GERAN Abis Protocols Interception Hands-On

SYNOPSIS

- **Hands-On Seminar**: understand GSM/GPRS/EGPRS technology and intercept Target Activity on Abis.
- Focus on tracing and intercepting Voice Calls and GPRS/EGPRS Radio protocols **on vendor specific Abis**.
- Gain solid understanding on how the Radio Protocols, Radio Parameters and Service Scenarios are reflected on Abis.

DURATION

- 6 Days

PREREQUISITES

- Basic knowledge of GSM, GPRS/EGPRS radio channels and physical layer functionality.

TARGET AUDIENCE

- Interception Experts, Field engineers.
- System architects, software and hardware engineers.
- Test planers and tester, technical staff responsible for O&M.

COURSE TARGETS

- The participants would become familiar with various vendor specific Abis interface configurations, Abis protocols and GSM/GPRS scenarios sampled on Abis.
- The participants would become familiar with GPRS and EGPRS architecture, service scenarios and radio protocols.
  - They would be able to describe the role of every protocol and understand the resource allocation scenarios and the end-to-end IP transport.
  - They would understand the message flows and recognize the important parameters and interception relevant information.
- The participants would gain experience in analyzing GPRS/EGPRS logs on multiple Abis configurations, including systematic trace investigation, mapping between trace and standard specification, correlating between different interface views and using the trace logs for intercepting target parameters.

Introduction & Service Principles

1. Service Terminology

a. GSM/GPRS Service Terminology
(Architecture, Mobility, Connection/TBF)

b. GSM Radio Protocols structure and layer model
(SAP, primitives, RIL-3 message structure)

2. GSM Principles and Basic Service Scenarios

a. GSM Network Architecture

b. GSM RAN Interfaces and Protocols

c. GSM Radio Technology and Radio Channels

d. GSM Radio Protocols Overview
(LAPDm,RR,NAS)

e. GSM Basic Service Scenarios

3. GPRS Principles and Basic Service Scenarios

a. GPRS Network Architecture

b. GPRS RAN Interfaces and Protocols

c. GPRS Radio Technology and Radio Channels

d. GPRS Radio Protocols Overview

e. GPRS Basic Service Scenarios

GSM Abis – Signalling and Traffic Contexts

4. GSM Abis Interface – BTSM and TRAU

a. GSM Abis Protocols over E1
(Abis Topology, RSL and OML Multiplexing, TRAU, **LAPD**)

b. Vendor/Model specific GSM Abis Configurations

c. **BTSM** Protocol and basic procedures

d. Radio Signalling Transfer in BTSM

e. **TRAU** Frame Formats (Voice and Data payload)

f. Blind detection of RSL and TRAU timeslots

g. Mapping Radio Scenarios to Abis
(Paging, Connection Setup, Handover, Security)

h. Abis over IP

i. **LAPD and RSL/OML Hands-On**

j. **Basic BTSM Scenarios Hands-On**

GSM Abis – Telephony and SMS Scenarios

5. **CS-Core Registration Scenarios**
   a. **GSM RR** Protocol and GPRS relevant subset
   b. **RR Protocol and GPRS RR Hands-On**
   c. **NAS MM** Protocol
   d. GSM Registration and Security Scenarios
   e. Map Registration Scenarios to Abis
   f. **NAS MM Hands-On**

6. **GSM Abis Telephony Scenarios**
   a. **NAS CC** Protocol and Call Scenarios
   (user identities, vocoder type)
   b. Map Telephony Scenarios to Abis
   c. Map Mobile-Identities to Radio/Abis Contexts
   (CC connection, RR Connection, Radio Timeslot
   SDCCH/FACCH/TCH, BTSM thread, Abis TRAU Sub-Channel)
   d. MAP Voice Calls between Abis Interfaces
   (pair MO/MT Call Legs, Handover correlation)
   e. **Abis Telephony Hands-On**

7. **GSM Abis SMS Scenarios**
   a. **NAS SMS** Protocols
   (user identities, SMS format, type/destination of contents)
   b. SMS Service Scenarios
   c. Map SMS Scenarios to Abis
   d. Map Mobile-Identities to Radio/Abis Channels
   (SMS Connection, RR Connection, Radio Timeslot SDCCH/FACCH,
   BTSM thread)
   e. **Abis SMS Hands-On**

GPRS Abis – Signalling and Traffic Contexts

8. GPRS RAN Architecture

a. GPRS Architecture
(**PCU** Role,SGSN/GGSN,Gn/Gb/Gs/Nokia Gbis)

b. GSM/GPRS Cell/Channels Configuration

9. GPRS Abis G-TRAU Frames and BTSM

a. GPRS Abis Protocols (RSL,PCU-16 Frames,)

b. Abis BTSM Subset for GPRS

c. Abis BTSM Subset for GPRS TBF Hands-On

d. Vendor specific GSM+GPRS Abis Configurations
(Dynamic sharing between Voice and GPRS)

e. Vendor specific DAP

f. principles and Dimensioning

g. Nokia EDAP frame structure

h. Blind detection of RSL, Voice and EDAP Pool

i. Nokia EDAP Hands-On

GPRS Abis – Packet-Core Service Scenarios

10. GPRS NAS Protocols

- **a. NAS GMM** Protocol
- b. Registration and Security Scenarios
- **c. NAS SM** Protocol
- d. PDP Context Scenarios
- e. Mapping GPRS Scenarios to Abis
- **f. GMM and SM Scenarios Hands-On**

11. GPRS Mobile-Network Tunneling Protocols

- a. Mobile-Network Tunneling
  LLC and **SNDCP** Protocols
- **b. LLC and SNDCP Hands-On**
- c. EGPRS+ Protocol Evolution

GPRS Abis – Radio Bearer Allocation Scenarios

12. GPRS/EGPRS Radio Bearer

a. What is EDGE

b. GPRS/EGPRS Enablers

c. GPRS/EGPRS Mobile Capabilities

d. GPRS radio channels and coding schemes

e. GPRS Physical Layer Procedures
(Timing Advance, Power Control, Radio Link Failure, Measurements)

f. GPRS Scheduling and arbitration principles

g. GPRS Services QoS and Bearer Model

h. GPRS/EGPRS **MAC** and **RLC** protocols

i. GPRS MAC and RLC Hands-On

j. MCS Adaptation Hands-On

13. GPRS/EGPRS Resource Allocation Scenarios

a. GRR - GPRS/EGPRS Radio Resource Protocol

b. GPRS/EGPRS Radio Messages

c. GPRS/EGPRS Bearer Allocation scenarios

d. GSM/GPRS Idle Mode Behavior (PSI)

e. PTM Mobility/Continuity
and Inter-RAT Scenarios

f. PTM Allocation Scenarios Hands-On

Abis Passive Interception

14. GPRS/EGPRS Radio Interception

a. GSM/GPRS Security and Security Continuation

b. Protected and Unprotected Radio Messages

c. Passive Intercepting on Abis
(Mapping Target Identities, Activity and Location)