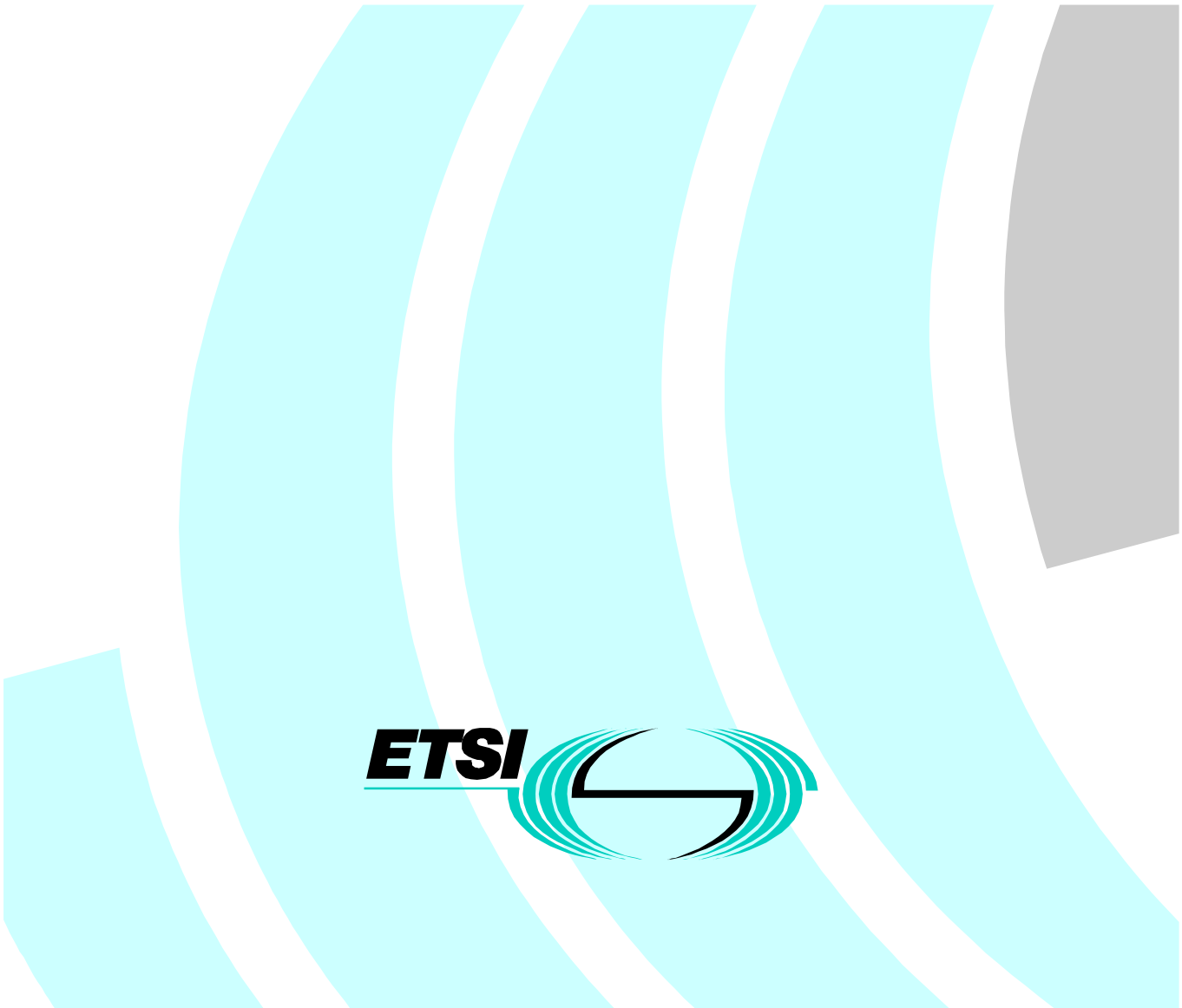
Draft ETSI EN 301 747 V1.1.1 (1999-08)

European Standard (Telecommunications series)

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



Reference
DEN/TETRA-03031 (g6c00ico.PDF)

Keywords
Internet, packet mode, security, TETRA,

ETSI

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - 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

Internet
secretariat@etsi.fr
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org
If you find errors in the present document, send your
comment to: editor@etsi.fr

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 SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

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

Foreword

This European Standard (Telecommunications series) has been produced by ETSI Project Terrestrial Trunked Radio (TETRA), and is now submitted for the Public Enquiry phase of the ETSI standards Two-step Approval Procedure.

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

1 Scope

The present document provides the definition of the Terrestrial Trunked Radio system (TETRA) Internet Protocol Interworking (IPI).

IPI for TETRA is intended to carry packet data between 2 TETRA SwMIs. This edition of the present document defines a method for carrying IP packets. The present document defines a means to support mobility for data communications by maintaining the service connection between the IP layers for the 2 scenarios below:

1) Migration between systems;

2) Connections between systems.

The present document defines a standard method of using published IP and TETRA protocols to provide the specific services required to support secure network to network connection for transfer of packet data, and for provision of mobility services to mobile hosts. The base models for these TETRA IPI services are mobile IP as defined in part by RFC2002, and TETRA ISI ANF-ISIMM as defined in ETS 300 392-3-5 [13]. In addition the packet data protocols described at the air interface shall apply.

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.

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

[2] ETS 300 392-5: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 5: Peripheral Equipment Interface (PEI)".

[3] RFC 1144: "Compressing TCP/IP Headers for Low-Speed Serial Links", V. Jacobson.

[4] ITU-T Recommendation V.42bis: "Data compression procedures for data circuit-terminating equipment (DCE) using error correction procedures".

[5] Wireless Application Protocol (WAP), Architecture Specification, Draft version 0.9 (1997-09).

[6] RFC 791 Internet Protocol, Version 4.

[7] RFC 1883 Internet Protocol, Version 6.

[8] RFC 2002, IP Mobility Support, C Perkins, October 1996.

[9] ETS 300 392-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".

[10] "Virtual Private Networking: An Overview", Microsoft Windows NT Server White Paper, Draft dated 18th March 1998.

[11] "Understanding PPTP", Microsoft Windows NT Server White Paper, 1997.

[12] ETS 300 392-3-3: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 3: Additional Network Functions Group Call (ANF-ISIGC)".

[13] 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 Functions Mobility Management (ANF-ISIMM)".

[14] ETS 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

[15] ITU-T 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".

3 Definitions 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.

Packet Data Channel (PDCH): control channel that is used to convey TETRA packet data datagrams.

Point to Point (PTP): mode of TETRA Packet data operation where the receiver end is an individual MS (characterized by ITSI) and IP packets are sent by using acknowledged service.

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

TETRA packet data: TETRA teleservice specified in this ETS. This version of the ETS describes how TETRA packet data may be used in conjunction with the Internet Protocol (IP). Future versions of this ETS may describe the operation of TETRA packet data with other higher layer protocols.

3.2 Abbreviations

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

ANF	Additional Network Function
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BS	Base Station
COMP	COMPression type identifier (for both header and data compression)
DLL	Data Link Layer
DNS	Domain Name Server
FEP	Front End Processor
FTP	File Transfer Protocol
GTSI	Group TETRA Subscriber Identity
HTTP	HyperText Transfer Protocol
IC	Individual Call
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPI	IP Interworking
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISDN	Integrated Services Digital Network
ISI	Inter System Interface

ISIMM	ISI Mobility Management
ISP	Internet Service Provider
ITSI	Individual TETRA Subscriber Identity
L2	Layer 2 (of protocol stack)
L3	Layer 3 (of protocol stack)
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunnelling Protocol
MIB	Management Information Base
MLE	Mobile Link Entity
MM	Mobility Management
MN	Mobile Node
MNI	Mobile Network Identity
MS	Mobile Station
NSAPI	Network layer Service Access Point Identity
PDCH	Packet Data Channel
PDP	Packet Data Protocol
PDU	Protocol Data Unit
PL-SAP	PEI DLL Service Access Point as defined in ETS 300 392-5 [2].
PPP	Point to Point Protocol
PPTP	Point To Point Tunnelling Protocol
PTP	Point to Point
QoS	Quality of Service
RFC	Request For Comment
SCK	Static Cipher Key
SDS	Short Data Service
SNDCP	Sub-Network Dependent Convergence Protocol
SSI	Short Subscriber Identity
SwMI	Switching and Management Infrastructure
TAxx	Tetra Algorithm xx (see ETS 300 392-7 [14])
TCP	Transmission Control Protocol
TSI	TETRA Subscriber Identity
UDP	User Datagram Protocol
V+D	Voice + Data, Refers to ETS 300 392-2 [1]
VPN	Virtual Private Network
WAP	Wireless Application Protocol

4 Reference scenarios

4.1 Introduction

A host on SwMI A wishes to communicate securely with a host on SwMI B. There are a number of scenarios:

- A host from SwMI A migrates to SwMI B and wishes to maintain all connections.
- A host from SwMI A registered to SwMI B wishes to establish a connection on SwMI B.
- A host from SwMI A registered to SwMI B wishes to establish a connection to SwMI A.

A host is defined as any device supporting a data application and may be a mobile user's MS, or a server computer in the SwMI.

There are two TETRA services to be provided at the IPI in order to support the above scenarios:

1) Mobility
2) Tunnelling
   - Dedicated path
   - Secure dedicated path

Tunnelling is the packet data network equivalent to call forwarding and may be invoked using a number of protocols. Within the Internet community as represented by the Internet Engineering Task Force (IETF) a number of drafts for standardization have been proposed. The IETF work on tunnelling falls in the family of Virtual Private Network (VPN) establishment protocols. ETSI may endorse standards or methods proposed by IETF by reference or by incorporation.

- Point-to-Point Tunnelling Protocol (PPTP).
- Layer 2 Forwarding (L2F).
- Layer 2 Tunnelling Protocol (L2TP).
- IPSec.

NOTE 1: PPTP has been defined by the following group of companies and has been proposed to the IETF as a standards track item: Microsoft Corporation, Ascend Communications, 3Com/Primary Access, ECI Telematics and US Robotics (who are now part of 3Com). This is an extension of PPP but is IP network specific (i.e. the tunnel is through an IP network only).

NOTE 2: L2F is a development made by Cisco and is router based and may use many protocols.

NOTE 3: L2TP is a development by IETF to combine the best features of L2F and PPTP that allows tunnelling through X.25 [15], Frame-relay and ATM networks.

NOTE 4: IPSec is the Ipv6 approach to VPN and tunnelling.

4.2 IPI architecture

There are a number of ways to view the IPI architecture. The proposal of the present document is to view each SwMI as an autonomous Internet Service Provider (ISP). The IPI connection and the services it provides to each TETRA IP host (MS) requires that each ISP provides the following:

- A tunnel client or ISP Front End Processor (FEP).
- A tunnel server.
- The tunnel is intended to establish a point to point link between two SwMIs. For connections between two participating SwMIs the tunnel shall be established either on the first migration of a user whose profile indicates that the ITSI is a user of IP services. In order to restrict the number of tunnels established the ISP shall be responsible for establishing the tunnel. This will limit the number of managed points of egress from the SwMI/ISP and should assist in maintaining security.. This is termed "compulsory tunnelling" as the host is mandated to use the tunnel established by the ISP. A compulsory tunnel shall be shared between all users of the inter-network connection.

4.3 Overview of IPI operation

IPI shall be invoked by the MLE/MM/PDP-Context process of the visited TETRA ISP when either of the following conditions is true:

- A foreign mobile host registers and requests IP service.
- A mobile host requests service from another TETRA ISP.

The IPI operations shall establish a transient virtual network. The connections between ISPs on this network shall be established using the protocols and tunnelling operations described in 4.1. The physical interconnection may be by means of X.25 [15], ISDN, ATM or other layer 2/1 interconnections.

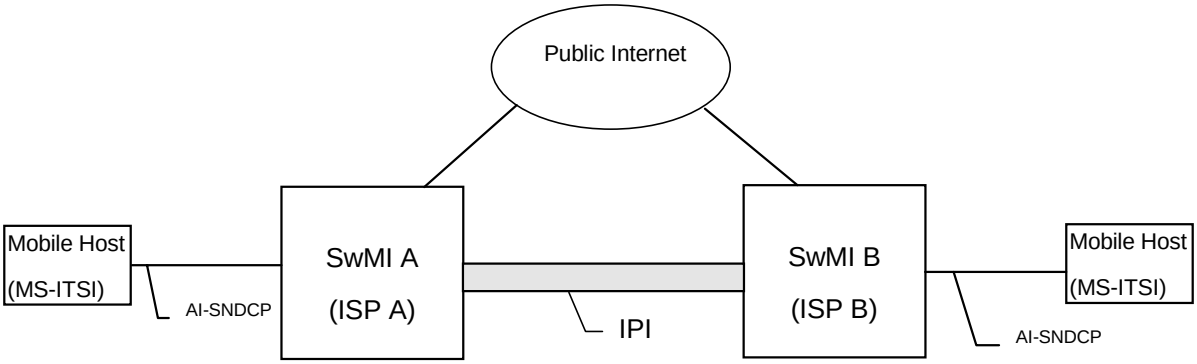


Figure 1: Basic IP interworking scenario for IPI

4.4 IPI Functional Entities and Reference Points

Figure 2 depicts the functional entities and reference points which are subject to standardization in this specification.

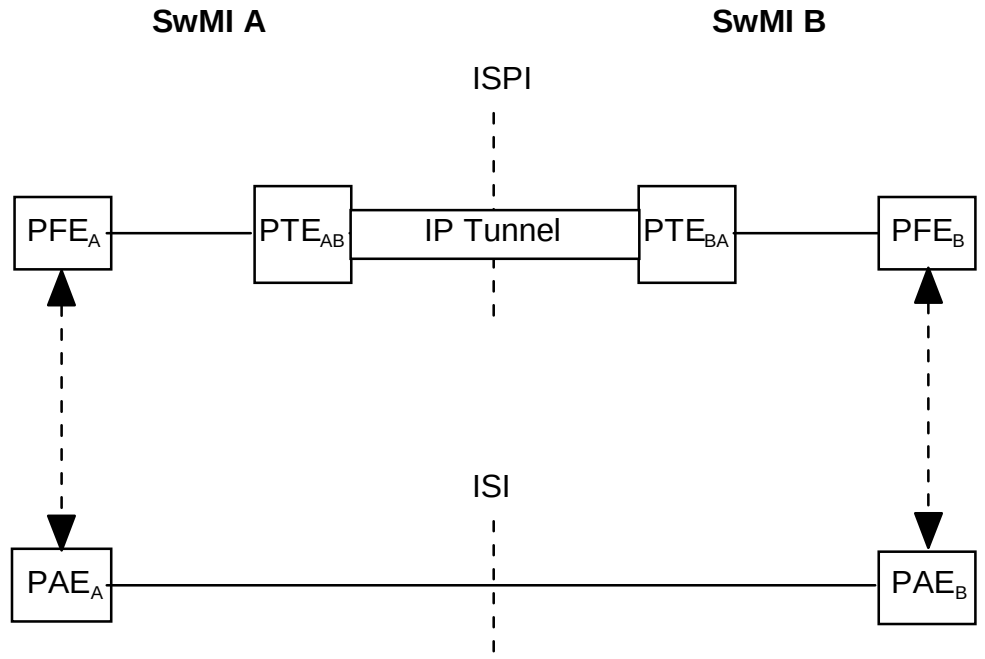


Figure 2: IPI Functional Entities and Reference Points

The Provisioning and Authentication Entity (PAE) is functionally a subset of MM (and ANF-ISIMM). PAE/MM is covered by the IPI only insofar as clause 7 acts as an input to ANF-ISIMM (ETS 300 392-3-5 [13]) and to the air interface description (ETS 300 392-2 [1]).

The Packet Tunnelling Entity (PTE) is functionally provided by the IPI-SAP. This is wholly covered by the IPI and the protocol describing the interaction of peer PTE entities is the subject of the IPI standard.

The Packet Forwarding Entity (PFE) is functionally provided by the TNL-SAP. This is covered by the IPI standard as a set of capabilities described by the primitives issued by the IPI layer to the TNL layer.

The SNDCP Network Endpoint (SNE) is the entity within the TETRA SwMI which terminates SNDCP over the TETRA Air Interface. This functional entity is also viewed as the device responsible for negotiating packet data parameters (such as MS IP address) during SNDCP Context Activation. The SNE shall not be subject to standardization within this IPI specification.

5 Addressing

There are a number of addressing scenarios to be considered for IPI operations.

In order to maintain individual control of IP address space the use of Network Address Translation (NAT) technology is recommended (see informative annex A for identification of further reference material). This shall allow protection of the address space of each ISP whilst making a public address known both to the global Internet and to the remote end of the tunnel.

5.1 Scenarios

This section addresses the scenarios to be considered by this specification.

5.1.1 a1.A to b1.B

MS which is at home in SwMI A communicating with a MS which is at home in SwMI B. SwMI A intercepts all packets destined for SwMI B and forwards them over the IPI. Likewise, SwMI B intercepts all packets destined for SwMI A and forwards them over the IPI.

5.1.1.1 Impact of Addressing Used

If we assume that the address assigned to a1.A is from SwMI A's address plan (i.e. identifiable as belonging to SwMI A) and the address assigned to b1.B is from SwMI B's address plan irrespective of whether the assigned address is static, dynamic or a Mobile IP COA, then addressing does not change the scenario. It is the responsibility of a1.A to find the address of b1.B (through DNS or other) and for SwMI A to recognize the address of b1.B as requiring forwarding over the IPI to SwMI B. Likewise for packets flowing from b1. B to a1.A.

The specification needs to consider this scenario when public addressing only is used by both SwMIs, when private address is used by both SwMIs with non-overlapping address spaces and when private address is used by both SwMIs with overlapping address spaces.

5.1.2 a1.A to a2.B

MS which is at home in SwMI A communicating with a MS which has migrated from its home in SwMI A to SwMI B. Note that the with various scenarios presented below, the addresses used by SwMI A and SwMI B may be public, private non-overlapping or private overlapping.

5.1.2.1 a2.B uses a Static (SwMI A) Address on SwMI B

On SwMI B, a2 requests use of a static address at context activation. The static address which it requests belongs to the address range of SwMI A. If SwMI B does not support the usage of this static address, then the context will be rejected. Otherwise, SwMI B shall check with SwMI A if a2 is permitted to use this static address. If SwMI A responds in the negative, then the context is rejected. If SwMI A responds in the affirmative, then the context may be accepted and a2 may use this address while this context remains active.

5.1.2.2 a2.B uses a Dynamically Assigned (SwMI B) Address on SwMI B

On SwMI B, a2 requests and is assigned a dynamic address from the range of addresses used by SwMI B.

5.1.2.3 a2.B uses a Mobile IP Foreign Agent Care of Address on SwMI B

On SwMI B, a2.B requests a Mobile IP Foreign Agent Care Of Address (COA) at context activation. If SwMI B supports the use of a Mobile IP Foreign Agent COA, then the context accept message shall include the IP address of the Foreign Agent located within SwMI B. a2.B will then perform Mobile IP registration with its Home Agent (optionally via the Foreign Agent). The Home Agent will be located in SwMI A 3. Once the Home Agent accepts the Mobile IP registration, all further packets arriving at the Home Agent will tunnelled to the Foreign Agent and then forwarded to a2.B.

5.1.2.4 a2.B uses a Mobile IP Co-located Care of Address on SwMI B

On SwMI B, a2.B requests a Mobile IP Co-located COA at context activation. If SwMI B supports Mobile IP Co-located Care of Addresses, then the context accept message shall include a dynamically assigned IP address which a2.B shall use as its Mobile IP Co-located COA. A2.B will then perform Mobile IP registration with its Home Agent. The Home Agent will be located in SwMI A. Once the Home Agent accepts the Mobile IP registration, all further packets arriving at the Home Agent will tunnelled directly to a2.B using the Co-located COA (i.e. tunnel extends over the air interface).

5.1.3 a2.B to b1.B

MS which is at home in SwMI B communicating with a MS which has migrated from its home in SwMI A to SwMI B. As all traffic originating from a2.B may be required to be forwarded back to SwMI A, then this scenario should be considered.

5.1.4 a1.B to a2.B

Two MSs which have migrated from their home in SwMI A to SwMI B. As with the previous scenario, as all traffic originating from a1.B and a2.B may be required to be forwarded back to SwMI A, then this scenario should also be considered.

6 IPI protocol

In providing IPI mobility the requirement from higher layer applications is that the service is maintained.

For higher layer services such as HTTP or FTP the combination of IP address and TCP/UDP port address is required to be static within a session. This is referred to as socket continuity.

Table 1: IPI Server state machine, state descriptions

State	Description
IDLE	No tunnel established, awaiting context activation requests from MS at AI
TUNNEL-PENDING	Tunnel being established
TUNNEL-ACTIVE	Tunnel available for particular ISP to ISP link

The following transitions between states (event in the form of a message) are allowed.

Table 2: IPI Server state machine, state transitions

Initial State	Event	New State	Remark
IDLE	IPI_Context_Activation_req	TUNNEL-PENDING	Allows tunnel to be established when a user migrates and his "home" is at another SwMI
IDLE	IPI_Data_Transfer_req	TUNNEL-PENDING	Allows tunnel to be established on demand of a data transfer between the two SwMI/ISPs
TUNNEL-PENDING	IPI_Tunnel_Active_conf	TUNNEL_ACTIVE	This is the positive response from the tunnel management process that the tunnel has been established.
TUNNEL-ACTIVE	IPI_Context_Activation_req	TUNNEL-ACTIVE	No change in IPI state, reset IPI keep awake timer Increment active context counter
TUNNEL-ACTIVE	IPI-Timer_expiry	IDLE	Stay alive time has expired, therefore the tunnel will be closed.
TUNNEL-ACTIVE	IPI_Data_Transfer_req	TUNNEL-ACTIVE	No change in IPI state, reset IPI keep awake timer
TUNNEL-ACTIVE	IPI_Context_DeActivation_req	TUNNEL-ACTIVE	Decrement active context counter
TUNNEL-ACTIVE	Context_count_zero_ind	IDLE	No active contexts exist so tunnel is closed (after timer expires ?)

The IPI_Context_activation_req may be initiated by one of the following sources:

1) The MS when making a context activation request over the air interface;

2) The MM process of the SwMI when registering a migrated user in which the profile of that user indicates that packet data services (IP services) are provided by the home SwMI.

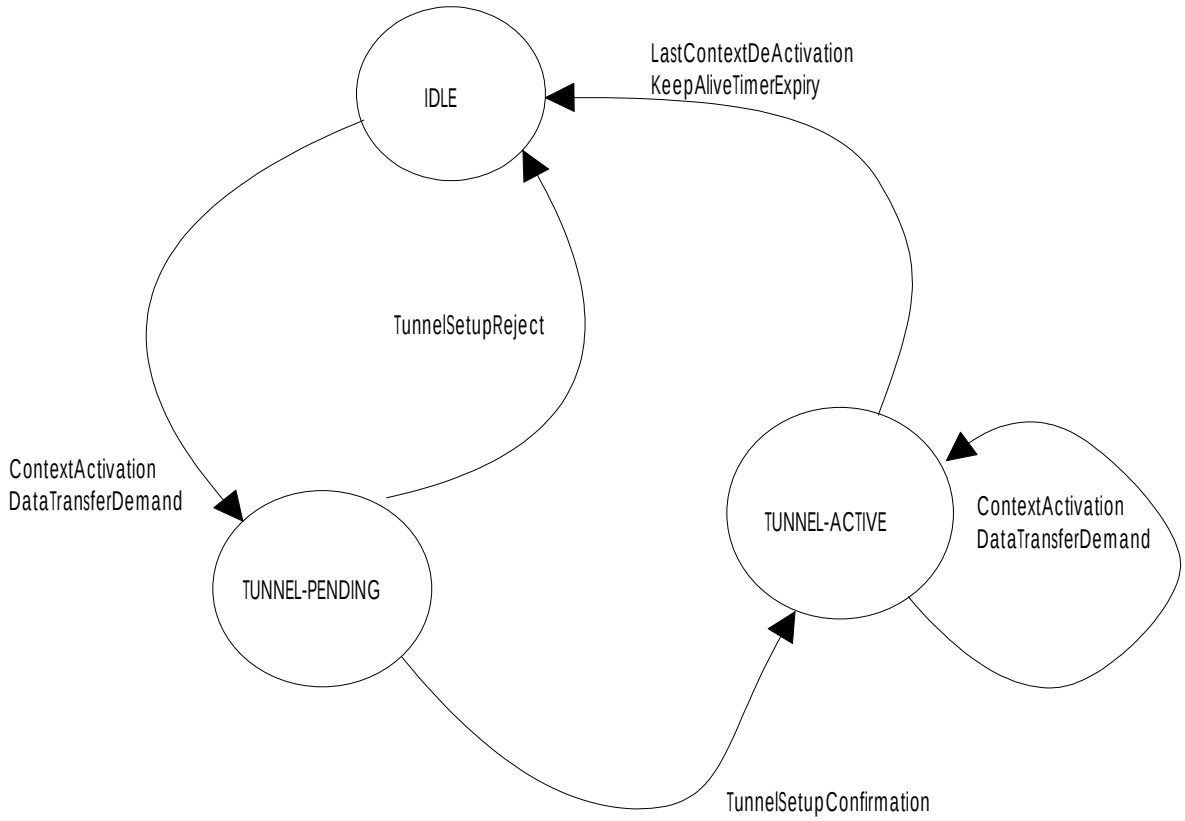


Figure 3: Simplified state diagram of IPI

The state diagram shown in 3 can be formalized described using SDL. In order to allow the SDL model to work a functional model of IPI is required. This is done in the present document in 2 stages:

1) A service model showing the primitives through which an application can communicate with the service;

2) A functional entity diagram.

The service model, shown in figure 4, defines a 2 layer service. The layer visible to the SwMI is the IPI Service layer, which communicates with the Tunnel Service layer. Access to the facilities of the tunnel shall only be provided in a SwMI through the IPI Service Layer and shall provide the following services:

- Context Activation.
- Context DeActivation.
- Data Transfer.

In addition the IPI Service Layer shall be able to indicate the state of the tunnel to the SwMI by indicating when no contexts are attached to the tunnel, and when the tunnel activity timer has expired.

The Tunnel Service layer shall provide a point to point IP carriage service using IP encapsulation. The service model shows the primitives used by the IPI Service Layer to communicate with the Tunnel Service layer. These primitives will not be fully described in the present document as their form may vary with the specific tunnel mechanism chosen. Instead these primitives shall be used to indicate the service requirements of a Tunnel protocol from the point of view of the IPI Service layer.

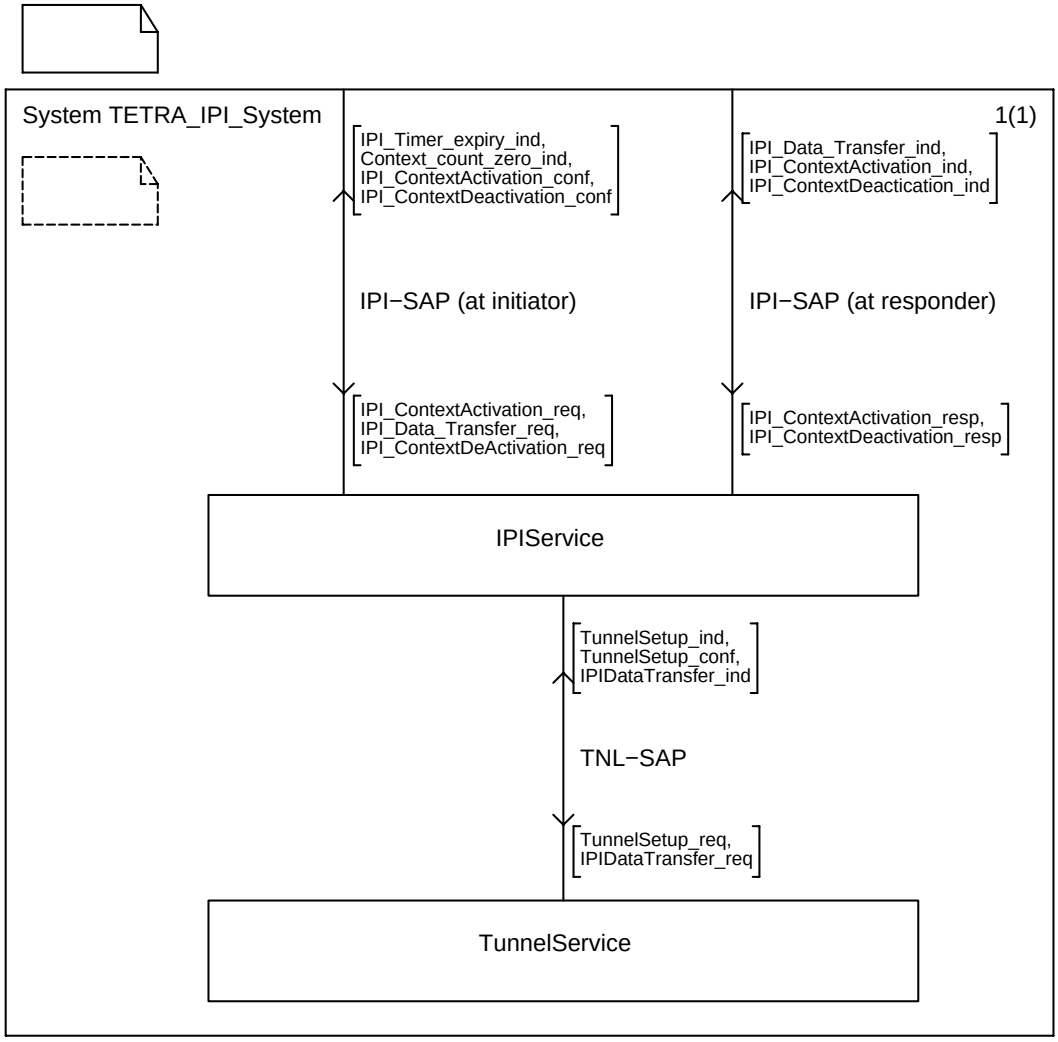


Figure 4: Service model of IPI

6.1 Overview of the IPI Service primitives

The primitives shown in figure 4 are more fully described in table 3.

Table 3: IPI Service primitives

Primitive name	Parameters	Request	Confirm	Indication	Response
IPI_ContextActivation	TETRA L3 Protocol	M	M	M	M
	IP Service	M	-	-	-
	Context Handle	-	M		M
	User ITSI	M			
	Home SwMI MNI	M	M		
	Visited SwMI MNI	M	M		
IPI_DataTransfer	Context Handle	M	-	M	-
	S-PDU	M	-	M	-
IPI_ContextDeActivation	Context Handle	M	M	M	M

The parameters may then take the following meanings (no encoding is given at this point):

TETRA L3 Protocol =

SNDCP (i.e. the MS is using IP at the air interface)

IP Service =

Ipv4, static address

Ipv4, dynamic address

Ipv6

Mobile IP

S-PDU =

As appropriate to TETRA L3 protocol

NOTE: The tunnel encapsulates the S-PDU and Context handle in an IP packet and delivers it to the peer L3 entity. Therefore the S-PDU can be of any format that fits to an IP envelope.

6.2 SDL model of IPI

The following SDL model (shown in figures 5, 6 and 7) of the state transitions shows the expansion of the basic state diagram of figure 3 to consider how the primitives shown in figure 4 are used.

The SDL is shown from the point of view of the IPI Service at the initiator side. Error conditions are not shown in any detail. Data checking is not shown in any detail.

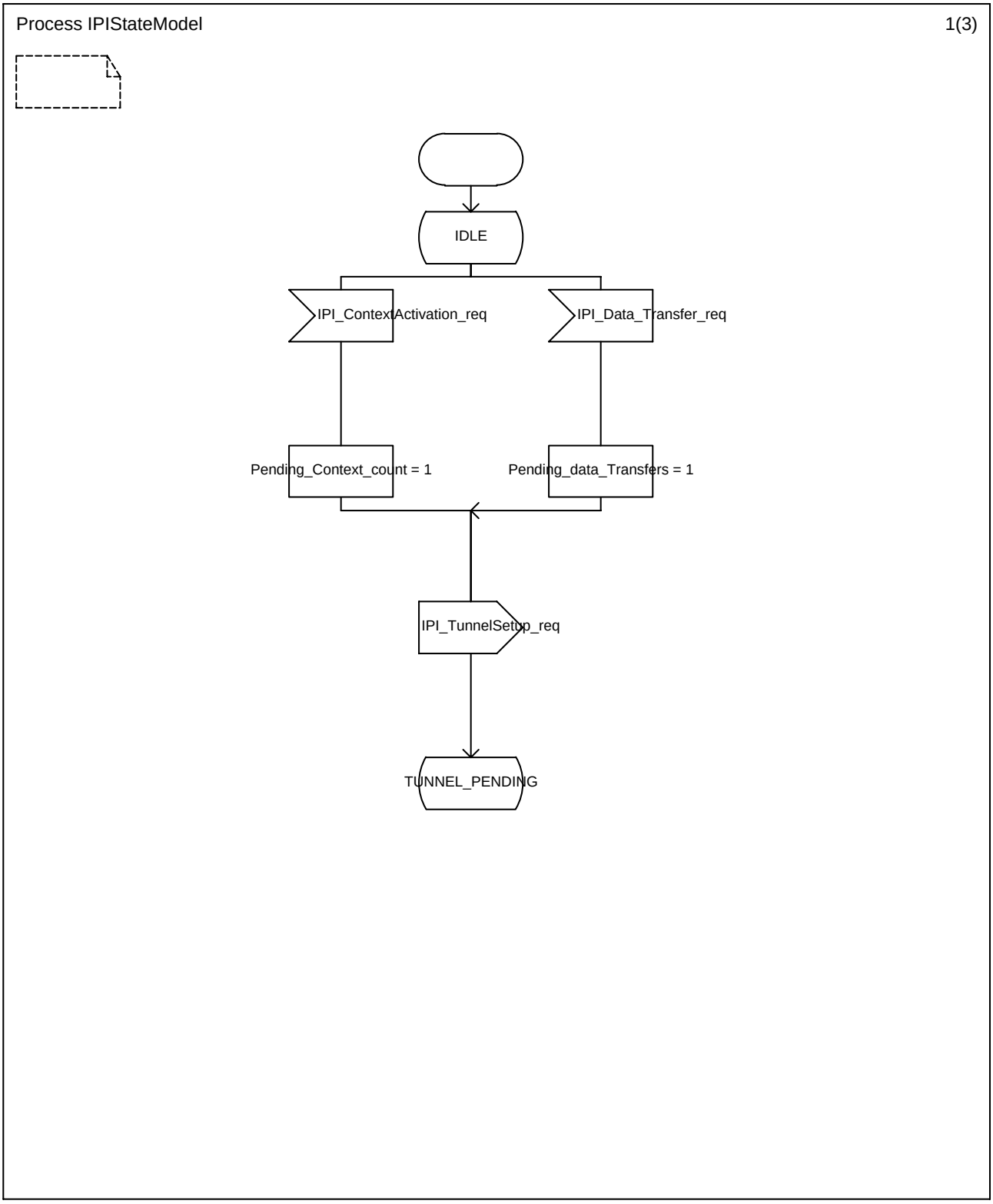


Figure 5: SDL of state transition model of IPI (Page 1 of 3)

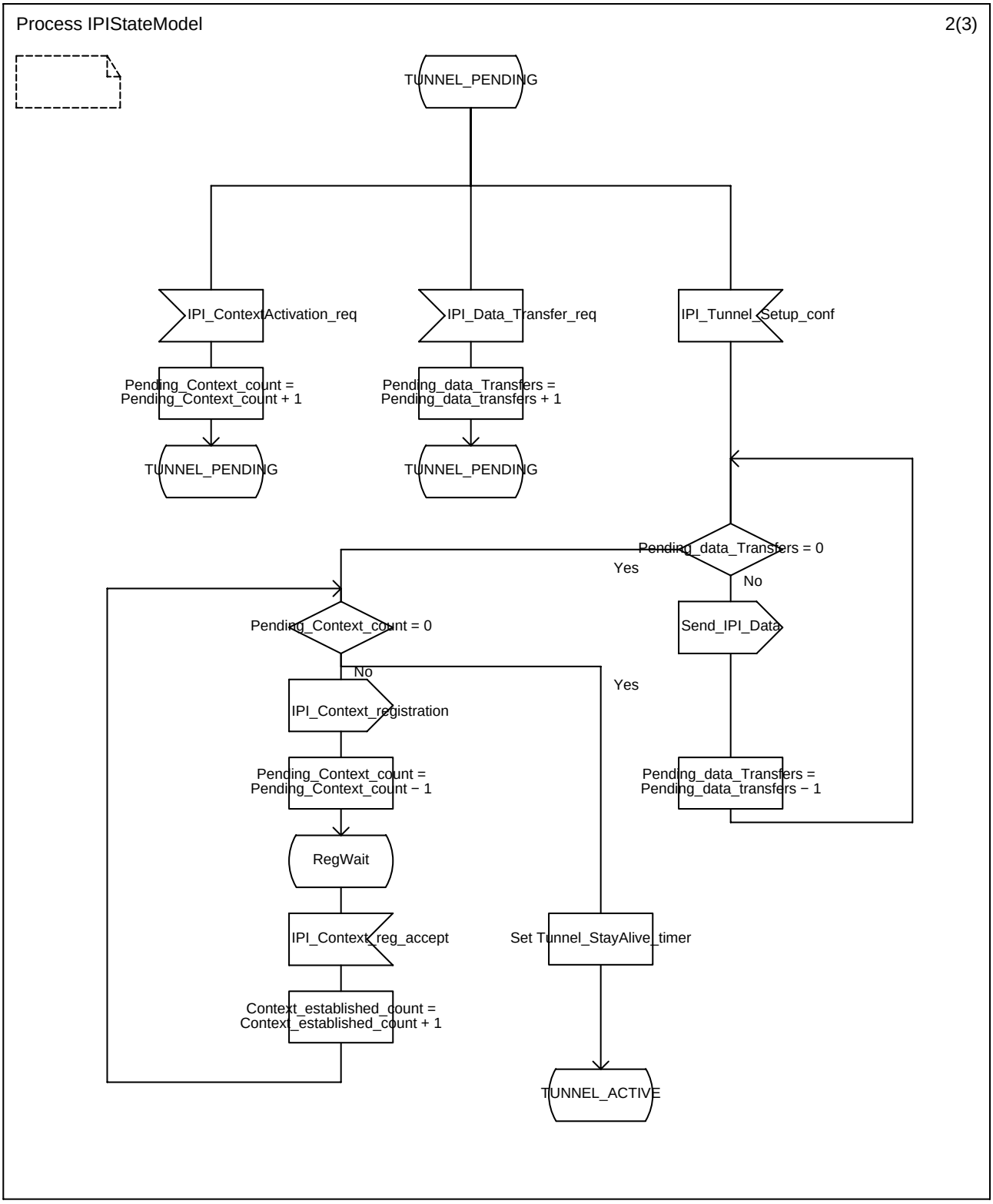


Figure 6: SDL of state transition model of IPI (Page 2 of 3)

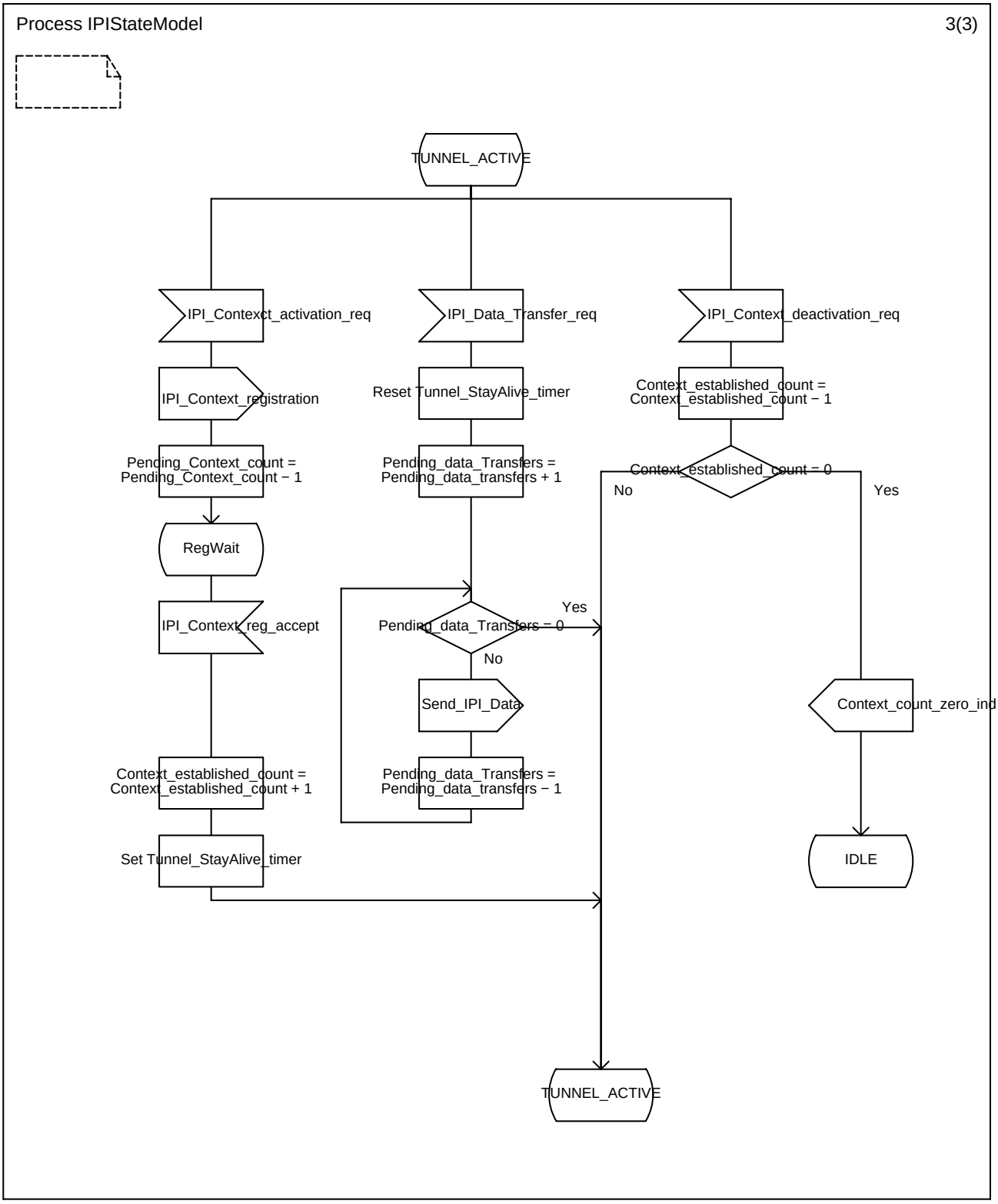


Figure 7: SDL of state transition model of IPI (Page 3 of 3)

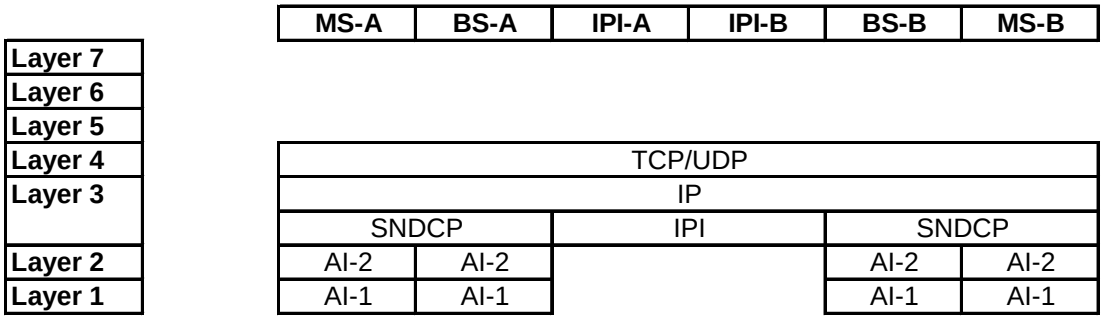


Figure 8: ISO/OSI layer model of IPI

In terms of the service being provided the model (shown in figure 4) is seen as a set of primitives made available to the service user. Which primitives apply depends upon the role of the user (e.g. initiator of the IPI or responder to it).

The service model shows two layers:

1) IPI;

2) Tunnel.

The intention is that IPI acts as a layer on top of a commercially available, or IETF standard, tunnel, and interacts with it through its published service primitives. The implication is that a tunnel is established on request of IPI and is then able to encapsulate the IPI data transfer and IPI Context registration commands so that they can be carried transparently to the peer IPI entity. The IPI layer itself acts for the TETRA mobile user and interfaces that user to the tunnel.

6.3 MSCs of IPI operations

The Message Sequence Charts (MSCs) shown in figures 9 through to 12 show how the user application in the SwMI uses the IPI Service primitives to communicate across the IPI Interface.

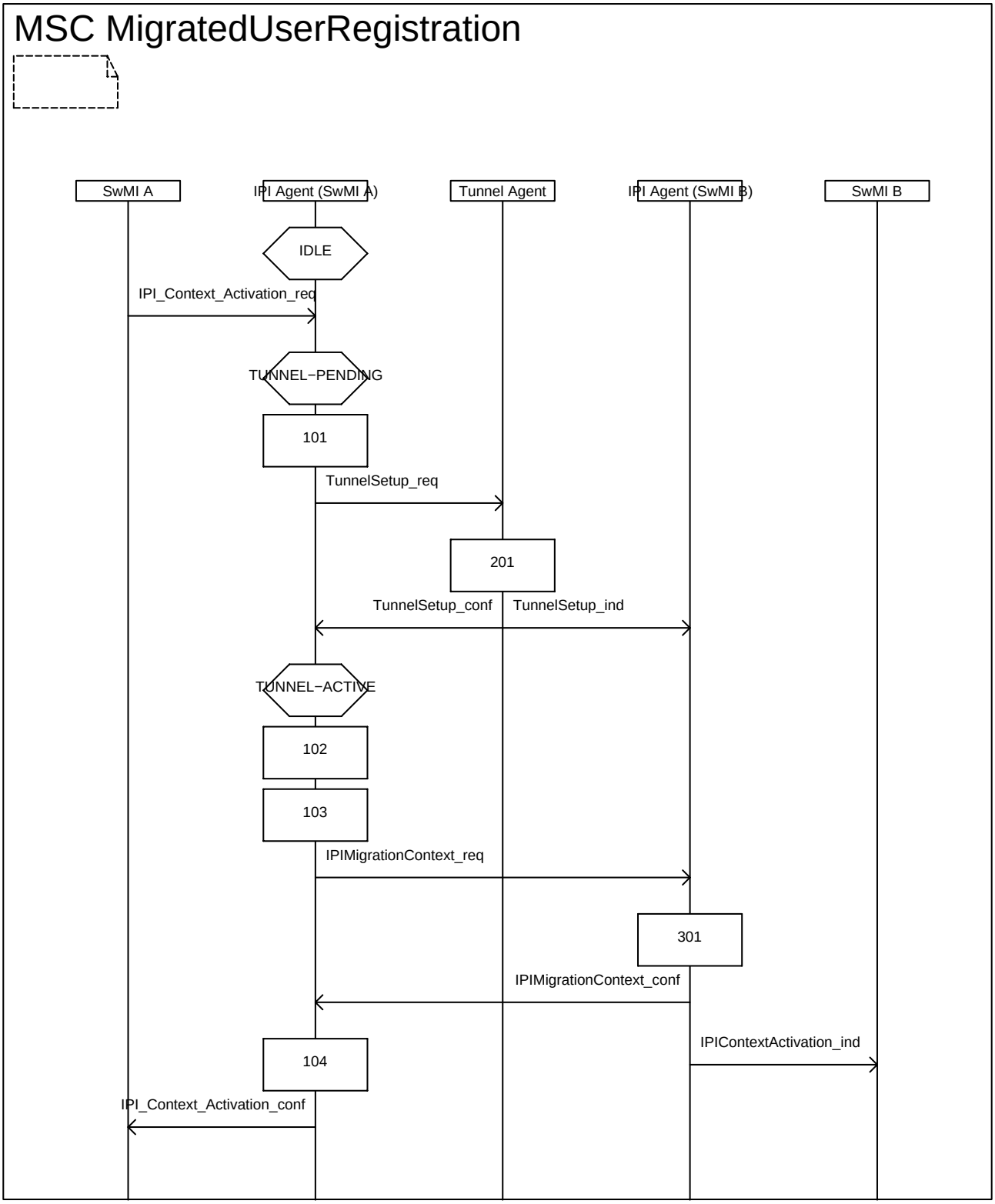


Figure 9: MSC for first migrated user of IPI establishing context

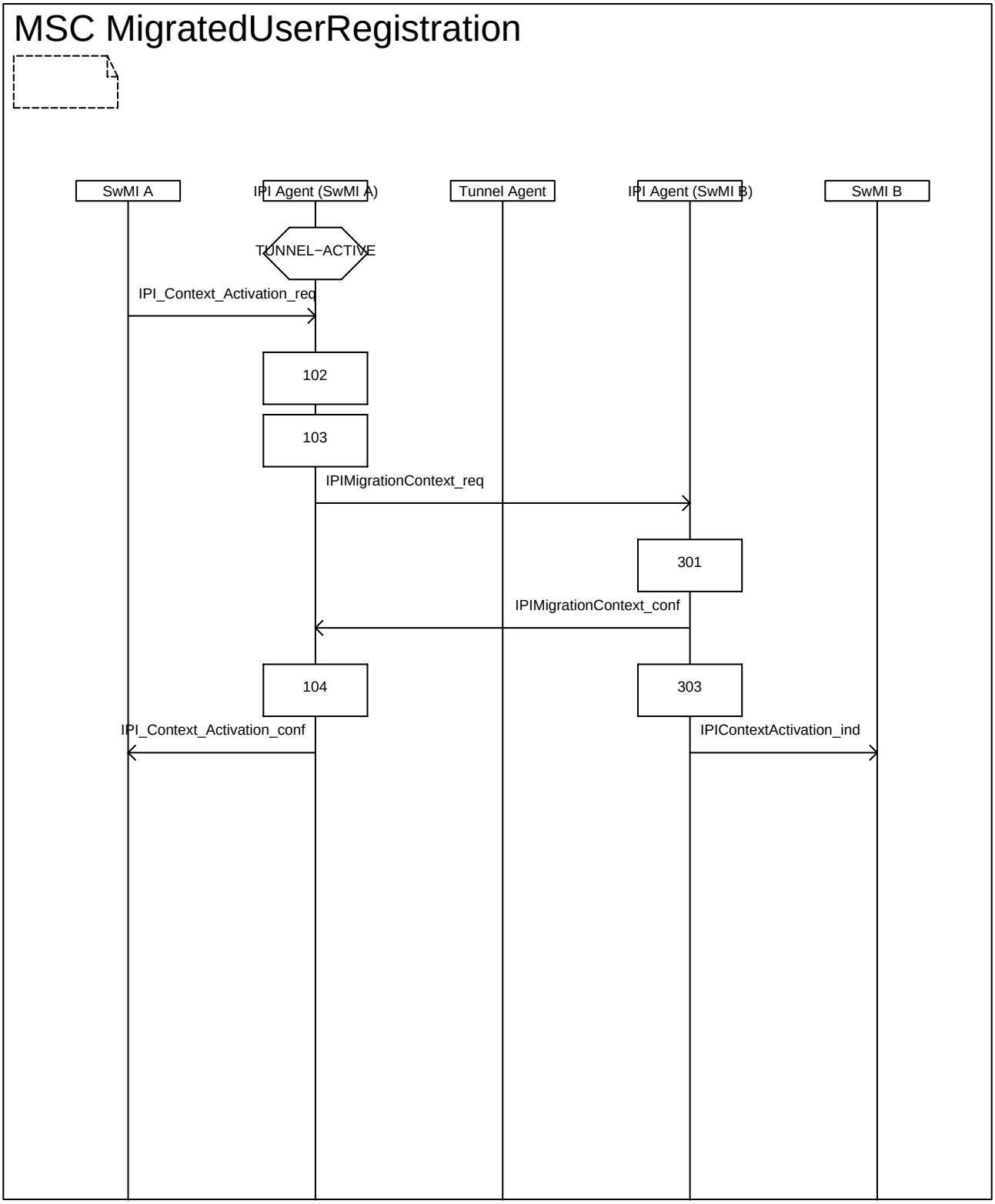


Figure 10: MSC for subsequent migrated user of IPI establishing context

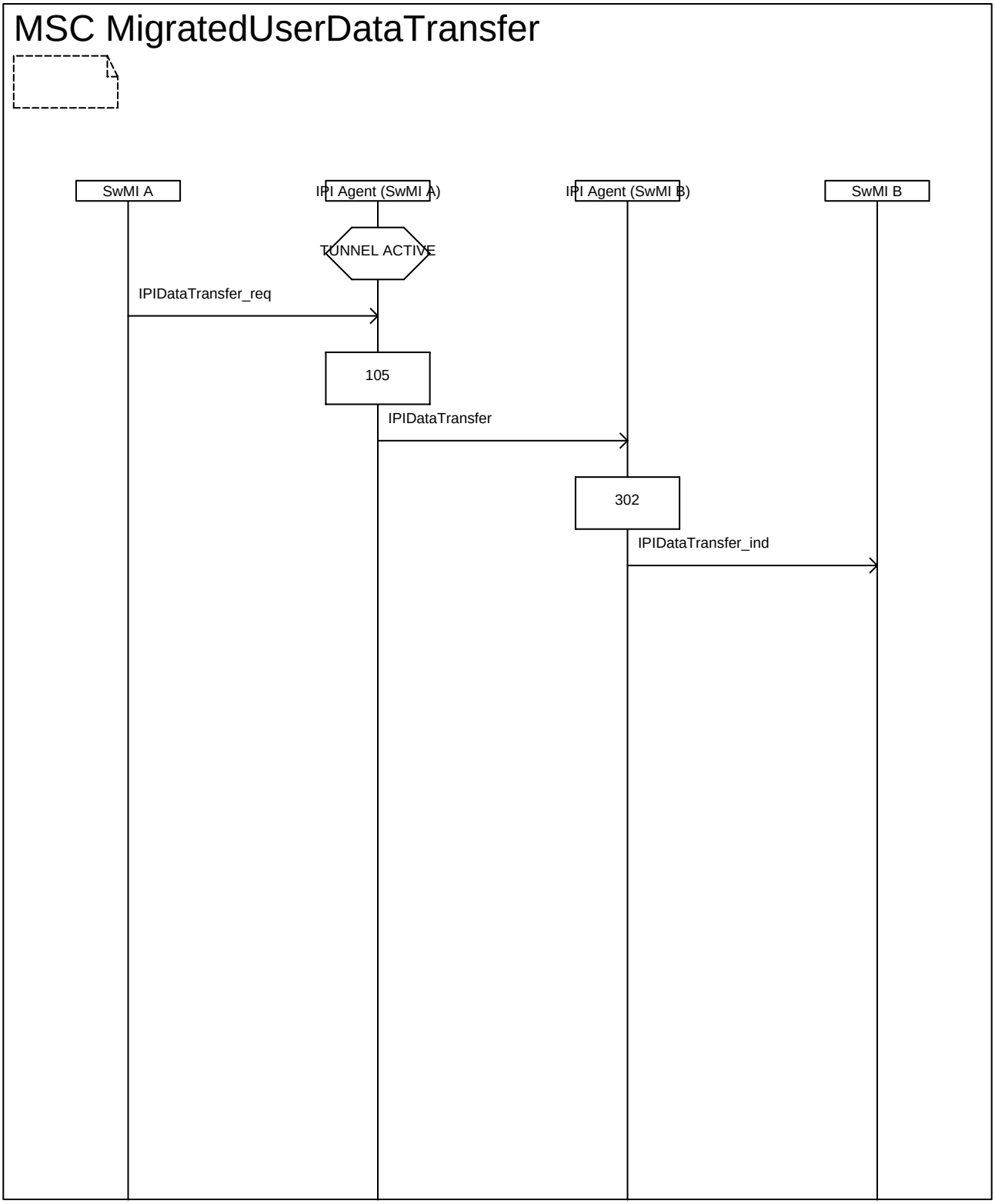


Figure 11: MSC for a migrated user transferring a data packet (unacknowledged service)

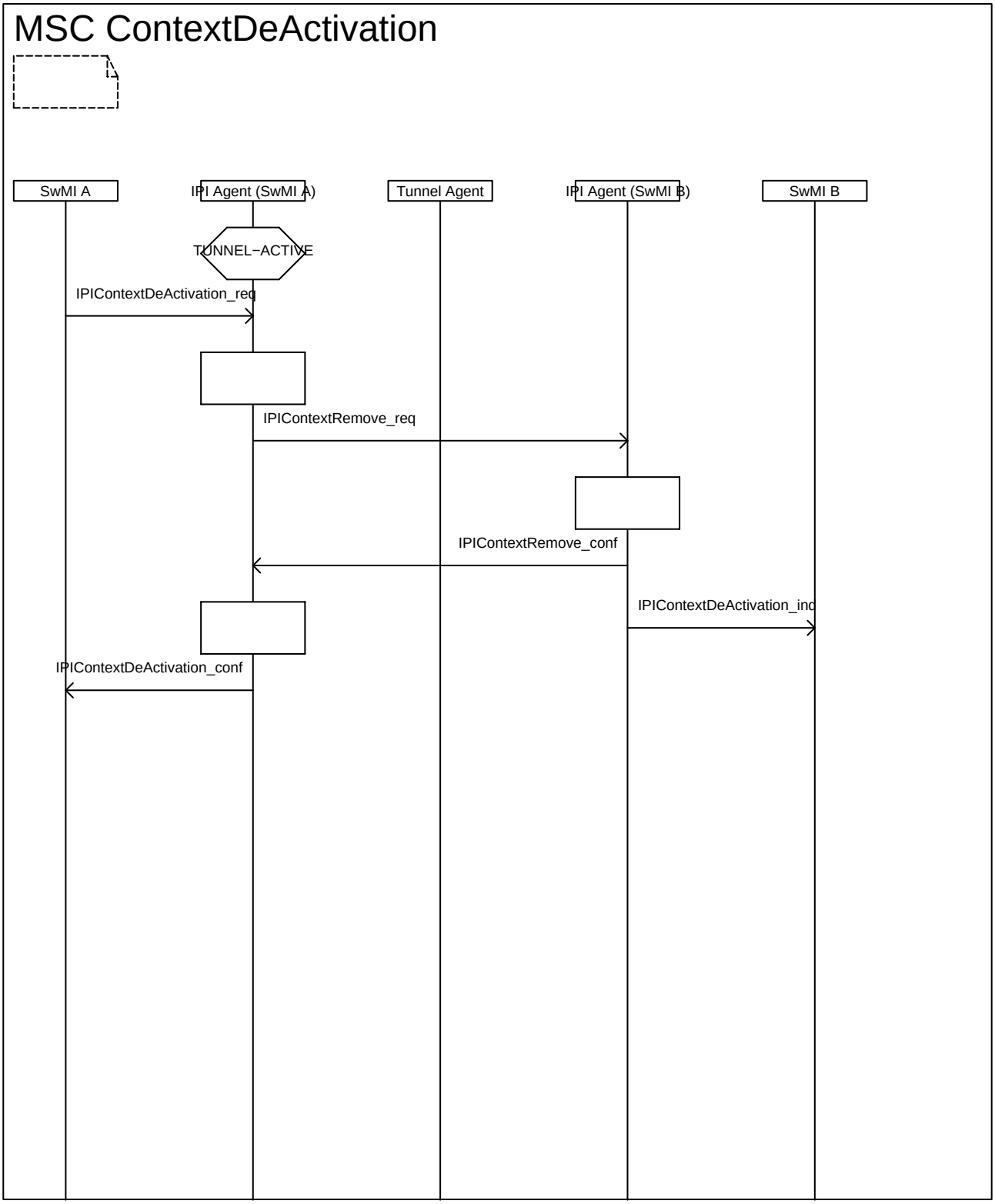


Figure 12: MSC for a migrated user deregistering

6.3.1 Actions of IPI Agent at migrated to SwMI

0) Receives IPI_Context_activation_req from MM agent in SwMI. This shows the home SwMI of the migrated user. The IPI Agent translates the hSwMI MNI into a gateway (tunnel server) IP address and then requests the local TunnelAgent to establish a tunnel to that address.

1) Receives confirmation from the local TunnelAgent that there is now a tunnel to the hSwMI of the migrated user.

2) Sends IPIMigrationContext_req to the peer IPI Agent on the user's hSwMI using the tunnel.

3) Receives an IPIMigrationContext_conf from the peer IPI Agent allowing the user to establish a local IP context and therefore indicating that IP data for that user shall be tunnelled to the visited SwMI for local routing. This is indicated to the SwMI using the IPI_Context_Activation_conf message.

4) Tunnel is active. Data transfer request from the user is sent via the tunnel to the peer IPI agent.

6.3.2 Actions of Tunnel Agent at migrated to SwMI

0) Receives TunnelSetup_req from to establish an IP tunnel to the indicated SwMI. When established the local SwMI is informed with the TunnelSetup_conf message and the remote SwMI is informed using the TunnelSetup_ind message.

6.3.3 Actions of IPI Agent at home SwMI

0) Receives IPIMIgrationContext_req from the peer agent in the remote SwMI. Interacts with the local MM to validate the Migrated service request. If accepted updates routing tables to point to the tunnel for the migrated user and confirms the routing using the IPIMigrationContext_conf message.

1) On receipt of an IPIDataTransfer_ind this is stripped of any tunnel specific encoding and given to the SwMI in a IPI_Data_transfer_ind primitive.

6.4 Protocol Data Units of TETRA IPI

The primitives shown in table 3 shall be delivered peer-to-peer between the PTEs as PDUs described in this subclause. Each PDU shall be encapsulated in an IP packet. The source address of the encapsulating IP packet shall be the public IP address of the Tunnel client. The destination address of the encapsulating IP packet shall be the public address of the Tunnel server.

Table 4: Mapping of service primitive to PDU

Service Primitive	PDU
IPI_ContextActivation req/ind	IPI_Context_Activation_Demand
IPI_ContextActivation conf/resp	IPI_Context_Activation_Accept
IPI_DataTransfer req/ind	IPI_Data_Transfer
IPI_ContextDeActivation req/ind	IPI_Context_DeActivation_Demand
IPI_ContextDeActivation conf/resp	IPI_Context_DeActivation_Accept

The source in each case in a confirmed information flow shall be a primitive of subtype request (req) that shall invoke the sending of the PDU. The received PDU shall be delivered to the destination application using the primitive subtype indication (ind). The confirmation shall be sent by the confirming node (the original destination) using the primitive subtype response (resp) to invoke the sending of the PDU which when received shall be delivered to the application using the primitive subtype confirmation (conf).

6.4.1 IPI_Context_Activation_Demand

Response expected IPI_Context_Activation_Accept

Table 5: IPI Context Activation Demand

Information element	M/O/C	Type	Size	Remark
IPI PDU type	M	1	3	000_2
User ITSI	M	1	48	
Home SwMI MNI	M	1	24	
Visited SwMI MNI	M	1	24	
Source handle	M	1	24	

6.4.2 IPI_Context_Activation_Accept

Response expected None

Table 6: IPI Context Activation Accept

Information element	M/O/C	Type	Size	Remark
IPI PDU type	M	1	3	001_2
Source handle	M	1	24	
Activation result	M	1	1	
Destination handle	C	1	24	If result is success

6.4.3 IPI_Data_Transfer_Demand

Response expected None

Table 7: IPI Data Transfer Demand

Information element	M/O/C	Type	Size	Remark
IPI PDU type	M	1	3	010_2
Source handle	M	1	24	
Destination handle	M	1	24	
Data packet	M	1	varies	IP packet

6.4.4 IPI_Context_DeActivation_Demand

Response expected IPI_Context_Activation_Accept

Table 8: IPI Context Deactivation Demand

Information element	M/O/C	Type	Size	Remark
IPI PDU type	M	1	3	011_2
Source handle	M	1	24	
Destination handle	M	1	24	

6.4.5 IPI_Context_DeActivation_Accept

Response expected None

Table 9: IPI Context Deactivation Demand

Information element	M/O/C	Type	Size	Remark
IPI PDU type	M	1	3	100_2
Result	M	1	1	

6.5 Information element encoding

The information elements identified in subclause 6.4 shall be encoded as shown in this subclause.

NOTE: Encoding of MNI, ITSI, and IP addresses are not shown in this subclause.

6.5.1 IPI PDU Type

Table 10: Encoding of IPI PDU Type information element

Information element	Size	Value	Remark
IPI PDU type	3	000	IPI_Context_Activation_Demand
		001	IPI_Context_Activation_Accept
		010	IPI_Data_Transfer
		011	IPI_Context_DeActivation_Demand
		100	IPI_Context_DeActivation_Accept
		101	Reserved
		110	Reserved
		111	Reserved

6.5.2 Result

Table 11: Encoding of Result information element

Information element	Size	Value	Remark
Result	1	0	Fail
		1	Success

6.5.3 Source/Destination Handle

Table 12: Encoding of Source/Destination Handle information element

Information element	Size	Value	Remark
Handle	24	any	Unique to source or destination domain

7 Interaction with ANF-ISIMM

7.1 Extension to profile

The profile exchanged between two SwMIs at migration registration shall be extended with the following optional fields. These fields shall be treated as mandatory when a subscriber is registered to use the IP service invoked by the SNDCP service.

This paper identifies additional data to be added to the ANF-ISIMM profile used in migration exchange to support IPI.

7.1.1 Modified tables

This updates table 128 of the public enquiry version of ANF-ISIMM (ETS 300 392-3-5 [13]) to include extended IP data. In addition the table includes a modification to add, as an optional item, the MSISDN of the subscriber. Note that the MSISDN has also be added to the primitives in table 40 of ETS 300 392-3-5 [13].

The updated encoding of the individual basic migration profile (original and temporary) shall be as defined in table 13.

Table 13: (cf. table 128 from ETS 300 392-3-5 [13]) Individual basic migration profile contents

Information element	Length	Type	C/O/M	Remark
Profile status	2	1	M	
MSISDN provision flag	1	1	M	
MSISDN	60	1	C	If flag is True
Point-to-point call service	2	1	M	
Point-to-multipoint call service	2	1	M	
Point-to-multipoint acknowledged call service	2	1	M	
Point-to-multipoint broadcast service	2	1	M	
Speech service	5	1	M	
Circuit mode unprotected data service	2	1	M	
Circuit mode protected (low) data service	2	1	M	
Circuit mode protected (high) data service	2	1	M	
Interleaving depth	5	1	M	
Duplex service	2	1	M	
CONS	2	1	M	
SCLNS	2	1	M	
IP service	2	1	M	
Authentication service	2	1	M	
OTAR SCK generation service	2	1	M	
OTAR SCK delivery service	2	1	M	
AI encryption state list	5	1	C	note 1
End-to-end encryption service	2	1	M	
Number of SS-information	6	1	M	
SS-information	8	1	C	note 2
SS-information response	8	1	C	note 3
Default SS-information	2	2	O	
SDS profile	6	2	O	
Advanced link service	2	2	O	
Maximum number of timeslots	3	2	O	
Call time-out timer (T310)	4	2	O	
Call time-out set-up phase timer (T301)	3	2	O	
Group information	44-*		C	note 4
Proprietary		3	O	

NOTE 1: The information element shall indicate:
- all supported states when the Profile status is "Profile update" or "Profile replacement";
- the selected state when the Profile status is "Profile Response"

NOTE 2: The information element shall be conditional on Profile status as follows:
- "Profile Response": element shall be present;
- "Profile update" or "Profile replacement": element shall not be present;

NOTE 3: The element shall appear as many times as indicated by the element "Number of SS-information".

NOTE 4: The "group information" information element may be repeated inside the type 3 element up to the length of the type 3 information element as sets as defined in subclause 33.2.87. There may be also multiple type 3 information elements, if the maximum length of type 3 elements would otherwise be exceeded.

In addition table 130 of the public enquiry version of ANF-ISIMM (ETS 300 392-3-5 [13]) shall be updated as shown in figure 14 to more fully identify and include extended IP data. Note that this data has also be added to the primitives in table 40 of ETS 300 392-3-5 [13].

The IP service element shall indicate if this type of service (i.e. Internet Protocol) is supported for the individual subscriber or for the group in the visited SwMI.

The support may be negotiated between the home SwMI MM and the visited SwMI MM as follows:

- the home SwMI shall send its preferred value to the visited SwMI MM;
- on receipt of the value sent by the home SwMI MM, the visited SwMI MM shall either use that value or change the value. If the visited SwMI MM changed the value, it may send the new value to the home SwMI.

Table 14: IP service element contents

Information element	Length	Value	Remark
IP service	2	00_2	Undefined – note 1
		01_2	Reserved
		10_2	Not supported
		11_2	Supported
IP type (note 2)	2	00	IPv4 fixed address
		01	IPv4 dynamic address
		10	Mobile IP
		11	IPv6
IPv4 address	32	any	If IPv4
Mobile IP care of address	32	any	If mobile IP

NOTE 1: The value "undefined" shall indicate that no information for this service is applicable e.g. in a profile update, the sending SwMI MM will encode the element as "undefined" if it has not been changed, and the receiving SwMI MM shall not treat this information element. This value shall not be used in a profile replacement and in the response profile of a profile replacement.

NOTE 2: This data is provided only when IP service element is equal to 11_2.

8 Quality of Service

There is no specific requirement for QoS. Tolerable delays suggested by users do not at this time suggest that the IP services will be used for streaming video or speech.

9 Security concerns

It is a requirement of IPI to provide similar levels of security to that of the TETRA air interface.

TETRA security class 3 mobiles and systems have strong security based upon encryption of all traffic and signalling between the MS and its BS, where the key is derived from a secret key authentication process. Authentication is mandatory in class 3 networks. The IPI shall provide authentication whereby the home agent for each MS on SwMI A and the foreign agent for each migrated MS on SwMI B mutually authenticate each other using algorithms equivalent to the TA11, TA12, TA21 and TA22 algorithms defined for air interface authentication in ETS 300 392-7 [14].

For class 2 systems a common cipher key (SCK-IPI) may be used to encrypt the content of tunnelled packets. Authentication is optional in class 2 networks, but where provided at the air interface shall be provided between the home agent and the foreign agent, and between the terminating points of an inter-network tunnel.

For class 1 systems where no air interface encryption is applied the tunnel cannot use TETRA-specific encryption methods. Authentication is optional in class 1 networks, but where provided at the air interface shall be provided between the home agent and the foreign agent, and between the terminating points of an inter-network tunnel.

Annex A (informative): Bibliography

TETRA IPI and its interfaces make use of available specifications from the Internet Community and from ETSI. Whilst the main body of the text of the present document makes direct reference only to those documents that appear in clause 2 as Normative references the authors have consulted many other papers to complete the present document. This bibliography covers much of what may be considered as background reading. Where these documents are given as URL references ETSI do not make any guarantee for the long term availability of any links.

Annex B (informative): Addressing scenarios

B.1 Introduction

This annex explores additional scenarios to those presented in the main text of the present document. This is intended to review those addressing scenarios considered in clause 5.

B.2 Information Flows

B.2.1 Signalling Information Flows

B.2.1.1 MS 'a1' migrates to SwMI B and requests a dynamic IP address at context activation

Figure B.1 shows the information flows for this scenario. The sequence of messages are numbered and described after the figure.

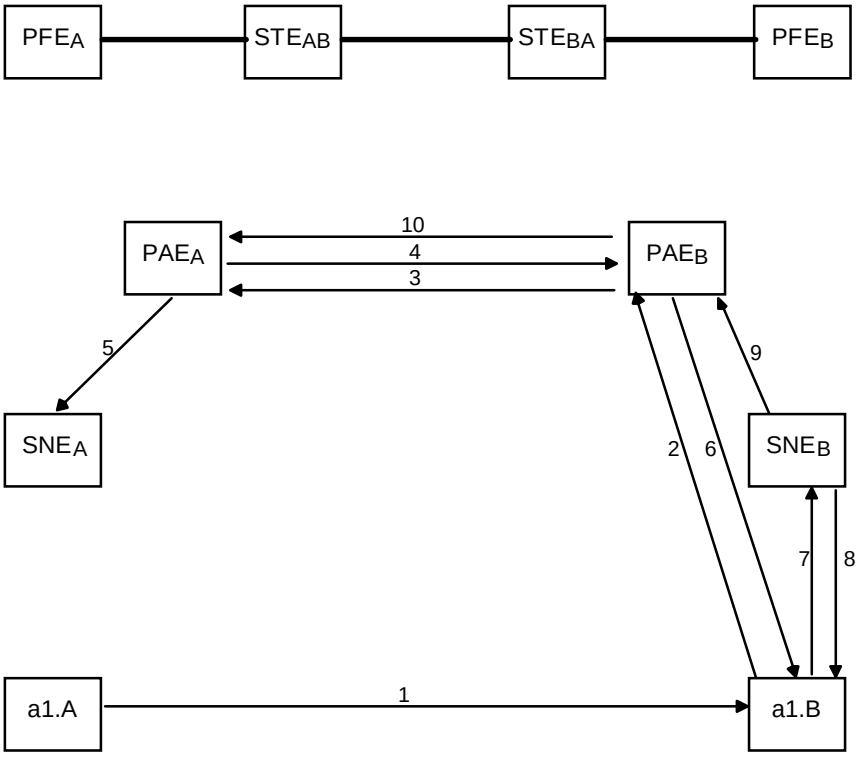


Figure B.1: MS a1 migrates to SwMI B and requests a dynamic IP address at context activation

1) MS a1 migrates from its home SwMI$_A$ to SwMIB;

2) a1 registers (V+D) on SwMI $_B$ using standard MM procedures (ETS 300 392-2 [1]);

3) Using standard ANF-ISIMM procedures, PAE$_B$ informs PAE$_A$ that a1 is now located on SwMIB, and requests Authentication and Provisioning information. (ETS 300 392-3-5 [13]);

4) PAE$_A$ returns the required information (ETS 300 392-3-5 [13]);

5) PAE_A informs SNE_A that a1 is no longer registered on $SwMI_A$, thus allowing SNE_A to delete any Contexts for a1 (Extension to ETS 300 392-2 [1]);

6) The V+D registration process for a1 completes successfully using standard MM procedures (ETS 300 392-2 [1]);

7) a1 sends a SN-Activate PDP Context Request PDU to SNE_B, requesting a dynamic address (Extension to ETS 300 392-2 [1]);

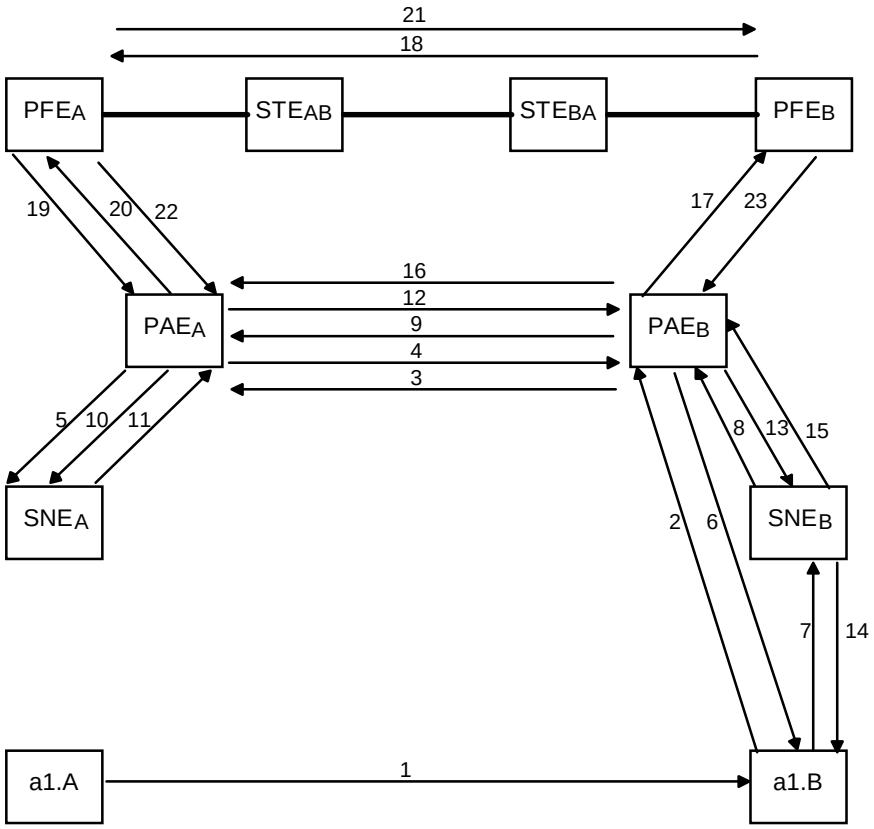
8) SNE_B accepts the Context request by sending a SN-Activate PDP Context Accept PDU to a1. (Extension to ETS 300 392-2 [1]);

9) SNE_B informs PAE_B that the Context has been successfully established and indicates the address which has been allocated;

10) PAE_B informs PAE_A that the Context has been successfully established and indicates the address which has been allocated.

B.2.1.2 MS 'a1' migrates to SwMI B and requests a static IP address at context activation

This scenario represents the case where a MS wishes to continue to use the same IP address after migration, as it was using prior to migration. Figure B.2 shows the information flows for this scenario. The sequence of messages are numbered and described following the figure.



The static IP address is from the address range of SwMI A.

Figure B.2: MS a1 migrates to SwMI B and requests a static IP address at context activation

1) MS a1 migrates from its home $SwMI_A$ to SwMIB;

2) a1 registers (V+D) on SwMIB using standard MM procedures;

3) Using standard ANF-ISIMM procedures, PAE_B informs PAE_A that a1 is now located on SwMIB, and requests Authentication and Provisioning information;

4) PAE_A returns the required information;

5) PAE_A informs SNE_A that a1 is no longer registered on $SwMI_A$, thus allowing SNE_A to delete any Contexts for a1;

6) The V+D registration process for a1 completes successfully using standard MM procedures;

7) a1 sends a SN-Activate PDP Context Request PDU to SNE_B, requesting a static address and presenting the IP address used in the previous SwMI (which may have been either a static or dynamically assigned IP address);

8) SNE_B queries PAE_B to see if a1 may use this static address;

9) PAE_B queries PAE_A to see if a1 may use this static address;

10) PAE_A checks with SNE_A to see if this address has been assigned to any other MS;

11) SNE_A replies to PAE_A saying that the address is available. It marks the address as assigned;

12) PAE_A replies to PAE_B saying a1 may use the specified address;

13) PAE_B informs SNE_B that the requested address is ok;

14) SNE_B accepts the Context request by sending a SN-Activate PDP Context Accept PDU to a1;

15) SNE_B informs PAE_B that the Context has been successfully established;

16) PAE_B informs PAE_A that the Context has been successfully established;

17) PAE_B requests PFE_B to establish a routing tunnel for a1. Note I do not describe here the secure tunnel i.e. the tunnel established between STE_{BA} and STE_{AB};

18) PFE_B requests that PFE_A tunnels all packets destined to a1, to PFE_B;

19) PFE_A seeks approval from PAE_A;

20) PAE_A approves the establishment of the routing tunnel;

21) PFE_A completes the establishment of the routing tunnel with PFE_B;

22) PFE_A informs PAE_A that the routing tunnel has been established;

23) PFE_B informs PAE_B that the routing tunnel has been established.

B.2.2 Data Information Flows

This section describes the data exchanges which take place when two MS attempt to communicate. The path a datagram takes is given and also the actions taken at each functional entity are described.

NOTE 1: The scenarios below may also apply when one or both of the communicating devices is a fixed host attached to the TETRA SwMI.

NOTE 2: The scenarios below assume the signalling which was presented in Section 5.1. of this paper has completed successfully.

B.2.2.1 a1.A using dynamic IP address (from address range of SwMI A). b1.B using dynamic IP address (from address range of SwMI B). a1.A sends a datagram to b1.B

This is a straight forward scenario representing the case where a MS at home in SwMI A wishes to send a datagram to a MS at home in SwMI B. Figure B.3 shows the information flows for this scenario. The sequence of messages are numbered and described following the figure.

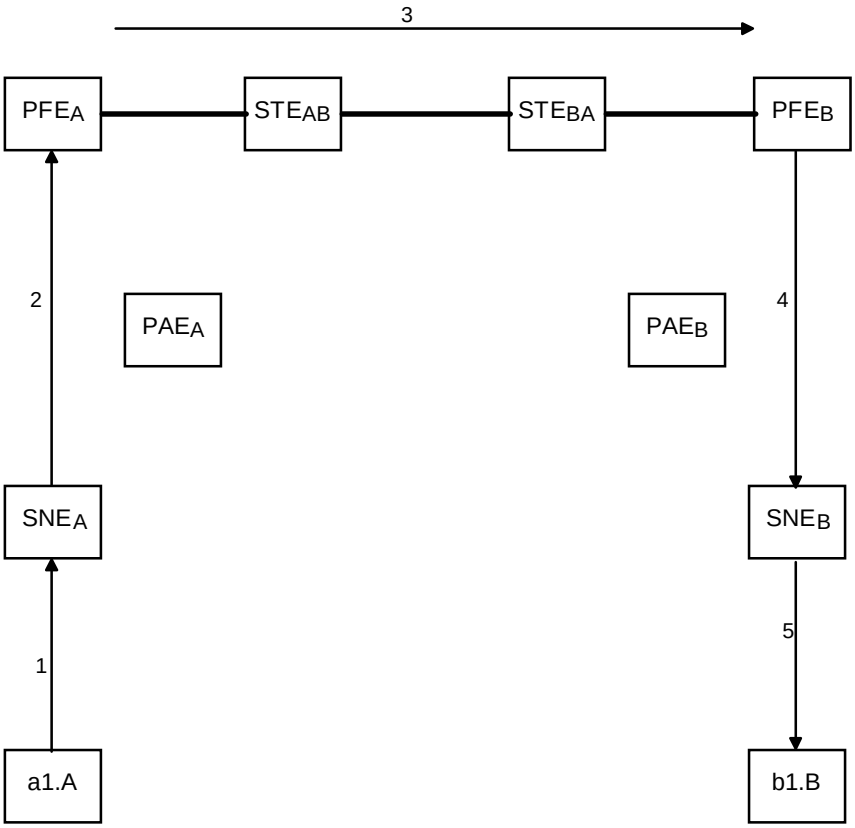


Figure B.3: a1.A using dynamic IP address (from address range of SwMI A). b1.B using dynamic IP address (from address range of SwMI B). a1.A sends a datagram to b1.B

1) a1.A forwards an IP datagram addressed to b1.B, to SNE_A. The IP address used for b1.B is from the address plan of SwMI B;

2) SNE_A checks the destination IP address of the datagram and based on information stored in its routing tables, forwards the datagram to PFE_A;

3) PFE_A checks the destination IP address of the datagram and based on information stored in its routing tables, forwards the datagram to PFE_B. PFE_A may use standard IP routing when forwarding the datagram to PFE_B, i.e. a routing tunnel should not be required. Where enhanced security is required, the datagram may pass through a secure tunnel established between STE_{AB} and STE_{BA}. To prevent hijacking of the secure tunnel, PFE_A should be configured to only forward datagrams that have been received directly from SNE_A;

4) PFE_B checks the destination IP address of the datagram and based on information stored in its routing tables, forwards the datagram to SNE_B;

5) SNE_B forwards the datagram to b1.B.

This example also encompasses the following scenarios:

1) datagram in the opposite direction i.e. b1.B sending to a1.A;

2) all combinations of static and dynamic addressing e.g. a1.A has statically configured IP address (from the address range of SwMI A) and b1.B has dynamically configured IP address (from the address range of SwMI B);

3) where public addressing or non-overlapping private addressing ranges are used by both SwMIs then standard routing may be used between PFE_A and PFE_B. A routing tunnel may exist between PFE_A and PFE_B however this is not necessary;

4) where the SwMIs use private addresses that overlap, then a form of Network Address Translation (NAT) will be required. The use of NAT is outside the scope of this specification. Where NAT is used in conjunction with secure tunnelling the NAT functionality should be implemented between STE_{AB} and STE_{BA}. In this case STE_{AB} and STE_{BA} should take on the functionality of Host NATs.

B.2.2.2 a1.A using dynamic IP address (from address range of SwMI A). a2.B using dynamic IP address (from address range of SwMI B). a1.A sends a datagram to a2.B

This scenario represents the case where a MS at home in SwMI A wishes to send a datagram to a MS which has migrated to SwMI B. The migrated MS has been assigned a dynamic IP address from the address range of SwMI B. Figure B.4 shows the information flows for this scenario. The sequence of messages are numbered and described following the figure.

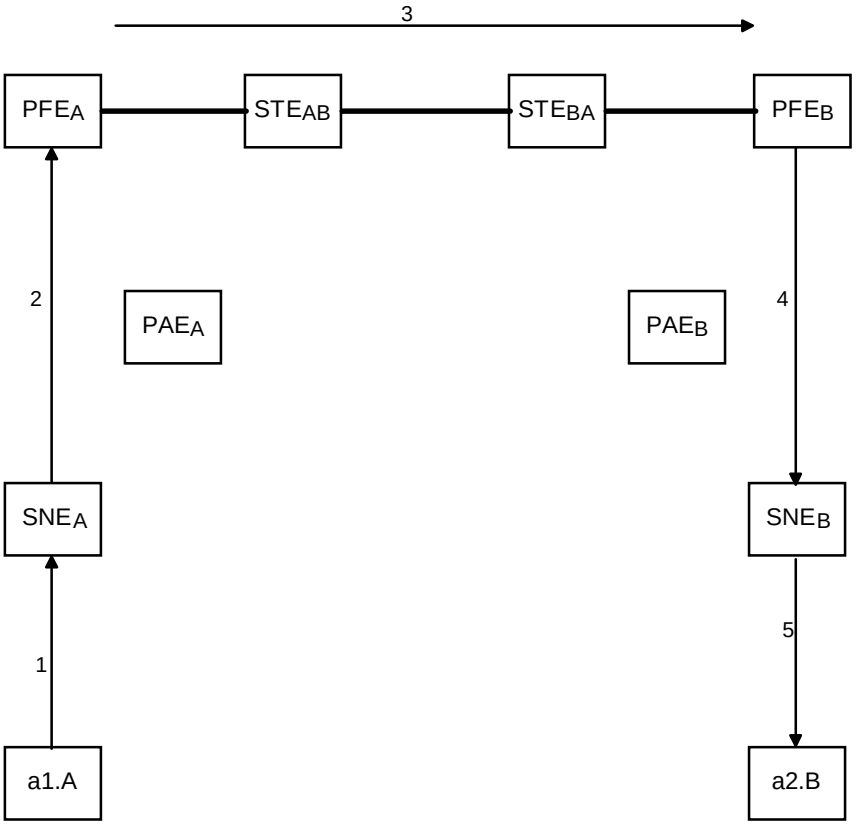


Figure B.4: a1.A using dynamic IP address (from address range of SwMI A). a2.B using dynamic IP address (from address range of SwMI B). a1.A sends a datagram to a2.B

1) a1.A forwards an IP datagram addressed to a2.B to SNE_A. The IP address used for a2.B is from the address plan of SwMI B;

2) SNE_A checks the destination IP address of the datagram and based on information stored in its routing tables, forwards the datagram to PFE_A.

   Any datagrams received by SNE_A, with the destination address set to a2.A (i.e. the address used by a2 prior to migration) should be returned to the source with an appropriate error message e.g. ICMP host unreachable;

3) PFE_A checks the destination IP address of the datagram and based on information stored in its routing tables, forwards the datagram to PFE_B. PFE_A may use standard IP routing when forwarding the datagram to PFE_B, i.e. a routing tunnel should not be required. Where enhanced security is required, the datagram may pass through a secure tunnel established between STE_{AB} and STE_{BA}. To prevent hijacking of the secure tunnel, PFE_A should be configured to only forward datagrams that have been received directly from SNE_A;

4) PFE_B checks the destination IP address of the datagram and based on information stored in its routing tables, forwards the datagram to SNE_B;

5) SNE_B forwards the datagram to a2.B.

This example also covers the following scenarios:

1) Same as above, except a1.A is assigned a statically configured address from the address range of SwMI A;

2) Datagram in the opposite i.e. a2.B sending to a1.A when a2.B has been assigned a dynamic IP address (from SwMI B's address plan).

B.2.2.3 a1.A using dynamic IP address (from address range of SwMI A). a2.B using static IP address (from address range of SwMI A). a1.A sends a datagram to a2.B

This scenario is similar to the previous scenario in that it represents the case where a MS which is at home in SwMI A is sending a datagram to a MS which has migrated to SwMI B. However in this case the migrated MS has requested and is assigned a static address from the address range of SwMI A. Figure B.5 shows the information flows for this scenario. The sequence of messages are numbered and described following the figure.

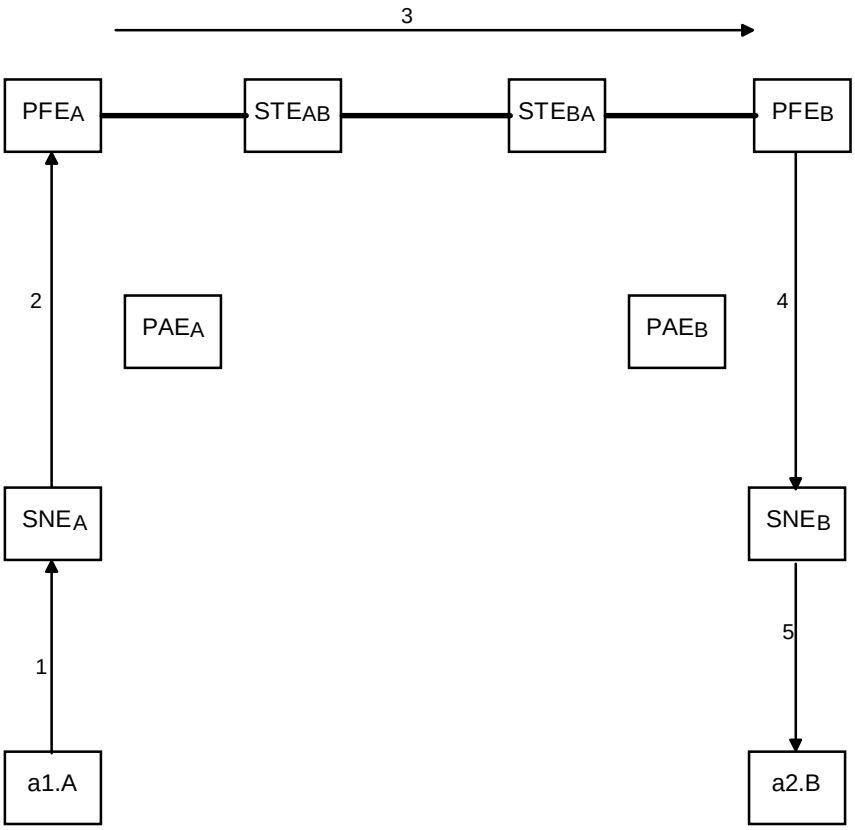


Figure B.5: a1.A using dynamic IP address (from address range of SwMI A). a2.B using static IP address (from address range of SwMI A). a1.A sends a datagram to a2.B

1) a1.A forwards an IP datagram addressed to a2.B to SNE_A. The IP address used for a2.B is from the address plan of SwMI A;

2) SNE_A on seeing that the destination address is from SwMI A's address plan does a further lookup to determine the ITSI associated with this IP address. This lookup will identify the MS as having migrated. SNE_A then forwards the datagram to $PFE_{A;}$

3) PFE_A checks the destination IP address of the datagram and identifies it as belonging to a migrated MS. As standard IP routing may not be used in this case when forwarding the datagram to PFE_B (because the address of a2.B is not topologically correct), PFE_A must use a routing tunnel to transport the datagram to PFE_B (PFE_B is the Care of Address (COA) for a2.B). This routing tunnel may be constructed using IP in IP encapsulation or some other form of encapsulation. The destination and source addresses in the outer IP header shall be those of PFE_B and PFE_A respectively. Where enhanced security is required, the datagram may pass through a secure tunnel

established between STE_{AB} and STE_{BA}. To prevent hijacking of the secure tunnel, ˚ PFE_A should be configured to only forward datagrams which have been received directly from SNE_A;

The routing and secure tunnels may be combined to form a single tunnel e.g. IPSec ESP protocol may be used to forward the datagram from PFE_A to PFE_B while at the same time ensuring confidentiality and authentication of datagrams being transported on the tunnel;

4) PFE_B checks the destination IP address of the datagram and based on information stored in its routing tables, forwards the datagram to SNE_B;

5) SNE_B forwards the datagram to a2.B.

This example also covers the following scenarios:

1) Same as above, except a1.A is assigned a statically configured address.

B.2.2.4 b1.B using dynamic IP address (from address range of SwMI B). a1.B using static IP address (from address range of SwMI A). b1.B sends a datagram to a1.B

This scenario represents the case where a MS which is at home in SwMI B wishes to send a datagram to a MS which has migrated to SwMI B. The migrated MS requested and is assigned a static address from the address range of SwMI A. Figure 8 below shows the information flows for this scenario. The sequence of messages are numbered and described below.

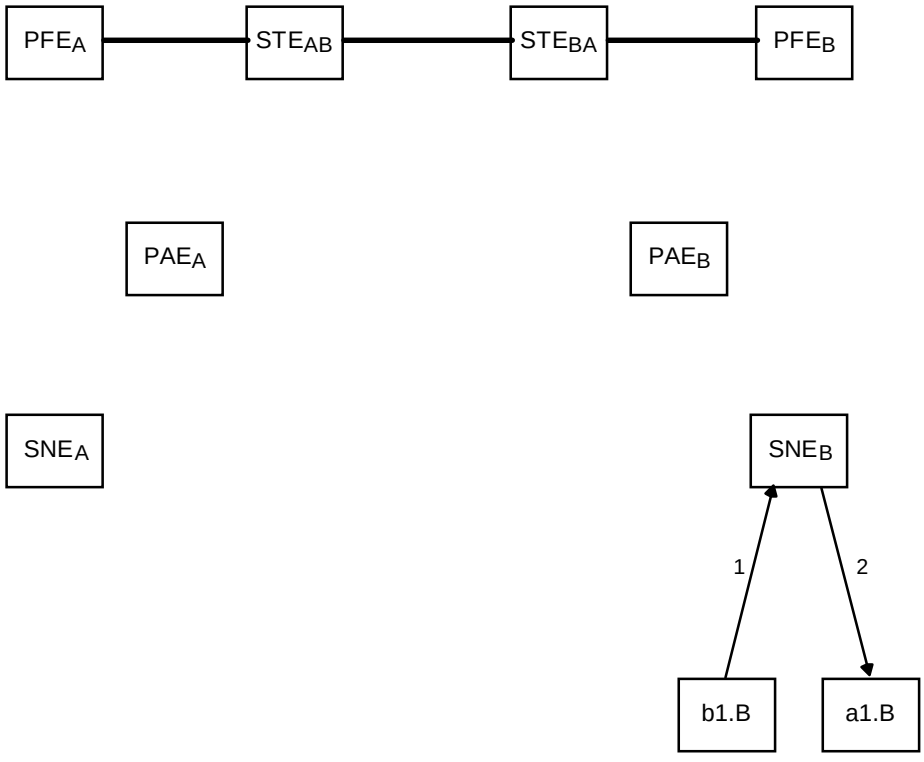


Figure B.7: b1.B using dynamic IP address (from address range of SwMI B). a1.B using static IP address (from address range of SwMI A). b1.B sends a datagram to a1.B

1) b1.B forwards an IP datagram addressed to a1.B to SNE_B. The IP address used for a1.B is from the address plan of SwMI A.;

2) SNE_B sees that the destination address is from SwMI A's address plan. It also notes that this IP address is assigned to a MS which is currently located on SwMI B. A further lookup determines the ITSI associated with this IP address. SNE_B then forwards the datagram to a1.B.

This example also covers the following scenarios:

1) Same as above, except b1.B is assigned a statically configured address (from SwMI B's address range).

B.2.2.5 a1.B using dynamic IP address (from address range of SwMI B). a2.B using dynamic IP address (from address range of SwMI B). a1.B sends a datagram to a2.B

This scenario represents the case where a two MS which have migrated to SwMI B, wish to communicate. Both of the migrated MS are assigned dynamic addresses from the address range of SwMI B. Figure B.8 shows the information flows for this scenario. The sequence of messages are numbered and described following the figure.

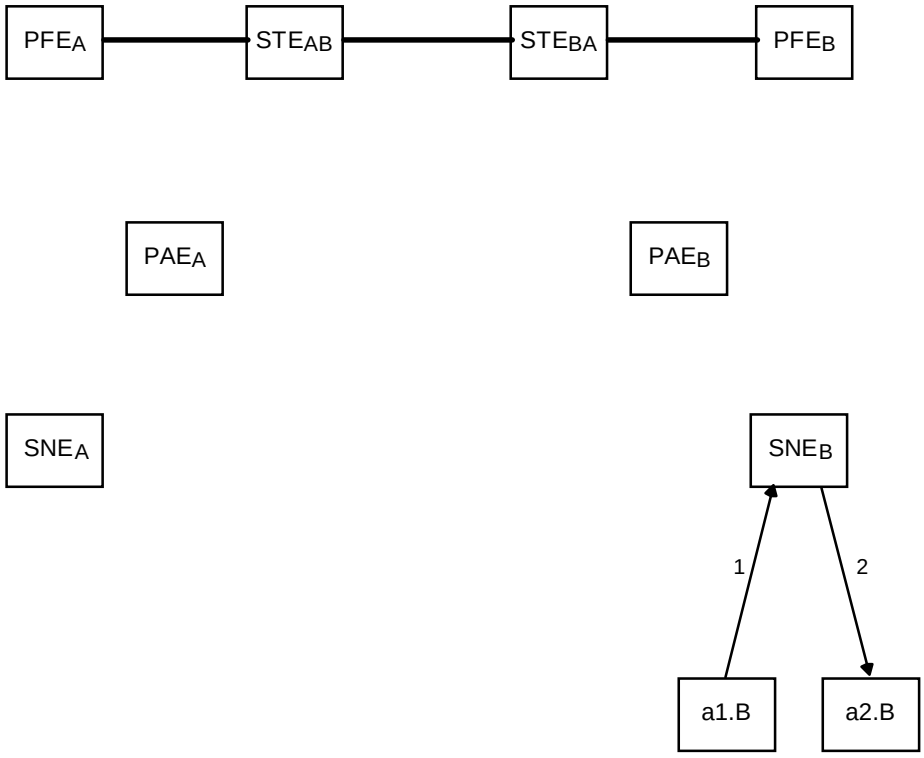


Figure B.8: a1.B using dynamic IP address (from address range of SwMI B). a2.B using dynamic IP address (from address range of SwMI B). a1.B sends a datagram to a2.B

1) a1.B forwards an IP datagram addressed to a2.B to SNE$_B$. The IP address used for a2.B is from the address plan of SwMI B;

2) SNE$_B$ on seeing that the destination address is from SwMI B's address plan does a further lookup to determine the ITSI associated with this IP address. SNE$_B$ then forwards the datagram to a2.B.

This example also covers the following scenarios:

1) Datagram in the opposite direction i.e. a2.B sending a datagram to a1.B.

B.2.2.6 Void

B.2.2.7 a1.B using static IP address (from address range of SwMI A). a2.B using dynamic IP address (from address range of SwMI B). a1.B sends a datagram to a2.B

This scenario is the same as the previous scenario in that it represents the case where a two MS which have migrated to SwMI B, wish to communicate. However in this case the source of the datagram requested and is assigned a static IP address from the address range of SwMI A. As in the previous scenario, the destination MS is assigned dynamic address from the address range of SwMI B. Figure B.9 shows the information flows for this scenario. The sequence of messages are numbered and described following the figure.

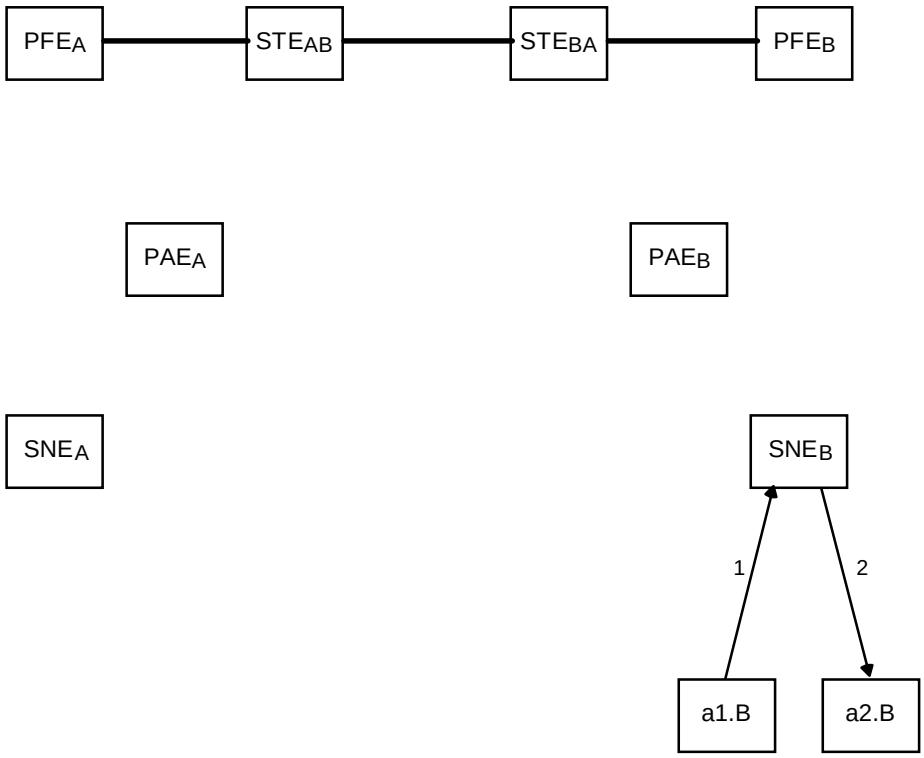


Figure B.9: a1.B using static IP address (from address range of SwMI A). a2.B using dynamic IP address (from address range of SwMI B). a1.B sends a datagram to a2.B

1) a1.B forwards an IP datagram addressed to a2.B to SNE_B. The IP address used for a2.B is from the address plan of SwMI B;

2) SNE_B on seeing that the destination address is from SwMI B's address plan does a further lookup to determine the ITSI associated with this IP address. SNE_B then forwards the datagram to a2.B.

B.2.2.8 a1.B using dynamic IP address (from address range of SwMI B). a2.B using static IP address (from address range of SwMI A). a1.B sends a datagram to a2.B

This scenario is the same as the previous scenario in that it represents the case where a two MS which have migrated to SwMI B, wish to communicate. However in this case the destination of the datagram requested and is assigned a static IP address from the address range of SwMI A. The source MS is assigned dynamic address from the address range of SwMI B. Figure B.10 shows the information flows for this scenario. The sequence of messages are numbered and described following the figure.

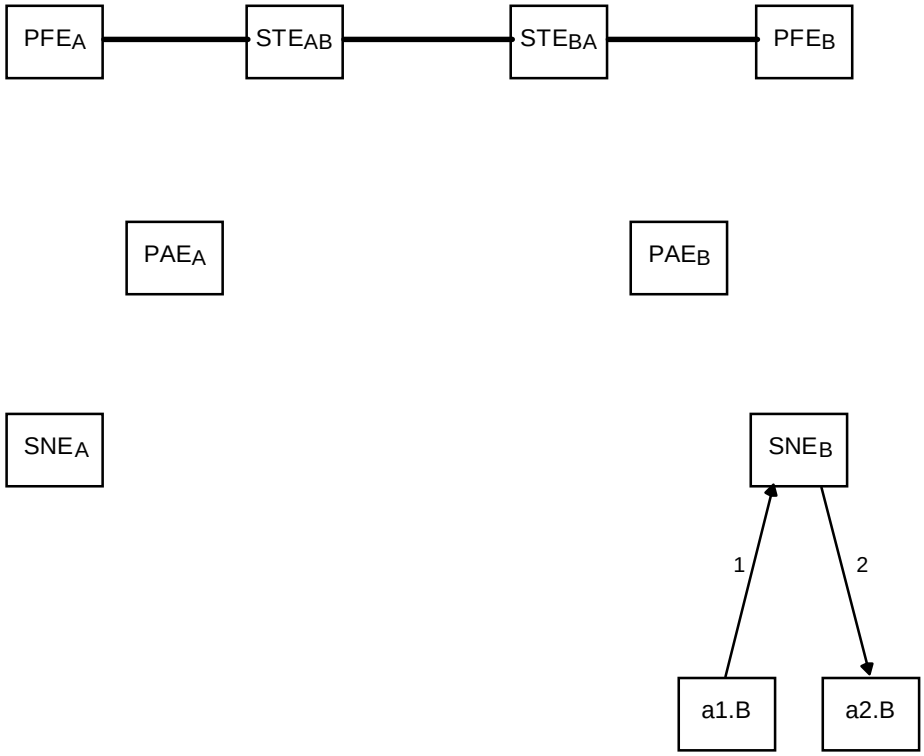


Figure B.10: a1.B using dynamic IP address (from address range of SwMI B). a2.B using static IP address (from address range of SwMI A). a1.B sends a datagram to a2.B

1) a1.B forwards an IP datagram addressed to a2.B to SNE_B. The IP address used for a2.B is from the address plan of SwMI A;

2) SNE_B sees that the destination address is from SwMI A's address plan. It also notes that this IP address is assigned to a MS which is currently located on SwMI B. A further lookup determines the ITSI associated with this IP address. SNE_B then forwards the datagram to a2.B.

B.2.2.9 a1.B using static IP address (from address range of SwMI A). a2.B using static IP address (from address range of SwMI A). a1.B sends a datagram to a2.B

In this scenario, again two MS which have migrated to SwMI B, wish to communicate. In this case both MS have requested and are assigned static IP addresses from the address range of SwMI A. Figure B.11 shows the information flows for this scenario. The sequence of messages are numbered and described following the figure.

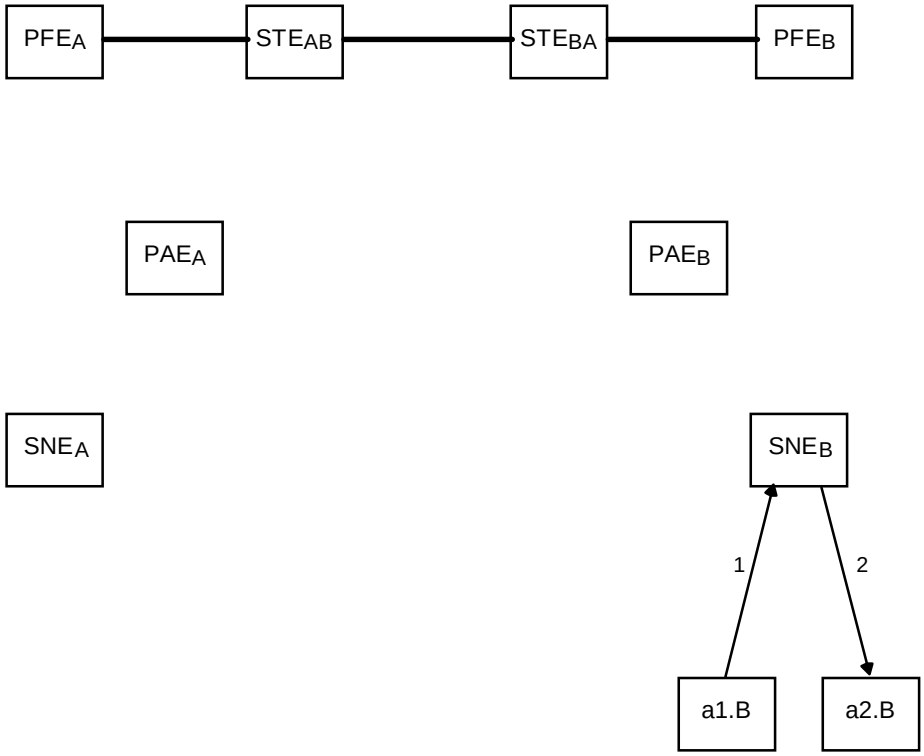


Figure B.11: a1.B using static IP address (from address range of SwMI A). a2.B using static IP address (from address range of SwMI A). a1.B sends a datagram to a2.B

1) a1.B forwards an IP datagram addressed to the a2.B to SNE$_B$. The IP address used for a2.B is from the address plan of SwMI B;

2) SNE$_B$ sees that the destination address is from SwMI A's address plan. It also notes that this IP address is assigned to a MS which is currently located on SwMI B. A further lookup determines the ITSI associated with this IP address. SNE$_B$ then forwards the datagram to a2.B.

History

Document history				
V1.1.1	August 1999	Public Enquiry	PE 9956:	1999-08-25 to 1999-12-24