v5.200

GPRS Rel. 5
Signaling & Protocol Analysis
(The Core Network)

Course Duration:

- 3 days

Course Description:

- This course is an upgrade of our well-established course “GPRS – Signaling & Protocol Analysis (The Core Network)”, which covered contents up to Rel. 99.
- It addresses the needs of engineers and technicians who are already experienced in GPRS.
- This second part of the GPRS signaling course series focuses on the aspects of GPRS within the core network and from the application perspective.

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

Pre-Requisites:

- Very good understanding of GSM networks, protocols, operation and parameters. If required, we advise our course “GSM – Signaling & Protocol Analysis” to be taken upfront.
- Previous knowledge of GPRS is essential. If required, we advise our course “GPRS from A – Z” to be taken in advance.
- Previous experience with GPRS network operation is optional but favorable.

Course Target:

- The student will be enabled to understand all relevant details of GPRS-procedures within the Core Network.
- The student will understand the interworking between the GPRS and the TCP/IP-protocol stack.
- The student will be enabled to analyze recording files taken on the Gn- / Gp- and Gi-Interfaces.

Some of your questions that will be answered:

- How can I evaluate GPRS trace files on the various new interfaces (Gb, Gn, Gp, Gi) ?
- How does the GPRS Tunneling Protocol (GTP) work?
- What is the differences between GTP and GTP' ?
- How are CDR's processed in GPRS networks? Which CDR's need to be considered ?
- What different means are there to provide IP-addresses to authorized GPRS subscribers ?
- Which statistical information can be retrieved by means of protocol testers to determine our network performance?
- In case of errors: How can I identify DNS/RADIUS/… server problems from problems within our GPRS network?
- How do WAP and SMS work with GPRS ?

Who should attend this class?

- Everybody who needs to optimize GPRS networks.
- Design Engineers of GPRS network equipment.
- Every engineer who is involved in the testing and operation of GPRS core networks.
- Field engineers who have to analyze GPRS recording files.
- All engineers who need to interpret GPRS recording files in the lab.

Table of Contents:

A Comprehensive Inside View on GPRS

Protocols within the GPRS Access Network

⇒ BSSGP and Network Service
⇒ LLC and SNDCP
⇒ Functions of RLC/MAC

The UMTS Protocol Stack between MS and Application

⇒ Packet-Switched Control Plane
  Access Stratum Protocols
  Non Access Stratum Protocols
⇒ Packet-Switched User Plane

Iu mode

⇒ GERAN – Core Network Interfaces with Release 5
⇒ IMS introduction in the Core Network

GERAN in Iu mode connected to PS Domain

  User Plane
  Control Plane
  New Identifier in Iu mode
  S-RNTI
  G-RNTI

Intra GERAN, inter GERAN – UTRAN interface

⇒ General principles of the Iur-g interface
⇒ GERAN Registration Area

Flexible Iu Connection

⇒ Load Distribution
⇒ Reduced Signaling
⇒ Capacity Upgrade
⇒ Node Redundancy
⇒ Flexible Iu Interface with Release 5
⇒ Packet Switched Pool Areas
⇒ Circuit Switched Pool Areas
  NRI transmission in A/Gb mode
  NRI transmission in Iu mode
⇒ Affected Network Nodes
  (1) Network Configuration Example

GPRS Mobility Management (GMM) and GERAN / UTRAN Interworking

Introduction to GPRS Mobility Management

⇒ Intra-PLMN and Inter-PLMN Roaming
⇒ GMM States in the SGSN and the Mobile Station (GPRS)
- The IDLE-State
- The READY-State
- The STANDBY-State

⇒ PMM States in the SGSN and the Mobile Station (UMTS)
- PMM-Detached-State
- PMM-Connected-State
- PMM-Idle-State

⇒ The Routing Area and the Null Routing Area
- The Routing Area Identification (RAI)
- The Routing Area Identification (RAI)

Other Important GMM-Identifiers

⇒ The P-TMSI and the P-TMSI Signature
⇒ The Ready Timer (T3314) (GPRS only)
⇒ The Ready Timer (T3314) (GPRS only)
- Operation of the Ready Timer (T3314)
- Operation of the Ready Timer (T3314)
- Implications of the Ready Timer:
- Reduction of the Paging Time

⇒ Periodic Routing Area Updating Timer (T3312) & Mobile Reachable Timer
- Expiry of T3312 in MS
- Allocation of T3312 and Mobile Reachable Timer
- Operation of T3312 and Mobile Reachable Timer
- Expiry of Mobile Reachable Timer

The GMM-Messages

⇒ Message Format for GMM
⇒ The GMM Message Types
- ATT_REQ
- ATT_ACC
- ATT_COM
- ATT_REJ
- DET_REQ
- DET_ACC
- RA_UPD_REQ
- RA_UPD_ACC
- RA_UPD_COM
- RA_UPD_REJ
- P-TMSI_REAL_CMD
- P-TMSI_REAL_COM
- AUTH_CIPH_REQ
- AUTH_CIPH_RSP

AUTH_CIPH_REJ
IDENT_REQ
IDENT_RSP
GMM_STATUS
GMM_INFO

(1) GMM-Procedures

⇒ GPRS Attach (new SGSN / NOM II / III, MS Class A, B or C)
- Initial Conditions
- Applicability of this Procedure
- Description

⇒ Combined Attach (no new SGSN, MS Class A or B)
- Initial Conditions
- Applicability of this Procedure
- Description

⇒ Combined RA / LA Update (Intra SGSN / MS-Class A or B)
- Initial Conditions
- Applicability of this Procedure
- Description

⇒ Inter SGSN Routing Area Update (GPRS in A/Gb-mode)
- Initial Conditions
- Applicability of this Procedure
- Description

⇒ Inter SGSN Routing Area Update (UMTS / MS-initiated)
- Initial Conditions
- Applicability of this Procedure
- Description

⇒ The GPRS Detach Procedure (Mobile Originating)
- Initial Conditions
- Applicability of this Procedure
- Description

⇒ The GPRS Detach Procedure (SGSN Originating)
- Initial Conditions
- Applicability of this Procedure
- Description

⇒ The GPRS Detach Procedure (HSS Originating)
- Initial Conditions
- Applicability of this Procedure
- Description

Interworking between UTRAN and GERAN

⇒ Overview

⇒ State Transitions GMM ⇔ PMM
- Case 2: From GERAN to UTRAN

Related Scenarios (Selection)

⇒ MS Initiated Inter-SGSN RA Update UMTS➔ GPRS
- Initial Conditions
- Applicability of this Procedure
- Description

⇒ SRNS-Relocation with RA-Update GPRS to UMTS (Iu-mode)
- Initial Conditions
- Applicability of this Procedure
- Description

The IP Backbone

Introducing the IP-Protocol Stack

⇒ The Structure of the IP-Protocol Stack

Details of the Internet Protocol

⇒ IP-Addresses
- IP-Address Classes
- Special IP-Address Notations
- Subnet-Addressing
- Supernetting and CIDR
- More Details of Classless Inter-Domain Routing

⇒ The IP-Header
- Overview
- Example of an IP-Header
- The IP-Header / Octet 1 – 4
- The TOS- Field (Type of Service)
- The TOS- Field / Differentiated Services
- The IP-Header / Octet 5 – 8
- Fragmentation Control in IP
- The IP-Header / Octet 9 – 20
- The IP-Header / Octet 21 – N (IP-Options)

Details of the Internet Control Message Protocol (ICMP)

⇒ ICMP-Message Format

⇒ ICMP-Messages
- Echo Reply
- Destination Unreachable
- Source Quench
- Redirect
- Echo Request
- Router Advertisement
- Router Solicitation
- Time Exceeded for a Datagram
- Parameter Problem on a Datagram

- Timestamp Request
- Timestamp Reply
- Information Request
- Information Reply
- Address Mask Request
- Address Mask Reply

⇒ Example of an ICMP-Message (Router Solicitation)

Details of the User Datagram Protocol (UDP)

⇒ Services of UDP
- Application Process Identification
- Connection-less / Unacknowledged Data Delivery
- Frame Protection (Checksum)

⇒ Port Numbers
- “Well known” Port Numbers
- Available Port Numbers

⇒ The UDP-Header
- Source Port (16 bit) / Destination Port (16 bit)
- Length (16 bit)
- Checksum (16 bit)
- UDP-Pseudo Header and UDP-Checksum

Details of the Transmission Control Protocol (TCP)

⇒ Services of TCP

⇒ TCP Connection Establishment
- (1) Example for TCP Connection Establishment

⇒ TCP Connection Release
- (1) Example for TCP Connection Release

⇒ The TCP-Header
- The TCP-Header / Octet 1 – 12
- The TCP-Header / Octet 13 – 20
- The TCP-Header / Octet 21 – n (Options)

⇒ Sliding Windows in TCP

The Process of IP-Address Allocation

⇒ The Dynamic Host Configuration Protocol (DHCP)
- Automatic Allocation
- Dynamic Allocation
- Manual Allocation

⇒ Operation of an initial DHCP Request

⇒ Operation of an initial DHCP Request

⇒ Operation of the DHCP in GPRS and UMTS

Private IP-Addresses

⇒ Mobile Subscribers entering the Internet

⇒ Private IP-Address Ranges

⇒ Using Network Address Translation (NAT) for Interconnection

⇒ Principles of Network Address Translation

⇒ Liabilities of NAT
  IPsec in Transport Mode
  Streaming Applications
  Push Services

Access to Applications ⇒ The Domain Name System (DNS)

⇒ Structure of the Domain Name System (DNS)
⇒ Structure of the Domain Name System (DNS)
⇒ Operation of DNS
⇒ Operation of DNS

Details of the Stream Control Transmission Protocol (SCTP)

Details of the Stream Control Transmission Protocol (SCTP)

⇒ The SCTP Header
⇒ The SCTP Header
⇒ The SCTP Chunks / Octet 13 - 16
⇒ The SCTP Chunks / Octet 13 - 16
⇒ SCTP Chunk Types
⇒ SCTP Association Establishment
⇒ SCTP Association Establishment

SIGTRAN

⇒ SCTP in the Signaling Gateway Function (SIGTRAN)
⇒ Transport Protocol Comparison

The Need for QoS in IP Networks

QoS Options in IP-Networks

⇒ Operation of Integrated Services
⇒ Operation of Differentiated Services
  Per-Hop forwarding Behavior (PHB)
⇒ DiffServ ⇔ IntServ
⇒ Operation of MPLS
  Routing Labels

Speed Proxies and their Operation

The GPRS Tunneling Protocol (GTP / GTP')

The Protocol Stack in the Core Network

⇒ Interconnecting the GGSN to External Packet Data Networks

Applicability of GTP-C, GTP-U and GTP'

⇒ GTP-C
⇒ GTP-U
⇒ GTP'

Definition of T-PDU, G-PDU and N-PDU

⇒ N-PDU
⇒ G-PDU
⇒ T-PDU

Definition of GTP Paths and Tunnels

⇒ GTP-Path
⇒ GTP-Tunnel
⇒ Allocation of the TEID during PDP-Context Establishment
⇒ GTP-Tunnel Establishment Procedure between two SGSNs

Functions of GTP

⇒ Path Management
⇒ Tunnel Management
⇒ Location Management
⇒ Mobility Management
⇒ GTP Procedures / Timer and Counter
  T3-Response Timer / N3-Request Counter
  T3-Tunnel Timer
  N3-Buffer Size

GTP-Messages

⇒ GTP-C PDU Format
  Version
  PT (Protocol Type)
  E-flag (Extension header-flag)
  S-flag (Sequence number flag)
  PN-flag (N-PDU number flag)
  Message Type
  Length
  TEID (Tunnel Endpoint Identifier)
  Sequence Number
  N-PDU No
⇒ Example of a GTP-C PDU
⇒ GTP-U PDU Format
⇒ GTP-U PDU Format
  Version
  PT (Protocol Type)
  E-flag (Extension header-flag)
  S-flag (Sequence number flag)

PN-flag (N-PDU number flag)
Message Type
Length
TEID (Tunnel Endpoint Identifier)
Sequence Number
N-PDU No

⇒ Example of a GTP-U PDU

⇒ Information Element Encoding in GTP-C, GTP-U and GTP'
Type-Value (TV) Encoding and Type-Length-Value (TLV) Encoding

⇒ The GTP'-Message Format
Version
PT (Protocol Type)
Message Type
Length
Sequence Number

⇒ The GTP/GTP'-Message Types
ECHO_REQ
ECHO_RSP
VERS_NOT_SUPP
NODE_ALIVE_REQ
NODE_ALIVE_RSP
REDIR_REQ
REDIR_RSP
CT_PDP_CT_REQ
CT_PDP_CT_RSP
UPD_PDP_CT_REQ
UPD_PDP_CT_RSP
DEL_PDP_CT_REQ
DEL_PDP_CT_RSP
ERR_IND
PDU_NOT_REQ
PDU_NOT_RSP
PDU_NOT_REJ_REQ
PDU_NOT_REJ_RSP
SEND_ROUT_INFO_GPRS_REQ
SEND_ROUT_INFO_GPRS_RSP
FAIL_REP_REQ
FAIL_REP_RSP
NOT_MS_GPRS_PRES_REQ
NOT_MS_GPRS_PRES_RSP
IDENT_REQ
IDENT_RSP
SGSN_CT_REQ
SGSN_CT_RSP
SGSN_CT_ACK
FW_RELOC_REQ
FW_RELOC_RSP

FW_RELOC_COM
RELOC_CANCEL_REQ
RELOC_CANCEL_RSP
FW_SRNS_CT
FW_RELOC_COM_ACK
FW_SRNS_CT_ACK
RAN_INFO_RELAY
DATA_REC_TRANS_REQ
DATA_REC_TRANS_RSP

⇒ Example of an ECHO RSP-Message

Types of Charging Data Records (CDR)

⇒ S-CDR
⇒ M-CDR
⇒ G-CDR
S-SMO-CDR / S-SMT-CDR
⇒ LCS-MO-CDR
⇒ LCS-MT-CDR
⇒ LCS-NI-CDR

Exchange of CDR's

⇒ Initial Conditions
⇒ Applicability of this Procedure
⇒ Description

Session Management (SM) in GPRS

Parameters of Session Management

⇒ The QoS-Parameters in Release '99 and beyond
⇒ Applicability of the QoS-Profile
⇒ Applicability of the QoS-Profile
⇒ The Traffic Classes
Conversational Class:
Streaming Class:
Interactive class:
Background class:
Relationship between QoS-Profile and Application
The File Transfer Protocol (FTP)
Voice over IP (VoIP)
The Packet Flow Context (PFC) and the Packet Flow Identifier (PFI)
⇒ The Different PDP-Types
⇒ The Access Point Name (APN)
The Network Identifier
The Operator Identifier
Example: Network Selection with APN = "*" and PDP-Type = IP

Example: Network Selection with APN = “WAP” and PDP-Type = IP
Example: Network Selection without provision of APN or PDP-Type
Example: Network Selection with APN = “UUDIAL.NET” (or without provision of APN) and PDP-Type = PPP

⇒ Protocol Configuration Options
⇒ PDP-Context Parameter Storage
⇒ Message Format for SM
⇒ Message Format for SM
⇒ The SM-Message Types
- ACT_PDP_CT_REQ
- ACT_PDP_CT_ACC
- ACT_PDP_CT_REJ
- REQ_PDP_CT_ACT
- REQ_PDP_CT_ACT_REJ
- DEACT_PDP_CT_REQ
- DEACT_PDP_CT_ACC
- MOD_PDP_CT_REQ (SGSN => MS)
- MOD_PDP_CT_ACC (MS => SGSN)
- MOD_PDP_CT_REQ (MS => SGSN)
- MOD_PDP_CT_ACC (SGSN => MS)
- MOD_PDP_CT_REJ
- ACT_SEC_PDP_CT_REQ
- ACT_SEC_PDP_CT_ACC
- ACT_SEC_PDP_CT_REJ
- SM_STATUS

Transparent Access to the Internet / Intranet

⇒ Network Configuration after Transparent Access

Non-Transparent Access to the Internet / Intranet

⇒ Network Configuration after Non-Transparent Access

Session Management Procedures

⇒ The Operation of Session Management Procedures
⇒ The Mobile Originating PDP-Context Activation Procedure
- Initial Conditions
- Applicability of this Procedure
- Description

⇒ The Mobile Terminating PDP-Context Activation Procedure
- Initial Conditions
- Applicability of this Procedure
- Description

⇒ PDP-Context Deactivation – Mobile Originating
- Initial Conditions
- Applicability of this Procedure
- Description

⇒ PDP-Context Deactivation – SGSN Originating

Initial Conditions
Applicability of this Procedure
Description

⇒ PDP-Context Deactivation – GGSN Originating
Initial Conditions
Applicability of this Procedure
Description

Virtual Private Networking with GPRS (VPN & IPsec)

Security Concerns for Internet Traffic

⇒ Privacy
⇒ Alteration
⇒ Spoofing

Security Analysis of Typical Network Configurations

⇒ Subnet ⇐ SECURE BACKBONE ⇒ Central Corporate
⇒ Subnet ⇐ LEASED LINE ⇒ Central Corporate
⇒ "Road Warrior" ⇐ DIAL UP / INTERNET ⇒ Central Corporate
⇒ Other Corporate Networks ⇐ INTERNET ⇒ Central Corporate

Alternatives for Network Security

⇒ Encryption and Authentication on Layer 1 / 2
⇒ Encryption and Authentication on the Network Layer
⇒ Encryption and Authentication on higher layers

VPN Operation Modes

⇒ IPsec in Transport Mode
Transport Mode and AH
Transport Mode and ESP
⇒ IPsec in Tunnel Mode
Tunnel Mode and AH
Tunnel Mode and ESP
⇒ VPN with IPsec in Tunnel Mode and Transport Mode
VPN with IPsec in Tunnel Mode
VPN with IPsec in Transport Mode

The IPsec Authentication Header (AH)

⇒ Next Header (8 bit)
⇒ Payload Length (8 bit)
⇒ Reserved (16 bit)
⇒ Security Parameters Index (SPI) (32 bit)
⇒ Sequence Number (32 bit)
⇒ Authentication Data (n bit)

The IPsec Encapsulating Security Payload (ESP)

⇒ Security Parameters Index (SPI) (32 bit)
⇒ Sequence Number (32 bit)
⇒ Payload Data (n bit)
⇒ Padding (0 – 255 octets)
⇒ Padding Length (8 bit)
⇒ Next Header (8 bit)
⇒ ESP Authentication Data (n bit)

The Security Association (SA)

Algorithms for IPsec

⇒ How does a Hash Algorithm Work ?
⇒ How does Encryption Work with IPsec ?

Establishment of an IPsec-Relationship

⇒ ISAKMP (Internet Security Association and Key Management Protocol)
  Authentication through Signatures
  Authentication through Pre-Shared Key
  Authentication through Public Key Encryption