC/NRUPC
  - session manager (SM) recovery happens
- The MS Change info message is not supported if it comes on UE level.

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 Actiontowards 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.

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*.

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.

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 *ECS 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.

Hash-Value Support for Header Enrichment

Hash-Value strings are implemented as a part of the Header Enrichment feature. P-GW is enhanced to receive and store hash values that are received from the PCRF for each subscriber. The stored hash value is inserted in the HTTP/WSP header making it available for operators to handle subscriber profiles.

Some Mobile Advertisement platforms generate a hashed string based on a subscriber's MSISDN value. When a hashed string is sent to Content Providers, they identify the subscriber's profile information and in turn insert advertisements on the subscriber's browser based on the user's profile.

To receive Hash-values from the PCRF, a new AVP: **Hash-Value**; with an octet-string data-type is implemented on the Gx interface. The AVP supports a maximum length of 80 characters. The P-GW ignores the hashed string if it exceeds the maximum length. The hash-value received from the PCRF is inserted in the HTTP/WSP header only if HTTP Header Enrichment is enabled for a subscriber.

The X-Header field is used to insert a Hash-Value in the HTTP/WSP headers. The Hash-Value can be encrypted based on the existing encryption mechanism of X-Header fields. These hash values (encrypted or not encrypted) are inserted in the HTTP/WSP header based on the x-header format configured under Charging Action configuration.

Note A Hash-Value is check-pointed as a part of the subscriber's session information. It is check-pointed immediately, once received from the PCRF.

IPNE Service Support

The P-GW supports the IP Network Enabler (IPNE) service. IPNE is a Mobile and IP Network Enabler (MINE) client component that collects and distributes session and network information to MINE servers. The MINE cloud service provides a central portal for wireless operators and partners to share and exchange session and network information to realize intelligent services. For detailed information on IPNE, refer to the *IP Network Enabler* chapter in this guide.

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 *NAT 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

Allows 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 *ADC 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 acknowledgement 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 *ECS Administration Guide*.

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

Features and Functionality - Optional Enhanced Feature Software

This section describes the optional enhanced features and functions for the P-GW 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*.

3GPP R13 Emergency Call Support on the ePDG and P-GW

The ePDG and P-GW support emergency call establishment over untrusted WiFi for the P-GW as per 3GPP Release 13. 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 normal attached UEs and, depending on local regulation, to UEs that are in limited service state. Receiving emergency services in a limited service state does not require a subscription.

Authentication Authorization Requests (AAA) to Diameter now carry the new Emergency-Indication AVP for Untrusted WiFi emergency calls. Diameter requests related to PDN connections for emergency services have the highest priority. Depending on regional/national requirements and network operator policy, these Diameter requests are the last to be throttled, in the event that the 3GPP AAA Server has to apply traffic reduction. For more information see *3GPP R13 Emergency Call Support on the ePDG and P-GW* section.

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.

Bulkstats for GTP-C Messages by ARP Value

To comply with the "Long Term Evolution (LTE) Access Network Government Industry Requirements (GIR) for National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority" to support emergency calls over Voice over LTE (VoLTE), several Key Performance Indicators (KPIs) have been introduced with this feature. This feature is utilized to collect statistics for total number of GTP-C messages received for Enhanced Multimedia Priority Service (eMPS) session for specified interval (in minutes). The list of GTP-C messages are defined in accordance with the GIR document. As part of this feature:

- The S-GW will generate peg counts of the total number of received GTP-C messages containing an Allocation and Retention Priority (ARP), chosen from the set of values allocated for NS/EP NGN-PS use, for a specified interval (in minutes). This peg count is administered at the S-GW level.
- The P-GW will generate peg counts of the total number of received GTP-C messages containing an ARP, chosen from the set of values allocated for NS/EP NGN-PS use, for a specified interval (in minutes). This peg count is administered at the specific P-GW level.
- The peg counts for GTP-C messages are broken down by message type similar to existing GTP-C message counters. The bulkstats are broken down by applicable S-GW and P-GW service and S5, S8, S11, and S4 interfaces.

In earlier releases, bulkstats were not present for eMPS session. With this release 21.1, bulkstats are added for eMPS session/message.

Piggy-back Message

For piggy-back messages, if either of the messages have matching ARP or result into converting non-eMPS session to eMPS session, then both messages are counted as eMPS message and corresponding statistics for both messages are incremented.

If Modify Bearer Request is piggy-backed with Create Bearer Response on S11 interface of S-GW and Create Bearer Response result into converting non-eMPS session into eMPS session, then Modify Bearer Response statistics will not increment for this Modify Bearer Request.

Bulkstats Collection and Reset

Bulkstats are added under eGTP-C Schema and pgw-egtpc-s5s8 Schema. These eMPS bulkstats in eGTP-C Schema and pgw-egtpc-s5s8 Schema holds value only for a bulkstat interval, that is, value of these bulkstats shows number of eMPS messages exchanged during the bulkstat interval.

For more information, see *Bulkstats for GTP-C Messages by ARP Value* section.

Common Gateway Access Support

Common Gateway Access support is a consolidated solution that combines 3G and 4G access technologies in a common gateway supporting logical services of HA, P-GW, and GGSN to allow users to have the same user experience, independent of the access technology available.

In today's scenario, an operator must have multiple access networks (CDMA, eHRPD, and LTE) plus a GSM/UMTS solution for international roaming. Therefore, operators require a solution to allow customers to access services with the same IP addressing behavior and to use a common set of egress interfaces, regardless of the access technology (3G or 4G).

This solution allows static customers to access their network services with the same IP addressing space assigned for wireless data, regardless of the type of connection (CDMA, eHRPD/LTE, or GSM/UMTS). Subscribers using static IP addressing will be able to get the same IP address regardless of the access technology.

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 representative for information on how to obtain a license.

Dynamic RADIUS extension support provide 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.

Expanded Prioritization for VoLTE/Emergency Calls

The National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority Services (NGN-PS) (formerly called NGN Government Emergency Telecommunications Service (GETS)) is a set of voice, video and data services that are based on services available from public packet-switched Service Providers. The NS/EP NGN-PS provides priority treatment for a Service User's NS/EP communications and is particularly needed when the Service Providers' networks are impaired due to congestion and/or damage from natural disasters (such as floods, earthquakes and hurricanes) and man-made disasters (such as physical, cyber or other forms of terrorist attacks).

In earlier releases, the DSCP marking of control message from P-GW and S-GW was based on associated egtpc-service configuration.

With Release 21.1, for control message belonging to eMPS session or containing Allocation and Retention Priority (ARP) associated with eMPS profile, the DSCP marking is based on eMPS profile configured DSCP value.

As part of this enhancement, support is also added for marking of certain GTP-C message at the P-GW and S-GW for priority treatment as defined in the Government Industry Requirements (GIR) NS/EP NGN. For more information, see *Expanded Prioritization for VoLTE/Emergency Calls* section.

ePDG Selection Using PCO

The purpose of this feature is to enable the PGW to send the ePDG IP addresses in an operator PCO so that when connected to a WiFi network the UE will attach to the closest geographic ePDG. This will aid in setting up the IPSEC tunnel to the closest ePDG and therefore reducing latency for VoWiFi and other features.

A new CLI has been introduced to customize PCO options in the network.

Important This is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

Important ePDG PCO is supported only for the CS request which are received on the S5-S8 interface. This feature is not applicable for the GGSN calls.

For more information on this feature, see *ePDG Selection Using PCO* chapter of 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

The S2a interface connects the standalone P-GW and P-GW of the SAEGW with the HSGW of the eHRPD.

Prior to StarOS release 20.0, GTP-based S2a interface support was available on the P-GW. With StarOS release 20.0, 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.

Operators deploying StarOS release 20.0 on the SAEGW are now able to integrate Trusted WiFi network functionality using this feature.

Supported functionality includes:

- Initial Attach
- WiFi-to-LTE handover

- LTE-to-WiFi handover
- Multi-PDN handovers

GTP-based S2b Interface Support

Use of WiFi Integration functionality requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

This section describes the GTP-based S2b interface implementation on the P-GW. The S2b interface connects the P-GW 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 supports the following:

- UE connecting to PDN via WiFi access
- UE multiple PDN connections
- Initial Attach
- LTE to WiFi Handoff
- WiFi to LTE Handoff

Important For more information on WiFi Integration functionality, refer to the *GTP-based S2b Interface Support on the P-GW and SAEGW*chapter in this guide.

Voice Over WiFi Support

When the UE moves from WiFI to LTE, the P-GW sends a Delete Bearer Request to the ePDG (WiFi access). Previously, the Delete Bearer Request was sent as soon as a Create Session Request for handoff was received at the P-GW. In some cases (for some specific handsets) this broke the IP sec tunnel between the handset and the WAP. In these instances, the handoff failed. To avoid handoff failure, the P-GW should send a Create Session Response first and delay the Delete Bearer Request until handoff is complete for UE. Next, UE generates a Modify Bearer Request to indicate handoff completion and the Delete Bearer Request is only generated after the P-GW receives the Modify Bearer Request. This indicates that at the P-GW both access types (WiFi and LTE) will remain active until the Modify Bearer Request is received. When UE moves from LTE to WiFi, handoff completion occurs at the Create Session Response.

GTP Throttling

Use of GTP and Diameter Interface Throttling requires that a valid license key be installed. Contact your Cisco account 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. It prevents the message flood from P-GW towards S-GW and MME. Currently, following outgoing messages are throttled by P-GW 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.

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.*

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.

Important For more information on these commands, refer to R12 GTP-C Load and Overload Support, on page 89.

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 PSC/PSC2 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 PSC/PSC2 failure will cause a PSC 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 interchassis 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 *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 local 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 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 uses 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.

Important For more information on configuring the Local Policy Decision Engine, refer to the *Configuring Local QoS Policy* section in the *PDN Gateway Configuration* chapter of this guide.

Modify Bearer Response using controlled parameters

The P-GW service provides configurable parameters to include Charging-ID, Charging FQDN or Charging Gateway address, and MSISDN in Modify Bearer Response. All Modify Bearer Response messages will send these parameters if CLI is enabled irrespective of scenarios like S-GW relocation and GnGp to LTE handover. This feature is not license-controlled and the behavior is controlled using CLI.

For more information on this feature, refer to the *Modify Bearer Response using controlled parameters* chapter in this guide.

MPLS Forwarding with LDP

Use of MPLS requires that a valid license key be installed. Contact your local 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 bound 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.

Important For more information on MPLS support, refer to the *Multi-Protocol Label Switching (MPLS) Support* chapter in this guide.

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 representative for information on how to obtain a license.

NEMO support in P-GW was added in earlier StarOS releases. In release 15.0, support was added for GGSN as well so that NEMO can be supported for subscribers roaming out on 3G (UMTS/GERAN) networks.

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.

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/IMSA/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/IMSA/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. From 3GPP Release 8 onwards, operator-specific/non-standard QCIs can be supported on P-GW/GGSN (not standalone GGSN) and carriers can define QCI 128-254 to differentiate between various services/applications carriers provide to the end users in their network.

Important For more information on non-standard QCI support, refer to the *Extended QCI Options* chapter in this guide.

NetLoc for WiFi EPC

With this feature, the IMS network can retrieve location information of the UE from WLAN access network. This improves location related feature and functionality for the operator. This feature also helps in charging subscribers based on location information.

Please note that the support for LTE NetLoc already exists from prior releases. With this release, NetLoc support is extended for WLAN access. Basic implementation is already supported for passing necessary parameter to different internal modules like SM, IMSA and ECS. For more information, see *NetLoc for WiFi EPC* section.

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.

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.

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. MBReq will have a new private extension IE to send "stop charging" and "start charging" indication to P-GW.

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 sending downlink packets after receiving "stop charging" request 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).

Important When Overcharging Protection feature is configured at both P-GW service and APN, configuration at APN takes priority.

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 GTP-C Load and Overload Support

GTP-C Load Control feature is a licensed, 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 situations for the overloaded node through actions taken by the peer node(s). This feature is supported over 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 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.

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 detailed 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, ((number of active sessions per service / 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.

Retrieve MDN from S6b

As per the current implementation, during an initial attach, P-GW selects Mobile Directory Number (MDN) or Mobile Station International Subscriber Directory Number (MSISDN) from the S6b interface. Later, when the call is handed off from P-GW to other services like eHRPD/trusted WiFi/untrusted WiFi or the handoff is done from these services to the P-GW, then the MDN/MSISDN is picked from the create session (CS) request and the S6b authorized MDN/MSISDN is lost. As a result, different values of MDN/MSISDN are sent in the Rf records. Since, typically, operators use MDN to charge subscribers, this results in revenue loss.

This feature retains the MDN/MSISDN value from the S6b interface or the CS request, during the initial attach and even during handoff between P-GW and eHRPD/ trusted WiFi/untrusted WiFi. The MDN/MSISDN value does not change in the call lifetime. As a result, all Rf records of a session have the same MDN/MSISDN values.

A new keyword retain-mdn has been added to the CLI command authorize-with-hss. This CLI command keyword, when configured, retains the MDN/MSISDN value. If the CLI command keyword is not configured, the MDN/MSISDN value is not received from the S6b interface. In this case, the MDN/MSISDN value received in the CS request is used.

Important This feature is not applicable to GnGp handoff.

For more information on this feature, see *Retrieve MDN from S6b* chapter of this guide.

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 PSC/PSC2 during the upgrade process.

Important For more information on session recovery support, refer to the *Session Recovery* chapter in the *System Administration 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 it 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, P-GW does a round-off to convert a Gx request into a GTP request. When 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 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 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 **suppress-ubr no-bitrate-change** 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 signalling.
- **Location Report**: The purpose of Location Report procedure is to provide the UE's current location to the MME. This procedure uses UE-associated signalling.

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 *MME 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)

Event Trigger From PCRF	CRA Sent to S4 SGSN
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 Actiontowards 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.

Configurable Behavior on PDN Type IPv4v6

With this enhancement, P-GW/GGSN provided a new CLI configuration to enable the following four options when MME/SGSN sets PDN type to IPv4v6 and Dual Address Flag (DAF) is set to False in Create Session Request or Create PDP Request.

1. Option 1: Assign IPv6 address using current method and respond with Create Session Response or Create PDP Response with Success and Cause Code #19 "New PDN type due to single address bearer only".
2. Option 2: Assign IPv4 address and respond with a Create Session Response or Create PDP Response with Success and Cause Code #19 "New PDN type due to single address bearer only".
3. Option 3: Assign IPv6 address and respond with a Create Session Response or Create PDP Response with Success and Cause Code #18 "New PDN type due to network preference".
4. Option 4: Assign IPv4 address and respond with a Create Session Response or Create PDP Response with Success and Cause Code #18 "New PDN type due to network preference".

When the CLI is not configured, the default behavior is Option 1. The gateway supports multiple PDN connections for the same APN to accommodate for Option 1, Option 2, and the UE attempting a second PDN connection. It is possible to configure the CLI for each APN differently.

Previously, there was no configurable support for the type of PDN assigned and the cause code returned in a Create Session Response or Create PDP Response when a Create Session Request or CPC was received for IPv4v6 PDN with DAF False at the P-GW and GGSN.

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
- GTP PDN Gateway Call/Session Procedures in an LTE-SAE Network

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 97
- PMIPv6 Lifetime Extension without Handover, on page 99
- PDN Connection Release Initiated by UE, on page 100
- PDN Connection Release Initiated by HSGW, on page 101
- PDN Connection Release Initiated by P-GW, on page 103

Initial Attach with IPv6/IPv4 Access

This section describes the procedure of initial attach and session establishment for a subscriber (UE).

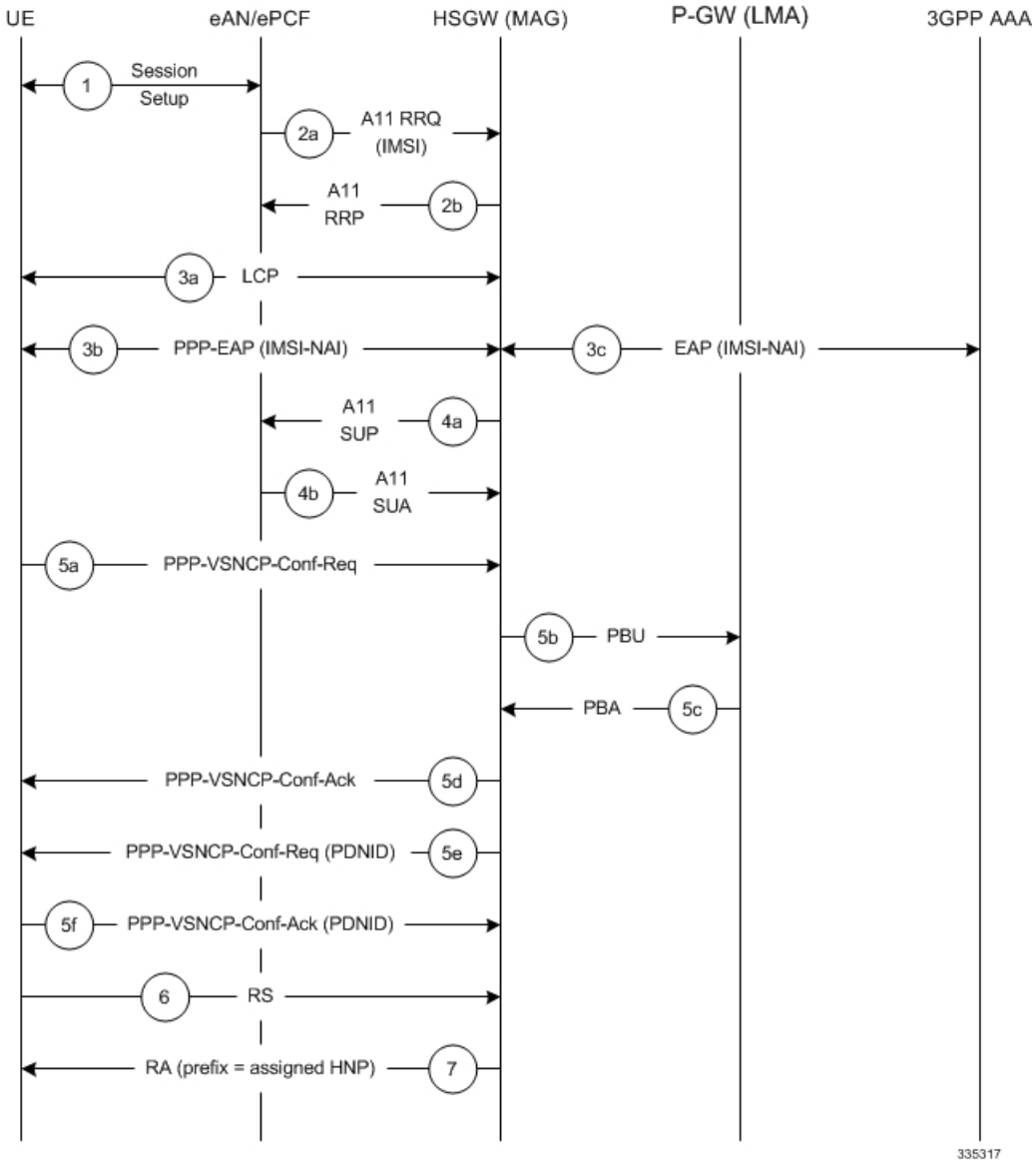


Table 6: Initial Attach with IPv6/IPv4 Access Call Flow Description

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.

Step	Description
3b	The UE performs EAP over PPP.
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 Acknowledgement (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.

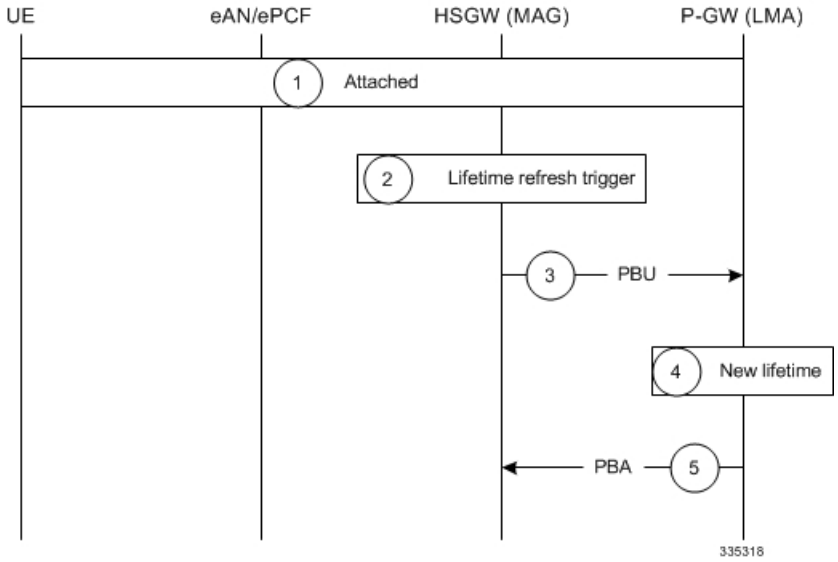


Table 7: PMIPv6 Lifetime Extension (without handover) Call Flow Description

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.

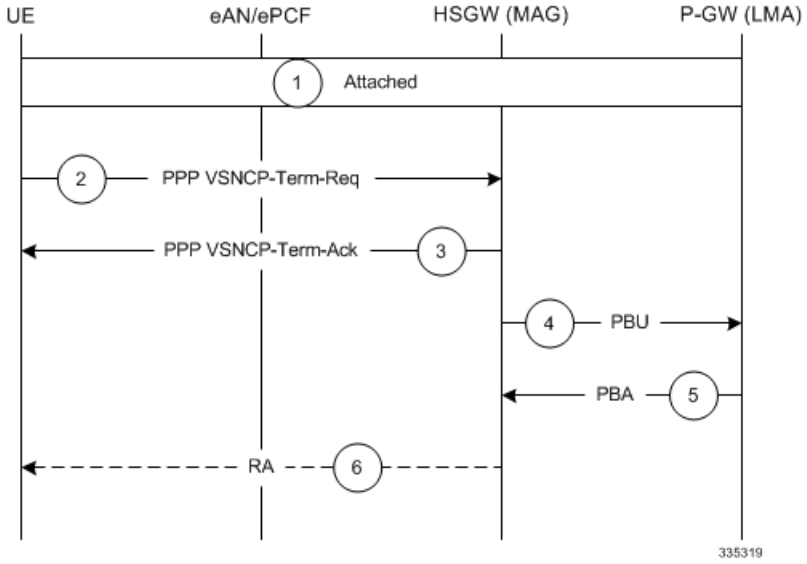


Table 8: PDN Connection Release by the UE Call Flow Description

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.
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.

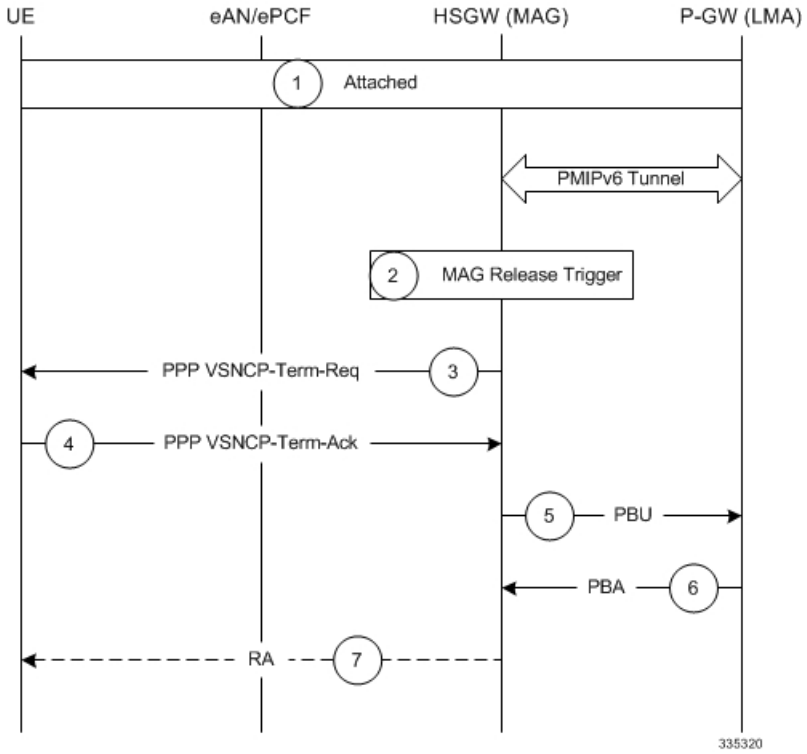


Table 9: PDN Connection Release by the HSGW Call Flow Description

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.
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).

Step	Description
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.

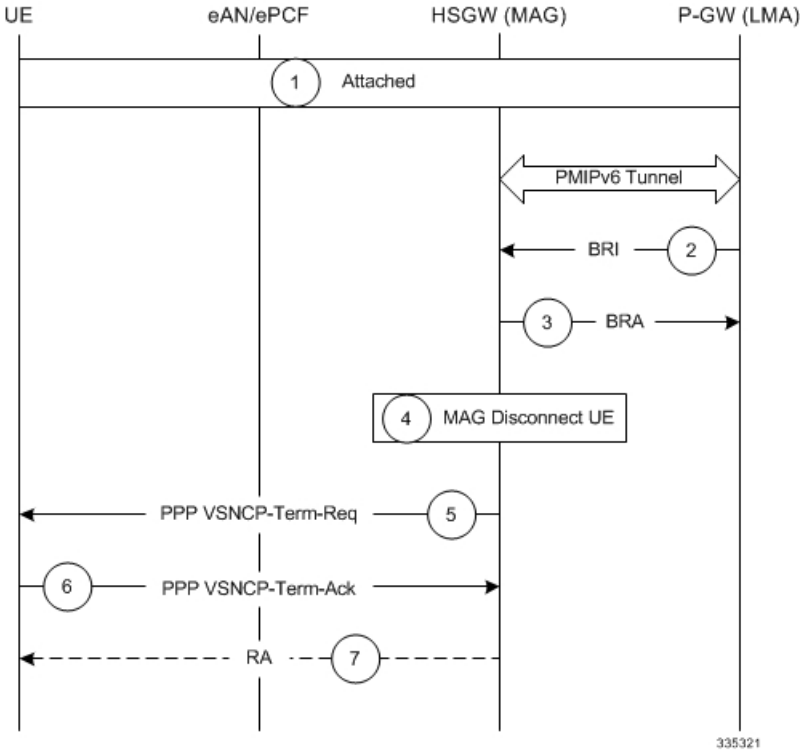


Table 10: PDN Connection Release by the P-GW Call Flow Description

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 P-GW 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 sane attributes (MNID, APN, HNP).
4	The HSGW MAG service triggers a disconnect of the UE PDN connection for PDNID=x.

Step	Description
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).
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)

This section describes the procedure of an initial attach to the EPC network by a subscriber.

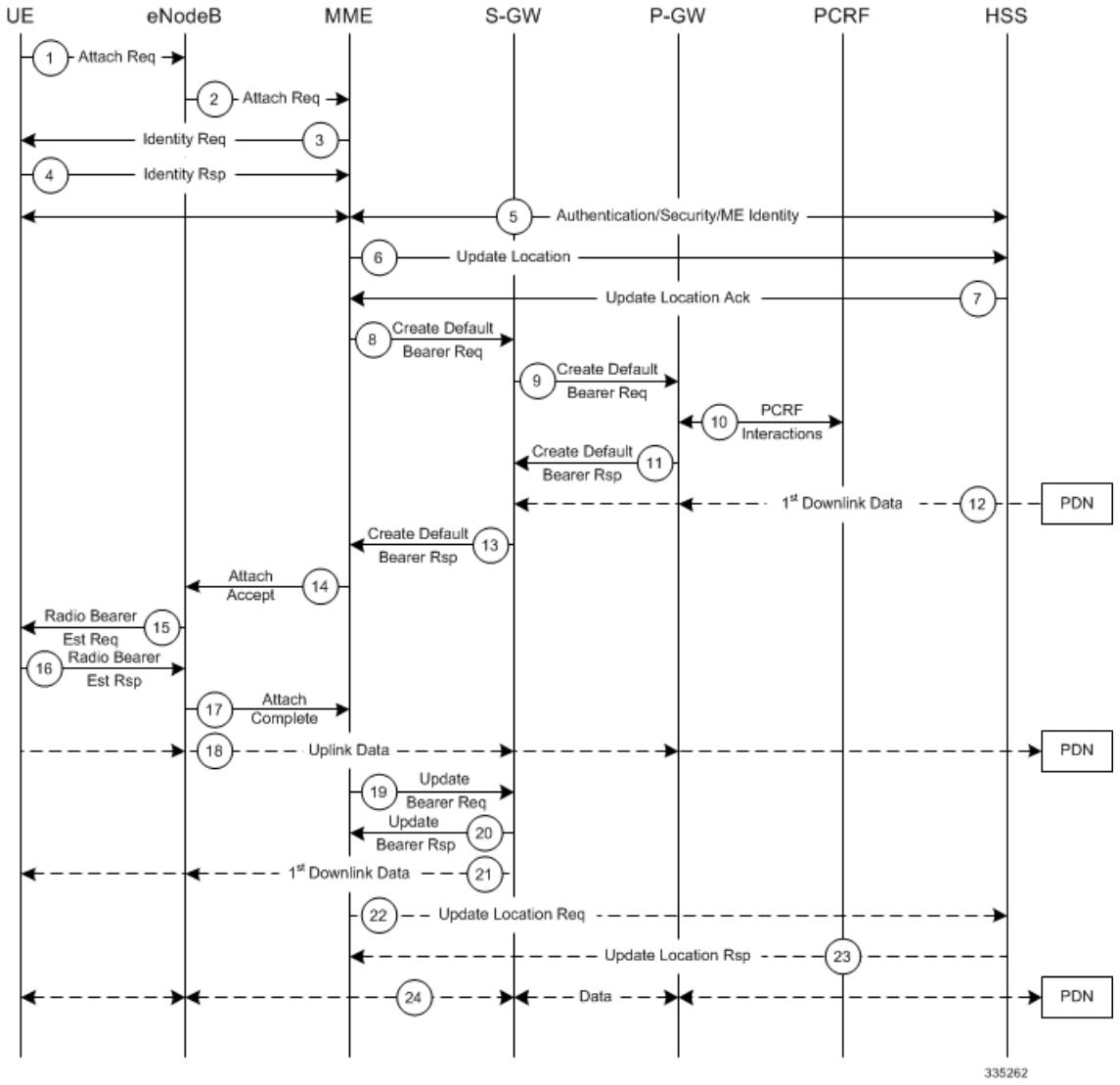


Table 11: Subscriber-initiated Attach (initial) Call Flow Description

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.

Step	Description
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.

Step	Description
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.

Step	Description
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.

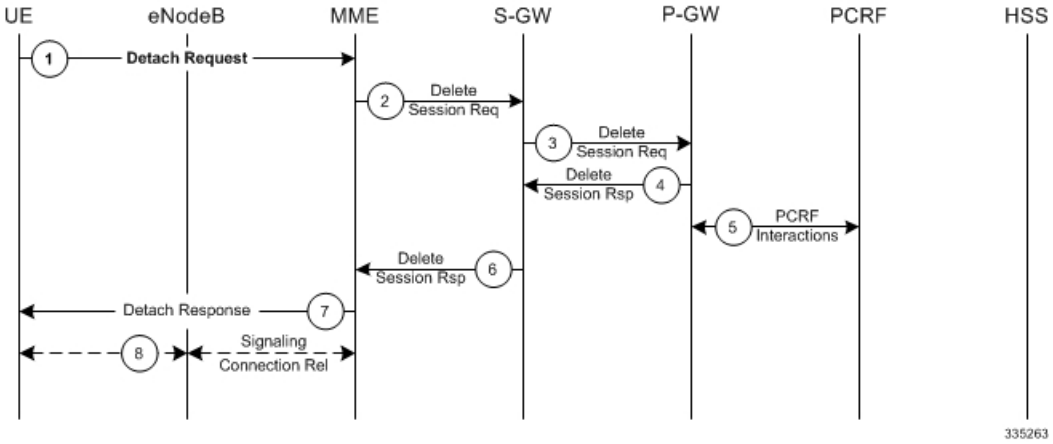


Table 12: Subscriber-initiated Detach Call Flow Description

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 signalling connection for the UE by sending an S1 Release command to the eNodeB with Cause = Detach.

Supported Standards

The P-GW service complies with the following standards.

- Release 12 3GPP References, on page 110
- Release 11 3GPP References, on page 110

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 3602: The AES-CBC Cipher Algorithm and Its Use with IPSec
- RFC 3646: DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 3715 IPSec-Network Address Translation (NAT) Compatibility Requirements
- RFC 3748: Extensible Authentication Protocol (EAP)
- RFC 3775: Mobility Support in IPv6
- RFC 3948: UDP Encapsulation of IPSec ESP Packets
- RFC 4004: Diameter Mobile IPv4 Application
- RFC 4005: Diameter Network Access Server Application
- RFC 4006: Diameter Credit-Control Application
- RFC 4187: Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)
- RFC 4282: The Network Access Identifier
- RFC 4283: Mobile Node Identifier Option for Mobile IPv6 (MIPv6)
- RFC 4303: IP Encapsulating Security Payload (ESP)
- RFC 4306: Internet Key Exchange Protocol Version 2
- RFC 4739: Multiple Authentication Exchange in IKEv2 protocol
- 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
- RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2)
- 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-pmipv6-mipv4-00.txt) Proxy Mobile IPv6 and Mobile IPv4 interworking

Object Management Group (OMG) Standards

- CORBA 2.6 Specification 01-09-35, Object Management Group