ERICSSON

EPG Technical Product Description Overview

TECHNICAL PRODUCT DESCRIPTION

2/221 02-AXB 250 12-V3 Uen FF

Contents

1 Introduction

This document provides an overview of the EPG for GSM, WCDMA, LTE, trusted non-3GPP network, and untrusted non-3GPP network.

The EPG supports simultaneous combination of the GGSN, PGW, and SGW functionality. The GGSN functionality is based on the GPRS architecture, and the SGW and PGW functionality is based on the EPS architecture. For more information on the packet core architecture, refer to Ericsson Packet Core Network Overview.

The purpose of this document is to provide an introduction to the network, the EPG and its functions, O&M of the EPG, software management, and the CPI. In addition, reference is provided to documents where detailed information can be found.

1.1 Scope

This document provides a high-level description of the EPG functions, and the interworking system. It also provides brief descriptions of the EPG interfaces in the GPRS and EPS networks. For more detailed information, see the references included in each section.

1.2 Target Groups

This document is intended as an introduction to the EPG for network operators, network and service planners, as well as system engineers and administrators. It assumes a basic knowledge of data communication and telecommunication.

2 Network Overview

The EPG supports simultaneous use of the GPRS and EPS technologies. The GPRS and EPS provide basic solutions for IP communication between the UE and the Internet, corporate intranets, and private data networks. The GPRS technology enables packet data services to the GSM and WCDMA systems. The Ericsson GPRS solution includes an SGSN and an EPG acting as a GGSN or PGW. The EPS technology enables packet data services to the LTE system and the non-3GPP networks, including the trusted non-3GPP network and the untrusted non-3GPP network. In the EPS network, the EPG acts either as a PGW, an SGW, or both a PGW and SGW simultaneously. For more information on GPRS and EPS, refer to Ericsson Packet Core Network Overview.

3 Network Functions

This section describes the network functions in the GSM, WCDMA, LTE, trusted non-3GPP networks, and untrusted non-3GPP network.

3.1 Role of the EPG in the GSM, WCDMA, LTE, and Trusted/Untrusted Non-3GPP Networks

In the GSM and WCDMA networks, the EPG provides an interface between the SGSN or RNC and Packet Data Networks (PDNs), such as the Internet, corporate intranets, and private data networks. In the LTE network, the EPG provides an interface between the MME and PDNs for control plane signaling, and the eNodeB and PDNs for user packets. In the trusted non-3GPP network, the EPG provides an interface between the Trusted WLAN Access Network (TWAN) or Mobile Access Gateway (MAG) and the PGW. In the untrusted non-3GPP network, the EPG provides an interface between the Evolved Packet Data Gateway (ePDG) and the PGW.

Note: Identified by an Access Point Name (APN), PDNs are often referred to as APN networks.

The EPG provides the following services:

Session Management
Manages connections between the UE and PDNs, and dynamic IP address allocation

Quality of Service (QoS) Control
Enables QoS differentiation through IP packet prioritization and allows bit rate enforcement for individual users and services

User Packet Handling
End-user information and associated data transfer control procedures, such as flow control, error detection, error correction, and error recovery

External Internet Service Provider (ISP) functions
Support for interfaces towards external Internet Service Provider (ISP) functions, like RADIUS servers, used for authentication, authorization, and accounting purposes

Routing Enables the EPG to support IP addresses that overlap APNs and allows for traffic separation between networks

Charging For each UE device, the EPG collects charging information, such as the external data network use and GPRS or EPS network resources

Service Aware Charging and Control (SACC)
Provides flexible charging and control of UE IP flows.

Tunneling Enables a packet to retain its original IP address and still be routed transparently across several network nodes and EPGs using a separate set of IP addresses

Security Resists and prevents attacks on the EPG on the network level, IP routing level, GPRS and EPS user level, and O&M level

Resilience Enables, through a combination of hardware and software redundancy, high levels of service resilience, and availability

3G Direct Tunnel (3GDT)
Enables user packets to be transported outside the SGSN, directly between the GGSN, PGW, or SGW, and the Radio Network Controller (RNC)

3.2 Standard Release

The EPG is generally compliant with 3GPP Release 10 specifications, with details and deviations described in the Statements of Compliance (SoCs) for relevant 3GPP TS.

3.3 Network Impact Report

The difference from a network perspective between the current EPG release and a previous EPG release is described in the Network Impact Report (NIR). For more information, refer to EPG Network Impact Report.

4 Cloud Environment

The virtual EPG is executed in a cloud environment, which consists of the following components:

— Cloud infrastructure: the Ericsson CEE or a third-party cloud infrastructure, providing Infrastructure as a Service (IaaS), where the virtual EPG executes on a cluster of Virtual Machines (VMs).

— Cloud management system: the Ericsson ECM or a third-party cloud management system, providing management and orchestration of the virtual resources.

— Ericsson Network Manager (ENM): providing network and element management of the Ericsson Physical Network Functions (PNFs) and Virtual Network Functions (VNFs). It also provides a VNF Lifecycle Manager (VNF-LCM) for the Ericsson VNFs.

— Legacy BSS systems of the operator.

The components are described in more detail in the following sections.

Figure 1 shows an example of a generic cloud environment.

Figure 1 Generic Cloud Environment

Figure 2 shows an example cloud environment with Ericsson components. It illustrates how the Ericsson components map to the following ETSI Network Functions Virtualization (NFV) functional blocks:

— NFV Infrastructure (NFVI)

— NFV Orchestrator (NFVO)

— Virtual Infrastructure Manager (VIM)

— VNF Lifecycle Manager (VNF-LCM)

Figure 2 Cloud Environment with Ericsson Components

4.1 Cloud Infrastructure

The following sections describe possible cloud infrastructures.

4.1.1 Ericsson Cloud Execution Environment

The Ericsson CEE provides a carrier grade IaaS cloud infrastructure and a VIM. The CEE is based on OpenStack components, the Kernel-based Virtual Machine (KVM) hypervisor, and the high performance Ericsson Virtual Switch (EVS) based on Open vSwitch (OVS). The CEE supports Ericsson or third-party COTS HW for compute, storage, and networking. For more information, see CEE documentation.

4.1.2 Third-Party Cloud Infrastructures

System integration with a third-party IaaS cloud infrastructure is possible. The virtual EPG has no explicit direct interface toward the cloud infrastructure. However, the virtual EPG has dependencies to the following:

— The VM environment exposed by the hypervisor, for example, KVM and VMware ESXi

— The infrastructure networking solution, for example, network bandwidth per host including the vSwitch bandwidth

— The performance, characteristics, and robustness of the infrastructure, for example, high availability design including link failover aspects

For requirements on the cloud infrastructure, refer to Virtual EPG Requirements on the Cloud System.

4.2 Cloud Management System

The following sections describe possible cloud management systems.

4.2.1 Ericsson Cloud Manager

The ECM provides management and orchestration of services running on virtualized resources. It is possible that one ECM serves multiple tenants and applications sharing infrastructure. The ECM supports onboarding and instantiation of virtual applications using the Open Virtualization Format (OVF) package standard. The ECM also supports general-purpose VNF life cycle management, which depending on the use case can substitute or complement parts of the ENM VNF-LCM functionality.

For more information, see ECM documentation.

4.2.2 Atlas

Atlas is a set of management tools included in CEE, that can be used as a simplified alternative to ECM. It is based on the open-source OpenStack components Horizon dashboard and Heat orchestration. Atlas also implements a custom component – an OVF to Heat Orchestration Template (HOT) translator. Atlas supports orchestration of virtual applications using either OVF or HOT format.

For more details, see CEE documentation.

4.2.3 Third-Party Cloud Management Systems

System integration with a third-party cloud management system is possible. The virtual EPG has no direct interface toward the cloud management system. However, the virtual EPG has dependencies to the following:

— The VM image and the VNF or VM template formats supported by the cloud management system. For example, it can be required to translate the virtual EPG OVF package to another format.

— The procedures for VNF life cycle management. For example, it can be required to integrate the VNF-LCM in the ENM with the third-party cloud management system. For more information, see Section 4.3 on page 6.

— The cloud management system ability to define virtual resource and policy requirements needed by the virtual EPG. For example, the cloud management system must support VM anti-affinity policies, or a solution to control the VM placement on the physical compute hosts.

For requirements on the cloud management system, refer to Virtual EPG Requirements on the Cloud System.

4.3 Ericsson Network Manager

The ENM is the Network Manager and the Element Manager for both the physical and the virtual EPG. The virtual EPG has the same northbound interfaces to ENM as the physical EPG. Therefore, both the physical and the virtual EPG can be managed together in a seamless way, with equal support from ENM.

Also, the ENM is the VNF-LCM for the virtual EPG. The VNF-LCM interfaces the cloud management system to provide life cycle management of the virtual EPG, for example, instantiating and scaling the virtual EPG. The VNF-LCM is not strictly needed for all life cycle management use cases. The need depends on the functionality of the cloud management system. For example, the ECM can be used without the VNF-LCM for instantiating the virtual EPG. However, the VNF-LCM can provide a higher degree of automation and management tailored for Ericsson VNFs, including the virtual EPG.

The VNF-LCM in the ENM provides a flexible framework for system integration with different cloud management systems. System integration with the legacy BSS systems of the operator is supported through ENM northbound interfaces.

The ENM can also provide a consolidated alarm and performance view by correlating the cloud infrastructure alarms and statistics with the virtual EPG alarms and statistics.

For more information, see ENM documentation.

For more information on how to install and execute virtual EPG workflow in VNF-LCM, see Virtual EPG VNF Lifecycle Manager Workflow Instruction.

5 EPG Overview

The components of the virtual EPG are deployed as Virtual Machines (VMs) in a cloud environment. A VM can take the role of a virtual Route-Processor (vRP) or Virtual Service-Forwarder (vSFO). A vSFO can be configured as control plane or user plane. Figure 3 shows an overview of the EPG in a cloud environment. For information on the architecture, refer to EPG Architecture.

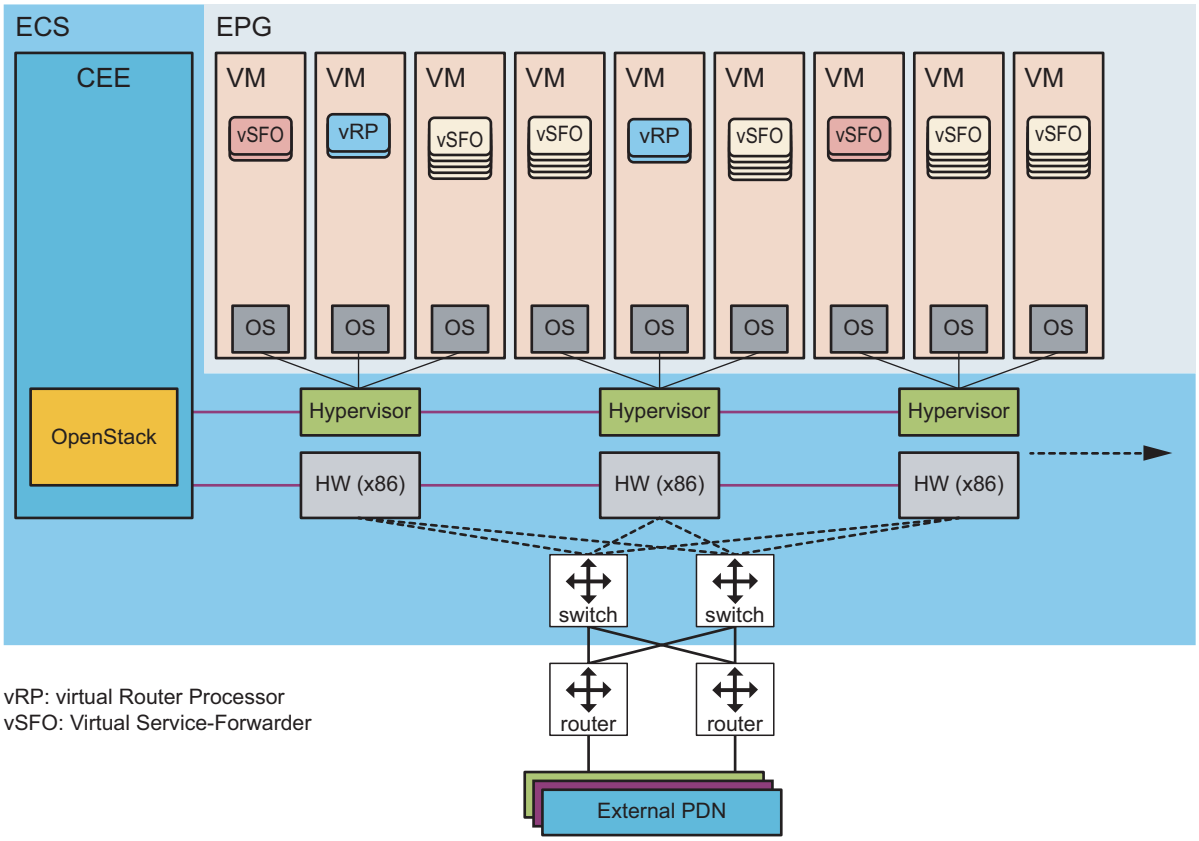

Figure 3 EPG Overview

5.1 Hardware

The virtual EPG is deployed in a cloud environment as VMs. The VMs run on Intel® x86 compute hosts.

5.2 Characteristics

The characteristics of the EPG depend on the chosen hardware and software configuration. For more information on capacity, throughput, and ISP, refer to EPG Characteristics.

5.3 Interfaces and Protocols

This section describes the interfaces connecting the EPG to other network nodes. A single EPG can be connected to many network nodes and APN networks.

Page 9 shows the supported interfaces in the GSM, WCDMA, LTE, and trusted/untrusted non-3GPP networks.

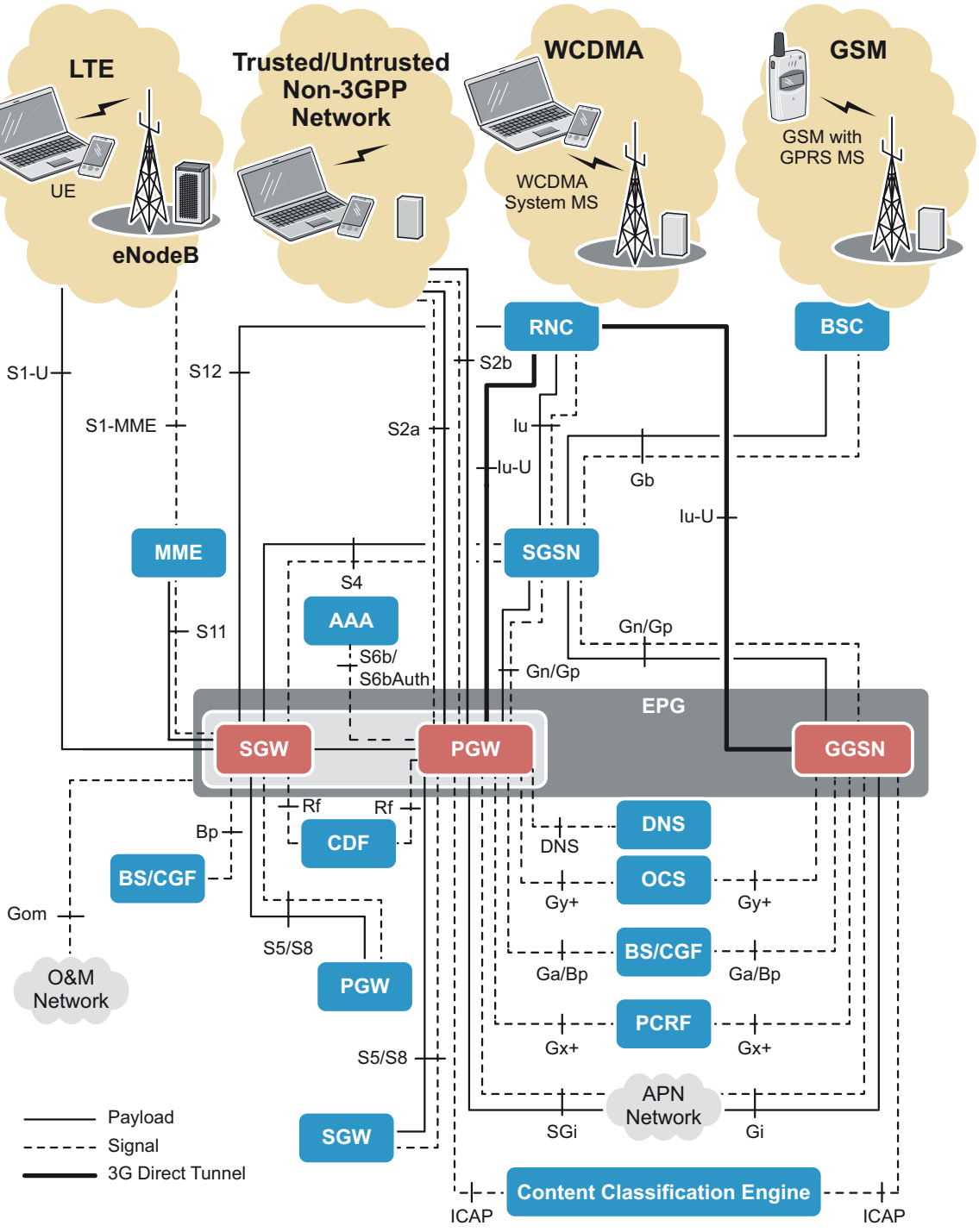

Figure 4 Interfaces in the GSM, WCDMA, LTE, and Trusted/Untrusted Non-3GPP Networks

The EPG supports the following interfaces:

Bp interface

The Bp interface connects the GGSN, PGW, and SGW to a Billing System (BS) responsible for handling Charging Data Records (CDRs) generated by traffic through the EPG. The connection to the BS can be mediated through a Charging Gateway Function (CGF). For more information, refer to CDR-Based Charging Interface Description.

Ga interface

The Ga interface connects the GGSN and PGW to a BS responsible for handling CDRs generated by traffic through the EPG. The connection to the BS can be mediated through a CGF. For more information, refer to CDR-Based Charging Interface Description.

Gi interface

The Gi interface connects the GGSN to external APN networks, allowing exchange of signaling and user data. The Gi interface also connects the GGSN to the SASN. If RADIUS is used, the Gi interface connects the GGSN to the RADIUS server. For more information on the Gi interface, refer to Gi and SGi Interface Description.

Gn interface

The Gn interface connects the GGSN and PGW to SGSNs within the same PLMN, allowing exchange of signaling and user data. For more information about the Gn Interface, refer to Gn/Gp Interface Description.

Gom interface

The proprietary Gom interface connects the EPG to external systems, for example, O&M networks allowing an operator to configure and monitor the EPG. For more information about other systems connected to the Gom interface, refer to Routing.

Gp interface

The Gp interface connects the GGSN and PGW to SGSNs in other PLMNs, allowing visiting subscribers to be routed through their home GGSN or PGW. For more information about the Gp Interface, refer to Gn/Gp Interface Description.

Gx+ interface

The Gx+ interface connects the GGSN and PGW to the Policy and Charging Rules Function (PCRF), allowing the GGSN and PGW to receive authorization and policy control information for SACC traffic. For more information, refer to Gx+ Interface Description.

Gy+ interface

The Gy+ interface connects the GGSN and PGW to an Online Charging System (OCS), allowing credit control for user traffic. The connection to the OCS can be mediated by an online mediation node. For more information, refer to Gy+ Interface Description.

Iu-U interface

The Iu-U interface connects the GGSN and PGW to RNCs, allowing for 3GDT functionality. For more information about 3GDT, refer to 3G Direct Tunnel.

Rf interface

The Rf interface connects the SGW and PGW to the Charging Data Function (CDF). The Rf interface is used for offline charging. For more information on the Rf interface, refer to PGW Rf Interface Description and SGW Rf Interface Description.

S1-U interface

The S1-U interface connects the SGW to eNodeBs, allowing for user data packet transportation. For more information about the S1-U interface, refer to S1-U and S12 Interface Description.

GTP-Based S2a interface

The GTP-based S2a interface connects the PGW to a TWAN (trusted non-3GPP network), allowing for both control and user plane signaling. On the control plane, it is used to create, update, and delete EPS bearers. On the user plane, it is used for user data packet transportation. For more information on the GTP-based S2a interface, refer to GTP-Based S2a Interface Description.

S2b Interface

The S2b interface connects the PGW to an ePDG (untrusted WLAN access network), allowing for both control and user plane signaling. For more information on the S2b interface, refer to S2b Interface Description.

S4 interface

The S4 interface connects the SGW to SGSNs, allowing exchange of signaling and user data. The S4 interface is based on the GTPv2-C and GTPv1-U protocol. For more information about the S4 interface, refer to S4 Interface Description.

S5/S8 interface

The S5/S8 interface connects the PGW to SGWs or the SGW to PGWs that are external to the EPG, allowing for both control and user plane signaling. On the control plane, it is used to create, update, and delete EPS bearers. On the user plane, it is used for user data packet transportation. The S5 interface connects to SGWs and PGWs in the same PLMN as the EPG. The S8 interface connects to SGWs and PGWs in other PLMNs, allowing visiting subscribers to be routed through their home PGW. For more information on the S5/S8 interface between the SGW and external PGWs, refer to SGW S5/S8 Interface Description. For more information on the S5/S8 interface between the PGW and external SGWs, refer to PGW S5/S8 Interface Description.

S6b Interface

The S6b interface connects the PGW to a 3GPP AAA server. This interface is used for UE authorization in a non-3GPP network. For more information on the S6b interface, refer to S6b Interface Description.

S6bAuth Interface

The S6b interface connects the PGW to a 3GPP AAA server. This interface is used for UE authorization in the LTE, CDMA, and untrusted WLAN networks. For more information on the S6b interface, refer to S6bAuth Interface Description.

PMIPv6-Based S2a interface

The PMIPv6-based S2a interface connects the PGW to a MAG in a CDMA2000 network (trusted non-3GPP network). This interface transports control data between the PGW and the MAG and sets up a Generic Routing Encapsulation (GRE) tunnel for user data. For more information about the PMIPv6-based S2a interface, refer to PMIPv6-Based S2a Interface Description.

S11 interface

The S11 interface connects the SGW to MMEs. This interface is used for control plane signaling, and to create, update, and delete EPS bearers. The S11 interface is also used for transferring user plane data. For more information on the S11 interface, refer to S11 Interface Description.

S12 interface

The S12 interface connects the SGW to RNCs, allowing for user data packet transportation. For more information on the S12 interface, refer to S1-U and S12 Interface Description.

SGi interface

The SGi interface connects the PGW to external APN networks, allowing exchange of signaling and user data. The SGi interface also connects the PGW to the SASN. If RADIUS is used, the SGi interface connects the PGW to the RADIUS server. For more information on the SGi interface, refer to Gi and SGi Interface Description. SGi interface also connects the PGW to service functions when service chaining is used.

ICAP interface

The ICAP interface connects the PGW to an external content classification engine used to retrieve content categories when content filtering is enabled. For more information on the ICAP interface, refer to ICAP Interface Description.

DNS interface

The DNS interface connects the PGW to a DNS server. This interface is used for DNS procedure in the LTE, CDMA, trusted WLAN, and untrusted WLAN networks. For more information on the DNS interface, refer to DNS Support.

6 EPG Functions

The following sections describe EPG functions, commercially available in basic and optional features. For more information on features, refer to EPG Features.

6.1 Session Management

Session management in the EPG establishes and handles the user sessions between the UE and an APN network, with the help of the SGSN in a GPRS network and the MME in an EPS network. For the GPRS, session management supports PDP context activation, deactivation, and modification. For the EPS, session management supports PDN connection creation, deletion, and modification. These procedures deal with allocation of IP addresses and QoS parameters.

PDP contexts and EPS bearers are set up and controlled through the GPRS Tunneling Protocol (GTP), refer to Tunneling and VPNs. GTP Control (GTP-C) is a tunnel control and management protocol that allows the EPG to provide PDN access for the UE, and is used to create, modify, and delete tunnels.

A user session starts when the UE connects to a PDN and ends when the connection closes. In the GPRS, the user session is realized in the UE, SGSN, RNC, and GGSN or PGW by one or several PDP contexts holding information about the connection. The EPG supports two types of PDP contexts: primary and secondary. A secondary PDP context is associated with a primary PDP context with which it shares IP address and APN. However, the secondary context has a different QoS profile than the primary PDP context. Figure 5 shows a logical view of a PDP session and its PDP contexts.

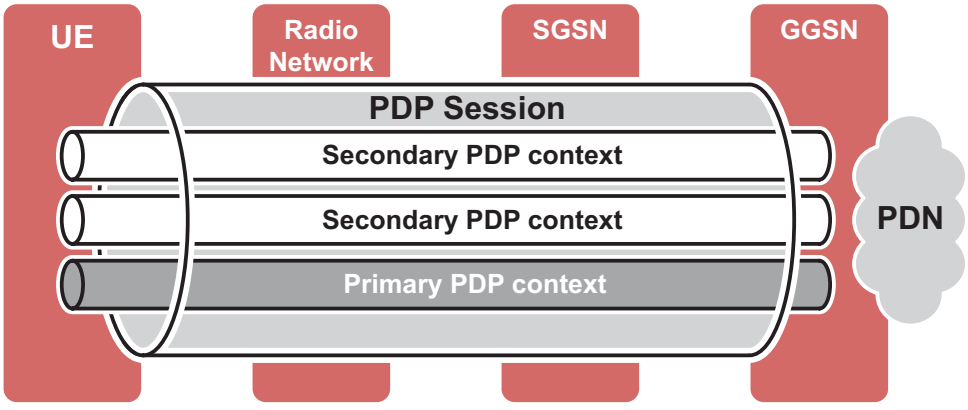

Figure 5 Logical View of a PDP Session

In the EPS, the user session is controlled by the MME and eNodeB but the payload is handled by the SGW and PGW only. The user session is realized in the UE, SGW, and PGW by one or several EPS bearers holding information about the connection. Every dedicated EPS bearer is associated with a default EPS bearer and shares its IP address. Figure 6 shows a logical view of a PDN connection and its EPS bearers.

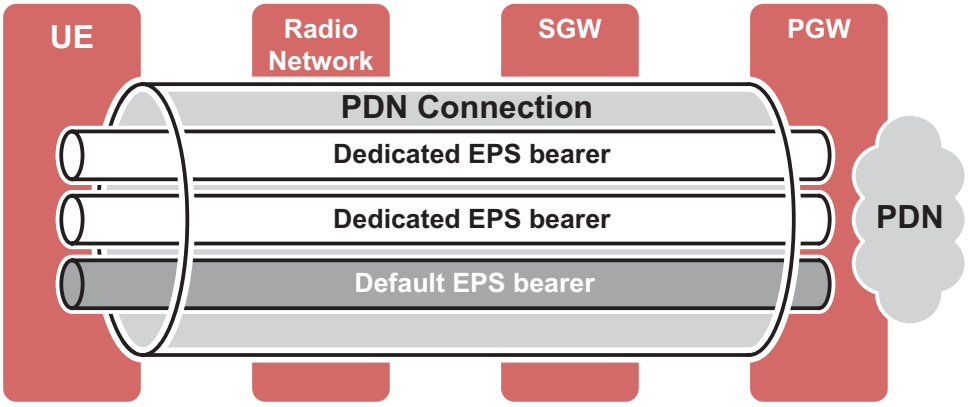

Figure 6 Logical View of a PDN Connection

In the GPRS connected to the EPC, the user session is controlled by the SGSN and RNC. The user session is realized in the UE by one or several PDP contexts holding information about the connection, and in the SGW and PGW by one or several EPS bearers holding information about the connection.

In a trusted non-3GPP network (WLAN), the user session is controlled by the TWAN and realized in the UE, TWAN, and PGW. In an untrusted non-3GPP network (WLAN), the user session is controlled by the ePDG and realized in the UE, ePDG, and PGW. A user session is realized by one default bearer holding information about the connection. Figure 7 shows a logical view of a user session for both access types.

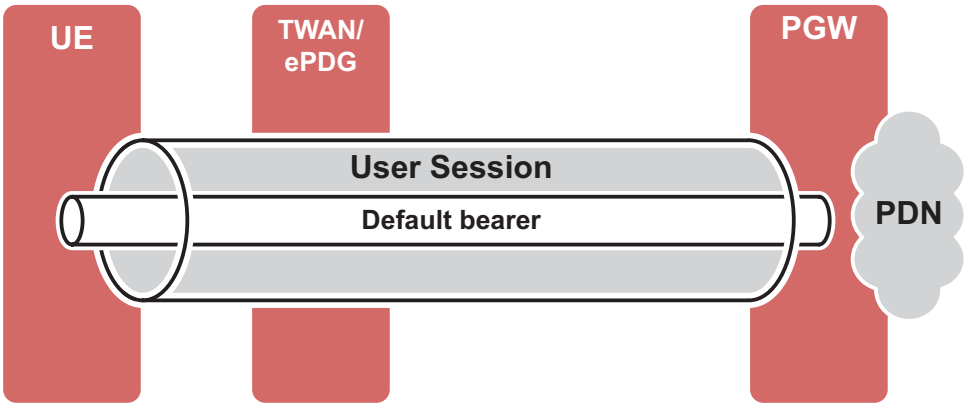

Figure 7 Logical View of a User Session for Trusted/Untrusted Non-3GPP Network Access

The GGSN supports service access through a WLAN and TTG. When a user accesses a service through a WLAN, the TTG assumes the role of the SGSN in the PDP context activation procedure.

The EPG supports access to CDMA2000 networks where the MAG controls PDN connections realized in the UE, MAG, and PGW, as illustrated in Figure 8.

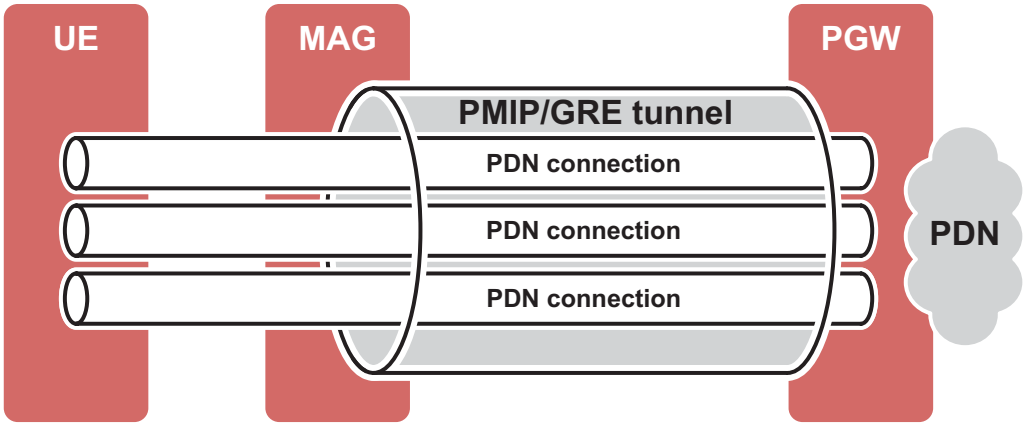

Figure 8 Logical View of PDN Connections over a PMIP/GRE Tunnel

For all network access types, the UE IP address is either public or private. The EPG supports both static and dynamic IP address allocation for IPv4 and IPv6. For more information about IP address allocation, refer to APN Configuration.

For more information about session management, refer to Session Management.

6.2 Quality of Service

The EPG negotiates and enforces QoS per session, per bearer, or both. The EPG supports networking QoS through DiffServ Code Point (DSCP) tagging of outbound IP packets. This is only used if the cloud system supports prioritization or traffic engineering based on the DSCP tag. The EPG also enforces the negotiated bit rates per EPS session, or bearer, or both. In addition, the EPG supports enforcing bit rate limits on individual services on a per user basis.

The EPG supports different mechanisms to control the QoS as part of the negotiation procedure:

— Local configuration based on session parameters

— QoS control over the Gx+ interface

For more information on QoS, refer to Quality of Service on the GGSN and PGW and Quality of Service on the SGW.

6.2.1 HSDPA

Enhanced Downlink, also referred to as High-Speed Downlink Packet Access (HSDPA), allows high bit rates in the downlink direction.

With HSDPA, the EPG can be configured to provide a maximum bit rate of up to 256 Mbit/s in the downlink per bearer. The rate used in transferring data is limited to a licensed downlink maximum. For the current HSDPA license limits, refer to EPG Characteristics.

The EPG uses the HSDPA option if the maximum bandwidth is configured to a value greater than 2 Mbit/s.

6.2.2 Enhanced Uplink

Enhanced uplink, also referred to as High-Speed Uplink Packet Access (HSUPA), allows high bit rates in the uplink direction.

With HSUPA, the EPG can be configured to provide a maximum bit rate of up to 256 Mbit/s in the uplink per bearer. The rate used in transferring data is limited to a licensed HSUPA maximum. For the current HSUPA license limits, refer to EPG Characteristics.

The enhanced uplink option is in operation if the maximum bandwidth is configured to a value greater than 2 Mbit/s.

6.2.3 LTE Uplink and Downlink

LTE is a radio technology that allows high bit rates in both the downlink and uplink direction for an EPS network. For more information on LTE uplink and downlink capacity, refer to EPG Characteristics.

6.3 User Packet Handling

The purpose of user packet handling in the EPG is to transport user packets through the user plane. User packets consist of end-user information and associated data transfer control information. In the GPRS, user packets are transported between the UE, the SGSN or RNC, GGSN, and the PDN. In the EPS, the user packets are transported between the UE, the eNodeB, the SGW and PGW, and the PDN. In the GPRS connected to the EPC, the user packets are transported between the UE, the SGSN using S4 or RNC, the SGW and PGW, and the PDN.

In a trusted non-3GPP network connected to the EPC, the user packets are transported between the UE, the TWAN or CDMA2000 network, the PGW, and the PDN. For PMIPv6 access, a PMIPv6 GRE tunnel for the user packets is created between the UE in the CDMA2000 network and the PGW. In an untrusted non-3GPP network connected to the EPC, the user packets are transported between the UE, the ePDG, the PGW, and the PDN.

Page 17 shows the different scenarios of user packet transfer.

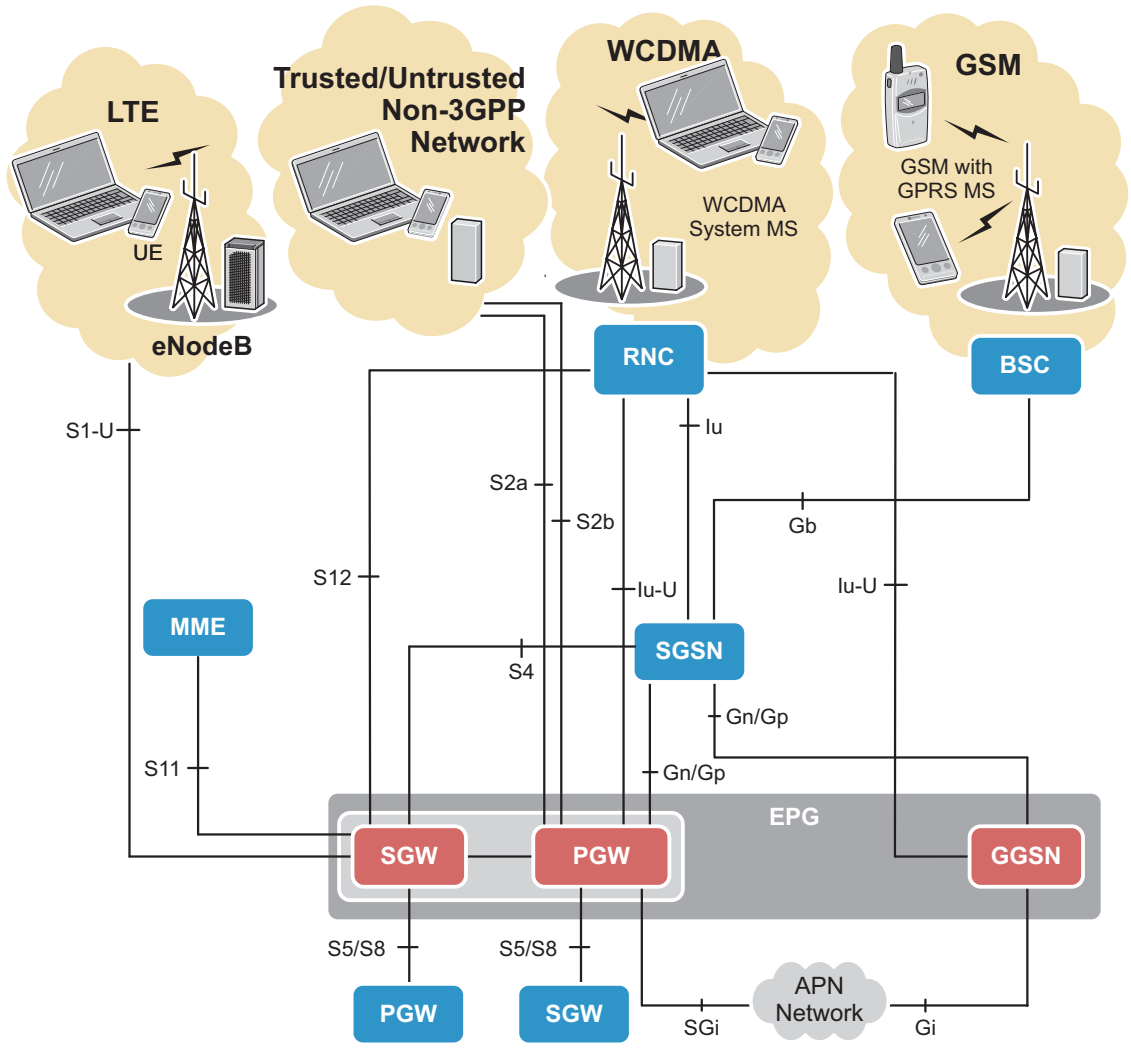

Figure 9 User Packet Transfer and Relevant User Plane Interfaces

The EPG supports IPv4 and IPv6 for end users. For more information about IPv6, refer to IPv6.

To use the uplink and downlink user packet transfer functions provided by the EPG, the UE must be attached and have a PDP context activated while connected to the GPRS. When connected to the EPS, the UE must have an established default EPS bearer.

For more information, refer to User Packet Handling.

6.4 3G Direct Tunnel

The 3G Direct Tunnel (3GDT) feature enables user packets in WCDMA systems to be transported outside the SGSN, directly between the GGSN or PGW and the RNC. Using the direct tunnel function requires proper configuration in the whole

network, including the HLR, SGSN, EPG, Domain Name System (DNS) server, and terminals. For more information on 3GDT, refer to 3G Direct Tunnel.

6.5 RADIUS

RADIUS is an authentication, authorization, and accounting client-server protocol. A RADIUS client, in this case the EPG, passes user information to a RADIUS server in an attached IP network (referred to as an APN network). The server processes user connection requests, authenticates the user, and returns configuration information necessary for the client to deliver service to the user. User passwords sent between the client and server are encrypted with a shared secret key to enhance security.

The EPG can be configured for APNs to interact with a RADIUS server in the following ways:

— Allocate public or private dynamic IP addresses to UE devices if user sessions are activated

— Authenticate UE users if user sessions are activated

— Dynamically create, modify, or terminate a subscriber service

— Provide L2TP parameters

— Select an APN for a user session

If the Routing Behind MS feature is enabled, an IPv4 address range can be provided together with the UE IPv4 address from RADIUS at user session creation. This enables a UE device to act as a router for an IPv4 network behind the UE device. For more information about Routing Behind MS, refer to RADIUS Support.

Note: The Routing Behind MS feature does not support IPv6 addresses.

The EPG can be configured to access either one single RADIUS server at a time, or multiple RADIUS servers using a round-robin method.

For detailed information about RADIUS, refer to RADIUS Support.

6.6 Routing

The main task of the EPG IP routing functions is to support IP addresses that overlap APNs and allow for traffic separation between networks. The basic activities involved in routing are determining the optimal routing paths and transporting packets through the networks.

For more information on routing, refer to Routing.

6.6.1 Aware Policy-Based Routing

The Aware Policy-Based Routing (APR) feature enables the EPG to divide traffic related to one UE device and one APN into several VPNs. The EPG selects the VPN to route traffic to, based on Packet Inspection and Service Classification (PISC) and bearer data. By using APR, it is, for example, possible to control which traffic flows are sent through data compression servers or security gateways. The configuration of the UE is simplified because one APN can be used to access several VPNs in the service or corporate networks of the operator.

For more information, refer to Aware Policy-Based Routing.

6.6.2 Routing Behind MS

The Routing Behind MS feature makes it possible for a UE device to act as a router for an IPv4 network behind the UE device. The feature is configured per APN.

Note: The Routing Behind MS feature does not support IPv6 addresses.

For more information, refer to RADIUS Support.

6.7 Offline Charging

Offline Charging in the EPG enables a Billing System (BS) to charge subscribers for GPRS and EPS data volume, time usage, and events based on charging records generated by the GGSN, PGW, or SGW. The EPG supports charging records in the form of CDRs or Rf ACRs.

The charging records contain usage information related to bearers in the EPG and can be used for non-real-time charging.

For more information, refer to Offline Charging.

6.7.1 CDR-Based Charging

The Charging Support feature enables generation of CDRs for charging of data volume, time usage, and events. Multiple sequential CDRs (partial CDRs) can be generated, for example, for an EPS bearer. CDR generation is supported by all node types and for all access networks supported by the EPG. CDRs can be transferred directly to the BS or through a CGF. The GPRS Tunneling Protocol Prime (GTP') over the Ga interface is used for near-real-time CDR transfer, whereas Secure FTP (SFTP) over the Bp interface is used for less time critical transfer.

Refer to CDR-Based Charging Interface Description for more information about the near-real-time and file-based CDR charging interfaces. For more information about the CDR format, refer to CDR Format for the SGW and CDR Format for the GGSN and PGW.

6.7.2 Rf Charging

The Rf Charging interface feature enables generation of Rf ACRs for charging of data volume. Rf ACRs are generated for PDN Connections, and multiple sequential Rf ACRs (Rf ACR Interims) can be generated for each PDN Connection. The SGW supports Rf ACR generation for LTE access network. The PGW supports Rf ACR generation for LTE and CDMA2000 networks.

Rf ACRs are transferred directly to a CDF using the Diameter-based Rf protocol.

Refer to PGW Rf Interface Description and SGW Rf Interface Description for more information about the interface, and detailed information about the structure of Rf messages. For more information about the ACR format, refer to ACR Format.

Rf charging can operate in a tight interworking with online charging. For more information, refer to Offline Charging.

6.8 Service Aware Charging and Control

SACC is a network solution allowing flexible charging and control of UE IP flows for bearers. The SACC solution enables, for example, authorization and policy control, bandwidth control, traffic redirection, and online and offline charging of individual services based on PISC.

Using separate APNs to differentiate between different services has disadvantages, due to the need to configure APN information both in the UE and the network, and also due to the need to handle several IP addresses in the UE. With SACC, it is possible to use a single APN for multiple end-user services. That is, operators can differentiate the bearer charging based on the services accessed by the bearers.

The SACC solution includes the following:

— PISC, which provides:

  - IP header inspection
  - Application layer inspection of, for example, Hypertext Transfer Protocol (HTTP) headers
  - Heuristic inspection of proprietary protocols, such as Peer-to-Peer (P2P) file sharing protocols

— Charging based on volume consumed, time used, and application-layer protocol events

— Online credit control of services

— Dynamic service authorization and policy control

— Automatic traffic redirection of unauthorized services

— Full support for offline charging for services through CDRs

— APR

— Gx+ Initiated QoS Modification

For more information on SACC, refer to SACC Overview.

6.9 PGW Pause Charging

PGW pause charging enables the SGW to notify the PGW, on a per PDN connection basis, to temporarily pause charging. Pause charging occurs when the UE is idle and the SGW has started to drop downlink user packets, resulting in the configured packets or bytes threshold being exceeded. When the UE is active again the SGW notifies the PGW to resume charging.

For more information on PGW pause charging, refer to Session Management.

For information on configuring PGW pause charging attributes, refer to PGW Pause Charging Configuration.

6.10 Tunneling

Generic tunneling in an IP network uses an extension of the existing mechanism of packet encapsulation to add another layer to the information being relayed. The packet contains the IP addresses of the source and destination client and server in its header fields.

Tunneling allows routers to use another set of source and destination IP addresses that remain transparent to end users. With tunneling, a packet can retain its original IP address and still be routed transparently across several nodes in the network using a separate set of IP addresses.

For more information on tunneling, refer to Tunneling and VPNs.

L2TP is a standard method for tunneling Point-to-Point Protocol (PPP). L2TP operates between two L2TP Control Connection Endpoints (LCCEs), tunneling traffic across a packet network.

The L2TP in the EPG uses the L2TP Access Concentrator (LAC)-L2TP Network Server (LNS) tunneling model where the EPG acts as an LAC and emulates a PPP connection from the radio network side, even though no PPP session is established between the remote system and the LAC inside the EPG.

Since the EPG also has a PPP client to provide PPP emulation, it supports UE devices sending IP packets (PDP type IP and not PPP packets), for encapsulation.

For more information, refer to Layer Two Tunneling Protocol (L2TP).

6.11 Security

The EPG provides four main mechanisms for perimeter defense:

Network Separation
Network separation is based on VPNs.

IP Packet Filtering
IP packet filtering allows only certain types of traffic over individual interfaces.

Tunneling Tunneling provides separation of traffic flows, encrypted and authenticated through SFTP over Bp

User Access Control
The EPG ensures that only authorized users have access.

It is possible to block sessions from an IP address to prevent Denial of Service (DoS) attacks, for example, if the number of sessions exceeds a configured limit. The EPG also provides surveillance mechanisms like counters, alarms, and logging.

For more information on security, refer to Security.

6.12 Resilience

The EPG is designed for high levels of service resilience and availability.

The following subsections describe ways of achieving resilience on the EPG application level.

6.12.1 Session-based N+1 Session Resilience

Session-based N+1 session resilience enables boards to provide session continuity in the event of a failure of one board. Session-based N+1 session resilience is achieved as a result of session data replication between active and standby sessions running on all available boards.

For more information on session-based N+1 session resilience, refer to Resilience.

6.12.2 Scalable Routing Redundancy

Scalable routing redundancy provides routing redundancy for an APN through a pair of GGSNs or a pair of PGWs. The GGSN or PGW reroutes packets received from an external PDN network through the outbound routing instance to a redundant node if the GGSN or PGW cannot find a related bearer.

Upon reception of a rerouted packet from the redundant node through the inbound routing instance, the GGSN or PGW sends the packet towards the UE, if the packet can be associated with a bearer. Otherwise, the rerouted packet is discarded.

For more information, refer to Scalable Routing Redundancy.

6.12.3 Scaling Operations

Support for scaling operations allows operators to increase the node capacity during runtime by adding new vSFOs, one at a time, without stopping and starting the EPG applications. During scaling operations, the characteristics are different depending on the node deployment type.

For more information on scaling operations, refer to Resilience and Scaling the EPG.

6.12.4 Auto-Healing

The virtual EPG supports auto-healing. If a VM fails, the virtual EPG does not request a replacement VM from the cloud system. The cloud system should instead strive to keep the already started VMs available, by automatically re-creating any failed VM. For example, if a compute host is lost or fails, the cloud system automatically evacuates the VMs on that particular compute host to another compute host. Such auto-healing functionality in the cloud system is recommended so that the virtual EPG quickly regains full capacity and full redundancy.

Note: The virtual EPG resilience mechanisms do not depend on auto-healing in the cloud system.

For more information on resilience, refer to Resilience.

6.13 Inter-Chassis Redundancy

Inter-Chassis Redundancy (ICR) improves the EPG availability by having a standby EPG ready for operation in case of a failure impacting the active EPG, such as a link failure.

ICR improves the in-service performance and minimizes the impact of an EPG failure. Disaster recovery is facilitated by having two EPGs configured as a mated pair in two different chassis situated in geographically separated areas. The two EPGs are considered as one by the surrounding network, and traffic is always handled only by the active EPG.

ICR can handle multiple ICR switchovers without the need for operator intervention.

The EPG can be configured for automatic fallback. This means that after a switchover caused by a failure, the EPG can do an automatic switchover.

Automatic fallback initiates a switchover, making the EPG configured as the preferred active EPG to become the active EPG again.

Note: ICR is supported for EPGs for the following deployment types:

- Standalone SGW
- Standalone PGW
- Combined SGW and PGW
- Standalone GGSN

For more information on ICR, refer to Inter-Chassis Redundancy.

6.14 Event-Based Monitoring

Event-Based Monitoring (EBM) enables the EPG to record event information in a formatted report. The formatted event report is streamed in real-time or near-real-time to an external post-processing system.

For more information on EBM, refer to Event-Based Monitoring.

6.15 Content Filtering

Content filtering enables the EPG to control access to web resources based on content categories or locally configured pass, block, and redirect lists.

For more information on content filtering, refer to Content Filtering.

6.16 UE Trace

The UE Trace feature allows the EPG to record detailed information about signaling information that it sends out, and payload. UE Trace is used for troubleshooting, monitoring, and optimization operations. It can be used separately on the control plane and user plane for one or more selected UE devices. The network operator identifies the selected UE device using the International Mobile Subscriber Identity (IMSI).

For more information on UE Trace, refer to UE Trace.

For more information on UE Trace log files, refer to UE Trace Log.

For more information on how to convert log files to plain text or PCAP format for UE Trace on Control Plane, refer to Toolbox Description.

6.17 Integrated Traffic Capture

Integrated Traffic Capture (ITC) is used to capture control plane traffic on all Control Processing Board (CPBs) and user plane traffic on all Packet Processing Boards (PPBs) simultaneously. ITC is used directly in the EPG without the need of external probes. The traffic is captured in ITC files in a Packet Capture (PCAP) format. The ITC files are used for troubleshooting connectivity issues.

For more information on ITC, refer to Integrated Traffic Capture.

6.18 TWAMP

The EPG supports Two-Way Active Measurement Protocol (TWAMP) light at application level for S5/S8-U interfaces in PGW and for S5-U, S8-U, and S5/S8-U interfaces in SGW for measuring and validating Service Level Agreement (SLA).

The EPG acts as light TWAMP responder, which means that TWAMP-Test packets are directly exchanged between TWAMP initiator and TWAMP responder without using TWAMP-Control procedures. The EPG supports TWAMP responder with unauthenticated mode.

For more information, refer to TWAMP.

6.19 Service Chaining

The Service Chaining feature enables the EPG to steer subscriber traffic to third party service functions in the (S)Gi-LAN.

The EPG selects the service chain, which consists of an ordered list of service functions, using the predefined or dynamic PCC rules. By using service chaining, EPG, for example, can control which traffic flows are sent through video optimizators or an MSP.

For more information, refer to Service Chaining.

7 EPG Operation and Maintenance

For information on EPG operation and maintenance, refer to Operation and Maintenance Description.

8 CPI

The CPI library is available through the Ericsson CPI extranet (provided that an e-business portal is available). The CPI library contains both descriptive documents and instructions for operation and maintenance. For more information, refer to CPI Library Description.

Reference List

IETF Standards

[1] RFC 1213, Management Information Base for Network Management of TCP/IP-based internets: MIB-II, RFC 1213

[2] RFC 1215, A Convention for Defining Traps for use with the SNMP, RFC 1215