

UMA / GAN from A - Z

Course Duration:

- 2 days

Some of your Questions that will be answered:

- Which network operators and which devices do support generic access?
- How can WiFi serve as bearer for GSM-/UMTS-based procedures like voice calls or short message delivery?
- What are the differences between serving, default and provisioning GANC's?
- How does a mobile phone setup an IPsec-tunnel towards a GANC?
- How does a mobile phone switch back and forth between GAN and GERAN/UTRAN, perhaps with an active voice call?

Table of Content:

Introduction and Overview

- **Targets and Basics of GAN**
 - ⇒ What is Generic Access?
 - ⇒ Generic Access in the Context of Alternative RAT's
- **Implementation Status of Generic Access**
 - ⇒ Operator Support
Generic Access and Femto Cells
 - ⇒ Supporting Cell Phones
- **Operation Principles**
 - ⇒ Mobile Station Operation Modes
GERAN/UTRAN only, GERAN/UTRAN preferred, GAN preferred, GAN only
 - ⇒ Procedures & Terminology
Rove In / Rove Out, GANC Discovery, GANC Registration, GANC De-Registration
- **Network Architecture**
 - ⇒ GAN and GANC in Context with WiFi and Legacy Networks
 - ⇒ GAN in Context of VoLGA
Principles of VoLGA
- **Protocol Stack and Protocol Architecture**

Details of WiFi-Operation

- **The IEEE 802.11 Alphabet**
 - IEEE 802.11-1999, IEEE 802.11b, IEEE 802.11g, IEEE 802.11a, IEEE 802.11e, IEEE 802.11i, IEEE 802.11k, IEEE 802.11r, IEEE 802.11u, IEEE 802.11ac, IEEE 802.11ad
 - ⇒ Important Changes with 802.11n
Smart Antenna related Enhancements, Packet Aggregation related Enhancements, Channel Bonding related Enhancements, Other Enhancements , More Data Subcarriers / Smaller Guardband, Performance Gain, Short Guard Interval (GI), Consequences of using a short GI, Logfile Extract: Indication of Short-GI in HT-SIG, FEC Changes, New Code Rate 5/6, Low Density Parity Check Coding (LDPC), Power Saving Enhancements, Legacy Modes: APSD and TIM-based Power Save Mode, SM Power Save, PSMP (Power Save Multi Poll), Reduced Inter Frame Space (RIFS), AIFS, DIFS, EIFS, RIFS, SIFS, Advantages of RIFS
- **The Physical Resource**
 - ⇒ The ISM Band in 2.4 GHz and 5 GHz
 - ⇒ Channel Numbers and Allocation / 2.4 GHz
 - ⇒ Channel Numbers and Allocation / 5 GHz
 - ⇒ Short Review of the PHY-Layer
Introduction to the OFDM in 802.11, Normal OFDM Symbol, Short OFDM-Symbol, Generation, Long OFDM-

Symbol, Generation, Distinction in case of different Channel Bandwidth (5, 10 and 20 MHz), Format of the PPDU with OFDM-PHY, PLCP Preamble, L-SIG (SIGNAL-Field), SERVICE-Field, PSDU, Tail Bits / Padding, Meaning of RATE for Modulation Scheme, Code Rate etc.

- **Network Architecture in WiFi**

Infrastructure Mode, Ad-hoc Mode

- **Protocol Stack of IEEE 802.11 in Context**

PDU-Types in the Protocol Stack, MSDU, MPDU, PPDU

⇒ Example of an IEEE 802.11 MPDU

- **Operation of IEEE 802.11**

⇒ **CSMA/CA - Resource Sharing and Network Access**

Principle Operation, Behavior in case of Collisions, Format and Content of the PLCP-PDU, Physical vs. Virtual Carrier Sensing, Physical Carrier Sensing, Virtual Carrier Sensing, Network Allocation Vector

⇒ **The Different MAC-Access Coordination Functions**

Overview, Distributed Coordination Function / Example Operation, SIFS-, Slot- and CW-Values for different PHY's, DCF with RTS/CTS-Enhancement, Point Coordination Function (PCF), Indication of an AP whether PCF is supported, Indication whether the AP supports 802.11e QoS, Enhanced Distributed Channel Access (EDCA), Parameterization of QoS-Settings, Calculating CW(min) / CW(max) from ECWmin and ECWmax, HCF Controlled Channel Access (HCCA), Example of a QoS-Data+CF-Ack+CF-Poll-Frame

- **Reviewing MAC-Frame Types and IE's**

⇒ **Generic MAC Frame (Data Frame)**

Frame Control field, Duration ID field, Address fields, Sequence Control field, QoS Control field, Frame Body, FCS field, Details of the Frame Control Field, Protocol Version field, Type and Subtype fields, To and From DS fields, More Frag field, Retry field, Power Mgt field, More Data field, WEP field, Order Field

⇒ **Control Frame Subtypes**

BlockAckReq and BlockAck, PS-Poll, RTS and CTS, Ack, CF-End and CF-End+CF-Ack, Control Wrapper

⇒ **Management Frame Subtypes**

Association request and Association response, Reassociation request and Reassociation response, Disassociation, Probe request and Probe response, Beacon, Announcement Traffic Information Message, Authentication and Deauthentication, Action, Action No Ack

⇒ **Data Frame Subtypes**

Data frames, Null frames, CF-Ack frames, CF-Poll frames, QoS frames, Usage of the Address Fields in Data Frames, Destination Address field, Source Address field, Receive Address field, Transmitter Address field, BSSID field

⇒ **Action Frames**

Spectrum management Action frames, QoS Action frames, DLS Action frames, Block Ack Action frames, HT Action frames

- **Aggregation through A-MSDU**

⇒ Practical Exercise: Evaluate a PPDU with A-MSDU inside

⇒ **Detailed Operation and Constraints**

From LLC-Frame to A-MSDU - Mapping Rules, Limitation of Frame Sizes (A-MSDU)

- **Aggregation through A-MPDU**

⇒ Example of an A-MPDU

⇒ **Detailed Operation and Constraints**

From LLC-Frame to A-MPDU - Mapping Rules, Limitation of Frame Sizes (A-MPDU)

- ⇒ Organization of MPDU's within an A-MPDU
- ⇒ Combination of A-MSDU and A-MPDU Aggregation
- ⇒ Practical Exercise: A-MSDU vs A-MPDU Aggregation

- **BlockAck-Procedures**

- ⇒ Reviewing Acknowledgement Policies
Normal Ack, No Ack, No explicit Ack, Block Ack
- ⇒ Option 1: Immediate BlockAck Procedure
Setup BlockAck, Transmission of data frames, Block Ack Request – Block Ack exchange, Termination of Block Ack
- ⇒ Option 2: Delayed Block Ack Procedure
Setup of Delayed BlockAck's, BlockAck Request – BlockAck exchange, Switch back to normal Ack procedure in the BlockAck period, Termination of Delayed BlockAck
- ⇒ Important Changes with 802.11n
New Format of the BlockAck Request Frame, Redefined BAR-Control Field, BA-Info, New Format of the BlockAck Frame, Redefined BA-Control Field, BA-Info, The Compressed Bitmap and its Interpretation

- **Security Technologies for IEEE 802.11**

- ⇒ Overview
Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA and WPA2), Virtual Private Networking (VPN)
- ⇒ WPA and WPA2: How to Create the Key Material
Master Keys (PSK, MK, PMK), Pairwise Transient Key (PTK), KCK, KEK and TK, The Process to generate the PMK = PSK, Beacon frames, Exchange of Probe Request and Probe Response Frames, Open System authentication, Association, Conditional: EAP Authentication, EAPOL 4-Way Handshake
- ⇒ WEP: How to generate the Shared Key
Authentication challenge, The WEP-Encryption Process

- **Association Process to an Access Point**

- Passive and Active Scanning, Authentication Procedures, Exchange of Association Request / Response Frames

Generic Access Elementary Procedures

- **GANC-Discovery and Registration**

- ⇒ Overview
GANC Discovery, GANC Registration
- ⇒ Types of GANC
Provisioning GANC, Serving GANC, Geographical Relationships, Default GANC, Typical GAN Use Cases
- ⇒ Practical Exercise: Examine a GAN Registration Logfile
Part 1: Register Request-message, Part 2: Register Accept Message

- **Tunnel Setup Procedures**

- ⇒ EAP-SIM
Initial Conditions, Applicability of this Procedure, Detailed Description

⇒ EAP-AKA

Initial Conditions, Applicability of this Procedure, Detailed Description

⇒ IKEv2

IKEv2-Procedure, Initial Conditions, Applicability of this Procedure, Detailed Description, Cryptographic Suites for GAN

● **The Protocol Suite within the GA-Environment**

⇒ GA-Specific Protocols

GA-RC (Generic Access - Resource Control), GA-CSR (Generic Access - Circuit-Switched Resources), GA-PSR (Generic Access - Packet-Switched Resources), GA-RRC (Generic Access - Radio Resource Control)

⇒ Protocol Stack Details

Circuit-switched Control Plane, Circuit-switched User Plane, Transcoding, Packet-switched Control Plane, Packet-switched User Plane

⇒ Message Format

GA-CR and GA-CSR, GA-PSR, GA-PSR over TCP, GA-PSR over UDP, GA-RRC, GA-RRC over TCP, GA-RRC over UDP

Generic Access within the GERAN/UTRAN Environment

● **Important Layer 3 Scenarios within GAN**

⇒ IMSI Attachment / Location Update

⇒ Mobile Originating Voice Call

⇒ Mobile Terminating SMS Transfer through GAN

● **Mapping between GERAN/UTRAN and GAN-Cells**

⇒ Important Questions

⇒ Rove In and...

⇒ ... Rove out

⇒ GAN Cell Descriptors

GAN Cell ID based on GERAN / UTRAN Location, GAN ARFCN / BSIC for Handover to GAN, Preparation of Handover from GERAN to GAN, Difference in UMTS

● **Handover Scenarios**

⇒ Handover from GERAN into GAN

Detailed Description

⇒ Handover from UTRAN into GAN

Detailed Description

⇒ Handover from GAN into GERAN

Detailed Description

⇒ Handover from GAN into UTRAN

Detailed Description

Solutions for Practical Exercises