V1.601

WiFi from A - Z

Course Duration:

2 days
+
1 optional day trace analysis

Course Description:

- This course focuses on a detailed description WiFi / WLAN with emphasis on PHY and MAC.
- Following a short view on WiFi fundamentals (architecture, standards, frequency bands), the course investigates the tasks, and the structure of the different IEEE 802.11 physical layers (1999, a, b, g).
- A major focus of this WiFi course is put on understanding and comparing the MAC functions used in the various variants of WiFi: 802.11, 11h, and 11e (QoS).
- Another focus is related to security aspects e.g. ciphering, authentication, association. Both, the service provider's, as well as the user's point of view is considered (802.11,11i, and EAP authentication).
- Whenever applicable, we use real live examples from various sources to provide a realistic view on WiFi issues.
- After beefy discussing WLAN deployment the course is focusing on new 802.11 standards where 11n is discussed in detail. The aspects of introduction or extension of WiFi into existing communication networks are discussed as well.
- Finally this training addresses the Vo802.11 aspects and the WiFi certificates.
- This course addresses the needs of engineers and technicians who shall be involved with WiFi hotspots and equipment.
- This course is particularly interesting for engineers already experienced in mobile radio networks.

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

Optionally the training can be extended for one more day in order to allow to analyze traces (also the customers own traces are possible).

Pre-Requisites:

- The student should possess detailed knowledge of wireless communications, particularly within the area of digital signal processing in wireless communications.
- This experience should stem from hands-on work in the area of design, integration, test or troubleshooting of GSM, CDMA or WCDMA-equipment.
- Comprehension of different digital modulation schemes like QAM or PSK and of different multiple access schemes like TDMA, FDMA and CDMA is required.

Course Target:

- The student will obtain detailed understanding of the WiFi standards and the related procedures and network operation and architectures.
- The student is enabled to access the WiFi technology with regard to deployment issues and product strategy issues.
- After the course the student will be enabled to design, test and operate WiFi networks and STA's.

Some of your questions that will be answered:

- What is the difference between IEEE 802.11a, b, e, f, g, i, and n?
- How to the different physical access schemes used in WiFi work?
- How is OFDM working and why it is used in the newer WiFi standards?
- What technologies are used in order to enhance the throughput of WiFi?
- What are the throughput limitations for the various WiFi derivatives?
- How scheduling is performed in the different 802.11 modes?
- What are the functions do the different WiFi-sublayers?
- How can I roam between several AP's while encryption is applied?
- How and by whom are concurrent accesses and priorities controlled?
- How voice services are provided using WiFi?
- What is the work split in-between IEEE and WiFi?
- What WiFi certificates the products have to adhere to?

Who should attend this class?

- Mobile network operators who want to add WiFi-Hot-Spots to their existing network infrastructure.
- Operator of WiFi networks.
- Engineers and technical staff who require detailed inside knowledge of the WiFi and IEEE 802.11 standards.
- Design and test engineers who would like to be enabled quickly for WiFi technology.

Table of Contents:

Introduction and Fundamentals

- **IEEE 802.11 Architecture Overview**
  STA, AP, DS, BSS, ESS, IBSS, QSTA and QAP
- **IEEE 802.11 Specification ABC**
  802.11-1999 , 802.11a, 802.11b , 802.11b/ Cor 1-2001 , 802.11d , 802.11e , 802.11g , 802.11h , 802.11i, 802.11j, 802.11-2007
- **IEEE 802.11 Protocol Stack Architecture**
  MAC, PLCP , PMD, MAC and PHY Management Entities, Station Management Entity (SME)
- **Physical Layer Overview**

  ⇒ TDD operation in an IEEE 802.11 Network

  ⇒ Current IEEE 802.11 Physical Layer Access Technologies
  FHSS, DSSS, IR, OFDM, HR-DSSS, ERP-DSSS/CCK, ERP-OFDM, ERP-PBCC, ERP-DSSS-OFDM

  ⇒ Frequency Bands being used for IEEE 802.11 Standards
- **Lessons Learned / Conclusions:**

Physical Layer procedures

- **General PLCP Burst**
- **FHSS Physical Layer**

  ⇒ FHSS PLCP Burst

  ⇒ GFSK Modulation

  ⇒ FHSS Signal Processing Chain
- **IR Physical Layer**

  ⇒ IR PLCP Burst
- **DSSS Physical Layer**

  ⇒ DSSS PLCP Burst

  ⇒ DBPSK and DQPSK Modulation

  ⇒ DSSS Signal Processing Chain
- **OFDM Physical Layer**

  ⇒ Introduction OFDM Technology
  Impact of Orthogonality in the Frequency Domain – 3 Steps, Practical Exercise: Physical Basics of OFDM, OFDM and IFFT, Using different Modulation Schemes on Different Subcarriers, Tackling Inter-Symbol Interference (ISI), Introduction, Cyclic Prefix or Guard Interval

⇒ OFDM PLCP Burst
Normal OFDM Symbol, Long OFDM Sync Symbol, Short OFDM Sync Symbol

⇒ Modulation and Data Rates of the OFDM Physical Layer

⇒ OFDM Signal Processing Chain
Modulation Schemes for OFDM, OFDM Convolutional Encoder, OFDM Physical Layer Puncturing

- **HS-DSSS Physical Layer**

⇒ HS-DSSS PLCP Burst

⇒ CCK Modulation

⇒ Details of CCK

⇒ PBCC Signal Processing Chain

- **DSSS-OFDM Hybrid Physical Layer**

⇒ DSSS-OFDM PLCP Burst

⇒ ERP-PBCC Processing Enhancements

- **Agility**
- **Lessons Learned / Conclusions:**

Medium Access Control

- **Basic MAC Functions**

⇒ Overview
Asynchronous Data Service, Security Service, MSDU Ordering

⇒ MAC Frames
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, 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, 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, Data Frame Body, Initialization Vector field, MSDU field, Integrity Check Value field

⇒ Fragmentation of MSDU's

⇒ MAC Access Coordination Functions
Distributed Coordination Function, Point Coordination Function, Hybrid Coordination Function

⇒ MAC Procedures
Timing governing the Access: SIFS, PIFS, and DIFS, SIFS, PIFS, DIFS, EIFS and AIFS, EIFS, AIFS, Scanning and Exchange of Management Frames, Passive scanning, Active scanning, Beacon frame, Exchange of management frames, Coexistence of PCF and DCF, Scheduling of CFP and CP, Behavior in the CP, Behavior in the CFP, Shortened CFP, DCF- Sensing Procedures, Physical carrier sensing, Virtual carrier sensing, DCA & Random Backoff Procedure, Concept of random backoff procedure, Behavior in case one STA accesses earlier than another, Resumption of the backoff procedure, Behavior in case of failure, DCF & Transmission of Fragments, RTS – CTS

procedure, Prolongation of the duration field and NAV for fragments, Contention Free Period Procedures – Example 1, Transmission of Beacon frames, Polling procedure, Bidirectional data flow, Contention Free Period Procedures – Example 2, Handling of errors , End of the CFP, Power Saving Procedure in the CP, Transmission of beacon frames, Polling of PS AP's, Transmission of multicast and broadcast traffic, Power Saving Procedure in CFP

⇒ Control Frames
RTS Frame, CTS and Ack Frame, PS-Poll Frame, CF-End (+Ack) Frame

- **Additional MAC Functions for later Standard Versions**

⇒ Overview
Asynchronous data service, Security services

⇒ DFS
Restricted association, Quieting of channel for measurements, Testing presence of radar, Switching to other channels in case of interference, Measurement report request

⇒ TPC
Coexistence with radar in the 5 GHz band, Adaptation of the TX power according to path loss and link margin, Use in other bands

⇒ Action Frames
Spectrum management Action frames, QoS Action frames, DLS Action frames, Block Ack Action frames

⇒ QoS
User Priorities, Background (BK), Best Effort (BE), Excellent Effort (EE), Controlled Load (CL), Video (VI), Voice (VO), Network Control (NC), Traffic Stream Establishment/Release Procedure, Establishment of a TS, Active phase of a TS, Teardown of a TS, Contents of the QoS Control Field, Traffic Identifier, End Of Service Period, Ack Policy, Transmission opportunities, Queues and buffers

⇒ Block Ack
Overview Ack Policies, Normal Ack, No Ack, No explicit Ack, Block Ack, Immediate Block Ack Procedure, Setup Block Ack, Transmission of data frames, Block Ack Request – Block Ack exchange, Teardown Block Ack, Delayed Block Ack Procedure , Setup of Delayed Block Ack's, Block Ack Request – Block Ack exchange, Switch back to normal Ack procedure in the Block Ack period, Teardown Block Ack, Block Ack Request Frame, Block Ack Frame

⇒ EDCA & HCCA
Changes Introduced by EDCA, New parameters for EDCA, QoS for 4 access classes, Multiple MSDU's in a frame sequence, Changes Introduced by HCCA, New parameters for HCCA, TXOP's by means of polling, QoS for 4 access classes, Multiple MSDU's in a frame sequence, Coexistence of DCF, PCF, and HCF, Establishment of DCA, Establishment of legacy CF access, Establishment of EDCA, Establishment of HCCA, Controlled access phases, QoS Interframe Space Timing Relations, SIFS, Slot, PIFS, DIFS, EIFS, AIFS, Default Timing for EDCA AC's, CW timing, AIFS timing, TXOP limit, Practical Exercise Timing of the CP, EDCA Procedure, Accessing the WM, Data transfer using the Block Ack policy, Data transfer using the normal Ack policy, HCCA Procedures – Example 1, Requesting TXOP's, Polling a TXOP, Indicating queue size, Reacting on a missing response, Terminating a TXOP ahead of time, HCCA Procedures – Example 2, RTS – CTS procedure in HCF, Termination of the HCCA Procedure

⇒ Direct Link Setup/Teardown Procedure
Setup of a direct link, Active phase of a direct link, Teardown of a direct link

- **Lessons Learned / Conclusions:**

Security

- **Security Challenges**

Unauthorized use, Forgery attacks, Man in the middle attacks (eavesdropping), Replay attack, Data truncation, concatenating, and splicing , Iterative guessing against the key, Redirection by modifying

the MPDU DA or RA field, Impersonation attacks by modifying the MPDU SA or TA field, Denial of service attack

- **Overview Security**
  Keys, Ciphering, Deciphering, Authentication, Integrity protection
- **Security Technologies in and over IEEE 802.11**

  ⇒ Overview
  Wired Equivalent Privacy (WEP), Robust Security Network (RSN), 802.1X, Extensible Authentication Protocol (EAP), Virtual Private Network

  ⇒ 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, Key Hierarchy – How to Create the TK's, Authentication credentials outside the WLAN, Master Keys, GTK and PTK, TK, Types of Security Association, Pairwise Master Key Security Association (PMKSA), Pairwise Transient Key Security Association (PTKSA), Group Temporal Key Security Association (GTKSA), STA to STA Link Master Key Security Association (SMKSA), STAkeySA , RSNA Encryption and Integrity Protection Protocols, Overview, Temporal Key Integrity Protocol (TKIP), CTR with CBC-MAC Protocol (CCMP), The TKIP Encryption and Integrity Protection Procedure, Key ID, Temporal Key Integrity Protocol Sequence Counter, (Extended) Initialization Vector, Key Mixing, Michael, MIC and MIC key, Integrity check value, The CCMP Encryption and Integrity Protection Procedure, Packet Number and key ID, Additional Authentication Data, Nonce, CCMP Header, MIC, CCM encryption

  ⇒ Advanced Authentication
  Authentication and Key Generation with an Authentication Server, Essentials on the IEEE 802.1X Protocol, Uncontrolled port, Controlled port, EAP Derivatives, LEAP, EAP-TLS, EAP-PSK, PEAP, EAP-FAST, EAP-SIM, EAP-AKA, EAPOL

  ⇒ Secure Session Overview
  Phases of a Session, Open System authentication, EAP authentication via 802.1X , 802.11i key exchange, Active session, Stop session, 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: Generation of IEEE 802.11 Keys, 1st message, 2nd message, 3rd message, 4.3.5.4.4 4th message, Session Phase 4 & 5: Active Session & Disassociation
- **EAP Details**

  ⇒ EAP Frames
  EAP Request and EAP Response Frames, EAP Success and EAP Failure Frames

  ⇒ EAP-AKA
  EAP-AKA Protocol Structure, EAP-AKA Procedure, EAP-AKA Procedure – Fast Re-Authentication

  ⇒ EAP-TLS
  EAP-TLS Protocol Structure, EAP-TLS Procedure, EAP-TLS Procedure – Fast Reconnect, EAP-TLS Procedure – Privacy

  ⇒ EAP-TTLS
  EAP-TTLSv0 Protocol Structure, EAP-TTLSv0 Procedure, EAP-TTLSv1 Protocol Structure, EAP-TTLSv0 vs. EAP-TTLSv1, Utilization of TLS/IA (inner application), Combination of authentication and other client-server exchanges in TLS, Mixing of session keys from authentication with TLS master secret (inner secret), Inner secret used to create MSK, Verification of previous phase by next phase, Protected final exchange

  ⇒ EAP-FAST
  EAP-FAST Protocol Structure, EAP-FAST Procedure

⇒ PEAP
PEAPv1 Protocol Structure, PEAPv1 Procedure, PEAPv0 Protocol Structure, PEAPv0 vs. PEAPv1, EAP encapsulation, Version field, EAP extensions method, PEAPv2 Protocol Structure, PEAPv1 vs. PEAPv2, Encapsulation of TLV's, Key derivation similar to EAP-FAST, Cryptographic binding, Protected termination

⇒ Summary
Security Features of EAP Methods, Vulnerabilities of EAP Methods, Finally: How Keying Material is used

- **Accessing External Resources using the VPN Approach**
- **Security Association in the Roaming Case**
  (Re)association followed by 802.1X procedure, Reuse of Keys in an ESS , In an ESS
- **Lessons Learned / Conclusions:**

Planning a Wireless LAN Deployment

- **Planning a WLAN**
- **Lessons Learned / Conclusions:**

Future / Recent Developments

- **New and Coming IEEE 802.11 Standards**
- **IEEE 802.11 and Bluetooth coexistence**
- **WLAN's Accessing a Mobile Radio Network Core**
  ⇒ I-WLAN Direct IP-Access
  ⇒ Details of I-WLAN 3GPP IP-Access
  ⇒ Details of GAN/UMAN-Access
  ⇒ MIP in Wireless Standards
- **IEEE 802.11n**
  ⇒ Practical Exercise: Scaling of OFDM / OFDMA-Systems
  ⇒ Key Changes in IEEE 802.11n
  ⇒ HT PPDU's
  ⇒ Smart Antenna Technology in IEEE 802.11
  Categorization of Smart Antenna Technologies, The Basics: Signal Fading Physics between TX and RX, Multipath Diversity, The Transmission Diversity Problem, The Wrong Way to Implement TX Diversity, Beamforming, Beamforming in IEEE 802.11, Practical Exercise: Draw the Antenna Diagram of Beamforming, CSD, STBC, MIMO, Multiple Input Multiple Output (MIMO), MIMO General Operation, MIMO Details, Motivation of MIMO combined with Beamforming, Multiple Rank Beamforming Procedure
  ⇒ How to Calculate the Data Rate of HT
  ⇒ Signal Processing Chain for the HT-SIGNAL Field
  ⇒ Signal Processing Chain for the HT-SERVICE and HT-data Fields

The optional LDPC encoder

- **Lessons Learned / Conclusions:**

Voice over WiFi

- **How to deliver VoIP Services**
- **QoS Issues**
- **Other Initial Obstacles for Vo802.11**
- **Deployment Examples**
- **Operation of Vo802.11 with a Softswitch**
- **Lessons Learned / Conclusions:**

The WiFi Alliance

- **The WiFi Forum and IEEE - Overview and Responsibilities**
- **WiFi Certification Programs**

  ⇒ Features of WPA and WPA2

  ⇒ Features of WMM
  WMM Compared to IEEE 802.11e , EDCA only, WMM capabilities are independent of IEEE 802.11e capabilities, Ack policies, QoS frames, 4 traffic queues only

  ⇒ WMM PS Compared to Legacy PS
  Mode 1: Unscheduled Automatic Power Save Delivery (U-APSD), Mode 2: Legacy as described in IEEE 802.11, Transmission of TIM, Negotiation of capabilities
- **Lessons Learned / Conclusions:**