ETSI TS 127 060 V3.4.0 (2000-03)

Technical Specification

Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
Mobile Station (MS) supporting Packet Switched Services
(3G TS 27.060 version 3.4.0 Release 1999)

GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

Reference

RTS/TSGN-0327060UR1

Keywords

GSM, UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at http://www.etsi.org/tb/status/

If you find errors in the present document, send your comment to:
editor@etsi.fr

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by the ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under www.etsi.org/key .

Contents

Foreword

This Technical Specification (TS) has been produced by the 3rd Generation Partnership Project (3GPP).

The present document defines the requirements for TE-MT interworking over the R-reference point for the Packet Domain, within the GSM and 3GPP systems. In addition, annex B describes the Octet Stream Protocol (OSP) PDP type.

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

The present document defines the requirements for TE-MT interworking over the R-reference point for the Packet Domain, within the GSM and 3GPP systems. It is up to the manufacturer how to implement the various functions but the present document and existing 3G TS 27.001, 27.002, and 27.003 shall be followed where applicable.

It is the intention that the present document shall remain as the specification to develop a MS for support of Packet Switched services and its text includes references to UMTS/GSM standards.

1 Scope

The UMTS/GSM PLMN supports a wide range of voice and non-voice services in the same network. In order to enable non-voice traffic in the PLMN there is a need to connect various kinds of terminal equipments to the Mobile Station (MS). The present document defines the requirements for TE-MT interworking over the R-reference point for the Packet Domain , including the protocols and signalling needed to support Packet Switched services, as defined in 3G TS 22.060 and 3G TS 23.060.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] GSM 01.04: “Digital cellular telecommunication system (Phase 2+); Abbreviations and acronyms”.

[2] 3G TS 22.002: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Circuit Bearer Services (BS) supported by a GSM Public Land Mobile Network (PLMN)".

[3] 3G TS 22.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service Description Stage 1".

[4] 3G TS 23.002: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network architecture".

[5] 3G TS 23.003: "3rd Generation Partnership Project; Technical Specification Group Core Network; Numbering, addressing and identification".

[6] GSM 03.10: "Digital cellular telecommunication system (Phase 2+); GSM Public Land Mobile Network (PLMN) connection types".

[7] 3G TS 23.122: "3rd Generation Partnership Project; Technical Specification Group Core Network; NAS Functions related to Mobile Station (MS) in idle mode".

[8] 3G TS 23.040: "3rd Generation Partnership Project; Technical Specification Group Terminals; Technical realization of the Short Message Service (SMS)".

[9] 3G TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Service Description Stage 2".

[10] GSM 04.02: "Digital cellular telecommunication system (Phase 2+); GSM Public Land Mobile Network (PLMN) access reference configuration".

[11] 3G TS 24.007: "3rd Generation Partnership Project; Technical Specification Group Core Network; Mobile radio interface signalling layer 3; General aspects".

[12] 3G TS 24.008: "3rd Generation Partnership Project; Universal Mobile Telecommunications System;Technical; Mobile radio interface layer 3 specification, Core Network Protocols - Stage 3".

[13] GSM 04.60: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Mobile Station (MS) - Base Station System (BSS) interface; Radio Link Control / Medium Access Control (RLC/MAC) protocol".

[14] GSM 04.64: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Logical Link Control (LLC)".

[15] 3G TS 24.065: "3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); Mobile Station (MS) - Serving GPRS Support Node (SGSN); Subnetwork Dependent Convergence Protocol (SNDCP)".

[16] 3G TS 27.007: "3rd Generation Partnership Project; Technical Specification Group Terminals; AT command set for 3GPP User Equipment (UE)".

[17] 3G TS 29.061: "3RD Generation Partnership Project; Technical Specification Group Core Network; Packet Domain; Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)".

[18] CCITT Recommendation E.164: "Numbering plan for the ISDN era".

[19] CCITT Recommendation V.42 bis: "Data communication over the telephone network – Data compression procedures for data circuit-terminating equipment (DCE) using error correction procedures".

[20] <VOID>

[21] <VOID>

[22] <VOID>

[23] <VOID>

[24] <VOID>

[25] <VOID>

[26] IETF RFC 768 (1980): "User Datagram Protocol" (STD 6).

[27] IETF RFC 791 (1981): "Internet Protocol" (STD 5).

[28] IETF RFC 792 (1981): "Internet Control Message Protocol" (STD 5).

[29] IETF RFC 793 (1981): "Transmission Control Protocol" (STD 7).

[30] ITU-T Recommendation V.250 (ex V.25ter): "Serial asynchronous automatic dialling and control".

[31] ITU-T Recommendation V.24: "List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE)".

[32] ITU-T Recommendation V.28: "Electrical Chracteristics for unbalanced double-current interchange circuits".

[33] ITU-T Recommendation V.80: "In-band DCE control and synchronous data modes for asynchronous DTE".

[34] IETF RFC 1661 (1994): “The Point-to-Point Protocol (PPP)” (STD 51).

[35] IETF RFC 1662 (1994): “PPP in HDLC-like framing” (STD 51).

[36] IETF RFC 1700 (1994): “Assigned Numbers” (STD 2).

[37] IETF RFC 1570 (1994): ”PPP LCP Extensions“.

[38] IETF RFC 1989 (1996): ”PPP Link Quality Monitoring“.

[39] IETF RFC 1332 (1992): ”The PPP Internet Protocol Control Protocol (IPCP)“.

[40] IETF RFC 1877 (1995): ”PPP IPCP Extensions for Name Server Addresses “.

[41] IETF RFC 2153 (1997): ”PPP Vendor Extensions“.

[42] IETF RFC 1334 (1992): ”PPP Authentication Protocols“.

[43] IETF RFC 1994 (1996): ”PPP Challenge Handshake Authentication Protocol“.

[44] IETF RFC 2686 (1999): ”The Multi-Class Extension to Multi-Link PPP”.

[45] IETF RFC 1990 (1996): ”The PPP Multilink Protocol (MP)“.

[46] IETF RFC 2472 (1998): ”IP Version 6 over PPP".

3 Definitions abbreviations and symbols

3.1 Definitions

For the purposes of the present document, the following terms and definitions given in 3G TS 22.060 and 3G TS 23.060 and the following apply:

2G- / 3G-: prefixes 2G- and 3G- refers to functionality that supports only GSM or UMTS, respectively, e.g., 2G-SGSN refers only to the GSM functionality of an SGSN. When the prefix is omitted, reference is made independently from the GSM or UMTS functionality.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

APN	Access Point Name
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSN	GPRS Support Node
GTP-U	GPRS Tunnelling Protocol for user plane
HDLC	High Level Data Link Control
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IHOSS	Internet Hosted Octet Stream Service
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LA	Location Area
LCP	Link Control Protocol
LLC	Logical Link Control
MAC	Medium Access Control
MCML	Multi-Class Multi-Link PPP
ME	Mobile Equipment
MP	Multilink PPP
MS	Mobile Station
MT	Mobile Termination
NCP	Network Control Protocol
OSP	Octet Stream Protocol
OSP:IHOSS	Octet Stream Protocol for Internet Hosted Octet Stream Service
PAD	Packet Assembler/Disassembler
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PDP	Packet Data Protocol , e.g., IP or PPP
PDU	Protocol Data Unit
PPP	Point-to-Point Protocol
PS	Packet Switched
PTM	Point To Multipoint
PTP	Point To Point
PVC	Permanent Virtual Circuit

RA	Routing Area
SGSN	Serving GPRS Support Node
SNDCP	SubNetwork Dependent Convergence Protocol
TCP	Transmission Control Protocol
TE	Terminal Equipment
TFT	Traffic Flow Template
UDP	User Datagram Protocol

3.3 Symbols

For the purposes of the present document, the following symbols apply:

Gb	Interface between a SGSN and a BSC.
Gi	Reference point between the Packet Domain and an external packet data network.
Gn	Interface between two GSNs within the same PLMN.
Gp	Interface between two GSNs in different PLMNs. The Gp interface allows support of Packet Domain network services across areas served by the co-operating PLMNs.
Gs	Interface between an SGSN and MSC.
Iu	Interface between the RNS and the core network. It is also considered as a reference point.
R	The reference point between a non-ISDN compatible TE and MT. Typically this reference point supports a standard serial interface.
Um	The interface between the MS and the GSM fixed network part. The Um interface is the GSM network interface for providing packet data services over the radio to the MS. The MT part of the MS is used to access the GSM services through this interface.
Uu	Interface between the mobile station (MS) and the UMTS fixed network part. The Uu interface is the UMTS network interface for providing packet data services over the radio to the MS. The MT part of the MS is used to access the UMTS services through this interface.

4 Access reference configuration

Figure 1 shows the relationship between the MS, its terminal equipment and the UMTS/GSM network in the overall Packet Domain environment.

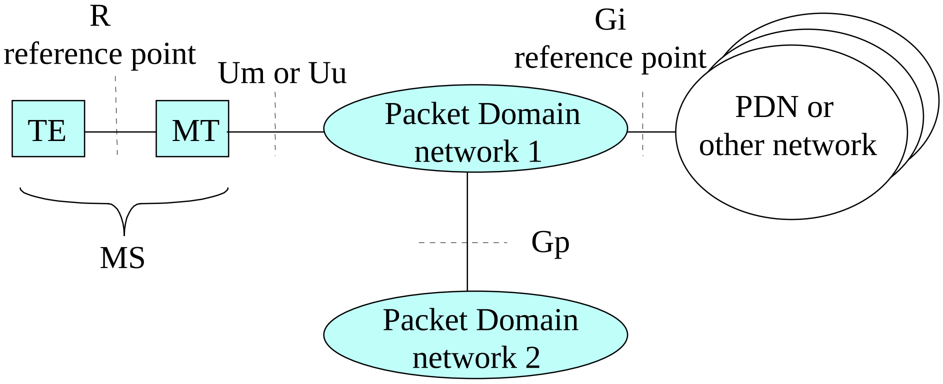


Figure 1: Packet Domain Access Interfaces and Reference Points

5 Functions to support data services

The main functions of the MT to support data services are:

- physical connection at the reference point R;
- flow control between TE and MT;
- mapping of user signalling to/from the Packet Domain bearer;

- mapping of packets belonging to different flows to appropriate PDP contexts;
- support of data integrity between the terminal equipment and the Packet Domain bearer;
- functions to support character based data;
- functions to support packet based data.

6 Interface to Packet Domain Bearer Services

6.1 GSM

The following figure 2 shows the relationship of the GSM Packet Domain Bearer, terminating at the SNDCP layer, to the rest of the GSM Packet Domain environment. It is shown for reference purposes only and detailed information can be found in 3G TS 23.060.

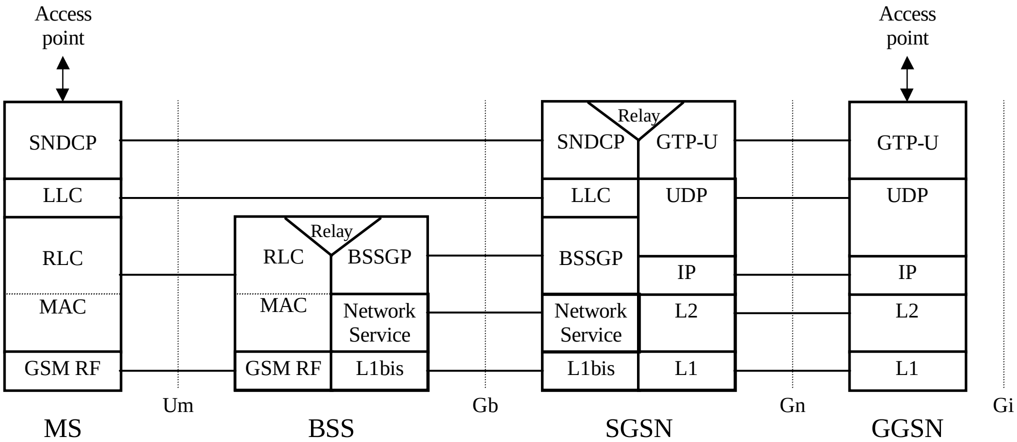


Figure 2: User Plane for Packet Domain services in GSM

6.2 UMTS

The following figure 2a shows the relationship of the UMTS Packet Domain Bearer, terminating at the PDCP layer, to the rest of the UMTS Packet Domain environment. It is shown for reference purposes only and detailed information can be found in 3G TS 23.060.

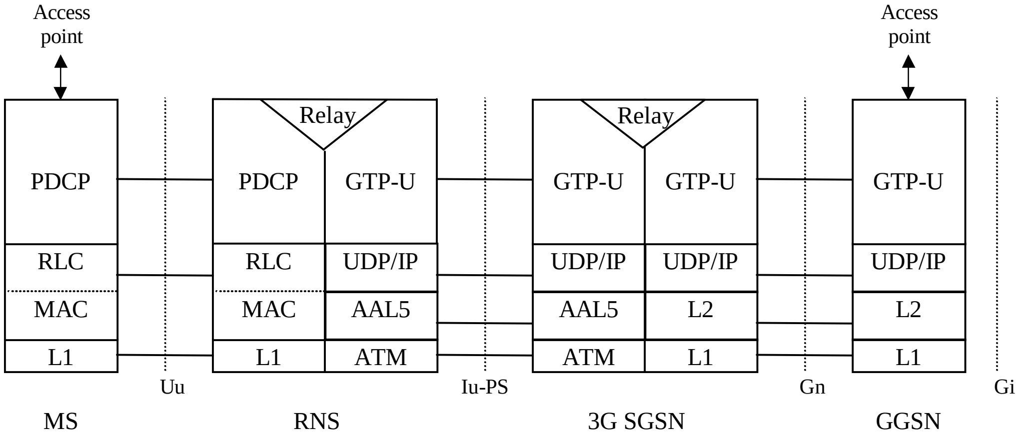


Figure 2a: User Plane for Packet Domain services in UMTS

7 Functions common to all configurations of a MS supporting Packet Switched Services

7.1 Mobile Station Modes of Operation

Three GSM MS modes of operation are identified: Class A, B, and C. These modes of operation are described in 3G TS 23.060.

Three UMTS MS modes of operation are supported in UMTS: A PS/CS mode of operation corresponds to class-A mode of operation in GSM. A PS mode of operation corresponds to class-C mode of operation in GSM. A CS mode of operation is out of scope in the present document.

7.2 Physical Interface

The physical interface between the TE and the MT may conform to CCITT/ITU-T V.24/V.28, or to IrDA IrPHY physical standard specification, or to PCMCIA PC-Card electrical specification. All signal levels and their operation shall be as specified in 3G TS 27.001, 27.002, and 27.003.

7.3 Terminal context procedures

This subclause describes the relationships for PS Attach and Detach, and PDP Context Activation, Modification and Deactivation. The procedures for these functions are described in 3G TS 23.060.

7.3.1 PS Attach

The PS Attach shall be performed prior to activating a PDP context. The PS Attach may be performed automatically or manually depending on the manufacturer's implementation and configuration.

7.3.2 PS Detach

The PS Detach may be performed automatically or manually depending on the manufacturer's implementation and configuration. The following cases are valid:

- if the connection between the TE and MT is broken then the MT may perform the PS Detach procedure;
- if the network originates a PS Detach the MT may inform the TE;
- if the radio connection is broken then the MT may inform the TE;
- if the TE deactivates the last PDP context then the MT may perform the PS Detach procedure.

7.3.3 MS Originated PDP Context Activation

The PDP Context Activation procedure may be performed automatically or manually depending on the manufacturer's implementation and configuration. Depending on the manufacturer's implementation and configuration, 0, 1, or more PDP contexts can be active simultaneously.

7.3.4 MS Originated Secondary PDP Context Activation

The Secondary PDP Context Activation procedure may be performed automatically or manually depending on the manufacturer's implementation and configuration. Depending on the manufacturer's implementation and configuration, 0, 1, or more PDP contexts can be active simultaneously for the same PDP address.

7.3.5 Network Requested PDP Context Activation.

The network can request a PS attached MS to activate a specific PDP context.

7.3.6 MS-Initiated PDP Context Modification

The MS-Initiated PDP Context Modification procedure may be performed automatically or manually depending on the manufacturer's implementation and configuration.

7.3.7 PDP Context Deactivation

The PDP Deactivation may be performed automatically or manually depending on the manufacturer's implementation and configuration. The following cases are valid:

- if the connection between the MT and the TE is broken then the MT may perform the PDP Context Deactivation procedure;
- if the radio connection is broken then the MT may inform the TE;
- if the TE deactivates the last PDP context then the MT may perform the PS Detach procedure.

7.3.8 PDP context related parameters

7.3.8.1 2G-MS

It shall be possible to enquire and/or set the following parameters:

- requested quality of service;
- traffic flow template;
- compression on or off;
- TCP/IP header compression on or off;
- PDP address;
- PDP type;
- Access Point Name (APN);
- protocol configuration options (if required by the PDP type).

7.3.8.2 3G-MS

It shall be possible to enquire and/or set the following parameters:

- requested quality of service;
- traffic flow template;
- protocol control information compression, on or off;
- PDP address;
- PDP type;
- Access Point Name (APN);
- protocol configuration options (if required by the PDP type).

8 <VOID>

9 IP Based Services

All protocols that are supported by the underlying IP protocol are applicable in the Packet Domain environment. However there may be some limitations due to the RF environment.

The IP protocol can be run over various underlying protocols as shown in the figure 6.

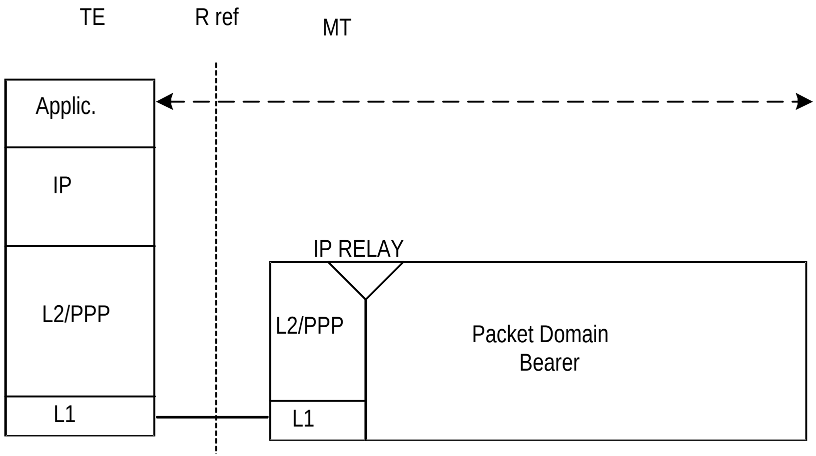


Figure 6: IP Based Services

PPP is a widely supported protocol in numerous operating systems and this alleviates the need for any Packet Domain specific protocol at the TE. PPP at the MT shall comply with the following specifications IETF STD 51 (RFC 1661, RFC 1662), RFC 1570, RFC 1989, RFC 1332, and optionally RFC 2472 for IPv6. The Domain Name Server information shall be delivered as defined in RFC 1877. The delivery of vendor-specific packets and options shall conform to RFC 2153.

As an alternative to PPP, an L2 protocol can be used which is defined as a manufacturer's operating system dependent protocol capable of carrying IP frames over the R reference point. An example for such an L2 protocol is the Multi-Class Multi-Link (MCML) PPP. The MCML is defined in RFC 2686 and is based on Multi-Link (MP) PPP which is defined in RFC 1990.

9.1 Example mapping of functions between the R reference point and the Packet Domain bearer for IP over PPP

The following example illustrates the case when the IP over PPP functionality is used in the MT. The example does not include all the details of PPP, but only describes the logical operation of PPP connection establishment, host authentication and IP configuration.

Each interface at the R reference point can support only one PPP connection and each PPP connection can support only one IP session. Therefore, in PPP mode only one IP PDP context can be activated per interface at the R reference point. However, it is possible for a PCMCIA card (or other multiplexed interfaces) to support multiple virtual interfaces (communications ports) at the R reference point. Multiple PPP connections and IP contexts are possible in this case.

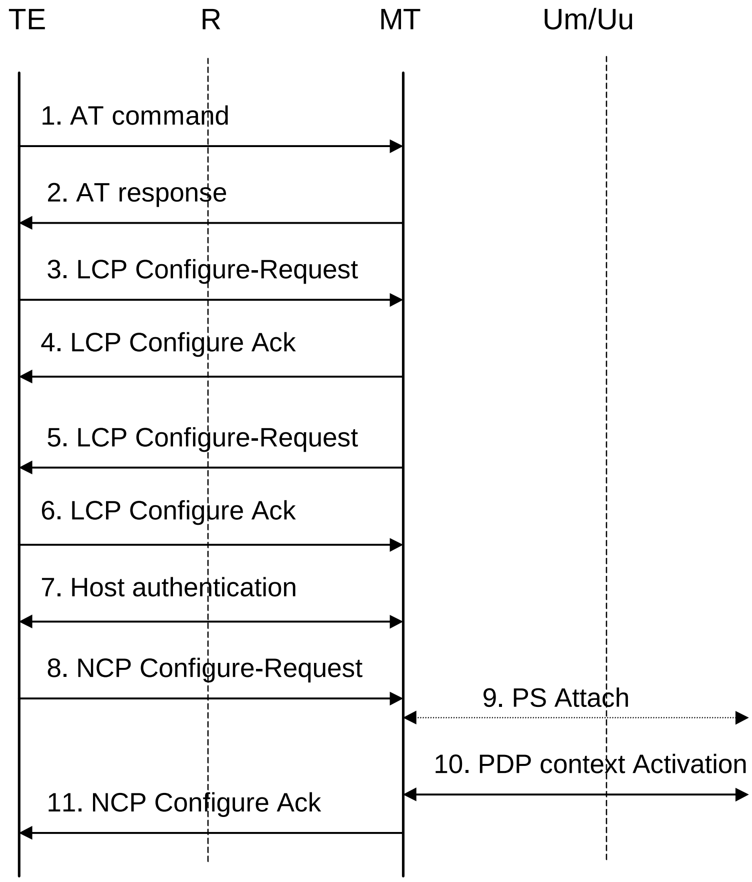


Figure 7: IP Over PPP Based Service

1) The TE issues AT commands to set up parameters and enter PPP mode (refer to subclause on AT commands for further details).

2) The MT sends AT responses to the TE.

3) The PPP protocol in the TE sends a LCP Configure-Request. This command is to establish a PPP link between the TE and the MT.

4) The MT returns LCP Configure-Ack to the TE to confirm that the PPP link has been established. The MT might previously have sent a LCP Configure-Nak in order to reject some options proposed by the TE. This in turn might have triggered a retransmission of the LCP Configure-Request with different options.

5) The PPP protocol in the MT sends a LCP Configure-Request in order to negotiate for the authentication protocol used for authentication of the host TE towards the MT. The MT shall initially negotiate for CHAP, and if this is unsuccessful, for PAP.

6) The TE returns a LCP Configure-Ack to the MT to confirm the use of the specified authentication protocol. The MT might previously have sent a LCP Configure-Nak in order to reject the protocol proposed by the TE. This in turn might have triggered a retransmission of the LCP Configure-Request with different options.

7) If the negotiated authentication protocol is either of CHAP or PAP, the TE authenticates itself towards the MT by means of that protocol. The MT stores the necessary authentication data and sends a locally generated positive acknowledgement of the authentication to the TE. If none of the protocols is supported by the host TE no authentication shall be performed. Refer to 3G TS 29.061 for further details on the authentication.

8) The PPP protocol in the TE sends to the MT a NCP Configure-Request. This command activates the IP protocol.

9) If the MS is not yet PS attached, the MT performs the PS Attach procedure as described in 3G TS 23.060.

10) The MT performs a PDP Context Activation as described in 3G TS 23.60. IP configuration parameters may be carried between the MT and the network in the Protocol Configuration Options IE in PDP Context Activation messages. The Protocol Configuration Options IE sent to the network may contain zero or one NCP Configure-Request packet (in addition to any LCP and authentication packets). The Protocol Configuration Options IE received from the network may contain zero or one NCP Configure-Ack, zero or one Configure-Nak and/or zero or one Configure-Reject packets (in addition to any LCP and authentication packets).

11) Based on the information received in the Protocol Configuration Options IE, the MT acknowledges to the PPP protocol in the TE that the IP protocol is now activated by sending a NCP Configure-Ack command. Before sending a NCP Configure-Ack, the MT might previously have sent a NCP Configure-Nak and/or Configure-Reject in order to reject some IP parameters proposed by the TE. This in turn might have triggered a retransmission of the NCP Configure-Request with different parameter values. The decision to reject a specific parameter or parameter value may be based on the information received from the network in the Protocol Configuration Options IE. NCP Configure-Ack may also carry IP protocol related parameters such as dynamic IP address to the TE. The MT shall also pass name server information to the TE if the TE has requested for it and if this information is provided by the GGSN. Other packet types and options may optionally be delivered. The MT may choose to immediately deactivate the PDP context due to the information received from the network in the Protocol Configurations Options IE.

9.2 Example mapping of functions between the R reference point and the Packet Domain bearer for IP over MCML PPP

When MCML is used instead of standard PPP [34] at the R-reference point, it is possible to support multiple IP sessions on one MCML connection. This is achieved by using an additional MP header after the standard PPP header. MCML provides two different MP headers, a 2-byte header to have four IP sessions and a 4-byte header to have sixteen IP sessions multiplexed over the MCML connection.

Since both MP and MCML closely follow the PPP connection establishment and negotiation model described in subclause 9.1, it is not replicated in this subclause. The major difference is the additional negotiation capabilities used during the LCP configuration negotiation [44], [45].

10 PPP Based Services

By means of the PDP type ‘PPP’ the Packet Domain may support interworking with networks based on the point-to-point protocol (PPP), as well as with networks based on any protocol supported by PPP through one of its Network Control Protocols (NCPs). It may also support interworking by means of tunnelled PPP, by e.g. the Layer Two Tunnelling Protocol (L2TP). The protocol configurations are depicted in figures 8a and 8b.

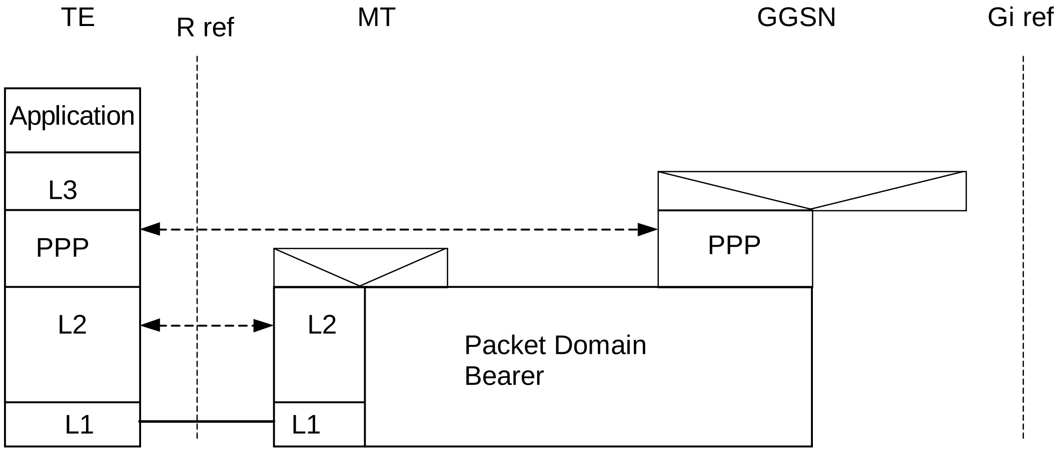
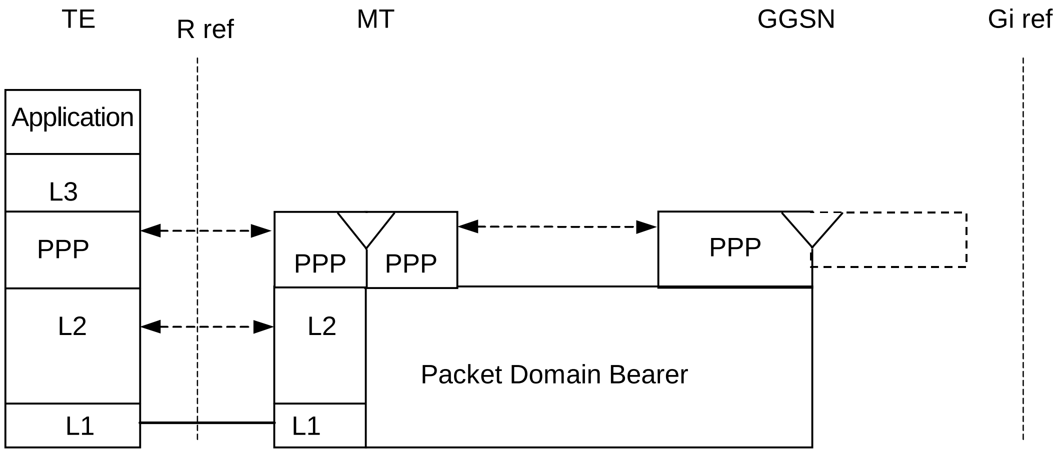


Figure 8a: PPP Based Services (transparent PPP negotiation)



NOTE. In the above case the 'L2' protocol is compliant with [35].

Figure 8b: PPP Based Services (relayed PPP negotiation)

The ‘L3’ protocol is a network layer protocol supported by one of the PPP NCP’s. All protocols currently supported by NCP’s are listed in [36].

The PPP is a widely supported protocol in numerous operating systems and this alleviates the need for any Packet Domain specific protocol at the TE. PPP at the GGSN shall comply with [34]. The Domain Name Server information shall be delivered as defined in [40]. The delivery of any vendor-specific packets and options shall conform to [41].

The ‘L2’ protocol may be the link layer protocol defined for the PPP suite [35]. As an alternative an 'L2' protocol can be used which is defined as a manufacturer’s operating system dependent protocol capable of carrying PPP frames over the R reference point. In case the link layer protocol defined for the PPP suite [35] is used as 'L2' protocol, the MT may negotiate LCP options related to the 'L2' framing (e.g. 'ACCM' [35], 'ACFC' [34] and 'FCS-Alternatives' [37]), with the TE. The MT shall remove the 'L1' and 'L2' specific framing from PPP frames in the uplink direction and add it in the downlink direction (see figure 8b).

10.1 Example mapping of functions between the R reference point and the Packet Domain bearer (transparent PPP negotiation)

The following example illustrates the case when the PPP negotiation is carried out transparently between the TE and the GGSN. The example does not include all the details of PPP, but only describes the logical operation of PPP LCP, host authentication and PPP NCP negotiations.

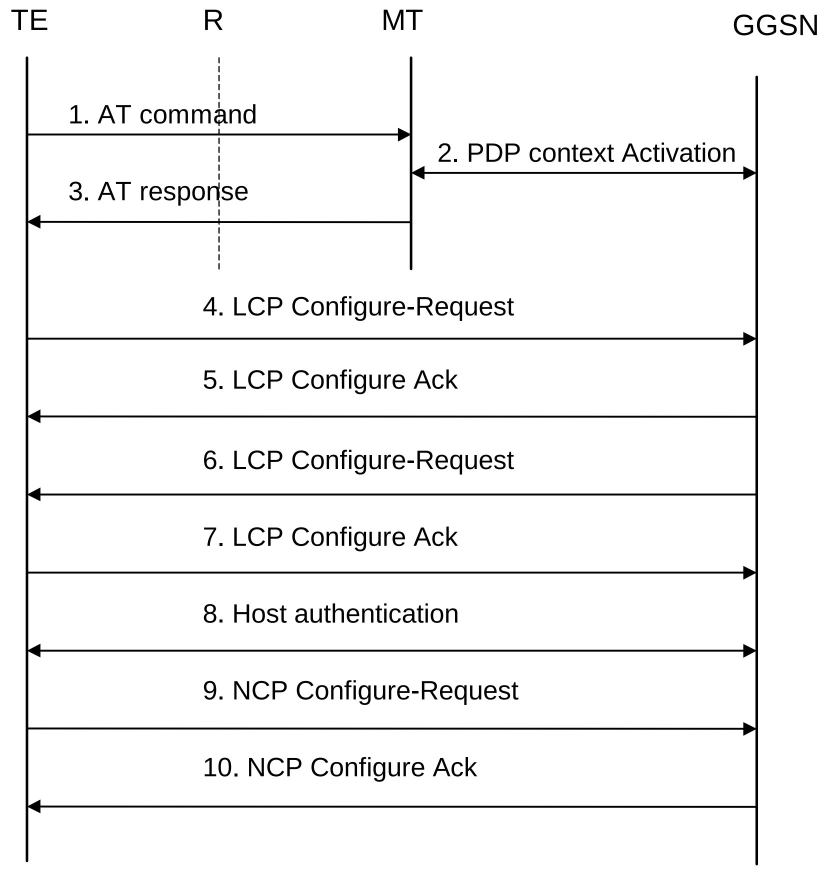


Figure 9a: PPP Based Service (transparent PPP negotiation)

1) The TE issues AT commands to set up parameters and activate a PDP Context (refer to sub-clause on AT commands for further details).

2) The MT performs a PDP Context Activation as described in 3G TS 23.060.

3) The MT sends AT responses to the TE.

4) The PPP protocol in the TE sends an LCP Configure-Request. This command establishes a PPP link between the TE and the GGSN.

5) The GGSN returns an LCP Configure-Ack to the TE to confirm that the PPP link has been established. The GGSN might previously have sent an LCP Configure-Nak in order to reject some options proposed by the TE. This in turn might have triggered a retransmission of the LCP Configure-Request with different options.

6) The PPP protocol in the GGSN sends an LCP Configure-Request in order to negotiate for the authentication protocol used for authentication of the host TE towards the GGSN.

7) The TE returns an LCP Configure-Ack to the GGSN to confirm the use of the specified authentication protocol. The GGSN might previously have sent an LCP Configure-Nak in order to reject the protocol proposed by the TE. This in turn might have triggered a retransmission of the LCP Configure-Request with different options.

8) The TE authenticates itself towards the GGSN by means of the negotiated protocol. If no authentication protocol can be negotiated the GGSN may reject the PPP connection. Refer to GSM 09.61 for further details on the authentication.

9) The PPP protocol in the TE sends to the GGSN an NCP Configure-Request. This command activates the network layer protocol.

10) The GGSN acknowledges to the PPP protocol in the TE that the network layer protocol is now activated by sending an NCP Configure-Ack command. Before sending an NCP Configure-Ack, the GGSN might previously have sent an NCP Configure-Nak in order to reject some parameters proposed by the TE. This in turn might have triggered a retransmission of the NCP Configure-Request with different parameter values.

10.2 Example mapping of functions between the R reference point and the Packet Domain bearer (relayed PPP negotiation)

The following example illustrates the case where the link layer protocol defined for the PPP suite [35] is used as 'L2' protocol. The LCP options related to the 'L2' framing (e.g. 'ACCM', 'ACFC' and 'FCS-Alternatives') are negotiated between the TE and the MT. All other PPP negotiation is relayed transparently between the TE and the GGSN. The example does not include all the details of PPP, but only describes the logical operation of PPP LCP, host authentication and PPP NCP negotiations.

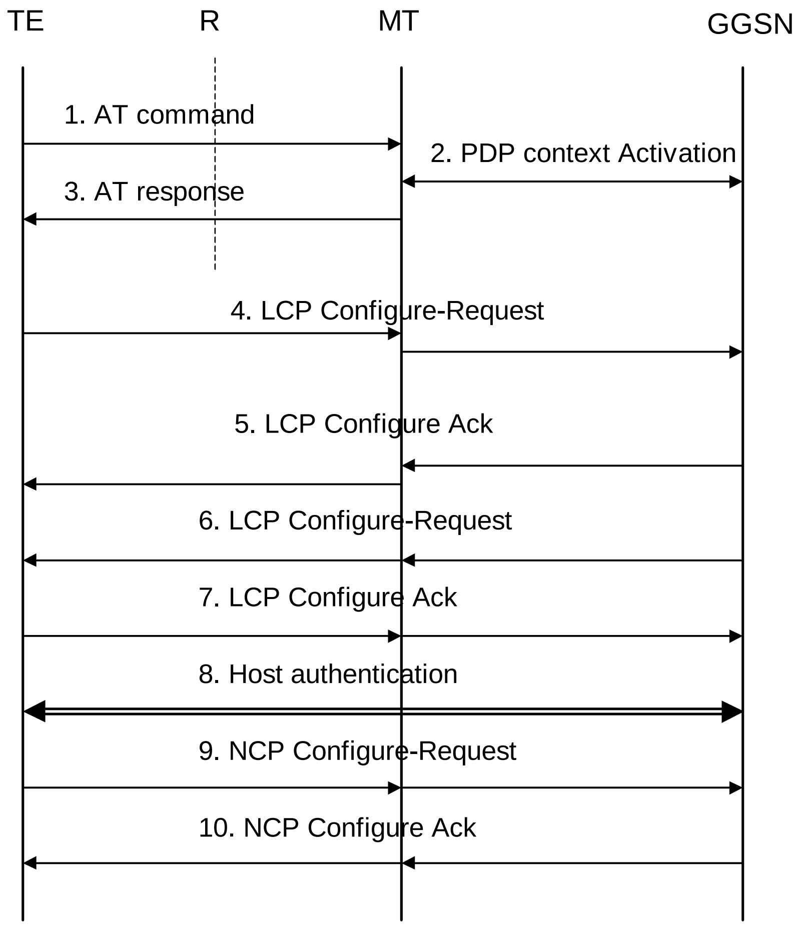


Figure 9b: PPP Based Service (relayed PPP negotiation)

1) The TE issues AT commands to set up parameters and activate a PDP Context (refer to sub-clause on AT commands for further details).

2) The MT performs a PDP Context Activation as described in 3G TS 23.060.

3) The MT sends AT responses to the TE.

4) The PPP protocol in the TE sends an LCP Configure-Request. If the request contains options related to the 'L2' framing these are negotiated by the MT. The LCP Configure-Request shall subsequently be relayed to the GGSN.

5) The GGSN returns an LCP Configure-Ack to the MT. The MT may change the value(s) of any options related to 'L2' framing and thereafter return an LCP Configure-Ack to the TE to confirm that the PPP link has been established. The MT might previously have sent an LCP Configure-Nak to the TE in order to reject some options proposed by the TE. This in turn might have triggered a retransmission of the LCP Configure-Request with different options.

6) The PPP protocol in the GGSN sends an LCP Configure-Request in order to negotiate for e.g. the authentication protocol used for authentication of the host TE towards the GGSN. The request is relayed to the TE.

7) The TE returns an LCP Configure-Ack to the MT to confirm the use of e.g. the specified authentication protocol. The acknowledgement is relayed to the GGSN. The GGSN might previously have sent an LCP Configure-Nak in order to reject the protocol proposed by the TE. This in turn might have triggered a retransmission of the LCP Configure-Request with different options.

8) The TE authenticates itself towards the GGSN by means of the negotiated protocol. The messages are relayed transparently by the MT. If no authentication protocol can be negotiated the GGSN may reject the PPP connection. Refer to 3G TS 29.061 for further details on the authentication.

9) The PPP protocol in the TE sends an NCP Configure-Request to the MT, which relays it transparently to the GGSN.

10) The GGSN acknowledges to the PPP protocol in the TE that the network layer protocol is now activated, by sending an NCP Configure-Ack command, transparently relayed by the MT. Before sending an NCP Configure-Ack, the GGSN might previously have sent an NCP Configure-Nak in order to reject some parameters proposed by the TE. This in turn might have triggered a retransmission of the NCP Configure-Request with different parameter values.

11 Internet Hosted Octet Stream Service (IHOSS)

11.1 Introduction

This subclause describes the MS aspects of the Packet Domain Internet Hosted Octet Stream Service (IHOSS). This is a MO-only, connection-oriented service that carries an unstructured octet (character) stream between a MS supporting Packet Switched services and an Internet Host.

IHOSS uses OSP:IHOSS which is a subset of the Octet Stream Protocol (OSP) PDP type to provide a 'character pipe' between the MS and the GGSN. In the GGSN there is a relay function between the OSP and the Internet Host protocol (usually TCP). An annex to the present document contains the generic description of OSP. The features of OSP that are used by OSP:IHOSS are described later in this subclause.

Figure 10 shows the scope of IHOSS and OSP:IHOSS.

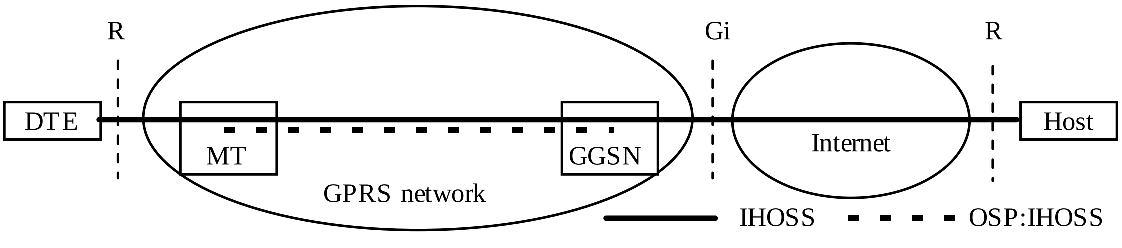


Figure 10: Scope of the Internet Hosted Octet Stream Service and Octet Stream Protocol

11.2 Example of protocol stacks at the MT

Figure 11 shows an example of the protocol stacks at the MT. The MT contains a relay function between OSP and an asynchronous character interface.

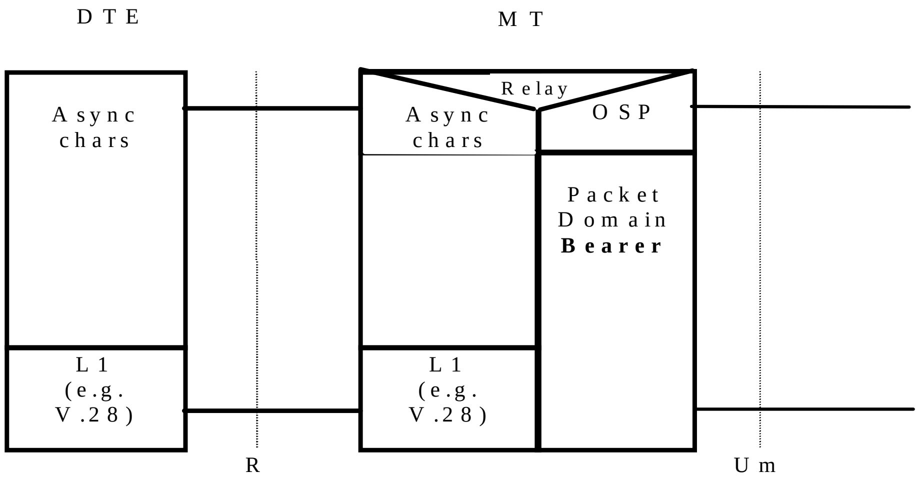


Figure 11: Example of protocol stacks for a MT with an asynchronous serial interface

11.3 IHOSS connection control and OSP PDP context management

Establishing an IHOSS connection involves setting up two segments, the PLMN segment (using the OSP) between the MS and GGSN, and the Internet segment between the GGSN and the Internet Host. There is a one-to-one mapping between the PLMN segment of an IHOSS connection and an OSP:IHOSS context. When the IHOSS connection is established, an OSP PDP context is activated. When the connection is released, the context is deactivated. It is possible for a suitably designed MT to activate multiple simultaneous OSP PDP contexts (subject to any limits imposed by the Packet Domain network), each context supporting one IHOSS connection.

11.3.1 Connection establishment and PDP context activation

Establishing the PLMN segment of an IHOSS connection follows the normal procedures for PDP context activation described in 3G TS 23.060 using messages described in 3G TS 24.008 (MS-SGSN) and 3G TS 29.060 (SGSN-GGSN). Figure 12 illustrates the procedure when TCP is used over the Internet.

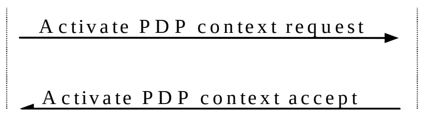


Figure 12: IHOSS connection establishment

The MS requests that an OSP PDP context be set up by sending an Activate PDP context request message. The PDP type is set to OSP:IHOSS. The PDP configuration options may provide information to enable the GGSN to set up a connection to the Internet host (Alternatively this information may be derived from subscription information in the HLR and configuration information within the GGSN).

In the case where TCP is used over the Internet, the response accepting the context activation request is returned to the MS only when the TCP connection to the Internet host has been established. If the TCP connection attempt fails, an Activate PDP context reject message is returned.

In the case where UDP is used over the Internet, the response accepting the context activation request is returned to the MS only when at least a successful DNS lookup of the Internet host name has been completed. If the lookup fails, an

Activate PDP context reject message is returned (The GGSN may perform additional checks before responding to the context activation request).

The format of the Activate PDP context request message is shown below:

Activate PDP Context Request (

NSAPI = generated within MS,

PDP type = OSP:IHOSS,

PDP address = null,

APN = as required or null - this may be provided by the HLR,

QoS requested = as defined in the generic OSP specification or null - this may be provided by the HLR,

PDP configuration options = (Internet hostname, port number, protocol type, maximum GGSN buffer sizes, OSP version number - all optional)

)

The format of the PDP configuration options is described in a later clause.

11.3.2 Connection release and PDP context deactivation

When the IHOSS connection is released the OSP:IHOSS context is deactivated. The disconnection can be originated either by the MT or the Internet host, or exceptionally by the SGSN under fault conditions. The MT initiates disconnection by sending a Deactivate PDP context request. This is acknowledged by the receipt of a Deactivate PDP context accept which indicates that the Internet connection has been cleared. An Internet host or SGSN initiated disconnection is signalled to the MT by the receipt of a Deactivate PDP context request which it acknowledges by sending a Deactivate PDP context accept.

11.4 OSP:IHOSS subset of OSP

11.4.1 Required features

The following features of OSP are required for the OSP:IHOSS subset of OSP.

11.4.1.1 User data transport

This is as specified in the generic OSP description.

11.4.1.2 Flow control

This shall map on to the local flow control mechanism at the DTE-MT interface.

11.4.2 Optional features

The following features of OSP are optional for the OSP:IHOSS subset of OSP.

11.4.2.1 Break handling

The OSP break procedure may be mapped on to the local break mechanism at the DTE-MT interface.

11.4.2.2 Packet Assembler/Disassembler

If the DTE-MT interface is character-oriented, a PAD is required in the OSP entity in the MT. The PAD may have pre-set values for the forwarding criteria parameters or they may configurable using, for example, an AT command.

If the interface to the application is block-oriented, for example in an embedded system, the PAD function is not needed.

11.4.2.3 GGSN maximum buffer size negotiation

Although the OSP entity in the GGSN does not have a PAD, it still requires buffers to hold the relayed packets. The following GGSN PAD parameters (in the Protocol Configuration Options) may be used to specify the maximum buffer sizes for the two directions of data transfer.

PAD Parameter	Direction;
Assembly buffer max size (253)	GGSN to MS;
Disassembly buffer max size (254)	MS to GGSN.

11.4.3 Not-required features

The following features of OSP are not required for the OSP:IHOSS subset of OSP:

- Control block transport;
- remote configuration of OSP PAD in the GGSN (appart from the optional GGSN buffer size configuration - see above);
- OSP protocol version negotiation (OSP: IHOSS uses the default version (0) of OSP).

11.5 Protocol option parameters

All these parameters in the PDP context activation request are optional. If not provided by the MT, this information may be derived from subscription information in the HLR and configuration information within the GGSN. The parameters use the syntax described in 3G TS 24.008.

11.5.1 Hostname

This refers to the Internet host to which the connection will be made.

Option ID 128.

Lengthnumber of characters in the Hostname:

Contents an IA5 character string which is the fully formed domain name extended hostname.

11.5.2 Port Number

This refers to the TCP or UDP port on the host identified by Hostname, which forms the endpoint of the Internet side of the connection.

Option ID 129.

Lengthnumber of characters in the Port Number.

Contents an IA5 character string which is the Port Number in decimal.

NOTE: If no port number is specified, a default value of 23 is used by the GGSN.

11.5.3 Protocol Type - TCP or UDP

This refers to the protocol used over IP on the GGSN to Internet host segment of the connection. The options available are Transmission Control Protocol (TCP) or User Datagram Protocol (UDP).

Option ID 130.

Length3.

Contents an IA5 character string which is either “TCP” or “UDP”. All other values are reserved.

If no Protocol Type is specified, TCP is used by the GGSN.

11.5.4 GGSN PAD parameters (maximum buffer sizes only)

The GGSN PAD options parameter is described in the generic OSP specification.

12 AT commands

3G TS 27.007 defines commands that a TE may use to control a MT supporting Packet Switched services, via either a non-multiplexed character-stream interface or a mutliplexed character stream interface (27.010). A non-multiplexed character stream interface places certain limitations on the functionality of the interface. For example, it is not possible for the MT to send control information to the TE or for the TE to send commands to the MT whilst the interface is in the V.250 online data state unless the layer 2 protocol itself supports this feature. However, a manufacturer-specific escape mechanism may be provided to enable the TE to switch the MT into the V.250 online command state. It is anticipated that MTs will vary widely in functionality. At one extreme, a class A or PS/CS MT might support multiple PDP types as well as circuit switched data, and use multiple external networks and QoS profiles. At the other extreme a class C or PS MT might support only a single PDP type using a single external network, and rely on the HLR to contain the context definition.

A comprehensive set of Packet Domain -specific AT commands is defined in 3G TS 27.007 to provide the flexibility needed by the more complex MT. The commands are designed to be expandable to accommodate new PDP types and interface protocols, merely by defining new values for many of the parameters. Multiple contexts may be activated if the interface link-layer protocol is able to support them. The commands use the extended information and error message capabilities described in 3G TS 27.007.

For MTs of intermediate complexity, most commands have simplified forms where certain parameters may be omitted.

For the simplest MTs, and for backwards compatibility with existing communications software, it is possible to control access to the Packet Domain using existing modem-compatible commands. A special dial-string syntax is defined for use with the D command. This "modem compatible" mode of operation is described in 3G TS 27.007.

Subclause 12.2 contains examples of command sequences for a number of applications.

Annex A of the present document lists the AT commands for the Packet Domain. They are fully defined in 3G TS 27.007.

12.1 General on AT commands

The following subclauses describe how the AT commands are used for the Packet Domain. The AT commands themselves are fully described in 3G TS 27.007. Reference to the particular AT command names are shown only for clarity. In all case refer to 3G TS 27.007 for the latest descriptions.

12.1.1 Interaction of AT commands, Packet Domain management and PDPs

State machines may be used to describe the behaviour of:

- AT commands (ITU-T V.250);
- PDP context management (3G TS 23.060);
- PDP startup, data transfer and termination (Packet Data Protocol specifications);
- the layer 2 protocol (if any) used across the TE-MT interface (layer 2 protocol specifications).

This subclause does not attempt to describe in detail how these state machines interact but rather to give some general guidance on their relationships.

12.1.1.1 AT commands and responses

AT commands may be issued and responses received by the TE only when the TE and MT are in V.250 command state.

The possibility of suspending the PDP and/or layer 2 protocol and entering V.250 online command state is not considered here; neither is the use of a multiplexed interface where the PDP and the AT commands use separate logical channels.

12.1.1.2 PDP and layer 2 protocol operation

The PDP (across the TE-MT interface) may startup, transfer data and terminate only when the TE and MT are in V.250 online data state. It may be necessary to startup a layer 2 protocol across the interface before starting the PDP. The PDP startup procedure may provide information needed for the PDP context activation procedure (see subclause 10.1.1.3.2).

12.1.1.3 Management of Packet Switched services

A particular PDP may be used to transfer data only when a context is active for that PDP. Before a context can be activated, the MT must be attached to the Packet Domain network.

In order to provide flexibility and support a variety of types of MT and PDP, AT commands are provided which give the TE explicit control over attachment and detachment (+CGATT), and context activation and deactivation (+CGACT) procedures. These commands allow the TE to retain control of the MT, and receive status information from the MT, after these actions have been performed.

12.1.1.3.1 PS attachment

The MT may be attached and detached using the +CGATT command. However, it may not be necessary to use the command since attachment may occur:

- on power up or reset;
- when an attempt is made to activate a context either explicitly (+CGACT) or as a result of a PDP startup - procedure;
- when the mobile class is changed (+CGCLASS).

Similarly, detachment may occur:

- as a result of a PDP termination procedure (if no other Packet Switched services are active);
- when the mobile class is changed (+CGCLASS).

12.1.1.3.2 PDP context activation

Certain information must be provided to the network in order for a context activation attempt to be successful. The TE may provide some of this information to the MT during the PDP startup procedure rather than through AT command procedures. In this case the context activation cannot be initiated by the +CGACT command but rather on receipt of the appropriate information during the PDP startup.

12.1.2 Use of default context parameter values

The activate context request message sent by the MT to the network contains a number of parameters whose values can usefully be set by the TE. Under certain circumstances the values for some or all of the parameters need not be provided by the TE, either via AT commands or the PDP startup procedure. The storage of context information in the SIM is not considered in the present document. Rules concerning what values shall be sent by the MT to the network under various circumstances are given in 3G TS 23.060.

One particular rule that is designed to simplify operation in modem compatibility mode is that if there is only one PDP context subscription in the HLR then all of PDP type, PDP address and APN may be omitted.

12.1.2.1 PDP type

This may be omitted:

- when the MT supports only one PDP type (it will be provided by the MT); or
- according to the rules given in 3G TS 23.060.

12.1.2.2 PDP address (of the MS)

This shall be omitted when:

- a dynamic address is required; or
- according to the rules given in 3G TS 23.060.

12.1.2.3 Access Point Name

This may be omitted:

- according to the rules given in 3G TS 23.060.

12.1.2.4 QoS Requested

This may be omitted when:

- the default subscribed QoS is acceptable.

12.1.2.5 PDP Configuration Options

These shall be omitted:

- when none are required for the PDP concerned; or
- according to the rules given for the PDP.

12.2 Example command sequences for dial-compatibility mode

12.2.1 PPP in dial compatibility mode

12.2.1.1 Mobile initiated IP context activation

In this mode of operation, the MT behaves like an originating modem and accepts the normal V.250 commands associated with placing and clearing a call to a dial-up PPP server. Although the procedures for setting up the IP context are initiated from the mobile end, IP-based sessions, for example the File Transfer Protocol (FTP), may be initiated from either end once the context is active.

For this example it is assumed that:

- the user has subscribed to only one PDP context (of type IP) and therefore no context parameter values are needed;
- the MT supports only PPP at the MT-TE interface and therefore no layer 2 protocol need be specified.

A possible sequence of events is:

- the MT begins in V.25 command state:
    - TE -> MT: AT<Packet Domain-specific configuration commands, if required>;
    - MT -> TE: OK.
- the TE sends a dial command requesting the Packet Switched service:
    - TE -> MT: ATD*99#;
    - MT -> TE CONNECT.
- the MT enters V.250 online data state:
    - TE starts up PPP (LCP exchange);
    - TE -> MT: LCP Configure-request;
    - MT -> TE: LCP Configure-ack:
        - PPP Authentication may take place (optional);
        - TE starts up IP (NCP for IP exchange):
            - TE -> MT: NCP(IP) Configure-request;
            - MT <-> network: MT performs the PS-attach procedure if the MT is not currently attached;
            - MT <-> network: MT performs the IP context activation procedure;
            - MT -> TE: NCP(IP) Configure-ack;
            - TE <-> MT< - > network: IP packets may now be transferred.
        - TE stops IP (optional):
            - TE-> MT: NCP(IP) Terminate-Request); this
            - MT<-> network: MT performs the IP context deactivation procedure); is
            - MT -> TE: NCP(IP) Terminate-Ack) optional.
        - TE stops PPP:
            - TE-> MT: LCP Terminate-Request;
            - MT <-> network: MT performs the IP context deactivation procedure if it has not already done so;
            - MT <-> network: MT may perform the PS-detach procedure if no other Packet Switched services are active;
            - MT -> TE: LCP Terminate-Ack.
- *the MT returns to V.250 command state and issues the final result code :*
    - MT -> TE NO CARRIER.

The TE may recognise this as a return to V.250 command state. However, if it is using procedures intended for controlling modems, it may attempt to force a disconnect since in the modem case it cannot rely on the remote modem dropping the carrier. It will use some combination of:

- TE -> MT: TE drops circuit 108/2 (Data Terminal Ready);
- TE -> MT: escape sequence (e.g. +++);
- TE -> MT: ATH.

The MT should respond according to V.250 even if it is already in command state.

If the connection is lost at any time, the MT shuts down PPP, returns to V.250 command state and issues the final result code:

- MT -> TE NO CARRIER.

12.2.1.2 Network requested IP context activation

In this mode of operation, the MT behaves like an answering modem and accepts the normal V.250 commands associated with answering a call to a PPP server. Although the procedures for setting up the IP context are initiated from the network end, IP-based sessions, for example the File Transfer Protocol (FTP), may be initiated from either end once the context is active.

Two example sequences of events are given, for the cases of automatic and manual answering:

Case 1: automatic answering

The MT begins in V.250 command state:

- TE -> MT: AT<Packet Domain -specific configuration commands, if required >.

The TE sets automatic answering mode:

- TE -> MT: ATS0=1:
    - MT <- > network: MT performs the PS-attach procedure if the MT is not currently attached.

Subsequently:

- network -> MT: Request PDP Context Activation message;
- MT -> TE: RING.

The MT returns the intermediate result code:

- MT -> TE CONNECT,

and enters V.250 online data state.

The TE and MT perform the PPP and IP startup procedures which include the MT requesting the network to activate the IP context.

Case 2: manual answering

The MT begins in V.250 command state:

- TE -> MT: AT<Packet Domain -specific configuration commands, if required >.

The TE sets manual answering mode and requests a PS-attach (if necessary):

- TE -> MT: ATS0=0;
- TE -> MT: AT+CGATT=1;
- MT <- > network: MT performs the PS-attach procedure if the MT is not currently attached;

- network -> MT: Request PDP Context Activation message;
- MT -> TE: RING.

The TE answers manually:

- TE -> MT: ATA;
- MT -> TE CONNECT,

and enters V.250 online data state.

The TE and MT perform the PPP and IP startup procedures which include the MT requesting the network to activate the IP context:

or the TE rejects the connection:

- TE -> MT: ATH.

and remains in V.250 command state.

Annex A (informative): Summary of AT commands for the Packet Domain

This informative annex lists the AT commands for the Packet Domain that are fully described in 3G TS 27.007.

Table A.1: Summary of AT commands for the packet domain

Command	Description
+CGACT	PDP context activate or deactivate
+CGANS	Manual response to a network request for PDP context activation
+CGATT	PS attach or detach
+CGAUTO	Automatic response to a network request for PDP context activation
+CGCLASS	PS mobile station class
+CGCLOSP	Configure local Octet Stream PAD parameters
+CGCLPAD	<VOID>
+CGDATA	Enter data state
+CGDCONT	Define PDP context
+CGEREP	Control unsolicited PS event reporting
+CGPADDR	Show PDP address
+CGREG	Packet Domain network registration status
+CGQMIN	Quality of service profile (minimum acceptable)
+CGQREQ	Quality of service profile (requested)
+CGSMS	Select service for MO SMS messages

Table A.2: Summary of Packet Domain Extensions to existing GSM AT commands

Command	Description
+CEER	Extended error report (refer to 27.007)
+CMEE	Report mobile equipment error (refer to 27.007)
+CR	Service reporting control (refer to 27.007)
+CRC	Cellular result codes (refer to 27.007)

Table A.3: Summary of AT commands for Packet Domain modem compatibility mode

Command	Description
A	Answer – manual acceptance of a network request for PDP context activation
D	Dial – request Packet Domain service
H	On-hook - manual rejection of a network request for PDP context activation
S0	Automatic answering control - automatic acceptance of a network request for PDP context activation

Annex B (informative): Octet Stream Protocol (OSP) PDP type

B.1 Scope

The Octet Stream Protocol (OSP) is used to carry an unstructured octet (character) stream between the MS and GGSN. It is used to provide a 'character pipe' to allow a MS to communicate (via the GGSN) with an arbitrary Internet host, or other character-based service. Unlike PDP types such as IP and X.25, OSP has no existence outside the PLMN. In the MS there is a character stream at the R reference point together with some optional control signals. In the GGSN there is a relay function, carrying the same character stream and control signals between the OSP entity and a fixed network protocol stack.

An OSP entity has two modes of operation. In octet mode, it uses a Packet Assembly function to assemble a number of user octets into a single packet for more efficient transport by the underlying packet protocol. A complementary Packet Disassembly function in the same OSP entity performs the reverse operation. In block mode, an OSP entity's Packet Assembly and Disassembly functions are bypassed. Data is transferred between the OSP user and the OSP entity in blocks of octets. Each block of octets is carried in a single packet of the underlying protocol. The selection of octet or block mode is made independently for each OSP entity as an implementation or configuration decision before a connection is established and remains fixed for the duration of that connection.

An example of the use of block mode is when OSP is used for interworking with a fixed network where the octet stream is also carried in packets. The use of the block mode in the OSP entity in the GGSN avoids the use of back-to-back PADs. Block mode could also be used in a MS where the MT function is embedded in a larger piece of equipment and the application transfers data in blocks of octets.

OSP uses the services of SNDCP between the MS and SGSN, and the services of GTP between the SGSN and GGSN. The Quality of Service is determined mainly by that provided by the underlying layers. However, the end-to-end delay may be affected by the presence of the PAD (Packet Assembler/Disassembler) function. For most applications it is anticipated that a reliable (acknowledged) service will be provided by the underlying layers.

In summary, the main functions of OSP are:

- transport of an unstructured octet stream;
- Packet Assembly/Disassembly (to make efficient use of network resources);
- end-to-end flow control.

In addition OSP may provide:

- transport of a 'break' signal;
- transport of blocks of control information between the OSP users;
- user control of packet assembly buffer forwarding;
- direct OSP user access to the underlying packet service, bypassing the PAD.

Figure B.1 shows how OSP fits into the overall Packet Domain protocol model.

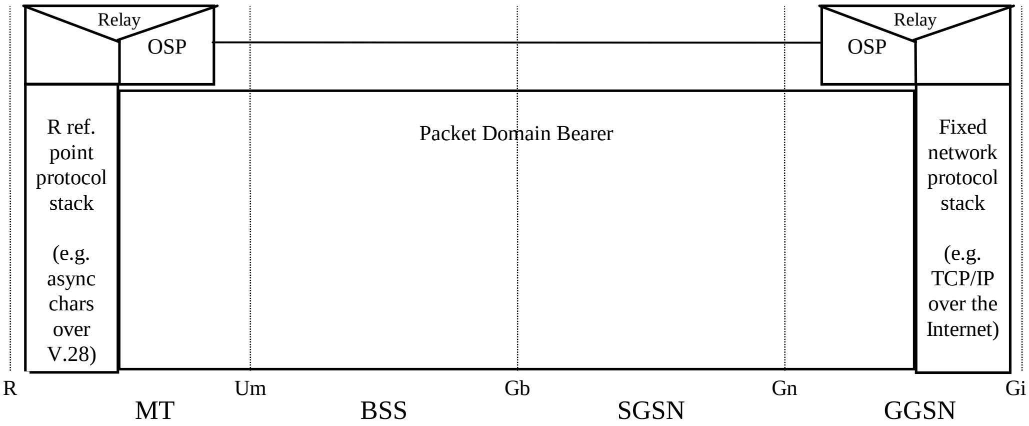


Figure B.1: Relationship of OSP to the rest of the packet domain protocol architecture

B.2 Service primitives

B.2.1 Service Primitives provided by the OSP layer

The service provided by the OSP layer to its user (the layer above) is described in terms of service primitives. An example of the use of the OS-DATA.request and OS-DATA.indications primitives to transfer an octet or block of octets from one OSP user to another is shown in figure B.2.

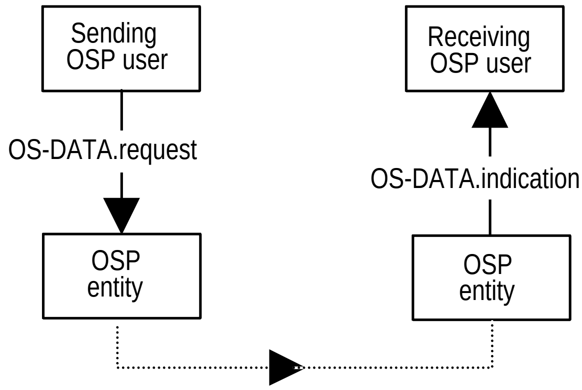


Figure B.2: An example of the use of the OS-DATA primitives

The primitives provided by the OSP layer are listed in table B.1.

Table B.1: OSP layer service primitives

Generic Name	Type				Parameters
	Request	Indication	Response	Confirm	
OSP User (MS or GGSN) <---> OSP					
OS-DATA	X	X	-	-	D-PDU (single octet or block of octets)
OS-UNITDATA	X	X	-	-	D-PDU (single octet or block of octets)
OS-FLOWCONTROL	X	X	-	-	Requested flow control state (STOP or START)
OS-BREAK	X	X	-	-	none
OS-CONTROL	X	X	-	-	C-PDU (block of octets)
OS-FORWARD	X	-	-	-	none

B.2.1.1 OS-DATA.request

Request used by the OSP user for transmission of a D-PDU. In octet mode, the D-PDU consists of a single octet. In block mode the D-PDU consists of a block of octets. This primitive is used when the underlying protocol layers are providing a reliable service.

B.2.1.2 OS-DATA.indication

Indication used by the OSP entity to deliver the received D-PDU to the OSP user. In octet mode, the D-PDU consists of a single octet. In block mode the D-PDU consists of a block of octets.

B.2.1.3 OS-UNITDATA.request

Request used by the OSP user for transmission of a D-PDU. In octet mode, the D-PDU consists of a single octet. In block mode the D-PDU consists of a block of octets. This primitive is used when the underlying protocol layers are providing an unreliable service.

B.2.1.4 OS-UNITDATA.indication

Indication used by the OSP entity to deliver the received D-PDU to the OSP user. In octet mode, the D-PDU consists of a single octet. In block mode the D-PDU consists of a block of octets.

B.2.1.5 OS-FLOWCONTROL.request

Request used by the OSP user for the peer OSP user to update its flow control state.

B.2.1.6 OS-FLOWCONTROL.indication

Indication used by the OSP entity to request the OSP user to update its flow control state.

B.2.1.7 OS-BREAK.request

Request used by the OSP user to send a break signal to the peer OSP user.

B.2.1.8 OS-BREAK.indication

Indication used by the OSP entity to deliver a break signal to the OSP user.

B.2.1.9 OS-CONTROL.request

Request used by the OSP user to request transmission of a C-PDU. The C-PDU consists of a block of octets. The reliability of the transmission is determined by the lower layer protocols.

B.2.1.10 OS-CONTROL.indication

Indication used by the OSP entity to deliver a received C-PDU to the OSP user.

B.2.1.11 OS-FORWARD.request

Request used by the OSP user to cause immediate forwarding of the OSP Packet Assembly buffer.

B.2.2 Service Primitives Used by the OSP Layer

The OSP layer uses the service primitives provided by the SNDCP layer (see table B.2) and the GTP layer (see table B.3). SNDCP is specified in GSM 04.65 and GTP in 3G TS 29.060.

Table B.2: SNDCP service primitives used by the OSP entity

Generic Name	Type				Parameters
	Request	Indication	Response	Confirm	
OSP <---> SNDCP					
SN-DATA	X	X	-	-	N-PDU, NSAPI
SN-UNITDATA	X	X	-	-	N-PDU, NSAPI, protection mode

B.2.2.1 SN-DATA.request

Request used by the SNDCP user for acknowledged transmission of an N-PDU. The successful transmission of an SN-PDU shall be confirmed by the LLC layer. The SN-DATA.request primitive conveys the NSAPI to identify the PDP using the service.

B.2.2.2 SN-DATA.indication

Indication used by the SNDCP entity to deliver a received N-PDU to the SNDCP user. Successful reception has been acknowledged by the LLC layer.

B.2.2.3 SN-UNITDATA.request

Request used by the SNDCP user for unacknowledged transmission of an N-PDU. The SN-UNITDATA.request primitive conveys the NSAPI to identify the PDP using the service and protection mode to identify the requested transmission mode.

B.2.2.4 SN-UNITDATA.indication

Indication used by the SNDCP entity to deliver a received N-PDU to the SNDCP user.

Table B.3: GTP service primitives used by the OSP entity

Generic Name	Type				Parameters
	Request	Indication	Response	Confirm	
OSP <---> GTP					
GT-DATA	X	X	-	-	N-PDU, TID
GT-UNITDATA	X	X	-	-	N-PDU, TID

B.2.2.5 GT-DATA.request

Request used by the GTP user for acknowledged transmission of an N-PDU. The successful transmission of an SN-PDU shall be confirmed by the TCP layer. The SN-DATA.request primitive conveys TID to identify the PDP using the service.

B.2.2.6 GT-DATA.indication

Indication used by the GTP entity to deliver the received N-PDU to the GTP user. Successful reception has been acknowledged by the TCP layer.

B.2.2.7 GT-UNITDATA.request

Request used by the GTP user for unacknowledged transmission of an N-PDU. The SN-UNITDATA.request primitive conveys TID to identify the PDP using the service. This uses UDP as the path protocol.

B.2.2.8 GT-UNITDATA.indication

Indication used by the GTP entity to deliver the received N-PDU to the GTP user.

B.3 OSP Functional model

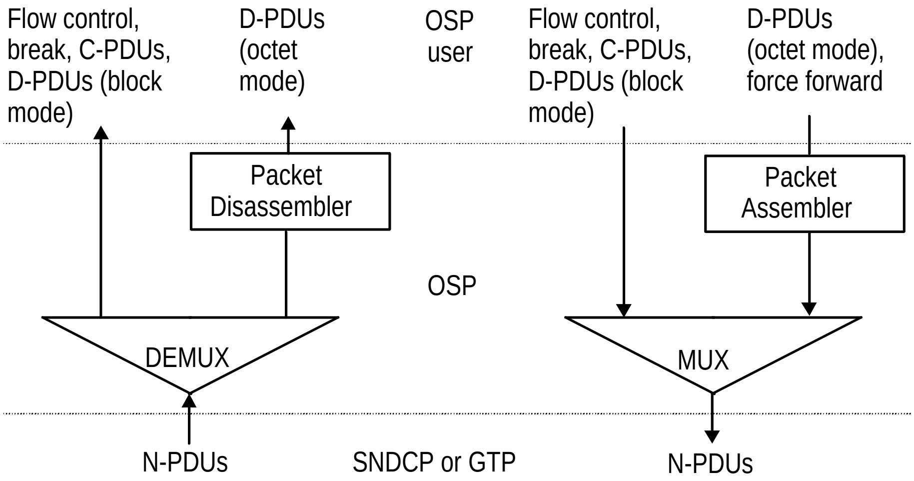


Figure B.3: OSP functional model

The main functions of the OSP entity are shown in figure B.3.

At the sending side, in octet mode, octets from the OSP user (D-PDUs) are accumulated by the Packet Assembler until some forwarding criterion is satisfied. Forwarding can be forced by the user if required. The resulting packet is then passed to the multiplexing function (MUX). In block mode, D-PDUs are passed directly to the MUX. The MUX combines these packets of user data with flow control requests and optionally break requests and control blocks (C-PDUs). (A control block is a delimited set of octets whose maximum size is determined by the limits imposed by the underlying protocol.) The resulting stream of N-PDUs is passed to the SNDCP or GTP layer below.

At the receiving side, the N-PDUs from the SNDCP or GTP layer below are passed to the demultiplexing (DEMUX) function. Here the packets of user data, flow control indications, and (if implemented) break indications and control blocks (C-PDUs) are separated out. In block mode, the packets of user data are passed directly to the OSP user. In octet mode, they are passed to the Packet Disassembler which regenerates the original stream of octets (D-PDUs).

B.4 OSP N-PDU (packet) format

Each N-PDU shall contain an integral number of octets, and shall comprise a header part and a data part. An N-PDU shall contain data from zero or more D-PDUs or a single C-PDU (D-PDUs and C-PDUs may not be mixed in the same N-PDU).

The bit and octet numbering convention used in the present document is illustrated in figure B.4. The bits are grouped into octets. The bits of an octet are shown horizontally and are numbered from 1 to 8. Multiple octets are shown vertically and are numbered from 1 to N.

Bit	8	7	6	5	4	3	2	1
Octet 1								
2								
…								
N-1								
Octet N								

Figure B.4: Numbering convention

N-PDUs are transferred between the OSP layer and the SNDCP or GTP layer in ascending numerical octet order (i.e. octet 1, 2, …, N-1, N).

B.4.1 OSP header

The OSP header is contained in octet 1. The use of bits 1-4 and bit 8 are described below. Bits 5-7 are not used in this version of the protocol and shall be set to zero by the sender and ignored by the receiver.

B.4.1.1 Bit 1 - Extension (E)

This is provided to allow the OSP header in future versions of the protocol to consist of more than one octet. In this version of the protocol E shall always be set to 1 by the sender and checked by the receiver.

B.4.1.2 Bit 2 - Ready to Receive (RTR) - flow control

This bit indicates if the OSP entity that sent the N-PDU is able to receive data from its peer OSP entity.

RTR = 0 not ready to receive.

RTR = 1 ready to receive.

B.4.1.3 Bit 3 - Break Request (BR)

This bit requests that the receiving OSP entity shall signal a break to its user.

BR = 0 no break.

BR = 1 signal break.

B.4.1.4 Bit 4 - Break Acknowledge (BA)

This bit indicates that the sending OSP entity has signalled a break to its user in response to a Break Request.

BA = 0 no acknowledge break.

BA = 1 acknowledge break.

B.4.1.5 bit 8 - payload type (PT)

This bit indicates whether the payload contains user data or a control block.

PT = 0 data (zero or more D-PDUs).

PT = 1 control (zero or one C-PDU).

B.4.2 OSP payload

This consists of one of the following.

B.4.2.1 User data

This consists of zero or more (up to some maximum - TBD) octets of user data (zero or more D-PDUs).

B.4.2.2 Control block

This consists of the contents of zero or one C-PDU.

B.5 Packet Assembly/Disassembly (PAD) function

In order to make efficient use of the network resources, particularly the radio resource, D-PDUs (octets) received from the OSP user are not forwarded immediately but are placed in a buffer. When some forwarding criterion is satisfied, the contents of the buffer are forwarded in the payload of an N-PDU to the layer below. At the receiving end, the payload of an N-PDU received from the layer below is placed in a buffer and the octets are delivered to the OSP user as a stream of D-PDUs (octets). The PAD is used only when the OSP entity is operating in octet mode. It is not used when the OSP entity is operating in block mode.

B.5.1 Packet Assembler

The packet assembler shall be able to detect the following forwarding criteria. When any one criterion is satisfied, the contents of the buffer shall be forwarded in an N-PDU (of type User Data) to the layer below, subject to any flow control condition. Whenever a buffer is forwarded, the inactivity timer is stopped (if it is running).

B.5.1.1 Buffer full

The buffer contents are forwarded when the number of octets in the buffer reaches the value of the maximum buffer size parameter.

The maximum N-PDU size is equal to the maximum buffer size plus the size of the OSP header. It should be chosen so as to make efficient use of the network resources, particularly the radio resources. Although it is possible to calculate the overhead imposed by the various underlying protocol layers, it is not possible to predict exactly how an N-PDU will be mapped on to radio frames even if the channel coding is known. This is because the SNDCP layer may use data compression, the efficiency of which depends on the compressibility of the data. However, since the SNDCP layer is able to segment and reassemble long N-PDUs, it is recommended that the maximum N-PDU size should be several times the largest radio frame size, allowing for a typical compression ratio of, say, 2:1. This will ensure that most radio frames are full.

The maximum size for the packet assembly buffer is specified by PAD parameter 253. The value is in the range 1-65 535 octets.

The maximum size for the packet disassembly buffer is specified by PAD parameter 254. The value is in the range 1-65 535 octets.

B.5.1.2 Inactivity timer expiry

Whenever an octet is placed in the buffer the inactivity timer shall be started, set to the value of the inactivity time parameter. When the timer expires, the buffer contents are forwarded. The timer has the following functions:

1. to ensure that octets don't remain in the buffer for ever;
2. to detect significant gaps in the stream of octets and try to ensure that these gaps match the N-PDU boundaries. This is beneficial for data that at the user level is in blocks of octets, e.g. a PPP frame. It means that the trailing octets of a block do not get delayed (since they are forwarded when the timer expires). Also, because the timer is restarted whenever a new octet appears, it ensures that blocks do not get split unless the buffer becomes full;

3. to give interactive traffic a reasonable response time.

The inactivity time parameter should be set to be longer than the inter-octet time but shorter than the inter-block time to ensure optimum forwarding of blocked data. It shall be possible to set it to an infinite time, i.e. the timer never expires.

The maximum buffer delay timer is specified by PAD parameter 4 and values shall be in the range 1-255 (units of 1/20 of a second). Additionally, the value 0 disables the timer. The default value is 0.

B.5.1.3 Maximum Buffer Delay timer expiry (optional)

When the first octet is placed into the (empty) buffer, a maximum buffer delay timer may optionally be started, set to the value of the maximum buffer delay parameter. When the timer expires, the buffer contents are forwarded. Thistimer ensures that no octet is delayed in the buffer for more than the specified time.

The maximum buffer delay timer is specified by PAD parameter 255 and values shall be in the range 1-255 (units of ½ of a second). Additionally, the value 0 disables the timer. The default value is 0.

B.5.1.4 Special character(s)

Whenever an octet has been placed in the buffer, it is compared (lower 7 bits only) with a list of 'special characters'. If it matches, the buffer is forwarded.

The possible characters and combinations of characters are specified by PAD parameter 3. Permitted values are listed below.

Value	Characters
0	disabled
1	A-Z, a-z, 0-9
2	CR
4	ESC, BEL, ENQ, ACK
8	DEL, CAN DC2
16	ETX, EOT
32	HT, LF, VT, FF
64	all characeters between NUL and US not listed above

Values may be added to create further combinations, e.g., 34 (=2+32) corresponds to CR, HT, LF, VT, FF.

B.5.1.5 Change in flow control state

An N-PDU (type User Data) carries flow control information in the OSP header as well as user data in the payload. If there is a need to signal a change in the Ready to Receive condition, the buffer shall be forwarded immediately with the appropriate (new) value of RTR in the OSP header, unless the change has already been signalled using an N-PDU with an empty payload.

B.5.1.6 Immediate forwarding request

When the OSP entity receives a OS-FORWARD.request primitive from its user, it shall immediately forward the buffer unless it is empty.

B.5.2 Packet Disassembler

The packet disassembler shall forward the contents of the N-PDU (type User data) payload to the OSP user, subject to any local flow control condition.

B.6 Flow control

The OSP entity maintains two variables indicating the readiness of the local OSP entity (itself) and the remote OSP entity (its peer) to receive data.

Local - variable RTRL.

The value of RTRL is updated as a result of the receipt of OS-FLOWCONTROL.request primitives from the OSP user and changes in buffer conditions within the OSP entity. When the user requests STOP, RTRL shall immediately be set to 0. When the user requests START, RTRL may be set to 1 immediately or this may be delayed subject to buffer conditions.

The value of RTRL is copied into the RTR bit of every N-PDU transmitted. Whenever RTRL changes, an N-PDU is sent immediately to signal the change to the peer OSP entity. This may be done by either sending an N-PDU with an empty payload or immediately forwarding the packetiser buffer.

RTRL may also be set to 0 or 1 by the OSP entity as a result of buffer conditions within the OSP entity.

Remote - variable RTRR.

The value of RTRR is updated from the RTR bit of every N-PDU received. When RTRR changes to 0, an OS-FLOWCONTROL.indication(STOP) primitive shall be sent immediately to the OSP user. When RTRR changes to 1, an OS-FLOWCONTROL.indication (START) primitive may be sent immediately to the OSP user or this may be delayed subject to buffer conditions.

STOP and START indications may also be sent at any time as a result of buffer conditions within the OSP entity.

B.7 Break handling

When an OSP entity receives an OS-BREAK.request from its user it shall immediately send an N-PDU (type User Data) with the Break Request (BR) bit in the OSP header set to 'signal break' and an empty payload. Any data in the packetiser buffer shall be discarded and not transmitted in the N-PDU. Further data received from the OSP user shall be processed in the normal way. The OSP entity shall discard any buffered data already received from its peer entity and, when operating over a reliable service, shall continue discarding received N-PDUs (type user data) until it receives one with the Break Acknowledge (BA) bit in the OSP header set to 'acknowledge break '. Any data in the received N-PDU shall be processed in the normal way. N-PDUs (type control) are not discarded.

When operating over an unreliable service, the OSP entity sending ‘signal break’ shall protect itself from the risk of lockup resulting from the loss of either or both of the N-PDUs containing ‘signal break’ or ‘break acknowledge’. This is implementation-dependent. (A simple implementation could resume processing received N-PDUs immediately and ignore any received ‘break acknowledge’.)When an OSP entity receives an N-PDU (type User Data) with the BR bit set to 'signal break' it shall immediately signal a break to its user with an OS-BREAK.indication. The OSP entity shall discard all buffered data for both directions of flow and acknowledge the break by sending an N-PDU (type User Data) with the Break Acknowledge (BA) bit in the OSP header set to 'acknowledge break'. This may either be sent immediately with no data or wait until one of the forwarding criteria is satisfied.

B.8 Control block transport

An OSP user may use the OS-CONTROL.request primitive to send a C-PDU (block of control information) consisting of zero or more octets to its peer user. An N-PDU (type Control Block) is sent immediately, regardless of whether there is any data in the packetiser buffer or flow control condition. If it is necessary to forward the buffer contents before sending the control block, the OSP user should issue an OS-FORWARD.request before the OS-CONTROL.request. The C-PDU is delivered immediately to the receiving OSP user with the OS-CONTROL.indication primitive, regardless of the state of the depacketiser buffer or local flow control condition. The octet ordering within the block and the block boundaries are preserved.

B.9 Quality of Service

The Quality of Service (QoS) provided by the OSP layer is determined almost entirely by that provided by the underlying protocol layers. However, the Packet Assembly and Disassembly functions introduce an additional variable delay into the transmission path. This delay can be limited at the risk of making less efficient use of network resources (particularly radio resources). The PAD function is described in detail in its own clause.

B.10 OSP version

In order to allow the possible coexistence in the future of multiple versions of OSP, each version shall be assigned a version number. The use of a particular version may be negotiated by the peer OSP entities using the OSP version subparameter of the protocol configuration options parameter in the PDP context activation request, accept and reject messages. The default in the event of no negotiation taking place is this initial version (0).

B.11 Protocol Configuration Options

The following generic OSP configuration options parameters are defined for use in the various PDP Context Activation control messages. They use the syntax described in 3G TS 24008. Option IDs 0-127 are reserved for generic use. Additional parameters with IDs in the range 128-255 may be defined for specific uses of the OSP.

Parameter values may be negotiated between the MT and GGSN OSP entities. This is a two phase negotiation with the MT making a set of proposals and the GGSN either accepting each value or proposing an alternative. The MT must either accept the new set or the connection attempt fails. The alternative values are proposed in either a PDP context activation accept or reject message.

The accept message should be used if there is a reasonable likelihood that the alternative will be acceptable to the MT, e.g. a downgrading of buffer size, since the connection may then immediately continue. If the alternative is unacceptable the MT immediately deactivates the context.

The reject message should be used if it is likely that the alternative will not be acceptable, or if a significant charge would be incurred if the context were to be activated by the GGSN and then immediately deactivated by the MT. If the alternative is acceptable the MT may reattempt context activation using the values supplied by the GGSN.

B.11.1 OSP version

This parameter is optional. It allows the MT and GGSN to negotiate a mutually acceptable version of OSP. If omitted, the initial (version 0) of OSP is assumed.

Option ID 0.

Length1.

Contents 0 indicates this (initial) version of OSP. Other values are reserved for future versions.

B.11.2 GGSN PAD parameters

This options parameter is optional and may be used if the OSP entity in the GGSN contains a PAD function. It allows the MT and GGSN to negotiate a mutually acceptable set of PAD parameters for the GGSN PAD. The maximum buffer size parameters may be negotiated even when the OSP entity in the GGSN does not contain a PAD. If not relevant to the GGSN OSP entity, the PAD options parameter shall be ignored.

Option ID 1.

Length3n (n = number of PAD parameters).

Contents Pairs of (PAD parameter, value).

The PAD parameter is 1 octet in length. The value is 2 octets in length.

Valid PAD parameters are listed in the clause describing the Packet Assembly/Disassembly function.

Annex C (informative): Change history

Change history						
TSG CN#	**Spec**	**Version**	**CR**	**Phase**	**New Version**	**Subject/Comment**
Apr 1999	GSM 07.60	6.2.1				Transferred to 3GPP CN1
CN#03	27.060				3.0.0	Approved at CN#03
CN#04	27.060	3.0.0	001	R99	3.1.0	Correction to +CGAUTO command
CN#04	27.060	3.0.0	002	R99	3.1.0	Move AT commands
CN#04	27.060	3.0.0	003	R99	3.1.0	Access to PDN's and ISP's with the PDP-type PPP
CN#04	27.060	3.0.0	004	R99	3.1.0	Internet Hosted Octet Stream Service (IHOSS) and Octet Stream Protocol
CN#05	27.060	3.1.0	005	R99	3.2.0	ATD Commands
CN#06	27.060	3.2.0	006	R99	3.3.0	IPCP Negotiation Interworking at the MT
CN#06	27.060	3.2.0	007	R99	3.3.0	Clarification on the PPP LCP Negotiation for PDP type PPP.
CN#06	27.060	3.2.0	008	R99	3.3.0	Streamlining
CN#06	27.060	3.2.0	009	R99	3.3.0	Parallel Handling of Multiple User Application Flows
CN#07	27.060	3.3.0	010	R99	3.4.0	Correction of the support for IPv6 for the MS
CN#07	27.060	3.3.0	011	R99	3.4.0	TSG CN1 Vocabulary Alignment
CN#07	27.060	3.3.0	012	R99	3.4.0	Removal of X.25.
CN#07	27.060	3.3.0	013	R99	3.4.0	Specification reference section clean-up

History

Document history		
V3.4.0	March 2000	Publication