Wireless Service Provider Solutions

GPRS Overview

PE/DCL/DD/0117 13.01/EN Preliminary July 2001
411–9001–117

NORTEL NETWORKS™

Wireless Service Provider Solutions

GPRS Overview

Document number:	PE/DCL/DD/0117 411–9001–117
Document status:	Preliminary
Document issue:	13.01/EN
Product release:	GSM/BSS V13
Date:	July 2001

Printed in France

NORTEL NETWORKS CONFIDENTIAL:

The information contained in this document is the property of Nortel Networks. Except as specifically authorized in writing by Nortel Networks, the holder of this document shall keep the information contained herein confidential and shall protect same in whole or in part from disclosure and dissemination to third parties and use for evaluation, operation and maintenance purposes only.

You may not reproduce, represent, or download through any means, the information contained herein in any way or in any form without prior written consent of Nortel Networks.

PUBLICATION HISTORY

System release: GSM/BSS V13

July 2001

Issue 13.01/EN Preliminary

Minor editorial update

System release: GSM/BSS V12

May 2001

Issue 12.09/EN Preliminary

Update according to the review report: PE/DCL/GES/0188 V01.02/FR.

February 2001

Issue 12.08/EN Draft

The following changes were made throughout the document:

- updated the manual for V12 system release
- Chapter 1 and Chapter 7, integrated Ga and Gd interfaces

September 2000

Issue 12.07/EN Standard

Update after internal review.

June 2000

Issue 12.06/EN Preliminary

Minor correction.

April 2000

Issue 12.05/EN Preliminary

Minor correction.

February 2000

Issue 12.04/EN Preliminary

Update according to the review report: PE/DCL/GES/0188 V01.01/FR.

January 2000

Issue 12.03/EN Draft

Update.

November 1999

Issue 12.02/EN Draft

Update.

September 1999

Issue 12.01/EN Draft

Creation.

ABOUT THIS DOCUMENT

This document presents the Base Station Subsystem (BSS) and Core Network architecture of a GPRS network.

Applicability

As the basis of the BSS and Core Network documentation, it briefly describes all the GPRS network elements for the V13 system release (BSS).

Audience

This document assumes that the reader has knowledge of the GSM system. It is intended for operations, maintenance, and other personnel who want to have an overview of the GPRS system.

Prerequisites

For more detailed information about BSS and Core Network components, refer to the NTPs listed below.

< 00 >	:	BSS Product Documentation Overview
< 01 >	:	BSS Overview
< 91 >	:	PCUSN Reference Manual

411–5201–500	GSM Passport Manager User Guide
411–5221–110	SGNS Parameters Reference Manual
411–5221–201	GSM Specifications for NSS Components of GPRS System Conformance Guide
411–5221–925	Gateway GPRS Support Node
411–5221–955	Passeport 15000–VSS with SGSN Functionality User Guide
411–5221–975	SS7/IP Gateway

Related Documents

The NTPs listed in the above paragraph are quoted in the document.

How this document is organized

This document describes the GPRS system overview and contains the following chapters:

- Chapter 1: Overview (General presentation)
- Chapter 2: PCUSN
- Chapter 3: SGSN
- Chapter 4: GGSN
- Chapter 5: SIG
- Chapter 6: OAM
- Chapter 7: Interfaces
- Chapter 8: Channels

Vocabulary conventions

The glossary is included in the NTP < 00 >.

1 OVERVIEW

1.1 GPRS functional overview

The General Packet Radio Service (GPRS) is a wireless packet data service that is an extension of the GSM network (see *Figure 1–1*). It provides an efficient method to transfer data by optimizing the use of network resources. The GPRS radio resources allocator is used to provide multiple radio channels to only one user in order to reach a high data user rate. Furthermore, one radio channel can be shared by multiple users in order to optimize the radio resources. So, the GPRS enables a high spectrum efficiency by sharing time slots between different users, supporting data rates up to 170 kbit/s and providing very low call set-up time (see *Figure 1–2*).

Additionally, GPRS offers direct Internet Protocol (IP) connectivity in a point-to-point or a point-to-multipoint mode and provides packet radio access to external packet data networks (PDN).

GPRS introduces a minimum impact on the BSS infrastructure and no new physical radio interface. The Nortel Networks GPRS network architecture is implemented on the existing wireless infrastructure with the inclusion of the following network entities:

- On the BSS side:
  - Packet Control Unit Support Node (PCUSN)
- On the Core Network side:
  - Serving GPRS Support Node (SGSN)
  - Gateway GPRS Support Node (GGSN)
  - SS7/IP Gateway (SIG)

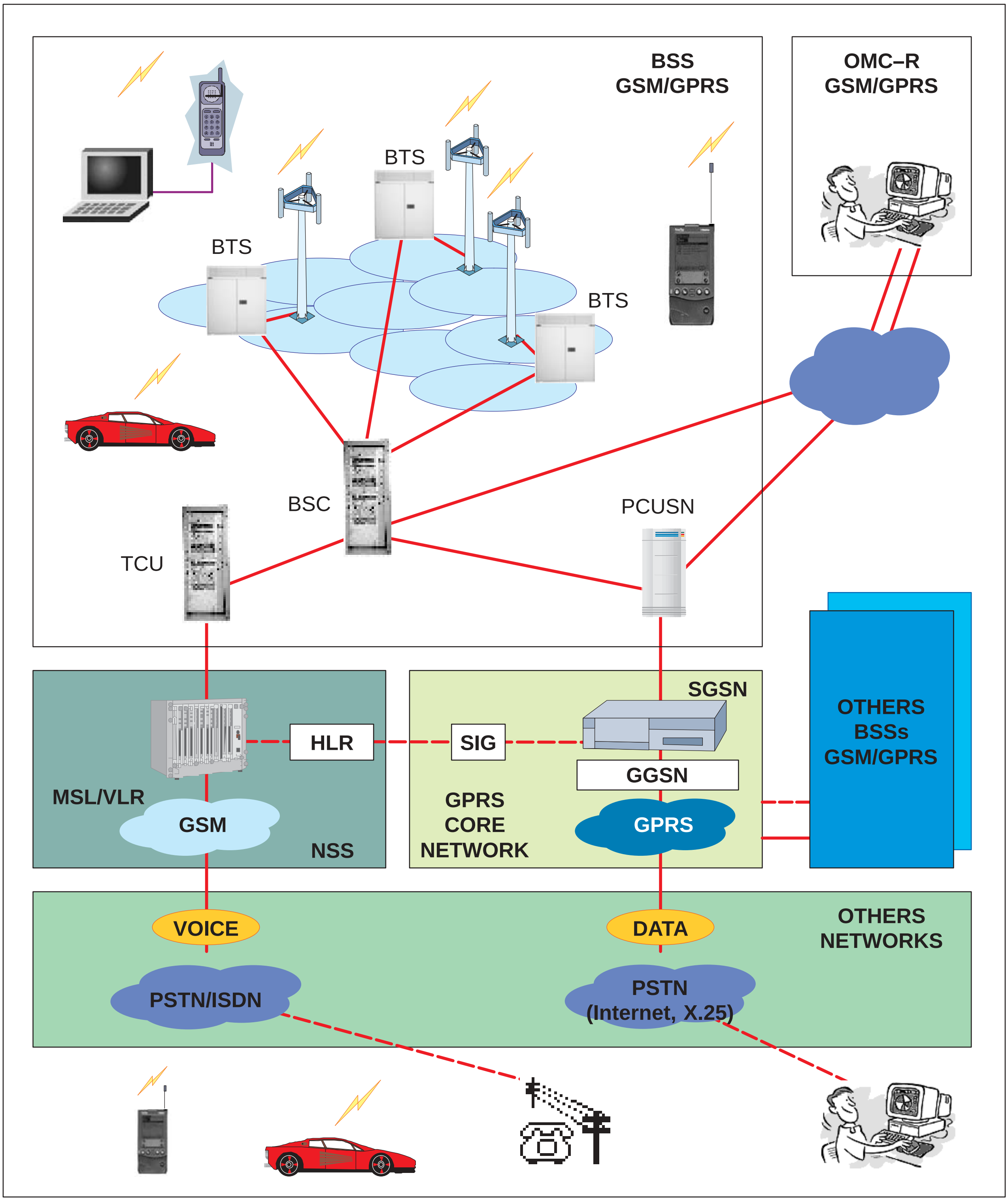
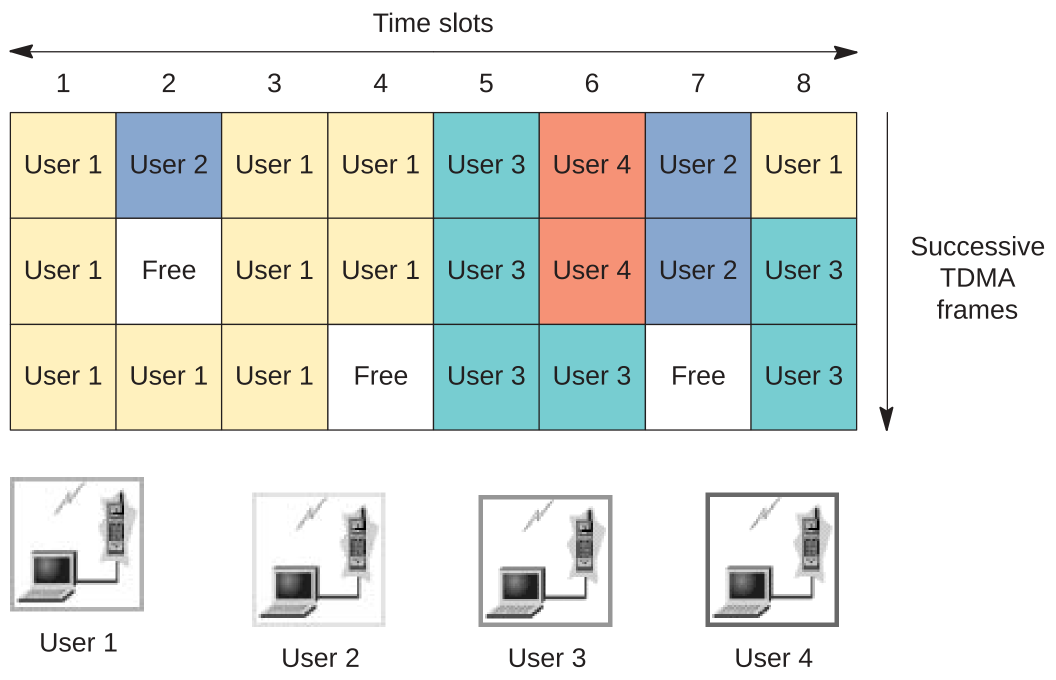


Figure 1–1 Functional presentation of the GSM/GPRS system



1	2	3	4	5	6	7	8
User 1	User 2	User 1	User 1	User 3	User 4	User 2	User 1
User 1	Free	User 1	User 1	User 3	User 4	User 2	User 3
User 1	User 1	User 1	Free	User 3	User 3	Free	User 3

Figure 1–2 Example of GPRS radio resource optimization

1.1.1 Base station subsystem (BSS)

The Base Station Subsystem (BSS) supports GPRS on the BTSs and supports an external PCUSN connected to one or more BSCs.

For the current BSS product family, GPRS needs a software upgrade for BTSs equipped with DCU4 boards or DRXs. If the BTS is equipped with DCU2 boards, an upgrade of DCU4 boards to support GPRS is required. In terms of BSC, only BSC12000 is supported.

1.1.2 Core network

The GPRS Core network includes:

- the Serving GPRS Support Node (SGSN)
- the Gateway GPRS Support Node (GGSN) and
- the SS7/IP Gateway (SIG)

The main functions of the SGSN are:

- to detect GPRS mobile stations in its service area
- to perform mobility management
- to implement authentication procedures
- to send/receive data packets to/from the mobile stations

The SGSN requests location information from the HLR through the Gr interface. These messages are routed through the SIG, which provides the interworking function between GPRS nodes in an IP network and GSM nodes in a signaling system 7 (SS7) network.

The GGSN provides the point of interconnection with external Public Data Networks for PLMNs supporting GPRS. This interconnection utilizes the Gi interface. The GGSN stores routing information for attached GPRS users. The routing information is used to tunnel Packet Data Units (PDU) to the current point of attachment of the MS; for example, the SGSN. The GGSN requests location information for mobile–terminated data packets from the HLR. This is accomplished transparently through the SGSN, utilizing the Gr interface.

1.1.3 Operation subsystem (OSS)

The Operation and Support Subsystem (OSS) contains three parts:

- the Radio Operations and Maintenance Centre (OMC-R)
- the Switching Operations and Maintenance Centre (OMC-S)
- the Data Operations and Maintenance Centre (OMC–D)

1.1.4 Interfaces

The GSM Packet Radio Service (GPRS) specifications define the various interfaces. These interfaces exist between GPRS elements and reference points on the internal and external sides of the GPRS system.

The following GPRS interfaces are:

1.1.4.1 Gb interface

The Gb interface is based on Frame Relay. It connects the PCUSN and the SGSN and allows:

- signaling information and user data to be exchanged on the same physical resource
- many users to be multiplexed over the same physical resource

1.1.4.2 Gn interface

Gn interfaces the GPRS Support Node (GSNs=SGSN and GGSN) within a PLMN.

1.1.4.3 Gi interface

Gi interfaces the GGSN with a data packet network (PDN). The PDN can be either a corporate Intranet or an Internet service provider (ISP).

1.1.4.4 Gr interface

The Gr interfaces an SGSN and an HLR. It allows the SGSN to access subscriber information located in the HLR. Since the SGSN and the HLR communicate using different protocols, the protocol messages must be routed through a conversion entity. In the GPRS application, this entity is known as the SS7/IP Gateway, or SIG. The use of the SIG necessitates two types of Gr interface: the Gr interface and the Gr' interface.

1.1.4.5 Gs interface

The Gs interfaces an SGSN and an MSC/VLR.

1.1.4.6 Ga interface

The Ga interface is a charging data collection interface between a CDR transmitting unit (GGSN or SGSN) and a CDR receiving functionality (CGF).

1.1.4.7 Gd interface

The Gd interface allows the transport of SMS messages through GPRS network.

1.1.4.8 Gp interface

The Gp interface provides support of GPRS network services across areas served by co–operating GPRS PLMNs.

1.1.4.9 OMN interface

The OMN interface provides communication between the BSC - OMC-R and PCUSN - OMC-R, using a data transmission network for centralized radio subsystem operations.

1.2 Physical overview

1.2.1 PCUSN and SGSN

The cabinet is built on the Nortel Networks 16-slot Passport platform. Access to its processor boards is from the front.

1.2.2 SIG

The SIG is a High Availability (HA) system that uses Hewlett Packard servers and HP Telecom Signaling Unit (TSU) SS7 units to achieve a high degree of reliability. The SIG, including both servers and TSUs, resides in a single HP cabinet.

1.2.3 GGSN

The Shasta–GGSN is based on the Contivity VPN (Virtual Private Network) 4500.

1.2.4 OMC-D

The OMC-D and OMC-R manage the GPRS network. The OMC-D is based on a Unix workstation which utilizes the HP OpenView Network Node Manager (NNM).

1.3 Regulatory information

1.3.1 Specific regulatory information

1.3.1.1 United States of America

The products comply with Part 68 of the FCC rules. On the equipment, there is a label that contains, among other information, the FCC registration. If requested, this information must be provided to the telephone company.

Each product uses the following standard connections and codes:

PCUSN	USOC CODE: TBD Service Order Code: TBD Facility Interface Code: TBD
SGSN	USOC CODE: TBD Service Order Code: TBD Facility Interface Code: TBD
GGSN	USOC CODE: TBD Service Order Code: TBD Facility Interface Code: TBD
SIG	USOC CODE: TBD Service Order Code: TBD Facility Interface Code: TBD

Table 1–1 Regulatory information

If the equipment causes harm to the telephone network, the telephone company will notify the customer in advance that temporary discontinuance of service may be required. But if advanced notice is not practical, the telephone company will notify the customer as soon as possible. Also the customer will be advised of his right to file a complaint with the FCC if he believes it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for the customer to make necessary modifications to maintain uninterrupted service.

No repairs can be performed by the user. If the customer experiences trouble with this equipment and for repair and warranty information, he will contact:

NORTEL NETWORKS
400 North Industrial
Richardson, Texas 75081
U.S.A.
Tel (972) 684-1000

If the equipment is causing harm to the telephone network, the telephone company may request that the customer disconnects the equipment until the problem is resolved.

This equipment cannot be used on a public coin phone service provided by the telephone company. Connection to a party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

1.3.1.2 Canada

”NOTICE: The Industry Canada Label identifies certified equipment. This certification means that the equipment meets telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee the equipment will operate to the user’s satisfaction.

Before installing this equipment, users should ensure that it is permissible to connect it to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.”

1.3.2 Electro–magnetic compatibility (EMC)

1.3.2.1 United States of America and Canada

GSM 1900 products

GSM 1900 products are classified under two categories:

- Class A devices: SIG, TBD
- Class B devices: Passport

For a Class A digital Device

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. If this equipment is used in a residential area, it may cause harmful interference that you must fix at your own expenses.

For a Class B digital Device

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

1.3.2.2 Europe and others

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference.

The EMC requirements have been selected to ensure an adequate level of compatibility for apparatus at residential, commercial, and light industrial environments. The levels however, do not cover extreme cases which may occur in any location but with low probability of occurrence. In particular, it may not cover those cases where a potential source of interference which is producing individually repeated transient phenomena, or a continuous phenomena, is permanently present, e.g. a radar or broadcast site in the near vicinity. In such a case it may be necessary to either limit the source of interference, or use special protection applied, to the interfered part, or both.

Compliance of radio communications equipment to the EMC requirements does not signify compliance to any requirement related to the use of the equipment (i.e. licensing requirements).

These products are compliant with the relevant parts of the following specifications:

Passport
TBD (EMC directive)
TBD (*) TBD
GSM (*) TBD
EN 55022
IEC 950
ENV (*) TBD
EN 60950

Table 1–2 Specifications

1.3.3 Operating conditions

1.3.3.1 For all countries

EMC compliance of the product is based on the following operating conditions (called normal operation):

- doors closed and/or cover in place
- external cables of the same type as specified by NORTEL NETWORKS
- no modification of any mechanical or electrical characteristics of the product

NORTEL NETWORKS responsibility regarding the product is disengaged by any change or modification made to the product without written approval from NORTEL NETWORKS.

1.3.4 Cable specifications

1.3.4.1 For all countries

The compliance to EMC requirements in force (89/336/EEC) has been verified using cables as specified by NORTEL NETWORKS. The continuing compliance of the product relies upon the correct cabling scheme, as specified by NORTEL NETWORKS.

1.3.5 PCM requirements

1.3.5.1 United States of America

This equipment complies with Part 68 of the FCC rules. The equipment label contains, among other information, the FCC registration number for this equipment. Upon request of the telephone company, you should provide the FCC registration number of the equipment which is connected to your T1 line.

No repairs can be performed by the user. If trouble is experienced with this equipment, please contact your NORTEL NETWORKS representative office. If the trouble is causing harm to the public network, the telephone company may request you remove the equipment from the network until the problem is resolved.

1.3.5.2 Canada

This equipment has been certified by the Industry Canada under CS03 requirements. The equipment label shows the certification number. This certification means that the equipment meets telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal equipment technical requirements document(s). The department dose not guarantee the equipment will operate to the user’s satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation in service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connection of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Users should not attempt to make such connections themselves, but should con tact the appropriate electric inspection authority, or electrician, as appropriate.

1.3.5.3 Europe

Compliance of the product to European PCM requirements has been verified against standards CTR 12 and TBR 13. They cover essential requirements (directive 91/263/EEC) for the physical and electrical characteristics of the terminal equipment interface, unstructured leased lines (U2048S) and structured leased lines (D2048S).

Conformance to these requirements does not guarantee end-to-end interoperability.

Conformance to these requirements does not guarantee user safety or safety of employees of public telecommunications networks operators, in so far as these requirements are covered by the Low Voltage Directive 73/23/EEC.

1.3.6 Radio approval

1.3.6.1 United Stares of America

TBD

1.3.6.2 Canada

TBD

1.3.6.3 Europe and others

There is a specific radio approval procedure for each country. It is not possible to list all the applicable approvals, since they will be dependent on markets and products. Please contact your local NORTEL NETWORKS representative for more information.

1.3.7 Product labeling

1.3.7.1 United States of America

To indicate compliance with FCC requirements, this device bears the following statement in a conspicuous location on the device:

- This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
  - (1) This device may not cause harmful interference
  - (2) This device must accept any interference received, including interference that may cause undesired operation.
- TX FCC ID: xxxxxxxxx (FCC Part 24 compliance)
- FCC ID: xxxxxxxxx Complies with part 68, FCC rules
- Manufacturer’s name
- Model Number
- Equipment designation: Example = S8000 Outdoor BTS GSM 1900

The label may be located inside or outside the product, provided that the user and/or maintenance people will have the information when working on the product.

1.3.7.2 Canada

To indicate compliance with the Canadian Standards, the device bears a label stating that the unit complies with all conditions set out in the special permission. The text contains the following information:

- This Class digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.
- CANADA ID: xxxxxxxxxx (RSS 133 compliance)
- CANADA ID: xxxxxxxxxx (CS03 compliance)
- Manufacturer’s name
- Model Number
- Equipment designation: Example = S8000 Outdoor BTS GSM 1900

The label may be located inside or outside the product, provided that the user and/or maintenance people will have the information when working on the product.

1.3.7.3 Europe and others

To indicate compliance with European Directives (EMC, Low Voltage, Terminal), this device bears the following label in a conspicuous location on the device:

- CE 0188 X
- Manufacturer’s name
- Model Number
- Equipment designation: Example = S8000 Outdoor BTS GSM 1800
- Any labelling requirement specific to a market (e.g. Type Approval)

The label may be located inside or outside the product, provided that the user and/or maintenance people will have the information when working on the product.

PAGE INTENTIONALLY LEFT BLANK

2 PCUSN

2.1 Introduction

The PCU Support Node is a stand-alone node in the BSS whose main purpose is to complement Nortel BSCs, with its PCU capability. The PCUSN can serve more than one BSC because it hosts many PCUs. The one–to–one relationship between a BSC and a remote PCU, which is stated in the ETSI standard GSM 03.60 [R2], is preserved by this characteristics of the PCUSN product (that is, the PCUSN supports several PCUs).

2.1.1 Scope and purpose

The PCUSN (Packet Control Unit Support Node) is a separate node in the BSS (Base Station Subsystem) in order to provide the specific packet processing (PCU) of the General Packet Radio Service (GPRS).

The primary PCU function is to provide the inter-working function between the radio Agprs interface (a synchronous connection–oriented PCM link) and the packet network Gb interface (asynchronous and connectionless).

2.1.2 PCUSN location

The PCUSN is located between the BSC and the SGSN, preferably at the BSC site.

It interacts, either directly or indirectly, with all the BSS nodes (BSC, BTS and OMC-R) except the TCU.

2.2 PCUSN hardware structure

2.2.1 Hardware overview

The PCUSN cabinet (see *Figure 2–1*) is built into the Nortel Networks 16–slot Passport platform.

Access to its processor boards is from the front.

The PCUSN cabinet is organized as follows:

- one PCU shelf
- one or two multiplexors
- termination and sparing panels

The PCU shelf contains:

- one or two control processor boards
- one to four four-ports DS1/E1 Channelized function processor boards
- one or two two-ports DS3/E3 Channelized AAL function processor boards

The E3C AAL FP board is the 32-port E1 AAL, and the DS3C AAL FP board is the 2-port DS3C AAL.

- one or two Voice Service function processors including:
  - the mother board with two SPM boards divided into:
    - one or two PCU Service Processor (PCUSP) boards
    - two SPMs (signal processing modules)
    - the hardware devices
  - the daughter board with ten SPMs

The number of boards depends on the capacity or whether redundancy is used or not.

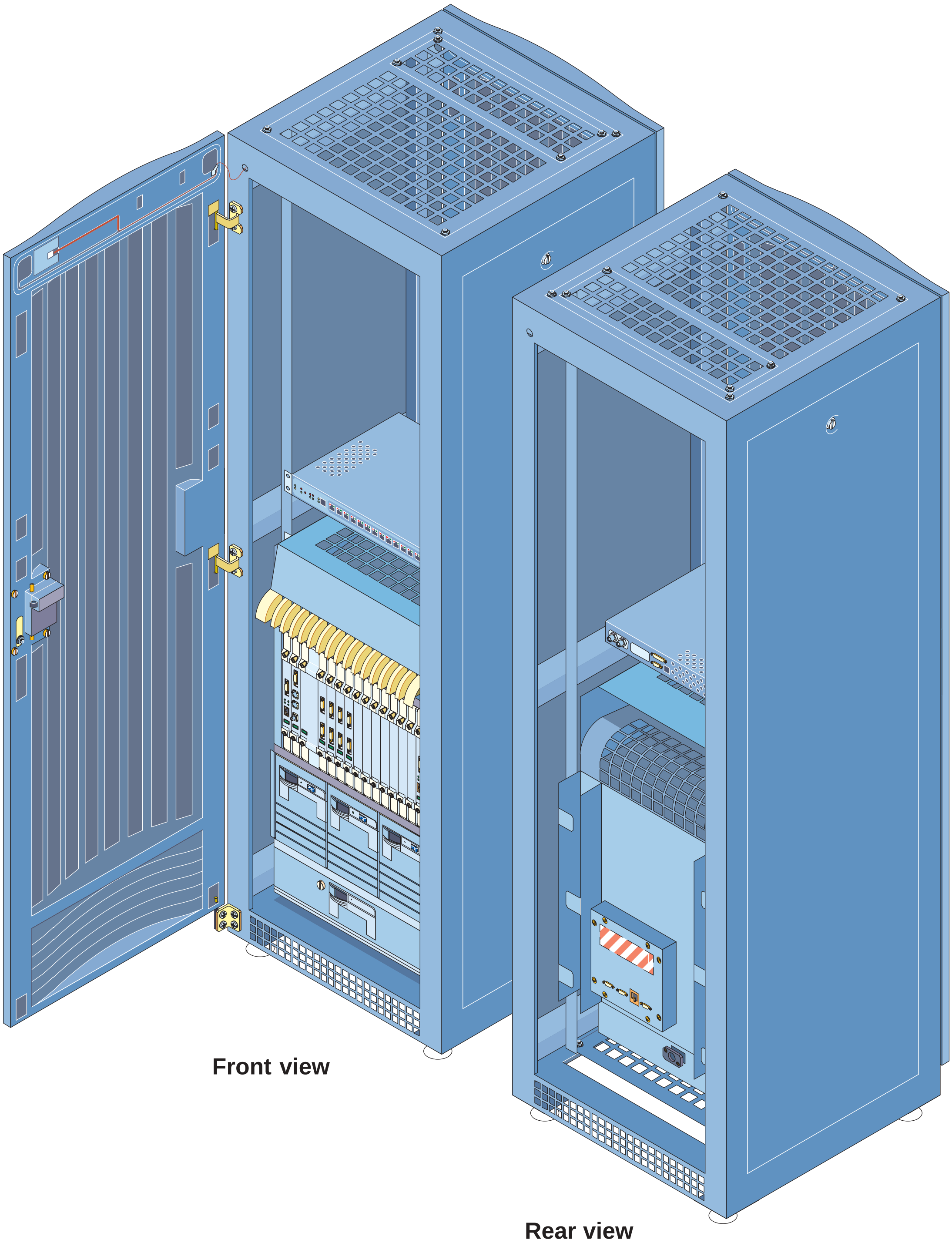


Figure 2–1 PCUSN cabinet

2.2.2 Physical characteristics

	Passport 7K/8K		Passport 15K
	Standard cabinet	**Seismic cabinet**	
Width:	60 cm (24 in.)	60 cm (24 in.)	60 cm (23 in.)
Depth:	70 cm (28 in.)	79 cm (31 in.)	60 cm (23 in.)
Height:	197 cm (78 in.)	197 cm (78 in.)	212.5 cm (84 in.)
Weight:	less than 313.3 kg (689 lbs)	less than 313.3 kg (689 lbs)	less than 588 kg (982 lbs)

Table 2–1 PCUSN: Dimensions and weight

2.2.3 Electrical characteristics

2.2.3.1 dc power supply

- nominal: -60 V dc to -48 V dc
- operational: -72 V dc to -40 V dc

2.2.3.2 Power consumption

- 600 W

2.2.4 Operating temperature

To operate correctly, the PCUSN cabinet requires an external temperature comprised between +10°C (+50°F) and +40°C (+104°F).

3 SGSN

3.1 Introduction

The SGSN is built into the Passport 15000–VSS platform. Passport is a high-speed packet switch providing an integrated set of data, voice, video, and image networking services.

3.1.1 SGSN features and functions

The SGSN performs similar functions to the MSC except that it processes packet data instead of circuit-switched data. The main functions of the SGSN include

- to detect new GPRS mobile stations in its service area
- to send and receive data packets to and from the mobile stations
- to record the location of mobile stations inside its service area

One of the main roles of the SGSN is to perform data packet routing, using IP as the network layer protocol. The Passport InterLan Switching (ILS) platform is implemented as the routing engine for the GPRS network developed by Nortel Networks. ILS has advanced capabilities such as label switching and the logical separation of different networks in one physical system.

Another key role of the SGSN is mobility management. This encompasses activities such as session management and state control. Mobility management also handles data packet routing on the downlink to the mobile station, including location tracking and authentication between the MS, the user, and the network using information on the subscriber-identity module (SIM) card.

In addition to these two key roles, the SGSN provides a number of other functionalities. These include ciphering and compression.

The SGSN capacity is scaleable and can be adapted to the operator model in terms of throughput and user capacity.

3.1.2 SGSN location

The geographic position of the SGSN has little effect on its operating capability. However, the choice of an appropriate site enhances hardware performance. For optimal performance, the SGSN should be located in an air conditioned environment, preferably with a fire retardant system. The best possible SGSN location in terms of specific network constraints is chosen by the operator.

3.2 SGSN hardware structure

3.2.1 Hardware overview

The SGSN (2pGPDsk, WPDS) is composed of (see *Figure 3–2*):

- a Passport 15000–VSS frame
- a Passport 7480 shelf
- a Passport 15000 shelf

The SGSN consists of three assemblies (see *Figure 3–2*):

- cable management assembly:
  - a cable guide
  - a housing assembly
- shelf assembly:
  - function processors (FP) and control processors (CP):
    - up to a total of 14 FPs and two CPs
    - up to a total of 15 FPs and one CP
  - three power converters
- cooling unit:
  - a fan assembly with two fans
  - a filter

Additional hardware consists of termination panels, and cables. Termination panels are installed in the same cabinet, a separate cabinet, or a rack, depending on the cabinet configuration.

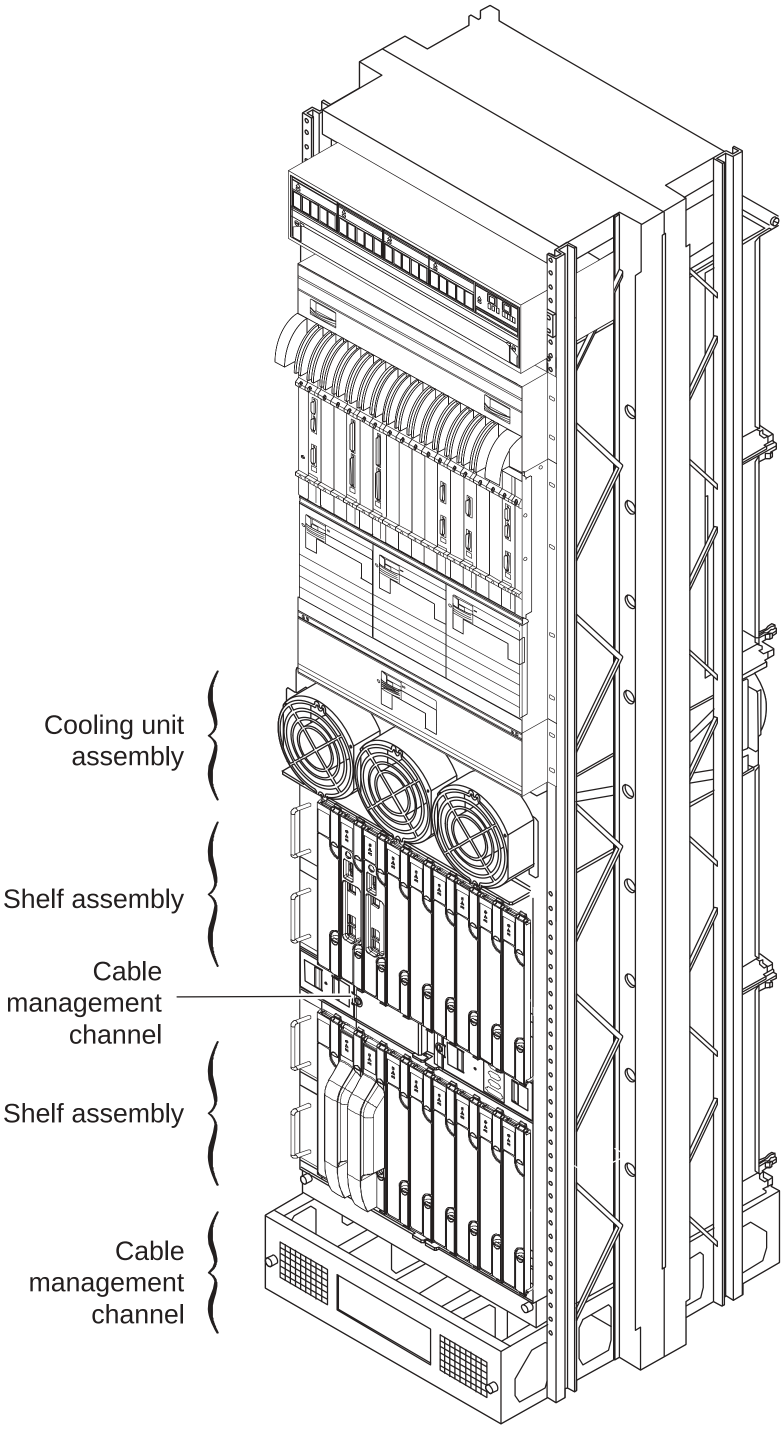


Figure 3–1 SGSN node assemblies in Passport cabinet

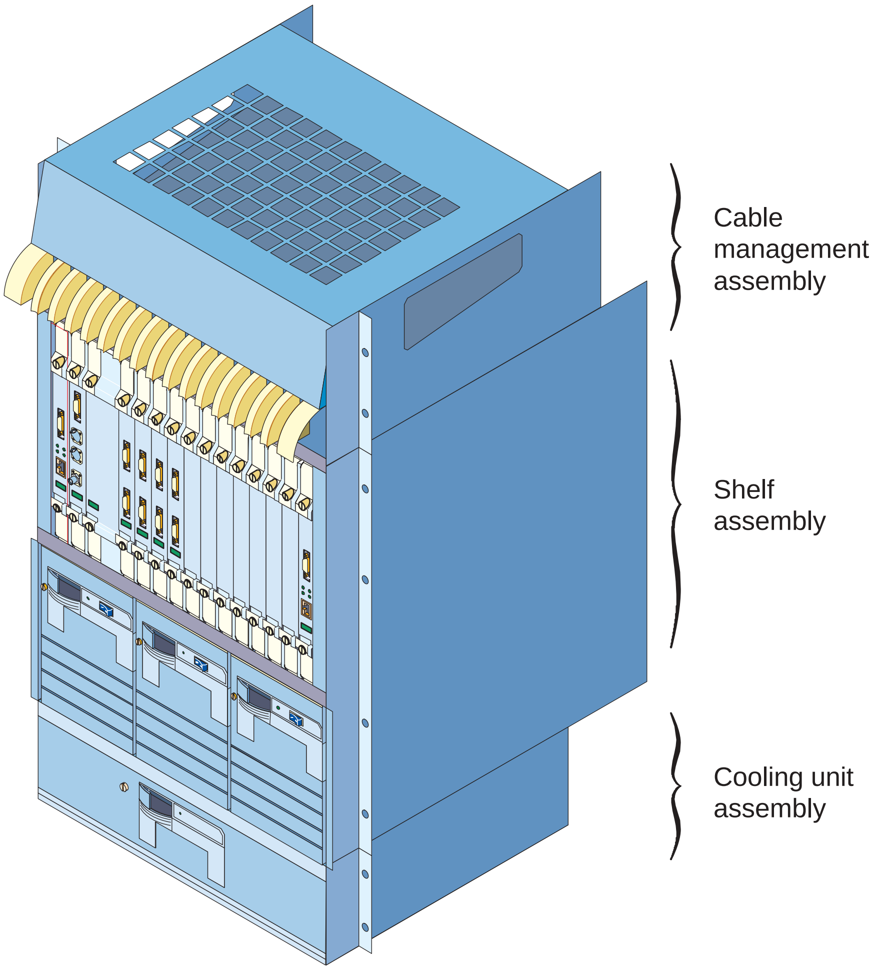


Figure 3–2 SGSN cabinet

The minimum recommended processor configuration for the SGSN is

- two CPs
- two 100BaseT Ethernet FPs
- six E1C (or DS1C) FPs:
  - three supporting GPRS Transport Layer (GTL) interface protocols
  - two supporting GPRS Subscriber Control (GSC) interface protocols

- an OC–3 ATM function processor, supporting GPRS Subscriber Layer Data (GSD) interface protocols
- three power converters

3.2.2 Physical characteristics

3.2.2.1 Dimensions and weight

Equipment	Outside dimensions (height x width x depth)	Weight
Passport example: a fully-configured, single-node cabinet with doors: 1 shelf assembly, cooling unit, air filter assembly, cable management unit, 3 power converters, 2 control processors, 14 function processors, and 14 termination panels (excluding cables)	197 cm x 60 cm x 70 cm (78 in. x 24 in. x 28 in.)	200.5 Kg (441 lbs)
Passport example: a fully-configured, dual-node cabinet with doors, 2 shelf assemblies, 2 cooling units, 2 air filter assemblies, 2 cable management units, 6 power converters, 4 control processors, 28 function processors, and 28 termination panels (on a rack) (excluding cables)	197 cm x 60 cm x 70 cm (78 in. x 24 in. x 28 in)	313.3 Kg (689 lbs)
Cabinet with doors (empty)	197 cm x 60 cm x 70 cm (78 in. x 24 in. x 28 in.)	87.7 Kg (193 lbs)
Node shelf assembly, with cooling unit, air filter assembly, cable management unit, 3 power converters, 2 control processors, 14 function processors	84.5 cm x 44.5 cm x 50 cm(33.25 in. x 17.5 in. x 19.75 in.)	80.6 Kg (177 lbs)
Node shelf assembly (empty).This set of dimensions does not include the cable management unit or the cooling unit. The depth measurement includes cable guides.	53.5 cm x 44.5 cm x 50 cm(21 in. x 17.5 in. x 19.75 in.)	20.9 Kg (46 lbs)

Table 3–1 SGSN: Dimensions and weight

3.2.2.2 Air cooling

Passport uses forced air for cooling internal assemblies. The intake draws air from both the base and front of the cabinet, and forces it vertically through the shelf where it exhausts to the rear of cabinet at the cable management section.

3.2.3 Electrical characteristics

- Nominal input voltage: -48 to -60 V with input operational range of -40 to -72 V
- Output power: cannot exceed 600 W

4 GGSN

4.1 Introduction

The Shasta–Gateway GPRS Support Node (GGSN) performs functions that are similar to the gateway MSC, except for packet data. The Shasta–GGSN provides the point of interconnection with external packet data networks (PDN) for the wireless PLMN supporting GPRS. This interconnection is performed via the Gi interface.

4.1.1 Shasta–GGSN features and functions

The Shasta–GGSN is well-suited to providing optimal benefits to the GPRS mobile user, providing the security and encapsulation techniques inherent to Virtual Private Networking (VPN) technology.

The Shasta–GGSN is primarily responsible for Packet Routing and Transfer, which includes the following general functions:

- Routing
- Tunneling
- Encapsulation
- Compression

The ability to provide security over insecure networks is incumbent upon the Shasta–GGSN. The GPRS standards suggest that IP Security (IPSec) Tunneling Protocol is ideally suited to providing the security that may be required by the mobile user in accessing the Internet or Intranet.

GPRS specifies the use of encapsulation techniques to facilitate mobile user access to the external packet data network. GPRS Tunneling Protocol (GTP) is used in the core network between GSN’s, and IPSec is optionally used in the external data network. Thus, the Shasta–GGSN is performing encapsulation / decapsulation on both the Gn and Gi interfaces.

4.1.2 Shasta–GGSN location

The geographic position of the Shasta–GGSN has little effect on its operating capability. However, the choice of an appropriate site enhances hardware performance. For optimal performance, the Shasta–GGSN should be located in an air conditioned environment, preferably with a fire retardant system. The best possible Shasta–GGSN location in terms of specific network constraints is chosen by the operator.

4.2 Shasta–GGSN hardware structure

4.2.1 Hardware overview

The Shasta–GGSN is based on the Contivity VPN 4500. It can be installed (see *Figure 4–1* and *Figure 4–2*) easily into a non-seismic Passport cabinet. It can also be installed in a customer-supplied EIA-standard cabinet, or in an EIA-standard 48.2 cm (19 in.) rack, as long as the environmental specifications are met.

The GGSN provides scalable, secure, manageable Extranet access for up to 75000 simultaneous users across the Public Data Network (PDN).

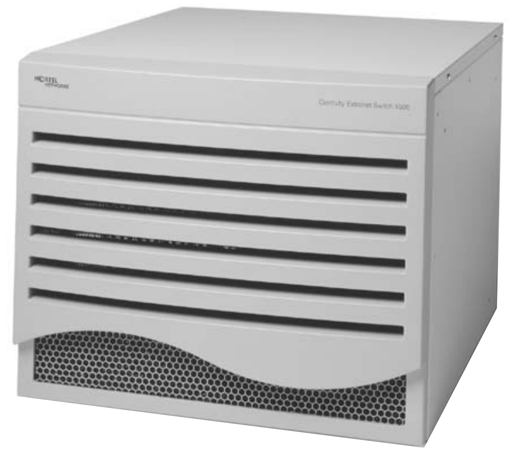


Figure 4–1 GGSN front view

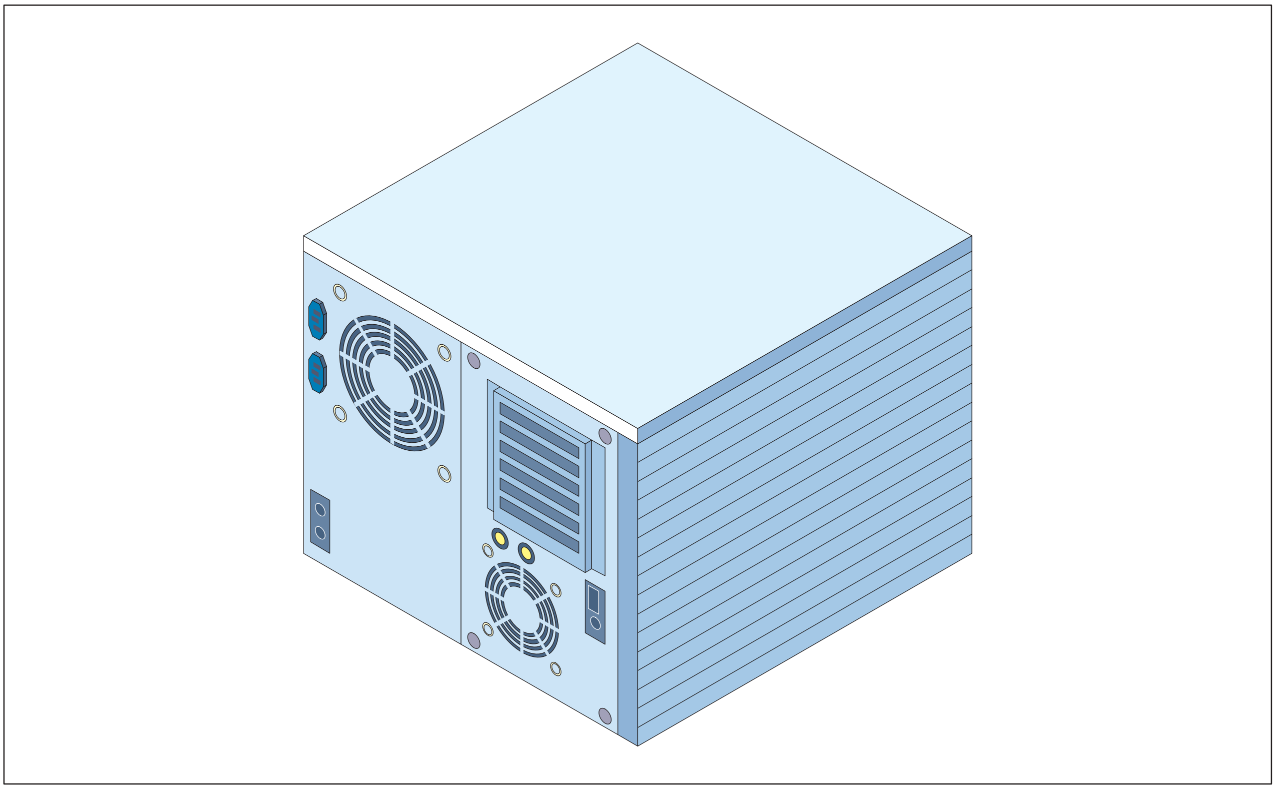


Figure 4–2 GGSN back view

4.2.1.1 LAN interface connections

The LAN interface connection provides a connection to the network.

100BASE-TX connections require Category 5, twisted-pair wires. The 100BASE-TX specification supports 100Mbps transmission over two pairs of Category 5 twisted-pair Ethernet wiring; one pair each for the transmit and receive operations.

100 meters (328 ft) is the maximum recommended cable segment length between a 100BASE-TX repeater and a workstation (due to signal timing requirements).

10BASE-T connections can use Category 3, 4, or 5 twisted-pair wiring.

4.2.1.2 Connector pinouts

The LAN connectors on the switch are RJ-45 straight-through. The figure below shows the Shasta–GGSN connector 10/100BASE-TX pinouts.

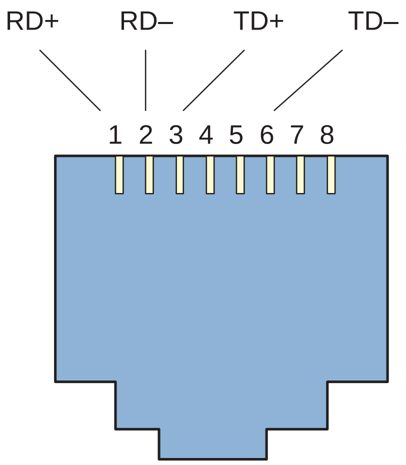


Figure 4–3 10/100BASE–TX pinouts

4.2.1.3 Serial interface cable (optional)

The Shasta–GGSN is shipped with a serial cable. Optionally, the customer can provide the Shasta–GGSN with a Management IP Address, subnet mask, and default gateway address among other things via the Serial Interface. It is recommended that the customer use the IP Address Configuration Utility diskette for easy initial IP address configuration. Later, the customer can use the serial interface configuration menu to perform management functions if problems were to arise.

4.2.2 Indicator LEDs

The Power LED is green when the power is on; if it is flashing, there is a hardware failure.

The Hard Disk LED is green, and when it flashes the Shasta–GGSN is either reading or writing to the disk.

The LAN Port LED is green, and when it flashes the Shasta–GGSN is either transmitting or receiving data.

4.2.3 Physical characteristics

4.2.3.1 Dimensions and weight

- **Shasta–GGSN:**

  Length: 40.64 cm (16 in.)

  Width: 43.18 cm (17 in.)

  Height: 35.56 cm (14 in.)

  Weight: 22.39 Kg (60 lbs)

- **Passport cabinet:**

  Length: 71.12cm (28 in.)

  Width: 60.96 cm (24 in.)

  height: 198.12 cm (78 in.)

  Weight: 87.7kg (193 lbs)

4.2.3.2 Air cooling

The GGSN uses forced air for cooling internal assemblies. The intake draws air from both the base and front of the cabinet, and forces it through the GGSN where it exhausts to the rear of cabinet.

4.2.4 Electrical characteristics

- Voltage: 100-240V
- Current: 3.0A
- Frequency: 50/60 Hz

5 SIG

5.1 Introduction

The SS7/IP Gateway (SIG) provides interworking between GPRS nodes in an IP network and GSM nodes in an SS7 network.

5.1.1 SIG functions

The SIG provides interworking between GPRS nodes in an IP network and GSM nodes in an SS7 network. Multiple SGSNs exist in the GPRS network, making the SIG responsible for routing messages from the GSM HLR to the correct SGSN. The SIG also routes messages originating from the SGSN to the MSC/VLR or HLR. Additionally, the SIG converts transaction capabilities application part (TCAP)/GSM mobile application part (MAP) messages originating from the GSM HLR in the SS7 network to User Data Protocol (UDP)/IP messages that contain the GSM MAP Client interface for GSM messages destined for the GPRS SGSN nodes. For messages originating from the SGSN IP network and destined for the HLR SS7 network, the SIG converts the UDP/IP messages into TCAP/GSM MAP messages. The SIG supports messaging operations between the SGSN (IP network) and HLR (SS7 network) in order to provide location management, subscriber management, authentication management, and fault recovery.

5.1.2 SIG location

The geographic position of the SIG has little effect on its operating capability. However, the choice of an appropriate site enhances hardware performance. For optimal performance, the SIG should be located in an air conditioned environment, preferably with a fire retardant system. The best possible SIG location in terms of specific network constraints is chosen by the operator.

5.2 SIG hardware structure

The SIG is a High Availability (HA) system that uses Hewlett Packard 9000 N series servers and HP Telecom Signaling Unit (TSU) SS7 units to achieve a high degree of reliability.

5.2.1 HP9000 N4000 system

The SIG system includes two Hewlett Packard (HP) 9000 N4000 servers (see *Figure 5–1*).

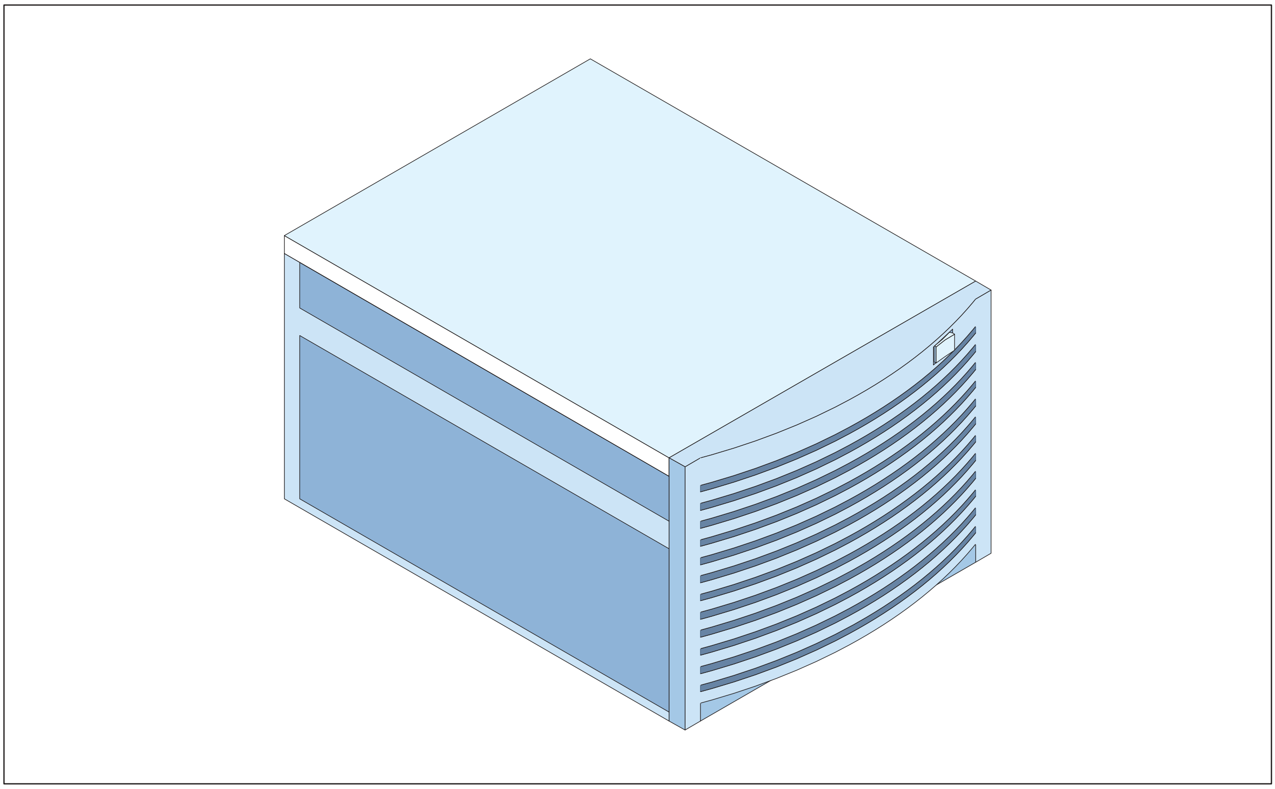


Figure 5–1 HP9000 N4000 front exterior

The HP9000 N4000 includes the following components:

- CPU - one or four 550 MHz PA8600 Processors
- Memory - Up to 16 GB
- 12 Hotplug 64-bit 60 MHz PCI I/O slots
- OS - HP-UX 11.0
- DVD drive

5.2.2 HP telecom signaling unit (TSU)

The TSU (see *Figure 5–2* and *Figure 5–3*) is a chassis that hosts Telecom Signaling Cards (TSCs). This chassis supports T1, E1, or V35 interfaces. A TSU can contain three E1/T1 or five V35 cards. The HP 9000 N4000 and TSU are connected using a dedicated point-to-point 100Base-T local area network (LAN) interface. A total of four TSUs maximum can be used per HP platform.

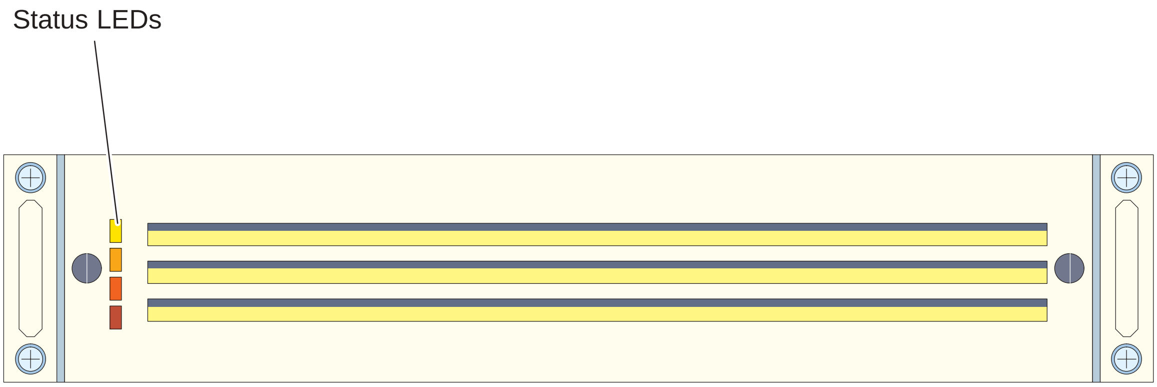


Figure 5–2 Telecom signaling unit: Front view

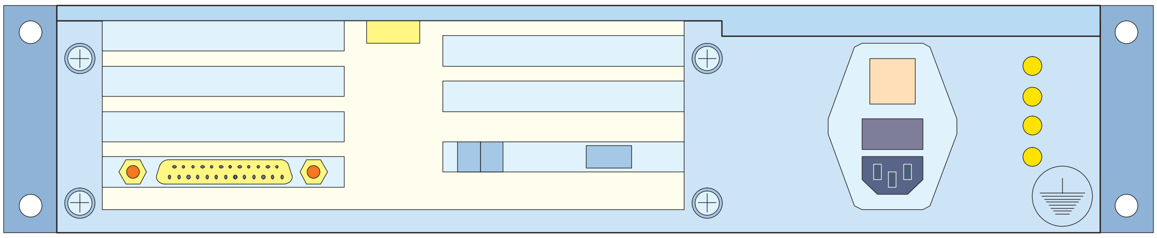


Figure 5–3 Telecom signaling unit: Back view

5.2.3 Location

The HP9000 N4000 based HP system, including both servers and TSUs, reside in a single standard HP cabinet (see *Figure 5–4*).

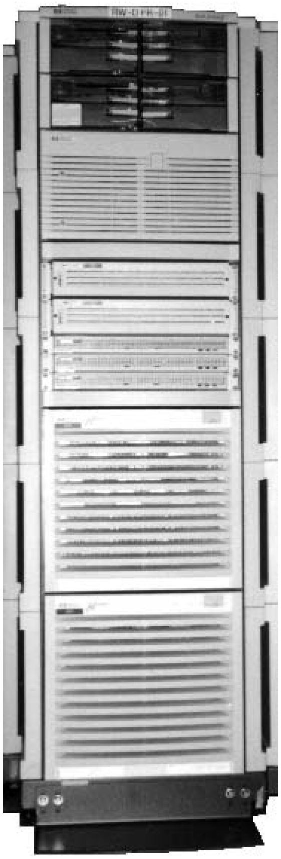


Figure 5–4 SIG system cabinet

5.2.4 Physical characteristics

5.2.4.1 HP system cabinet

- Depth: 1000 mm (39 in.)
- Width: 600 mm (23.62 in.)
- Height: 200 cm (78.74 in.)
- Weight: 250 kg (551.15 lbs)

5.2.4.2 HP9000 N4000 server

- Depth: 812 mm (31.97 in.)
- Width: 482 mm (18.98 in.)
- Height: 445 mm (17.52 in.)

5.2.4.3 TSU

- Depth: 464.21 mm (18.27 in.)
- Width: 431.8 mm (17 in.)
- Height: 86.89 mm (3.42 in.)

5.2.5 Electrical characteristics

5.2.5.1 HP9000 N4000

- ac input power: 200-240V, autorange 50-60 Hz
- Current requirements at 220V: 13.8 A

5.2.5.2 TSU

- ac/dc

  Input power: 100-127/200-240 V

  Current requirements at 120 V: 3.0 A

  Current requirements at 240 V: 1.3 A
- dc/dc

  Input power: -40 to -72 V dc

  Current requirements: 8.0 A

PAGE INTENTIONALLY LEFT BLANK

6 GPRS OAM

6.1 Introduction

GPRS Operation Administration and Maintenance (OAM) covers the new GPRS elements.

The network management of the PCUSN for the BSS, is integrated into the existing OMC-R transparently except some parts which are managed from the PCUSN OAM workstation (MDM or NMS application). The PCUSN elements are added to the BSS elements from the OMC-R point of view.

The network management for the GPRS Core Network is known as the OMC-D and is based on a client–server architecture.

The OMC-D completes Nortel Network's system consisting in OMC-R, OMC-S for respectively the BSS and NSS part (see *Figure 6–1*).

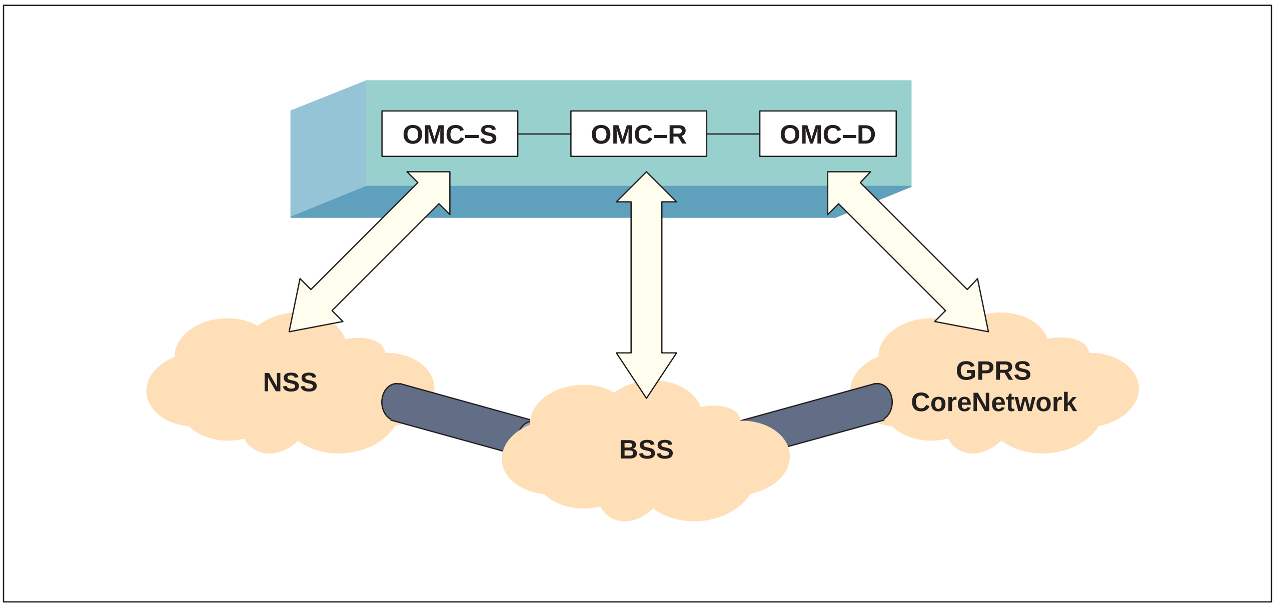


Figure 6–1 Network management architecture

6.2 PCUSN OAM

6.2.1 Introduction

The OAM functions available for the PCUSN are the same as the ones available for the rest of the BSS, including:

- Fault Management
- Configuration management
- Performance Management
- Software Management
- Security Management

The PCUSN OAM functionalities are performed by the PCU OAM server (see *Figure 6–2*).

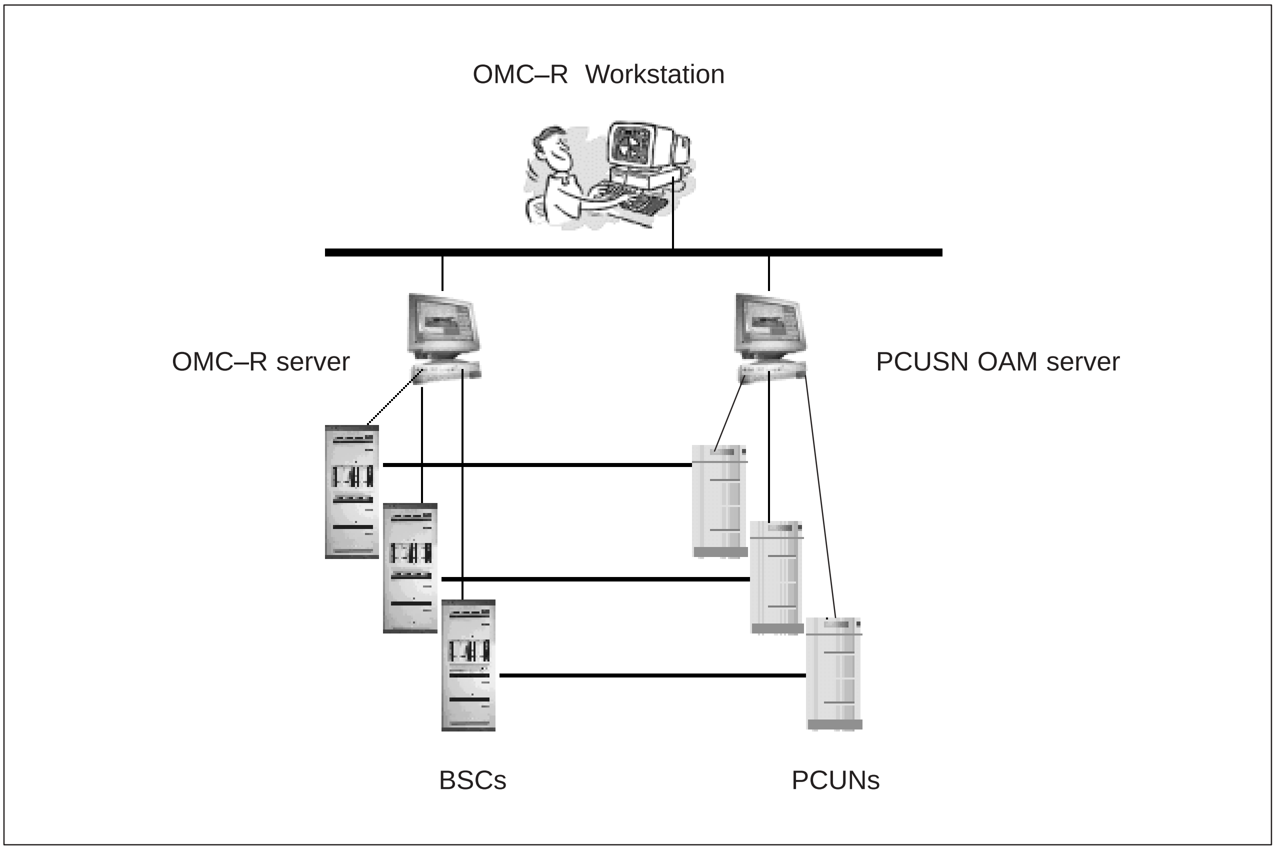


Figure 6–2 The PCU OAM server

The architecture of the PCUSN OAM server consists of two components:

- Multiservice Data Manager (MDM), known as the Network Management System (NMS) for Passport
- Magellan Data Provider (MDP)

The two units are described below.

6.2.2 Hardware characteristics

The PCUSN OAM software is hosted on a Sun Ultra5 workstation with the following characteristics:

- Processor Ultra Sparc 360 MHz
- 256 MB of RAM memory
- Internal disk of 8.4 GB
- Internal 1.44 MB floppy disk drive
- External DAT ‘mm tape drive
- PCI/SCSI2 board
- monitor
- Solaris Operating System

6.3 OMC–D

The OMC-D is introduced to perform the configuration, fault and real–time performance management of the SGSN, GGSN, SS7, Preside DNS, DHCP and Gateway. The OMC-D is based on Nortel Networks Integrated Network Management technology (INM) through which the Passport manager system (MDM) and the Contivity manager system (Optivity) are integrated in a single federating environment.

The OMC-D provides the following standard functions:

- Fault Management (FM)
- Performance Management (PM)
- Configuration Management (CM)
- Security Management (SM)
- Software Download (SD)

A network viewer provides a map of the whole network topology where the state of its elements is reflected. Access to the list of active alarms is provided and the alarms can be cleared automatically with device notifications. Real time performances can be displayed in graphical format for the SGSN and GGSN, while the counters are displayed.

6.4 Multiservice Data Manager (MDM)

6.4.1 Overview

The MDM is a workstation-based network management system that lets you maintain and monitor a complete network from a central or a decentralized network control center. The MDM has a full suite of applications and external systems interfaces to manage a number of different devices. The MDM also supports the capability to integrate equipment from other manufacturers.

The MDM provides the following features:

- a highly scalable architecture that allows a large amount of network growth
- a comprehensive set of applications for managing faults, configuration, accounting, performance, and security
- the ability to manage your network from a single console
- an easy-to-use graphic interface
- extensive online help
- data collection for performance analysis, tracking network use, billing, network engineering, and customer reports
- the ability to change the look and behavior of the NMS

6.4.2 Network views

The MDM can access data from multiple network elements at the same time and use this data in its applications. This capability enables the MDM to present a unified view of the network to the operator.

The MDM has two network views:

- a hierarchical component view that provides information about all modules in the network, their subcomponents, and their attributes (such as states).
- an organization view groups objects in a way that reflects the required view of your network. You can group objects by area or by function.

6.4.3 Management functions

MDM provides the following functions:

6.4.3.1 Fault management (FM)

FM is the process that detects, analyzes, and corrects network faults or degradation conditions. The MDM application for network fault management is Advisor. You can use an alarm-based or state-based method to detect faults in your network. Advisor allows you to get detailed information about faults, analyze the fault information, and take action to correct the fault. Advisor also provides an alarm acknowledgment utility.

Advisor includes the following tools:

- the Network Status Bar (NSB), which provides a high-level view of the network status. The NSB monitors a set of statistical indicators gathered from the General Management Data Router (GMDR) database. Some of these indicators determine the quantity of troubled elements in the network and include the number of active alarms or of out-of-service components.
- the Network Viewer (NV), which displays a real-time graphic network map that includes components, trunks, and links. The NV represents different node types by the shape of an icon and represents the states of components by the color of the icon.

  The NV displays:

  - different levels of the network at the same time (for example, regional, site, and module levels).
  - views at different levels of detail
- the Component Status Display (CSD), which displays a text version of the state information that the Network Viewer displays with graphics. The CSD can show a greater level of detail about the network.
- the Alarm Display (AD) tool, which provides a list of active alarms and alarm logs. The AD allows you to view alarms received in a single window. The display refreshes automatically after the list of active alarms changes.
- the Component Information Viewer (CIV), which provides you with in-depth information about components and subcomponents of a network element. The CIV provides this information in text format.

  The CIV allows you to perform the following tasks:

  - determine the effect of these faults
  - view the current state and problem state of these components
  - view the alarms and status received from these components

- The Performance Viewer (PV), which compiles status information and displays it as graphics and text. The PV application provides real-time performance graphs of important statistical information to help determine the behavior of element components.

  The PV provides the following capabilities:

  - It helps trace faults in the network.
  - It collects information about network load.
  - It generates statistics for reports and analysis.
- The Command Console (CC), which is the user interface for communication between NMS and Passport. You can use a single instance of this tool to issue commands to multiple components for configuration or fault management purposes.

Multiple windows allow you to run several Advisor tools at the same time. This capability increases the speed and ability to correct faults. For example, with the Network Viewer and the Component Status Display, you can look at the state of multiple components at the same time. With the Component Information Viewer, you can look at a single component and its related components to find more detailed information.

6.4.3.2 Configuration management

Configuration management includes the following tasks:

- defining the network, its modules, its software, and all of its services
- dynamically controlling the state of the network, its modules, and its services

The Architect tools and the Network Model provide network configuration. These applications make use of the management capabilities that are in all Passport modules. You can deploy these applications on the same workstation.

You can arrange configuration management capabilities in a hierarchy that reflects:

- the operational priorities
- the requirement to meet regulations
- the geographic distribution of network administration

6.4.3.3 Performance management

Planning and performance management is the process of planning, monitoring, and adjusting the performance of network devices. Network engineers can use the reporting tools to access online information to determine if network performance meets current needs.

The reporting tools include the Enhanced Statistics Reporter (ESR) application to analyze and report the characteristics of Passport network devices based on processed statistical data. Network managers use the reports to perform network planning and monitoring.

6.4.3.4 Security management

Security management is the process of establishing, maintaining, and controlling network management permission levels and requirements for network access.

6.4.4 Other MDM tools and utilities

You can use other tools and utilities with MDM, including Application Programming Interfaces (APIs), reporting tools, tools for administration tasks, and general purpose utilities.

MDM Application Programming Interfaces (APIs) are open, public interfaces. APIs allow other network management systems and custom programs to access MDM data. Other Nortel Networks software packages use APIs (for example, MDM workstation software).

With APIs, external applications can:

- collect data as required
- set selected data, such as provisioning data
- filter the data before reception
- receive notification when selected events occur

6.4.5 Common software

The network management applications are built on a common software module that provides color graphics, menus, icons, help screens, online documentation, and multiple windows. Common software also provides communication with the MDM mediation environment layer, and communication between applications.

6.4.6 MDM toolsets window

The primary MDM window in the workspace is the MDM Toolsets window. The Toolsets window provides access to all available MDM toolsets. Toolsets are collections of applications, or tools, that you use to perform network management tasks such as configuration and fault management. You access the MDM toolsets and their related tools from a pop-up menu on the MDM Toolsets window.

6.5 Management Data Provider (MDP)

6.5.1 Introduction

The Management Data Provider (MDP) is a bulk data collection and processing system for network accounting and statistical information. The MDP collects metric data from the switches using bulk file transfer protocol (FTP) transfers to minimize the performance degradation that typically results from constant metric polling. The data is then correlated to provide a historical account and statistical records. The records can be customized in content and format to ensure stability by external systems for billing, customer network management, planning and analysis.

The benefits of the MDP are:

- consolidated data collection
- high data integrity
- extensive data content
- scalable solution for all network sizes
- ease-of-fit into operational environments
- complete planning and analysis solution
- a client/server architecture used for MDP configuration and administration

The components of the MDP data collection system function together:

- to collect accounting records and performance monitoring records
- to process collected records and convert them to ASCII Bulk Data Format (BDF)
- to transfer records to customer hosts where they can be used to bill users and analyze system performance
- to generate network availability reports

6.5.2 MDP processes

6.5.2.1 File manager

A File Manager process performs the following functions:

- It periodically checks for the arrival of data files in the spool directory.
- It is responsible for coordinating the conversion, transfer, and deletion of data files (the File Manager initiates either the *Bulk Data Format (BDF) Converter* or the *Published Format Converter*). Converted files are placed in the dump directory.
- If required, it copies files from the spool directory to the backup directory for archiving.
- It places log files in the admin directory.

6.5.2.2 File mover

The File Mover process periodically checks for the arrival of successfully converted files in each dump directory. If files are found, the File Mover transfers the files to a specified customer billing or network engineering host for further processing and analysis.

6.5.2.3 Disk manager

The Disk Manager process:

- must start before the File Manager process
- coordinates the execution of the File Cleanup process (which deletes files from specified directories after a user-specified retention period has elapsed)
- ensures that sufficient disk space is available at all times

7 INTERFACES

The different interfaces are shown in *Figure 7–1*.

GSM interfaces

For more details, refer to the NTP < 01 >.

GPRS interfaces

The GSM Packet Radio Service (GPRS) specifications define various interfaces. These interfaces exist between GPRS elements and reference points on the internal and external sides of the GPRS system. This chapter discusses the following GPRS interfaces:

- Gb
- Gn
- Gi
- Gr
- Gs
- Ga
- Gd
- Gp
- Agprs
- OMN

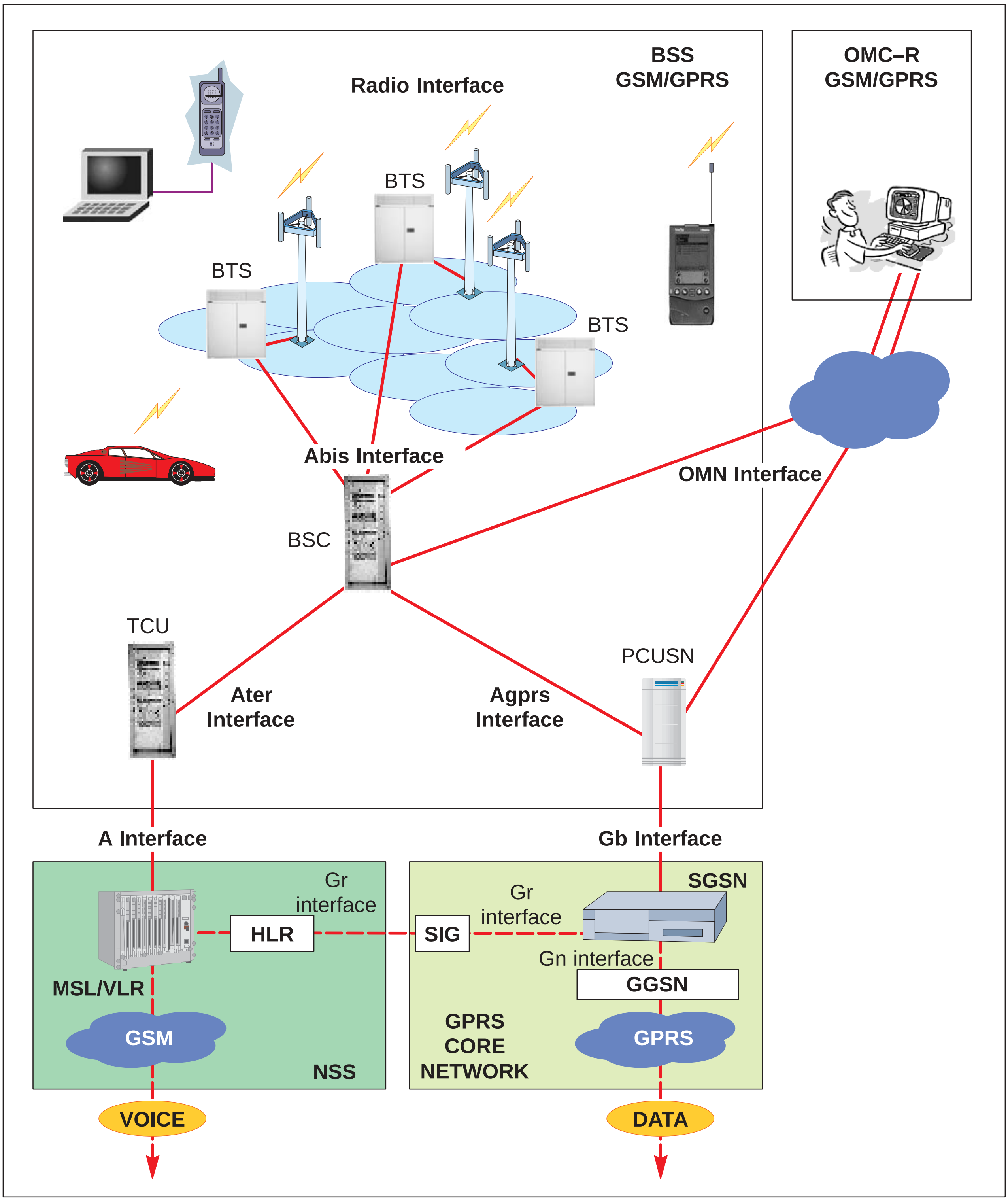


Figure 7–1 Interfaces

7.1 Gb interface

Gb interfaces the PCUSN and the SGSN.

7.1.1 Gb interface functions

The Gb interface is a new GPRS interface, and it does not play a role in the existing GSM network. It allows:

- exchange of signaling information and user data on the same physical resource
- many users to be multiplexed over the same physical resource

Resources are given to a user upon activity (when data are sent or received) and are reallocated immediately thereafter.

This is in contrast to the A–interface where a single user has exclusive use of a dedicated physical resource throughout the lifetime of a call irrespective of activity.

Access rate per user may vary from zero data to the maximum possible line rate.

7.1.2 Link layer protocols

A compliant Gb interface is implemented on both PCUSN and SGSN equipment.

They are connected through a frame relay (see *Figure 7–2*) which is used for signaling and data transmission.

The frame relay virtual circuits are established between the PCUSN and the SGSN.

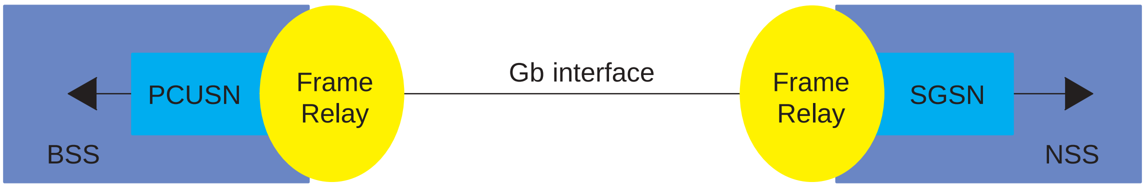


Figure 7–2 Gb interface between PCUSN and SGSN

The relay function is the means by which a node (PCUSN or SGSN) forwards frames from one node to the next node. The frames from many users are multiplexed on these virtual circuits.

The link layer is configured by the NMS-Passport.

Across the Gb-interface the following peer protocols have been identified (see *Figure 7–3*):

- the Base Station Subsystem GPRS Protocol (BSSGP)
- the underlying Network Service (NS)

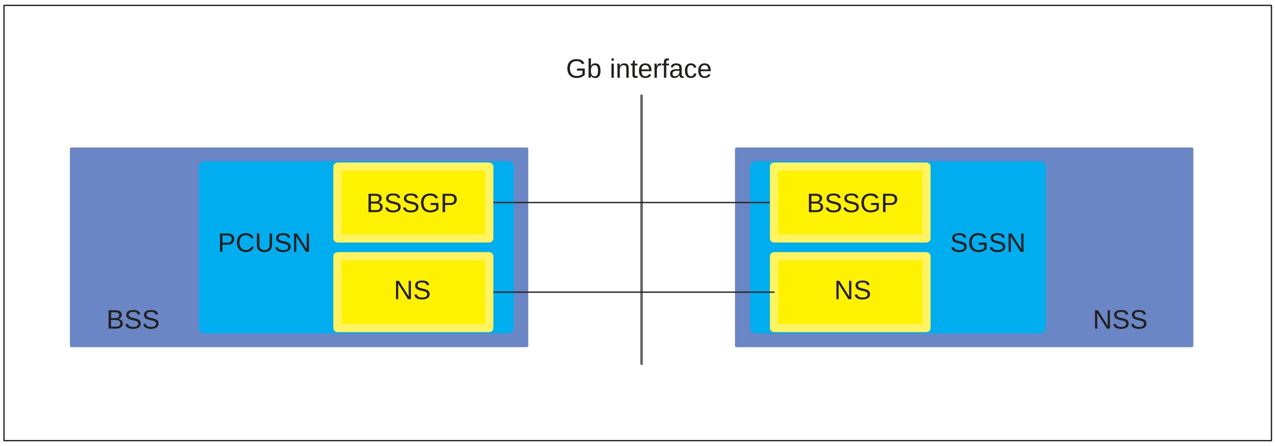


Figure 7–3 Gb interface protocol

7.1.3 BSS GPRS protocol (BSSGP)

The primary functions of the BSSGP include:

- the transfer of frames between the SGSN and the PCUSN
- the provision of functionality to enable two physically distinct nodes (SGSN and PCUSN), to operate node management control functions

This is the application part of the Gb interface. It is packet oriented and divided into three parts (see *Figure 7–4*):

- RL (relay) for functions controlling the transfer of frames between the RLC/MAC function and the BSSGP
- “GMM” (GPRS Mobility Management) for functions associated with mobility management between the SGSN and the PCUSN
- “NM” (Network Management) for functions associated with the Gb interface and PCUSN-SGSN node management

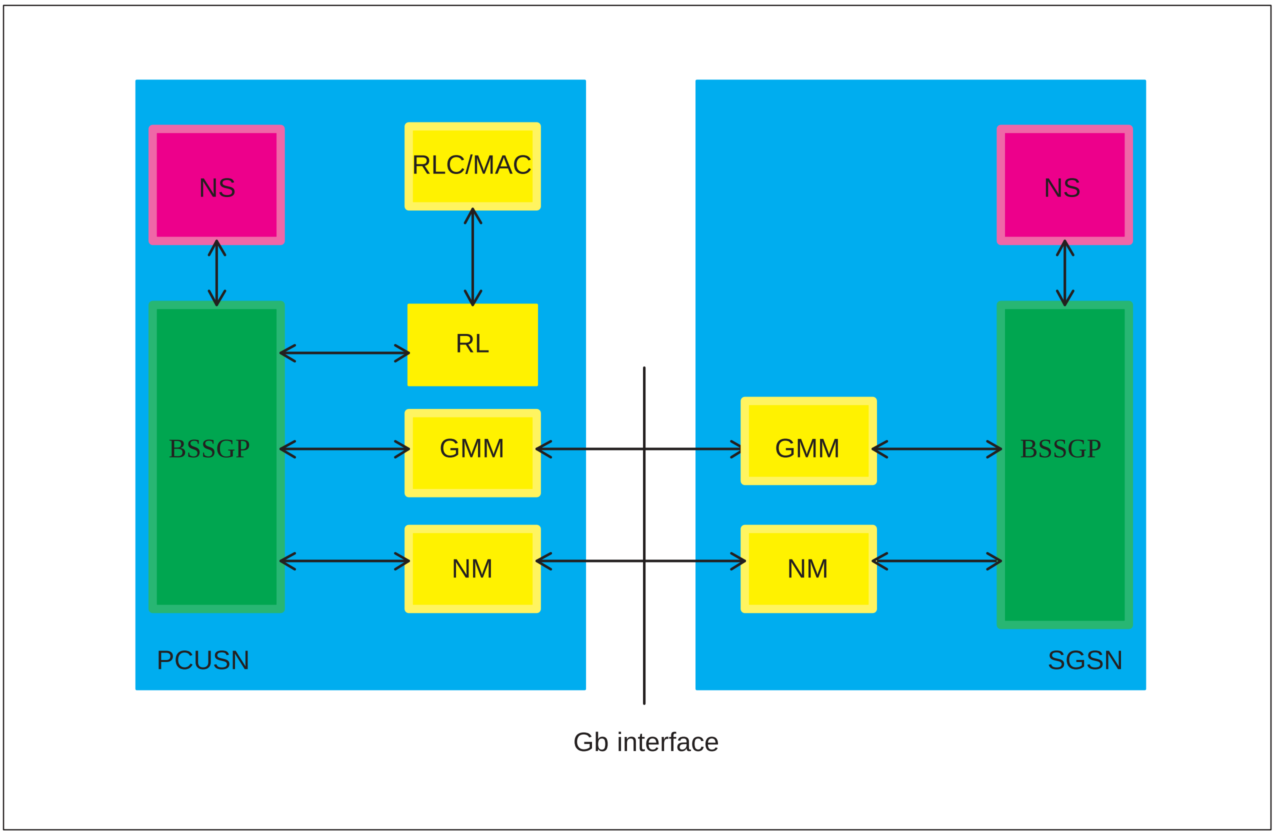


Figure 7–4 BSSGP protocol

RL contains the bearer packets, GMM contains the radio–related signaling packets and NM contains the Gb management–related signaling packets.

There is a one-to-one relationship between the BSSGP protocol in the SGSN and in the PCUSN. If one SGSN handles multiple PCUSNs, the SGSN has to have one BSSGP protocol machine for each PCUSN.

BSSGP is configured by the NMS-Passport and indirectly by the OMC-R (during creation/deletion of cells).

7.1.4 Network service (NS)

The Network Service entity (NS) provides a communication service to NS user peers. A Network Service Entity communicates with only one peer Network Service Entity.

The NS entity performs the transport of Service Data Units (SDU) between the SGSN and PCUSN. The services provided to the NS user are:

- Network Service SDU transfer. The NS entity provides network service primitives allowing for transmission and reception of upper layer protocol data units between the PCUSN and SGSN.

- Network congestion indication. Congestion recovery control actions may be performed by the Sub-Network Service (for example, Frame Relay). Congestion reporting mechanisms available in the Sub-Network Service implementation is used by the Network Service to report congestion.
- Status indication. Status indication is used to inform the NS user of NS affecting events (for example: change in the available transmission capabilities).

The Network Service entity is composed of (see *Figure 7–5*):

- a control entity, which is independent of the network: the Network Service Control
- an entity which is dependent on the intermediate transmission network used on the Gb interface: the Sub-Network Service

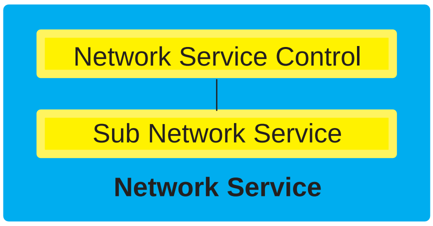


Figure 7–5 Internal architecture of the network service

The Network Service Control entity is responsible for the following functions:

- Service Data Unit transmission
- Load sharing
- Management of the blocking procedure

The Sub-Network Service entity provides a communication service to Network Service Control peer entities. Network Service Control peer entities use the Sub-Network Service to communicate with each other.

7.2 Gn Interface

Gn interfaces the GPRS Support Node (GSNs) within a PLMN.

7.2.1 Interface protocol

The Gn interface uses the GPRS tunneling protocol (GTP). The GTP protocol is implemented by SGSNs and GGSNs.

GTP is the means by which tunnels are established, used, managed, and released. (A tunnel forwards packets between an external packet data network and a mobile station (MS) user.)

GTP tunnels multiprotocol packets through the GPRS backbone between GPRS Support Nodes (GSNs). For protocols that need a reliable data link (for example, X.25), GTP tunnels use TCP/IP. For protocols that do not need a reliable data link (for example, internet protocol), GTP tunnels use UDP/IP. *Figure 7-6* shows the protocol stack for GTP.

Note: Release GGSN01 does *not* support TCP/IP.

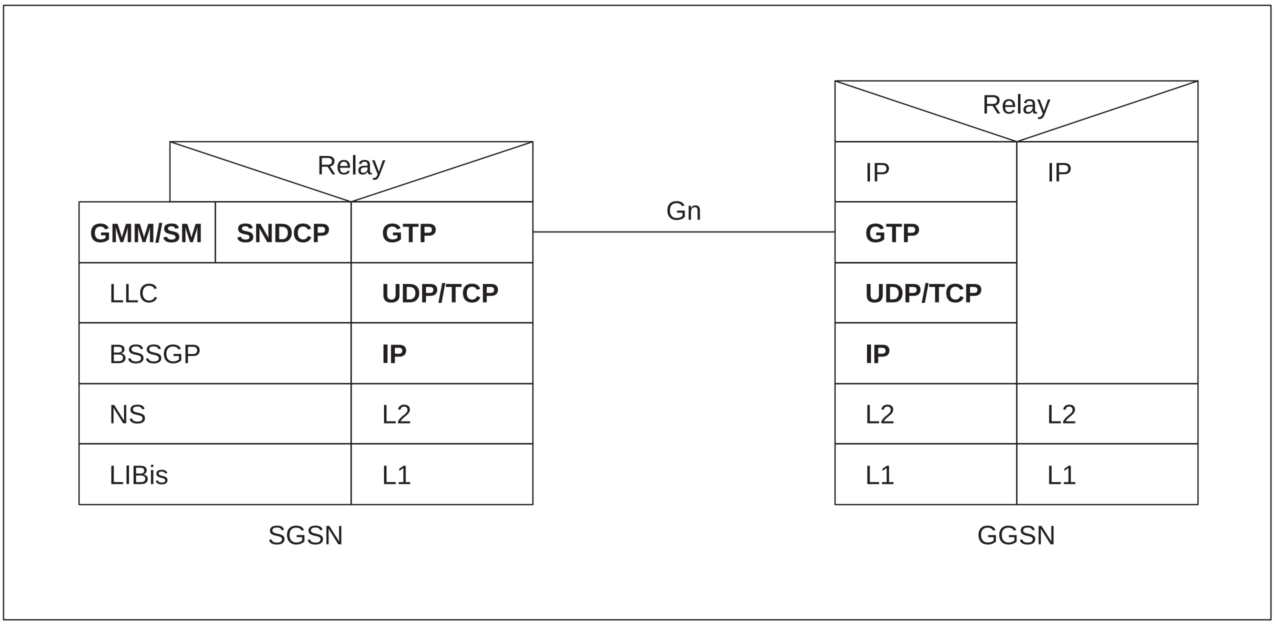


Figure 7–6 GTP protocol stack

In the signaling plane, GTP specifies a tunnel control and management protocol. This protocol allows the SGSN to provide GPRS network access for an MS. Signaling is used to create, modify, and delete tunnels.

In the transmission plane, GTP uses a tunneling mechanism to provide service for carrying user data packets.

GTP handles both signaling messages and user data traffic. GTP signaling messages create, modify, and delete tunnels. Functionally, GTP in the SGSN handles the following functions:

- It interacts with session management (SM) in the SGSN to initiate all GTP signaling messages or handle signaling messages coming from the GGSN node.
- It interacts with the SNDCP layer to handle user data packets from and to the SNDCP layer.
- It interacts with the UDP/TCP IP layers to tunnel GTP messages (both signaling and T-PDU data packets) from and to its peer GGSN node.
- It handles echo messages between GSNs.

7.2.2 Reliable delivery of signaling messages

Multiple signaling messages can be sent simultaneously over a single path. Each Request message should be responded to within the T3_RESPONSE time frame. If no response is received within that time period, the message is resent. This retry is repeated for up to N3_REQUEST times unless a response is received.

To have each Request message properly retransmitted when needed, each Request message is assigned a counter. Each counter determines if the limit on the N3_REQUESTS times for an individual signaling message is exceeded.

Although multiple signaling messages are sent simultaneously, their waiting for response is handled independently. Waiting for a response for one message does not block the delivery of other messages.

This setup has the following advantages:

- It uses the GTP layer efficiently.
- Multiple GTP signaling messages can be sent simultaneously to lower layers.

7.2.3 Message types

Following is a list of the various types of GTP messages:

- Echo Request
- Echo Response
- Version Not Supported
- Create PDP Context Request
- Create PDP Context Response
- Delete PDP Context Request
- Delete PDP Context Response

- Error Indication
- Identification Request
- Identification Response
- SGSN Context Request
- SGSN Context Response
- SGSN Context Acknowledge
- Node Alive Request
- Node Alive Response
- Redirection Request
- Redirection Response
- Data Record Transfer Request
- Data Record Transfer Response

The following paragraphs briefly describe the various types of GTP messages. The request and response messages are discussed together since they are related to one another.

7.2.3.1 The echo request and response messages

An Echo *Request* is sent on a path to another GSN to determine if the GSN is alive. An Echo Request message may be sent for each path in use. A path is considered to be in use if at least one PDP context uses the path to the other GSN. When and how often an Echo Request message is sent is specified during implementation. However, an Echo Request may *not* be sent more often than every 60 minutes on each path.

An Echo *Response* is sent in response to a received Echo Request. The recovery information element contains the local restart counter value for the GSN that sends the Echo Response message.

The GSN that receives the Echo Response from a peer GSN compares the received restart counter value with the previous restart counter value stored for the peer GSN. If a previous value was not stored, the received restart counter value is stored for the peer GSN.

If the previously stored restart counter value differs from the received restart counter value, the GSN that sent the Echo Response message is considered restarted by the GSN that received the message. The new restart counter value is stored by the receiving entity.

If the sending GSN is a GGSN and the receiving GSN is an SGSN, the SGSN notifies an affected MS the next time the MS contacts the SGSN. An affected MS is an MS that has at least one activated PDP context using the restarted GGSN. The SGSN considers all PDP contexts using the path as inactive.

7.2.3.2 The version not supported message

This message contains only the GTP header. This message indicates the latest GTP version supported by the GTP entity on the identified UDP/IP address.

7.2.3.3 The create PDP context request and response messages

The SGSN node sends a Create PDP Context *Request* to a GGSN node during the GPRS PDP context activation procedure. A valid request initiates the creation of a tunnel between a PDP context in an SGSN and a PDP context in a GGSN. If the procedure is not successfully completed, the SGSN repeats the Create PDP Context Request message to the next GGSN address in the list of IP addresses (if there is another address). If the list is exhausted, the activation procedure fails.

The GGSN node sends a Create PDP Context *Response* to an SGSN node in response to the Create PDP Context Request message. The cause value in the response message indicates if a PDP context was created in the GGSN. A PDP context was not created in the GGSN if the cause value differs from “request accepted.”

7.2.3.4 The delete PDP context request and response messages

An SGSN node sends a Delete PDP Context *Request* message to a GGSN node during either the

- either GPRS detach procedure
- or GPRS PDP context deactivation procedure

Also, the GGSN sends a Delete PDP Context Request message to an SGSN during the PDP context deactivation initiated by the GGSN procedure. The request is used to deactivate an activated PDP context.

The Delete PDP Context *Response* message is sent only when the context has an idle timeout or the administrator forcibly deleted the context.

7.2.3.5 The error indication message

The SGSN sends an Error Indication message to the GGSN if

- a PDP context does not exist
- the PDP context is inactive for a received G-PDU
- a no mobility management (MM) context does not exist for a received G-PDU

When the GGSN receives an error indication, the GGSN deletes its PDP context and notifies the operation and maintenance network element.

A new SGSN sends this message to an old SGSN if an active PDP context does not exist for a received G-PDU. The old SGSN deletes its PDP context and notifies the operation and maintenance network element.

Also, a GGSN sends an error indication to the SGSN if a PDP context does not exist for a received G-PDU. The SGSN tells the MS when a PDP context is deleted due to the reception of an error indication. The MS then requests the PDP context be re-established.

7.2.3.6 The identification request and response messages

A new SGSN sends an Identification *Request* message to an old SGSN when an MS (at GPRS attach) indicates it has changed SGSNs since detach.

The old SGSN sends an Identification *Response* message to the new SGSN in response to a previous Identification Request message. If the Cause value is "Request accepted," the response contains IMSI information, possibly one or several authentication triplet information elements, and optional vendor or operator-specific information.

7.2.3.7 The SGSN context request and response messages

A new SGSN sends an SGSN Context *Request* message to an old SGSN in an effort to obtain MM and PDP contexts for an MS.

The old SGSN sends an SGSN Context *Response* message to the new SGSN in response to the request message. If the Cause value is "Request accepted," the response message contains the following:

- a Flow Label Signaling field
- IMSI information element
- possibly one or several Receive State Variable information elements
- mobility management and security parameters
- active PDP contexts from the old SGSN
- optional vendor or operator-specific information

7.2.3.8 The SGSN context acknowledge message

A new SGSN sends an SGSN Context Acknowledge message to an old SGSN in response to the SGSN Context Response message. This message indicates that the new SGSN has correctly received PDP context information and is ready to receive data packets identified by the corresponding TID values. The old SGSN forwards user data packets only *after* receiving the SGSN Context Acknowledge message.

7.2.3.9 The node alive request and response messages

The purpose of this message is to inform that a node in the network has started its service (for example after a service break due to software or hardware maintenance or data service stop after a threatening overflow situation). A node may also send another Node Address than its own in the information element, for example when telling the “next node in chain” (which is located on the other side of the sender of this message) has come up. This message type maynot be used if Path Protocol is TCP.

This message allows quicker reconnect capability than the Echo Request based polling can provide, and its usage loads the network absolutely minimally also when the number of network nodes using GTP is high. It may also be used to tell about a new node who has not before been active in the network. If Echo Request is also used, the usage of Node Alive allows the interval of Echo Request to be longer than otherwise, and the network is then less loaded with the Echo Requests.

The node alive response message shall be sent as a response of a received node alive request. This message type may not be used if Path Protocol is TCP.

7.2.3.10 The redirection request and response message

There are two kind of use for this message. One purpose is to advise the incoming CDR traffic to be redirected to some other CGF due to this node soon stopping service (due to for example a maintenance break or an error situation or a threatening overflow situation). Another purpose is to inform a node (SGSN) sending data to this node (CG), that the next node (a mediator device or Billing Computer) after this node has no further connection to this node (CG).

The redirection response message shall be sent as a response to a received redirection request.

7.2.3.11 The data record transfer request and response message

The data record transfer request message is used in GPRS charging to transmit CDR information. CDR information is placed in the Data Record information element. When the receiver of this message (in a GPRS network the receiver is typically a CGF) wants to interpret the CDR information, it first interprets the CDR type (S–CDR or G–CDR or M–CDR), and then picks the CDR record fields from the Data Record.

The data record transfer response message shall be sent as a response to a received data record transfer request. Also, several data record transfer requests can be answered by a single data record transfer response.

7.2.4 Message flows

This section discusses the message flow that exists among the GTP-related components. The following scenarios illustrate the details of the message flows:

- PDP context activation and deactivation
- echo request and response
- error

7.2.4.1 PDP context activation (MS initiated)

During the PDP context activation procedure, the SGSN sends a Created PDP Context Request to a GGSN. The GGSN IP address is the first IP address in the list of IP addresses provided by the DNS server. The DNS server provides the IP addresses in its response to the query of the Access Point Name (APN) received in the Activate Request.

Note 1: A list of IP addresses represents a list of Gn interfaces. GTP path management messages monitor a Gn interface if the interface is used by some PDP context(s). GTP also maintains the link status of each monitored interface.

Note 2: If the previous try has failed on a PDP Context Activation request, GTP tries each of the addresses in the address list. GTP tries the addresses in order from the first address to the last address, regardless of the recorded link status of the aforementioned interface. This is because the link status information is inaccurate since only one echo message can be sent every 60 seconds.

Note 3: The link status of a path indicates if a path failure has occurred and how long the path has been in a failed status. When the age of a path failure exceeds a predefined value, the GGSN on the path is considered to be out of service.

Figure 7–7 illustrates the message sequence for the PDP context activation procedure.

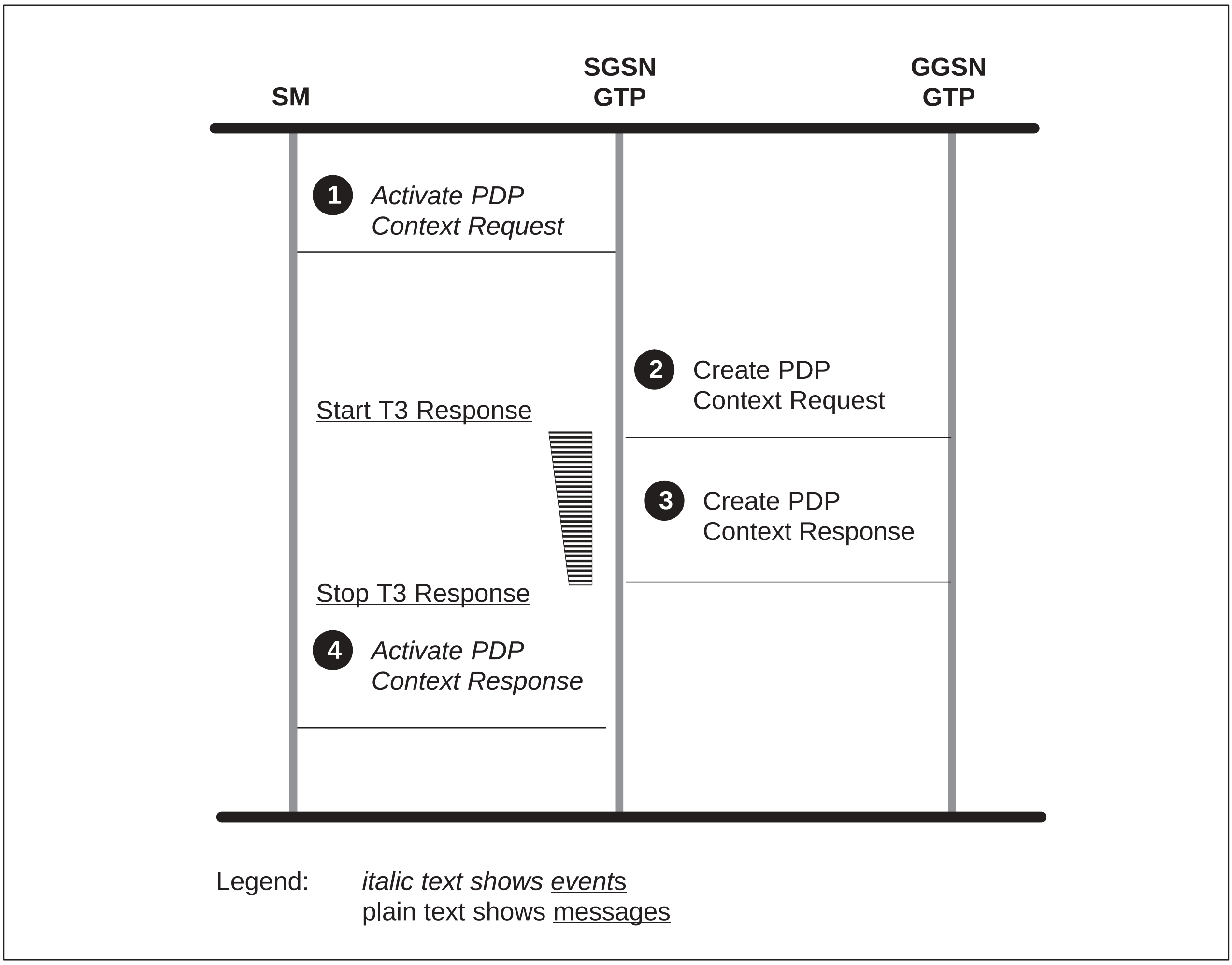

SM
SGSN GTP
GGSN GTP
1 Activate PDP Context Request
2 Create PDP Context Request
Start T3 Response
3 Create PDP Context Response
Stop T3 Response
4 Activate PDP Context Response
Legend: italic text shows events
plain text shows messages

Figure 7–7 Message sequence for PDP context activation procedure

The following bullets explain the steps highlighted in *Figure 7–7* :

1. The SM sends a message to trigger the SGSN/GTP to send a GTP Create PDP Context Request message to the proper GGSN/GTP node.

2. The SGSN/GTP message (Create PDP Context Request) tunnels to the GGSN node to create a PDP Context in the GGSN node. A timer of T3_Response is started.

3. The GGSN/GTP message (Create PDP Context Response) tunnels to the GTP in SGSN node. The timer is stopped.

Note 1: GTP uses a timer and a counter for each outgoing signaling message. For each signaling message sent out, a response is received before the T3_response timer expires. If a timeout occurs, the GTP resends the message for another N3_requests-1 time.

Note 2: The Create PDP Context Response message may optionally include a Recovery IE in it. GTP checks the recovery IE to see if the peer GGSN has restarted. If the peer GGSN has restarted, the GTP must notify the SM of the change so the SM can take proper action on it.

Note 3: If PDP Context Activation fails on one Gn interface, GTP repeats the Create PDP Context Request to the next GGSN address if one exists.

7.2.4.2 PDP context deactivation (MS initiated)

During the PDP context deactivation procedure, the SGSN sends a Delete PDP Context Request to a GGSN. The request is used to deactivate an activated PDP context.

The GSN sends a Delete PDP Context Response in response to a Delete PDP Context Request. The GSN always replies to a request even if the PDP context does not exist.

Figure 7–8 illustrates the message sequence for the PDP context deactivation procedure.

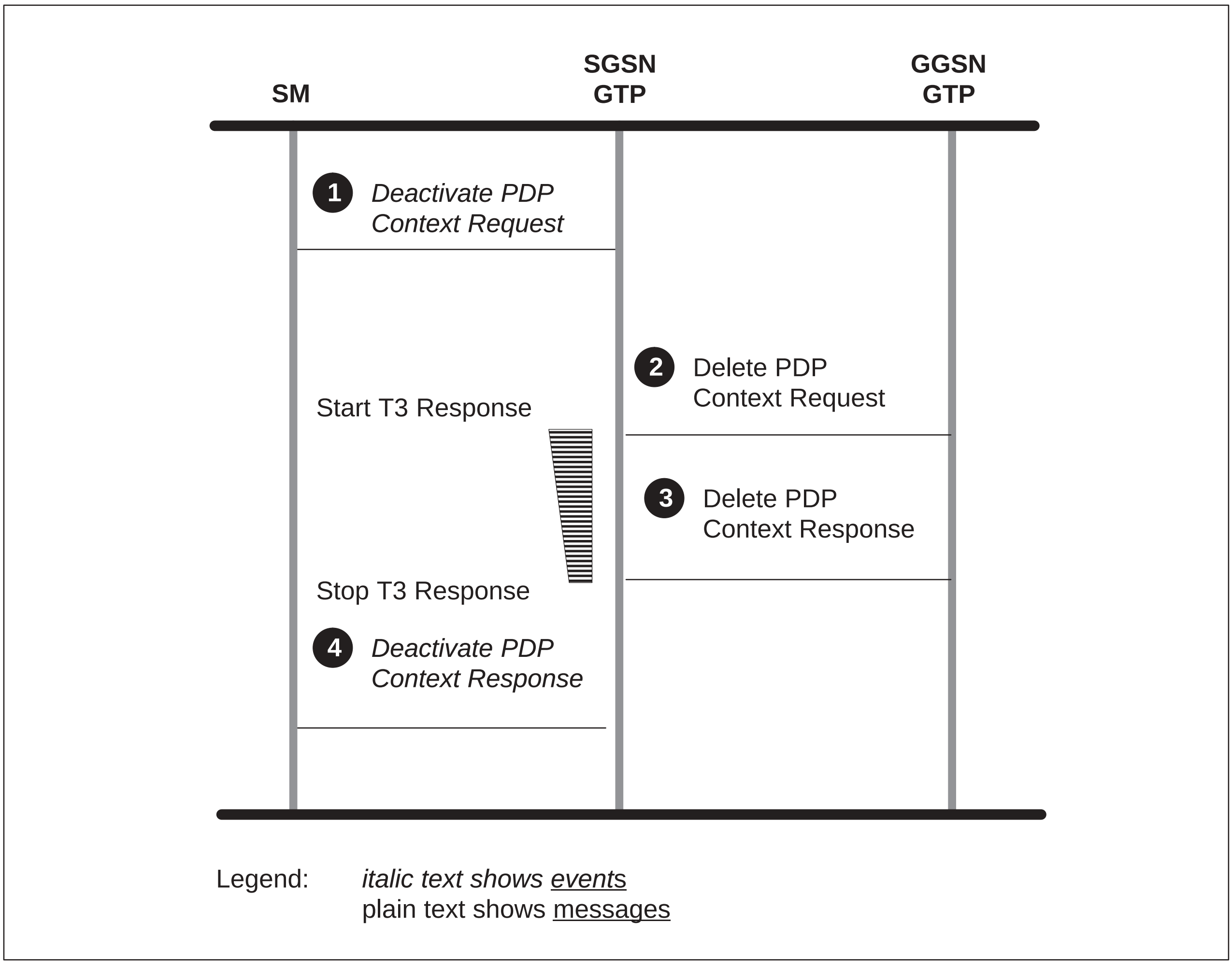

SM
SGSN GTP
GGSN GTP
1 Deactivate PDP Context Request
2 Delete PDP Context Request
Start T3 Response
3 Delete PDP Context Response
Stop T3 Response
4 Deactivate PDP Context Response
Legend: italic text shows events
plain text shows messages

Figure 7–8 Message sequence for PDP context deactivation procedure

The following bullets explain the steps highlighted in *Figure 7–8*.

1. The SM sends a message to trigger the SGSN/GTP to send a GTP Delete PDP Context Request message to the proper GGSN node.
2. The SGSN/GTP message (Delete PDP Context Request) tunnels to the GGSN node to delete a PDP Context. A timer of T3_Response is started.
3. The GGSN/GTP message (Delete PDP Context Response) tunnels to the GTP in SGSN node. The timer is stopped.

Note 1: GTP uses a timer and a counter for each outgoing signaling message. For each signaling message sent out, a response is received before the T3_response timer expires. If a timeout occurs, the GTP resends the message for another N3_requests-1 time.

4. The message is forwarded to the SM.

7.2.4.3 Echo request on signaling path and data path

A path is a physical connection (direct or indirect) between a pair of source and destination IP addresses. Path management can be performed on any path in use. The path is considered to be in use if at least one PDP context uses the path to the other GSN. *Figure 7–9* shows an example of a pair of GSN nodes. In this example, each Gn interface has four paths (one signaling path and three data paths).

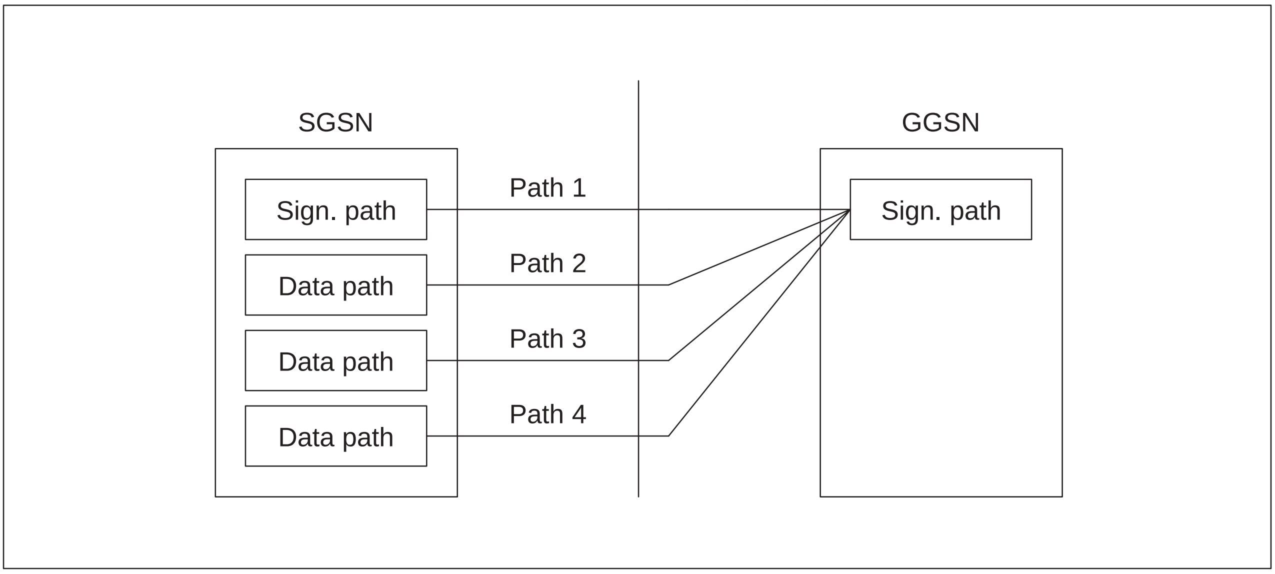


Figure 7–9 Example of a pair of GSN nodes

If all paths in the example are in use, the system may send an Echo Request message for each signaling path. These messages are sent to determine if the peer GSN is alive.

The SGSN GTP uses a timer and a counter for each Echo Request message that it sends. A response must be received before the T3_response timer expires. If a timeout occurs, the GTP resends the message for another N3_REQUESTS-1 times (five times by default). If the response is not received after the N3_REQUEST times of attempts, the path is considered down.

7.2.4.4 Echo response on signaling path and data path

The SGSN responds to any echo request it receives. *Figure 7–10* shows the message sequence for the echo response procedure.

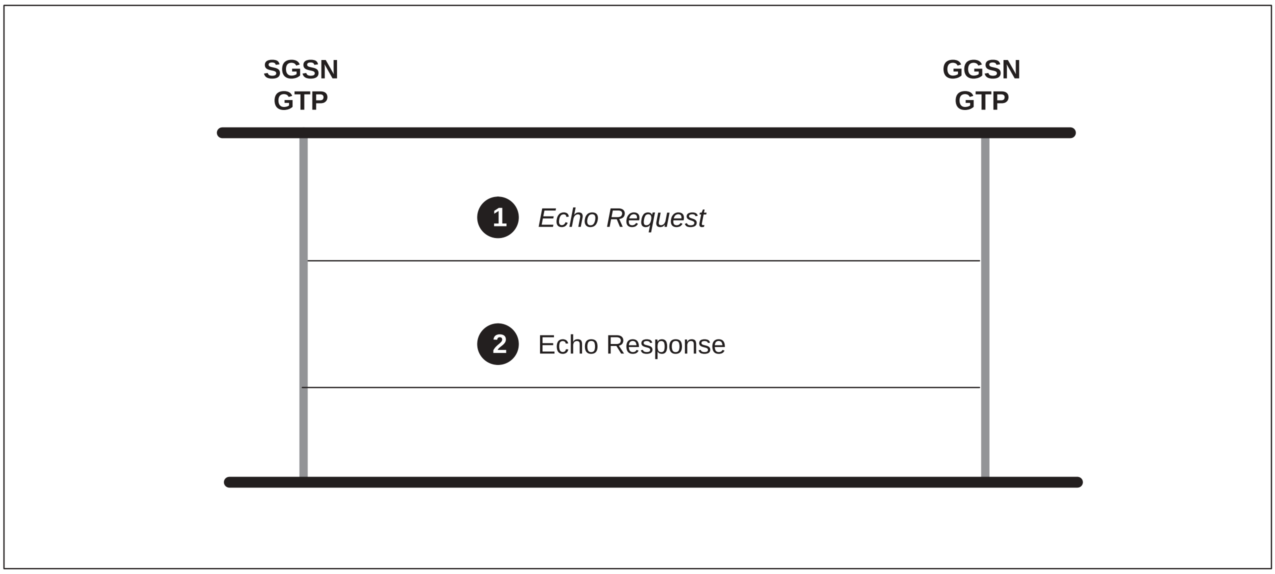


Figure 7–10 Message sequence for the echo response procedure on signalling path and data path

The following bullets explain the steps highlighted in *Figure 7–10*:

1. The GGSN sends a GTP Echo Request message to the SGSN. This message occurs at a certain rate (for example, every five minutes).
2. The SGSN sends an Echo Response with Recovery IE to the GGSN to tell the GGSN node its current status.

Note: The restart counter values in the SGSN/GTP message is included in order to tell if the SGSN node has restarted or not.

7.3 Gi interface

Gi interfaces the GGSN with a data packet network (PDN). The PDN can be either a corporate intranet or an internet service provider (ISP).

GGSN01/02 supports an internet protocol (IP) PDN. Typically, IP networks use IP routers to perform the interworking with subnetworks. From the IP network’s point of view, the GGSN is an IP router. The interworking point with IP networks is at the Gi reference point as shown in *Figure 7–11*.

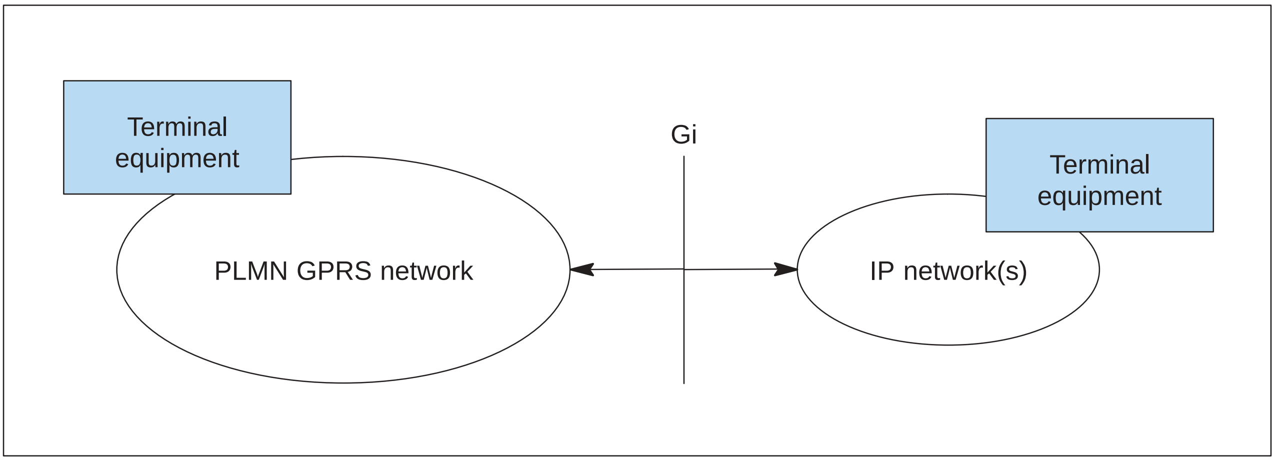


Figure 7–11 IP network interworking

7.3.1 Physical interface

In GGSN01, the GGSN supports one 10 or 100 Mb Ethernet Gi interface.

7.3.2 Accessing the internet

The GPRS Technical Specification 9.61 mandates the following two modes of access to the PLMN:

- transparent access to the Internet
- non-transparent access to the Internet

Note: The terms “transparent” and “non-transparent” describe the connectivity from the perspective of the GGSN.

7.3.2.1 Transparent access to the Internet

With transparent access, the GPRS operator offers a basic Internet services protocol (ISP) service. The mobile does not send any authentication request at PDP context activation and the GGSN does not take part in user authentication or authorization process. GPRS provides cursory authentication as part of the Network Access Control procedures executed between the MS and the SGSN.

The operator issues the GPRS user a public IP address. This IP address is allocated either at subscription or at PDP context activation. When the IP address is allocated at subscription, the process is called static address allocation. When the IP address is allocated at PDP context activation, the process is called dynamic address allocation.

The transparent case provides at least a basic ISP service. As a consequence of this, it may provide a bearer service for a tunnel (for example, IPSec, PPTP, L2TP) to a private Intranet. User level configuration may then be carried out between the MS and the Intranet/ISP and is *transparent* to the GGSN.

Figure 7–12 and *Figure 7–13* illustrate two possible transparent configurations.

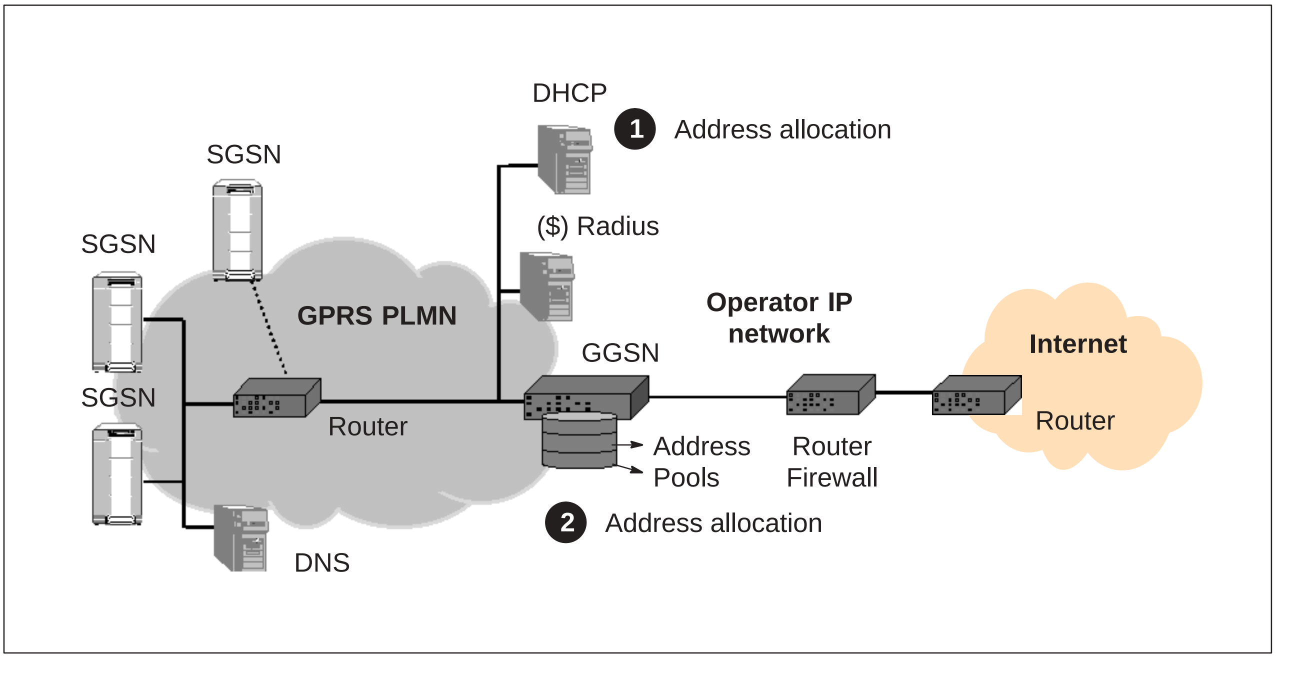


Figure 7–12 Transparent mode for a basic Internet service

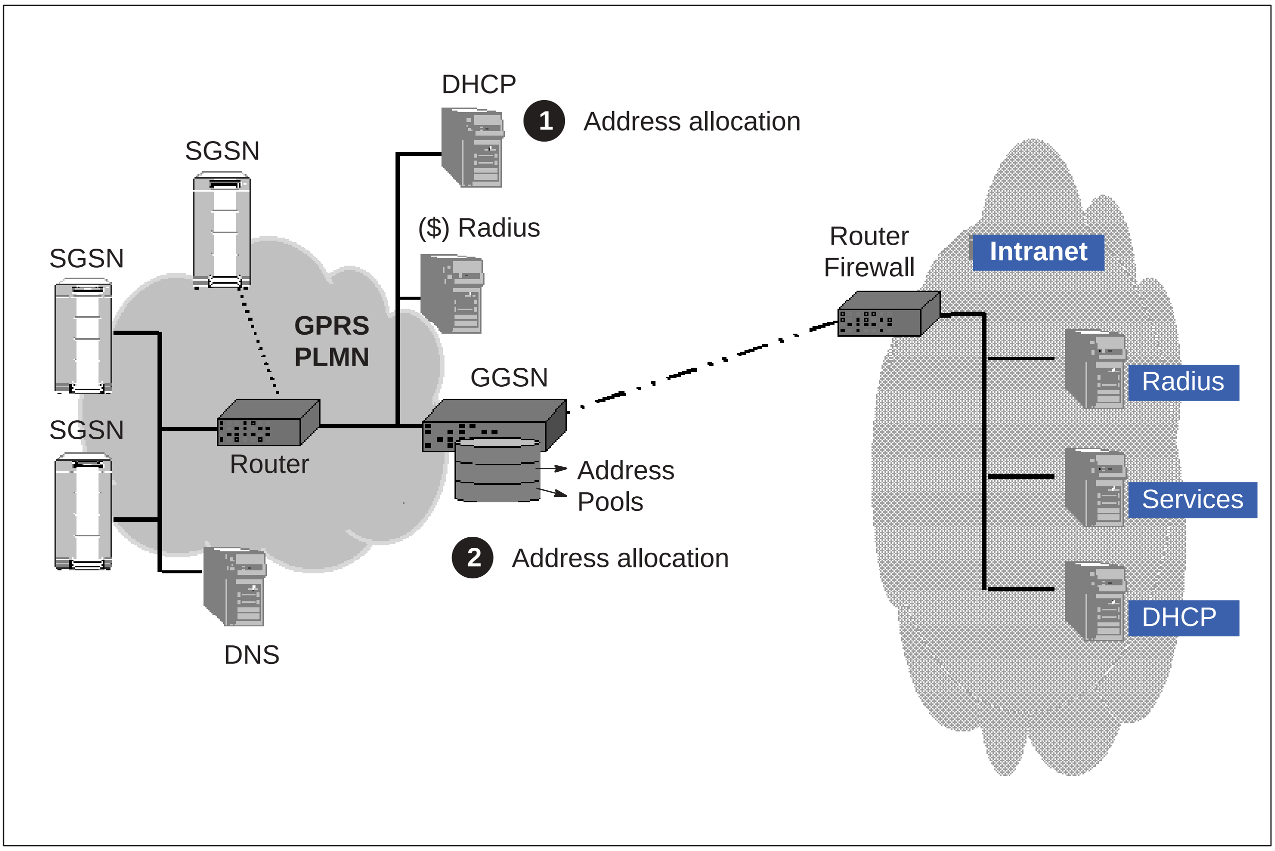


Figure 7–13 Transparent mode for dedicated intranet access

7.3.2.2 Non–transparent access to an Intranet or ISP

With non-transparent access, the GGSN facilitates user access to the ISP or Intranet. The basic principles of non-transparent GPRS access are

- The MS is allocated a private IP address belonging to the ISP or Intranet.
- The GGSN requests user authentication using the user authentication information in the Protocol Configuration Option IE at packet data protocol (PDP) context activation.
- A basic security protocol, such as IPSec, is used between the GGSN and the ISP or intranet if the connection is over an insecure IP network.

In GGSN01, Nortel Networks offers one type of non-transparent interconnection to external IP networks. This type of non-transparent interconnection is called a simplified non-transparent access.

Simplified non-transparent access

The simplified non-transparent access mode is a Nortel Networks solution that provides ISP and Intranet interconnectivity. It is a “simulated PPP PDU type” of interconnection. The simplified non-transparent access mode is an “open standards” solution (with respect to IETF) that is interoperable with CPE tunnel servers (the Intranet external gateway).

In the simplified non-transparent access mode, the GGSN

- terminates a GTP tunnel from the SGSN on an activated PDP context and
- creates an associated PPP session that runs over an L2TP tunnel to the external packet data network (PDN)

The tunnel mapping at the GGSN is one-to-one (GTP to PPP). The GGSN may create the L2TP tunnel using IPSec transfer mode if data transfer is over an insecure network (such as the Internet). In this configuration, the GGSN functions as an L2TP access controller (LAC). The termination point of the L2TP tunnel is called the L2TP network server (LNS). This configuration implicitly gives multi-customer capability for authentication and IP assignment.

With a simplified non-transparent access mode, the GGSN participates in security but not in user authentication. Authentication is performed by the far-end device.

7.3.3 Interface protocols

The following protocols are used on the Gi interface:

- IP protocol
- tunneling protocol

7.3.3.1 IP protocol

For GGSN01, the Gi interface uses IP v4 for interworking with external PDNs. The GGSN supports IP fragmentation.

7.3.3.2 Tunneling protocol

Normally, the type of tunnel implemented between the GGSN and the external IP network is based on mutual agreement. IPSec is supported and recommended if connectivity is established across an insecure network. IPSec minimizes exposure to security risks. IPSec supports both the AH and ESP headers.

The GGSN01 release bases the non-transparent mode of access on the simplified non-transparent access mode or “L2TP over IPSec.” The GPRS specifications suggest a one-to-one tunnel mapping from GTP to IPSec. However, the L2TP over IPSec solution offers the following advantages:

- It supports overlapping IP address allowing multi-customer capability.
- It provides a high level of interoperability with other vendors.

Other tunneling protocols are supported on the CES, such as PPTP and L2F. These tunnels are not currently used for GPRS configurations but can be used for other purposes such as remote customer administration support.

7.4 Gr and Gr’ interfaces

The Gr interfaces an SGSN and an HLR. Since the SGSN and the HLR communicate using different protocols, the protocol messages must be routed through a conversion entity. In the GPRS application, this entity is known as the SS7/IP Gateway, or SIG. The use of the SIG necessitates two types of interface: the Gr interface and the Gr’ interface.

7.4.1 Purpose of the Gr interface

The Gr interfaces the SGSN and the HLR. All operations relevant to SS7 signaling and the HLR in the GPRS system are handled through the Gr interface,which uses Mobile Application Part (MAP).

Figure 7–14 shows the location of the Gr interface.

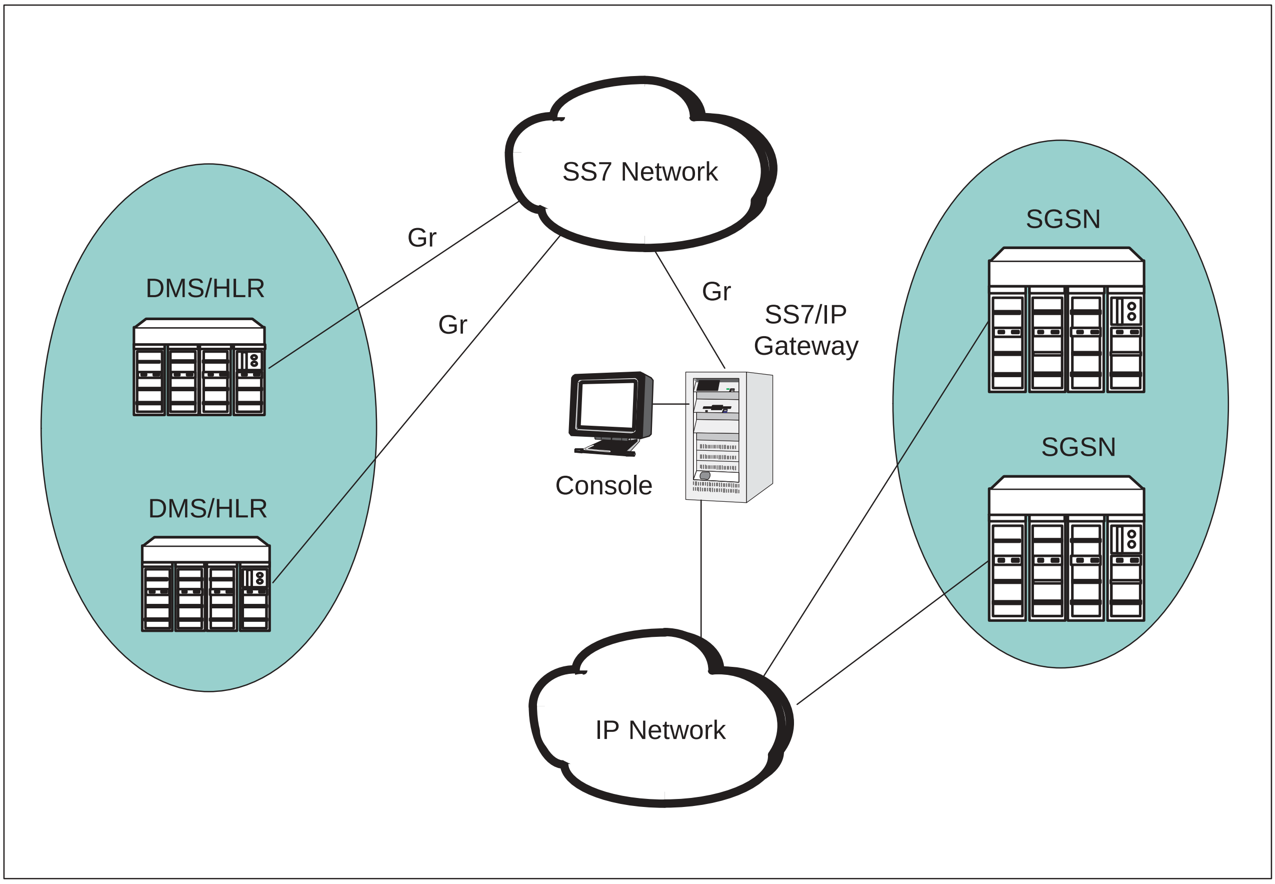


Figure 7–14 Location of the Gr interface

7.4.2 Purpose of the Gr’ interface

Gr’ is a Nortel Networks proprietary signaling protocol that interfaces the SIG and the SGSN. The Gr’ interface uses a protocol layer called SGSN MAP Clients to SS7/IP Gateway Interface Protocol (SSIP). The SSIP protocol layer transports MAP data to and from the IP network as defined in the GSM 09.02 specification. The SSIP protocol layer contains “MAP Intent” data and information that allows nodes to identify and correlate MAP dialogs.

Figure 7–15 shows the location of the Gr’ interface.

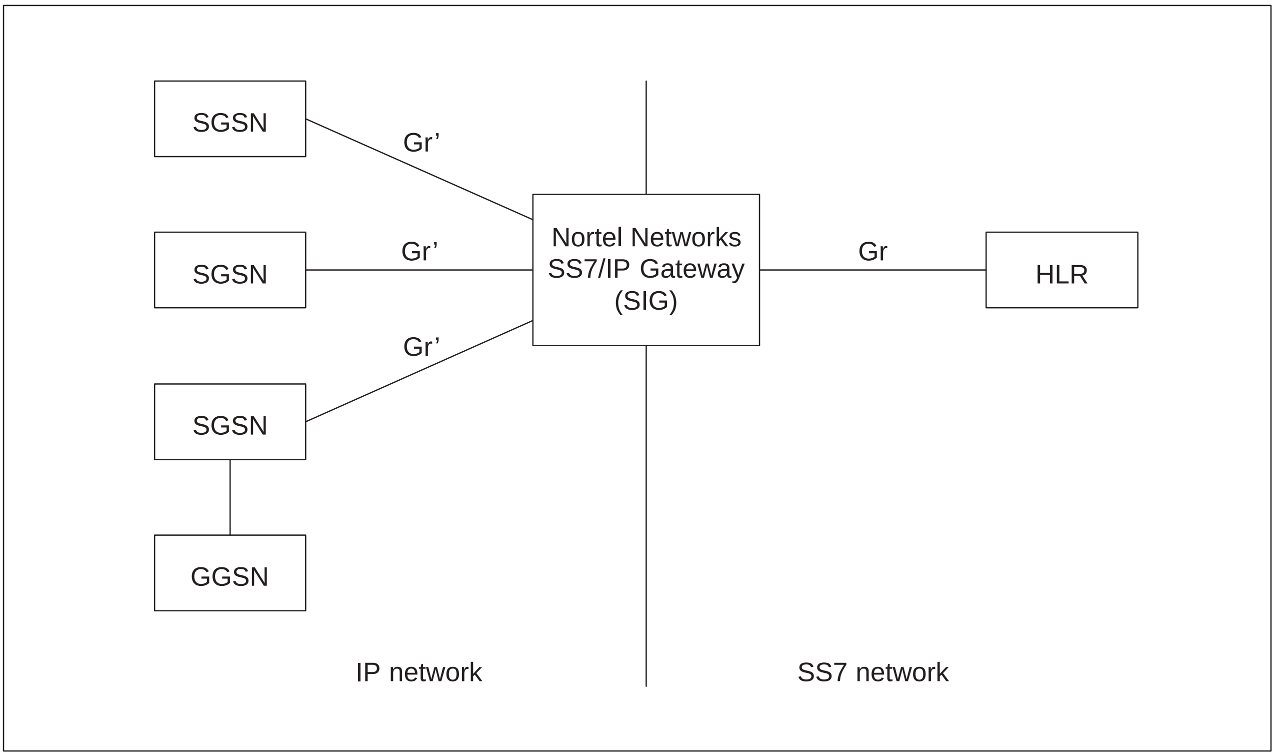


Figure 7–15 Location of the Gr’ interface

In the Nortel Networks GPRS implementation, the SIG provides the TCAP and MAP protocol functions. The SIG also performs the SS7 and IP interworking functions between the SGSN and HLR.

7.4.3 Physical interface

The Gr interface can be a T1, E1, or V.35 interface.

The Gr’ interface is a 100 Base-T Ethernet interface.

7.4.4 Message protocol stacks

The Gr’ and Gr interfaces use different protocol stacks. The Gr’ interface uses the protocol stack used by the SGSN. This protocol stack is referred to as the SGSN MAP Client (MC) protocol stack. The Gr interface uses the protocol stack used by the HLR.

Figure 7–16 illustrates the message protocol stacks for the SGSN MC, SIG, and HLR.

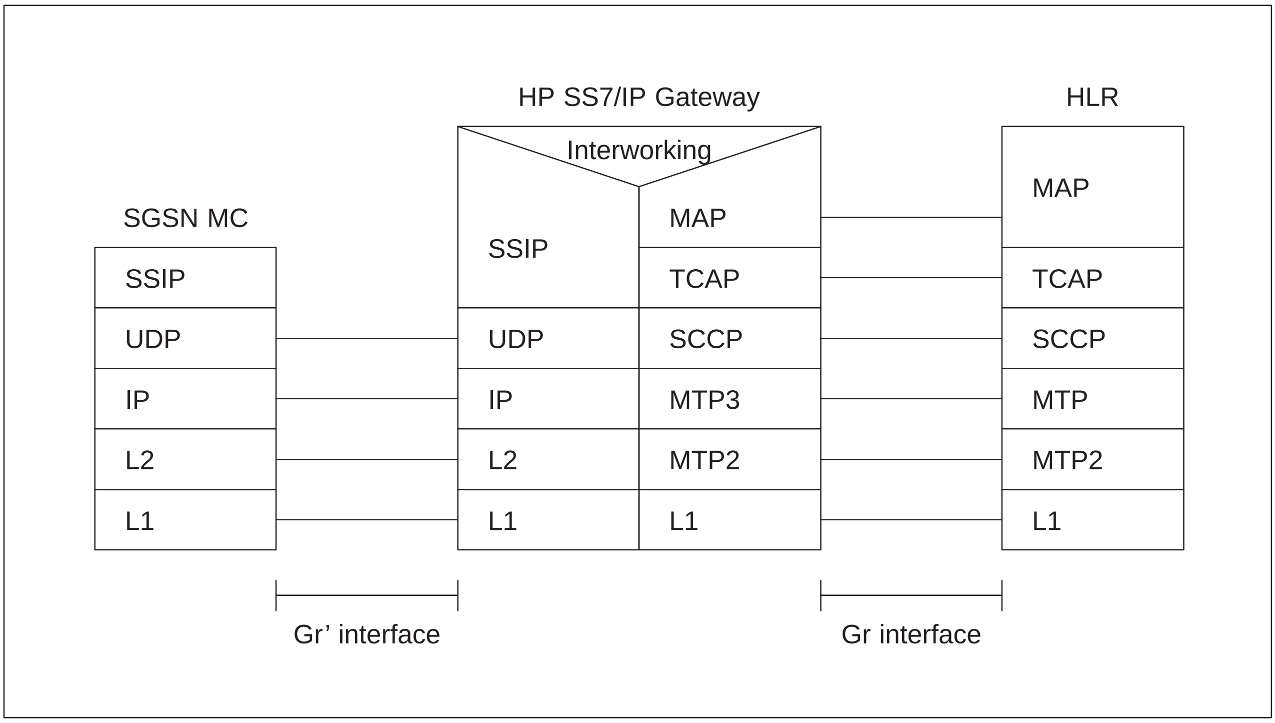


Figure 7–16 Protocol stack for MC, SIG, and HLR

7.4.4.1 The SGSN MC protocol stack

As previously stated, the Gr’ interface uses the SGSN MC protocol stack. MAP Client (MC) is an application that resides on the SGSN. MAP Client enables the SGSN:

- to receive a decoded MAP message from the HLR through the SIG
- to send a decoded MAP message to the HLR through the SIG

The SGSN MC protocol stack is comprised of the SSIP, TCP, and IP protocol layers. The following paragraphs describe the SSIP, UDP, and IP layers.

The SSIP layer

The SSIP portion of the stack performs the following functions:

- It supports signaling exchange with the HLR through the SIG.
- It receives, sends, and processes messages from the SIG.
- It supports the following mobility management operations:
  - updateGprsLocation
  - reset
  - insertSubscriberData
  - deleteSubscriberData
  - cancelLocation
  - sendAuthenticationInfo
- It provides MAP Client Timer for the following messages:
  - insertSubscriberData
  - sendAuthenticationInfo
  - updateGprsLocation
- It provides retry attempts for the following messages when the MAP Client Timer expires:
  - sendAuthenticationInfo
  - updateGprsLocation
- It maps messages sent and received between the MAP Client and the SIG.
- It counts the number of messages received in the SGSN.
- It counts the number of messages sent by the SGSN.
- It handles errors.
- It counts mobility management operations.
- It counts errors.

The IP layer

The Internet Protocol (IP) layer is a connectionless datagram service that provides

- internetwork-wide addressing
- fragmentation and re-assembly
- time-to-live control of datagrams
- checksum verification of header contents

7.4.4.2 The HLR protocol stack

As previously stated, the Gr interface uses the HLR protocol stack shown in *Figure 7–16*. The following paragraphs describe the TCAP, SCCP, and MTP layers found in the protocol stack. For a description of the MAP layer, refer to the GSM 09.02 specification.

The TCAP layer

This layer of the protocol stack provides the signaling function for network databases. TCAP is an SS7 application protocol that provides the platform to support non-circuit related, transaction-based information exchange between network entities.

The SCCP layer

SCCP is part of the ITU-T no. 7 signaling protocol and the SS7 protocol. SCCP provides additional routing and management functions for transferring messages other than call setup between signaling points. SCCP supports TCAP.

The MTP layers

The MTP layers provide functions for basic routing of signaling messages between signaling points.

7.5 Gs and Gs’ interfaces

The Gs interfaces an SGSN and an MSC/VLR. Since the SGSN and the MSC/VLR communicate using different protocols, the messages are routed through the SS7/IP Gateway (SIG) for conversion. The interface between the SIG and the SGSN is known as the Gs’ interface.

7.5.1 Purpose of the Gs interface

The Gs interfaces the SIG and the MSC/VLR.

7.5.2 Purpose of the Gs’ interface

The Gs’ is a Nortel Networks proprietary interface for passing decoded/encoded messages between the SGSN and the SIG. The Gs’ interface uses TCP/IP transport between the SGSN and SIG. The SIG encodes/decodes the SS7/TCAP/BSSAP messages destined for/received from the MSC/VLR in the SS7 network.

7.6 Ga interface

The Ga interfaces the GSNs and the CGF. The GSNs and the CGF are enhanced to support the GTP’ protocol for the Ga interface (GSNs to CGF). GTP’ can be used to collect CDRs from any GPRS element that supports this interface. This feature is desirable for operators who have multiple GPRS suppliers in the core network and plan to collect billing records at a common CGF platform.

7.7 Gd interface

The Gd interface is defined between the SGSN and the GMSC/IWMSC. The interface is capable of utilizing the GPRS backbone to deliver SMS messages. The Gd interface is similar to the Gr interface. Benefits of this method of SMS delivery include:

- Optimisation of network resources
- decreased SMS delivery time
- decreased messaging overhead.

7.8 Gp interface

Gp which exists between Border Gateways for Inter–PLMN roaming allows subscribers to access the HPLMN GGSN from a VPLMN SGSN through a highly secure interface, that is to say an IPSec tunnel. The Gp interface consists of the same signalling messages as those defined for the Gn interface, except the GSN’s are located in different GPRS PLMN’s. Supported Gp signalling includes the same set of Tunnel Management and Path Management messages as supported on the Gn interface.

7.9 Agprs interface

The Agprs interface handles messages between the BSC and the PCUSN.

7.9.1 Agprs OML BSC – PCUSN

It conveys all messages dedicated to OAM for radio related issues.

It is mainly composed of:

- Cell and TDMA Configuration from the BSC to the PCUSN to indicate OMC-R configuration regarding radio–related issues (Cell properties, number of Static TSs dedicated to GPRS)
- Mapping of Static TS to Agprs interface from the BSC to the PCUSN
- PCUSN supervision (event reports from the PCUSN to the BSC)

7.9.2 Agprs RSL BSC – PCUSN

This conveys all the messages dedicated to the allocation of GPRS time slots and dynamic radio time–slot sharing between GSM & GPRS.

It is mainly composed of:

- Indication from the BSC to the PCUSN to define the availability/unavailability of radio TDMA and radio CELL for GPRS
- Time–slot sharing–related messages

7.9.3 Agprs GSL BTS – PCUSN (through BSC)

The BTS terminates the Um CCCH and forwards all the GPRS–specific messages on the GSL to the BSC, which concentrates all BTS messages to the PCUSN.

It is mainly composed of:

- Channel Requests from the mobile station
- Immediate Assignment from the PCUSN to the mobile station
- Paging from the PCUSN to the mobile station

7.9.4 Agprs TRAFFIC BTS – PCUSN (through BSC)

The interface is composed of GPRS traffic at n*16kb/s. The GPRS traffic uses Abis 16Kb/s TS between the BSC and the BTS, and Agprs 16Kb/s TS between the BSC and the PCUSN. They are transparently switched by the BSC.

7.10 OMN interface

For more details, refer to NTP < 01 >.

8 GPRS CHANNELS

8.1 Packet data logical channels and their mapping

8.1.1 General

This section describes the packet data logical channels supported by the radio subsystem.

They are mapped onto the physical channels that are dedicated to packet data. The different packet–data logical channels can be multiplexed (on the downlink or the uplink) onto the same physical channel (i.e. PDCH). The physical channel dedicated to packet data traffic is called a Packet Data CHannel (PDCH).

These channels are provisioned on the OMC-R with two characteristics:

- GPRS–Only channels: These time slots are permanently allocated to GPRS.
- GPRS/GSM Shared channels: These time slots support GPRS but are dynamically configured for GSM or GPRS use.

8.1.2 PCCCH

The Packet Common Control CHannels (PCCCH) are used for the common control signaling required to initiate packet transfers. Four different channels are defined:

- PRACH: random access channel used by the mobile station to access the network (uplink only)
- PPCH: paging channel used to page a mobile station belonging to a given paging group (downlink only)
- PAGCH: Access Grant channel used to assign resources to a mobile station during the packet transfer establishment phase (downlink only)
- PNCH is used to send a PTM-M (Point To Multipoint - Multicast) notification to a group of mobile stations (downlink only).

The mapping of PCCCH onto the physical channels, when it exists, follows one the following rules:

- PCCCH is mapped onto one or several physical channels according to a 51-multiframe. In this case, it occupies the whole of the physical channels along with the PBCCH.
- PCCCH is mapped onto one or several physical channels according to a 52-multiframe. In this case, the PCCCH, PBCCH and PDTCH share the same physical channels (PDCHs).

8.1.3 PBCCH

The Packet Broadcast Control Channel (PBCCH) is used to broadcast System Information (for downlink only). Alternatively, the BCCH (for GSM) can be used.

The PBCCH is mapped onto one or several physical channels. The exact mapping onto each physical channel follows a predefined rule, as it is done for the BCCH.

8.1.4 PDTCH

The Packet Data Traffic CHannel (PDTCH) is allocated for user data transfer. It is temporarily dedicated to one mobile station or to a group of mobile stations in the PTM-M case. In multislot operation, one mobile station may use multiple PDTCHs in parallel for individual packet transfer.

All packet data traffic channels are uni-directional:

- PDTCH/U for a mobile–originated packet transfer (uplink only)
- PDTCH/D) for a mobile–terminated packet transfer (downlink only)

One PDTCH is mapped onto one physical channel. Up to eight PDTCHs, with different time slots but with the same frequency parameters, can be allocated to one mobile station at the same time.

8.1.5 PACCH

The Packet Associated Control CHannel (PACCH) conveys the signaling information related to a given mobile station. It is used to send signaling associated with a packet transfer and resource assignment. PACCH shares resources with the PDTCHs that are currently assigned to one mobile station. Additionally, a mobile station that is currently involved in a packet transfer can be paged for circuit–switched services on PACCH.

PACCH is of a bi-directional nature. It is dynamically allocated:

- on a block basis on the same physical channel as carrying PDTCHs
- both on the uplink and downlink regardless of whether the corresponding PDTCH assignment is for the uplink or the downlink

8.1.6 PTCCH

Two different Packet Timing advance Control CHannels are defined (PTCCH):

- PTCCH/U is used to transmit access bursts to allow estimation of the timing advance for one mobile station
- PTCCH/D is used to transmit timing advance updates for several mobile stations.

8.2 Mapping of logical channels

The mapping of logical channels is defined by a multiframe structure. The multiframe structure for PDCH consists of 52 TDMA frames, divided into 12 blocks of 4 frames, 2 idle frames and 2 frames used for the PTCCH (see *Figure 8–1*).

On a PDCH that does not contain a PCCCH, all the blocks can be used as PDTCH or PACCH.

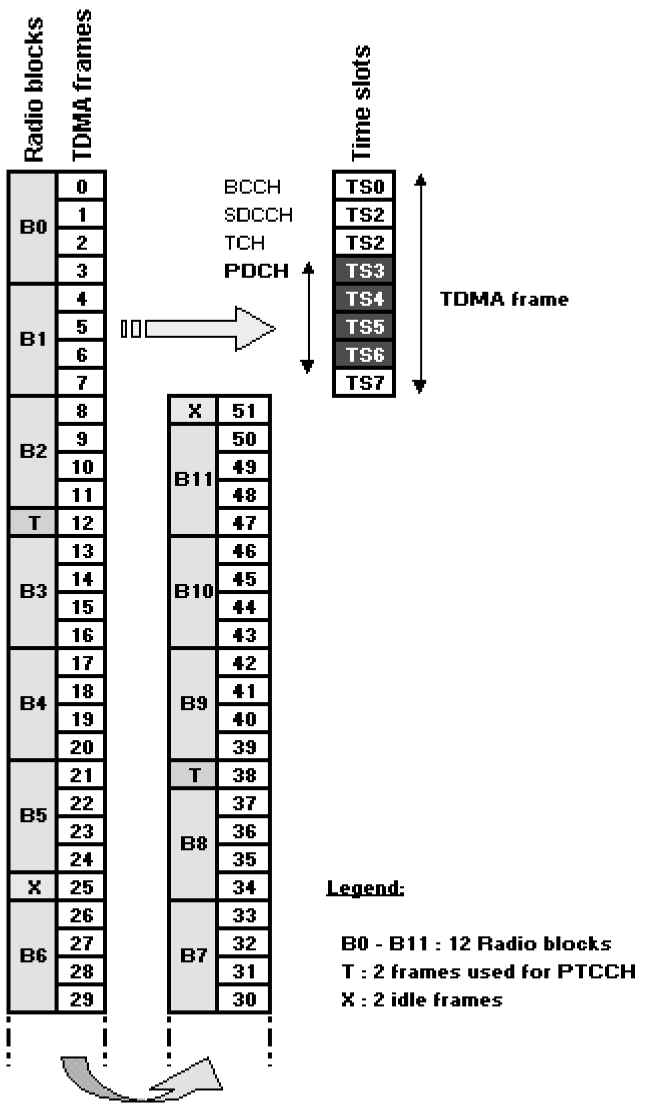


Figure 8–1 Radio interface (Um): Multiframe structure for PDCH

8.3 Radio block structures

Two radio block structures (see *Figure 8–2*) are defined for data transfer and control message transfer purposes. The Radio Block consists of the MAC (Medium Access Control) Header, an RLC (Radio Link Control) Data Block or an RLC/MAC Control Block, and a Block Check Sequence (BCS).

It is always carried by four normal bursts.

- The MAC Header (1 octet) comprises:
  - Uplink State Fag (USF): 3 bits
  - RLC Block Type (T): 1 bit. This indicates whether the RLC block is an RLC data or an RLC/MAC control block.
  - Power Control (PC): 4 bits. This contains the transmitted power level from the BTS (in downlink).
- The RLC Data Block is formed by:
  - The RLC Data Block Header which consists of:
    - Temporary Flow Identity (TFI): 7 bits. This identifies the Temporary Block Flow (TBF) to which the RLC data block belongs.
    - Supplementary/Polling (S/P): 1 bit. On the downlink, this is used to poll the MS to send an acknowledgment for current downlink transfer.
    - Block Sequence Number (BSN): 7 bits. This contains the number associated to current block (in order to reassemble the LLC frame).
    - Extension (E): 1 bit. This indicates whether there is an extension field (1 extra octet).
  - RLC Data Block information.
- The BCS is used for backward error correction; its length depends on the Coding.

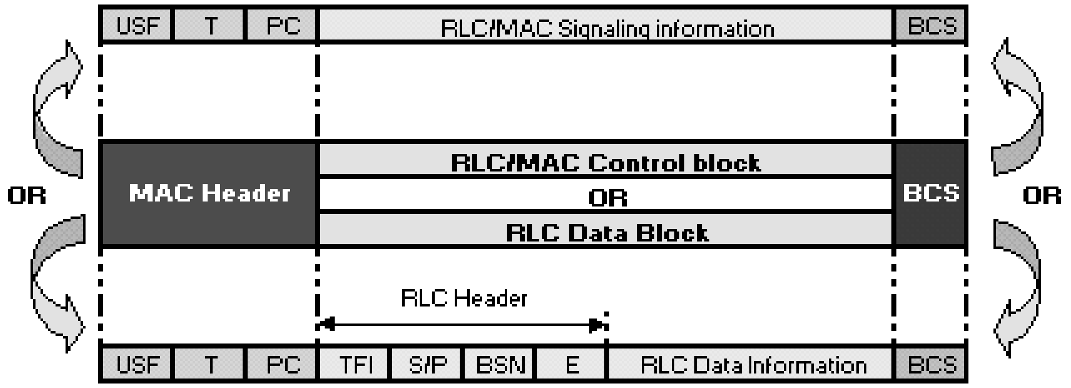


Figure 8–2 Radio block structures

PAGE INTENTIONALLY LEFT BLANK

Wireless Service Provider Solutions
GPRS Overview

Publication Reference
PE/DCL/DD/0117 411–9001–117
13.01/EN
July 2001
Printed in France

NORTEL NETWORKS

For more information, please contact:

For all countries, except USA:

Documentation Department
1, Place des Frères Montgolfier
GUYANCOURT
78928 YVELINES CEDEX 9
FRANCE
Email : gsmntp@nortelnetworks.com
Fax : (33) (1) 39–44–50–29

In the USA:

2221 Lakeside Boulevard
Richardson TX 75082
USA
Tel: 1–800–4 NORTEL
1–800–466–7838 or (972) 684–5935

Internet Address:

*http://***www.nortelnetworks.com**