v 1.310

LTE – Signaling & Protocol Analysis
Focus: RAN and UE

Course Duration:

- 3 days

Course Description:

- This course is a must for everybody who requires a detailed understanding of the protocols and signaling procedures within E-UTRAN and the EPC. In that respect the clear focus of this course is on the protocols of the UE and the E-UTRAN.
- The course starts with a review of the LTE physical layer and the concepts and protocol stacks of E-UTRAN. This part concludes with the review of the EPS network architecture.
- Immediately afterwards we jump into real-life call flows and scenarios and confront the student with the look & feel of the LTE protocol suite. This part ends with an assessment of what will be the focus of the following chapters.
- The next chapters are dedicated to the different protocols EMM, ESM, MAC, RLC, RRC, S1-AP, X2-AP, SGs-AP and S101-AP.
- The training course concludes with the presentation and analysis of LTE signaling flows and real-life call flows.

  As in all INACON courses we integrated several interactive exercises for a perfect learning experience.

Prerequisites:

- The student must possess a thorough understanding of LTE and EPS before coming to this course.
- We recommend our courses LTE from A-Z and SAE from A-Z to be taken beforehand.
- Practical experience with protocol testers and IP-sniffers is necessary.

Course Target:

- The student is enabled to understand the concepts of the LTE protocol stack.
- The student is able to develop and to test the higher layer protocol stack of LTE.
- The student will be enabled to effectively communicate LTE protocol stack issues with his/her peers.

Some of your Questions that will be answered:

- How do attachment, session establishment and bearer setup work in LTE?
- How does a circuit-switched fallback scenario look and which messages are exchanged among which network nodes when and why?
- Can I obtain an e2e-scenario that explains how the PCRF authorizes and initiates a dedicated EPS-bearer establishment?
- How are the LTE protocol stack entities organized and which channels are established between them?
- How do the PDU's of MAC, PLC, PDCP, RRC, S1-AP and the X2-AP look like?
- According to which guidelines MAC is scheduling the traffic and how is the flow control in between UE and eNodeB performed?
- What are the benefits of multiplexing logical channels on transport blocks and to apply a flexible RLC PDU size?
- What new security concepts are applied in PDCP?
- What are the key differences of RRC in E-UTRAN vs RRC in UTRAN?
- How do we interpret ASN.1 PER encoded call flows like in RRC and in S1-AP?
- How the concept of the initial context setup procedure s allowing for a very low control plane latency?
- How are system information messages structured and transmitted in LTE?
- How is the interworking with cdma2000 embedded and realized in LTE?
- What are the mechanisms to create a self-organizing network?
- How do the various handover scenarios in LTE work?

Who should attend this Course:

- Test engineers who need to understand the details of the LTE signaling protocols.
- Design staff of handsets and E-UTRAN who requires a deep inside view of the LTE-related protocols.
- 2nd and 3rd level troubleshooters who need to understand the LTE protocol stack in detail.

Table of Content:

Revisiting important Details of the EPS

- **Architecture Overview**

  ⇒ Evolved Packet Core in Context
  EPC vs. EPS, Non-3GPP Access Networks (trusted / non-trusted)

  ⇒ Zoom into the EPS
  Functional Overview of Core Network Elements within the EPC

  ⇒ Network Elements and their Functions within the EPC
  Mobility Management Entity (MME), Characteristics, Identification, Interfaces & Protocols, Tasks & Functions of the MME, NAS-Signaling towards the UE, S1-Signaling towards the eNodeB, S-GW and P-GW Selection, Other Selection Functions, Local Breakout, IMS and Local Breakout, Serving Gateway (S-GW), Characteristics, Identification, Interfaces & Protocols, Tasks & Functions of the S-GW, Packet Routing / Relaying, Legal Interception, QCI-based Packet Tagging, Accounting, PDN Gateway (P-GW or PDN-GW), Characteristics, Identification, Interfaces & Protocols, Tasks & Functions of the P-GW, UE IP Address Allocation, QCI-based Packet Tagging, Policy Enforcement, Legal Interception, Home Agent Function, enhanced Packet Data Gateway (ePDG), Characteristics, Identification, Interfaces & Protocols, Tasks & Functions of the ePDG, ESP-Tunnel Mgmt towards UE's, QoS-specific Packet Tagging in UL-Direction, Legal Interception, MAG-Function for PMIPv6, EPS Architecture for Voice Support (CSFB or VoIPIMS with SRVCC) – How is SMS supported?

- **Protocol Stacks**

  ⇒ Control Plane / E-UTRAN - EPC

  ⇒ User Plane E-UTRAN – EPC (S5/S8 GTP-based)

  ⇒ User Plane E-UTRAN – EPC (S5/S8 PMIPv6/GRE-based)

- **Security Architecture**

  ⇒ Overview & Introduction
  Essentials, EPS-AKA, Security is performed independently in two protocol layers, Algorithms

  ⇒ Operation of UMTS-AKA

  ⇒ Key Derivation Function (KDF)
  Comprehension Check & Practical Exercise:
  The KDF S(10) for K(ASME), Input Parameters

  ⇒ EPS-AKA in Operation during Initial Attach Procedure

  ⇒ Use of the different Security Algorithms

The Non-Access-Stratum: EMM & ESM

⇒ Important EMM-Procedures
Common Procedures, Specific Procedures, Connection Management Procedures

⇒ State Machine
Relationship between EMM and ECM, EMM-DEREGISTERED & ECM-IDLE, EMM-REGISTERED & ECM-IDLE, EMM-REGISTERED & ECM-CONNECTED, UE Mode of Operation upon Attach – Voice Domain Preference and UE's Usage Setting

⇒ Message Format
Security Header

⇒ Important EMM-Scenarios
Attachment through E-UTRAN / new MME, Comprehension Check & Practical Exercise: Building your own EMM: ATT_REQ-Message, Tracking Area Update (Inter-MME / with new S-GW), Initial Conditions, Detailed Description, Comprehension Check & Practical Exercise: EMM-Message Decode

⇒ Important ESM-Procedures
MME-initiated, UE-initiated

⇒ State Machine

⇒ Message Format
Security Header, Procedure Transaction Identity

⇒ Dedicated EPS Bearer Establishment
Network Initiated (IMS triggered during Call Establishment) , Initial Conditions, Detailed Description, Network Initiated (IMS triggered during Call Establishment) , Detailed Description

Radio Resource Control

- **Overview**
  Transmission of broadcast information, Establish and maintain services, QoS control, Transfer of dedicated control information
- **State Characteristics of RRC**
  RRC_IDLE, RRC_CONNECTED
- **Signaling Radio Bearers (SRB)**

⇒ Overview
SRB0, SRB1, SRB2

⇒ Control Plane Protocol Stack Review
Air Interface protocols

⇒ User Plane Protocol Stack Review
Air Interface protocols, S1 protocol

⇒ Overview on Channel Types and User Bearers
Review of eNB DL Channels, Review of eNB UL Channels

⇒ Mapping of RRC-Messages to SRB's and to Channels
Messages on BCCH (MIB and SIB), Messages on PCCH and DL-CCCH, Messages on DL-DCCH and DL-DTCH, Messages on UL-CCCH, UL-DCCH and UL-DTCH

- **Message Encoding through ASN.1 PER-unaligned**

⇒ Example: The ASN.1-Code of RRC_CONN_REQ ...

⇒ … and the compiled Message Structure (Tree View)

⇒ Comprehension Check & Practical Exercise:
Encoding an RRC_CONN_REQ-Message

- **RRC Procedures**

⇒ System Information Broadcast
Overview, Overview of Functions of the System Information Blocks, Example of an MIB, Example of an SIB1, Example of an SIB2, Example of an SIB3

⇒ Connection Management Related Procedures
Paging Procedure, RRC Connection Establishment Procedure, SRB1 Default Configuration, Physical Layer Default Configuration, UE Capability Transfer Procedure, RRC Initial Security Activation Procedure, RRC Connection Reconfiguration Procedure, SRB2 Default Configuration, Counter Check Procedure, RRC Connection Reestablishment Procedure, RRC Connection Release Procedure

⇒ Inter RAT RRC Procedures

⇒ E-UTRAN Measurements
Overview, Definition of Measurements in E-UTRAN, Measurement Events in E-UTRAN, Measurement Definition in the Standard – Measurement Object, Measurement Definition in the Standard – Report Configuration and Measurement ID, Structure Measurement Report

⇒ Other RRC Procedures

⇒ RRC Procedure Delay
Introduction, Values

⇒ Idle Mode Procedures – Neighbor Cell Monitoring & Cell Reselection
Priority-Based Cell Reselection of Multi-RAT UE's, SPID - Subscriber Profile ID for RAT/Frequency priority, E-UTRAN priority-based Cell Reselection Details, UTRAN priority-based Cell Reselection Details, GERAN priority-based Cell Reselection Details, Cell Selection in E-UTRAN, PLMN selection in E-UTRAN, Cell Selection and Reselection, Cell Selection Process, Cell Selection Criterion, Cell Reselection Evaluation Process in E-UTRAN, Reselection Priorities Handling, Measurement Rules for Cell Re-Selection, Mobility States in E-UTRAN, Scaling Rules based on Mobility State, E-UTRAN Inter-Freq and IRAT Cell Reselection Criteria, Intra-Freq and equal Priority Inter-Freq Reselection Criteria, Cell Ranking Criterion in E-UTRAN for equal Priority inter-Freq and intra-Freq, Cell Reselection towards lower Priority E-UTRAN Freq or IRAT Freq than Serving Freq

- **GERAN to E-UTRAN Cell Reselection**

⇒ IRAT Measurements when camping in GSM or GPRS

⇒ IRAT Cell Reselection based on Priority – 2G to 3G / LTE
Cell Reselection Criteria's, Cell Reselection from GERAN towards higher prioritized IRAT Frequency, Cell Reselection from GERAN towards lower prioritized IRAT Frequency

Lower Layers of the Uu-Interface: MAC, RLC & PDCP

- **Features of MAC**

⇒ Overview
Data transfer logical channels ⟷ transport channels, Radio resource allocation, Special procedures

⇒ Radio Network Temporary Identifiers (RNTI's) in E-UTRAN
Usage of RNTI's, RNTI Values

⇒ MAC Random Access Procedure
Contention Based Random Access Procedure, Non-contention based random access procedure

⇒ Structure of MAC-PDU
MAC control element, Normal (non-transparent) MAC SDU, Transparent MAC SDU

⇒ MAC Control Elements

Contention resolution ID, Timing Advance, DRX, Padding, Power headroom report, C-RNTI, Short, long and truncated buffer status reports

⇒ Practical Exercise: MAC Operation

⇒ Practical Exercise: DL MAC PDU Construction

⇒ MAC Configuration
MAC Configuration in the Standard

- **Features of RLC**

⇒ Overview
Data transfer, Error detection and recovery, Reset

⇒ Structure of RLC PDU

⇒ Structure of RLC AM with PDCP PDU Segments

⇒ RLC Configuration
RLC Configuration in the Standard

- **Features of PDCP**

⇒ Overview
RoHC, Numbering of PDCP PDU's, In-sequence delivery of PDU's, Duplicate deletion, Encryption, Integrity Protection

⇒ Structure of PDCP PDU

⇒ PDCP Configuration
PDCP Configuration in the Standard

- **How a TCP/IP MTU is reaching the UE / the Internet**
TCP/IP layer, PDCP layer, RLC layer, MAC layer, PHY layer

X2- and S1-Interfaces: X2AP- and S1-AP-Protocols

- **The X2AP Protocol**

⇒ Protocol Stack on the X2-interface

⇒ Tasks & Functions
Mobility Management, Load Management, X2-Interface Management

⇒ X2-based Handover Scenario
Initial Conditions, Detailed Description

- **The S1-AP Protocol**

⇒ Overview & Introduction

⇒ S1-based Handover Scenario
Initial Conditions, Detailed Description