3GPP TSG_CN#6 **NP-99431**

ETSI SMG3 Plenary Meeting #6,

Nice, France

13th – 15th December 1999

Agenda item: **5.3.3**

Source: **TSG_N WG3**

Title: **CRs to 3G Work Item GPRS**

<u>Introduction</u>:

This document contains **"12"** CRs **on Work Item GPRS** agreed by **TSG_N WG3** and forwarded to **TSG_N Plenary** meeting #6 for approval.

Tdoc	Spec	CR	Rev	CAT	Rel.	Old Ver	New Ver	Subject
N3-99462	07.60	A020		D	R98	7.1.0		IPCP NEGOTIATION INTERWORKING AT THE MT FOR NON-TRANSPARENT IP
N3-99461	07.60	A019		D	R97	6.4.0		IPCP NEGOTIATION INTERWORKING AT THE MT FOR NON-TRANSPARENT IP
N3-99465	09.61	A013		D	R98	7.1.0		IPCP NEGOTIATION INTERWORKING AT THE MT FOR NON-TRANSPARENT IP
N3-99464	09.61	A012		D	R97	6.3.0		IPCP NEGOTIATION INTERWORKING AT THE MT FOR NON-TRANSPARENT IP
N3-99463	27.060	006		D	R99	3.2.0	3.3.0	IPCP NEGOTIATION INTERWORKING AT THE MT FOR NON-TRANSPARENT IP
N3-99469	27.060	007		D	R99	3.2.0	3.3.0	CLARIFICATION ON THE TASKS OF THE MT FOR PDP TYPE PPP
N3-99484	27.060	008		B	R99	3.2.0	3.3.0	STREAMLINING
N3-99468	27.060	009		B	R99	3.2.0	3.3.0	Parallel handling of multiple user application flows
N3-99470	29.061	003		D	R99	3.1.0	3.2.0	CLARIFICATION ON THE PPP LCP NEGOTIATION FOR PDP TYPE PPP
N3-99482	29.061	004		C	R99	3.1.0	3.2.0	ENHANCEMENT TO NUMBERING AND ADDRESSING TO INCLUDE THE APN
N3-99466	29.061	005		D	R99	3.1.0	3.2.0	IPCP NEGOTIATION INTERWORKING AT THE MT FOR NON-TRANSPARENT IP
N3-99499	29.061	008		B	R99	3.1.0	3.2.0	STREAMLINING

3GPP TSG-CN WG3/SMG3 WPD Meeting #7
Sophia-Antipolis, France, 29 Nov-03 Dec 1999

***Document* N3-99462**

e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

07.60 CR A020 Current Version: 7.1.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to: CN#6	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑	for information		non-strategic	X	

Form: CR cover sheet, version 2 for 3GPP and SMG The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]
(at least one should be marked with an X)

Source: TSG_N3 **Date:** 1999-11-29

Subject: IPCP negotiation interworking at the MT for non-transparent IP

Work item: GPRS

Category:
(only one category shall be marked with an X)

F	Correction		**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	X
D	Editorial modification	X		Release 99	
				Release 00	

Reason for change: During the PDP context activation procedure for PDP type IP, the MT may receive PPP IPCP packets, carried in the Protocol Configuration Options IE, from the network. It is not entirely clear in the current text how the MT shall act upon the reception of Configure-Ack, Configure-Nak and Configure-Reject packets.

Clauses affected: 9.1

Other specs affected:

Other 3G core specifications		→ List of CRs:
Other GSM core specifications		→ List of CRs:
MS test specifications		→ List of CRs:
BSS test specifications		→ List of CRs:
O&M specifications		→ List of CRs:

Other comments: There is also a corresponding CR for GSM 09.61 v7.1.0.

help.doc

<--------- double-click here for help and instructions on how to create a CR.

9.1 Example mapping of functions between the R reference point and the GPRS 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 interface) to support multiple virtual interfaces (communications ports) at the R reference point. Multiple PPP connections and IP contexts are possible in this case.

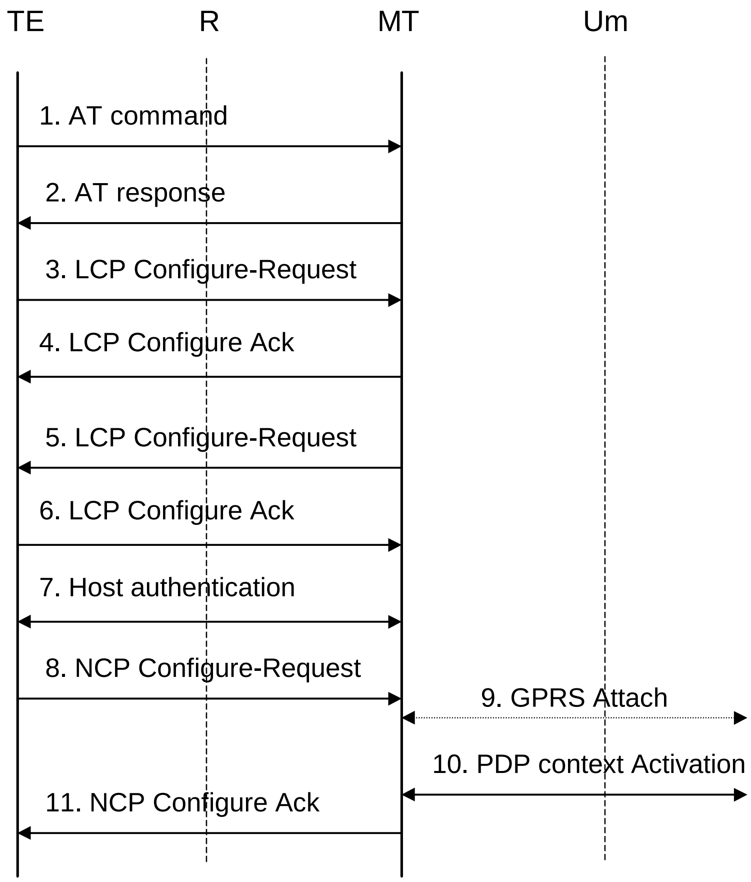


Figure 7: IP Over PPP Based Service

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 GSM 09.61 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 GPRS attached, the MT performs the GPRS Attach procedure as described in GSM 03.60.

10) The MT performs a PDP Context Activation as described in GSM 03.60. 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, t~~T~~he 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.

3GPP TSG-CN WG3/SMG3 WPD Meeting #7
Sophia-Antipolis, France, 29 Nov-03 Dec 1999

Document N3-99461
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

07.60	**CR**	**A019**	Current Version:	6.4.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	CN#6	for approval	X	strategic		*(for SMG*
list expected approval meeting # here ↑		for information		non-strategic	X	*use only)*

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)*	(U)SIM		ME	X	UTRAN / Radio		Core Network	

Source:	TSG_N3	**Date:**	1999-11-29
Subject:	IPCP negotiation interworking at the MT for non-transparent IP		
Work item:	GPRS		

Category:	F	Correction		**Release:**	Phase 2	
	A	Corresponds to a correction in an earlier release			Release 96	
(only one category	B	Addition of feature			Release 97	X
shall be marked	C	Functional modification of feature			Release 98	
with an X)	D	Editorial modification	X		Release 99	
					Release 00	

Reason for change:	During the PDP context activation procedure for PDP type IP, the MT may receive PPP IPCP packets, carried in the Protocol Configuration Options IE, from the network. It is not entirely clear in the current text how the MT shall act upon the reception of Configure-Ack, Configure-Nak and Configure-Reject packets.
Clauses affected:	9.1

Other specs affected:	Other 3G core specifications		→ List of CRs:	
	Other GSM core specifications		→ List of CRs:	
	MS test specifications		→ List of CRs:	
	BSS test specifications		→ List of CRs:	
	O&M specifications		→ List of CRs:	

Other comments:	There is also a corresponding CR for GSM 09.61 v6.3.0.

help.doc

<--------- double-click here for help and instructions on how to create a CR.

9.1 Example mapping of functions between the R reference point and the GPRS 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 interface) to support multiple virtual interfaces (communications ports) at the R reference point. Multiple PPP connections and IP contexts are possible in this case.

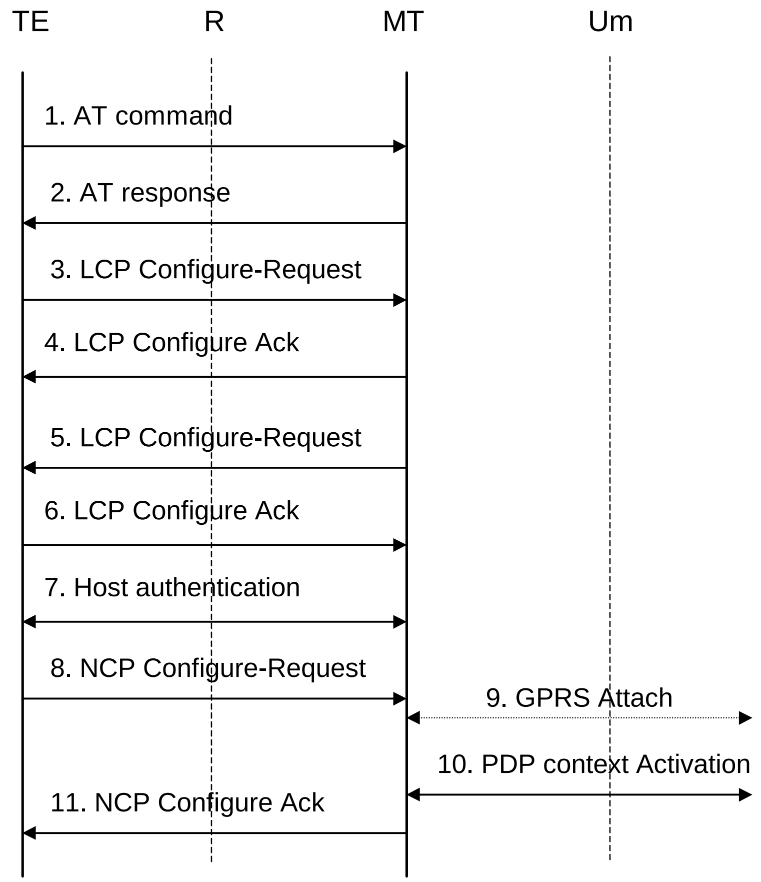


Figure 7: IP Over PPP Based Service

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 GSM 09.61 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 GPRS attached, the MT performs the GPRS Attach procedure as described in GSM 03.60.

10) The MT performs a PDP Context Activation as described in GSM 03.60. 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, t~~T~~he 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.

3GPP TSG-CN WG3/SMG3 WPD Meeting #7
Sophia-Antipolis, France, 29 Nov-03 Dec 1999

Document N3-99465
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

09.61	**CR**	**A013**	Current Version:	7.1.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	CN#6	for approval	X	strategic		*(for SMG use only)*
list expected approval meeting # here ↑		for information		non-strategic	X	

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from:* ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: *(at least one should be marked with an X)*	(U)SIM		ME	X	UTRAN / Radio		Core Network	X

Source:	TSG_N3	**Date:**	1999-11-29
Subject:	IPCP negotiation at the GGSN for non-transparent IP		
Work item:	GPRS		

Category:	F	Correction		**Release:**	Phase 2	
	A	Corresponds to a correction in an earlier release			Release 96	
(only one category	B	Addition of feature			Release 97	
shall be marked	C	Functional modification of feature			Release 98	X
with an X)	D	Editorial modification	X		Release 99	
					Release 00	

Reason for change: During the activation of a PDP Context for non-transparent IP the GGSN may receive PPP IPCP Configure-Request packets, from the MS, contained in the Protocol Configuration Options IE. Depending on the options and/or the requested values for the options the GGSN may choose to either acknowledge or reject the options and/or their proposed values. It is not entirely clear in the current text how this should be done.

Clauses affected: 11.2.1.2

Other specs affected:	Other 3G core specifications		→ List of CRs:	
	Other GSM core specifications		→ List of CRs:	
	MS test specifications		→ List of CRs:	
	BSS test specifications		→ List of CRs:	
	O&M specifications		→ List of CRs:	

Other comments: There is also a corresponding CR for GSM 07.60 v7.1.0.

help.doc

<--------- double-click here for help and instructions on how to create a CR.

11.2.1.2 Non Transparent access to an Intranet or ISP

In this case;

- the MS is given an address belonging to the Intranet/ISP addressing space. The address is given either at subscription in which case it is a static address or at PDP context activation in which case it is a dynamic address. This address is used for packet forwarding within the GGSN and for packet forwarding on the Intranet/ISP. This requires a link between the GGSN and an address allocation server, like Radius, DHCP, …, belonging to the Intranet/ISP;

- the MS shall send an authentication request at PDP context activation and the GGSN requests user authentication from a server, like Radius, DHCP, …, belonging to the Intranet/ISP;

- the protocol configuration options are retrieved (if requested by the MS at PDP context activation) from some server (Radius or DHCP, …) belonging to the Intranet/ISP;

- the communication between the GPRS PLMN and the Intranet/ISP may be performed over any network, even an insecure e.g. the Internet. In case of an insecure connection between the GGSN and the Intranet/ISP there may be a specific security protocol in between. This security protocol is defined by mutual agreement between GPRS PLMN operator and Intranet/ISP administrator.

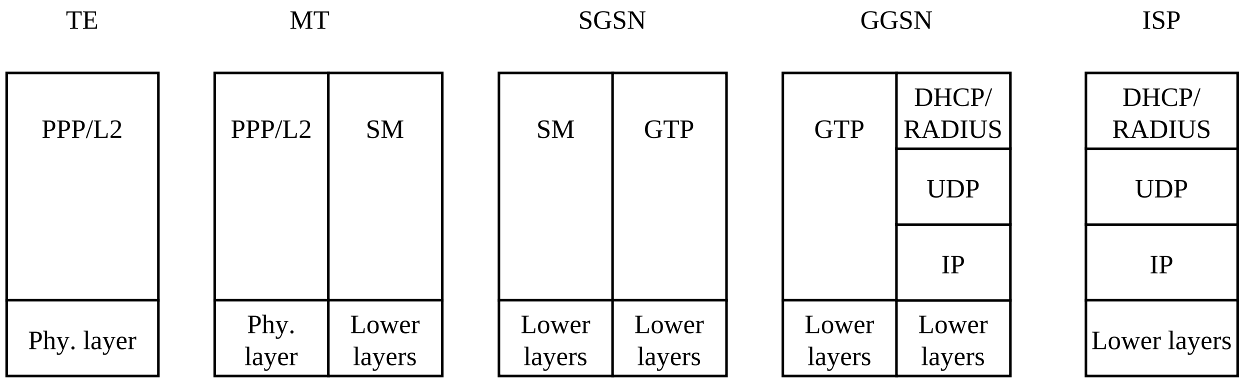


Figure 11: Signalling plane of non transparent case

The following description bullet items describe the signal flow.

1) The TE sends an AT-command to the MT to set up parameters and enter PPP mode. The MT responds with an AT-response.

2) LCP negotiates Maximum-Receive-Unit and authentication protocol. The negotiated authentication protocol is, either CHAP, PAP or ‘none’. The MT shall try to negotiate for CHAP as first priority.

3) 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 forced positive acknowledgement of the authentication to the TE.

4) The TE requests IP configuration by sending the IPCP Configure-Request message to the MT indicating either the static IP address that shall be used or that an IP-address shall be dynamically allocated.

5) The MT sends the Activate PDP context request message to the SGSN, including the Protocol Configuration Options. The SGSN sends the Create PDP context req message to the chosen GGSN including the unmodified Protocol Configuration Options.

6) The GGSN deduces from the APN :

    - the server(s) to be used for address allocation, authentication and protocol configuration options retrieval;

    - the protocol like Radius, DHCP, … to be used with this / those server(s);

    - the communication and security feature needed to dialogue with this / those server(s) e.g. tunnel ,IPSec security association, dial-up connection (using possibly PPP), ….

    As an example the GGSN may use one of the following options:

- RADIUS for authentication and IP-address allocation.. The RADIUS server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN.

- RADIUS for authentication and DHCP for host configuration and address allocation. The RADIUS server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN. After a successful authentication, the DHCP client discovers the DHCP server(s) in the ISP/Intranet and receives host configuration data. ~~.~~

If the received Protocol Configurations Options IE contains a PPP IPCP Configure-Request packet, the GGSN shall analyse all the contained IPCP options and their requested values. In accordance with the relevant PPP RFC[20] the GGSN shall respond with the following messages:

- Zero or one PPP IPCP Configure-Reject packet containing options not supported and options which values cannot be returned,

- zero or one PPP IPCP Configure-Nak packet containing options that are supported but has requested values that are incorrect/unsupported and

- zero or one PPP IPCP Configure-Ack packet containing options that are supported and has requested values that are correct/supported.

Any returned PPP IPCP packets shall be contained in the Protocol Configurations Options IE.

7) The GGSN sends back to the SGSN a Create PDP Context Response message, containing the Protocol Configuration Options IE. The cause value shall be set according to the outcome of the host -authentication and -configuration. A PDP context activation shall not be rejected solely due to the presence of unsupported or incorrect PPP IPCP options or option values, received from the MS in the Protocol Configurations Options IE. The MS may however later decide to immediately deactivate the activated PDP context due to the information received in the Protocol Configurations Options IE received from the network.

8) Depending on the cause value received in the Create PDP Context Response the SGSN sends either an Activate PDP Context Accept or an Activate PDP Context Reject, to the MS.

   If Protocol Configuration Options are received from the GGSN, the SGSN shall relay those to the MS. The MT sends either the configuration-ack packet (e.g. IPCP Configure Ack in PPP case), the configure-nack packet in case of dynamic address allocation (e.g. IPCP Configure Nack in PPP case), or a link Terminate request (LCP Terminate-Request in PPP case) back to the TE. In the case where a configure-nack packet was sent by the MT, a local negotiation may take place at the R reference point (i.e. the TE proposes the new value to the MT), after which a configuration-ack packet is sent to the TE.

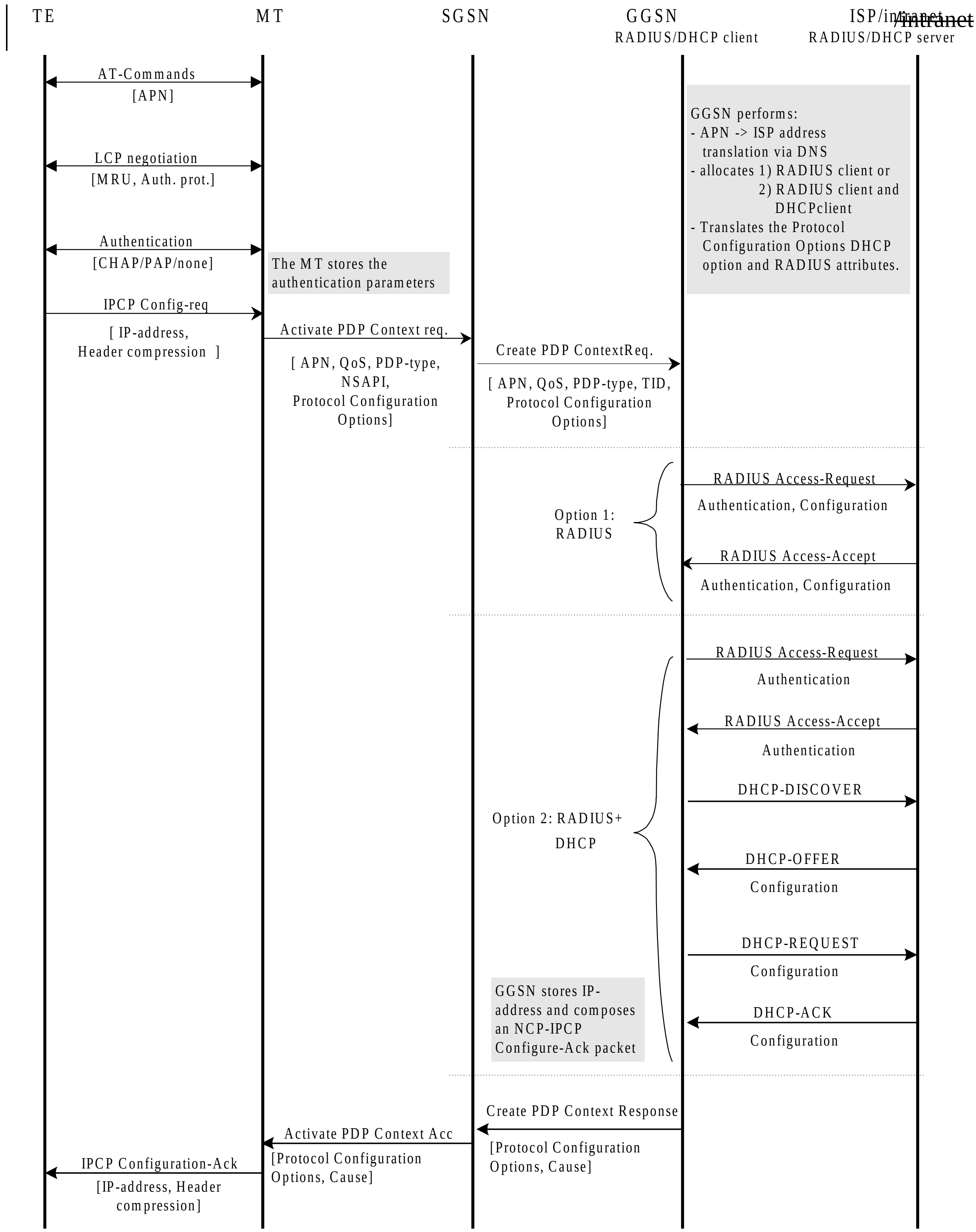
9) In case a configuration-ack packet was sent to the TE, the link from the TE to the external ISP/Intranet is established and IP packets may be exchanged.

   In case a link terminate request packet was sent to the TE, the TE and MT negotiates for link termination. The MT may then send a final AT-response to inform the TE about the rejected PDP Context activation.

A link terminate request packet (such as LCP Terminate-request in PPP case) causes a PDP context deactivation.

Example: In the following example PPP is used as layer 2 protocol over the R reference point.

The MT acts as a PPP server and translates Protocol Configuration Options into SM message IEs. GTP carries this information unchanged to the GGSN which uses the information e.g. for DHCP or RADIUS authentication and host configuration. The result of the host authentication and configuration is carried via GTP to the SGSN which relays the information to the MT. The MT sends an IPCP Configure-Ack to the TE with the appropriate options included.


TE
MT
SGSN
GGSN
RADIUS/DHCP client
ISP/intranet
/intranet
RADIUS/DHCP server
AT-Commands
[APN]
LCP negotiation
[MRU, Auth. prot.]
Authentication
[CHAP/PAP/none]
The MT stores the authentication parameters
IPCP Config-req
[IP-address, Header compression]
Activate PDP Context req.
[APN, QoS, PDP-type, NSAPI, Protocol Configuration Options]
Create PDP ContextReq.
[APN, QoS, PDP-type, TID, Protocol Configuration Options]
GGSN performs:
- APN -> ISP address translation via DNS
- allocates 1) RADIUS client or
2) RADIUS client and DHCPclient
- Translates the Protocol Configuration Options DHCP option and RADIUS attributes.
Option 1: RADIUS
RADIUS Access-Request
Authentication, Configuration
RADIUS Access-Accept
Authentication, Configuration
Option 2: RADIUS+ DHCP
RADIUS Access-Request
Authentication
RADIUS Access-Accept
Authentication
DHCP-DISCOVER
DHCP-OFFER
Configuration
DHCP-REQUEST
Configuration
GGSN stores IP-address and composes an NCP-IPCP Configure-Ack packet
DHCP-ACK
Configuration
Create PDP Context Response
[Protocol Configuration Options, Cause]
Activate PDP Context Acc
[Protocol Configuration Options, Cause]
IPCP Configuration-Ack
[IP-address, Header compression]

3GPP TSG-CN WG3/SMG3 WPD Meeting #7
Sophia-Antipolis, France, 29 Nov-03 Dec 1999

Document N3-9964

e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

09.61	**CR**	**A012**	Current Version:	6.3.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	CN#6	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic	X	

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from:* ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [X]
(at least one should be marked with an X)

Source: TSG_N3 **Date:** 1999-11-29

Subject: IPCP negotiation at the GGSN for non-transparent IP

Work item: GPRS

Category: *(only one category shall be marked with an X)*

F	Correction		
A	Corresponds to a correction in an earlier release		
B	Addition of feature		
C	Functional modification of feature		
D	Editorial modification	X	

Release:

Phase 2	
Release 96	
Release 97	X
Release 98	
Release 99	
Release 00	

Reason for change: During the activation of a PDP Context for non-transparent IP the GGSN may receive PPP IPCP Configure-Request packets, from the MS, contained in the Protocol Configuration Options IE. Depending on the options and/or the requested values for the options the GGSN may choose to either acknowledge or reject the options and/or their proposed values. It is not entirely clear in the current text how this should be done.

Clauses affected: 2, 11.2.1.2

Other specs affected:

Other 3G core specifications		→ List of CRs:
Other GSM core specifications		→ List of CRs:
MS test specifications		→ List of CRs:
BSS test specifications		→ List of CRs:
O&M specifications		→ List of CRs:

Other comments: There is also a corresponding CR for GSM 07.60 v6.4.0.

help.doc

<--------- double-click here for help and instructions on how to create a CR.

2 Normative References

[20] IETF RFC 1661 (1994): " The Point-to-Point Protocol (PPP)" (STD 51).

***************************Next affected section*********************************

11.2.1.2 Non Transparent access to an Intranet or ISP

In this case;

- the MS is given an address belonging to the Intranet/ISP addressing space. The address is given either at subscription in which case it is a static address or at PDP context activation in which case it is a dynamic address. This address is used for packet forwarding within the GGSN and for packet forwarding on the Intranet/ISP. This requires a link between the GGSN and an address allocation server, like Radius, DHCP, …, belonging to the Intranet/ISP;
- the MS shall send an authentication request at PDP context activation and the GGSN requests user authentication from a server, like Radius, DHCP, …, belonging to the Intranet/ISP;
- the protocol configuration options are retrieved (if requested by the MS at PDP context activation) from some server (Radius or DHCP, …) belonging to the Intranet/ISP;
- the communication between the GPRS PLMN and the Intranet/ISP may be performed over any network, even an insecure e.g. the Internet. In case of an insecure connection between the GGSN and the Intranet/ISP there may be a specific security protocol in between. This security protocol is defined by mutual agreement between GPRS PLMN operator and Intranet/ISP administrator.

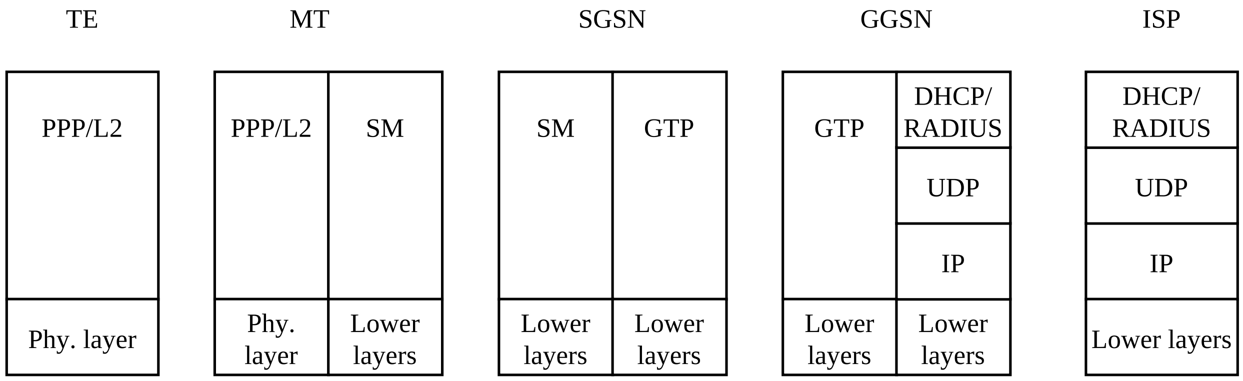


Figure 11: Signalling plane of non transparent case

The following description bullet items describe the signal flow.

1) The TE sends an AT-command to the MT to set up parameters and enter PPP mode. The MT responds with an AT-response.

2) LCP negotiates Maximum-Receive-Unit and authentication protocol. The negotiated authentication protocol is, either CHAP, PAP or ‘none’. The MT shall try to negotiate for CHAP as first priority.

3) 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 forced positive acknowledgement of the authentication to the TE.

4) The TE requests IP configuration by sending the IPCP Configure-Request message to the MT indicating either the static IP address that shall be used or that an IP-address shall be dynamically allocated.

5) The MT sends the Activate PDP context request message to the SGSN, including the Protocol Configuration Options. The SGSN sends the Create PDP context req message to the chosen GGSN including the unmodified Protocol Configuration Options.

6) The GGSN deduces from the APN :

- the server(s) to be used for address allocation, authentication and protocol configuration options retrieval;
- the protocol like Radius, DHCP, … to be used with this / those server(s);
- the communication and security feature needed to dialogue with this / those server(s) e.g. tunnel ,IPSec security association, dial-up connection (using possibly PPP), ….

As an example the GGSN may use one of the following options:

- RADIUS for authentication and IP-address allocation.. The RADIUS server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN.

- RADIUS for authentication and DHCP for host configuration and address allocation. The RADIUS server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN. After a successful authentication, the DHCP client discovers the DHCP server(s) in the ISP/Intranet and receives host configuration data. ~~.~~

If the received Protocol Configurations Options IE contains a PPP IPCP Configure-Request packet, the GGSN shall analyse all the contained IPCP options and their requested values. In accordance with the relevant PPP RFC[20] the GGSN shall respond with the following messages:

- Zero or one PPP IPCP Configure-Reject packet containing options not supported and options which values cannot be returned,

- zero or one PPP IPCP Configure-Nak packet containing options that are supported but has requested values that are incorrect/unsupported and

- zero or one PPP IPCP Configure-Ack packet containing options that are supported and has requested values that are correct/supported.

Any returned PPP IPCP packets shall be contained in the Protocol Configurations Options IE.

7) The GGSN sends back to the SGSN a Create PDP Context Response message, containing the Protocol Configuration Options IE. The cause value shall be set according to the outcome of the host -authentication and -configuration. A PDP context activation shall not be rejected solely due to the presence of unsupported or incorrect PPP IPCP options or option values, received from the MS in the Protocol Configurations Options IE. The MS may however later decide to immediately deactivate the activated PDP context due to the information received in the Protocol Configurations Options IE received from the network.

8) Depending on the cause value received in the Create PDP Context Response the SGSN sends either an Activate PDP Context Accept or an Activate PDP Context Reject, to the MS.

   If Protocol Configuration Options are received from the GGSN, the SGSN shall relay those to the MS. The MT sends either the configuration-ack packet (e.g. IPCP Configure Ack in PPP case), the configure-na~~c~~k packet in case of dynamic address allocation (e.g. IPCP Configure Na~~c~~k in PPP case), or a link Terminate request (LCP Terminate-Request in PPP case) back to the TE. In the case where a configure-na~~c~~k packet was sent by the MT, a local negotiation may take place at the R reference point (i.e. the TE proposes the new value to the MT), after which a configuration-ack packet is sent to the TE.

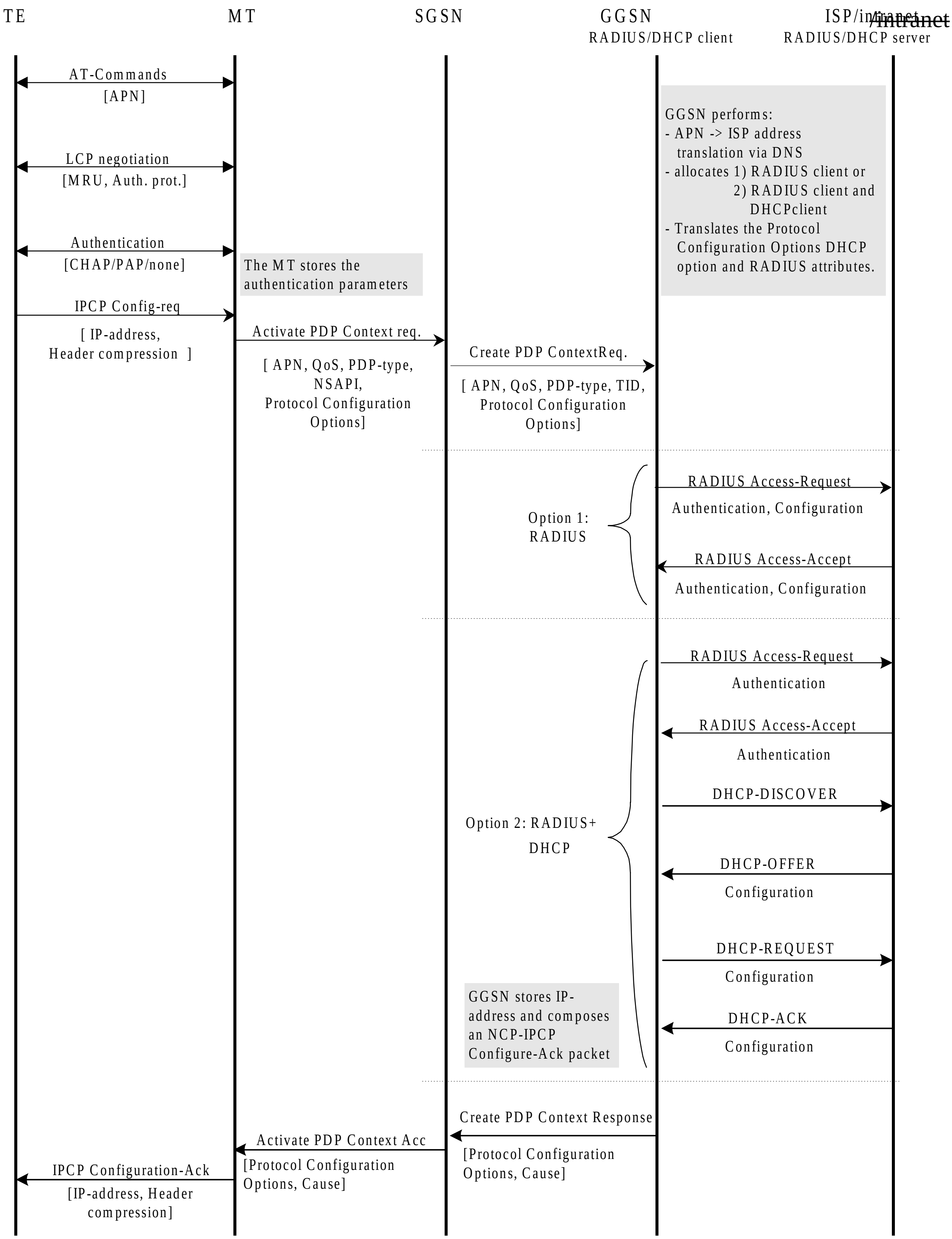
9) In case a configuration-ack packet was sent to the TE, the link from the TE to the external ISP/Intranet is established and IP packets may be exchanged.

   In case a link terminate request packet was sent to the TE, the TE and MT negotiates for link termination. The MT may then send a final AT-response to inform the TE about the rejected PDP Context activation.

A link terminate request packet (such as LCP Terminate-request in PPP case) causes a PDP context deactivation.

Example: In the following example PPP is used as layer 2 protocol over the R reference point.

The MT acts as a PPP server and translates Protocol Configuration Options into SM message IEs. GTP carries this information unchanged to the GGSN which uses the information e.g. for DHCP or RADIUS authentication and host configuration. The result of the host authentication and configuration is carried via GTP to the SGSN which relays the information to the MT. The MT sends an IPCP Configure-Ack to the TE with the appropriate options included.


TE
MT
SGSN
GGSN
RADIUS/DHCP client
ISP/intranet
RADIUS/DHCP server
AT-Commands
[APN]
LCP negotiation
[MRU, Auth. prot.]
Authentication
[CHAP/PAP/none]
The MT stores the authentication parameters
IPCP Config-req
[IP-address, Header compression]
Activate PDP Context req.
[APN, QoS, PDP-type, NSAPI, Protocol Configuration Options]
Create PDP ContextReq.
[APN, QoS, PDP-type, TID, Protocol Configuration Options]
GGSN performs:
- APN -> ISP address translation via DNS
- allocates 1) RADIUS client or 2) RADIUS client and DHCPclient
- Translates the Protocol Configuration Options DHCP option and RADIUS attributes.
Option 1: RADIUS
RADIUS Access-Request
Authentication, Configuration
RADIUS Access-Accept
Authentication, Configuration
Option 2: RADIUS+ DHCP
RADIUS Access-Request
Authentication
RADIUS Access-Accept
Authentication
DHCP-DISCOVER
DHCP-OFFER
Configuration
DHCP-REQUEST
Configuration
DHCP-ACK
Configuration
GGSN stores IP-address and composes an NCP-IPCP Configure-Ack packet
Create PDP Context Response
[Protocol Configuration Options, Cause]
Activate PDP Context Acc
[Protocol Configuration Options, Cause]
IPCP Configuration-Ack
[IP-address, Header compression]

3GPP TSG-CN WG3/SMG3 WPD Meeting #7
Sophia-Antipolis, France, 29 Nov-03 Dec 1999

***Document* N3-99463**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

27.060 CR 006 Current Version: 3.2.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	CN#6	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)*	(U)SIM		ME	X	UTRAN / Radio		Core Network	

Source: Ericsson **Date:** 1999-11-29

Subject: IPCP negotiation interworking at the MT for non-transparent IP

Work item: GPRS

Category:				**Release:**		
	F	Correction			Phase 2	
	A	Corresponds to a correction in an earlier release			Release 96	
(only one category	B	Addition of feature			Release 97	
shall be marked	C	Functional modification of feature			Release 98	
with an X)	D	Editorial modification	X		Release 99	X
					Release 00	

Reason for change: During the PDP context activation procedure for PDP type IP, the MT may receive PPP IPCP packets, carried in the Protocol Configuration Options IE, from the network. It is not entirely clear in the current text how the MT shall act upon the reception of Configure-Ack, Configure-Nak and Configure-Reject packets.

Clauses affected: 9.1

Other specs affected:			
	Other 3G core specifications		→ List of CRs:
	Other GSM core specifications		→ List of CRs:
	MS test specifications		→ List of CRs:
	BSS test specifications		→ List of CRs:
	O&M specifications		→ List of CRs:

Other comments: There is also a corresponding CR for 3G TS 29.061 v3.1.0.

help.doc

<--------- double-click here for help and instructions on how to create a CR.

9.1 Example mapping of functions between the R reference point and the GPRS 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 interface) to support multiple virtual interfaces (communications ports) at the R reference point. Multiple PPP connections and IP contexts are possible in this case.

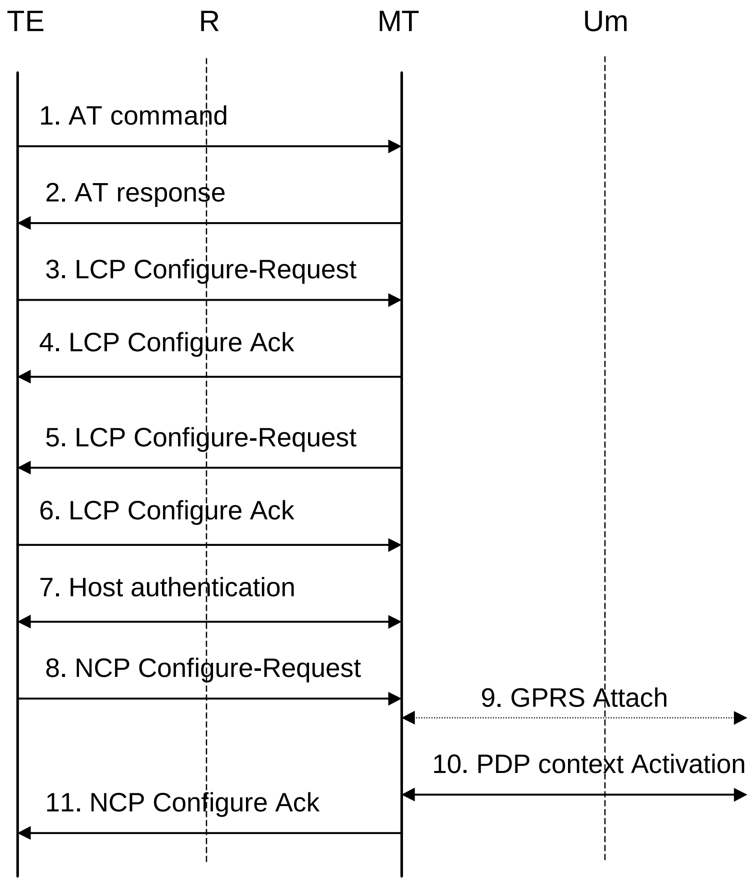


Figure 7: IP Over PPP Based Service

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 GSM 09.61 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 GPRS attached, the MT performs the GPRS Attach procedure as described in GSM 03.60.

10) The MT performs a PDP Context Activation as described in GSM 03.60. 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, t~~T~~he 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.

3GPP TSG-CN WG3/SMG3 WPD Meeting #7
Sophia-Antipolis, France, 29 Nov-03 Dec 1999

Document N3-99469
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

27.060	**CR**	**007**	Current Version:	3.2.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG_CN#6	for approval	X	strategic		*(for SMG*
list expected approval meeting # here ↑		for information		non-strategic		*Use only)*

Proposed change affects: (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]
(at least one should be marked with an X)

Source: TSG_N3 **Date:** 1999-11-29

Subject: Clarification on the tasks of the MT for PDP type PPP.

Work item: GPRS

Category:				**Release:**		
	F	Correction			Phase 2	
	A	Corresponds to a correction in an earlier release			Release 96	
(only one category	B	Addition of feature			Release 97	
shall be marked	C	Functional modification of feature			Release 98	
with an X)	D	Editorial modification	X		Release 99	X
					Release 00	

Reason for change: During the R2#7 meeting a number of issues were brought up concerning the tasks of the MT regarding PPP framing and LCP negotiation for PDP type PPP. This CR clarifies these issues.

Clauses affected: 10, 10.1

Other specs affected:			
	Other 3G core specifications		→ List of CRs:
	Other GSM core specifications		→ List of CRs:
	MS test specifications		→ List of CRs:
	BSS test specifications		→ List of CRs:
	O&M specifications		→ List of CRs:

Other comments: There is also a corresponding CR for 3G TS 29.061 v3.1.0.

help.doc

<--------- double-click here for help and instructions on how to create a CR.

10 PPP Based Services

By means of the PDP type 'PPP' GPRS 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 configuration is depicted in figure 8.

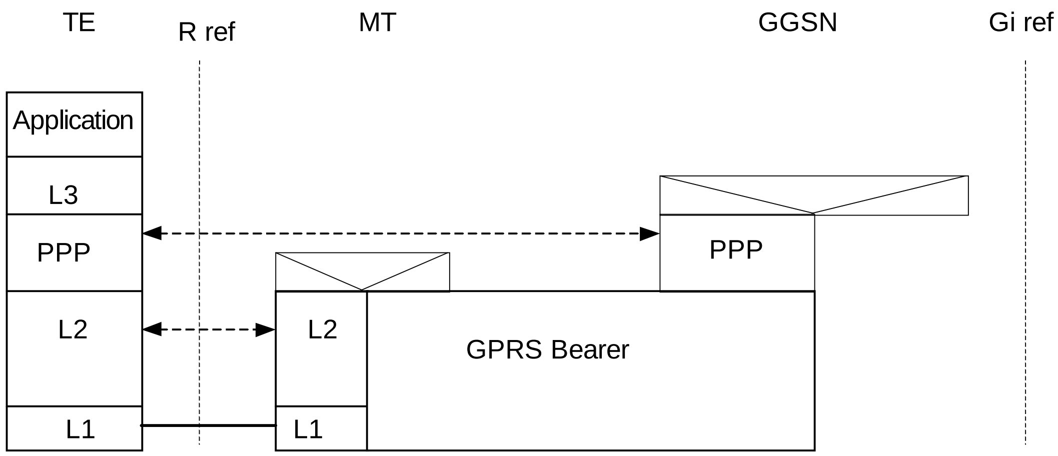
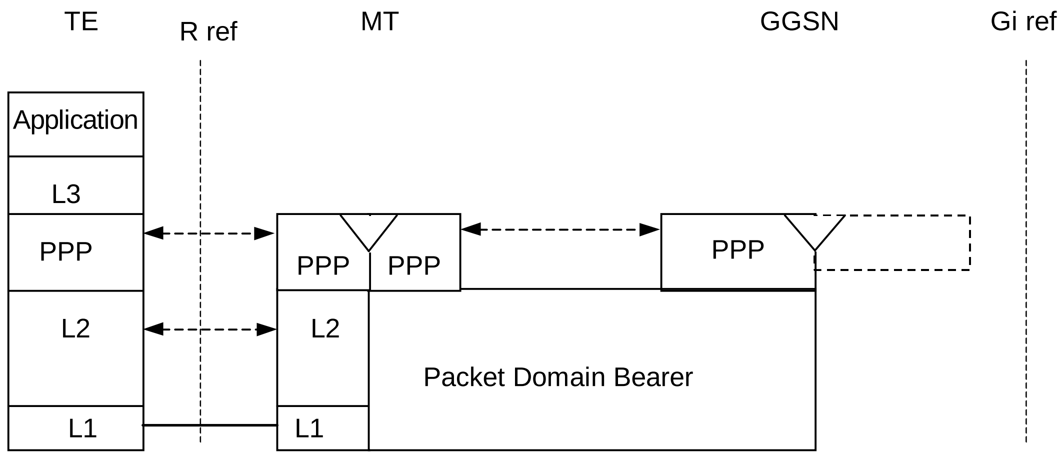


Figure 8: PPP Based Services (transparent PPP negotiation)



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

Figure X: 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 GPRS 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 X).

10.1 Example mapping of functions between the R reference point and the GPRS 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.

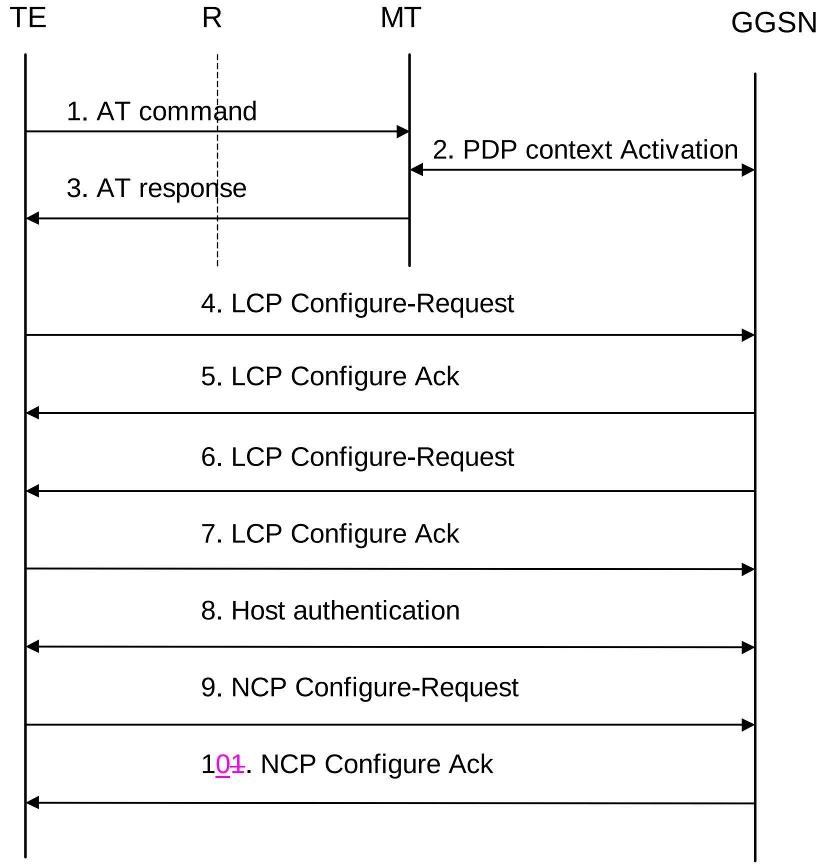


Figure 9: PPP Based Service (transparent PPP negotiation)

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 GSM 03.60.

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.

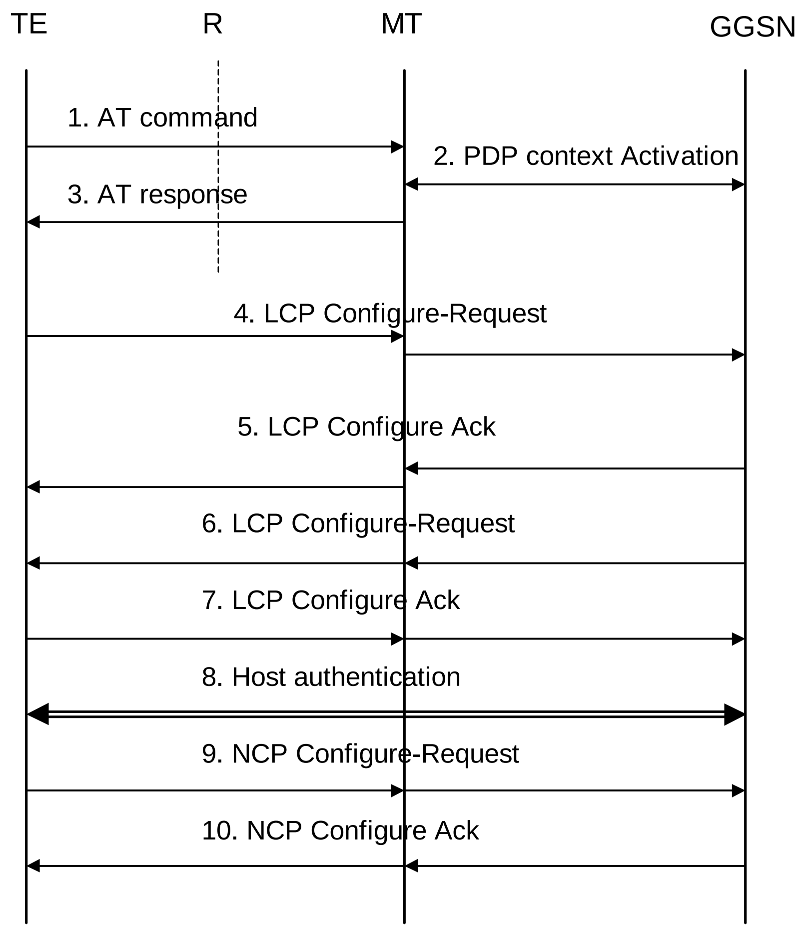


Figure Y: PPP Based Service (relayed PPP negotiation)

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 ~~GSM 0~~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.

3GPP TSG-CN WG3/SMG3 WPD Meeting #7
Sophia-Antipolis, France, 29/11-3/12 1999

Document N3-99484
e.g. for 3GPP use the format TP-99xxx or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

27.060 CR 008 Current Version: 3.2.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	CN #6	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: *(at least one should be marked with an X)*	(U)SIM		ME	X	UTRAN / Radio		Core Network

Source: TSG CN3 **Date:** 1999-11-30

Subject: Alignment to 23.060 v3.1.0 Draft 3

Work item: GPRS

Category:				**Release:**		
	F	Correction			Phase 2	
	A	Corresponds to a correction in an earlier release			Release 96	
(only one category	B	Addition of feature			Release 97	
shall be marked	C	Functional modification of feature	X		Release 98	
with an X)	D	Editorial modification			Release 99	X
					Release 00	

Reason for change: The 23.060 is in the process of being updated to describe the R'99 of the GPRS and UMTS Packet Domain. The 27.060 should undergo the same treatment.

Clauses affected: All

Other specs affected:				
	Other 3G core specifications	X	→ List of CRs:	23.060
	Other GSM core specifications		→ List of CRs:	
	MS test specifications		→ List of CRs:	
	BSS test specifications		→ List of CRs:	
	O&M specifications		→ List of CRs:	

Other comments: This CR relates to the agreed CRs on 23.060, which update the 23.060 to describe the R'99 of the GPRS and UMTS packet Domain.

3G TS 27.060 V3.3~~1~~.0 (1999-11~~08~~)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Core Network;
Packet Domain~~General Packet Radio Service (GPRS)~~;
Mobile Station (MS) supporting Packet Switched Services~~GPRS~~
(3G TS 27.060 version 3.3~~1~~.0)

Reference

DTS/TSGN-0327060U

Keywords

3GPP, CN

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3GPP.

~~This TS provides the necessary information to develop a MS for support of GPRS within the 3GPP system.~~

The present document defines the requirements for TE-MT interworking over the R-reference point for~~for GPRS within GSM and~~ 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 this TS, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version 3.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 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 specification;

Introduction

Thi~~se present~~ document defines the requirements for TE-MT interworking over the R-reference point- for the Packet Domain, within the GSM and 3GPP systems.~~The present document contains the necessary information to develop a MS for support of GPRS.~~ It is up to the manufacturer how to implement the various functions but this specification and existing ~~GSM~~ 3G TS ~~07.0~~27.001, ~~07.0~~27.002, and ~~07.0~~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 ~~GPRS~~ 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 ~~GSM~~ 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 ~~in the~~ the Packet Domain ~~The present document describes the functionality of a MS supporting GPRS~~, including the protocols and signalling needed to support Packet Switched services~~the first phase of GPRS~~, as defined in 3G TS 22.060~~GSM 02.60~~ and 3G TS 23.060~~03.60 (packet based services)~~.

2 References

[All references need to be checked once release 99 stabilizes.]

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.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

~~For this Release 1998 document, references to GSM documents are for Release 1998 versions (version 7.x.y).~~

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

[2] GSM 02.02: "Digital cellular telecommunication system (Phase 2+); Bearer Services (BS) supported by a GSM Public Land Mobile Network (PLMN)".

[3] 3G TS ~~GSM 02~~22.060: "Digital cellular telecommunication system (Phase 2+); General Packet Radio Service (GPRS); Service Description Stage 1".

[4] GSM 03.02: "Digital cellular telecommunication system (Phase 2+); Network architecture".

[5] 3G TS ~~GSM 02~~23.003: "Digital cellular telecommunications system (Phase 2+); 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 ~~GSM 02~~23.022: "Digital cellular telecommunications system (Phase 2+); Functions related to Mobile Station (MS) in idle mode and group receive mode".

[8] 3G TS ~~GSM 02~~23.040: "Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS); Point-to-Point (PP)".

[9] 3G TS ~~GSM 02~~23.060: "Digital cellular telecommunication system (Phase 2+); 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 ~~GSM 02~~24.007: "Digital cellular telecommunications system (Phase 2+); Mobile radio interface signalling layer 3; General aspects".

[12] 3G TS ~~GSM 0~~24.008: "Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification".

[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] GSM 04.65: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Subnetwork Dependent Convergence Protocol (SNDCP)".

[16] 3G TS ~~GSM 0~~27.007: "Digital cellular telecommunication system (Phase 2+); AT command set for GSM Mobile Equipment (ME)".

[17] 3G TS ~~GSM 0~~29.061: "3RD Generation Partnership Project; Technical Specification Group Core Network; Packet Domain;~~Digital cellular telecommunication system (Phase 2+); General Packet Radio Service (GPRS);~~ Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services~~GPRS~~ 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] CCITT Recommendation X.3: "Packet assembly disassembly facility (PAD) in a public data network".

[21] CCITT Recommendation X.25: "Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit".

[22] CCITT Recommendation X.28: "DTE / DCE interface for a start-stop mode data terminal equipment accessing the packet assembly / disassembly facility (PAD) in a public data network situated in the same country".

[23] CCITT Recommendation X.29: "Procedures for the exchange of control information and user data between a packet assembly / disassembly (PAD) facility and a packet mode DTE or another PAD".

[24] CCITT Recommendation X.75: "Packet-switched signalling system between public networks providing data transmission services".

[25] CCITT Recommendation X.121: "International Numbering Plan for Public Data Networks".

[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).

[3]7 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“.

3 Definitions abbreviations and symbols

3.1 Definitions

~~Refer to: 3G TS GSM 022.060 [2].~~

~~In GSM 3G TS 02.022.002 the bearer services are described. The general network configuration is described in GSM 03.02 and the GSM PLMN access reference configuration is defined in GSM 3G TS 024.002. The various connection types used in the GSM PLMN are presented in GSM 03.10. Terminology used in the present document is presented in GSM 01.04. For support of data services between GSM PLMN and other networks see GSM 3G TS 029 series of Specifications.~~

Refer to 3G TS 22.060 and 3G TS 23.060.

2G- / 3G- The prefixes 2G- and 3G- refers to functionality that supports only GSM GPRS or UMTS, respectively, e.g., 2G-SGSN refers only to the GSM GPRS functionality of an SGSN. When the prefix is omitted, reference is made independently from the GSM GPRS 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~~	~~GPRS Tunnelling Protocol~~
GTP-U	GPRS Tunnelling Protocol for user plane
HDLC	High Level Data Link Control
ICMP	Internet Control Message Protocol
IHOSS	Internet Hosted Octet Stream Service
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LA	Location Area
LAPB	Link Access Protocol Balanced
LCP	Link Control Protocol
LLC	Logical Link Control
MAC	Medium Access Control
ME	Mobile Equipment
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, X.25 or PPP
PDU	Protocol Data Unit
PPP	Point-to-Point Protocol
PS	Packet Switched
~~PS attach~~	~~Packet Switched attach~~
PSPDN	Packet Switched Public Data Network
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
TE	Terminal Equipment
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

3.3 Symbols

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

Gb	Interface between a~~n~~ SGSN and a BSC.
Gi	Reference point between ~~GPRS~~ 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 ~~GPRS~~ Packet Domain network services across areas served by the co-operating ~~GPRS~~ PLMNs.
Gs	Interface between an SGSN and MSC.
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 GPRS fixed network part. The Um interface is the GPRS network interface for providing packet data services over the radio to the MS. The MT part of the MS is used to access the GPRS 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~~GPRS~~ environment.

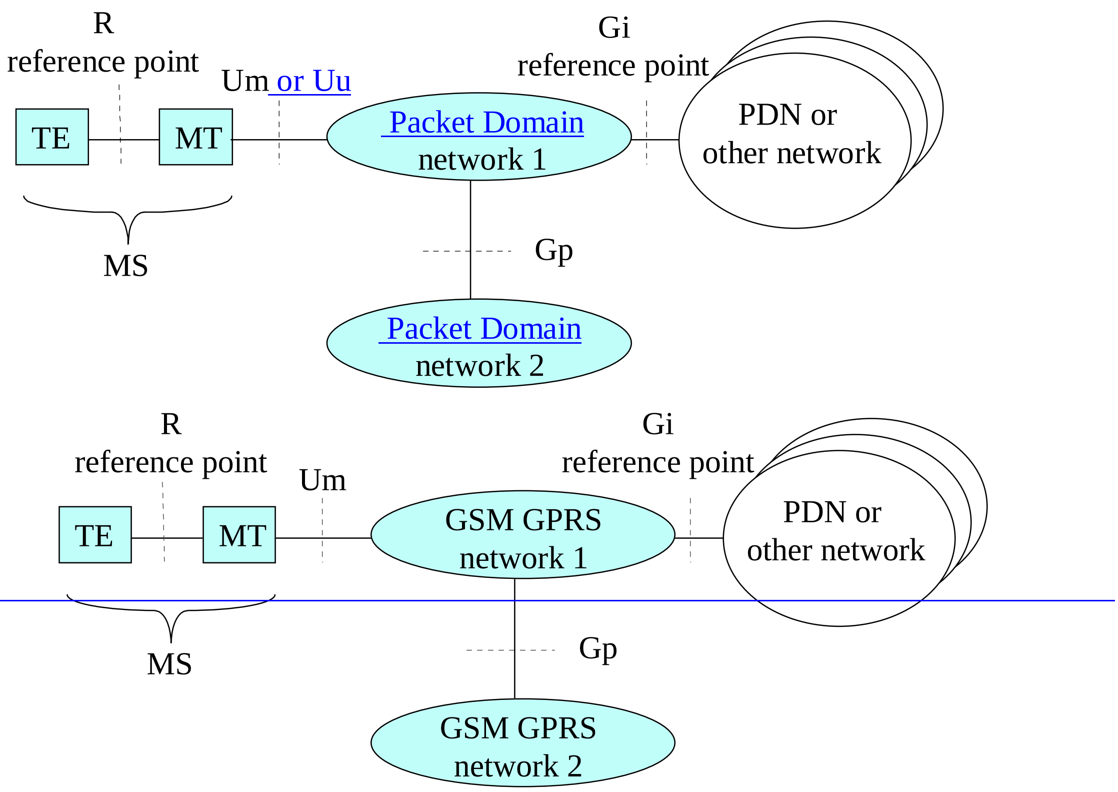


Figure 1: ~~GPRS~~ Packet Domain Access Interfaces and Reference Points

5 Functions to support data services

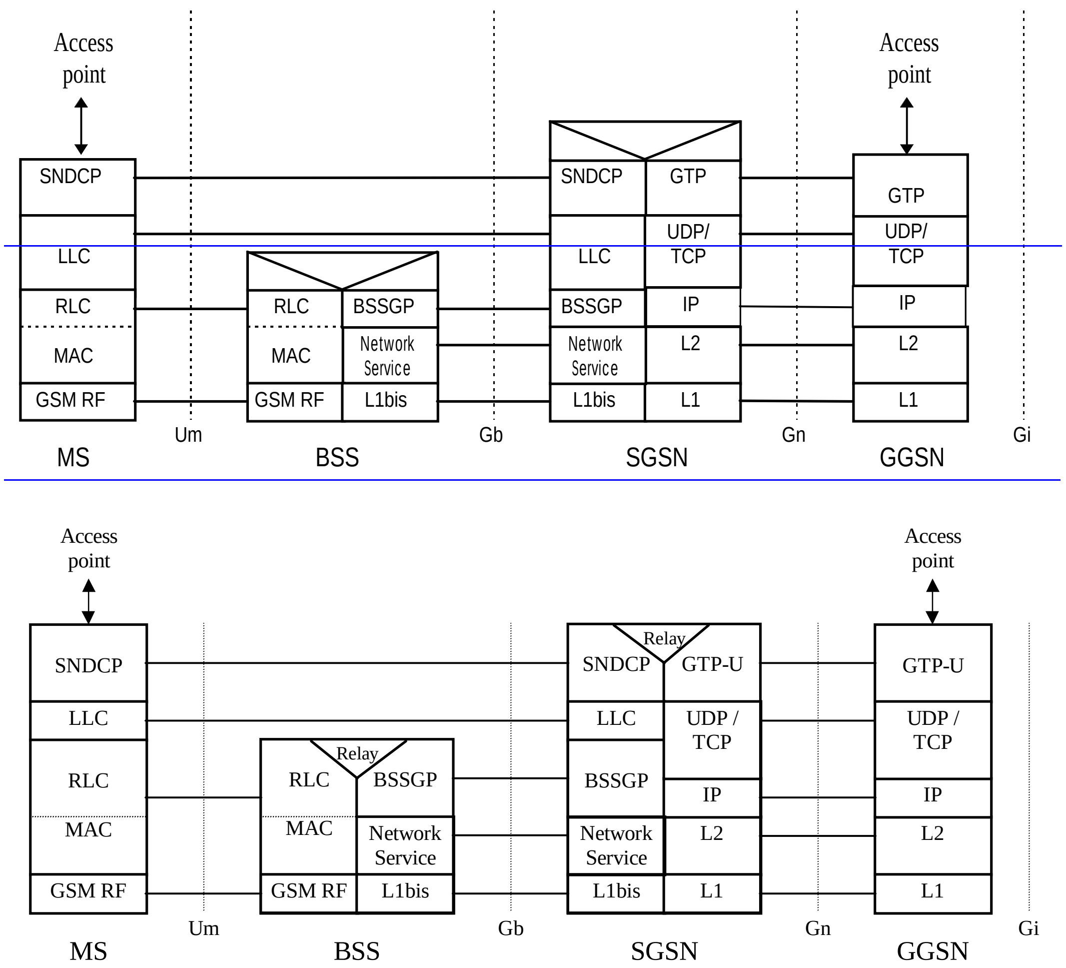
The main functions of the MT to support data services are:

- physical connection at the reference point R;
- flow control between TE and MT;
- mapping of user signalling to/from the ~~GPRS~~ Packet Domain bearer;
- support of data integrity between the terminal equipment and the Packet Domain~~GPRS~~ bearer;
- functions to support character based data;
- functions to support packet based data;

6 Interface to ~~GPRS~~ Packet Domain Bearer Services

6.1 GPRS

The following figure 2~~: Transmission Plane~~ shows the relationship of the GPRS Bearer, terminating at the SNDCP layer, to the rest of the GPRS environment. It is shown for reference purposes only and detailed information can be found in ~~GSM 03.60~~3G TS 23.060.



NOTE: In the SGSN and GGSN UDP is mandatory. TCP is optional but recommended for X.25 services.

Figure 2: GPRS ~~Transmission~~ User Plane

6.2 UMTS

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

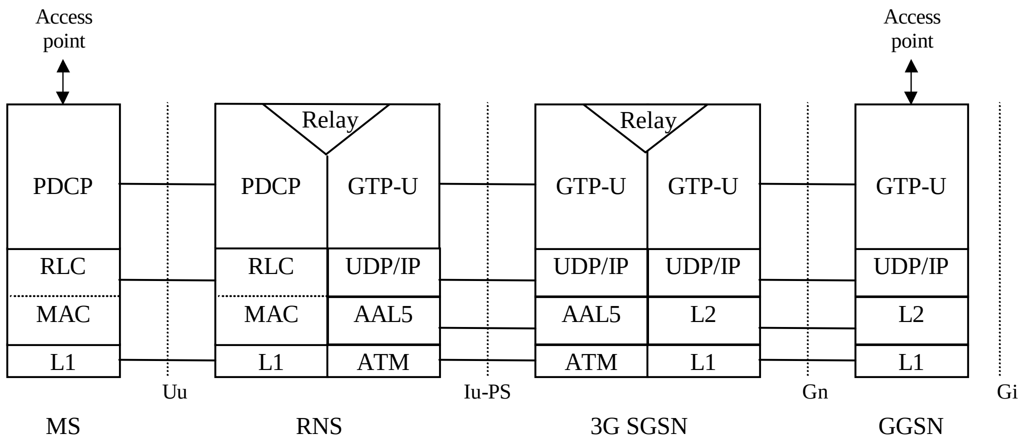


Figure X: UMTS User Plane

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

7.1 Mobile Station Modes of Operation~~Classes~~

Three GPRS MS ~~c~~modes of operation~~lasses~~ are identified: Class A, B, and C. These modes of operation~~classes~~ are described in ~~GSM 02.60~~3G TS 23~~2~~.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 GPRS. A PS mode of operation corresponds to class-C mode of operation in GPRS. A CS mode of operation is out of scope in this specification.

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 ~~GSM~~ 3G TS ~~0~~27.001, ~~0~~27.002, and ~~0~~27.003. ~~This shall not preclude any new developments such as USB (Universal Serial Bus).~~

7.3 Terminal context procedures

This subclause describes the relationships for ~~GPRS~~ PS Attach and Detach, and PDP Context Activation, Modification and Deactivation. The procedures for these functions are described in 3G TS 23.060~~GSM 03.60~~.

7.3.1 ~~G~~P~~R~~S Attach

The ~~G~~P~~R~~S Attach shall be performed prior to activating a PDP context. The ~~G~~P~~R~~S Attach may be performed automatically or manually depending on the manufacturer’s implementation and configuration.

7.3.2 ~~G~~P~~R~~S Detach

The ~~G~~P~~R~~S 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 ~~G~~P~~R~~S Detach procedure;
- if the network originates a ~~G~~P~~R~~S 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 ~~G~~P~~R~~S Detach procedure.

7.3.3 MS~~obile~~ 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.x MS~~obile~~ 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.

7.3.4 Network Requested PDP Context Activation.

The network can request a ~~G~~P~~R~~S attached MS to activate a specific PDP context.

7.3.y 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.

7.3.5 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 ~~G~~P~~R~~S Detach procedure.

7.3.6 PDP context related parameters

7.3.6.1 GPRS

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

- Requested Quality of Service.
  (this includes the peak bit rate, the mean bit rate, the delay requirements, the service precedence, and the reliability level)
- Data 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)

7.3.6.2 UMTS

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

- Requested Quality of Service.
  (this includes Traffic class, Maximum bitrate, Guaranteed bitrate, Delivery order, Maximum SDU size, SDU format information, SDU loss ratio, Residual bit error ratio, Delivery of erroneous SDUs, Transfer delay, Traffic handling priority, Allocation/Retention Priority)
- 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 X.25 Based Services for GPRS

This clause describes the use of X.25 based services over the ~~GPRS~~Packet Domain bearer. Two services are specified at the R reference point -

1) Character mode (specified in ITU-T X.3, X.28, X.29) with the triple X PAD in the MT.

2) Packet mode (specified in ITU-T X.25).

NOTE: In order to maintain consistency within UMTS/GSM specifications, the term TE is used when referring to what CCITT/ITU-T X.25 calls a DTE. Exceptionally, in text quoted from an ITU-T Recommendation, the term DTE is retained.

8.1 X.25 Character mode (triple X PAD) service

This mode is an asynchronous character based service allowing the application to set up a single connection using the CCITT/ITU-T X.28 / X.29 procedures. This supports both mobile originate and mobile terminate calls. The MT terminates the X.25 packet layer and provides a triple X PAD function.

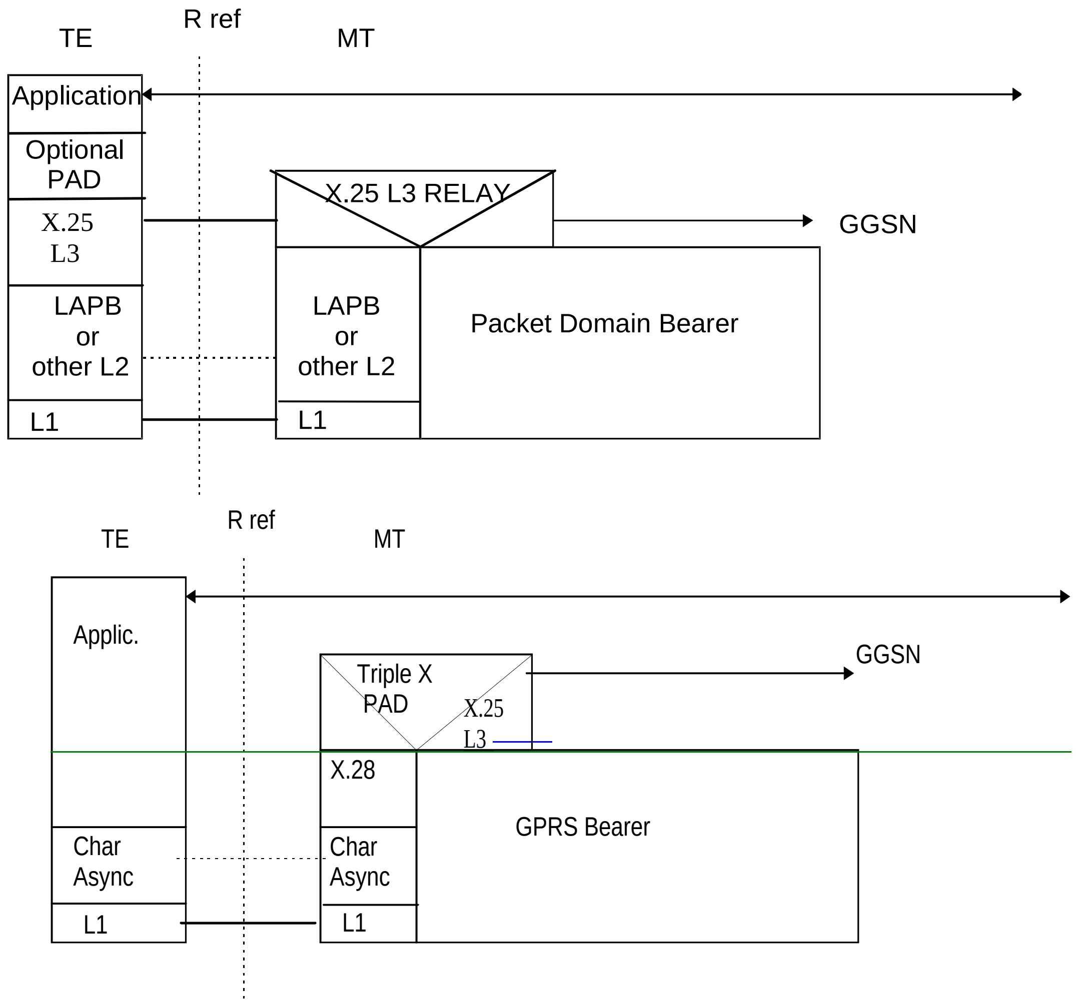


Figure 3: Character (Triple X PAD) mode

8.1.1 PAD Parameters

The following table lists the minimum set of X.3 parameters that shall be implemented. A full range is specified in the CCITT/ITU-T X series documents and those parameters not implemented shall be fixed to their defined defaults.

Table 1: Table of Minimum X.3 Parameters

Parameter Number	Description	Default Value	Valid Values	Value/Function
1	PAD Recall Character	1	0 1 32-36	(None) DLE Binary representation of decimal value
2	Echo	0	0 1	Off On
3	Data Forwarding Character	2	0 1 2 4 8 16 32 64	(on 128th data byte) A-Z, a-z, 0-9 CR ESC, BEL, ENQ, ACK DEL, CAN, DC2 ETX, EOT HT, LF, VT, FF All characters between NUL & US not listed above
4	Delay Timer	0	0 1-255	Disabled Period of TXD cct inactivity before data forwarded (1/20 of a second). The minimum time-out is 0.5s. Any value of parameter 4 between 1 & 10 will default to 0.5s.
5	Flow Control from Pad (to DTE)	0	0 1	None XON/XOFF
6	Service Signals	5	0 1 5	Disabled Enabled, excluding prompt Enabled, including prompt
7	Action on Break	8	8	PAD escapes from data transfer state
11	Data Rate	13	2 3 4 6 12 13 14	300 bps 1200 bps 600 bps 150 bps 2400 bps 4800 bps 9600 bps Other values may be implemented as long as they conform to the CCITT/ITU-T specifications.
12	Flow Control to Pad (from DTE)	0	0 1	None XON/OFF
13	Line Feed insertion	0	0 1	None LF inserted after CR to DTE
15	Character Deletion	0	0 1	Disabled Enabled

Although not CCITT/ITU-T defined, to be able to specify either X.28 or X.29 modes a Parameter 0 can be used as follows.

For X.28 mode parameter 0 shall be set to 0.

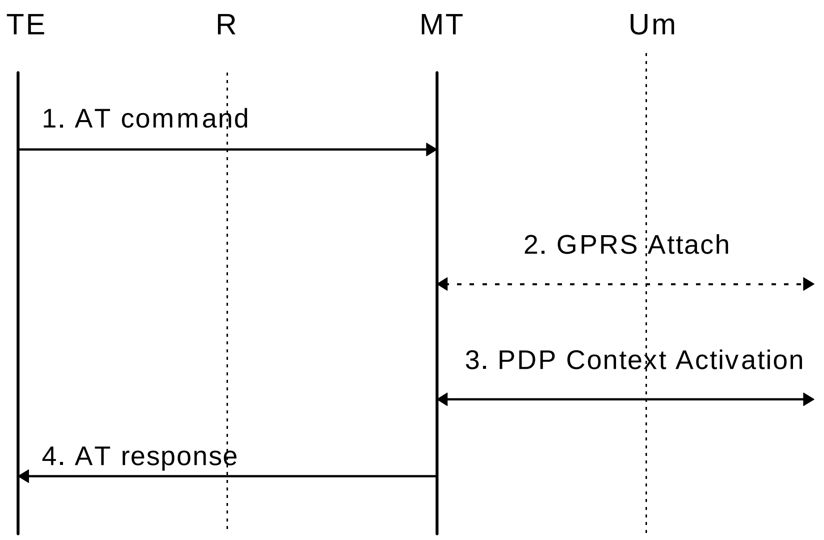
For the four X.29 variants available, each with a corresponding protocol identifier, the parameter value is set as listed below. The identifier octet is supplied with the call request packet when setting up a call.

Value	Description	Protocol Identifier Octet
2	CCITT use	00000001
3	National use	01xxxxxx
4	International User Bodies	10xxxxxx
5	DTE - DTE use	11xxxxxx

x - this digit may be represented by either a 1 or 0 (to be specified in ITU-T Recommendation X.244).

8.1.2 Example mapping of functions between the R reference point and the ~~GPRS~~Packet Domain bearer

The following example illustrates the case when the PAD functionality is used in the MT. In PAD mode only one PDP context can be activated per R reference point.



NOTE: The 2 ended arrows indicate an exchange of 0 or more messages.

Figure 4: PAD Service

1) The TE issues an AT command to activate PAD mode.

2) If the MS is not yet ~~G~~P~~R~~S attached, the MT performs the ~~G~~P~~R~~S Attach procedure as described in 3G TS 23.060~~GSM 03.60~~.

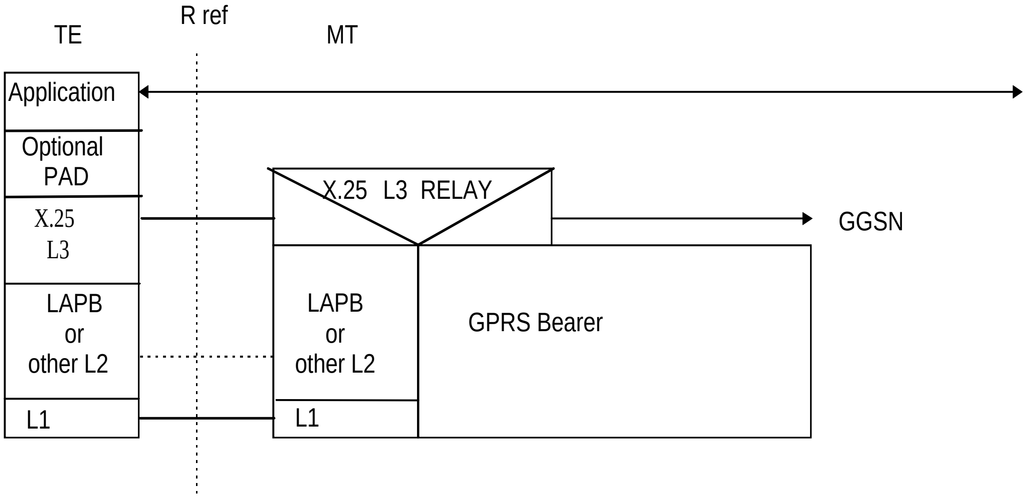
3) The MT performs the PDP Context Activation as described in 3G TS 23.060~~GSM 03.60~~.

4) The MT sends an AT response to the TE. Following a positive AT response the PAD prompt is issued.

8.2 X.25 Packet mode service

This mode offers a packet based service allowing the application to set up one or more virtual calls using the CCITT/ITU-T X.25 procedures. The maximum permitted number of concurrent virtual calls is implementation dependent. Both mobile originate and mobile terminate calls are supported. The MT performs a relay function for X.25 layer 3 which is terminated in the TE. The layer 2 protocol at the R reference point is terminated in the TE and the MT.

Depending on the application, the TE may or may not incorporate a triple X PAD function.



NOTE: The "other L2" could be ~~GSM~~ 3G TS ~~07.10~~27.010 or a manufacturer's defined layer 2

Figure 5: Packet mode

8.2.1 Layer 1 and Layer 2 options

This subclause describes standardized layers 1 and 2 which may be used for the TE-MT interface. As an alternative, the multiplexing protocol specified in ~~GSM~~ 3G TS ~~07.10~~27.010 or a manufacturer's defined layers 1 and 2 may be used providing they meet the requirements for carrying X.25 layer 3 frames over the R reference point.

8.2.1.1 Synchronous serial interface

For TEs with a synchronous serial port -

Layer 1 is synchronous X.21 or X.21bis (V.24/V.28).

Layer 2 is LAP B (X.25 L2) based on bit-oriented HDLC.

NOTE: Configuration of the MT in this case is outside the scope of this specification.

8.2.1.2 Asynchronous serial interface

For TEs with an asynchronous serial port -

Layer 1 is asynchronous V.24/V.28.

Layer 2 is LAP B (X.25 L2) based on character-oriented HDLC.

NOTE: The methods described in ITU-T Rec. V.80 may be applicable here.

8.2.1.3 Synchronous and asynchronous (dual mode) interface

For TEs with a serial port that can operate in both synchronous and asynchronous modes the following mechanism may be used where the interface supports AT commands. The interface starts in asynchronous mode and AT commands may be used to configure the MT. When configuration is complete, the interface switches to synchronous mode and X.25 starts up in the usual way. Setting Data Terminal Ready (circuit 108/2) to off is a protocol independent way of returning to asynchronous mode. Alternatively, the closing down of LAP B could be used as the signal.

8.2.2 Example mappings of functions between the R reference point and the ~~GPRS~~ Packet Domain bearer

The minimum requirement is that the MT shall be ~~G~~P~~R~~S-attached and the X.25 context activated whilst an X.25 virtual call is in progress. Any extension to this requirement depends on whether the MT implements any other ~~GPRS~~ Packet Domain-supported services (e.g. SMS) which might require that the MT remains ~~G~~P~~R~~S-attached even when there is no X.25 virtual call in progress.

The following subclauses describe only the X.25 requirements. These actions may be filtered by the requirements of any other ~~GPRS~~ Packet Domain-supported service. For example, if a ~~G~~P~~R~~S-only MT also supports SMS, a request for 'disconnection' of the X.25 service would result in a deactivation of the X.25 context but not a ~~G~~P~~R~~S-detach.

8.2.2.1 Standardized X.25 TE

This case applies to TEs which implement only the X.25 procedures, i.e. they have no support for AT commands. The layer 1 and 2 options described in subclause 8.2.1.1 and 8.2.1.2 apply.

Because of the different implementations of X.25 procedures in existing DTEs, attach/detach and activate/deactivate may need to be controlled at layer 1, 2 or 3 of the X.25 interface. Whilst it is always possible to use layer 3 control, this requires the most complete implementation of the X.25 protocol stack in the MT. Control at a lower layer may result in a simpler implementation. The procedures for connection and disconnection at all three layers are described in CCITT/ITU-T X.25.

In all cases it may be desirable to incorporate a timer to delay the deactivate/detach procedures in order to avoid excessive changes of the activation and attachment states in the course of a number of consecutive calls.

NOTE: The activation and deactivation of an X.25 context to carry packets over ~~GPRS~~the Packet Domain is analogous to setting up and clearing a switched ISDN B channel connection to carry them over an ISDN. The call control mapping procedures used in the ISDN case are described in detail in ITU-T X.31 clause 7.3 (layer 1) and appendix I (layers 2 and 3).

8.2.2.1.1 Layer 1 control

This applies to X.25 DTEs which disconnect at the physical layer when no virtual calls are in progress. The TE and MT signal to one another by using V.24 or X.21 control signals.

From TE -

Physical layer connect received by MT -> attach, activate

Physical layer disconnect received by MT -> deactivate, detach

From network -

If the X.25 context is not currently active, an attempt by the network to offer a mobile terminated X.25 virtual call will be signalled by the receipt at the MT of a Request PDP Context Activation message. The MT signals this to the TE by using V.24 or X.21 control signalling and, if successful, -> attach, activate.

A network request that the X.25 context should be deactivated or a failure of the radio link will result in the MT performing a physical layer disconnect.

8.2.2.1.2 Layer 2 control

This applies to X.25 DTEs which keep layer 1 active but disconnect at the data link layer when no virtual calls are in progress. The TE and MT signal to one another by starting and stopping the data link layer protocol.

From TE -

Data link layer set-up received by MT -> attach, activate

Data link layer disconnect received by MT -> deactivate, detach

From network -

If the X.25 context is not currently active, an attempt by the network to offer a mobile terminated X.25 virtual call will be signalled by the receipt at the MT of a Request PDP Context Activation message. The MT signals this to the TE by attempting to start the data link layer and, if successful, -> attach, activate.

A network request that the X.25 context should be deactivated or a failure of the radio link will result in the MT performing a data link layer disconnect.

8.2.2.1.3 Layer 3 control

This applies to X.25 DTEs which keep layers 1 and 2 active when no virtual calls are in progress.

From TE -

Call Request packet received by the MT -> attach, activate
(Action is taken only if there are no X.25 virtual calls already in progress)

Clear Confirmation packet received by the MT from the TE -> deactivate, detach
(Action is taken only if there are no more X.25 virtual calls in progress.)

From network -

If the X.25 context is not currently active, an attempt by the network to offer a mobile terminated X.25 virtual call will be signalled by the receipt at the MT of a Request PDP Context Activation message. Following activation by the MT, an X.25 Call Request packet will be received from the network.

Clear Confirmation packet received by the MT from the network -> deactivate, detach
(Action is taken only if there are no more X.25 virtual calls in progress.)

A network request that the X.25 context should be deactivated or a failure of the radio link will result in the MT clearing any outstanding X.25 virtual calls.

The above refer only to normal clearing situations. An actual implementation shall take into account exceptional conditions such as the receipt of a Clear Request packet from the TE but no acknowledging Clear Confirmation from the network.

8.2.2.2 X.25 TE with support for AT commands

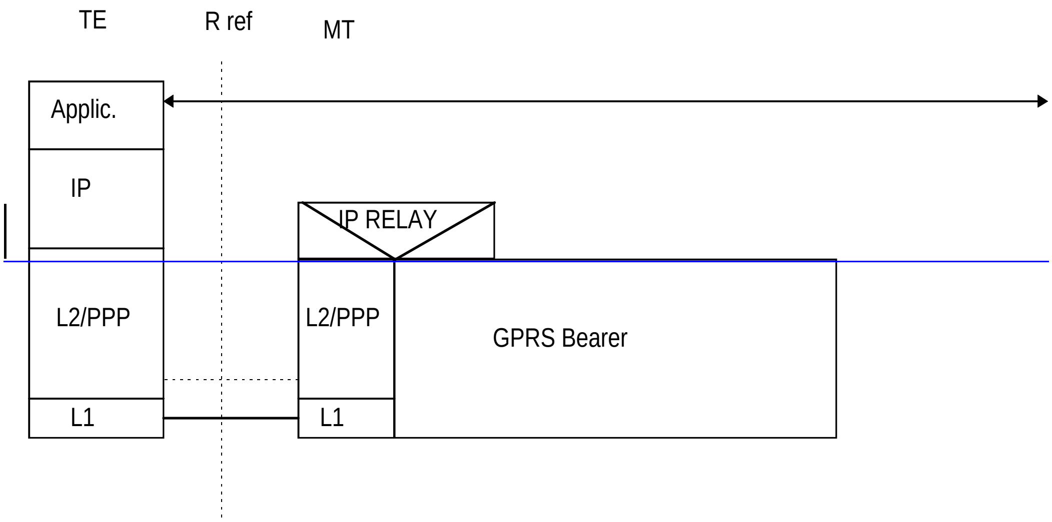
This case applies to TEs which implement AT commands in addition to supporting X.25 procedures. The layer 1 and 2 options described in subclauses 8.2.1.2 and 8.2.1.3 apply.

The TE sends ~~GPRS~~ Packet Domain AT commands to configure the MT, followed by a command to switch the interface into packet mode and start X.25. A mode of operation may be supported which provides compatibility with existing modem dial procedures.

9 IP Based Services

All protocols that are supported by the underlying IP protocol are applicable in the ~~GPRS~~ 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 following figure.



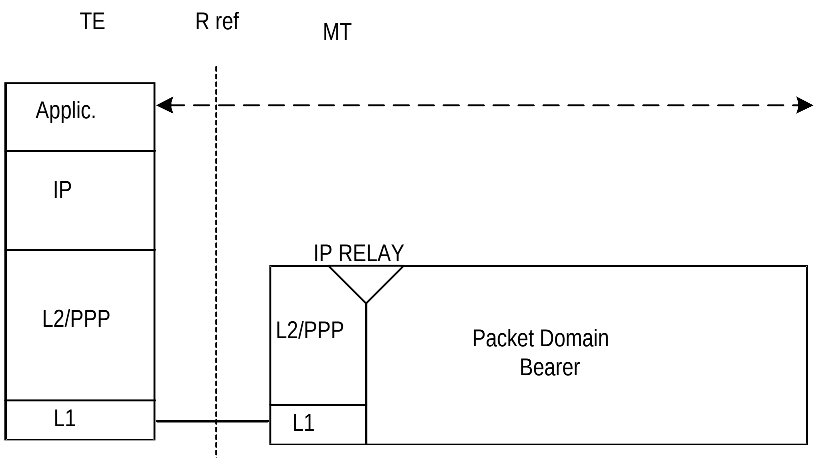


Figure 6: IP Based Services

PPP is a widely supported protocol in numerous operating systems and this alleviates the need for any ~~GPRS~~ 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, and RFC 1332. 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.

9.1 Example mapping of functions between the R reference point and the ~~GPRS~~ 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 interface) to support multiple virtual interfaces (communications ports) at the R reference point. Multiple PPP connections and IP contexts are possible in this case.

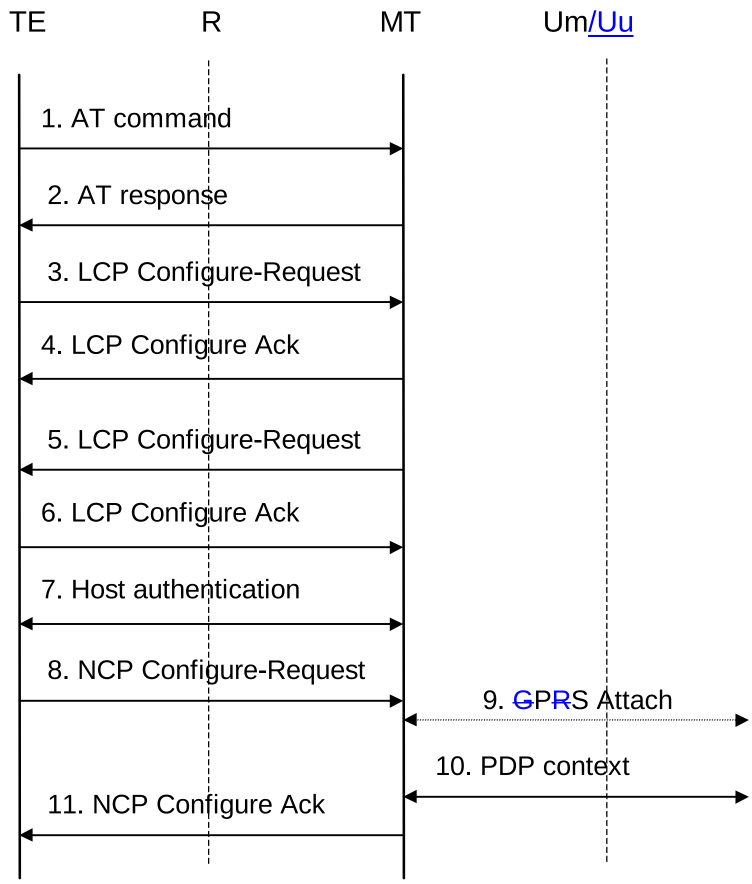


Figure 7: IP Over PPP Based Service

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 ~~GSM~~ 3G TS ~~0~~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 ~~G~~P~~R~~S attached, the MT performs the ~~G~~P~~R~~S Attach procedure as described in 3G TS 23.060~~GSM 03.60~~.

10) The MT performs a PDP Context Activation as described in 3G TS 23.060~~GSM 03.60~~. IP configuration parameters may be carried between the MT and the network in PDP Context Activation messages.

11) 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 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. 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.

10 PPP Based Services

By means of the PDP type 'PPP' ~~GPRS~~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 configuration is depicted in figure 8.

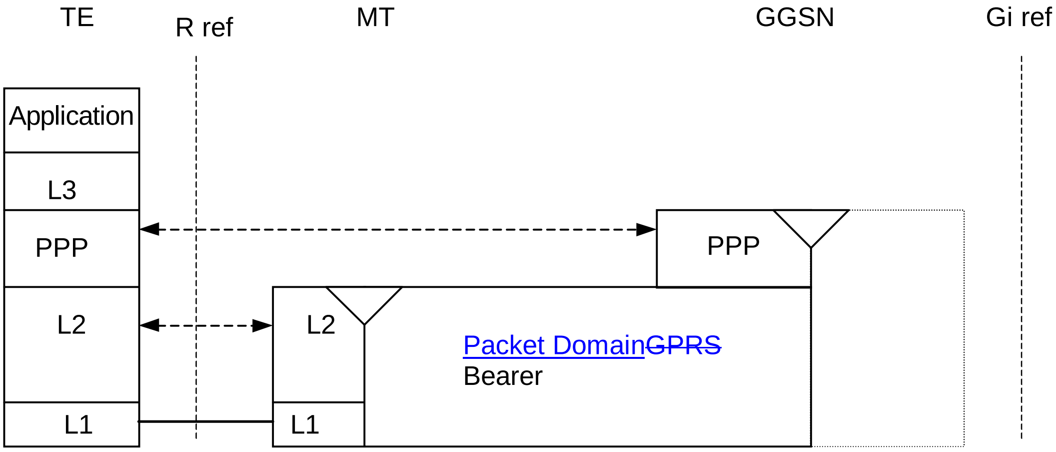


Figure 8: PPP Based Services

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 ~~GPRS~~ 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.

10.1 Example mapping of functions between the R reference point and the ~~GPRS~~ Packet Domain bearer

The following example illustrates the case when the PPP negotiation is carried out 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.

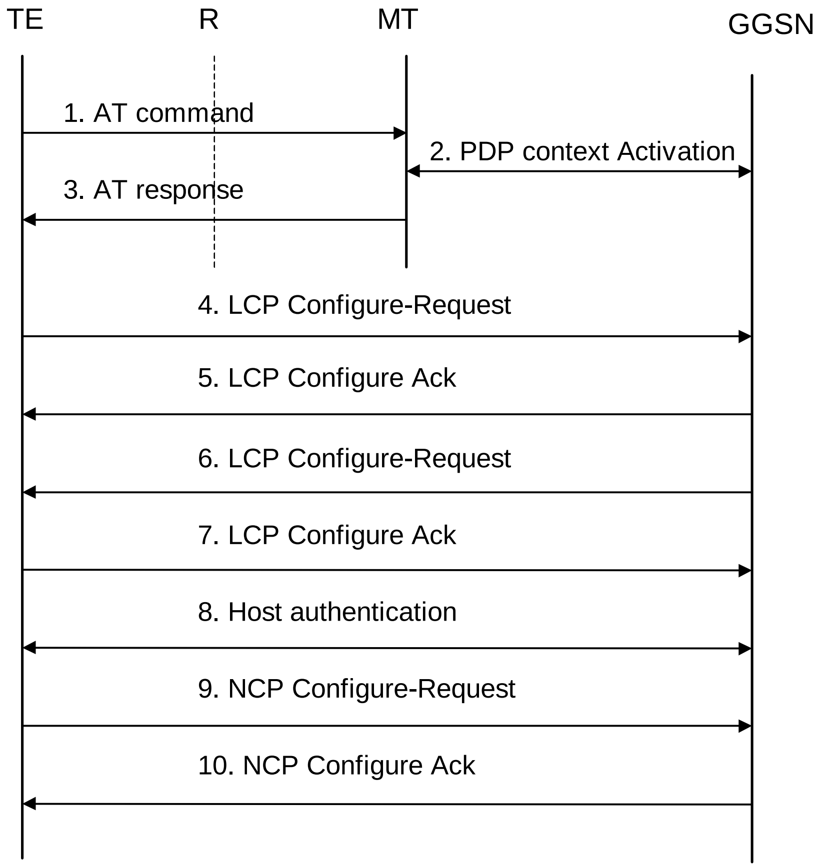


Figure 9: PPP Based Service

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~~GSM 03.60~~.

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~~ 3G TS ~~0~~29.061 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.

11 Internet Hosted Octet Stream Service (IHOSS)

11.1 Introduction

This section describes the MS aspects of the ~~GPRS~~ 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 ~~GPRS~~ 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 this specification contains the generic description of OSP. The features of OSP that are used by OSP:IHOSS are described later in this section.

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

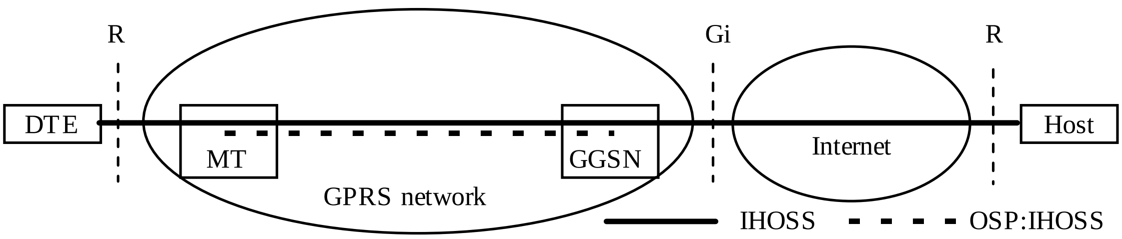


Figure 10: Scope of the Internet Hosted Octet Stream Service and Octet Stream Protocol

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.

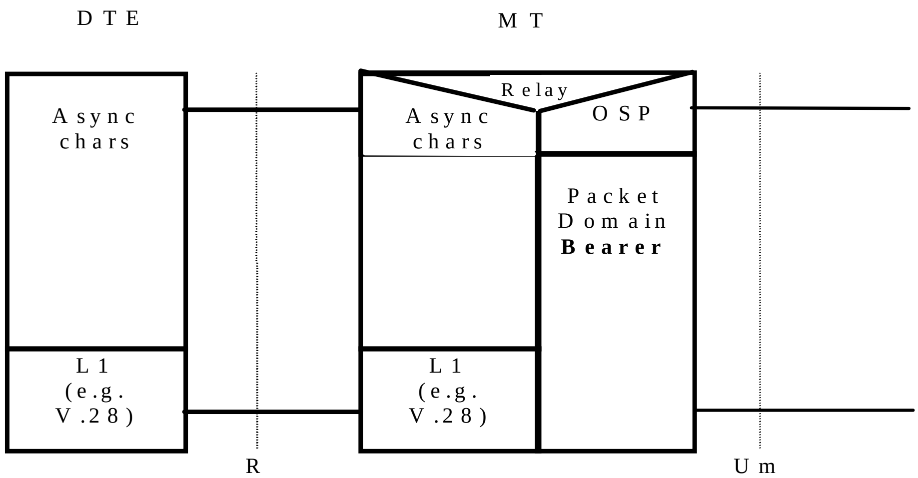


Figure 11: Example of protocol stacks for a~~n~~ MT with an asynchronous serial interface

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 ~~GPRS~~ 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~~GSM 03.60~~ using messages described in ~~GSM~~ 3G TS ~~0~~24.008 (MS-SGSN) and ~~GSM~~ 3G TS ~~0~~29.060 (SGSN-GGSN). Figure 12 illustrates the procedure when TCP is used over the Internet.

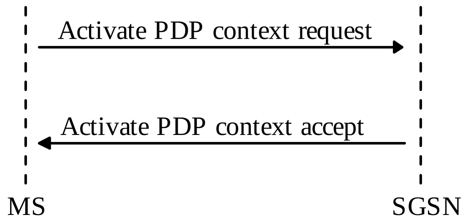


Figure 12: IHOSS connection establishment

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 section.

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 ~~GSM~~ 3G TS ~~0~~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

~~GSM~~ 3G TS ~~07.0~~27.007 defines commands that a TE may use to control a ~~GPRS~~ 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~~This~~ 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. ~~The use of a multiplexed interface, for example that specified in GSM 3G TS 07.1027.010, is not considered here.~~

It is anticipated that ~~GPRS~~ 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 ~~GPRS~~Packet Domain -specific AT commands is defined in ~~GSM~~ 3G TS ~~07.0~~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 ~~GSM~~ 3G TS ~~07.0~~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 ~~GPRS~~ 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 ~~GSM~~ 3G TS ~~07.0~~27.007.

Subclause 12~~0~~.2 contains examples of command sequences for a number of applications.

Annex A of this document lists the AT commands for the Packet Domain~~GPRS~~. They are fully defined in ~~GSM~~ 3G TS ~~07.0~~27.007,

12.1 General on AT commands

The following sections describe how the AT commands are used for the Packet Domain~~GPRS~~. The AT commands themselves are fully described in ~~GSM~~ 3G TS ~~07.0~~27.007. Reference to the particular AT command names are shown only for clarity. In all case refer to ~~GSM~~ 3G TS ~~07.0~~27.007 for the latest descriptions.

12.1.1 Interaction of AT commands, Packet Domain~~GPRS~~ management and PDPs

State machines may be used to describe the behaviour of -

AT commands (ITU-T V.250).

~~GPRS~~ PDP context management (3G TS 23.060~~GSM 03.60~~).

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 10.1.1.3.2).

12.1.1.3 ~~GPRS m~~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~~GPRS~~ network.

In order to provide flexibility and support a variety of types of ~~GPRS~~ 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 ~~G~~P~~R~~S 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~~GPRS~~ 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 this specification. Rules concerning what values shall be sent by the MT to the network under various circumstances are given in 3G TS 23.060~~03.60~~.

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~~03.60~~.

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~~03.60~~.

12.1.2.3 Access Point Name

This may be omitted:

according to the rules given in 3G TS 23.060~~03.60~~.

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.250 command state.

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

MT -> TE: OK

The TE sends a dial command requesting the Packet Switched service~~GPRS~~.

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 ~~G~~P~~R~~S-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 ~~G~~P~~R~~S-detach procedure if no other Packet Switched~~GPRS~~ 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 ~~GPRS~~-specific configuration commands, if required >

The TE sets automatic answering mode -

TE -> MT: ATS0=1

MT <- > network: MT performs the ~~G~~P~~R~~S-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 ~~GPRS~~-specific configuration commands, if required >

The TE sets manual answering mode and requests a ~~G~~P~~R~~S-attach (if necessary) -

TE -> MT: ATS0=0

TE -> MT: AT+CGATT=1

MT <- > network: MT performs the ~~G~~P~~R~~S-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

12.2.2 MO X.25 virtual call using a triple-X PAD in dial compatibility mode

This example shows how the `<called_address>` string may be used in the D command to make an X.25 call to a specified X.121 address.

The MT begins in V.250 command state.

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

MT -> TE: OK

The TE sends a dial command requesting the Packet Switched service~~GPRS~~ to X.121 address 1234567890.

TE -> MT: ATD*99*1234567890#

MT -> TE CONNECT

The MT enters V.250 online data state, performs a ~~G~~P~~R~~S attach if necessary and activates the X.25 context. It then automatically makes an X.25 call to the specified address, bypassing the PAD prompt. If the call is successful the MT responds with the PAD connect message -

1234567890 COM

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

This informative annex lists the AT commands for the Packet Domain~~GPRS~~ that are fully described in ~~GSM~~ 3G TS ~~07.0~~27.007.

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

Command	Description
+CGACT	PDP context activate or deactivate
+CGANS	Manual response to a network request for PDP context activation
+CGATT	~~G~~P~~R~~S attach or detach
+CGAUTO	Automatic response to a network request for PDP context activation
+CGCLASS	~~G~~P~~R~~S mobile station class
+CGCLOSP	Configure local Octet Stream PAD parameters
+CGCLPAD	Configure local triple-X PAD parameters
+CGDATA	Enter data state
+CGDCONT	Define PDP context
+CGEREP	Control unsolicited ~~G~~P~~R~~S event reporting
+CGPADDR	Show PDP address
+CGREG	Packet Domain~~GPRS~~ 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~~GPRS~~ Extensions to existing GSM AT commands

Command	Description
+CEER	Extended error report (refer to ~~07.0~~27.007)
+CMEE	Report mobile equipment error (refer to ~~07.0~~27.007)
+CR	Service reporting control (refer to ~~07.0~~27.007)
+CRC	Cellular result codes (refer to ~~07.0~~27.007)

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

Command	Description
A	Answer – manual acceptance of a network request for PDP context activation
D	Dial – request Packet Domain~~GPRS~~ 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~~GPRS~~ protocol model.

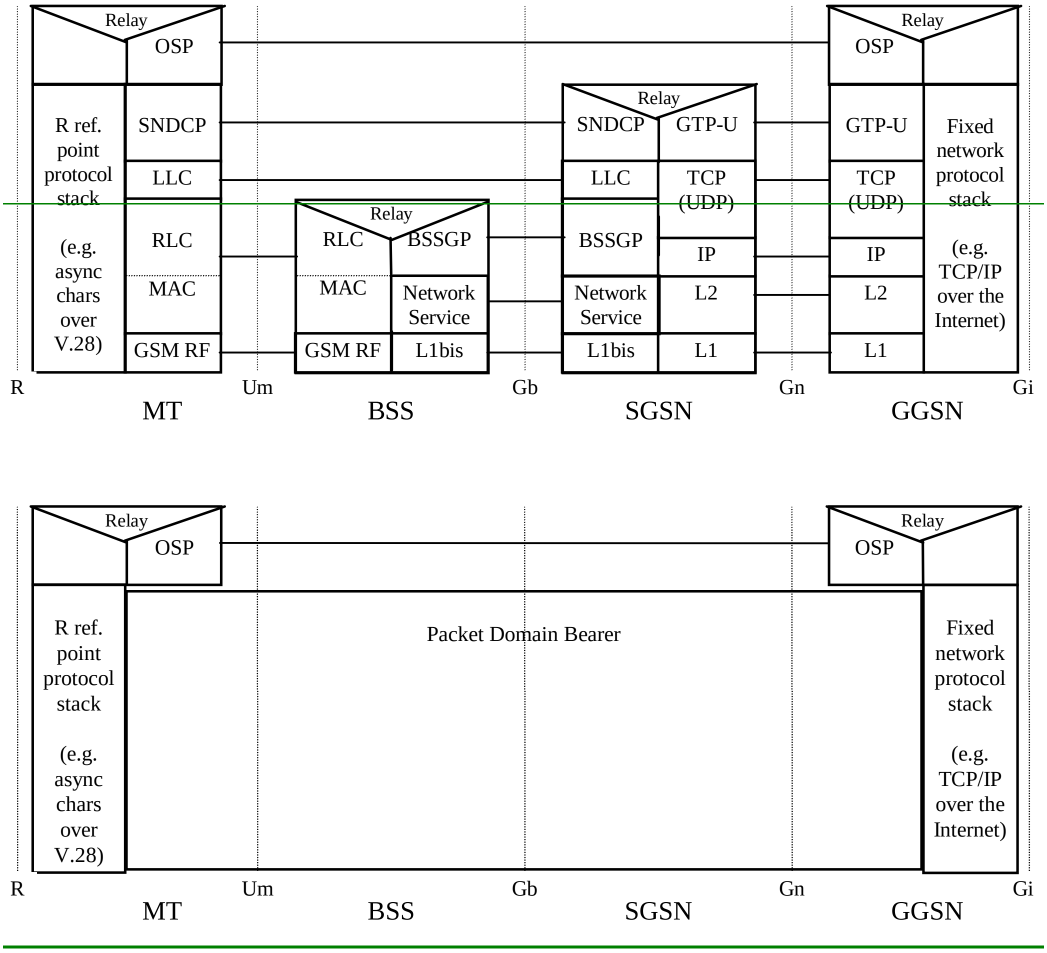


Figure B.1: Relationship of OSP to the rest of the packet domain~~GPRS~~ protocol architecture

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.

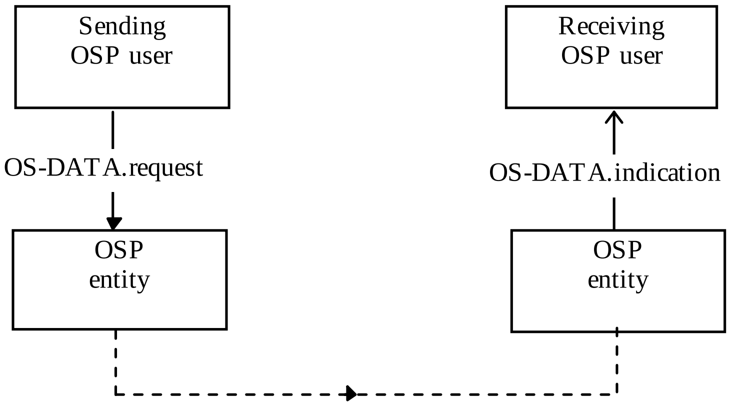


Figure B.2: An example of the use of the OS-DATA primitives

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 ~~GSM~~ 3G TS ~~0~~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	**Type**				**Parameters**
Name	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

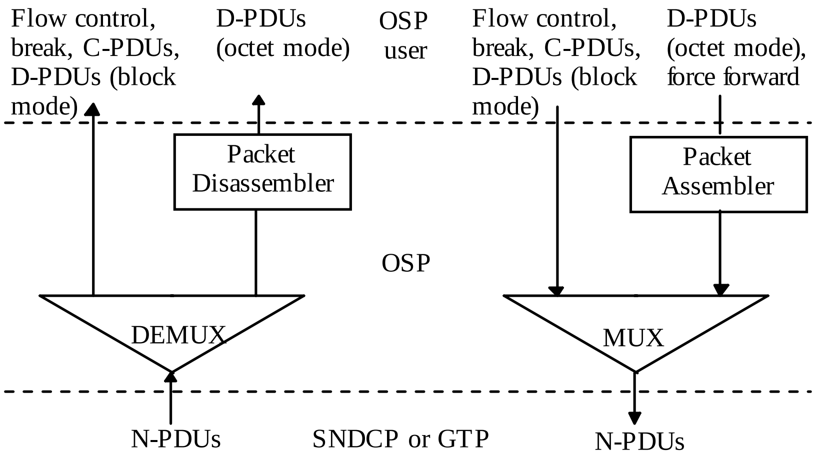


Figure B.3: OSP functional model

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 this specification 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 1-65535 octets.

The maximum size for the packet disassembly buffer is specified by PAD parameter 254. The value is in the range 1-65535 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 1/2 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 section.

~~The QoS provided by the underlying protocol layers is defined by the QoS profile assigned to the OSP context.~~

~~Precedence class - as required~~

~~Delay class - as required but should be consistent with the PAD forwarding strategy~~

~~Reliability class - class 1 for reliable service, class 3 for unreliable service~~

~~Peak throughput class - as required~~

~~Mean throughput class - as required~~

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 ~~GSM~~ 3G TS ~~0~~24~~.~~008. 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

Length 1

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 section describing the Packet Assembly/Disassembly function.

Annex C:
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

History

Document history		
V3.0.0	May 1999	Approved at TSGN #3. Under TSG TSG CN Change Control.
V3.1.0	August 1999	CRs 001, 002, 003, 004 Approved by E-mail after TSGN#4

3GPP TSG-CN WG3/SMG3 WPD Meeting #7
Sophia-Antipolis, France, 27 Nov-03 Dec 1999

Document N3-99468
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

27.060	**CR**	**009**	Current Version:	3.2.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	CN#6	for approval	X	strategic	(for SMG
list expected approval meeting # here ↑		for information		non-strategic	use only)

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from:* ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: *(at least one should be marked with an X)* (U)SIM		ME	X	UTRAN / Radio		Core Network	

Source:	TSG_N3	**Date:**	1999-11-29
Subject:	Parallel handling of multiple user application flows		
Work item:	GPRS		

Category:	F	Correction		**Release:** Phase 2	
	A	Corresponds to a correction in an earlier release		Release 96	
(only one category	B	Addition of feature	X	Release 97	
shall be marked	C	Functional modification of feature		Release 98	
with an X)	D	Editorial modification		Release 99	X
				Release 00	

Reason for change:	This CR introduces changes necessary due to the new feature of parallel handling of multiple user application flows.
Clauses affected:	2, 3.2, 5, 7.3.6, 9. New section 9.2.

Other specs affected:	Other 3G core specifications		→ List of CRs:
	Other GSM core specifications		→ List of CRs:
	MS test specifications		→ List of CRs:
	BSS test specifications		→ List of CRs:
	O&M specifications		→ List of CRs:

Other comments:	

<--------- double-click here for help and instructions on how to create a CR.

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.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.
- For this Release 1998 document, references to GSM documents are for Release 1998 versions (version 7.x.y).

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

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

3.2 Abbreviations

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

MCML Multi-Class Multi-Link PPP
MP Multilink PPP
TFT Traffic Flow Template

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;

7.3.6 PDP context related parameters

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

- Requested Quality of Service.
  (this includes the peak bit rate, the mean bit rate, the delay requirements, the service precedence, and the reliability level)
- Traffic Flow Template
- Data 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)

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 following figure.

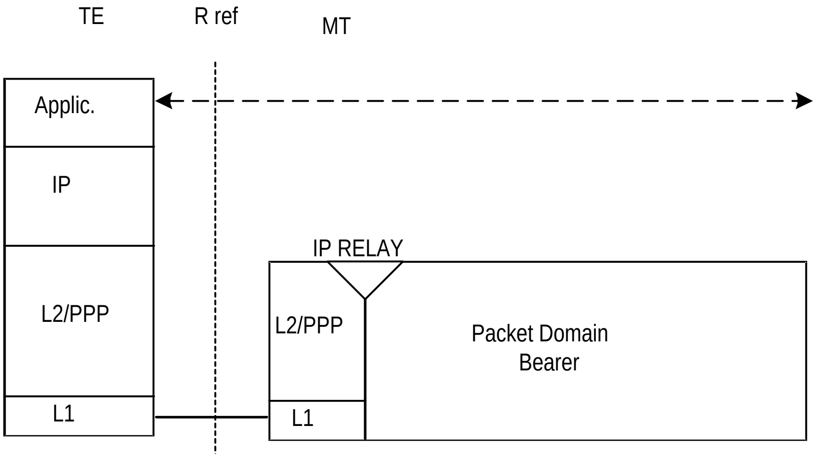


Figure 6: IP Based Services

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, and RFC 1332. 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.

9.2 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 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 section 9.1, it is not replicated in this section. The major difference is the additional negotiation capabilities used during the LCP configuration negotiation.

3GPP TSG-CN WG3/SMG3 WPD Meeting #7
Sophia-Antipolis, France, 29 Nov-03 Dec 1999

***Document* N3-99470**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

29.061	**CR**	**003**	Current Version:	3.1.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	CN#6	for approval	X	strategic		*(for SMG use only)*
list expected approval meeting # here ↑		For information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from:* ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: *(at least one should be marked with an X)*	(U)SIM		ME		UTRAN / Radio		Core Network	X

Source:	TSG_N3
Date:	1999-11-29
Subject:	Clarification on the PPP LCP negotiation for PDP type PPP.
Work item:	GPRS

Category:				**Release:**		
	F	Correction			Phase 2	
	A	Corresponds to a correction in an earlier release			Release 96	
(only one category	B	Addition of feature			Release 97	
shall be marked	C	Functional modification of feature			Release 98	
with an X)	D	Editorial modification	X		Release 99	X
					Release 00	

Reason for change:	During the R2#7 meeting a number of issues were brought up concerning PPP LCP negotiation for PDP type PPP. This CR clarifies some of these issues.
Clauses affected:	12.2.1.2

Other specs affected:				
	Other 3G core specifications		→ List of CRs:	
	Other GSM core specifications		→ List of CRs:	
	MS test specifications		→ List of CRs:	
	BSS test specifications		→ List of CRs:	
	O&M specifications		→ List of CRs:	

Other comments:	There is also a corresponding CR for 3G TS 27.060 v3.2.0.

help.doc

<--------- double-click here for help and instructions on how to create a CR.

12.2.1.2 Procedural description

In this case;

- the MS is given an address belonging to the Intranet/ISP addressing space. The address is given either at subscription in which case it is a static address or at PDP context activation in which case it is a dynamic address. This address is used for packet forwarding within the GGSN and for packet forwarding on the Intranet/ISP. This requires a link between the GGSN and an address allocation server, such as Radius, or DHCP, belonging to the Intranet/ISP;

- the communication between the GPRS PLMN and the Intranet/ISP may be performed over any network, even an insecure e.g. the Internet. In case of an insecure connection between the GGSN and the Intranet/ISP there may be a specific security protocol in between. This security protocol is defined by mutual agreement between GPRS PLMN operator and Intranet/ISP administrator.

The following description bullet items describe the signal flow.

1) The TE sends an AT-command to the MT to set up parameters.

2) The MT sends the Activate PDP context request message to the SGSN which sends the Create PDP context request message to the chosen GGSN.

3) The GGSN deduces from the APN:

   - the server(s) to be used for address allocation and authentication;

   - the protocol such as Radius, DHCP or L2TP to be used with this / those server(s);

   - the communication and security feature needed to dialogue with this / those server(s) e.g. tunnel ,IPSec security association, dial-up connection (using possibly PPP).

   As an example the GGSN may use one of the following options:

   - RADIUS for authentication and IP-address allocation.. The RADIUS server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN.

   - RADIUS for authentication and DHCP for host configuration and address allocation. The RADIUS server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN. After a successful authentication, the DHCP client discovers the DHCP server(s) in the ISP/Intranet and receives host configuration data.

   - L2TP for forwarding PPP frames to a L2TP Network Server.

4) The GGSN sends back to the SGSN a Create PDP Context Response message.

5) Depending on the cause value received in the Create PDP Context Response the SGSN may either send the Activate PDP Context Accept message or send the Activate PDP Context Reject message to the MS.

6) The MT responds with an AT-response that may indicate whether the context activation was successful or not. In the case of a non-successful context activation the response may also indicate the cause.

7) In case of a successful context activation, the TE will start its PPP protocol after the LLC link has been established. The LCP, Authentication and IPCP (in case of IP) negotiations are then carried out ~~end-to-end, or between the TE and the GGSN~~. During these negotiations the GGSN may acknowledge values, for any LCP options related to 'L2' framing (e.g. 'ACCM', 'ACFC' and 'FCS-Alternatives'), as proposed by the MT, which itself is forwarding these negotiations from the TE.

Note: With the <PDP Type>”PPP” the MT may provide a PPP relay (or proxy) function between the TE and GGSN. This gives the opportunity for the MT to intercept the ‘L2’ framing end to end negotiations.

3GPP TSG-CN WG3/SMG3 WPD Meeting #7
Sophia-Antipolis, France, 29 Nov-03 Dec 1999

Document N3-99482
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

29.061	**CR**	**004**	Current Version:	3.1.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑   *↑ CR number as allocated by MCC support team*

For submission to:	CN#6	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from:* ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [X]
(at least one should be marked with an X)

Source:	TSG_N3	**Date:**	1999-11-25
Subject:	Enhancement to the section on Numbering and Addressing to include the APN		
Work item:	GPRS		

Category:	F	Correction		**Release:**	Phase 2	
	A	Corresponds to a correction in an earlier release			Release 96	
(only one category shall be marked with an X)	B	Addition of feature			Release 97	
	C	Functional modification of feature	X		Release 98	
	D	Editorial modification			Release 99	X
					Release 00	

Reason for change:

This CR proposes an enhancement to the section on Numbering and Addressing, where a second scenario is added for interworking with private networks.

It explains that PDP Address can not be used alone to establish uniqueness during Context Activation collisions, but that the pair of values APN and PDP address can.

This is a clarification in line with proposed changes to specifications: 27.007, 29.060, 24.008, and 23.060. These changes add the functionality and message parameters required for correct behaviour during Context Activation collisions.

Clauses affected: 11.3

Other specs affected:	Other 3G core specifications		→ List of CRs:	
	Other GSM core specifications		→ List of CRs:	
	MS test specifications		→ List of CRs:	
	BSS test specifications		→ List of CRs:	
	O&M specifications		→ List of CRs:	

Other comments:

*** Modified Section ***

11.3 Numbering and Addressing

In the case of interworking with ~~the~~ public IP networks (such as the Internet), the GPRS operator shall use public network addresses. These public addresses can be reserved from the responsible IP numbering body, or from an ISP with which the GPRS operator has an agreement.

In the case of interworking with ~~the~~ private IP networks, two scenarios can be identified:

1. ~~t~~The GPRS operator manages internally the subnetwork addresses. Each private network is assigned a unique subnetwork address. Normal routing functions are used to route packets to the appropriate private network.

2. Each private network manages its own addressing. In general this will result in different private networks having overlapping address ranges. A logically separate connection (e.g. an IP in IP tunnel or layer 2 virtual circuit) is used between the GGSN and each private network. In this case the IP address alone is not necessarily unique. The pair of values, Access Point Name (APN) and IP address, is unique.

The GPRS operator allocates the IP addresses for the subscribers in either of the following ways.

- The GPRS operator allocates a static IP address when the subscription record is built. The IP address is reserved from a pool of free IP addresses. Each external network has its own pool of addresses.

- The GPRS operator allocates (either on its own or in conjunction with the external network ~~an ISP~~) a dynamic IP address when the MS performs the PDP Context Activation procedure with dynamic address allocation as described in ~~GSM 03.60~~3G TS 23.060.

***Document* N3-99466**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

29.061	**CR**	**005**	Current Version:	3.1.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	CN#6	for approval	X	strategic		*(for SMG use only)*
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from:* ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: *(at least one should be marked with an X)*	(U)SIM		ME	X	UTRAN / Radio		Core Network	X

Source:	TSG_N3	**Date:**	1999-11-29
Subject:	IPCP negotiation at the GGSN for non-transparent IP		
Work item:	GPRS		

Category:	F	Correction		**Release:**	Phase 2	
	A	Corresponds to a correction in an earlier release			Release 96	
(only one category	B	Addition of feature			Release 97	
shall be marked	C	Functional modification of feature			Release 98	
with an X)	D	Editorial modification	X		Release 99	X
					Release 00	

Reason for change:	During the activation of a PDP Context for non-transparent IP the GGSN may receive PPP IPCP Configure-Request packets, from the MS, contained in the Protocol Configuration Options IE. Depending on the options and/or the requested values for the options the GGSN may choose to either acknowledge or reject the options and/or their proposed values. It is not entirely clear in the current text how this should be done.
Clauses affected:	11.2.1.2

Other specs affected:	Other 3G core specifications		→ List of CRs:	
	Other GSM core specifications		→ List of CRs:	
	MS test specifications		→ List of CRs:	
	BSS test specifications		→ List of CRs:	
	O&M specifications		→ List of CRs:	

Other comments:	There is also a corresponding CR for 3G TS 27.060 v3.2.0.

help.doc

<--------- double-click here for help and instructions on how to create a CR.

11.2.1.2 Non Transparent access to an Intranet or ISP

In this case;

- the MS is given an address belonging to the Intranet/ISP addressing space. The address is given either at subscription in which case it is a static address or at PDP context activation in which case it is a dynamic address. This address is used for packet forwarding within the GGSN and for packet forwarding on the Intranet/ISP. This requires a link between the GGSN and an address allocation server, like Radius, DHCP, …, belonging to the Intranet/ISP;
- the MS shall send an authentication request at PDP context activation and the GGSN requests user authentication from a server, like Radius, DHCP, …, belonging to the Intranet/ISP;
- the protocol configuration options are retrieved (if requested by the MS at PDP context activation) from some server (Radius or DHCP, …) belonging to the Intranet/ISP;
- the communication between the GPRS PLMN and the Intranet/ISP may be performed over any network, even an insecure e.g. the Internet. In case of an insecure connection between the GGSN and the Intranet/ISP there may be a specific security protocol in between. This security protocol is defined by mutual agreement between GPRS PLMN operator and Intranet/ISP administrator.

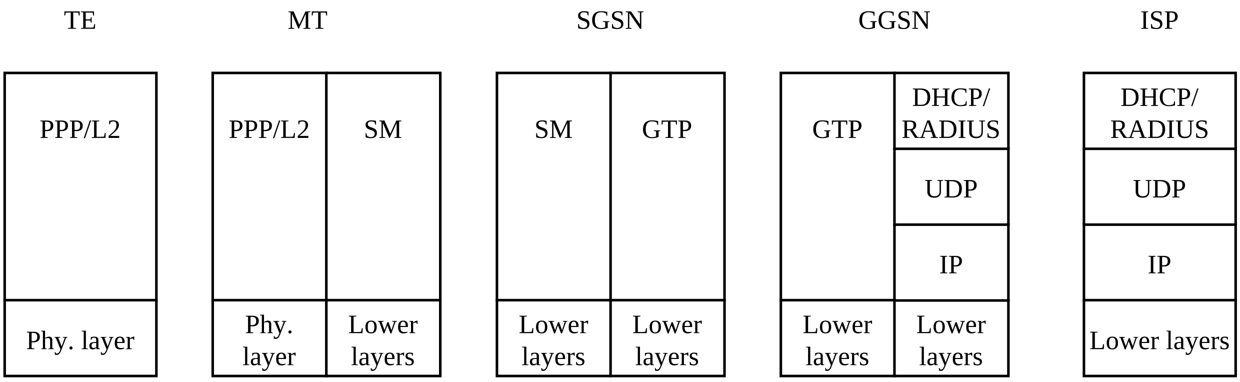


Figure 11: Signalling plane of non transparent case

The following description bullet items describe the signal flow.

1) The TE sends an AT-command to the MT to set up parameters and enter PPP mode. The MT responds with an AT-response.

2) LCP negotiates Maximum-Receive-Unit and authentication protocol. The negotiated authentication protocol is, either CHAP, PAP or ‘none’. The MT shall try to negotiate for CHAP as first priority.

3) 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 forced positive acknowledgement of the authentication to the TE.

4) The TE requests IP configuration by sending the IPCP Configure-Request message to the MT indicating either the static IP address that shall be used or that an IP-address shall be dynamically allocated.

5) The MT sends the Activate PDP context request message to the SGSN, including the Protocol Configuration Options. The SGSN sends the Create PDP context req message to the chosen GGSN including the unmodified Protocol Configuration Options.

6) The GGSN deduces from the APN :

    - the server(s) to be used for address allocation, authentication and protocol configuration options retrieval;
    - the protocol like Radius, DHCP, … to be used with this / those server(s);
    - the communication and security feature needed to dialogue with this / those server(s) e.g. tunnel ,IPSec security association, dial-up connection (using possibly PPP), ….

    As an example the GGSN may use one of the following options:

- RADIUS for authentication and IP-address allocation.. The RADIUS server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN.

- RADIUS for authentication and DHCP for host configuration and address allocation. The RADIUS server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN. After a successful authentication, the DHCP client discovers the DHCP server(s) in the ISP/Intranet and receives host configuration data. ~~.~~

If the received Protocol Configurations Options IE contains a PPP IPCP Configure-Request packet, the GGSN shall analyse all the contained IPCP options and their requested values. In accordance with the relevant PPP RFC[20] the GGSN shall respond with the following messages:

- Zero or one PPP IPCP Configure-Reject packet containing options not supported and options which values cannot be returned,

- zero or one PPP IPCP Configure-Nak packet containing options that are supported but has requested values that are incorrect/unsupported and

- zero or one PPP IPCP Configure-Ack packet containing options that are supported and has requested values that are correct/supported.

Any returned PPP IPCP packets shall be contained in the Protocol Configurations Options IE.

7) The GGSN sends back to the SGSN a Create PDP Context Response message, containing the Protocol Configuration Options IE. The cause value shall be set according to the outcome of the host -authentication and -configuration. A PDP context activation shall not be rejected solely due to the presence of unsupported or incorrect PPP IPCP options or option values, received from the MS in the Protocol Configurations Options IE. The MS may however later decide to immediately deactivate the activated PDP context due to the information received in the Protocol Configurations Options IE received from the network.

8) Depending on the cause value received in the Create PDP Context Response the SGSN sends either an Activate PDP Context Accept or an Activate PDP Context Reject, to the MS.

   If Protocol Configuration Options are received from the GGSN, the SGSN shall relay those to the MS. The MT sends either the configuration-ack packet (e.g. IPCP Configure Ack in PPP case), the configure-nack packet in case of dynamic address allocation (e.g. IPCP Configure Nack in PPP case), or a link Terminate request (LCP Terminate-Request in PPP case) back to the TE. In the case where a configure-nack packet was sent by the MT, a local negotiation may take place at the R reference point (i.e. the TE proposes the new value to the MT), after which a configuration-ack packet is sent to the TE.

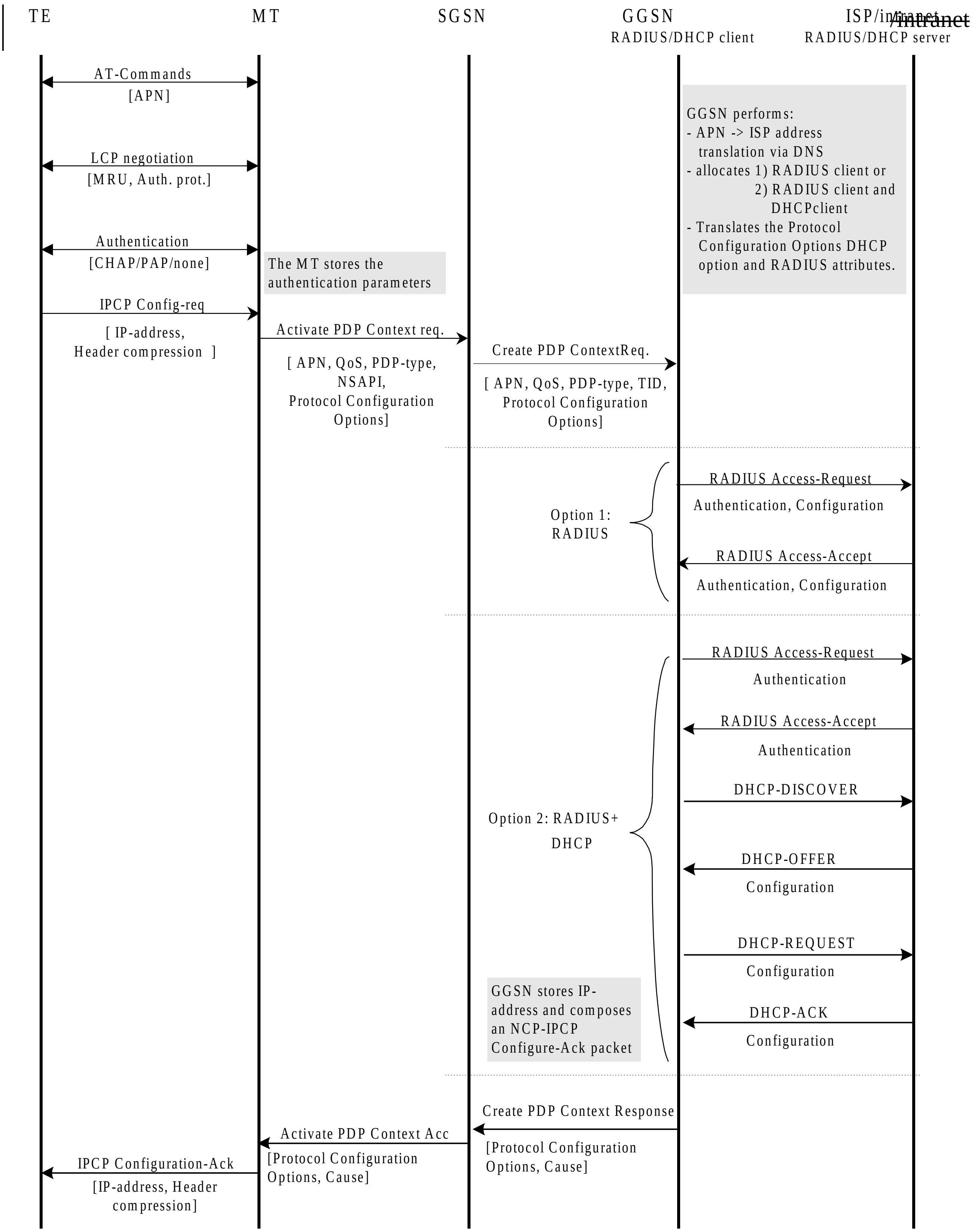
9) In case a configuration-ack packet was sent to the TE, the link from the TE to the external ISP/Intranet is established and IP packets may be exchanged.

   In case a link terminate request packet was sent to the TE, the TE and MT negotiates for link termination. The MT may then send a final AT-response to inform the TE about the rejected PDP Context activation.

A link terminate request packet (such as LCP Terminate-request in PPP case) causes a PDP context deactivation.

Example: In the following example PPP is used as layer 2 protocol over the R reference point.

The MT acts as a PPP server and translates Protocol Configuration Options into SM message IEs. GTP carries this information unchanged to the GGSN which uses the information e.g. for DHCP or RADIUS authentication and host configuration. The result of the host authentication and configuration is carried via GTP to the SGSN which relays the information to the MT. The MT sends an IPCP Configure-Ack to the TE with the appropriate options included.


TE
MT
SGSN
GGSN
RADIUS/DHCP client
ISP/intranet
RADIUS/DHCP server
AT-Commands
[APN]
LCP negotiation
[MRU, Auth. prot.]
Authentication
[CHAP/PAP/none]
The MT stores the authentication parameters
IPCP Config-req
[IP-address, Header compression]
Activate PDP Context req.
[APN, QoS, PDP-type, NSAPI, Protocol Configuration Options]
Create PDP ContextReq.
[APN, QoS, PDP-type, TID, Protocol Configuration Options]
GGSN performs:
- APN -> ISP address translation via DNS
- allocates 1) RADIUS client or
2) RADIUS client and DHCPclient
- Translates the Protocol Configuration Options DHCP option and RADIUS attributes.
Option 1: RADIUS
RADIUS Access-Request
Authentication, Configuration
RADIUS Access-Accept
Authentication, Configuration
Option 2: RADIUS+ DHCP
RADIUS Access-Request
Authentication
RADIUS Access-Accept
Authentication
DHCP-DISCOVER
DHCP-OFFER
Configuration
DHCP-REQUEST
Configuration
DHCP-ACK
Configuration
GGSN stores IP-address and composes an NCP-IPCP Configure-Ack packet
Create PDP Context Response
[Protocol Configuration Options, Cause]
Activate PDP Context Acc
[Protocol Configuration Options, Cause]
IPCP Configuration-Ack
[IP-address, Header compression]

3GPP TSG-CN WG3/SMG3 WPD Meeting #7
Sophia-Antipolis, France, 29 Nov-03 Dec 1999

***Document* N3-99499**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

29.061	**CR**	**008**		Current Version:	3.1.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	CN#6	for approval	X	strategic		*(for SMG use only)*
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)*	(U)SIM		ME		UTRAN / Radio		Core Network	X

Source:	TSG_CN3 PS	**Date:**	1999-11-29
Subject:	Alignment to 23.060 v3.1.0 Draft 3		
Work item:	GPRS		

Category:	F	Correction		**Release:**	Phase 2	
	A	Corresponds to a correction in an earlier release			Release 96	
(only one category	B	Addition of feature			Release 97	
shall be marked	C	Functional modification of feature			Release 98	
with an X)	D	Editorial modification	X		Release 99	X
					Release 00	

Reason for change:	The 23.060 is in the process of being updated to describe the R'99 of the GPRS and UMTS Packet Domain. The 29.061 should undergo the same treatment.
Clauses affected:	ALL

Other specs affected:	Other 3G core specifications		→ List of CRs:	23.060
	Other GSM core specifications		→ List of CRs:	
	MS test specifications		→ List of CRs:	
	BSS test specifications		→ List of CRs:	
	O&M specifications		→ List of CRs:	

Other comments:	This CR relates to the agreed CRs on 23.060, which update the 23.060 to describe the R'99 of the GPRS and UMTS packet Domain.

help.doc

<--------- double-click here for help and instructions on how to create a CR.

3G TS 29.061 V3.2~~1~~.0 (1999-11~~08~~

Technical Specificati

3rd Generation Partnership Project;
Technical Specification Group Core Network;
Packet Domain~~General Packet Radio Service (GPRS)~~;
Interworking between the Public Land Mobile Network (PLMN)
supporting Packet Based Services~~GPRS~~ and Packet Data Networks (PDN)
(3G TS 29.061 version 3.2~~1~~.0)

Reference

DTS/TSGN-0329061U

Keywords

3GPP, CN

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

–

Contents

Foreword

This Technical Specification has been produced by the 3GPP.

This TS describes the network interworking for the Packet Domain~~GSM service General Packet Radio Service (GPRS)~~. Interworking to various external networks is defined together with the interworking for data forwarding while subscribers roam within the 3GPP system.

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 this TS, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version 3.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 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 specification;

1 Scope

The~~e present~~is document defines the requirements for Packet Domain~~General Packet Radio Service (GPRS)~~ interworking between a:

a) PLMN and PSDN

b) PLMN and IP Networks

c) PLMN and PLMN

In addition, annex X describes the special requirements for interworking between a PCS1900 PLMN and a PSDN within a BOC's LATA.

2 ~~2~~ References

rapporteur comment – to be cleaned up)

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.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.
- ~~For this Release 1998 document, references to GSM documents are for Release 1998 versions (version 7.x.y).~~

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

[2] 3G TS ~~GSM 0~~22.060: "Digital cellular telecommunication system (Phase 2+); General Packet Radio Service (GPRS): Stage 1 Service Description".

[3] 3G TS ~~GSM 0~~23.060: "Digital cellular telecommunication system (Phase 2+); General Packet Radio Service (GPRS); Stage 2 Service Description ".

[4] GSM 03.61: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Point to Multipoint Multicast Service Description; Stage 2".

[5] GSM 03.62: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Point to Multipoint Group Call Service Description; Stage 2".

[6] GSM 03.64: "Digital cellular telecommunications system (Phase 2+);General Packet Radio Service (GPRS); Overall description of the Radio interface; Stage 2".

[7] 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".

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

[9] GSM 04.65: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Subnetwork Dependent Convergence Protocol (SNDCP)".

[10] 3G TS ~~GSM 0~~27.060: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Mobile Station (MS) supporting GPRS".

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

[12] CCITT Recommendation X.25: "Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit".

[13] CCITT Recommendation X.75: "Packet-switched signalling system between public networks providing data transmission services".

[14] CCITT Recommendation X.121: "International Numbering Plan for Public Data Networks".

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

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

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

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

[19] IETF RFC 1034 (1987): "Domain Names – Concepts and Facilities" (STD 7).

[20] Bellcore GR-000301 Issue 2 December 1997; "Public Packet Switched Network Generic Requirements (PPSNGR)".

[21] IETF RFC 1661 and 1662 (1994): "The Point-to-Point Protocol (PPP)" (STD 51).

[22] IETF RFC 1700 (1994): "Assigned Numbers" (STD 2).3

[23] UMTS 24.008: "Mobile radio interface layer 3 specification; Core Network Protocols – Stage 3".

[24] UMTS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface".

3 Definitions, abbreviations and Symbols

3.1 ~~3.1~~ Definitions

~~See GSM 02.60.~~
~~In GSM 02.02 the bearer services are described. The general network configuration is described in GSM 03.02 and the GSM PLMN access reference configuration is defined in GSM 04.02. The various connection types used in the GSM PLMN are presented in GSM 03.10. Terminology used in this Specification is presented in GSM 01.04. For support of data services between GSM PLMN and other networks see GSM 09-series of Specifications.~~

Refer to UMTS 22.060 and UMTS 23.060.

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

3.2 Abbreviations

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

APN	Access Point Name
ATM	Asynchronous Transfer Mode
BG	Border Gateway
BOC	Bell Operating Company
CHAP	Challenge Handshake Authentication Protocol

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System~~Server~~
DNIC	Data Network Identification Code
DSE	Data Switch Exchange
GGSN	Gateway GPRS Support Node
GTP-U	GPRS Tunnelling Protocol for user plane
IC	Interexchange Carrier
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
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LATA	Local Access and Transport Area
LAPB	Link Access Protocol Balanced
LAC	L2TP Access Concentrator
LNS	L2TP Network Server
MS	Mobile Station
MT	Mobile Terminal
OSP	Octet Stream Protocol
OSP:IHOSS	Octet Stream Protocol for Internet Hosted Octet Stream Service
PAP	Password Authentication Protocol
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PDU	Protocol Data Unit
PHF	Packet Handler Function
PNIC	Pseudo Network Identification Code
PPP	Point-to-Point Protocol
PS	Packet Switched
PPSN	Public Packet Switched Network
PSDN	Packet Switched Data Network
PSPDN	Packet Switched Public Data Network
RADIUS	Remote Authentication Dial In User Service
SGSN	Serving GPRS Support Node
SMDS	Switched Multimegabit Data Service
TE	Terminal Equipment
TEID	Tunnel End-point Identifier
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

3.3 Symbols

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

Gb	Interface between an SGSN and a BSC.
Gi	Reference point between ~~GPRS~~ 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 ~~GPRS~~ Packet Domain network services across areas served by the co-operating ~~GPRS~~ PLMNs.
Gs	Interface between an SGSN and MSC.
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 GPRS fixed network part. The Um interface is the GPRS network interface for providing packet data services over the radio to the MS. The MT part of the MS is used to access the GPRS 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 Network characteristics

4.1 Key characteristics of PLMN

The ~~GSM~~ PLMN is fully defined in the UMTS~~GSM~~ technical specifications. The Packet Domain~~GPRS~~ related key characteristics are found in ~~GSM~~3G TS 22.060~~02.60~~ and 3G TS 23.060~~03.60~~.

4.2 Key characteristics of PSDN

Packet Switched Data Networks (PSDNs) are defined in the relevant CCITT/ITU-T X series.

4.3 Key characteristics of IP Networks

The Internet is a conglomeration of networks utilising a common set of protocols. IP protocols are defined in the relevant IETF STD specifications and RFCs. The networks topologies may be based on LANs (e.g. ethernet), Point to Point leased lines, PSTN, ISDN, X.25 or WANs using switched technology (e.g. SMDS, ATM).

5 Interworking Classifications

5.1 Service Interworking

Service interworking is required when the Teleservice at the calling and called terminals are different. For Packet Domain~~GPRS~~, service interworking is not applicable at the Gi reference point.

5.2 Network Interworking

Network interworking is required whenever a PLMN is involved in communications with another network to provide end-to-end communications. The PLMN shall interconnect in a manner consistent with that of a normal Packet Data Network (type defined by the requirements e.g. IP, PSDN X.75). Interworking appears exactly like that of Packet Data Networks.

5.3 Numbering and Addressing

See 3G TS~~GSM~~ ~~0~~23.003 and the relevant sections for X.25 and IP addressing below.

6 Access reference configuration

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

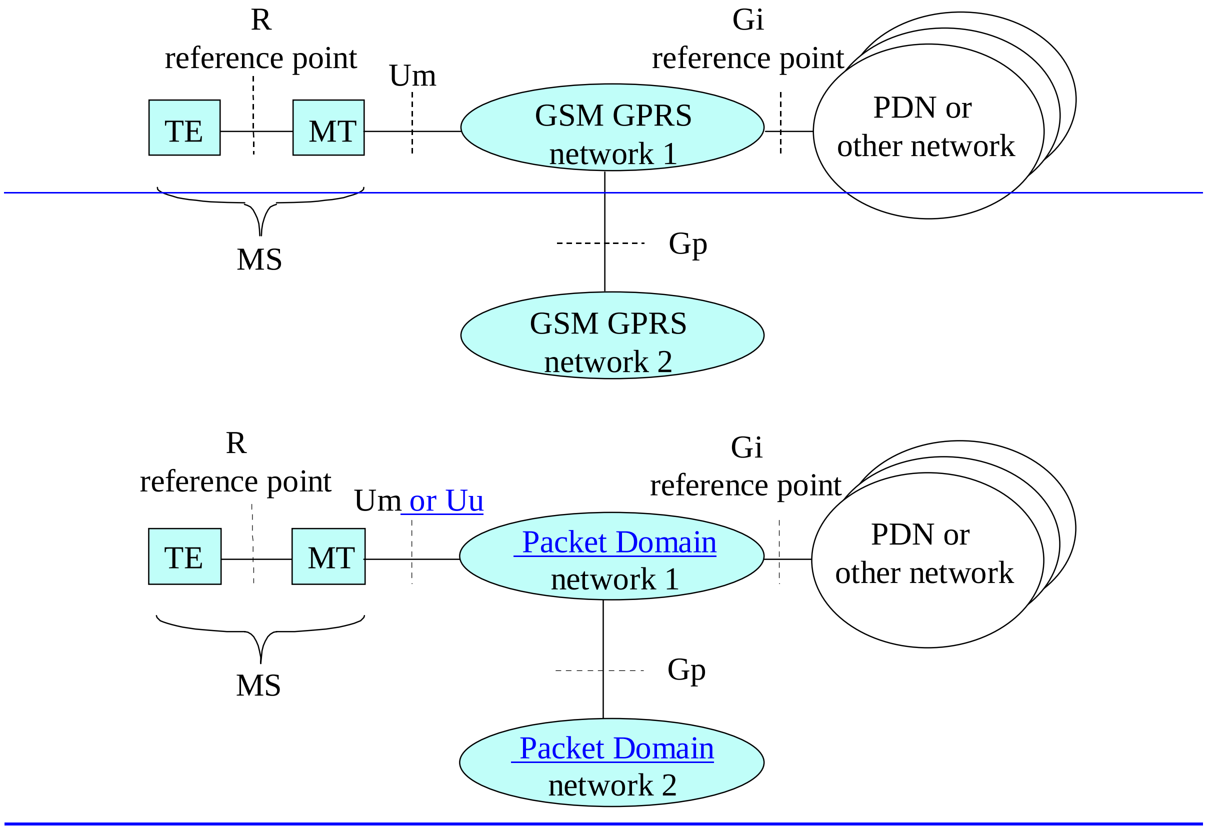
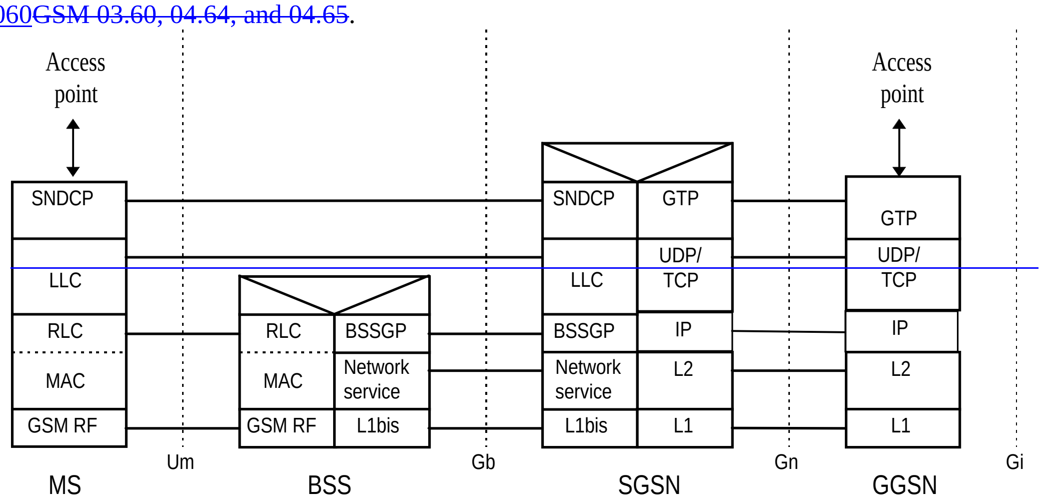


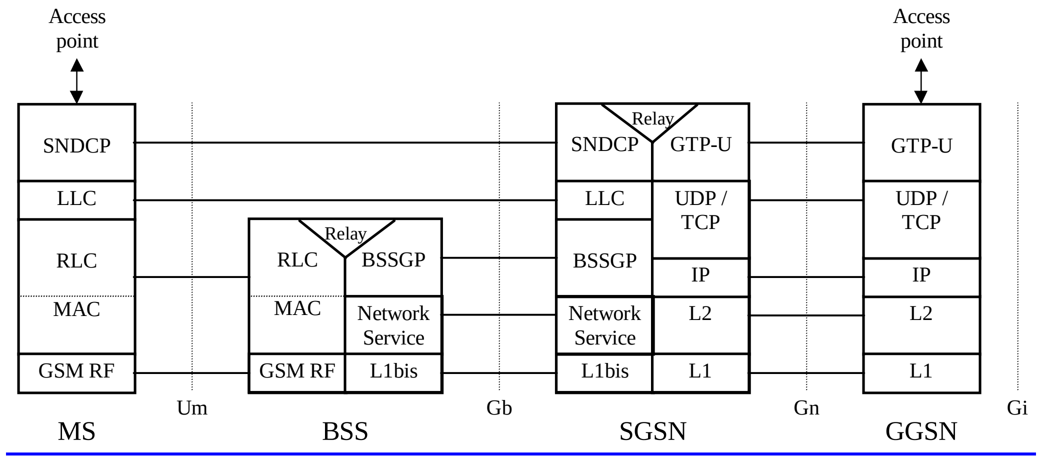
Figure 1: Packet Domain~~GPRS~~ Access Interfaces and Reference Points

7 ~~7~~ Interface to Packet Domain Bearer~~GPRS Bearer~~ Services

7.1 GPRS

The following Figure 2~~: Transmission Plane~~ shows the relationship of the GPRS Bearer terminating at the SNDCP layer to the rest of the GPRS environment. It is shown for reference purposes only and detailed information can be found in 3G TS 23.060~~GSM 03.60, 04.64, and 04.65~~.





NOTE: In the SGSN and GGSN UDP is mandatory. TCP is optional but recommended for X.25 services.

Figure 2: GPRS Transmission Plane

7.2 UMTS

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

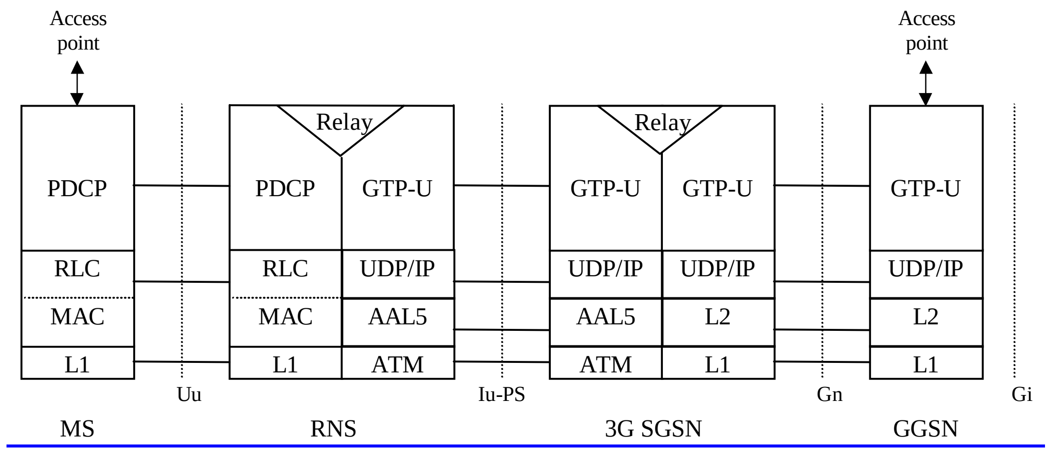


Figure X: UMTS User Plane

8 Subscription checking

Subscription is checked during the ~~GPRS~~PS Attach procedure and also during the PDP Context Activation procedure as described in 3G TS 23.060~~GSM 03.60~~. The GGSN implicitly checks its internal context related to the destination address for each mobile terminated packet. If there is a context associated with the PDP address the packet shall be forwarded to the MS, otherwise the packet shall be discarded or rejected depending on the implemented protocol.

9 Message Screening

Screening function~~'~~s reside within the Packet Domain~~GPRS network and has three levels~~ as described in 3G TS 22.060~~GSM 02.60~~ and 3G TS 23.060~~03.60~~. Screening may be applicable for only certain protocols. Screening is outside the scope of this specification~~GPRS standardisation, however, the following types of screening shall be supported.~~ .

~~9.1 Network controlled screening~~

~~The PLMN administration and/or the GPRS service provider shall set basic screening functionality, if applicable, (e.g. firewall) to reduce the risk of fraud and misuse. This is to ensure the integrity of the network and to protect subscribers.~~

~~9.2 Subscription controlled screening~~

~~This will not be in GPRS phase 1.~~

~~9.3 User controlled screening~~

~~This will not be in GPRS phase 1.~~

10 Interworking with PSDN (X.75/X.25)

10.1 General

~~GPRS~~The Packet Domain shall support interworking with PSDN networks. The interworking may be either direct or through a transit network.
~~GPRS~~Packet Domain shall support both CCITT/ITU-T X.121 and CCITT/ITU-T E.164 addressing.
~~GPRS~~Packet Domain shall provide support for CCITT/ITU-T X.25 and CCITT/ITU-T X.75.
The ~~GPRS~~Packet Domain TE's shall have addresses provided , and controlled, by their ~~GPRS~~PLMN operator. The PSDN TE sends data to the ~~GPRS~~Packet Domain TE by use of that TE's ~~GPRS~~Packet Domain DNIC (Data Network Identification Code) or equivalent which uniquely identifies that ~~GPRS~~Packet Domain network worldwide.
The GGSN for interworking with PSDNs is the access point of the ~~GSM GPRS~~Packet Domain ~~data~~ network.
There are two models for PSDN interworking.

- X.75 over the Gi reference point.
- X.25 over the Gi reference point with the DCE located within the PSDN and the DTE located within the TE of the ~~GPRS~~ PLMN.

Both X.75 and X.25 access methods are supported when mobile users are resident on HPLMN or VPLMN. A roaming user may be allocated a dynamic address from the VPLMN.

10.2 PSDN Interworking Models

The two models of X.75 and X.25 represent the different scenarios for PSDN interworking with the ~~GPRS~~Packet Domain network.
The model differences lie in the interconnection protocol over the Gi reference point.

10.2.1 X.75 Interworking at the Gi Reference Point

Figure 3 represents the case where X.75 is used as the interworking protocol, as used between interconnect X.25 PSDNs currently. The ~~GPRS~~Packet Domain network will look like any other PSDN in all respects and uses X.75 addressing. Figure 4 shows the interconnecting protocol stacks to the ~~GPRS~~Packet Domain bearer. The ~~GPRS~~Packet Domain bearer is described in 3G TS ~~GSM 0~~27.060, which uses the protocols described in ~~GSM 0~~3G TS 23.060.

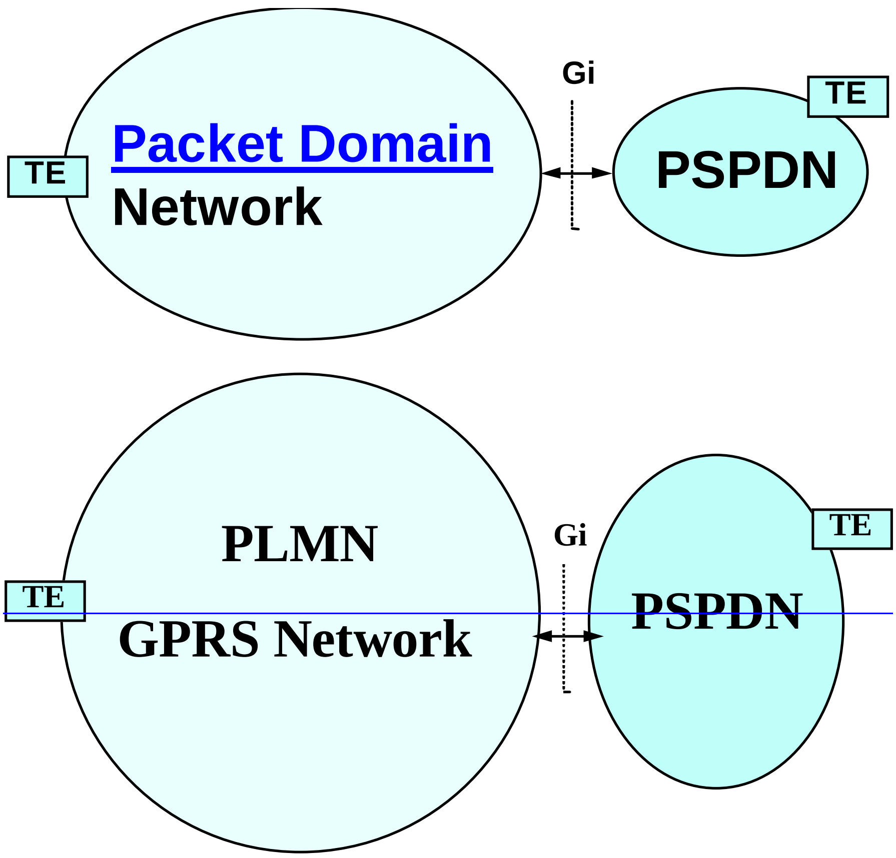
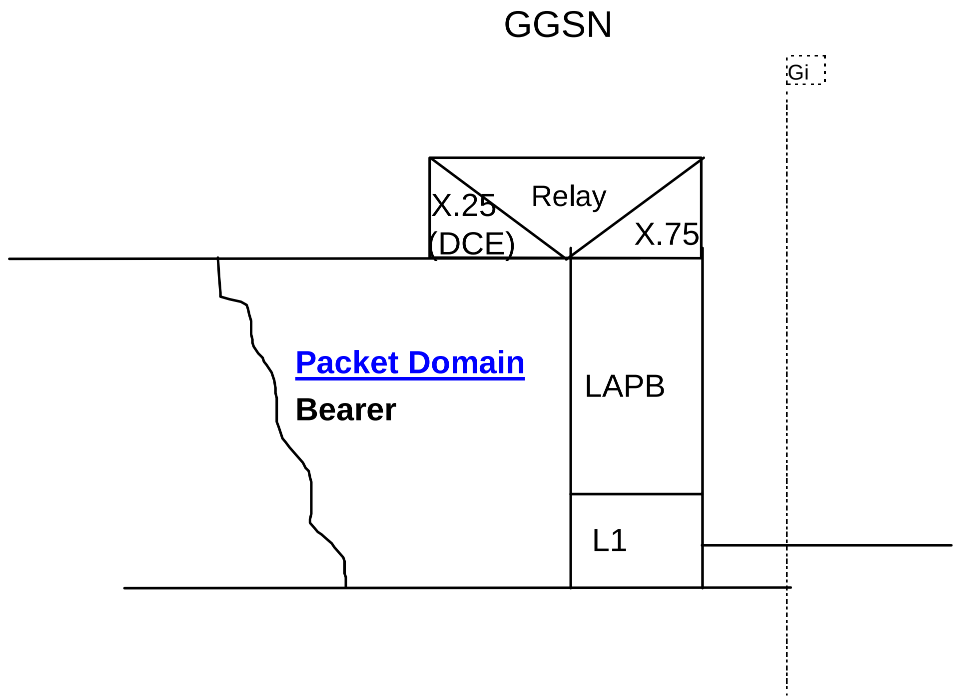


Figure 3: PSPDN Interworking with X.75 at Gi Reference Point



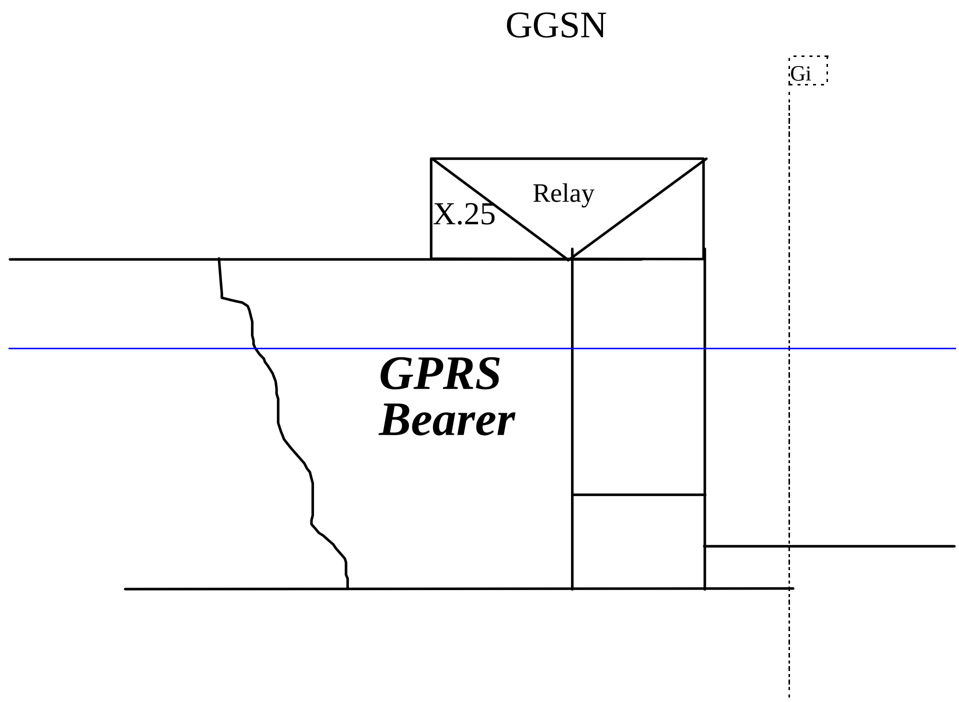


Figure 4: The Protocol Stack for the X.75 Gi Reference Point

10.2.1.1 Numbering and Addressing

A PLMN ~~GPRS network~~ interworking with PSPDN requires a DNIC or PNIC.
X.121 addresses allocated to subscribers belong to the PLMN operator.

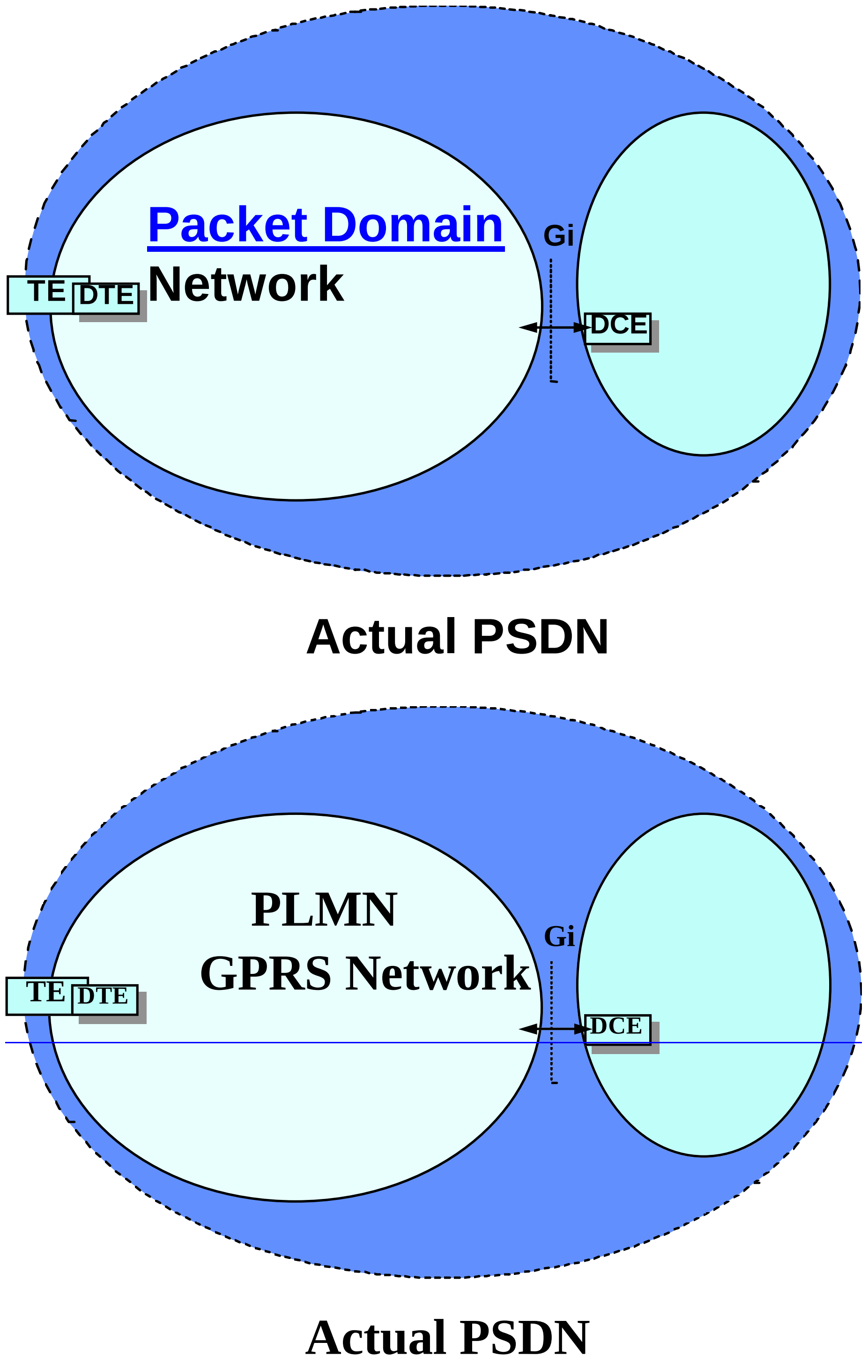
10.2.1.2 Charging

Charging of X.25 packets is done at the GGSN.

10.2.2 X.25 Interworking at the Gi Reference Point

Figure 5 represents the case where X.25 is used as the interconnect protocol between a DCE and a DTE. The DTE resides within the Packet Domain~~GPRS~~ network. The DCE resides within the PSDN.

The ~~GPRS~~ Packet Domain Network is seen as part of the PSDN, as the Gi reference point is the interconnect point between the DCE and the DTE.
The protocol stack for this model is shown in Figure 6.



NOTE: The PSDN can interwork at X.75 to other PSDN's

Figure 5: PSDN Interworking with X.25 over Gi Interface

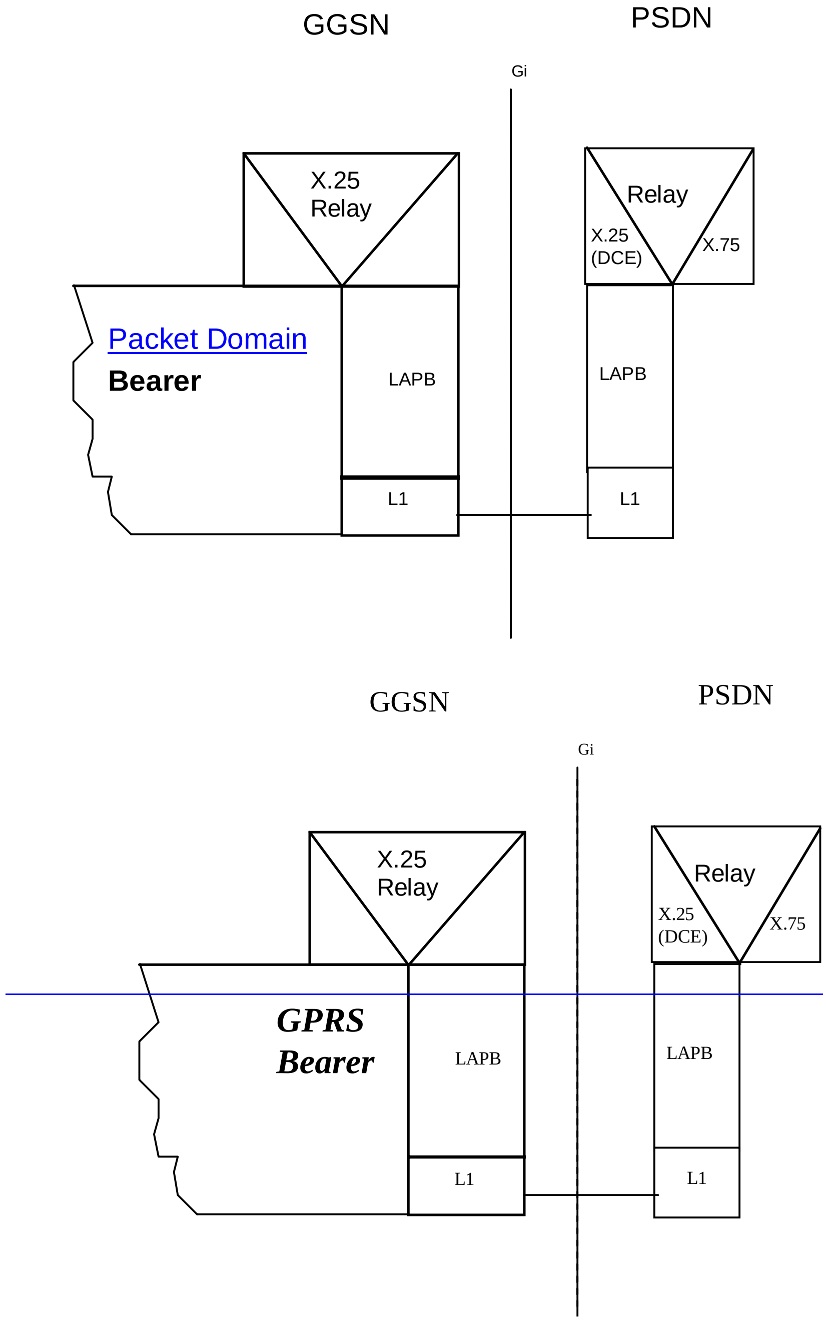


Figure 6: The Protocol Stack for the X.25 / Gi Reference point

Figure 6 shows the transmission plane only. In this case the GGSN shall resolve the association between the ~~MS GPRS~~Packet Domain bearer and the X.25 DCE. L1 is left to operators to determine connection to other networks. The X.25 Relay performs the following:

- mapping of logical channel numbers.

10.2.2.1 Numbering and Addressing

A fixed X.121 address for the MS maybe allocated by the PSDN operator, and is integral to the PSDN numbering plan. A dynamic X.121 address can also be used which is assigned by the Packet Domain ~~GPRS~~ network at PDP context activation.

10.2.2.2 Charging

The charging information may be collected in the X.25 network, depending upon the agreement between the ~~GPRS~~ PLMN operator and the PSDN operator. The charging may also be collected in the Packet Domain~~GPRS~~ network. If the

VPLMN assigns the dynamic address, the charging of the ~~GPRS~~ Packet Domain and the external network shall be gathered and sent to the HPLMN.

10.3 User Facilities

The set of user facilities as defined in CCITT/ITU-T X.25 may be supported.
As a minimum the following shall be supported:

- reverse charging;
- reverse charging acceptance;
- fast select restricted;
- fast select unrestricted;
- fast select acceptance.

10.4 The Packet Domain~~GPRS~~ Interworking to PSDN Characteristics

The following table describes the differences in addressing, and user profile for each interconnect type. The static X.121 address in the following table indicates an address which is permanently allocated to the ~~GPRS~~ subscriber by the network operator. The dynamic X.121 address is assigned automatically on the PDP Context Activation procedure. The dynamic address is allocated from a free pool held in the GGSN. This is described in GSM 03.60.

Table 1: PSPDN Packet Domain~~GPRS~~ Interconnection Characteristics

Metric	X.75 – Stand Alone PSPDN X.25 – PSPDN Sub Network	
	Static X.121 address	Dynamic X.121 address
X.25 profile	User determined in X.25 DCE	Only Default Profiles allowed in X.25 DCE- Selected upon PDP context activation
X.28/X.29 PAD	Address in GGSN	Address in GGSN after PDP Context Activation

11 Interworking with PDN (IP)

11.1 General

Packet Domain~~GPRS~~ shall support interworking with networks based on the Internet Protocol (IP). These interworked networks may be either intranets or the Internet.

11.2 PDN Interworking Model

When interworking with the IP networks, the Packet Domain~~GPRS~~ can operate IPv4 or Ipv6. The interworking point with IP networks is at the Gi reference point as shown in Figure 7.

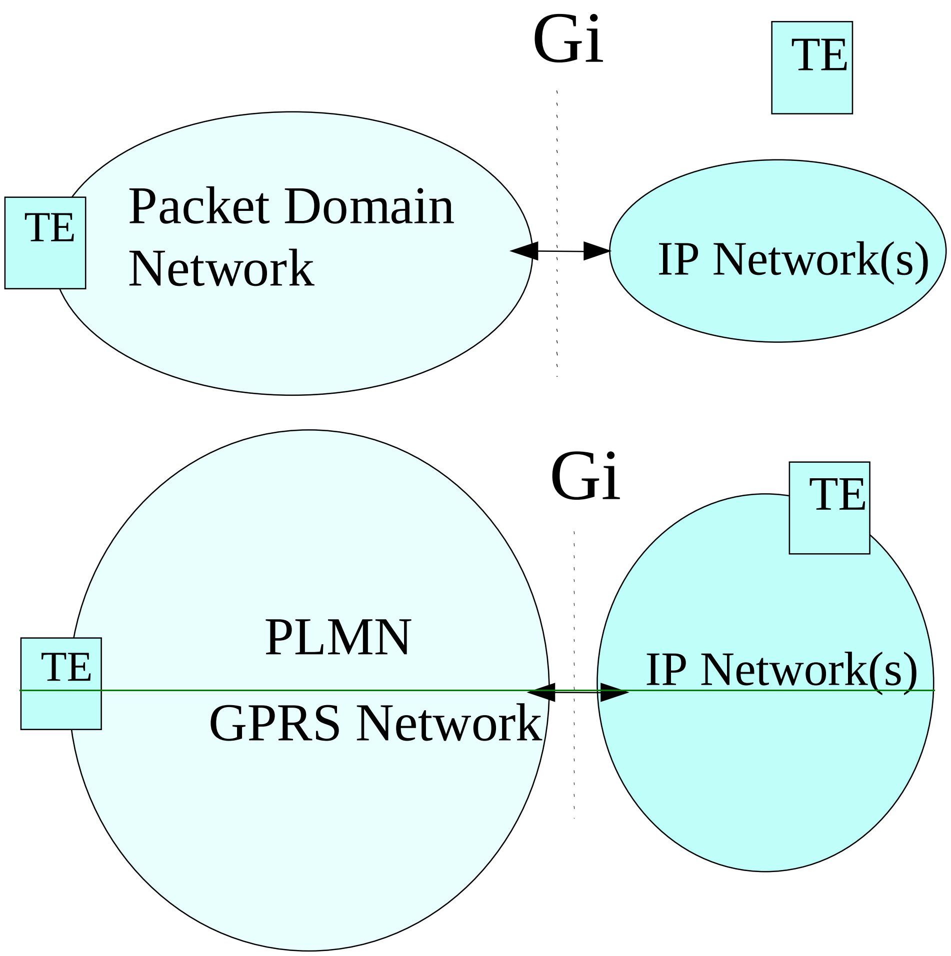
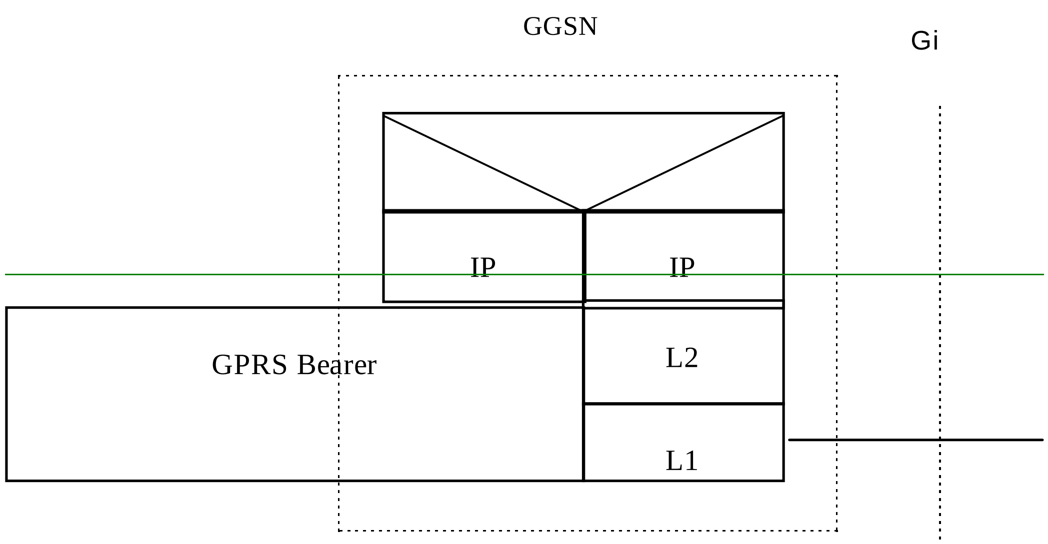


Figure 7: IP network interworking

The GGSN for interworking with the IP network is the access point of the Packet Domain~~GSM GPRS data network~~ (see Figure 8). In this case the ~~GPRS~~ Packet Domain network will look like any other IP network or subnetwork.



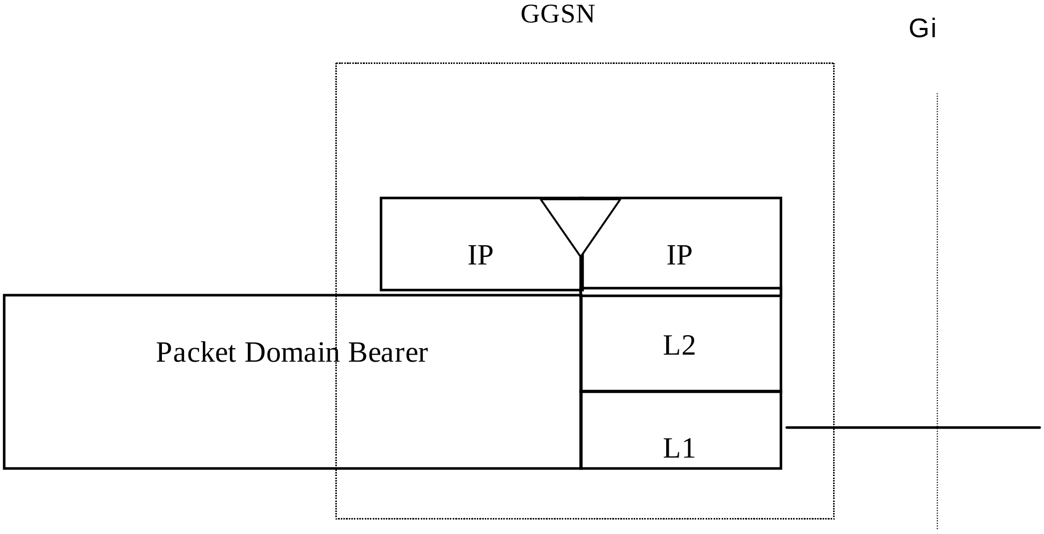


Figure 8: The protocol stacks for the IP / Gi~~GiIP~~ reference point

Typically in the IP networks, the interworking with subnetworks is done via IP routers. The Gi reference point is between the GGSN and the external IP network. From the external IP network's point of view, the GGSN is seen as a normal IP router. The L2 and L1 layers are operator specific.
It is out of the scope of this specification to standardise the router functions and the used protocols in the Gi reference point.
Interworking with user defined ISPs and private/public IP networks is subject to interconnect agreements between the network operators.
No user data or header compression is done in the GGSN.
~~The following working assumptions are valid in the generic case:~~

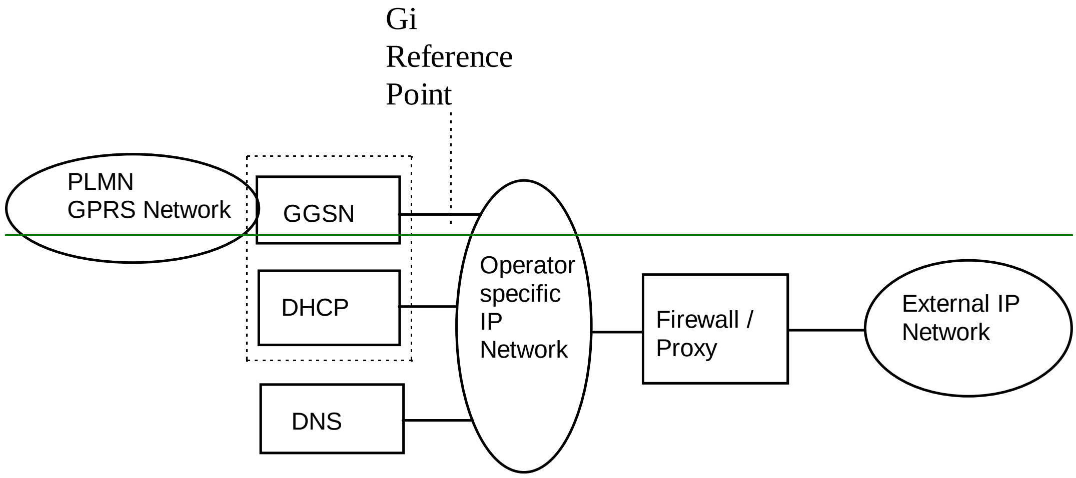
- ~~A firewall is configured by the GPRS operator. In general, all applications that are using IP as the underlying protocol are supported, but the GPRS operator may restrict their usage.~~
- ~~A Domain Name Server is managed by the GPRS operator. Alternatively, the Domain Name Server can be managed by the external IP network operator.~~
- ~~From the GPRS network's point of view, the allocation of a dynamic IP address is done by the GGSN as described in GSM 03.60. The GGSN may allocate these addresses by itself or use an external device such as an DHCP server. This external device may be operated by an external organisation such as an ISP or Intranet operator.~~

11.2.1 Access to Internet, Intranet or ISP through Packet Domain~~GPRS~~

The access to Internet, Intranet or ISP may involve specific functions such as : user authentication, user's authorization, end to end encryption between MS and Intranet/ISP, allocation of a dynamic address belonging to the PLMN/Intranet/ISP addressing space, etc.
For this purpose the Packet Domain~~GPRS PLMN~~ may offer:

- either direct transparent access to the Internet.
- or a non transparent access to the Intranet/ISP. In this case the Packet Domain~~GPRS PLMN~~, i.e. the GGSN, takes part in the functions listed above.

11.2.1.1 Transparent access to the Internet



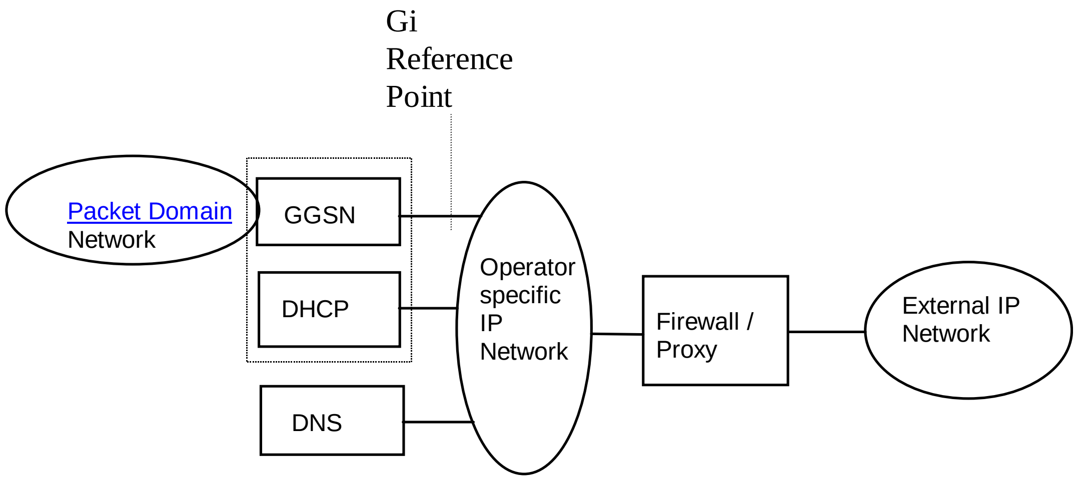


Figure 9: Example of the PDN Interworking Model, transparent case

In this case (see Figure 9),

- The MS is given an address belonging to the operator addressing space. The address is given either at subscription in which case it is a static address or at PDP context activation in which case it is a dynamic address. This address is used for packet forwarding between the Internet and the GGSN and within the GGSN.

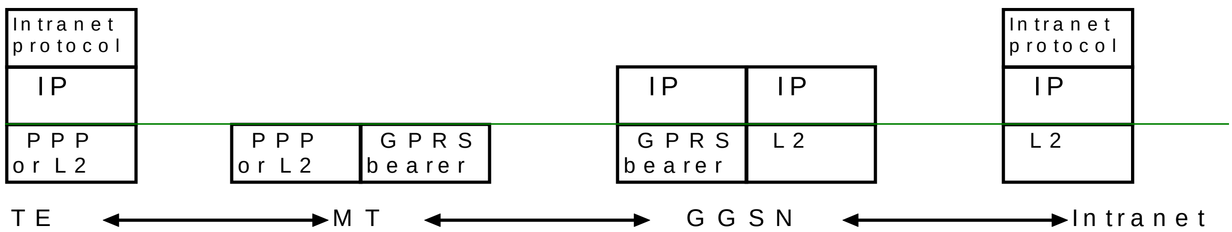
- The MS need not send any authentication request at PDP context activation and the GGSN need not take any part in the user authentication/authorization process.

The transparent case provides at least a basic ISP service. As a consequence of this it may therefore provide a bearer service for a tunnel to a private Intranet.

NB The remainder of this section deals with this specific case.

- The user level configuration may be carried out between the TE and the intranet, the Packet Domain~~GPRS~~ network is transparent to this procedure.

The used protocol stack is depicted in Figure 10.



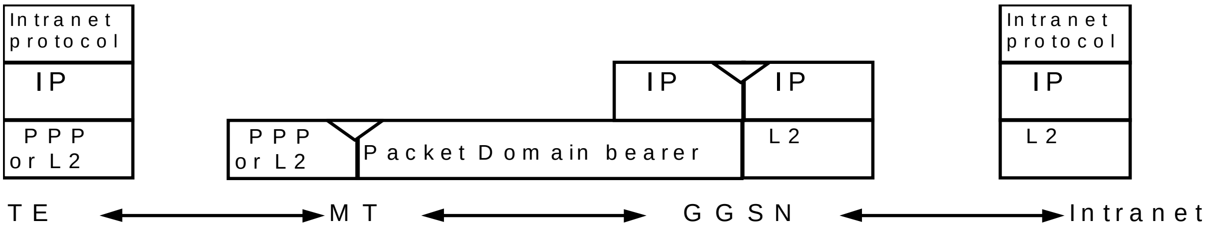


Figure 10: Transparent access to an Intranet

The communication between the ~~GPRS~~ PLMN and the Intranet may be performed over any network, even an insecure network e.g. the Internet. There is no specific security protocol between GGSN and the Intranet because security is ensured on an end to end basis between MS and the intranet by the «Intranet protocol».
User authentication and encryption of user data are done within the «Intranet protocol» if either of them is needed. This «Intranet protocol» may also carry private (IP) addresses belonging to the address space of the Intranet.
An example of an «Intranet protocol» is IPsec (see RFC 1825). If IPsec is used for this purpose then IPsec authentication header or security header may be used for user (data) authentication and for the confidentiality of user data (see RFC 1826 and RFC 1827). In this case private IP tunnelling within public IP takes place.

11.2.1.2 Non Transparent access to an Intranet or ISP

In this case;

- the MS is given an address belonging to the Intranet/ISP addressing space. The address is given either at subscription in which case it is a static address or at PDP context activation in which case it is a dynamic address. This address is used for packet forwarding within the GGSN and for packet forwarding on the Intranet/ISP. This requires a link between the GGSN and an address allocation server, like Radius, DHCP, …, belonging to the Intranet/ISP;

- the MS shall send an authentication request at PDP context activation and the GGSN requests user authentication from a server, like Radius, DHCP, …, belonging to the Intranet/ISP;

- the protocol configuration options are retrieved (if requested by the MS at PDP context activation) from some server (Radius or DHCP, …) belonging to the Intranet/ISP;

- the communication between the ~~GPRS PLMN~~ Packet Domain and the Intranet/ISP may be performed over any network, even an insecure e.g. the Internet. In case of an insecure connection between the GGSN and the Intranet/ISP there may be a specific security protocol in between. This security protocol is defined by mutual agreement between ~~GPRS PLM~~PLMN~~N~~ operator and Intranet/ISP administrator.

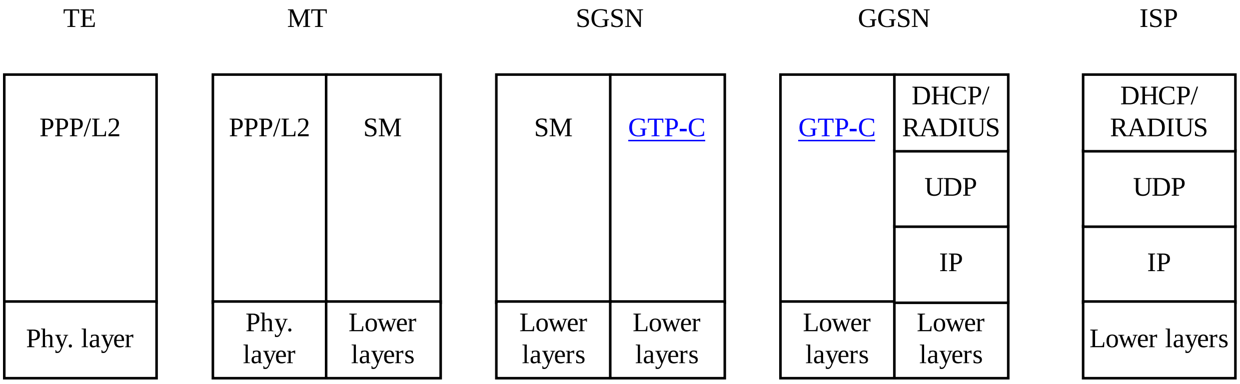


Figure 11: Signalling plane of non transparent case

The following description bullet items describe the signal flow.

1) The TE sends an AT-command to the MT to set up parameters and enter PPP mode. The MT responds with an AT-response.

2) LCP negotiates Maximum-Receive-Unit and authentication protocol. The negotiated authentication protocol is, either CHAP, PAP or 'none'. The MT shall try to negotiate for CHAP as first priority.

3) 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 forced positive acknowledgement of the authentication to the TE.

4) The TE requests IP configuration by sending the IPCP Configure-Request message to the MT indicating either the static IP address that shall be used or that an IP-address shall be dynamically allocated.

5) The MT sends the Activate PDP context request message to the SGSN, including the Protocol Configuration Options. The SGSN sends the Create PDP context req message to the chosen GGSN including the unmodified Protocol Configuration Options.

6) The GGSN deduces from the APN :

   - the server(s) to be used for address allocation, authentication and protocol configuration options retrieval;

   - the protocol like Radius, DHCP, … to be used with this / those server(s);

   - the communication and security feature needed to dialogue with this / those server(s) e.g. tunnel ,IPSec security association, dial-up connection (using possibly PPP), ….

   As an example the GGSN may use one of the following options:

   - RADIUS for authentication and IP-address allocation.. The RADIUS server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN.

   - RADIUS for authentication and DHCP for host configuration and address allocation. The RADIUS server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN. After a successful authentication, the DHCP client discovers the DHCP server(s) in the ISP/Intranet and receives host configuration data. .

7) The GGSN sends back to the SGSN a Create PDP Context Response message, containing the Protocol Configuration Options IE. The cause value shall be set according to the outcome of the host -authentication and -configuration.

8) Depending on the cause value received in the Create PDP Context Response the SGSN sends either an Activate PDP Context Accept or an Activate PDP Context Reject, to the MS.

   If Protocol Configuration Options are received from the GGSN, the SGSN shall relay those to the MS. The MT sends either the configuration-ack packet (e.g. IPCP Configure Ack in PPP case), the configure-nack packet in case of dynamic address allocation (e.g. IPCP Configure Nack in PPP case), or a link Terminate request (LCP Terminate-Request in PPP case) back to the TE. In the case where a configure-nack packet was sent by the MT, a local negotiation may take place at the R reference point (i.e. the TE proposes the new value to the MT), after which a configuration-ack packet is sent to the TE.

9) In case a configuration-ack packet was sent to the TE, the link from the TE to the external ISP/Intranet is established and IP packets may be exchanged.

   In case a link terminate request packet was sent to the TE, the TE and MT negotiates for link termination. The MT may then send a final AT-response to inform the TE about the rejected PDP Context activation.

A link terminate request packet (such as LCP Terminate-request in PPP case) causes a PDP context deactivation.
Example: In the following example PPP is used as layer 2 protocol over the R reference point.
The MT acts as a PPP server and translates Protocol Configuration Options into SM message IEs. GTP-C carries this information unchanged to the GGSN which uses the information e.g. for DHCP or RADIUS authentication and host configuration. The result of the host authentication and configuration is carried via GTP-C to the SGSN which relays the information to the MT. The MT sends an IPCP Configure-Ack to the TE with the appropriate options included.

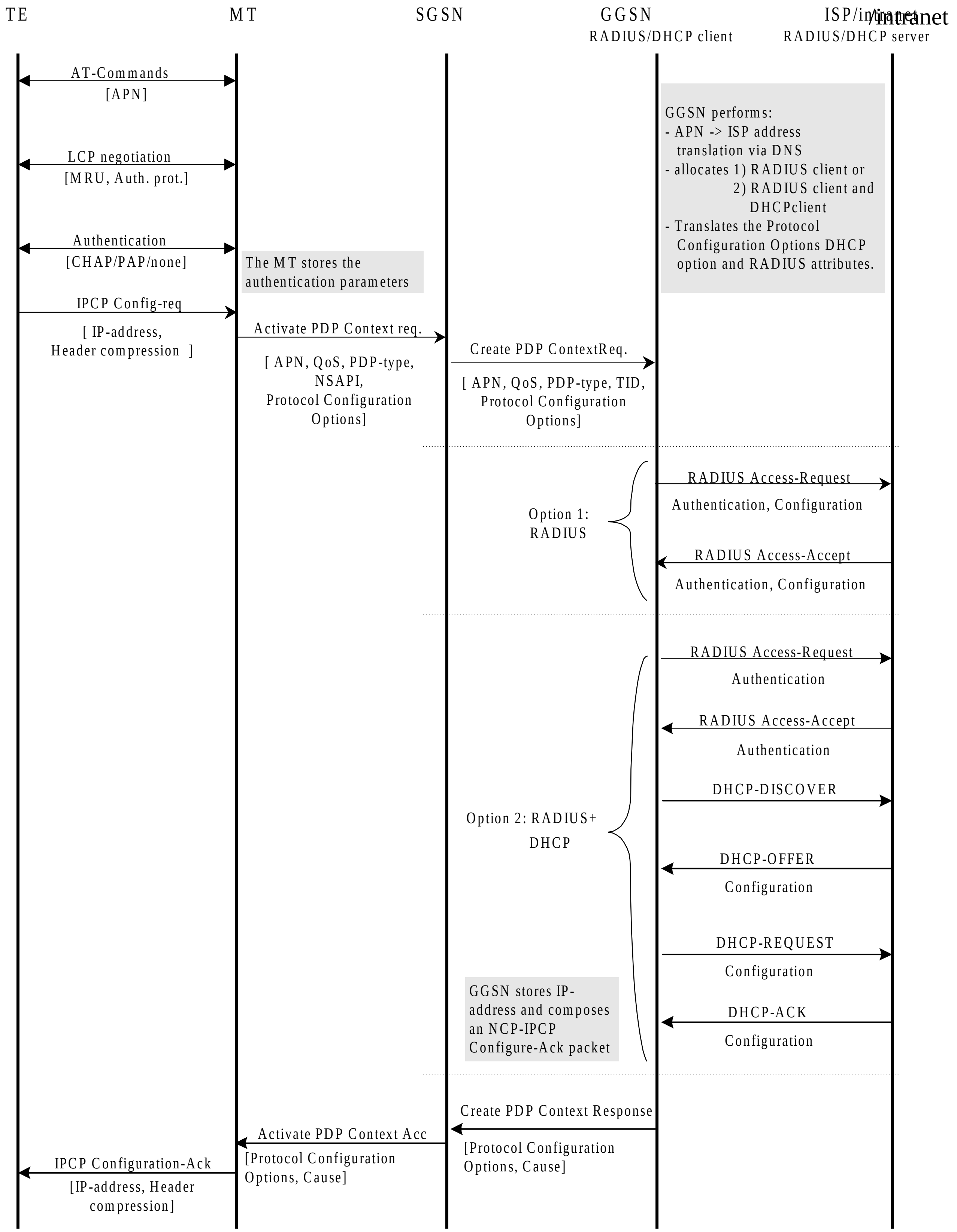


Figure Z: PDP Context Activation for the Non-transparent IP case

11.3 Numbering and Addressing

In the case of interworking with the public IP networks (such as the Internet), the PLMN~~GPRS~~ operator shall use public network addresses. These public addresses can be reserved from the responsible IP numbering body, or from an ISP with which the PLMN~~GPRS~~ operator has an agreement. In the case of interworking with the private IP networks, the PLMN~~GPRS~~ operator manages internally the subnetwork addresses.
The PLMN~~GPRS~~ operator allocates the IP addresses for the subscribers in either of the following ways.

- The PLMN~~GPRS~~ operator allocates a static IP address when the subscription record is built. The IP address is reserved from a pool of free IP addresses.

- The PLMN~~GPRS~~ operator allocates (either on its own or in conjunction with an ISP) a dynamic IP address when the MS performs the PDP Context Activation procedure with dynamic address allocation as described in 3G TS 23.060~~GSM 03.60~~.

11.4 Charging

The PLMN~~GPRS~~ operator may define the accuracy of the charging mechanism using one of the following categories:

- Every source/destination pair is logged separately.

- Source/destination pairs are logged to an accuracy of subnetworks.

- Source/destination pairs are logged to an accuracy of connection types (e.g., external data network, corporate network, another mobile).

11.5 Domain Name System Server (DNS Server)

Provision of Domain Name services shall be provided by the PLMN~~GPRS~~ operators in the transparent case and the ISP in the non transparent case. ~~Domain name registration is handled by RIPE (Réseaux IP Européens) in Europe~~ (DNS documentation is provided in RFC 1034 and RFC 1035).

11.6 Screening

The way the PLMN~~GPRS operator~~ is performing the operator controlled screening and the subscription controlled screening is out of the scope of this specification. These functions may be done, for example, in a firewall.

12 Interworking with PDN (PPP)

12.1 General

By means of the PDP type ‘PPP’ Packet Domain~~GPRS~~ 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). All protocols currently supported by PPP NCP’s are listed in [21]. It may also support interworking by means of tunnelled PPP, by e.g. the Layer Two Tunnelling Protocol (L2TP).

12.2 PDN Interworking Model

The interworking point is at the Gi reference point. The GGSN for interworking with the ISP/PDN is the access point of the Packet Domain~~GSM GPRS data network~~ (see Figure 13). The GGSN will either terminate the PPP connection towards the MS or may further relay PPP frames to the PDN. The PPP frames may be tunnelled in e.g. L2TP.

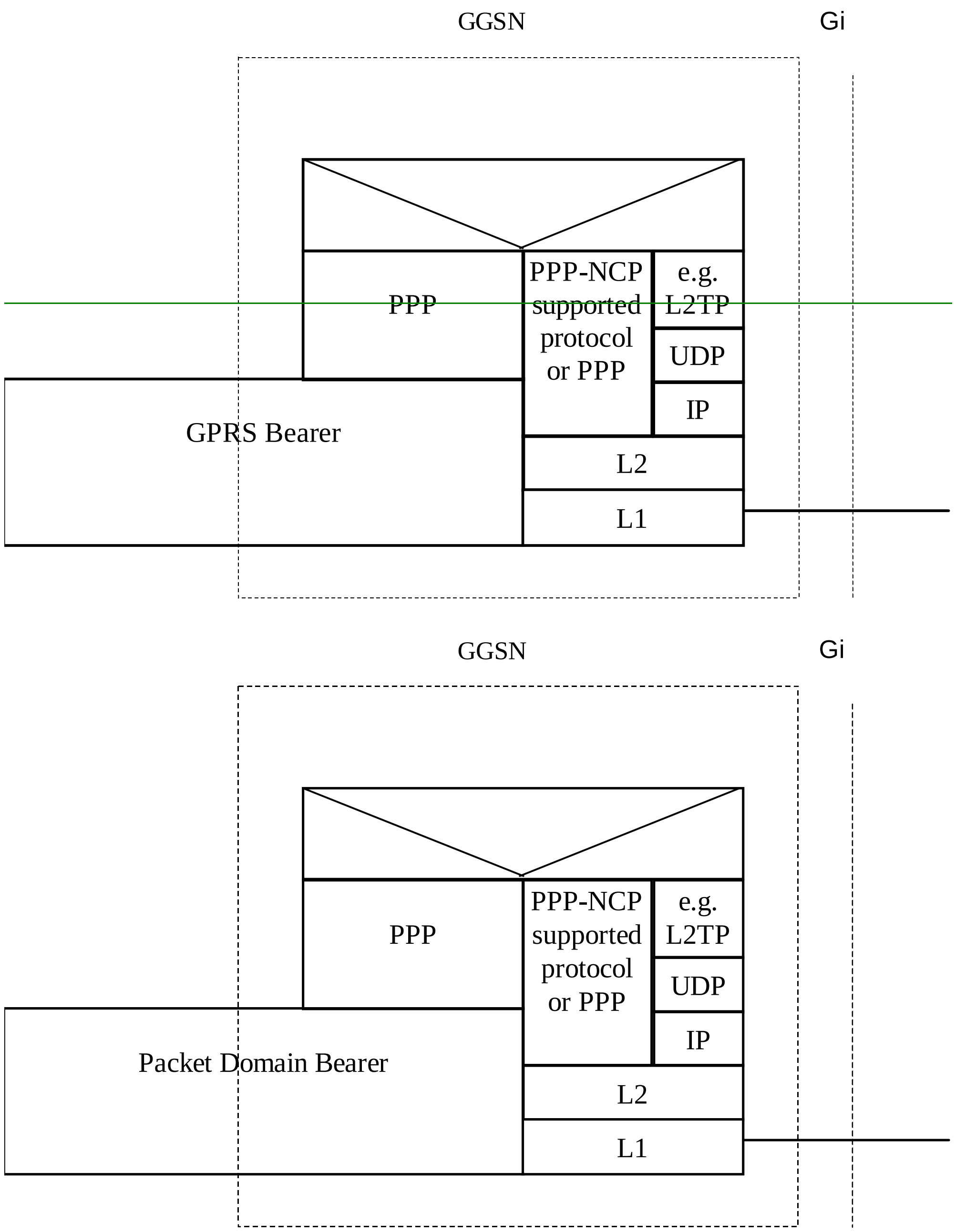


Figure 13: The protocol stacks for the Gi PPP reference point

In case the external PDN is an IP based network and the GGSN terminates PPP the same description applies as specified in section 11.2.

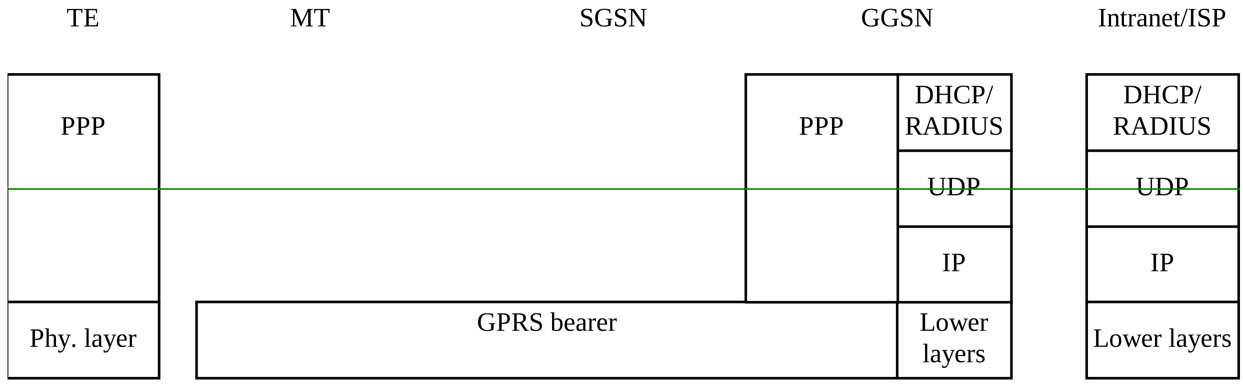
In case the GGSN tunne~~l~~ls PPP frames to the PDN, the GGSN may behave like a LAC towards the external network.

12.2.1 Virtual dial-up- and direct Access to PDNs, or ISPs through Packet Domain~~GPRS~~

The access to PDNs, or ISPs may involve specific functions such as: user authentication, user's authorization, end to end encryption between MS and PDN/ISP, allocation of a dynamic address belonging to the PLMN/PDN/ISP addressing space, etc.

For this purpose the ~~GPRS~~ PLMN may offer, based on configuration data:

- Direct access to an IP based Intranet/ISP using a protocol configuration as depicted in figure 14. Here DHCP and/or RADIUS are used between the GGSN and Intranet/ISP for performing the specific functions mentioned above. The Packet Domain~~GPRS PLMN~~ may also offer access to networks based on any protocol supported by PPP through one of its Network Control Protocols (NCPs).



–

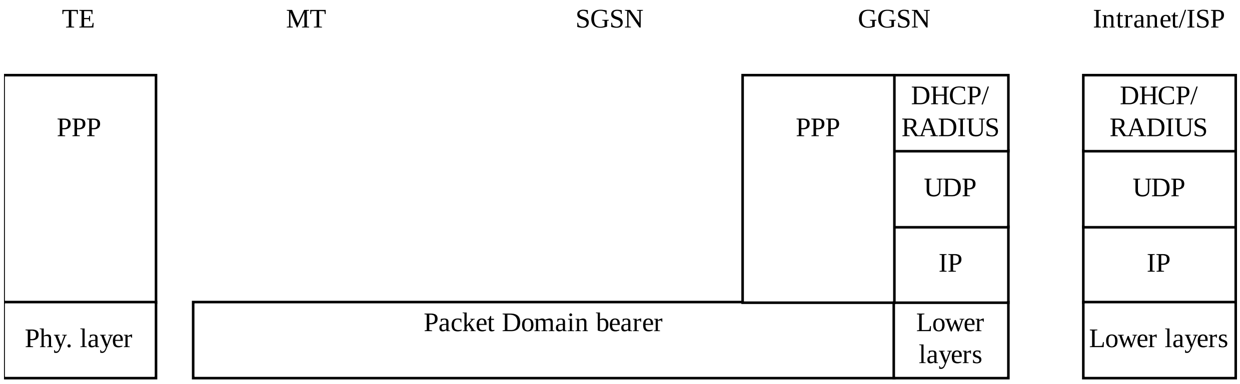
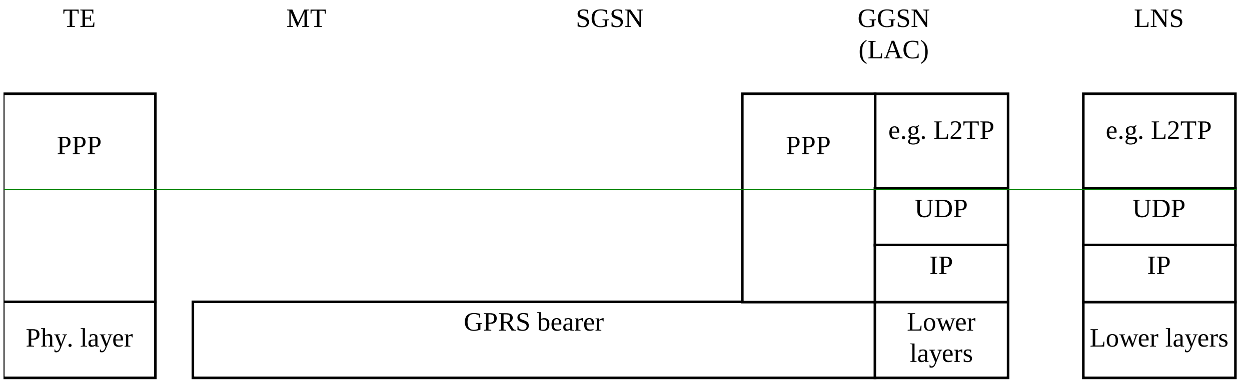


Figure 14: Protocol stack for direct access to IP-based Intranets/ISPs

- Virtual dial-up access to a PDN with PPP frame tunnelling as depicted in figure 15.



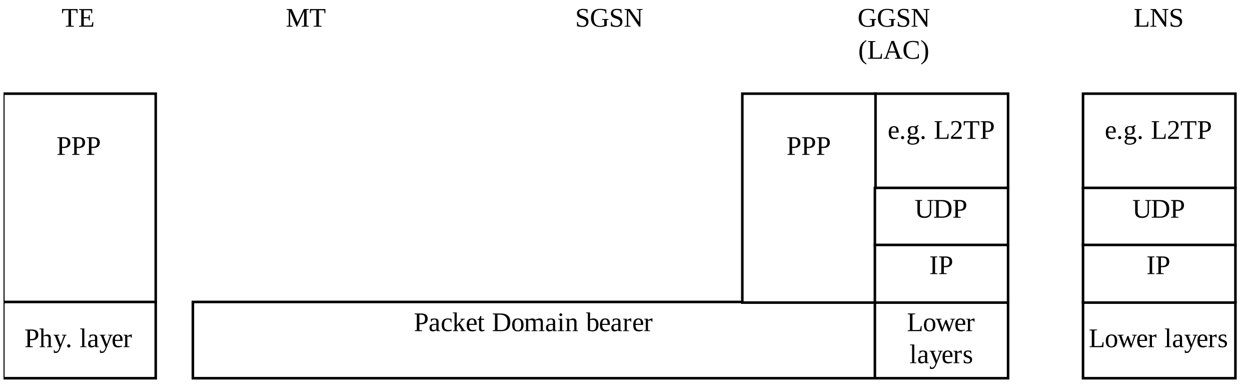


Figure 15: Protocol stack for virtual dial-up access with PPP frame tunnelling

12.2.1.2 Procedural description

In this case;

- the MS is given an address belonging to the Intranet/ISP addressing space. The address is given either at subscription in which case it is a static address or at PDP context activation in which case it is a dynamic address. This address is used for packet forwarding within the GGSN and for packet forwarding on the Intranet/ISP. This requires a link between the GGSN and an address allocation server, such as Radius, or DHCP, belonging to the Intranet/ISP;

- the communication between the Packet Domain~~GPRS PLMN~~ and the Intranet/ISP may be performed over any network, even an insecure e.g. the Internet. In case of an insecure connection between the GGSN and the Intranet/ISP there may be a specific security protocol in between. This security protocol is defined by mutual agreement between ~~GPRS~~ PLMN operator and Intranet/ISP administrator.

The following description bullet items describe the signal flow.

1) The TE sends an AT-command to the MT to set up parameters.

2) The MT sends the Activate PDP context request message to the SGSN which sends the Create PDP context request message to the chosen GGSN.

3) The GGSN deduces from the APN:

   - the server(s) to be used for address allocation and authentication;

   - the protocol such as Radius, DHCP or L2TP to be used with this / those server(s);

   - the communication and security feature needed to dialogue with this / those server(s) e.g. tunnel ,IPSec security association, dial-up connection (using possibly PPP).

   As an example the GGSN may use one of the following options:

     - RADIUS for authentication and IP-address allocation.. The RADIUS server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN.

     - RADIUS for authentication and DHCP for host configuration and address allocation. The RADIUS server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN. After a successful authentication, the DHCP client discovers the DHCP server(s) in the ISP/Intranet and receives host configuration data.

- L2TP for forwarding PPP frames to a L2TP Network Server.

4) The GGSN sends back to the SGSN a Create PDP Context Response message.

5) Depending on the cause value received in the Create PDP Context Response the SGSN may either send the Activate PDP Context Accept message or send the Activate PDP Context Reject message to the MS.

6) The MT responds with an AT-response that may indicate whether the context activation was successful or not. In the case of a non-successful context activation the response may also indicate the cause.

7) In case of a successful context activation, the TE will start its PPP protocol after the LLC link has been established. The LCP, Authentication and IPCP (in case of IP) negotiations are then carried out end-to-end, or between the TE and the GGSN.

Example: In the following example the successful PDP context activation is shown.

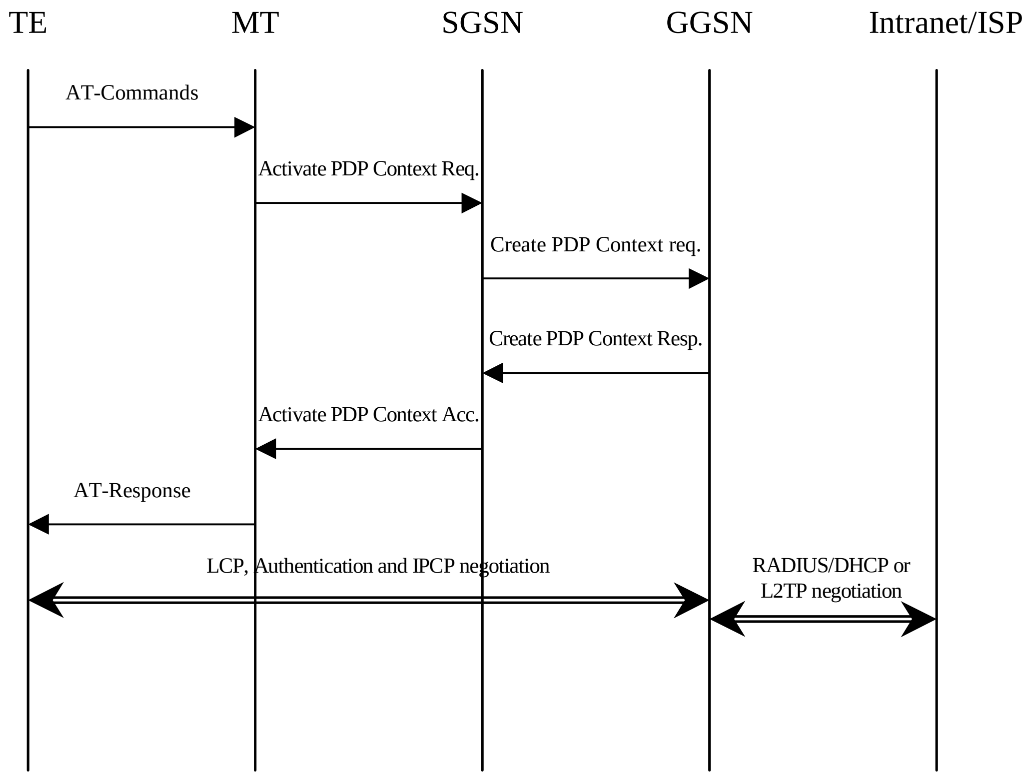


Figure 16

13 Internet Hosted Octet Stream Service (IHOSS)

13.1 Introduction

This section describes the GGSN aspects of the Packet Domain~~GPRS~~ Internet Hosted Octet Stream Service (IHOSS). This is a MO-only, connection-oriented service that carries an unstructured octet (character) stream between a Packet Domain~~GPRS~~ MS 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 3G TS ~~GSM 0~~27.060 contains the generic description of OSP. The subset of features of OSP that are used by OSP:IHOSS is also described in 3G TS ~~GSM 0~~27.060.
Figure 17 shows the scope of IHOSS and OSP:IHOSS.

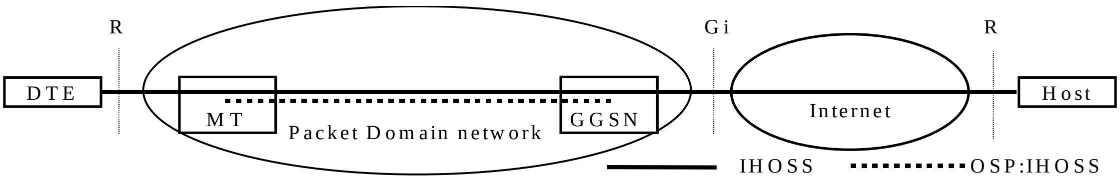


Figure 17: Scope of the Internet Hosted Octet Stream Service and Octet Stream Protocol

13.2 Protocol stacks at the GGSN

Figure 18 shows the protocol stacks at the GGSN. The GGSN contains a relay function between OSP and and the protocol used on the Internet (usually TCP, alternatively UDP).

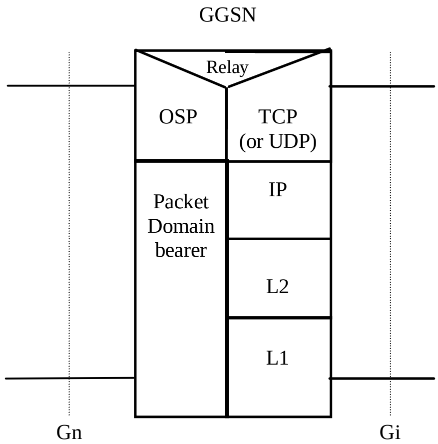


Figure 18: Protocol stacks at the GGSN

13.3 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. Each context supports only one IHOSS connection.

13.3.1 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 ~~GSM 0~~23.060 using messages described in 3G TS ~~GSM 0~~24.008 [23] (MS-SGSN) and 3G TS ~~GSM 0~~29.060 [24] (SGSN-GGSN).

A request to establish an IHOSS connection is signalled to the GGSN by the receipt of a Create PDP context Request message from an SGSN with the PDP type set to OSP:IHOSS. The PDP configuration options may provide information to enable the GGSN to set up a connection to the Internet host. (The contents and format of the PDP configuration options are described in 3G TS ~~GSM 0~~27.060.) Alternatively this information may be derived from subscription information in the HLR and configuration information within the GGSN.

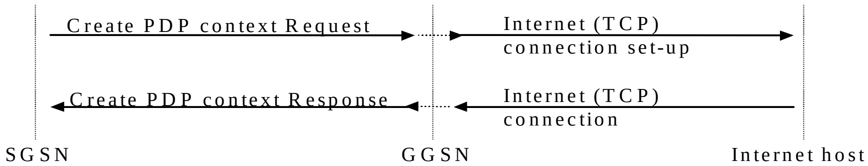


Figure 19: IHOSS connection establishment (TCP over the Internet)

In the case where TCP is used over the Internet (figure 19), the response creating the context activation request is returned to the SGSN only when the TCP connection to the Internet host has been established. If the TCP connection attempt fails, the request to create a context is rejected.

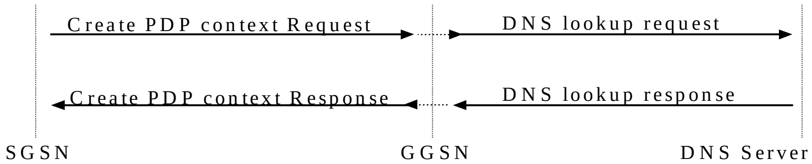


Figure 20: IHOSS connection establishment (UDP over the Internet)

In the case where UDP is used over the Internet (figure 20), the response accepting the context activation request is returned to the SGSN only when a successful DNS lookup of the Internet host name has been completed. If the lookup fails, the request to create a context is rejected. (The GGSN may perform additional checks before responding to the context activation request but these are not specified here.)

13.3.2 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 MS or the Internet host (TCP only), or exceptionally by the SGSN under fault conditions. A~~n~~ MS-initiated or SGSN-initiated disconnection is signalled to the GGSN by the receipt of a Delete PDP context request from an SGSN.
In the case where TCP is used over the Internet, the GGSN first clears the TCP connection and then sends a Delete PDP context response to the SGSN.
In the case where UDP is used over the Internet, the GGSN sends a Delete PDP context response to the SGSN immediately, there being no actual Internet connection to clear.
The GGSN signals an Internet host-initiated disconnection to the SGSN by sending a Delete PDP context request.

13.4 OSP:IHOSS - TCP (UDP) relay

13.4.1 Required feature

13.4.1.1 Flow control

The OSP flow control procedures shall map on to the TCP flow control procedures. There is no flow control mapping in the case of UDP.

13.4.2 Optional features

13.4.2.1 Break handling

The OSP break procedure may map on to the TCP break procedure. There is no break mapping in the case of UDP.

13.4.2.2 GGSN maximum buffer size

Although the OSP entity in the GGSN does not have a PAD, it still requires buffers to hold the relayed packets. The GGSN PAD maximum buffer size parameters (in the Protocol Configuration Options) may be used to specify the maximum buffer sizes for the two directions of data transfer. Details are given in 3G TS ~~GSM 0~~27.060.

14 Interworking between Packet Domains~~GPRS networks~~

The primary reason for the interworking between Packet Domains~~the GPRS networks~~ is to support roaming ~~GPRS~~ subscribers as described in TS 23.060~~GSM 03.60~~. The general model for Packet Domain~~GPRS network~~ interworking is shown in Figure 21.

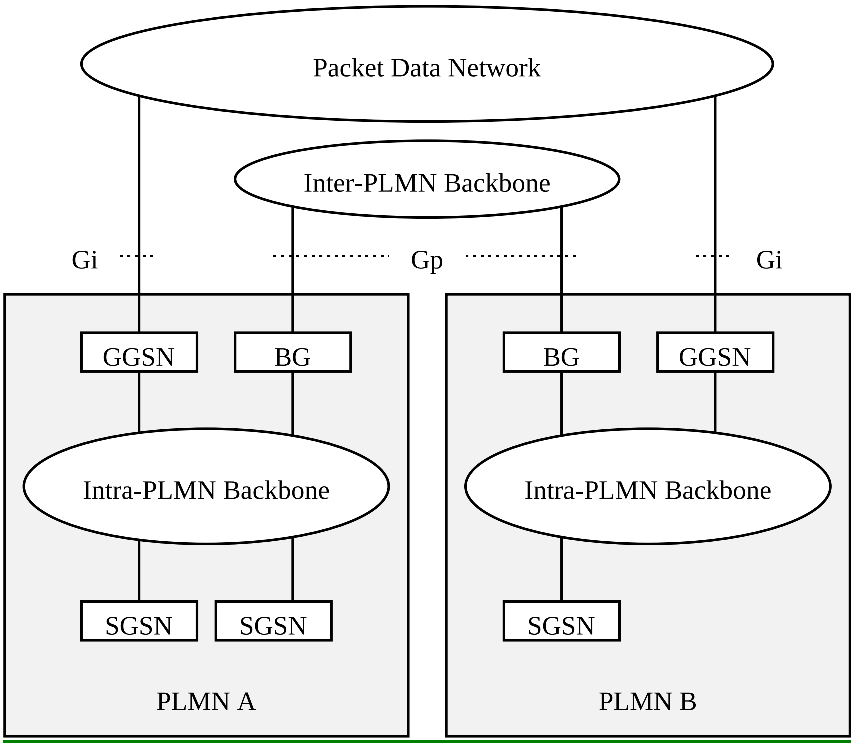


Figure 21: General interworking between Packet Domains~~GPRS networks~~ to support roaming subscribers

For roaming subscribers that have a PDP address allocated from the HPLMN a forwarding route between the HPLMN and the VPLMN is created. This route is used for both mobile terminated and mobile originated data traffic. The communication is done via the BGs (Border Gateways) as described in 3G TS 23.060~~GSM 03.60~~.
The procedures to set the link between the SGSN in the VPLMN and the GGSN in the HPLMN are~~is~~ described in 3G TS 23.060~~GSM 03.60~~.
The inter-PLMN link may be any packet data network or dedicated link as described in 3G TS 23.060~~GSM 03.60~~. The PLMN~~GPRS~~ operators may have a dedicated inter-PLMN link to fulfil the QoS requirements of a certain protocol.

14.1 Security Agreements

Each PLMN~~GPRS~~ operator may support IPsec (RFC 1825) and accompanying specifications for authentication (RFC 1826) and encryption (RFC 1827) as a basic set of security functionality in its border gateways. The PLMN~~GPRS~~ operators may decide to use other security protocols based on bilateral agreements.

14.2 Routing protocol agreements

Each PLMN~~GPRS~~ operator may support BGP (RFC 1771) as a basic set of routing functionality in its border gateways. The PLMN~~GPRS~~ operators may decide to use other routing protocols based on bilateral agreements.

14.3 Charging agreements

Sharing the cost of the inter-PLMN link is subject to the agreement between the PLMN~~GPRS~~ operators.
There may be a requirement to collect charging information in the Border Gateway (see Figure ~~1~~21 in section 14) and this is down to the normal interconnect agreement between PLMN and PDN operators.

Annex A (normative): Interworking PCS1900 with PSDNs

A.1 Key characteristics of interworking PCS1900 with PSDNs

Bell Operating Company's (BOC's) Public Packet Switching Networks provide data transport services within it's LATA and support data transport as follows:

- between Terminal Equipment (TE) and host computers,
- between TE to TE, between host computer to host computer,
- and interface to Private Networks within LATA.

The interface to other Packet Switched Public Data Networks (PSPDNs) outside the LATA is via Interexchange Carriers (ICs).
For PCS1900, two types of PSDN may exist - those outside a BOC's LATA and those inside.

A.1.1 PSPDNs which are outside the BOC's LATA

PSPDNs which are outside the BOCs LATA are connected via X.75 interface. Interworking is the same as described in section 10.2.1, X.75 Interworking at the Gi Reference Point.

A.1.2 PSPDNs which are inside the BOC's LATA

BOCs PPSN consists of Data Switching Exchanges (DSE) and ISDN Packet Handler Functions (PHFs).
The Bellcore defined X.75' protocol is used on intranetwork DSE to DSE, DSE to ISDN Packet Handler Function (PHF), and ISDN PHF to ISDN PHF within BOC administered networks, and is used for intra-LATA packet data calls. X.75 interface is used on ICs connected to other PSPDNs outside the LATA.
Therefore, in order to support packet data services within BOC's LATA for PCS 1900 subscribers, support of Bellcore defined X.75' interface is required at the Gi interface.
Bellcore defined X.75' protocol is an extension of X.75 protocol. The extension consists primarily of additional utilities some of which are analogous to X.25 facilities The extension is necessary to maintain service transparency when interconnection equipment supplied by different manufacturers within a single network.
The rest of this annex describes X.75' interworking.

A.2 Subscription checking

Subscriptions checking for Bellcore defined X.75' interface is outside the scope of this specification.

A.3 Interworking PCS1900 with PSDN using X.75'

A.3.1 General

The Packet Domain~~GPRS~~ shall support interworking with PSDN networks. The interworking may be either direct or through a transit network (e.g. ISDN).
The Packet Domain~~GPRS~~ shall support both ITU-T X.121 and ITU-T E.164 addressing.
The Packet Domain~~GPRS~~ shall provide support for interworking using Bellcore specified X.75' protocol for data transport within BOC's LATA.

The Packet Domain~~GPRS~~ TE’s shall have addresses provided, and controlled, by their Packet Domain~~GPRS~~ operator.
The PSDN TE sends data to the Packet Domain~~GPRS~~ TE by use of that TE’s Packet Domain~~GPRS~~ DNIC (Data Network Identification Code) or equivalent which uniquely identifies that GPRS network worldwide.
The GGSN for interworking with PSDNs is the access point of the Packet Domain~~GSM GPRS~~ data network.
The X.75’ access method is supported when mobile users are resident on HPLMN or VPLMN. A roaming user may be allocated a dynamic address from the VPLMN.

A.3.2 PSDN Interworking Model using X.75' Interworking at the Gi Reference Point

Figure A~~X~~.1 represents the case where X.75’ is used as the interworking protocol, as used between interconnect X.25 PSDNs within the BOC’s LATA. The GPRS network will look like any other PSDN in the BOC’s LATA and will use X.75’ addressing. Figure 4 shows the interconnecting protocol stacks to the Packet Domain~~GPRS~~ bearer. The Packet Domain~~GPRS~~ bearer is described in 3G TS~~GSM 0~~27.060, which uses the protocols described in 3G TS ~~GSM 0~~23.060.

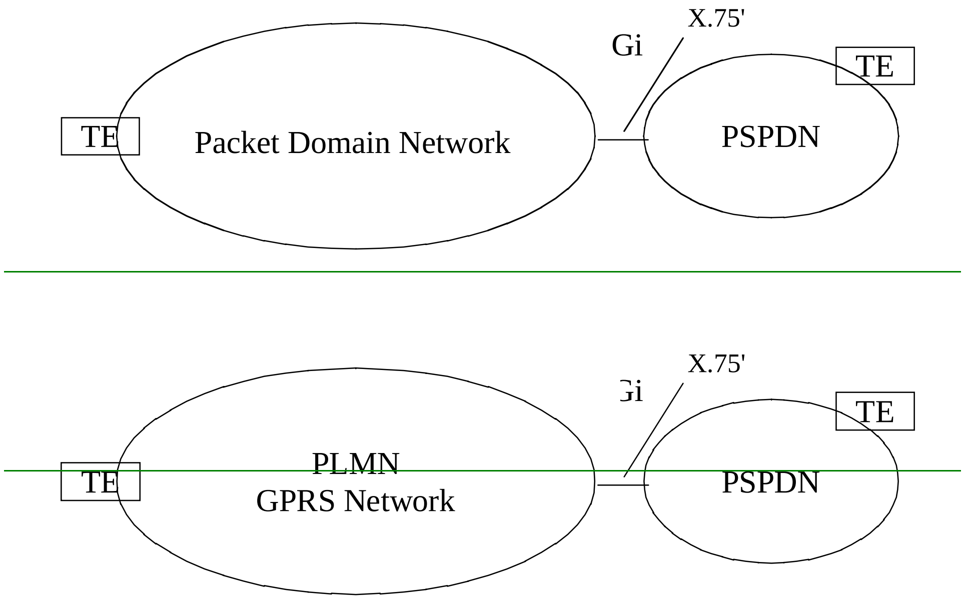


Figure A.1: PSPDN Interworking with X.75’ at Gi Reference Point

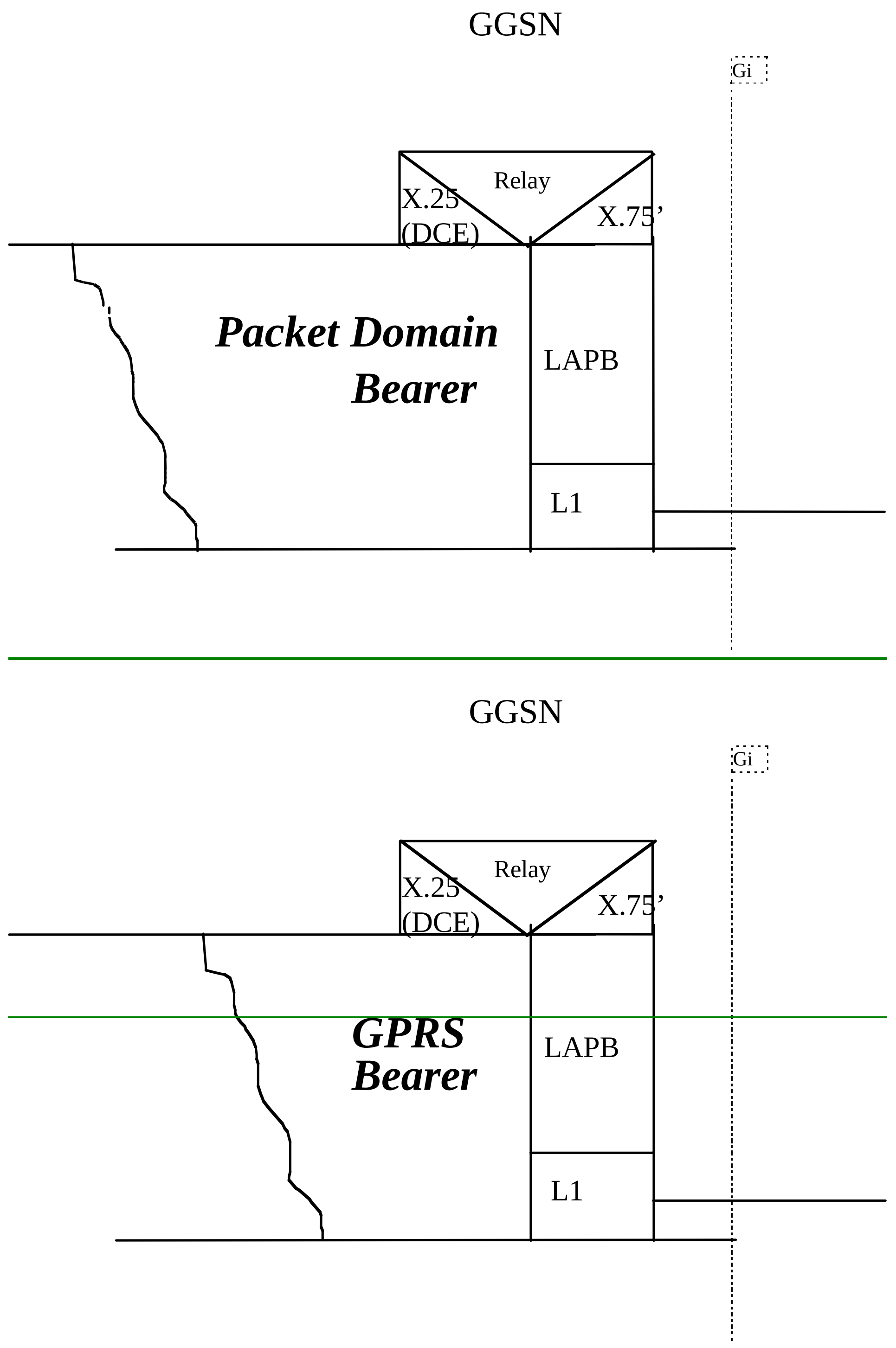


Figure A.2: The Protocol Stack for the X.75' Gi Reference Point

A.3.3 Numbering and Addressing

A PLMN interworking with a PSPDN~~GPRS network~~ requires a DNIC or PNIC.
X.121 addresses allocated to subscribers belong to the PLMN operator.

A.3.4 Charging

Charging of X.25 packets is done at the GGSN.

A.3.5 User Facilities

These are the same as in section 10.3 in the main part of this specification.

A.3.6 The Packet Domain~~GPRS~~ Interworking to PSDN Characteristics

These are the same as in section 10.4 in the main part of this specification.

Annex B:
Change history

Change history						
TSG CN#	**Spec**	**Version**	**CR**	**<Phase>**	**New Version**	**Subject/Comment**
Apr 1999	GSM 09.61	7.0.0				Transferred to 3GPP CN1
CN#03	29.061				3.0.0	Approved at CN#03
CN#04	29.061	3.0.0	001		3.1.0	Access to PDNs and ISPs with the PDP-type PPP
CN#04	29.061	3.0.0	002		3.1.0	GPRS Internet Hosted Octet Stream Service (IHOSS)

History

Document history		
V3.0.0	May 1999	Approved at TSGN #3. Under TSG TSG CN Change Control.
V3.1.0	August 1999	CRs 001 and 002 Approved by E-mail after TSGN#4