Publicly Available Specification

PAS 0001-1-2

Version: 3.0.1

Date: 16 March 1998

Source: TETRAPOL Forum

Work Item No: 0001

Key word: TETRAPOL

TETRAPOL Specifications;
Part 1: General Network Design;
Part 2: Voice and Data Services in Network and Direct Mode

TETRAPOL FORUM

TETRAPOL Secretariat

Postal address: BP 40 78392 Bois d'Arcy CEDEX - FRANCE
Office address: Rue Jean-Pierre Timbaud 78392 Bois d'Arcy CEDEX - FRANCE
Tel.: +33 1 34 60 55 88 - Fax: +33 1 30 45 28 35

Contents

Foreword

This document is the Publicly Available Specification (PAS) of the TETRAPOL land mobile radio system, which shall provide digital narrow band voice, messaging, and data services. Its main objective is to provide specifications dedicated to the more demanding PMR segment: the public safety. These specifications are also applicable to most PMR networks.

This PAS is a multipart document which consists of:

Part 1	General Network Design
Part 2	Radio Air interface
Part 3	Air Interface Protocol
Part 4	Gateway to X.400 MTA
Part 5	Dispatch Centre interface
Part 6	Line Connected Terminal interface
Part 7	Codec
Part 8	Radio conformance tests
Part 9	Air interface protocol conformance tests
Part 10	Inter System Interface
Part 11	Gateway to PABX, ISDN, PDN
Part 12	Network Management Centre interface
Part 13	User Data Terminal to System Terminal interface
Part 14	System Simulator
Part 15	Gateway to External Data Terminal
Part 16	Security
Part 17	Guide to TETRAPOL features
Part 18	Base station to Radioswitch interface
Part 19	Stand Alone Dispatch Position interface

1. Scope

This subpart describes the Voice and Data Services in Network Mode and in Direct Mode which are included in TETRAPOL specifications.

The related security mechanisms and key management are fully described in PAS 0001-16 [2].

2. Normative references

This PAS incorporates by dated and undated reference, provisions from other applications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revision of any of these publications apply to this PAS only when incorporated in it by amendment or revision. For undated references the latest edition of publication referred to applies.

[1] PAS 0001-1-1: "TETRAPOL Specifications; General Network Design; Reference Model".

[2] PAS 0001-16: "TETRAPOL Specifications; Security Mechanisms and Key Management".

[3] PAS 0001-1-3: "TETRAPOL Specifications; General Network Design; Network services".

3. Definitions and abbreviations

3.1. Definitions

For the purposes of this PAS, the following definitions apply:

Active participant: a system terminal is an active participant in a Group Communication when it is either listening to that communication or transmitting.

Additional Network Feature (ANF): feature provided by a TETRAPOL Network which can improve the handling of certain calls or the performance of the network as a whole rather than benefiting any particular served user. As there is no served user, these features are not called supplementary services.

Alternate Recipient: this term is used in messaging services, when a system terminal is designated as a destination when the delivery to primary recipient fails.

Anti-talkative mechanism: mechanism limiting the duration of terminal voice transmission.

Back-up Terminal: this term is used in messaging. Designates a recipient defined by the System, for those messages which cannot be delivered neither to the primary nor to the alternate recipient.

Regional network (RN): elementary network which is the smallest entity able to operate in normal network connected mode and to provide all nominal services and features available in normal network connected mode. It includes one RSW and one or more BSs and corresponds to a subdivision of the coverage of a network.

Candidate: a Terminal is candidate to a Group Communication once the user of the terminal has requested to participate into the Group Communication and if the terminal is authorized.

Cell coverage area: area within which a defined quality of reception is provided. Planned radio coverage of a cell.

Cell re-selection: act of changing the serving cell from an old cell to a new cell. When the re-selection is made, the MS is said to be attached to the cell.

Control Channel: bi-directional BS-RT physical radio channel used for transmitting signalling and data.

Coverage (COV): A coverage designates a list of radio Cells and Line Access Base Stations (LABSs) all located within one regional network.

Data Terminal (DT): Data Terminals include User Data Terminals (UDTs) which are part of the System as well as External Data Terminals (EDTs) which are not System Terminals.

Data Application Server (DAS): IP addressable customer data equipment.

Designated Recipient: this term is used in messaging. Recipient designated by the originator of the message, before the address is interpreted by the system.

Disabled terminal: a terminal may be either traffic disabled or access disabled, in which case it can no longer operate in Network connected mode nor in Direct mode nor in Repeater mode nor can it register any more.

Dispatch Centre: The dispatch centre includes a dispatch centre serveur and a dispatch centre switch providing TETRAPOL services and computer-telephony integrated services to dispatchers.

Dispatch Position: Dispatch Positions (DPs) are Stand Alone Dispatch Positions (SADPs) and Dispatch Positions at the Dispatch Centre.

Effective participant: a terminal is an effective participant in a Group Communication when it can transmit an activation request or accept an activation command for this communication.

Failure: termination of the ability of an "item" to perform a "required function".

Fault: inability of an "item" to perform a "required function".

Fleet: Individual addressing subdivision.

Group communication: communication between several users sharing access rights. Group communications include Open Channels, Talkgroups and Broadcast Calls.

Home Located Terminal: terminal registered in its Home regional network.

Home Radioswitch (HRSW): RSW which stores the reference data base for all Terminals belonging to one regional network. The Home RSW processes the functions of the Home Location Register. The Home RSW is designated by the R field in the subscriber RFSI address.

Line Access Base Station (LABS): network interface to Line Connected Terminals and SADPs, also known as Line Connection Interface Unit (LCIU).

Open channel: Generic term for group communications including multi-site open channel, emergency open channel, crisis open channel and broadcast open channel.

Operational Group: an Operational Group (OG) is a group of subscribers all of whom share a certain right to participate in a Group Communication or set-up a Multi-site Open Channel.

Primary Recipient: this term is used in messaging. Recipient known by the System after it has interpreted the designated recipient address, before forwarding and before activating secure delivery procedures.

Private Call: point-to-point or point-to-multipoint communication between one or more system users and/or one external network subscriber. Private Calls do not involve setting-up of any Open Channel. Private Calls include Individual, Multiparty and Interconnect Calls.

Queuing: the procedure in which calls are kept pending for reasons of congestion or when the called party is occupied.

Registration: act of becoming a recognised Network user by exchange with the SwMI of appropriate information.

Serving Cell: Cell containing the BS with which the MS is currently communicating, whether registered or pending registration..

Suspended Terminal: A suspended terminal continues to register. It cannot be used for communication neither in Network connected mode nor in RP nor in Direct mode. A Terminal Management Command (at the OMC) shall be used to enable it again.

System terminal: Radio terminal or line-connected terminal, providing TETRAPOL services to a user.

Traffic Channel: bi-directional BS - RT physical radio channel used for transmitting voice or data.

Visited Radioswitch: a Terminal's Visited RSW is the RSW of the regional network where the Terminal is registered. It may be the Terminal's Home RSW.

Visitor Terminal: terminal whose Home regional network and Visited regional network are different.

3.2. Abbreviations

For the purposes of this PAS, the following abbreviations apply:

A/I	Air Interface
BCH	Broadcast CHannel
BN	Regional network
BS	Base Station
CCH	Control CHannel
CODEC	Speech enCOder DECoder
COV	COVerage
CRP	Connexion Reference Point
CUG	Closed User Group
DAS	Data Application Server
DB	DataBase
DC	Dispatch Centre
DCN	Delivery Confirmation Notification
DCRP	Data Connection Reference Point
DFN	Delivery Failure Notification
DM	Direct Mode
DM/NM	Direct Mode / Network Monitoring
DP	Dispatch Position
EDT	External Data Terminal
EPBS	Emitted Power of a Base Station
EPT	Emitted Power of a Terminal
EXAM	EXternal Application Messaging
FBM	FallBack Mode
HRSW	Home RadioSWitch
IPM	Inter-Personal Messaging
ISI	Inter System Interface
ITU-T	International Telecommunication Union - Telecommunication Standardisation Sector
KMC	Key Management Centre
LABS	Line Access Base Station
LCT	Line Connected Terminal
LLC	Logical Link Control
MAC	Medium Access Control
MCC	Main Control Channel
MM	Mobility Management
MMI	Man-Machine Interface
MOCH	Multisite Open CHannel
MRI	Mobile Random Identifier
MS	Mobile Station
MSG APPLI	MeSsaging APPLIcation
MSG-Id	MeSsaGe Identifier
MSW	Main radio SWitch

NMC	Network Management Centre
OG	Operational Group
OMC	Operation and Maintenance Centre
PABX	Private Automatic Branch eXchange
PRN	Preferred Regional network
PCH	Paging CHannel
PSTN	Public Switched Telecommunications Network
PTT	Push-To-Talk
RDP	Radio Dispatch Position
RFS	Regional network - Fleet - Subfleet address
RFSI	Regional network - Fleet - Subfleet - Individual address
Ri	Reference point index i
RN	Regional network
RNLM	Regional network Local Messaging
RNOP	Regional network OPerator
RP	RePeater
RSW	RadioSWitch
RT	Radio Terminal
RTA	Radio Transmission Acknowledgement
SADP	Stand Alone Dispatch Position
SCH	Signalling CHannel
SCN	Submit Confirmation Notification
SDL	Specification and Description Language
SDP	Submit/Delivery Protocol
SFN	Submit Failure Notification
SIM	Subscriber Identity Module
ST	System Terminal
SwMI	Switching and Management Infrastructure
TCH	Traffic CHannel
TCP/IP	Transmission Control Protocol/Internet Protocol
TE	Terminal Equipment
TMSG-Id	Temporary MeSsaGe Identifier
UA	User Agent
UDP	User Datagram Protocol in TCP/IP
UDT	User Data Terminal
VCRP	Voice Connection Reference Point
VRSW	Visited RadioSWitch
X.400 MTA	X.400 Message Transfer Agent

4. Voice Services in Network Connected Mode

4.1. Group communications

4.1.1. Multisite Open Channel

4.1.1.1. Basic Service

4.1.1.1.1. Presentation

The Multisite Open Channel (MOCH) service shall provide half-duplex multi-group-addressed voice communications to system terminals located within a coverage of the system.

Once established, an MOCH may be continually activated for voice transmissions between the members of the related groups, until the MOCH is released.

Assuming a group member is within the coverage of the MOCH, he may select a MOCH; he then automatically makes a late entry and participates in the conversation until he withdraws from the MOCH.

4.1.1.1.2. Coverage

The coverage of a MOCH shall be defined as a list of radio cells and line access base stations from several sites, all contained within one initiating regional network of the system.

The multi-regional-network supplementary service requires an additional definition list of destination regional networks where the MOCH is defined, so that a MOCH coverage can automatically span over more than one regional network.

Upon modification of the coverage of a MOCH while it is established, the MOCH with the previous coverage definition is released.

4.1.1.1.3. Participants

Prerequisites for a system terminal to participate in a MOCH are as follows:

- The system terminal shall be a member of at least one of the participation groups of the MOCH, i.e. it shall own an operational group (OG) associated to the MOCH.
- The system terminal shall be within the coverage of the MOCH.
- A system terminal can participate in a MOCH if it is registered in the system or pending registration, in which case it shall have been previously registered in the systemand shall have received the MOCH operational parameters.

4.1.1.1.4. Establishment of a Multisite Open Channel

4.1.1.1.4.1. Purpose

The MOCH establishment consists in allocating network resources for the MOCH and connecting them together in order to build a voice path. Whether radio traffic channels are allocated and connected to the voice path upon establishment depends on the trunking mode:

- When the MOCH operates in message trunking mode, traffic channels are allocated upon establishment of the MOCH.

- When the MOCH operates in activation-based trunking mode, traffic channels are set-up only upon activation of the MOCH for transmission purpose, not upon establishment of the MOCH.

4.1.1.1.4.2. Authorized terminals

Terminals that are authorized to request the network to establish a MOCH shall be members of a group embodied by the establishement OG associated to that MOCH.

4.1.1.1.4.3. Conditions for establishment

Priori to being established in the system, a MOCH shall be first created and defined using service management procedures from the operation and maintenance domain.

4.1.1.1.4.4. Establishment Procedure

The network shall attempt to establish the MOCH over the predefined coverage. Its requests for being allocated resources may be queued. If the available coverage does not match the entire requested coverage, the network shall continually try to extend the actual coverage.

When the MOCH coverage is established, the system shall update the list of MOCH established in each cell and shall broadcast the updated list periodically.

Each system terminal periodically receives the updated list of MOCH established the cell where it is registered, so that it can determine to which MOCH it is allowed to participate.

4.1.1.1.5. Entry into Multisite Open Channel

4.1.1.1.5.1. Presentation

A Terminal may enter into a MOCH established in a cell through:

- spontaneous entry into a MOCH;
- return to a MOCH at the end of another call;
- automatic re-entry into a MOCH.

4.1.1.1.5.2. Spontaneous Entry

Upon selection of a MOCH by the user, the system terminal becomes a candidate for the MOCH. When the MOCH is activated in the cell, the terminal enters the MOCH.

The network shall broadcast the list of MOCH established in the cell. When the terminal roams into a cell where the selected MOCH is already active, the terminal automatically enters the MOCH upon receipt of the list of active MOCH.

On a user's request, the radio terminal can display the latest list of authorized MOCH that are established in the serving cell according to the OG access control conditions.

4.1.1.1.5.3. Candidate State

If the system terminal user requests to enter into a MOCH that is not established in the cell or for which the system terminal is not authorized:

- the system terminal accepts the command and becomes a candidate for late entry into the MOCH;
- the system terminal informs the user that it is impossible to participate in the chosen MOCH.

If the system terminal is a candidate for a MOCH:

- as long as the entry into the MOCH is impossible, the system terminal informs the user;
- when the entry into the MOCH becomes possible, the system terminal can execute an automatic entry into this communication and inform the user.

This applies also when the cell is not in the coverage of the MOCH or if the user is not authorized for the MOCH.

4.1.1.1.5.3.1. Return at the end of a call

A terminal which is participating in a MOCH can be temporarily involved in another call, e.g. a private call or a data transmision. Depending on that call and upon conditions regarding the MOCH,the terminal may automatically re-enter into the previous MOCH.

4.1.1.1.5.4. Automatic Re-entry

If a terminal participating in a MOCH leaves the cell in which it was registered, it remains a candidate for the MOCH. If the terminal then registers again within the same cell or within another cell, where the same MOCH is established, it then executes automatically a spontaneous entry into this communication.

Two MOCH which are established in two different regional networks and have the same MOCH identifier are considered to be either the same or different regarding the automatic re-entry, depending on the system.

The automatic MOCH re-entry feature is lost when the user commands the Terminal to cease being a candidate for the MOCH:

- if the terminal requests entry into another MOCH;
- if the terminal leaves the MOCH because the user hangs up.

4.1.1.1.6. Exit from Multisite Open Channel

4.1.1.1.6.1. Exit events

A Terminal leaves a MOCH in the following cases:

- going on hook;
- entry into another call;
- loss of the link to the Network;
- loss of the access right;
- coverage restriction;
- MOCH release.

4.1.1.1.6.2. Going on hook

Going on hook is a deliberate action from the user of the terminal. The terminal shall leave the MOCH immediately.

The terminal shall no longer be a candidate for the MOCH.

4.1.1.1.6.3. Entry into another call

A terminal which is participating in a MOCH can enter another call directly without having to explicitly leave the MOCH.

During the time while the terminal is participating in the other call, its candidature to the MOCH shall be suspended.

When a radio terminal or line-connected terminal leaves the new call, it shall become a candidate for the MOCH again. If conditions allow, it shall re-enter into the MOCH.

4.1.1.1.6.4. Loss of the link to the Network

If the link to the network is lost, the terminal shall leave the MOCH. It shall remain a candidate for this MOCH.

If the terminal re-establishes the link to the network, either within the same cell or within another cell, it may automatically re-enter the MOCH.

4.1.1.1.6.5. Loss of the access right

The MOCH participation Operational Group and a terminal Operational Groups may be modified with a service management command while that terminal is participating in a MOCH or provided from an external source.

The network broadcasts these modifications. From these, it shall deduce the list of MOCH it has the right to participate in. If it looses the right to participate in the MOCH it is currently participating in, it shall leave the MOCH and shall inform the user. The terminal shall remain a candidate for the MOCH.

If a Terminal which was either registered or pending registration becomes non-registered, it shall loose its right to participate in MOCHs.

4.1.1.1.6.6. Coverage Restriction

A MOCH actual coverage can be restricted following a fault or the pre-emption of a resource by another call.

A Terminal which is participating in such a MOCH shall leave the communication. It shall remain a candidate for the MOCH. It shall execute an Automatic Re-entry when the coverage is re-established.

4.1.1.1.6.6.1. Release

If a Terminal is participating in a MOCH and that MOCH is released, the terminal shall remain a candidate for the MOCH and shall inform the user of the MOCH unavailability.

4.1.1.1.7. Release of Multisite Open Channel

4.1.1.1.7.1. Purpose of Release

Upon MOCH release request from an authorized terminal, the participant system terminals shall be dispersed and the resources allocated to the MOCH shall be released.

4.1.1.1.7.2. Authorized Terminals for Release

The terminal allowed to establish a MOCH are those allowed to release it.

4.1.1.1.7.3. Conditions for Release

The System Terminal, the dispatch position or the OMC that requests the MOCH release shall be able to send a release request to the ad-hoc master RSW. If the request is accepted by the network, but can not be perfomed immediately, its execution is deferred by the network.

4.1.1.1.7.4. Execution of Release

In the coverage of the MOCH, the network broadcasts a request for the participant in the MOCH to leave the traffic channel to be deallocated.

4.1.1.1.8. Addressing

OG addressing applies in order to define the establishment group and the participation groups of a MOCH.

4.1.1.1.9. Priority

Different priorities may be considered as specified in [3].

4.1.1.1.10. Access Control

Operational Group Access Control can be activated or inhibited with a service management commandfrom the OMC. Participation Operational Groups may be provided at establishment time from a dispatch position.

A MOCH subject to Access Control shall be associated with:

- one establishment Operational Group;
- one or several default participation Operational Groups defined at the OMC;
- one or several participation Operational Groups selected by the SADP or DC that replace the default ones at set-up.

A Terminal shall be authorized to set-up a Multisite Open Channel if it owns the establishment operational group.

A terminal shall be authorized to participate in a MOCH if it owns one of the participation operational groups of the MOCH.

4.1.1.1.10.1. Authorization

A Multisite Open Channel can be established and released:

- at the OMC;
- by an RT or an LCT authorized (by configuration) to set-up and release Open Channels
- by an authorized SADP or a DC.

The request from the system terminal shall be able to reach the ad-hoc RSW in the network. The Terminal shall be within nominal Open Channel Coverage.

Multisite Open Channel Set-up and Release shall be subject to OG Access Control conditions: to set-up and release a Multisite Open Channel, the Terminal shall ownthe MOCH establishment Operational Group.

The establishment of an MOCH in unencrypted mode can only be requested from the OMC.

4.1.1.1.11. Anti-talkative feature

A Terminal which starts to transmit can keep transmitting for a maximum time limited by an "anti-talkative" mechanism.

The Multisite Open Channel can remain set-up during an unlimited period of time. If all of the participants leave the communication this shall not cause the Multisite Open Channel to be released.

4.1.1.1.12. Preferred Multisite Open Channel

A radio terminal may select a preferred multisite open channel, as one of the criteria for cell selection and cell reselection, as specified in part 1-3 of the specification.

4.1.1.1.13. Multi-Regional-networks MOCH

The multi-RN MOCH supplementary service enables a MOCH to be defined over a coverage involving an initiating RN and other RN.

The multi-RN MOCH shall be defined in all relevant RN.

The multi-RN shall only be set-up and released from its initiating RN.

Participation operation groups are valid on a per-RN basis. The MOCH re-entry between participating MOCHs to a same multi-RN MOCH relies only on the characteristics of each participating MOCH. The automatic re-entry shall then only be possible between participating MOCHs having the same identity (number) in their RNs.

4.1.1.2. Supplementary Services

4.1.1.2.1. Ambience listening

Ambience listening may be activated during a MOCH and consists in a remote transmission grant to a terminal, without its user being informed, so that its microphone is remotely turned on.

4.1.1.2.2. Area Selection

The coverage of a MOCH shall be defined upon MOCH creation with service management commands .

Any modification of a Multisite Open Channel requested coverage shall be taken into account for the next MOCH establishment.

4.1.1.2.3. Call Forwarding

Call Forwarding is not applicable to Multisite Open Channel.

4.1.1.2.4. Call Transfer

Call Transfer is not applicable to the Multisite Open Channel.

4.1.1.2.5. Call Waiting

Call Waiting is not applicable to Multisite Open Channel.

4.1.1.2.6. Calling Party Identification

Calling Party Identification is not applicable to Multisite Open Channel.

4.1.1.2.7. Discreet Listening

Discreet Listening is not applicable to Multisite Open Channel.

4.1.1.2.8. Dynamic Group Number Assignment

If the OG parameters of a Multisite Open Channel are modified after the set-up, the new parameters shall be taken into account after the update delay for the RSWs and the STs involved.

4.1.1.2.9. Group Merging

Group merging is not applicable to MOCH.

4.1.1.2.10. Interconnect Access

Interconnect Access is not applicable to Multisite Open Channel.

4.1.1.2.11. Intrusion

Intrusion is not applicable to Multisite Open Channel.

4.1.1.2.12. Late Entry

Late Entry shall be available on User Request and on Communication Activation.

4.1.1.2.12.1. Late Entry on User Request

A Terminal which is in Network Connected Mode within a Cell shall receive the list of the Multisite Open Channels set-up within that Cell.

The Terminal shall display the list of its authorized Open Channels as defined by OG Access Control conditions.

The user can then ask to participate in the Multisite Open Channel through spontaneous Entry.

4.1.1.2.12.2. Late Entry on Communication Activation

The Network shall signal the activation of a MOCH to the terminals through broadcast messages in the cells.

These messages shall be broadcast on a regular basis during the activation phase. Upon receipt of an activation indication for a MOCH, a system terminal may then switch to the that MOCH, if it has selected it.

4.1.1.2.13. Priority

This supplementary service shall be activated using the External Priority as a queueing priority.

The External Priority can take the values ROUTINE and FLASH. The default value shall be ROUTINE, unless the terminal user specifies FLASH priority.

4.1.1.2.14. Pre-emptive Priority

This supplementary service shall be activated using the External Priority as a priority for resource preemption.

The External Priority can take the values ROUTINE and FLASH. The default value shall be ROUTINE. unless the terminal user specifies FLASH priority.

4.1.1.2.15. Priority Scanning

A Terminal may be a candidate to a list of MOCH, including a priority MOCH and other non-priority MOCH. The maximum number of MOCH in a scanning is a constant parameter of a System Terminal.

- Upon activation of one of.the non-priorty MOCH from the list, the terminal participates into it, until it is deactivated or until the priority MOCH is activated.
- Whenever the priority MOCH is activated, the terminal switches to that MOCH until it is deactivated.

The preceding rules apply unless the user of the terminal requests to skip a currently active MOCH and resume scanning other MOCH;

When no MOCH is active while scanning in sequential listening mode, a push-to-talk request shall activate the priority MOCH.

When a MOCH is deactivated, the scanning shall be resumed and the next active MOCH shall be listened to.

4.1.1.2.16. Talking Party Identification

Talking Party Identification is available as a MOCH supplementary service.

The individual explicit address of the talking user shall be transmitted by the network. The SADP and the DC shall provide the talking party identification to the dispatchers.

4.1.1.3. Fault handling

The purpose of the fault handling functions is to attempt maintaining the MOCH service even in the event of a technical fault.

When a fault occurs, the network reconfigures automatically in order to try to maintain the service.

4.1.2. Talkgroup

4.1.2.1. Basic Service

4.1.2.1.1. Presentation

A Talkgroup service is a half duplex group communication defined for a group over a coverage area whereby traffic resources are shared between groups. A Talkgroup is permanently activable, once created at the OMC

Assuming a group member is within the coverage of the talkgroup, he may select a talkgroup. He then automatically makes a late entry and participates in the conversation until he withdraws from the talkgroup. He may also enter the talkgroup with a push-to-talk request.

4.1.2.1.2. Coverage

A Talkgroup is associated with a coverage that designates a set of trunked network resources. The coverage defines the cells and LABSs where that Talkgroup communication is available and activable.

4.1.2.1.3. Participants

A talkgroup communication concerns terminals that have selected the same group: one of these terminals activates the talkgroup to transmit and the others shall receive.

Prior to participate in any talkgroup, a terminal shall have received its list of OG.

Prerequisites for members of a group to participate into the talkgroup include:

- own the OG for that talkgroup
- select the group
- be within the talkgroup coverage
- be registered or pending registration, if previously registered within the regional network.

4.1.2.1.4. Establishment

The establishment relates to the coverage made as a set of trunked network backbones that define virtual pathes and is a network action upon operation and maintenance triggers.

4.1.2.1.5. Entry into Talkgroup

4.1.2.1.5.1. Presentation

A Terminal may enter a Talkgroup within its current Cell through:

- spontaneous entry into a Talkgroup;
- return to a Talkgroup at the end of a call;
- automatic re-entry into a Talkgroup.

4.1.2.1.5.2. Spontaneous Entry

Upon receipt from the user to enter a talkgroup, the System Terminal shall check the latest list of (OG, COV) delivered by the network.

A user can request entry into a Talkgroup. The user shall indicate the Talkgroup identity (number). The System Terminal (ST) becomes a candidate for this communication.

The network shall broadcast to the system terminal the list of the coverages established in the cell

At user request, the terminal displays the list of its authorized Talkgroups available within the current Cell. The Terminal provides the list of Talkgroups according to the COV supported by the current Cell, and the list of Talkgroups authorized for the Terminal.

4.1.2.1.5.3. Candidate state

If the user requests entry into a Talkgroup whose COV is not supported by the Cell or for which the system terminal is not authorized:

- the system terminal accepts the command and becomes a candidate for the Talkgroup;
- the system terminal informs the user that it is impossible to enter into the chosen Talkgroup.

If the user request to entry into a talkgroup but does not own the OG related to the talkgroup:

- the system terminal rejects the command and informs the user.

If the Terminal is a candidate for a Talkgroup:

- the Terminal shall inform the user as long as the entry into the Talkgroup is impossible;
- when the entry into the Talkgroup becomes possible, the Terminal shall enter automatically into this communication and shall inform the user.

4.1.2.1.5.4. Return at the end of a call

A Terminal which is participating in a Talkgroup can request an outgoing call or accept an incoming call and then start a new communication. When the terminal exits from this new communication, it can automatically re-enter the same Talkgroup.

4.1.2.1.5.5. Automatic Re-entry

If a Terminal participating in a Talkgroup leaves the Cell in which it was registered, it remains a candidate for the Talkgroup. If the Terminal then registers again within the same Cell or within another Cell, where the same Talkgroup is available, it then executes automatically a Spontaneous Entry into this communication.

The Automatic Talkgroup Re-entry feature is lost when the user commands the Terminal to cease being a candidate for the Talkgroup:

- if the user requests entry into another Talkgroup;
- if the terminal leaves the Talkgroup because the user hangs up.

In each of these cases, the Terminal deliberately and definitively leaves the Talkgroup.

4.1.2.1.6. Exit from Talkgroup

4.1.2.1.6.1. Exit events

A Terminal leaves a Talkgroup in the following cases:

- going on hook;
- entry into another call;
- loss of the link to the Network;
- loss of access right;
- coverage restriction.

4.1.2.1.6.2. Going on hook

Going on hook is a deliberate action on the Terminal user part. The Terminal leaves the Talkgroup.

The Terminal is no longer a candidate for the Talkgroup.

4.1.2.1.6.3. Entry into another call

A terminal which is participating in a Talkgroup can enter into another call directly, without having to explicitly leave the Talkgroup.

During the time while the Terminal is involved in the other call, its candidature to the Talkgroup is suspended.

Upon completion of that call and depending on the type of call, the terminal may becomea candidate for the Talkgroup again, assuming same .conditions apply as before that call. If conditions allow for a late entry, it shall re-enter the Talkgroup.

4.1.2.1.6.4. Loss of the link to the Network

If the link to the Network is lost, the Terminal shall leave the Talkgroup. It shall remain a candidate for this Talkgroup.

If the Terminal re-establishes the link to the Network, either within the same Cell or within another Cell, it shall automatically re-enter the Talkgroup, assuming same .conditions apply as before the loss of the link.

4.1.2.1.6.5. Loss of the access right

The right to participate in a Talkgroup may be modified while that Terminal is participating in a Talkgroup.

The Terminal receives these modifications from the Network. From these, it deduces the list of Talkgroups it has the right to participate in. If it looses the right to participate in the Talkgroup it is currently participating in, it shall leave the Talkgroup and inform the user.

If a Terminal which was either "registered" or "pending registration" becomes "non-registered", it shall loose its right to participate in Talkgroups.

4.1.2.1.6.6. Coverage Restriction

A COV can be restricted following a fault, the pre-emption of a resource by another call, or if it is put out service.

A Terminal which is participating in a Talkgroup associated to that COV shall leave the communication. It shall remain a candidate for the Talkgroup. It shall execute an Automatic Re-entry when the coverage is re-established.

4.1.2.1.7. Addressing

Talkgroups are addressed through an OG identifier.

4.1.2.1.8. Priority

At activation waiting queue level, between two trunked group communications, a Trunking Priority mechanism shall process the contention.

A Trunking Priority value is associated to every Talkgroup, upon creation at the OMC.

4.1.2.1.9. Access Control

A terminal is authorized to participate in a Talkgroup if it belongs to the Operational Group defined for that Talkgroup.

4.1.2.1.9.1. Anti-talkative feature

A Terminal which starts to transmit can keep transmitting for a maximum time limited by an "anti-talkative" mechanism.

4.1.2.1.10. Preferred Talkgroup

A radio terminal may select a preferred talkgroup, as one of the criteria for cell selection and cell reselection, as specified in part 1-3 of the specification.

4.1.2.2. Supplementary Services

4.1.2.2.1. Ambience listening

Ambience listening may be activated during a talkgroup and consists in a remote transmission grant to a terminal, without its user being informed, so that its microphone is remotely turned on.

4.1.2.2.2. Area Selection

The Talkgroup coverage shall be defined by the COV parameters at Talkgroup creation by Service management commands at the OMC.

Any modification of COV parameter of a Talkgroup shall be taken into account by redistribution of the Talkgroup authorization to any system terminal involved.

4.1.2.2.3. Call Forwarding

Call Forwarding is not applicable to Talkgroup communications.

4.1.2.2.4. Call Transfer

Call Transfer is not applicable to Talkgroup communications.

4.1.2.2.5. Call Waiting

Call Waiting is not applicable to Talkgroup communications.

4.1.2.2.6. Calling Party Identification

Calling Party Identification is not applicable to Talkgroup communications.

4.1.2.2.7. Discreet Listening

Discreet Listening is not applicable to Talkgroup communications.

4.1.2.2.8. Talkgroup Merging

Merging talkgroups is the action from a dispatch position whereby one or several on-going talkgroups are replaced by one equivalent service over the same coverage, where the system terminal participants of the previous talkgroups can communicate all together.

4.1.2.2.9. Dynamic Group Number Assignment

If the parameters of a Talkgroup are modified, the new parameters shall be taken into account after the update delay for the RSWs and the STs involved.

4.1.2.2.10. Interconnect Access

Interconnect Access is not applicable to Talkgroup communications.

4.1.2.2.11. Intrusion

Intrusion is not applicable to Talkgroup communications.

4.1.2.2.12. Late Entry

Late entry is available on Communication Activation

The Network shall signal the activation of a Talkgroup to the Terminals through broadcast messages. These messages are broadcast on a regular basis during the activation phase. An system terminal which did not receive the initial activation message may receive one of the following ones.

4.1.2.2.13. Scanning

A Terminal may be a simultaneously candidate to a list of talkgroups. This service is referred to as a scanning service in sequential listening mode. The maximum number of talkgroups in a scanning is a constant parameter of a system terminal. Upon activation of one of.the talkgroups from the list, the terminal participates into one of them according to the following criteria:

When no talkgroup is active, the user can activate directly the first talkgroup of the list by pressing PTT.

When a talkgroup from the list is activated and the terminal is not already participating in another talkgroup from the list, then the terminal participates into that talkgroup. Push-to-talk then apply to that talkgroup.

When this talkgroup is deactivated or on a user request to skip the currently listened-to talkgroup, the scanning shall be resumed and the next active talkgroup shall be listened to.

4.1.2.2.14. Priority Call

This supplementary service shall be activated using the user priority and the trunking priority.The system calculates an internal priority based on these parameters. A queue is defined per cell according to the internal priority in order to allocate radio resources.

The activation request which cannot be allocated a free resource shall be queued according to its internal priority and to the rule of minimal number of traffic channels guaranteed

4.1.2.2.15. Pre-emptive Priority Call

Preemptive Priority Call is not applicable to Talkgroup communications.

4.1.2.2.16. Talking Party Identification

An RFSI address shall be transmitted by the network as the talking party identification. The SADP and the DC shall provide the talking party identification to the dispatchers.

.

4.1.3. Broadcast MOCH

The Broadcast MOCH is a one-way Multisite Open Channel (MOCH) set-up at a dispatcher request. The characteristics of a Broadcast MOCH are:

- participation of the recipient STs shall be required;
- recipient RTs shall be those located under the MOCH's coverage and belonging to its associated Operational Groups (OGs);
- ST's Push-to-Talk shall be suspended: STs are not allowed to transmit, they only receive what Dispatch Positions (Stand Alone or at Dispatch Centre) transmit;
- the External Priority shall be set by the System.

Broadcast MOCH set-up shall be possible from a Dispatch Position (Stand Alone or at Dispatch Centre) . It consists in selecting the appropriate MOCH identifier to set-up the associated MOCH with broadcast Priority.

The dispatcher requesting the set-up shall belong to the set-up Operational Group of this MOCH. If the MOCH access is authorized without restrictions, any system terminal may be involved, whatever its Operational Group is.

4.1.4. Group call

4.1.4.1. Basic Service

4.1.4.1.1. Presentation

A group call is a point-to-multipoint group-addressed call over a predefined coverage, whereby the calling party communicates with a group he selects.

The calling party is not a member of the called group, otherwise the talkgroup service applies.

Terminals that are within the coverage of the group and that are members of that group shall be able to participate to the group call. Entry into the group call make them communicate with other members of the same group and with the calling party.

4.1.4.1.2. Coverage

A group call is associated with a coverage that designates a set of cells.

4.1.4.1.3. Participants

4.1.4.1.3.1. Calling terminal

A terminal owns a list of groups it is allowed to call, or may call any group depending on partitionning requirements. This list defines emission rights for the terminal.

The calling terminal shall be within the coverage of the called group.

4.1.4.1.3.2. Called terminals

Apart from the calling party, participants in a group call shall be STs that are within the coverage of the group call and that are members of that group.

A terminal shall participate to any group call associated to the groups it belongs to.

A System Terminal can participate in a group call if it is registered or pending registration. It shall have been registered previously within the Regional network, and be aware of its authorization to participate in the group call.

4.1.4.1.4. Set-up

The group call is setup and activated over the coverage of the group.

4.1.4.1.5. Release

The group call is released by the network.

4.1.4.1.6. Entry into a group call

The same mechanism as for talkgroup applies.

4.1.4.1.7. Exit from a group call

The same mechanism as for talkgroup applies.

4.1.4.1.8. Addressing

Groups are addressed through an OG identifier.

4.1.4.1.9. Priority

Upon activation of a trunked group call, a Trunking Priority mechanism shall process the contention with other calls. A Trunking Priority value is associated to every group call, as defined at the OMC.

4.1.4.1.10. Access Control

Apart from the calling terminal, a terminal is authorized to participate in a group call if it is a member of the operational group.

4.1.4.1.11. Anti-talkative feature

A Terminal which starts to transmit can keep transmitting for a maximum time limited by an "anti-talkative" mechanism.

4.1.4.2. Supplementary Services

4.1.4.2.1. Area Selection

The coverage of a group call is the coverage associated to the called group, as defined with Service management commands.

4.1.4.2.2. Call Forwarding

Call Forwarding is not applicable to group call.

4.1.4.2.3. Call Transfer

Call Transfer is not applicable to group call.

4.1.4.2.4. Call Waiting

Call Waiting is not applicable to group call.

4.1.4.2.5. Calling Party Identification

Calling Party Identification is not applicable to group call.

4.1.4.2.6. Discreet Listening

Discreet Listening is not applicable to group call.

4.1.4.2.7. Dynamic Group Number Assignment

If the parameters of a group call are modified, the new parameters shall be taken into account after the update delay for the RSWs and the STs involved.

4.1.4.2.8. Interconnect Access

Interconnect Access is not applicable to group call.

4.1.4.2.9. Intrusion

Intrusion is not applicable to group call.

4.1.4.2.10. Late Entry

Late entry is available on Communication Activation

The Network shall signal the activation of a group call to the Terminals through broadcast messages. These messages are broadcast on a regular basis during the activation phase. An system terminal which did not receive the initial activation message may receive one of the following ones.

4.1.4.2.11. Scanning

Scanning is not applicable to group call.

4.1.4.2.12. Priority Call

This supplementary service shall be activated using the user priority and the trunking priority.

The system calculates an internal priority based on these parameters.

The activation request which cannot be allocated a free resource shall be queued according to priority rules as defined in part 1.3 of the specification.

4.1.4.2.13. Pre-emptive Priority Call

Preemptive Priority Call is not applicable to group call.

4.1.4.2.14. Talking Party Identification

Talking Party Identification is available as a group call supplementary service.

An RFSI address shall be transmitted by the network as the talking party identification. The SADP and the DC shall provide the talking party identification to the dispatcher.

4.1.4.2.15. Barring of incoming/outgoing call

Barring is not applicable to group calls.

4.1.4.2.16. Notification

A terminal may be notified a group call activation.

4.1.4.2.17. Do not disturb

Do not disturb is not applicable to group call.

4.2. Private communications

4.2.1. Individual Call

4.2.1.1. Basic Service

4.2.1.1.1. Presentation

An Individual Call sets up a voice communication between a Calling Party and a Called Party.

4.2.1.1.2. Participants

Calling and Called Parties shall be registered System Terminals exclusively.

4.2.1.1.3. Coverage

The Calling Party can request for an Individual Call to be routed to a Called Party registered in any Cell of the system.

If the Called Party's RN is unknown to the routing tables of the calling Party's Visited Radioswitch, the call shall be rejected.

4.2.1.1.4. Set-up of Individual Call

4.2.1.1.4.1. Authorized Terminals for Set-up

This subject is dealt with in subclause: "Call Authorization".

4.2.1.1.4.2. Execution of Set-up

The Network shall locate the Called Party and set-up a voice circuit between the Calling Party's and the Called Party connection reference points.

The Calling Party's RSW and the Called Party's RSW shall request radio traffic resources for the call. When the resources are assigned to the communication, the Network shall open the communication.

The Called Party's RSW shall make the call to the Called Party's Terminal. The call procedure shall depend on the Called Party's communication status.

The call is active when the Called Party answers (either automatically or manually).

4.2.1.1.5. Release of Individual Call

A Terminal leaves an Individual Call in the following cases:

- going on hook;
- loss of the link to the Network;
- Individual Call Release.

4.2.1.1.5.1. User withdrawal

Going on hook is a deliberate action on the user's part at the Terminal. It shall cause the terminal to leave the call. It may then, depending on the case:

- either enter the Stand-by status;
- or make a late entryinto a group communication previously selected before the individual call occured.

4.2.1.1.5.2. Loss of the link to the Network

When it looses the link to the Network, the Terminal shall leave the call definitively. This applies also when changing cell while roaming.

4.2.1.1.5.3. Call Release

The following events shall cause a normal release of the call:

- the calling or the called Terminal withdraws from the call;
- the call is released by the Network due to voice inactivity;
- the call is released due to a remote call clearing action.

The following events shall cause an aBNormal release of the call:

- a failure occurs in the voice circuit between the participants;
- a radio resource is lost;
- a radio resource or a Voice Circuit resource is pre-empted by the System in favour of another call.

If a Terminal is participating in a call and this call is released, the Terminal shall behave as in subclause: "Going on Hook".

4.2.1.1.6. Remote call clearing of the Individual Call

4.2.1.1.6.1. Authorized Terminals

A SADP or DC, and the OMC shall be authorized to remotely clear an individual call.

The dispatcher requesting the remote clearing of an individual call should belong to the same Fleet as one of the participants (Calling or Called Terminal).

A Network Management Function available at the OMC also makes it possible to release an Individual Call.

4.2.1.1.7. Addressing

The address entered for an individual call set-up request may be:

- an individual explicit address;
- an individual implicit address.

4.2.1.1.8. Priority

Priority rules are dealt with in part 1.3 of this specification..

4.2.1.1.9. Access Control

Any Terminal authorized to make an Individual Call can call any Terminal in the System.

4.2.1.1.10. Anti-talkative feature

A terminal which has started transmitting can keep transmitting for a maximum amount of time which shall be limited by an "anti-talkative" mechanism.

4.2.1.2. Supplementary Services

4.2.1.2.1. Ambience listening

Ambience listening may be activated during an individual call and consists in a remote transmission grant to the called terminal, without the called user being informed.

4.2.1.2.2. Area Selection

The Individual Call coverage shall be selected by the Network according to the Calling and Called Party locations.

4.2.1.2.3. Call Forwarding

In an Individual Call, the Called Terminal can be forwarded unconditionally.

4.2.1.2.4. Call Transfer

Call Transfer is authorized by Terminal configuration.

Call Transfer shall apply to an already set-up Individual Call. It shall allow the Called Party to transfer the call to a new Called Party so that the communication is set-up between the Calling Party and the new Called Party. The previous Called Party, who asked for the Transfer, shall leave the call definitively. The calling party is informed of the new called party address.

The new Called Party shall meet the Called Party requirements for Individual Calls.

If the new Called Party is identified by a PABX Gateway address, the Individual Call shall automatically become an "Interconnect Call".

The Call Transfer set-up conditions shall be identical to those of Individual Calls.

If the Call Transfer fails, the call is released.

4.2.1.2.5. Call Waiting

The Individual Call set-up procedure shall offer call queuing if no radio resource is available on the Calling Party or on the Called Party side;

If, at time-out, the call is not set-up, then it is removed from the queue and cancelled. The calling Terminal shall be advised.

4.2.1.2.6. Calling Party Identification

The Calling Terminal address shall be transmitted to the Called Terminal along with the call signalling.

4.2.1.2.7. Discreet Listening

Discreet Listening is not applicable to the individual call.

4.2.1.2.8. Dynamic Group Number Assignment

Dynamic Group Number Assignment is not applicable to the Individual Call.

4.2.1.2.9. Group Merging

Group Merging is not applicable to the Individual Call.

4.2.1.2.10. Interconnect Access

Interconnect Access to an external PABX is available as a supplementary service to the Individual Call. This subject is dealt with in subclause: "Interconnect Call".

4.2.1.2.11. Intrusion

Individual Calls shall allow intrusion from Dispatch Positions (SADP or DC) and authorized line connected terminals as an option.

The authorized party requesting intrusion in an individual call should belong to the same fleet as either the calling terminal or the called terminal..

4.2.1.2.12. Late Entry

Late Entry is not applicable to the Individual Call.

4.2.1.2.13. Priority Call

This supplementary service shall be activated using the external priority and the user priority.

The External Priority can take the values ROUTINE or FLASH. The default value shall be ROUTINE. The Calling Terminal can specify the FLASH Priority.

Using this priority and according to priority rules, the system calculates an internal priority.

The Individual Call shall become a Priority Call if its internal priority is greater than that of the calls waiting for resources and lower than the retention priority of the established calls.

4.2.1.2.14. Pre-emptive Priority Call

This supplementary service shall be activated using the External Priority.

The External Priority can take the values ROUTINE and FLASH. The default value shall be ROUTINE. The terminal which enters the Set-up command can specify the FLASH priority.

With this priority and according to the priority rules, the system calculates an internal priority.

The Individual Call shall become a Preemptive Priority Call if its internal priority is greater than the retention priority of the established calls.

4.2.1.2.15. Scanning

Scanning is not applicable to the Individual Call.

4.2.1.2.16. Silent call

The silent call supplementary service enables to setup an individual call with automatic hook-off at the called terminal side, without the called user being informed.

4.2.1.2.17. Talking Party Identification

Talking Party Identification is available as an Individual Call supplementary service. An RFSI address shall be transmitted by the network as the talking party identification. The SADP and the DC shall provide the talking party identification to the dispatcher.

4.2.2. Multiparty Call

4.2.2.1. Basic Service

4.2.2.1.1. Presentation

A Multiparty Call is a private voice call between a Calling Party and several Called Parties. The maximum number of called parties is a system constant parameter.

4.2.2.1.2. Participants

Calling and Called Parties shall be registered System Terminals exclusively.

4.2.2.1.3. Coverage

A Multiparty Call is routed to the called parties wherever they are located in the system.

4.2.2.1.4. Set-up of Multiparty Call

4.2.2.1.4.1. Authorized Terminals for Set-up

The subject of the authorized terminals for Multiparty Call Set-up is dealt with in subclause: "Call Authorization".

4.2.2.1.4.2. Execution of Set-up

The Network shall locate the called Parties. It may not be able to locate some of them. The procedure shall continue with those Called Parties who can be located in the Regional network.

The Network shall set up a voice circuit on the fixed Network between the Calling Party's RSW and the Called Parties' RSWs. The necessary resources shall be allocated to the call.

The Network shall request radio resources for each Base Station involved in the call. The request has a waiting condition which is protected by a time-out.

The waiting for the radio resources shall end either when all the requested radio resources are allocated or when the time-out expires. The call shall proceed with all the Called Parties for whom radio resources has been allocated.

The next step shall consist in calling the Called Parties. The communication shall be activated when the first Called Party answers.

4.2.2.1.5. Release of Multiparty Call

An system terminal shall leave a Multiparty Call in the following cases:

- going on hook;
- loss of the link to the Network;
- Multiparty Call Release.

The following events shall cause a Normal Release of the Multiparty Call:

- the Calling Party or the last Called Party still in the call exits the call;
- the call is released by the Network due to voice inactivity;
- the call is released due to a remote call clearing action.

The following events shall cause an ABNormal Release of the Multiparty Call:

- a failure occurs in the voice circuit link to the calling Party or the last called Party still in the call;
- a voice circuit resource link to the Calling Party or to the last Called Party still in the call is pre-empted by the System.

4.2.2.1.6. Remote call clearing of a Multiparty Call

4.2.2.1.6.1. Authorized Terminals

Dispatch Positions (Stand Alone or at Dispatch Centre) and OMCshall be authorized to remotely clear Multiparty Calls.

The dispatcher requesting the release of a Multiparty Call should belong to the same Fleet as one of the participants (calling or called Terminal).

4.2.2.1.7. Addressing

The Called Parties addresses shall be entered:

- a sequence of up to 4 individual addresses;
- or as a list address.

4.2.2.1.8. Access Control

Access control is not applicable to the Multiparty Call.

4.2.2.1.9. Anti-talkative feature

A Terminal which has started transmitting can keep transmitting for a maximum amount of time which shall be limited by an "anti-talkative" mechanism.

The communication duration itself shall only be limited by a Release mechanism which shall release the call if no system terminal has requested transmission (no PTT depression) during a given amount of time (call release on voice inactivity).

4.2.2.2. Supplementary Services

4.2.2.2.1. Ambience listening

Ambience listening may be activated during a multiparty call and consists in a remote transmission grant to the called terminal, without the called user being informed.

4.2.2.2.2. Area Selection

The Multiparty Call coverage shall be selected by the Network according to the locations of the actual participants.

All participants shall be located within the same Regional network. Called Terminals located out of the Calling Party's RN shall not participate in the Multiparty Call.

4.2.2.2.3. Call Forwarding

In a Multiparty Call, a Called Terminal can be forwarded. The Host Terminal address shall replace the Forwarded Terminal address in the list of Called Party addresses.

The Host Terminal shall be located within the same visited Regional network, otherwise the Call Forwarding shall fail.

4.2.2.2.4. Call Transfer

Call Transfer is not applicable to the Multiparty Call.

4.2.2.2.5. Call Waiting

The Multiparty Call Set-up procedure shall offer Call queuing in the following cases:

- no TCH is available for the Calling Party or for a Called Party;
- a Called system terminal is busy or does not reply to the call signalling.

At time-out:

- if none of the Called Parties is able to participate in the call, the call shall not be queued but lost. The calling Terminal shall be advised;
- if only some of the called Parties have answered, the call shall be lost for the other Called Parties.

4.2.2.2.6. Calling Party Identification

Calling Party Identification is applicable to the Multiparty Call.

The Calling Terminal address is transmitted to the called Terminals.

4.2.2.2.7. Discreet Listening

Discreet Listening is not applicable to a Multiparty Call.

4.2.2.2.8. Dynamic Group Number Assignment

Dynamic Group Number Assignment is not applicable to the Multiparty Call.

4.2.2.2.9. Group Merging

Group Merging is not applicable to the Multiparty Call.

4.2.2.2.10. Interconnect Access

Interconnect Access not applicable to the Multiparty Call.

4.2.2.2.11. Intrusion

Multiparty Calls shall allow Intrusion only from Dispatch Positions (SADP or DC) or authorized line connected terminals, as an option.

The dispatcher requesting Intrusion in a Multiparty Call should belong to the same Fleet as the calling terminal or one of the called terminals.

4.2.2.2.12. Late Entry

Late Entry is not applicable to the Multiparty Call.

4.2.2.2.13. Priority Call

Priority Call is applicable to the Multiparty Call as it is to the Individual Call.

4.2.2.2.14. Pre-emptive Priority Call

Pre-emptive Priority Call is applicable to the Multiparty Call as it is to the Individual Call.

4.2.2.2.15. Scanning

Scanning is not applicable to multiparty calls.

4.2.2.2.16. Talking Party Identification

Talking Party Identification is available as a Multiparty Call supplementary service. An RFSI address shall be transmitted by the network as the talking party identification. The SADP and the DC shall provide the talking party identification to the dispatcher.

4.2.2.3. Fault handling

If the Calling Party and one Called Party remain in the call, it shall continue with the remaining participants. If there is either no Calling Party or no Called Party remaining in the call, it shall be released.

4.2.3. Interconnect Call

The Interconnect Call is an Individual Call where the Interconnect Access supplementary service is activated.

Calls may be routed to an SADP for dispatcher authorization.

Extra facilities may be provided through a dispatch centre.

4.2.3.1. Basic Service

4.2.3.1.1. Presentation

An Interconnect Call shall set-up a communication between a TETRAPOL subscriber and a PABX subscriber. Incoming calls refer to calls from the PABX to the SwMI; outgoing calls refer to calls from the SwMI to the PABX.

The PABX gateway shall support:

- outgoing calls from a TETRAPOL subscriber to a PABX user, identified with a number in the PABX numbering plan.
- outgoing calls from a TETRAPOL subscriber to a default PABX user
- incoming calls from a PABX user to an addressed TETRAPOL subscriber, identified with an address in the TETRAPOL addressing plan.
- incoming calls from a PABX user to a default TETRAPOL subscriber, e.g. an SADP dispatcher

4.2.3.1.2. Participants

The participants in an Interconnect Call shall be:

- a registered System Terminal;
- a user connected to or throught the PABX;

4.2.3.1.3. Coverage

A call from the SwMI to a PABX shall be routed through a PABX gateway located in the regional network of the TETRAPOL calling subscriber.

A call from a PABX to a TETRAPOL called subscriber shall be routed from the PABX gateway to the cell where the called subscriber is actually located.

4.2.3.1.4. Set-up of the Outgoing Interconnect Call

The outgoing Set-up process within the System shall be the same as that of an Individual Call.

If an extension number is specified by the Calling ST, it must be dialled in the PABX numbering plan (may be local or external number): this extension shall be transparently transmitted by the PABX Gateway to the PABX.

If no extension number is given by the Calling ST, the PABX Gateway shall provide a default PABX number..

The PABX Gateway shall manage the signalling interface so that the System can detect when the Called Party goes off hook.

4.2.3.1.5. Set-up of the Incoming Interconnect Call

An incoming interconnect call request shall be routed like an individual call request in the network, either to the called system terminal whose address has been provided in the request, or to a predefined address, e.g. an SADP address.

4.2.3.1.6. Communication Established

The call is half-duplex. A "voice activity detection" algorithm is implemented to interface the half-duplex System with the duplex PABX.

All other conditions shall be the same as those applicable to an Individual Call.

4.2.3.1.7. Exit from Interconnect Call

The conditions for leaving an Interconnect Call shall be the same as those applicable to an Individual Call.

4.2.3.1.8. Release of Interconnect Call

The conditions for releasing an Interconnect Call shall be the same as those applicable to an Individual Call.

4.2.3.1.9. Addressing

The address provided as a parameter to an outgoing Interconnect Call request shall be the RFSI address of the PABX gateway.

In addition, a subaddress may be provided in the PABX numbering plan

4.2.3.1.10. Priority

The Outgoing Interconnect Call External Priority shall be identical to that of an Individual Call. Priority is taken into account up to the PABX Gateway, and is not transmitted to the PABX.

The Incoming Interconnect Call External Priority shall be ROUTINE.

4.2.3.1.11. Access Control

Access Control is not applicable to Interconnect Calls. A terminal which is authorized to make a private call Call may call a PABX Gateway, using the appropriate PABX gateway implicit address. An incoming call from a PABX gateway may address any TETRAPOL subscriber.

4.2.3.1.12. Call Authorization

Interconnect Calls have a Call Authorization Control which shall use the Discrimination parameter.

4.2.3.2. Supplementary Services

4.2.3.2.1. Area Selection

Area selection is not applicable to Interconnect Calls.

4.2.3.2.2. Call Forwarding

If the Recipient Terminal of an Incoming Interconnect Call is forwarded, the System shall forward the call as it would do for an Individual Call.

The PABX Gateway address shall not be forwarded.

4.2.3.2.3. Call Transfer

Incoming Interconnect Calls allow Call Transfer by the Called system terminal to another ST. Transfer mechanisms shall be the same as those applicable to an Individual Call.

4.2.3.2.4. Call Waiting

Not applicable to interconnect calls

.4.2.3.2.5. Calling Party Identification

The calling system terminal address is not transmitted to the called PABX.

The calling PABX Gateway address (or a better explicit information) shall be transmitted to the called ST.

4.2.3.2.6. Discreet Listening

Discreet listening is not applicable to the Interconnect Call.

4.2.3.2.7. Dynamic Group Number Assignment

Dynamic Group Number Assignment is not applicable to the Interconnect Call.

4.2.3.2.8. Group Merging

Group Merging is not applicable to the Interconnect Call.

4.2.3.2.9. Interconnect Access

Interconnect Access is activated in the case of Interconnect Call.

4.2.3.2.10. Intrusion

Interconnect Calls shall allow Intrusion in the same conditions as for individual calls.

4.2.3.2.11. Late Entry

Late Entry is not applicable to Interconnect Calls.

4.2.3.2.12. Priority Call

Priority Call is applicable to the Outgoing Interconnect Call as it is to the Individual Call.

Priority Call is not applicable to the Incoming Interconnect Call.

4.2.3.2.13. Pre-emptive Priority Call

Pre-emptive Priority Call is applicable to the Outgoing Interconnect Call as it is to the Individual Call.

Pre-emptive Priority Call is not applicable to the Incoming Interconnect Call.

4.2.3.2.14. Priority Scanning

Priority Scanning is not applicable to the Interconnect Call.

4.2.3.2.15. Talking Party Identification

Talking Party Identification is not available as an Interconnect Call supplementary service. An RFSI address shall be transmitted by the network as the talking party identification. The SADP and the DC shall provide the talking party identification to the dispatcher.

4.2.3.3. Fault handling

Identical to fault handling in the Individual Call case.

4.3. Emergency communications

4.3.1. Emergency Call

4.3.1.1. Basic Service

4.3.1.1.1. Presentation

Upon request from a user in emergency situation, an emergency call shall be activated The resulting action depends on the state of the terminal and the network at the time of the call.

4.3.1.1.2. Participants

Emergency Calls shall be transmitted to the network only from registered Radio Terminals in Network Mode. Direct mode emergency calls apply to terminals operating in direct mode.

4.3.1.1.3. Sequence of events

A user of a radio terminal may request an emergency call by depressing the special emergency button of a radio terminal.
The operation of an emergency call depends on the configuration of the initiating terminal, on his organization profile, and on whether the cell where it is located is not in fallback mode.

If a user of a radio terminal makes an emergency call request, pending the terminal registration in a cell, the terminal shall use a high Priority level to request registration in the cell. Once registered, the radio terminal shall transmit the Emergency Call to the Network.

The outcome of an emergency call for a terminal in network mode is as follows. If the terminal is located in a cell that is not isolated from the rest of the network, the network informs predefined dispatchers and may selects one of the following exclusive actions

- Automatic crisis open channel establishment: A crisis open channel may be automatically established over a coverage, as predefined by the tactical operator for the organization of the initiating user.
- Automatic emergency open channel establishment: An emergency open channel may be automatically established in the cell where the initiating terminal is located.
- Dispatch-acknowledged crisis open channel establishment: Predefined dispatchers are informed of the emergency call requested by the initiating user. A dispatcher may accept and acknowledge the crisis open channel establishment for the related organization. The initiating user is then informed of the outcome of his request.

The predefined dispatchers usually belong to the same organization as the initiating user. The coverage of the crisis open channel depends on the location of the initiating user, as predefined for the organization of the initiating user in the cell where he is located.

- Dispatch private communication: Predefined dispatchers are informed of the emergency call requested by the initiating user. A dispatcher may reject the crisis open channel establishment and either accept to establish a private communication to the initiating user with emergency priority. The initiating user is then informed of the outcome of his request.
- Dispatch rejection of the emergency call: Predefined dispatchers are informed of the emergency call requested by the initiating user. A dispatcher may reject to neither establish a crisis open channel nor establish a private communication with the initiating terminal. The initiating user is then informed with a negative acknowledgment.
- Dispatch-requested emergency open channel establishment: The establishment of the emergency open channel may be manually requested by a dispatcher, upon being informed of the emergency call request or whenever as a dispatcher's choice.

Emergency outcome in isolated-cell fallback network mode

- Automatic emergency open channel establishment: The initiating terminal may automatically enter into a local emergency open channel automatically established in the isolated cell.

Emergency outcome if the initiating terminal receives no reply from the network

- Switch from crisis open channel to emergency open channel: In case a crisis open channel can not be established, then the network establishes an emergency open channel as a fallback mode communication.

- Switch to direct mode emergency as a fallback mode: If the initiating terminal receives no acknowledgment reply from the network and no communication has been established after a certain time and if the terminal is personalized to support direct mode emergency, then the terminal establishes a direct mode emergency call. The nature of the communication resulting from the call is indicated to the user, once the communication is established.

The emergency call has the following outcome in direct mode

- Direct mode emergency call: If the terminal is in direct mode, or out of the network coverage, then the emergency call may be optionally a direct mode emergency call , assuming direct mode emergency is supported by the terminal.

4.3.1.2. Supplementary Services

There are no Supplementary Services applicable to the Emergency Call.

There is no interaction with any call unrelated supplementary service, hence a forwarded terminal may issue an emergency call request.

4.3.2. crisis open channel

4.3.2.1. Basic service

4.3.2.1.1. Presentation

A crisis open channel enables a calling user who requested an emergency call to communicate with up to 5 groups of terminal users when they are located over a predefined set of cells.

4.3.2.1.2. Participants

Groups of terminals and SADP and dispatch centres concerned by a crisis open channel are identified with an establishment OG and a list of participation Ogs associated to the crisis open channel:

The users of terminals or dispatchers allowed to establish or release the crisis open channel are the members of a group identified by the establishment OG of the crisis open channel.

The users that want to participate in the crisis open channel shall select the crisis open channel and shall be members of groups that are listed as the participation Ogs, provided upon crisis open channel establishment, or per default as defined at the crisis open channel creation.

When a user selects a crisis open channel on his terminal, he may then request to transmit and the other users that have selected the crisis open channel on their terminal may receive.

Prior to participate in any crisis open channel, a terminal shall have received its list of allowed Ogs.

4.3.2.1.3. Coverage

A crisis open channel is defined over a set of cells, defined as a coverage.

4.3.2.1.4. Establishment and release

A user of a terminal or a dispatcher may be allowed to establish and release a crisis open channel, if his terminal owns the establishment OG for the crisis open channel and if the terminal is within the coverage associated with the crisis open channel.

In order to establish the crisis open channel, the user indicates the crisis open channel reference number and optionally a set-up priority.

The terminal that requests the establishment of the crisis open channel actually participates to the crisis open channel only if it owns one of the participation OG of the crisis open channel.

If the crisis open channel does not span over more than one regional network, the dispatcher may provide a list of participation OG that overrides the default list.

A terminal may enter a crisis open channel by:

- a spontaneous entry into a crisis open channel selected by the user,
- an automatic re-entry into a selected crisis open channel, at cell roaming,
- a return to the selected crisis open channel at the end of a private call or a data transfer.

A user of a terminal may display a list of crisis open channel he is allowed to operate on. A SADP dispatcher may supervise the operational state of the coverage of a crisis open channel. A SADP dispatcher may display the operational state of the crisis open channel he is allowed to supervise, including also those that are created but not established and list their OG, and may supervise their activations.

Participation in the crisis open channel: If a crisis open channel is indicated in the list of authorized crisis open channel in the terminal,its user may participate in this crisis open channel.

The network provides the radio terminal with a list of the crisis open channel that are defined in the cell where the radio terminal is registered and the list of OGs that are allowed for the terminal. These lists is updated whenever there is a change.

A user of a terminal, that participates in a crisis open channel, may request transmission by pressing the push-to-talk button of the terminal.

- If the current cell is not within the effective coverage of the crisis open channel, the request is rejected by the terminal,

- If the crisis open channel is not active, then the crisis open channel is activated and the network transmits the voice to the other participants of the crisis open channel.

- If the crisis open channel is already active, the network transmits the voice to other terminals.

The dispatcher has a preemptive priority to transmit over radio terminals.

Leaving a crisis open channel: A terminal leaves a crisis open channel in the following cases:

- hang up,

- entry into another call,

- loss of the link to the network,

- loss of the right to take part in the crisis open channel

- out of crisis open channel coverage.

A user may temporarily leave a crisis open channel in order to establish or receive a private call.

If the link to the network is lost, the terminal leaves the crisis open channel but remains as a candidate for this crisis open channel.

If the terminal re-establishes the link to the network, either under the same cell or under another cell, it may, in the stated cases, automatically re-enter the crisis open channel.

4.3.2.2. Supplementary Services

4.3.2.2.1. Ambience listening

Ambience listening may be activated during a crisis open channel and consists in a remote transmission grant to a terminal, without its user being informed, so that its microphone is remotely turned on.

4.3.2.2.2. Area Selection

The coverage of a crisis open channel shall be defined with service management commands .

Any modification of a coverage of a crisis open channel shall be taken into account for the next establishment of the crisis open channel.

4.3.2.2.3. Call Forwarding

Call Forwarding is not applicable to crisis open channel.

4.3.2.2.4. Call Transfer

Call Transfer is not applicable to crisis open channel.

4.3.2.2.5. Call Waiting

Call Waiting is not applicable to crisis open channel.

4.3.2.2.6. Calling Party Identification

Calling Party Identification is not applicable to crisis open channel.

4.3.2.2.7. Discreet Listening

Discreet Listening is not applicable to crisis open channel.

4.3.2.2.8. Dynamic Group Number Assignment

If the OG parameters of a crisis open channel are modified after the set-up, the new parameters shall be taken into account after the update delay for the RSWs and the STs involved.

4.3.2.2.9. Group Merging

Group merging is not applicable to crisis open channel.

4.3.2.2.10. Interconnect Access

Interconnect Access is not applicable to crisis open channel.

4.3.2.2.11. Intrusion

Intrusion is not applicable to crisis open channel.

4.3.2.2.12. Late Entry

Late Entry shall be available on User Request and on Communication Activation.

4.3.2.2.12.1. Late Entry on User Request

A Terminal which is in Network Connected Mode within a Cell shall receive the list of the crisis open channel established in that Cell.

The Terminal shall display the list of its authorized Open Channels as defined by OG Access Control conditions.

The user can then ask to participate in the crisis Open Channel through spontaneous Entry.

4.3.2.2.12.2. Late Entry on Communication Activation

The Network shall signal the activation of a crisis open channel to the terminals through broadcast messages in the cells.

These messages shall be broadcast on a regular basis during the activation phase. Upon receipt of an activation indication for a crisis open channel, a system terminal may then switch to that crisis open channel, if it has selected it.

4.3.2.2.13. Priority

This supplementary service shall be activated using the External Priority as a queueing priority.

The External Priority can take the CRI SIS value

4.3.2.2.14. Pre-emptive Priority

This supplementary service shall be activated using the External Priority as a priority for resource preemption.

The External Priority can take the CRISIS value

4.3.2.2.15. Priority Scanning

A Terminal may be a candidate to a list of MOCH and crisis open channels, including a priority MOCH and other non-priority MOCH. The maximum number of MOCH in a scanning is a constant parameter of a System Terminal.

- Upon activation of one of.the non-priorty MOCH from the list, the terminal participates into it, until it is deactivated or until the priority MOCH is activated.
- Whenever the priority MOCH is activated, the terminal switches to that MOCH until it is deactivated.

The preceding rules apply unless the user of the terminal requests to skip a currently active MOCH and resume scanning other MOCH;

When no MOCH is active while scanning in sequential listening mode, a push-to-talk request shall activate the priority MOCH.

When a MOCH is deactivated, the scanning shall be resumed and the next active MOCH shall be listened to.

4.3.2.2.16. Talking Party Identification

Talking Party Identification is available as a supplementary service for crisis open channel.

The individual explicit address of the talking user shall be transmitted by the network. The SADP and the DC shall provide the talking party identification to the dispatchers.

4.3.2.3. Fault handling

The purpose of the fault handling functions is to attempt maintaining the MOCH service even in the event of a technical fault.

When a fault occurs, the network reconfigures automatically in order to try to maintain the service.

4.3.3. Emergency Open Channel

4.3.3.1. Basic Service

4.3.3.1.1. Presentation

An emergency open channel enables an initiating user to communicate with any terminal users, when they are located in the same cell.

An emergency open channel is a message-trunked group communication established within a pre-defined coverage including one radio cell, using the emergency preemptive priority if they are in the same radio cell.

4.3.3.1.2. Coverage

The coverage of the Emergency Open Channel shall be defined for each radio cell. It shall include:

- the radio Base Station of the cell where the Emergency Call is initiated;
- a number of Line Access Base Stations within the same RN as the initiating Cell, as part of the coverage of the Emergency Open Channel.

There shall be a maximum number of Line Access Base Stations within the coverage of an Emergency Open Channel.

4.3.3.1.3. Access control

Any Terminal in the coverage of an Emergency Open Channel can participate in this communication.

Registration requirements shall be identical to those applicable to Multisite Open Channels.

Participation in the Emergency Open Channel shall not be subject to Operational Group Access Control.

4.3.3.1.4. Main steps

Executing the Emergency Call to the Network shall consist of two independent processes:

- the RT shall send an Emergency Status message to the Network; the Network shall deliver this status message to a predefined set of SADPs and a DC;
- the RT or a SADP or a DC shall transmit an Emergency Open Channel request to the Network; the Network shall set up the Open Channel on the available coverage; it shall then broadcast an Emergency Notification signalling on this coverage.

4.3.3.1.5. Set-up of Emergency Open Channel

4.3.3.1.5.1. Purpose of Set-up

Emergency Open Channel Set-up consists in effectively establishing the Open Channel on the Network.

The Emergency Open Channel Set-up shall allocate the necessary System resources to this communication with an emergency priority.

4.3.3.1.5.2. Conditions for Set-up

An Emergency Open Channel shall be created before Set-up.

4.3.3.1.5.3. Execution of Set-up

The Emergency Open Channel shall be automatically set-up by the System when it receives the Emergency Call.

A message shall be sent to the OMC of the Regional network. This message shall include the address and location of the terminal which originated the Emergency Call.

The Network shall set up the Emergency Open Channel on the Cell, LCTs, SADPs and DC within coverage. At time-out, the System shall open the Emergency Open Channel even if it has not been able to introduce in the actual coverage all the LCTs, SADPs and DC of the nominal coverage. These can be introduced in the coverage later on, as they become available.

If an Emergency Open Channel is already set-up within the Cell when the Emergency Call is received, the System shall not set-up a new Emergency Open Channel, it shall use the one which is already set-up.

In both cases, the Network shall broadcast - a predefined number of times - an Emergency Notification signalling on all the Channels of the Radio Cell and to the LCTs, SADPs and DC in the actual coverage on communication activation.

4.3.3.1.6. Emergency Notifications

4.3.3.1.6.1. Presentation

The Network shall broadcast an Emergency Notification to the actual coverage of the Emergency Open Channel. It shall be broadcast after the Emergency Open Channel has been set-up. It shall be broadcast several times.

The Emergency Notification shall include the address of the RT which originated the Emergency Call to the Network.

Upon receipt of an emergency notification, a terminal that is within the coverage is thus informed of the existence of a set-up Emergency Open Channel as they would be for a Multisite Open Channel and can make a late entry into the Emergency Open Channel.

Terminals with "Emergency Notification Signalling" activated by configuration shall alert their user when they receive Emergency Notifications. Terminals with "Emergency Notification Signalling" not activated by configuration shall not alert their user when they receive Emergency Notifications.

4.3.3.1.6.2. Notification Handling

Upon receipt of an emergency notification, Terminals that are configured to alert the user shall alert their user with an Emergency tone. The address of the RT which sent the Emergency Call shall be displayed.The alerted user may either accept the Emergency Call or refuse it.

Upon acceptance by the alerted user, or automatically, the terminal shall makean Entry into the Emergency Open Channel. From then on, the user shall no longer be disturbed by the signalling for that Emergency Call. He only will be alerted in case of other Emergency Notifications.

Upon refusal from the alerted user, the terminal communication status is not modified. The user shall no longer be disturbed by the Emergency Notification for this Emergency Call.

If there are several successive Emergency Calls, the user shall receive a different Emergency Notification for each call. If the user remains in the Emergency Open Channel, it shall only be alerted once for Emergency Notifications originated by the same Terminal.

4.3.3.1.6.3. Radio Terminals

Radio Terminals can only receive Emergency Notifications for the Emergency Open Channel set-up within their Visited Cell. These notifications may signal Emergency Calls originated by several RTs.

When a Terminal participates in an Emergency Open Channel, it shall receive the Emergency Notifications transmitted within its Visited Cell. When this happens, the terminal shall signal to the user in a specific way the occurrence of an Emergency Call within the Cell. No action shall be required on the user part.

4.3.3.1.6.4. Line Connected Terminals and Dispatch Positions

LCTs, SADPs and DC may belong to the coverage of one or more Emergency Open Channels. They shall receive Emergency Notifications for Emergency Open Channels which are set-up within different Cells.

If an LCT or an SADP which is participating an Emergency Open Channel receives an Emergency Notification, it alerts the user in one of the following ways.

If the Notification involves an Emergency Call transmitted in the same Cell as that of the Emergency Open Channel in which it is participating, it behaves in the same way as a Radio Terminal.

If the notification involves an Emergency Call transmitted in a different Cell the Terminal alerts the user by means of a succession of discreet signals. If the user goes on hook meanwhile he can then enter the new Emergency Open Channel by going off hook again.

Upon receipt of an emergency notification, an SADP alerts the dispatcher. If the SADP dispatch is involved in another communication, he shall go on hook from his current communication, prior to requesting entry into the Emergency Open Channel.

LCT and SADP users may also make an Entry into any Emergency Open Channel set-up under their Line Access Base Stations.

Upon receipt of an emergency notification, the DC may decide to enter the emergency open channel.

4.3.3.1.7. Entry into Emergency Open Channel

4.3.3.1.7.1. Presentation

A Terminal can enter an Emergency Open Channel through:

- accepting the Emergency Call Notification;
- making a Spontaneous Entry into the Emergency Open Channel;
- returning to the Emergency Open Channel at the end of a call.

4.3.3.1.7.2. Acceptance of an Emergency Call Notification

This case is described above.

4.3.3.1.7.3. Spontaneous Entry

The procedure for Spontaneous Entry into an Emergency Open Channel shall be the same as for Spontaneous Entry into a Multisite Open Channel.

For the user of an RT, the Emergency Open Channel shall be identified by an Emergency Open identifier, which is the same under all the Cells.

For the user of an LCT, the Emergency Open Channel shall be designated by the Cell's identifier.

4.3.3.1.7.4. Candidate State

If the terminal is authorized to participate in an Emergency Open Channel, it shall accept the user's request to enter the Open Channel: the terminal shall be a candidate for this communication.

If the terminal is not authorized to participate in the Emergency Open Channel, the entry request shall be rejected, the terminal shall not be a candidate for this communication.

4.3.3.1.7.5. Return at the end of a call

The Return to Multisite Open Channel at the end of call procedure shall apply to Emergency Open Channels.

A terminal that participates in an Emergency Open Channel can exit to participate in other calls. The candidature to the Emergency Open Channel shall be suspended for the call duration. At the end of the call, the terminal may re-enter the Emergency Open Channel under the same conditions as if it were re-entering a Multisite Open Channel.

4.3.3.1.8. Terminal in Emergency Open Channel

4.3.3.1.8.1. Communication Established

A Terminal which has started to transmit can keep transmitting for a maximum period of time which shall be limited by an "anti-talkative" mechanism.

The Emergency Open Channel can remain set-up for an unlimited amount of time. The exit of all the participants shall not cause the Emergency Open Channel to be released.

4.3.3.1.8.2. Automatic Re-entry

The Automatic Re-entry into Multisite Open Channel shall apply to the Emergency Open Channel, except that re-entry cases are different.

A terminal in an Emergency Open Channel which looses the link to the Network and then finds the same Cell again, under which the same Emergency Open Channel is still set-up, may execute an automatic re-entry to the Emergency Open Channel.

A Terminal in an Emergency Open Channel which moves from its visited Cell and enters a new Cell under which an Emergency Open Channel is also set-up shall not execute an Automatic Re-entry into this Emergency Open Channel.

4.3.3.1.9. Exit from the Emergency Open Channel

A terminal shall leave an Emergency Open Channel in the following cases:

- going on hook;
- entry into another call;
- loss of the link to the Network;
- coverage restriction;
- call release.

4.3.3.1.9.1. Going on hook

Going on hook is a deliberate action on the terminal user part. The terminal shall leave the Emergency Open Channel.

The terminal shall no longer be a candidate for the Emergency Open Channel.

4.3.3.1.9.2. Entry into another call

A terminal which is participating in an Emergency Open Channel can enter another call directly without necessarily leaving the Emergency Open Channel.

While the Terminal is taking part in the other call, its candidature to the Emergency Open Channel shall be suspended.

When the Terminal leaves the "new call", it shall become a candidate for the Emergency Open Channel again. The different cases are described in the subclause: "Return at the end of a call". If conditions allow, it shall automatically re-enter the Emergency Open Channel.

4.3.3.1.9.3. Loss of the link to the Network

If the link to the Network is lost, the terminal shall leave the Emergency Open Channel. It shall remain a candidate to the Emergency Open Channel.

If the link to the Network is re-established within the same Cell, the Terminal may automatically re-enter the Emergency Open Channel.

4.3.3.1.9.4. Coverage Restriction

An Emergency Open Channel actual coverage can be restricted because of a fault. It shall not be restricted because of the pre-emption of a resource by another call, since it has the highest pre-emptive priority.

In case of coverage restriction, an system terminal which is participating in that Emergency Open Channel shall exit. It shall no longer be a candidate for the Emergency Open Channel. It shall not execute an automatic re-entry when the coverage is restored.

4.3.3.1.9.5. Release

If the Terminal is participating in an Emergency Open Channel and this communication is released, then the Terminal shall no longer be a candidate for the Emergency Open Channel and it shall inform the user of the Emergency Open Channel unavailability.

4.3.3.1.10. Release of Emergency Open Channel

Release of an Emergency Open Channel is identical to Multisite Open Channel Release.

4.3.3.1.11. Addressing

The Emergency Open Channel shall be signalled to the potential participants under coverage.

4.3.3.1.12. Access Control

Access Control is not applicable to Emergency Open Channel.

The Operational Group Access Control shall not apply to the Emergency Open Channel access.

4.3.3.1.13. Set-up and release authorization

The Emergency Open Channel shall be set-up automatically when the RSW receives an Emergency Call from a Radio Terminal, or when the dispatcher requests an Emergency Call set-up.

The terminals authorized to release an Emergency Open Channel shall be:

- Dispatch Positions (Stand Alone or at Dispatch Centre);
- other STs which are authorized by configuration to release an Emergency Open Channel and which are under its actual coverage.

4.3.3.2. Supplementary Services

4.3.3.2.1. Area Selection

The Emergency Open Channel coverage shall be defined prior to the setup.

If the coverage of an Emergency Open Channel is modified while the communication is already set-up, the Emergency Open Channel shall be released.

4.3.3.2.2. Call Forwarding

Call Forwarding is not applicable to Emergency Open Channel. However, it should be noted that forwarded STs can receive Emergency Calls and accept them.

4.3.3.2.3. Call Transfer

Call Transfer is not applicable to the Emergency Open Channel.

4.3.3.2.4. Calling Party Identification

Terminals that receive the Emergency Notification shall receive the address of the RT which originated the Emergency Call.

4.3.3.2.5. Call Waiting

Call Waiting is not applicable to Emergency Open Channel.

4.3.3.2.6. Discreet Listening

Discreet Listening is not applicable to Emergency Open Channel.

4.3.3.2.7. Group Merging

Group Merging is not applicable to Emergency Open Channel

4.3.3.2.8. Dynamic Group Number Assignment

Dynamic Group Number Assignment is not applicable to Emergency Open Channel.

4.3.3.2.9. Interconnect Access

Interconnect Access is not applicable to the Emergency Open Channel.

4.3.3.2.10. Intrusion

Intrusion is not applicable to Emergency Open Channels.

4.3.3.2.11. Late Entry

A terminal which is in Network Connected Mode in a Cell shall be informed whenever an Emergency Open Channel is set-up within that Cell. The user can obtain this information at any time.

The terminal can request Spontaneous Entry into the Emergency Open Channel.

4.3.3.2.12. Priority Call

Priority Call is not applicable to the Emergency Open Channel.

4.3.3.2.13. Pre-emptive Priority Call

The Emergency Open Channel is always preemptive.

4.3.3.2.14. Priority Scanning

Priority Scanning is not applicable to the Emergency Open Channel.

4.3.3.2.15. Talking Party Identification

Talking Party Identification is available as an Emergency Open Channel supplementary service. An RFSI address shall be transmitted by the network as the talking party identification. The SADP and the DC shall provide the talking party identification to the dispatcher.

4.3.3.3. Fault handling

Faults shall be handled in the same way for an Emergency Open Channel as a Multisite Open Channel.

5. Voice Services in Direct Mode and in Repeater Mode

5.1. Direct Mode Call

5.1.1. Basic Service

5.1.1.1. Presentation

A Direct Mode shall allow direct communication from Radio Terminal to Radio Terminal, without use of a Base Station.

5.1.1.2. Participants

Any Radio Terminal can participate in a Direct Mode call.

5.1.1.3. Coverage

The coverage of a Direct Mode call is determined by radio propagation conditions.

5.1.1.4. Set-up of Direct Mode Call

Direct Mode shall be not require use of any Network resource.

A Direct Mode Call shall be set-up when at least two RTs enter Direct Mode on the same Channel. The Channel shall be selected by the user.

5.1.1.5. Entry into Direct Mode Call

A terminal can switch to Direct Mode:

- on a user's explicit command (choice of Direct Mode and of a Channel);
- on transmission of a Direct Mode Emergency Call;
- on answer to a Direct Mode Emergency Call.

5.1.1.6. Communication

Communication in Direct Mode is half-duplex.

When the Push-to-talk key is depressed, the system terminal shall start transmitting. The occupation status of the physical radio Channel may not be checked.

5.1.1.7. Exit from Direct Mode Call

A terminal shall leave the Direct Mode on a user's command.

The terminal in Direct mode cannot be called by the Network. This service is accessible through Direct Mode with Network monitoring.

5.1.2. Supplementary Services

There are no Supplementary Services applicable to Direct Mode.

5.2. Direct Mode with Network Monitoring (Dual Watch)

5.2.1. Basic Service

5.2.1.1. Presentation

A Direct Mode Call with Network Monitoring (DM/NM) shall allow a Radio Terminal:

- to register under a Base Station, if possible, and to change its visited Base Station;
- when its status is idle, to monitor both voice activity on one Direct Mode Channel and signalling on its visited Base Station's CCH at the same time;
- to enter a Direct Mode Call on the chosen Direct Mode Channel by depressing the Push-to-talk key or when voice activity is detected on the Direct Mode Channel;
- to enter the Network connected mode if a call which concerns it is detected on the monitored CCH.

Compared to messaging services and data transmission services that are supported both as outcoming and incoming services when the terminal is paged on the Air Interface, the following incoming voice services can be received by a terminal in DM/NM:

- private voice calls (individual, multiparty, interconnect access);
- emergency notifications;
- broadcast calls;

In these communications, the Called Terminal shall be designated by the Network by its individual explicit address.

The state of a terminal in "DM/NM mode" is transparent to the Network.

A terminal in DM/NM may send or receive a Direct Mode Emergency Call: for all the duration of the emergency call, the terminal is considered in Direct Mode (without Network Monitoring).

5.2.1.2. Participants

Any Radio Terminal can select the DM/NM mode.

5.2.1.3. Coverage

The coverage in DM/NM mode shall be identical to the corresponding coverage in Network Connected Mode and in Direct Mode.

5.2.1.4. Set-up of DM/NM mode

The DM/NM mode shall allow the Terminal to communicate either in Network Mode or in Direct Mode.

The set-up conditions are those applicable to each of these modes.

5.2.1.5. Entry into DM/NM mode

A terminal enters the DM/NM mode on an explicit user's command.

5.2.1.6. Communication in DM/NM mode

A terminal in DM/NM mode can have one of several communication status:

- DM/NM - Idle;
- DM/NM - Direct Mode;
- DM/NM - Network Connected Mode.

5.2.1.6.1. Idle state

When in DM/NM Idle state, the terminal is on stand-by.

The Radio Terminal shall monitor periodically:

- the CCH of the Cell in which it is registered; if the Terminal receives an individual signalling from the Network, it shall enter the DM/NM - Network connected mode in its visited Cell; this shall happen for Private voice Calls and messaging;
- the selected Direct Mode Channel. if the Terminal detects activity on the Direct Mode Channel, it shall enter the DM/NM - Direct Mode on that Channel;
- the Direct Mode signalling Channel. if the Terminal receives a Direct Mode Emergency Signalling, it shall behave as expected: the Terminal shall switch to the Direct Mode Emergency traffic Channel if the user accepts the call.

The terminal in DM/NM - Direct Mode shall start transmitting by depressing the Push-to-talk key.

5.2.1.6.2. Direct Mode state

When in DM/NM Direct Mode state, the terminal shall operate as in normal Direct Mode.

If there is no activity during a given time the terminal shall switch back to DM/NM - Idle mode.

5.2.1.6.3. Network connected mode state

When being in DM/NM, the terminal is registered in the Network.

If the transaction involved is a Private Call or an Emergency signalling or a broadcast call or a messaging service or a data transmission service, the terminal shall behave as in Network connected mode.

If not, then the terminal shall occasionally monitor the Direct Mode Channel. If the terminal detects activity, it shall switch to Direct Mode.

If the current Network transaction is a voice transaction, a depression of the Push-to-talk key shall be handled as in normal Network Mode;

If the current Network transaction is not a private call, a depression depressing on the Push-to-talk key shall make the Terminal enter the DM/NM - Direct Mode and transmit on the Direct Mode Channel.

5.2.1.7. Exit from DM/NM mode

A terminal shall leave the DM/NM mode on a user's command.

5.2.2. Supplementary Services

There are no Supplementary Services applicable to DM/NM mode.

5.3. Repeater Mode Call

5.3.1. Basic Service

5.3.1.1. Presentation

A Repeater Mode Call consists in using an independent Repeater (RP) which is not linked to the Network.

The RP service shall offer an Open Channel communication with Push-to-talk requests control at the RT.

5.3.1.2. Participants

Any Radio Terminal in the system can participate in a RP Mode Call.

5.3.1.3. Coverage

The coverage of a communication in RP mode shall be determined by the radio propagation conditions around the Repeater.

5.3.1.4. Set-up of Repeater Mode Call

The communication in RP mode shall be set-up by transmission activation.

5.3.1.5. Entry into Repeater Mode Call

A terminal can enter the RP mode only on a user's explicit command.

The command shall specify the Channel Number.

5.3.1.6. Communication Established

Communication in RP mode is half duplex.

5.3.1.7. Exit from Repeater Mode Call

A terminal shall leave the RP mode on a user's command.

5.3.1.8. Release of Repeater Mode Call

The communication in RP mode shall be released when the RP transmission is released.

5.3.2. Supplementary Services

There are no Supplementary Services applicable to the RP mode.

5.4. Direct Mode Emergency Call

5.4.1. Basic Service

5.4.1.1. Presentation

The Direct Mode Emergency Call shall implement an Emergency Call mechanism.

It shall be used by terminals when they are unable to execute an Emergency Call (which results in an Emergency Open Channel set-up).

It shall transmit a signal to the terminals which are geographically close and which periodically monitor the Direct Mode signalling Channel.

5.4.1.2. Participants

A Radio Terminal shall make a Direct Mode Emergency Call if its user depresses the Emergency key and:

- if the terminal is not in Network connected mode, e.g., in the following cases: RT not registered which has not been able to register within a given time after the activation of the emergency mechanism, RT in CCH Control Channel search, RT having lost the link to the Network, RT in RSW disconnected fallback mode, RT in BS disconnected fallback mode, RT in Direct Mode, RT in RP mode;
- or if the terminal is in Network connected mode and the Emergency Open Channel set-up request has not succeeded within a given time;
- or if the terminal is in DM/NM mode.

5.4.1.3. Coverage

The coverage of a Direct Mode Emergency Call is determined by the radio propagation conditions around the terminal which originates the Call.

5.4.1.4. Sequence of events

The terminal shall transmit a signal on the Direct Mode signalling Channel for a given time.

At the end of transmission, the terminal shall enter Direct Mode on the Direct Mode Emergency Traffic Channel.

5.4.2. Supplementary Services

5.4.2.1. Direct Mode Emergency Call Signalling

Depending on the value of a Terminal configuration parameter, Direct Mode Emergency Notifications may be signalled to the Terminal or not.

5.5. Response to Direct Mode Emergency Call

5.5.1. Basic Service

5.5.1.1. Presentation

The Response to a Direct Mode Emergency Call shall be used to switch to Direct Mode on the Direct Mode Emergency Traffic Channel after an Emergency Call has been received on the Direct Mode Signalling Channel.

5.5.1.2. Participants

The terminals which can receive a Direct Mode Emergency Call shall be those which periodically monitor the Direct Mode signalling Channel:

- terminals in Network connected mode and DM/NM - Network connected mode, except RTs engaged in signalling or data transactions, transmitting RTs and a few short transients;
- Terminals in stand-alone BS mode (RSW disconnected FBM), except transmitting RTs and few short transients;
- RTs in Cell Selection, in Direct Mode, in DM/NM - Idle or Direct Mode status, except transmitting RTs and a few short transients;
- RTs in RP mode, except transmitting RTs and a few short transients, only when a system radio channel is used for the RP Mode.

5.5.1.3. Coverage

The coverage of the Direct Mode Emergency Call is determined by radio propagation conditions around the terminal which originated the Call.

5.5.1.4. Sequence of events

The Radio Terminal which receives a Direct Mode Emergency Call shall alert the user using a characteristic audible signal, if the "Direct Mode Emergency Call Signalling" is activated at the Terminal.

The user can accept the call using a simple action.

If the user accepts the call, the terminal shall enter into Direct Mode on the Direct Mode Emergency Traffic Channel. This Channel is known to the terminal.

If the terminal is in DM/NM mode, it shall remain in DM/NM mode - on the Direct Mode Emergency traffic Channel - after accepting the Direct Mode Emergency Call.

5.5.2. Supplementary Services

There are no Supplementary Services applicable to the Direct Mode Emergency Call Response.

6. Data Services

6.1. Introduction to data services provided to applications

Data services allow point-to-point or point-to-multipoint, connection oriented or connectionless data transfers.

The data connection points between a user data terminal and a radio terminal are the following TETRAPOL reference points:

- R1.ipms for inter-personal messaging services (IPMS) over SDP
- R1.exams for external application messaging services (EXAMS) over SDP
- R1.RNlms for local messaging services (RNLMS) over SDP
- R1.udp for data transmission services over UDP

The same data connection points apply between a user data terminal and a line connected terminal.

The data connection points in the network are the following TETRAPOL reference points:

- R8 for an access to an X.400 MTA
- R10 for an access to an external data terminal (EDT)
- R15 for an IP router access
- R16 for an X.25 network access

The data services are supported in two configurations:

- UDT to UDT data transfer, via the network
- UDT to a DAS or to a EDT

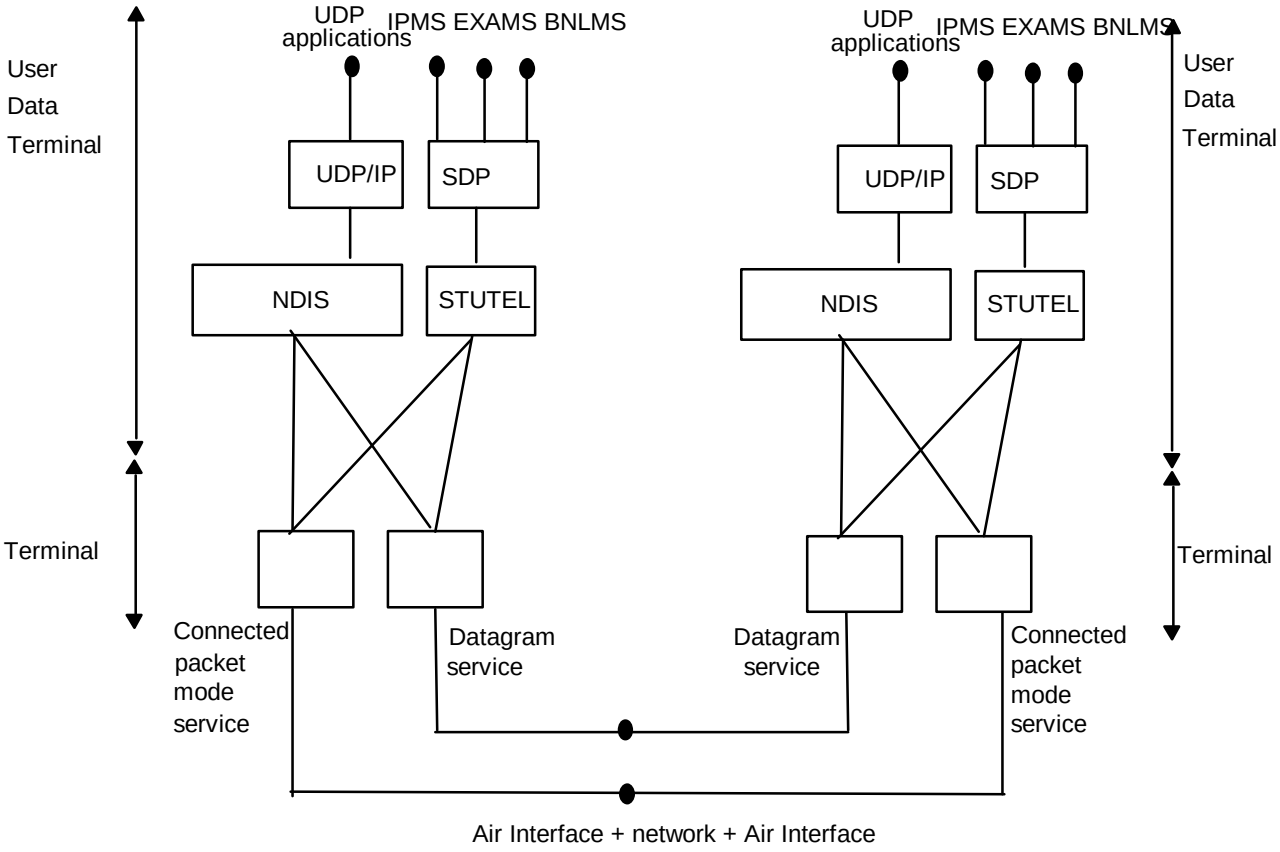

Figure 1: UDT to UDT configuration

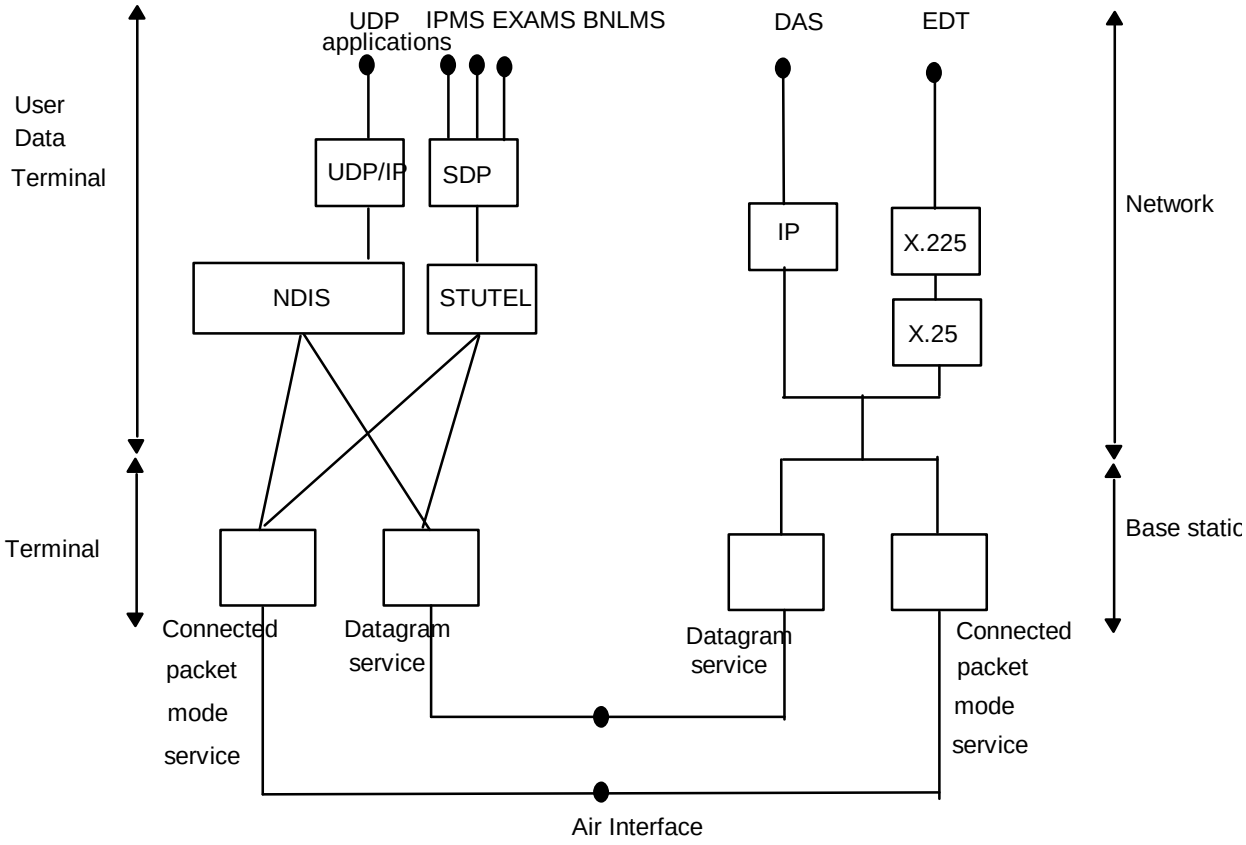

Figure 2: UDT to network data connection point configuration

NOTE: A network driver interface standard (Microsoft NDIS) or a STUTEL protocol stack [ETS 300 075] provide the interface driver services between the user data terminal and the terminal.

Each data transmission may be split into up to three phases:

- An uplink transmission from the UDT to the network or a submission from an external server
- Routing in the network
- A downlink transmission from the network to one UDT or to a group of UDT, or a delivery to an external server.

6.2. Messaging Services

6.2.1. Presentation

6.2.1.1. Participants

The System provides messaging services. that can be used to transmit messages between data transmission devices connected to System "Data Connection Reference Points" (DCRPs). For more details on Reference points, see PAS 0001-1-1.

A DCRP shall be defined by:

- the System device it is located on, RSW or system terminal;
- the communication protocols that can be used.

The System DCRPs shall be:

- the ST-DCRP, which connects a User Data terminal (UDT) to a System Terminal. An system terminal can only connect one UDT; this DCRP corresponds to Reference Points R1 and R2 as specified in PAS 0001-1-1;

- the ET-DCRP, which connects an External Data terminal to the Network. An MSW can only connect one EDT; this DCRP corresponds to Reference Point R10 as specified in PAS 0001-1-1;
- the X.400-DCRP which connects an X.400 MTA message handling switch to the Network. The connection is made through an X.400 MTA which is responsible for connection to the other X.400 MTAs; this DCRP corresponds to Reference Point R8 as specified in PAS 0001-1-1.

The UDT shall be addressed by its connecting ST's address. A UDT does not have an address of its own.

The Messaging Service shall use an "equipped with UDT" system terminal attribute to check whether it is enabled for message transmission and reception or not.

This attribute shall be set to "true" by default when an system terminal attribute is unreachable (Fallback Modes).

The EDT shall be designated by a System address or by a range of addresses. The R field of the address shall be that of its connecting RSW.

6.2.1.2. Range of Services

The System shall provide several user messaging services:

- Inter-Personal Messaging (IPM);
- External Application Messaging (EXAM);
- RN Local Messaging (RNLM).

The ST-DCRP shall provide the data transmission services to the UDT, which is the System user. The specific functions related to the UDT are outside the scope of the present Specification.

Message Delivery shall be done in "direct delivery" mode: reception on the destination Terminal is automatic, i.e. there shall be no user intervention. The System does not manage Mail Boxes.

The System shall not carry out Presentation conversion on the contents. The originator and recipient Terminals shall use compatible presentation characteristics. If two users wish to exchange a series of messages, each message shall be handled separately by the system. The Data Terminals (DTs) shall implement the segmentation and re-assembly functions themselves, taking into account the fact that the System does not guarantee the sequential delivery of messages.

6.2.1.3. Elements involved

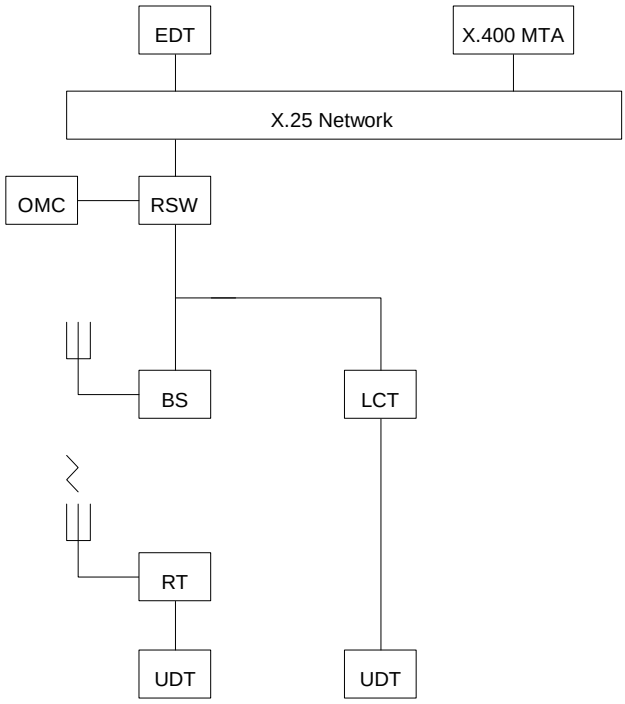

Figure 3: Elements involved in user messaging services

6.2.2. Inter-Personal Messaging Service

6.2.2.1. Basic Service

6.2.2.1.1. Presentation

The Inter-Personal Messaging Service (IPM) shall provide a message transmission service between:

- a UDT connected to an ST's ST-DCRP;
- an EDT connected to an RSW's ET-DCRP;
- an X.400 MTA connected to the X.400-DCRP of one or more RSWs.

The Inter-Personal Messaging Service shall be "message secure". This means that the MTA takes charge of the message which is stored on disk. This security mechanism guarantees that the message is handled even if there is an incident, except if the disks are lost. If the System transmits a Submit Confirmation Notification (SCN) for a message, it means either that the message is delivered to a primary recipient or an alternate recipient or a back-up recipient, or that a Delivery Failure Notification (DFN) isdelivered to the originator.

The Inter-Personal Messaging Service shall be "distribution secure". This means that when a message cannot be delivered to its primary recipient, the HRSW shall implement back-up mechanisms to distribute the message: it shall send the message to the Alternate recipient or, in case of failure, to the Back-up recipient.

The purpose of connecting the System's Inter-Personal Messaging Service to standard X.400 Message Handling Service is to allow exchanges between UDTs and X.400 External Network subscribers.

6.2.2.1.2. Message transmission

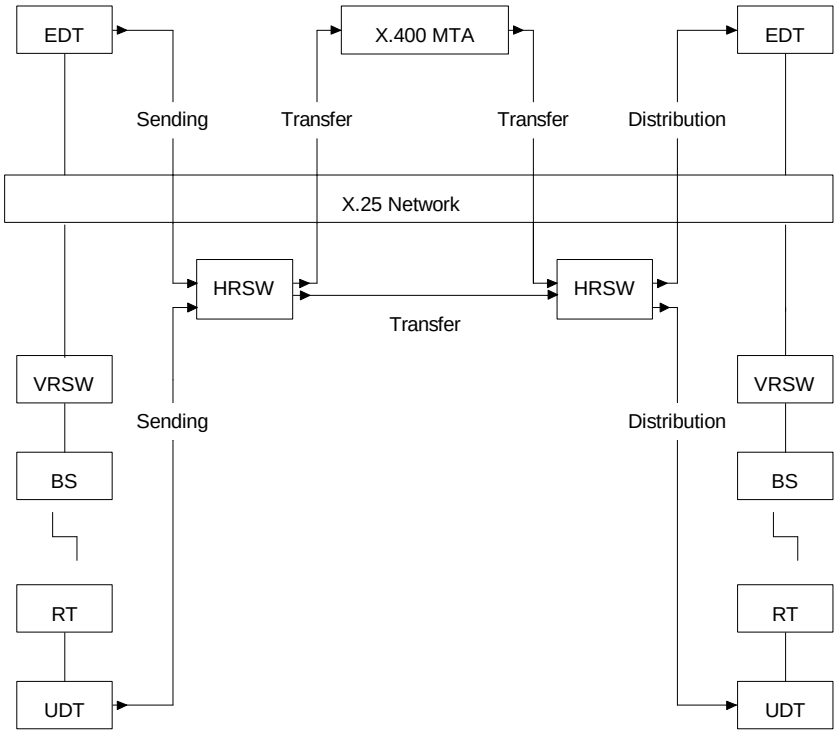

Figure 4: Message Transmission in Inter-Personal Messaging

6.2.2.1.3. Participants

The participants in the Inter-Personal Messaging service shall be:

- the UDT connected to an system terminal in Network connected mode;
- the EDT connected to an RSW via the X.25 Network;
- the X.400 MTA connected to an RSW via the X.25 Network.

The possible transmissions shall be:

- from UDT to UDT;
- from UDT to EDT;
- from EDT to UDT;
- from UDT to X.400 MTA;
- from X.400 MTA to UDT.

Transmissions which do not involve at least one UDT are not taken into account by the System.

6.2.2.1.4. Coverage

The Inter-Personal Messaging System can transmit messages over the entire Network.

6.2.2.1.5. Sending and Submission

6.2.2.1.5.1. Sending

Sending is the function whereby a messaging subscriber transmits a message to the Inter-Personal Messaging access function.

The message originator shall transmit a message to the Data Connection Reference Point (DCRP) which conforms to that DCRP's format specifications and protocol.

Parameters applied to the message on transmission shall be:

- the recipient's address;
- the external Priority (optional);
- the originator's address in case it is an EDT;
- the Delivery Confirmation Notification request (optional);
- the message's text.

If the originator is a UDT, the UDT status conditions for sending a message depend on priority rules.

The UDT can only transmit one message at a time on the physical radio Channel. The UDT shall wait for the Radio Transmission Acknowledgement (positive or negative), which is sent to it by the ST, before any new transmission takes place.

The UDT shall set a timer at the end of which it shall consider the handling of the transmitted message to be terminated (the message is delivered to its recipient or the System reports the submission or transfer failure).

The case where a Delivery Confirmation Notification is requested is discussed in subclause: "Delivery Confirmation Notification" in Supplementary Services.

6.2.2.1.5.2. Submission

Submission is the operation whereby the Inter-Personal Messaging access function transmits a message to the MTA. Inter-Personal Messaging Submission at the MTA shall include the "message secure" procedure.

If the subscriber is a UDT, the connecting MTA shall be that of its HRSW.

If the subscriber is an EDT, the connecting MTA shall be that of its connecting RSW.

Inter-Personal Messaging shall send a Submit Confirmation Notification (SCN) to the originator. The SCN shall include a Message Identifier (MSG-Id) allocated by the System, and used for identification in the System.

The SCN means that the message has been submitted to the MTA of the originator's HRSW. The "message secure" procedure shall be executed by the System. If the originator does not receive the SCN, it does not know if the message or the SCN has been lost. SCN transmission is neither "message secure" nor "distribution secure".

If the HRSW cannot handle the message, it shall transmit a Submit Failure Notification (SFN) to the originating UDT or EDT. SFN transmission is neither "message secure" nor "distribution secure".

6.2.2.1.6. Transfer

Transfer is the transmission of the message between the originator's connecting MTA and the recipient's connecting MTA.

The transfers the System participates in shall be:

- originator's HRSW to recipient's HRSW;
- originator's HRSW to X.400 MTA;
- X.400 MTA to recipient's HRSW.

The transfer protocol shall conform to ITU-T Recommendations X.410 and X.411 (1984). This protocol is "message secure".

If the Transfer is executed successfully it means that the recipient MTA has received and secured the message. The originator MTA can then erase the message stored on disk.

The originator MTA shall make several attempts to transfer the message to the recipient MTA before declaring the failure to the user. In which case, the originator MTA shall send a Delivery Failure Notification (DFN) to the originating Data Terminal (DT). The DFN is "message secure" and "distribution secure".

The services requested by an MTA which are not provided for by Inter-Personal Messaging shall be refused, in conformity with the ITU-T X.400 series Recommendations (1984).

6.2.2.1.7. Delivery and Distribution

6.2.2.1.7.1. Delivery

Delivery is the function whereby the MTA hands over the message to the HRSW's Inter-Personal Messaging access function.

6.2.2.1.7.2. Distribution

Distribution is the function whereby the Inter-Personal Messaging access function transmits the message to the recipient.

The recipient's HRSW shall implement the distribution of the message to the UDT or to the local EDT.

If the recipient is a UDT, the System shall locate the UDT's connecting ST. The message shall be transmitted first to the VRSW then to the ST.

The system terminal shall receive the message and send a distribution acknowledgement to its HRSW, then it shall transmit the message to the UDT.

If the recipient is an EDT, the receiving HRSW shall transmit the message to the local EDT. The EDT shall send a distribution acknowledgement to its connecting RSW.

When the distribution acknowledgement is received by the HRSW, the MTA can erase the message stored on disk.

The message transmitted by the system terminal to the UDT, or by the RSW to the EDT, shall include the following parameters:

- the originator's address;
- the message's External Priority;
- the Message Identifier (MSG-Id);
- the list of the message's designated recipients;
- the distribution step, depending on whether they are primary, Alternate or Back-up recipients;
- the message's text.

6.2.2.1.8. Copy to the EDT

An RSW's Inter-Personal Messaging server may send that RSW's EDT log function a copy of all the messages handled by that RSW, as an HRSW, at the end of the Submission and Delivery processes.

The copy transmissions to the EDT log function shall use the copy service. The copies are not "message secure".

The EDT may select from among the data received, it cannot ask the HRSW to filter the transmitted data.

The IPM service messages transmitted as copies by the HRSW to the EDT log function shall be:

- messages transmitted by a DT (header and body) after successful submission;
- messages to be distributed to a DT (header and body) after the message has been transmitted by the MTA to the Inter-Personal Messaging service's access function for delivery;

- SFNs generated by the originator's HRSW in case of submission failure;
- DCNs and DFNs received by the originating RN.

Copies of SCNs are not sent to the EDT.

If both originator and recipient of a message have the same HRSW, the RSW's EDT shall receive two copies of the message, one at the end of the submission and one on delivery.

6.2.2.1.9. Addressing

The addressing of a message's recipients may include one or more addresses.

The types of addresses allowed shall be:

- explicit addresses;
- implicit addresses;
- list addresses.

The UDT can to use:

- explicit addresses;
- implicit addresses;
- list addresses defined at the VRSW or at the HRSW of its attached ST.

The EDT can use:

- explicit addresses;
- implicit addresses;
- list addresses defined at its connecting RSW.

The X.400 MTA shall use only explicit and implicit addresses.

If an address does not conform to the System's Numbering plan, the originator's HRSW shall refuse the message and send an SFN to the message originator.

X.400 recipients are designated by X.400 O/R names.

6.2.2.1.10. Priority

A message is transmitted along with its External Priority. The External Priority can take the values ROUTINE, URGENT and FLASH.

The recommended default value set at the UDT should be ROUTINE.

The message transmission and reception handling procedures according to External priority are described in the clause Priority Rules of part 1.3 of the specification.

6.2.2.2. Supplementary Services

6.2.2.2.1. Message Forwarding

The System shall handle the forwarding of a message according to the process defined in Figure 3 given below. This diagram defines the "distribution secure" mechanism.

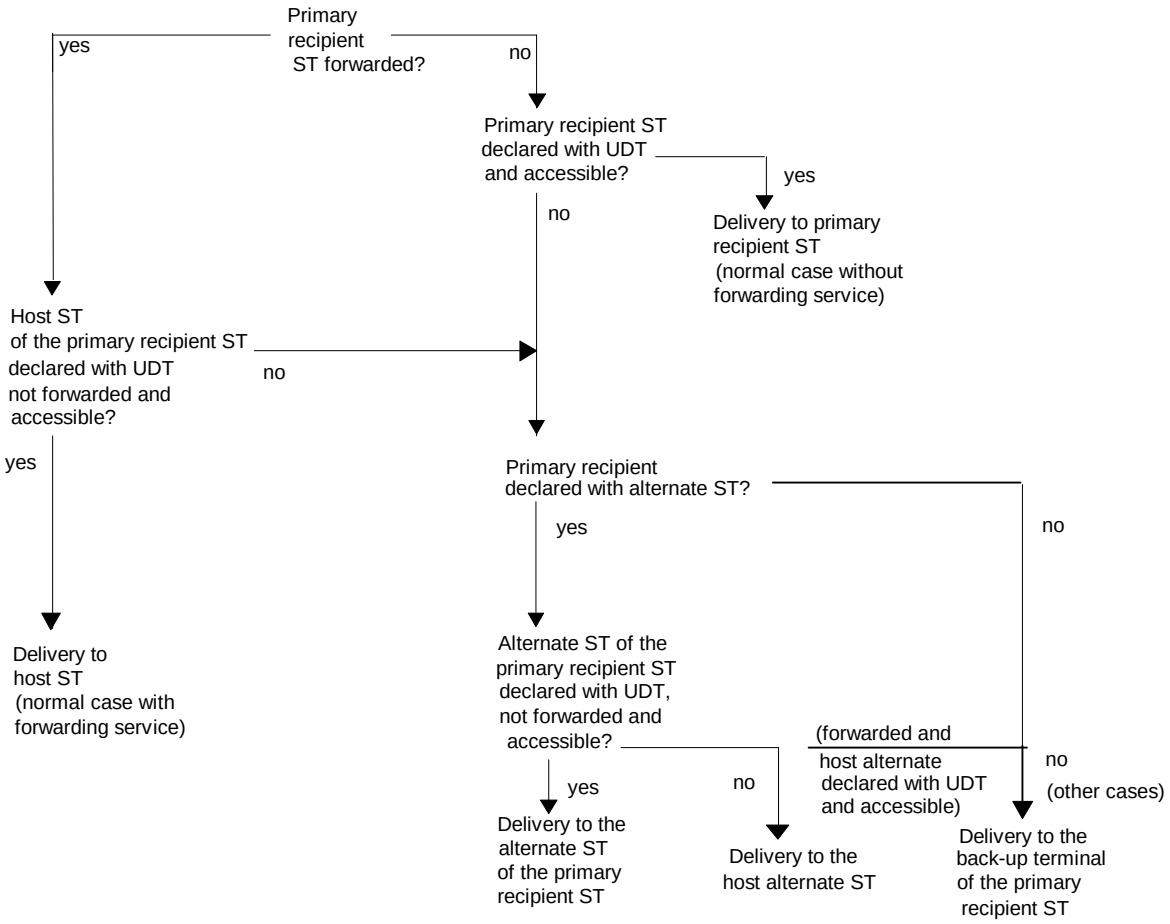

Figure 5: "distribution secure" procedure

An system terminal which is disabled or suspended shall be considered to be unreachable.

An implicit address is defined with a list of explicit addresses. The forwarding service for an implicit address occurs only if all explicit addresses from the list are forwarded. In that case, the host address of the implicit address is the one of the first explicit address of the list.

An EDT shall not be forwarded nor be host recipient.

6.2.2.2.2. Alternate Recipient

A Terminal designated by its individual explicit or implicit address can be associated with an Alternate address. The Alternate address of an implicit address is the one of the first explicit address of the list that defines the implicit address and that has been associated with an Alternate address.

The Alternate address shall be used to designate a Terminal to which the Network delivers the message if it cannot be delivered to the designated recipient.

The Alternate address shall be an individual explicit or implicit address.

There is no Alternate address for an implicit address if no system terminal of the implicit address have an Alternate address.

As soon as an Alternate address is selected, this choice is definitive.

The Alternate address shall belong to the same name RN as the recipient address does.

The Alternate address can designate a UDT or an EDT.

The HRSW procedure for delivering the message to the designated recipient shall take account of:

- the recipient's "forwarded" status;
- the recipient's "equipped with UDT" attribute.

The delivery procedure is described in the diagram given in subclause: "Message Forwarding".

An EDT does not have an Alternate address.

6.2.2.2.3. Back-up Recipient

A Back-up Terminal should be defined in each RN of the system. The Back-up Terminal shall be a predefined EDT.

The decision procedure of Back-up Terminal message delivery shall be described in the diagram given in subclause: "Message Forwarding".

The Back-up Terminal shall receive:

- a copy of the message;
- a distribution report with the list of primary recipients which have not been reached neither in primary nor in alternate distribution.

The Back-up Terminal shall give separate acknowledgements for the message and for the distribution report.

6.2.2.2.4. Garbage Messaging Collector

A Garbage Messaging Collector shall be defined in each RN and be line-connected to the MSW.

The Garbage Messaging Collector shall receive the errored messages which cannot be handled by the RSW as well as the rejection reports (see subclause: "Faults during the transmission phase").

6.2.2.2.5. Delivery Confirmation Notification

The originating Terminal (UDT or EDT) can request a Delivery Confirmation Notification (DCN) for a given message. If the delivery is executed correctly, each recipient MTA shall transmit one or more Delivery Confirmation Notifications to the originator. Those DCNs shall contain the list of primary recipients reached through their Primary, Alternate or Back-up addresses.

In the case of a multi-recipient message, a Data Terminal (DT) can receive one or more DCNs and one or more DFNs.

The default value shall be "Delivery Confirmation Notification not requested".

The Delivery Confirmation Notification is "message secure" and "distribution secure".

6.2.2.3. Fault handling

6.2.2.3.1. Faults during the sending phase

This subclause describes the faults which can occur during the phase when the originator is transmitting the message to its HRSW.

6.2.2.3.1.1. Submission failures

The sending UDT shall be notified in the following events:

- a transmission failure occurs between the sending UDT and the VRSW ,
- the system terminal refuses to transmit the message,
- a congestion in the network occurs.

6.2.2.3.1.2. Failure in the network

The originator UDT shall be notified in the following events, if required while the message is routed in the network:

- The MSW of the originating regional network is unreachable or can not handle the message
- The MSW of the home regional network of the sending UDT is unreachable or can not handle the message
- The MSW of the home regional network of the destination UDT is unreachable or can not handle the message
- The MSW of the visited regional network of the destination UDT is unreachable or can not handle the message
- The visited RSW of the visited regional network of the destination UDT is unreachable or can not handle the message
- The message is lost due to an RSW failure

If the VMSW cannot transmit the message to the originator's HRSW because the VMSW is an isolated RN or the HRSW is unreachable:

- the VRSW shall notify the originator;
- the VRSW shall send its RN's Garbage Messaging Collector a "rejection report" containing the message's body.

6.2.2.3.1.3. Message loss on the EDT - HRSW segment

The EDT shall detect a loss of message when it does not receive an SCN or an SFN.

6.2.2.3.1.4. Loss of the SCN

Reception of the SCN informs the originator that the message has been received and secured by its HRSW's MTA. If it does not receive the SCN, the originator cannot decide if the message or the SCN is lost. In which case the originator may send the message again with a "possible duplicate" annotation in the message's text.

6.2.2.3.2. Faults during the transfer phase

This subclause describes the handling of faults which occur whilst the message is held by an MTA or during transfers between MTAs.

The MTAs shall record the message. The STs transfer procedure between MTAs is "message secure".

If the originator MTA cannot transmit the message to the recipient MTA, it shall send the originator a Delivery Failure Notification (DFN). The DFN shall contain the MSG-Id.

During this phase, rare double faults can cause a DFN to be sent after the expiration of the UDT's DFN reception time-out (about 15 minutes).

The relevant cases are:

- the originating HRSW is congested and the message expired;
- the RSW restarts with an incorrect time whilst some messages are being handled, which causes an apparent message expiration;
- in the case of a switch-over during the connection to the recipient MTA or during the message transfer, the originator MTA may generate DFNs for the messages waiting for transfer which have expired.

The message "lifetime" depends on the message's priority.

If the message which has expired is a DFN, the RSW shall send a fault message to the OMC. No signal shall be sent to the originator.

Originator and recipient HRSW switch-over may lead to multiple delivery of a message.

6.2.2.3.3. Faults during the delivery phase

Some faults during the delivery phase can cause a DFN to be sent after the expiration of the UDT's DFN reception time-out (about 15 minutes).

These rare faults are cases of double faults. The receiving HRSW shall send a DFN to the originating HRSW.

The relevant cases are:

- the recipient HRSW is congested and the message's lifetime is expired;
- the RSW restarts with an incorrect time whilst some messages are being handled, which causes an apparent expiration of a message's lifetime;
- the RSW switches-over or restarts with the correct time but the messages whose lifetimes have expired are waiting for distribution at the back-up terminal.

The RSW shall send a fault message to the OMC for the DFNs whose lifetimes have expired.

6.2.2.3.4. Faults during the distribution phase

This subclause describes the faults which occur during the transmission phase from the recipient HRSW to the recipient Data Terminal.

A technical fault on the HRSW - system terminal link can lead to the loss of the message or of its acknowledgement transmitted by the recipient entity.

The loss of the acknowledgement can lead to double delivery: the message was delivered to the recipient UDT but the acknowledgement transmitted by the system terminal has been lost. The RSW shall execute a "distribution secure" procedure. The message shall be received by the Alternate Terminal or by the Back-up Terminal.

If the distribution procedure fails, the system terminal shall be considered to be unreachable. An system terminal is declared to be unreachable after several attempts by the RSW. The number of attempts is a function of the message's priority: the maximum number of attempts may not be reached if the RSW becomes congested.

The system terminal shall be considered to be unreachable in case of incoming call collision. Incoming call signalling rshall be made each time the RSW attempts to deliver a message.

When the system terminal is considered as being unreachable, the Network shall implement the "distribution secure" mechanisms. These mechanisms are described in the diagram in subclause: "Message Forwarding". In the case of a notification (DCN or DFN), the "distribution secure" procedure is carried out by the Back-up Terminal, the notification shall not be transmitted to the Alternate Terminal.

If a fault occurs on the system terminal - UDT link when the system terminal has acknowledged the message, the message shall remain in the ST's storage memory. The system terminal cannot receive any incoming message until that message is transmitted to the UDT. The "message blocked" information shall be displayed on the ST's remote control unit.

If the system terminal has detected that the UDT is unreachable, the system terminal shall refuse the distribution request made by the VRSW. The Network shall consider that the system terminal is unreachable for that message distribution.

If the EDT is unreachable or if there is an EDT- RSW communication failure, the System shall transmit the message to the back-up terminal.

The loss of the message acknowledgement can lead to a double delivery (EDT and back-up terminal).

If the Back-up Terminal is unreachable, the System shall queue the messages for the back-up terminal.

If the queue is overflowed, the oldest message in the queue is removed:

- an alarm shall be sent to the OMC;
- if this message is a data message, a DFN shall be generated.

If the Garbage Messaging Collector is unreachable, the message shall be lost. No alarm shall be sent to the OMC.

6.2.2.3.5. Faults during the distribution of the EDT copy

If the copy of a message cannot be transmitted to the EDT, it shall be queued and transmitted when the HRSW - EDT link becomes available.

The copy may be lost during transmission from the HRSW to the EDT at a higher level than the security mechanisms provided by layers 3 and 5. In this case, no retransmission shall take place.

If the queue is overflowed, the oldest copies in the queue shall be lost.

If the copy is lost at the EDT, the System operator may check the end of transaction reports.

6.2.3. External Application Messaging Service

6.2.3.1. Basic Service

6.2.3.1.1. Presentation

The External Application Messaging Service (EXAM) shall provide a message transmission service between a User Data Terminal (UDT) connected to a System Terminal Data Reference Connection Point (ST-DCRP) and an External Data Terminal (EDT) connected to an External Terminal Data Reference Connection Point (ET-DCRP) of that ST's HRSW.

The message shall be transmitted directly from the originator to the recipient without intermediate recording on the HRSW disk (no "message secure" nor "distribution secure" procedure).

The originator shall not receive any Submit Confirmation Notification. If the Network cannot handle the message, it may send a SFN. This transmission is not guaranteed, the report is neither "message secure" nor "distribution secure". The originator is not advised of the loss of the message.

6.2.3.1.2. Message transmission

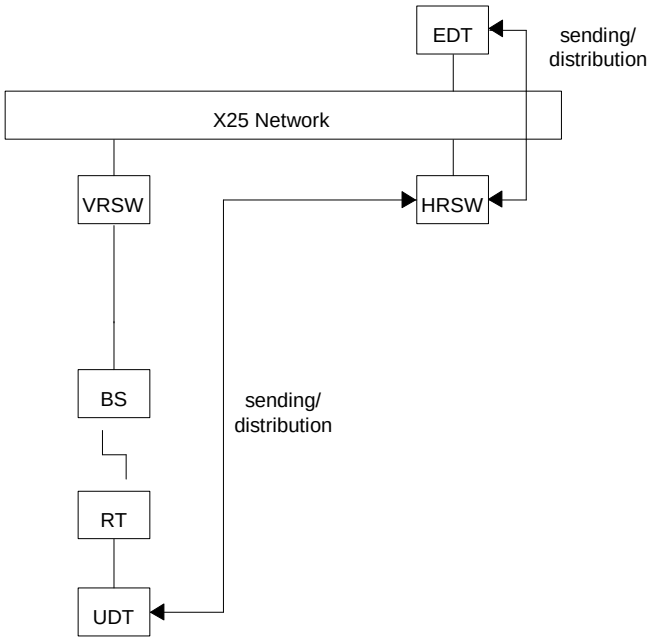

Figure 6: Message Transmission in External Application Messaging

6.2.3.1.3. Participants

The participants in the External Application Messaging Service shall be:

- the UDT connected to an system terminal in Network connected mode;
- the EDT connected to a RSW.

The possible transmissions shall be:

- from UDT to EDT;
- from EDT to UDT.

The HRSW of the system terminal to which the UDT is connected shall be the RSW to which the EDT is connected.

6.2.3.1.4. Coverage

The External Application Messaging Service shall allow messages to be transmitted throughout the Network.

6.2.3.1.5. Sending and Submission

6.2.3.1.5.1. Sending

The message originator transmits a message to the Data Connection Reference Point (DCRP) which conforms to that DCRP's format and protocol specifications.

Parameters applied on message transmission shall be:

- the recipient's address;
- the External priority (optional);
- the message's text;
- the originator's address (if it is an EDT).

If the originator is a UDT, the system terminal communication status conditions which shall hold for the UDT to be able to transmit depend on priority rules.

The message shall be transmitted to the originator's HRSW.

6.2.3.1.5.2. Submission

The message shall be transmitted from the External Application Messaging (EXAM) access function to the EXAM server of the same HRSW.

The HRSW shall assign a Message Identifier (MSG-Id) to the message.

The EXAM shall not transmit any Submit Confirmation Notification. If submission is not possible, the External Application Messaging Service shall send a Submit Failure Notification to the originator.

6.2.3.1.6. Transfer

The External Application Messaging Service shall not include any phase corresponding to the Transfer between the originator HRSW and the recipient HRSW phase. The originator HRSW and the recipient HRSW shall be combined.

6.2.3.1.7. Delivery and Distribution

6.2.3.1.7.1. Delivery

The recipient HRSW's External Application Messaging server shall deliver the message to the External Application Messaging access function of the same RSW.

6.2.3.1.7.2. Distribution

The recipient HRSW's External Application Messaging access function shall distribute the message. The message shall be transmitted from the recipient HRSW to the message recipient.

If the recipient is a UDT, the System shall locate that UDT's connecting ST. The message shall be transmitted first to the VRSW then to the ST.

The system terminal shall receive the message and send a distribution acknowledgement. This acknowledgement is local to the system terminal - VRSW segment. The system terminal shall then transmit the message to the UDT.

If the recipient is an EDT, the HRSW shall transmit the message to the local EDT. The HRSW does not expect an acknowledgement.

The message transmitted to the UDT or EDT shall contain:

- the originator's address;
- the Message Identifier;
- the list of designated recipients;
- the distribution step (primary);
- the message's text.

6.2.3.1.8. Copy to the EDT

A copy of the message shall be sent to the EDT's log function when the message is transmitted by the External Application Messaging server to the External Application Messaging (EXAM) access function for delivery.

The transmission of copies to the EDT's log function shall be carried out using the copy service. The copies are not "message secure".

The EXAM messages transmitted as copies by the HRSW to the EDT log function shall be:

- the messages to be distributed to a Data Terminal (DT);
- the SFNs generated by the HRSW in case of submission failure.

6.2.3.1.9. Addressing

The EDT may use one or more addresses. All types are allowed.

The EDT shall use:

- explicit or implicit individual addresses;
- list addresses defined on its visiting RSW.

The UDT shall use only one explicit address, that of the EDT connected to its HRSW.

6.2.3.2. Supplementary Services

6.2.3.2.1. Message Forwarding

This service is not applicable to External Application Messaging.

6.2.3.2.2. Alternate Recipient

This service is not applicable to External Application Messaging. A message which is not delivered to its primary recipient shall be lost.

6.2.3.2.3. Back-up Recipient

This service is not applicable to External Application Messaging.

6.2.3.2.4. Garbage Messaging Collector

This terminal is the Regional network Operator (RNOP). It shall receive the errored messages which are not handled by the RN's HRSW.

6.2.3.3. Fault handling

6.2.3.3.1. Faults during the sending phase

Refer to subclause: "Faults during the sending phase" in Inter-Personal Messaging.

6.2.3.3.1.1. HRSW unable to handle the message

The HRSW shall generate an SFN in the following cases:

- the DTs have used an unauthorized address (address does not correspond to an address within their home RN, incorrect address type);
- the EDT has used a List Address containing addresses outside of the home RN or an EDT address;
- there has been a message decryption failure;
- the system is congested;
- the message is incorrect.

There is no "rejection report" in External Application Messaging.

6.2.3.3.2. Faults during the distribution phase

6.2.3.3.2.1. Message loss on the HRSW - system terminal segment

A technical fault on the HRSW - system terminal link may lead to the loss of the message or of its acknowledgement transmitted by the recipient entity (ST - RSW fault). The originator is not advised.

6.2.3.3.2.2. Unreachable ST

If the distribution procedure fails, the system terminal shall be considered to be unreachable (see "unreachable ST" subclause in Inter-personal Messaging "faults during the delivery phase"). The message shall be lost, no "distribution secure" procedure being executed.

6.2.3.3.2.3. Message blocked at the ST

If a fault occurs on the system terminal - UDT link when the system terminal has acknowledged the message, the message shall remain in the ST's storage memory. The system terminal can no longer receive an incoming message until the message has been transmitted to the UDT. This status shall have no effect on voice communications. The "message blocked" information shall be displayed on the ST's remote control unit.

6.2.3.3.2.4. UDT unreachable by the ST

If the system terminal has detected that the UDT is unreachable, the system terminal shall refuse the distribution request sent by the VRSW. The Network shall consider that the system terminal is unreachable for the distribution of that message and the message shall be lost.

6.2.3.3.2.5. EDT unreachable

If the EDT is unreachable: the message shall be queued (External Application Messaging queue for the EDT) and transmitted when the RSW - EDT link becomes available.

6.2.3.3.2.6. EDT Message queue overflow

If the queue is overflowed, the oldest messages in the queue shall be lost.

6.2.4. RN Local Messaging Service

6.2.4.1. Basic Service

6.2.4.1.1. Presentation

The RN Local Messaging Service (RNLM) shall provide a message transmission service between:

- a UDT connected to an ST's ST-DCRP;
- an EDT connected to a Network's ET-DCRP.

The term "Local" means that the originator and the recipients are located within the same Regional network.

6.2.4.1.2. Message transmission

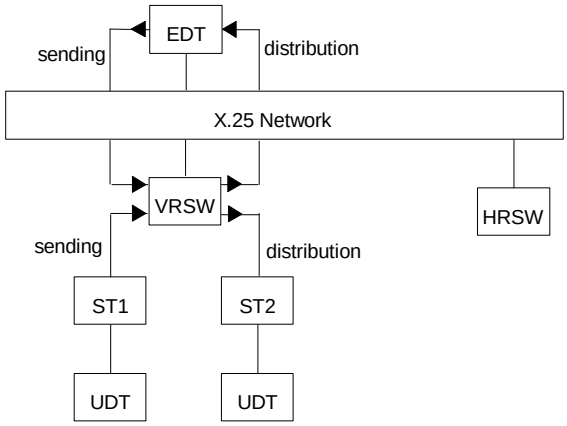

Figure 7: Message Transmission in Local Messaging

ST1 and ST2 shall be home located or visitor terminals in the VRSW.

6.2.4.1.3. Participants

The participants in the Local Messaging Service shall be:

- the UDT connected to an system terminal in Network connected mode;
- the EDT connected to a RSW via the X.25 Network.

The possible transmissions shall be:

- from UDT to UDT;
- from UDT to EDT;
- from EDT to UDT.

The EDT shall be the EDT of the UDT's visited RN.

6.2.4.1.4. Coverage

The Local Messaging Service coverage shall include a single Regional network as well as the local EDT connected to this RN.

6.2.4.1.5. Sending and Submission

6.2.4.1.5.1. Sending

Sending is the function whereby a messaging service subscriber transmits a message to the Local Messaging Service access function.

The message originator shall transmit a message to the DCRP which conforms to that DCRP's format and protocol specifications.

Parameters applied on message transmission shall be:

- the recipient's address;
- the originator's address, if it is an EDT;
- the external priority (optional);
- the message's text.

If the originator is a UDT, the system terminal communication status conditions which shall hold for the UDT to be able to transmit depend on priority rules.

6.2.4.1.5.2. Submission

Submission is the function whereby the RN Local Messaging Access Function transmits a message to the VRSW's Local Messaging server.

The RSW shall transmit an SFN to the originator if the message does not conform (incorrect number or type of addresses, encryption error).

Before starting the delivery phase, the RN Local Messaging service shall check:

- if the following conditions are true for each receiving system terminal:
    - equipped with UDT located in the originator RN;
    - access enabled;
    - traffic enabled;
    - in service;
    - registered;
- in case the EDT is the recipient, if it is reachable.

If, following verification of these conditions, there is no recipient which can receive the message, an SFN shall be sent to the originator.

6.2.4.1.6. Transfer

Transfer is not applicable to Local Messaging.

6.2.4.1.7. Delivery and Distribution

6.2.4.1.7.1. Delivery

The Local Messaging server shall deliver the message to the Local Messaging access function.

6.2.4.1.7.2. Distribution

Distribution is the function whereby the Local Messaging access function transmits the message to the recipient.

The VRSW shall distribute the message to the recipient UDT or to the local EDT.

If the recipient is a UDT, the System shall locate that UDT's connecting ST. The message shall be transmitted from the VRSW to the ST.

If the recipient is an EDT, the VRSW shall transmit the message to the X.25 Network.

The message transmitted by the system terminal to the UDT or by the RSW to the EDT shall contain:

- the originator's address;
- the message's External priority;
- the Message Identifier;
- the list of the message's designated recipients;
- the distribution step (primary);
- the message's text.

If distribution to the recipient fails, the message shall not be delivered to the back-up terminal. The originator is not notified.

6.2.4.1.8. Copy to the EDT

Copies of the messages handled by the RSW shall be sent to the EDT's log function by the Local Messaging server when they are delivered to the RN Local Messaging access function.

The transmission of copies to the EDT's log function shall use the copy service.

The Local Messaging service messages transmitted as copies by the HRSW to the EDT log function shall be:

- the messages transmitted to a Data Terminal (DT);
- the SFNs generated by the originator's VRSW in case of submission failure.

6.2.4.1.9. Addressing

The EDT can use one or more addresses. Explicit, implicit and list addresses defined on its VRSW are allowed. Addresses shall designate only STs.

The UDT can use one or more addresses. Explicit, implicit and list addresses defined on its VRN are allowed to designate STs, or explicit addresses of the VRSW for the EDT.

If an address does not conform to the System's addressing plan, the VRSW shall refuse the message and send an SFN to the message originator.

If there is at least one reachable recipient, the message shall be distributed to the reachable recipients. The originator shall not be informed that the message has not been distributed to some planned recipients.

An SFN shall be generated if none of the recipients is reachable.

6.2.4.2. Supplementary Services

6.2.4.2.1. Message Forwarding

The designated recipient of a message can be forwarded.

If the host system terminal is located within the same RN as the forwarded ST, the message shall be transmitted to the host ST. If not, the VRSW shall send an SFN to the originator (unreachable ST).

The host ST's status shall be checked. If the system terminal is unreachable, the RSW shall generate an SFN.

6.2.4.2.2. Alternate Recipient

This service is not applicable.

Messages are not "distribution secure" in Local Messaging. A message which is not delivered to its primary recipient shall be lost.

6.2.4.2.3. Back-up Recipient

This Service is not applicable.

6.2.4.3. Fault handling

6.2.4.3.1. Faults during the sending phase

This subclause describes the faults which occur while the originator is transmitting the message to the VRSW.

6.2.4.3.1.1. Message loss on the UDT - system terminal segment

The message transmission procedure between the UDT and the system terminal is protected. Message losses shall be detected and reported to the UDT.

6.2.4.3.1.2. ST refusal to transmit the message

The system terminal can refuse to transmit the message on the physical radio Channel. The UDT shall be advised of the failure.

6.2.4.3.1.3. Message loss on the system terminal - VRSW segment

A technical fault on the system terminal - VRSW segment can cause a non-reported loss of the message. The user shall not be informed that the message has been lost.

6.2.4.3.1.4. VRSW unable to handle the message

If the VRSW is unable to handle the message (incorrect message, etc.), it shall send an SFN to the originator. The SFN shall include the TMSG-Id and an error code.

6.2.4.3.1.5. Message loss at the VRSW

A fault in the VRSW may lead to a non-reported loss of the message. The user is not informed.

6.2.4.3.1.6. EDT - VRSW link failure

If the EDT is unreachable, the VRSW shall send an SFN to the originator.

6.2.4.3.2. Faults during the distribution phase

This subclause describes the faults which occur during the VRSW to recipient message transmission.

6.2.4.3.2.1. Message loss on the VRSW - system terminal segment

A technical fault on the VRSW - system terminal link may lead to loss of the message.

6.2.4.3.2.2. Unreachable ST

In case of distribution procedure failure, the system terminal shall be considered to be unreachable (see "unreachable ST" subclause in Inter-personal Messaging "faults during the delivery phase"). The message shall be lost.

6.2.4.3.2.3. Message blocked at the ST

If a fault occurs on the system terminal - UDT link after the system terminal has acknowledged the message, it shall remain in the ST's storage memory. The system terminal cannot receive any incoming message until that message has been transmitted to the UDT.

6.2.4.3.2.4. UDT unreachable by the ST

If the system terminal has detected that the UDT is unreachable, the system terminal shall refuse the distribution request sent by the VRSW and the message shall be lost.

6.2.4.3.2.5. EDT unreachable

If there is an EDT - RSW communication failure, the message shall be lost.

6.3. Status Messaging Service

The System shall provide Status messaging services which are transmitted either at user's request or automatically by the System.

All status messages shall be addressed to Dispatch Positions (Stand Alone or at Dispatch Centre). RTs and LCTs shall not receive status messages. LCTs shall not request the emission of status messages.

Predefined status messages transmitted by RTs to SADPs and DC shall be:

- Emergency status;
- dispatcher Call Me Back status.

RT users may also request the sending of an "operational user status". Status code is then given by the user (MMI), but not interpreted by the System (user to dispatcher status).

Predefined status messages may be transmitted by DPs to other DPs.

Status messages sent by RTs shall be addressed to a predefined set of SADPs and DC, depending on the visiting cell and the Fleet of the originator RT:

- when creating a Cell, the operator at the OMC shall designate a List Address for each Fleet, as being the addressee of status messages sent by RTs belonging to a given Fleet;
- this List Address shall be defined at the OMC. It shall contain the list of SADP and DC addresses designated to be effective recipients of the status messages;
- whenever an RT sends a status message, the System shall automatically consider both the Fleet and the visiting cell of the originator RT to determine the destination List Address. The system shall then deliver the status message to the concerned set of Dispatch Positions (Stand Alone or at Dispatch Centre).

All status message transactions shall use the Control Channel.

6.4. Data transmission services

6.4.1. Services offered over UDP

6.4.1.1. Basic service

6.4.1.1.1. Presentation

The data transmission services offered over UDP provide non-transparent data transfers

- between a user data terminal (UDT) and another user data terminal or a group of user data terminals or an data application server (DAS)
- between a DAS and an UDT or a group of UDTs.

To transmit a UDP datagram, the source application shall provide:

- the source informations (IP address and UDP port)
- the destination informations (IP address and UDP port)
- the priority level of the UDP datagram
- the encryption mode of the UDP datagram

Because of the multiple possibilities of recipients and the variety of the radio services in the TETRAPOL system, the source application shall provide the appropriate radio modes to transmit the datagram through the system.

To transmit a UDP datagram to a DAS, the source application in the UDT shall provide:

- the radio submission mode requested to transmit the UDP datagram from the terminal to the network

To transmit a UDP datagram to a UDT or a group of UDTs, the source application in the DAS shall provide:

- the radio delivery mode requested to transmit the UDP datagram from the network to the terminal or the group of terminal

To transmit a UDP datagram to a UDT or a group of UDTs, the source application in the UDT shall provide:

- the radio submission mode requested to transmit the UDP datagram from the terminal to the network
- the radio delivery mode requested to transmit the UDP datagram from the network to the terminal or the group of terminal

Priority level, encryption mode, radio transmission mode are encoded in the UDP source port (low byte).

6.4.1.1.2. Participants

Participants in a UDP data transmission include UDTs, groups of UDTs and a DAS.

In order to receive a group-addressed UDP data transfer, the terminals that are members of the group shall be within the coverage associated to the group during the transfer.

6.4.1.1.3. Data transmission on radio channel

6.4.1.1.3.1. General procedure

The UDT shall select the UDP source ports for data transfer according to the submission and delivery mode, prority level and encryption mode.

The recipient terminals shall deliver the datagrams to their respective UDT.

6.4.1.1.3.2. Submission modes

The following submission modes may be requested by the UDT and apply over the air interface segment:

- connected packet standard submission mode
- datagram submission mode
- datagram periodic polling mode

6.4.1.1.3.2.1. Connected packet standard submission mode

In this mode, the UDT application shall transmit a datagram containing up to 1472 bytes of applicative data.

The terminal provides an arbitration between the data request and the current service based on exclusion and priority rules.

A transport connection is established on CCH for data submission and a terminal authentication is provided by the system.

Data unit integrity and encryption are provided.

A radio submission acknowledgement is provided by the terminal to the UDT. The UDT application is advised, if it has requested.

6.4.1.1.3.2.2. Datagram submission mode

In this mode, the UDT application shall transmit a datagram containing up to 9 bytes of applicative data.

Data are transmited in a connectionless mode on CCH under the terminal control.

Data unit integrity and encryption are provided.

A radio submission acknowledgement is provided by the terminal to the UDT. The UDT application is advised, if it has requested.

6.4.1.1.3.2.3. Datagram periodic polling mode

In this mode, the UDT application shall transmit a periodic flow of datagrams containing up to 9 bytes of applicative data.

Data are transmited in a connectionless mode on CCH under the network control.

Data unit integrity and encryption are provided.

6.4.1.1.3.3. Delivery modes

The following delivery modes may be requested by the UDT or a DAS and apply over the air interface segment:

- connected packet standard delivery mode
- announced datagram delivery mode
- unannounced datagram delivery mode
- multi-channel datagram delivery mode

6.4.1.1.3.3.1. Connected packet standard delivery mode

In this mode, the application shall transmit a datagram containing up to 1472 bytes of applicative data.

The recipient shall be a UDT.

The network makes an arbitration between the data request and the current service based on exclusion and priority rules.

A transport connection is established on CCH for data delivery and a terminal authentication is done by the system.

Data unit integrity and encryption are provided.

6.4.1.1.3.3.2. Announced datagram delivery mode

In this mode, the application shall transmit a datagram containing up to 1472 bytes of applicative data.

The recipient shall be a UDT or a group of UDTs.

An announced datagram delivery is preceded by an announce on CCH and TCH in order to take part in the transmission.

The terminal makes an arbitration between the data request and the current service based on exclusion and priority rules.

Data are transmited in connectionless mode on CCH under the network control.

Data unit integrity and encryption are provided.

6.4.1.1.3.3.3. Unannounced datagram delivery mode

In this mode, the application shall transmit a datagram containing up to 1472 bytes of applicative data.

The recipient shall be a UDT or a group of UDTs.

Data are transmited in connectionless mode on CCH under the network control.

Data are lost for the terminal if it is on TCH or busy on CCH.

Data unit integrity and encryption are provided.

6.4.1.1.3.3.4. Multi-channel datagram delivery mode

In this mode, the application shall transmit a datagram containing up to 5 bytes of applicative data.

The recipient shall be a UDT or a group of UDTs.

Data are transmited in connectionless mode on CCH and TCH under the network control.

Data are received by the terminal without interaction with the current service.

Data unit integrity and encryption are provided.

6.4.1.1.4. Coverage

Point-to-point UDP data transmission may occur between two UDTs registered in the network

Point-to-multipoint group addressed UDP data shall be transmitted over the coverage associated with the group.

6.4.1.1.5. Addressing

IP addressing shall be used for source and destination addresses.

Class A IP addresses shall be used to designate:

- a UDT in relation with the RFSI individual explicit address of the terminal it is attached to
- a group of UDT related to a group address their associated terminals belong to
- a functional entity in the SwMI or a external network (DAS).

6.4.1.1.6. Transmission priority

Priorities are routine, urgent and flash.

6.4.1.1.7. Encryption mode

Two encryption modes apply; mandatory encryption or facultative encryption.

6.4.1.2. Supplementary services

6.4.1.2.1. Data transfer forwarding

This supplementary service is not applicable.

6.4.1.3. Fault handling

6.4.1.3.1. Faults during the submission

Interactions between concurrent datagram transfers or between a datagram transfer and a connected packet transfer shall be handled by the terminal and the network.

6.4.1.3.2. Faults during the delivery

Interactions between concurrent datagram transfers or between a datagram transfer and a connected packet transfer shall be handled by the terminal and the network.

6.4.2. Services offered over TCP

6.4.2.1. Basic service

6.4.2.1.1. Presentation

The data transmission services offered over TCP provide non-transparent data transfers in connected mode

- between a user data terminal (UDT) and another UDT or an data application server (DAS)
- between a DAS and an UDT.

To establish a TCP connection, the source application shall provide:

- the source informations (IP address and TCP port)
- the destination informations (IP address and TCP port)
- the priority level of the TCP connection
- the encryption mode of the flow.

Because of the multiple possibilities of recipients and the variety of the radio services in the TETRAPOL system, the source application shall provide the appropriate connected packet radio modes to transmit the TCP/IP flow through the system.

To establish a TCP/IP connection to a DAS or a UDT, the source application in the UDT shall provide:

- the radio submission mode requested to transmit the TCP/IP messages from the terminal to the network, among the different connected modes

To establish a TCP/IP connection to a UDT, the source application in the DAS or in the UDT shall provide:

- the radio delivery mode requested to transmit the TCP message from the network to the terminal.

Priority level, encryption mode, radio transmission mode are encoded in the TCP source port (low byte).

6.4.2.1.2. Participants

Participants in a TCP/IP data transmission include a UDT and a UDT or a DAS.

6.4.2.1.3. Data transmission on radio channel

6.4.2.1.3.1. General procedure

The UDT shall select the TCP source ports for data transfer according to the submission and delivery mode, prority level and encryption mode.

The recipient terminals shall deliver the datagrams to their respective UDT.

6.4.2.1.3.2. Connected packet submission modes

The following submission modes may be requested by the UDT and apply over the air interface segment:

- connected packet standard submission mode on CCH
- connected packet standard submission mode on DCH

In these modes, the UDT application shall transmit a datagram containing up to 1472 bytes of applicative data.

The terminal provides an arbitration between the data request and the current service based on exclusion and priority rules.

A transport connection is established on CCH or on DCH for data submission and a terminal authentication is provided by the system.

Data unit integrity and encryption are provided.

A radio submission acknowledgement is provided by the terminal to the UDT. The UDT application is advised, if it has requested.

6.4.2.1.3.2.1. Connected packet delivery mode

In this mode, the application shall transmit a datagram containing up to 1472 bytes of applicative data.

The recipient shall be a UDT.

The network makes an arbitration between the data request and the current service based on exclusion and priority rules.

A transport connection is established on CCH or on DCH for data delivery and a terminal authentication is done by the system.

Data unit integrity and encryption are provided.

6.4.2.1.4. Coverage

Point-to-point TCP data transmission may occur between two UDTs or DAS registered in the network

Point-to-multipoint group addressed UDP data shall be transmitted over the coverage associated with the group.

6.4.2.1.5. Addressing

IP addressing shall be used for source and destination addresses.

Class A IP addresses shall be used to designate:

- a UDT in relation with the RFSI individual explicit address of the terminal it is attached to
- a functional entity in the SwMI or a external network (DAS).

6.4.2.1.6. Transmission priority

Priorities are routine, urgent and flash.

6.4.2.1.7. Encryption mode

Two encryption modes apply; mandatory encryption or facultative encryption.

6.4.2.2. Supplementary services

6.4.2.2.1. Data transfer forwarding

This supplementary service is not applicable.

6.4.2.3. Fault handling

6.4.2.3.1. Faults during the submission

Interactions between concurrent datagram transfers or between a datagram transfer and a connected packet transfer shall be handled by the terminal and the network.

6.4.2.3.2. Faults during the delivery

Interactions between concurrent datagram transfers or between a datagram transfer and a connected packet transfer shall be handled by the terminal and the network.

7. Services in Fallback modes

7.1. Presentation

This clause describes the fallback mode characteristics which are common to the voice and data services in network mode when a sub-part of the network (SwMI) is temporarily isolated from the rest of the network, until the connection is recovered.

7.2. Inter-RN disconnected FBM services

7.2.1. Overview

Should a regional network be isolated from the rest of the network, then voice and data services within the regional network are still possible in the regional network, as long as neither remote location information nor voice circuit allocation is required from other regional networks.. Voice calls whose voice circuit shall use a Network component which is external to the RN cannot be set-up. Data services in which one participant is external to the RN cannot be provided.

Visiting terminals registrations are local until the isolated regional network reconnects to the rest of the network.

When the EDT is unreachable, the External Application Messaging Service is unavailable; if a UDT sends a EXAMS message to the EDT, the Network shall send an SFN to the originator.

7.2.2. IPMS and RNLMS messaging fallback mode

7.2.2.1. Participants, sending, submission and transfer

When a RSW or a regional network is isolated from the data and signalling network, only transmissions between UDTs are possible.

When a regional network is isolated from the rest of the network, the UDTs that are involved in an inter-personal or local messaging service shall be both registered in that same regional network. In case of Inter-personal messaging service, this common regional network shall be their home regional network.

Otherwise either an SFN or a DFN is sent and rejection report containing the contents of the initial IPMS message shall be transmitted to the Garbage Messaging Collector of the VRSW'S RN.

Normal processing of local messaging sending and submission procedures applies.

An IPMS transfer attempt shall cause the HRSW to send a Delivery Failure Notification to the originator. Transfer is not applicable to RNLMS.

7.2.2.2. Delivery and distribution

Upon HRSW location failure of the recipient STs in the Regional network for the purpose of an IMPS distribution, the distribution secured message forwarding procedure applies.

Normal processing of local messaging service applies.

7.2.2.3. Copy to the EDT

When the EDT is unreachable from the HRSW, IPMS copies shall be queued until HRSW-EDT link recovery.

7.2.2.4. Addressing

The IPMS message may contain one or more addresses. X.400 O/R name type addresses are not available in this fallback mode of the Inter-Personal Messaging Service.The use of any address which does not belong to the home RN shall cause a DFN to be sent to the originator.

The UDT uses one or several single individual explicit address or, implicit address, list address from the visited RN for local messaging.

7.2.2.5. Message processing

The IPMS message forwarding mechanism requires that the terminal be forwarded to a terminal located in the same Regional network, otherwise the "distribution secure" mechanisms apply

Normal mode processing applies for message forwarding in the local messaging service.

Normal mode processing applies for IPMS alternate recipient.

If the IPSM Back-up Terminal is reachable, it shall back-up the messages; otherwise, they shall be queued.

The IPMS Garbage Messaging Collector shall receive the errored messages and the rejection reports concerning the Visitor Terminals.

During sending or distribution phase, the normal mode processing applies, with the VRSW and the HRSW combined, excluding the EDT faults upon delivery.

The IMPS procedure for copy queue overflow fault applies in case of a fault during distribution of the EDT copy.

7.3. MSW-RSW disconnected FBM services

7.3.1. Overview

Should a RSW be disconnect from another RSW , then a recovery procedure shall try to rebuild the initial coverage for all affected group communications.

During this recovery procedure, each isolated part (i.e. the isolated RSW and the rest of the network) shall dynamically reconfigure its resources and provide the best available partial coverage for on-going group communications, untill the initial coverage is recovered when the RSW reconnects to the rest of the network.

Should a RSW be disconnect from another RSW required for database access, e.g. a MSW, then a recovery procedure shall try to rebuild the link and the signalling flow shall be re-routed.

Terminals registered under base stations attached to an isolated RSW shall be provided with the same on-going group communications, but on a reduced coverage. Private calls can be setup between terminal attached to the same isolated part of the network.

Should an MOCH or ECH be partially established in the rest of the network while the RSW is disconnected, the total coverage of that communication is recovered, upon RSW reconnection with the rest of the network.

Should an MOCH or ECH be released in the rest of the network while the RSW is disconnected, that communication is released in the RSW upon reconnection with the rest of the network.

When the EDT is unreachable, the External Application Messaging Service is unavailable; if a UDT sends a message to the EDT, the Network shall send an SFN to the originator.

The Inter-Personal Messaging service shall not be available in RSW disconnected FBM. The RSW that detects that an VRSW is unreachable shall transmit to the originator an SFN containing the Temporary Message Identifier provided by the UDT with an error code.

7.3.2. Local messaging fallback mode

7.3.2.1. Presentation, participants and coverage

This fallback mode procedures applies to RNLMS for MSW-RSW disconnected FBM and for RSW disconnected FBM.

When the VRSW is unreachable, the service shall be provided by the RSW which was elected as the controlling RSW when the switch-over to RSW disconnected FBM occurred.

The possible participants in the Local Messaging service shall be the UDTs.The Local Messaging Service in FBM is available on the coverage defined by the set of RSWs still connected together and that are isolated from the previous MSW.

7.3.2.2. Sending and Submission, delivery and distribution

The sending and submission phases are only possible for those UDTs connected to an system terminal located within the coverage of the RSWs operating in RSW disconnected FBM. Otherwise, the controlling RSW shall generate a SFN.

Transmissions to the EDT shall always result in an SFN.

Transfer is not applicable.

The controlling RSW shall locate the recipient for message distribution.

Copying to the EDT is not applicable to RSW disconnected FBM.

Normal addressing procedure applies, with explicit and implicit addresses, but list addresses and EDT addresses are not supported in this FBM.

Normal procedure applies for message forwarding.

7.3.2.3. Faults during the sending phase or during the distribution phase

Normal procedure applies, excluding the EDT faults. The VRSW shall be replaced by the controlling RSW.

7.4. RSW disconnected FBM services

Should a base station be disconnect from its RSW, then users of radio terminals involved in on-going group communications shall still be provided with the same group communications, but on a coverage reduced to the isolated cell.

As the EDT is unreachable, the External Application Messaging Service is unavailable; if a UDT sends a message to the EDT, the Network shall send an SFN to the originator.

7.5. BSC disconnected FBM services

Should one transmitter/receiver be unavailable or be disconnected from its base station controllers (BSC), then the services shall be provided in the cell with the remaining transmitters/receivers. The reallocation of the frequencies shall be performed automatically so that the operation can proceed with the terminals.

Should all transmitters/receivers be disconnected from the BSC, then, in this rarely encountered mode, the base station shall automatically provide an open channel with no OG access restriction to those terminals that cannot reselect another cell, as an end stage of fallback mode capabilities. Other services are not available.

History

Document history		
Date	**Status**	**Comment**
27 September 1995	First version	Version 1.0.0
2 November 1995	Update after review	Version 1.0.1
14 November 1995	Precision on phase	Version 1.0.2
12 December 1995	Editorial corrections -Scope	Version 1.0.3
2 January 1996	Edition	Version 1.0.4
28 February 1996	Update	Version 1.0.5
29 March 1996	Add priority rules, security, talkgroup	Version 1.0.6
15 April 1996	Update after review	Version 1.1.0
30 April 1996	Tetrapol Forum approval	Version 2.0.0
30 June 1996	Update	Version 2.0.1
18 July 1996	Review	Version 2.0.2
31 July 1996	Approved version	Version 2.1.0
15 January 1997	Update	Version 2.1.1
19 February 1997	System review 12 march 1997	Version 2.1.2
19 April 1997	Update after review	Version 2.1.3
19 December 1997	Emergency call, crisis open channel, silent call, ambiance listening, TCP/IP, connected packet mode on CCH or DCH	Version 2.1.4
25 June 1997	Tetrapol Forum approval	Version 3.0.0
16 March 1998	Update	Version 3.0.1