ERICSSON

Tunneling and VPNs

TECHNICAL PRODUCT DESCRIPTION

12/221 02-AXB 250 10/4-V3 Uen BC

Contents

1	**Introduction**	**1**
1.1	Scope	1
1.2	Target Groups	1
2	**Overview**	**1**
2.1	Tunneling Protocols	1
2.2	VPNs	2
3	**GTP Overview**	**3**
3.1	GTP Subprotocols	3
3.2	GTP-C and GTP-U	4
3.3	GTP Protocol Stack	5
4	**VPNs**	**9**
4.1	APN Network VPN	9
4.2	GTP' VPN	10
4.3	EPG Interfaces and Contexts	10
5	**Supported VPN Interface Types**	**11**
6	**Counters**	**11**
Reference List		**13**

1 Introduction

This document describes tunneling and Virtual Private Networks (VPNs) in the EPG for GSM, WCMDA, LTE, trusted non-3GPP network, and untrusted non-3GPP network.

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. With tunneling, EPG can use another layer of source and destination IP addresses that remain transparent to UE. The transferred data packet can then retain its original IP address and still be routed transparently using a separate set of IP addresses.

In EPG context, a VPN is an IP-based network that uses tunneling and allows other networks with overlapping IP address spaces to coexist on a shared network topology.

1.1 Scope

The document covers an overview presenting the context of tunneling and VPNs in the EPG, a description of the GPRS Tunneling Protocol (GTP), and a description of VPN routing. The document also provides examples of supported VPN types.

1.2 Target Groups

This document is intended as an introduction to tunneling and VPNs 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 Overview

The following sections provide a brief overview of tunneling and VPN concepts.

2.1 Tunneling Protocols

Tunneling protocols commonly add special protocol headers to routed packets at the start and end points of the tunneling. The headers carry additional information concerning the tunnel, such as a tunnel identifier. Tunnels can also create embedded routing domains inside other routing domains.

GTP is the GPRS Tunneling Protocol on the Gn interface between the GGSN and SGSN. In EPS networks, GTP is the tunneling protocol on the S5/S8 interface between the PGW and SGW, on the S11 interface between the SGW and the MME, on the S4 interface between the SGW and the SGSN, on the S12 interface between the SGW and the RNC, on the GTP-based S2a interface between the PGW and the Trusted WLAN Access Network (TWAN), on the S2b interface between the PGW and the Evolved Packet Data Gateway (ePDG), and on the S1-U interface between the SGW and the eNodeB.

For traffic to Access Point Name (APN) networks on the Gi/SGi interface, several tunneling protocols can be used to encapsulate the IP traffic. For more information, refer toSection 5 on page 10 .

2.2 VPNs

A VPN consists of two interconnected network areas: the provider's network and the customer's network. The provider's network consists of routers that provide VPN services to a customer's network and routers that provide other services. The customer's network is commonly located at multiple physical sites and is also private (non-Internet).

Note: For some applications, a complete VPN can also reside entirely within a provider's network.

To ensure that VPNs remain private and isolated from other VPNs and from the public Internet, the provider's network maintains policies that keep routing information from different VPNs separate. A customer site can belong to multiple VPNs as long as it keeps routes from the different VPNs separate.

VPNs typically include the following types of network devices:

— Provider Edge (PE) routers

  Routers in the provider's network that connect to customer edge devices at customer sites.

— Provider (P) routers

  Transit router of the core network.

— Customer Edge (CE) devices

  Router at the customer premises that is connected to the PE of a service provider IP/MPLS network. CE peers with the PE and exchanges routes with the corresponding VRF inside the PE.

The EPG configuration can include VPNs, which allows it to act as a VPN PE router toward the connected APN networks and optionally toward the Gn/S5 network. For more information on other VPNs that can be configured on the EPG, refer to Routing.

VPNs allow connected APN networks to manage their own IP address space and routing tables using IP routing protocols. Regardless of the role of the EPG in a VPN, the VPNs used do not provide any privacy or security guarantees for the network devices or customer traffic.

3 GTP Overview

In GPRS, the tunneling protocol GTP can be used to tunnel packets between the WCDMA Terrestrial Radio Access Network (RAN) and the SGSN, and between the SGSN and GGSN on the Gn interface. Alternatively, packets can be tunneled directly between the WCDMA RAN and the GGSN. In mobile networks, tunneling with GTP provides transparent routing within the GPRS core. GTP is not used between the UE and the radio network, or between the GGSN and the Internet or private IP network.

In EPS, GTP can be used to tunnel packets between the eNodeB and the SGW on the S1-U interface and between the SGW and the PGW on the S5/S8 interface. In GPRS access connected to EPC, GTP can be used to tunnel packets between the SGSN and the SGW on the S4 interface or between the RNC and the SGW on the S12 interface, and between the SGW and the PGW on the S5/S8 interface. In trusted non-3GPP access connected to EPC, GTP can be used to tunnel packets between the PGW and the TWAN on the GTP-based S2a interface. In untrusted non-3GPP access connected to EPC, GTP can be used to tunnel packets between the PGW and the ePDG on the S2b interface. GTP-Control plane (GTP-C) is used for control plane signalling between the SGW and the MME through the S11 interface, between the PGW and the TWAN on the GTP-based S2a interface, between the PGW and the ePDG on the S2b interface, and between the SGW and the SGSN through the S4 interface. GTP is not used between the UE and the eNodeB/RNC/TWAN/ePDG, or between the PGW and the Internet or private IP network.

3.1 GTP Subprotocols

GTP includes two subprotocols:

GPRS Tunneling Protocol Control (GTP-C)
: Creates, modifies, and deletes tunnels and exchanges other control signalling information.

GPRS Tunneling Protocol User (GTP-U)
: Encapsulates and carries bearer traffic on the user plane.

Note: The EPG also supports GTP Prime (GTP') over the Ga interface. For more information, refer to CDR-Based Charging Interface Description.

3.2 GTP-C and GTP-U

GTP-C sets up and maintains the tunnels for the GTP-U packets carrying user data. The tunnels are set up between the GGSN using Gn interface, the SGSN, and the WCDMA RAN using the Gn interface. In EPS, the tunnels are set up on the S4, S5/S8, S11, S12, GTP-based S2a, S2b, and S1-U interfaces.

At the endpoints of the GTP tunnels, a GTP header is placed on the Layer 3 (L3) packet or Layer 2 (L2) frame sent from a UE device to another device in an IP network. The inner Packet Data Protocol (PDP) Protocol Data Unit (PDU) is placed inside a connectionless User Datagram Protocol (UDP) segment and then inside the outer IP packet. The outer Layer 3 packet is then sent inside another Ethernet frame, a Layer 2 frame, or any other network frame structure.

The IP addresses found in the outer IP packet header sent are those of the GTP tunnel endpoints. The inner IP packet sent between the UE and an IP network uses the IP address of the UE and the IP network device. The GTP-U header identifies the tunnel and carries additional information about the PDP PDU carrying the application payload.

Figure 1 shows the encapsulation sequence at the GTP-U tunnel endpoint and the relationship between headers and addresses.

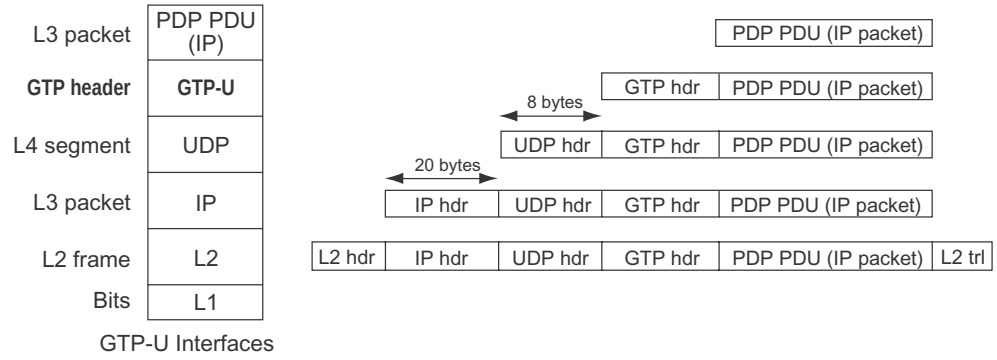

Figure 1 GTP-U Headers and Addresses

The application payload inside the PDP PDU receives an IP header from the UE and forms a complete inner Layer 3 IP packet. The SGSN or RNC in the case of 3G Direct Tunnel (3GDT) and SGW add a GTP-U header, a UDP header (forming a Layer 4 segment), another IP header and address pair for the tunnel endpoints (forming the outer Layer 3 packet), and a Layer 2 frame header and trailer.

The GGSN or PGW terminates the GTP-U tunnel, processes the GTP header, and routes the inner packet to the proper APN network over the Gi/SGi interface.

Many of the specifics for the packet handling between the SGSN, SGW, (RNC in the case of 3GDT), GGSN, TWAN, ePDG, and PGW are determined by the PDP context or EPS bearer for the particular packet flow. For more information, refer to Session Management.

3.3 GTP Protocol Stack

The GTP protocol stack used in GPRS (WCDMA) when packets are tunneled through the SGSN using Gn interface, is shown in Figure 2. If packets are tunneled directly between the WCDMA RAN and the GGSN, Figure 3 shows the GTP protocol stack. The dashed lines mark standard architectural interfaces.

GTP can be used over the Gn interface (or directly between the WCDMA RAN and the GGSN in case of 3G Direct Tunnel) for the user plane for packet-switched services (Iu-PS), but not the Gi and Uu interfaces. The application payload from the UE can be placed inside an IP packet, Point-to-Point Protocol (PPP) frame, or even another type of PDU.

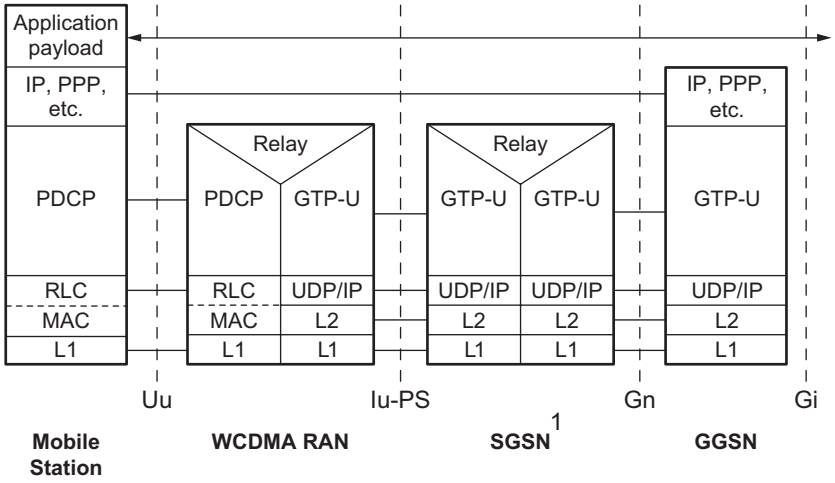

Figure 2 GTP Protocol Stack in WCDMA

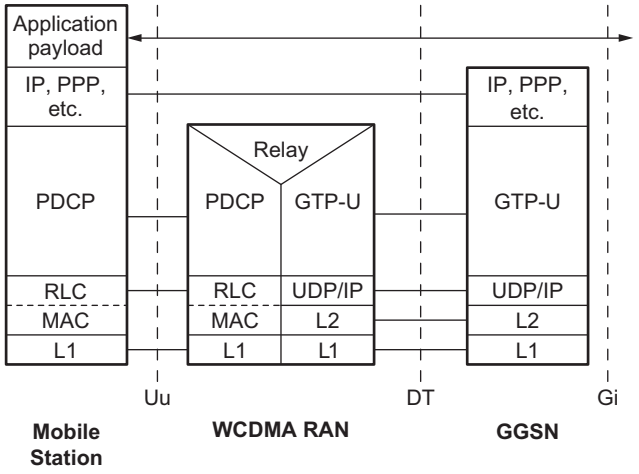

Figure 3 GTP Protocol Stack in WCDMA with the use of 3G Direct Tunnel

The packet is given Packet Data Convergence Protocol (PDCP) and Radio Link Controller (RLC) headers, placed in a Media Access Control (MAC) frame for the air interface employed, and sent as a Layer 1 (L1) bit stream to the WCDMA RAN. The WCDMA RAN performs no routing, simply relaying the contents onto the GTP-U tunnel to the SGSN (or directly to the GGSN in case of 3G Direct Tunnel) using the proper GTP-U header, a UDP segment, and an outer IP packet header over the interface to the SGSN or directly to the GGSN in case of 3G Direct Tunnel (Figure 3). If the packets are tunneled through the SGSN the SGSN relays the GTP-U packet onto the tunnel to the GGSN, using the appropriate Layer 2 frame, otherwise the WCDMA RAN relays the GTP-U packet.

The GTP protocol stack used in EPS (LTE) when packets are tunneled through the SGW, is shown in Figure 4. The dashed lines mark standard architectural interfaces.

GTP can be used over the S5/S8 interface for the user plane for packet-switched services, but not the SGi and LTE-Uu interfaces. The application payload from the UE can be placed inside an IP packet, PPP frame, or even another type of PDU.

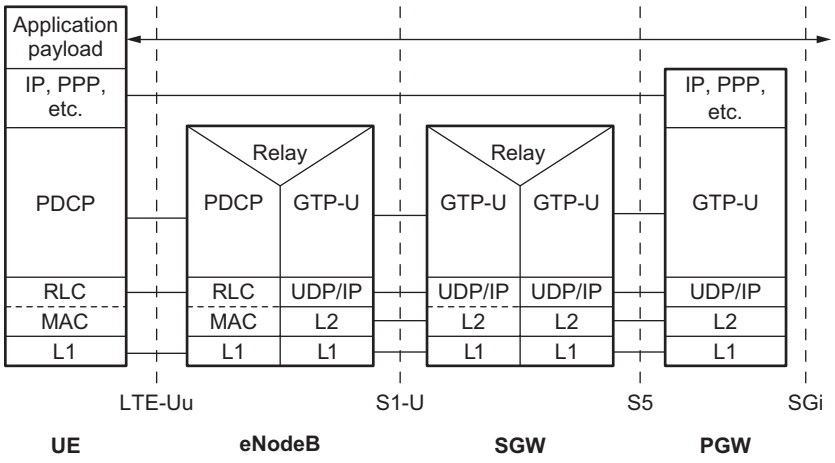

Figure 4 GTP Protocol Stack in LTE

The packet is given Packet Data Convergence Protocol (PDCP) and Radio Link Controller (RLC) headers, placed in a Media Access Control (MAC) frame for the air interface employed, and sent as a Layer 1 (L1) bit stream to the eNodeB. The eNodeB performs no routing, simply relaying the contents onto the GTP-U tunnel to the SGW using the proper GTP-U header, a UDP segment, and an outer IP packet header over the interface to the SGW. If the packets are tunneled through the SGW, the SGW relays the GTP-U packet onto the tunnel to the PGW, using the appropriate Layer 2 frame, otherwise the eNodeB relays the GTP-U packet.

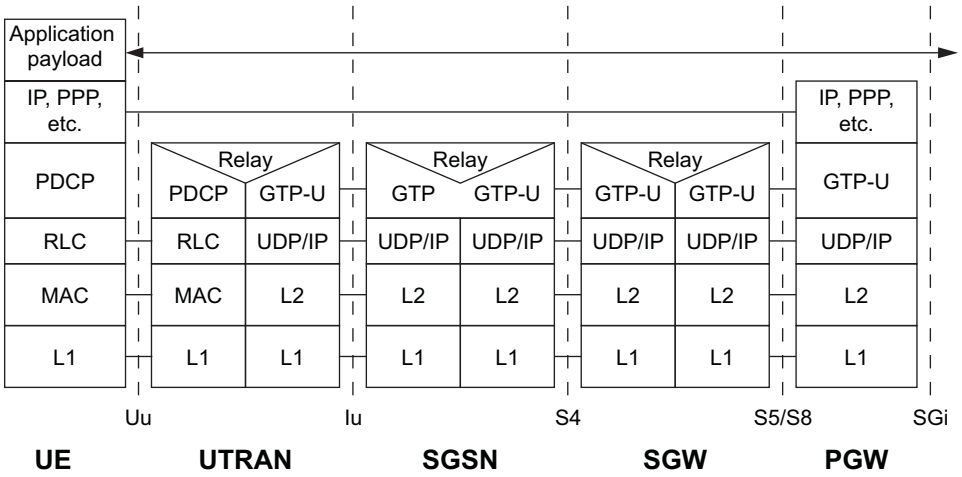

Figure 5 GTP Protocol Stack for WCDMA Access Connected to EPC without Direct Tunnel

The GTP protocol stack used for WCDMA access in EPC when packets are tunneled through the SGW, is shown in Figure 5. The dashed lines mark standard architectural interfaces.

The packet is given Packet Data Convergence Protocol (PDCP) and Radio Link Controller (RLC) headers, placed in a Media Access Control (MAC) frame for the air interface employed, and sent as a Layer 1 (L1) bit stream to the UTRAN. The UTRAN performs no routing, simply relaying the contents onto the GTP-U tunnel to the SGSN using the proper GTP-U header, a UDP segment, and an outer IP packet header over the interface to the SGSN. The SGSN relays the GTP-U packet onto the tunnel to the SGW, using the appropriate Layer 2 frame, otherwise the UTRAN relays the GTP-U packet.

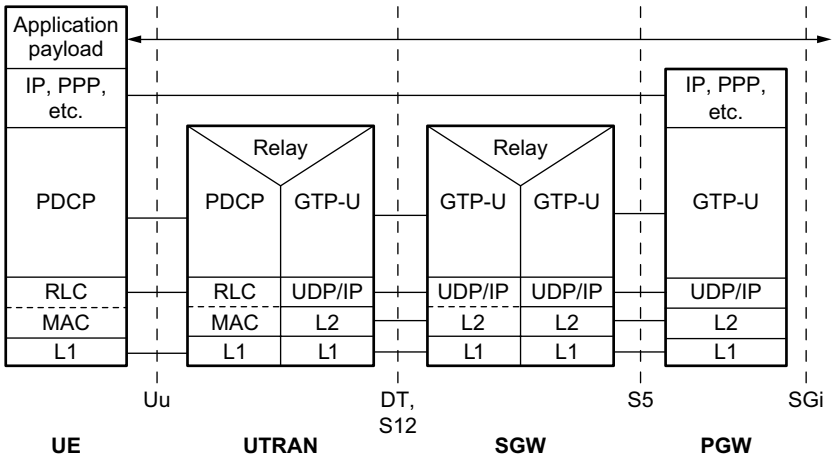

Figure 6 GTP Protocol Stack for WCDMA Access Connected to EPC with Direct Tunnel (S12)

The GTP protocol stack used for WCDMA access in EPC, when packets are in the direct tunnel mode, is shown in Figure 6. The dashed lines mark standard architectural interfaces

The packet is given Packet Data Convergence Protocol (PDCP) and Radio Link Controller (RLC) headers, placed in a Media Access Control (MAC) frame for the air interface employed, and sent as a Layer 1 (L1) bit stream to the UTRAN. The UTRAN performs no routing, simply relaying the contents onto the GTP-U tunnel to the SGW using the proper GTP-U header, a UDP segment, and an outer IP packet header over the interface to the SGW. The SGW relays the GTP-U packet onto the tunnel to the PGW, using the appropriate Layer 2 frame, otherwise the UTRAN relays the GTP-U packet.

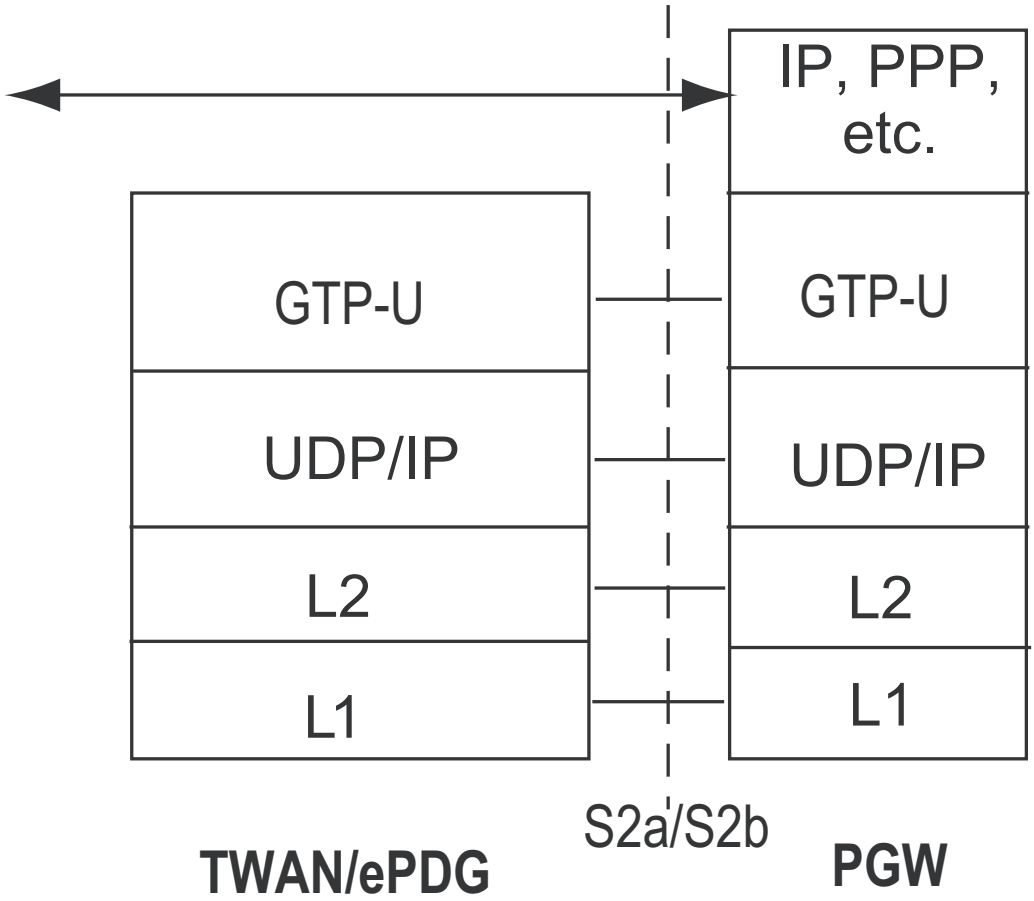

Figure 7 GTP Protocol Stack for Trusted/Untrusted Non-3GPP Accesses Connected to EPC

The GTP protocol stack used for the trusted or untrusted non-3GPP access in EPC, when packets are tunneled through the PGW, is shown in Figure 7. The dashed lines mark standard architectural interfaces.

GTP can be used over the GTP-based S2a and S2b interfaces for the user plane for packet-switched services. The application payload from the UE can be placed inside an IP packet, PPP frame, or even another type of PDU.

Figure 2 to Figure 7 show the GGSN, RNC, TWAN, ePDG, and PGW as the endpoints of the GTP-U tunnel, but do not show the additional routing done to forward the inner packet with the application payload over the Gi or SGi interface to the Packet Data Network (PDN).

When an uplink packet arrives, the EPG performs IP address verification to prevent spoofing. It first examines the IP source address of the packet, then matches it to the address of the PDP context or EPS bearer of the packet and finally verifies the IP address of the SGSN, TWAN, ePDG or SGW. If an address discrepancy is detected, the EPG drops the packet to prevent UE from sending packets with spoofed IP addresses into the IP network.

4 VPNs

An EPG VPN can be configured to include such network devices as EPG boards, Dynamic Host Configuration Protocol (DHCP) servers, and RADIUS servers to support APN networks with overlapping IP address spaces. An APN network VPN can support one or several APNs.

Note: Only one APN per VPN is allowed when the network is configured with the RADIUS attribute Framed-IP-Netmask.

EPG boards and charging gateway servers can be included in a VPN configured to support GTP'.

Note: The EPG can be configured for several VPNs on the Gi/SGi interface but only uses one each on the Gn, S5, GTP-based S2a, S2b, and Gom interfaces.

VPNs used by the EPG employ non-local contexts to separate traffic to allow APNs to use overlapping or duplicate IP address spaces. For more information about VPNs and contexts, refer to Routing.

4.1 APN Network VPN

Any APN network using private IP addresses should be supported by a VPN, which allows the APN network to manage its own IP address space and routing tables. Configuring a minimum number of VPNs can simplify configuration and management.

An APN network VPN can support IP subnetworks. For example, an APN network VPN might have two subnets, one for EPG boards and the other for UE devices.

Note: The following example is only used for explanatory purposes and is not to be used as a recommendation for an actual network setup.

This example describes example configurations for an EPG that is supporting APNs for five clients: First Company, Second Company, Third Company, Fourth Company, and Fifth Company. Both First Company and Fourth Company are using private IP addresses. APN networks that use public IP addresses can be associated with the local context, as shown in Table 1.

Table 1 Example of Routing Instances and APN Networks

Client	APN Network	Example Configuration
First Company	first_company	Non-local context (context-1)
Second Company	second_company_a	Local context
Second Company	second_company_b	Local context
Third Company	third_company	Local context
Fourth Company	fourth_company_a	Non-local context (context-4)
Fourth Company	fourth_company_b	Non-local context (context-4)
Fourth Company	fourth_company_c	Non-local context (context-4)
Fifth Company	fifth_company	Local context

Note: Multiple APN networks can use the same context as shown in the table.

4.2 GTP' VPN

When GTP' is the delivery method for the Charging Data Record (CDR), a VPN to support GTP' should be used. The VPN includes all the EPG boards and the charging gateway server. For more information, refer to CDR-Based Charging Interface Description.

4.3 EPG Interfaces and Contexts

For more information on EPG interfaces, refer to EPG Technical Product Description Overview.

For information on what interfaces that can use the local context or VPNs, refer to Routing or Traffic Separation Configuration.

5 Supported VPN Interface Types

Table 2 shows the supported VPN interface types that can be associated with a context in the EPG.

Table 2 VPN Interface Types

VPN Interface Type	Layer Type
GRE Tunnel	L3
MPLS Label Switched Paths (LSP) (IETF RFC2547)	L3
Ethernet Virtual Local Area Network (VLAN)	L2
Layer 2 Tunneling Protocol (L2TP)(1)	L2

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

6 Counters

For information on counters related to tunneling and VPN, refer to Counters and Gauges for the SGW and Counters and Gauges for the GGSN and PGW.

Reference List

Standards

[1] BGP/MPLS VPNs, IETF RFC2547