ISITEP
D4.4.2 - TETRAPOL-TETRAPOL GATEWAY INTERFACES DESIGN

Document Manager:	Serge DELMAS	Cassidian SAS	Editor

Programme:	Inter System Interoperability for Tetra-TetraPol Networks
Project Acronym:	ISITEP
Contract Number:	312484
Project Coordinator:	Selex ES
SP Leader:	CAS FI

Document ID N°:	ISITEP_D4.4.2_20140630_V1.0	**Version:**	V1.0
Deliverable:	D4.4.2	**Date:**	30/06/2014
		Status:	Approved

Document classification	**PUblic**

Approval Status	
Prepared by:	Serge DELMAS (CAS FR)
Approved by (WP Leader):	Serge DELMAS (CAS FR)
Approved by (SP Leader):	Jaakko SAIJONMAA (CAS FI)
Approved by (Coordinator)	Paolo DI MICHELE (SES)
Security Approval (Advisory Board Coordinator)	Etienne LEZAACK (BFP)

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Cassidian France team	Cassidian France	Telecom engineers specialized in PMR networks

DISTRIBUTION LIST

Name	Company / Organization	Role / Title
All Company Project Managers	All involved companies	Members of the Steering Committee
Elina MANOVA	EC DG REA	EC Programme Officer

REVISION TABLE

Version	Date	Modified Pages	Modified Sections	Comments
V1.0	30/06/14			Final version

Publishable extended abstract

This document is a technical definition of the interface that will be used to connect 2 TETRAPOL networks in ISITEP project. It is based on the technical requirements of D4.4.1 deduced from operational requirements gathered in WP2.

CONTENTS

1. INTRODUCTION

1.1 ISITEP at a glance

ISITEP (Inter System Interfaces for TETRA-TETRAPOL Networks) project will achieve operational

interoperability among European first responders addressing the regulative, organizational, operational and technical level. ISITEP (Inter System Interfaces for TETRA-TETRAPOL Networks) project will achieve operational interoperability among European first responders addressing the regulative, organizational, operational and technical level.

The project will define public specifications of technical and procedural innovations, as well as novel processes for safety applications.

Figure 1: ISITEP framework

The general objective is obtained jointly addressing four components that are coherently defined, developed and integrated through a novel Framework which is constituted by:

A Mission-oriented Framework containing a standardized model of operational procedures and associated functional radio model

A European Inter System Interface (ISI) cloud network integrating the PPDR national infrastructures to allow roaming capability services within a secure framework.

Enhanced User Terminals: integrating TETRA/TETRAPOL technology into a novel terminal architecture based on programmable devices (Tablet, Smartphones).

Interoperability enabling tools including tools for infrastructures dimensioning, training, business model assessment and services for safety operations.

1.2. WP44 and status of this deliverable in WP44

In this work package, a hardware and software solution for ISITEP will be developed so that interoperability between two TETRAPOL networks meets user requirements dealing with security, quality of service, performance and connectivity. In the WP, this connection will also tested with deployable network for a TETRA connection

The solution will connect to the TETRAPOL networks via CC API providing required access to the common services offered by both networks (PTT voice, voice groups, status)

Specific objectives include:

• Verification of ISITEP requirements for TETRAPOL-TETRAPOL interoperability.

• Interface design and parameterisation.

• Hardware and software development.

• Unitary testing.

• testing with deployable network

This deliverable D44.2 constitutes the interface design of the TETRAPOL gateway.

Please note that TETRAPOL ISI is not defined in TETRAPOL specifications and no implementation of such an interface is deployed on existing TETRAPOL networks.

1.3. TETRAPOL Overview

1.3.1. General Overview

The International Telecommunications Union (ITU) – a specialised agency responsible for the standardisation of telecommunications at the world level – has officially recognised TETRAPOL as an effective solution for professional digital radio communication networks.

Moreover, the European Union Police Co-operation Group, combining the police forces of 12 European Union countries, took an official position recognising TETRAPOL as an appropriate technology for Public Safety (May 98). This statement was ratified (April 1999), by the Schengen Executive Committee, to be applicable within all the European Union.

TETRAPOL networks main manufacturer is Airbus DS. In Europe, we can list various TETRAPOL networks for example: Acropol (France), Rubis (France), Pegas (Czech Republic), Polycom (Switzerland), SITNO (Slovakia), PHOENIX (Romania) and Sirdee (Spain). We can see in the next figure the worldwide map of TETRAPOL networks.

Figure 2 : TETRAPOL networks around the worls

TETRAPOL is a digital cellular trunked radio system which shall provide digital narrowband voice and data services for public safety.

It is mainly intended for:

- Security and emergency forces: police force, army, fire brigade, ambulance service, etc.,
- Transport services and industry: port, industrial site, bus, train, airport, etc.

It offers the following services to fixed and mobile users:

- voice services: individual call, group communication, direct mode, emergency call, etc.,
- data services: messaging, data transmission between the customer's IP applications, etc.

These services are secured, in particular, through user authentication and Communication encryption mechanisms.

1.3.2. Transmission characteristics

Based on an FDMA (frequency division multiple access) multiplex approach using a narrow-band channel operating at 12.5 KHz, the TETRAPOL solution is a resource–sharing system (trunking function), fully digital.

The TETRAPOL speech coding requires the use of a CELP (Code Excited Linear Prediction) speech coding.

The frequency band allocated is: 380 MHz – 430 MHz and 440 MHz – 490 MHz.

Transmission on a radio channel uses **Gaussian Minimum Shift Keying (GMSK)** modulation.

1.3.3. TETRAPOL system Architecture

A TETRAPOL network consists of:

- a fixed infrastructure, called a network, composed mainly of **switches, radio base stations** and equipment **for interfacing** with internal systems (system for recording communications, vehicle location system) or external systems. The elements of this fixed infrastructure are linked with either IP or E1/T1 interfaces depending on the network,
- **line connected** and **radio terminals**, through which users can access system services,
- an **operating and maintenance network**, mainly comprising system management stations and a management server,
- **maintenance equipment** not connected to the network,
- a **recording system** for recording group communications.

It can be connected to the following external systems:

- an **analog** network,
- a private or public **telephone network** (PSTN),
- an **INTERNET network** for accessing databases or transferring data from a data terminal,
- a dispatch centre.

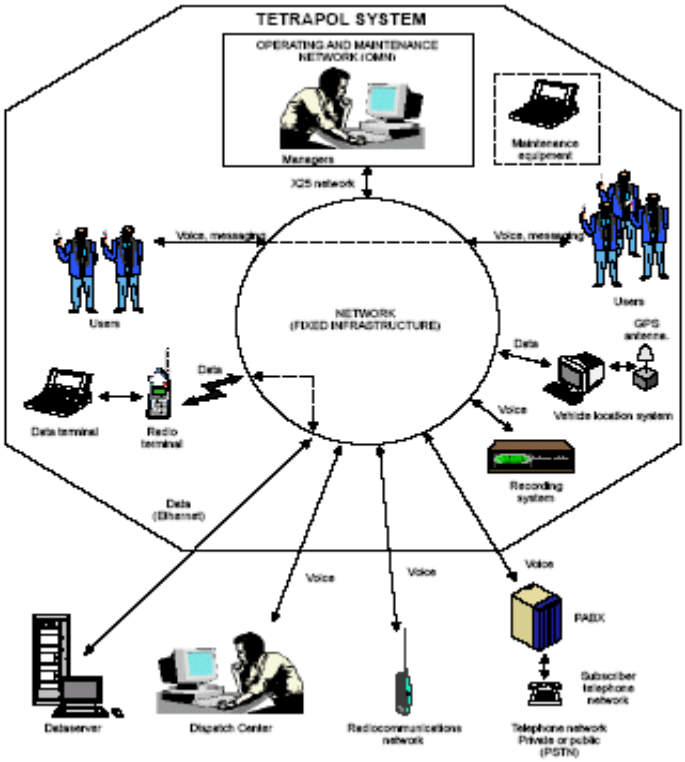


Figure 3 TETRAPOL System Architecture

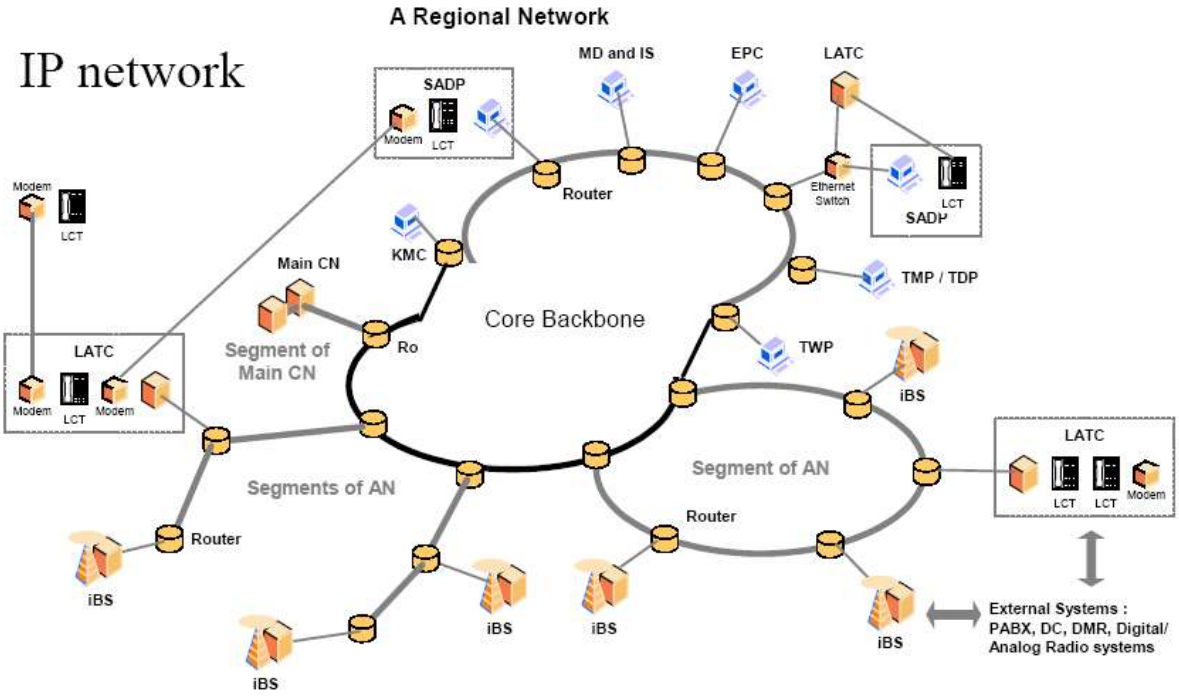


Figure 4 TETRAPOL IP System Architecture

1.3.4. Organisation and management characteristics

Different entities (local police, taxis, fire brigade, etc.) can access the services offered by the network. These entities, called organizations, group together users and managers.

Network management is divided into three main functions:

- **technical management**, carried out on the Technical Management Position(s), whose functions include configuration, monitoring, alarm management, network supervision and maintenance. All organisations in the network are managed by one or more technical operators
- **tactical management**, carried out on the Tactical Working Position, whose functions include management of terminals and users, and management of groups and communications. Several organisations can be managed by a single tactical operator, or conversely, one tactical operator can be dedicated to a single organisation
- **the operational management of communications**, carried out by a stand alone dispatch position or a dispatch centre, whose function includes the supervision of communications and users.

An operator can set up and participate in all types of communication (private, group, emergency, etc.)

Several organisations can be managed by a single tactical operator, or conversely, one tactical operator can be dedicated to a single organisation.

1.3.5. Transmission modes

Radio communications between terminals are carried out:

- either in base station connected mode, i.e. via at least one radio base station,
- or in **direct mode**, i.e. without using any intermediate equipment (radio base station or independent repeater),
- or in **repeater mode**, i.e. via an independent repeater,

The frequency band is divided into physical radio channels. Frequency ranges are allocated to each of these 3 modes.

1.3.6. TETRAPOL Radio communications

1.3.6.1. Voice communications

Voice communications are **semi–duplex**, i.e. they operate via the push–to–talk function: a terminal engaged in a communication either transmits or receives.

Voice services are divided into four categories:

- **private communications,** set up at a caller's request towards one or more individual called parties
- **group communications**, already set up on a given coverage and intended for one or more groups
- **direct mode communications**, which are communications between terminals within radio–electric range on channels reserved for this purpose
- **repeater mode communications**, which are communications between terminals within radio–electric range of an independent digital repeater, on channels reserved for this purpose

1.3.6.2. Private communications

The TETRAPOL system offers two types of private communication:

- An **individual call** is a voice communication between a calling party and a called party, in base station connected mode. The subscribers (calling party and called party) can be standard users and / or stand alone dispatch position operator or a dispatch centre operator. They can be located anywhere within the coverage of a TETRAPOL system. One of the two subscribers can belong to an external network.
- A **multi–party call** is a voice communication between a calling party and up to 4 called parties, in base station connected mode. Each called party is addressed individually. The subscribers (calling party and called party) can be standard users and / or stand alone dispatch position operator or a dispatch centre operator. They must be located in the same regional network.

1.3.6.3. Group communications

The TETRAPOL system offers four types of group communication:

- A **talkgroup** is a group communication that enables subscribers belonging to the **same operating group** to communicate together when they are located under a defined **geographical area.**
- An **open channel** is a multi-group communication that enables subscribers belonging to **several operating groups** to communicate together when they are located under a defined **geographical area.**
- An **emergency call** is a function which allows any user of a radio terminal, via the emergency key on his terminal, to make a call informing other subscribers of an emergency situation requiring assistance. Recipients are notified of the emergency call by a particular ring tone from the terminal. The terminal displays the call and identity of the calling terminal. The consequences of an emergency call **depend on the terminal configuration** set by the network managers and the operational conditions.
- The **broadcast call** is a **one-way communication** from a calling dispatcher (stand alone dispatch position operator or dispatch centre operator) to one or several groups.

1.3.7. Communications in direct mode

The TETRAPOL system offers two types of communication in direct mode:

- **Direct mode** (also called walkie–talkie mode) is a service that enables terminals within radio–electric range to communicate with each other on channels reserved for this purpose. These communications do not use network resources (infrastructure), and can therefore be made outside network coverage.
- **A direct mode emergency call** allows a terminal to transmit an emergency signal on a special channel, called a direct mode emergency call channel, to all terminals operating in Base Station connected mode or in direct mode which are within radio–electric range. The user who has transmitted the signal can then communicate on a direct channel with the terminals which answered the call.

A terminal may have the direct mode with network monitoring functionality (also called dual watch). This is a function allowing a terminal in direct mode to continue to receive network calls or messages if there is no traffic on the direct channel.

1.3.8. Communications in repeater mode

Repeater mode is a service that enables terminals within radio–electric range of an independent digital repeater to communicate with each other on channels reserved for this purpose. These communications do not use network resources (infrastructure), and can therefore be made outside network coverage.

1.3.9. Supplementary services

Supplementary services cannot be accessed by direct mode or repeater mode communications, except to identify the speaker.

The supplementary services available for each basic service are presented:

- **Access control** ensures that a subscriber wishing to participate in a communication is authorised to do so.
- **Ambience listening** enables an authorized operator to force the transmission of a terminal in order to listen to what is happening in the terminal's environment.
- **Zone restriction** limits the registration of a terminal to a list of regional networks.
- **Call forwarding** is used to direct a call sent to one subscriber to another subscriber.
- **Calling party identification** allows the identity of a caller to be recorded and/or displayed on an item of equipment (terminal, recorder, etc.…) when the call is set up.
- **Call transfer** allows a subscriber who is called to transfer the ongoing call to another subscriber.
- **Eavesdropping** enables an operator to listen to a private communication, without the knowledge of the speakers concerned.
- **Group merging** enables the user to obtain a new operating group by bringing together several groups in the same open channel.
- **Interconnection** provides connection to another network
- **Late entry** is a network device enabling terminals which have not entered a communication at the start to do so later if they need to.
- **Scan** allows a terminal to participate in several group communications (talkgroups or open channel) defined in a scan list: each active group communication is scanned.
- **Priority scan** the first open channel in the scan list is declared as priority: the terminal toggles automatically into this open channel as soon as it is enabled. When the priority open channel is disabled, the terminal can listen to other open channels in the list without being able to take part. The push to talk is always associated with the priority open channel.
- **Silent call** sets up an individual call without making the called terminal ring and automatically unhooks the terminal.
- **Call waiting**1 informs a subscriber involved in a communication of a new incoming call waiting to be answered.
- **Talking party identification** displays the identity of the subscriber speaking in a communication.

1.3.10. Data communications

The TETRAPOL system offers two types of data services:

- **IP data** service,
- short message service (**SMS**).

1.3.11. IP data services

1 The availability of call waiting per type of communication depends on the type of incoming call.

The TETRAPOL system offers data architecture based on the standard IP protocol. It enables the transmission of data through the network:

- between mobile data terminals connected to radio terminals,
- between one or more mobile data terminals and a server.

These elements support the applications defined by the customer. The network behaves like a gateway as regards the transmission of data between these elements.

1.3.12. Short message service (SMS)

There are two types of message service:

- **text message** to exchange short messages of a limited size (not more than 150 characters) defined by the user (“free text”)
- **status message** to exchange short predefined messages (not more than 24 characters), called statuses. Statuses are predefined by organisation

SMS Transmission may be by one sender to one or more recipients, located in the TETRAPOL network. The SMS service transmits messages between the following entities:

- TETRAPOL terminals
- stand alone dispatch position / dispatch centre station
- data server

1.3.13. Routing

The following paragraph deals only with TETRAPOL IP systems.

The following diagram shows possible interconnection topologies for IP Tetrapol PMR sites with the participation of an IP service provider:

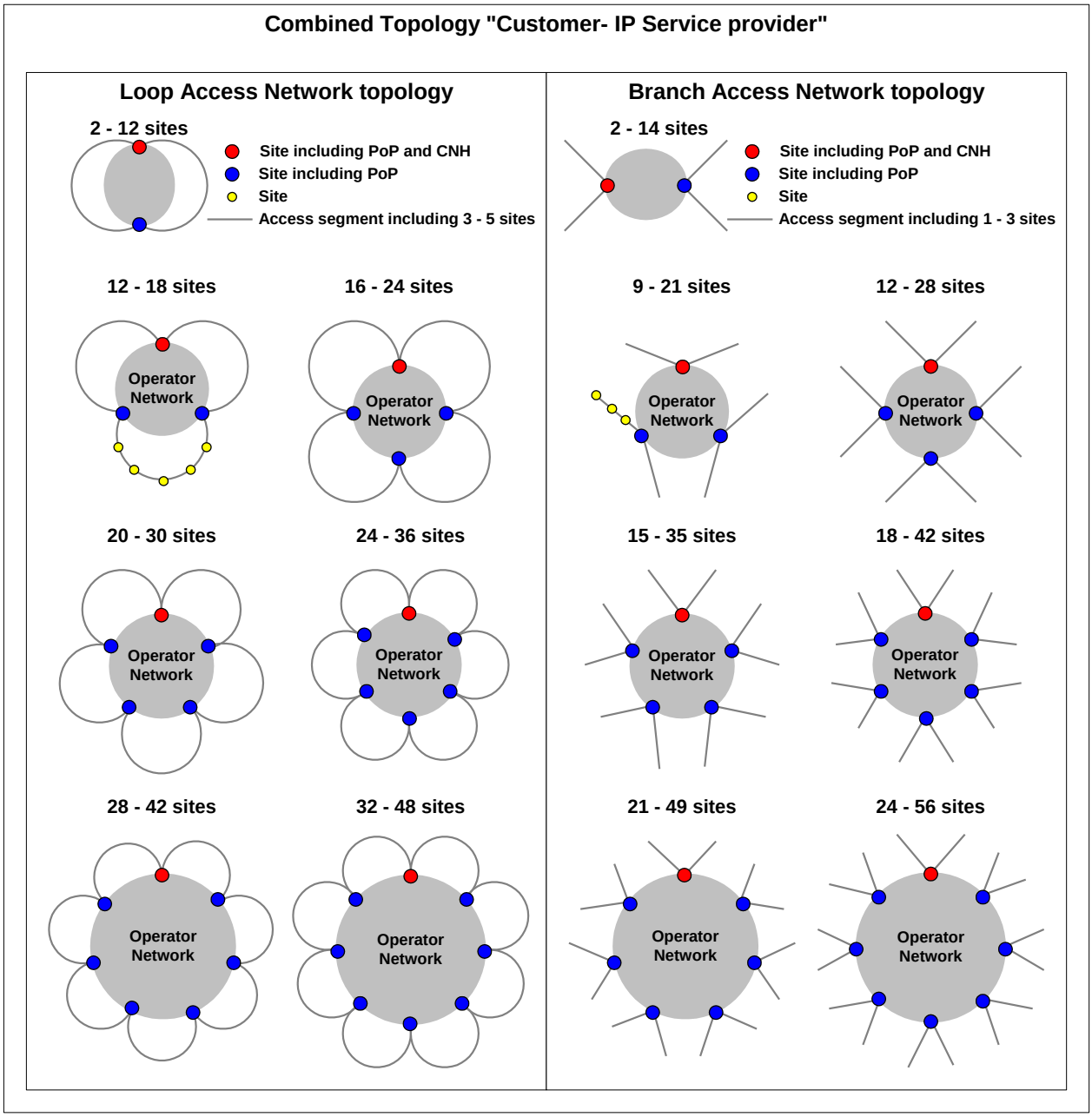


Figure 5 TETRAPOL IP topologies

Architecture: The basic scenario is that each Tetrapol site close to a service provider POP will be connected to one CPE. In reality, the sites (often radio) will frequently be at locations which are poorly served by a POP. In such cases, a loop of sites will, if possible, be constituted, with both extremities connected to the service provider network (CPE). The sites in a loop will be connected to each other by leased lines or radio links or using other appropriate solutions (see service provider's offer).

Tetrapol Sites: There are different types of Tetrapol PMR equipment. Each of these types of equipment can in itself constitute a site (e.g. iBS). It is also possible to group a number of types of equipment to form a Tetrapol site (e.g. CNH + MD + PS + TMP).

1- Switching equipment (CNH): This set of equipment manages, controls and supervises, for **one** regional network, the Tetrapol PMR network voice and data signalling, the administration of the technical, tactical and operational databases and the management of group calls (multi-unicast management of RTP/RTCP sessions). The CNH sites are normally positioned in such a way as to connect easily to a POP.

2- Access Network Equipment (iBS and LATC): Interconnected (in a branch of 1 to 3 sites or in a loop of 3 to 5 sites) and linked to one CPE (in case of branch) or two CPE (in case of loop), this equipment provides PMR users with radio or fixed-line access to the network and communicate using radio coverage. The number of such sites and associated fixed-line or radio channels determines the bandwidth required for the leased lines or radio links and, at the extremities, for the service provider CPE.

3- Operating equipment (MD, PS, TMP, TWP and SADP): These equipment provide the operator of the PMR network with the tools and resources needed for the administration, supervision and management of the Tetrapol private radio network.

4- Key management equipment (KMC): This equipment enables management of regional networks encryption keys for a national PMR network (equipment present only if there is an interconnection between a number of regional networks).

5- External equipment: These equipment enable the network user to take advantage of external applications using the Tetrapol network (e.g. satellite vehicle location, data server, PABX interconnection and digital call recording)

The routing protocols used in the TETRAPOL IP solution are standard protocols (OSPF, BGP). The objective is to minimize the convergence duration for QoS reasons (service availability).

1.3.14. QoS management

The following paragraph deals only with TETRAPOL IP systems.

QoS: DiffServ marking is used to indicate the priorities for the IP packets. The following table resumes the classification of the IP Tetrapol flows encountered:

The following table resumes the classification of the IP TETRAPOL flows:

Class	Applications	Critical parameters	*E.g. DiffServ*
1-Voice	RTP TETRAPOL voice sessions	Minimum bandwidth guaranteed Low packet-loss, latency and jitter	*EF*
2-Critical Data	Critical TETRAPOL operational data	Minimum bandwidth guaranteed Low packet-loss rate Latency and jitter controlled	*AF 11*
3-Non-Critical Data	Non-critical TETRAPOL data No minimum transmission-speed guarantee	Minimum bandwidth guaranteed Performance not managed	*AF 12*
	Non-TETRAPOL customer applications	Best effort Performance not managed	*Best Effort*

Service provider IP network performances: Given the real-time application (voice) transmitted on the service provider IP network, certain boundary values must be guaranteed by the IP network service provider.

The table below resumes the 3 quality indicators which enable the customer to monitor the IP service provider service commitments:

Indicators	Impact on the network
Service availability	Respect of convergence time for (re)routing of IP packets Security for network equipment Security for network links
Latency	End-to-end transit time (one-way and roundtrip delays) Jitter
Bandwidth by service class	Bandwidth guaranteed end-to-end Load sharing and balancing Sharing of WAN bandwidth

Bandwidth: The bandwidth required for an IP access provided by the operator depends on the Tetrapol equipment connected to the access and on the recommended topology (loop or branch). Following the network engineering, a bandwidth is

requested to the service provider, who then undertakes to guarantee that bandwidth.

E.g.: bandwidth required for a base station 4 carriers = 190kb/s

"One way" max. latency: Depends on the IP/UDP/RTP communications, the maximal one-way transit delay required are :

- **40 ms** for an IP/UDP/RTP communication between two **intra-RN** Tetrapol network equipment (CNH, iBS or LATC)
- **40 ms** for an IP/UDP/RTP communication between two **inter-RN** Tetrapol switching equipment (CNH)
- **80 ms** for an IP/UDP/RTP communication between two **inter-RN** Tetrapol Access Network equipment (iBS or LATC)

Jitter: Depends on the IP/UDP/RTP communications, the maximal transit delay variation (jitter) required are :

- **20 ms** for an IP/UDP/RTP communication between two **intra-RN** Tetrapol network equipment (CNH, iBS or LATC)
- **20 ms** for an IP/UDP/RTP communication between two **inter-RN** Tetrapol switching equipment (CN)
- **40 ms** for an IP/UDP/RTP communication between two **inter-RN** Tetrapol Access Network equipment (iBS or LATC)

Packet loss: The service provider is required to ensure that the IP packet-loss rate does not exceed **2%** for the Diffserv service class EF (all IP/UDP/RTP packets).

Availability: For the majority of customers, the service provider is required to provide service availability of approximately **99,999%**. This is equivalent to disconnection totalling less than 1 second in 24 hours.

Description of the QoS rules to be implemented on the CPE equipment (router)

- **DiffServ marking:** The CPE must be capable from the LAN interface of identifying the IP flows by applications port (UDP or TCP) in order to provide a WAN interface order of priority for each of these flows. The DiffServ marking (marking of the DSCP field in the IP header) makes it possible to identify the Tetrapol IP flows broken down into 3 service classes (EF, AF11 and AF12) as described above
- **Congestion management (LLQ ou PQ/CBWFQ method):** Once the IP flows have been identified and ordered by service class at the LAN input, they must be directed to queues with different priorities based on these service classes, at the WAN or LAN outputs. The management of these priorities on the access routers will, therefore, be performed using at least 3 queues: one queue with high priority (class EF), one queue with normal priority (class AF11) and one queue with low priority (AF12). Different methods are used for different network equipment manufacturers. We need to be able

to guarantee a strict bandwidth for Tetrapol voice flows as well as a specific, sufficient bandwidth for the other Tetrapol flows (class AF11 and AF12). When the bandwidth allocated for voice is not fully used (as is most frequently the case), it must be possible to use the available bandwidth for the other, lower-priority flows. The access routers must manage this resource-sharing mechanism: LLQ or PQ/CBWFQ method.

- **Congestion avoidance (WRED method):** We recommend the implementation of congestion avoidance techniques enabling network traffic to be monitored with a view to anticipating congestion and avoiding incidents by dropping IP packets. Of the most commonly-used congestion avoidance mechanisms, WRED (Weighted Random Early Detection) is the best-suited for TCP flows, which, by definition, adjust their transmission speeds depending on network congestion levels.
- **IP fragmentation:** We recommend IP-packet fragmentation when a large IP packet is transmitted on a low speed WAN access (e.g. 128 kbps) leading to increased network latency and resultant voice chopping despite QOS management. This functionality is necessary when the router WAN access is below 1.2 Mbps (speed calculated at PPP level).

Security management

The TETRAPOL system employs the following security services:

- **authentication** of terminals before they are used on the network
- **encryption** of communications
- **confidentiality** of information
- suspending access or traffic to a terminal

Authentication of a terminal

A terminal cannot be used until authenticated by the network. Authentication consists in checking that the terminal parameters (individual address, secret key, etc.) match those recorded when the terminal was registered.

Encryption of communications

Encryption of communications is end to end**:**

- on the entire network for voice communications
- on each regional network for data communications
- between the transmitting terminal and the receiving terminals for direct mode or repeater communications

Encryption is systematic for communications in Base Station connected mode, except for:

- emergency open channels to enable all terminals to take part in the open channel
- communications in disconnected cells (Fallback Mode)

In direct or repeater mode, it is the terminal user who chooses whether or not to encrypt the communication.

Communications, whether in Base Station connected mode or not, can be over-ciphered by users who have the necessary rights.

The system can manage encrypted organisations and unencrypted organizations inside a single network.

Encryption is based on the exchange of keys between the Key Manager Centre, the TETRAPOL core network and terminals. The keys are generated by the Key Manager Centre and main switch. Some keys are transferred with diskettes, others via the network. Each of them has a different life cycle.

Confidentiality

Confidentiality is provided by:

- the transmission of **padding** frames, sent on certain channels to simulate traffic,
- use of **temporary terminal identity**. The network provides the terminal with a **temporary terminal identity** for an unspecified period when the terminal registers. The **temporary terminal identity** is then used at each exchange between the terminal and the network, thus avoiding transmitting the address of the subscriber.

Suspended terminal or disabled terminal

If a terminal is lost or stolen, the system provides two levels of protection:

a terminal can be **suspended** by the network tactical operator, thus losing the authorisation to transmit or receive communications in all system modes. The terminal must then be made operational again **by the tactical operator** before it can make any calls,

a terminal can be **disabled** by the network tactical operator, thus losing the authorisation to transmit or receive communications in all system modes. The terminal must then be **returned to the maintenance centre** to receive its rights again.

2. DESCRIPTION OF LEGACY NETWORKS INTERFACES

2.1. On-air interfaces

In case mobiles use the same standard (here we deal with TETRAPOL-TETRAPOL but the same applies for TETRA-TETRA), Air interface is compatible between mobiles as far as they use the same frequency band. This should not be an issue as all Public Safety Networks use the same band in Europe.

Each TETRA network has Mobile Country Code and a network code. These codes are different from one network to another and from one country to another. This mechanism implies that Mobiles must be able to use and be connected on different networks with different mobile and country codes.

Over these initial mechanisms, encryption is used on Public Safety networks. Each country has its own encryption and key mechanism and this information could not be transferred for security reasons to foreign countries. It is therefore necessary to have mechanism on the network to allow other mobiles without any encryption to communicate on a visited network.

The mobiles should use the same standard (TETRA or TETRAPOL) and, if it is applicable, the same encryption mecanism and key.

The visiting mobiles should be pre provisonned in the visited network infrastructure, and the visiting network known from the mobile terminals. If these points are fulfilled then all use cases are allowed. If all these issues are not solved there is no interoperability on-Air interface.

2.2. INI – Inter Network Interface

TETRAPOL ISI is not defined in TETRAPOL specifications and no implementation of such an interface is deployed on existing TETRAPOL networks.

2.3. CONTROL ROOM INTERFACE

The TETRAPOL Control Room Interface is the only interface available on TETRAPOL to have access to basic services on the TETRAPOL network.

The TETRAPOL Control Room interface is specified in the TETRAPOL specifications and is called CC-API. This interface is not directly accessible on some networks such as Polycom in Switzerland, where an additional layer has been added over the CC-API and the interface is called S-PRO connector.

This interface can be complement with the CC-IS interface to allow provision and setup additional mobiles on the visiting network.

2.4. Access security

Each radio terminal of one of the TETRAPOL networks shall be registred into the network and is reconnized by its ID.
Therefore, at the gateway level, it shall be possible to authorize or not each radio terminal.to perform one facility or another.

2.5. Status on legacy PMR networks external interfaces : TETRAPOL network

2.5.1. TETRAPOL network

2.5.1.1. System overview

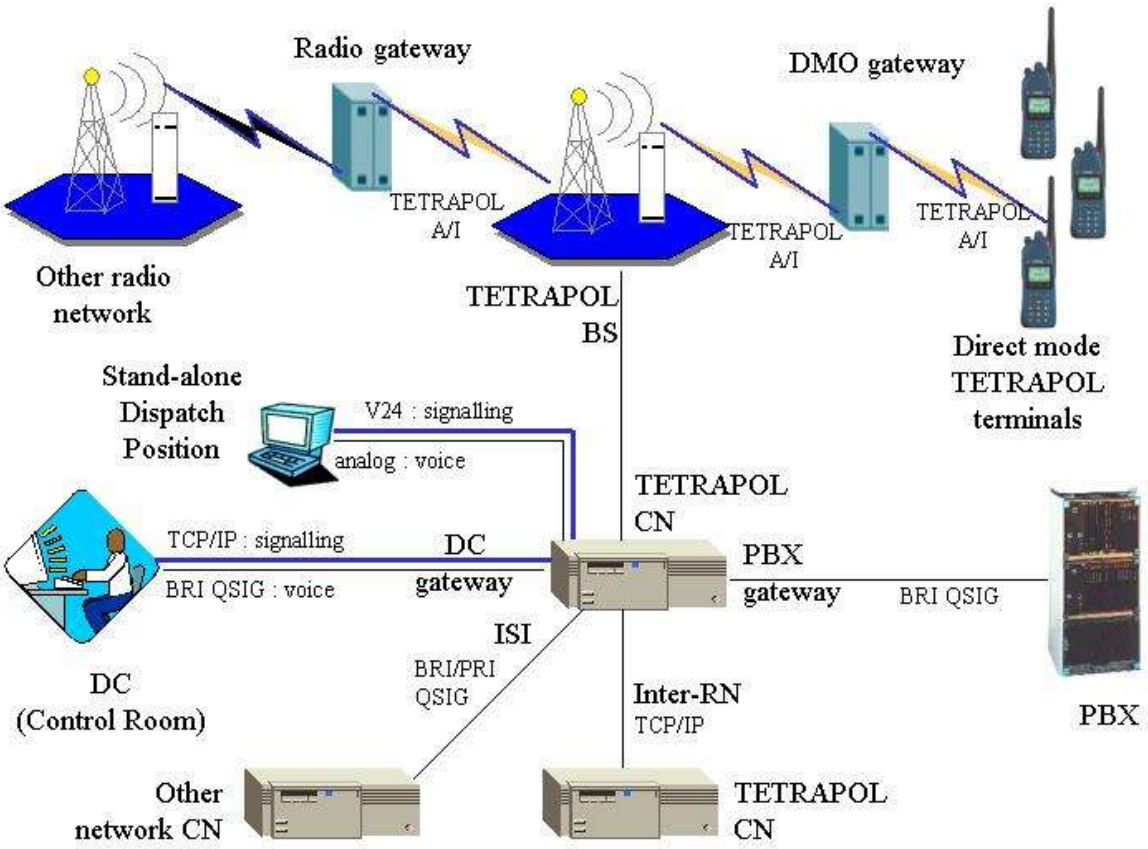


Figure 6 : TETRAPOL network elements (and interfaces)

Interfaces are classified as:

- **Terminal interface**: They are based on a device that has the same functions as a radio or wired TETRAPOL terminal. In particular, they support communications from between an Access Gate (AG) and external interface point, with voice in clear, analog or G711 coded.
- **Network interface**: They are connected on the Control Node (CN) and are considered as infrastructure links. They support CN to CN service with voice coded and encrypted.

2.5.1.2. TETRAPOL Terminal based interfaces

2.5.1.2.1. TETRAPOL Stand-alone dispatch position (SADP) interface

This interface provides voice and signalling interfaces from a TETRAPOL CN to a dispatch position.

Services:

- All voice services
- Status
- SMS services
- Network state information
- End to end encryption is supported from TETRAPOL users up to the gateway.

Interface:

- The component, so named access gate (AG), is embedded in the dispatch position.
- The signalling interface uses a V24 link that carries control signalling, status and system state signalling.
- The AG converts coded and ciphered voice into analog clear.
- The voice interface contains one analog with 4-wire voice line + 2-wire signalling for PTT management.
- The SADP contains a single AG that supports a single communication.

Availability:

- Existing equipment.

2.5.1.2.2. TETRAPOL Control room gateway

This gateway provides voice and signalling interfaces from a TETRAPOL CN (Control Node) to a control room.

Services:

- All voice services
- Status
- SMS services
- Network state information
- End to end encryption is supported from TETRAPOL terminals up to the gateway.

Interface:

- Components, so named access gates (AG), are wire-connected and embedded in the CN, or connected by TETRAPOL radio.
- The AG converts voice coding into G711 or analog and translates ciphered flows in clear.
- The CORBA-based signalling interface uses a TCP/IP link common to all access gates. It supports call control signalling, status and system state signalling.
- The voice interface presents one link for each AG that can be analog or digital :
  - Analog : uses 4-wires voice line + 2-wires signalling for PTT management
  - Digital: uses an ISDN BRI with a single permanent voice channel in B-channel and PTT management in QSIG FACILITY messages.
- An AG supports a single communication. A digital control room interface is generally made of several AG. The number of BRI at DC side shall be equal to the number of AG (only one B-channel is used).

Availability:

- Existing equipment.

2.5.1.2.3. TETRAPOL PBX gateway

This gateway connects a TETRAPOL RSW to a PBX via an ISDN BRI line with QSIG signalling.

Services:

- Individual call
- End to end encryption is supported from TETRAPOL terminals up to the gateway.

Interface:

- Components, so named access gates (AG), are embedded in the CN. Using several access gates provides the possibility to manage several simultaneous calls.
- The AG converts voice coding into G711 and translates ciphered flows in clear.
- Each AG presents a single ISDN BRI interface using standard QSIG-BC signalling. This interface does not manage end-to-end PTT. Half duplex is managed by the AG using VAD.

- An AG supports a single communication. A PBX interface is generally made of several AG's. The number of BRI at PBX side shall be equal to the number of AG (only one B-channel is used).

Availability:

- Existing equipment

2.5.1.2.4. TETRAPOL Gateway to external radio network

This gateway provides an interface between TETRAPOL and another network via the air interface.

Services:

- Group communication.
- End to end encryption is supported from TETRAPOL users up to the gateway. The same for the other network.

Interface:

- The gateway is made of a TETRAPOL device that behaves like a radio terminal and of a similar device of the opposite network. In particular, they have to register in their respective network.
- The TETRAPOL side converts TETRAPOL coded and ciphered flows into analog and clear. The same is done at other network side.
- They are connected by a line that transmits voice and PTT signalling at the other side without any processing.
- A gateway supports a single communication.

Availability:

- Existing equipment.

2.5.1.5. TETRAPOL DMO gateway

This gateway ensures the continuity between a TETRAPOL group communication and a group of TETRAPOL terminals in direct mode.

Services:

- Group communication.
- Network end-to-end encryption is supported from TETRAPOL users up to the gateway. Direct mode encryption is supported from users in direct mode up to the gateway.

Interface:

- The conception of the DMO gateway is close from above external radio network gateway. Users can select the TETRAPOL group communication and the direct mode channel they want to connect together. This is done by gateway MMI.

- A gateway supports a single communication.

Availability:

- Existing equipment.

2.5.1.16. TETRAPOL Network interfaces

- TETRAPOL Inter RN link

Inter-RN links connect TETRAPOL CN and provide complete interoperability of terminals of the RN relative to the connected CN.

Services:

- All voice and data end to end services
- Supplementary services
- Mobility
- Continuity of TETRAPOL interfaces.

Interface:

- TCP/IP link with proprietary signalling and RTP for voice packets.
- On this interface, voice is coded and ciphered.

Availability:

- This is not a standard TETRAPOL interface (proprietary).

- TETRAPOL Inter-System Interface (ISI)

No ISI product exists at this time.

Availability:

- Not implemented.

2.6. Inter system gateway

This possibility considers that legacy system is Tetrapol, and new system (required to interoperate with Tetrapol) is SIP/RTP based.
Same services as Tetrapol can be supported by BB server for Broadband Radio Users.

This solution consider to isolate completely both systems and interoperate (for narrowband services supported by Tetrapol) through Inter-RN interface at Tetrapol side, and through interoperabilityt inter system interface at IP side.
It requires a tough GW in order to transcript Tetrapol Inter-RN to IP protocol, and vice versa.

This solution is expensive and there is no real reuse possibility:

- Gateway is new and requires new and specific complex design. Main constraint of this solution is to transcode two protocols having very few in common. Typically, complexity comes from the coverage control (dynamic under Tetrapol), and from the Key protocols completely different. In Tetrapol, the key to be used between Terminals is elected and sent during Group call management, on the flow, by AU. This last point requires protocols to be transcoded from Tetrapol to IP at Gateway level, even if keys are the same.
- At legacy side, there is no possibility to evolve to any defined standard protocol under IP(which is necessary, but available only at IP side)
- Note that Broadband side can be any Broadband based technology. (1 Gateway may be used per techno)
- Media can be :
    - deciphering Tetrapol format and enciphering Broadband format (AES or any ciphering mode). This increases complexity of security and key management at Gateway.
    - Not deciphering inside GW, if AU Tetrapol Protocol of on the flow election of key is used under standard broadband protocol at Broadband terminals side… which is not to happen due to enhanced complexity.

So, this solution is not chosen due to:

- Complexity of the solution is too expensive and too complex to consider.
- No advantage – except capacity in number of Group Calls, if needed
- No reuse or synergy with any other technologies (1 GW required per couple of techno)
- This proposes a mitigated answer to obsolescence of HW/SW, as no modification of CN Tetrapol, and very poor possibility to evolve to Multimedia support.
- It pushes also to an even more proprietary specific solution.

Nevertheless, one of the (the only?) advantage of this solution is to be independent at legacy side of any standard protocol definition at Broadband side. But this require 1 (HW and SW) solution different for each system we want to interoperate with…We will see with other solutions that this advantage can also be handled in a more efficient manner.

3. GENERAL INTERFACE DESIGN

3.1. General design of the interface

As there is no ISI interface available between TETRAPOL networks, they must be interconnected through a gateway connected to the two networks via the TETRAPOL Control Room Interface made up of Access Gates for voice and CC-API server and client for signalling.

Two configurations can be setup. Either the two core networks are co-located or are on different sites.

The easiest way from a gateway point of view is to have only one gateway connected to the two networks. However, it is more probable that TETRAPOL switches of two different networks will not be located in the same place. In such a case an interface between the gateways must be defined. In the following document and synoptic, this interface is named INI.

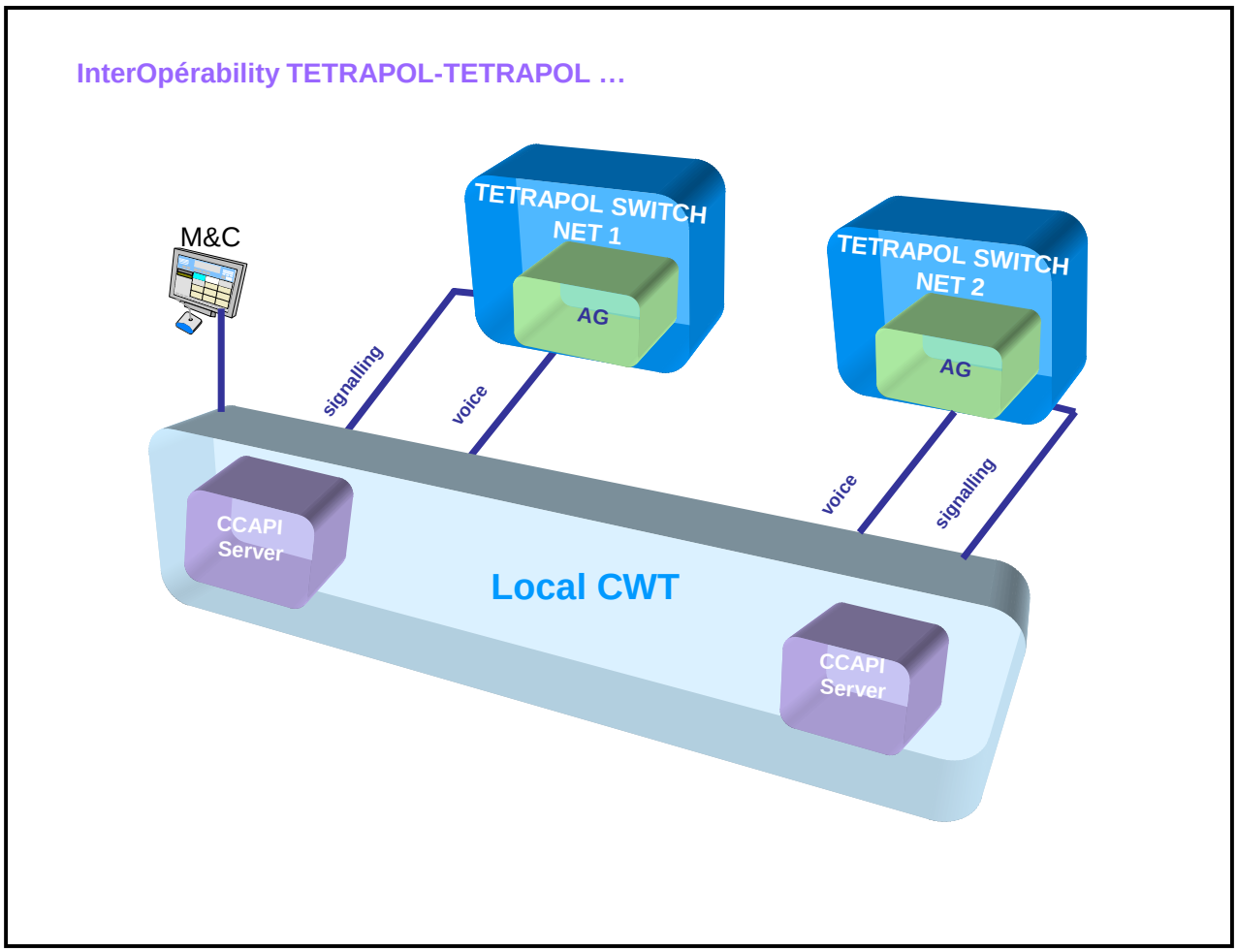


Figure 7 : TETRAPOL/TETRAPOL interoperability ; one local gateway

InterOperability TETRAPOL-TETRAPOL …

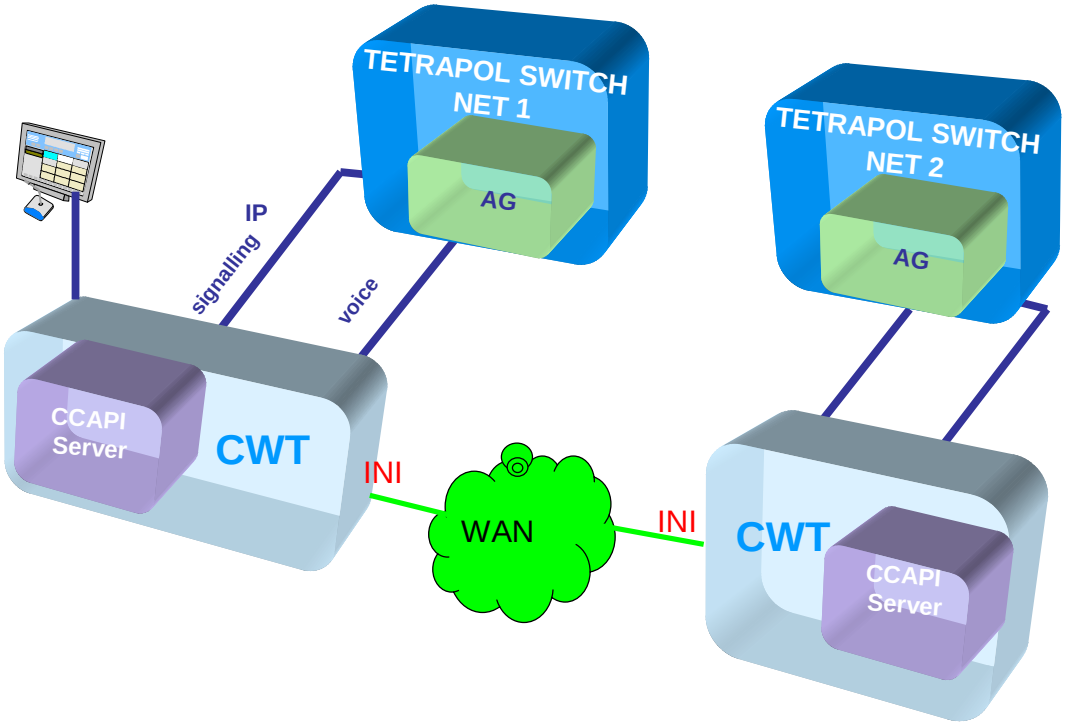
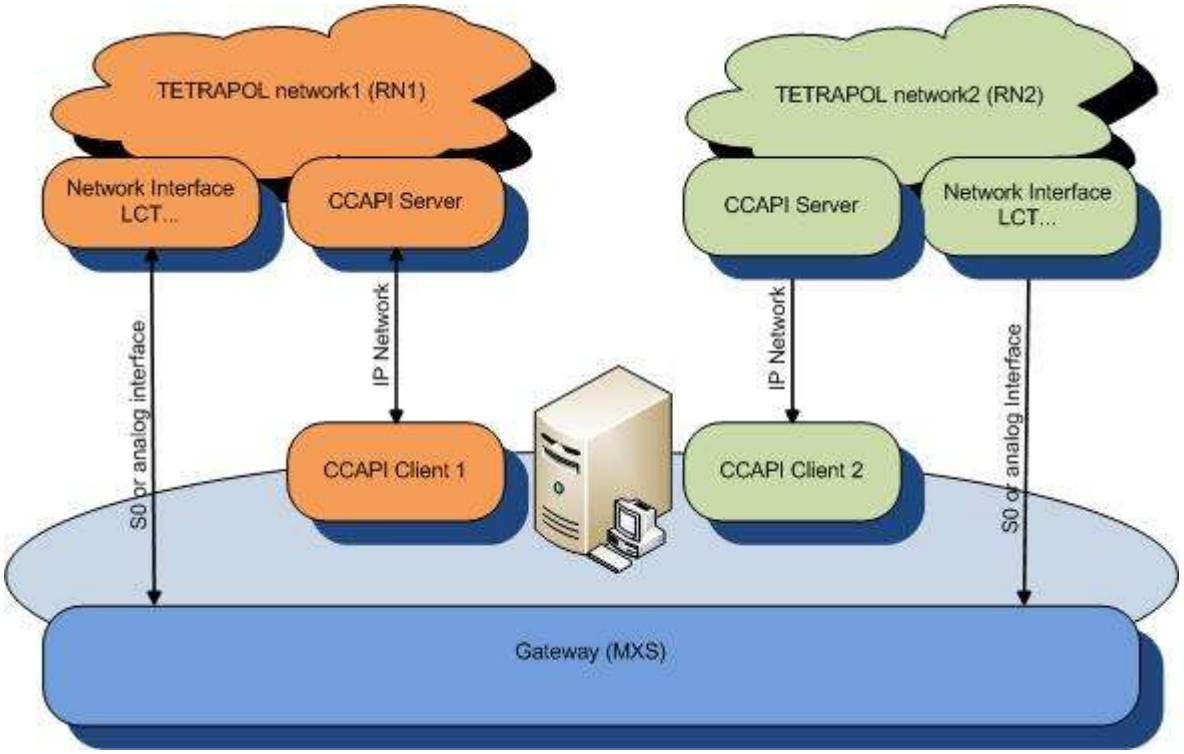


Figure 8 : TETRAPOL/TETRAPOL interoperability using 2 half gateways and interconnected through WAN

The same features are available whatever the location of the TETRAPOL networks.

One can see there are in fact two interfaces between the gateway and each network. The media or the user plane is conveyed through an analog interface. The signaling is conveyed through an IP network on the control room interface. In the case TETRAPOL interconnection is assumed by one single gateway :



Targeted features :

- Group call (TalkGroup, merging/conference),
  - Group call enables the users that have selected the same talk group in their mobile radios to communicate with each other on a half-duplex basis.
- Private call
  - Individual call is a one-to-one call between two mobile radios.
- Emergency Call
  - Emergency call automatically alerts the affiliated control room dispatcher and other terminal users whom belong to the same Talkgroup.
- Status
  - Status messages allow defining preconfigured status messages that are identified by unique number. The system interprets messages numbers to messages. There could be different associations for message numbers in different networks. In this project, we will consider that Status are managed by the CC-API (which is not always the case in TETRAPOL networks).
- SMS
  - SMS is a free text of 140 byte per message maxi. In this project, we will consider that SMS are managed by the CC-API (which is not always the case in TETRAPOL networks).

Not available Features:

- Emergency group call : ESOCH (Emergency Single Open Channel) TETRAPOL
- Notification of an emergency private call
- Notification of an emergency group call (CRISIS or ESOCH)

The gateway will be able to achieve the correct matching between the communications through a radio channel manager (GVR).

Example of matching table needed between the two TETRAPOL networks :

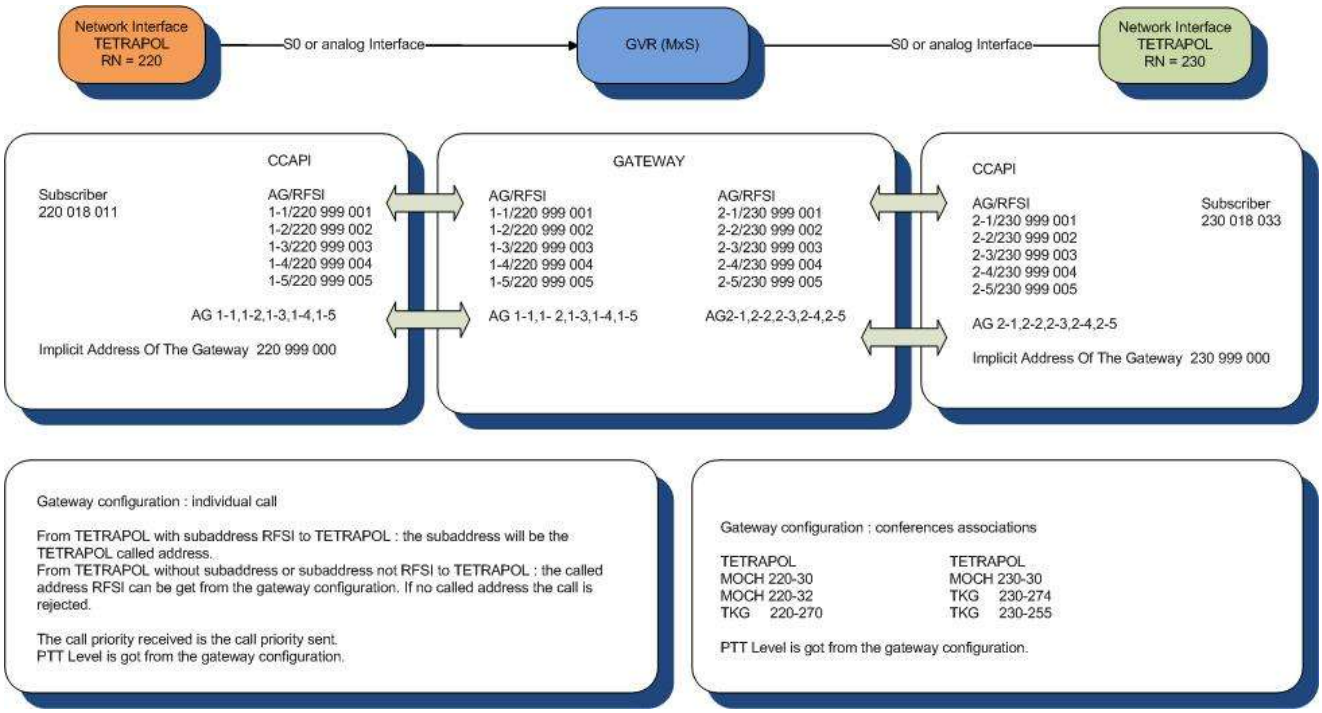
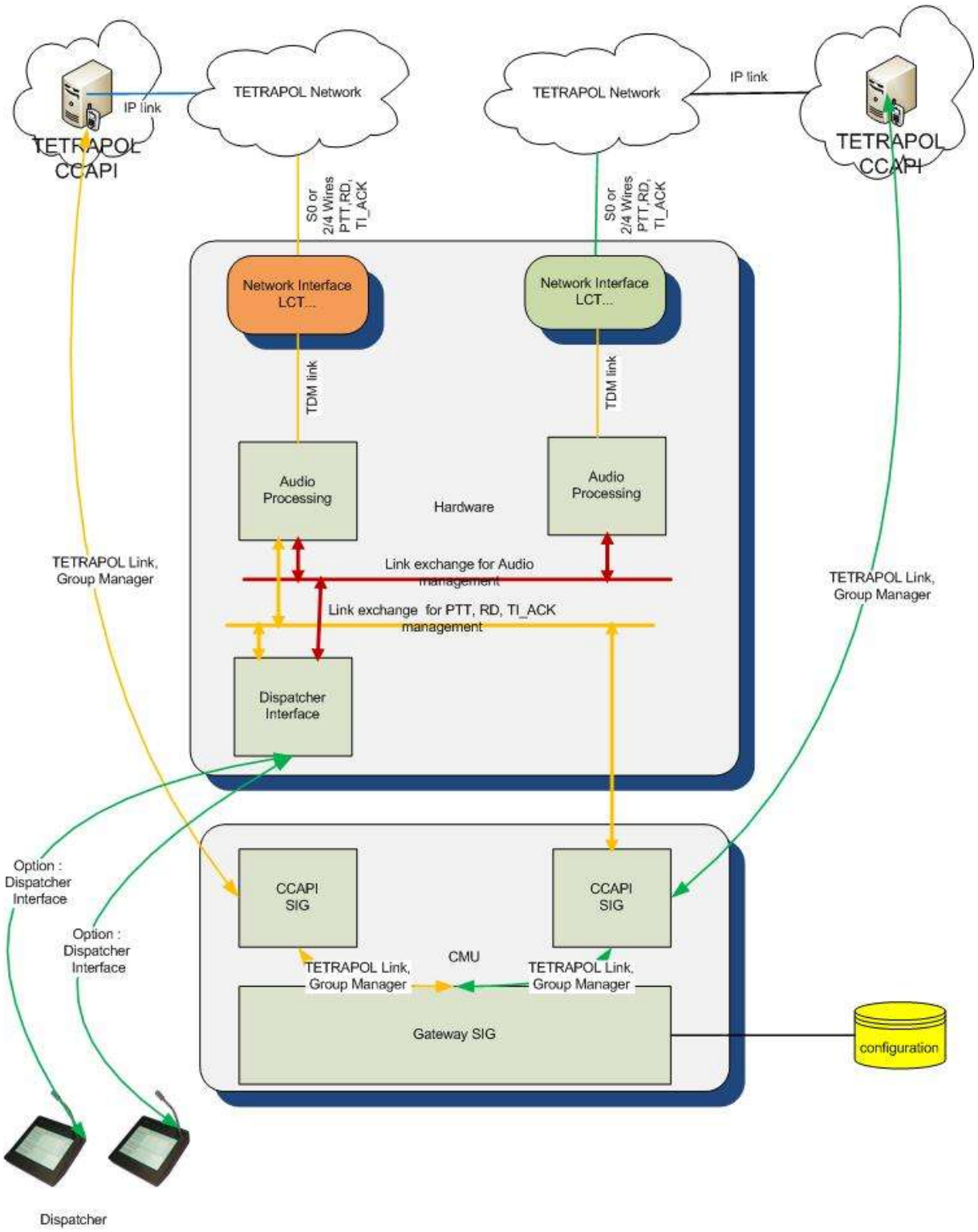


Figure 9 : matching table needed between the two TETRAPOL networks

3.2. GATEWAY architecture

3.2.1. Gateway description



3.2.2. System description

The system consists of:

- A central management unit (CMU); this function could be duplicated,

- It contains treatments (processing):
    - The system configuration,
    - The interface MMI of configuration,
    - The supervision inter CMU,
    - The application to manage the CCAPI,
- The network interfaces TETRAPOL (hardware),

The gateway consists of a rack for network LCT connections, to which could be associated two CMU (Central management units) allowing to configure and to accommodate the customer API (integrated into the function DCS).

3.2.3. Hardware gateway

The Gateway essentially consists of:
- A set of electronic boards placed in a system rack 19 ', assuring the management of the audio treatments,
- A system consists of R racks (R min =1) of this type,
- Every rack includes:
    - a card of management of internal communication, card CTL (controller),
    - from 1 to N cards for AUDIO management,
    - the possible network connections are:
        - IP: for the operators, and optionally network access,
        - Analog + PTT / TI_ACK / RD,
        - Digital technology S0 (1 channel B and signaling PTT / TI_ACK / RD),

3.2.4. Gateway CC API

The CCAPI treats the functions of call processing.
The audio connections are connected on analog links (600 Ohms 0 dBm, with 3 control signals PTT, TI_ACK, RD) or S0 links (coding 711, law A with 3 control signals PTT, TI_ACK, RD).

At the level of the resources Group Call system or private call:
- One board manages the AUDIO matrix for N accesses,
- The board manages the Audio communication of / towards TETRAPOL network and optionally dispatchers.

3.2.5. Detail of signalling exchange

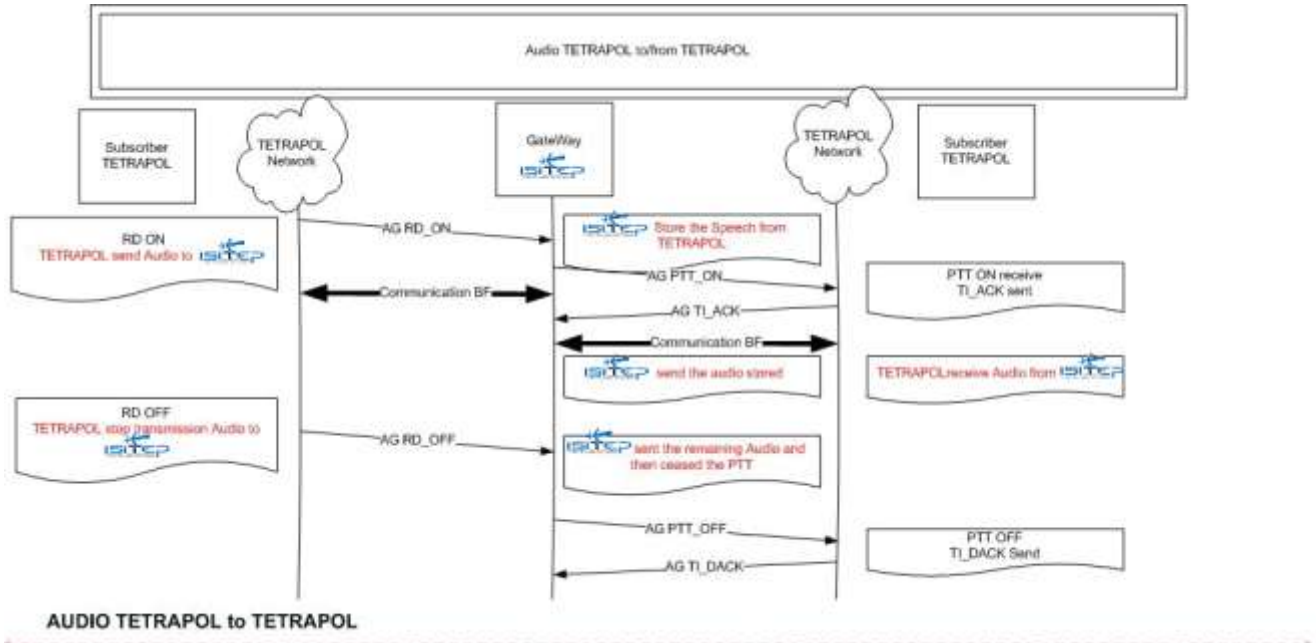


Figure 10 : Example 1: Audio exchange

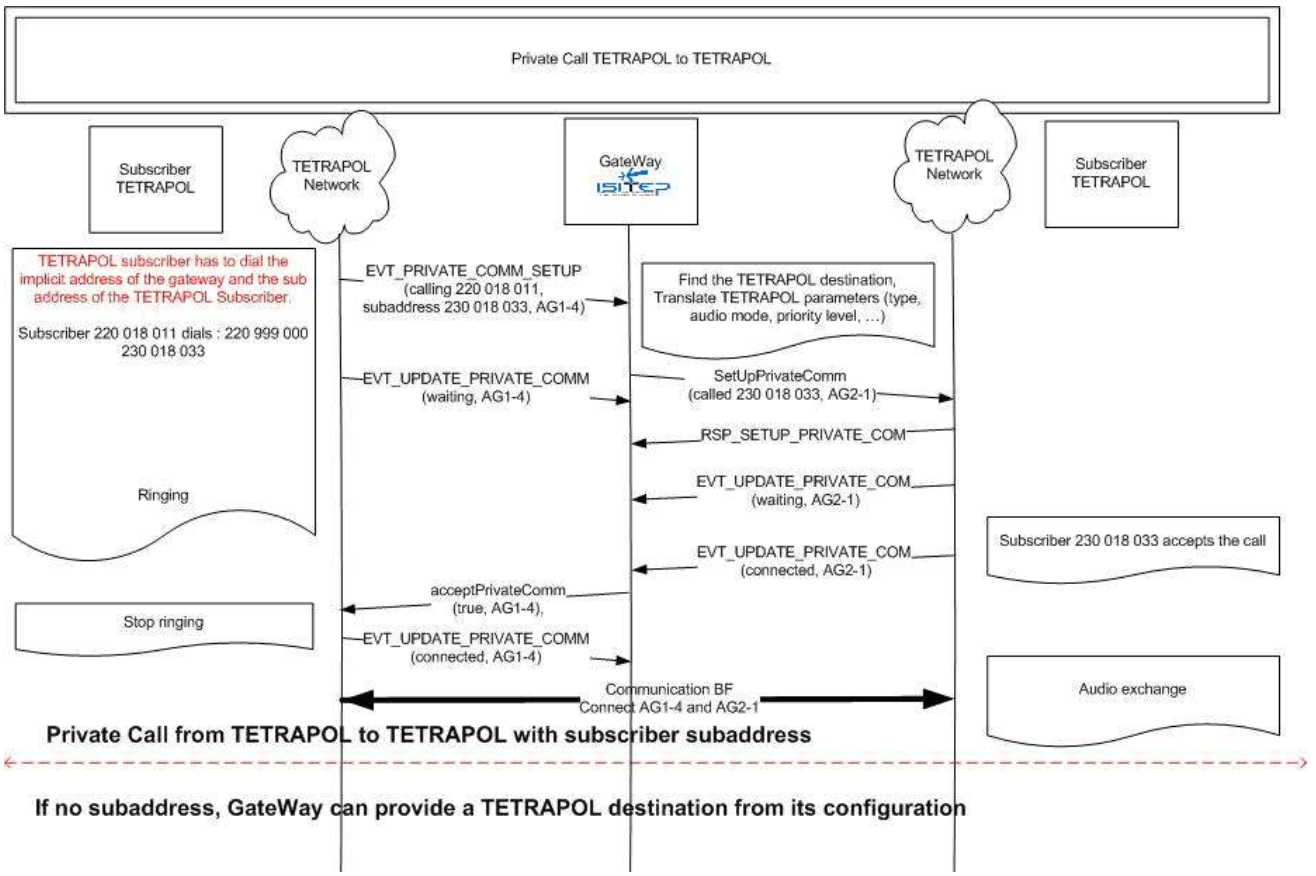


Figure 11 : Private call exchange

3.3. Single gateway implementation

3.3.1. Hardware implementation

The single gateway makes possible 2 TETRAPOL interconnections. This gateway is made up of:

- An Embedded computer which manages the signalling between the networks,
- A rack to host the gateway interfaces:
  - Analog 8 wire access for the first TETRAPOL network,
  - Analog 8 wire access for the other TETRAPOL network,

An Ethernet switch to manage the IP connectivity for configuration and signalling.

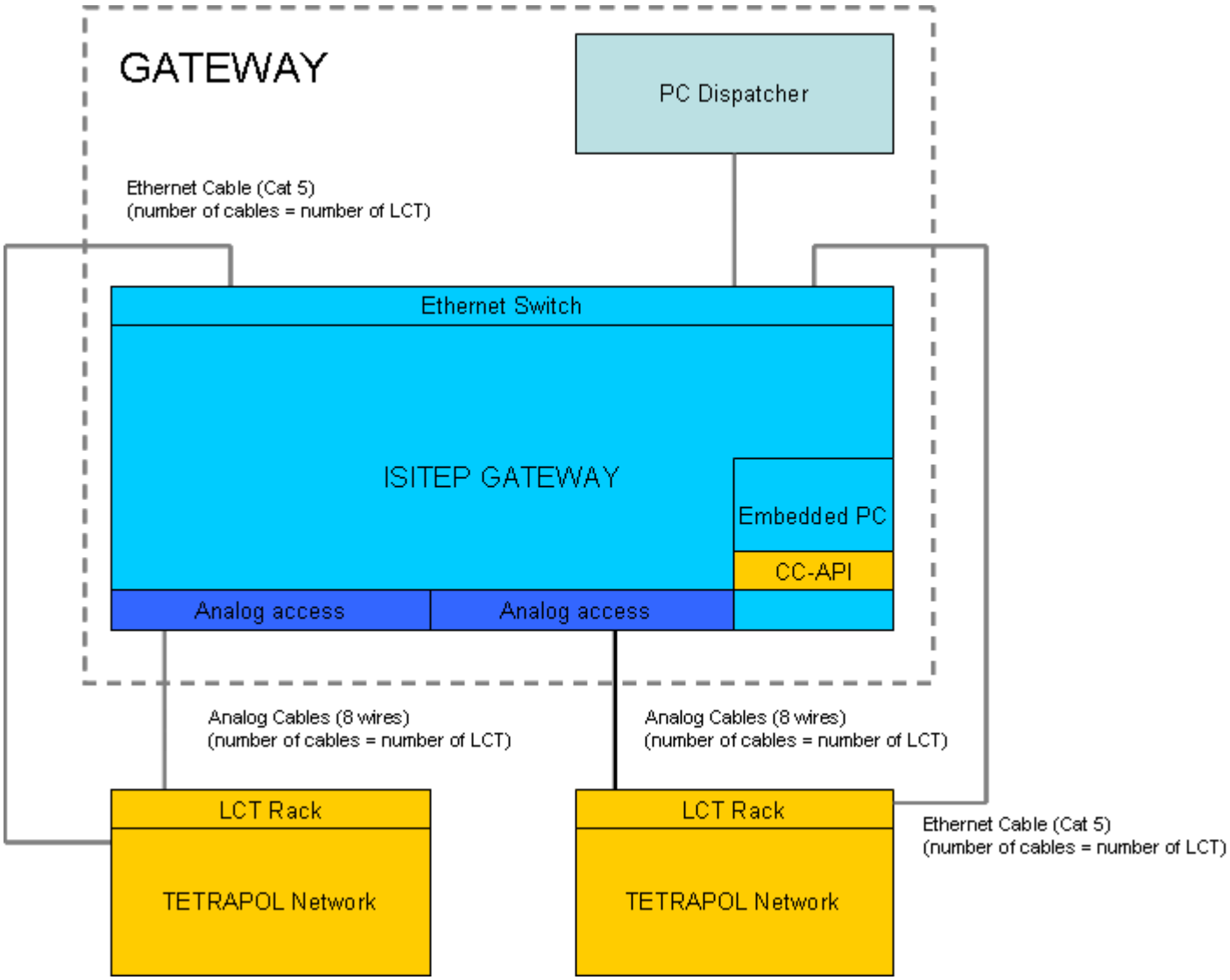
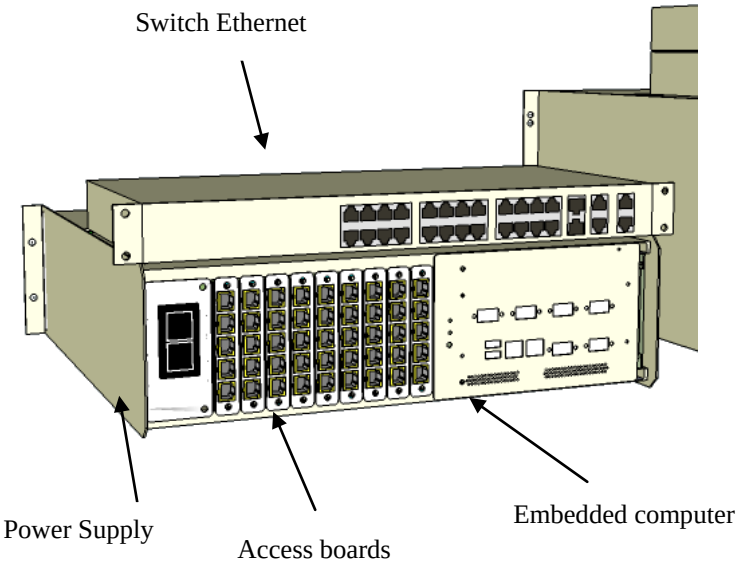


Figure 12 : TETRAPOL TETRAPOL single gateway

The physical implementation of the gateway should look like the next figure :



3.3.2. Software implementation

The Central Management Unit (CMU) will be hosted on the embedded computer and is one of the key organs of the Gateway and performs many essential operations:

Supervision of the Gateway access and modules,
Signalling interface with digital networks (TETRAPOL networks…),
Administration, equipment configuration and setup (network access, operator access, profiles, resource partitioning, priority levels, operation plans ...)
Interface for remote maintenance,
Event Log (events, alarms, communications…).

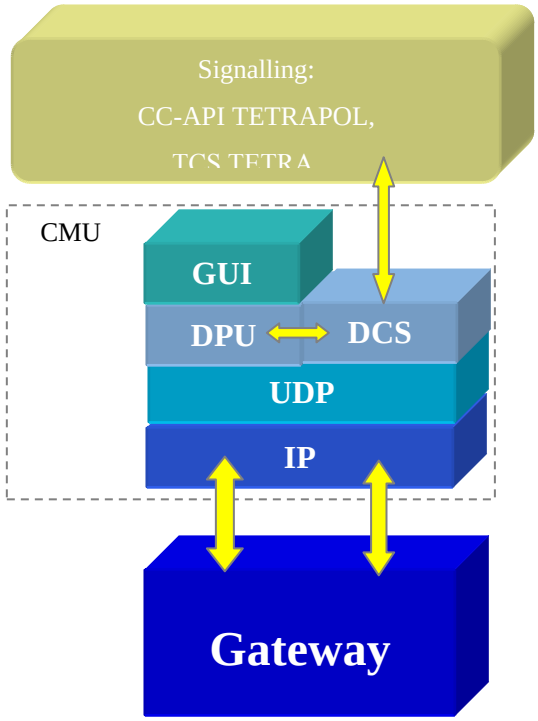
The Gateway Setup function and the processing of Gateway data are provided by the Data Processing Unit (DTU). The DPU deals:

- The access status,
- Conferences, Group calls, connections,
- Backup and recovery of configuration data stored on the CMU.

The real time call processing function is ensured by the Dispatch Control Server (DCS). The DCS has an essential role in the exchange of signalling with digital radio networks connected on the Gateway (example: data exchange with the TETRAPOL CC-API). The DCS is also used when multiple Gateway are interconnected.

Finally, the display function is provided by the Graphical Interface Unit (GIU). This GIU is a client process that can be installed on multiple machines, allowing multiple users to work simultaneously. In practice, a GIU may be present on each operator's computer.

Software layers for the signalling.



Real time media are directly managed by access board that will handle coding, transcoding, mixing, and interface adaptation through DSP associated with Access boards.

3.4. Dual gateway implementation

For this project another implementation has been proposed in order to take into account operational constraints. In fact, every national public safety radio network has their own procedure to authorize connection and interconnection on their network to ensure and maintain a high degree of security and confidentiality. Every administration wants to manage by themselves the authorization to allow the interoperability with another network on their network. It means that each operator can manage the settings on its own network.

For this reason, we can propose a dual gateway implementation defining an INI (Inter-Network-Interface) between the interoperability gateways.

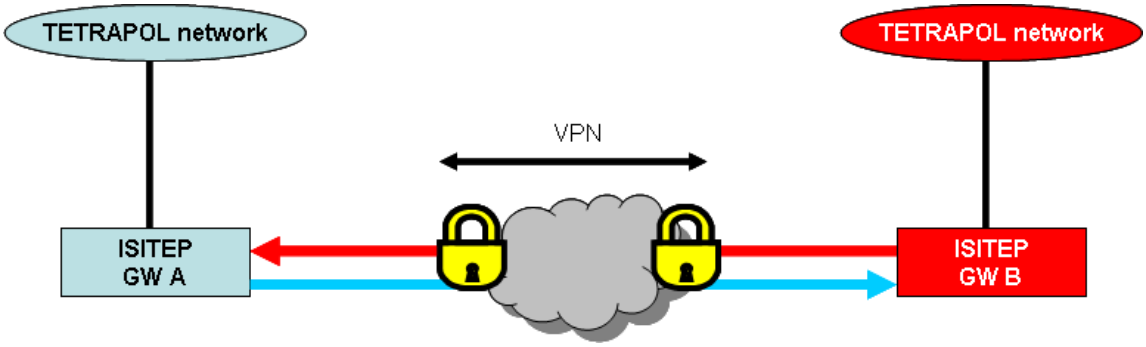


Figure 13 : Dual gateway implementation

The physical implementation of the dual gateway is similar to the single one except that each gateway will connect only one type of network and will have a secured IP connection with the other gateway.

The media flow can be encrypted between the two sites and above, an encrypted VPN can be set between the two remote sites.

Each gateway manages the configuration of its network (TETRAPOL). It means that each operator can authorize or not the access of the user of the other network.

For the TETRAPOL network, the gateway is made up of:

An Embedded computer which manages the signalling between the networks,
A rack to host the gateway interfaces:
Analog 8 wires access for TETRAPOL,
IP access for the interconnection with the remote gateway,
An Ethernet switch to manage the IP connectivity for configuration and signalling.

To facilitate the operations, it is possible to have an application that will display the available talkgroup where an interconnection is possible. This type of interface is much more suitable for operational rather than technical people. In fact, the solution should be put in place easily once installed and not require a technical staff anytime an interconnection is necessary.

3.4.1. TETRAPOL-TETRAPOL platform

The TETRA and TETRAPOL networks must be interconnected through 2 gateways.

The gateways are connected through an IP network:

- Signaling through SGP Signaling XML interface,
- Voice through an UDP/IP interface for audio an RFC 2833 for audio control (PTT ...).
- This interface is based on R33 NF 399 specification.

Each gateway is connected to its network thru a Control Room Interface composed of

- TETRAPOL :
  - Analogue Access Gates (4w+Ti-Ack+RD+PTT loops),
  - Or S0 interfaces (voice+Signaling Ti-Ack+RD+PTT) for voice,
  - CC-API interface for signaling.

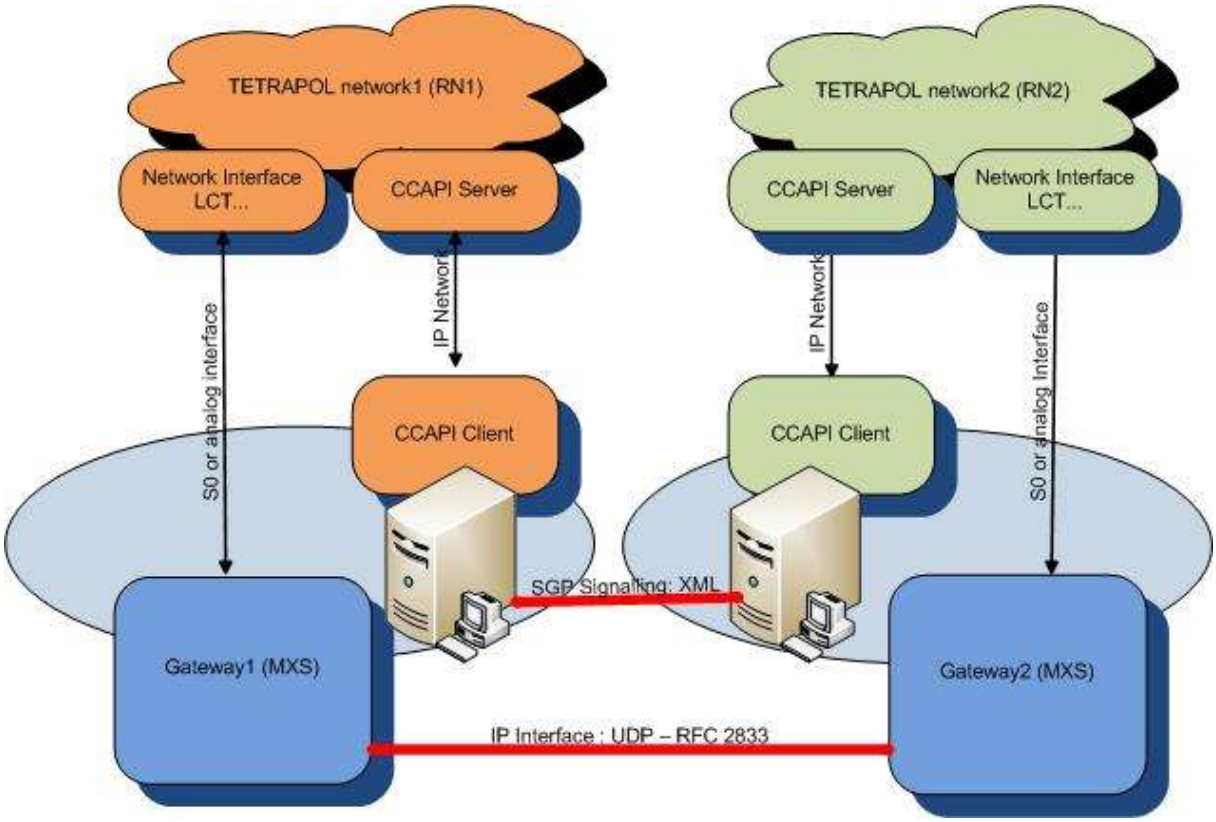


Figure 14 : TETRAPOL TETRAPOL half gateways

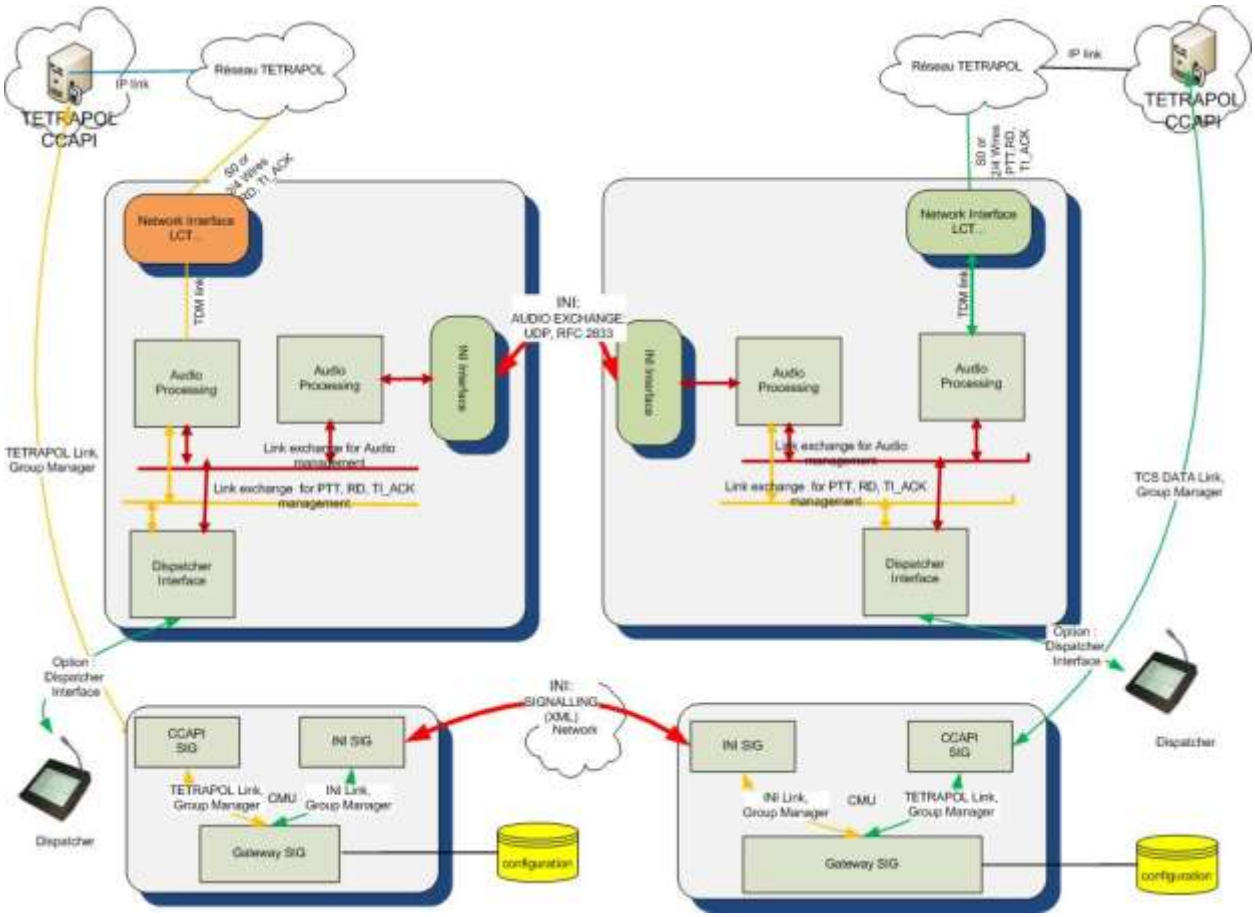
Targeted Features:

- Group call (TalkGroup, merging/conference): group call enable the users that have selected the same group call in their mobile radios to communicate with each other on a half-duplex basis.
- Emergency group call : CRISIS
- Private call: private call is a one-to-one call between two mobile radios.
- Status: status messages allow defining preconfigured status messages that are identified by unique number. The system interprets messages numbers to messages. There could be different associations for message numbers in different networks. In this project, we will consider that Status are managed by the CC-API (which is not always the case in TETRAPOL networks).
- SMS: SMS is a free text of 140 byte per message maxi. In this project, we will consider that SMS are managed by the CC-API (which is not always the case in TETRAPOL networks).

Not available Features:

- Emergency group call : ESOCH (Emergency Single Open Channel) TETRAPOL
- Notification of an emergency private call
- Notification of an emergency group call (CRISIS or ESOCH)

3.4.2. TETRAPOL-TETRAPOL description



3.4.3. GATEWAY Architecture

The 2 platforms are connected through an IP link of interconnection between TETRAPOL and TETRAPOL,
Each platform is independent, it treats its own calls and talkgroups,
Networks are independent in term of infrastructure,
A process of interconnection between 2 systems is based on the normalization GT 399 of reference R33,
The resources of called interconnections inter SGP (Management system of Telephony: Système de Gestion de Phonie) are decomposed there:

- A connection of commands and indications (signaling) between CMU, for the exchanges of commands(orders),
- Physical interfaces IP for the transport of the audio: UDP associated with synchronous commands of PTT, and RD at the beginning and the end of audio communication.
  These interfaces are used for the interconnections TETRAPOL-TETRAPOL.

4. INTER RADIO NETWORK INTERFACE

4.1. Call processing

- TCP/UDP protocol
- Each Gateway may be client and server at the same time :
  - server for the remote gateway
  - client of the remote gateway
- XML exchange messages.

4.2. Audio signalling

- UDP standard protocol
- rfc2833.

4.3. Numbering

- The numbering contains two types of information in ASCII :
  - Numbering type
  - Number

4.4. TETRAPOL : private call

It is the number of a TETRAPOL network access (mobile, Access Gate).
Dialling is closed at 9 digits defined in the following way: RFGI
R: 3 digits for the base network
F: 1 digit for the fleet
G: 2 digits for the group
I: 3 digits for the subscriber

The private call has a priority: ROUTINE, FLASH or EMERGENCY.

In the inter INI interface is used:

- The numbering type "rfgi"
- - And the 9-digit numbering from 0 to 9

The TETRAPOL interface messages are those of the private call: in CCAPI, this corresponds to «Manager Private Communication ". In private call, we talk about call establishment and call release.

4.5. TETRAPOL : conference

The conference is indicated in an RN.
There are 3 types of conferences:

- TKG: conference of a group of subscribers. It is identified with its group number (OG).
- OCH: conference of several groups of subscribers. It is identified by its number. According to its priority, OCH is called Moch (FLASH and ROUTINE priorities); BOCH (BROADCAST priority) or EMOCH (CRISIS priority)
- ESOCH: distress conference. It is identified by the Radio Switch (RSW) and the cell (CELL) where the distress has been initiated. (network option)

The numbering of a TKG conference is: R + OG.
The numbering of an OCH conference is: R + OCH.
The numbering of an ESOCH conference: R + RSW + CELL.

In the INI interface:

- R is defined with 1 to 3 digits
- OG can take values from 0 to 1499
- OCH can take values from 0 to 255
- RSW can take values from 0 to 255
- CELL can take values from 0 to 255.

The messages of the TETRAPOL interface are those of the group communication: in CCAPI, this corresponds to the «Manager Group Communication". In conference, we talk about opening, closing, taking part and removal.

5. TETRAPOL FEATURES

5.1. Transmission to remote Gateway

5.1.1. Outgoing simple private call

It is possible to launch an outgoing simple TETRAPOL private call with or without sub-address. The destination address is of RFGI-type. The sub-address is limited to 15 digits. The priority may be ROUTINE, EMERGENCY or FLASH.

Example:

```
<CC_CALL_PRIVATE>
        <reference>123</reference>
        <priority>FLASH</priority>
        <rfgi>220123456</rfgi>
        <sub-address>1234</sub-address>
        <channel>101</channel>
</CC_CALL_PRIVATE >
```

5.1.2. Outgoing multiple private call

It is possible to launch an outgoing multiple TETRAPOL private call. Destination addresses are of RFGI-type. The number of addresses is limited to 4. The priority may be ROUTINE or FLASH.

Example:

```
<CC_CALL_MULTIPLE>
        <reference>123</reference>
        <rfgi>220123456</rfgi>
        <rfgi>220123789</rfgi>
        <rfgi>220123012</rfgi>
        <channel>101</channel>
</CC_CALL_MULTIPLE >
```

5.1.3. Transfer of incoming TETRAPOL private calls

It is possible to transfer an incoming TETRAPOL private call to another number.

Example:

```
<CC_CALL_TRANSFER>
        <reference>123</reference>
        <rfgi>220123456</rfgi>
        <sub-address>1234</sub-address>
```

</CC_CALL_TRANSFER>

5.1.4. Request to open a MOCH conference

It is possible to request the opening of a MOCH conference with ROUTINE or FLASH priority. The conference number is of MOCH type. The number is of MOCH or FOCH type.

Example:

```
<CC_OPEN>
        <reference>123</reference>
        <channel>101</channel>
        <moch rn=”220” num=”31” />
</CC_OPEN>
```

5.1.5. Request to close a MOCH conference

It is possible to request the closing of a MOCH conference. The conference number is of MOCH, FOCH BOCH or EMOCH type.

Example:

```
<CC_CLOSE>
        <reference>123</reference>
        <channel>101</channel>
        <moch rn=”220” num=”31” />
</CC_CLOSE>
```

5.1.6. Taking part to a MOCH conference

It is possible to request to take part to a MOCH conference. The conference number is of MOCH, FOCH BOCH or EMOCH type.

Example: taking part to an MOCH conference in normal mode without superencryption

```
<CC_SELECT>
        <reference>123</reference>
        <moch rn=”220” moch=”31” />
        <channel>101</channel>
</CC_ SELECT >
```

Example: taking part to an MOCH conference in degraded mode without superencryption

```
<CC_ SELECT >
        <reference>123</reference>
        <moch rn=”220” moch=”31” mode=”FB2” />
        <channel>101</channel>
</CC_ SELECT >
```

5.1.7. Removal from a MOCH conference

It is possible to request the removal from a TKG conference.

Example:
<CC_RELEASE>
<reference>12</reference>
</CC_ RELEASE >

5.1.8. Taking part to a TKG conference

It is possible to request to take part to a TKG conference. The conference number is of TKG type.

Example:
<CC_ SELECT >
<reference>123</reference>
<tkg rn=”220” og=”270” />
<channel>101</channel>
</CC_ SELECT >

5.1.9. Removal from a TKG conference

It is possible to request the removal from a TKG conference.

Example:
<CC_ RELEASE >
<reference>12</reference>
</CC_ RELEASE >

5.1.10. MOCH or TKG conference scanning

It is not possible to request MOCH or TKG conference scanning in a remote Gateway.

5.1.11. Request to close an ESOCH conference

It is possible to request the closing of an ESOCH conference. The conference number is of ESOCH type.

Example:
<CC_CLOSE>

```
        <reference>123</reference>
        <esoch rn=”220” rsw=”1” cell=”4” />
</CC_CLOSE>
```

5.1.12. Taking part to an ESOCH conference

It is possible to request to take part to an ESOCH conference. The conference number is of ESOCH type.

Example: taking part to an ESOCH conference in normal mode

```
<CC_SELECT>
        <reference>123</reference>
        <esoch rn=”220” rsw=”3” cell=”1” />
        <channel>11</channel>
</CC_ SELECT >
```

Example: taking part to an ESOCH conference in degraded mode

```
<CC_ SELECT >
        <reference>123</reference>
        <esoch rn=”220” rsw=”3” cell=”1”  mode=”FB2” />
        <channel>11</channel>
</CC_ SELECT >
```

5.1.13. Removal from an ESOCH conference

It is possible to request the removal from an ESOCH conference.

Example:

```
<CC_ RELEASE >
        <reference>12</reference>
</CC_ RELEASE >
```

5.1.14. Group Call – PTT priority

It is possible to indicate that the call is part or is no longer part of a group call. This message allows to change the PTT priority on the AG of the remote Gateway.

Example: beginning of a group call

```
<CC_PTT_LEVEL>
        <reference>12</reference>
        <level>1</level >
</CC_PTT_LEVEL>
```

5.1.15. Transmission of a SMS received from TETRAPOL

It is not possible to transmit an SMS.

5.2. Transmission from the remote Gateway

5.2.1. Incoming private call

It is possible to receive a TETRAPOL incoming private call

Example:

```
<CC_CALL_PRIVATE>
        <reference>123</reference>
        <priority>FLASH</priority>
        <sub-address>1234</sub-address>
        <from>220123456</from>
        <channel>101</channel>
</CC_CALL_PRIVATE >
```

5.2.2. Indication of conference opening/closing on an inter SGP access

It is possible to receive the indications of TETRAPOL conference opening / closing on an inter SGP access.

Example:

```
<CA_CONF>
        <reference>10103</reference>
        <state>OPENED</state>
        <moch rn=”220” num=”30” />
</CA_CONF>
<CA_CONF>
        <reference>10103</reference>
        <state>OPENED</state>
        <moch rn=”220” num=”12” />
</CA_CONF>
<CA_CONF>
        <reference>10103</reference>
        <state>OPENED</state>
        <moch rn=”220” num=”12” mode=”FB2” />
</CA_CONF>
<CA_CONF>
        <reference>10103</reference>
        <state>OPENED</state>
        <esoch rn=”220” rsw=”1” cell=”4” />
```

</CA_CONF>

5.2.3. Indication of notification of a crisis or distress

It is possible to receive the initiator's ID of a crisis or distress. The number is of "RFGI type."

Example:
<CA_NOTIF>
<emoch rn=”220” num=”120” />
<rfgi>220123987</rfgi>
</CA_NOTIF>

5.2.4. Receiving a SMS

It is not possible to transmit an SMS between Gateways

5.2.5. Speaker's ID reception

It is possible to receive the speaker's ID.

Example:
<CC_TALKING_PARTY>
<reference>123</reference>
<rfgi>220123456</rfgi>
</CC_TALKING_PARTY>