v1.700

Course Sequence: ***IP for Telecom Professionals***

Module 1: "Quo vadis" / Module 2: The Basics / *Module 3:* ***Advanced Issues***

Course Duration:

3 days

Course Description:

- This course is targeted at telecom engineers and technicians who are already familiar with TCP/IP-protocol suite and who require detailed and practical knowledge about advanced IP-related issues like VoIP, SS7 and QoS in IP-networks and security in IP-networks.
- The final 3 days of the course sequence "IP for Telecom Professionals" are called "Advanced Issues". After a short review of the IP-protocol suite the course explains in detail the Interworking between IP and SS7 (⇔ SIGTRAN).
- In the next parts, the course makes the students familiar with SIP-based VoIP and how these sessions are setup and released. The hands-on part requires the student to record some SIP-sessions and evaluate these recordings. Note that our test network will include the related SIP-servers and clients.
- One major focus of the course is on QoS and how to provide it in IP-based networks. We present the major technical options like DiffServ and IntServ and we included a practical part in which QoS-parameters are configured within our test network by the students.
- The final highlight of this course is on security issues in IP-networks and how to tackle them. We illustrate the different technical possibilities and we included various hands-on exercises and presentations to make the students familiar with this very important IP-issue.

Pre-Requisites:

- The student should possess detailed knowledge of wireline and/or wireless communications, particularly within the area of operation or engineering.
- Very good knowledge of the TCP/IP-protocol suite and its architecture is necessary.

Course Target:

- The student will be familiar with the important telecommunication related aspects of the IP-protocol suite.
- The student will understand what the difficulties are in providing QoS in an IP-network. This enables the student to setup and operate their own QoS-aware IP-networks.
- The student will be familiar with state-of-the-art IP-sniffers and how to use them to analyze network problems.
- Last but not least, the student will know the different options how to secure any data transfer in IP-networks. Like for all the other parts, this includes the "playing around" with authentication and encryption setup, configuration and analysis in our test network.

Table of Contents:

⇒ Indirect Routing
Next Hop Routing
Static Routing
Dynamic Routing

IP Networks as Transport in Telecommunication

Architectural Overview Future All-IP Network

High Level View at the IMS and its Environment
⇒ Mobility Issues
⇒ Relationship to other Networks
⇒ User Terminals
⇒ Performance Figures of the Different IP-CAN's

(1) Example: IP Datacast (IPDC) over DVB-H
⇒ What is the IMS?
⇒ And what is inside the IMS?
⇒ Protocols of the IMS
⇒ The Perspective of the Mobile Station

Introduction to SIP-T
⇒ SIP-Bridging
(1) Message Flow for SIP-Bridging
⇒ PSTN-Originating Session
⇒ SIP-Originating Session

What is SIGTRAN?
⇒ SCTP in the Signaling Gateway Function (SIGTRAN)

Mobile IP Issues

Some Mobility Considerations
⇒ Personal Mobility
⇒ Terminal Mobility
⇒ Mobility at the Access Network
Micro mobility
⇒ Mobility in IP networking environments (today)
PPP dialup
DHCP
Macro mobility

Mobile IP
⇒ Mobile IP Operation Overview

⇒ Host A
⇒ Home Agent
⇒ Foreign Agent
⇒ Mobile Host B
⇒ S
⇒ Mobile Agent Advertisement Extensions
⇒ Mobile Agent Solicitation Extensions
⇒ Prefix-Lengths Extension
⇒ (2) Selected Message Formats
⇒ Mobile IP Registration Request
⇒ (3) Selected Message Formats
⇒ Mobile IP Registration Reply
⇒ M
⇒ Tunneling more Mobile IP Considerati
⇒ Reverse Tunneling
⇒ Broadcast
⇒ Move detection
⇒ ARP Considerations
Proxy ARP
Gratuitous ARP
⇒ Mobile IP Security Considerations
⇒ Mobile IP usage: Trusted Non-3GPP RAT's in SAE / EPC
⇒ Signaling Procedures if MIPv4 is used

Voice over IP (VoIP)

Reasons for VoIP
⇒ Network Convergence
⇒ Growth of Data Networks
⇒ Resource Efficiency
⇒ Service Flexibility

The H.248 Protocol
⇒ H.248 ⇔ MEGACO
⇒ Principles of Media Gateway Operation
⇒ Interworking MSC-S ⇔ MGW
⇒ The H.248 Command Set

Examples of Media Gateway Operation through H.248

Examples of Media Gateway Operation through H.248
⇒ Mobile Originating Call Establishment
⇒ The H.248 Message Structure
Overview
Part 1: H.248 Message Header

Part 2: Transaction Encoding
Part 3: Action Request Encoding
Part 4: Command ADD-Request Encoding

The H.323-Protocol and Network Architecture
⇒ Network Architecture
H.323-Terminals
Gatekeepers
Gateways
Multipoint Control Unit
⇒ The H.323-Protocol Suite
⇒ The H.323-Protocol Suite
H.225.0 (RAS)
H.225.0 (Call Control / Q.931)
H.245 (Media Control)
⇒ The H.323-Protocol Stack
⇒ The H.323-Protocol Stack

(1) Registration and Call Setup with H.323
⇒ Initial Conditions
⇒ Applicability of this Procedure
⇒ Description

Scope of SIP
⇒ Session Establishment
⇒ Clarification of the Term “Session”
⇒ Session Modification
⇒ Session Release
⇒ Philosophy of SIP-Operation
Session Completion Phase
Session Active Phase
Session Active Phase
⇒ Comparison between SIP and HTTP

(1) Different Implementations of SIP
⇒ Option 1: Amateur Use of SIP
⇒ Option 2: Semi-Professional Use of SIP
⇒ Option 3: Professional Use of SIP for VoIP (PSTN-Replacement)

Simple Example of a SIP-Scenario: VoIP Call Setup with SIP
⇒ Overview
⇒ Summary: Some SIP-Terminology

SIP-Message Format
⇒ General Information
⇒ Request Messages
⇒ Response Messages

SIP-Message Contents

⇒ The Request Line (Request Messages only)
⇒ T
  REGISTER
  INVITE
  ACK
  CANCEL
  BYE
  OPTIONS
  INFO
  MESSAGE
  SUBSCRIBE
  NOTIFY
  PUBLISH
  PRACK
  REFER
  UPDATE
⇒ Address Specification / Request-URI
  The “tel”-URI
  The SIP(S)-URI
⇒ The Status Line
  Status Code and Reason Phrase
⇒ The “From:” and the “To:” Header Fields
  Display-Name
  Tag
⇒ The “Call-ID:” and “Max-Forwards:” Header Fields
  Call-ID
  Max-Forwards
⇒ The “CSeq:” Header Field
⇒ The “Via:” Header Field
⇒ The “Contact:” Header Field

The Session Description Protocol (SDP)

⇒ The Offer / Answer Model
⇒ Structure of SDP-Parameters within a SIP-Message
⇒ S
  SDP-Protocol Version Number
  Origin of Session and Session Identifier
  Session Name
  Session Information
  URI of Information to additional Conference Description
  e-mail Address and Telephone Number
  Connection Information
  Bandwidth Information
  Time Zone Adjustments
  Encryption Key

Session Attributes
⇒ Media Description Items
Media Name and Transport Address
Media Title
Connection Information
Bandwidth Information
Encryption Key
RTP Mapping Attribute
⇒ Time Description Items
Start and Stop Time when the Session is active
Repeat Times
⇒ Example: Session and Media Descriptors through SDP

Problems of VoIP
⇒ Delay
⇒ Jitter (Packet Arrival Time Variance)
⇒ Packet Loss
⇒ Bandwidth Bottlenecks

Quality of Service (QoS) in IP Networks

The Need for QoS in IP Networks

QoS Options in IP-Networks
⇒ Operation of Integrated Services
IntServ Parameter Descriptors
IntServ Parameter Descriptors
⇒ FilterSpec
⇒ FlowSpec
Tspec
Rspec
(1) Operation of the Resource Reservation Protocol (RSVP)
Sending of RSVP: Path-Messages
Sending of RSVP: Resv-Messages
Tearing Down a Path
RSVP Message Format
RSVP Message Format
Some RSVP Message Details
Some RSVP Message Details
RSVP PATH Message
RSVP RESV Message
⇒ Operation of Differentiated Services
DiffServ Edge Router
DiffServ Edge Router
⇒ Classifier
⇒ Meter

⇒ Marker
⇒ Shaper / Dropper
Per-Hop forwarding Behavior (PHB)

Routing over mixed IntServ – DiffServ Networks

Routing over mixed IntServ – DiffServ Networks
⇒ DiffServ ⇔ IntServ
⇒ Operation of MPLS
Routing Labels

IPv6 Details

Format of the IPv6 Header
⇒ Format of the Internet Protocol Version 6
⇒ IPv6 Multiple Extension Header
⇒ IPv6 Routing Header
⇒ IPv6 Routing Header
⇒ IPv6 Fragmentation Header
⇒ IPv6 Fragmentation Header
⇒ IPv6 Fragmentation
⇒ IPv6 Fragmentation
⇒ IPv6 Address Formats
⇒ IPv6 Address Formats
⇒ Unicast Address
⇒ Multicast Address
⇒ Anycast Address

IPv6 Special Multicast AddressesIPv6 Special Multicast Addresses

IPv6 Special Multicast Addresses
IPv6 ⇔ IPv4 Address Mapping

ICMPv6 Messages

ICMPv6 Messages

Security in IP Networks

RADIUS Message Format
⇒ Message Codes

DIAMETER Overview

DIAMETER Overview

Diameter Base Protocol (DBP)
⇒ Characteristics

Diameter vs RADIUS
Better Transport
Better Proxying
Better Session Control
Better Security
⇒ Diameter Message Format
⇒ Diameter AVP Messages
⇒ Diameter AVP Messages

Details of RSA-based Authentication and Encryption
⇒ X.509 Certificate Structure
⇒ Generating and Signing an X.509-Certificate

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

SSL Overview
⇒ SSL Handshake

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
⇒ Reviewing some of the used Algorithms
⇒ Reviewing some of the used Algorithms
The HMAC with SHA-1-Algorithm
The DES-Algorithm (Data Encryption Standard)
DES-Operation in CBC-Mode (Cipher Block Chaining)
The 3-DES-Algorithm (Triple Data Encryption Standard)
The AES-Algorithm in CCM-Mode
Operation of AES in CCM-Mode

List of Acronyms

Index: