ETSI TS 101 747 V1.1.1 (2001-07)

Technical Specification

Terrestrial Trunked Radio (TETRA);
Voice plus Data (V+D);
IP Interworking (IPI)

Reference

DTS/TETRA-03031

Keywords

internet, interworking, IP, packet mode, security, TETRA

ETSI

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

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

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

Contents

Intellectual Property Rights

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

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

Foreword

This Technical Specification (TS) has been produced by ETSI Project Terrestrial Trunked Radio (TETRA).

1 Scope

The present document defines IP Interworking (IPI) between two TETRA networks for the transfer of IP data while MS migrates from one SwMI to another.

The present document defines the use of GPRS Tunnelling Protocol (GTP), the Gateway GPRS Support Node (GGSN) and ISI for IPI.

The present document proposes limited extension to SNDCP of the TETRA Air Interface and ISI in order to use the IP interworking functionality of the GGSN and to use standardized Gn and Gp interfaces. As a consequence, the protocols and signalling messages already defined and developed for GPRS can be used. The use of standard GGSN and other GPRS Backbone elements and the existing interworking functions is described for IPI. The architecture ensures re-use of the already standardized TETRA ISI Mobility Management, HDB and VDB functions and TETRA registration procedures between the Mobile Station and SwMI.

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 and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] ETSI EN 300 392-2 (V2.3.2): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".

[2] ETSI ETS 300 392-3-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 1: General design".

[3] ETSI ETS 300 392-3-5: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 5: Additional Network Feature for Mobility Management (ANF-ISIMM)".

[4] ETSI EN 300 927: "Digital cellular telecommunications system (Phase 2+) (GSM); Numbering, addressing and identification (GSM 03.03 version 5.4.1 Release 1996)".

[5] ETSI EN 301 344: "Digital cellular telecommunications system (Phase 2+) (GSM); General Packet Radio Service (GPRS); Service description; Stage 2 (GSM 03.60 version 7.4.1 Release 1998)".

[6] ETSI EN 301 347: "Digital cellular telecommunications system (Phase 2+) (GSM); General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface (GSM 09.60 version 7.5.1 Release 1998)".

[7] ETSI TS 101 348: "Digital cellular telecommunications system (Phase 2+) (GSM); General Packet Radio Service (GPRS); Interworking between the Public Land Mobile Network (PLMN) supporting GPRS and Packet Data Networks (PDN) (GSM 09.61 version 7.2.0 Release 1998)".

[8] STD 6, RFC 768: "User Datagram Protocol".

[9] RFC 1334: "PPP Authentication Protocols". Obsoleted by RFC 1994.

[10] RFC 1994: "PPP Challenge Handshake Authentication Protocol (CHAP)". Obsoletes RFC 1334 (except for PAP).

[11] RFC 2138: "Remote Authentication Dial In User Service (RADIUS)". Obsoletes RFC 2058.

[12] RFC 2181: "Clarifications to the DNS Specification". Updates RFC 1034, RFC 1035, RFC 1123.

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

IP address: Internet Protocol address, either version 4 or version 6

IP Backbone: private IP network interconnecting IP network nodes, such as GGSN and BG

PDP context: unique relation between upper protocol layer address (e.g. IP address), user identity and NSAPI in SwMI, MS and GGSN

TETRA Network: network consisting of a TETRA SwMI and an IP Backbone which are connected together and controlled by one and the same operator

TETRA PDP: TETRA Packet Data Protocol

NOTE: In addition to its literal meaning the term has also a more generic interpretation such as *TETRA PDP service* or *TETRA packet data service*.

3.2 Symbols

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

Gi reference point between an IP Backbone and an external IP PDN
Gn interface between SwMI and GGSN within the same TETRA Network
Gp interface between IP backbones
R0 reference point at the TETRA Air Interface for IP packet data
R1 TETRA reference point between a packet mode TE and an MT

3.3 Abbreviations

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

AI-1 Air Interface layer one
APN Access Point Name
BG Border Gateway
CHAP Challenge Handshake Authentication Protocol
DHCP Dynamic Host Configuration Protocol
DNS Domain Name System
GGSN Gateway GPRS Support Node
GPRS General Packet Radio Service
GSM Global System for Mobile communication
GTP GPRS Tunnelling Protocol
HDB Home DataBase
IP Internet Protocol
IPCP IP Control Protocol
IPI IP Interworking
IPSEC IP SECurity architecture
ISI Inter System Interface
ISIMM ISI Mobility Management
ISP Internet Service Provider
ITSI Individual TETRA Subscriber Identity
L1 Layer one
L2 Layer two
LCP Link Control Protocol

MAC	Medium Access Control
MM	Mobility Management
MS	Mobile Station
MT	Mobile Terminated
NSAPI	Network layer Service Access Point Identity
PAP	Password Authentication Protocol
PDN	Packet Data Network
PDP	Packet Data Protocol
PDU	Protocol Data Unit
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
RFC	Request For Comment
SGSN	Serving GPRS Support Node
SNDCP	SubNetwork Dependent Convergence Protocol (NL)
SwMI	Switching and Management Infrastructure
TCP	Transmission Control Protocol
TE	Terminal Equipment
TID	Tunnel IDentifier
UDP	User Datagram Protocol
VDB	Visitor Data Base
VPN	Virtual Private Network

4 Introduction

The TETRA Packet Data Protocol (PDP) extends TETRA to act as an IP subnet. The working of the TETRA PDP at the Air Interface is defined in EN 300 392-2 [1].

The present document describes the use of GPRS Tunnelling Protocol (GTP) defined in EN 301 347 [6] for IPI by mandating the functionality of the Gateway GPRS Support Node (GGSN) within the TETRA network. In GPRS strict separation between the radio subsystem and network subsystem is maintained, allowing the network subsystem to be reused with other radio access technologies, in this case by using TETRA PDP as an alternative to the GPRS radio part.

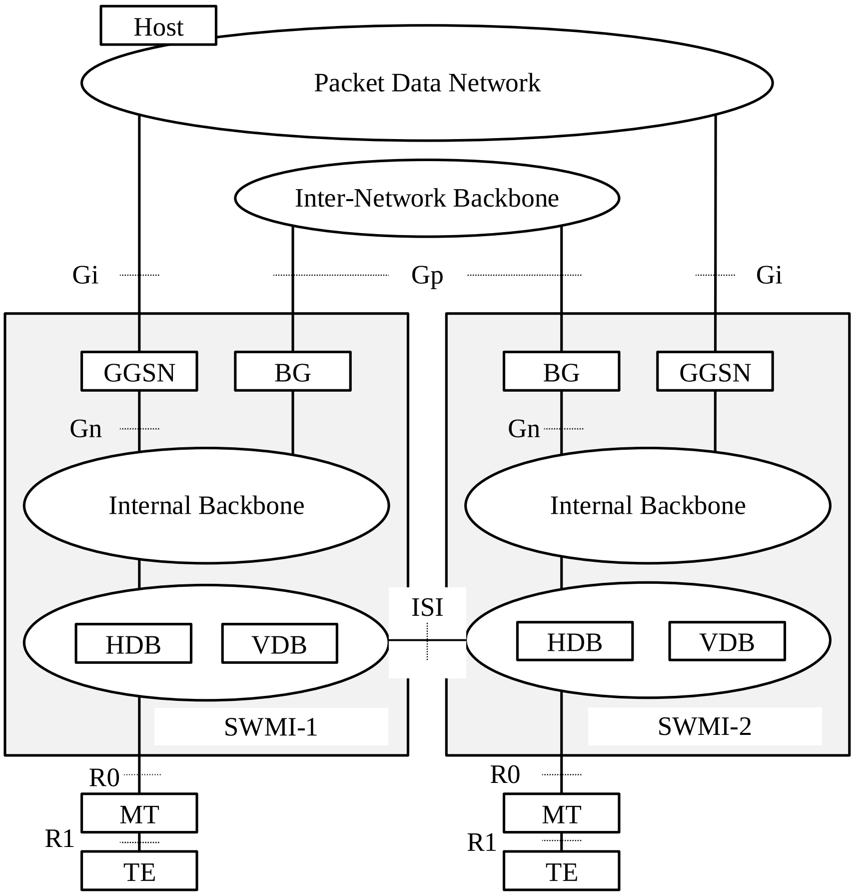
The GGSN provides interworking with external packet data networks and it is connected by GTP to the TETRA SwMI. When an MS migrates from one TETRA network to another the GGSN acts as an anchor for IP traffic keeping open PDP contexts active. This ensures socket continuity required for IP applications (IP addresses and port numbers at both ends of a TCP or UDP connection remain the same).

GTP is used to tunnel GTP PDUs between SwMI and GGSN and between IP Backbones.

5 IPI Concept

5.1 IPI Reference model

In figure 1 is illustrated the reference model of IPI. In the model the ISI is used for MM between SwMIs and the Gp interface is used for tunnelling and routing IP datagrams between IP Backbones. The internal structure of the SwMIs shown in figure 1 is an implementation option and does not set any requirements.



BG:	Border Gateway
GGSN:	Gateway GPRS Support Node defined in EN 301 344 [5]
Gi:	The reference point between an IP Backbone and an external IP PDN, TS 101 348 [7] defines the interworking with IP networks
Gn:	Optional interface between SwMI and GGSN within the same TETRA Network
Gp:	The interface between IP Backbones
HDB:	A database that comprises information about subscribers and is located in the subscriber's home SwMI
Host:	An IP host computer, such as an e-mail server or an ordinary PC
IP Backbone:	A private IP network interconnecting IP network nodes, such as GGSN and BG
IP PDN:	An IP Packet Data Network, such as the Internet or a private intranet
ISI:	Inter-System Interface for interconnecting TETRA SwMIs
MT:	A TETRA Mobile Termination with IP Packet Data support
R0:	The reference point at the TETRA Air Interface for IP packet data
R1:	The TETRA reference point between the packet mode TE and MT
SwMI:	TETRA Switching and Management Infrastructure
TE:	IP packet mode Terminal Equipment, such as a laptop
VDB:	A database that comprises temporary information about subscribers and is located in the visited SwMI

Figure 1: IP Interworking between two TETRA Networks

5.2 Transmission plane

Figure 2 illustrates the transmission plane of TETRA IPI showing protocol stacks for Gn interface. The protocol structure is a combination of transmission planes described in TETRA and GPRS specifications. The connection is done by a relay function on the SwMI, which relays PDP PDUs between the R0 and Gn interfaces. If the Gn interface is not used the related protocol stacks may exist in different format or not at all.

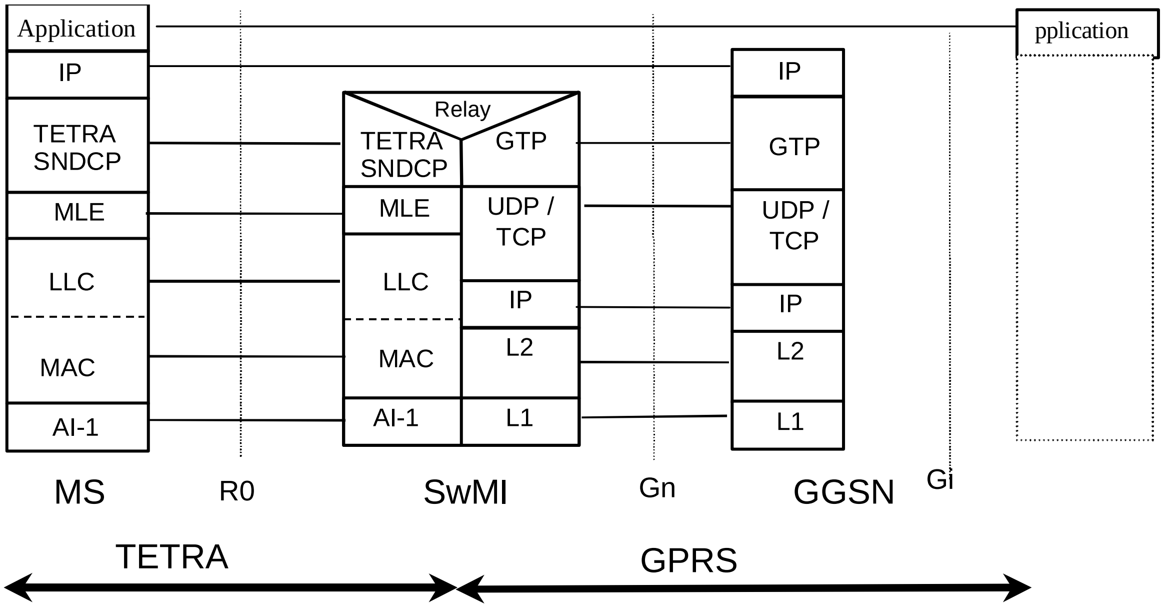


Figure 2: The transmission plane of TETRA IPI

5.3 GTP Signalling plane

5.3.1 SwMI - GGSN and SwMI - SwMI, Gn

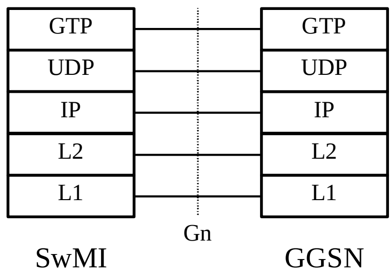


Figure 3: Signalling Plane SwMI - GGSN

GTP tunnels user data and signalling messages between SwMI and GGSN and between SwMI and SwMI.

User Datagram Protocol (UDP) transfers signalling messages between SwMI and GGSN and between SwMI and SwMI. UDP is defined in STD 6, RFC 768 [8].

5.3.2 Between IP Backbones, Gp

The Gp interface provides the functionality of the Gn interface and the security functions required for communication between IP Backbones. The signalling in the Gp interface is the same as in the Gn interface. The communication is done via Border Gateways (BG) which provide security functions.

NOTE: Definition of security protocols is outside of the scope of present document.

5.3.3 IMSI - ITSI Association

When SwMI sends a Create PDP Context request to GGSN, IMSI is a part of TID as defined in EN 301 347 [6]. In TETRA Air Interface ITSI is used instead of IMSI and therefore the relay function between the TETRA SNDCP and GTP shall provide the support for IMSI - ITSI association.

5.4 Mobility management

5.4.1 User Mobility

The ISI defined in ETS 300 392-3-1 [2], provides the TETRA Mobility Management between SwMIs as defined in ETS 300 392-3-5 [3].

The ISI is used to transfer the IP service profile from home SwMI to visited SwMI when migration occurs. IPI sets additional requirements for information to be included in IP service profile as defined in annex B.

5.4.2 PDP Context Mobility

When a PDP context is established instances of the context shall be created in the following locations:

- MS;
- SwMI; and
- GGSN.

To connect contexts in SwMI and GGSN a GTP tunnel shall be established. Both ends of the GTP tunnel shall know the IP address of the other end of the tunnel. For GGSN this means that it knows the IP address of the Gn interface in SwMI. This address shall be stored in GGSN PDP Context in the *SGSN Address* field which is defined in EN 301 344 [5].

When an MS migrates from one SwMI to another the GGSN acts as an anchor for IP traffic keeping open PDP contexts active. This ensures the socket continuity required for IP applications (IP addresses and port numbers at both ends of a TCP or UDP connection remain the same). The visited SwMI shall signal the corresponding GGSN to update the address of the Gn interface, i.e. the other end of the tunnel is moved from the previous visited SwMI to visited SwMI. This shall be done by using the GTP signalling message Update PDP Context Request as defined in EN 301 347 [6]. Example signalling diagrams are described in annex A.

5.5 Access Point Name (APN)

5.5.1 Definition of APN

In the IP Backbone an Access Point Name (APN) defined in EN 300 927 [4] is a reference to a GGSN and inside the GGSN the APN identifies the external IP network to be used. The DNS (Domain Name System) functionality of the IP Backbone is used to translate the APN into the IP address of the GGSN.

The APN is composed of two parts as follows:

- the APN Network Identifier. This defines a GGSN and then inside this selected GGSN it identifies which external network to connect to. This first part of the APN is mandatory;
- the APN Operator Identifier. This defines in which IP Backbone the GGSN is located. This second part of the APN is optional.

The APN Operator Identifier is placed after the APN Network Identifier. An APN consisting of both the Network Identifier and Operator Identifier corresponds to a DNS name of a GGSN. The syntax of the APN shall follow the Name Syntax as defined in RFC 2181 [12].

5.5.2 APN selection

When MS sends a PDP context activation request, in the request there may exist an optional APN index field. If the field exists, SwMI shall use it for selecting an APN to be used when PDP context is activated. APN index points to an APN in a group of APNs.

NOTE: Only a subpart of possible APNs may be provisioned for a subscriber. This provisioning may be stored in HDB.

If the field is not present in the PDP context activation request then SwMI shall use a default APN provisioned for the subscriber.

6 Security issues

6.1 MS Authentication

The TETRA specifications support a two-way authentication to guarantee the authenticity of both parties in the air interface. An MS can be authenticated by an SwMI and an SwMI can be authenticated by a MS. Authentication takes place as part of the MS registration.

6.2 Air-Interface Encryption

Air-interface Encryption is a standardized but not a mandatory feature of the TETRA. Negotiation of encryption and cipher keys is a part of the MS registration.

6.3 IP User Authentication

In EN 300 392-2 [1], an independent IP user authentication for TETRA PDP is defined. The most widely supported authentication protocols for PPP are the Password Authentication Protocol (PAP) defined in RFC 1334 [9] and the Challenge Handshake Authentication Protocol (CHAP) defined in RFC 1994 [10]. They are also supported in TETRA AI.

The authentication information is sent from MS to SwMI in SN-ACTIVATE PDP CONTEXT DEMAND PDU. When the TETRA AI encryption is used, the PDUs used for authentication are also encrypted.

6.4 Gp Interface Between IP Backbones

Two IP Backbones are connected via the Gp using BGs which provide security functions needed for secure transport of IP Datagrams. The security functionality is based on mutual agreement between operators.

NOTE: For example VPN solutions which include tunnelling and encryption may be used.

6.5 End-to-end Security

The communication between an IP Backbone and an intranet may be performed over any network, even an insecure network e.g. the Internet. Security is ensured on an end-to-end basis between MS and the intranet by user specified protocols e.g. IPSEC.

Annex A (informative): Use Cases

A.1 Migrated to visited SwMI and activating a new PDP Context

This clause presents an example scenario to migration and PDP context activation. Figure A.1 illustrates the model where the MT has migrated from its home SwMI-1 to visited SwMI-2. For IP PDP services the MT has provisioned to access an external IP PDN, e.g. an intranet or an ISP's network. The SwMI-1 side is connected to the IP PDN through GGSN that is located in the IP Backbone of the SwMI-1.

For IP authentication there is an AAA server supporting RADIUS protocol defined in RFC 2138 [11] and for IP address allocation a DHCP server. Both servers are located in the IP PDN thus having the non-transparent access in this case.

Following assumptions are made:

- PPP is the link layer protocol between the TE and the MT;
- there is a requirement to authenticate the TE using PAP or CHAP;
- there is a requirement to support the PPP authentication with the centralized AAA server which is accessed by RADIUS protocol;
- there is a requirement to allocate an IP address from the external IP PDN;
- the PAP or CHAP authentication information collected by the MT is forwarded over the TETRA Air Interface to the SwMI as defined in EN 300 392-2 [1];
- for IP address allocation the DHCP server located in the external IP PDN is used;
- inside the GGSN there is a RADIUS and a DHCP client entity which forwards the authentication and IP address allocation requests to the servers in the IP PDN.

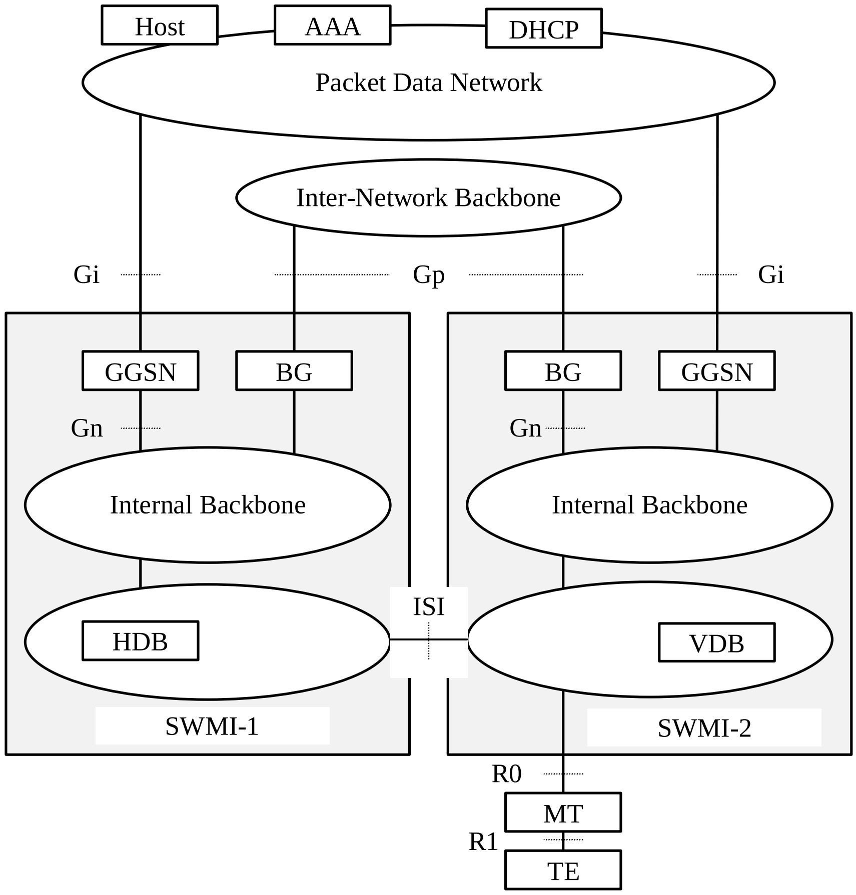


Figure A.1: Migrated to visited SwMI and activating a new PDP Context

Legend (see also previous figures):

- **AAA:** a server supporting Radius protocol, used for IP user authentication;
- **DHCP:** a server used for IP address allocation;
- **DNS:** a Domain Name System for translating DNS names into IP addresses.

A PDP Context Activation procedure with a successful authentication using CHAP or PAP and an IP address allocation using external DHCP server is illustrated in figure A.2. Each numbered step is explained in the following list.

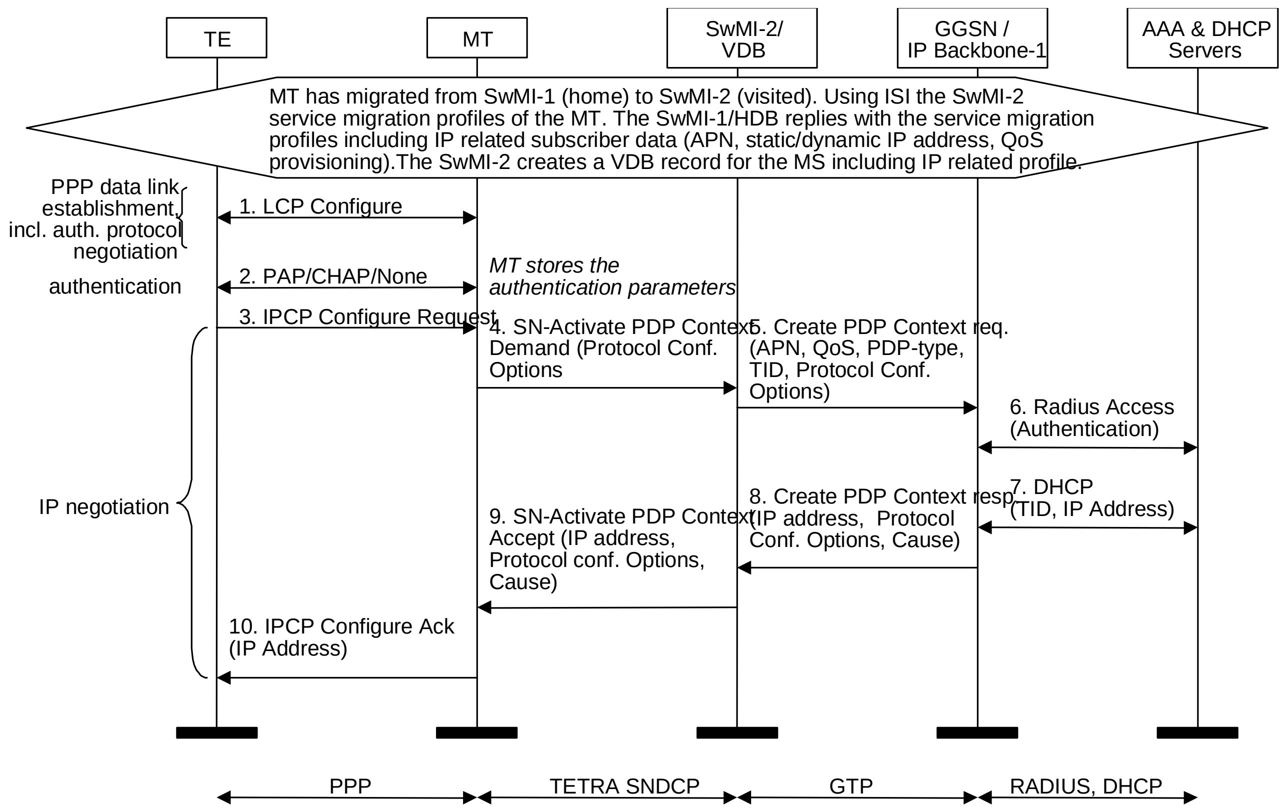


Figure A.2: A PDP Context is activated using AAA and DHCP Servers

Starting point:

- the MT has migrated from the home SwMI-1 to the visited SwMI-2. It registers to the visited SwMI-2 using a full ITSI;
- using ISI the visited SwMI-2 informs the home SwMI-1/HDB about the new location of the MT and requests the information needed in registration and service migration profiles of the MT. The home SwMI-1/HDB replies with the service migration profiles including IP related subscriber data (APN, optional APN indexes provisioned for the subscriber, static/dynamic IP address, QoS provisioning);
- after a successful registration the visited SwMI-2 creates a VDB record for the MT including IP related profile:

1) LCP negotiates the Maximum-Receive-Unit and the authentication protocol to be used. The negotiated authentication protocol is, CHAP, PAP or none. The MT shall try to negotiate for CHAP as first priority;

2) if the negotiated authentication protocol is either CHAP or PAP, the TE authenticates itself to the MT. The MT stores the necessary authentication data and sends a positive acknowledgement of the authentication to the TE;

3) the TE requests IP configuration by sending an 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;

4) the MT sends a SN-Activate PDP Context Demand to the SwMI-2, including the Protocol Configuration Options and optional APN index;

5) the SwMI-2 sends a Create PDP Context Request to the chosen GGSN including the unmodified Protocol Configuration Options. The APN used in the request is retrieved from the subscriber data in the VDB. (The APN is used to find the IP address of the GGSN in the IP Backbone of SwMI-1. DNS is used to translate the APN into the IP address.) If optional APN index is sent by the MT then the index is used when selecting APN from VDB;

6) the GGSN deduces from the APN:

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

   - the protocols like Radius and DHCP to be used with the server(s);

   - the communication and security features used with the server(s), e.g. tunnelling, security protocols like IPSEC, etc.

In this example, RADIUS is used for authentication and DHCP for host configuration and IP address allocation. The RADIUS server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN. Access-Accept is assumed here.

1) the DHCP client discovers the DHCP server(s) in the IP PDN (ISP/intranet) and receives an IP address and host configuration data for the TE;

2) the GGSN sends back to the SwMI-2 a Create PDP Context Response message containing the allocated IP address and Protocol Configuration Options. The cause value shall be set according to the outcome of the authentication and the host configuration;

3) depending on the cause value received in the Create PDP Context Response the SwMI-2 sends either a SN-Activate PDP Context Accept or a SN-Activate PDP Context Reject to the MT. Accept is assumed here;

4) MT sends an IPCP Configure Ack to TE and the link is open (or dropped if negotiation failed).

In case an IPCP Configure Ack packet is sent to the TE, the link from the TE to the external IP PDN (ISP/intranet) is established and IP packets may be exchanged.

Annex B (normative): Additions and extensions to ISI

The ISI MM shall be used for transferring IP related subscriber data when MS migrates. The following information shall be included in the IP service profile:

- default APN;
- APN index - APN pairs provisioned for the subscriber;
- static/dynamic IP address;
- QoS provisioning.

History

Document history		
V1.1.1	July 2001	Publication