v 2.110

IEEE 802.11n - Design Details & Protocol Analysis

Course Duration:

- 2 days

Course Description:

- This course describes in detail HT-related enhancements which the IEEE specified in the 802.11n extension of the WLAN / WiFi standard series.
- Starting out with a primer on "before n", the course initially focuses on 802.11 operation with respect to channel access and resource sharing. Namely the different channel access functions DCF, PCF, EDCA and HCCA are repeated and their differences and specifics are pointed out.
- During this part, the course also repeats the most important other characteristics of the OFDM-PHY and the MAC-layer. This includes a detailed consideration as to how QoS is enabled in 802.11.
- The following chapter starts with an overview of the different groups of features which are added by the "n"-extension of the standard. After this initial overview, this chapter already discusses in detail enhancements like "Short GI" (Guard Interval), more subcarriers, enhanced channel coding, new power saving modes (namely SM Power Save and PSMP) and the new RIFS (Reduced InterFrame Space).
- After this, the course focuses on the description and discussion of smart antenna techniques, namely MIMO, beamforming and STBC. The students will learn *without needing any mathematical formulas*, how these techniques work and how they are applied in 802.11n.
- Another section deals with the discussion of the "HT-Capabilities" information element and its contents. Target is to enable the students to more efficiently evaluate related logfiles during their daily work.
- The chapter concludes with a review of all "n"-related features but with a new focus: .Which features are mandatory or optional according to the IEEE and to the WiFi-alliance. This part is particularly interesting for those who require information regarding device certification.
- The next chapter is dedicated to all PHY-related aspects of 802.11n that have not been discussed yet. This includes features like 40 MHz-operation, PCO (Phased Coexistence Operation), PLCP-PDU types for greenfield and mixed operation, beamforming feedback and antenna selection.
- The MAC-related chapter starts with pointing out the differences in the MAC-frame structure with respect to new information elements and new Action-frame types. Focus is however on the presentation and detailed description of the new aggregation features of 802.11n. Both options, A-MPDU and A-MSDU aggregation are described in all detail. This includes a comparison of the two methods with respect to performance.
- This chapter continues with the detailed discussion of the BlockAck-feature or rather the improvements that have been introduced with 802.11n. This part includes the evaluation of a real-life BlockAck-session through the students.

- The MAC-chapter ends with a detailed description as to how scheduled PSMP operates.
- The final chapter of this course is dedicated to advanced security mechanisms of WiFi, namely EAP-based mechanisms, Fast Reconnect and Pre-Authentication. Please note that this chapter is no longer part of the 2-days course but is kept in the book as bonus material!
- This chapter starts with a primer on legacy security mechanisms in WiFi which relates to WEP, WPA and WPA2 and points out the differences among those.
- After this, we discuss two EAP-procedures (EAP-TLS and EAP-AKA) in full detail and we point out, how the 802.11-key material is finally generated after applying either of these two EAP-procedures. This section includes the practical evaluation of an EAP-logfile through the students.

As in all INACON courses we integrated several interactive exercises for a perfect learning experience. Many of these exercises are based on already prepared WIRESHARK logfiles which are provided to the students by the trainer. For those who don't have a PC with them or who do not use WIRESHARK, the logfiles are made available as printouts.

Prerequisites:

- The student must possess a thorough understanding in wireless and/or cellular communication technology before coming to this course. This knowledge should stem from multiple years of design or test experience with these technologies.
- At the least, we recommend our webinars or web based training courses WiFi to be taken beforehand.

Course Target:

- The student is enabled to develop, test and integrate 802.11n-equipment and to operate related networks.

Who should attend this Course:

- Test engineers who need to understand the 802.11n-features and their implications in detail.
- Designers of 802.11n-equipment who require a deep inside view of the various enhancements.

Some of your Questions that will be answered:

- How does WiFi support the distinction of different QoS-requirements?
- What are the various 802.11n-related enhancements?
- How do MIMO, STBC, antenna selection and beamforming work?
- How does an access point communicate which of the so called HT-features it supports?
- How does the OFDM-specific PPDU-format change with 802.11n?
- What are the specifics of channel bonding?
- What is greenfield operation?
- When is 40 MHz operation possible and when not?
- Which changes and modifications does 802.11n require in the structure and format of the different MAC-frames?
- How exactly do A-MPDU and A-MPDU aggregation work and how do they differ from each other?
- What changes have been added to the BlockAck-procedure with 802.11n and which improvements do those changes offer?
- How do security procedures operate in 802.11 in general?
- Which additional gain is provided by EAP?
- How do different EAP-procedures like EAP-TLS or EAP-AKA work?
- What is pre-authentication and how does it work?

Table of Content:

Reviewing 802.11 Wireless LAN

Overview of 802.11n and its Enhancements

- **Introduction to 802.11n-Enhancements**
  - ⇒ The Big Picture
  - ⇒ 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), Principles and Performance, 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), Summarizing the Defined IFS's, AIFS, DIFS, EIFS, RIFS, SIFS, Advantages of RIFS
- **Generic Assessment of Smart Antenna Techniques**
  - ⇒ Terminology & Introduction
    SISO, SIMO, MISO, MIMO, Physical Basics of the Multipath Dimension, Signal Fading and Alteration between Tx and Rx, Scattering, Refraction, Reflection, Diffraction, Consequences for the different Signal Paths, Macro-Diversity vs Micro-Diversity
  - ⇒ MIMO
    Specifics of MIMO, How MIMO basically works ..., Increased Performance
  - ⇒ STBC (Space Time Block Coding)
  - ⇒ Transmit Beamforming
- **Wrapping Things Up**
  - ⇒ Beacon-Frame with HT-Information Elements
  - ⇒ Practical Exercise: Evaluate a Beacon Frame with HT-Information Elements
  - ⇒ Feature Support according to the WiFi-Alliance and IEEE
    The Certification Matrix of the WiFi-Alliance

Detailed Analysis of the 802.11n PHY

- **HT-PPDU Formats**
  Legacy Format
  - ⇒ Mixed Format
    Non-HT / Legacy Preamble, L-SIG, HT-SIG, HT-STF, HT-LTF, DLTF, ELTF, SERVICE-Field
  - ⇒ Greenfield Format
    HT-GF-STF, HT-LTF1, HT-SIG, HT-STF, HT-LTF, DLTF, ELTF, SERVICE-Field
- **Operation with 40 MHz Bandwidth**
  - ⇒ Overview
    Number of Subcarriers and Pilot Allocation

⇒ Phased Coexistence Operation (PCO)

- **Transmit Beamforming ...**

⇒ ... with Implicit Feedback
... with explicit Feedback

- **Antenna Selection**

Detailed Analysis of the 802.11n MAC

- **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

⇒ Practical Exercise: Analyze a Real-Life BlockAck Session

- **Power Save Multi Poll (PSMP)**

⇒ Operation of PSMP
Format and Content of the PSMP-Frame

Advanced Security through EAP

- **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 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, Variants of EAP, LEAP, EAP-TLS, EAP-PSK, PEAP, EAP-FAST, EAP-SIM, EAP-AKA, (EAPOL)

⇒ Secure Session Overview
Different Phases, 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: 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

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

- **Analysis of EAP-TLS**
  - ⇒ EAP-TLS Protocol Structure
  - ⇒ EAP-TLS Procedure
    Detailed Description
  - ⇒ Practical Exercise: Analysis of Real-Life EAP-TLS Logfile
  - ⇒ EAP-TLS Procedure – Fast Reconnect
    Detailed Description
- **Analysis of EAP-AKA**
  - ⇒ EAP-AKA Protocol Structure
  - ⇒ EAP-AKA Procedure
    Initial Conditions, Applicability of this Procedure, Detailed Description
  - ⇒ EAP-AKA Procedure – Fast Re-Authentication
- **Pre-Authentication**
  Initial Conditions, Operation