



CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Electrical Engineering
Department of Telecommunication Engineering

Master Thesis

Academic Base Station

Study program: Communication, Multimedia and Electronics

Branch of study: Networks of Electronic Communication, MSc

Thesis advisor: Ing. Robert Bešťák, Ph.D.

Zagroz Aziz, Bc.

Prague, 2014

Čestné prohlášení

Prohlašuji, že jsem zadanou diplomovou práci zpracovala sama s přispěním vedoucího práce a konzultanta a používala jsem pouze literaturu v práci uvedenou. Dále prohlašuji, že nemám námitek proti půjčování nebo zveřejňování mé diplomové práce nebo její části se souhlasem katedry.

Datum: 12.5.2014

.....

Podpis diplomanta

Poděkování

Tímto bych ráda poděkovala vedoucímu mé diplomové práce panu Ing. Robertovi Bešt'ákovi, PhD. a to především za jeho odbornou pomoc, cenné rady, empatii, trpělivost, věnovaný čas a vstřícnost při zpracovávání této práce.

České vysoké učení technické v Praze
Fakulta elektrotechnická

katedra telekomunikační techniky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Student: **Aziz Zagroz**

Studijní program:
Obor: Sítě elektronických komunikací

Název tématu: **Akademická základnová stanice mobilní sítě**

Pokyny pro vypracování:

The aim of project is to connect an academic base station that is placed at CTU to a partners mobile network testbed infrastructure. The interconnection should be then tested for different scenarios such as voice or data communications.

Seznam odborné literatury:

- [1] T. Halonen, J. Romero, J. Melero: GSM, GPRS and EDGE performance, second edition. John Wiley & Sons, Ltd. England 2003. ISBN 0470866942.
- [2] D. Chambers: Femtocell Primer, first edition. ISBN: 978-1-4092-2647-5
- [3] H. Holma, A. Toskala: HSDPA/HSUPA for UMTS. John Wiley&Sons. England 2006. ISBN 0470018844.
- [4] B.H. Walke: Mobile Radio Networks, networking and protocols. John Wiley & Sons. Stuttgart 1999. ISBN 0471975958.

Vedoucí: Ing. Robert Bešťák, Ph.D.

Platnost zadání: do konce zimního semestru 2014/2015

L.S.

prof. Ing. Boris Šimák, CSc.
vedoucí katedry

prof. Ing. Pavel Ripka, CSc.
děkan

V Praze dne 20. 11. 2013

Abstract

The thesis discusses connection of remote GSM base station, located at a workplace at CTU-FEE in Prague, to mobile research network built at Satakunta University in Pori (Finland) via internet connection. To verify the network performance and its ability to achieve mobile services successfully, different tests and measurements are made after the establishment in order.

Abstrakt

Diplomová práce popisuje připojení vzdálené základnové stanice sítě GSM, jež je umístěná na pracovišti ČVUT-FEL v Praze, k výzkumné mobilní síti vybudované na univerzitě Satakunta v Pori, (Finsko) prostřednictvím Internetu. K ověření funkčnosti spojení a poskytování služeb, bylo provedeny měření a testovány různé scénáře.

Keywords

Mobile network, Global system for mobile communication, Base station, Internet, Testing platform.

Klíčová slova

Mobilní síť, Globální systém pro mobilní komunikaci, Základnová stanice, Internet, Testovací platforma.

Contents

List of Figures.....	7
List of Tables.....	7
Introduction.....	8
Chapter One	10
GSM Channel Concept.....	10
1.1 Logical Channels	10
1.1.1 Traffic Channels	11
1.1.2 Control Channels	11
1.2 Physical Channels	13
1.2.1 Modulation	13
1.2.2 Multiple Access.....	15
1.3 Channel Mapping	16
Chapter Two	18
BSS Interfaces and Protocol Architecture	18
2.1 A-interface [1].....	18
2.2 Abis interface [3]	19
2.3 Um interface.....	20
2.4 Protocols.....	20
Chapter Three.....	23
SAMK Network Architecture	23
1. Network Topology Setup.....	23
1.1. IPsec Parameters Setup.....	23
1.2. Ethernet and Circuit Emulation Service.....	26
Configuration of CES.....	28
2. SAMK NGN Network Architecture.....	29
2.1. InSite base station	31
Mobile Switching Center	37
Base Station Controller.....	44
Chapter Four.....	48
Measurements and Assessments.....	48
Connection Test ‘end-to-end’.....	48

NetHawk Protocol Analyzer.....	49
Mobility Management.....	50
Wireshark	51
GPRS Activation Procedure	53
Nokia NetMonitor	54
Chapter Five.....	55
Conclusion	55
Annex.....	57
Annex 1 - Pori CES Configuration	57
Annex 2 - Prague CES Configuration.....	58
Annex 3 - GPRS Procedure over Gb.....	59
Abbreviations and Acronyms	69
References.....	73

List of Figures

Figure 1.1 Logical Channels and Signaling during connection setup for an incoming call	10
Figure 1.2 GSM digital modulation	11
Figure 1.3 Impulse response for GMSK transmitter filter blocks building	12
Figure 1.4 FDMA/TDMA structure in GSM	13
Figure 1.5 Hierarchy of frames in GSM system	15
Figure 2.1 A-interface in the OSI protocol stack	16
Figure 2.2 OSI protocol stack on Abis interface	17
Figure 2.3 Signaling SS7 stack for GSM	18
Figure 2.4 Protocol Architecture for Signaling	19
Figure 3.1 Pori-Prague Network Topology	23
Figure 3.2 Telco Systems T-Marc 254	24
Figure 3.3 Circuit Emulation Service over Packet	25
Figure 3.4 Structured Emulation	25
Figure 3.5 Unstructured Emulation	25
Figure 3.6 SAMK NGN network architecture	28
Figure 3.7 InSite base station	29
Figure 3.8 Nokia InSite BTS Manager	33
Figure 3.9 MSCi Structure with functional units	36
Figure 3.10 Nokia DX 200 MSCi	41
Figure 3.11 BSCi Architecture	42
Figure 3.12 MCMU structure	44
Figure 4.1 T-Marc connection test	46
Figure 4.2 NetHawk analyzer interface	47
Figure 4.3 Nethawk Analyzer	48
Figure 4.4 WireShark interface	49
Figure 4.5 Nokia NetMonitor	52
Figure 5.1 3G network with the academic base station	53
Figure 5.2 Two InSite BTSs network	54
Figure 5.3 Two different generation networks	54

List of Tables

Table 1.1 Logical channels classification	8
Table 3.1 IPv4 Address Assignments	22
Table 3.2 IPsec and ISAKMP parameters setup	23
Table 3.3 Technical data for integrated antenna	32
Table 3.4 RF performance	32
Table 3.5 Prague InSite Configuration	34
Table 3.6 Comparison between BSC and BTS functions	45
Table 4.1 Mobility Management	50

Introduction

The term of mobile communication is more than what it means in fact and it plays a big role in our lives nowadays and even became something that can't be apart from us. The need of mobile phone is rising every day and the necessity of understanding the different scenarios that have been done within a mobile communication network becomes a priority for telecom engineers especially those who are interested in mobile communication networks area. Global System for Mobile Communications (GSM) is one of the most common mobile networks that is used in the entire world and still serves properly since the early of 90s.

In Satakunta University for Applied Sciences (SAMK), a standardized mobile network laboratory is built for academic purposes including 2nd generation, 3rd generation and fixed line networks from different vendors such as Nokia and Ericsson. Apart from charging and billing system because it's not a commercial network, SAMK has provided a perfect environment for the researchers to do there tests or any academic or scientific researches without problems whether related to core network or radio access field and furthermore, they are sharing this network with some other universities inside and outside Finland in order to be used for their academic purposes too. Czech technical University (CTU) in Prague is one of the universities who attended to be beneficiary and to be part of this network via a project which is about installing one Nokia InSite base Station Time division Multiple Access (TDMA) based.

This base station is located in Prague/CTU providing 2nd generation mobile network with GPRS and other supplementary services to CTU telecom laboratories and this is done over public network/internet via creating a Virtual Private Network (VPN) tunnel between Pori/SAMK and Prague/CTU and by using Circuit Emulator Service/T-Marc which is TDMA/Ethernet device used to send TDMA frames over IP in packets. The Nokia base station band is 1800 MHz and it's designed for indoor purposes (Optimized for picocellular indoor use) while the capacity is only 1 TRX.

Once the project is done and the InSite base station is launched, many softwares and programs can be used later for different approaches for instance; tracing mobile phone signal via using NetHawk analyzer which is a software used for network optimization, monitoring and troubleshooting in order to know the scenarios and routes while making the phone call and to know the role of each part in the system and study it in details via using Nokia Electronic Documentation (NED) which is one of most detailed documentation library used by beginners/advanced system users, during location updating, paging, General Packet Radio Service (GPRS) attach/detach , frequency handover, Short Message Service (SMS), network messages, the protocols that are used in different areas of the network such as Base Station Subsystem (BSS), Network Switching Subsystem (NSS), the packet switching and the circuit switching, the interfaces such as air interface, A-interface and many more schemes. So when you say mobile networks, with this title you could build a faculty holding different departments

and specializations such as programming, telecommunications, electronics, microelectronics, radio and electromagnetic field and power engineering. And what's really interesting in this project is, when you have a plan to establish a mobile network and especially based on 2nd or 3rd generation networks, you must have a quite good enough budget to even think about because building a mobile network costs an incredible money and no matter for what reason. In our case, which is an academic aim, it's very economic and reliable solution. The network is already launched so the only part to participate in the network with, is to have a Base Transceiver station (BTS) in order to have full access to the network and no matter where the BTS is. Internet made this happens easily in spite of the location of the BTS or the location of the core network via using VPN with providing firewall and secured system.

The topic will be about how to establish a mobile base station in Prague/CTU but first, by going through the GSM channel concept and BSS protocol and interface architecture which are very important to know in order to be familiar with the essential parameters. Then starting explaining about all the elements and materials that are used in establishing this network starting from SAMK testbed, routers/switches, T-Marc and finally the base station.

And of course, any mobile network can't be launched without tests and assessments first. So by going through some tests and scenarios that can be done by some softwares which are very common used in telecommunications sector.

Chapter One

GSM CHANNEL CONCEPT

1.1 Logical Channels

GSM defines a set of logical channels which refers to layer 1 of OSI reference model and they can be in two modes, unassigned random access mode or dedicated mode which is assigned to a specific user. Logical channel is definition of two categories, traffic channels and signaling or control channels [1].

Logical channels data is transmitted in the related time slots of the physical channel and during this process, the logical channels would occupy a part of the physical channel or the whole channel [2], logical channel classification shown in table 1.1.

Group		Channel	Function	Direction
Traffic Channel	Traffic Channel (TCH)	TCH/FR, Bm	Full Rate TCH	MS ↔ BSS
		TCH/HR, Lm	Half Rate TCH	MS ↔ BSS
Signaling Channels	Broadcast Channel	BCCH	Broadcast Control	MS ← BSS
		FCCH	Frequency Correction	MS ← BSS
		SCH	Synchronization	MS ← BSS
	Common Control Channel (CCCH)	RACH	Random Access	MS → BSS
		AGCH	Access Grant	MS ← BSS
		PCH	Paging	MS ← BSS
		NCH	Notification	MS ← BSS
	Dedicated Control Channel (DCCH)	SDCCH	Stand-Alone Dedicated Control	MS ↔ BSS
		SACCH	Slow Associated Control	MS ↔ BSS
FACCH		Fast Associated Control	MS ↔ BSS	

Table 1.1 Logical channels classification [i]

1.1.1 Traffic Channels

Traffic channels are classified as logical channels since they are used to transmit user data, speech and messages but they don't carry any control data of layer 3 and communication over traffic channel whether is circuit-switched or packet-switched and may either be full-rate channel or be divided into two half-rate channels which they are allocated to two different subscribers [3].

There are two types of traffic channels [4]:

B_m – channel is full-rate traffic channel and the data rate of 22 Kbit/s is carried out. Digitalizing and coded speech only require 13 Kbit/s to transmit the speech information and the rest will be used for error correction and it's possible to transmit data at 12, 6 or 3.6 Kbit/s over B_m – channel [5].

L_m – channel is with less transmission bandwidth with rate of 11.4 Kbit/s and it allows data to be transmitted with bit rates 6 or 3.6 Kbit/s [6].

1.1.2 Control Channels

A lot of different control channels are used in GSM in order to control medium access. Control channels divided into three groups and each one of them consists of sub channels [7]:

- **Broadcast Control Channel (BCCH):** This channel has been used by the BTS to signal information to all mobile subscribers within a cell like cell identifier, frequency hopping, comparing frequencies which are available with the neighboring cells. Frequency Correction Channel (FCCH) is responsible for frequency correction in the BTS while Synchronization Channel (SCH) sends information about time synchronization and both mentioned channels are sub channels of BCCH [8].
- **Common Control Channel (CCCH):** All information about connection setup between BTS and MS has been handled by CCCH, from BTS toward MS is controlled via Paging Channel (PCH) for paging the appropriate MS and meanwhile, Random Access Channel (RACH) is handling the call setup messages from MS toward the BTS so all MSs may access this channel. This is where a collision could occur among the MSs which send the request. In this case, BTS uses Access Grant Channel to control an MS whether it can use a TCH or just SDCCH for further connection setup [9].
- **Dedicated Control Channel (DCCH) [10]:** This is bidirectional point-point control channel using three dedicating control sub channels as long as the MS has not established a TCH yet with the BTS. These sub channels are used to send data for call control at different bit rates.

DCCH uses Stand-alone Dedicated Control Channel (SDCCH) for transmitting MS information about registration, authentication, location area updating and data for call setup (See figure 1.1) with capacity of 782 bit/s which is much lower than of a TCH while it uses Slow Associated Dedicated Control Channel (SACCH) at a data rate of 383 bit/s to be allocated in parallel with a TCH or an SDCCH which is responsible for sending system information from the network to the MS and retrieving measurements on signal strength and receive quality from the MS in front.

If more signaling information has to be sent or for a short term and there is a time slot which is dedicated for the TCH, Fast Associated Dedicated Control Channel (FACCH) uses that time slot in case of an impending handover or to exchange larger amounts of data which is necessary to be transmitted.

Moreover, in addition to these channels, there is another channel which is defined for a certain purpose and it shares a physical channel together with SDCCH; Cell Broadcast Channel (CBCH) is responsible for broadcasting the messages of Short Message Service Cell Broadcast (SMSCB) [11].

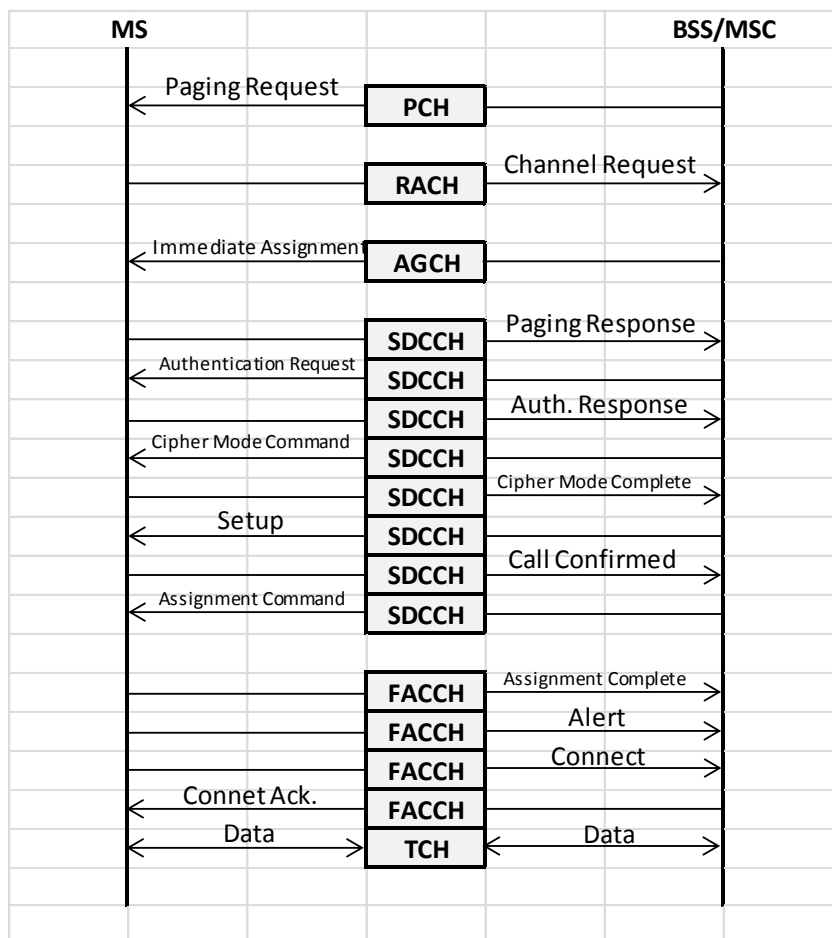


Figure 1.1 Logical Channels and Signaling during connection setup for an incoming call [ii]

1.2 Physical Channels

Via air interface, physical channels transport logical channel and the way how the logical channels are placed on physical channels is called mapping.

The physical channel is determined by the carrier frequency or number of carrier frequencies with defining the hopping sequence and time slot number [12].

1.2.1 Modulation

The modulation that's used on the radio channel is Gaussian Minimum Shift Keying (GMSK) which belongs to Continuous Phase Modulation. With narrow transmitter power spectrum and low adjacent channel interference while it has also a constant amplitude envelope that allows simple amplifier usage with no special linearity requirements (Class C amplifiers that has a high efficiency which provides longer operation while it is operating on battery charge).

The digital modulation for GSM air interface consists of many steps in order to generate a high frequency signal from channel coded and enciphered data blocks as shown in figure 1.2



Figure 1.2 GSM digital modulation

Data d_i reaches at the modulator with a bit rate 270.83 kbit/s which is gross data rate and first differential coded:

$$d'_i = (d_i + d_{i-1}) \bmod 2, \quad d_i \in (0; 1) \quad (1)$$

From this differential data, the modulation data are formed which stands for a sequence of Dirac pluses:

$$a_i = 1 - 2d'_i \quad (2)$$

This bipolar sequence of modulation data is implemented into the transmitter filter which is also called frequency filter in order to create the phase $\Phi(t)$ of the modulation signal while the impulse response $g(t)$ of this linear filter is defined by convolution of the impulse response $h(t)$ of a Gaussian low-pass with a rectangular step function:

$$g(t) = h(t) \times \text{rect}\left(\frac{t}{T}\right) \quad (3)$$

$$\text{rect}\left(\frac{t}{T}\right) = \begin{cases} 1/T, & \text{for } |t| < T/2 \\ 0, & \text{for } |t| \geq T/2 \end{cases} \quad (4)$$

$$h(t) = \frac{1}{\sqrt{2\pi}\sigma T} e^{-\frac{t^2}{2\sigma^2 T^2}}, \quad \sigma = \frac{\sqrt{\ln 2}}{2\pi B T}, \quad B T = 0.3 \quad (5)$$

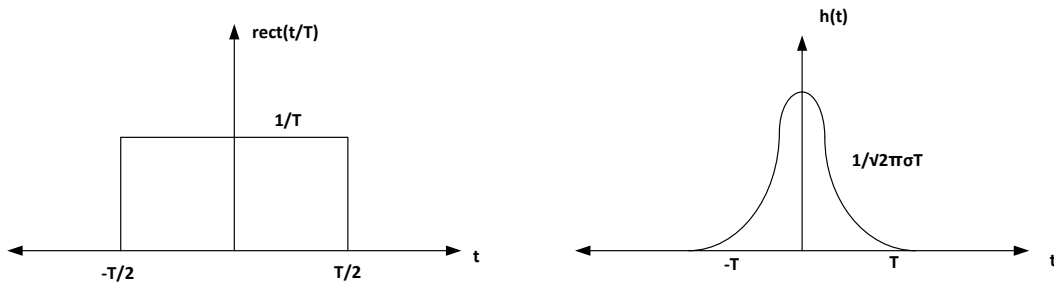


Figure 1.3 Impulse response for GMSK transmitter filter blocks building

As shown in the equation, B is 3 dB which is the bandwidth of the filter $h(t)$ while T is the bit duration of incoming bit stream. What is shown in figure 1.3 is the step rectangular function with Gaussian low pass impulse response for some value BT [13].

This modulation contains also a Minimum Shift keying MSK procedure which the data are filtered through an additional Gaussian low pass before Continuous Phase Modulation CPM with the rectangular filter and that is why called GMSK where the Gaussian low pass adds more smoothing effects in one hand while on the other hand it's broadening the impulse response $g(t)$, so it means that the signal power spectrum becomes narrower but the intersymbol interference increases as long as the individual impulse responses are spread during many bit durations. This partial response behavior has to be balanced in the receiver by an equalizer.

The modulation signal phase is impulse response convolution $g(t)$ of the frequency filter with Dirac impulse sequence a_i of the modulated data:

$$\varphi(t) = \sum_i a_i \pi \eta \int_{-\infty}^{t-iT} g(u) du \quad (6)$$

The maximal phase shift is $\pi/2$ per bit duration with the modulation index $\eta = 1/2$ and the GSM modulation is designed as 0.3-GMSK with $\pi/2$ phase shift. The modulated high frequency carrier signal can be then represented by following formula [14]:

$$x(t) = \frac{\sqrt{2E_c}}{T} \cos(2\pi f_0 t + \varphi(t) + \varphi_0) \quad (7)$$

Where E_c = Energy per modulated data bit rate

f_0 = Carrier frequency

ϕ = Random phase and constant during a burst

1.2.2 Multiple Access

GSM uses both Frequency Division Multiple Access (FDMA) and Time Division Multiple Access (TDMA) together and this occurs on Radio interface whereas two dimension channel is obtained (See figure 1.4). FDMA is an old standard where used in the old mobile system generations but using only FDMA structure caused overload problems and by increasing the demand, this was leading to serious issues regarding frequency usage since each subscriber is using one specific frequency during a call.

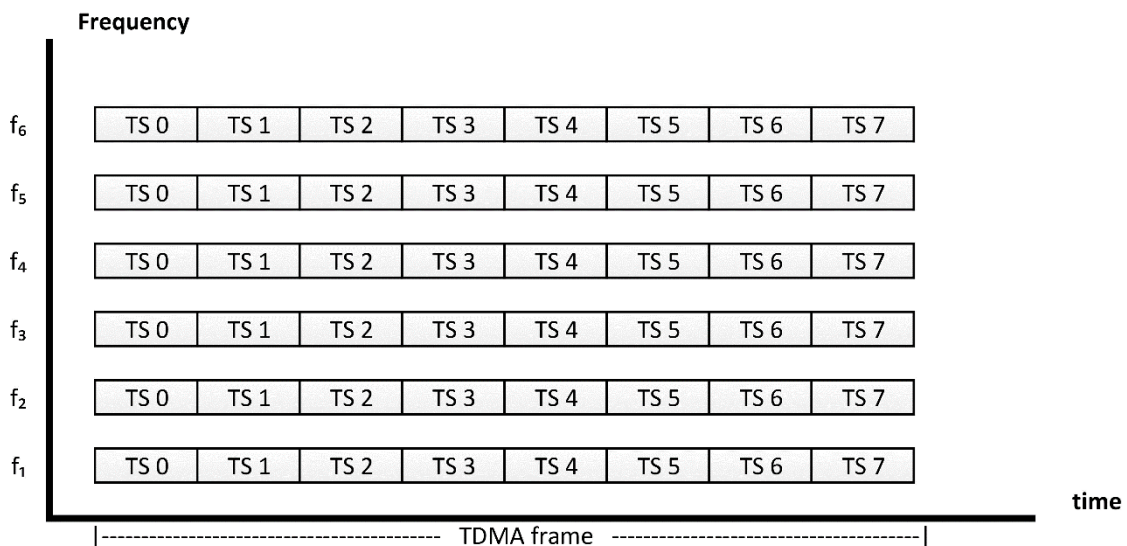


Figure 1.4 FDMA/TDMA structure in GSM

In TDMA, the user sends an impulse which more like signal within a period but the FDMA user occupies the channel permanently so the TDMA can serve seven users or channels on the same frequency while in the same case, the FDMA uses seven different frequencies to serve the same number of channels [15].

1.3 Channel Mapping

GSM system has in a total 25MHz for uplink and downlink and each one is divided among 124 channels of 200 kHz. There is one thing to be mentioned, the number of channels are totally 125 but the lowest channel is not used as it may interfere with close non-GSM networks.

Each channel operates at different carrier frequency and any individual channel is time division multiple accessed by users. The frame duration is 4.615 ms divided among eight timeslots and each timeslot is physical channel occupied and carries traffic and control information in a burst form. The duration of any channel is 0.577 ms [16].

At the base station, Time Division Multiple Access TDMA frames on all radio channel frequency channels in both uplink and downlink are aligned and to avoid simultaneous transmitting and receiving, in the beginning of any uplink TDMA frame will be delayed by a fixed period of exactly three timeslots with respect to the downlink and the stumbling TDMA frames allows the same timeslot number to be used in both downlink and uplink.

The timeslot number (TN) inside a frame is numbered from 0 to 7 while higher order frames are called multiframe which consists of 26 TDMA frames and holds TCH, SACCH and FACCH. Moreover, a 51-frame multiframe has a duration of 235.365 ms that means 51×4.615 ms so one superframe holds 51 traffic multiframes or 26 control multiframes and consists of 51×26 TDMA frames with a total duration of 6.12 sec. (51×120 ms) [17].

The 26 TDMA frame multiframe supports traffic and Associated Control Channels ACC while the 51 frame multiframe supports Broadband Common Control BCC and Stand Alone Dedicated Control Channels. The highest order frame consists of 2048 superframes ($2,715,648$ frames = $2048 \times 51 \times 26$) with time duration 3 hours, 28 minutes and 52.76 seconds and this type of frame is called hyperframe (See figure 1.5) [18].

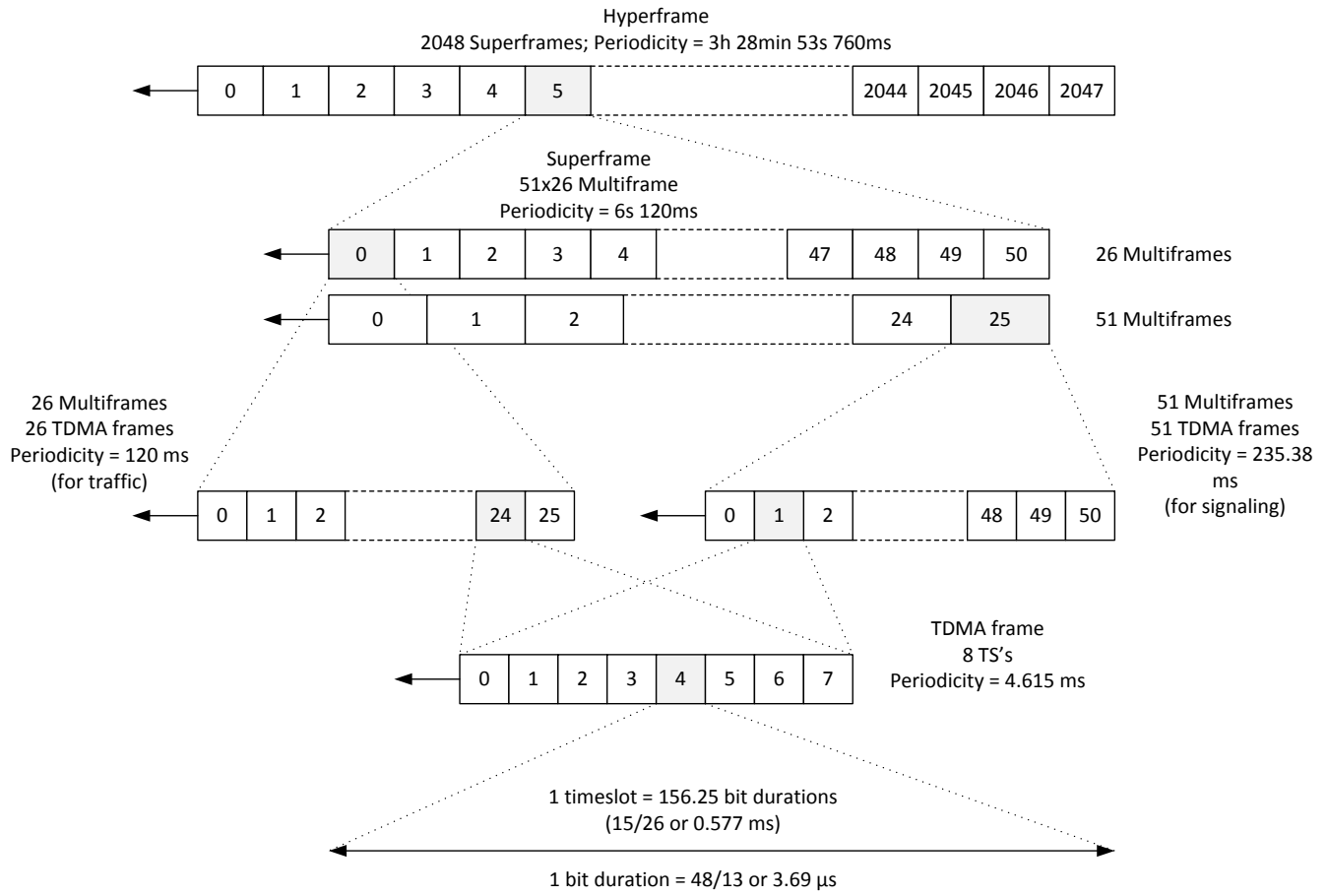


Figure 1.5 Hierarchy of frames in GSM system [iii]

Chapter Two

BSS INTERFACES AND PROTOCOL ARCHITECTURE

2.1 A-interface [1]

Part of the signaling unit which is located between MSC and BSS and it uses signaling number 7 with the Signaling Connection Control Part SCCP as the user part and it defines a new application which is BSSAP and this BSSAP separated into Base Station Subsystem Management Part BSSMAP and Direct Transfer Application DTAP. So the results in OSI protocol Stack are presented in figure 2.1 [2]. A-interface is responsible of the following:

1. Handles the signaling between the mobile and the base station which is Base Station System Application Part (BSSAP)
2. Look after the Message Transfer Part (MTP) decentralized functions
3. Controls the signaling messages and functions which are part of signaling channels

User data	DTAP
Layer 1-3	BSSMAP
	SCCP
	MTP 1-3

Figure 2.1 A-interface in the OSI protocol stack

Within A-interface, two signaling messages are distinguished, the one between Mobile Switching Center (MSC) and the Mobile Station and the other one is between MSC and BSS. The messages Mobility Management and Connection Management (CC, MM) which are directed to the Mobile Station MS, are transparently passed through BSS via Direct Transfer Application Protocol (DTAP) (responsible of transferring layer 3 messages and part of BSSAP) without any analysis and interpreting by the BSS (BSC, BTS) see figure 2.4 for protocol architecture.

2.2 Abis interface [3]

It can be indicated between the BTS and BSC and specified by ITU in the G-series recommendations. With transmission rate of 2 Mbps which is divided into 32 channels and each on 64 Kbps while any of these 64 Kbps channels packs up to 8 GSM traffic channels.

Signaling on Abis-interface:

1. OSI Protocol Stack

Abis interface brings layers one through three of the OSI protocol stack into service. Layer one forms D-channel which points out to the ISDN channel that signaling information is carried by with 16 Kbit/s bit rate.

The Link Access Protocol D-channel (LAPD) which is a bit-oriented and part of ISDN protocol suite runs at layer two while layer three is split up into TRX Management TRXM, Common Channel Management CCM, Radio Link Management RLM and Dedicated Channel Management DCM (Figure 2.2 shows OSI protocol stack on Abis interface).

Higher layer	User data (CC, RR, MM)			
Layer 3	TRXM	CCM	RLM	DCM
Layer 2	LAPD			
Layer 1	D channel			

Figure 2.2 OSI protocol stack on Abis interface

2. Layer two

Which consists of Link Access Protocol for D-channel. The ISDN D-channel protocol that GSM has widely has adopted, provides the basics of signaling on the Abis interface which is also referred to as LAPD, defined by ITU in Q.920 and Q.921.

2.3 U_m interface

It's also called the radio interface or the air interface. It's located between the mobile station and the base station and includes many mechanisms and schemes. GSM applies Space Division Multiple Access SDMA scheme which is used for allocating a separated space to users in the network by combining among more than one scheme and basically involves assigning an optimal base station to a mobile station due to receiving several base station signals with different quality and moreover, FDD is used to separate downlink and uplink.

In GSM 900, 124 channels and each with 200 kHz wide for FDMA while for GSM 1800, 374 channels and for some technical reason, channel 1 and 124 are not used so in general, only 32 channels are used for data management while the remaining 90 channels are used for traffic [4].

All those topics were mentioned in chapter one are giving the same explanation for air interface.

2.4 Protocols

Open System Interconnection (OSI) seven layer model explains mainly the telecommunication protocols and many layers especially Signaling System SS7 which is a set of mobile signaling protocols as shown in figure 2.3.

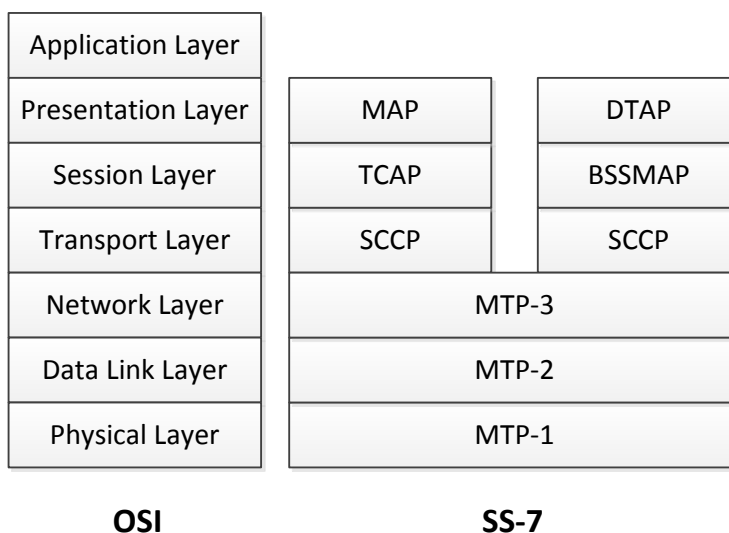


Figure 2.3 Signaling SS7 stack for GSM

The Message Transfer Part 1 (MTP-1) protocol provides the physical description about the transmission medium on layer 1 of OSI model and on data link layer, the messages are transformed into packets with identifying the beginning and the end of each packet in order to be detected correctly by the receiver and this is equivalent to MTP-2 protocol in SS7 stack while the network layer is responsible for packet routing by labeling each packet with source and destination address and in SS7 stack, this is done by MTP-3 protocol. The rest of the layers and protocols depending on the type of application [5].

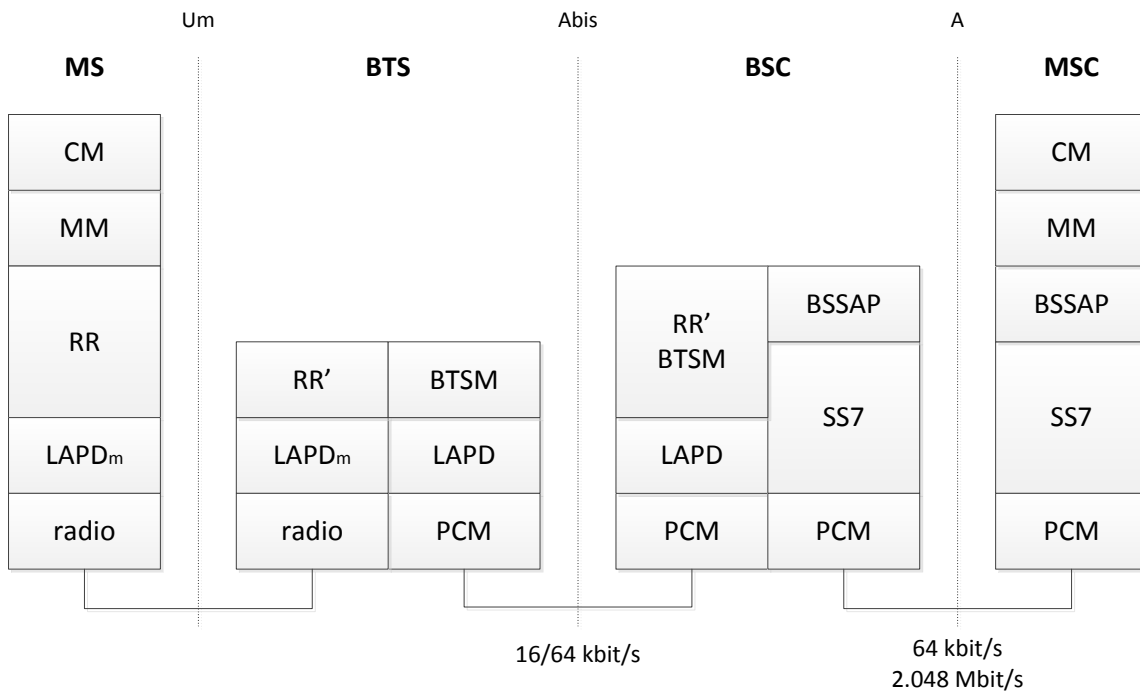


Figure 2.4 Protocol Architecture for Signaling

The ISDN User Part (ISUP) is used in messages which are sent for establishing or clearing a call while SCCP in SS7 is used for communication between the switching center and the databases which is equivalent to transport layer in OSI. For database access and query, Transaction Capability Application Part (TCAP) is used and Mobile Application Part (MAP) protocol is used for communication between the switching center and the database center in order to maintain subscriber information [6].

The DTAP protocol is used between the Mobile Station MS and the Mobile Switching Center (MSC) for transparent communication while BSSMAP protocol is used for communication between MSC and radio access network [7].

GSM network elements require higher layers for signaling, therefore; LAPDm protocol is introduced (Figure 2.4 explains all the protocols which are introduced for signaling in GSM system) at radio interface level for layer two and it's derived from LAPD in ISDN systems. For error detection, LAPDm does not need synchronization flags or checksumming and provides reliable data transfer connections, data frames and flow control re-sequencing. LAPDm is also providing data segmentation and reassembly as well as for data transfer acknowledgement [8].

The network layer introduces many sublayers in GSM system and the lowest one is Radio Resource management (RR) as shown in figure 2.4 but is not totally implemented into the base station, BSC also has part of this sublayer as well and its functionalities are supported by Base Transceiver Station Management (BTSM) in the BSC. RR provides generally the radio channels setup, maintenance and release and moreover, it has direct access to the physical layer for radio information and providing connection to the next higher layer [9].

Mobility Management (MM) consists of registration, authentication and location updating functions and while Call or Connection Management (CM) has Call Control, Short Message Service (SMS) and Supplementary Services (SS) [10].

Chapter Three

SAMK NETWORK ARCHITECTURE

1. Network Topology Setup

The main idea of having such a network is to establish an academic base station in Czech Technical University CTU for academic reason. As it's known to have a complete GSM mobile network or any another release of mobile network costs a lot of money and takes time plus a lot work and space so the alternate plan is to share the network that can be provided by a university which has already established a mobile network and in our case, SAMK university for applied science in Pori has a very well organized network including 2nd, 3rd generation and PSTN.

SAMK is providing GSM mobile network to Prague/CTU over internet by creating a virtual network between CTU and SAMK. GSM is a TDM based network which means it has to be converted to an IP based in order to be transmitted over the internet, therefore; a Circuit Emulation Services T-Marc is used to deliver TDM over Ethernet (For the used IP address see table 3.1).

To create that Virtual Private Tunnel VPN which is a virtual end-to-end point connection via using Internet Protocol Security from internet layer family (IPsec, a protocol suite for internet protocol security), PfSense is used on one side which is an open source firewall/router computer software distribution based on FreeBSD and on the other side, Mikrotik is used which is basically used as router while its operating system based on Linux kernel (Unix-like operating system kernel), (See figure 3.1 and for the detailed configured Mikrotik, see annex 4).

1.1. IPsec Parameters Setup

IPsec provides authentication and encryption services to avoid unauthorized view and modification of data even when it travels over unprotected network. The security appliance uses usually IPsec for LAN-to-LAN VPN connections. In IPsec terminology, 'peer' is a remote access client or another secure gateway.

During tunnel establishment, the two peers negotiate security association to control authentication, encryption and key management and the negotiation is about two phases, establish the tunnel and then control the traffic within the tunnel. But it's necessary to know that IPsec does not work alone to create the VPN, Internet Security Association and Key Management Protocol (ISAKMP) is also part of the establishment which is a negotiation protocol that lets two hosts/peers agree on how to build an IPsec Security association and it separates the negotiation into two phases:

Phase 1: Creates the first tunnel that protects later ISAKMP negotiation messages

Phase2: Creates the tunnel which protects the tunnel

IPsec and ISAKMP have some parameters to configure in order to secure the VPN, (See table 2.2 for IPsec and ISAKMP parameters chosen for the VPN):

1. ISAKMP authentication - Easy to setup in a small network but not scalable with growing network
2. Encryption algorithm - It's an encryption policy that specifies the symmetric encryption algorithm which protects the transmitted data between two IPsec peers
3. Authentication algorithm or policy hash - Used to ensure data integrity
4. Keylife or lifetime - Defines the Security Association SA lifetime, shorter life means more security
5. ISAKMP group - Identifies the Diffie-Hellman group that let the two peers share secret without transmitting it to each other, Higher group number means greater security and lower means less CPU time to execute

Network Device/Segment	IPv4 Address/Range
Prague WAN IP	147.32.211.103
Prague WAN range	147.32.211.0/25
Prague LAN GW	192.168.51.1
Prague LAN range	192.168.51.0/24
Pori WAN IP	193.166.41.158
Pori WAN range	193.166.41.144/28
Pori LAN GW	192.168.1.1
Pori LAN range	192.168.1.0/24

Table 3.1 IPv4 Address Assignments

Parameters	Value
ISAKMP authentication	pre-share (Default)
Encryption algorithm - Phase 1	3DES/168-bit Triple DEs(Default)
Authentication algorithm - Phase 1	SHA-1
Lifetime - Phase 1	28800 s
Encryption algorithm - Phase 2	3DES/168-bit Triple DEs(Default)
Authentication algorithm - Phase 2	SHA-1
ISAKMP policy group	DH group 2 (1024-bit)(Default)
Lifetime - Phase 1	3600 s
Perfect Forward Secrecy PFS	Enabled (Optional)

Table 3.2 IPsec and ISAKMP parameters setup

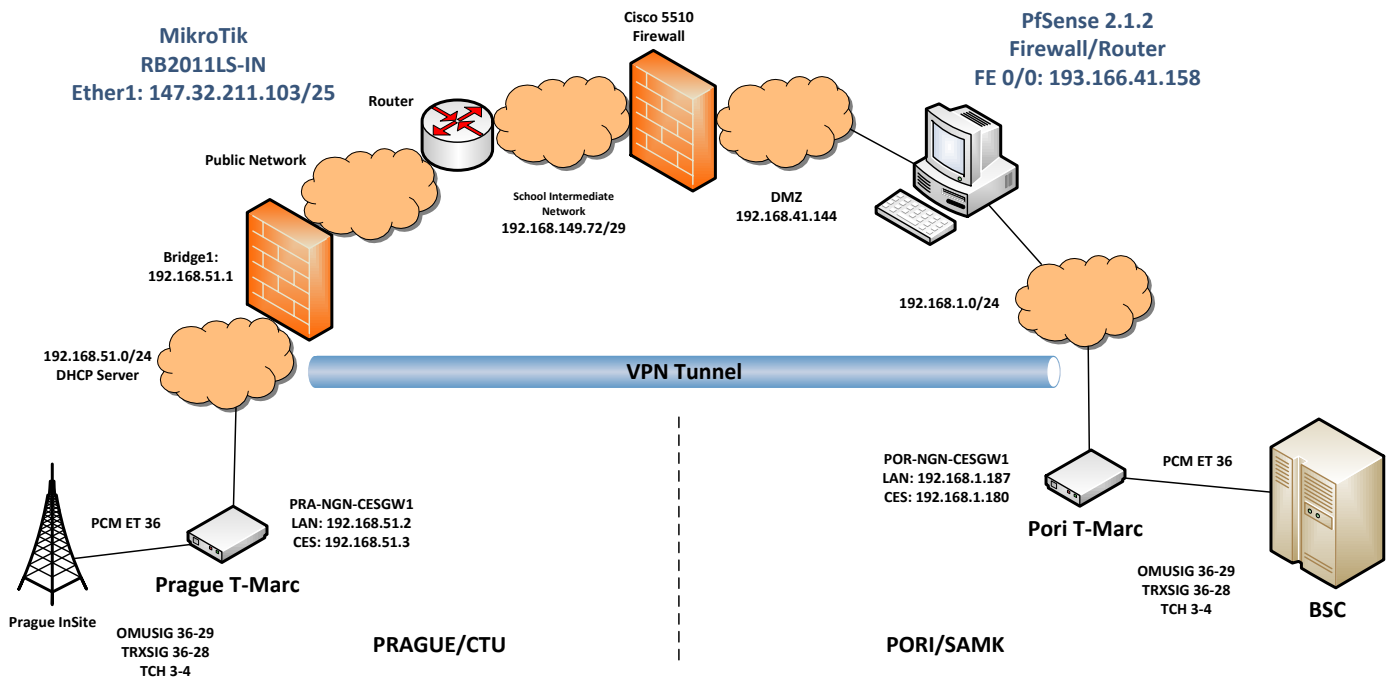


Figure 3.1 Pori-Prague Network Topology

1.2. Ethernet and Circuit Emulation Service

Telco systems T-Marc products and exactly T-Marc 254 which is one of the steps in our project taking a big role in converging up to 4 digital T1/E1 TDM trunks and 10/100/1000 copper or fiber optic links over IP, MPLS or Ethernet packed-based networks.

T-Marc supports Pseudo-wire Circuit –Emulation Service (PWE3) utilizes 802.3ah Ethernet First Mile (EFM) and 802.1ag (IEEE, ITU, MEF) standards that provide extensive end-end Operation Administration and Maintenance (OAM) facilities like performance monitoring, fault management, loopback and remote failure indications which lower OPEX through minimizing unnecessary expenses of truck rolls and providing performance and Service Legal Agreement (SLA) control and monitoring.

T-Marc also reduces service provide costs (CAPEX) via CES functionality. The platform has an integrated wire-speed non-blocking switch with user Ethernet-enhanced VLAN support, advanced QoS and reliability features providing different GoS. T-Marc has Command Line Interface (CLI) user interfaces and it can be managed by higher-level Simple Network Management Protocol (SNMP) based management platforms [1].

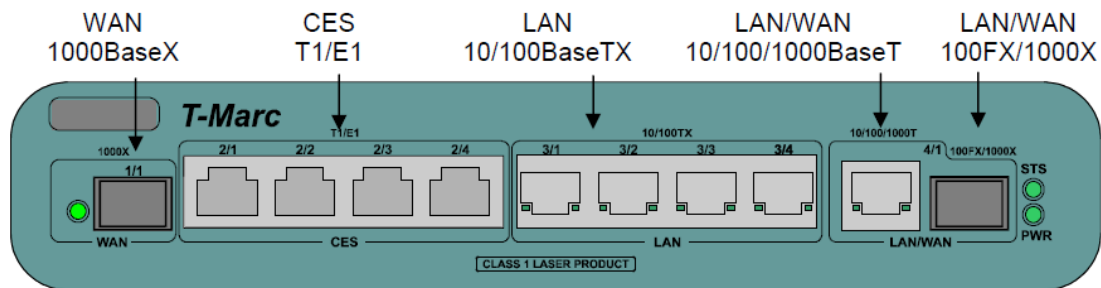


Figure 3.2 Telco Systems T-Marc 254

General Features:

- 1- Differential Service Code Point (DSCP)/Terms of Service (ToS)/802.1p QoS mode
- 2- Flexible 10/100/1000BaseT or 100BaseFX/1000BaseSX (via Small Form-Factor Pluggable (SFP)) LAN/WAN interface selection [2]
- 3- Flexible packet over T1/E1, T3/E3 (via SFP) interface selector

CES Features:

- 1- Connectivity providing for TDM devices over packet-based networks, See Figure 1.2
- 2- Up to 4 E1/T1s
- 3- E1/T1 frames or bundle of timeslots are transported over network using PWE3 encapsulation over Ethernet/IP/Martini Virtual Leased Lines (VLL)s
- 4- Support emerging market standards (MEF 3, MEF 8, IETF/SAToP, and IETF/CESoPSN) [3]

Academic Base Station

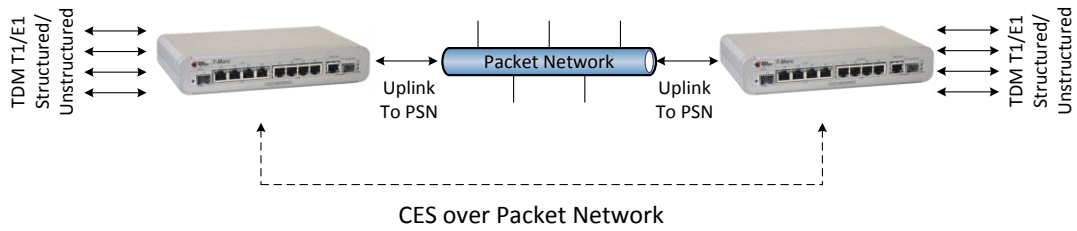


Figure 3.3 Circuit Emulation Service over Packet

Ethernet Switching Support:

- 1- 802.1Q support with full range of VLAN ID support
- 2- Port based VLAN
- 3- 256 (GigE variants) active VLANs
- 4- MAC address table: Total size 8K mac-addresses
- 5- TLS VLAN stacking Q-in-Q
- 6- 802.3x (pause) flow control and backpressure

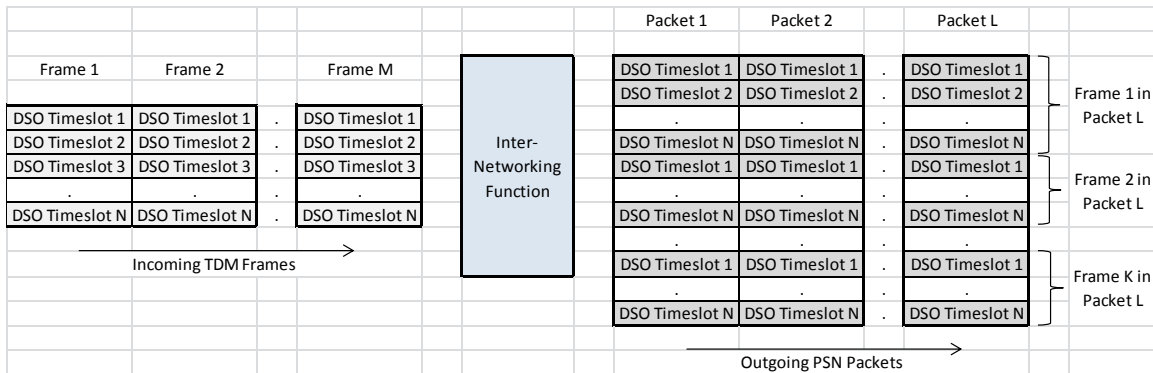


Figure 3.4 Structured Emulation

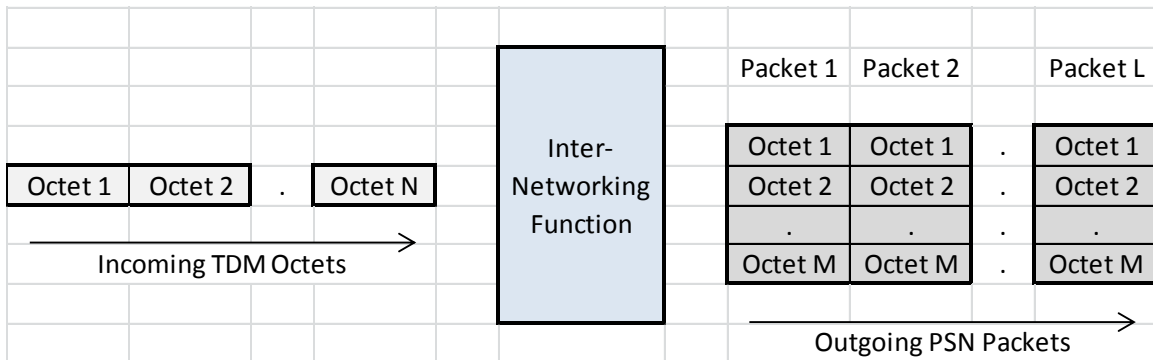


Figure 3.5 Unstructured Emulation

T-Marc Built-In Self-Test:

T-Marc can handle a set of basic hardware and validity assessments. BIST can be used whether during the startup of using the T-Marc or by request. The first mentioned BIST is automatically used by the T-Marc while the second one can be performed by request only.

Below is the list of the supported tests:

- 1- CPU Core Test
- 2- CPU Interface Test
- 3- Testing Switch Core
- 4- Data Buffer Test

Configuration of CES

Circuit Emulation Services over Packet-Switched Network (CESoPSN) is the method of tunneling TDM circuit whether it's E1 or T1 through PSN which is transparent to the end users. According to the network obtained in Pori and exactly in SAMK/NGN laboratory, CES over PSN should be used because the network in NGN laboratory is GSM which is based on TDM method, therefore; the E1 must be converted into packet data in order to transport later through the VPN and there are two types of emulating structured and unstructured as shown in figure 3.4 and 3.5 respectively.

The same E1 which was used last year for Budapest project is going to be used again for Prague but using different timeslots. The timeslots 3rd, 4th, 28th and 29th are dedicated for Prague project, 3rd and 4th are dedicated for speech traffic while 28th is dedicated for TRXSIG and 29th for OMUSIG.

Pori CES Configuration:

By using protocol CESoPSN, Pori T-Marc is configured with destination IP address 192.168.51.3 via port 2000 and UDP local port 2001 and the Tx rate is 1000 packets per second while the maximum jitter buffer delay used is 40 ms with 8/32 frames/bytes in payload. See annex 1 for more details about the parameters used in Pori CES configuration.

Prague CES Configuration:

All above parameters which are mentioned for Pori CES configuration is going to be the same for Prague side except the destination IP address which is 192.168.1.180 and using port 2000 while port 2001 is used for UDP local port with same maximum jitter buffer delay 40 ms usage. See annex 2 for Prague configuration details.

2. SAMK NGN Network Architecture

SAMK NGN laboratory holds a complete mobile communication network including 2G, 3G networks and meanwhile, fixed-line network is part of the laboratory as well (See figure 3.6).

SAMK NGN mobile network has mainly supported by two giant vendors, NSN and Ericsson which are the pioneers in providing the absolute support for establishing a mobile communication network.

Nokia Digital Exchange (DX) 200 'i-series' platform is roughly, occupying a big part of the network by including MSC, SGSN and BSC. Though it's an old release but still can serve in parallel with the newer versions. By another meaning, Nokia DX 200 is versatile, fault tolerant, modular and highly scalable with high performance which allows live migration as well as software update during live operation.

Many generic operating systems can be ported to DX 200 but Linux, ChorusOS and DMX are most frequent OS used. DX 200 platform supports the following common features:

- Distributed processing architecture
- Modularity
- Common hardware
- Fault tolerance

The distributed processing architecture in DX 200 platform facilitates high availability and reliability in systems using these platforms and meanwhile, the control functions are very easy to use. DX 200 is modular, scalable and redundant. Faulty modules can be changed without service breaks as well as during capacity increasing, hardware and software upgrades while new software releases can be tested on trial side before using them on active side.

Academic Base Station

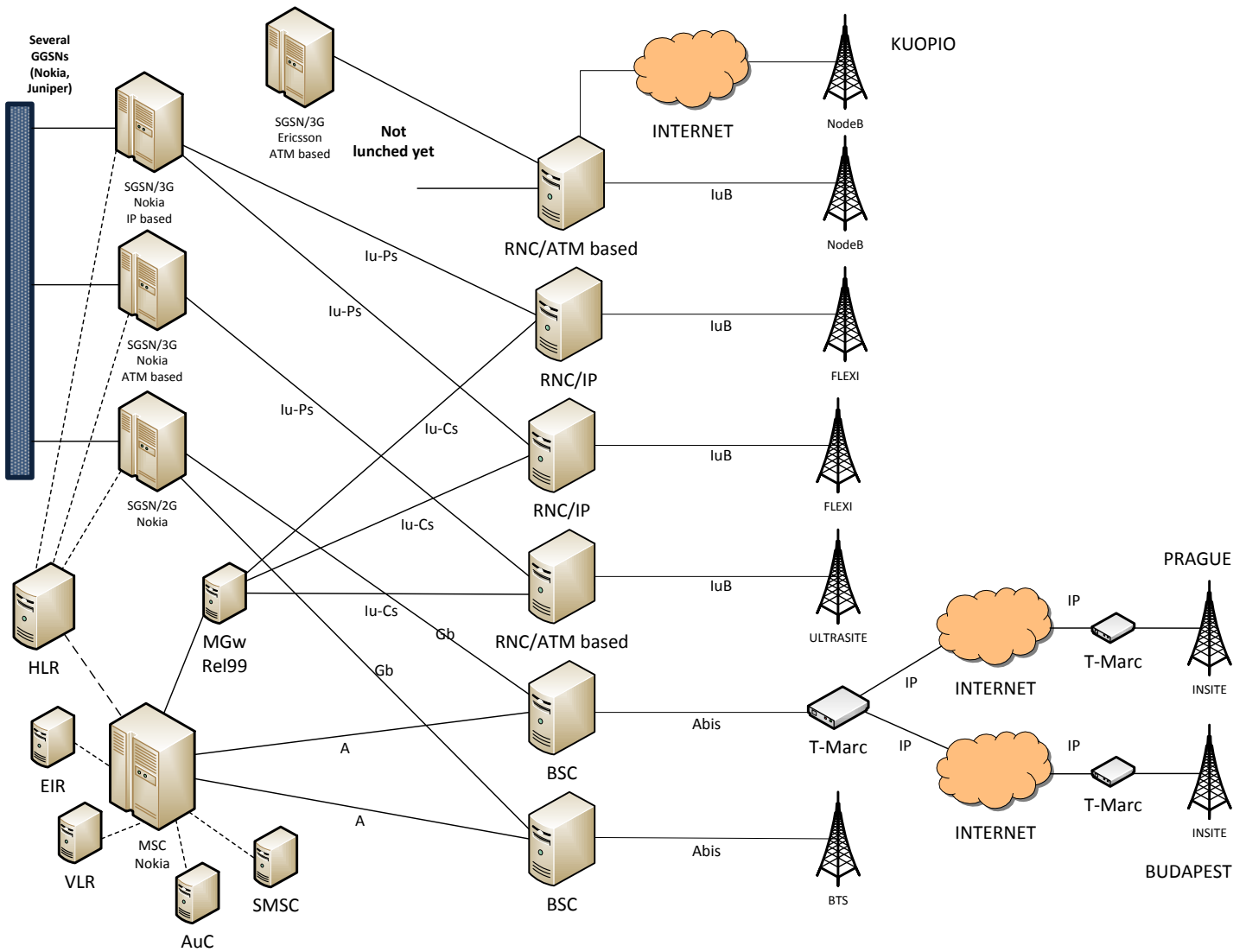


Figure 3.6 SAMK NGN network architecture

2.1. InSite base station

Nokia has introduced InSite base station for indoor use but it's output power optimized and integrated antenna. InSite usually has 1 TRX capacity for all GSM frequency bands with built-in transmission interfaces. Another feature that has been added to this base station generation which automatic picocell planning and auto channel finder while it's operating silently, See figure 3.7.

There are mainly two standard integrated antennas GSM 900 MHz and 1800/1900 MHz. The integrated antenna gain is 4 dBi for GSM 1800 while 2 dBi is used for GSM 1900 MHz. So it's ideal for indoor installation and meanwhile, the battery backup time holds for 30 minutes [4].

Nokia InSite base station supports dual band solution, 900 and 1800 MHz which means BTSs can be chained be together. The dual band feature does not only increase the capacity but also maintains the high quality of calls. As it is mentioned that InSite is optimized output power for indoor needs, this is another support for the quality of calls.

InSite can be improved by having 2 TRXs in the same cell and this is achieved by implementing overlapping and using Directed Retry feature but in such a case, the field strength with two 1-TRX BTSs is better than one 2-TRX BTS [5].



Figure 3.7 InSite base station

InSite telecom features:

1. Speech services

- **Full Rate, Half Rate and Enhanced Full Rate Speech/Data**
Usually Half Rate achieves double of available traffic which enables 8 kbit/channel and Full Rate provides 16 kbit/channels in Ater and Abis interfaces while Enhanced Full Rate improves the voice quality in all channel conditions.
- **Active Channel Interface Estimation**
InSite has ability to measure the interface level of active channel.
- **Dual Band Network support**
Usually dual band mobiles capable of performing handovers between the bands during the call.
- **DTX (Discontinuous Transmission activated by speech) support for the uplink**
By using this function, the mobile station transmits only when the subscriber is speaking.
- **Directed Retry**
Each InSite BTS TRX has seven TCHs with capacity of 2.5 Erlang and 1% blocking. By using two BTSs close to each other, the trunking gain will be 7.35 Erlang capacity with two completely overlapping InSite BTSs and this can be obtained by using Directed Retry feature [6].
- **Dynamic SDCCH**
Dynamic SDCCH allocation allows SDCCH resources to be configured according to the actual SDCCH traffic situation of a cell. In case of greater SDCCH capacity than normal, the idle TCH resources are configured for SDCCH use by the BSC.

2. Data services

- **High Speed Circuit Switched Data (HSCSD)**
This feature provides accelerated data rates for the end-user applications like WWW, file transfer and facsimile.
- **14.1 kbit/s GSM data services**

- **Non-transparent and transparent data (9600, 4800 and 2400 bit/s)**
When the data rate is able to be changed automatically during the call, especially due to increased traffic, this feature called non-transparent while transparent data is with fixed data rate even during peak-hour.
- **SMS cell broadcast/DRX**
Short textual messages can be broadcasted to all GSM mobile stations in a specific area.
- **General Packet Radio Service (GPRS)**
By supporting Coding Schemes (CS-1) which is 8 kbit/s with GMSK modulation and code rate $\frac{1}{2}$ and Coding Scheme (CS-2) providing 12 kbit/s with GMSK and code rate $\frac{2}{3}$.

Highly Automated Configuration

1. Automatic Picocell Planning and Channel Finder

When deploying InSite base station into offices, a need for easy frequency planning becomes obvious. Therefore; Automatic Picocell Planning (APP) feature has been introduced by Nokia which is easy to use tool for planning, commissioning, integration and verification.

APP has following functionalities:

- Frequency allocation for InSite base station by scanning the network and selecting an interference free frequency
- Fully automatic detection of the neighboring cells
- BTS parameterization according to the predefined parameter sets
- Coverage and performance verification

And meanwhile, APP includes Channel Finder which is used for maintaining good quality in the office and it's triggered with any change in the surrounding network and it's fast reacting to changes before the indoor quality decreases. The Channel Finder is based on statistics of reported signal levels.

2. Nokia Auto configuration

By using auto configuration, the customers are able to minimize both time and cost of network integration. This feature provides the tools for customers to use efficient and straightforward procedures to automatically configure the transmission and integrate the base station once the cellular network expanded [7].

The Nokia Auto configuration network is capable to organize itself by providing the followings:

- The new installed BTS to be automatically detected by the network
- The BTS to be able to locate the correct BSC
- The BSC is automatically recognize the required capacity by the new installed base station

Technical data

1. Integrated antenna data

The following table 1.1 is technical data for integrated antenna with regards to the used bands:

Item	GSM 900	GSM 1800	GSM 1900
Frequency of operation	Rx: 880-915 MHz Tx: 925-960 MHz	Rx: 1710-1785 MHz Tx: 1805-1880 MHz	Rx: 1850-1910 MHz Tx: 1930-1990 MHz
3 dB beamwidth (typical)	70°/50° H/E	60°/80° H/E	60°/90° H/E
6 dB beamwidth (typical)	100°/180° H/E	90°/160° H/E	90°/160° H/E
Gain (typical)	+3 dBi	+4 dBi	+4 dBi

Table 3.3 Technical data for integrated antenna [iv]

2. RF performance

Product Variant	Output Power	Output Power Range	Static Power Levels	Typical RX Sensitivity
GSM 900 (M2 Micro BTS)	80 mW	18 dB, 2 dB steps	10	-100 dBm
GSM 1800 (M3 Micro BTS)	160 mW	22dB, 2 dB steps	12	-100 dBm
GSM 1900 (M3 Micro BTS)	160 mW	22 dB, 2 dB steps	12	-100 dBm

Table 3.4 RF performance [v]

3. Configuration data

This part is done in SAMK NGN lab by using NetAct which is used for configuring, maintaining and operating. While the Pulse Code Modulation (PCM = 2Mbit/s) 36 used from BSC towards the InSite base station which is located in Budapest, the same PCM is used back for the same reason in Prague but by using different timeslots. Timeslot 29th with 64 kbit/s is used for OMU purpose signaling OMUSIG which is named after Prague by OMUPR while timeslot number 28th with 64 kbit/s is used for TRX signaling usage TRXSIG and named TRXPR.

By defining the signaling timeslots 28th and 29th, 3rd and 4th timeslots are configured for speech. This can be done by using Nokia InSite BTS Manager Software which is provided by Nokia in order to configure the Abis timeslot allocation and handling the other parameters as well. See the figure below which is the interface of the software mentioned above and the table 3.5 shows some specific configuration of the parameters used for Prague InSite base station:

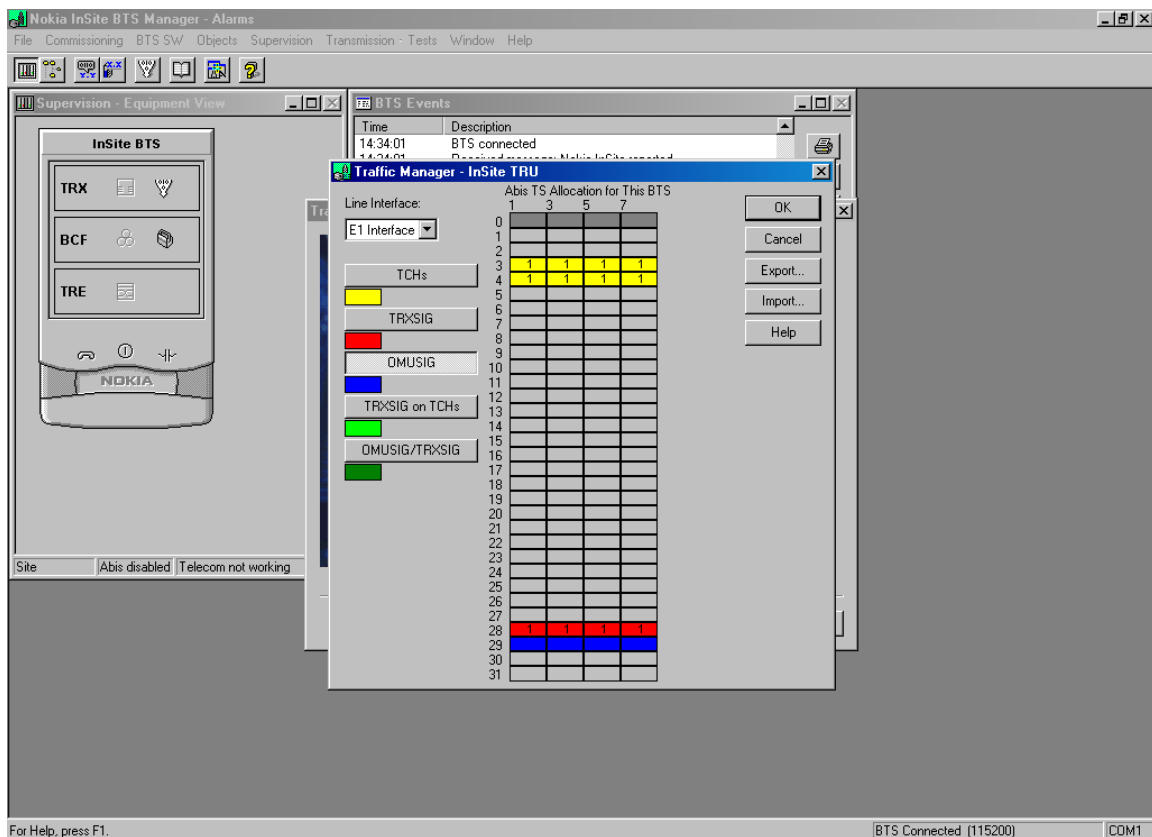


Figure 3.8 Nokia InSite BTS Manager

Site Name	PRAGUE
BCF	3
BTS	3
OMUSIG	PCM 36 - TS 29
TRXSIG	PCM 36 - TS 28
LAC	7
CI	3

Table 3.5 Prague InSite Configuration

After using 3rd, 4th, 28th and 29th timeslots, the Location Area Code (LAC) is defined and each LAC is represented in a number that many base stations share. The location area is used by the BSC and MSC to identify the location of the BTS in order to optimize the signaling used for paging when there is message needed to be broadcasted to all the BTSs by the MSC and BSC in case of location update, call related issues, broadcast messages, handover and so on. So for Prague InSite, the LAC is defined to be 7 with Cell Identity CI 3 which the same for Base Station Control Function BCF which is used to provide operation and maintenance, alarm handling and managing the operational states of all TRXs within the BTS.

InSite base station in brief:

- Timing BCCH and CCCH
- Sending BTS and MS measurements to the BSC
- RACHs detection from MSs
- Channel coding/decoding on the radio path
- Interleaving/deinterleaving on the radio path
- Encryption/decryption
- Handling frequency hopping
- GMSK modulation/demodulation
- RF Tx signal combining and power amplifying
- RF Rx signal filtering and amplifying
- Traffic channel quality reporting to the BSC

Mobile Switching Center

Is the central element of the mobile network and is called Public Land Mobile Network (PLMN) as well in the standards. All connections in classic circuit-switched network are managed by MSC and routed over the switching matrix. The MSC is split into two parts in virtual circuit-switched network, MSC Server and Media Gateway and the IP-based media gateway replaces the switching matrix while MSC Server contains the same logic for subscriber management and call control like the CPU of classic MSC.

Functions of MSC:

- Paging
- Coordination of call setup
- Dynamic allocation of resources
- Location update and registration
- Interworking between different network elements
- Handover management
- Billing for all subscribers within its area
- Reallocation of frequencies to BTSs in its area to meet heavy demands
- Encryption
- Echo canceler
- Signaling exchange among different interfaces
- Synchronization with BSSs
- Possibility of interfacing different BSSs
- Gateway to SMS

SAMK NGN MSC is based on Nokia DX 200 platform which is basically called MSCi. In GSM, DX 200 platform has served and continues to serve as a reliable platform and consists of the BSC, MSC, HLR and 2G SGSN. Over time, it has improved and evolved from subrack to cartridge and finally to I-series technology. These upgrades were base to serve the need of GPRS, EDGE and 3G networks.

Functional units of MSCi (Shown in figure 3.7) [7]:

- **Base Station Signaling Unit (BSU)**
BSU handles the CCS7 signaling between MSCi and BSC and Radio Network Controller RNC signaling between MSCi and Radio Access Network RAN. BSU also controls the PCMs linked to the Base Station Subsystem BSS. BSU can handle up to 64 PCMs ETSI/84 PCMs ANSI and 32 signaling links. For the backed up, BSU uses n+1 redundancy principle.

- **Basic Data Communications Unit (BDCU)**

It contains communication links to the operation and maintenance network (analog/digital X.25; LAN/Ethernet), to the short message center and to the billing system center.

MSCi can hold up to 4 BDCU if it has two GCS cabinets; otherwise, the maximum BDCU could have is 3 and minimum that is required for all configurations is 2 units and meanwhile, Redundancy of the OSI/LAN connection is released using OSI management.

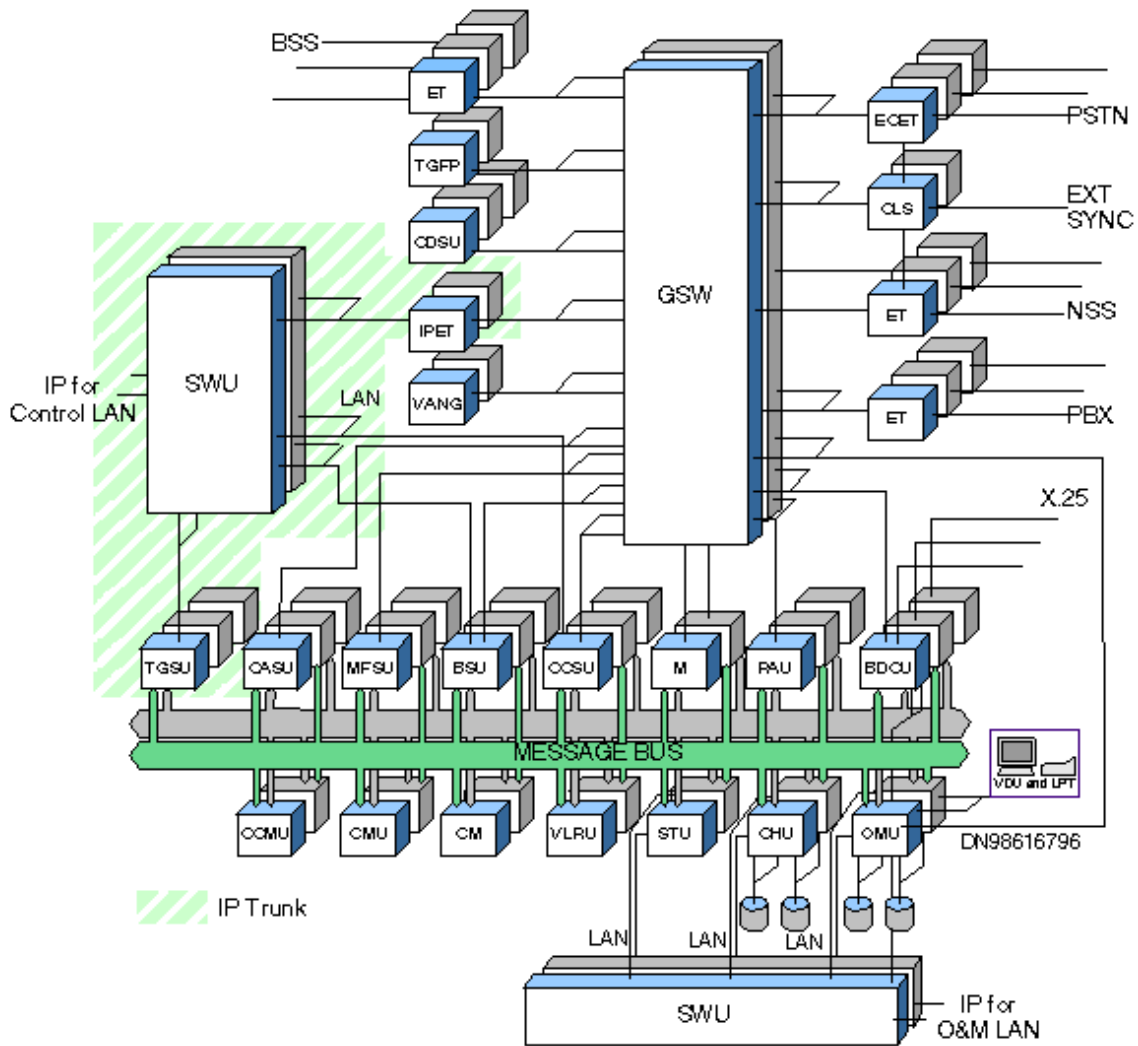


Figure 3.9 MSCi Structure with functional units [vi]

- **Cellular Management Unit (CMU)**

The CMU controls the cellular radio network and the Compact Data Service Units (CDSU) of the network element. It also provides system support functions, such as Private Numbering Plan (PNP) translations. Usually MSCi has two CMUs.
The redundancy backup principle for CMU is with 2n.
- **Central Memory (CM)**

The semipermanent files of the Central Memory contain the system tariffing, signaling routes and configuration data which are basis that other units make decisions when the call is established.
The MSCi contains usually two CMs and the redundancy principle of backup is with 2n.
- **Channel Associated Signaling Unit (CASU)**

The CASU is usually installed only when Channel Associated Signaling (CAS) is needed between MSCi and the PSTN. In the I-series MSCs, the Multi-Frequency Service Unit handles the transceiver of Multi-Frequency signals while CASU handles the CAS related line signaling functions [8].
One CAS can control up to 64 CAS PCM lines and the redundancy principle for backup is with n+1.
- **Charging Unit (CHU)**

The charging unit collects and stores charging data. One pair of CHUs is required even in the minimum configuration while four pairs is the maximum number within one MSCi and always installed in pairs. CHU also hosts the optional LAN switch unit which collects SIGTRAN and IPET control signaling data between the CCSUs and/or TGSUs and IP network. The backup will be with 2n redundancy principle [9].
- **Clock System (CLS)**

CLS contains two standard units, the Clock System Unit (CLSU) and Clock and Alarm Buffer Unit (CLBU) while there is an optional unit for synchronizing signal interfaces called Synchronization Signal Interface (SSIF-S):

 1. **Clock System Unit (CLSU)**

It is located in the Main Operation and Maintenance Cabinet (MOMC) cabinet, generates the necessary clock signal for synchronizing MSCi functions and transmitting them further to the CLBU units. One CLSU unit can handle the timing of up to 15 cartridges and for backup, it works with 2n redundancy principle.
 2. **Clock and Alarm Buffer Unit (CLBU)**

The duplicated CLBUs distribute the clock signals which are generated by the CLSUs to the units in the same cabinet. One CLBU unit handles the timing up to 15 cartridges and the backup redundancy principle is with 2n.

3. Synchronization Signal Interface (SSIF-S)

It is an optional unit and used for generating additional synchronization signals which has been fed from the exchange to partner equipment. SSIF-S usually receives an input signal from CLBUs in the same cabinet with four 2.048 MHz output signals from its four interfaces, two of them are balanced while the other two interfaces are not balanced but all of them can be used simultaneously. The output signals obey ITU-T recommendation G.703.

In case of SSIF-S units' necessity, two will be installed due to redundancy issues.

- **Common Channel Signaling Management Unit (CCMU)**

It's responsible for CCS7 network management functions of the exchange and it also features the VANG-A plug-in units which handle the voice announcement functions. The backup is with 2n redundancy principle.

- **Common Channel Signaling Unit (CCSU)**

It controls CCS7 functions for the external PCM lines towards both PSTN and the other network elements in Network Switching Subsystem NSS. Signaling traffic among NSS elements can be also carried over IP network with SIGTRAN. CCSU also monitors the Exchange Terminals (ET) allocated to the Basic Data Communication Unit (BDCU). CCSU handles up to 64 PCMs ETSI and up to 84 PCMs ANSI and 32 signaling links. The backup is with n+1 redundancy principle [10].

- **Compact Data Service Unit (CDSU)**

CDSU offers standard GSM data services which include modem-based digital connections towards the PSTN and digital connections towards ISDN. CDSUs are installed in Interworking Cabinet (IWC) of MSCi and is configured with one of three different types of data pools:

1. General Pool which is called CDSU Pool for all data call types like modem, fax and UDI.
2. UDI Pool (NDS Pool), for UDI calls to ISDN using standard ISDN Primary Rate (PRI/ISDN) interface.
3. Modem Pool or NDSM Pool, for modem-based data calls to PSTN with transmission rates up to 28.8 kbit/s and group 3 facsimile [11].

The redundancy is supported for CDSU Data pools, therefore; the exchange should always have at least two pools and with the same kind which are built into cartridges with voltage supplies from different Power Distributed Fuse Units (PDFU).

- **Exchange Terminal (ET)**

ET performs the electrical synchronization and adaptation of an external PCM line, coding and decoding of HDB3/AMI/B8ZS, alarm bits inserting into the outgoing direction and producing PCM frame structure. Usually the number of used ETs is the same as the number of GSW PCM lines.

- **Echo Canceling and Terminal (ECET)**

The same functionalities as ET except ECET provides external PCM lines which also processes with echo canceling functions and another exception is ECET used only in connections towards PSTN.
- **Group Switch 2048 (GSW 2048)**

It is the switching fabric of MSCi which is controlled by Marker. MSCi is always provided with a GSW equipped for capacity 2048 x 2048 PCMs which is already the maximum capacity while HLR GSW handles only 512 PCMs [12].
The backup is with 2n redundancy principle and each is installed in a separate GSW Cabinet (GSWC).
- **IP interfaces in MSCi**
 1. **SWU for Control LAN**

Which collects SIGTRAN signaling data from CCSUs and sends it further to the IP network via external LAN switches and routers with data rate 100 Mbit/s uplink and it's backed up with 2n redundancy principle.
 2. **SWU for OAM LAN**

Collects data from operation and maintenance signaling data from computer units and sends it to external routers and IP network at data rate of 100 Mbit/s uplink with backup of 2n redundancy principle.
 3. **LAN management over RS232**

It's carried out via CPLAN-A panel to an external serial port server (Cisco 2610) which provides connection for LAN monitoring. Usually CPLAN-A panel and RS232 cables are included with the network element delivery.
- **IP Trunk functional units**
 - Internet Protocol Exchange Terminal (IPET)**

It converts TDM speech frames arriving from the switch matrix into IP packets and sends them to the IP network.
Each IPET has an individual IP address which is defined in the call setup and it obeys speech codecs and RTP/RTCP protocols for speech framing.
- **LAN for IP Trunk**

In IP trunk, both control plane and user plane traffic are carried over IP. SWU units connect TGSWs (Control Plane Traffic) and IPETs (User Plane Traffic) to the external control LAN and then to the IP network.
The SWUs are equipped in the IPC, VLRC and GCS cabinets of MSCi. An external LAN cabinet is included also in the hardware implementation of each IP trunk which contains external SWUs, Cisco 3550 and OSRs (Optical Service Routers).
The CPLAN-A panels are routing the LAN signaling from SWUs to the external SWUs which is Cisco 3550.

- **SWU units in IPETC-A**
Switches and collects control plane and user plane IP traffic among TGSUs, IPETs and external routers. The SWU unit is connected to the external SWUs, Cisco 3550 with 100 Mbit/s data rate through via router. Backup is with 2n redundancy principle.
- **Trunk Gateway Signaling Unit (TGSU)**
Handles call control signaling functions over IP network via LAN. TGSU by using SIP supervises, control and load the IPET units with ISUP tunneling as the call control protocol over IP and it can control up to 64 PCMs with backup n+1 redundancy principle.
- **Marker (M)**
Supervises and controls the GSWs and it's responsible for connecting and releasing all connections and each MSCi contains usually two Markers which is backed up with 2n redundancy principle.
- **Message Bus (MB)**
It's the physical connection between computer units, controlled by a bi-directional Message Bus interface plug-in unit located in every computer unit with transfer rate of 32 or 64 Mbyte/s and backed up with 2n redundancy principle.
- **Multi-Frequency Signaling Unit (MFSU)**
Handles the transmission of R2 or ANSI MF signals (The main control unit is CASU). MFSU also checks the continuity, conference call control functions and identification of push-button dialing. N+1/L redundancy principle is used for backup.
The capacity of the basic configuration is [13]:
 1. 48 conference calls
 2. 32 push-button dialing identification channels
 3. 64 channel continuity checking channels
- **Operation and Maintenance Unit (OMU)**
OMU handles supervision of alarms, recovery functions and connections toward user interface (MMI-System). It has dedicated storage devices in order to save any change in the system, alarm history and so on.
- **Power Distributed Fuse Unit (PDFU)**
PDFU distributes -48/-60V power from the rectifier or batteries to the cartridges via distributed cables which each one of them has a fuse along with alarm circuits.
- **Primary Rate Access Unit (PAU)**
When there is need of PBX signaling between MSCi and PBX, PAU is needed to be installed. There are two alternative protocols for the PBX signaling; ISDN primary rate access 30B+D and DPNSS1. The minimum need of PAU is two and each holds up to 64 signaling links and controls up to 64 external PCM lines [14].



Figure 3.10 Nokia DX 200 MSCi

- **Statistical Unit (STU)**
Collects performance and measurement data from the entire network and contains LAN switch unit in order to collect SIGTRAN and IPET signaling data between CCSUs and/or TGSUs and IP network. Backup is 2n redundancy principle.
- **Storage Device Cartridge (SD4C)**
These memory units are responsible of managing large database. They have feature hard disks and magneto-optical (MO) disk drives and located in separate storage cartridges.
CHU and OMU in MSCi are equipped with storage devices and it's backed up with 2n redundancy principle. They are usually allocated in pairs, with two memory units for one pair of master units. Each pair is installed in two SD4C cartridges with one memory unit in each cartridge.
SDU contains hard disks, DAT drives and optionally floppy disk drives and 2n redundancy principle for backup.
- **Visitor Location Register Unit (VLRU)**
VLR contains information of subscribers which were served currently by MSC and it's always installed in pairs and the maximum VLR pairs is eight and each pair can hold 100,000 subscribers. The backup is 2n redundancy principle.

Base Station Controller

The Base Station Controller in the Nokia DX 200 platform basically consists of the following units (Table 4.3 shows the comparison between BSC and BTS functions):

- **BCSU**

Every BSC consists of several Base Station Controller Signaling Unit BCSU which controls all BSC functions. They are totally dependent on the amount of traffic and mainly divided into two parts for both A and Abis interfaces. MC1C cartridge holds the BCSU which is the microcomputer of BCSU. Each BCSU is responsible of several TRXs [1].

TRXs up to 16 are usually standards and TRXs that are between 16 and 32 called large capacity while up to 32 per BCSU are high capacity TRXs and they are used only with BSCi and BSC2i applications.

BCSU is usually supervising the 2 Mbit/s PCM lines where interface units and switching network are connected through [2].

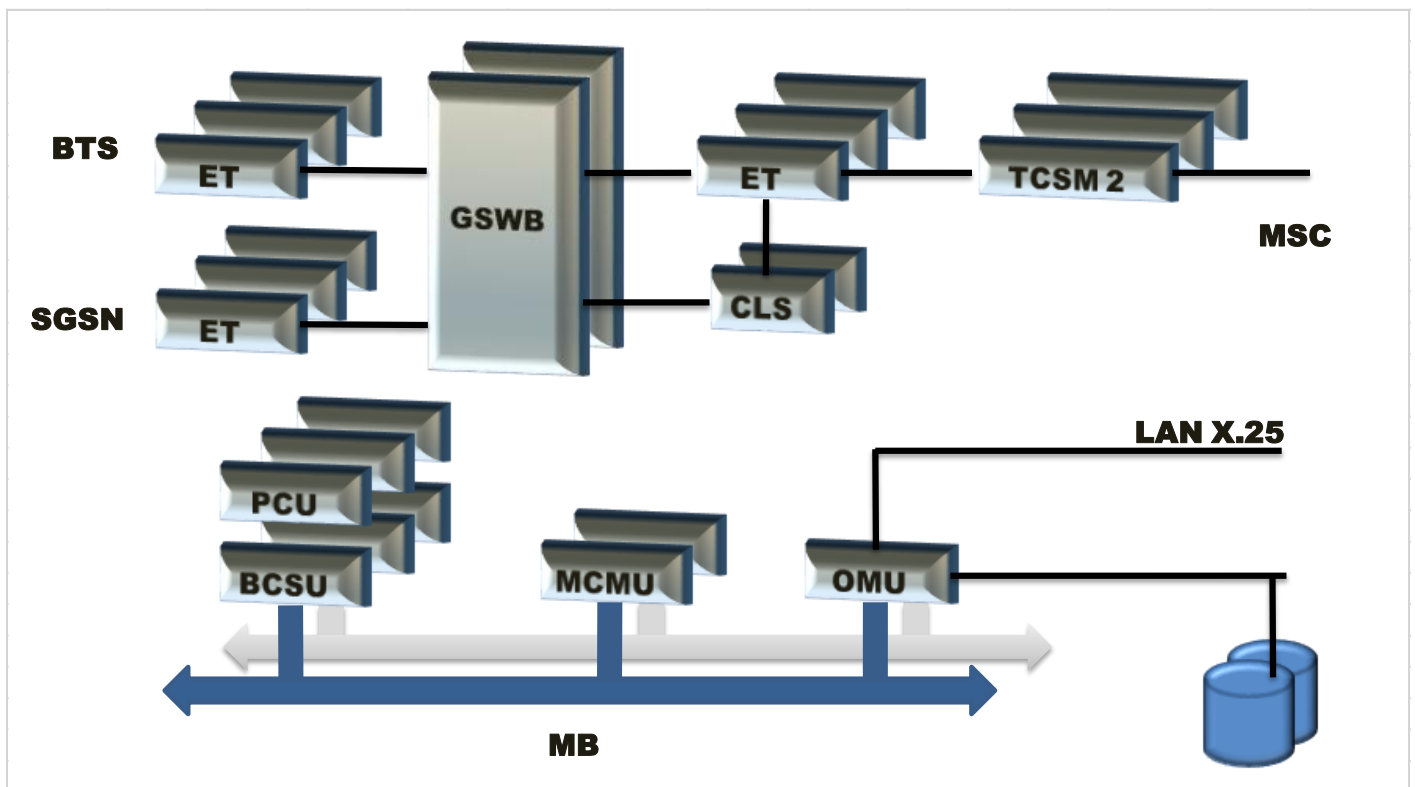


Figure 3.11 BSCi Architecture

- **Transcoder, TCSM 2**

Transcoder Submultiplexer Equipment Performing transcoding functions in the BSC and handles also submultiplexing scheme between the BSC and the transcoder. In Europe, TCSM2E is used with 2 Mbit/s (Figure shows the position of TCSM2 in the BSC architecture) and it's usually located either in the MSC or BSC but it's considered as part of BSC [3].

Nokia DX 200 TCSM2 unit has mainly four main blocks [4]:

1. Transcoder Controller plug-in unit (TRCO)
2. Several transcoder plug-in units (TR-16-S or TR12-T)
3. Exchange Terminal plug-in units (ET2E)
4. Power Supply unit (PSC1 or PSC1-S)

TCSM2 has seven trunk interfaces as maximum which are directed to the MSC and only one to the BSC. The line interfaces are handled in the ET2 units and TCSM2 supports variety of traffic alternatives for processing and transmitting. For speech, full-rate (FR), enhanced full-rate (EFR), half-rate (HR) and adaptive multirate (AMR) submultiplexing are provided while for data, full-rate and half-rate submultiplexing, High Speed Circuit Switched Data (HSCSD) transmission at the rates of maximum $2 \times$ FR data (HS2) and maximum $4 \times$ FR data (HS4) are available [5].

- **Marker and Cellular Management Unit (MCMU)**

Controls and supervises Bit Group Switch (BGW) which is responsible of establishing the needed connections to the signaling units and submultiplexing functions in the BSC and MCMU is also responsible of connecting and releasing of the switching network circuits and it's connected to OMU and BCSU through the Message Bus (MB) [6].

MCMU is performs the control functions of a switching matrix and BSC specific management functions of the radio resources. Three components are the main characters in MCMU structure which are microcomputer, Switch Control Interface and Message Bus Interface (See figure 4.8) [7].

- **Clock and Synchronization Unit (CLS)**

It's responsible of distributing timing reference signals to the functional units inside the BSC and the CLS oscillator is synchronized to an external source but usually the source is the MSC via a PCM line and up two PCM inputs more for redundancy [8].

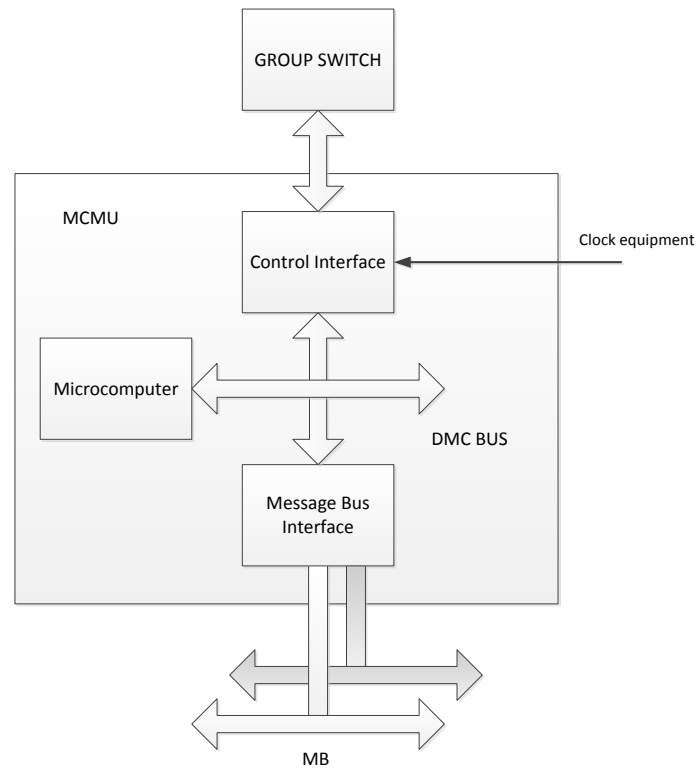


Figure 3.12 MCMU structure

- **Packet Control Unit (PCU)**

Handles all the data processing tasks which belong to GPRS traffic and responsible of implementing both Gb and Abis interfaces in the BSC but the main functions of PCU are GPRS traffic radio resource management such as connection establishment, resource allocation, scheduling and data transfer. Each PCU comes with N+1 redundancy principle [9].

- **Operation and Maintenance Unit (OMU)**

Located between BSC and higher network management system. It receives fault indications from the BSC and responsible of [10]:

- 1- Traffic control functions
- 2- Maintenance functions
- 3- System configuration administration functions
- 4- System management functions

- **Message Bus (MB)**

It's responsible of data transferring between OMU and call Control Computers of the BSC and the length of each message is indicated individually via a message length parameter at the beginning of the message [11].

- **Exchange Terminal (ET)**

It performs the electrical synchronization and adaptation of external PCM lines and all 2 Mbit/s interfaces are connected to ETs while adapt the external PCM circuits to the GSWB and synchronize to the system clock with bit frame inclusion [12].

- **Disk Units**

Each BSC has duplicated disk unit and generally fallback BSC and BTS software including BTS HW database plus traffic measurements [13].

BSC functions in brief [14]:

- Terrestrial channel management
- Traffic channel configurations and management
- Paging
- Frequency hopping control
- BTS and MS power control
- Idle channel quality monitor
- Active channel quality and field strength control
- Handover control
- BTS/BSC maintenance

Function	BTS	BSC
Function BTS BSC		X
Management of radio channels		X
Frequency hopping	X	X
Management of terrestrial channels		X
Mapping of terrestrial onto radio channels		
Channel coding and decoding	X	
Rate adaptation	X	
Encryption and decryption	X	X
Paging	X	X
Uplink signal measurement	X	
Traffic measurement		X
Authentication		X
Location registry, location update		X
Handover management		X

Table 3.6 Comparison between BSC and BTS functions

Chapter Four

MEASUREMENTS AND ASSESSMENTS

Connection Test 'end-to-end'

T-Marc or the CES circuit is adding another advantage via testing 'end-end' connection, starting from Pori T-Marc which is carrying the E1 frames over IP through the VPN tunnel to Prague T-Marc which is the destination used to emulate the E1 frames which were carried over IP to converge it back again into TDM based towards the InSite base station. The result, as given below, shows that the jitter buffer delay is about 5.894 ms while the maximum is 40.617 ms which means that the used maximum jitter during setting the T-Marc parameters up was defined properly. In the case above, it's shown that the T-Marc has self-diagnostic and monitoring functions which can be used in need of testing the VPN tunnel. See figure 4.1 for more details about the tested parameters.

```

Circuit is used for clock source           :No
Circuit clocking mode                     :Loopback-Master
Data on circuit is transmitted on TDM port :No
Data on circuit is received on TDM port   :Yes
Jitter buffer current delay               :5.894 ms
Jitter buffer max level delay             :40.617 ms
Jitter buffer min level delay             :NA
Packet Delay Variation (PDV)              :NA
Valid Ethernet packets per second        :1000
Handled Ethernet packets                  :358070061
Late Ethernet packets                     :384136
Lost Ethernet packets                     :NA
Malformed Frames                          :0
Unordered Ethernet packets                :3482
Packets with L bit                        :234634549
Packets with R bit                        :99
Underrun Ethernet packets                 :2382
Overrun Ethernet packets                  :0
Out-of-sequence Ethernet packets          :0
Duplicate Ethernet packets                :NA
Current Tx rate (packets per second)      :1000
Restarts transmit bit stream               :52
Restarts receive bit stream               :1
Peer Information                           :
  Peer is available                        :
  Peer next hop MAC Address                :00:22:19:56:E0:BC

```

Figure 4.1 T-Marc connection test

NetHawk Protocol Analyzer

The NetHawk GSM Analyzer is an effective PC-based protocol analyzer used in real-time for monitoring and analysis of GSM, GPRS, EDGE and SS7 networks. It's easy-to-use and powerful tool for protocol monitoring and call scenarios and session analysis for both network element manufacturers and operators providing crucial help in many areas like:

- System integration
- Interoperability testing
- Installation and commissioning
- Network optimization
- Network monitoring
- Troubleshooting

It's wide support for 2G/2.5G protocols and they can be analyzed at multiple network interfaces simultaneously. In GERAN (GSM EDGE Radio Access Network), Abis, A and Gb interfaces can be traced easily while at core network, there is signaling number 7 such as C, D, E, F, G, Gc, Gd, Gf, Gr and High Speed Signaling Link (HSL), SIGTRAN (SS7 over IP), PSTN, Ga, Gi, Gn, Gp and Gs which can be monitored as well [1].

NetHawk is also pioneer in tracing, filtering calls and sessions by following Circuit-Switched calls and GPRS sessions. Filtering is done within different ways with reference to problems encountered in IMSI, IMEI or TMSI values or call failure issues such as drop calls, silent calls within a certain area and important to be mentioned that call trace can handle verification of BSC in controlling BTSs and handover procedures.

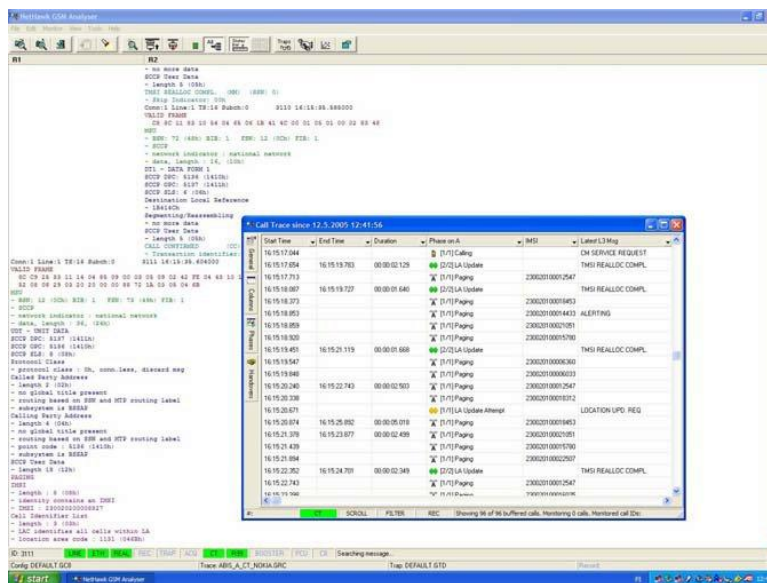


Figure 4.2 NetHawk analyzer interface

Mobility Management

Once the Mobile Station MS started to boot, it sends location area requests in order to update its location. By providing the Location Area Identity which includes Mobile Country Code (MCC = 244), Mobile Network Code (MNC = 15) and Location Area Code (LAC = 7). The IMSI is attached to send the authentication request and the identity request as well, the location update is accepted after responding clearly to the authentication and identity requests and according to the given parameters which are already defined in HLR, the MS is temporarily registered to provided location area in Visitor Location Register VLR while it's attached to the network. This procedure data is obviously provided and in real-time via NetHawk analyzer while it's connected to the A-interface (see figure 4.3) [2].

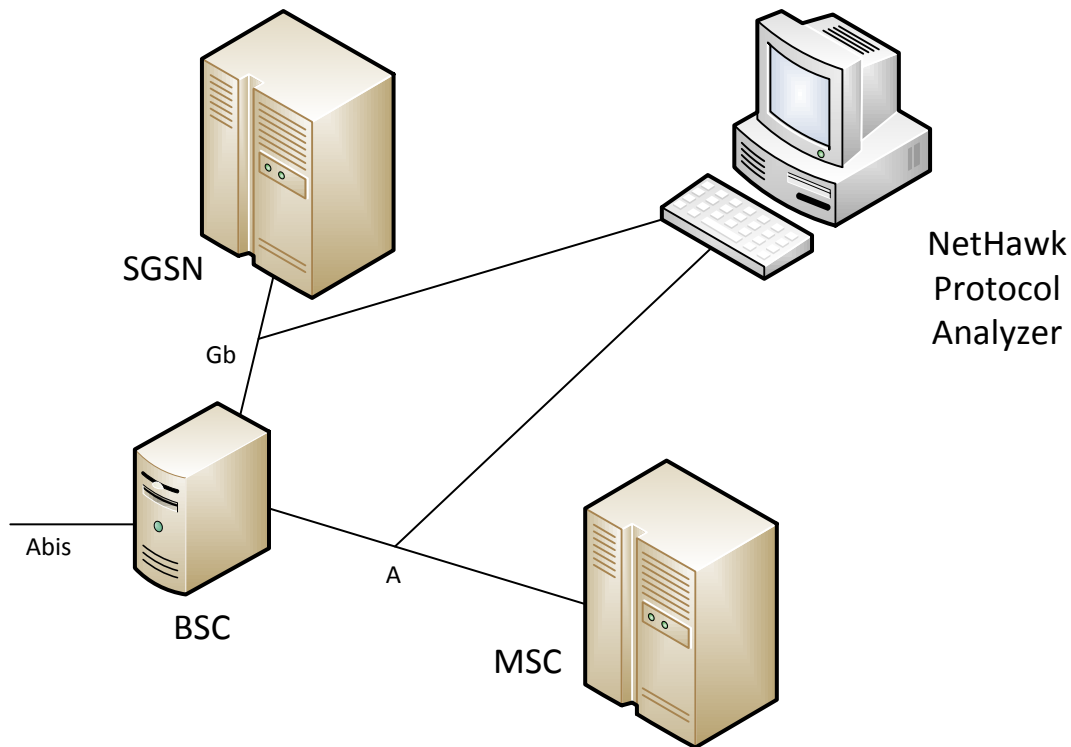


Figure 4.3 Nethawk Analyzer

Once the MS is attached to the network, the Connection Management CM service request will be sent to provide the services such as mobile originating call, emergency call, short message transfer and the supplementary services like call forwarding and call barring.

Some other CM services within the request which has been sent are the Radio Frequency RF power capability to control the strength of the MS signal in order to prevent interference and meanwhile, the MS user phone class or the cellphone version is sent because the cellphone will clarify which service should be provided, table 1.1 shows the detailed procedure for Mobility Management.

Ciphering key sequence is also part of the message that includes encryption algorithm A5 types namely A5/1, A5/2 and A5/3 which are a stream of ciphering keys used to protect the confidentiality of the voice calls over air-communication. The table 1.1 shows the procedure of the Mobility Management starting from location update to the acceptance of the Cm services [3].

Wireshark

It's an open source network packet analyzer used to troubleshoot network problems, test security issues while developers use to debug protocol implementations, normal users use it in order to learn network protocol internals. The variety in using Wireshark, made it one of the best packet analyzer available nowadays [4] (Figure 4.4 shows the interface of WireShark).

Wireshark captures packets and then allows the users to examine their content and the important point is that all these can be done in real-time. With WireShark, all traffic data and what's inside a network cable are visible but it is not an intrusion detection system and does not manipulate things on the network except measuring [5].

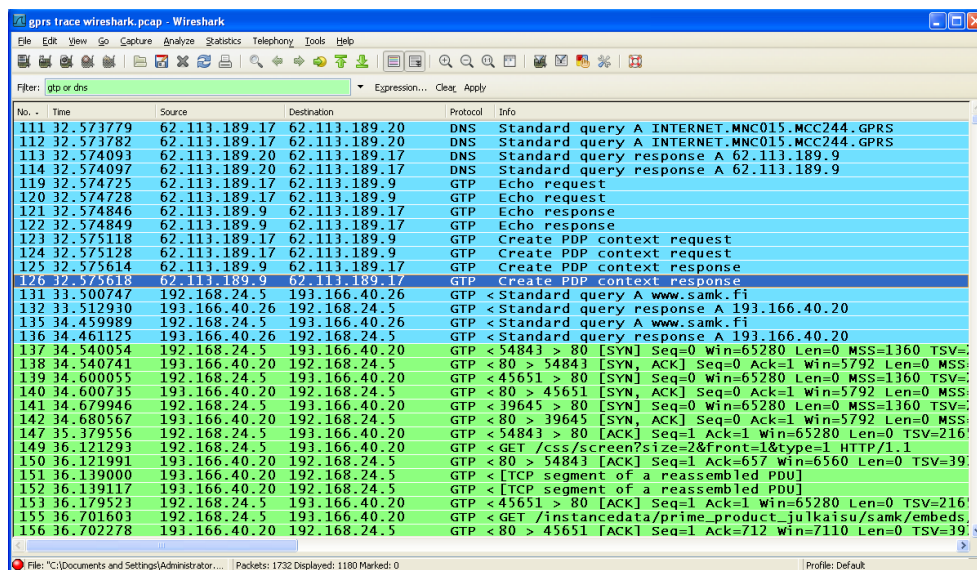


Figure 4.4 Wireshark interface

Direction Chart	Connection	Stack	Protocol	Content
BSC --> CS-MGW	A-interface	A	L3MM	LOCATION UPD REQ
Node1 --> Node2	VLR-HLR	Signaling over PCM	MAP	SEND AUTHENTICATION INFO ARG
Node1 <-- Node2	VLR-HLR	Signaling over PCM	MAP	SEND AUTHENTICATION INFO RES
BSC <-- CS-MGW	A-interface	A	L3MM	AUTH REQ
BSC --> CS-MGW	A-interface	A	L3MM	AUTH RESP
BSC <-- CS-MGW	A-interface	A	L3MM	ID REQ
BSC --> CS-MGW	A-interface	A	L3MM	ID RESP
Node1 --> Node2	VLR-HLR	Signaling over PCM	MAP	CHECK IMEI ARG
Node1 <-- Node2	VLR-HLR	Signaling over PCM	MAP	CHECK IMEI RES
Node1 --> Node2	VLR-HLR	Signaling over PCM	MAP	UPDATE LOCATION ARG
Node1 <-- Node2	VLR-HLR	Signaling over PCM	MAP	INSERT SUBSCRIBER DATA ARG
Node1 --> Node2	VLR-HLR	Signaling over PCM	MAP	INSERT SUBSCRIBER DATA RES
Node1 <-- Node2	VLR-HLR	Signaling over PCM	MAP	UPDATE LOCATION RES
BSC <-- CS-MGW	A-interface	A	L3MM	LOCATION UPD ACC
BSC --> CS-MGW	A-interface	A	L3MM	LOCATION UPD REQ
Node1 --> Node2	VLR-HLR	Signaling over PCM	MAP	SEND AUTHENTICATION INFO ARG
Node1 <-- Node2	VLR-HLR	Signaling over PCM	MAP	SEND AUTHENTICATION INFO RES
BSC <-- CS-MGW	A-interface	A	L3MM	AUTH REQ
BSC --> CS-MGW	A-interface	A	L3MM	AUTH RESP
BSC <-- CS-MGW	A-interface	A	L3MM	ID REQ
BSC --> CS-MGW	A-interface	A	L3MM	ID RESP
Node1 --> Node2	VLR-HLR	Signaling over PCM	MAP	CHECK IMEI ARG
Node1 <-- Node2	VLR-HLR	Signaling over PCM	MAP	CHECK IMEI RES
Node1 --> Node2	VLR-HLR	Signaling over PCM	MAP	UPDATE LOCATION ARG
Node1 <-- Node2	VLR-HLR	Signaling over PCM	MAP	INSERT SUBSCRIBER DATA ARG
Node1 --> Node2	VLR-HLR	Signaling over PCM	MAP	INSERT SUBSCRIBER DATA RES
Node1 <-- Node2	VLR-HLR	Signaling over PCM	MAP	UPDATE LOCATION RES
BSC <-- CS-MGW	A-interface	A	L3MM	LOCATION UPD ACC
BSC --> CS-MGW	A-interface	A	L3MM	CM SERV REQ
BSC <-- CS-MGW	A-interface	A	L3MM	CM SERV ACC
BSC --> CS-MGW	A-interface	A	L3MM	CM SERV REQ
BSC <-- CS-MGW	A-interface	A	L3MM	CM SERV ACC
BSC --> CS-MGW	A-interface	A	L3MM	CM SERV REQ
BSC <-- CS-MGW	A-interface	A	L3MM	CM SERV ACC

Table 4.1 Mobility Management

GPRS Activation Procedure

Each Mobile Station is basically going through three steps during its stay in the network via Mobility Management which defines the state of the MS. These three states are; idle state when the Mobile Station is not attached GPRS MM, standby state when the MS has attached to GPRS but still some location information is missing and finally ready state where the location data is identified on cell level.

Once the MS attach is accepted through identifying the location area (Mobile Equipment ME release, GERAN feature package type, access technology and RF power class with 22 dBm), the MS has to go through another step which is activating Packet Data protocol PDP context by introducing subscriber's session information and PDP context is a data structure built on both SGSN Serving GPRS Support Node and GGSN Gateway GPRS Support Node which includes chosen IP address for the Mobile Station, IMSI and the Tunnel Endpoint ID at GGSN with Tunnel Endpoint ID at SGSN side. See annex 4 that provides the detailed trace message for GPRS activation procedure.

In fact, PDP type number is IP version 4 with given access point name and using UDP protocol and in our case, the source IP address used is 192.168.24.2 while the destination is 193.166.152.241.

PDP context is usually stored Mobile Station, HLR, SGSN and GGSN and contains mapping and routing data for transmitted packages from GGSN to MS and vice versa and during the activation of PDP context, Quality of Service QoS profile verification is also included in order to indicate the radio and network resources which are required for data exchanges.

The QoS profile includes:

- **Precedence class**
Specifies three priority levels; High, Normal and Low for each user
- **Delay class**
The end-to-end transfer time which includes all delay time within the GPRS network and it refers to four different levels (Our tracking of the PDP context message indicates that the best effort is chosen which means without constraints)
- **Reliability class**
Different reliability classes are defined:
 1. Probability of data loss
 2. Probability of data delivered out of sequence
 3. Duplicate data delivery probability
 4. Corrupted data probability

- **Throughput class**

Characterizes the expected bandwidth which required for PDP context and it's defined by:

1. Peak throughput which identifies the maximum transfer data rate and this achievement depends on Mobile Station ability and radio resource availability but it's independent of the delay class
2. Mean throughput identifies the average transfer data rate across the GPRS network and best-effort mean throughput is indicated according to our tracing message

Nokia NetMonitor

Nokia provides Network Monitor Mode for most of its cell phone users which is used for network parameter measurements such as serving cell information, identifying neighbor cells, network selection display and other network parameters. Below some figures (Figure 4.5) from Prague InSite BTS shows the recorded parameters via using Nokia 7110 including 130 pages of parameters:

- **Page 01: Serving Cell information**

1. Carrier number = 761
2. Rx level = -86 dBm
3. Path loss criterion C1 = 20 (Used for cell selection and for satisfaction should be $C1 > 0$)
4. Reselection criterion C2 = 20 (Used for cell reselection only)
5. Current channel = CCCH (Common Control Channel)



Figure 4.5 Nokia NetMonitor

- **Page 11: Network parameters**

1. The first row shows the Country Code CC which is MCC = 244 and Network Code NC which represents MNC = 15
2. Location Area Code LAC = 7
3. Carrier number = 761
4. Cell Identity CI = 3

Chapter Five

CONCLUSION

During this project, I have been talking about how easy is to establish a mobile base station anywhere when you have a testbed and no matter where it could be located and as it's known because of the internet, I was able to build our base station far from the core network through the VPN tunnel but to transmit the TDMA frames over IP in packets, I must use an emulator in order to be able to continue with this process so when I use emulator to carry the TDMA frames, I have to use another emulator in the other end to return the signal to its origin. And using extra equipment means extra money which is basically unacceptable in telecommunication world and also economically should be with less expense while technically I face some complexity.

So what could be next?

After establishing the network in Prague, I can establish another InSite BTS working as a neighbor to the first one since the T-Marc is able to handle four Pulse Code Modulations (PCM) at the same time (See figure I) but what is the advantage or the aim form this step? When I have two InSite BTSs at one location, there will be different scenarios held such handover, location updating of the MS while moving from one InSite BTS to the other InSite BTS and also the different scenarios of handover; hard and soft handovers and meanwhile, handover between two BTSs, two BSCs or two MSCs could be held.

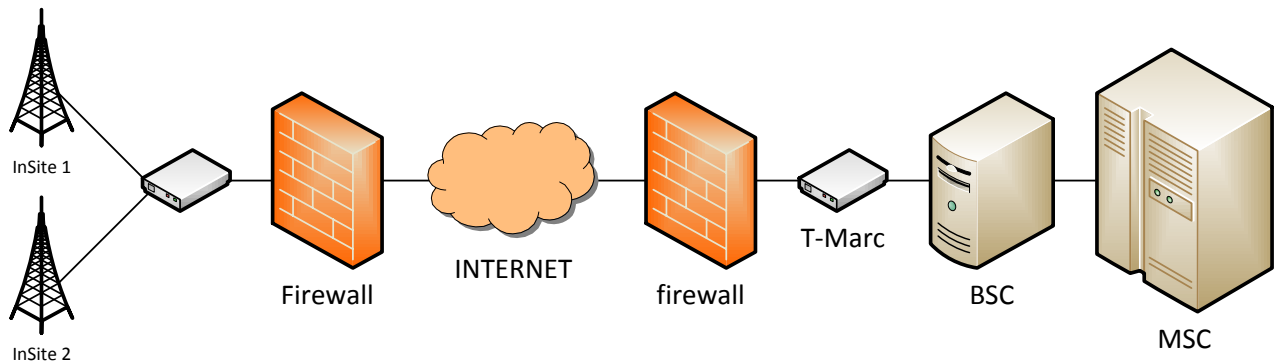


Figure 5.1 Two InSite BTSs network

In 3G network, Radio Access Network (RAN) and the rest of the network element are based on IP which means no more emulators will be needed and the network will be pure IP based as shown in figure II describing the testbed for 3G network.

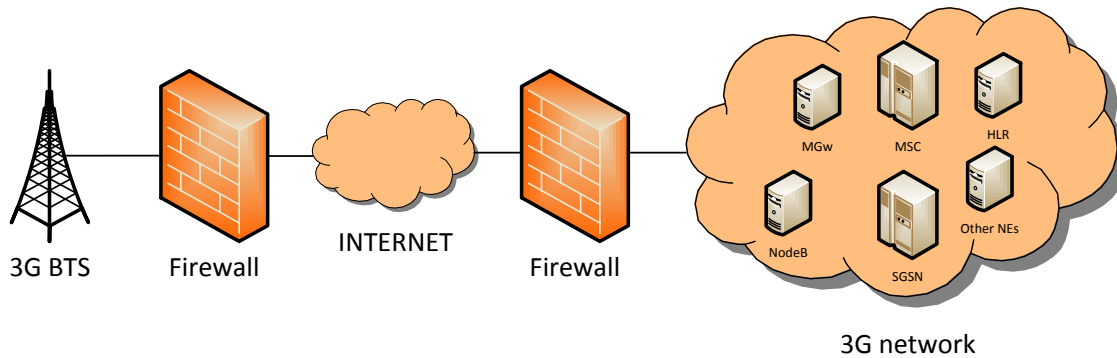


Figure 5.2 3G network with the academic base station

Another idea is to keep the GSM InSite BTS and add a 3G BTS so in this case there will be more scenarios and challenges to face such as handover between two different generation networks including the above mentioned handovers, location updating, call setup, GPRS to 3G data service and vice versa as shown in the below figure III.

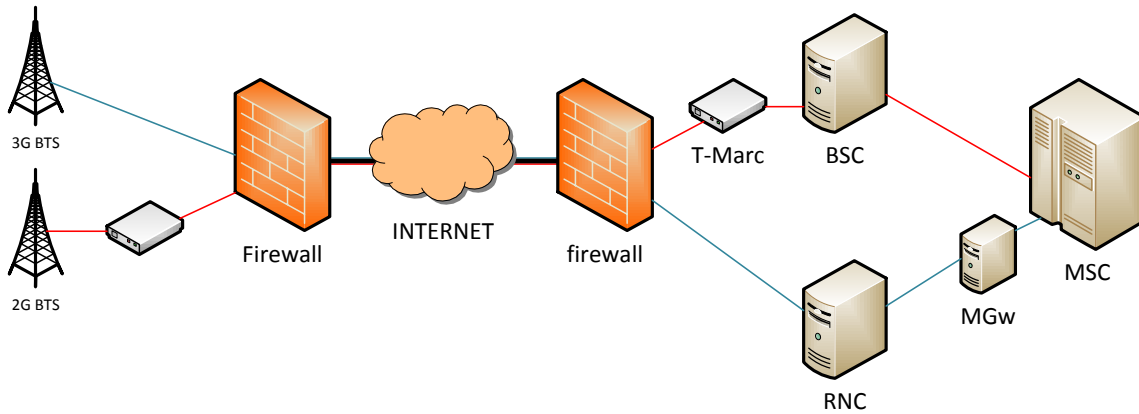


Figure 5.3 Two different generation networks

ANNEX

Annex 1 - Pori CES Configuration

POR-NGN-CESGW1#show ces 1/2 circuit 2

```
Ces circuit 2                               :Enabled
Circuit Enable Time                         :MON FEB 01 21:50:16 1993
Circuit mode type is                       :Structured
Used protocol                              :cesopsn
Destination ip                             :192.168.51.3 port 2000
UDP Local port                             :2001
Vlan/Priority                              :Disabled
Maximum jitter buffer delay                :40 ms
Frames/Bytes in payload                    :8/32
```

Timeslot configuration of channel-group 2

```
-----
|Timeslots | 0  0  1  1  2  2  33 |
|           | 0  5  0  5  0  5  01 |
|-----|
```

```
-----
|Port 1    | f--XX-----XX-- |
|Port 2    | ----- |
|Port 3    | ----- |
|Port 4    | ----- |
|-----|
```

```
X time slot is selected
- time slot is not selected
f framing information regenerated
s signaling information is transmitted over a path other than the data stream
Circuit is used for clock source           :No
Circuit clocking mode                     :Loopback-Master
Data on circuit is transmitted on TDM port :No
Data on circuit is received on TDM port   :No
Jitter buffer statistics information exists :No
Valid Ethernet packets per second         :0
Handled Ethernet packets                  :0
Late Ethernet packets                     :0
Lost Ethernet packets                     :NA
Malformed Frames                          :0
Unordered Ethernet packets                :0
Packets with L bit                        :0
Packets with R bit                        :0
Underrun Ethernet packets                 :0
Overrun Ethernet packets                  :0
Out-of-sequence Ethernet packets          :0
Duplicate Ethernet packets                :NA
Current Tx rate (packets per second)      :1000
Restarts transmit bit stream               :1
Restarts receive bit stream               :0
Peer Information                           :
Peer not available
```

Annex 2 - Prague CES Configuration

Prague-NGN-CESGW#sho ces 1/2 circuit 1

```
Ces circuit 1 :Enabled
Circuit Enable Time :FRI JAN 01 00:34:25 1993
Circuit mode type is :Structured
Used protocol :cesopsn
Destination ip :192.168.1.180 port 2001
UDP Local port :2000
Vlan/Priority :Disabled
Maximum jitter buffer delay :40 ms
Frames/Bytes in payload :8/32
```

Timeslot configuration of channel-group 1

```
-----
|Timeslots |0  0  1  1  2  2  33 |
|          |0  5  0  5  0  5  01 |
|          |-----|
```

```
-----
|Port 1    |f--XX-----XX-- |
|Port 2    |-----|
|Port 3    |-----|
|Port 4    |-----|
|          |-----|
```

```
-----
X time slot is selected
- time slot is not selected
f framing information regenerated
s signaling information is transmitted over a path other than the data stream
Circuit is used for clock source :No
Circuit clocking mode :Holdover
Data on circuit is transmitted on TDM port :No
Data on circuit is received on TDM port :No
Jitter buffer statistics information exists :No
Valid Ethernet packets per second :0
Handled Ethernet packets :0
Late Ethernet packets :0
Lost Ethernet packets :NA
Malformed Frames :0
Unordered Ethernet packets :0
Packets with L bit :0
Packets with R bit :0
Underrun Ethernet packets :0
Overrun Ethernet packets :0
Out-of-sequence Ethernet packets :0
Duplicate Ethernet packets :NA
Current Tx rate (packets per second) :1000
Restarts transmit bit stream :1
Restarts receive bit stream :0
Peer Information :
Peer not available
```

Annex 3 - GPRS Procedure over Gb

R1

ATTACH REQUEST

Skip Indicator: 0 (00h)

MS Network Capability

- Length: 2 (02h)
- Encryption algorithm GEA/1 available (1)
- SM capabilities via dedicated channels: MS supports mobile terminated point to point SMS via CS domain (1)
- SM capabilities via GPRS channels: MS supports mobile terminated point to point SMS via PS domain (1)
- Use of default alphabet over UCS2 preferred (0)
- SS Screening Indicator: Capability of ellipsis notation and phase 2 error handling (01h)
- ME does not support SoLSA (0)
- MS supporting R99 or later versions (1)
- MS supports BSS packet flow procedures (1)
- Encryption algorithm GEA/2 available (1)
- Encryption algorithm GEA/3 not available (0)
- Encryption algorithm GEA/4 not available (0)
- Encryption algorithm GEA/5 not available (0)
- Encryption algorithm GEA/6 not available (0)
- Encryption algorithm GEA/7 not available (0)
- Location request notification via PS domain not supported (0)

Attach Type

- GPRS attach (01h)
- No follow-on request pending (0)

GPRS Ciphering Key Sequence Number: 7 (07h)

DRX Parameter

- Split PG Cycle Code: 7 (07h)
- CN Specific DRX Cycle Length Coefficient: Not specified by the MS (00h)
- Split PG cycle on CCCH not supported (0)
- Max. 8 sec non-DRX mode after transfer state (04h)

Mobile Identity

- Length: 5 (05h)
- TMSI/P-TMSI: CD7E753B

Routing Area Identification

- Mobile Country Code: 244
- Mobile Network Code: 15
- Location Area Code: 7 (07h)
- Routing Area Code: 1 (01h)

MS Radio Access Capability

- Length: 12 (0Ch)

R2

Academic Base Station

- Access Technology Type: GSM 900-E (01h)
- Access Capabilities Struct:
 - Length: 51 bits (33h)
 - Radio Capability: 4 (04h)
 - Encryption algorithm A5/1 available (1)
 - Encryption algorithm A5/2 available (1)
 - Encryption algorithm A5/3 not available (0)
 - Encryption algorithm A5/4 not available (0)
 - Encryption algorithm A5/5 not available (0)
 - Encryption algorithm A5/6 not available (0)
 - Encryption algorithm A5/7 not available (0)
 - Controlled early classmark sending implemented (1)
 - PS capability not present (0)
 - VGCS capability and notifications not wanted (0)
 - VBS capability and notifications not wanted (0)
 - HSCSD Multislot Class: 6 (06h)
 - GPRS Multislot Class: 10 (0Ah)
 - GPRS extended dynamic allocation capability not implemented (0)
 - EGPRS Multislot Class: 6 (06h)
 - EGPRS Extended Dynamic Allocation Capability not implemented (0)
 - RF Power Class: E3, max 23 dBm
 - COMPACT interference measurement capability is not implemented (0)
 - ME is release '99 onwards (1)
 - UMTS FDD not supported (0)
 - UMTS 3.84 Mcps TDD not supported (0)
 - CDMA2000 not supported (0)
 - UMTS 1.28 Mcps TDD not supported (0)
 - GERAN feature package 1 supported (1)
 - Modulation based multislot class not supported (0)
- Access Technology Type: GSM 1800 (03h)
- Access Capabilities Struct:
 - Length: 21 bits (15h)
 - RF Power Class: 1, max 1 W (30 dBm)
 - Controlled early classmark sending implemented (1)
 - PS capability not present (0)
 - VGCS capability and notifications not wanted (0)
 - VBS capability and notifications not wanted (0)
 - RF Power Class: E2, max 22 dBm
 - COMPACT interference measurement capability is not implemented (0)
 - ME is release '99 onwards (1)
 - UMTS FDD not supported (0)
 - UMTS 3.84 Mcps TDD not supported (0)
 - CDMA2000 not supported (0)

Academic Base Station

- UMTS 1.28 Mcps TDD not supported (0)
- GERAN feature package 1 supported (1)
- Modulation based multislot class not supported (0)
- Timer Value: 44 sec (16h)

IDENTITY RESPONSE

Skip Indicator: 0 (00h)

Mobile Identity

- Length: 8 (08h)
- IMSI: 244151111110019

ATTACH COMPLETE

Skip Indicator: 0 (00h)

ACTIVATE PDP CONTEXT REQUEST

Transaction Identifier: 0 (00h)

TI Flag: The message is sent from the side that originates the TI (0)

Network Service Access Point Identifier: 5 (05h)

LLC SAPI: 3 (03h)

Quality of Service

- Length: 3 (03h)
- Reliability Class: Subscribed (MS only) (00h)
- Delay Class: Subscribed (00h)
- Precedence Class: Subscribed (00h)
- Peak Throughput: Subscribed (00h)

IDENTITY REQUEST

Skip Indicator: 0 (00h)

Identity Type 2: IMSI (01h)

Force to Standby: Not indicated (00h)

ATTACH ACCEPT

Skip Indicator: 0 (00h)

Attach Result

- GPRS only attached (01h)
- Force to Standby: Indicated (01h)
- Timer Value: 30 min (05h)
- Radio Priority: Priority level 3 (03h)
- Radio Priority for TOM8: Priority level 4 (00h)

Routing Area Identification

- Mobile Country Code: 244
- Mobile Network Code: 15
- Location Area Code: 7 (07h)
- Routing Area Code: 1 (01h)
- Timer Value: 44 sec (16h)

P-TMSI

- Length: 5 (05h)
- TMSI/P-TMSI: CD7D233B

Academic Base Station

- Mean Throughput: Best effort (1Fh)

Packet Data Protocol Address

- Length: 2 (02h)
- PDP Type Organisation: IETF allocated address (01h)
- PDP Type Number: IPv4 (21h)

Access Point Name

- Length: 9 (09h)
- Value: internet

Protocol Configuration Options

- Length: 48 (30h)
- Configuration Protocol: 0 (00h) (interpreted as PPP)
 - Password Authentication Protocol (PAP) (C023h)
 - Length: 6 (06h)
 - Contents: 01 01 00 06 00 00
 - Internet Protocol Control Protocol (IPCP) (8021h)
 - Length: 16 (10h)
 - Contents: 01 01 00 10 81 06 00 00 00 00 83 06 00 00 00 00
 - Internet Protocol Control Protocol (IPCP) (8021h)
 - Length: 16 (10h)
 - Contents: 01 00 00 10 81 06 00 00 00 00 83 06 00 00 00 00

ACTIVATE PDP CONTEXT ACCEPT

Transaction Identifier: 0 (00h)

TI Flag: The message is sent to the side that originates the TI (1)

LLC SAPI: 5 (05h)

Quality of Service

- Length: 3 (03h)
- Reliability Class: Unack GTP, ack LLC and RLC, protected data (02h)
- Delay Class: Delay class 4 (best effort) (04h)
- Precedence Class: Normal priority (02h)
- Peak Throughput: Up to 256 000 octet/s (09h)
- Mean Throughput: Best effort (1Fh)

Radio Priority: Priority level 3 (03h)

Packet Data Protocol Address

- Length: 6 (06h)
- PDP Type Organisation: IETF allocated address (01h)
- PDP Type Number: IPv4 (21h)
- Address: 192.168.24.2

Protocol Configuration Options

- Length: 27 (1Bh)
- Configuration Protocol: 0 (00h) (interpreted as PPP)
 - Internet Protocol Control Protocol (IPCP) (8021h)
 - Length: 10 (0Ah)
 - Contents: 03 00 00 0A 81 06 C1 A6 98 F1

Academic Base Station

- Internet Protocol Control Protocol (IPCP) (8021h)
- Length: 10 (0Ah)
- Contents: 04 00 00 0A 83 06 00 00 00 00

IPv4 Datagram

IP Version: 4 (04h)

Internet Header Length: 20 octets (05h)

Type of Service

- Precedence: Routine (00h)
- Normal delay (minimize delay) (0)
- Normal throughput (0)
- Normal reliability (0)

Total Length: 55 octets (37h)

Identification: 0 (0h)

Flags

- May fragment (0)
- Last fragment (0)

Fragment Offset: 0 octets (00h)

Time to Live: 254 sec (FEh)

Protocol: UDP (11h)

Header Checksum: 35187 (8973h)

Source Address: 192.168.24.2

Destination Address: 193.166.152.241

IPv4 Pseudo Header

Source Address: 192.168.24.2

Destination Address: 193.166.152.241

Protocol: UDP (11h)

TCP/UDP Datagram Length: 35 (23h)

Data (35 octets)

UDP DATAGRAM

Source Port: blackjack 1025 (401h)

Destination Port: Domain Name Server 53 (35h)

Length: 35 (23h)

Checksum: 7296 (1C80h)

User Data (27 octets)

IPv4 Datagram

IP Version: 4 (04h)

Internet Header Length: 20 octets (05h)

Type of Service

- Precedence: Routine (00h)
- Normal delay (minimize delay) (0)
- Normal throughput (0)
- Normal reliability (0)

Total Length: 55 octets (37h)

Academic Base Station

Identification: 0 (0h)

Flags

- May fragment (0)

- Last fragment (0)

Fragment Offset: 0 octets (00h)

Time to Live: 254 sec (FEh)

Protocol: UDP (11h)

Header Checksum: 35187 (8973h)

Source Address: 192.168.24.2

Destination Address: 193.166.152.241

IPv4 Pseudo Header

Source Address: 192.168.24.2

Destination Address: 193.166.152.241

Protocol: UDP (11h)

TCP/UDP Datagram Length: 35 (23h)

Data (35 octets)

UDP DATAGRAM

Source Port: blackjack 1025 (401h)

Destination Port: Domain Name Server 53 (35h)

Length: 35 (23h)

Checksum: 7296 (1C80h)

User Data (27 octets)

IPv4 Datagram

IP Version: 4 (04h)

Internet Header Length: 20 octets (05h)

Type of Service

- Precedence: Routine (00h)

- Normal delay (minimize delay) (0)

- Normal throughput (0)

- Normal reliability (0)

Total Length: 249 octets (F9h)

Identification: 0 (0h)

Flags

- Don't fragment (1)

- Last fragment (0)

Fragment Offset: 0 octets (00h)

Time to Live: 63 sec (3Fh)

Protocol: UDP (11h)

Header Checksum: 1970 (7B2h)

Source Address: 193.166.152.241

Destination Address: 192.168.24.2

IPv4 Pseudo Header

Source Address: 193.166.152.241

Destination Address: 192.168.24.2
Protocol: UDP (11h)
TCP/UDP Datagram Length: 229 (E5h)
Data (229 octets)
UDP DATAGRAM
Source Port: Domain Name Server 53 (35h)
Destination Port: Unassigned type 1025 (401h)
Length: 229 (E5h)
Checksum: 7452 (1D1Ch)
User Data (221 octets)
IPv4 Datagram
IP Version: 4 (04h)
Internet Header Length: 20 octets (05h)
Type of Service
- Precedence: Routine (00h)
- Normal delay (minimize delay) (0)
- Normal throughput (0)
- Normal reliability (0)
Total Length: 249 octets (F9h)
Identification: 0 (0h)
Flags
- Don't fragment (1)
- Last fragment (0)
Fragment Offset: 0 octets (00h)
Time to Live: 63 sec (3Fh)
Protocol: UDP (11h)
Header Checksum: 1970 (7B2h)
Source Address: 193.166.152.241
Destination Address: 192.168.24.2
IPv4 Pseudo Header
Source Address: 193.166.152.241
Destination Address: 192.168.24.2
Protocol: UDP (11h)
TCP/UDP Datagram Length: 229 (E5h)
Data (229 octets)
UDP DATAGRAM
Source Port: Domain Name Server 53 (35h)
Destination Port: Unassigned type 1025 (401h)
Length: 229 (E5h)
Checksum: 7452 (1D1Ch)
User Data (221 octets)

Annex 4 – Prague MikroTik Configuration

- **IPv4 Address and Routing Setup:**

```
[admin@MikroTik] > /ip address
```

```
add address=147.32.211.102/25 interface=ether1 network=147.32.211.0
```

```
add address=192.168.51.1/24 interface=bridge1 network=192.168.51.0
```

- **IPv4 Firewall Setup:**

```
/ip firewall filter
```

```
add chain=input comment="IPsec IP protocol 50 (ESP)" protocol=ipsec-esp src-  
address=193.166.41.146
```

```
add chain=input comment="IPsec ISAKMP/IKE" dst-port=500 protocol=udp src-  
address=193.166.41.146
```

```
add chain=input comment="IPsec NAT-T" dst-port=4500 protocol=udp src-  
address=193.166.41.146
```

```
add chain=input comment="Accept Winbox from WAN" connection-state=new dst-port=8291  
protocol=tcp src-address=147.32.211.0/25
```

```
add chain=input comment="Accept Winbox from LAN" connection-state=new dst-port=8291  
protocol=tcp src-address=192.168.51.0/24
```

```
add chain=input comment="Accept SSH from WAN" connection-state=new dst-port=22  
protocol=tcp src-address=147.32.211.0/25
```

```
add chain=input comment="Accept SSH from LAN" connection-state=new dst-port=22  
protocol=tcp src-address=192.168.51.0/24
```

```
add chain=input comment="Accept established connections" connection-  
state=established
```

```
add chain=input comment="Accept related connections" connection-state=related
```

```
add chain=input comment="Accept ICMP" protocol=icmp
```

Academic Base Station

```
add action=drop chain=input comment="Drop invalid connections" connection-  
state=invalid
```

```
add action=drop chain=input comment="Drop everything else"
```

```
/ip firewall nat
```

```
add chain=srcnat comment="IPsec Tunnel" dst-address=192.168.1.0/24 src-  
address=192.168.51.0/24
```

```
add action=masquerade chain=srcnat comment="WAN IPv4 NAT" out-interface=ether1 src-  
address=192.168.51.0/24 to-addresses=0.0.0.0
```

- **IPv4 IPsec Setup:**

```
/ip ipsec policy group
```

```
set default name=default
```

```
/ip ipsec proposal
```

```
set [ find default=yes ] auth-algorithms=sha1 disabled=no enc-algorithms=3des
```

```
lifetime=1h name=default pfs-group=modp1024
```

```
/ip ipsec peer
```

```
add address=193.166.41.146/32 auth-method=pre-shared-key dh-group=modp1024
```

```
disabled=no dpd-interval=2m dpd-maximum-failures=5 enc-algorithm=3des exchange-
```

```
mode=main generate-policy=no hash-algorithm=sha1 lifebytes=0 lifetime=8h nat-
```

```
traversal=no passive=no port=500 proposal-check=obey secret=NGN_Pori-Prague send-
```

```
initial-contact=yes
```

```
/ip ipsec policy
```

```
add action=encrypt disabled=no dst-address=192.168.1.0/24 dst-port=any ipsec-
```

```
protocols=esp level=require priority=0 proposal=default protocol=all sa-dst-
```

```
address=193.166.41.146 sa-src-address=147.32.211.102 src-address=192.168.51.0/24
```

```
src-port=any tunnel=yes
```

Academic Base Station

- **IPv4 DHCP Server Setup:**

```
/ip dhcp-server
```

```
add address-pool=pool1 authoritative=after-2sec-delay bootp-support=static
```

```
disabled=no interface=bridge1 lease-script="" lease-time=3d name=server1 src-  
address=192.168.51.1
```

```
/ip dhcp-server config
```

```
set store-leases-disk=5m
```

```
/ip dhcp-server network
```

```
add address=192.168.51.0/24 dhcp-option="" dns-server=147.32.192.250
```

```
gateway=192.168.51.1 netmask=24 ntp-server=195.113.144.201 wins-server=""
```

- **NTP Client Setup**

```
/system ntp client
```

```
set enabled=yes primary-ntp=195.113.144.201 secondary-ntp=195.113.144.238
```

ABBREVIATIONS AND ACRONYMS

GSM	Global System for Mobile Communications
TDMA	Time division Multiple Access
VPN	Virtual Private Network
GPRS	General Packet Radio Service
BSS	Base Station Subsystem
NSS	Network Switching Subsystem
BTS	Base Transceiver station
TCH	Traffic Channel
CCCH	Common Control Channel
DCCH	Dedicated Control Channel
BCCH	Broadcast Control Channel
SDCCH	Stand-alone Dedicated Control Channel
SACCH	Slow Associated Dedicated Control Channel
FACCH	Fast Associated Dedicated Control Channel
CBCH	Cell Broadcast Channel
SMSCB	Short Message Service Cell Broadcast
FDMA	Frequency Division Multiple Access
TN	timeslot number
BSSAP	Base Station System Application Part
MTP	Message Transfer Part
CM	Connection Management
MM	Mobility Management
MSC	Mobile Switching Center
DTAP	Direct Transfer Application Protocol
LAPD	Link Access Protocol D-channel
ISDN	Integrated Services for Digital Network
OSI	Open System Interconnection

Academic Base Station

MTP-1	Message Transfer Part 1
ISUP	ISDN User Part
TCAP	Transaction Capability Application Part
MAP	Mobile Application Part
RR	Radio Resource
BTSM	Base Transceiver Station Management
SS	Supplementary Services
PSTN	Public Switched Telephone Network
IPS	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
PWE3	Pseudo-wire Circuit –Emulation Service
EFM	Ethernet First Mile
OAM	Operation Administration and Maintenance
CAPEX	Capital Expenditures
OPEX	Operational Expenditure
CES	Circuit Emulation Services
LAN	Land Area Network
WAN	Wide area Network
IEEE	Institute of Electrical and Electronics Engineers
DSCP	Differentiated Services code Point
QoS	Quality of Service
ToS	Terms of Service
MEF 3, 8	Metro Ethernet Forum
IETF	Internet Engineering Task Force
SAToP	Structured Agnostic Traffic over Packet
CESoPSN	Circuit Emulation Service over Packet Switched
VLAN	Virtual Local Area Network
HSCSD	High Speed Circuit Switched Data

Academic Base Station

APP	Automatic Picocell Planning
PCM	Pulse Code Modulation
PLMN	Public Land Mobile Network
BSSU	Base Station Signaling Unit
BDCU	Basic Data Communications Unit
CMU	Cellular Management Unit
CM	Central Memory
CASU	Channel Associated Signaling Unit
CU	Charging Unit
CS	Clock System
CABU	Clock and Alarm Buffer Unit
SSI	Synchronization Signal Interface
CCSU	Common Channel Signaling Unit
CDSU	Compact Data Service Unit
IWC	Interworking Cabinet
ET	Exchange Terminal
ECT	Echo Canceling and Terminal
IPET	Internet Protocol Exchange Terminal
TGSU	Trunk Gateway Signaling Unit
MFSU	Multi-Frequency Signaling Unit
PDFU	Power Distributed Fuse Unit
PRAU	Primary Rate Access Unit
VLRU	Visitor Location Register Unit
IP	Internet Protocol
SA	Security Association
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
CLI	Command Line Interface

Academic Base Station

DSCP	Differential Services Code Point
SFP	Small Form-Factor Pluggable
VLL	Virtual Leased Line
GMSK	Gaussian Minimum Shift Keying
DX	Digital Exchange
CS	Coding Scheme
MCC	Mobile Country Code
MNC	Mobile National Code
TC	Transcoder Controller plug-in unit
MCM	Marker and Cellular Management
HSL	High Speed Signaling Link
RAN	Radio Access Network

REFERENCES

CHAPTER ONE

[1][i] Jörg Eberspächer, ans-Jörg Vögel, Christian Bettstetter, Christian Hartmann, GSM Architecture, Protocols and Services, ISBN: 978-0-470-03070-7 (H/B) Third Edition, 2009, p57-58

[2] Bernhard H. Walke, Mobile Radio Networks, Networking and Protocols, ISBN: 0-471-97595-8, 1999, Second Edition, p142

[3][ii] Jörg Eberspächer, ans-Jörg Vögel, Christian Bettstetter, Christian Hartmann, GSM Switching, Services and Protocols, Online ISBN: 0-470-841 74-5, Second Edition, 2001, p57-58, 60

[4][5][6] Bernhard H. Walke, Mobile Radio Networks, Networking and Protocols, ISBN: 0-471-97595-8, Second Edition, 1999, p143

[7][8][9] Jochen Schiller, Mobile Communications, ISBN: 0 321 12381 6, Second Edition, 2003, p108

[10] Bernhard H. Walke, Mobile Radio Networks, Networking and Protocols, ISBN: 0-471-97595-8, Second Edition, 1999, p145

[11] Jörg Eberspächer, ans-Jörg Vögel, Christian Bettstetter, Christian Hartmann, GSM Switching, Services and Protocols, Online ISBN: 0-470-841 74-5, Second Edition, 2001, p60

[12][13][14] Jörg Eberspächer, ans-Jörg Vögel, Christian Bettstetter, Christian Hartmann, GSM Architecture, Protocols and Services, ISBN: 978-0-470-03070-7 (H/B), 3rd Edition, 2009, p62-64

[15][iii] Gunnar Heine, GSM Networks: Protocols, Terminology and Implementation, ISBN: 0-89006-471-7, 1999, p89-90, 92

[16][17] Asha Mehrotra, GSM System Engineering, Asha Mehrotra, ISBN: 0-89006-860-7, 1997, p70-71

[18] Gunnar Heine, GSM Networks: Protocols, Terminology and Implementation, ISBN: 0-89006-471-7, 1999, p91-92

CHAPTER TWO

[1] Jörg Eberspächer, ans-Jörg Vögel, Christian Bettstetter, Christian Hartmann, GSM Switching, Services and Protocols, Online ISBN: 0-470-841 74-5, Second Edition, 2001, p172-173

[2] Gunnar Heine, GSM Networks: Protocols, Terminology and Implementation, ISBN: 0-89006-471-7, 1999, p172-174

[3] Gunnar Heine, GSM Networks: Protocols, Terminology and Implementation, ISBN: 0-89006-471-7, 1999, p51, p55-57

[4] Jochen Schiller, Mobile Communications, ISBN: 0 321 12381 6, Second Edition, 2003, p105

[5][6][7] Martin Sauter, From GSM to LTE: An introduction to mobile networks and mobile broadband, ePDF ISBN: 978-0-470-97824-5, First Edition, 2011, p6-8

[8][9][10] Jochen Schiller, Mobile Communications, ISBN: 0 321 12381 6, Second Edition, 2003, p110-114

CHAPTER THREE

[1][2][3] T-Marc, Ethernet and Circuit Emulation Service, Network Demarcation Solution, (T-Marc 254 / T-Marc 250), Installation Guide, MN100144 Rev B03, 2006, p2-1, 2-2, 4-1

[4][5][6][iv][v] Nokia InSite Base Station, Product Description, User Manual, Version 4, 468951A.404, DN99258696, p14, 16-19, 36, 46

[7-14][vi] Nokia Electronic Documentation NED 5.x, 6.0, Online Documentation, Nokia Siemens Network, Mobile Switching Center Nokia DX 200 'i-series'

[1][2] Nokia DX 200, Release no. 2003282, Nokia BSC S10.5 ED, PRODUCT DOCUMENT, BCSU

[3][4][5] Nokia DX 200, Release no. 200319, Nokia BSC/TCSM S11, Engineering for TCSM2, p13-14, 17

[6][7] Nokia DX 200, Release no. 2003330, Nokia BSC S10.5 ED, ver. 2, Base Station Controller, BSC2E/A, BSCE, p28-29

[8] Nokia DX 200, Release no. 2003330, Nokia BSC S10.5 ED, ver. 2, Base Station Controller, BSC2E/A, BSCE, p35

[9] Nokia DX 200, Release no. 2003330, Nokia BSC S10.5 ED, ver. 2, Base Station Controller, BSC2E/A, BSCE, p31

[10][11][12] Nokia DX 200, Release no. 2003330, Nokia BSC S10.5 ED, ver. 2, Base Station Controller, BSC2E/A, BSCE, p31-34

[13] Nokia DX 200, Release no. 2003330, Nokia BSC S10.5 ED, ver. 2, Base Station Controller, BSC2E/A, BSCE, p37

[14] Base Station Subsystem Remote Fault Management, BSSRF – BSS overview, ver. OS85351EN52GLA0, p5-6

CHAPTER FOUR

[1][2][3] NetHawk, Data Sheet version 8.1, www.nethawk.fi, NetHawk GSM Analyzer – Complete solution for 2G/2.5G network monitoring

[4][5] Wireshark User's Guide, v1.11.4-rc1-257-gb5120cd for Wireshark 1.11, Ulf Lamping, Richard Sharpe, NS Computer Software and Services P/L, Ed Warnicke, p1-3