v 1.001

LTE - Interworking with WiFi

Course Duration:

- 2 days

Course Description:

- This course addresses the needs of managers, engineers and technicians who are involved in the design, consideration and development of interworking implementations between LTE and other 3GPP cellular standards on one hand and WiFi on the other hand. In that respect, the course focuses on both sides, UE/Mobile as well as network.

- The course starts with an overview of the Mobile Network Architecture with Protocol Stacks, Access capabilities and applicability as well as handover principles.

- We will then review different interworking options, such as I-WLAN, WISPr, tunneling through GAN / UMAN / VoLGA or as non-trusted, non 3GPP access network connecting to LTE infrastructure with DSMIP or PMIP as well as reviewing voice call setups with and without IMS support.

- The course will continue with a detailed review of the 802.11 variants, differences and internal functions. This part provides a roadmap from 802.11-1999 up to the most recent 802.11n version.

- We will discuss WiFi access mechanisms to the physical transport, such as CSMA/CD and the function and purpose of the DCF access function. This is done as it is crucial to understand the specifics and differences of WiFi vs. cellular network operation.

- The interworking with the Physical Protocol Layer will be discussed both from the perspective of the terminal and from the network side with constraints, access permission mechanisms, how to obtain IP addresses etc.

- The course will conclude with a comparison of the different access architectures, related handover types and recommendations regarding a most suitable implementation.

Prerequisites:

- The student should possess good knowledge in wireless and/or cellular communication technology before coming to the course.

- We would recommend our webinars or web based training courses on WiFi and LTE to be taken as course preparation.

Course Target:

- The student is enabled to understand, design and integrate WiFi based access networks and UE's as alternative to 3GPP access networks.

Some of your Questions that will be answered:

- Why is there a need for WiFi to interwork with the EPC of 3GPP Rel. 8 and later and what are the different options for the network access?
- How does a voice call setup work with WiFi , what are the options and what are the benefits of using VoLGA or IMS?
- How is authentication of the terminal being done in case of a roaming through WiFi instead of a LTE access?
- What is the protocol stack in case of a WiFi access network and what is the difference between DSMIP and PMIP?
- Which are the implementation options for QoS in WiFi and how can the the performance be improved for certain services?
- Which roles may the network and the UE take on when it comes to interworking?
- How does a handover work between 3GPP access networks and a WiFi access network in case of a roaming mobile?
- How is access permission being handled in case of non trusted non 3GPP access networks?

Who should attend this Course:

- The course is particular useful to engineers and technicians who are involved in the design, operation and interworking of LTE networks with WiFi access networks.
- Network operators and technical staff who need understand the application of non trusted, non 3GPP access networks in a LTE environment.
- Everybody who requires detailed knowledge about WiFi interworking with LTE.

Table of Content:

Overview & Applicability

Implementation Options of Interworking

Circuit-Switched Control Plane, Circuit-Switched User Plane

⇒ Network Architecture in case of VOLGA

- **WISPr**

  ⇒ Important Facts of WISPr

  ⇒ WISPr Logon Procedure

  ⇒ The Welcome and Logon Screens

  ⇒ Difficulty of WISPr with respect to Support of the UE

- **Implementation of WiFi as non-trusted Non-3GPP Access Network**

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

  ⇒ Related Network Architecture

  ⇒ Signaling Procedures if IKEv2 and PMIPv6 are used

  ⇒ Signaling Procedures if IKEv2 and DSMIPv6 are used

- **Implementation of WiFi as another IP-CAN in the IMS-Context**

  ⇒ Network Architecture

  ⇒ Operation: Network Attachment

  ⇒ Operation: IMS-Registration

Inside WiFi

- **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 802.11n, IEEE 802.11r, IEEE 802.1u, IEEE 802.11ac, IEEE 802.11ad

- **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

- **Network Architecture**
  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

- **Security Technologies for IEEE 802.11**

⇒ Overview
Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA and WPA2), Virtual Private Networking (VPN)

⇒ EAP and PSK: How to Create the Key Material
Master Keys (PSK, MK, PMK), Pairwise Transient Key (PTK), KCK, KEK and TK

⇒ Pre - RSNA Procedures
Open System Authentication, Shared Key Authentication, Authentication challenge, The “Wired Equivalent Privacy” Procedure

⇒ RSNA Procedures
RSNA Policy Selection, Probe Response frames and Beacon frames, Open System authentication, Association

⇒ Advanced Authentication
Network Overview: Supplicant, Authenticator, Authentication Server, Redirection, Uncontrolled port, Controlled port, Session Phase 1: Probing & Association, Beacon frames, Exchange of Probe Request and Probe Response Frames, Open System authentication, Association, Session Phase 2: EAP Authentication, EAPOL start, EAPOL identity exchange, EAPOL challenge, EAPOL success, Session Phase 3: EAPOL 4-Way Handshake, 1st EAPOL message, The 2nd EAPOL message, The 3rd EAPOL message, The 4th EAPOL message, Session Phase 4 & 5: Active Session & Disassociation

⇒ Power Saving Techniques in WiFi

⇒ Overview
Legacy Modes: APSD and TIM-based Power Save Mode, SM Power Save, PSMP (Power Save Multi Poll)

⇒ Case Study: Operation of PSMP
Format and Content of the PSMP-Frame

Interworking Issues within the Physical Layer

- **The Perspective of the UE**

⇒ Constraints
Multiple Radio Issue, Measurements, Supported / Preferred Handover Types

⇒ Handover Types: Make before Break vs. Break before Make

⇒ Physical and Time Behavior during Network Transition
Case 1: Preferred Network fades away, Case 2: Preferred Network becomes available

⇒ Support though the ANDSF
Problem Description, Interworking with the ANDSF

⇒ The Connection Manager

- **The Perspective of the Network Operator**

  ⇒ Constraints

  Variety of Implementation Choices, Quality of Service, Competition from UE Manufacturers, Mobility Support through the EPC, Related Network Architecture, Signaling Procedure (NBM / PMIPv6 on S2b)