Saku Oja

Lower layer protocols in TETRA Inter-System Interface

Thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Engineering.

Espoo, August 21, 2000

Supervisor
Professor Arto Karila

Instructor
MSc Olli Mikkola, Nokia Networks
**HELSINKI UNIVERSITY OF TECHNOLOGY**

**ABSTRACT OF THE MASTER'S THESIS**

<table>
<thead>
<tr>
<th>Author: Saku Oja</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the thesis: Lower layer protocols in TETRA Inter-System Interface</td>
</tr>
<tr>
<td>Date: August 21, 2000</td>
</tr>
<tr>
<td>Faculty: Department of Computer Science and Engineering</td>
</tr>
<tr>
<td>Professorship: Tik-110</td>
</tr>
<tr>
<td>Supervisor: Professor Arto Karila</td>
</tr>
<tr>
<td>Instructor: MSc Olli Mikkola, Nokia Networks</td>
</tr>
</tbody>
</table>

TETRA is a new and emerging standard for professional digital mobile networks. This master's thesis deals with the Inter-System Interface (ISI) interconnecting two or more TETRA networks. TETRA and ISI have been standardised by European Telecommunications Standards Institute (ETSI) for enabling vendor interoperability. The current standard defines ISI to be implemented on top of QSIG protocol, which is an ISDN Q.931 like protocol for digital private networks. However, the standardised solution has several drawbacks and alternative choices are needed also for keeping up with the current evolution of telecommunications networks.

This master's thesis proposes an IP based solution to TETRA ISI, however relying on existing ETSI standards. The analogy to current standards has been maintained for facilitating possible implementation and standardisation work related to IP based TETRA ISI. The adoption of two Voice over IP signalling protocols, H.323 and Session Initiation Protocol (SIP), to ISI is presented in the thesis, and comparison between use of H.323 and SIP and between QSIG and IP based solutions is performed. Furthermore, the functionality of TETRA Packet Data Protocol (PDP) is described and its relation to ISI is presented.

The results of the work show that these two Voice over IP protocols provide the possibility to transfer all required TETRA proprietary signalling over TETRA ISI and to control TETRA speech channels over ISI. However, the IP network in question should be kept private in nature as well as the needed capacity should be carefully designed to prevent Quality of Service (QoS) problems. In addition, security of IP based TETRA ISI is considered in the thesis and the use of IPsec is brought up as an important security measure.

The master's thesis also states that some measures may be required in order to keep the QoS on an acceptable level: this thesis proposes the use of Multiprotocol Label Switching (MPLS) joint with Differentiated Services (DS).

**Keywords:** TETRA, Inter-System Interface, PDP, QSIG, IP, H.323, SIP, Quality of Service, IPsec


Työssä todetaan myös, että joitakin menetelmiä saattaa tarvita palvelun laadun pitämiseksi hyväksyttävällä tasolla. Työssä kerrotaan, miten Multiprotocol Label Switching (MPLS) ja Differentiated Services (DS) soveltuvat näiden ongelmiin ratkaisemiseen.

Avainsanat: TETRA, ISI-rajapinta, PDP, QSIG, IP, H.323, SIP, palvelun laatu, IPsec
# TABLE OF CONTENTS

1. INTRODUCTION ..........................................................................................................1

2. TETRA..........................................................................................................................3
   2.1 TETRA IN GENERAL .................................................................................................3
      2.1.1 What is TETRA? .................................................................................................3
      2.1.2 Special requirements for TETRA networks and terminals.................................3
      2.1.3 TETRA standardisation in ETSI .........................................................................4
      2.1.4 TETRA call types and services ...........................................................................5
      2.1.5 Numbering .........................................................................................................6
      2.1.6 Mobility management (MM) ...............................................................................7
   2.2 NETWORK ARCHITECTURE IN TETRA .................................................................20
      2.2.1 Basic network elements ....................................................................................8
      2.2.2 Digital Exchange for TETRA (DXT) ................................................................9
   2.3 TETRA AIR INTERFACE ..........................................................................................11
      2.3.1 Protocol stack ....................................................................................................11
      2.3.2 Radio path .........................................................................................................12
   2.4 TETRA TERMINAL EQUIPMENT ...........................................................................12
   2.5 TETRA SECURITY ...................................................................................................13
      2.5.1 TETRA user authentication ..............................................................................13
      2.5.2 Air Interface encryption ....................................................................................14
      2.5.3 End-to-end encryption ......................................................................................15
   2.6 TETRA PACKET DATA PROTOCOL ....................................................................15
      2.6.1 The need for Packet Data Protocol ...................................................................15
      2.6.2 PDP protocol stack .........................................................................................16
      2.6.3 Current Nokia PDP implementation ..................................................................17
      2.6.4 Future PDP implementation using GPRS concepts .........................................17
      2.6.5 IP user authentication with PDP ....................................................................19

3. TETRA INTER-SYSTEM INTERFACE .........................................................................20
   3.1 ETSI ISI IN GENERAL ..........................................................................................20
      3.1.1 ISI related concepts and issues in TETRA .........................................................20
      3.1.2 ETSI ISI protocol model ..................................................................................20
      3.1.3 ETSI ISI Additional Network Features ............................................................21
      3.1.4 QSIG protocol with Generic Functional Transport ...........................................22
      3.1.5 Remote Operations Service Element and Segmentation Service Element .......23
      3.1.6 ISI call setup with call related TETRA proprietary information .......................24
      3.1.7 Establishing of a call independent signalling connection ..................................25
   3.2 ADDITIONAL NETWORK FEATURE FOR MOBILITY MANAGEMENT ............25
   3.3 ADDITIONAL NETWORK FEATURE FOR INDIVIDUAL CALL .......................27
   3.4 ADDITIONAL NETWORK FEATURE FOR GROUP CALL ................................27
   3.5 TETRA PACKET DATA PROTOCOL BETWEEN NETWORKS .........................28

4. TETRA ISI OVER IP ....................................................................................................31
   4.1 VOICE OVER IP PROTOCOLS ...............................................................................31
      4.1.1 Shortcomings in underlying IP protocol suite .....................................................31
      4.1.2 Real-time Transport Protocol ...........................................................................32
      4.1.3 Quality of Service in IP networks .....................................................................34
      4.1.4 H.323 protocol suite and network elements ......................................................37
      4.1.5 Session Initiation Protocol (SIP) suite and network elements .............................41
   4.2 IP SECURITY ...........................................................................................................43
      4.2.1 IPsec introduction .............................................................................................43
      4.2.2 Authentication Header (AH) and used algorithms .............................................43
      4.2.3 Encapsulating Security Payload (ESP) and used algorithms ..............................44
      4.2.4 Internet Key Exchange (IKE) ............................................................................45
4.2.5 Additional H.323 security ...................................................... 45
4.2.6 Additional SIP security .......................................................... 45
4.3 TETRA ISI OVER H.323 SIGNALLING ........................................ 46
  4.3.1 Network architecture .............................................................. 46
  4.3.2 Protocol model utilising H.450.1 ................................................. 48
  4.3.3 ISI call setup over H.323 .......................................................... 49
  4.3.4 Establishing of call independent signalling connection over H.323  50
4.4 TETRA ISI OVER SIP ............................................................... 51
  4.4.1 Network architecture .............................................................. 51
  4.4.2 Altered protocol model ............................................................ 52
  4.4.3 SIP messages with TETRA proprietary information .................... 53
  4.4.4 ISI call setup over SIP ............................................................. 53
  4.4.5 Establishing of call independent signalling connection over SIP .... 54
4.5 COMPARISON OF H.323 AND SIP BASED SOLUTIONS ................. 55
  4.5.1 Comparison of these protocols in general .................................. 55
  4.5.2 Suitability of these protocols to TETRA ISI .............................. 57
5. COMPARISON OF QSIG AND IP BASED SOLUTIONS IN ISI .............. 59
  5.1 General comparison ..................................................................... 59
  5.2 Achieving security and QoS with IP based ISI ............................... 60
6. SUMMARY ..................................................................................... 62
  6.1 Conclusions ............................................................................... 62
  6.2 Future Work ............................................................................... 62
7. REFERENCES .................................................................................. 64

APPENDIX A. EXAMPLE OF ENCODING A TETRA ANF-ISIIC INFORMATION
ELEMENT IN A PSS1 SETUP MESSAGE .................................................. 67

APPENDIX B. EXAMPLE OF ENCODING A TETRA ANF-ISIIC INFORMATION
ELEMENT IN A H.323 SETUP MESSAGE ............................................... 68

APPENDIX C. EXAMPLE OF ENCODING A TETRA ANF-ISIIC INFORMATION
ELEMENT IN A SIP INVITE MESSAGE .................................................. 69
FOREWORD

This thesis was made at Professional Mobile Radio business unit in Nokia Networks. I would warmly like to thank the instructor of the thesis, Olli Mikkola, for evaluating the work and also for the helpful comments and support. Furthermore, I would like to thank Olli-Pekka Lahtinen for the useful advice and comments, and all the other people in Nokia who have helped and supported me during the process.

I would also like to thank professor Arto Karila for comments and for evaluating the thesis.

Espoo, August 21, 2000

Saku Oja
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3G</td>
<td>3rd Generation (Mobile Networks)</td>
</tr>
<tr>
<td>AAA</td>
<td>Authentication, Authorisation and Accounting</td>
</tr>
<tr>
<td>ACELP</td>
<td>Algebraic Code-Excited Linear Predictive</td>
</tr>
<tr>
<td>ACU</td>
<td>Authentication Centre Unit</td>
</tr>
<tr>
<td>AF</td>
<td>Assured Forwarding</td>
</tr>
<tr>
<td>AH</td>
<td>Authentication Header</td>
</tr>
<tr>
<td>AI</td>
<td>Air Interface</td>
</tr>
<tr>
<td>ANF</td>
<td>Additional Network Feature</td>
</tr>
<tr>
<td>APDU</td>
<td>Application Protocol Data Unit</td>
</tr>
<tr>
<td>APN</td>
<td>Access Point Name</td>
</tr>
<tr>
<td>ASN.1</td>
<td>Abstract Syntax Notation 1</td>
</tr>
<tr>
<td>ATM</td>
<td>Asynchronous Transfer Mode</td>
</tr>
<tr>
<td>BDSU</td>
<td>Base Station &amp; Dispatcher Station Signalling Unit</td>
</tr>
<tr>
<td>BER</td>
<td>Basic Encoding Rules</td>
</tr>
<tr>
<td>BG</td>
<td>Border Gateway</td>
</tr>
<tr>
<td>BS</td>
<td>Base Station</td>
</tr>
<tr>
<td>BSC</td>
<td>Base Station Controller</td>
</tr>
<tr>
<td>CBC</td>
<td>Cipher Block Chaining</td>
</tr>
<tr>
<td>CCC</td>
<td>Call Control Computer</td>
</tr>
<tr>
<td>CCK</td>
<td>Common Cipher Key</td>
</tr>
<tr>
<td>CCSU</td>
<td>Common Channel Signalling Unit</td>
</tr>
<tr>
<td>CG</td>
<td>Charging Gateway</td>
</tr>
<tr>
<td>CHAP</td>
<td>Challenge Handshake Authentication Protocol</td>
</tr>
<tr>
<td>CIS API</td>
<td>Communications Interface Server Application Programming Interface</td>
</tr>
<tr>
<td>CUS API</td>
<td>Customer Care Application Programming Interface</td>
</tr>
<tr>
<td>CLAB</td>
<td>Clock and Alarm Buffer</td>
</tr>
<tr>
<td>CLIP</td>
<td>Calling Line Identification Presentation</td>
</tr>
<tr>
<td>CLIR</td>
<td>Calling Line Identification Restriction</td>
</tr>
<tr>
<td>CLP</td>
<td>Cell Loss Priority</td>
</tr>
<tr>
<td>CLS</td>
<td>Clock and Synchronisation Unit</td>
</tr>
<tr>
<td>CM</td>
<td>Central Memory</td>
</tr>
<tr>
<td>CMCE</td>
<td>Circuit Mode Control Entity</td>
</tr>
<tr>
<td>CSRC</td>
<td>Contributing Source</td>
</tr>
<tr>
<td>CUS API</td>
<td>Customer Care Application Programming Interface</td>
</tr>
<tr>
<td>DKCK</td>
<td>Derived Cipher Key</td>
</tr>
<tr>
<td>DECT</td>
<td>Digital Enhanced Cordless Telephone</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DGNA</td>
<td>Dynamic Group Number Assignment</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DLL</td>
<td>Data Link Layer</td>
</tr>
<tr>
<td>DMO</td>
<td>Direct Mode Operation</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DS</td>
<td>Differentiated Services</td>
</tr>
<tr>
<td>DSC</td>
<td>Dispatcher Station Controller</td>
</tr>
<tr>
<td>DSL</td>
<td>Digital Subscriber Line</td>
</tr>
<tr>
<td>DSS1</td>
<td>Digital Subscriber Signalling 1 (ISDN)</td>
</tr>
<tr>
<td>DWS</td>
<td>Dispatcher Workstation</td>
</tr>
<tr>
<td>DXT</td>
<td>Digital Exchange for TETRA</td>
</tr>
<tr>
<td>EC2ET</td>
<td>Echo Cancelling Exchange Terminal</td>
</tr>
<tr>
<td>EDU</td>
<td>Enhanced Data Unit</td>
</tr>
<tr>
<td>EF</td>
<td>Expedited Forwarding</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Payload</td>
</tr>
<tr>
<td>ET</td>
<td>Exchange Terminal</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute</td>
</tr>
</tbody>
</table>
FNIM  Fixed Network Interface Module
GC    Group Call
GCK   Group Cipher Key
GDR   Group Database Recovery
GFP   Generic Functional Protocol
GFT   Generic Functional Transport
GGSN  Gateway GPRS Support Node
GK    Gatekeeper
GPRS  General Packet Radio Service
GSM   Global System for Mobile Communications (previously Groupe Speciale Mobile)
GSSI  Group Short Subscriber Identity
GSWB  Bit-oriented Group Switch
GTP   GPRS Tunneling Protocol
GTSI  Group TETRA Subscriber Identity
GW    Gateway
HDB   Home Database
HMAC  Hashed Message Authentication Code
HTTP  Hypertext Transfer Protocol
IC    Individual Call
IDR   Individual subscriber Database Recovery
IE    Information Element
IEC   International Electrotechnical Committee
IETF  Internet Engineering Task Force
IKE   Internet Key Exchange
IMSI  International Mobile Subscriber Identity
IP    Internet Protocol
IPCP  Internet Protocol Control Protocol
IPI   IP Interworking
IPsec Security Architecture for IP
ISAKMP Internet Security Association and Key Management Protocol
ISDN  Integrated Services Digital Network
ISI   Inter-System Interface
ISO   International Standardisation Organisation
ISSI  Individual Short Subscriber Identity
ITSI  Individual TETRA Subscriber Identity
ITU-T International Telecommunications Union – Telecommunications Standardisation Sector
IV    Initial Value or Initialisation Vector
KS    Session Authentication Key
KSG   Key Stream Generator
LAN   Local Area Network
LAPD  Link Access Procedure for D-channels
LCP   Link Control Protocol
LDP   Label Distribution Protocol
LE    Late Entry
LLC   Logical Link Control
MAC   Medium Access Control
MCC   Mobile Country Code
MD5   Message Digest 5
MG    Media Gateway
MGC   Modified Group Cipher Key / Media Gateway Controller
MIME  Multipurpose Internet Mail Extensions
MLE   Mobile Link Control Entity
MM    Mobility Management
MNC   Mobile Network Code
MNI   Mobile Network Identity
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MoU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multiprotocol Label Switching</td>
</tr>
<tr>
<td>MS</td>
<td>Mobile Station</td>
</tr>
<tr>
<td>MSC</td>
<td>Mobile Switching Centre</td>
</tr>
<tr>
<td>MSISDN</td>
<td>Mobile Subscriber ISDN number</td>
</tr>
<tr>
<td>MT</td>
<td>Mobile Terminal</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transfer Unit</td>
</tr>
<tr>
<td>NMS</td>
<td>Network Management System</td>
</tr>
<tr>
<td>NMWS</td>
<td>Network Management Workstation</td>
</tr>
<tr>
<td>NSAPI</td>
<td>Network Service Access Point Identifier</td>
</tr>
<tr>
<td>NTDU</td>
<td>Applications Data Communications Unit</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>NTS</td>
<td>Nokia TETRA System</td>
</tr>
<tr>
<td>OMU</td>
<td>Operation and Maintenance Unit</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconection</td>
</tr>
<tr>
<td>OTAR</td>
<td>Over The Air Re-keying</td>
</tr>
<tr>
<td>PABX</td>
<td>Public Analogue Branch Exchange</td>
</tr>
<tr>
<td>PAMR</td>
<td>Public Access Mobile Radio</td>
</tr>
<tr>
<td>PAP</td>
<td>Password Authentication Protocol</td>
</tr>
<tr>
<td>PAU</td>
<td>Primary Access Unit</td>
</tr>
<tr>
<td>PDCU</td>
<td>Packet Data Computer Unit</td>
</tr>
<tr>
<td>PDGW</td>
<td>Packet Data Gateway</td>
</tr>
<tr>
<td>PDN</td>
<td>Packet Data Network</td>
</tr>
<tr>
<td>PDO</td>
<td>Packet Data Optimised</td>
</tr>
<tr>
<td>PDP</td>
<td>Packet Data Protocol</td>
</tr>
<tr>
<td>PDU</td>
<td>Protocol Data Unit</td>
</tr>
<tr>
<td>PEI</td>
<td>Peripheral Equipment Interface</td>
</tr>
<tr>
<td>PER</td>
<td>Packed Encoding Rules</td>
</tr>
<tr>
<td>PGP</td>
<td>Pretty Good Privacy</td>
</tr>
<tr>
<td>PHB</td>
<td>Per Hop Behaviour</td>
</tr>
<tr>
<td>PINX</td>
<td>Private Integrated Services Network Exchange</td>
</tr>
<tr>
<td>PISN</td>
<td>Private Integrated Services Network</td>
</tr>
<tr>
<td>PLMN</td>
<td>Public Land Mobile Network</td>
</tr>
<tr>
<td>PMR</td>
<td>Professional Mobile Radio (previously Private Mobile Radio)</td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-Point Protocol</td>
</tr>
<tr>
<td>PRA</td>
<td>Primary Rate Access</td>
</tr>
<tr>
<td>PS&amp;S</td>
<td>Public Safety &amp; Security</td>
</tr>
<tr>
<td>PSS1</td>
<td>Private Signalling System 1</td>
</tr>
<tr>
<td>PSTN</td>
<td>Public Switched Telephone Network</td>
</tr>
<tr>
<td>PTT</td>
<td>Push-to-Talk (button)</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial In User Service</td>
</tr>
<tr>
<td>RAS</td>
<td>Registration, Admission and Status</td>
</tr>
<tr>
<td>RCMU</td>
<td>Radio Network Configuration and Radio Channel Management Unit</td>
</tr>
<tr>
<td>RFC</td>
<td>Request For Comments</td>
</tr>
<tr>
<td>ROS</td>
<td>Remote Operations</td>
</tr>
<tr>
<td>ROSE</td>
<td>Remote Operations Service Element</td>
</tr>
<tr>
<td>RS</td>
<td>Random Seed</td>
</tr>
<tr>
<td>RSI</td>
<td>Removal of Subscriber Information</td>
</tr>
<tr>
<td>RSVP</td>
<td>Resource Reservation Protocol</td>
</tr>
<tr>
<td>RTCP</td>
<td>Real-Time Control Protocol</td>
</tr>
<tr>
<td>RTP</td>
<td>Real-time Transport Protocol</td>
</tr>
<tr>
<td>RTT</td>
<td>Round Trip Time</td>
</tr>
<tr>
<td>SA</td>
<td>Security Association</td>
</tr>
<tr>
<td>SAD</td>
<td>Security Association Database</td>
</tr>
<tr>
<td>SCK</td>
<td>Static Cipher Key</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>SDP</td>
<td>Session Description Protocol</td>
</tr>
<tr>
<td>SDS</td>
<td>Short Data Service</td>
</tr>
<tr>
<td>SDSI</td>
<td>Status and Short Data Service Interface</td>
</tr>
<tr>
<td>SGSN</td>
<td>Serving GPRS Support Node</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>SNDCP</td>
<td>Subnetwork Dependent Convergence Protocol</td>
</tr>
<tr>
<td>SPI</td>
<td>Security Parameter Index</td>
</tr>
<tr>
<td>SS</td>
<td>Supplementary Service</td>
</tr>
<tr>
<td>SSE</td>
<td>Segmentation Service Element</td>
</tr>
<tr>
<td>SSRC</td>
<td>Synchronisation Source</td>
</tr>
<tr>
<td>STU</td>
<td>Statistical Unit</td>
</tr>
<tr>
<td>SwMI</td>
<td>Switching and Management Infrastructure</td>
</tr>
<tr>
<td>TBS</td>
<td>TETRA Base Station</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TDMA</td>
<td>Time Division Multiple Access</td>
</tr>
<tr>
<td>TE</td>
<td>Terminal Equipment</td>
</tr>
<tr>
<td>TETRA</td>
<td>Terrestrial Trunked Radio</td>
</tr>
<tr>
<td>THR</td>
<td>TETRA Handportable Radio</td>
</tr>
<tr>
<td>TID</td>
<td>Tunnel Identifier</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TMO</td>
<td>Trunking Mode Operation</td>
</tr>
<tr>
<td>TMR</td>
<td>TETRA Mobile Radio</td>
</tr>
<tr>
<td>TOS</td>
<td>Type Of Service</td>
</tr>
<tr>
<td>TPST</td>
<td>TETRA PCM Speech Transcoder</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications System</td>
</tr>
<tr>
<td>V+D</td>
<td>Voice plus Data</td>
</tr>
<tr>
<td>VAC</td>
<td>Visitor Authentication Centre</td>
</tr>
<tr>
<td>VATSI</td>
<td>Visiting Alias Temporary Subscriber Identity</td>
</tr>
<tr>
<td>VDB</td>
<td>Visitor Database</td>
</tr>
<tr>
<td>VIRVE</td>
<td>Viranomaisverkko</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over IP</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WAP</td>
<td>Wireless Application Protocol</td>
</tr>
</tbody>
</table>
1. Introduction

TETRA (Terrestrial Trunked Radio) is a digital mobile phone standard. It is standardised by ETSI (European Telecommunications Standards Institute). ETSI is also responsible for standardising GSM. TETRA networks and mobile phones are aimed to be used by authorities, companies and other professional users. TETRA products are currently manufactured by several companies, Nokia and Motorola being the largest among them.

The authority and professional use of TETRA networks and equipment places several strict requirements for the network. The most important of these requirements are fast connecting time, group call, general reliability and the availability of speech channels. With these properties, TETRA is rapidly gaining popularity among authorities and other professional users.

As TETRA networks are taken into use in several countries by authorities, the need for interconnecting these networks is becoming evident. This possibility becomes more and more important because the role of the European Union and increasing cooperation between authorities in different EU-countries. With TETRA Inter-System Interface (ISI), same mobile equipment is fully functional also in foreign networks. Also (commercial) professional cellular users and operators need the Inter-System Interface for connecting their networks.

In Nokia Professional Mobile Radio business unit, there is a Networking Group that deals with TETRA ISI issues. The work of the Networking Group and the results of this master's thesis will both affect future plans and project decisions related to implementation of ISI. In the near future, it is even possible to contribute to telecommunications standards, because Nokia is one participant in ETSI TETRA ISI standardisation process.

In this master's thesis, ISI over QSIG in a standardised way is shortly described. Then, ISI over IP is considered. These IP considerations are important part of this work, largely because the current trends globally and also inside Nokia. Planning of the IP-based solution is useful also in the sense that it can be utilised when connecting different kinds of networks, for example PSTN, GSM and 3G, with IP.

Also TETRA packet data users are taken into account: the amount of data when compared to normal speech is increasing constantly in all digital mobile networks. It is important for also these packet data users to be independent of the network they currently are in, and therefore in this master's thesis also TETRA packet data is thought of related to ISI. Also TETRA and IP related security issues are dealt with: TETRA Air Interface authentication and encryption, TETRA packet data user authentication and IP security with packet data and ISI are thought of.

TETRA, being a new and emerging standard, has not yet achieved similar foothold as GSM in the digital mobile networks and phones market. Among professional and PS&S users, TETRA is however a well recognised standard corresponding to users' needs and demands, and new TETRA users are constantly arising among the traditional users of GSM mobile services. This would predict a strong growth for TETRA also in the near future.

However, there are fears that the existing enthusiasm and discussion about third generation mobile phone (UMTS) networks and phones decelerates growth of TETRA. TETRA has, nevertheless, for professional users many such advantages that even new 3G networks can not provide.

In this master's thesis, a development path from existing ETSI TETRA ISI standards towards IP based ISI is drawn. For both Voice over IP signalling protocols, H.323 and
1. Introduction

SIP, a solution is described which is as analogous as possible with the standardised one. This approach has been taken in order to reduce possible standardisation and implementation work.
2. TETRA

2.1 TETRA in general

2.1.1 What is TETRA?

TETRA is the first open digital PMR (Professional Mobile Radio) standard in the world. PMR networks are most commonly used by demanding professional users, who place strict requirements to the the network. The most important property of PMR networks is a group call for an arbitrary number of simultaneous participants.

The standardisation of TETRA is open in order to facilitate contributions from different network and radio terminal manufacturers. The aim is to produce practical and functional TETRA products and networks and to achieve a good interoperability between different vendors’ solutions.

Analogue PMR networks (for example Nokia Actionet) have several millions of users in Europe, and of course much more worldwide. The users and operators of these networks are now provided with a chance to move to digital technology with TETRA. This digital technology is very necessary especially when data communications possibilities and security are thought of.

The users of the PMR networks are traditionally divided into two different categories, and this applies also to the users of TETRA networks. These first of them is the private PMR operators. They are in total control of their networks, have personally tailored services and demand an extremely high level of reliability from the network. They can be Public Safety & Security (PS&S) related (for example police, fire brigades or rescue services) or companies (for example gas and water companies, transportation companies or construction companies).

The other category of users of these networks is PAMR (Public Access Mobile Radio) operators, which operate on a commercial basis and sell their services to customers. These customers can be private users, companies or communities. For the commercial operators the most important things are that the network features and functions are flexible and easily programmable according to the needs of different customers. For PAMR operators the charging is also an important issue.

An example of a PS&S use of a TETRA network is the finnish VIRVE (Viranomaisverkko) project, which is a network for governmental and communal security authorities. Nokia is the supplier of the network infrastructure and terminal equipment in this project. According to schedule, this network will cover the whole southern Finland by the end of the year 2000. [46]

An example of a commercial operator of a TETRA network is the European operator Dolphin, which operates in several countries. It offers TETRA services to private users, communities and companies. Of the countries where Dolphin operates, the networks in the UK and France are built by Nokia. In August 1999, 86 percent of the population of the UK were within coverage of this network. [6]

2.1.2 Special requirements for TETRA networks and terminals

Because TETRA networks are utilised in special and often critical situations, there are some special requirements that the terminals and the network itself has to fulfill. When for example a GSM mobile terminal is thought of, some things must be changed when moving to a professional use of mobile terminals.

The first of these requirements is fast call setup time, which is very highly demanded by customers. The reason for the fast call setup time requirements is obviously the
emergency situations where no time can be wasted. Another requirements for TETRA networks are general reliability and the availability of speech channels. General reliability is achieved in Nokia TETRA System by using DX200 digital exchange as a base for the Digital Exchange for TETRA (DXT). Also Nokia Mobile Switching Centres in GSM networks are based on this DX200 technology, and it has proven to be very highly reliable. In addition to this, the availability of speech channels is guaranteed so that in (especially in PS&S) networks the maximum capacity is much higher than usually would be needed. TETRA networks also have the concept of an emergency call, which disconnects a call with lower priority if no speech channels are available.

In addition to these requirements, the radio terminals need to be stronger and more resistant to external factors than for example GSM terminals. They are often used in extreme conditions, and if the users of these terminals fail to communicate the results might be catastrophic.

2.1.3 TETRA standardisation in ETSI

ETSI (European Telecommunications Standards Institute) is a non-profit making organisation whose purpose is to produce mainly telecommunications standards. It has members from 51 countries, and interoperates with other standadisation bodies like ITU-T (International Telecommunications Union – Telecommunications Standardisation Sector). An addition to TETRA, ETSI is responsible for standardising for example GSM, DECT (Digital Enhanced Cordless Telephone), xDSL (Digital Subscriber Line) and VPN (Virtual Private Network). [16]

The ETSI standardisation process consists of several parts, the most important one being the adoption phase. In the TETRA case, the adoption phase includes a so called Two-step Approval Procedure. The standard goes first to national standardising organisations for public enquiry, and those results go to the corresponding ETSI Technical Body for resolution. After this, national standardising organisations vote if the resulting standard is to be published. [16]

ETSI started to standardise TETRA in the year 1988. After lots of background work in the first years, the core parts of the actual standards were completed in years 1995-1998. Some of them are still under constant development, and new versions will be published also in the near future. There are two separate standards series, TETRA Voice plus data (V+D) and TETRA Packet data optimised (PDO). Nokia has chosen to implement TETRA system according to the V+D standard. PDO was not chosen, because it is based on outdated X.25 technology and thus has no customer demand. Furthermore, the V+D standard also includes the definition for packet data. These V+D documents are numbered in ETSI from "ETS 300 392-1" to "ETS 300 392-16". In addition, related standards are for example "ETS 300 395" for the TETRA speech codec and "ETS 300 396" for TETRA Direct Mode Operation (DMO).

In addition to ETSI, an organisation called TETRA MoU (Memorandum of Understanding) has been formed in the year 1994 to promote TETRA issues. It has members from 60 organisation in 18 countries. Some of its aims are to support ETSI TETRA standardisation, to support the initiative to obtain radio frequencies to TETRA and to develops a certification mark identifying standardised TETRA equipment. [45]

The actual TETRA standards differ from GSM standards in the sense that in TETRA less physical components in the network are standardised. In GSM all network elements (for example Mobile Switching Centre, Base Station and Home Location Register) and interfaces between them are standardised, but in TETRA only interfaces of more external nature are standardised. The internal implementation of the network infrastructure itself is left to be manufacturer specific. This allows for more flexible solutions according to each vendor’s capabilities.
2. TETRA

The ETSI standardised interfaces are the Air Interface (AI), Inter-System Interface (ISI), Peripheral Equipment Interface (PEI) for data communication between radio terminal and data terminal, Direct Mode Operation (DMO) for direct mobile-to-mobile communication, Network Management interface for network configuration and maintenance functions, Line Station interface for terminals fixedly attached to network and Gateway interfaces to external networks (for example to PSTN and ISDN). [1]

2.1.4 TETRA call types and services

The first basic TETRA call type is Individual Call (IC). It is just a point-to-point call from A-subscriber (calling party) to B-subscriber (called party). These subscribers can be TETRA radio terminal users, PSTN- or other external network users or dispatchers. A dispatcher workstation (DWS) is a special, Nokia specific network element in TETRA networks, used for controlling and surveillance purposes.

Individual Call can be made in two modes: duplex and semi-duplex. Duplex mode means that the A- and B-subscriber can both speak and listen to each other at the same time, and thus the call is much like a normal GSM call. The semi-duplex mode requires the attendees to press the push-to-talk (PTT) button in their radio terminals when they want to communicate. When the PTT button is held down, only the subscriber in question is able to transmit and the other subscriber has to listen.

The semi-duplex mode has the important property of saving radio resources: a need exists for only one reserved speech channel in the Air Interface for both uplink and downlink direction, that means, two speech channels are needed altogether. In duplex mode, two channels have to be reserved for each direction, which adds up to four reserved speech channels. The possibility to use the semi-duplex mode is an advantage for TETRA when compared with GSM.

In Nokia TETRA system, an Individual Call also differs from a GSM call in that sense that the resources for a call are not reserved until the B-subscriber has answered. This is done to avoid unnecessary load in the network when setting up a call, but can result in the fact that the B-subscriber is put in a queue when he answers. This does not of course apply to an emergency call, which is always set up. [1]

The other basic TETRA call type is Group Call (GC), and it differs totally from the concept of an Individual Call. Group Call is perhaps the main strength of TETRA when the system is compared with GSM. Group Call is a call between members of a predefined group, and everyone in that group are able to communicate when participating in the call. The Group Calls are always set up in semi-duplex mode, and each member gets to speak by pressing the PTT button. When a member of the group has been granted a speech item and thus gets permission to speak, his identity is shown to other members. It must be noted that Group Call does not consume much radio resources: only one channel needs to be reserved in the Air Interface for downlink direction even though there are several participants in the area. Thus within the area of one base station, always a maximum of two speech channels are needed for a Group Call.

In Group Calls, the speech items are granted according to priorities assigned to each group member. It means that if a member has a lower priority than somebody else in the group, he may have to wait for the permission to speak. A speaker makes a transmission request by pressing the PTT button, and when the system has to choose from members having the same priority level, the one having the oldest transmission request is chosen. The member is informed by a sound and display signal when the item is granted. [2]

Dispatchers are closely involved in Group Calls. They can configure the groups from the DWS, add new members into the groups and monitor the audio events. They can
also use a so called pre-emptive speech item in a Group Call, which means that it
interrupts all ongoing speech and gets through immediately. It is used for example
when making important announcements.

All of the things that have been explained in this chapter so far happen in the normal
TETRA operation mode Trunking Mode Operation (TMO). It means the involvement of
the network infrastructure in a call, much the same way than in a GSM call. A special
operation mode of TETRA radio terminals is Direct Mode Operation (DMO) where no
network infrastructure or base stations are needed at all, and the radio terminals
communicate directly with each other. When the radio terminals are for example out of
coverage, they can manually switch to DMO from TMO.

A totally different set of features are the TETRA data services. The first of them is
TETRA Short Data Service (SDS), which very closely corresponds to the GSM SMS.
One short message has 126 characters of self defined information (later this amount
will be doubled to 255 characters per message). Another, for the professional users
maybe even more useful service, are the predefined status messages. They are
number codes (the range is from 32768 to 65535) transmitted from a subscriber to
another, each having a special meaning of its own preprogrammed in the terminals.
For example, code number 32990 might mean "I am going to have lunch", but the code
itself is totally hidden from the user. He chooses only the message. [1]

Perhaps the most important data service is the TETRA IP packet data service based
on TETRA Packet Data Protocol (PDP). It is to some extent comparable with GSM
General Packet Radio Service (GPRS), and will as a whole be dealt with later in the
text.

TETRA standards define also a variety of supplementary services (SS), of which only a
few are implemented so far in Nokia TETRA system. Even the ETSI standardisation
work itself is unfinished for some of them. The most important of the already
implemented ones are CLIP (Calling Line Identification Presentation), CLIR (Calling
Line Identification Restriction), DGNA (Dynamic Group Number Assignment) for
dispatchers controlling a Group Call and LE (Late Entry) for group members joining an
already ongoing Group Call. [1]

2.1.5 Numbering

The basic TETRA identity code is TETRA Subscriber Identity (TSI), and its structure is
depicted in Figure 1. A TETRA TSI is unique in whole TETRA domain (comprising all
TETRA networks), and a TETRA SSI is unique in one TETRA network. TETRA
networks have separate identities for individual callers and groups: an individual
identity is called ITSI (containing the corresponding ISSI) and a group identity is called
GTSI (containing the corresponding GSSI). The Mobile Country Code (MCC) and
Mobile Network Code (MNC) of a subscriber form a subscriber Mobile Network Identity
(MNI).
2. TETRA

2.1.6 Mobility management (MM)

TETRA has a mobility management which somewhat resembles GSM MM. To the user mobility management basically means that the ongoing communication may always continue uninterrupted when moving in the network. Few terms need to be explained here: first, a handover means (like in GSM) moving from one cell to another when engaged in a call. Roaming in TETRA is different than GSM, however: it means changing the Location Area in network. Location Area is only a part of one TETRA network and often comprises several cells. In TETRA, the act of roaming to another network is called migration.

There are four kinds of handovers supported by ETSI TETRA standards, and all of them are not yet implemented in Nokia TETRA system. The currently supported cell-reselection strategies work so that the radio terminal registers in a new cell without it knowing in advance about the registration. In the future, some cell-reselection strategies that are more network-controlled will be added. [34]

2.2 Network architecture in TETRA

As previously said, in TETRA only the external interfaces are standardised which leaves the network infrastructure to be implemented by each manufacturer in his own way. That means that the network architecture and elements depicted in this chapter are Nokia specific.

The design of the Nokia TETRA system is largely based on analysis of user requirements and aims to making the operating of a PMR network easy. The network architecture is also scalable: one TETRA network can include one or several of each network elements. One Digital Exchange for TETRA (DXT) serves up to 256 carriers. Currently one network can have a maximum of 100000 subscribers, but this amount will soon increase the target being one million subscribers per TETRA network infrastructure. [2]

There are some differences in typical network configurations between commercial and PS&S operators. PS&S operators prefer more a distributed database architecture, which means that the home database and visitor database are both included in all DXTs in the network. Commercial operators need a more centralised solution, the home databases being in only some of the "upper level" DXTs (DXTTs). [1]

Saku Oja: Lower layer protocols in TETRA Inter-System Interface
In the following figure (Figure 2), a small TETRA network is depicted. Each network element is shortly described in the next chapter.

Figure 2. A small Nokia TETRA network [2].

2.2.1 Basic network elements

**Digital Exchange for TETRA DXT64**

DXT64 switches speech and data between network users, radio users as well as dispatchers. In group communication it allocates the speech items and handles the priorities. The exchange has subscriber home and visitor databases for subscriber identification and call rights data. Radio subscriber data is entered to database using a CUS API or a DWS (both are explained later). Radio user location information is also stored in the DXT.

**Digital Exchange for TETRA DXT256**

The properties of DXT256 are similar to DXT64, but with an increased capacity. The physical size of the exchange is also doubled from the DXT64.

**Digital Exchange for TETRA DXTT**
DXTT is an exchange for connecting other DXT exchanges into the network. It is a transit exchange to facilitate dynamic call routing, and can not have connections to TETRA Base Stations (TBS).

**TETRA Base Station (TBS)**

TBS provides together with radio terminals the wireless communication in TETRA system. There are separate base stations for indoor and outdoor use. The TBS consists of one or two cabinets, both having a maximum of 16 radio channels. Thus the maximum amount of channels in one TBS is 31 traffic channels plus a control channel. A TBS can use one, two or three receiver antennas. The TBS is flexible in the sense that more radio units or power supply modules can be added later according to the needs of the user. [2]

**Dispatcher system**

The dispatcher system consists of the following main elements: the Dispatcher Station Controller (DSC) which controls up to six Dispatcher Workstations (DWS). In addition, there are audio peripherals such as microphones, headsets, handsets, loudspeakers and manual switches attached to the DWS. The DWS itself provides for detailed information of the whole TETRA system or just a part of the network. It can, similarly to a normal radio terminal, make individual and Group Calls and send and receive short messages or status messages. Important tasks of a DWS user are often emergency call handling, group configuration management and addition of new groups. [1]

**Network management system**

Network management system is also an important part of TETRA network. It enables tasks related to implementation and functioning of the radio network, operative management for planning and configuring services and features and management of subscribers. Two solutions for Nokia TETRA network management are available. For middle-sized and large networks Nokia NMS/400 should be used; it enables effective management of large numbers of DXTs, base stations and dispatcher systems. For smaller networks, Network Management Workstation (NMWS) is enough. It provides some PC-based tools for management purposes. [2]

**Other interfaces**

In addition to the standard network management system, third party applications are allowed to manage radio subscribers and other system activity outside Nokia TETRA system by using a Customer Care Application Programming Interface (CUS API) or a Communications Interface Server Application Programming Interface (CIS API). Also a Status and Short Data Service Interface (SDSI) is provided, which enables the sending of status and short data messages by third party applications outside Nokia TETRA system. [2]

2.2.2 Digital Exchange for TETRA (DXT)

Digital Exchange for TETRA (DXT) is the heart and basic component of the Nokia TETRA system and is based on Nokia's DX200 Digital Exchange platform. DX200 is especially designed to be used in telecommunications applications, and has appropriate properties like modular structure, low power consumption and high reliability. The DX200 platform provides the basic hardware and software building blocks for DXT. Almost the same DX200 platform is used in Nokia fixed and GSM network exchanges, the minor differences are because the special requirements and properties of TETRA networks.
2. TETRA

DXT is based on distributed call control architecture, where each microcomputer unit executes their own tasks and communicate with each other via a message bus. With dedicated tasks for each unit, the software for the units can be optimised to perform certain functions better. An important design principle in DX200 and DXT is also the redundancy principle: every unit has a backup unit in case of faults, and even the message bus is duplicated. The backup units are kept in a stand-by state when DXT is running, and changeover can happen immediately after the fault has occurred.

In the following figure (Figure 3), a block diagram of DXT is depicted. The purpose and functionality of each unit is shortly described below.

![DXT 256 block diagram](image)

**Group Switch (GSWB)**

The switching system and a main component of DXT is a bit-oriented Group Switch (GSWB). It is a non-blocking, one stage combined time-space switch, where any number of bits can be switched as a block. The connections are switched in both active and spare units at the same time for call maintenance in case of a changeover. [1]

**Call Control Computer (CCC)**

Call Control Computer is a unit controlling the Group Switch. In addition to call control related tasks, it handles radio network resource management. The unit also controls the connections to PABX/PSTN networks and other TETRA networks via the Inter-System Interface.

**Central Memory (CM)**

Central Memory unit handles DXT database services for other computer units, and controls the signalling to other DXTs in the same TETRA network.

**Base Station & Dispatcher Station Signalling Unit (BDSU)**

BDSU controls signalling to TETRA Base Stations and Dispatcher System.

**Operation and Maintenance Unit (OMU)**
Operation and Maintenance Unit has some system supervision, maintenance and alarms related tasks. It acts as an interface between maintenance personnel and the TETRA system. The recovery functions of DXT in faulty situations are performed by OMU in co-operation with CM. [2]

**Interface units**

There are three kinds of units for connecting DXT256 to other components of Nokia TETRA System. An Exchange Terminal (ET) connects DXT to TETRA Base Stations, Network Management Systems, Dispatcher Systems and other DXTs. Furthermore, an Echo Cancelling Exchange Terminal (EC2ET) connects ISDN PRA lines to DXT, and a Fixed Network Interface Module (FNIM) connects DXT to analogue PSTN/PABX networks and analogue PMR networks.

**Other units**

Other units in DXT are Clock and Synchronisation Unit (CLS), Clock and Alarm Buffer (CLAB), Fixed Network Interface Module (FNIM) for connecting analogue lines from PSTN, PABX or other PMR networks to DXT, Applications Data Communications Unit (NTDU) for providing CUS and CIS APIs, Packet Data Computer Unit (PDCU) for handling IP packet data communications, Statistical Unit (STU) for collecting charging and statistics information, Common Channel Signalling Unit (CCSU), Primary Access Unit (PAU) for ISDN call handling, Authentication Centre Unit (ACU), Radio Network Configuration and Radio Channel Management Unit (RCMU) and Enhanced Data Unit (EDU) for future purposes. [2]

### 2.3 TETRA Air Interface

#### 2.3.1 Protocol stack

ETSI TETRA standards define the three lowest layers of protocol stack in Al. The following figure (Figure 4) presents the layers and their sub-layers for the Control Plane (signalling). The User Plane (speech) protocol stack consists only of Layer 1 and the two lowest sub-layers of Layer 2. [8]

![Figure 4. TETRA Control Plane protocol stack in Al 7, [9].](image)

**Physical layer**

The physical layer handles the transfer of bursts, multiplexes logical channels into bursts and modulates the signal.

**Link layer**

The lower Medium Access Control (MAC) sub-layer provides functions such as control of radio resources, signal strength measurements and transfer of upper MAC Protocol Data Units by using the physical layer. The upper MAC sub-layer provides frame
synchronisation, security issues and radio path establishment. The Logical Link Control (LLC) sub-layer provides data transfer services to the network layer. [1]

**Network layer**

The Mobile Link Control Entity (MLE) sub-layer is responsible for mobile station to base station association management and identity management. On top of MLE there is a Mobility Management Entity (MM), a Circuit Mode Control Entity (CMCE) and Subnetwork Dependent Convergence Protocol (SNDCP) for TETRA Packet Data.

**2.3.2 Radio path**

For efficient bandwidth usage on the radio path, TETRA uses an Algebraic Code-Excited Linear Predictive (ACELP) codec for speech compression. In this coding method, the speech is A/D converted and the samples are coded. After that, basically the two consecutive samples are compared with each other, and only the difference between the samples is transmitted. The ACELP speech codec produces a very low speech bit rate of 4,567 kbit/s, but the speech quality is still good. The codec is designed also to take the characteristics of human voice into account and to eliminate background noise. [1]

In TETRA Air Interface, four timeslots (each having an effective bit rate of 7,2 kbit/s) are multiplexed into one 25 kHz carrier using a Time Division Multiple Access (TDMA) technology. The gross bit rate of one TDMA frame with four traffic channels is 36 kbit/s, because the additional channel coding. The 25kHz carrier spacing is chosen for interoperability with analogue PMR systems, which mostly use 25 kHz or 12,5 kHz carrier spacing. [1]

**2.4 TETRA terminal equipment**

Nokia produces two kinds of TETRA mobile terminals. TETRA Mobile Radio (TMR) is a radio to be fixedly installed in a vehicle or an office. There is a separate control unit, radio unit and push-to-talk button with a microphone. The radio has a large keypad with some programmable function keys and a large display. Also a robust aluminium housing for the radio unit is provided. This kind of radio is presented in Figure 5.
The other kind of radio terminal is called a TETRA Handportable Radio (THR). It somewhat resembles a GSM radio terminal. However, it has a push-to-talk button, and a mechanically very durable design. Of the two kinds of TETRA Handportable Radios, the outlook of THR600 is more GSM-like and a THR420 is more like a radio for traditional PMR use. In Figure 5, a THR420 radio is also presented.

2.5 TETRA security

2.5.1 TETRA user authentication

The user authentication in TETRA aims at achieving a mutual trust between a mobile terminal user and the network infrastructure. The authentication scheme is somewhat extended when compared to GSM authentication: in addition to the network infrastructure which authenticates the user, a user can also authenticate the network infrastructure. The user authentication is obviously needed in preventing unauthorised network intrusion, whereas the network authentication is useful in preventing connecting to a possibly hostile TETRA network.

Both ways, the authentication of is based on the knowledge of a common secret, authentication key K. The authenticating parties in TETRA are the Mobile Station (MS) having a certain ITSI number, the Authentication Centre in TETRA Switching and Management Infrastructure (SwMI) and the Base Station (BS). In the Nokia TETRA system, the Authentication Centre resides in DXT.

The authentication of a TETRA user is presented in Figure 6. First, a session authentication key (KS) is calculated with algorithm TA11, which takes also a random seed (RS) as an input. Then, RS and KS is passed on to the Base Station, which generates random number RAND1 and sends it and the RS to the Mobile Station. In MS, algorithm TA11 is utilised again, and after that also algorithm TA12 is utilised in
MS and at the same time in the BS. Now, the results are compared and if they match, a user is correctly authenticated. [15]

![Authentication of a user by the infrastructure](image)

**Figure 6. Authentication of a user by the infrastructure [15].**

This way, a Derived Cipher Key 1 (DCK1) is generated. The authentication of the network infrastructure by the user is a symmetric procedure with different algorithms TA21 and TA22. From that procedure, a DCK2 is obtained. From DCK1 and DCK2, a DCK for encrypted communication (described in the next chapter) is generated in both Base Station and Mobile Station with an algorithm TB4. If only unilateral authentication is in use, the other component of DCK is set to zero when calculating the DCK. [15]

2.5.2 Air Interface encryption

The TETRA Air Interface encryption is important for preventing eavesdropping in the radio path. In TETRA, the importance of speech, data traffic and signalling encryption is even higher than in GSM. This is obviously due to the Public Safety & Security use of TETRA networks.

The encryption key used for Individual Calls is DCK, which is obtained as a result of successful authentication. DCK is also used for encryption of uplink direction in Group Calls. A different encryption key called Common Cipher Key (CCK) is used in downlink encryption of Group Calls. It is distributed to the group in signalling messages, and the key is sealed as a function of DCK for preserving the confidentiality. [1]

For enhanced security in Group Calls, the group may further have a group specific encryption key for this downlink communication encrypting. If this is the case, this Group Cipher Key (GCK) is distributed to the group in addition to CCK. From these two, a Modified Group Cipher Key (MGC) is obtained with algorithm TA71, and is used for encryption. [15]
Also a Static Cipher Key (SCK) exists, and it is designed mainly for performing encryption when the MS is in Direct Mode Operation. There are up to 32 SCKs available for each MS, and they are known beforehand by the Mobile Stations as well as the network infrastructure. [1]

The encryption itself is made at the upper MAC layer in the protocol stack. It is performed as a simple stream ciphering, and the process is depicted in Figure 7. First, a Key Stream Generator (KSG) takes the CK and an Initial Value (IV) as input. IV is generated by the BS and distributed to the MS. Now, the KSG produced key stream is xor-ed with the plain data, and encrypted data is obtained. The inverse process is exactly the same. [15]

![Figure 7. Speech and control information encryption [15].](image)

2.5.3 End-to-end encryption

ETSI TETRA standards define end-to-end encryption by providing an interface for a transparent transfer of binary data through the system after the call set-up. The end-to-end encryption may be applied in addition to the standard Air Interface encryption for increasing the security level of the communication.

The standard does not define any exact algorithms or key management protocols here: they are left to be organisation specific. The end-to-end encryption is performed above the upper MAC layer at the protocol stack, and only for the User Plane (speech) traffic. [15]

2.6 TETRA Packet Data Protocol

2.6.1 The need for Packet Data Protocol

Nowadays, the amount of data related to speech is constantly increasing in all mobile networks. Partially this means short messages which are already supported in TETRA. There are definitely needs, however, to get application level data transferred via TETRA network infrastructure.

The solution to this is the TETRA Packet Data Protocol (PDP). Basic property of TETRA single-slot packet data is the relatively low bit rate of 2,4 kbit/s. Without error correction, the bit rate is doubled to 4,8 kbit/s. However, the TETRA standard supports multislot data up to four slots, and an implementation of multislot data will follow later. In any case, these bit rates are best suitable for transferring textual data. However, there are many important ways to utilise this text based data for example among PS&S network users.
With TETRA packet data, users can make authenticated and secured connections to their own (for example police) intranets, where they can make for example important database queries. For police, this means access to criminal and other records. Furthermore, other necessary textual information can be transferred: location information, route descriptions, traffic information or e-mails reach the personnel who are on duty. In addition to this, also automated applications like surveillance equipment or burglar alarm can make use of TETRA packet data to inform about emergencies.

In addition to these applications, a very important extension based on TETRA packet data is Wireless Application Protocol (WAP). Nokia has initiated the adaptation of WAP to TETRA in April 1999, and TETRA was later included in WAP standard version 1.2. With TETRA, WAP can be chosen to run either over PDP or SDS. In the near future, TETRA mobile terminals with larger displays and WAP make access to corporate intranet even easier than now.

2.6.2 PDP protocol stack

ETSI standards related to TETRA PDP give means to convey different higher layer protocols. In practice however, this means that IPv4 (later also IPv6) is used as the network layer protocol. With PDP, TETRA is extended to act as an IP subnetwork. According to the standard, the application utilising IP data may be located either in the Mobile Terminal MT (for example a WAP application) or in another Terminal Equipment TE (an IP application running on a computer). The PDP protocol stack in the Air Interface is presented in Figure 8.

In the Mobile Terminal and the Switching and Management Infrastructure, the IP protocols are run above the Subnetwork Dependent Convergence Protocol (SNDCP). It is a TETRA specific network layer protocol with some important functions. SNDCP negotiates and maintains PDP contexts between MT and the SwMI. A unique PDP context identifier is given for each active PDP connection. During the context activation procedure, a TETRA ITSI is bound to the PDP context identifier.

In addition, SNDCP allows also a single data link connection to be shared by multiple IP addresses by assigning separate Network Service Access Point Identifiers (NSAPI) to the connections. SNDCP also performs TCP/IP header compression to the messages and controls the data transfer between MT and SwMI allowing the service user to select acknowledged or unacknowledged layer 2 services over the Air Interface.

At the MT and TE, the Peripheral Equipment Interface Data Link Layer (PEI DLL) services are provided to the IP layer by Peripheral Link Service Access Point (PL-SAP). In practice, the Point-to-Point Protocol (PPP) is used as the PEI DLL protocol.
2. TETRA

The PPP provides a Link Control Protocol (LCP) for establishing, configuring and testing the data link connection, and the Internet Protocol Control Protocol (IPCP) for configuring the IP protocol between MT and TE. [14]

With TETRA PDP, IP user authentication is supported. For this, the PPP Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) is used. The IP user authentication is more precisely dealt with in chapter 2.6.5.

2.6.3 Current Nokia PDP implementation

The current Nokia PDP implementation is presented in Figure 9. One Nokia TETRA System (NTS) network infrastructure acts as an IP subnetwork. It is connected via IP backbone routers and a firewall into a corporate intranet or the Internet.

![Figure 9. Current TETRA packet data implementation [38].](image)

Each Packet Data Gateway (PDGW) has two connections to the TETRA IP backbone. Physically, one PDGW resides in DXT and consists of two Packet Data Communication Units (PDCU). The two units work simultaneously and share the IP traffic load. [38]

The IP addresses of hosts (Terminal Equipments) within the system are managed by a DXT. The first possibility is that the IP address of a host is statically bound to a TETRA ITS. Now, when the PDP context is requested by the MS, the static IP address for that MS is returned. Another possibility is that the IP address is dynamically allocated from a common host identifier pool, when the PDP context is formed. The IP address is bound to ITS during the PDP context creation, and the allocation takes place in a DXT. After this, more PDP contexts with different IP addresses can be created for the same TE. [38]

Though being a fully functional IP packet data solution, the current implementation has several drawbacks. One of them is clearly the missing IP user authentication, and others are for example the non-allocability of IP addresses from (for example commercial) TETRA user's own address space; the address is now simply allocated from the pool of the operator.

2.6.4 Future PDP implementation using GPRS concepts

For an enhanced TETRA packet data implementation, a new approach has been taken. It is based on General Packet Radio Service (GPRS) concepts which are adopted from GSM world. Among GSM operators, GPRS is rapidly gaining popularity and new network elements are installed. Also GSM Mobile Stations with GPRS support are coming to the market.

GPRS is a GSM Phase 2+ technology for packet switching, and it is standardised by ETSI. The main work in GPRS standardisation was completed in 1998. In GPRS, two new network nodes are introduced. A Serving GPRS Support Node (SGSN) is connected to the Base Station Controller (BSC), and is at the same hierarchical level as the Mobile Switching Centre (MSC). It routes the packet traffic from the BSC to the Intra-PLMN IP backbone (Gn interface) and thus handles the protocol conversion...
between the IP backbone protocols and the GSM SNDCP and LLC protocols used between the BSC and MS. SGSN also handles the GPRS MS authentication, registration and mobility management functions. [30]

Another node, a Gateway GPRS Support Node (GGSN) routes the packet traffic from the Intra-PLMN IP backbone to the Internet. From the external networks' point of view, the GGSN is a router to a subnetwork. However, GGSN hides the GPRS and GSM specific implementation of the subnetwork. Between SGSN and GGSN, the GPRS packet data and signalling is transmitted using the GPRS Tunneling Protocol (GTP). It is a protocol on top of the underlying IP protocol suite allowing the tunneling of multiprotocol packets between the GSNs. [30]

The future implementation of TETRA PDP is based on adoption of GGSN and GTP to the TETRA world with some GPRS related concepts and security features. In this scenario, TETRA SwMI (in practice, one of the DXTs) acts as a SGSN and is connected to GGSN (Gn interface) using GTP. The TETRA IP backbone and TETRA SwMI both belong to a TETRA PLMN, which is usually controlled by one operator. The architecture is presented in Figure 10.

![Figure 10. Architecture of TETRA PDP with GGSN [42].](image)

In addition to normal DXT functionality, the DXT connected to TETRA IP backbone has some SGSN-like functions: it controls GTP tunneling to GGSN and performs the needed protocol conversion between the GTP and TETRA SNDCP and vice versa. In the other end of GTP tunnel resides GGSN, which has some important functions related to IP address management and IP user authentication. In addition to GGSN, a Charging Gateway (CG) can exist in the IP backbone. It collects charging records from GGSN and passes them on to the operator’s billing system. It also acts as an entry point to the system for billing configuration. [42]

Moreover, some GPRS adopted concepts must be explained. An Access Point Name (APN) is a reference to a GGSN which the GTP tunnel will be formed to. In TETRA, the ITSI is statically bound to a certain APN in SwMI (DXT). The APN consists of an APN Network Identifier (identifying the external IP network and GGSN) and the APN Operator Identifier (identifying the TETRA network in question). An identifier for the PDP context between the SwMI and GGSN is the Tunnel Identifier (TID), which is a reference to a certain GTP tunnel. It is created in SwMI. Additionally, an International Mobile Subscriber Identity (IMSI) for the TETRA subscriber is needed because the use of GGSN. It stored in both HDB and GGSN and has a one to one relation to the corresponding ITSI.

In the following figure (Figure 11), a basic signalling example related to PDP context creation (establishing of packet data communication) is presented.
2. TETRA

![Diagram](image)

**Figure 11. MS originated PDP context activation [42].**

First, the MS sends a SN-Activate PDP Context Demand message to SwMI, also indicating if it wants to use a static or dynamically created IP address (1). Now, the TID is created in SwMI by combining the ITSI of the MS with the NSAPI received from the MS. The APN identifying the GGSN is requested from Home Database (HDB), and it is translated to IP address of GGSN by using the DNS functionality in TETRA IP backbone. [42]

Now, SwMI sends a Create PDP Context Request message to GGSN with the created TID (2). GGSN creates a new entry in its PDP context table and generates a charging ID. If a dynamic IP address was requested, GGSN allocates the address using a DHCP server in external network. Then, GGSN returns a Create PDP Context Response message to the SwMI (3) containing the IP address (if it was requested for). Now, the SwMI sends the SN-Activate PDP Context Accept message to the MS (4). [42]

### 2.6.5 IP user authentication with PDP

One of the key benefits of the GPRS based solution is the support for IP user authentication with a Remote Authentication Dial In User Service (RADIUS). If authentication is in use, some messages are added to the signalling example in Figure 11.

The authentication parameters are first exchanged between the Mobile Terminal and Terminal Equipment (computer). This is done before sending the SN-Activate PDP Context Demand message to SwMI and by using PAP or CHAP. With CHAP, a random challenge is first sent from the MT to TE. A cryptographically hashed response is obtained in MT using this challenge and a secret key. TE sends response to MT and after this MT sends a success indication to TE. Also PAP can be used but it is not recommended, because PAP is not a strong authentication method. User identification and password are sent from TE to MT in clear, and MT replies to this with success. [44]

It must be noted, however, that here success is given to TE in all cases; the actual authentication is performed later by GGSN acting as a RADIUS client. The PAP or CHAP authentication information is passed on to GGSN with the messages SN-Activate PDP Context Demand and Create PDP Context Request. With this information, GGSN makes a RADIUS protocol Access-Request to the Authentication, Authorisation and Accounting (AAA) server in the external network. If the information was correct, an Access-Accept message is returned to GGSN. Otherwise, an Access-Reject is given. [9], [40]

Now, based on the reply received from the RADIUS server, GGSN sends a Create PDP Context Response with a positive or negative cause value to the SwMI. After this, the SwMI sends a SN-Activate PDP Context Accept or a SN-Activate PDP Context Reject message to the MT. [42]
3. TETRA Inter-System Interface

3. TETRA INTER-SYSTEM INTERFACE

The Inter-System Interface (ISI) is an interface between two separate TETRA networks. These networks can be located in different countries, but a country may as well have several separate TETRA networks. TETRA ISI is depicted in Figure 12.

![Figure 12. TETRA Inter-System Interface.](image)

3.1 ETSI ISI in general

3.1.1 ISI related concepts and issues in TETRA

Basically, for a TETRA user ISI means same services and same usability of the network both in home and foreign networks. In addition, the migration to another network may happen when a call or a packet data communication is active, and in that case the connection must be restored immediately after migration to the new network has been completed.

All of this functionality rises some new concepts that must be taken into use in TETRA. First, there must now be a clear conceptual distinction between a Home Database (HDB) and a Visitor Database (VDB). HDB contains information about the subscribers of the network in question, and VDB contains temporary information about visiting subscribers from other networks. The HDB must contain information about subscriber location at each moment, that means, which network the subscriber has migrated to. Also basic and optionally supplementary service profiles of the subscriber must be available in the HDB. [10]

When a subscriber has migrated, a new kind of temporary identity, Visiting Alias Temporary Subscriber Identity (VATSI) is assigned to him. It is only a ITSI which is chosen from a certain range to identify visiting subscribers. Now, in the VDB, there must be a mapping between the global TETRA subscriber identity ITSI and the VATSI assigned for the subscriber. Also, the basic and optionally supplementary service profiles are fetched into VDB when a subscriber is migrating. [10]

Concerning the migration, Mobility Management, Individual Call and Group Call, there are several cases with differing signalling flows. A subscriber can migrate from home SwMI to a visited SwMI, from a visited SwMI to home SwMI or from a previous visited SwMI to a new visited SwMI. When in a call, all call participants can be in their home SwMIs, all in visited SwMIs or some of them can be in home SwMIs and some in visited SwMIs.

3.1.2 ETSI ISI protocol model

In the following figure (Figure 13), TETRA ISI protocol model is presented. Currently, the ETSI standards define the lower protocol layers to be QSIG with the Generic Functional Protocol (GFP) to perform the needed functionality for TETRA ISI. These protocols and other components in the figure are explained in the following chapters.
3. TETRA Inter-System Interface

3.1.3 ETSI ISI Additional Network Features

The Additional Network Features (ANFs) are the highest level standardised entities in TETRA. There are five of them: ANF-ISIIC (Individual Call), ANF-ISIGC (Group Call), ANF-ISISS (Supplementary Services), ANF-ISISD (Short Data Service) and ANF-ISIMM (Mobility Management). The ANFs for Individual Call, Group Call and Mobility Management are dealt with more precisely in this chapter, whereas the ANFs for Short Data Service and Supplementary Services are still mostly unstandardised and are thus left without a more comprehensive look. [10]

The standards describing these ISI ANFs form the major part of TETRA ISI standardisation. They are all described using a three-stage methodology standardised by ITU-T. The first stage describes the services the ANF provides for the users, the second stage describes the signalling flows related to the services and the third stage describes the signalling protocols and encoding rules for the flows.

As can be seen from Figure 13, Supplementary Services, Short Data Service and Mobility Management ANFs are placed on upper part of the figure whereas the Individual Call and Group Call ANFs are located straight on top of lower layer protocols. This is because the signalling flows related to calls are in close connection with basic QSIG call setup signalling flows. IC and GC still have a connection to the other entities, however, for the call related TETRA proprietary signalling information. As an example of this, ITSI number of the called party can be mentioned: it is non-relevant information to the underlying QSIG protocol.

Figure 13. ETSI ISI protocol model [10].
3.1.4 QSIG protocol with Generic Functional Transport

ETSI ISI applications are built on top of the QSIG protocol, which is also known as the Private Signalling System 1 (PSS1) protocol. It is a protocol for interconnecting Private Integrated Services Network Exchanges (PINXs) to form a Private Integrated Services Network (PISN) and, furthermore, a protocol for interconnecting several PISNs. PSS1 is standardised by International Standardisation Organisation (ISO), and these ISO standards have been used as a reference when the use of PSS1 is defined in ETSI TETRA standards.

QSIG/PSS1 is a protocol largely resembling the widely-used ISDN Digital Subscriber Signalling 1 (DSS1) protocol. The most noticeable difference between ISDN DSS1 and QSIG is that DSS1 is asymmetric whereas QSIG is symmetric. It means that when utilising DSS1 signalling one has always a concept of user side and the network side of the signalling connection, but with QSIG signalling this is unnecessary.

Two ISO standards are involved here: first, there is the document for PSS1 basic call, numbered ISO11572. It describes the basic PSS1 call messages like SETUP, ALERTING, CONNECT and RELEASE COMPLETE. In addition to this document, the Generic Functional Protocol (GFP) for PSS1, ISO11582, is referenced. It describes the means to transfer supplementary service or end-to-end application level information with PSS1. This functionality is achieved by utilising a Facility information element in the existing PSS1 messages or by using a separate FACILITY message. In the above Figure 13, the block named "GFT Control" in practice refers to the use of Facility information element as a means to transfer TETRA proprietary information.

In ETSI ISI the layer below PSS1, Data link layer, is in accordance with the ETSI 300 402-2 Link Access Procedure for D-channels (LAPD) standard. This standard is based on ITU-T Q.921 (Data link layer for DSS1). Physically, the lines are PCM lines with 2 Mbit/s capacity and have 30 B-channels (for speech and data) plus one D-channel (for signalling and user proprietary information). Thus the capacity of each speech channel is the standard 64 Kbit/s. According to standard, however, only one eighth (8 Kbit/s) of each slot is used to transmit TETRA coded speech, rest being empty. [10]

The standards allow still an optional way to physically transmit the speech or data: eight TETRA speech channels can be included in one 64 Kbit/s PCM timeslot, and thus the capacity of the PCM line can fully be utilised. Furthermore, a possible extension to current standards exists: eight B-channels can be multiplexed into one B-channel near the TETRA SwMI, and the one B-channel can be demultiplexed back to eight B-channels near the other SwMI. Now, the endpoints do not need to be aware of the altered solution at all. [10]

The actual PSS1 connection is formed only between the TETRA networks (SwMIs), which map to PISNs at the PSS1 level. A PSS1 connection is always terminated on a border of a SwMI. Now, each SwMI can have several gateways to other SwMIs and thus, at the PSS1 level, several PINXs. TETRA ISI calls and signalling can be routed based on a PISN number: in this case, the PSS1 connection terminates to an arbitrary PINX at the border of the destination SwMI. Calls and signalling can, however, be also routed based on a PINX number which implicitly specified the used gateway to the destination SwMI. In TETRA SwMIs, it is configurable which numbering scheme is used as a default. Additionally, the SwMIs can agree on using the other numbering anytime.

Now, the SwMIs with Inter-System Interfaces may simply have tables listing the Mobile Network Identities (part of ITS) and the corresponding PISN and PINX numbers for each MNI. In this way, the messages are routed to a right SwMI at the PSS1 level. If the called party has migrated in a visited SwMI, the correct PISN or PINX number may be obtained based on information in the HDB (if calling from home SwMI of the called
3. TETRA Inter-System Interface

3.1.5 Remote Operations Service Element and Segmentation Service Element

Remote Operations Service Element (ROSE) is a protocol standardised by ITU-T (recommendation X.229). It is a protocol supporting communication of concurrent interactive applications in a distributed open systems environment, that means, to distinct between the simultaneous connections related to different users. The interactions are modelled as Remote Operations. For the information transfer, the ETSI ISI standards mainly utilise one of the four ROSE service types, namely ROSE INVOKE Application Protocol Data Unit (APDU). Furthermore, a ROSE RESULT APDU is used for ending the information exchange between ANFs, ROSE ERROR APDU is used in certain error situations and ROSE REJECT APDU is used in case of for example invalid parameters in ROSE APDUs. [28], [10]

The ROSE APDU is encapsulated in the PSS1 Facility Information Element. This way, the five ANF entities utilise the services of ROSE to convey PDUs through the PISN. If the ROSE APDU exceeds its possible maximum length inside the Facility IE, it can be segmented by a Segmentation Service Element (SSE). The ROSE APDU is thus transparently transported in spite of its length. SSE is a TETRA specific way for segmenting ROSE APDUs, and is not based on any other standard. However, it must be noted that the segmentation is allowed only for ROSE APDUs inside FACILITY messages. Inside all other PSS1 call messages, the ROSE APDUs must remain unsegmented. Thus, when opening the PSS1 connection, lengthy ROSE APDUs may have to wait for transportation until the PSS1 FACILITY message can be sent. [10]

There is also an optional way to perform segmentation, and it is implemented (if present) in the PSS1 layer of the protocol stack. It means, that for example a FACILITY message user, the maximum length of the message is several times greater than the largest message that actually can be transmitted. This is achieved by, transparently to the user, segmenting the FACILITY message at the PSS1 layer before actually sending it.

The co-ordination function in Figure 13 simply co-ordinates information delivery between ANFs, GFT control, ROSE and SSE. For example, it delivers PDU from the Facility IE to a destination entity, either ROSE or SSE if the ROSE APDU was segmented. Additionally, if a received ROSE INVOKE APDU was addressed to an ANF which is not present in the SwMI, the ROSE entity is requested to generate a ROSE REJECT APDU by the co-ordinating function. In this case, the co-ordination function also most commonly clears the connection. [10]

In the ETSI TETRA standard, a ROSE APDU Argument named "TetralsiMessage" is defined using Abstract Syntax Notation 1 (ASN.1). It is also defined that the ROSE APDUs are encoded using ASN.1 Basic Encoding Rules (BER). [10]

Now, the series of encapsulations performed on the ANF-ISI PDU, the actual TETRA proprietary information in the ISI, can be reviewed. A clarifying example of this encapsulation process with a PSS1 SETUP message can be found in 0. At the lowest level, the PSS1 message contains a Facility Information Element. Now, in the "Service APDU" field of this Information Element, a ROSE INVOKE APDU is encapsulated. In case the ROSE INVOKE APDU needs segmentation, the SSE segment is put in "Service APDU" field instead of the whole ROSE APDU. [10]

Now, in the ROSE INVOKE APDU, inside field "Argument" resides the "TetralsiMessage". The "TetralsiMessage" includes three fields: "destinationEntity", "originEntity" and "options". [10]
3. TETRA Inter-System Interface

identifying the destination ANF for the information, "sourceEntity" for source ANF for the information and "TetraMessage" containing the actual ANF-ISI PDU, that means, the highest level TETRA proprietary information that is then interpreted by the corresponding ANF entity. [10]

3.1.6 ISI call setup with call related TETRA proprietary information

An actual PSS1 call with a speech communication capability is set up, when either a normal TETRA Individual Call or Group Call is in question. Now, because the call signalling contains also TETRA proprietary information, Facility Information Elements are included in some of the basic call messages. The messages allowing this inclusion of proprietary information are the following: SETUP, ALERTING, CONNECT and DISCONNECT. [22]

During the call, more TETRA proprietary information related to the call in question can be transmitted using a FACILITY message. The originating SwMI can send FACILITY after it has sent CALL PROCEEDING, and the called SwMI can send FACILITY after it has received a FACILITY or ALERTING message. As an example, the signalling flow of TETRA ISI Individual Call setup and release is presented in Figure 14.

Figure 14. TETRA ISI Individual Call setup and release [21], [11].
3. TETRA Inter-System Interface

3.1.7 Establishing of a call independent signalling connection

A PSS1 call independent, connection oriented signalling connection is set up, when information related to Short Data Service, Mobility Management or TETRA Supplementary Services must be transferred. The standards define, that a new signalling connection may be opened every time or an existing signalling connection may be utilised when some information related to previously mentioned ANFs must be sent. However, in order to avoid unnecessary signalling on D-channel, an existing connection should be utilised as much as possible. In this case, only FACILITY messages are required for the TETRA proprietary information. [10]

After being set up, this signalling connection is utilised for transferring TETRA proprietary information through the ISI. However, this proprietary information can already be included in SETUP and CONNECT messages. This way, the information is transmitted as soon as possible from the source ANF entity to the destination ANF entity. In the following figure (Figure 15), the establishing a call independent signalling connection with a TETRA Mobility Management message exchange is presented. This signalling takes place when a subscriber migrates from one SwMI to another. Figure also presents the clearing of this call independent connection. In the figure, also ROSE level transactions are depicted to highlight the use of ROSE RESULT APDU when ending the TETRA ISI level signalling procedure. [22], [13]

![Figure 15. TETRA Mobility Management (migration) message exchange [22], [13].](image)

3.2 Additional Network Feature for Mobility Management

The ETSI ISI standards part covering the ANF-ISIMM is very wide, including several services related to Mobility Management. Some of them are mandatory and some are optional when implementing the ANF-ISIMM in the SwMI. Also, the ANF-ISIMM includes some services related to group attachment. These services are mandatory only if also the ANF-ISIGC is implemented in the SwMI. All of the ANF-ISIMM services utilise the call independent signalling connection (as described in chapter 3.1.7) for transferring information between the ANF-ISIMM entities.
The migration service is used, when the subscriber migrates to any visited SwMI. The subscriber information in the Home Database (for location tracking purposes) is updated. In addition, a new Visitor Database record and the mapping between ITSI and VATSI is created. The migration service also supports call restoration when the individual subscriber migrates during an Individual Call or a Group Call. [13]

A different service, Removal of Subscriber Information (RSI) service is invoked, if a previous visited SwMI exists for the migrating subscriber. After the migration is done, the RSI service performs the removal of the subscriber's profile (the VDB record) and the mapping between ITSI and VATSI from the VDB. Also, the Visitor Authentication Centre (VAC) record is removed, if any exists. The authentication over ISI is explained later in this chapter. [13]

A separate service from RSI, de-registration, is used when the migrated user indicates that he wants to de-register from the SwMI. This is done most commonly when the power of MT is turned off when in a foreign network. Now, when compared to the RSI service, exactly the same information is removed from the VDB. Also the information in the HDB is updated. The user has to register again using the migration service, to be able to communicate in the visited SwMI. [13]

Two separate profile update services are provided. The first one is the basic migration profile update service, and the second one is Supplementary Service profile update service. Both are optional. In both cases when service is invoked, the home SwMI updates the subscriber (or group) profile in the visited SwMI. [13]

The authentication service enables the visited SwMI to authenticate the migrated individual subscriber. In addition, it enables the individual subscriber to authenticate the SwMI; actually in this case the home SwMI is authenticated because the authentication parameters originate from there. When the authentication service is invoked, the visited SwMI fetches the needed session authentication key (KS), the Random Seed (RS) and their validity time from the home SwMI. It must be noted, that if the authentication of the infrastructure is in question, the visited SwMI fetches KS' which is separate from KS. Then, the visited SwMI uses these parameters to authenticate the subscriber, to let the subscriber authenticate the home SwMI or to perform authentication both ways. As a result, a Derived Cipher Key for encrypted communication in the visited SwMI is obtained. [13]

The authentication of a migrated subscriber (when performed) must be carried out simultaneously with the migration itself. When the migration request is sent from the visited SwMI to the home SwMI, it is indicated that also authentication service is invoked for the subscriber. Now, the home SwMI does not update subscribers location in the HDB before it has received an indication about a successful authentication. The reason for this is to avoid updating the subscriber information in case of a malicious intruder. [13]

Also, an Over The Air Re-keying (OTAR) service for a migrated subscriber is optionally provided. It is used for assigning and delivering Static Cipher Keys (the keys mainly used when the MT is communicating in Direct Mode Operation). The service includes two possibilities: the first one is that the SCKs can be delivered to the individual subscriber straight from the home SwMI. If this is the case, they are delivered in sealed form to subscriber and the visited SwMI can not utilise them in any way. Another possibility is that the SCK creating parameters are brought to the Visitor Authentication Centre from the Home Authentication Centre, and the SCKs are created in the visited SwMI. [13]

For faulty situations, Individual and Group subscriber Database Recovery (IDR and GDR) services are provided. They are mandatory services which can be invoked after a system, database or connection close-down, or after any occurrence which can make
the information in a database erroneous. Service can be invoked to restore the information about individual subscribers or groups either in the HDB or the VDB. After the invocation of the service, the SwMI in question fetches the information from another SwMI to make the databases consistent again. [13]

Related to Group Calls, a group attachment and a group detachment service is provided. They support the extension of Group Calls across the ISI, and are closely related to the ANF-ISIGC. The attachment of a migrated subscriber can be done in two ways. The visited SwMI invokes the service to the home SwMI in case of a migrating subscriber requesting to be attached to a group. The home SwMI can also invoke service when a subscriber (or a dispatcher) in the home SwMI wants a migrating subscriber in the visited SwMI to be attached. As a part of this group attachment service, the visited SwMI creates the migration profile (and optionally the SS profile) of the group in the VDB. The profile is saved in VDB until the last person of the group in the visited SwMI requests detachment service. [13]

Furthermore, an optional group linking and unlinking service is provided. Group linking means simply joining groups together in the way that when a Group Call is invoked in one of the groups, it automatically extends to all groups. When the group linking is invoked for some groups, one SwMI will act as a linking controlling SwMI for this linking service. It is a home SwMI for at least one of the groups to be linked together. Similarly, the linking controlling SwMI co-ordinates the group unlinking service when it is invoked. [13]

3.3 Additional Network Feature for Individual Call

Basically, ANF-ISIIC enables a normal point to point call to be established from one SwMI to another SwMI. Additionally (as described in chapter 3.1.6), ANF-ISIIC allows any TETRA signalling information related to this Individual Call to be passed from SwMI to another SwMI. In addition, ANF-ISIIC participates in call restoration when a user has migrated to another TETRA network during a call.

A few new concepts are brought up, when dealing with Individual Call over ISI. When a subscriber in SwMI A calls to a subscriber in SwMI B, the latter can possibly have migrated to another SwMI C, without SwMI A knowing it. Now, depending on the ANF mode of operation, this call must be forward switched (passed through SwMI B) or re-routed (straight to SwMI C from SwMI A). Additionally, a specific scenario related to call re-routing exists when the called subscriber has migrated to SwMI A, without call control knowing it. Now, the ISI call is cleared for the purpose of avoiding a trombone connection, and a new intra-SwMI call is established. [11]

ANF-ISIIC has to deal with speech item distribution in a semi-duplex call: when other participant releases the PTT button, information is sent to the other participant that he has the right to begin transmitting. As previously said, the ANF-ISIIC also participates in call restoration when a user migrates. When requested by the call control application, the ANF-ISIIC entity puts the ongoing call on hold for the time of the migration. After this, a new connection to the SwMI where the user is migrating to is created, and the call is restored after the user has successfully migrated. Thus, the call is now routed through the old SwMI until the call is cleared. [11]

3.4 Additional Network Feature for Group Call

ANF-ISIGC enables point to multipoint calls to be set up between TETRA users located in several SwMIs. The calls are set up through the ISI as described in chapter 3.1.6, and after the call setup TETRA proprietary information can be transmitted.

The Group Calls are invoked only for members of the same group. This means that in order for a subscriber to be able to participate in a Group Call, a group attachment
service of ANF-ISIMM must first be performed for that subscriber. When a subscriber makes a request for Group Call setup, the originating SwMI analyses the subscriber profile of the subscriber to find out if the caller belongs to the group. If this is the case, an ANF-ISIGC entity is invoked. [1]

When a Group Call is requested for, there are separate cases in which the ANF-ISIGC is invoked. The first one is that the caller is currently in the home SwMI of the group, but at least one of the group members has migrated to a visited SwMI. Another possibility is that the caller has migrated into a visited SwMI when performing the request for a Group Call. An even more complex case is reached when several groups in different SwMIs are linked together. In this case, the ANF-ISIGC invoke request must be forwarded to the linking controlling SwMI of these groups, which shall then take care of the Group Call establishment. [12]

After the ANF-ISIGC has been invoked, the originating and the participating SwMIs check whether resources (Air Interface and infrastructure resources) necessary for the Group Call exist. If the answer is positive, needed resources are reserved. If a participating SwMI can not allocate resources for the Group Call, it informs the controlling SwMI of the Group Call about the situation. Now, the controlling SwMI makes a decision if the Group Call is set up as a partial Group Call, or if it is completely cleared. [12]

Another possibility is that a participating SwMI can delay its inclusion in the Group Call. In this case, it informs the controlling SwMI about the situation and waits for the needed resources to be available. The delaying SwMI can only wait for a certain period of time, otherwise it is totally dropped out of the Group Call. When the resources are available, the delaying SwMI proceeds with the call set up, and the subscribers join the call using a late entry service. [12]

During the Group Call, call restoration is performed for a migrating user in the same way as with an Individual Call. However, if in the old SwMI of the subscriber still some other subscribers remain engaged in the same Group Call, the ISI call connection must not be cleared between the controlling SwMI and the old SwMI. Similarly, if in the new SwMI where the subscriber is migrating to, already are members engaged in the same Group Call, no need exists for a new ISI connection. [12]

When in a Group Call, there is always additional TETRA proprietary information that must be sent to participants of the call. This information has mainly to do with the speech item distribution, or in other words, subscriber transmission control. Messages are constantly sent informing that a subscriber has ceased transmitting, that a subscriber has requested his turn to transmit and that the permission to transmit has been granted to a subscriber. Also in case that the resources are needed elsewhere, information is sent that the transmission is temporarily withdrawn, as well as the information that the resources are available and the transmission is continued. [12]

3.5 TETRA Packet Data Protocol between networks

A possibility of transferring TETRA packet data between TETRA SwMIs is still unstandardised in ETSI. However, a concept of IP Interworking (IPI) between TETRA networks has been proposed by Nokia to enable transferring of packet data between TETRA SwMIs. A draft of these ISI/IPI related issues has recently been sent to ETSI, which will most probably consider standardising PDP between TETRA SwMIs to some extent.

Basically, IPI means that TETRA PDP services can be used also in other than the home SwMI of the subscriber. A user can activate the PDP context, then migrate to another SwMI and the PDP connection with the IP based services can be restored. The IPI concept is based on the future PDP solution implemented using GPRS adopted
3. TETRA Inter-System Interface

GGSN and GTP (this was presented in chapter 2.6.4). In the following figure (Figure 16), the IPI reference model is presented.

![Figure 16. TETRA IPI reference model [42].](image)

In this reference model, the standard ISI is used for Mobility Management between the SwMIs and a GPRS adopted interface, Gp, is used for routing IP datagrams between TETRA IP backbones. The packets are tunneled using GTP, and pass through Border Gateways (BG) which provide some security functions for the IP backbones. In the following figure (Figure 17), an experimental signalling example of a migrating PDP user is presented. The migration happens from a previous visited SwMI to a visited SwMI.

![Figure 17. Migration with an active PDP context [42].](image)
During the first four steps in Figure 17, the actual migration from the viewpoint of ANF-ISIMM is performed. It includes registration to the visited SwMI, database update in the home SwMI and Removal of Subscriber Information from the previous visited SwMI. However, some new parameters related to the PDP and GPRS must now be obtained to visited SwMI during step 2: Access Point Name (APN) of the GGSN, IMSI of the subscriber, IP address (if the TE has a static IP address) and some Quality of Service parameters (if present). [42]

The fifth message, SN-Migrate PDP Context Demand, is a new TETRA Packet Data Protocol message that is still to be defined. Its purpose is to send status information about currently active PDP contexts to the visited SwMI. The message also informs about NSAPIs in use. Now, in step 6, the visited SwMI sends with GTP a PDP context request to the previous visited SwMI to get all the necessary information related to PDP contexts. In step 6, the visited SwMI also sends its IP address to be able to receive packets. In step 7, the previous visited SwMI acknowledges with PDP context information (including a Tunnel ID related to GTP). [42]

Now, in step 8, when the previous visited SwMI receives tunneled IP datagrams belonging to the PDP contexts of the migrated subscriber, it sends them forward. In step 9, the actual Update PDP Context Request is sent to GGSN for permanently rerouting the datagrams. The request includes the IP address of the visited SwMI and the related TIDs. Now, the GGSN updates its IP address information of the TETRA SwMI (corresponding to SGSN address) and acknowledges the request. [42]

Now, the visited SwMI sends a message to the previous visited SwMI for removing its PDP context information, and the message is acknowledged (steps 11 and 12). After this, the visited SwMI creates the new PDP context entries. A new TETRA PDP message is still needed to Air Interface for informing the TE about the successful packet data connection restoration in the visited SwMI. Now, the exchange of IP datagrams can go on using the same IP addresses as before migration. [42]

There are some new issues that need to be defined before an implementation of this IP Interworking scenario is possible. In addition to adopting the new GTP messages to TETRA, the two new Al messages (steps 5 and 13 in Figure 17) have to be defined and standardised, as well as the new PDP related parameters inside the standardised TETRA Mobility Management messages in step 2 of the figure.
4. TETRA ISI OVER IP

4.1 Voice over IP protocols

4.1.1 Shortcomings in underlying IP protocol suite

The Internet Protocol (IP) suite is nowadays the keyword when interconnecting all kinds of computers or even telecommunications devices. It is a network layer protocol, roughly corresponding to layer three of OSI model. Its main strengths lie in the fact that IP data is totally transparent to the underlying network hardware and technology. Physically, the data path can be a copper wire or an optical fibre. In addition, there are many options for lower layer technologies. To name a few, it can be ATM, Frame Relay or Ethernet.

IP is a packet switching protocol for routing IP packets, passing through several routers, to the final destination. IP is connectionless, in the sense that no connection is set up on a per-flow basis. In the routers, routing tables define the right direction for the packets based on the IP destination address. Also a conversion between IP destination address and a corresponding layer two address must be made.

IP offers an unreliable service; IP datagrams can get lost. Also, the datagrams can arrive out of order. For these reasons, two alternate protocols, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), are used on top of IP. These protocols work on transport layer (layer four) of OSI stack.

TCP, first of all, provides sequence numbering for packets. It guarantees that the contents of the packets will not go to application layers out of order. TCP provides a connection oriented data transfer for IP packets by establishing a data flow between communicating entities. The data flow is established between two IP addresses and ports related to both addresses. Port is an abstraction for maintaining simultaneous data flows for different applications. Furthermore, TCP provides error control (possible retransmission) for IP packets and congestion control by decreasing and increasing the transmission frequency.

UDP, on the other hand, offers very little functionality on top of IP. It provides only for ports and thus multiplexed connections between the source and the destination, and an optional checksum over transmitted data for detecting possible errors. Thus, UDP is a connectionless service and has no retransmission mechanism.

All of the IP protocols have originally been designed for data communications only with no real-time or telecommunications requirements in mind whatsoever. Thus there are some issues that have to be dealt with when these protocols are utilised for real-time information, and some additional protocols are obviously needed on top of these protocols.

The basic problem with real-time information and IP is the fact that every real-time data flow has some kind of requirement for average bandwidth and maximum delay in order to perform a successful communication. However, in IP networks no Quality of Service is automatically guaranteed. These issues are dealt with more precisely in chapter 4.1.3. Furthermore, packets arriving out of order can be a problem for real-time applications. This can happen if packets are routed through different paths to destination.

With TCP, one of the properties not suitable for real-time applications is the connection establishment, which is performed as a three way handshake procedure. First, the connection establisher sends a TCP SYN packet to the destination. The destination replies with SYN and ACK packets, and after this the original source replies with an ACK. When expressed with a relative time measure round trip (a time from message...
4. TETRA ISI over IP

sending to receiving an acknowledgement), the connection establishment takes a time of 1.5 round trips. UDP, being connectionless, has an advantage in this sense.

Another property of TCP which makes it non-suitable for real-time information is the retransmission in case of errors or missing packets; this can cause too long a delay. Generally, TCP is more appropriate for transferring non real-time unicast data, which requires a reliable delivery. In telecommunications, this means signalling information and data.

UDP, being lightweight and simple, is more applicable for transferring real-time information. It does not add any extra delay into the real-time stream which is crucial when for example a speech call is in question. Until now, TCP has been much more widely used in the Internet than UDP. However, this gap will become smaller in the near future when the real-time applications gain more popularity.

4.1.2 Real-time Transport Protocol

Real-time Transport Protocol (RTP) is a protocol defined by Internet Engineering Task Force (IETF). Protocol specification is presented in RFC 1889, and a newer version is already published as an Internet draft being soon an obsoleting RFC.

Purpose of RTP is to provide some end-to-end delivery services for the real-time information itself. It is utilised by both leading Voice over IP standards, H.323 and Session Initiation Protocol (SIP). RTP has a companion protocol, Real-Time Control Protocol (RTCP) for monitoring Quality of Service. Both protocols are run on top of UDP. RTP (and RTCP) is most commonly integrated into the upper layers of the end applications rather than being implemented as a separate layer in the communications protocol stack. [43]

An RTP session is defined by an IP destination address and a separate UDP destination port for RTP and RTCP packets. These port numbers are always consecutive so that an even port number is assigned to RTP stream and the next higher odd port number is assigned for RTCP information. RTP can be used in both unicast and multicast scenarios. With speech, one RTP session to each direction is adequate for successful communication, but for example when both video and audio are concerned, two sessions for each participant are needed. [43], [3]

In order to tailor RTP according to a particular application's needs, two additional components are needed. First, a RTP payload format specification is needed for the audio or video encoding in question. They are published as additional separate RFCs for each encoding. In these documents, it is presented how a particular payload is to be carried using RTP. [3]

In addition, a profile specification document is needed where a set of all payload type codes (to be used in RTP header) are defined for one class of applications. The application profile specification can also define some additional fields to be appended into RTP and RTCP header or the security mechanisms to be supported by that class of applications. For example, the main profile for audio and video applications can be found from the accompanying RFC 1890 (a newer version is already published as an Internet draft). When a new application is taken into use, an existing profile should be extended rather than making a separate profile. This facilitates interoperation among applications. [43]

The RTP packet header includes a sequence number for detecting missing packets and placing them in correct order at the receiving side. The sender chooses at random a certain sequence number for the first packet, and the number is then incremented by one for each packet. The packet header also has a timestamp, which however is most commonly used in the same way as sequence number; it is always incremented by one
and does not express any absolute time. The timestamp then only tells the receiver to play the packets out with even intervals. [3]

In addition, the RTP header includes a Synchronisation Source (SSRC) identifier. It is a randomly chosen unique value identifying a transmitter of the information during one RTP session. Also, a Contributing Source (CSRC) list must be included if mixing is performed for the real-time information stream. It identifies all the contributors in the SSRC real-time stream in question. Other fields in the header are RTP version field (V), padding field (P) indicating if payload includes padding, extension (X) field indicating if header is followed by an extension, CSRC count field (CC) indicating number of CSRCs, marker (M) field for profile specific use and a payload type (PT) field for defining the payload. The header is presented in Figure 18. [3]

When RTP is utilised also the accompanying protocol, RTCP, must be present. As already mentioned, its primary use is transmitting Quality of Service information about the RTP connection. RTCP control packets are sent periodically to all participants of the RTP session. RTCP packets are multiplexed with RTP data packets by simply taking advantage of different port numbers provided by underlying UDP. [3]

The Quality of Service information sent consists of figures like packet loss rate, cumulative packet loss, delay and jitter. Accordingly, the sender can make use of this information and adapt the transmission rate or the encoding scheme used. The procedure aims in maximising the quality of real-time data at the receiving end. In addition to these flow and congestion control functions, this information can be very useful in diagnosing faults and determining whether the problem is local or global. [43]

An additional function of RTCP is conveying a canonical name and other user information (CNAME) of a participant to other participants in the session. CNAME is of format 'user® host' and it is unique for one physical participant in a session. It is useful for example in cases where a sender generates multiple data streams with different SSRCs. Other information includes user name, which is used by applications for listing the participants of the session. Also, email address and phone number can be included in RTCP packets. [3]

Furthermore, RTCP can be used in multicast sessions to determine the total number of participants. This is important when the number of participants increases: the bandwidth taken by RTCP messages must be kept on an acceptable level. [3]

The two main RTCP packet types are Receiver Report (RR) and Sender Report (SR). The RR packet is sent periodically by participants that only receive information and do not send it. The Sender Report (SR) is utilised by sending participants. Both of these packets are sent to all participants in a session, and include QoS information for control purposes described above. Furthermore, the Source Description (SDES) packet is

---

**Figure 18. RTP packet header [43].**

<table>
<thead>
<tr>
<th>Bytes</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>7</th>
<th>8</th>
<th>15</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>V</td>
<td>P</td>
<td>X</td>
<td>CC</td>
<td>M</td>
<td>PT</td>
<td>Sequence number</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Timestamp**
- **SSRC**
- **CSRC**
  - (another CSRC)
periodically sent by data sending participants for expressing CNAME and other user information of the source. [3]

Other RTCP packet types are BYE packet and Application (APP) packet. The BYE packet is sent by a source who wishes to indicate that it is no longer active. It can be sent for example when one source does not anymore contribute to mixed stream having several CSRCs. The Application packet can be used for experimental application specific purposes. [3]

The security of RTP and RTCP can be achieved at lower layers (IP security issues are dealt with in chapter 4.2). However, RFC 1889 describes some alternate security methods to be used at RTP level. For achieving confidentiality, the RTP packets can be encrypted using Data Encryption Standard (DES) algorithm in Cipher Block Chaining (CBC) mode. However, also other algorithms can be used. Using other algorithms is preferable because DES is too weak for any professional use. Furthermore, RTP profiles can be used to define additional RTP payloads including encrypted application level data. [43]

4.1.3 Quality of Service in IP networks

As previously mentioned, IP datagram delivery is traditionally best-effort and thus not suitable for real-time data. Only exception is a case where network load is guaranteed to be low enough for the whole path from source to receiver. This can be the case only in a private and isolated intranet, and certainly not in the Internet. Hence, most commonly an adequate network dimensioning with some kind of service differentiation among different data flows is required.

A basic problem with VoIP is a possibility of network congestion because of UDP packets. Most of the traffic has previously been over TCP, which has a congestion control mechanism providing each data flow for fair share of bandwidth. Now, when the UDP traffic increases, TCP data flows can be forced to back off their transmission and TCP users are left without proper QoS. With VoIP, this is a problem for signalling which usually runs on top of TCP. This problem can, however, be addressed using QoS aware routers guaranteeing TCP traffic a configurable share of the bandwidth. [3]

Another basic issue when trying to achieve guaranteed QoS is keeping the size of sent IP datagrams below the Maximum Transfer Unit (MTU) of the network on the data path. This can be done by using a path MTU discovery mechanism beforehand. Namely, if routers receive datagrams that are too big, the datagrams are fragmented. Now, the headers of higher protocol layers are present only in the first fragment, and this is unwanted because many QoS techniques partially rely on information present in those headers. [3]

A simple method for achieving QoS is using the Type of Service (TOS) field standardised in IPv4 header. Three bits in the header express coarse grained control of service, and indicate whether the packet has a preference for low delay, high throughput or high reliability. The other three bits are for fine grained control, and express priority. These precedence bits were originally standardised for service differentiation among data flows. Unfortunately, most legacy routes ignore all of the TOS bits totally. However, most of the voice-aware up-to-date routers by the major vendors take these bits into account if desired. [3]

In practice, some more advanced methods for achieving QoS over IP are often needed. Such methods are Resource Reservation Protocol (RSVP), IETF Integrated Services (IntServ), IETF Differentiated Services (DiffServ or DS) and the latest trend in IP QoS and routing, Multiprotocol Label Switching (MPLS). These all are briefly dealt with in the rest of this chapter.
RSVP is a reservation protocol for reserving resources along the route which the underlying routing protocol has chosen. RSVP is defined in RFC 2205, and it is originally designed to be used joint with IETF Integrated Services. Every reservation made by RSVP applies to packets of exactly one communications session. RSVP identifies the session by combination of a destination address, transport layer protocol and destination port number. The RFC defines that RSVP messages are encapsulated directly into IP datagrams, much the same way like Internet control protocol or other management protocols. [5]

The reservation creation process is roughly the following: firstly, when the source begins to send data, it also begins sending RSVP Path messages to the destination. These messages "mark" the path of the IP datagrams belonging to the session. Furthermore, these messages (when reaching their destination) inform the receiver of path and sender characteristics. The actual reservation is made from receiver to source; when possessing the necessary information for making the reservation, the receiver can make a reservation attempt with a RSVP Resv message. This message traverses the whole path hop-by-hop trying to establish a reservation, and a successful reservation is acknowledged with a ResvConf message. Afterwards, the reservation can be cancelled with a ResvTear message and the path marking correspondingly removed with a PathTear message. [5]

The IETF Integrated Services include two service classes, which (if supported by the routers) can provide the data flow with certain QoS commitments. Two IntServ QoS classes are currently defined: Controlled-Load Service (RFC 2211) and Guaranteed Service (RFC 2212). The Controlled-Load Service class provides the data session a service equivalent to best-effort in a lightly loaded network, and the service quality does not decrease even though the network load increases. The Guaranteed Service class provides a firmer service quality: an assured level of bandwidth, a certain end-to-end delay bound and no queuing loss for the packets.

RSVP is used joint with Integrated Services by passing the IntServ class QoS request to the routers with RSVP. After the Path message (sent by source and including some initial parameters), the actual reservation is sent with Resv message by the receiver, containing the Integrated Services class that is wanted to be invoked and needed parameters for setting up the end-to-end commitment for the data session. Thus, the QoS classes are programmable on a per-session basis and the exact service they provide depend on the parameters sent by the receiving end. Now, the Resv message traverses the path hop-by-hop, and these parameters joint with Path initial parameters define the reservation and QoS state in the router for that session. [47]

A newer, and perhaps even more actual means to achieve QoS over IP is IETF Differentiated Services. The DS architecture is defined in RFC 2475, providing for a simple and coarse-grained QoS method in the core network. DS differs from IntServ in the sense that it does not deal with individual sessions and data flows, but with traffic aggregates, that means, collections of data flows to which similar QoS needs apply.

For DS, two Per Hop Behaviours (PHB) have been defined: Assured Forwarding (AF) and Expedited Forwarding (EF). The PHBs are means for routers to accomplish the wanted QoS level. The packets are classified and marked with a code value at the ingress (edge) router of the DS domain, which is the part of the network where DS compliant routers are present. The IETF has defined that in IPv4 header the DS field expressing the QoS level for routers replaces the standard TOS field, implying that there are exactly six bits of space to express the wished quality level. [4]

The Assured Forwarding PHB has four service classes, and three dropping precedence levels for each. Thus there are twelve predefined code values which map to AF PHB in a router. With AF, the router primarily handles the packets based on the chosen service class, and if the class traffic is congested, secondarily based on the
dropping precedence. Thus the probability for packets with low dropping precedence to get discarded is higher than for packets with high dropping precedence. [4]

The Expedited Forwarding PHB provides even more guarantees to transfer: low loss, latency and jitter with an assured bandwidth. EF PHB is not compulsory to be implemented in DS routers, but when in use, exactly one predefined code value maps to EF in routers. EF appears to the utilising endpoints like a virtual leased line: it guarantees that the minimum departure rate of EF packets is always greater than the arrival rate, or in other words, that no queues are present for EF packets. [4]

A topic closely related to DS, Multiprotocol Label Switching (MPLS), is newly defined by IETF and is not yet published as an RFC. It is a means for accelerating routing in IP networks, and means that the switching is done only based on data link layer or MPLS additional header information, label, and upper layers are left without examination in switches. MPLS can be used with several data link layer technologies (for example Frame Relay, ATM or Ethernet). Most commonly, however, the underlying technology is ATM.

The MPLS enhanced routing process is as follows: on the edge of MPLS network, IP datagram is examined and the packet is assigned a data link layer label. At subsequent hops, no IP routing table is used. An another table is used instead, giving (based on the label) a next hop data link layer address and a new label for the packet. The old label is replaced with the new label before sending the packet further to the next hop. As mentioned, the label can either be present in the data link layer protocol header or in an additional MPLS header which is placed between the network layer header and the data link layer header. The first choice is obviously better for switch speed and functional simplicity causes. [41]

The information about existing labels and their contexts, that means, information about new labels and data link layer addresses for packets has to be conveyed between MPLS capable switches. This transferring of information is done either by request or on automated basis. For this purpose, either a previously existing protocol (for example RSVP), or a totally new protocol, Label Distribution Protocol (LDP) is used. [41]

This label based switching offers many benefits: the ingress router which labels the packets, can determine the label based on also other information than IP destination address. It can, for example, label packets with different IP port numbers differently. Also, distinct ingress routers can assign different labels to similar packets, causing a different routing depending on source. Even a behaviour similar to IP source routing can be achieved, by a special label which maps to one specific path. Most obvious advantage with MPLS, however, is the increased speed for the routing process as the IP layer is left totally uninspected. [41]

Furthermore, a way of bringing the Differentiated Services QoS assurance into MPLS networks has been described in an IETF draft. For MPLS switches, the DS code values in IP header defining the QoS are not visible. Thus, the DS code values must be either brought to the data link layer header or the additional MPLS header, or they must be deduced from labels by other means. The document specifies procedures which utilise both of these methods: firstly, the incoming label value now means for switches also the wanted DS treatment in routers in addition with the physical next hop of the IP packet. Secondly, more fine grained DS information, like drop probability, can be conveyed with ATM header field Cell Loss Priority (CLP) or MPLS header EXP field. It must be noted, however, that the treatment information deduced from labels must correspond to defined DS PHB descriptions. [35]

The MPLS packet forwarding process is now slightly different when also DS is involved. Firstly, the MPLS label of the packet and the data link or MPLS additional header additional information are examined. Based on both of these, a correct
4. TETRA ISI over IP

treatment is given to the received packet. Now, a new label and a next hop data link layer address is defined, and the new label is encoded into ATM header or an additional header. Additionally, extensions to LDP for conveying also DS information with the labels are defined. [35]

As a summary, it can be said that many IP QoS techniques have been defined, and their interoperability has mostly been thought of. Unfortunately, the implementations for them are mostly in test phase, and lots of research and larger scale implementation result analysis work is still ahead. However, the current methods seem to be able to bring adequate help to future QoS problems with VoIP.

4.1.4 H.323 protocol suite and network elements

H.323 is a Voice over IP standard developed by ITU-T. It is the first complete VoIP standard published, and is still under constant development. It is developed for an IP network with no QoS guarantees, but naturally deployment of QoS means enhances H.323 performance. The H.323 itself is a so-called umbrella standard, which refers to other ITU-T standards. These other standards documents are mainly H.225.0 and H.245. However, the whole suite of protocols is named H.323 for simplicity. Below, the basic elements of an H.323 system are introduced.

Terminal

A H.323 terminal is the communicating endpoint on the network. The H.323 standards define that the audio communication capability of a terminal is mandatory, whereas video and data capability is optional.

Gatekeeper (GK)

A gatekeeper is not a mandatory part of an H.323 system, but when present, it performs some important call control and other functions. Firstly, GK performs the address translation (for a terminal or a gateway) from a LAN alias address to an IP address. A LAN alias address is a method for addressing a terminal, and it can be a telephone number of an email address. GK adds an entry to the translation table when a terminal registers to a GK announcing its alias address. An alias address is unique within a H.323 zone, which is controlled by exactly one GK. [26]

An optional function of a GK is bandwidth management. It may reject calls from a terminal due to bandwidth limitations, for example high network load. Optionally, also authorisation may be performed with a GK. Furthermore, GK can participate in call signalling so that the H.225 channel and H.245 control channel messages pass through the GK. [26]

Gateway (GW)

A gateway is an optional part of a H.323 system, but when present, it allows the H.323 system to interoperate with other telecommunications systems. Most likely, these other systems are ISDN or PSTN networks. [3]

Protocol stack

The H.323 protocol stack of an audio terminal is depicted in Figure 19, and the purpose of each block is explained below.
4. TETRA ISI over IP

<table>
<thead>
<tr>
<th>Audio application</th>
<th>Terminal control and management</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.7xx speech codec</td>
<td>RTCP RAS terminal to gatekeeper signalling H.225 call signalling H.245 control channel</td>
</tr>
<tr>
<td>RTP</td>
<td>UDP TCP IP</td>
</tr>
</tbody>
</table>

Figure 19. H.323 Protocol stack [23].

Registration, Admission and Status (RAS) channel

RAS channel is used mainly for gatekeeper discovery, terminal registration and address translation purposes, but also for admission and bandwidth request purposes. Gatekeeper discovery process begins by sending (using multicast and a well-known port) a Gatekeeper Request (GRQ) RAS message. A GK acknowledges this by sending a Gatekeeper Confirmation (GCF) or a Gatekeeper Reject (GRJ) message. Similarly, terminal registration is performed (to a well-known port) with a Registration Request (RRQ) and a Registration Confirm (RCF) or a Registration Reject (RRJ) messages. Address translation, admission and bandwidth change requests are handled with similar procedures by the GK. [23], [26]

H.225 call signalling channel

The H.225 call signalling channel is used to setting up a call. The H.225 channel messages are a subset of ITU-T Q.931 (ISDN) messages. The H.225 standard specifies, which Q.931 messages are mandatory to be implemented in an H.323 system and which are optional. Setting up a H.323 call somewhat resembles an ISDN call setup, and is depicted as a whole later in this chapter. The H.225 channel has a well-known TCP port which the caller uses when contacting the called party. In these call setup messages, a TCP port for the forthcoming H.245 control channel is agreed with, and the H.225 channel can be closed as soon as the H.245 channel is set up. However, it may be left open: standard defines a way to encapsulate H.245 messages inside Q.931 messages. When this "H.245 channel tunneling" is used, no separate channel needs to be opened for H.245 messages. [26]

H.245 control channel

The main procedures made using the H.245 control channel are terminal capability exchange, master/slave determination (concerning multipoint conference calls) and RTP/RTCP setup information exchange. With terminal capability exchange, terminals announce to each other which voice (or other) codecs they support. Once this has been done, a codec is agreed with and both terminals announce the UDP ports to which they want to receive RTP and RTCP packets. [26]
4. TETRA ISI over IP

Call setup signalling

Now, if a gatekeeper is present the H.225 channel and H.245 control channel signalling can either go straight from an endpoint to another endpoint, via only one gatekeeper or all of the signalling can be routed via both gatekeepers. As an example, in the following figure (Figure 20) a signalling chart for a successful call set-up is presented. The example depicts routing via both gatekeepers.

[Diagram]

Figure 20. Gatekeeper routed H.323 call setup [26].

In the example, first the calling endpoint sends a RAS Admission Request (ARQ) to its own gatekeeper (GK1). After this, GK1 multicasts a RAS Location Request (LRQ) message to find out the IP address of the other gatekeeper (GK2). Now, GK2 acknowledges with Location Confirmation (LCF) containing the IP address of GK2, and GK1 acknowledges to calling endpoint with Admission Confirmation (ACF). However, the steps two and three (LRQ and LCF) are unnecessary if the GK1 knows IP address of GK2 beforehand. It can for example deduce it (after step one) from IP address of the called endpoint. [26]

Now, all signalling is ready to be routed via both gatekeepers. Calling endpoint sends Q.931 SETUP message via gatekeepers to the other endpoint, and the other endpoint responds with CALL PROCEEDING. After the other endpoint has also been granted admission, it continues call setup signalling by sending an ALERTING message and eventually a CONNECT message. After this, the H.225 signalling channel may be closed, and H.245 control channel signalling begins. This signalling can also be routed via gatekeepers if wished. Finally, sending of RTP and RTCP packets begins. [26]
As can be found out from the above presentation of a H.323 connect procedure, the call setup is quite complex and requires a lot of signalling. The setup takes several round trips, even if the RAS admission messages are neglected. Furthermore, for a complete message exchange depiction for call setup, the TCP handshake messages and H.245 control channel messages should be added in Figure 20. However, a fast call setup can be a crucial factor for some VoIP applications, and thus some enhancements have been presented to signalling for reducing the call setup time.

The most commonly used enhancement for speeding up call setup is the H.323 fast connect procedure presented in the ITU-T H.323 basic document. It is a procedure for establishing a basic point-to-point call with minimal message exchange. It also makes separate H.245 control channel messages unnecessary: after this signalling, the real-time data over RTP can immediately be delivered. Call setup with the fast connect procedure is presented in Figure 21.

![Figure 21. H.323 call setup with fast connect procedure [26].](image)

First, the same RAS signalling as in Figure 20 takes place. Like in the previous example, GK1 can however get to know the IP address of GK2 by using some other method: in this case, the messages LRQ and LCF are not needed. Now, the calling endpoint sends a SETUP message, containing an indication about invocation of the fast connect procedure. The SETUP message furthermore includes a list of proposed channels for the real-time (RTP) information exchange, properties (for example, used voice codecs) for each of these channels and an RTCP channel to be used. [26]

After the called endpoint has received the SETUP message, it chooses an appropriate RTP channel with its properties from the list that was included in SETUP. Now, after the RAS admission procedure, the called endpoint can already begin sending real-time information, and it must be noted that the calling endpoint must be prepared to receive real-time information on any of the channels it proposed. Finally, the called endpoint sends a message back indicating the acceptance of fast call setup. This message can either be CALL PROCEEDING, PROGRESS, ALERTING or CONNECT. CONNECT is used in this example. [26]

In addition to the fast connect procedure, another enhancement has been defined in document H.323 Annex E for accelerating the call setup. It is the use of UDP instead of TCP for call signalling. It includes a concept of a reliable UDP transport, which in practice means acknowledging the received UDP datagrams. A retransmission is made if a transport level acknowledgement is not received within a certain time. When this UDP based call setup is used joint with the fast connect procedure, the call setup is...
4. TETRA ISI over IP

exactly the same as in Figure 21. The only difference is that the preceding TCP handshake procedure is not required and time of one round trip between the endpoints is eliminated. [25]

4.1.5 Session Initiation Protocol (SIP) suite and network elements

SIP is a Voice over IP protocol defined by IETF. As H.323 can be said to be very telecom oriented, SIP is completely a product of the Internet community. The main document defining SIP is RFC 2543, but also many additional Internet drafts are presented which will be added to the standard later. Furthermore, a closely related document is RFC 2327, which presents the Session Description Protocol (SDP). SDP is a protocol for describing properties of a real-time session. The SIP protocol stack for an audio application is depicted in Figure 22.

![SIP protocol stack](image)

Figure 22. SIP protocol stack [19].

As can be seen from Figure 22, both UDP and TCP have been included in the figure as transport layer protocols for SIP: they are optional so that only one or both of them may be supported by the SIP implementation. RTP with UDP is used as the protocol for real-time data. In the case of UDP as the SIP transport layer protocol, SIP has its built-in reliability mechanisms for datagram delivery. This reliability is achieved by sending the SIP request again, and every time doubling the interval between the transmissions and continuing sending until a certain amount of repeated transmissions have been made. The transmissions cease when an appropriate SIP acknowledgement is received. [19]

The SIP addressing scheme is similar to the one with emails: SIP addresses are of form user@host, where the user name can be a name or a telephone number, and the host name can either be a domain name or an IP address. Thus a SIP address for a person can even actually be the same as his email address. When establishing a SIP connection, if the host name portion is a domain name, a Domain Name System (DNS) server must be used to obtain the corresponding IP address. [3]

When SIP is used, some SIP specific network elements are included. Firstly, two optional servers for call routing exist: a proxy server and a redirect server. They can physically be the same server, but that server acts either as a proxy server or a redirect server when the SIP connection is set up. Furthermore, a SIP location server exists which is always contacted by a proxy server or a redirect server. The location server has the knowledge about where in the Internet a SIP called party is located at that moment, thus being responsible for the user mobility support that SIP provides. [19]
A proxy server functions in such way that all call related messages pass through it. It hides a possible new temporary SIP address of a person (that was obtained from the location server) so that the caller always just contacts the proxy server with the original SIP address. A redirect server is contacted only once, and it returns the user's possible new SIP address to the caller after having asked it from the location server. Whenever a user changes its location, it informs its new location to a proxy or redirect server by using the SIP REGISTER method. This way, the location server keeps its information up to date. In the next example (Figure 23), a SIP connection establishment in the case of a proxy server is presented. [3]

**Figure 23. SIP connection establishment with a proxy server [19].**

Here, the caller begins to set up a call with SIP INVITE method. The proxy server accepts the request and asks the location server for the current location of the user. After having received the reply, it forwards the call setup request to the right address. Now, the called party returns a 200 OK success indication which is forwarded to the caller. Finally, this is acknowledged with SIP ACK method. It must be noted that the location query to location server by proxy server is not done using SIP signalling: the protocol is left unspecified. [19]

As can already be seen, SIP somewhat resembles Hypertext Transfer Protocol (HTTP). SIP is text-based, and it has several methods to be used with SIP requests. It also has status codes to be used in responses, and they are mostly inherited from HTTP version 1.1. In the following figure (Figure 24), SIP request message structure is presented. The headers are of variable size, because SIP is text-based. The general and request (or response) headers have pre-defined fields, some of which are optional. [19]

**Figure 24. SIP request message structure [3].**

The request line contains the used SIP method, SIP address of the person the request is sent to and the SIP protocol version used. The general header part includes fields like Via (SIP proxies that have been on the path of the message), From and To (source and destination SIP addresses), Call-ID (unique ID for the call) and CSeq (sequence number for the request). Furthermore, the request header part includes fields like Subject, Content-Type and Content-Length. Entity header part, if present, can include some meta information for message body. [3]
The message body often includes some additional information in Session Description Protocol (SDP) format. This way, the SIP caller negotiates with the called party about the parameters concerning the SIP session: these parameters are for example the used voice codecs, required bandwidth and ports for the RTP real-time data stream. In a simple case, the caller sends information about codecs it supports and RTP port it wants to use in the initial INVITE request. The called party chooses which ones of these codecs it is willing to accept, and sends this information together with its RTP port back to the caller in the response 200 OK. [19]

4. IP security

4.2 IPsec introduction

Security Architecture for IP (IPsec) is a means defined by IETF for achieving an adequate basic security level in all IP based networks. The standard is defined in several RFCs (numbered 2401-2412). The security means defined in these RFCs are planned to form a fixed part of the forthcoming IPv6, but by implementing a subset of these features these means can be adopted to IPv4. The basic idea with IPsec is that the traffic is encrypted at IP layer, making the encryption totally transparent for the upper layers and the users of applications. [33]

The IPsec architecture covers all of the most important sectors of network security. Among other things, these include access control, connectionless integrity, data origin authentication, protection against replays and confidentiality with encryption. For achieving these goals, IPsec standards define two security protocols, Authentication Header (AH) and Encapsulating Security Payload (ESP). They are dealt with more precisely in following chapters 4.2.2 and 4.2.3. Also a key management mechanism, Internet Key Exchange (IKE), is defined (dealt with in chapter 4.2.4). Furthermore, IPsec standard covers some authentication and encryption algorithms and other additional components of IPsec architecture. [33]

When IPsec is used, the granularity at which the security services are offered can be configured. Between two security gateways (IPsec enhanced network elements), for example all traffic can be encrypted or a separate encrypted tunnel can be opened for each TCP connection between these gateways. [33]

A very relevant concept related to IPsec is a Security Association (SA). It is a definition of one unidirectional connection (or a connectionless path) and the IPsec security protocol that is used for that connection. Thus, a typical bi-directional communication would require two Security Associations. The SA is a triple consisting of an IP destination address, security protocol used (AH or ESP) and a Security Parameter Index (SPI) uniquely identifying the SA. The SAs are maintained in Security Association Databases (SAD), which exist in every IPsec enhanced host or a security gateway. [33]

Furthermore, two kinds of SAs exist, one for IPsec transport mode and one for tunnel mode. The first means that traffic is always encrypted at the source host and decrypted at the destination host, whereas the latter means that data is encrypted between certain network elements (hosts, routers or firewalls) in the network. [33]

4.2.2 Authentication Header (AH) and used algorithms

The simpler one of the two IPsec protocols is the Authentication Header (AH). The use of it guarantees two security aspects: connectionless data integrity and data origin authentication. Also an optional protection against replays is provided. However, AH can be said to give less security guarantees than the other IPsec protocol ESP. [31]

The integrity and authentication are provided by the AH, which is a header placed in the datagram immediately after IP header. The IP payload then follows the AH. When
the IPsec source sends the datagram to be authenticated, it calculates a checksum over the IP payload, immutable fields of the IP header and the AH header (excluding the checksum itself). Furthermore, this checksum is calculated as a function of a session key. This procedure is made for authentication at datagram destination. Now, when datagram arrives at destination similar procedures are made, and integrity check and authentication are thus performed. [31]

The optional protection against replay is performed with a sequence number in the AH followingly: every time the source sends a packet, it increments the counter. However, if the counter has reached its maximum value, a new packet for that Security Association must not be sent. Instead, a new SA is created for that connection, and datagram sending may continue. [31]

The algorithms used for authentication can be defined on a SA basis. However, the IPsec standard requires two authentication algorithms to be present with an AH implementation. The first of them is a HMAC-MD5-96 (Hashed Message Authentication Code – Message Digest 5), developed by R. Rivest. It operates on 64-byte blocks of data, takes a 128-bit key and produces a 128-bit authenticator value. The first 96 bits of this are included in AH, and the receiver compares his result with this stored value. The other algorithm is HMAC-SHA-1-96 (Secure Hash Algorithm). It works in exactly similar way, except a 160-bit authenticator value is produced with a 160-bit key. From the value, 96 bits are again compared. [36], [37]

4.2.3 Encapsulating Security Payload (ESP) and used algorithms

Encapsulating Security Payload (ESP) is the more comprehensive one of the IPsec protocols, and ensures confidentiality, data origin authentication, connectionless integrity and an optional anti-replay service. Thus ESP includes the same security guarantees as AH, and leaves the use of a separate AH unnecessary when the ESP confidentiality feature is needed. [32]

When ESP is used, an ESP header is inserted between the IP header and the IP payload data. However, also some additional information is inserted at the end of the datagram. The structure of an ESP encrypted datagram is depicted in Figure 25, and explained below. [32]

![Figure 25. An encrypted IP datagram [32].](image)

When IPsec enhanced source sends a datagram using ESP method, firstly it encrypts the original payload and the ESP trailer using the session key. ESP trailer includes necessary padding for the encryption algorithm, padding length information and an identifier for the payload protocol (most commonly TCP or UDP). After this, an explicit Initialisation Vector (if any exists) for the encryption algorithm is inserted as plaintext at the beginning of the payload field. The ESP header field includes Security Parameters Index identifying the SA and a sequence number for the optional anti-replay feature. Now, if authentication is also used, a checksum is calculated (as a function of the session key) over ESP header, payload and ESP trailer, and placed at the end of the IP datagram. [32]
4. TETRA ISI over IP

IPsec standard defines that the algorithm used for encryption can be variable, but DES in Cipher Block Chaining (CBC) mode is mandatory to be implemented with ESP protocol. With DES in CBC mode, a 64-bit Initialisation Vector affects to the first block of data in the encryption/decryption process, and after that the previous block always affects to the next block. This way the data is more protected. However, one has to bear in mind that DES is quite a weak encryption method nowadays, and that for higher security for example triple DES can (and should) be used.

4.2.4 Internet Key Exchange (IKE)

The Internet Key Exchange (IKE) is a mechanism of IPsec for a scalable and automated creation and management of Security Associations (SA). This includes the exchange of the session key information. The actual protocol used for the SA creation and key management is called Internet Security Association and Key Management Protocol (ISAKMP). [20]

The IPsec SA is established with ISAKMP in a two-phase process. In the first phase, a secure way to create the IPsec SA is agreed with. Here, the parties authenticate each other using either signatures, public keys or pre-shared keys, and as a result have a secure communication channel for the actual SA creation and key information exchange. In the second phase, the parties communicate using encrypted messages and exchange the key material, and finally create the SAs for IPsec. After this, the parties can begin transmitting IP datagrams using IPsec AH or ESP protocols. [20]

4.2.5 Additional H.323 security

ITU-T has separately defined some security mechanisms for H.323, and they are presented in document H.235. These mechanisms can be considered alternative to IPsec: if the security of all H.323 related connections is dealt with already at lower level, no need exists for repeating the same procedures at the H.323 level. As an alternative to IPsec, H.235 proposes the use Transport Layer Security (TLS) as the underlying security technology. [24]

First of all, H.235 provides a framework for authentication of the H.323 communicating parties. The authentication procedure takes place on the H.245 control channel, and four options for performing the authentication are provided. The key for encrypted real-time data (RTP) communications can either be obtained as a result of authentication, or it can be negotiated on the H.245 control channel as an extension to the existing H.323 capability exchange. [24]

The first option is a Diffie-Hellman exchange with optional authentication, and at the end of the procedure the communicating parties have a shared secret key along with a chosen algorithm for a secure media channel communication. The second option is an authentication with symmetric encryption based on previously known ID and password, third option is the same than second but with additional hashing, and the final option is certificate-based authentication with signatures. As a result of these authentication procedures or other negotiation a key for encrypted communication on the real-time data (RTP) channel is obtained. If re-keying is wished later, it can be done via the H.245 channel. [24]

4.2.6 Additional SIP security

Also for SIP, security mechanisms have been defined. They are presented in the basic SIP document RFC 2543. They address all of the most important aspects of security: confidentiality, integrity, authorisation and access control. All of these rely on using an asymmetric (public-key) mechanism. The standard does not enforce using any particular system, but recommends Pretty Good Privacy (PGP). As with H.323, the
4. TETRA ISI over IP

security of SIP connection can as well be ensured on lower layers of the protocol stack (with IPsec or TLS). [19]

The confidentiality of SIP messages is assured with PGP end-to-end encryption. At SIP message sending, the sending party encrypts most of the message with the recipient's public key. The parts that are left clear are some header fields that need to be processed by SIP proxy and redirection servers. These unencrypted fields are right in the beginning of the SIP message, after which the encrypted header fields and message body follow. The recipient can now decrypt the message using his private PGP key. [19]

The message integrity and access control is addressed with PGP authentication using digital signatures. When the SIP message is sent, some of the header fields and the entire payload is signed with the private PGP key of the sending party. The resulting signature is inserted in SIP header "Authorization" field. The fields preceding this field are not signed because they are mutable, whereas all of the fields after the "Authorization" and the payload are included in the signature. Now, the recipient can authenticate the sending party with public key of the sender. At the same time, the message integrity is checked: the signature includes a hash value calculated from fields that were signed. [19]

These procedures provide firm security guarantees for SIP messages. Both, authentication and encryption, can be used simultaneously. It must be noted that in this case message must be encrypted before it is signed, and at the receiving end, the signature is checked before decrypting the message. [19]

4.3 TETRA ISI over H.323 signalling

In this chapter, a possible ISI implementation utilising H.323 protocol suite is considered. It includes the use of H.323 specific network elements and mapping them to the TETRA world. It must be noted that there are also other possibilities to implement ISI over H.323 signalling; this one is presented because the solution is as analogous as possible with the existing ETSI standards. This will most probably facilitate later possible standardisation and implementation work regarding this issue.

4.3.1 Network architecture

This solution is based on mapping the functionality of a H.323 gatekeeper (GK) to a DXT residing at the edge of a TETRA network infrastructure. The Inter-System Interface thus means in the H.323 sense communication between two gatekeepers, and the signalling conforms to the gatekeeper routed model. The network architecture is depicted in Figure 26.
4. TETRA ISI over IP

It must be noted that the TETRA network infrastructure itself is here circuit switched like the current Nokia TETRA System, but the DXT at the edge of the network performs outwards all required tasks of a H.323 GK hiding the internal implementation of the TETRA network infrastructure. It also means, that a "H.323 terminal" does not actually exist. However, the DXT at the edge of the network hides also this fact from the outside world, mapping the concept of a H.323 terminal to the TETRA internal concept Mobile Terminal. Furthermore, a development path for the future still exists: if the TETRA network infrastructure itself will also be run over IP, the GK location will clearly remain the same.

Furthermore, this solution requires that in addition to the H.323 signalling the RTP traffic is routed via the DXT. Also following must be stated at this point: as this solution concentrates on protocols and signalling between two TETRA networks, it is presumed that the actual speech over RTP is maintained in TETRA internal ACELP format. To fully conform to the H.323 standard this requires that TETRA codec is accepted as an official codec for H.323.

Another option (which will be quite probable when also other than TETRA networks are connected to the IP backbone) is that the speech encoding is changed into an universal format at the edge of the TETRA network. However, the transcoding of speech increases propagation delay, which is unfavourable.

As already said, the IP connection terminates at the edge of TETRA network infrastructure. Each GK has a unique IP address, and because each TETRA network can have several GK/DXTs, every TETRA network can have several IP addresses. Now, when gatekeepers are involved, H.323 standards define that alias addresses can be used to address a called H.323 subscriber: with H.323 the receiving GK then performs the mapping from the alias address to the IP address of the individual subscriber. In this case, IP addresses are clearly not used inside network infrastructure. The TETRA ITSI is used all the way at the H.323 level to address the called subscriber in a H.323 call.

However, in case of a call independent signalling connection, an existing connection may be utilised, and the destination of the information flow is not always a TETRA subscriber. Thus, a general purpose number (not corresponding to any TETRA subscriber) attached with the correct MNI is used. Now, for routing the datagrams to a right SwMI, every GK/DXT only has tables consisting of destination MNIs and corresponding IP destination addresses. Several IP addresses can correspond to a MNI, and the GK/DXT can choose one randomly or by some other method. [26]
4.3.2 Protocol model utilising H.450.1

Resembling the standardised ETSI ISI over QSIG, this solution is based on using Generic Functional Protocol (GFP) on top of the H.323 for additional functionality. GFP for H.323 is defined in document H.450.1, and it is somewhat analogous to the one defined in document ISO/IEC 11582 (GFP for PSS1). The protocol model for ISI over H.323 is presented in Figure 27, and the blocks that differ when compared to Figure 13 (chapter 3.1.2) are explained below.

![Diagram of protocol model of ISI over H.323.]

**H.450.1 provides means for transporting Application Protocol Data Units (APDUs) inside H.323 call messages. For TETRA, this means the standard ISI call control messages that have to be transmitted from one infrastructure to another. Even though the basic principle is the same, there are some differences when the solution is compared with QSIG GFP: H.450.1 defines that the user proprietary information is encapsulated in User-to-User Information Elements, not Facility IEs. [27]**

Furthermore, H.450.1 defines that the user proprietary information is at the upper level encapsulated inside Remote Operations (ROS) APDU, which then is placed into the User-to-User IE. ROS is presented in ITU-T document X.880; the document is only a revision of the original ITU-T ROSE document X.229. ROSE was presented in chapter 3.1.5, and ROS has the same functionality: it is a protocol for performing distinct concurrent interactions between two applications. [29]

Other blocks in Figure 27 have similar functionality to the ETSI ISI case. A Segmentation Service Element (SSE) is required with H.323 as well: the H.450.1 defines a maximum length for the user proprietary data and the MTU in IP networks furthermore regulates the size of the H.323 message.

The H.323 standards state that the user proprietary data residing in the User-to-User IE is defined using ASN.1. A notable difference to the ETSI ISI standard however is that the ASN.1 must be encoded using a variant of Packed Encoding Rules (PER). It
produces a more packed representation for the data than BER, but the use of it also implies that a certain parameter inside the ASN.1 structure can not be pinpointed by knowing a bit position.

As an example, Appendix B presents the encapsulation of TETRA proprietary data for Individual Call into a H.323 (H.225) SETUP message. As can be seen from the table, User-to-User IE in SETUP has a complementary part "Setup UUIE" which includes some additional information related to the SETUP message. Secondly, the User-to-User IE includes the actual user proprietary data, which is in this case a H.450.1 Supplementary Service APDU. Now, in the Service APDU field of the latter resides the ROS Invoke APDU, and the Argument of that includes the actual TETRA ISI message.

4.3.3 ISI call setup over H.323

An actual H.323 call is set up when the ISI is utilised by Individual Call (ANF-ISIIC) or Group Call (ANF-ISIGC) entities. The call setup is based on H.323 fast connect procedure presented in chapter 4.1.4. The motivation for choosing fast connect procedure here instead of basic call setup procedure is very evident: the basic call setup is complicated and in case of TETRA, fast call setup time is very crucial. However, either one of the transport protocols can be used with this scheme: TCP provides built-in reliability whereas UDP based setup with reliability mechanism (H.323 Annex E) is appropriate if the setup time is wished to be further reduced.

The TETRA ISI Individual Call or Group Call setup naturally also includes the need for sending the TETRA proprietary information. This type of information can be sent already in the User-to-User IEs of the two call setup messages, and when the actual real-time data (RTP) channel is established, the TETRA proprietary information can be transmitted in the User-to-User IEs of the H.323 FACILITY messages. It must be noted that also the RELEASE COMPLETE message is allowed to include TETRA proprietary information. As an example, call setup and release of a TETRA ISI Individual Call is depicted in Figure 28.

![Diagram](image_url)

**Figure 28. ISI Individual Call setup and release over H.323 [26], [11].**
In the SETUP and CONNECT messages, both DXT/GKs inform each other about the IP address and UDP port that they wish to use for receiving the RTP and RTCP packets. To identify the H.323 call, a unique call identifier is present in the SETUP message, and the same value follows unchanged in all subsequent H.323 signalling messages.

As already presented in chapter 4.1.2, for speech a separate RTP session is opened in both directions. Both of these sessions have a unique Synchronisation Source (SSRC) identifier which remains unchanged throughout the sessions. Now, both DXT/GKs have to keep track of the H.323 call identifier, and its relation to the Synchronisation Source (SSRC) identifiers of the two RTP sessions related to the call. Additionally, the port that is used for receiving and transmitting RTP packets for these SSRCs has to be memorised.

4.3.4 Establishing of call independent signalling connection over H.323

The call independent H.323 signalling connection is set up, when the ISI is utilised by Mobility Management (ANF-ISIMM), Short Data Service (ANF-ISISD) or Supplementary Service (ANF-ISISS) entities. For the call independent signalling connection, no separate RTP connections are needed.

The same applies here than for the presentation of ETSI ISI solution: to avoid unnecessary signalling, an existing call independent connection should be re-utilised for the messages from the ANF entities. Utilising of an existing connection is feasible especially with IP, because no need exists for sharing the signalling load between PCM lines and opening new signalling connections for that reason.

In addition to FACILITY, the TETRA proprietary information can be present in the SETUP, CONNECT and RELEASE COMPLETE messages. In the following examples, TETRA migration Mobility Management message exchange is presented. Figure 29 presents the message exchange when opening and closing a call independent signalling connection, whereas Figure 30 present the message exchange utilising an existing connection. In these figures, also ROS level transactions are presented for emphasising the ending of a TETRA level signalling transaction with a ROS ReturnResult APDU.

![Diagram of TETRA Mobility Management (migration) message exchange over H.323: opening and closing the connection](image-url)

Figure 29. TETRA Mobility Management (migration) message exchange over H.323: opening and closing the connection [26], [13].
4. TETRA ISI over IP

DXT/GK 1:
FACILITY (ROS Invoke: ISI-Migration PDU)

DXT/GK 2:
FACILITY (ROS Invoke: ISI-Migration Response PDU)

FACILITY (ROS ReturnResult)

Figure 30. TETRA Mobility Management (migration) message exchange over H.323: utilising an existing connection [27], [13].

4.4 TETRA ISI over SIP

In this chapter, a possibility of ISI over SIP signalling is considered. As SIP is a product of the Internet community whereas QSIG and H.323 originate from telecommunications world, it places some more challenges for adapting the signalling into the IP environment. However, again the existing ETSI ISI standards are considered as basis for the scheme in what comes to upper level TETRA signalling itself.

4.4.1 Network architecture

Network architecture is based on model which maps the functionality of a SIP Proxy server to the DXT at the edge of TETRA network infrastructure. This choice has not been made only for the fact that the DXT at the edge of the network works as a proxy forwarding the signalling further to TETRA network, but also again for the possible future development path towards an all-IP-solution. The solution is presented in Figure 31.

Figure 31. TETRA ISI over SIP.

For the TETRA SwMIs, same applies than for the H.323 based solution: they are still circuit switched. Thus the DXT functions as a SIP proxy only towards the IP backbone, hiding the circuit switched TETRA network. Before a connection over ISI is formed, information about a TETRA subscriber in TETRA HDB is in some cases utilised. However, the HDB can not be considered a SIP Location server, because the mobility management is dealt with at the TETRA level. Due to this, separate mobility management and Location server with SIP is unnecessary.
4. TETRA ISI over IP

In addition to the signalling, also the actual real-time data passes through the DXT, which conceptually functions both as a Media Gateway and as a Media Gateway Controller. For the real-time RTP speech in TETRA format, the TETRA ACELP coded speech has to be registered as a new Multipurpose Internet Mail Extensions (MIME) type.

The addressing scheme is in this case somewhat similar when compared to the H.323 case. Each TETRA SwMI has a unique IP address for routing both SIP and RTP traffic. As was presented in chapter 4.1.5 SIP addresses are of form user@host: in the TETRA ISI case, for a TETRA call the user portion is the ITSI/GTSI of the TETRA subscriber or in case of a call independent signalling connection a general purpose identifier attached with a correct MNI. The host portion is always the IP address of destination SwMI in numerical form. Thus for routing at the IP level, the DXT only has to know correspondences between MNIs and the IP addresses of the SwMIs.

4.4.2 Altered protocol model

The protocol model is based on using SIP as the underlying ISI call protocol and encapsulating the TETRA proprietary information inside SIP message bodies. This information can be included in all SIP messages. Furthermore, SIP INFO method is utilised for sending TETRA proprietary information when a SIP session has already been established.

The use of the INFO method can be considered analogous to the use of FACILITY message with H.323 or QSIG. It is a means to transparently send application level information without changing the properties of the SIP session. INFO method is a newly proposed extension to SIP by IETF, and will be part of the SIP standard. However, for the time being, the use of the INFO method is described in an IETF draft. [7]

Furthermore, Remote Operations (ROS) and Segmentation Service Element (SSE) are required also in the SIP ISI case. The first is needed for uniquely identifying and distincting TETRA application level transactions, whereas the latter is required for avoiding the IP level fragmentation by keeping the size of the datagram below the MTU of the network. The protocol model for ISI over SIP is presented in Figure 32.
4.4.3 SIP messages with TETRA proprietary information

As already stated in chapter 4.1.5, SIP messages are completely text-based. Headers are in textual format as well as the message body which, if exists, is presented with Session Description Language. SDP is registered as a MIME type in IETF. Now, if TETRA information is included, also MIME types for the two possible TETRA related types which are transported over SIP, ROS and TETRA-SSE, must be registered. These TETRA related MIME types must be of binary form, that means, the TETRA proprietary information is encoded octet by octet inside SIP message.

Furthermore, if TETRA proprietary information is wanted to be included in the message body of all SIP messages, some of the messages must contain a MIME multipart payload because also SDP information must be present if properties for RTP channel are negotiated. MIME multipart means simply that the message body consists of several elements, each possibly being of a different MIME type. An example of TETRA proprietary information encoded in a SIP INVITE message is presented in Appendix C. The actual TETRA proprietary information is in binary form, but it includes exactly the same information than the ROS Invoke in Appendix B.

4.4.4 ISI call setup over SIP

An actual SIP speech call is set up, when a TETRA Individual Call or Group Call needs to be established over the ISI. As already described, the actual SIP connection over ISI is made between two SIP proxies: thus the destination IP address in all SIP messages is the same as the "Via" field identifying the SIP Proxy that this message will pass through. The call establishment and release follow the normal SIP call setup procedure, and TETRA proprietary information can be included in all SIP messages.

In addition, any number of SIP INFO messages can be sent in either direction for sending additional TETRA proprietary information. After having received a SIP INFO request, DXT acknowledges it by sending a 200 OK message. For avoiding...
unnecessary signalling, TETRA proprietary information can be included also in these 200 OK messages. As an example, TETRA ISI Individual Call setup and release over SIP is presented in Figure 33.

![Diagram of ISI Individual Call setup and release over SIP](image)

**Figure 33. ISI Individual Call setup and release over SIP [19], [11].**

When an ISI call is set up, the SwMI which the call is originating from assigns a unique Call-ID value which is present in the SIP INVITE message and remains unchanged in rest of the messages. Now, concerning every SIP call over ISI, the DXT must keep track of the relation of this Call-ID to the two SSRC values identifying the related RTP sessions. Furthermore, the RTP/RTCP ports that are agreed on during the capability exchange in INVITE and 200 OK messages must be bound to the corresponding Call-ID and SSRC identifiers.

### 4.4.5 Establishing of call independent signalling connection over SIP

A call independent signalling connection over SIP is utilised for transferring Mobility Management, Short Data Service or TETRA Supplementary Service information. The SIP standard itself does not define a concept of call independent signalling connection, but the protocol can as well be used without opening the RTP connections for speech.

To avoid unnecessary signalling, the same applies than for H.323 based solution: an existing connection should always be utilised to avoid unnecessary signalling for creating and ending the SIP session. In the following examples (Figure 34 and 35), TETRA ISI migration Mobility Management signalling exchange is presented. The first example presents the migration with setup and release of a SIP signalling connection whereas the second example presents migration utilising an existing SIP connection. Again, also ROS level transactions are presented for emphasising the ending of TETRA level signalling transaction.
4. TETRA ISI over IP

DXT/SIP Proxy 1: DXT/SIP Proxy 2:

INVITE (ROS Invoke: ISI-Migration PDU)

200 OK (ROS Invoke: ISI-Migration Response PDU)

ACK (ROS ReturnResult)

BYE

200 OK

Figure 34. TETRA Mobility Management (migration) message exchange over SIP: opening and closing the connection [19], [13].

INFO (ROS Invoke: ISI-Migration PDU)

200 OK (ROS Invoke: ISI-Migration Response PDU)

INFO (ROS ReturnResult)

200 OK

Figure 35. TETRA Mobility Management (migration) message exchange over SIP: utilising an existing connection [13].

The SIP messages for call independent connection differ from the ones for the SIP call in the sense that they never contain a SDP part in their message bodies. This is due to the fact that an RTP channel does not need to be opened and thus properties are not negotiated. The structure of the messages thus becomes more simple: the message bodies always contain only the TETRA proprietary information, and MIME multipart message bodies are not needed.

4.5 Comparison of H.323 and SIP based solutions

4.5.1 Comparison of these protocols in general

Making a thorough comparison between H.323 and SIP is a very complicated task, and includes consideration of several aspects. The comparison is furthermore aggravated by missing real-world implementations and thorough traffic tests between systems. This especially applies to SIP.

The advantages of H.323 lie in the fact that it is already proven to be a working and quite stable standard, and it has been under development already for five years. There are several third-party vendors from which H.323 terminal implementations and protocol stack components can be purchased: for example the widely used Microsoft
Netmeeting relies on H.323 standard. An additional advantage for H.323 is good interoperability with traditional telephony standards as H.323 is derived from them, as well as full backward compatibility to previous H.323 versions.

However, the worst disadvantages of H.323 originate from the fact that it is telecom oriented. The protocol is very complex, the protocol stack is heavy and hard to implement and the protocol specification is spread to several large documents. The implementation is made difficult also by the binary ASN.1 PER encoding of the H.323 messages: a special parser is required to process them. Finally, standardisation process of H.323 related issues in ITU is stiff and makes fast adoption of new ideas difficult.

SIP, on the other hand, is designed from a totally different viewpoint. Because the specifications are published by IETF, SIP can be said to be very Internet oriented: it is designed with no legacy from old telecommunications protocols. Adoption of new issues to SIP is easier than with H.323: it follows the normal IETF process where the paper is first published as a draft, and later possibly as an RFC. The protocol itself is light and simple, and can be easily implemented. It is also text based, which makes parsing of messages very easy, and there are only a few simple request message types. The responses to the requests are previously known to web oriented people being the same as with HTTP.

A clear advantage for SIP when compared to H.323 (and QSIG) is also the fact that the size of signalling messages is not limited in any way by the standard. Naturally, the MTU of the IP network places some limits to packet size at a lower level but these limits are totally transparent to SIP. With SIP, the Segmentation Service Element (SSE) can thus even become unnecessary if regulation of the size of signalling messages is not wished.

SIP has a number of disadvantages as well: the protocol is very new, and the first (and so far only) RFC was published in 1999. Lots of features have been added since and published as IETF drafts. However, there are still some open and unsolved issues, and thus the standard can be said to be somewhat unfinished.

Finally, call setup delays for both H.323 and SIP are examined. For simplifying the presentation, it is presumed that these messages are exchanged directly between endpoints. However, in the signalling sense, they can as well be H.323 GKs or SIP Proxies. Furthermore, a UDP based call setup is considered for both protocols. However, a TCP based call setup differs for both SIP and H.323 cases only by time of one round trip (RTT): with TCP, the caller first sends SYN, the called party replies with SYN/ACK and the first H.323 or SIP message can be sent immediately after the caller has sent the final TCP ACK message. Message exchanges for both H.323 and SIP are presented in Figure 36.
4. TETRA ISI over IP

Figure 36. Fast H.323 and SIP call setup. [25], [19].

As can be seen from the left part of Figure 36, with H.323 over UDP and with Fast connect procedure the audio from the called party can reach the caller as soon as within one Round Trip Time (RTT) from sending of first message, and the audio from caller to called party goes through in 1.5 RTT. With SIP over UDP, the audio from caller reaches called party in 1.5 RTT, and audio from called party reaches the caller in 2 RTT. It can thus be seen that times for H.323 and SIP are almost identical, H.323 being slightly faster.

4.5.2 Suitability of these protocols to TETRA ISI

For TETRA ISI call setup and signalling, two of the most important properties are fast connection setup and reliability. Reliability with IP can easily be achieved by using TCP, but this increases connection setup time. The problem with connection setup time is however most commonly present only with Individual Call and Group Call and not with call independent signalling connection. This is due to reuse of an existing H.323 or SIP signalling connection: only a FACILITY or INFO over an existing connection is needed to convey the information over the ISI.

For both H.323 and SIP, an UDP based fast call setup with additional reliability mechanisms has been defined. The retransmission mechanism is similar for both protocols: during the setup, if an acknowledgement to a message (H.323 SETUP, H.323 CONNECT, SIP INVITE or SIP 200 OK) is not received, the message is retransmitted after 500 milliseconds. After this, the interval is increased by a factor of 2 (SIP) or 2.1 (H.323). SIP stops doubling the interval after five messages and stops re-sending after seven messages, whereas H.323 stops re-sending after eight messages. [25], [19]

For H.323 the reliability is achieved by immediately acknowledging the sent H.323 call message with a transport level Ack message. This causes retransmissions to cease. The need for acknowledgement is announced in the sent H.323 message, and if the acknowledgement was wished for, application gives a command to the enhanced transport layer for sending it. [25]

With SIP, the reliability issue is taken care of with a provisional (1xx) or final (200) response, which is sent for INVITE and causes retransmissions to cease. In TETRA ISI case, sending a provisional response immediately upon arrival of INVITE is very much justified because the delay with call setup in TETRA SwMI. Namely, when a provisional response is not used and if call setup takes lots of time in SwMI, another INVITE is
sent because the retransmission timer. In addition, the called party retransmits message 200 OK if an ACK message is not received within a certain time. [19]

Additionally, the reliability mechanisms for H.323 and SIP over UDP differ to some extent from each other. With H.323, the mechanism described in Annex E is quite clear and similar to all H.323 messages whereas the definition of the mechanism with SIP is very obscure and mechanism is variable between different SIP messages. However, implementation for the H.323 case is more complicated because it requires some changes to the transport layer of the protocol stack.

Finally, setup times and signalling related to the TETRA ISI case are compared in the figure below. The consideration of setup times addresses only the ISI part, neglecting the time needed for call establishment within TETRA SwMIs. Furthermore, the optional TETRA PDU ISI-Setup Prolongation is not taken into account.

Figure 37. Comparison of TETRA ISI Individual Call setup signalling in ISI [26], [11], [19].

As can be seen from the sequences, with H.323 only five signalling messages are needed. With SIP, TETRA ISI call setup requires seven signalling messages to be sent. This is a slight advantage for H.323. When setup times are thought of, only one actual difference between these protocols can be found. With SIP, DXT/SIP Proxy 2 has to wait for ACK message before ISI-Alerting PDU can be sent whereas with H.323 the ISI-Alerting PDU can be sent immediately if wished.

However, in addition to the technical and other properties of the protocols, also trends and selections made elsewhere and inside Nokia largely affect to the selection of the protocol. Though working implementations have been over H.323 until now, SIP is very rapidly gaining popularity. In 2000, SIP was chosen as the Air Interface call control protocol for 3G mobile networks, and these kind of decisions may have a large impact on TETRA case. This is mainly due to reasons like future interoperability and a possible ease of implementation.
5. COMPARISON OF QSIG AND IP BASED SOLUTIONS IN ISI

5.1 General comparison

Generally, comparison between QSIG and IP based solutions means comparison between a circuit switched and a packet switched solution, and requires many aspects to be considered. Some tests with a simulated ISI and all of the related protocols would be required to make some final and complete conclusions, but as no test network could be built and no measurements were made, all considerations are based on theory and earlier knowledge of the author.

First of all, a circuit switched solution is not so well scalable as a packet switched solution. With a circuit switched solution, if more capacity is needed some (often leased) PCM lines must be acquired as well as more Exchange Terminals (ETs) must be added into the DXT. Problems especially appear if there is no space for additional ETs in the DXT. Furthermore, lots of configuration work related to the PCM lines is needed, which is a clear disadvantage. With a packet switched solution in DXT, changing the Ethernet card and buying some more bandwidth from the network owner is enough when more capacity is needed. Thus with a packet switched solution it is simpler and cheaper to add capacity.

Another problem with a circuit switched solution is that some load sharing must be performed between PCM lines. Furthermore, all B-channels of a certain PCM line can be already reserved when trying to make a call: in this case, an another PCM line must be used. With a packet switched solution, these kind of issues do not have to be considered and the implementation work is easier.

QSIG has some advantages and disadvantages. A clear advantage is its reliability and better suitability when interworking with TETRA as it originates from the telecommunications world. A QSIG PCM connection is, unlike IP network based solutions, originally designed for transferring speech.

However, from this fact originates one disadvantage of QSIG: for every 30 speech 13-channels in one PCM, only one D-channel for signalling is provided. Now, when also TETRA proprietary signalling without a related speech channel is concerned, the D-channels can get overloaded by heavy usage.

Another disadvantage is the fact that the current ETSI standards define that for every 64 kbit/s B-channel, only 8 kbit/s it utilised and the rest is left empty. This unnecessarily wastes resources. An option is however to include eight 8 kbit/s TETRA speech channels into one 64 kbit/s PCM B-channel, which makes use of resources more efficient. Nevertheless, this is also problematic because the use of D-channels further increases and this can raise difficulties. A problem with this solution is also that it unstandardised. It is mentioned in an ETSI TETRA standards document, but the QSIG standard does not support it.

The PCM lines can also be multiplexed and demultiplexed near DXTs so that B-channels from eight PCM lines are included into one PCM. Now the endpoints still conform to ETSI TETRA standard. However, the problem with this solution is that lots of multiplexers and demultiplexers are needed and lots of configuration work has to be done.

An advantage with IP is the fact that both TETRA signalling and TETRA speech are transferred in same IP payloads, instead of having a separate channel for signalling. This means that the amount of signalling compared to speech can be arbitrary and only the total amount of sent information matters from viewpoint of the network. However, QoS must be taken care of correctly for both signalling and speech. Another clear advantage for IP is that no resources are wasted because no speech channels need to
be reserved at all and especially because 88 percent of speech transferring capacity is not wasted unlike when implementing ISI with ETSI basic scheme.

Another advantage with IP based ISI is its close relation to TETRA IP packet data between TETRA networks (IPI). For TETRA signalling, speech and packet data, the same IP connection between TETRA networks can be utilised. This can be very well found out from Figure 16 in chapter 3.5. Thus, implementing also ISI over IP eliminates the need for two separate kinds of connections between TETRA networks. This may save considerable amount of money, as the networks may reside several thousand kilometers away from each other.

And finally, IP based ISI is a step towards the future in the sense of what the trends are today and what issues are today most commonly discussed in telecommunications and datacommunications standardisation areas. A good example of this is the 3G (UMTS) standards, which are currently developing and becoming more and more IP centric. This development may eventually lead to a joint network where all of the current standardised networks (for example GSM, TETRA and 3G) are equal parts providing somewhat different services. Furthermore, this scheme will most likely be built on top of IP. This clearly would imply that choosing of IP now reduces costs and implementation work in the future.

IP based solution has some disadvantages as well. One of them is the fact that when routing the information, the whole TETRA SwMI can not correspond to only one number like with QSIG and PISN numbers. Only the addressing scheme corresponding to QSIG PINX numbering can be used, and each ISI GW of the TETRA SwMI has a separate IP address.

Other disadvantages of IP have to do with Quality of Service problems in IP networks as well as the insufficient security in IP networks. In TETRA ISI case, however, the network can be very private in nature and not connected to any public IP network: this gives some security guarantees but does not prevent eavesdropping. To prevent QoS related problems, capacity must be carefully calculated in order to be prepared for traffic also at busy times. It is very important to include both call related and call unrelated traffic in these capacity calculations for getting a correct result.

In any case, depending on the exact situation, it can be necessary to address QoS and security issues with IP based ISI, and this need will most likely grow in the future. In the next chapter, combining of QoS and security issues with IP based ISI is examined. When these things are addressed, security with IP is at a better level than with QSIG and QoS can be extremely close to the one with QSIG.

5.2 Achieving security and QoS with IP based ISI

Security for IP based ISI is based on IPsec architecture presented in chapter 4.2. IPsec is chosen because it provides firm security guarantees at IP protocol layer and no additional mechanisms are needed for any of the used protocols. Security for both TETRA speech over RTP and signalling messages over FI.323 or QSIG can be provided at the same time, regardless of transport layer protocol.

In the private IP backbone connecting two or more TETRA SwMIs, a secure IPsec tunnel is formed for all inter TETRA SwMI connections. This tunnel is always formed for the connections when the endpoints of the connections (DXTs at the edge of SwMIs) start up and the secure tunnel stays unchanged after that. If one of these DXTs has to reboot itself, the tunnel has to be re-created.

The creation happens by using ISAKMP of the IPsec architecture for exchanging keys between the endpoints and creating the appropriate tunnel mode Security Associations (SA). Once the tunnel has been created, no additional signalling is needed between the
endpoints for maintaining a secure connection. The secure and authenticated transport itself is achieved by utilising IPsec ESP protocol between DXTs at the edge of the different TETRA SwMIs, in IPsec tunnel mode.

Part of the QoS assurance should be performed by taking MPLS into use in the network which connects two or more TETRA SwMIs. To maximise speed, efficiency and reliability, the IP core network should be run over ATM, but also other choices are possible. Now, when MPLS is used the packets are labelled when they leave TETRA infrastructure and routing in the network is performed based on that information.

Furthermore, Differentiated Services (DS) should be used joint with MPLS to assure QoS for packets as described in chapter 4.1.3. The information about QoS levels should be conveyed to all switches either by using LDP or RSVP or by pre-configuring the meanings of the labels to the routers. Pre-configuring is feasible because there are only few wished routes between the SwMIs and for the packets only few different DS QoS levels are required. In addition, all of this information will most probably stay unchanged.

When DS is used, also different needs for signalling and speech must be taken into account. For speech, minimising the delay is very important but the dropping probability for packets might be set quite high for the speech to still be understandable. For signalling, delay may be greater but the amount of lost packets must be kept as low as possible. These requirements for speech and signalling can be met by using the different QoS levels of DS.

To summarise, the presented security and QoS techniques are listed in Figure 38.

![Figure 38. Security and QoS in IP backbone.](image-url)
6. SUMMARY

6.1 Conclusions

This work shows that implementing an IP based ISI is feasible using existing and standardised IP based protocols. Both VoIP signalling protocols, H.323 and SIP, are technically somewhat equally suitable for ISI. However, neither of the protocols contain sufficient means for assuring Quality of Service or security: additional protocols are needed for these purposes. With both protocols, RTP is used for transferring speech: QoS and security issues need to be addressed also here. This thesis proposes MPLS joint with DS as the preferred method to assure QoS for all traffic and IPsec as the preferred method for achieving adequate security in the network.

There are certain differences between the protocols, which may affect to the final decision on the issue. Despite the heaviness of the protocol stack, H.323 may be an attractive choice to ISI because its resemblance to other telecommunications protocols and its proven reliability. Additionally, this thesis shows that using fast call setup procedure, TETRA ISI call setup is slightly faster with H.323 than with SIP. This can be considered the most important advantage of H.323 in TETRA ISI case.

Choosing SIP, on the other hand, can be regarded more as a step towards the future: SIP is designed from viewpoint of the Internet and the protocol stack is much lighter than the protocol stack of H.323. The most important advantage of SIP is the fact that it is currently dominant in the telecommunications and datacommunications world and several vendors and operators are preferring it to H.323.

However, as long as the decision and work for a prototype implementation for an IP based ISI is still pending at Nokia, no exact information is available concerning delays and other figures in the IP backbone. With a private IP network and the IP QoS means presented in this master’s thesis, delays in the IP backbone will however most probably not be a problem.

6.2 Future work

The IP based ISI and IP packet data solutions presented here will most probably not be the endpoint for development of IP based solutions in TETRA. If current trends remain, the whole TETRA system will be developed more IP centric: the development guidelines of the third generation mobile networks are also reflected to TETRA.

An obvious area of development is also the interface to other networks. TETRA ISI can be further developed in such way that also calls from and to other networks can be managed. This clearly means that signalling and real-time information must be expressed in ISI in a more universal manner than the encoding specified by this master’s thesis. Another possibility is the use of a separate gateway, where calls to other networks are directed. This gateway manages the changes in signalling and real-time information encoding.

Furthermore, as TETRA packet data solution is largely inherited from the GSM/GPRS scheme, even more GSM and GPRS network elements and concepts can be adopted to TETRA. This is reasonable also because the 3G network architecture is somewhat based on GSM/GPRS architecture.

For ensuring potential for the success of TETRA also in more distant future, standardisation work of next generation Professional Mobile Radio networks is already beginning at ETSI. The standard is called TETRA Digital Advanced Wireless Services (DAWS). DAWS is a more advanced standard than the current 3G UMTS standard and includes versatile services and very high bit-rate data. Because DAWS is aimed
primarily at PS&S sector, all of the current TETRA services are present in an enhanced form.

All in all, the future of TETRA looks promising and TETRA has an individual and clear position in the rapidly developing mobile telecommunications world. Variety of interconnected networks will exist and 3G mobile networks will gain strong foothold. However, TETRA can provide its own and relevant services to the users with certain needs and thus be a constant part of the joint architecture. To ensure this, the development of TETRA must be unceasing and rapid.
7. REFERENCES


[8] ETSI, ETS 300 392-1: Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design, February 1996.


[10] ETSI, ETS 300 392-3-1: Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 1: General design, January 1999.

[11] ETSI, ETS 300 392-3-2 DRAFT: Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 2: Additional Network Feature for Individual Call (ANF-ISIIC), May 2000.

[12] ETSI, ETS 300 392-3-3 FINAL DRAFT: Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 3: Additional Network Feature for Group Call (ANF-ISIGC), December 1999.

[13] ETSI, ETS 300 392-3-5: Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 5: Additional Network Feature for Mobility Management (ANF-ISIMM), January 2000.


7. References


[34] Lahdensuo, Kari, Feature Description: TETRA Mobility Management (Nokia Internal Document), 1996.


7. References


Appendix A. Example of encoding a TETRA ANF-ISIIC information element in a PSS1 SETUP message [10], [11].

<table>
<thead>
<tr>
<th>PSS1 SETUP message</th>
<th>M/O/C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol discriminator</td>
<td>M</td>
</tr>
<tr>
<td>Call reference</td>
<td>M</td>
</tr>
<tr>
<td>Message type</td>
<td>M</td>
</tr>
<tr>
<td>Sending complete</td>
<td></td>
</tr>
<tr>
<td>Bearer capability</td>
<td></td>
</tr>
<tr>
<td>Channel Identification</td>
<td>O</td>
</tr>
<tr>
<td>Progress Indicator</td>
<td>O</td>
</tr>
<tr>
<td>Calling party number</td>
<td>M</td>
</tr>
<tr>
<td>Called party subaddress</td>
<td>M</td>
</tr>
<tr>
<td>Called party number</td>
<td>M</td>
</tr>
<tr>
<td>Called party subaddress</td>
<td>M</td>
</tr>
<tr>
<td>Low layer compatibility</td>
<td></td>
</tr>
<tr>
<td>High layer compatibility</td>
<td></td>
</tr>
</tbody>
</table>

**Facility**

- Identifier | M
- Length | M
- Protocol profile (Networking Extensions) | M
- Network Facility Extension (NFE) | M
- Network Protocol Profile | M
- Interpretation APDU | O

**Service APDU: ROSE INVOKE**

- Identifier | M
- Invoke ID | M
- Linked ID | M
- Operation Value | M

**Argument: Tetra ISI Message**

- Source Entity | M
- Destination Entity | M

**Tetra Message**

- PDU Type | M
- Originating SwMI MNI | M
- Forward switched | M
- Last forwarding SwMI MNI | M
- Routing method choice | M
- Call time-out, set-up phase | M
- Call time-out | M
- Hook method selection | M
- Simplex/duplex selection | M
- Basic service information | M
- Speech service requested | C
- Security level at calling user air interface | M
- Transmission grant | M
- Transmission request permission | M
- Call priority | M
- Called/diverted-to party address SSI | M
- Called/diverted-to party extension | M
- Called external subscriber number length | M
- Called external subscriber number digits | C
- SS-CLIR invoked for calling party | M
- Calling party address SSI | M
- Calling party extension | M
- Calling external subscriber number length | M
- Calling external subscriber number digits | C
- Override SS-CAD invocation | M
- Speech services supported | O
- Notification indicator | O
- Proprietary | O

**END of Tetra Message**

**Extension** | O

**END of Service APDU**

**END of Facility**

**Notification Indicator** | O

**END of PSS1 SETUP Message** | O
Appendix B. Example of encoding a TETRA ANF-ISIIC information element in a H.323 SETUP message [23], [27], [29], [11].

<table>
<thead>
<tr>
<th>H.323 SETUP message</th>
<th>M/O/C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol discriminator</td>
<td>M</td>
</tr>
<tr>
<td>Call reference</td>
<td>M</td>
</tr>
<tr>
<td>Message type</td>
<td>M</td>
</tr>
<tr>
<td>Bearer capability</td>
<td>M</td>
</tr>
<tr>
<td>Facility</td>
<td>O</td>
</tr>
<tr>
<td>Calling party number</td>
<td>O</td>
</tr>
<tr>
<td>Called party number</td>
<td>O</td>
</tr>
<tr>
<td>User-to-User</td>
<td></td>
</tr>
<tr>
<td>Setup-UUIE</td>
<td>M</td>
</tr>
<tr>
<td>Non Standard Data</td>
<td>O</td>
</tr>
<tr>
<td>H.450.1 Supplementary Service APDU</td>
<td></td>
</tr>
<tr>
<td>Network Facility Extension (NFE)</td>
<td>O</td>
</tr>
<tr>
<td>Interpretation APDU</td>
<td>M</td>
</tr>
<tr>
<td>Service APDU: ROS Invoke</td>
<td></td>
</tr>
<tr>
<td>Invoke ID</td>
<td>M</td>
</tr>
<tr>
<td>Linked ID</td>
<td>O</td>
</tr>
<tr>
<td>Opcode</td>
<td>M</td>
</tr>
<tr>
<td>Argument: Tetra ISI Message</td>
<td></td>
</tr>
<tr>
<td>Source Entity</td>
<td>M</td>
</tr>
<tr>
<td>Destination Entity</td>
<td>M</td>
</tr>
<tr>
<td>Tetra Message</td>
<td></td>
</tr>
<tr>
<td>PDU Type</td>
<td>M</td>
</tr>
<tr>
<td>Originating SwMI MNI</td>
<td>M</td>
</tr>
<tr>
<td>Forward switched</td>
<td>M</td>
</tr>
<tr>
<td>Last forwarding SwMI MNI</td>
<td>M</td>
</tr>
<tr>
<td>Routing method choice</td>
<td>M</td>
</tr>
<tr>
<td>Call time-out, set-up phase</td>
<td>M</td>
</tr>
<tr>
<td>Call time-out</td>
<td>M</td>
</tr>
<tr>
<td>Hook method selection</td>
<td>M</td>
</tr>
<tr>
<td>Simplex/duplex selection</td>
<td>M</td>
</tr>
<tr>
<td>Basic service information</td>
<td>M</td>
</tr>
<tr>
<td>Speech service requested</td>
<td>C</td>
</tr>
<tr>
<td>Security level at calling user air interface</td>
<td>M</td>
</tr>
<tr>
<td>Transmission grant</td>
<td>M</td>
</tr>
<tr>
<td>Transmission request permission</td>
<td>M</td>
</tr>
<tr>
<td>Call priority</td>
<td>M</td>
</tr>
<tr>
<td>Called/diverted-to party address SSI</td>
<td>M</td>
</tr>
<tr>
<td>Called/diverted-to party extension</td>
<td>M</td>
</tr>
<tr>
<td>Called external subscriber number length</td>
<td>M</td>
</tr>
<tr>
<td>Called external subscriber number digits</td>
<td>C</td>
</tr>
<tr>
<td>SS-CLIR invoked for calling party</td>
<td>M</td>
</tr>
<tr>
<td>Calling party address SSI</td>
<td>M</td>
</tr>
<tr>
<td>Calling party extension</td>
<td>M</td>
</tr>
<tr>
<td>Calling external subscriber number length</td>
<td>M</td>
</tr>
<tr>
<td>Calling external subscriber number digits</td>
<td>C</td>
</tr>
<tr>
<td>Override SS-CAD invocation</td>
<td>M</td>
</tr>
<tr>
<td>Speech services supported</td>
<td>O</td>
</tr>
<tr>
<td>Notification indicator</td>
<td>O</td>
</tr>
<tr>
<td>Proprietary</td>
<td>O</td>
</tr>
<tr>
<td>END of Tetra Message</td>
<td></td>
</tr>
<tr>
<td>Extension</td>
<td>O</td>
</tr>
<tr>
<td>END of Argument</td>
<td></td>
</tr>
<tr>
<td>END of Service APDU</td>
<td></td>
</tr>
<tr>
<td>END of H.450.1 Supplementary Service APDU</td>
<td></td>
</tr>
<tr>
<td>H.245 Tunneling</td>
<td>M</td>
</tr>
<tr>
<td>H.245 Control</td>
<td>O</td>
</tr>
<tr>
<td>Non Standard Control</td>
<td>O</td>
</tr>
<tr>
<td>END of User-to-User</td>
<td></td>
</tr>
<tr>
<td>END of H.323 SETUP Message</td>
<td></td>
</tr>
</tbody>
</table>

Saku Oja: Lower layer protocols in TETRA Inter-System Interface 68
Appendix C. Example of encoding a TETRA ANF-ISIIC information element in a SIP INVITE message [19], [17].

INVITE sip:+358601234567@130.233.249.7 SIP/2.0
Via: SIP/2.0/UDP 130.233.249.7
From: +358707654321 <sip:+358707654321@130.233.224.50>
To: +358601234567 <sip:+358601234567@130.233.149.7>
Call-ID: 3298420296@130.233.224.50
CSeq: 1 INVITE
Content-Length: 411
Content-Type: multipart/mixed; boundary=unique-boundary-1
MIME-Version: 1.0

--unique-boundary-1
Content-Type: application/SDP; charset=ISO-10646

v=0
o=- 53655765 2353687637 IN IP4 130.233.224.50
s=TETRA ISI call
c=IN IP4 130.233.224.50
t=2873397496 28734044696
m=audio 3456 RTP/AVP 51

--unique-boundary-1
Content-Type: application/ROS
Content-Transfer-Encoding: binary
dflgsfdghdlgh908ut45r41ktj5435j353l05j3rjht4welhtrtkgh
kdflklsghdsfougioiu5456i54lk6j45lk6jjh56kj56kjh56kjh56lkj

--unique-boundary-1--

Legend for the parameters in SDR (RTF capability negotiation) part [18]:

**Version:** the "v=" field gives the version of the SDR protocol used.

**Origin:** the "o=" field contains the user id of the sender (in this case none), a SDP session id (a Network Time Protocol timestamp), SDP announcement version (a NTP timestamp), network type (IN=internet), IP protocol version and origin IP address or domain name.

**Session:** the "s=" field gives a name for the SDP session.

**Connection data:** the "c=" field contains the network type (IN=internet), IP protocol version and connection IP address.

**Time:** the "t=" field gives a start and stop time for the session. They are expressed in NTP time units.

**Media:** the "m=" field contains the media type, RTP port for received real-time data, protocol identifier (RTP/AVP) and the RTP payload type identifier as defined in RTP Audio/Video Profile (an unassigned number which could in the future correspond to TETRA/ACELP).