v1.600

3GSM & TCP/IP
Protocols, Operation & Services

Course Duration:

- 3 Days

Course Description:

- This course addresses the needs of engineers and technicians who need to enable packet data applications on top of GPRS and UMTS.
- The course first introduces the student into the details of TCP/IP and its application protocols and operation. This section is followed by pointing out the different options for IP address allocation and advanced TCP/IP operation.
- The next part clearly lines out the differences between the different Packet Data Protocols that are supported by GPRS and UMTS.
- The course concludes with the consideration of TCP/IP-performance measurements and possibilities to determine this performance in the wireless environment.

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

Pre-Requisites:

- A basic understanding of TCP/IP is required.
- A basic understanding of GPRS and UMTS data transmission characteristics is required.

Course Target:

- The student is enabled to understand and judge the behavior and specific problems of TCP/IP in the wireless environment.
- In addition the student learns the different options for allocating IP-addresses to mobile subscribers, incl. through VPN-access. In that respect, the student also learns about IPsec.
- The student will be enabled to effectively communicate to content providers and IT-people when it comes to the configuration, restrictions and benefits of potential services for 3GSM packet data networks.

Some of your questions that will be answered:

- Why is the TCP back off mechanism critical in the wireless environment ? What can we do to minimize its impact in case of cell reselections ?
- Does it make sense to allocate private IP-addresses to our mobile subscribers? What are the implications of using Network Address Translation ?
- What is the difference between the GPRS application protocols PPP and IP?
- How can we implement a virtual dial-up service to an external ISP over our network?
- What is required to establish VPN access for our volume customers?
- How does IPsec operate? How can we implement it in our network?
- What options are there for authenticating a user? What differences are there between PAP/CHAP and RADIUS?
- How can we measure and improve the performance of our GPRS-network?

Who should attend this class ?

- Everybody who needs to optimize GPRS networks
- Everybody who needs to understand the implications of merging IP and 3GSM
- Content and Service Providers of Mobile Packet Data

Table of Contents:

⇒ 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

Using ICMP for Roundtrip Time (RTT) Measurements in GPRS

⇒ Use Trace Route to Determine the IP-Address of the 1st Router
Ping with 32 Octets of Data (no Segmentation)
Ping with 544 Octets of Data (still no Segmentation)
Ping with 1000 Octets of Data (Segmentation)

Transport Protocols on Top of IP

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
Example for TCP Connection Establishment
⇒ TCP Connection Release
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)

Details of TCP-Operation

⇒ The Roundtrip Time (RTT) in TCP-Connections
Roundtrip Time (RTT) and Retransmission Timeout (RTO)
Long Term Behavior of SRTT and RTO
⇒ Advanced TCP-Features
⇒ The Nagle Algorithm and Delayed Acknowledgements
⇒ The Slow Start and Congestion Avoidance Algorithms
Introduction
Slow Start and Congestion Avoidance in Operation
Long Term Characteristics
⇒ The Ultimate Importance of RTT and CWND for GPRS
The formula for calculating SRTT and RTO is tailored for wireline connections
In GPRS, the RTT is highly variable and may therefore cause unnecessary retransmissions
Slow start memorizes instances when RTT ≥ 2 x SRTT
RTT variance in GPRS can have many reasons
⇒ Consequences of the RTT-Variance for the GPRS Performance
Example: FTP-Upload at 150 km/h
⇒ Latency Requirements
⇒ The Fast Retransmit Algorithm
⇒ The Fast Recovery Algorithm

And what about TCP/IP in GPRS ?

⇒ Some Basic Questions
How do the various TCP/IP algorithms impact GPRS operation ?
Can GPRS be considered as a typical Dial-Up Service ? (which implicitly requires similar settings)
How critical is the high variance of RTT during a GPRS data transfer when it comes to unnecessary retransmissions ?
⇒ The Bandwidth Delay Product
Some Example Calculations for GPRS and Dial-Up
Consequences for GPRS

Performance Improvement through MSS-Adjustment
Setting of the Parameter IPMTU in WINDOWS 98
Setting of the Parameter DefaultRcvWindow in WINDOWS 98

VPN-Operation and 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

The Point-to-Point Protocol (PPP) and PDP-Context Activation

GPRS Dial Up Network Access
⇒ The Point-to-Point Protocol (PPP) Frame Format
⇒ Operation of Dial Up Network Access
Link Establishment Phase
Authentication and Network Layer Setup
Link Termination
(1) Example for Dial-Up Network Access using the PPP
⇒ The Mobile Originating PDP-Context Activation Procedure
Initial Conditions
Applicability of this Procedure
Description

Examples for Application Protocols

Important Application Protocols
Access to Applications ⇒ The Domain Name System (DNS)
⇒ The Hypertext Transfer Protocol (HTTP)
The HTTP-Message Format
Operation of the Hypertext Transfer Protocol
Download of a given Web Page
⇒ GPRS Performance Measurements with HTTP
Definition of Trigger Points