IEEE 802.11n - Design Details & Protocol Analysis

INACON GmbH
Kriegsstrasse 154
76133 Karlsruhe
Germany
www.inacon.com
e-mail: inacon@inacon.de

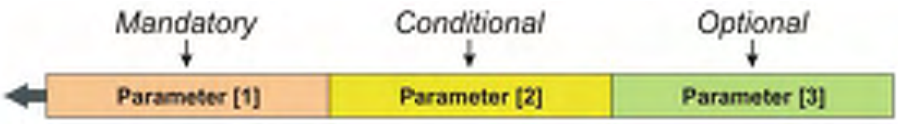
Cover design by Stefan Kohler

Kriegsstrasse 154
76133 Karlsruhe

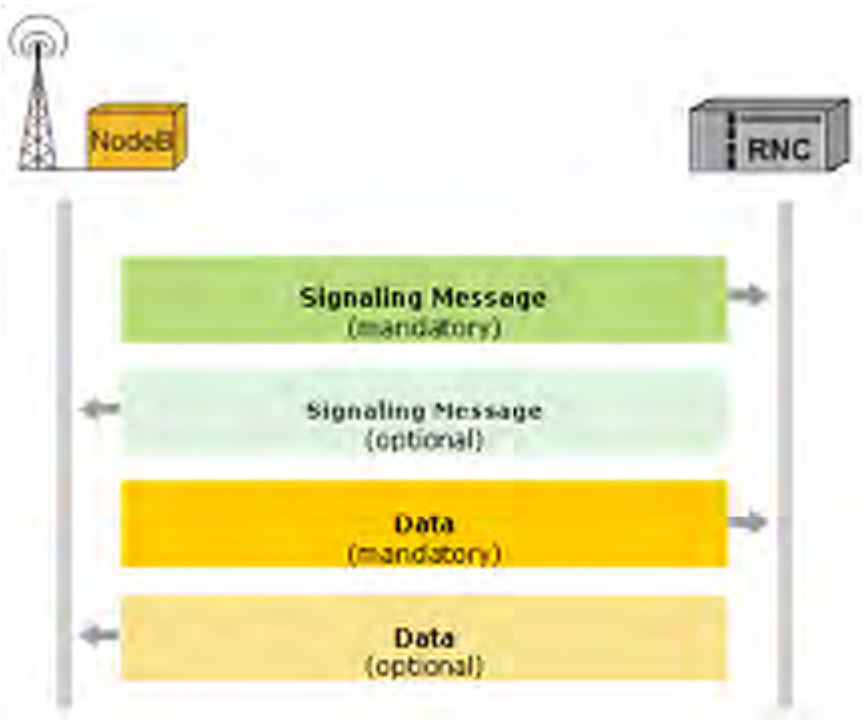
Legend:

All INACON publications use the same color codes to distinguish mandatory from optional or conditional parts in frame formats or optional from mandatory data blocks or signaling messages in scenarios. The different color codes are explained underneath:

- **Color Codes in Frame Formats:**



- **Color Codes in Scenarios:**



Foreword of the Publisher:

Dear Reader:

Note that this book is primarily a training document because the primary business of INACON GmbH is the training and consulting market for mobile communications. As such, we are proud to providing high-end training courses to many clients worldwide, among them operators like Chungwa Telecom in Taiwan, INMARSAT, SWISSCOM or T-MOBILE and equipment suppliers like ALCATEL-LUCENT, ERICSSON and SONY-ERICSSON, MOTOROLA, NOKIA-SIEMENS and RIM.

INACON GmbH is not one of the old-fashioned publishers. With respect to time-to-market, form-factor, homogeneous quality over all books and most importantly with respect to after-sales support, INACON GmbH is moving into a new direction. Therefore, INACON GmbH does not leave you alone with your issues and this book but we offer you to contact the author directly through e-mail (inacon@inacon.de), if you have any questions. All our authors are employees of INACON GmbH and all of them are proven experts in their area with usually many years of practical experience.

The most important assets and features of the book in front of you are:

- **Extreme degree of detailed information about a certain technology.**
- **Extensive and detailed index to allow instant access to information about virtually every parameter, timer and detail of this technology.**
- **Incorporation of several practical exercises.**
- **If applicable, incorporation of examples from our practical field experiences and real life recordings.**
- **References to the respective standards and recommendations on virtually every page.**

Finally, we again like to congratulate you to the purchase of this book and we like to wish you success in using it during your daily work.

Sincerely,

Gunnar Heine / President & CEO of INACON GmbH

Table of Content

Reviewing 802.11 Wireless LAN.....1

1.1 The IEEE 802.11 Alphabet.....2
1.1.1 IEEE 802.11-1999.....2
1.1.2 IEEE 802.11b.....2
1.1.3 IEEE 802.11g.....2
1.1.4 IEEE 802.11a.....2
1.1.5 IEEE 802.11e.....2
1.1.6 IEEE 802.11i.....3
1.1.7 IEEE 802.11n.....3
1.2. The Physical Resource.....4
1.2.1 The ISM Band in 2.4 GHz and 5 GHz.....4
1.2.2 Channel Numbers and Allocation / 2.4 GHz.....6
1.2.3 Channel Numbers and Allocation / 5 GHz.....8
1.3 Network Architecture.....10
1.3.1 Infrastructure Mode.....10
1.3.2 Ad-hoc Mode.....11
1.4 Protocol Stack of IEEE 802.11 in Context.....12
1.4.1 PDU-Types in the Protocol Stack.....13
1.4.1.1 MSDU.....13
1.4.1.2 MPDU.....13
1.4.1.3 PPDU.....13
1.4.2 Example of an IEEE 802.11 MPDU.....14
1.5 Operation of IEEE 802.11.....16
1.5.1 CSMA/CA - Resource Sharing and Network Access.....16
1.5.1.1 Principle Operation.....16
1.5.1.2 Format and Content of the PLCP-PDU.....18
1.5.1.3 Physical vs. Virtual Carrier Sensing.....20
1.5.1.3.1 Physical Carrier Sensing.....21
1.5.1.3.2 Virtual Carrier Sensing.....21
1.5.1.3.3 Network Allocation Vector.....21
1.5.2 The Different MAC-Access Coordination Functions.....22
1.5.2.1 Overview.....22
1.5.2.2 Distributed Coordination Function / Example Operation.....24
1.5.2.2.1 DCF with RTS/CTS-Enhancement.....38
1.5.2.3 Point Coordination Function (PCF).....40
1.5.2.3.1 Indication of an AP whether PCF is supported.....42
1.5.2.3.2 Indication whether the AP supports 802.11e QoS.....43
1.5.2.4 Enhanced Distributed Channel Access (EDCA).....44
1.5.2.4.1 Parameterization of QoS-Settings.....46
1.5.2.5 HCF Controlled Channel Access (HCCA).....48

1.5.2.5.1 Example of a QoS-Data+CF-Ack+CF-Poll-Frame.....50
1.6 OFDM in IEEE 802.11.....52
1.6.1 Introduction.....52
1.6.2 Normal OFDM Symbol.....53
1.6.3 Short OFDM-Symbol.....54
1.6.3.1 Generation.....54
1.6.4 Long OFDM-Symbol.....56
1.6.4.1 Generation.....56
1.6.4.2 Distinction in case of different Channel Bandwidth (5, 10 and 20 MHz).....57
1.6.5 Format of the PPDU with OFDM-PHY.....58
1.6.5.1 PLCP Preamble.....58
1.6.5.2 L-SIG (SIGNAL-Field).....58
1.6.5.3 SERVICE-Field.....60
1.6.5.4 PSDU.....60
1.6.5.5 Tail Bits / Padding.....60
1.7 Association Process to an Access Point.....62
1.7.1 Passive Scanning.....63
1.7.2 Active Scanning.....63
1.7.3 Beacon Frame.....63
1.7.4 Exchange of Association Request / Response Frames.....63

Overview of 802.11n and its Enhancements.....65

2.1 Introduction to 802.11n-Enhancements.....66
2.1.1 The Big Picture.....66
2.1.2 Smart Antenna related Enhancements.....68
2.1.3 Packet Aggregation related Enhancements.....70
2.1.4 Channel Bonding related Enhancements.....72
2.1.5 Other Enhancements 74
2.1.5.1 More Data Subcarriers / Smaller Guardband.....74
2.1.5.1.1 Performance Gain.....75
2.1.5.2 Short Guard Interval (GI).....76
2.1.5.2.1 Consequences of using a short GI.....77
2.1.5.2.2 Logfile Extract: Indication of Short-GI in HT-SIG.....78
2.1.5.3 FEC Changes.....80
2.1.5.3.1 New Code Rate 5/6.....80
2.1.5.3.2 Low Density Parity Check Coding (LDPC).....82
2.1.5.3.2.1 Principles and Performance.....82
2.1.5.4 Power Saving Enhancements.....84
2.1.5.4.1 Legacy Modes: APSD and TIM-based Power Save Mode.....84
2.1.5.4.2 SM Power Save.....85
2.1.5.4.3 PSMP (Power Save Multi Poll).....85
2.1.5.5 Reduced Inter Frame Space (RIFS).....86
2.1.5.5.1 Summarizing the Defined IFS's.....86
2.1.5.6.1.1 AIFS.....86
2.1.5.6.1.2 DIFS.....86

2.1.5.5.1.3 EIFS....88
2.1.5.5.1.4 RIFS....88
2.1.5.5.1.5 SIFS....88
2.1.5.5.2 Advantages of RIFS....88
2.2 Generic Assessment of Smart Antenna Techniques....90
2.2.1 Terminology & Introduction....90
2.2.1.1 SISO....91
2.2.1.2 SIMO....91
2.2.1.3 MISO....91
2.2.1.4 MIMO....91
2.2.1.1 Physical Basics of the Multipath Dimension....92
2.2.1.1.1 Signal Fading and Alteration between Tx and Rx....92
2.2.1.1.1.1 Scattering....92
2.2.1.1.1.2 Refraction....93
2.2.1.1.1.3 Reflection....93
2.2.1.1.1.4 Diffraction....93
2.2.1.2 Consequences for the different Signal Paths....94
2.2.1.2.1 Macro-Diversity vs Micro-Diversity....95
2.2.2 MIMO....96
2.2.2.1 Specifics of MIMO....96
2.2.2.2 How MIMO basically works....98
2.2.2.3 Increased Performance....100
2.2.3 STBC (Space Time Block Coding)....102
2.2.4 Transmit Beamforming....104
2.3 Wrapping Things Up....106
2.3.1 Beacon-Frame with HT-Information Elements....106
2.3.2 Practical Exercise: Evaluate a Beacon Frame with HT-Information Elements....110
2.3.3 Feature Support according to the WiFi-Alliance and IEEE....112
2.3.3.2 The Certification Matrix of the WiFi-Alliance....114
Detailed Analysis of the 802.11n PHY....117
3.1 HT-PPDU Formats....118
3.1.1 Legacy Format....118
3.1.2 Mixed Format....120
3.1.2.1 Non-HT / Legacy Preamble....120
3.1.2.2 L-SIG....120
3.1.2.3 HT-SIG....122
3.1.2.4 HT-STF....122
3.1.2.5 HT-LTF....122
3.1.2.5.1 DLTF....122
3.1.2.5.2 ELTF....122
3.1.2.6 SERVICE-Field....122
3.1.3 Greenfield Format....124
3.1.3.1 HT-GF-STF....124
3.1.3.2 HT-LTF1....124
3.1.3.3 HT-SIG....126

3.1.2.4 HT-STF....126
3.1.2.5 HT-LTF....126
3.1.3.5.1 DLTF....126
3.1.3.5.2 ELTF....126
3.1.3.6 SERVICE-Field....126
3.2 Operation with 40 MHz Bandwidth....128
3.2.1 Overview....128
3.2.2 Number of Subcarriers and Pilot Allocation....128
3.2.3 Phased Coexistence Operation (PCO)....130
3.3 Transmit Beamforming....132
3.3.1 ... with Implicit Feedback....132
3.3.2 ... with explicit Feedback....133
3.4 Antenna Selection....134

Detailed Analysis of the 802.11n MAC....137

4.1 Reviewing MAC-Frame Types and IE's....138
4.1.1 Generic MAC Frame (Data Frame)....138
4.1.1.1 Frame Control field....138
4.1.1.2 Duration ID field....138
4.1.1.3 Address fields....139
4.1.1.4 Sequence Control field....139
4.1.1.5 QoS Control field....139
4.1.1.6 Frame Body....139
4.1.1.7 FCS field....139
4.1.1.8 Details of the Frame Control Field....140
4.1.1.8.1 Protocol Version field....140
4.1.1.8.2 Type and Subtype fields....140
4.1.1.8.3 To and From DS fields....140
4.1.1.8.4 More Frag field....141
4.1.1.8.5 Retry field....141
4.1.1.8.6 Power Mgt field....141
4.1.1.8.7 More Data field....141
4.1.1.8.8 WEP field....141
4.1.1.8.9 Order Field....141
4.1.2 Control Frame Subtypes....142
4.1.2.1 BlockAckReq and BlockAck....143
4.1.2.2 PS-Poll....143
4.1.2.3 RTS and CTS....143
4.1.2.4 Ack....143
4.1.2.5 CF-End and CF-End+CF-Ack....143
4.1.3 Management Frame Subtypes....144
4.1.3.1 Association request and Association response....145
4.1.3.2 Reassociation request and Reassociation response....145
4.1.3.3 Disassociation....145
4.1.3.4 Probe request and Probe response....146
4.1.3.5 Beacon....146
4.1.3.6 Announcement Traffic Information Message....146

4.1.3.7 Authentication and Deauthentication....146
4.1.3.8 Action....146
4.1.3.9 Action No Ack....146
4.1.4 Data Frame Subtypes....148
4.1.4.1 Data frames....149
4.1.4.2 Null frames....149
4.1.4.3 CF-Ack frames....149
4.1.4.4 CF-Poll frames....149
4.1.4.5 QoS frames....149
4.1.4.6 Usage of the Address Fields in Data Frames....150
4.1.4.6.1 Destination Address field....150
4.1.4.6.2 Source Address field....150
4.1.4.6.3 Receive Address field....150
4.1.4.6.4 Transmitter Address field....150
4.1.4.6.5 BSSID field....151
4.1.5 Action Frames....152
4.1.5.1 Spectrum management Action frames....152
4.1.5.2 QoS Action frames....152
4.1.5.3 DLS Action frames....153
4.1.5.4 Block Ack Action frames....153
4.1.5.5 HT Action frames....153
4.2 Aggregation through A-MSDU....154
4.2.1 Practical Exercise: Evaluate a PPDU with A-MSDU inside....154
4.2.2 Detailed Operation and Constraints....156
4.2.2.1 From LLC-Frame to A-MSDU - Mapping Rules....156
4.2.2.2 Limitation of Frame Sizes (A-MSDU)....157
4.3. Aggregation through A-MPDU....158
4.3.1 Example of an A-MPDU....158
4.3.2 Detailed Operation and Constraints....160
4.3.2.1 From LLC-Frame to A-MPDU - Mapping Rules....160
4.3.2.2 Limitation of Frame Sizes (A-MPDU)....161
4.3.3 Combination of A-MSDU and A-MPDU Aggregation....162
4.3.4 Practical Exercise: A-MSDU vs A-MPDU Aggregation....164
4.4 BlockAck-Procedures....166
4.4.1 Reviewing Acknowledgement Policies....166
4.4.1.1 Normal Ack....167
4.4.1.2 No Ack....167
4.4.1.3 No explicit Ack....167
4.4.1.4 Block Ack....167
4.4.2 Option 1: Immediate BlockAck Procedure....168
4.4.2.1 Setup BlockAck....170
4.4.2.2 Transmission of data frames....170
4.4.2.3 Block Ack Request – Block Ack exchange....170
4.4.2.4 Termination of Block Ack....170
4.4.3 Option 2: Delayed Block Ack Procedure....172
4.4.3.1 Setup of Delayed BlockAck's....173
4.4.3.2 BlockAck Request – BlockAck exchange....173
4.4.3.3 Switch back to normal Ack procedure in the BlockAck period....173

4.4.3.4 Termination of Delayed BlockAck....173
4.4.4 Important Changes with 802.11n....174
4.4.4.1 New Format of the BlockAck Request Frame....176
4.4.4.1.1 Redefined BAR-Control Field....176
4.4.4.1.2 BA-Info....176
4.4.4.2 New Format of the BlockAck Frame....178
4.4.4.2.1 Redefined BA-Control Field....178
4.4.4.2.2 BA-Info....179
4.4.4.2.3 The Compressed Bitmap and its Interpretation....180
4.4.5 Practical Exercise: Analyze a Real-Life BlockAck Session....182
4.5 Power Save Multi Poll (PSMP)....186
4.5.1 Operation of PSMP....186
4.5.2 Format and Content of the PSMP-Frame....186

Advanced Security through EAP....189

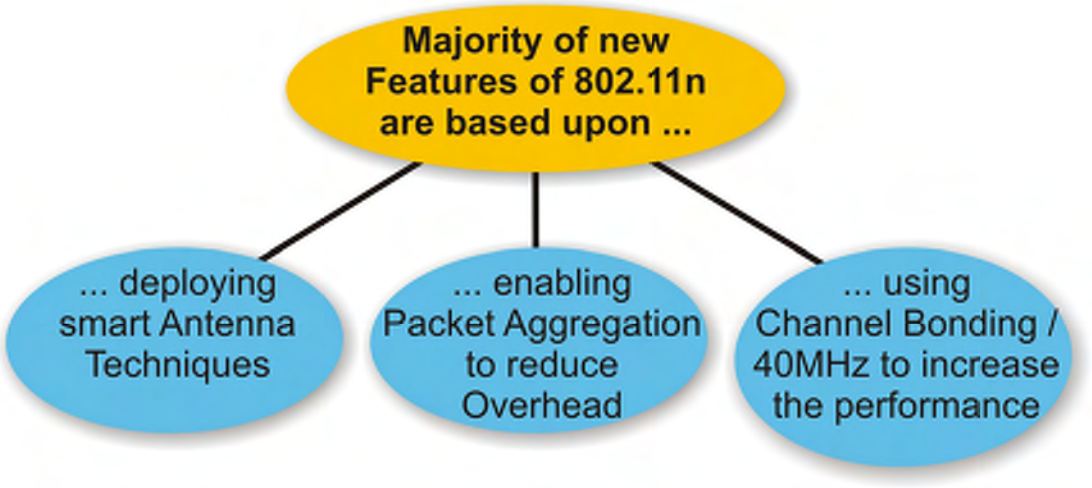
5.1 Security Challenges....190
5.1.1 Unauthorized use....191
5.1.2 Forgery attacks....191
5.1.3 Man in the middle attacks (eavesdropping)....191
5.1.4 Replay attack....191
5.1.6 Data truncation, concatenating, and splicing 191
5.1.7 Iterative guessing against the key....191
5.1.8 Redirection by modifying the MPDU DA or RA field....191
5.1.9 Impersonation attacks by modifying the MPDU SA or TA field....191
5.1.10 Denial of service attack....191
5.2 Overview Security....192
5.2.1 Keys....193
5.2.2 Ciphering....193
5.2.3 Deciphering....193
5.2.4 Authentication....193
5.2.5 Integrity protection....193
5.3 Security Technologies for IEEE 802.11....194
5.3.1 Overview....194
5.3.1.1 Wired Equivalent Privacy (WEP)....195
5.3.1.2 Robust Security Network (RSN)....195
5.3.1.3 802.1X....195
5.3.1.4 Extensible Authentication Protocol (EAP)....195
5.3.1.5 Virtual Private Network....195
5.3.2 Pre - RSNA Procedures....196
5.3.2.1 Open System Authentication....196
5.3.2.2 Shared Key Authentication....198
5.3.2.2.1 Authentication challenge....199
5.3.2.3 The “Wired Equivalent Privacy” Procedure....200

5.3.3 RSNA Procedures.....202
5.3.3.1 RSNA Policy Selection.....202
5.3.3.1.1 Probe Response frames and Beacon frames.....203
5.3.3.1.2 Open System authentication.....203
5.3.3.1.3 Association.....203
5.3.3.2 Key Hierarchy – How to Create the TK's.....204
5.3.3.2.1 Authentication credentials outside the WLAN.....204
5.3.3.2.2 Master Keys (GMK, PMK).....205
5.3.3.2.3 GTK and PTK.....205
5.3.3.2.4 TK.....205
5.3.3.3 Types of Security Associations.....206
5.3.3.3.1 Pairwise Master Key Security Association (PMKSA).....207
5.3.3.3.2 Pairwise Transient Key Security Association (PTKSA).....207
5.3.3.3.3 Group Temporal Key Security Association (GTKSA).....207
5.3.3.3.4 STA to STA Link Master Key Security Association (SMKSA) 207
5.3.3.3.5 STAkeySA 207
5.3.3.4 RSNA Encryption and Integrity Protection Protocols.....208
5.3.3.4.1 Overview.....208
5.3.3.4.1.1 Temporal Key Integrity Protocol (TKIP).....209
5.3.3.4.1.2 CTR with CBC-MAC Protocol (CCMP).....209
5.3.3.4.2 The TKIP Encryption and Integrity Protection Procedure…210
5.3.3.4.2.1 Key ID.....210
5.3.3.4.2.2 Temporal Key Integrity Protocol Sequence Counter..210
5.3.3.4.2.3 (Extended) Initialization Vector.....211
5.3.3.4.2.4 Key Mixing.....211
5.3.3.4.2.5 Michael.....211
5.3.3.4.2.6 MIC and MIC key.....211
5.3.3.4.2.7 Integrity check value.....211
5.3.3.4.3 The CCMP Encryption and Integrity Protection Procedure 212
5.3.3.4.3.1 Packet Number and key ID.....213
5.3.3.4.3.2 Additional Authentication Data.....213
5.3.3.4.3.3 Nonce.....213
5.3.3.4.3.4 CCMP Header.....213
5.3.3.4.3.5 MIC.....213
5.3.3.4.3.6 CCM encryption.....213
5.3.4 Advanced Authentication.....214
5.3.4.1 Network Overview: Supplicant, Authenticator, Authentication Server.....214
5.3.4.2 Redirection.....216
5.3.4.2.1 Uncontrolled port.....217
5.3.4.2.2 Controlled port.....217
5.3.4.3 Variants of EAP.....218
5.3.4.3.1 LEAP.....220
5.3.4.3.2 EAP-TLS.....220
5.3.4.3.3 EAP-PSK.....220
5.3.4.3.4 PEAP.....220
5.3.4.3.5 EAP-FAST.....220
5.3.4.3.6 EAP-SIM.....220
5.3.4.3.7 EAP-AKA.....220
5.3.4.3.8 (EAPOL).....220
5.3.5 Secure Session Overview.....222
5.3.5.1 Different Phases.....222

5.3.5.1.1 Open System authentication....223
5.3.5.1.2 EAP authentication via 802.1X....223
5.3.5.1.3 802.11i key exchange....223
5.3.5.1.4 Active session....223
5.3.5.1.5 Stop session....223
5.3.5.2 Session Phase 1: Probing & Association....224
5.3.5.2.1 Beacon frames....225
5.3.5.2.2 Exchange of Probe Request and Probe Response Frames....225
5.3.5.2.3 Open System authentication....225
5.3.5.2.4 Association....225
5.3.5.3 Session Phase 2: EAP Authentication....226
5.3.5.3.1 EAPOL start....226
5.3.5.3.2 EAPOL identity exchange....227
5.3.5.3.3 EAPOL challenge....227
5.3.5.3.4 EAPOL success....227
5.3.5.4 Session Phase 3: EAPOL 4-Way Handshake....228
5.3.5.4.1 1st EAPOL message....228
5.3.5.4.2 The 2nd EAPOL message....229
5.3.5.4.3 The 3rd EAPOL message....229
5.3.5.4.4 The 4th EAPOL message....229
5.3.5.5 Session Phase 4 & 5: Active Session & Disassociation....230
5.3.6 EAP Frame Formats....232
5.3.6.1 EAP Request and EAP Response Frames....232
5.3.6.2 EAP Success and EAP Failure Frames....234
5.4 Analysis of EAP-TLS....236
5.4.1 EAP-TLS Protocol Structure....236
5.4.2 EAP-TLS Procedure....238
5.4.2.1 Detailed Description....238
5.4.3 Practical Exercise: Analysis of Real-Life EAP-TLS Logfile....246
5.4.4 EAP-TLS Procedure – Fast Reconnect....248
5.4.4.1 Detailed Description....248
5.5 Analysis of EAP-AKA....252
5.5.1 EAP-AKA Protocol Structure....252
5.5.2 EAP-AKA Procedure....254
5.5.2.1 Initial Conditions....254
5.5.2.2 Applicability of this Procedure....256
5.5.2.3 Detailed Description....256
5.5.3 EAP-AKA Procedure – Fast Re-Authentication....264

2.1 Introduction to 802.11n-Enhancements

2.1.1 The Big Picture

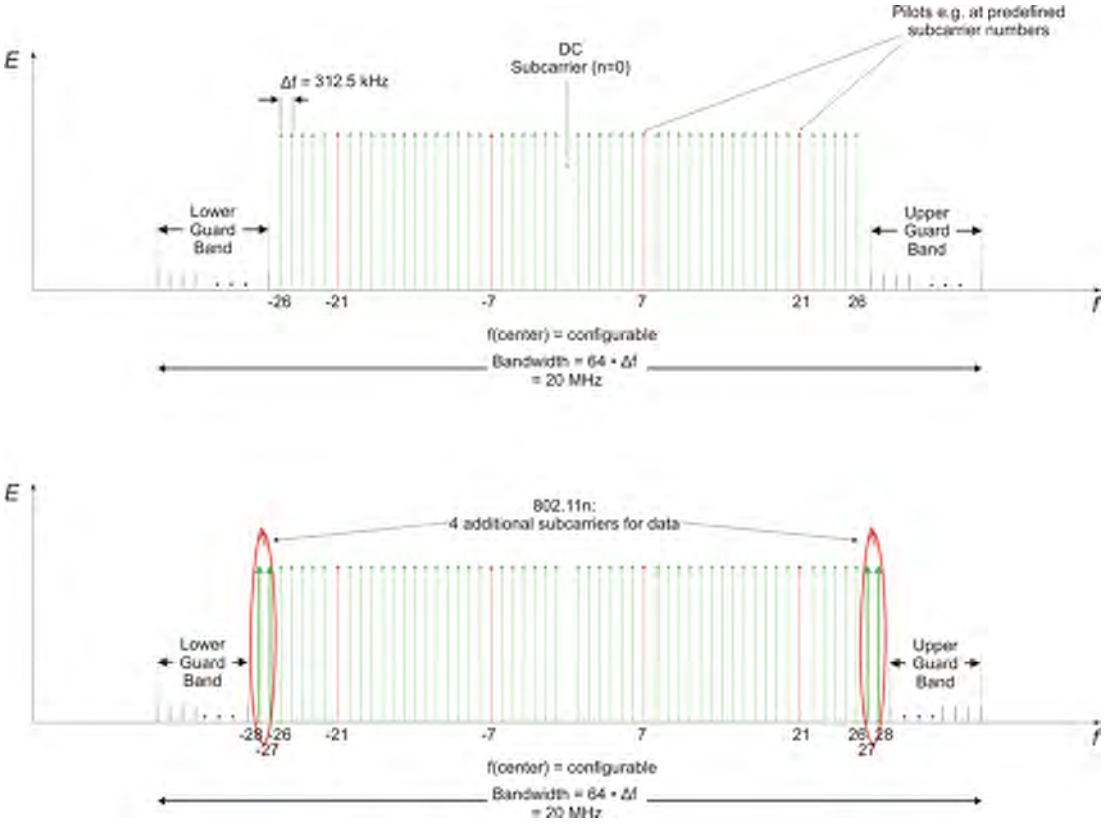


The objective of this section is to structure the IEEE 802.11n enhancements into a few groups to ease the understanding of the following sections.

Remark
The image states "majority" because a few enhancements are not covered by the presented feature groups. They are presented in the following sections.

2.1.5 Other Enhancements

2.1.5.1 More Data Subcarriers / Smaller Guardband



The objective of this section is to illustrate that 802.11n uses four additional data subcarriers by reducing the upper and lower guardbands.

The support for these additional 4 subcarriers is mandatory in IEEE 802.11n and needs to be supported by compliant AP's and STA's.

Image Description

- The image illustrates in the upper part the legacy constellation. Out of the 64 subcarriers, only 52 are useful and 4 of them are used as pilots. This leaves us with a number of 48 data subcarriers.
- In the lower part of the image we see the situation with 802.11n: Four additional subcarriers are provided by reducing the upper and lower guard bands. To be more precise: Subcarrier numbers (-28), (-27), 27 and 28 are used within 802.11n.

2.1.5.1.1 Performance Gain

The performance gain compared to using 48 data subcarriers is 4/48 = 8.33%.

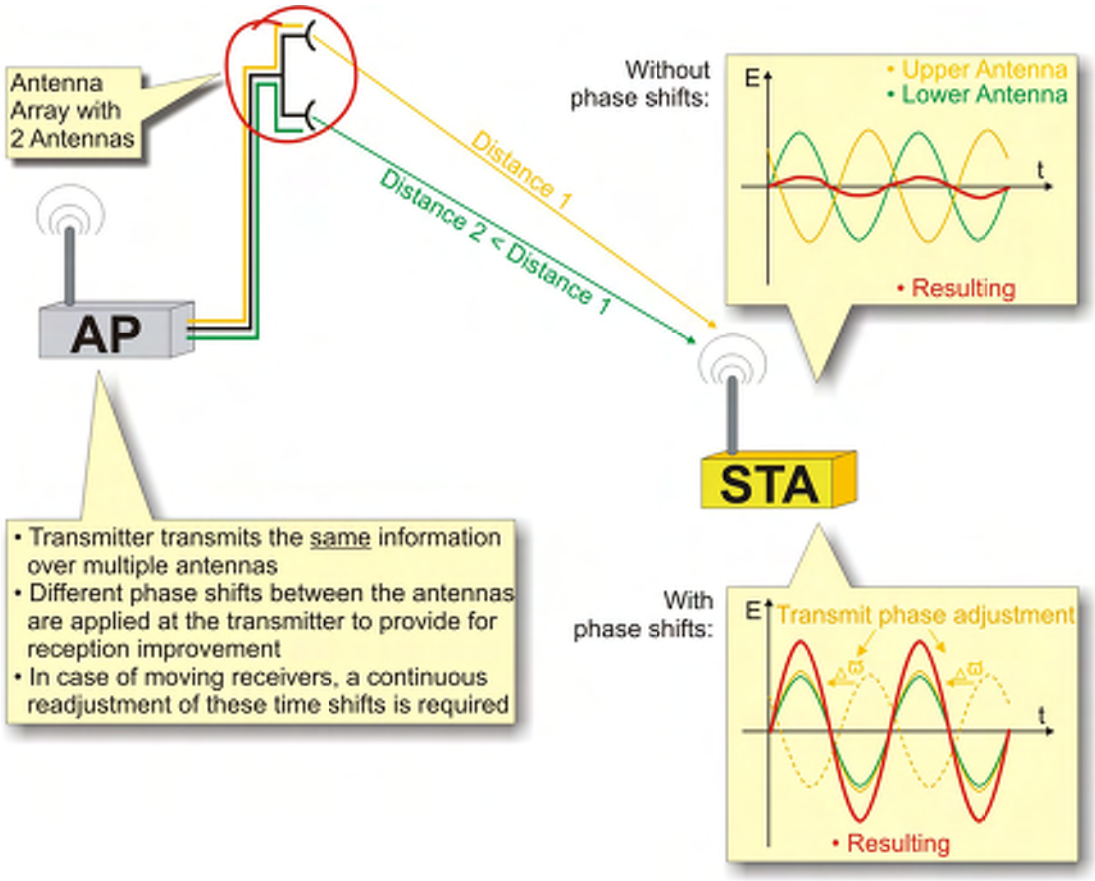
[IEEE 802.11n (20.3.6)]

Room for your Notes:

- **Abbreviations of this Section:**

AP	Access Point (IEEE 802.11, 802.16)	**kHz**	Kilo Hertz (10^3 Hertz)
DC	Direct Current	**MHz**	Mega Hertz (10^6 Hertz)
IEEE	Institute of Electrical and Electronics Engineers	**STA**	Station

2.2.4 Transmit Beamforming



The objective of this system is to illustrate the principle operation of beam forming antenna arrays.

Key point of this section is that beamforming requires some sort of feedback channel so that the antenna array can be readjusted. In a TDD-system with its channel reciprocity, this feedback channel may simply be the STA's standard uplink channel.

Image Description

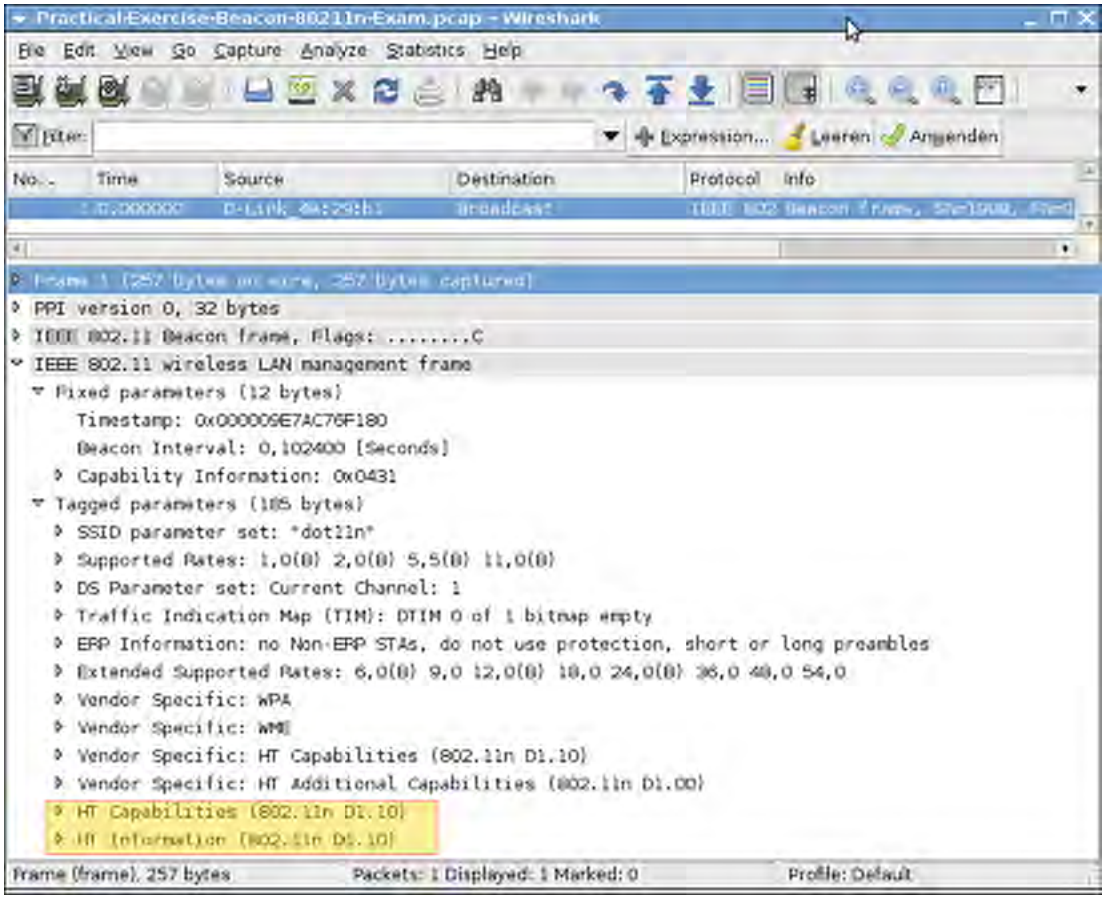
- The image illustrates an AP with two transmit antennas. Because of the physical distance between these two antennas, also the distance and the propagation paths of the two antennas to the STA is different.
- Based on the feedback that the AP receives for each antenna, different phase shifts are applied to both signals so that the “Resulting” matches the red waveform in the lower right diagram.

Room for your Notes:

- **Abbreviations of this Section:**

AP	Access Point (IEEE 802.11, 802.16)	**STA**	Station
		TDD	Time Division Duplex

2.3.2 Practical Exercise: Evaluate a Beacon Frame with HT-Information Elements



The objectives of this section are to: (1) See the various presented features of 802.11n in a real-life logfile. (2) Understand how an AP communicates its HT-related capabilities to STA's

Please answer the following questions, using:

- Enclosure 1: Practical-Exercise-Beacon-80211n-Exam.pdf (spec extract)
- Log file 1: Practical-Exercise-Beacon-80211n-Exam.pcap (or use printout)

Question No 7: What is the maximum A-MPDU length that the AP supports in receive direction?

Question No 8: What is the maximum A-MSDU length that the AP supports in receive direction?

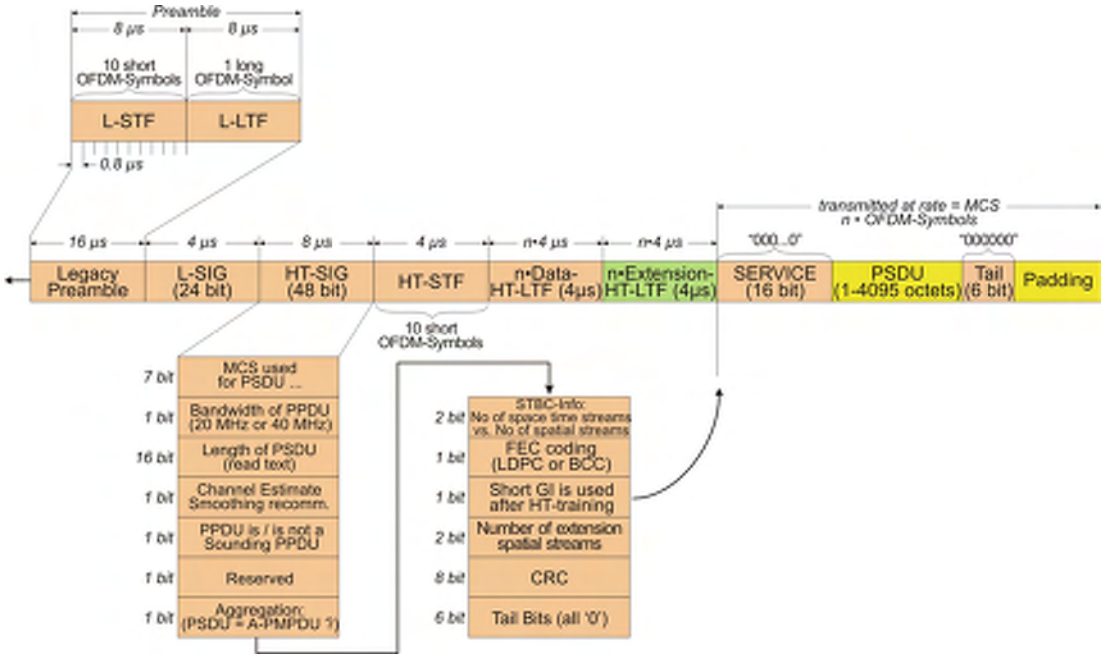
Question No 9: Does the AP support 40 MHz operation? If yes, is the secondary channel above or underneath the primary channel? Which channel number does the primary channel have?

Question No 10: Which MCS's does this AP support?

Question No 11: Are there currently any non-greenfield operation capable STA's associated to this AP?

Room for your Notes:

3.1.2 Mixed Format



The objective of this section is to present the format and content of the mixed format PPDU which is used to transmit HT (High Throughput) PPDU's.

Key point of this section is that support for mixed format is mandatory for all 802.11n-compliant STA's (incl. AP's).

3.1.2.1 Non-HT / Legacy Preamble

The legacy preamble in the header of the mixed format PPDU is there to provide for backward compatibility with legacy STA's. Please see section 1.6.5 for more details [IEEE 802.11n (20.3.9.3)].

3.1.2.2 L-SIG

Like the legacy preamble, L-SIG is there for backward compatibility with legacy devices that operate in the same BSS.
The RATE-field in the L-SIG shall always be set to 6 Mbit/s. This allows for the longest possible duration of the remaining part of the PPDU, because receiving legacy devices will calculate that duration based on RATE and LENGTH.

If RATE = 6 Mbit/s, then those legacy STA's will assume BPSK-modulation with 1/2-rate coding, thus together with the LENGTH-field rather long durations can be indicated.

However, with the mixed format, the maximum PSDU-length (and therefore also the maximum MPDU- and A-MPDU-length) equals 4095 octets [IEEE 802.11n (9.13.4)].

[IEEE 802.11n (20.3.2)]

to be continued on the next page

- **Abbreviations of this Section:**

A-MPDU	Aggregated MAC Protocol Data Unit (IEEE 802.11)	**LTF**	Long Training Field
AP	Access Point (IEEE 802.11, 802.16)	**MCS**	Modulation and Coding Scheme
BCC	Broadcast Call Control (3GTS 44.069)	**MPDU**	MAC Protocol Data Unit
BCC	Binary Convolutional Coding	**OFDM**	Orthogonal Frequency Division Multiplexing
BPSK	Binary or Bipolar Phase Shift Keying	**PPDU**	PLCP Protocol Data Unit
BSS	Basic Service Set	**PSDU**	PLCP Service Data Unit
CRC	Cyclic Redundancy Check	**SIG**	Special Interest Group (e.g. Bluetooth)
FEC	Forward Error Correction	**SIG**	Signaling Field (IEEE 802.11)
GI	Guard Interval	**STA**	Station
HT	High Throughput	**STBC**	Space Time Block Coding
LDPC	Low Density Parity Check	**STF**	Short Training Field
		TE	Terminal Equipment

3.1.2.3 HT-SIG

The HT-SIG contains various fields, similar to L-SIG as the image indicates [IEEE 802.11n (20.3.9.4.3)]. It is quite important to realize that the LENGTH-field is 16 long and can therefore reference PSDU-lengths of up to 65,535 octets. Still, in mixed environments no more than 4095 octets long PSDU's are acceptable (see statement above). The LENGTH-value = 0 is also possible and refers to NDP's (Null Data Packet) w/o data field which are used for sounding-PPDU's.

Note that HT-SIG will also use BPSK as modulation scheme, however, the symbols will be 90° rotated and therefore occupy the Q-plane rather than the I-plane as applies for the L-SIG.

3.1.2.4 HT-STF

The HT short training field is used to improve automatic gain control in a MIMO-system. In regular 20 MHz-operation, the HT-STF equals the L-STF and thus consists of 10 short OFDM-symbols. For 40 MHz-operation, please refer to [IEEE 802.11n (20.3.9.4.5)].

3.1.2.5 HT-LTF

The HT long training field is used to enable better estimation of the MIMO channel. Please note that there are data HT-LTF's (DLTF) and extension HT-LTF's. (ELTF)

The number of HT-LTF's per PPDU (combination of DLTF's and ELTF's) shall not exceed 5 [IEEE 802.11n (20.3.9.4.6)]

3.1.2.5.1 DLTF

There are one up to four DLTF's per mixed PPDU. The number depends on the number of spatial streams used whereas this number (1 .. 4) matches the number of DLTF's with one exception. If there are three spatial streams, there shall be four DLTF's [IEEE 802.11n (20.3.9.4.6)].

3.1.2.5.2 ELTF

ELTF's are optional (also their support is optional) and they shall only be present to sound extra spatial dimensions of the MIMO-channel which are not used by the HT-data portion [IEEE 802.11n (20.3.9.4.6)].

3.1.2.6 SERVICE-Field

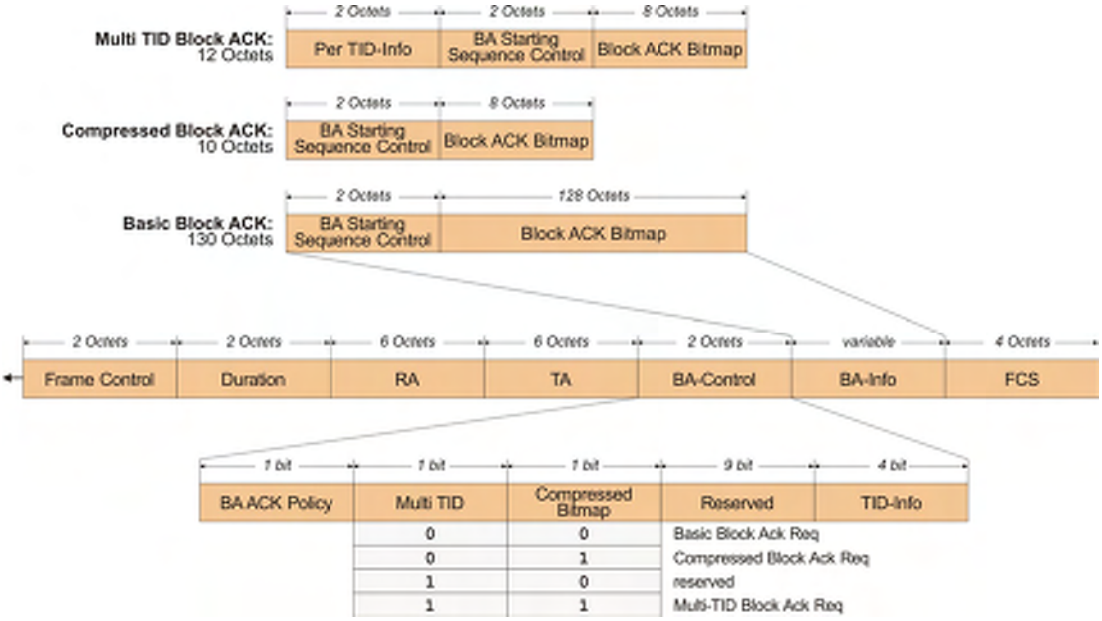
The SERVICE-field remains in use as in legacy PPDU's. All bits are set to '0' and the bits are used used to synchronize the de-scrambler at the receiver [IEEE 802.11n (20.3.9.4.6)].

Room for your Notes:

- **Abbreviations of this Section:**

BPSK	Binary or Bipolar Phase Shift Keying	**MIMO**	Multiple In / Multiple Out (antenna system)
DLTF	Data Long Training Field (IEEE 802.11)	**NDP**	Null Data Packet (IEEE 802.11)
ELTF	Extension Long Training Field (IEEE 802.11)	**OFDM**	Orthogonal Frequency Division Multiplexing
HT	High Throughput	**PPDU**	PLCP Protocol Data Unit
IEEE	Institute of Electrical and Electronics Engineers	**PSDU**	PLCP Service Data Unit
LTF	Long Training Field	**SIG**	Signaling Field (IEEE 802.11)
MHz	Mega Hertz (10^6 Hertz)	**STF**	Short Training Field

4.4.4.2 New Format of the BlockAck Frame



The objective of this section is to analyze the format changes of the BlockAck frame and to understand which new parameters are included with 80211n.

There are three different BlockAck types: Basic BlockAck, Compressed Bitmap BlockAck and Multi-TID BlockAck that can be asked for by a new BlockAck Request.

MAC-Header
The MAC-header is still the same as prior to 802.11n.

4.4.4.2.1 Redefined BA-Control Field

- Similarly to the BlockAck Req, "Multi-TID"-field together with "Compressed Bitmap" identify which information is included in the BA-Info field.
- The "BAR Ack Policy" bit indicates whether the receiver of the BlockAck Request-message shall return an ACK-message to confirm receipt of the BlockAck Request-message.

4.4.4.2.2 BA-Info

- As illustrated, the content of the BA-info field depends on the BlockAck-type.
- Three types may have been requested by the preceding BlockAck Request:: "Basic", "Compressed" and "Multi-TID".

[IEEE 802.11n (7.2.1.8)]

Room for your Notes:

- **Abbreviations of this Section:**

BA	Block Ack	**RA**	Receive Address
BAR	Block Ack Request	**TA**	Transmitter Address
FCS	Frame Check Sequence (CRC-Check)	**TID**	Traffic Identifier
MAC	Medium Access Control		