

Wireless LANs (WLANs)

Inhaltsverzeichnis

Wireless LANs.....	1
1 - Historie.....	1
2 - Einleitung.....	2
3 - Grundlagen.....	8
3.1 - Funknetzaufbau.....	8
3.2 - WLAN-Modi.....	9
3.3 - WLAN-Topologien / WLAN-Architekturen / WLAN-Service-Sets.....	13
3.3.1 - Basic Service-Set (BSS).....	13
3.3.2 - Independent Basic Service-Set (IBSS).....	14
3.3.3 - Personal BSS (PBSS).....	14
3.3.4 - Infrastruktur BSS.....	15
3.3.5 - Quality of Servide BSS (QBSS).....	15
3.3.6 - Extended Service Set (ESS).....	16
3.4 - Handover / Roaming.....	17
3.5 - Mobile IP.....	18
3.6 - Sicherheit.....	19
3.7 - Frequenz-Bänder.....	20
3.7.1 - Das 2,4 GHz-Band.....	21
3.7.2 - Das 5 GHz-Band.....	23
3.7.3 - Das 6 GHz-Band.....	25
3.7.4 - Das 60 GHz-Band.....	25
3.8 - Reichweiten.....	26
3.9 - Multiplexverfahren.....	27
3.9.1 - SDMA.....	29
3.9.2 - FDMA.....	31
3.9.3 - TDMA.....	32
3.9.4 - CDMA.....	33
3.10 - Modulationsarten.....	35
3.10.1 - QPSK.....	36
3.10.2 - CCK.....	37
3.10.3 - QAM-Modulation.....	38
3.10.4 - 16-QAM.....	39
3.10.5 - 64-QAM.....	40
3.10.6 - 1024-QAM.....	41
4 - IEEE-802.11 im ISO-7-Schichtenmodell.....	42
4.1 - Aufteilung der Ebenen.....	42
4.2 - Layer-Management.....	44
4.3 - Ausgetauschte Dateneinheiten.....	47
4.4 - PHY-Layer.....	49
4.4.1 - PMD.....	49
4.4.2 - Bandspreizverfahren.....	51
4.4.2.1 - FHSS.....	51
4.4.2.1.1 - FHSS-Technologie.....	52
4.4.2.1.2 - FHSS-Modulationsverfahren.....	53
4.4.2.1.2.1 - 2GFSK.....	53
4.4.2.1.2.2 - 4GFSK.....	54

4.4.2.1.3 - FHSS-Frameformat.....	54
4.4.3 - DSSS.....	56
4.4.3.1 - DSSS-Signalspreizung.....	56
4.4.3.2 - DSSS-Modulation.....	56
4.4.3.3 - DSSS-Frameformat.....	57
4.4.4 - OFDM.....	58
4.4.4.1 - Beschreibung der verwendeten Parameter.....	60
4.4.4.2 - Übersicht des Sendevorgangs in der PHY-Schicht.....	61
4.4.4.3 - Übersicht des Empfangsvorgangs in der PHY-Schicht.....	62
4.4.4.4 - Scrambler.....	63
4.4.4.5 - Faltungscodierer.....	64
4.4.4.6 - Punktierung.....	65
4.4.4.7 - Beispiel für Faltungscodierung und Punktierung.....	66
4.4.4.8 - Interleaving.....	67
4.4.4.9 - Kanalabschätzung mit Trainingssequenzen.....	71
4.4.4.10 - OFDM-Übertragungsverfahren.....	76
4.4.4.11 - PLCP Sendeprozedur.....	82
4.4.4.12 - PLCP Empfangsprozedur.....	85
4.4.5 - Vergleich von FHSS DSSS und OFDM.....	88
4.5 - MAC-Ebene.....	89
4.5.1 - MPDU-Header-Aufbau.....	89
4.5.1.1 - Frame-Control-Feld.....	90
4.5.1.2 - Duration-Feld.....	92
4.5.1.3 - Adress-Felder.....	93
4.5.1.4 - Sequence-Feld.....	94
4.5.1.5 - Daten-Feld.....	94
4.5.1.6 - Frame Check Sequence – Feld (FCS).....	94
4.5.2 - Kanalzugriff.....	95
4.5.2.1 - Zugriffsverfahren.....	95
4.5.2.2 - Erweiterungen zu DCF und PCF.....	95
4.5.2.3 - DCF.....	96
4.5.2.3.1 - Backoff-Time.....	96
4.5.2.3.2 - Inter Frame Spaces (IFS).....	97
4.5.2.3.3 - Quittungen.....	99
4.5.2.3.4 - DCF Ablaufbeispiel.....	101
4.5.2.3.5 - Einstellung von RTS/CTS.....	104
4.5.2.3.6 - Hidden-Station-Problem.....	105
4.5.2.3.7 - Exposed-Station-Problem.....	108
4.5.2.4 - PCF.....	109
4.5.3 - Fragmentierung.....	112
4.5.4 - Synchronisation der Stationen.....	114
4.5.5 - Steuerung der Leistungsaufnahme.....	115
4.5.6 - Management-Frames.....	117
4.5.6.1 - Authentication-Algorithm-Feld.....	119
4.5.6.2 - Authentication-Transaction.Sequence-Number-Feld.....	119
4.5.6.3 - Beacon-Interval-Feld.....	119
4.5.6.4 - Capability-Infomation-Feld.....	119
4.5.6.5 - Current-AP-Feld.....	120
4.5.6.6 - Listen-Interval-Feld.....	120

4.5.6.7 - Reason-Code-Feld.....	120
4.5.6.8 - Association-ID-Feld.....	120
4.5.6.9 - Status-Code-Feld.....	120
4.5.6.10 - Timestamp-Feld.....	120
4.5.6.11 - Informations-Elemente.....	121
4.5.6.12 - Herstellerspezifische Informationselemente.....	121
5 - Der IEEE-802.11 - Standard.....	122
5.1 - Übersicht.....	122
5.2 - Anfänge von IEEE-802.11.....	123
5.2.1 - Eigenschaften.....	123
5.2.2 - WLAN-Frame nach IEEE-802.11.....	124
5.3 - Verbesserungen.....	126
5.3.1 - IEEE-802.11a/h.....	126
5.3.2 - IEEE-802.11b.....	127
5.3.3 - IEEE-802.11g.....	128
5.3.4 - IEEE-802.11n.....	131
5.3.4.1 - Eigenschaften.....	131
5.3.4.2 - MIMO.....	132
5.3.4.3 - Selection Combining.....	132
5.3.4.4 - Transmit Beamforming.....	134
5.3.4.5 - Adaptives Beamforming.....	134
5.3.4.6 - Raum-Zeit-Codes.....	134
5.3.4.7 - Raum-Multiplex-Verfahren.....	135
5.3.4.8 - Zusätzliche Coderate.....	136
5.3.4.9 - Verkürztes Guard-Intervall.....	136
5.3.4.10 - Verdopplung der Kanalbandbreite von 20 MHz auf 40MHz.....	136
5.3.4.11 - Low Density Parity-Check.....	137
5.3.4.12 - Zusammenfassung der Schritte zur Verbesserungen der Datenübertragungsraten.....	138
5.3.4.13 - Vergleich der spektrale Effizienzsteigerung.....	138
5.3.4.14 - Modualtion Coding Scheme (MCS).....	139
5.3.4.14.1 - MCS 32.....	140
5.3.4.14.2 - Verwaltung der MCS-Varianten.....	140
5.3.4.15 - IEEE-802.11n-PPDU-Formate.....	141
5.3.4.16 - HT-Signal-Felder.....	142
5.3.4.17 - Sendeleistung.....	143
5.3.4.18 - CCA-Empfindlichkeit.....	143
5.3.4.19 - Empfängerempfindlichkeit.....	143
5.3.4.20 - 802.11n-MAC.....	144
5.3.4.20.1 - Reduced IFS.....	144
5.3.4.20.2 - Aggregationsverfahren.....	144
5.3.4.20.2.1 - A-MPDU.....	144
5.3.4.20.2.2 - A-MSDU.....	145
5.3.4.20.3 - Block-Acknowledgement.....	146
5.3.4.20.4 - BlockACK-Frame-Format.....	147
5.3.4.20.4.1 - BlockACK-Request.....	147
5.3.4.20.4.1.1. Basic BlockACK-Request Variante.....	148
5.3.4.20.4.1.2. Compressed BlockACK-Request Variante.....	148
5.3.4.20.4.1.3. Extended Compressed BlockACK-Request Variante.....	148
5.3.4.20.4.1.4. Multi-TID BlockACK-Request Variante.....	148

5.3.4.20.4.1.5. GCR BlockACK-Request Variante.....	148
5.3.4.20.4.2 - BlockACK Frame.....	149
5.3.4.20.4.2.1. Basic BlockACK Variante.....	149
5.3.4.20.4.2.2. Compressed BlockACK Variante.....	149
5.3.4.20.4.2.3. Multi-TID BlockACK Varianten.....	149
5.3.4.20.4.2.4. Extended Compressed BlockACK Variante.....	150
5.3.4.20.4.2.5. GCR BlockACK Variante.....	150
5.3.4.20.5 - PoE-Stromversorgung.....	151
5.3.4.20.6 - Protection Mechanismus.....	151
5.3.4.20.7 - 20- und 40MHz-Betrieb.....	152
5.3.4.20.8 - Phased Coexistence Operation (mittlerweile obsolet).....	152
5.3.4.20.9 - Dual-CTS-to-Self-Verfahren.....	154
5.3.5 - IEEE-802.11ac.....	155
5.3.5.1 - Eigenschaften.....	155
5.3.5.2 - Neuerungen.....	155
Im 5GHz-Breit gibt es 3 zusammenhängende Bereiche von denen der untere für den Indoor-Bereich gedacht ist. Deshalb ist dort die DFS (Dynamic Frequency Selection) nicht erforderlich. Im Außenbereich muss DFS angewendet werden, da es dort passieren kann, dass die Primäruser unterwegs sind.....	156
5.3.5.3 - 802.11ac-Beamforming.....	157
5.3.5.4 - Multi-User-MIMO.....	157
5.3.5.5 - Kanalbündelung.....	158
5.3.5.6 - CCA-Empfindlichkeit.....	159
5.3.5.7 - Empfängerempfindlichkeit.....	159
5.3.5.8 - VHT-PPDU-Format.....	160
5.3.6 - IEEE-802.11ad.....	161
5.3.7 - IEEE-802.11af.....	162
5.3.8 - IEEE-802.11ah.....	163
5.3.9 - IEEE-802.11ax.....	164
5.3.9.1 - Betriebsmodi für die Versorgung mehrerer User.....	164
5.3.9.2 - OFDMA.....	166
5.3.9.3 - Beamforming.....	172
5.3.9.4 - BSS-Coloring.....	173
5.3.9.5 - PPDU-Formate.....	176
5.3.9.6 - Frame-Format-Details.....	177
5.3.9.6.1 - HE-SIG-A.....	177
5.3.9.6.2 - HE-SIG-B.....	178
5.3.9.6.3 - Zuordnung der RUs zu den Tone-Segmenten.....	179
5.3.9.7 - Multiuser-Betrieb.....	181
5.3.9.8 - OFDMA-Padding.....	181
5.3.9.9 - Wi-Fi 6E.....	182
5.3.10 - Künftiger Standard Wi-Fi-7 (IEEE802.11be).....	184
5.3.10.1 - Multi-Link Operation (MLO).....	185
5.3.10.1.1 - Simultaneous Transmit and Receive (STR).....	185
5.3.10.1.1.1 - Durchsatzsteigerung.....	187
5.3.10.1.1.2 - Reduzierung der Latenzzeit.....	187
5.3.10.1.1.3 - Robustheit.....	188
5.3.10.1.2 - Enhanced Multi-Link Multi Radio (EMLMR).....	188
5.3.10.1.3 - Enhanced Multi-Link Single Radio (EMLSR).....	188

5.3.10.1.4 - Multi-Link Single Radio (MLSR).....	189
5.3.10.2 - Optimierungen am Medienzugriffsverfahren OFDMA.....	189
5.4 - Vergleich der IEEE-802.11-Standards.....	190
5.5 - Zusätzliche Entwicklungen für den IEEE-802.11-Standard.....	191
5.5.1 - IEEE-802.11d.....	192
5.5.2 - IEEE-802.11e.....	193
5.5.3 - IEEE-802.11f.....	195
5.5.4 - IEEE-802.11i.....	196
5.5.5 - IEEE-802.11k-v-r.....	196
5.5.5.1 - IEEE-802.11k.....	197
5.5.5.2 - IEEE-802.11v.....	197
5.5.5.3 - IEEE-802.11r.....	197
5.6 - Betrieb von IEEE-802.11.....	198
5.6.1 - Beacon-Frames.....	199
5.6.2 - Verbindungsvorgang.....	202
5.6.2.1 - Scanning.....	202
5.6.2.1.1 - Passive Scanning.....	202
5.6.2.1.2 - Active Scanning.....	203
5.6.2.2 - Authentifizierung.....	204
5.6.2.2.1 - Stati.....	204
5.6.2.2.2 - Ablauf.....	207
5.6.2.2.2.1 - Aus Sicht des Requesters.....	207
5.6.2.2.2.2 - Aus Sicht des Responders.....	207
5.6.2.2.3 - Open-System-Authentifizierung.....	208
5.6.2.2.4 - Shared-Key-Authentifizierung.....	209
5.6.2.3 - Assoziation.....	211
5.6.2.4 - Reassoziation.....	212
5.6.3 - Dynamischer Schlüsselaustausch nach IEEE-802.1x.....	213
6 - WLAN-Antennen.....	217
6.1 - Allgemeines.....	217
6.2 - Einführung.....	217
6.3 - Grundlagen.....	218
6.4 - Antennenbauformen.....	218
6.5 - Richtantennen.....	218
6.6 - Freiraumdämpfung.....	219
6.7 - Halbwellendipole.....	221
6.8 - Stabantenne.....	222
6.9 - Dipolgruppen.....	222
6.10 - Patchantennen.....	223
6.11 - Richtantennen.....	223
6.11.1 - Öffnungswinkel / Halbwertsbreite.....	224
6.11.2 - Vor- Rückverhältnis.....	225
6.12 - Fresnel-Zone.....	225
6.13 - Diversity-Antennen.....	227
6.14 - Antennenleitungen.....	227
6.15 - Equivalent Isotropically Radiated Power (EIRP).....	228
6.16 - Reichweite.....	228
7 - Sicherheit.....	231
7.1 - Einführung.....	231

7.1.1 - Verschlüsselung.....	231
7.1.2 - Probleme.....	232
7.1.3 - Datenverfälschung.....	232
7.2 - Verschlüsselung.....	232
7.3 - Entschlüsselung.....	234
7.4 - Zusammenfassung der WEP-Probleme.....	234
7.5 - Wi-Fi Protected Access (WPA).....	235
7.6 - WPA 2.....	236
7.6.1 - Einführung.....	236
7.6.2 - Master Key.....	237
7.6.3 - Transient Key.....	237
7.6.4 - Schlüsselarten.....	237
7.6.5 - Verfahren zur Erzeugung von Zufallszahlen.....	238
7.6.5.1 - Pseudo-Random Number Generator (PRNG).....	238
7.6.5.2 - Pseudo-Random Function (PRF).....	238
7.6.6 - Paarweise Schlüssel.....	239
7.6.7 - Gruppenschlüssel.....	242
7.6.8 - Schlüsselwechsel.....	242
7.6.9 - Temporal Key Integrity Protocol (TKIP).....	243
7.6.10 - Verschlüsselung mit TKIP.....	243
7.6.11 - Transport der Daten-Bits mit TKIP.....	244
7.6.12 - Entschlüsselung mit TKIP.....	245
7.6.13 - MIC-Fehler.....	246
7.7 - CCMP.....	247
7.7.1 - Verschlüsselung mit CCMP.....	248
7.7.1.1 - Ablauf der Verschlüsselung.....	248
7.7.1.2 - CCMP-MIC-Berechnung.....	249
7.7.2 - Transport der Daten mit CCMP.....	250
7.7.3 - Entschlüsselung mit CCMP.....	250
7.7.4 - Broadcast / Multicast Integrity Protocol (BIP).....	251
7.8 - WPA3.....	251
7.9 - Angriffs-Szenarien.....	252
7.9.1 - Daten-Umleitung.....	252
7.9.2 - Replay (Wiederholung von Paketen).....	253
7.9.3 - Wörterbuch mit Schlüsselsequenzen.....	253
7.9.4 - Known-Plain-Text Angriff.....	253
7.9.5 - Schwache Schlüssel.....	254
7.9.6 - IV-Kollisionen.....	254
7.9.7 - Einschleusen von Nachrichten.....	254
7.9.8 - Denial-of-Service.....	254
7.9.9 - Man-in-the-Middle.....	255
7.9.10 - Session Hijacking.....	256
7.9.11 - Deauthentication.....	256
8 - Planungsgrundlagen.....	257
8.1 - Einleitung.....	257
8.2 - Konfigurationsbeispiele.....	258
8.2.1 - Erweiterung des vorhandenen LANS um ein WLAN.....	258
8.2.2 - Überdeckung einer großen Fläche mit einem WLAN.....	259
8.2.3 - Viele Clients im selben WLAN.....	260

8.2.4 - Ausfallsicherheit und Redundanz.....	260
8.2.5 - Funkverbindung zwischen zwei LANs.....	261
8.3 - Antennenbeispiele.....	262
8.3.1 - Flächenabdeckung mit omnidirektionalen Antennen.....	262
8.3.2 - Flächenabdeckung mit Dipol-Antennen.....	262
9 - WLAN-Geräte.....	263
9.1 - Clients.....	263
9.2 - WLAN-Telefon.....	263
9.3 - Access Points (APs).....	263
9.4 - WLAN-Controller.....	264
9.5 - WLAN-Switches.....	264
10 - Gesundheitliche Aspekte.....	265
11 - Abkürzungsverzeichnis.....	266
12 - Abbildungsverzeichnis.....	275
IT-Security.....	275
Einleitung.....	275
Begriffe und Definitionen.....	275
IT-System.....	275
Soziotechnisches System.....	275
Objekte.....	275
Informationen.....	277
Subjekte.....	277
Autorisierung.....	277
Verlässlichkeit.....	277
Informationskanäle.....	277
Speicherkanäle.....	277
Legitime Informationskanäle.....	277
Verdeckte Informationskanäle.....	277
Sicherheit.....	278
Allgemeines.....	278
Funktionssicherheit.....	280
Informationssicherheit.....	280
Datensicherheit.....	280
Datenschutz.....	280
Schutzziele.....	280
Authentizität.....	280
Authentifikation.....	280
Subjekt-Authentifikation.....	280
Objekt-Authentifikation.....	280
Datenintegrität.....	282
Vertraulichkeit.....	282
Verfügbarkeit.....	282
Verbindlichkeit.....	282
Abrechenbarkeit.....	282
Anonymität.....	282
Pseudomisierung.....	282
Informationelle Selbstbestimmung.....	283
Schwachstelle.....	284
Verwundbarkeit.....	284

Bedrohungen.....	284
Risiko.....	284
Gewichtung.....	284
Angriff.....	284
Passiver Angriff.....	284
Sniffer.....	285
Aktiver Angriff.....	285
Spoofing.....	285
Denial of Service (DoS).....	285
Social Engineering.....	285
Viren.....	286
Würmer.....	287
Trojaner.....	287
Abwehr von Angriffen.....	287
Verschlüsselung.....	287
Rechte-Reduzierung.....	287
Monitoring.....	287
Angreifer Typen.....	289
Hacker.....	289
Cracker.....	289
Skript-Kiddie.....	289
Rechtliche Rahmenbedingungen.....	290
Relevante Gesetze.....	290
Bundes Datenschutzgesetz (BDSG).....	290
Telekommunikationsgesetz (TKG).....	290
Betriebsverfassungsgesetz (BetrVG).....	290
Strafgesetzbuch (StGB).....	290
Bürgerliches Gesetzbuch (BGB).....	291
Gesetz zur Kontrolle und Transparenz im Unternehmen (KonTraG).....	291
Aktiengesetz (AktG).....	291
GmbH-Gesetz (GmbHG).....	291
Haftung.....	291
Geheimer Datenaustausch.....	293
Verschlüsselung.....	293
Kryptographie.....	295
Kryptoanalyse.....	295
Statistische Kryptoanalyse.....	295
Differentielle Kryptoanalyse.....	295
Lineare Kryptoanalyse.....	295
Kryptoregulierung.....	295
Chiffrierer.....	296
Stromchiffrierer.....	296
Blockchiffrierer.....	298
ECB-Modus.....	298
CBC-Modus.....	299
Schlüsselverfahren.....	301
Symmetrische Schlüsselverfahren.....	301
Asymmetrische Schlüsselverfahren.....	301
Übersicht über Schlüsselverfahren.....	303

Verschlüsselungsstandards.....	303
Verwendete Methoden.....	303
S-Boxen.....	303
Byte-Umstellung.....	303
Pseudo-Hadamard-Transformation (PHT).....	303
Transformation / Verschiebungschiffre.....	304
Substitutionschiffre.....	305
Symmetrische Verschlüsselungsstandards.....	306
DES (Data Encryption Standard).....	306
TripleDES / 3DES.....	306
International Data Encryption Algorithm (IDEA).....	306
Blowfish.....	307
RC4.....	307
AES.....	307
Asymmetrische Verschlüsselungsstandards.....	309
Diffie-Hellmann.....	309
RSA.....	310
Hash-Funktionen.....	311
MD5.....	312
SHA / SHA-1.....	312
RIPEMD-160.....	312
Tiger.....	312
Vergleich der beschrieben Hash-Funktionen.....	313
MAC.....	313
HMAC.....	313
Public Key Infrastructure (PKI).....	314
Zertifikate.....	314
Komponenten einer PKI.....	315
Virtuelle Private Netzwerke (VPN).....	316
Unterschiedliche Tunnel-Protokolle.....	316
Layer-2-Tunnelprotokolle.....	316
Voluntary Tunneling.....	317
Compulsory Tunneling.....	318
Layer-3-Tunnelprotokolle.....	319
IP-in-IP.....	319
Generic Routing Encapsulation (GRE).....	319
Internet Protocol Security (IPSec).....	319
IPSec Key Exchange (IKE).....	320
RADIUS (Remote Authentication Dial In User Service).....	321
Allgemeines.....	321
Ablauf einer Authentifizierung.....	322
Authentifizierungsprotokolle bei RADIUS.....	324
PAP.....	324
CHAP.....	324
EAP.....	325
Externe Benutzerdaten.....	326
Accounting.....	326
Ausblick auf die weitere Entwicklung.....	326
Quellen.....	326

Inhaltsverzeichnis

1 - Literaturverzeichnis.....	333
2 - Stichwortverzeichnis.....	334
3 - Anhänge.....	344
3.1 - Beacon-Frame-Informationen.....	344
3.2 - Status-Codes.....	352
3.3 - Reason-Codes.....	356
4 - Formelanhang.....	360
4.1 - DB-Leistungsverhältnisse.....	360
4.2 - dbw.....	360
4.3 - dbm.....	360

Wireless LANs

1 - Historie

Drahtlose Datenübertragung war lange Zeit eine Sache von verschiedenen Anbietern, die mit proprietären Produkten auf den Markt gingen. Wer sich für eine solche Lösung interessierte, hatte immer die Abhängigkeit zu einem Hersteller zu beachten. Dies führte dazu, dass sich Funknetzwerke nicht besonders verbreiteten.

Seit 1990 hatte sich bei IEEE eine Arbeitsgruppe (IEEE-802.11) mit der Entwicklung eines Standards beschäftigt. [IEEE-802.11-2016][KAUF-WLANS-2002][Rech-WLAN-2012]

Da hierbei nur der kleinste gemeinsame Nenner zwischen unterschiedlichsten Herstellern und Anforderungen erreicht wurde, waren viele Freiheitsgrade offen geblieben. Die Weiterentwicklungen wurden weltweit von unterschiedlichen Herstellern betrieben. Deshalb war die Interoperabilität der Produkte unterschiedlicher Hersteller oft nicht gegeben. Zusätzlich sind auch noch nationale Gegebenheiten zu berücksichtigen. Dies führte dazu, dass die unterschiedlichen Weiterentwicklungen unkoordiniert und zeitlich versetzt auf den Markt kamen. Sie wurden in verschiedenen Ländern mit unterschiedlichen Ausprägungen, wie z. B. Sendeleistungen, auf den Markt gebracht.

Nachdem 1997 - trotz der langen Entwicklungszeit - die erste Veröffentlichung verfügbar war, waren im ersten Wurf die Verbindungsmöglichkeiten zwischen unterschiedlichen Herstellern mehr theoretischen Natur.

Die so genannte Interoperabilität wurde erst geschaffen als die Wireless Compatibility Alliance (WECA) den Begriff Wireless Fidelity (Wi-Fi) einführt. Die Produkte von Herstellern, die in der Wi-Fi-Testumgebung funktionierten, bekamen das Wi-Fi-Zertifikat.



Abbildung 1: Wi-Fi-Logo

Ein weiteres Problem war, dass die Sicherheit anfänglich vernachlässigt worden war. Erst mit der Einführung von WPA wurde am Markt eine Akzeptanz geschaffen.

Die öffentliche Verfügbarkeit von WLANs, die einen Zugriff auf das Internet wie z. B. auf Flughäfen ermöglichen haben dazu beigetragen, dass das Thema WLAN immer weiter in das allgemeine Interesse rückt. Die so genannten Hotspots, welche diese Funktionalität bieten, sind mittlerweile ein normales Tor zum Internet für viele Reisende geworden.

Einen weiteren Schub gab die Entwicklung des Centrino-Chipsatzes von Intel. Hier ist eine WLAN-Integration, nach dem Standard IEEE-802.11b, im Chipsatz realisiert. Für Besitzer von Notebooks der neueren Generationen bedeutet dies keine zusätzlichen Karten oder Anschlüsse, da bereits alles Notwendige im Gerät integriert ist.

Durch den Preisverfall bei den Access Points (APs) im Small Office Home Office (SOHO)-Bereich ist auch für viele privaten Anwender die Möglichkeit der Nutzung dieser Technologie gekommen. Die weiteren Entwicklungen haben sich zum einen mit der Erhöhung der Datenrate als auch mit der Sicherheit beschäftigt und diese stetig verbessert.

Spätestens seit der Einführung von WPA2 ist das Thema Sicherheit kein grundsätzliches KO-Kriterium mehr.

2 - Einleitung

Es gibt gute Gründe für die Vernetzung von Rechnern mittels WLAN:

- ➊ Räumliche Flexibilität innerhalb des Empfangsbereichs.
- ➋ Keine Verkabelungsprobleme. Verkabelung ist nicht nur teuer, sondern unter bestimmten Umständen gar nicht möglich. Wie zum Beispiel bei denkmalgeschützten Gebäuden kann nicht an beliebigen Stellen die Wand aufgestemmt werden und mal eben eine Leitung eingezogen werden. Wer seine Firma über mehrere Gebäude in einer Stadt evtl. gegenüber auf der anderen Straßenseite untergebracht hatte, musste über teure Stand- oder Wählleitungen die Verbindungen herstellen.
- ➌ Ad-hoc-Netzwerke ohne aufwändige Planung möglich.
- ➍ Keine Lizenzen (Genehmigungen / Gebühren) erforderlich.

Dem gegenüber stehen jedoch auch Nachteile:

- ➊ Gegenüber Verkabelung langsam.
- ➋ Hohe Bitfehlerraten im Vergleich zu LANs.
- ➌ Nationale Restriktionen (es gibt keine einheitlichen international gültigen Frequenzbänder)
- ➍ Sicherheit durch die Funkstrecke als „Shared Media“. WLANs bedeuten einen nicht unerheblichen Mehraufwand durch zusätzliche Maßnahmen die für Sicherheit erforderlich werden.
- ➎ Kosten. Wer ein WLAN in Betrieb nimmt, muss trotzdem erst einmal verkabeln, denn die Access-Points (APs) müssen ebenfalls angeschlossen werden (sowohl an ein LAN als auch an eine Stromversorgung).

Einsatzgebiete ergeben sich in vielfältiger Weise:

- ➊ Erweiterung der vorhandenen Infrastruktur
- ➋ Denkmalgeschützte Gebäude
- ➌ Freilandforschung
- ➍ Hot Spots (Flughäfen, ...)
- ➎ Messen, Museen
- ➏ Krankenhäuser
- ➐ Lagerverwaltung
- ➑ ...

Parallel zu den WLANs gibt es den kleineren Sendebereich, die so genannten Wireless Personal Area Networks (WPANs). Bei IEEE sind die Themen in diesem Zusammenhang unter der Norm IEEE-802.15 zusammengefasst.

● IEEE-802.15.1

Entspricht der Bluetooth SIG (Bluetooth Special Interest Group). Die aktuelle Version vom 17. Dezember 2009 ist 4.0. Sie enthält zwei verschiedene Protokollstapel (protocol stacks), die mit unterschiedlichem Zeitbedarf eine *unilaterale* Übertragung oder bidirektionale verbindungsorientierte Kommunikation aufbauen.

Bluetooth arbeitet mit einem Frequency Hopping Verfahren wie IEEE-802.11 im 2,4 GHz-Band. Obwohl die Reichweite geringer als bei IEEE-802.11 ist, stehen die beiden Standards im Betrieb in Konkurrenz und stören sich.

● IEEE-802.15.2

Hier wird empfohlen wie WPANs mit WLANs zusammenarbeiten sollen. Dies schließt auch Bluetooth, ZigBee, CSS, und UWB mit ein.

● IEEE-802.15.3

Hier soll der Energieverbrauch und die Datenübertragungsraten bei WPANs (11, 22, 33, 44, 55 Mbit/s) geregelt werden. Die Spezifikation umfasst die Medium Access Control (MAC) und den Physical Layer (PHY).

● IEEE-802.15.4

Hier werden die Übertragungsverfahren für geringe Übertragungsraten behandelt. Diese werden beispielsweise bei Fernbedienungen, Sensoren und für einfache Übertragungsnetzwerke verwendet.

● IEEE-802.15.5

Diese 2009 veröffentlichte Norm beschäftigt sich mit der Vermischung von WPANs.

● IEEE-802.15.6

Hier werden die so genannten Body-Area-Networks (BAN) beschrieben. Das Anwendungsgebiet der Geräte ist auf, in und um einen Körper (menschlich oder tierisch) definiert.

● IEEE-802.15.7

Spezifiziert den Aufbau von PHY und MAC für die Verwendung von Licht als Übertragungsmedium (siehe Visible Light Communications)

Für den Sendebereich, der über den von WLANs hinaus geht, gibt es bei den Wireless Metropolitan Area Networks (WMANs) mit dem Standard IEEE802.16 (WiMAX) Lösungen.

Mobilfunkstandards

Diese Standards sind historisch entstanden und wurden von Generation zu Generation weiter entwickelt. Je nach verfügbarer Verbindung kommt die bestmögliche Verbindung zustande.

- GPRS
- UMTS
- LTE
- 5G

Bei den neueren Mobilfunkstandards ist vor allem die Verfügbarkeit nicht überall gegeben. Während in den Ballungsgebieten die Versorgung gut ist, gibt es in ländlichen Umgebungen immer noch viele weiße Flecken.

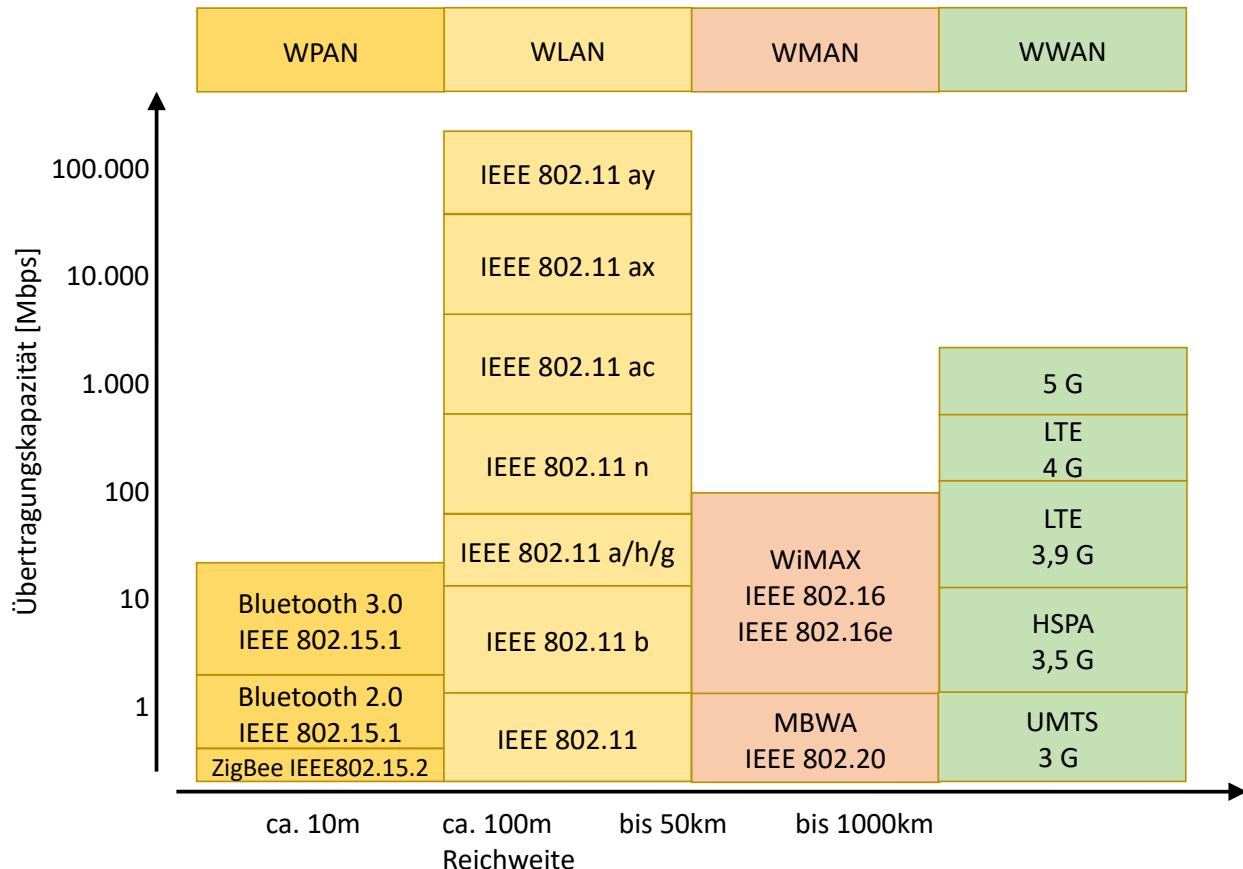


Abbildung 2: Abgrenzung zwischen WPAN, WLAN, WMAN und WWAN

Es gab noch weitere Versuche einen Standard für die drahtlose Datenübertragung zu etablieren, doch waren diese Ansätze nicht erfolgreich. Darunter sind:

- ➊ ETSI Hiperlan2 (ETSI = European Telecommunications Standard Institute)

Dies ist der europäische Versuch einen Standard für Funknetze zu schaffen. Er arbeitet im 5GHz-Band und mit OFDM (Orthogonal Frequency Division Multiplexing) als Modulationsverfahren kann bis zu 54Mbps übertragen werden. Dieser Standard bietet QoS (Quality of Service) sowie DFS (Dynamic Frequency Selection) und TPC (Transmission Power Control). Da er ähnlich wie ATM arbeitet, hatte er auch den Namen wireless ATM bekommen. Bei dieser Technik wird immer ein AP benötigt, was zur Folge hat, dass es eine Peer-to-Peer-Verbindung wie im IEEE-802.11-Ad-hoc-Modus nicht möglich ist. Nach dem Ausstieg von Ericsson aus der Hiperlan2-Entwicklung im Dezember 2001, ist diese WLAN-Alternative so gut wie tot. Funktionen wie DFS oder TPC sind jedoch in andere Standards wie z. B. IEEE-802.11h übernommen worden.

- ➋ RadioLAN

Arbeitet im 5,8 Ghz-Band. Hatte nur in den USA Anwendung gefunden.

- ➌ HomeRF

Ist für den Büro und Heimbereich konzipiert und bietet somit sowohl Peer-to-Peer-Netze als auch einen Infrastruktur-Modus ähnlichen Betrieb. HomeRF ist in zwei Versionen auf den Markt gekommen in der ersten Version waren maximal 1,6Mbps möglich. In der zweiten Version sind 10 Mbps möglich. Für das Zugriffs-Verfahren wird CSMA/CA verwendet. Durch Priorisierungs-Mechanismen ist für Multimedia eine Streaming-Funktionalität möglich. Zusätzlich ist eine Sprachübertragung nach DECT möglich.

- ➍ DECT Digital Enhanced Cordless Telephone

Arbeitet im Frequenzbereich von 1880 -1900 MHz. Wurde um die DECT Multimedia Access Profile erweitert und bietet eine skalierbar garantierte Bandbreite die von der Entfernung unabhängig ist.

- ➎ Infrarot

Dieser Versuch wurde zwar im IEEE-802.11-Standard spezifiziert, ist jedoch nie mit funktionierenden Geräten untermauert worden und hat keine Bedeutung mehr.

3 - Grundlagen

3.1 - Funknetzaufbau

Der allgemeine Aufbau eines Funknetzes sieht vereinfacht folgendermaßen aus.

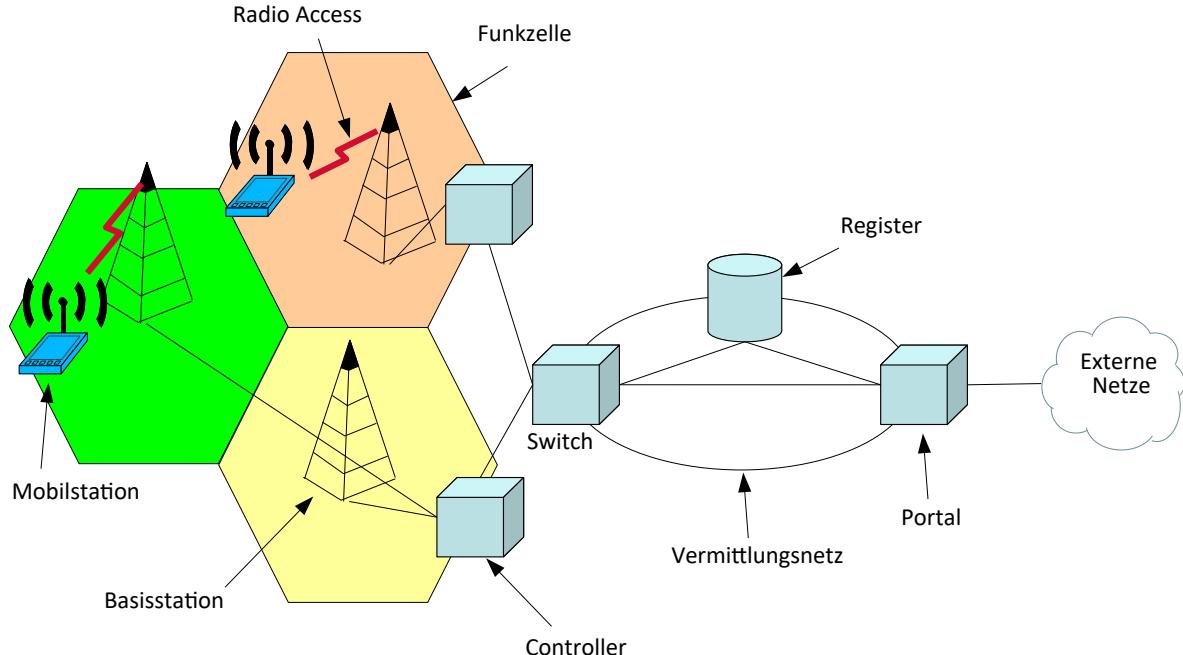


Abbildung 3: Allgemeiner Funknetzaufbau

Ein großes flächendeckendes Funknetzwerk wird durch mehrere Funkzellen aufgebaut.

In jeder Funkzelle steht eine Basisstation, welche die Funkzelle über eine Antenne mit einem Funknetz abdeckt und so mit den Mobilstationen kommuniziert. Die einzelnen Basisstationen werden über Controller verwaltet.

Die Controller hingegen sind über ein Vermittlungsnetzwerk miteinander verbunden. Im Vermittlungsnetzwerk ist auch die Registriereinheit lokalisiert, welche erkennt, wann eine Mobilstation zu einer Funkzelle hinzukommt, sie verlässt oder von einer Funkzelle in eine andere wechselt. Dies stellt die Basis zur Abrechnung dar. Zusätzlich stellt das Vermittlungsnetzwerk mit dem Portal die Verbindung mit externen Netzwerken her.

3.2 - WLAN-Modi

Mit den Modi werden die Beziehungen zwischen zwei WLAN-Kommunikationspartnern beschrieben. Davon abhängig ist die Anzahl der Teilnehmer und die Art des Medium-Zugriffs.

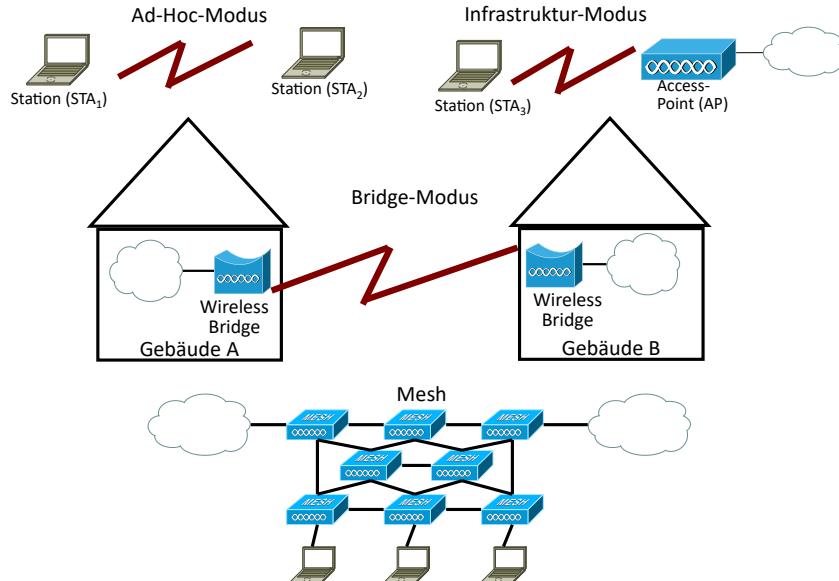


Abbildung 4: WLAN-Modi

Es gibt mehrere Modi, in denen WLANs betrieben werden können:

- Im Ad-hoc-Modus können zwei oder mehrere Stationen über eine WLAN-Verbindung direkt miteinander kommunizieren.
- Da der Infrastruktur-Modus der Default-Modus ist, muss der Ad-hoc-Modus erst manuell eingestellt werden. Um diesen Modus einzustellen, bieten viele WLAN-Adapter zwei Einstellmöglichkeiten.
- 802.11-Ad-hoc-Modus
 - Pseudo-Ad-hoc-Modus

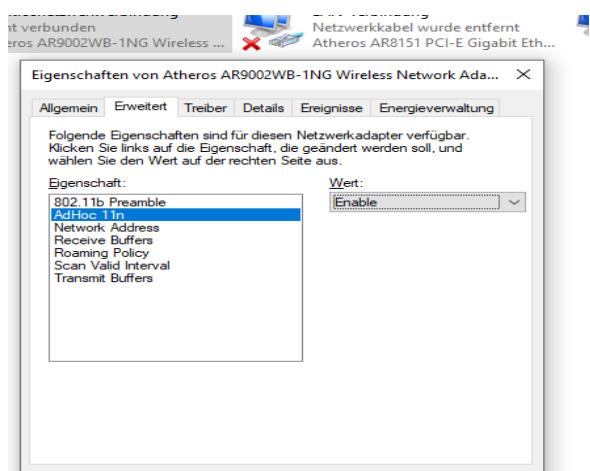


Abbildung 5: Ad-hoc-Modus unter Windows10

Nach Möglichkeit sollte der 802.11-Ad-Hoc-Modus eingestellt werden. (Im Beispiel Links gibt es nur eine Einstellmöglichkeit auf AdHoc 11n)

Grundsätzlich müssen alle Geräte, die miteinander kommunizieren sollen, den gleichen Modus eingestellt haben.

Unter Windows kann der Ad-Hoc-Modus folgendermaßen eingestellt werden:

Netzwerkverbindungen:

- Drahtlosnetzwerkverbindung auswählen
- Eigenschaften (über rechte Maustaste)
- Adapter Konfigurieren (anklicken)
- Menü-Erweitert

- ➊ Im Infrastruktur-Modus wird eine WLAN-Zelle von einem Access Point (AP) verwaltet. Jede Kommunikation zwischen den Teilnehmern des Netzwerks geht über den AP. Direkte Verbindungen zwischen den Stationen sind im Default nicht vorgesehen. Oft bieten die APs eine Verbindung zu anderen Netzwerken.
Der Infrastruktur-Modus ist bei Stationen der Default-Modus.
Damit lassen sich Stationen, die nur über eine WLAN-Schnittstelle verfügen, agieren als seien sie mir einer kupferbasierten Verbindung angeschlossen. Damit könne sie an einen drahtgebundenen Server oder an das Internet anschließen. Das Netzwerk kann mit entsprechenden Antennen räumlich ausgedehnt werden. So sind zwischen 30m in Räumen und bis zu einigen Kilometern im Freien möglich. Auch Filtermöglichkeiten sind in APs untergebracht. So kann auf MAC-Adressen oder Protokolle gefiltert werden. Da die Funkwellen auch Wände durchdringen können, ist zumindest bei den kurzen Distanzen nicht auf die LOS (Line of Sight) zu achten.
- ➋ Im Bridge-Modus können z. B. zwei Gebäude und das dort vorhandene LAN über eine WLAN-Verbindung mit WLAN-Bridges und gerichteten Antennen (Yagi-Uda-Antenne) verbunden werden. Hierbei ist auf eine Sichtverbindung LOS (Line Of Sight) zu achten.
- ➌ Ein Mesh-WLAN ermöglicht es eine drahtlose Infrastruktur, ohne zugehöriges LAN-Distributionsnetzwerk, zu erstellen. Stattdessen wird im IEEE-802.11s mit einem Wireless Distribution System (WDS) die Verbindung der Accesspoints beschrieben.
In der Arbeitsgruppe IEEE-802.11s wurde das Mesh-WLAN erarbeitet. Ein vermaschtes BSS ist ein WLAN, das aus autonomen Stationen besteht. Die Stationen bauen untereinander drahtlose Verbindungen auf um wechselseitig MSDUs auszutauschen. Innerhalb des Mesh-BSS (MBSS) nutzen die Stationen die Mesh Coordination Function (MCF) um auf den Kanal zuzugreifen. Die MCF basiert auf der QoS.

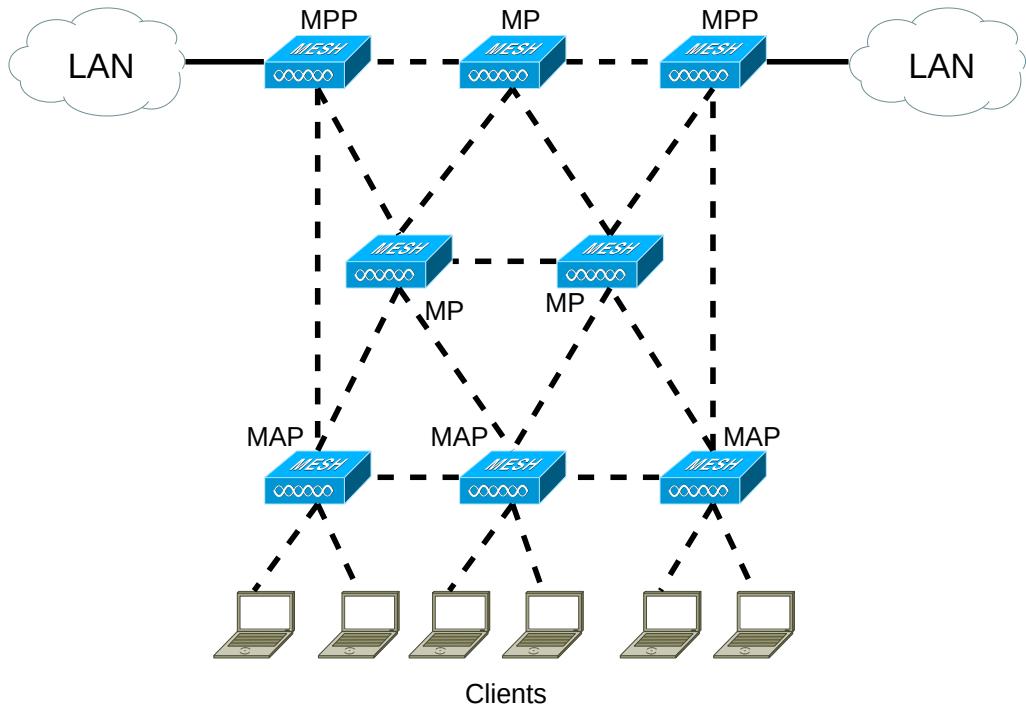


Abbildung 6: Mesh-WLAN

Bei einem Mesh-WLAN werden 3 neue Stationsformen eingesetzt:

- ➊ Mesh Access Points (MAPs)

Diese Geräte stellen die Verbindungen zu den Clients her und verhalten sich gegenüber ihnen wie Access Points (APs). Damit bieten sie den Clients den Zugangspunkt zum WLAN. Weiterhin halten sie über ein weiteres WLAN-Interface die Verbindung zu anderen MAPs, MPs und MPPs. Die WLAN-Interfaces arbeiten entweder im selben oder anderen Frequenzbändern.

- ➋ Mesh Points (MPs)

Diese Geräte dienen nur dem Weitertransport von WLAN-Daten über WLAN und bieten daher für Clients keinen Zugangspunkt an. MPs dienen daher nur der Vergrößerung der Ausdehnung des WLANs.

- ➌ Mesh Portals (MPPs)

MPPs bieten eine Gateway-Funktion in andere Netzwerke oder andere WLANs. Sie haben also z. b. eine LAN-Schnittstelle. In einem Mesh-WLAN können mehrere MPPs vorhanden sein.

Die Verwaltung eines Mesh erfolgt autonom. Dazu erkennen die Knoten ihre Nachbarn automatisch. Sie wählen zusammen die Kanäle aus und erstellen die Verbindungen. Anpassungen erfolgen automatisch. D. h. Hinzukommende und wegfallende Mesh-Knoten werden automatisch eingefügt oder entfernt. Dazu senden die Mesh-Knoten zyklisch Informationen aus anhand derer die benachbarten Mesh-Knoten die Existenz von Nachbarknoten in Erfahrung bringen können.

Die Wegewahl durch das Mesh erfolgt auf der Basis von größter Bandbreite, kürzeste Latenzzeit und geringste Anzahl von Hops. Sie erfolgt auf der MAC-Ebene und ist für die WLAN-Stationen, sowie für höhere Protokollsichten, transparent.

3.3 - WLAN-Topologien / WLAN-Architekturen / WLAN-Service-Sets

An dieser Stelle wird in der Literatur oft von Topologien gesprochen. Im Sinne von Netzwerk-Topologien haben WLANS jedoch die Ausprägung von Zellen.

Man kann die folgenden Ausprägungen auch als unterschiedliche Architekturen beschreiben. Um jedoch Verwechslungen mit unterschiedlichen Protokoll-Architekturen zu vermeiden, soll im Folgenden von Service-Sets gesprochen werden.

Während die Modi die Anzahl der Teilnehmer und die Art der Verbindung zwischen WLAN-Geräten beschreibt, zeigen die Service-Sets auf, wie mehrere WLAN-Geräte zu Gruppen mit unterschiedlichen Abhängigkeiten zusammen gefasst werden können.

3.3.1 - Basic Service-Set (BSS)

Jeder Rechner, der einen entsprechenden Adapter eingebaut hat, kann eine Funkzelle aufbauen. Bei WLANS spricht man hierbei von Stationen. Im einfachsten Fall hat eine Station einen kugelförmigen Funk-Abdeckungsraum um sich herum aufgebaut. Eine Station kann ein Smartphone, ein Notebook oder aber auch ein Accesspoint (AP) sein, der noch keine besondere Aufgabe übernommen hat und daher wie ein Endgerät agiert.

Der Bereich, in dem sich die Abdeckungsbereiche zweier Funkzellen überschneiden, kann für einen Datenaustausch genutzt werden, sobald die Stationen eine Verbindung aufgebaut haben. Diese einfachste Form einer Zelle mit zwei Stationen wird Basic Service Set (BSS) genannt. In der Abbildung 7 sind zwei BSSs dargestellt. Im BSS1 haben zwei Stationen, die jeweils eine kreisförmigen Funkzelle besitzen, in einem ovalen Überschneidungsbereich ein BSS (BSS1) aufgebaut.

Mit der Einführung von Directional Multi-Gigabit (DMG) kann die Form einer Funkzelle mit Beamforming zu einer Keule geformt und in der Richtung ausgerichtet werden. Das ermöglicht es wie beim BSS2 die Richtung, die Größe und somit auch in der Reichweite der Funkzellen zu optimieren. Damit können Überschneidungen und somit auch Störungen von anderen BSSs reduziert werden.

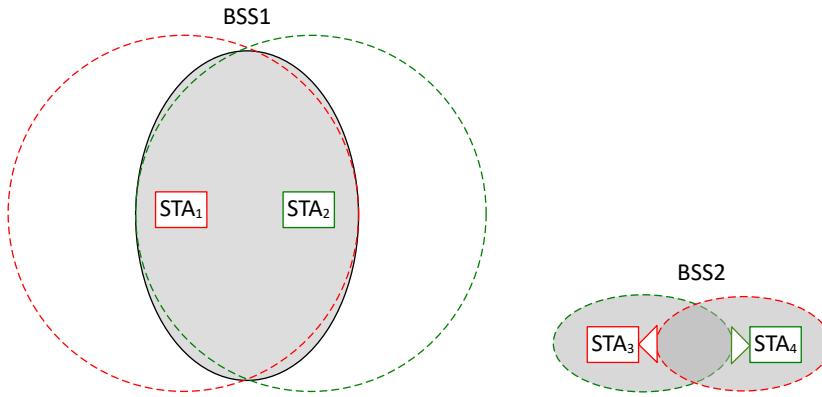


Abbildung 7: BSS in der einfachsten Ausprägung

Der Aufbau eines BSS ist sehr einfach und bedarf keiner besonderen Planung oder Verkabelung. Oft wird diese Form nur für die kurze Zeit eines Datenaustauschs aufgebaut und genutzt. Die Mitgliedschaft einer Station in einem BSS ist dynamisch. Sie können jederzeit aufgebaut und wieder abgebaut werden. Mobile Stationen kommen in den Funkbereich eines BSS und sie verlassen den Funkbereich auch wieder. Um ein Mitglied in einer BSS zu werden und alle Dienste zu nutzen, müssen die Stationen sich mit dem BSS assoziieren.

3.3.2 - Independent Basic Service-Set (IBSS)

Zu einem BSS können noch weitere Stationen hinzukommen. Haben die Stationen außer ihren Funkverbindungen keine weiteren Verbindungen in andere Netzwerke, spricht man von einem Independent Basic Service Set (IBSS). Dies ist die einfachste Form eines BSS. Typischerweise handelt es sich hierbei um Netzwerke im Ad-hoc-Modus. Die dabei genutzten Verbindungen sind Peer-to-Peer-Verbindungen, also Verbindungen, gleichberechtigter Partner. Es gibt keine Station, die Dienste verwaltet.

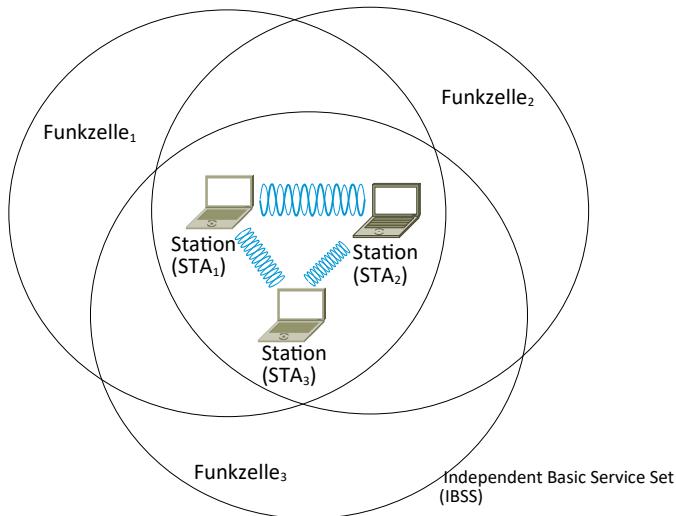


Abbildung 8: Independent Basic Service Set (IBSS)

Beim Verbindungsprozess arbeiten auch Geräte, die später zu einem Infrastruktur-BSS gehören, am Anfang im Ad-hoc-Modus. Erst später, wenn die Verbindung etabliert (assoziiert ist) ist eine Station im Infrastruktur-Modus.

3.3.3 - Personal BSS (PBSS)

Ähnlich wie ein Independent Basic Service Set (IBSS) besteht ein Personal BSS (PBSS) aus Stationen die miteinander kommunizieren können, ohne dass Verbindungen in andere Netzwerke bestehen.

Der Unterschied zu einem IBSS besteht darin, dass eine Station zu einem PBSS Control Point (PCP) wird. Damit gibt es eine zentrale Verwaltungseinheit, welche z. B. die Zeitsynchronisierung verwaltet und mit Service-Perioden Dienste verwalten und zuteilen kann.

Ein PBSS kann nur von einer DMG Stationen aufgebaut werden. Allerdings ist nicht jede DMG BSS eine PBSS. Eine DMG BSS kann PBSS, IBSS oder einer Infrastruktur BSS sein.

3.3.4 - Infrastruktur BSS

Hat eine BSS mit einem Access Point (AP) noch eine Verbindung zu einem andern Netzwerk aufgebaut, spricht man von einer Infrastruktur BSS. Das ist allerdings keine IBSS! Siehe hierzu auch das Kapitel Fehler: Verweis nicht gefunden.

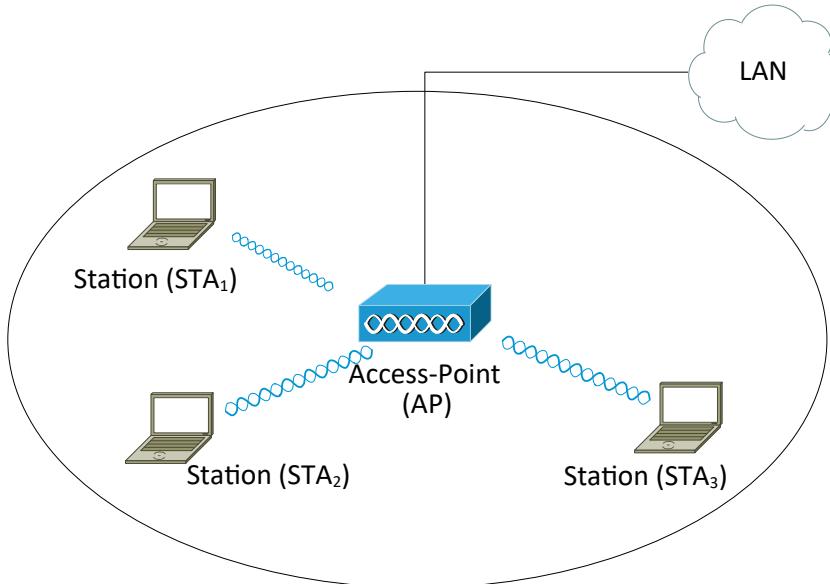


Abbildung 9: Infrastruktur BSS

Die Größe einer solchen BSS ist von folgenden Bedingungen abhängig:

- Sendeleistungen
- Antennen
- Bauliche Gegebenheiten

Dabei sind Distanzen von 30m in Gebäuden bis zu mehreren Kilometern im Freien mit Richtantennen möglich.

Je nach Umfang des WLANs fallen die Controller, Switches und Register zu einem Gerät (dem AP) zusammen, oder werden auf unterschiedliche Geräte verteilt. Dies gilt vor allem dann, wenn mehrere Funkzellen (BSSs) betrieben werden.

3.3.5 - Quality of Service BSS (QBSS)

Sobald die APs auch die **Quality of Service Funktionen (QoS)** abhandeln können spricht man von **Quality of Service APs (QAPs)** die ein **Quality of Service BSS (QBSS)** bereit stellen.

3.3.6 - Extended Service Set (ESS)

Mehrere Infrastruktur-BSSs können über ein Backbone-System, das so genannte Distributions-System (DS), miteinander zu einem Extended Service-Set (ESS) zusammen geschaltet werden. Im Allgemeinen wird ein LAN als Distribution System verwendet, denn so kann auch die Verbindung zu anderen kabelgebundenen Netzwerken und somit auch weiteren Diensten ermöglicht werden.

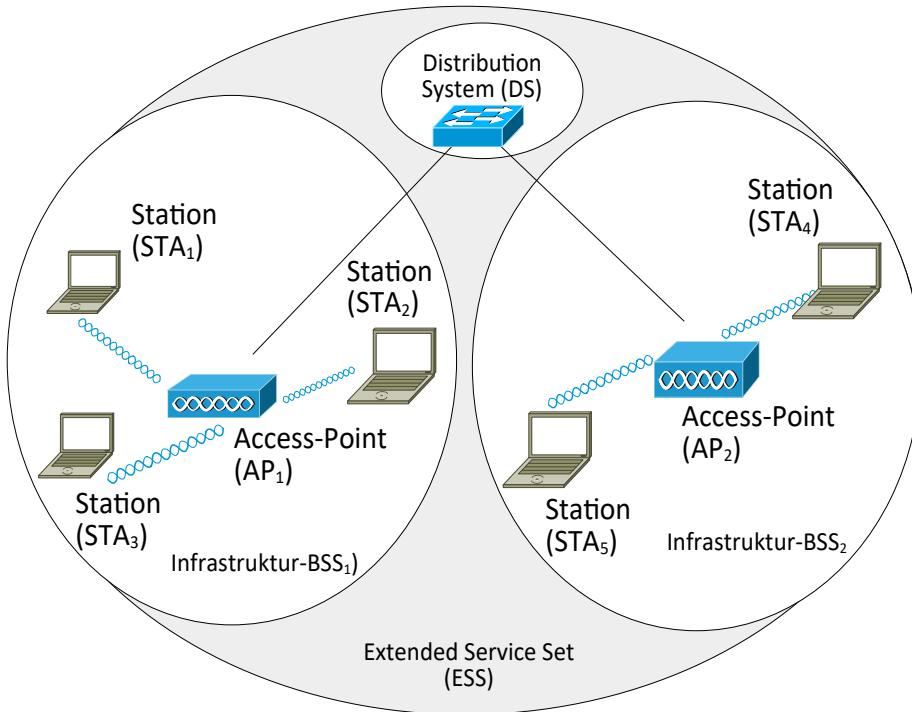


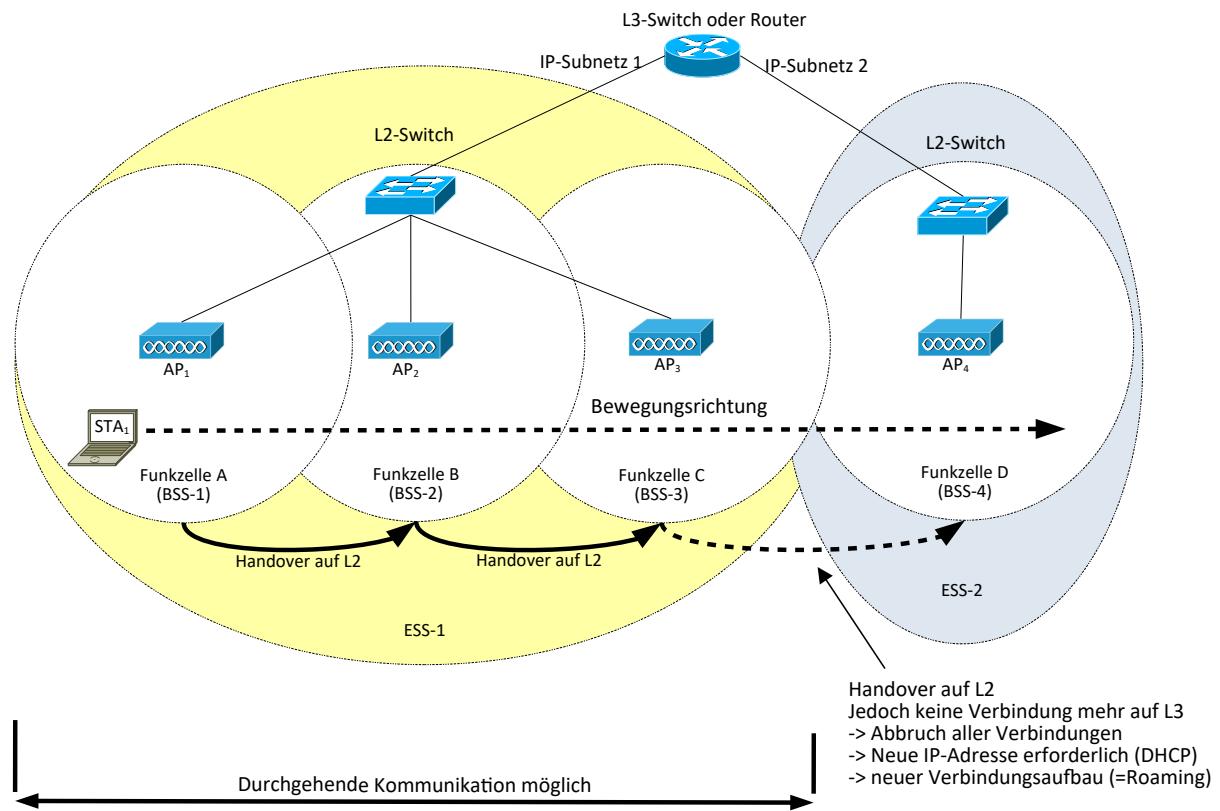
Abbildung 10: Extended Service Set

Zusammen mit dem DS bildet ein ESS ein flaches Layer-2-Netzwerk.

Innerhalb eines ESS kann eine Station sich frei bewegen. Dabei wird die Kommunikation auf den Ebenen >2 nicht unterbrochen.

Wechselt die Station von einer Funkzelle in eine andere, wird dieser Vorgang BSS-Transition oder auch Handover genannt. Dabei muss eine Übergabe von der Ausgangs-BSS an die Ziel-BSS erfolgen.

3.4 - Handover / Roaming



IEEE-802.11 beinhaltet keine nähere Spezifikation des DS. Wi-Fi hingegen legt fest, dass für das DS ein Ethernet zu verwenden ist. Daher kommt auch der Marketingbegriff „Wireless Ethernet“. Da schon die Zugriffs-Verfahren unterschiedlich sind, ist dieser Begriff eher irreführend. Man kann einen AP eher als Bridge im Sinne von Verbinder zwischen Token-Ring und Ethernet sehen.

Bewegt sich ein Client von einer Funkzelle zur nächsten, wird auf Ebene 2 ein Handover (BSS-Transition) vom Client-Adapter durchgeführt. Die Kommunikationsverbindungen bleiben bestehen. Zellenwechsel können jedoch auch durch schwankende Sendequalität entstehen.

Der Ablauf beim AP-Wechsel ist ähnlich wie beim ersten Verbindungsaufbau

- ➊ Scanning (aktiv / passiv)
- ➋ Reassocation Request
Station sendet Anfrage an APs
- ➌ Reassocation Response
Bei einem Erfolg (AP hat geantwortet)
Bei einem Misserfolg wird weiter gescannt
- ➍ AP akzeptiert Reassocation Request
Meldung der neuen Station am Distribution-System
Distribution-System aktualisiert daraufhin seinen Datenbestand
Alter AP wird vom Distribution-System informiert

Im allgemeinen Sprachgebrauch wird das Wechseln von einer Funkzelle in eine andere ebenfalls als Roaming bezeichnet. Dies ist falsch! Nur der Wechsel eines Endgerätes von einem Subnetz zu einem anderen bzw. der Wechsel eines Endgerätes von einem Netzsegment (z. B. IP-Netzwerk) zu einem anderen entspricht einem Roaming. Somit findet Roaming nur auf Ebene 3 statt und nicht auf den Ebenen 1-2 in denen WLANs aktiv sind.

Sobald jedoch der Client das IP-Subnetz wechselt, bleibt zwar die Verbindung auf Ebene 2 bestehen, jedoch ab Ebene 3 aufwärts besteht keine Verbindung mehr. Dies bedeutet, dass eine neue IP-Adresse vergeben werden muss. Die Kommunikation zwischen den Applikationen ist ebenfalls abgeschnitten und muss neu aufgebaut werden.

Soll nun zwischen unterschiedlichen IP-Subnetzen gewechselt werden, gibt es zwei Möglichkeiten:

- Dynamische IP-Adress-Vergabe mittels DHCP. Dabei ist ein Neustart der Applikation oder gar des Systems erforderlich.
- Mobile IP ermöglicht die Verwendung einer einzigen IP-Adresse auch bei einem IP-Subnetzwechsel. Dies wird dadurch ermöglicht, dass die Pakete an das Heimat-Netz geroutet werden und von da aus an das aktuelle IP-Subnetz getunnelt werden.

3.5 - Mobile IP

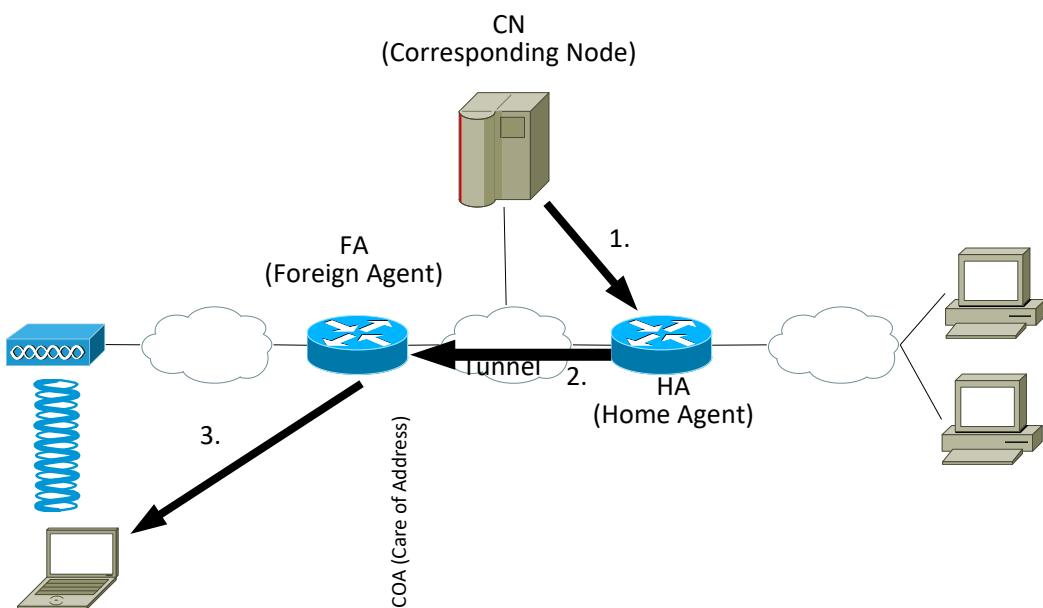


Abbildung 12: Mobile IP

Cisco bietet noch Proxy IP-Mobile. Dabei übernimmt der AP, stellvertretend für den Client, die IP-Adresse und stellt somit die Verfügbarkeit sicher.

3.6 - Sicherheit

WLANS haben durch die Funkschnittstelle einen unsicheren Bereich der sich schlecht vor Zugriffen schützen lässt. Zumindest das Mithören ist einfach möglich.

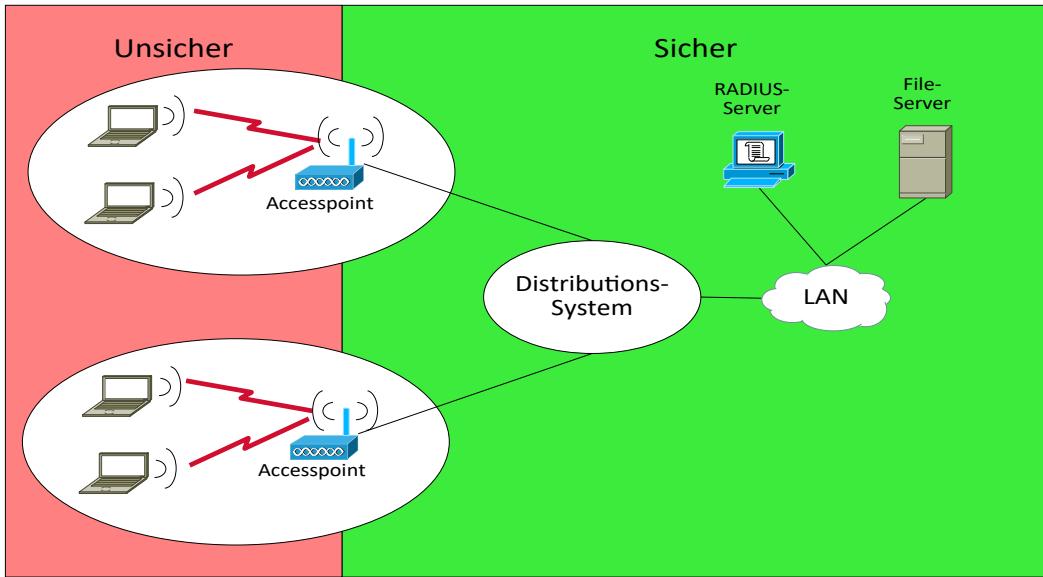


Abbildung 13: WLAN Allgemeiner Aufbau

Beim Übergang von der Funkschnittstelle zum LAN im AP ist durch geeignete Maßnahmen dafür zu sorgen, dass nur der erwünschte Datenverkehr stattfindet.

Dazu werden im Allgemeinen entweder Firewalls verwendet oder bereits am Access Point (AP), entsprechende Authentifizierungs-Mechanismen, wie IEEE-802.1x zusammen mit einem RADIUS-Server (Remote Authentication Dial In User Service) verwendet.

3.7 - Frequenz-Bänder

Die Frequenzbänder, in denen WLANs betrieben werden, sind zwischen Frequenzbänder für Telefon und Mautsystemen sowie weiteren Benutzern, wie Radar und Navigations-Systemen, untergebracht.

Tabelle 1: WLAN-Frequenzbänder

MHz	System		
168,4125 - 169,8125	ERMES (European Radio Messages System) z. B. Pager		
380 - 400	TETRA (Trans European Trunked Radio) z. B. Bündelfunk Taxi, Busse, Polizei		
419 - 430	TETRA (Trans European Trunked Radio) z. B. Bündelfunk Taxi, Busse, Polizei		
450 - 470	TETRA (Trans European Trunked Radio) z. B. Bündelfunk Taxi, Busse, Polizei		
863 – 868,6	IEEE-802.11ah (in Europa mit max. 25 mW)		
870 - 875	TETRA (Trans European Trunked Radio) z. B. Bündelfunk Taxi, Busse, Polizei		
876 – 880	GSM - R		
880 – 890	GSM Extension		
890 – 915	GSM 900		
901 - 928	IEEE-802.11ah (in USA mit max. 1 W)		
915 – 921	TETRA (Trans European Trunked Radio) z. B. Bündelfunk Taxi, Busse, Polizei		
925 – 935	GSM Extension		
935 – 960	GSM 900		
1710 – 1785	GSM 1800		
1805 – 1880	GSM 1800		
1880 – 1900	DECT		
1900 – 1980	UMTS		
1980 - 2010	UMTS Satellite		
2010 – 2025	UMTS		
2110 – 2170	UMTS		
2170 – 2200	UMTS Satellite		
2400 – 2500	ISM (IEEE-802.11b/g/n/ax, Bluetooth, Home-RF, Mikrowellenofen, Bewegungsmelder)		
4200 – 5725	Primärnutzer: Navigation	Sekundärnutzer	
		5150 – 5250	HIPERLAN 1 & 2, IEEE-802.11a/h/n/ac/ax
		5250 – 5350	HIPERLAN 2, IEEE-802.11a/h/n/ac/ax
		5470 – 5725	HIPERLAN 2, IEEE-802.11a/h/n/ac/ax
5725 – 5875	ISM (RTTT Road Transport Telefon Telematics = Österreichische Maut)		
5925 - 7125	U-NII-5 bis U-NII-8 in den USA für IEEE-802.11ax (Wi-Fi 6E) mit max. 1 W innen und max. 4W außen		
:	:		
61000 - 61500	IEEE-802.11ad/ay		

WLANs werden in so genannten ISM-Bändern betrieben. ISM steht für die Bereiche Industrial Scientific Medical.

In diesen Bändern darf lizenziert mit begrenzten Sendeleistungen gesendet werden.

In Tabelle 1 ist auch zu sehen, dass es mehrere ISM-Bänder gibt. Unterschiedliche Frequenzen haben unterschiedliche Reichweiten und unterschiedliche maximale Sendeleitungen. In diesen Bändern sind oft noch weitere Nutzer unterwegs, die einen Sendebetrieb stören können. In diesen Bändern müssen Störungen durch andere Bandnutzer toleriert werden. Dies bedeutet auch, dass mit Störeinflüssen durch andere Systeme umgegangen werden muss.

In Europa richten sich die Länder nach den Freigaben der ETSI und international nach der ITU. In Deutschland ist für die Vergabe von Frequenzbändern die Bundesnetzagentur (BNetzA) zuständig. In Österreich regelt die Rundfunk und Telekom Regulierungs-GmbH (RTR) und in der Schweiz das Bundesamt für Kommunikation (BAKOM) die Frequenzfreigabe.

In den USA werden die 5 und 6 GHz-Bänder in den so genannten Unlicensed National Information Infrastructure (U-NII)-Bändern von der Federal Communications Commission (FCC) verwaltet.

3.7.1 - Das 2,4 GHz-Band

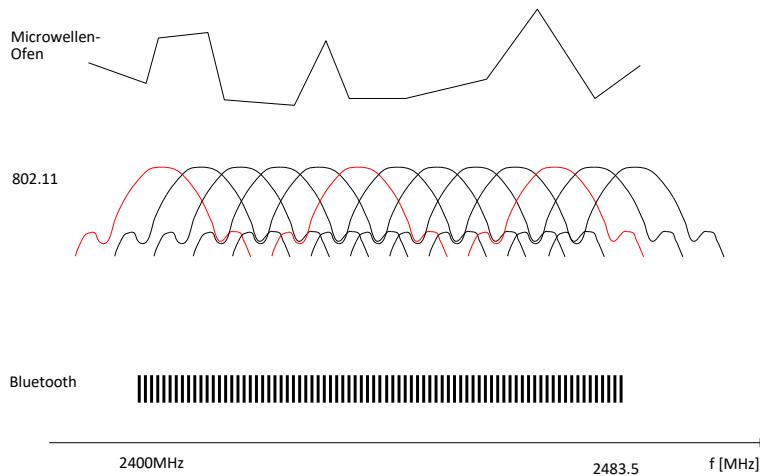


Abbildung 14: Der 2,4 GHz-Bereich

Bluetooth 1600 mal in der Sekunde gewechselt.

Das für WLANs genutzte ISM-Band im 2,4 GHz-Band hat viel Konkurrenz. Es muss sich gegen medizinische Geräte, Bluetooth, schnurlose Telefone, Bewegungsmelder so wie auch z. B. Mikrowellenöfen durchsetzen.

Während die industriellen Mikrowellenöfen den gesamten Bereich abdecken zeigen Mikrowellenöfen in privaten Haushalten nur Störungen im Kanal 9 und 10 bei 2,455GHz.

Für Bluetooth stehen 79 Kanäle zur Verfügung. Diese Kanäle werden von

In diesem Bereich sind die Standards IEEE-802.11/b/g/n/ax angesiedelt. Vor allem im Small Office / Home Office Bereich (SOHO-Bereich) sind hier Produkte zu finden. Die Aufteilung des 2,4GHz-Bandes in Kanäle ist in den Regionen unterschiedlich organisiert. Die Tabelle 2 zeigt eine Übersicht der Kanalverfügbarkeit in den Regionen.

Tabelle 2: Zuordnung der Kanäle im 2,4GHz-Band je Region

Kanal	Center Frequency [GHz]	ETSI (Europa)	Japan	FCC (USA)	Israel
1	2,412	100mW	100mW	1W	verboten
2	2,417	100mW	100mW	1W	verboten
3	2,422	100mW	100mW	1W	*
4	2,427	100mW	100mW	1W	*
5	2,432	100mW	100mW	1W	*
6	2,437	100mW	100mW	1W	*
7	2,442	100mW	100mW	1W	*
8	2,447	100mW	100mW	1W	*
9	2,452	100mW	100mW	1W	*
10	2,457	100mW	100mW	1W	verboten
11	2,462	100mW	100mW	1W	verboten
12	2,467	100mW	100mW	verboten	verboten
13	2,472	100mW	100mW	verboten	verboten
14	2,484	verboten	verboten	verboten	verboten

In Japan und fast allen Ländern Europas sind als Sendeleistung 100mW zugelassen. In den USA ist 1W zugelassen. Dafür gibt es in den USA jedoch zwei Kanäle weniger!

Im 2,4GHz-Band waren für die ersten Standards nur Kanäle mit einer Bandbreite von 20 MHz vorgesehen. In der Abbildung 15 ist ein solches Band mit seiner sende-seitigen Spektralmaske dargestellt.

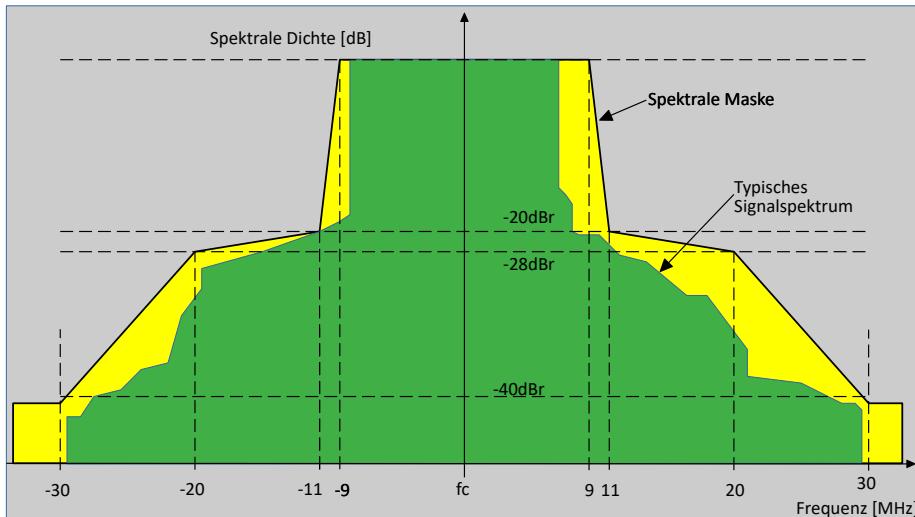


Abbildung 15: Spektralmaske für einen Sender mit 20MHz Bandbreite im 2,4GHz-Band

Der Kanalabstand ist bei WLANs (mit Ausnahme von Kanal 14) auf 5MHz festgelegt. Da die beim WLAN genutzten Kanäle jedoch mindestens 20MHz breit sind, gibt es Überlappungen. Diese wirken sich in den unterschiedlichen Regionen unterschiedlich aus.

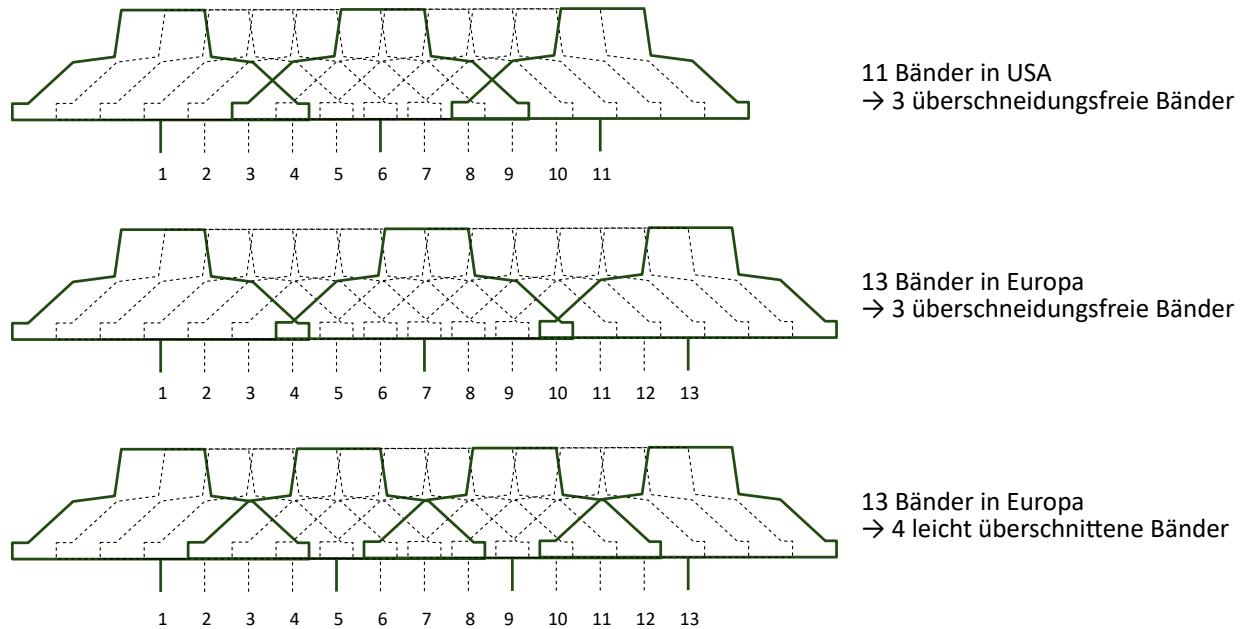


Abbildung 16: Regionale Unterschiede bei den Frequenzbändern und die Konsequenzen

Die Überschneidungen sind bei geringem Abstand der WLAN-Teilnehmer nicht problematisch. Bei größeren Abständen wird es schwierig, vor allem höhere Datenraten, aufrecht zu halten.

3.7.2 - Das 5 GHz-Band

Im 5 GHz-Band sind noch weitere Nutzer wie Wetterradaranlagen, Satelliten-Verbindungen und Flug-Navigationsdienste unterwegs. Vor allem im Freien gelten sie als Primärnutzer und haben Vorrang bei der Belegung des Frequenzbandes. Die WLAN-Standards gelten als Sekundärnutzer und haben sich den Gegebenheiten in der entsprechenden Umgebung anzupassen. Dies bedeutet auch drastische Einschränkungen bei der Sendeleistung.

Als WLAN-Standards sind die Standards IEEE-802.11a/h/n/ac/ax tätig. Weltweit sind die Kanäle und Sendeleistungen unterschiedlich zugelassen. Die RegTP (Regulierungsbehörde für Telekommunikation und Post) und die ECC (Electronic Communication Commission) der europäischen Behörde CEPT (Conference Européenne des Administration des Postes et des Télécommunications) haben die in Tabelle 3 gezeigten Frequenzen freigegeben.

Damit existieren im unteren Bereich 19 Kanäle zur Verwendung bei WLANs. In Deutschland gibt es noch folgende Einschränkungen:

- Kanäle 36 – 64: Sendeleistung im Innenbereich bis 200mW ohne TPC und DFS (*)
- Kanäle 100 – 140: Sendeleistung bis 1W im Außenbereich nur bei Verwendung von DFS (Dynamic Frequency Select) und TPC (Transmission Power Control) (**)
- Kanäle 155 – 171: sind für „Broadband Fixed Wireless Access“ (BFWA) für gewerbliche Zwecke freigegeben und damit meldepflichtig. Hier kann bis zu 4W Sendeleistung verwendet werden. Auf Basis der Short Range Device (SRD) Zulassung darf in Europa im Bereich der Kanäle 149 bis 165) (5725 bis 5850 MHz) mit bis zu 25mW gesendet werden.(***)

Tabelle 3: Bänder, Frequenzen und Sendeleistung je Region

Kanal	Mitten-Frequenz [GHz]	Fast alle Länder der Welt	USA Australien	China Singapur Israel
36	5,180	200mW*	erlaubt	erlaubt
40	5,200	200mW*	erlaubt	erlaubt
44	5,220	200mW*	erlaubt	erlaubt
48	5,240	200mW*	erlaubt	erlaubt
52	5,260	200mW*	erlaubt	erlaubt
56	5,280	200mW*	erlaubt	erlaubt
60	5,300	200mW*	erlaubt	erlaubt
64	5,320	200mW*	erlaubt	erlaubt
100	5,500	1W**	erlaubt	verboten
104	5,520	1W**	erlaubt	verboten
108	5,540	1W**	erlaubt	verboten
112	5,560	1W**	erlaubt	verboten
116	5,580	1W**	erlaubt	verboten
120	5,600	1W**	verboten	verboten
124	5,720	1W**	verboten	verboten
128	5,640	1W**	verboten	verboten
132	5,660	1W**	erlaubt	verboten
136	5,680	1W**	erlaubt	verboten
140	5,700	1W**	erlaubt	verboten

Fortsetzung: nächste Seite

Kanal	Mitten-Frequenz [GHz]	Europa	USA China	Japan Türkei Israel
149	5,745	25mW***	erlaubt	verboten
153	5,765	25mW***	erlaubt	verboten
157	5,785	25mW***	erlaubt	verboten
161	5,805	25mW***	erlaubt	verboten
165	5,825	25mW***	erlaubt	verboten

Quelle: [Wireless Local Area Network – Wikipedia](#)

Die Sendeleistung von bis zu 200 mW, wirkt von der Reichweite her ähnlich der der Sendeleistung von IEEE 802.11b-Netzen aus. Damit ist eine Reichweite von ca. 100 m möglich. Bei der Zählung der Kanäle hat man hier bereits jeweils 4 Kanäle zusammengefasst um die Mindestbandbreite von 20MHz zu berücksichtigen.

Die Spektralmaske sieht für die 5GHz-Variante bis auf die dBr-Werte wie für die 2,4GHz-Variante aus.

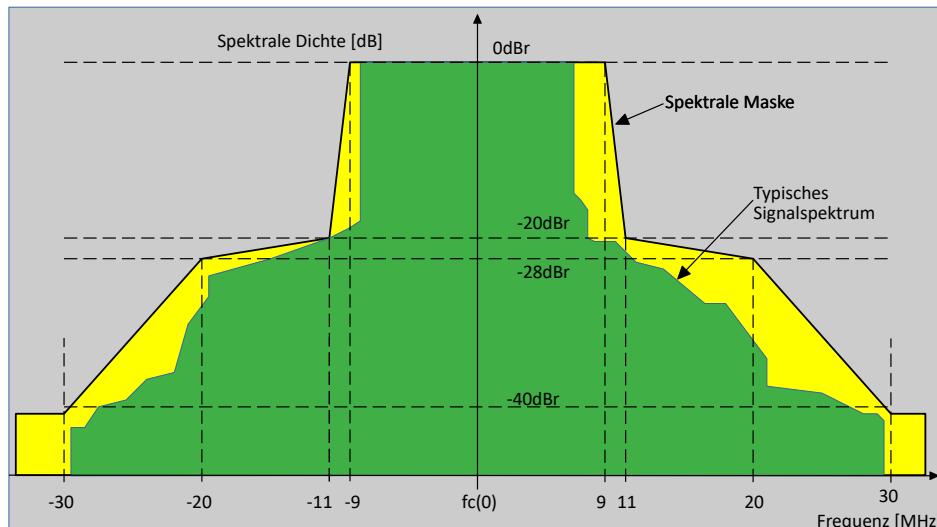


Abbildung 17: Spektralmaske für einen Sender mit 20MHz Bandbreite im 5GHz-Band

Untere und mittlere U-NII-Bänder:
8 Träger mit einem Kanalabstand von 20 MHz

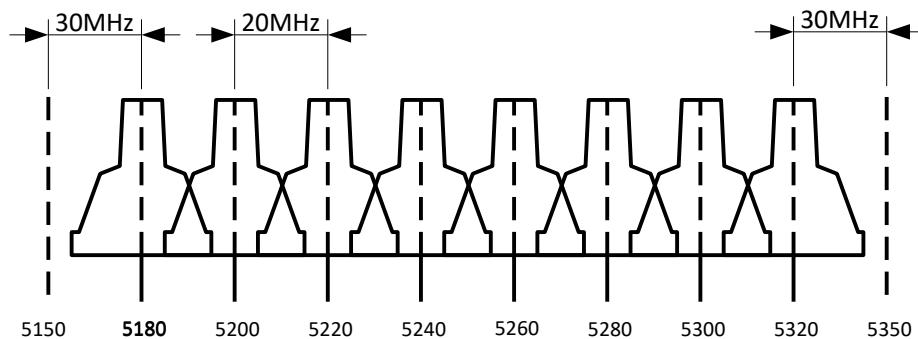


Abbildung 18: Überlappungsfreie Kanäle im 5GHz-Band

3.7.3 - Das 6 GHz-Band

Die US-amerikanische Regulierungsbehörde Federal Communications Commission (FCC) hat am 24. April 2020 weitere Frequenzbänder im 6GHz-Bereich freigegeben. Dabei handelt es sich um Bänder in der so genannten Unlicensed National Infomation Infrastructure (U-NII) :

- 5.925 – 6.425 MHz (U-NII-5)
- 6.425 – 6.525 MHz (U-NII-6)
- 6.525 – 6.875 MHz (U-NII-7)
- 6.875 – 7.125 MHz (U-NII-8)

Damit kann eine Bandbreite von 1200 MHz für WLAN genutzt werden, womit mit IEEE-802.11ax (Wi-Fi 6) eine theoretische Datenübertragungsrate von 60GBit/s auf kurze Distanzen möglich wird. Geräte, welche diese Bänder abdecken werden unter dem Begriff Wi-Fi 6E vermarktet.

In den USA kann ein AP im Freien in den U-NII-Bändern 7 und 8 mit einer maximalen Sendeleistung von bis zu 4 Watt (EIRP) senden. Stationen dürfen mit maximal 1 Watt senden. Das gilt übrigens innerhalb von Gebäuden auch für APs.

In Europa sind diese Frequenzen noch nicht freigegeben, weshalb hier Wi-Fi 6E nur ein Marketing-Spruch ist. Immerhin beschäftigt sich die ETSI seit Oktober 2018 bzw. März 2019 mit diesen Frequenzbereichen.

3.7.4 - Das 60 GHz-Band

Für die Standards IEEE-802.11ad und IEEE-802.11ay wurden im 60 GHz-Band ein 2000 MHz breites Band freigegeben. Damit stehen hier 4 Kanäle zur Verfügung. Siehe: Tabelle 4

Tabelle 4: Kanäle und Frequenzen im 60GHz-Band

Kanal	Mittenfrequenz [GHz]
1	58,320
2	60,480
3	62,640
4	65,880

3.8 - Reichweiten

Elementare Eigenschaften von Funk-Verbindungen sind Reichweiten-Probleme. Die Empfangsleistung nimmt quadratisch mit dem Abstand zum Sender ab und ist somit begrenzt. Dieses Verhalten ist zudem noch frequenzabhängig. Je höher die Frequenz ist, desto stärker ist die Abschwächung mit größerer Entfernung. Weitere Informationen zum Thema gibt es im Kapitel Freiraumdämpfung auf Seite 213.

Vergleicht man die Reichweiten zwischen IEEE-802.11a (5 GHz-Band) und IEEE-802.11b (2,4 GHz-Band), bei ähnlichen Sendeleistungen, kommt man zu dem Schluss, dass IEEE-802.11b zwar diverse Probleme hat, jedoch etwas größere Reichweiten aufgrund der geringeren Dämpfung bietet.

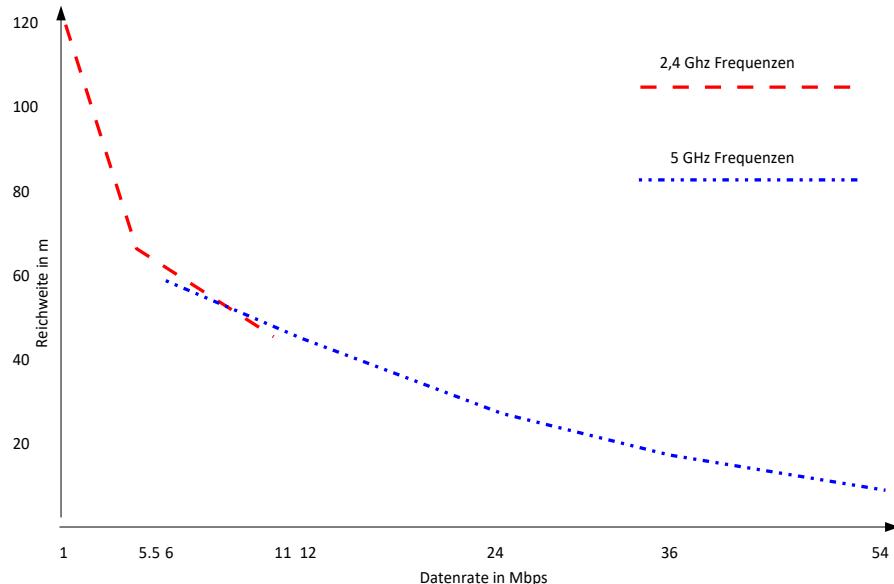


Abbildung 19: WLAN – Reichweiten-Vergleich

Dies wird durch die Bebauung, unterschiedliche Antennen, sowie unterschiedliche Sendeleistungen jedoch wieder relativiert. In der obigen Darstellung ist die Sendeleistung bei 5 GHz nur 60 mW. Dies bedeutet, dass bei entsprechender Erhöhung der Sendeleistung auch größere Reichweiten erzielbar sind.

Im Rahmen der bei IEEE-802.11h beschriebenen Zusatzfeatures TPC und DFS kann die Sendeleistung bis auf 1 W gesteigert werden.

3.9 - Multiplexverfahren

In der obigen Tabelle ist zu sehen, dass für die unterschiedlichen Anwendungen unterschiedliche Frequenzbereiche vergeben sind. Wenn nun mehrere Nutzer gleichzeitig ein Funknetz benutzen wollen, kommen wiederum neue Probleme ins Spiel. Da Funk ein „Shared Medium“ ist, können sich die Signale auf einer Frequenz überlagern und gegenseitig beeinflussen (Interferenz). Um nun trotzdem alle Nutzer über Funk gleichberechtigt kommunizieren zu lassen, müssen Regelungsmechanismen, wie Multiplexing, den Kanalzugriff und Kanaluweisung, den Verkehr regeln.

Beim Multiplexing sind zwei Ausprägungen interessant:

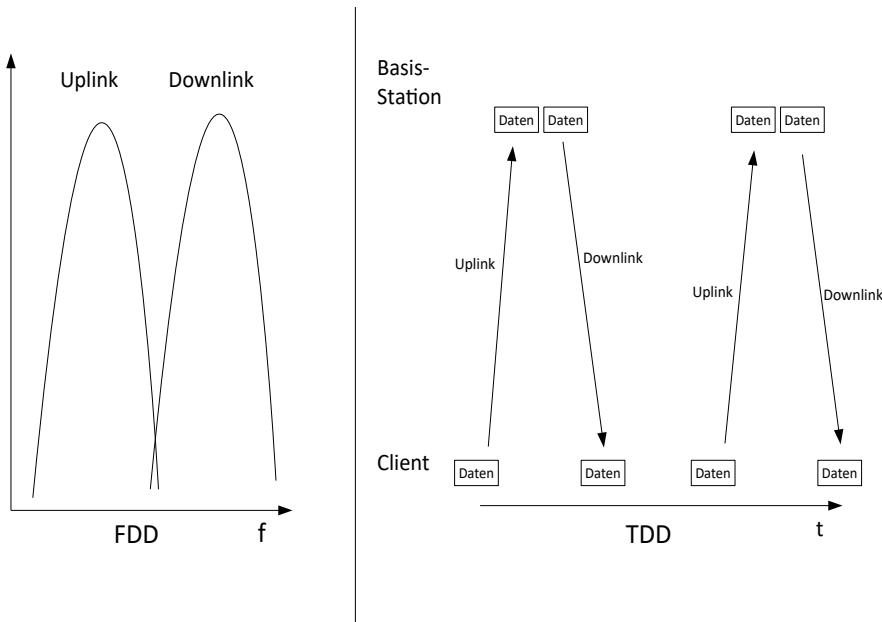


Abbildung 20: FDD / TDD

Zwischen **zwei** Kommunikationspartnern kann eine Trennung zwischen Uplink und Downlink erfolgen. Dies ermöglicht eine Kommunikation in 2 Richtungen quasi gleichzeitig.

Hierbei sind die folgenden Verfahren gängig:

- FDD (Frequency Division Duplex)

Jeder Kanal bekommt dabei einen eigenen Frequenzbereich.

Dies erhöht den Bandbreitenbedarf.

- TDD (Time Division Duplex)

Jeder Teilnehmer bekommt zum Senden innerhalb eines Zeit-Rahmens einen Zeitschlitz zugewiesen.

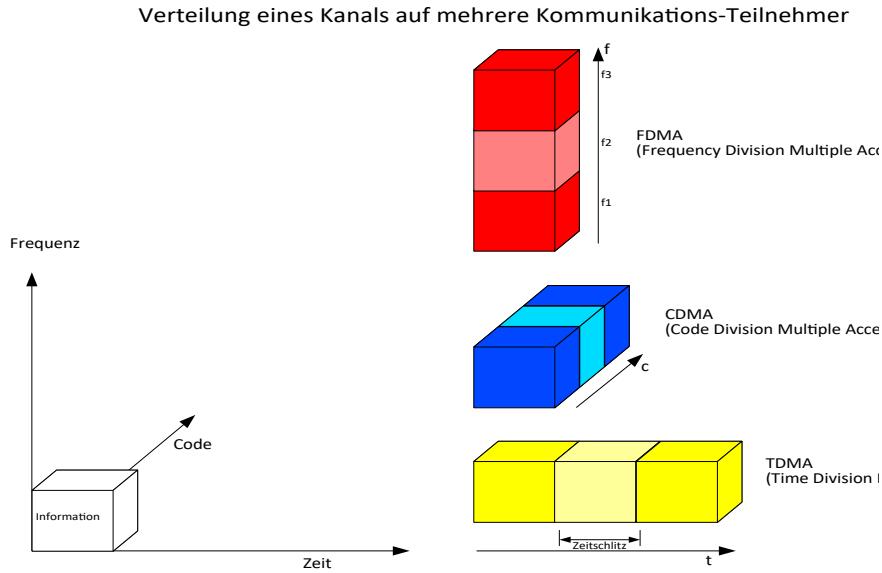


Abbildung 21: Multiplexverfahren

Sollen **mehr als zwei** Kommunikations-Teilnehmern gleichberechtigt kommunizieren können, gibt es die Möglichkeiten, die vom Message-Cube abgeleitet werden können.

Möglichkeiten des Multiplexing.

- ➊ **FDMA (Frequency Division Multiple Access)**
Beruht auf der Verwendung von FDM (Frequency Division Multiplex). Dabei werden den Übertragungskanälen für die Rauer der Übertragung die Frequenzen zugewiesen.
- ➋ **TDMA (Time Division Multiple Access)**
Verwendung von Zeitschlitten, in denen jeweils ein Gerät sendet.
- ➌ **CDMA (Code Division Multiple Access)**
Verwendung von unterschiedlichen Codierungs-Verfahren
- ➍ **SDMA (Space Division Multiple Access)**
Räumliche Aufteilung der Kanäle über unterschiedliche Sendemasten

Mischformen aus den Formen sind sowohl möglich als auch sinnvoll.

3.9.1 - SDMA

Beim Space Division Multiple Access handelt es sich um ein Raum-Multiplex-Verfahren. Die Sendemasten sind hierbei räumlich voneinander getrennt. Damit kann die Kommunikation nur in einem bestimmten regionalen Bereich erfolgen.

Bei Nutzung von nur einer Frequenz ist ein Schutzabstand notwendig. Oder jeder Sender würde eine eigene Frequenz benötigen. Deshalb ist das Raum-Multiplex-Verfahren nur in Kombination mit anderen Multiplexverfahren sinnvoll.

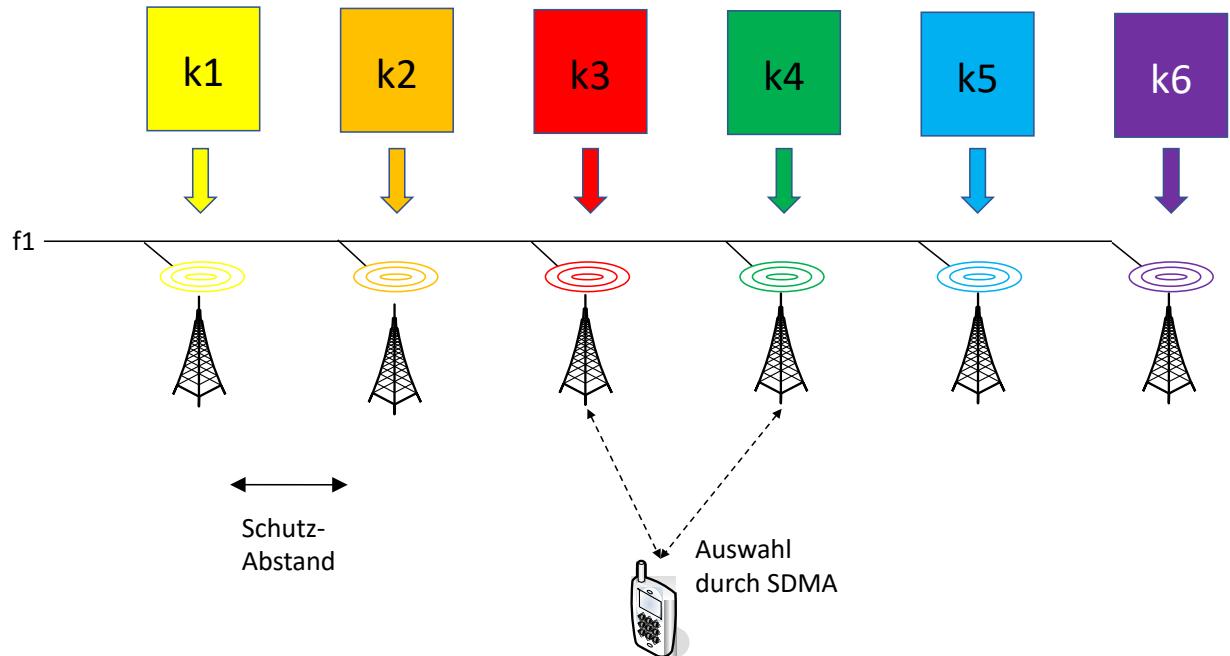


Abbildung 22: SDMA

Da Mobilfunknetze in Zellen aufgeteilt werden und die Anzahl der verfügbaren Frequenzbereiche endlich ist, muss ein Wiederverwendungsabstand eingeführt werden.

Die Reichweite von Funkzellen ist begrenzt. Deshalb müssen mehrere Funkzellen aneinander gelegt werden um größere Flächen abzudecken. Dies ist möglich, führt jedoch zu Problemen, wenn die aneinander liegenden Funkzellen das gleiche Frequenzband benutzen. Durch die Interferenzen, die durch die Überlagerung der Funkwellen entstehen kann der Funkverkehr stark beeinträchtigt werden. Deshalb müssen aneinander liegende Funkzellen mit unterschiedlichen Frequenzen arbeiten. Da die Kanalanzahl jedoch begrenzt ist, tritt hier der Begriff des Wiederverwendungsabstands auf. Er ist ein Maß dafür, ab welchem Abstand der gleiche Kanal nochmals verwendet werden kann.

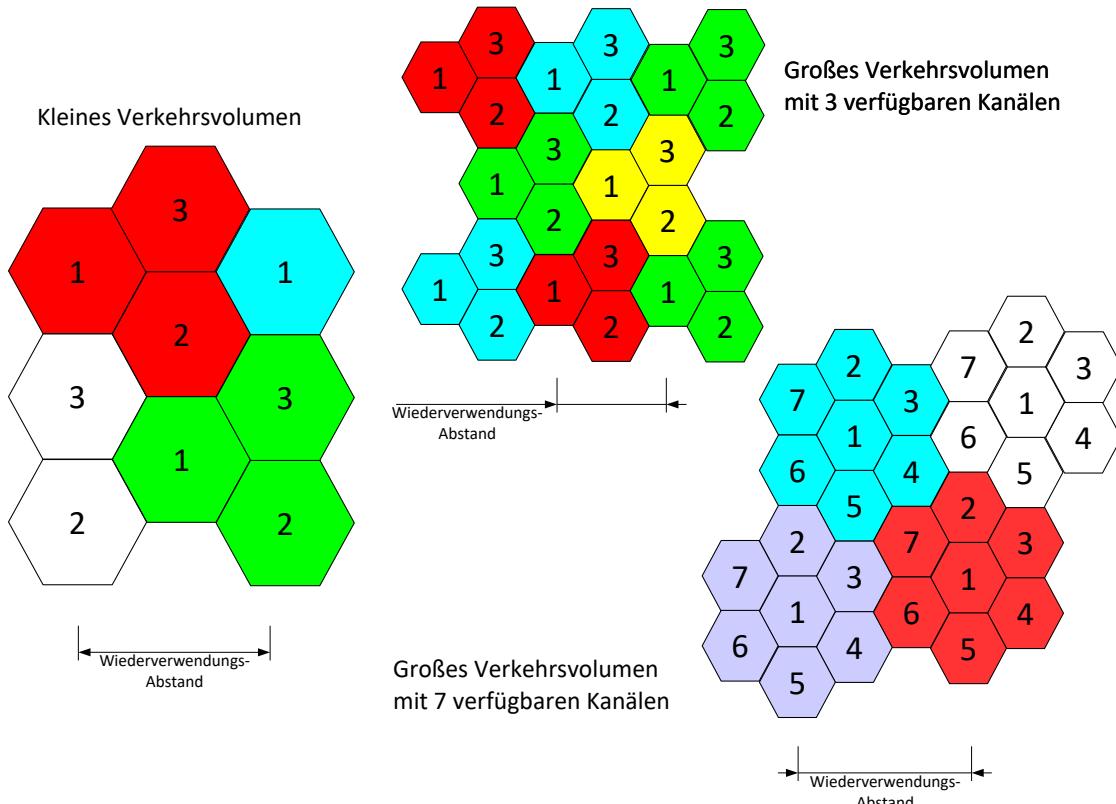


Abbildung 23: Wiederverwendungsabstand

Die flächendeckende Abdeckung muss auch berücksichtigen wie viele mobile Clients mit der Basisstation kommunizieren wollen.

Sind zu viele Clients an einer Basisstation assoziiert, sinkt die Datenrate der einzelnen Verbindungen entsprechend ab, da es sich bei Funk um ein Shared Media handelt, das sich alle teilen müssen.

Hier kann nur durch Verkleinerung der Funkzellen eine Erhöhung der Anzahl der Stationen entgegengewirkt werden. Entsprechend muss die Sendeleistung der APs angepasst werden.

3.9.2 - FDMA

Unterschiedliche Frequenzen werden z. B. beim Rundfunk eingesetzt. Jeder Sender hat seine eigene, ihm zugewiesene, feste Frequenz.

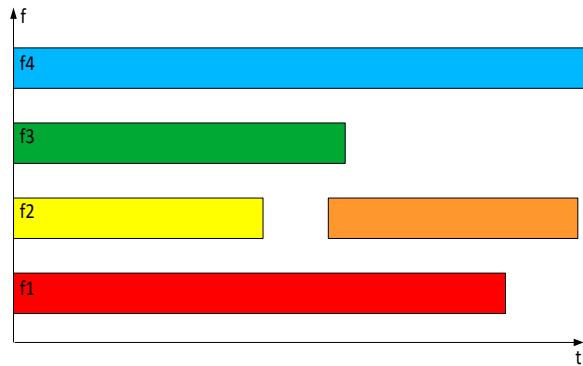


Abbildung 24: FDMA

Diese Vorgehensweise wird typischerweise in analogen Funknetzen angewendet. Die Bandbreite pro Kanal sowie die Anzahl der Frequenzbänder sind hierbei die begrenzenden Faktoren für die Datenübertragungsrate. Jeder Teilnehmer belegt den Kanal so lange wie er senden möchte. Dies kann zu langen Wartezeiten führen, wenn alle Kanäle belegt sind. Zusätzlich benötigt jeder Kanal einen eigenen Transceiver in der Basisstation. Dadurch ist diese Technik teuer.

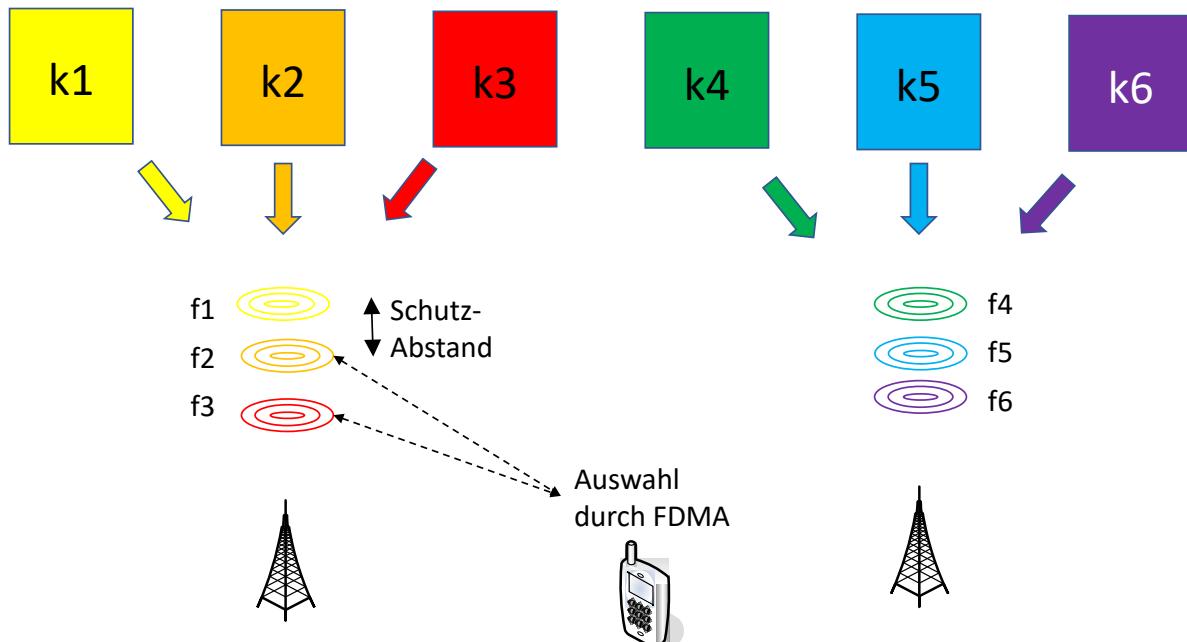


Abbildung 25: FDMA-Kanalauswahl

3.9.3 - TDMA

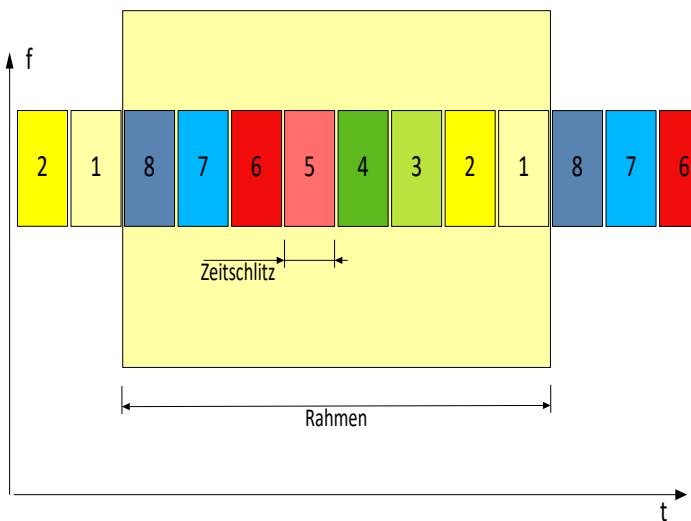


Abbildung 26: TDMA

TDMA beruht auf TDM (Time Division Multiplexing). Das Übertragungsmedium wird einem Übertragungskanal eine bestimmte Zeit zugewiesen. Hierbei wird nur auf einer Frequenz gesendet.

Innerhalb eines Zeit-Rahmens hat jeder Teilnehmer einen Zeitschlitz, den er für das Senden nutzen kann. Bandbreite, Rahmendauer, Anzahl der Zeitschlüsse pro Rahmen sowie die Zeitschlitzdauer sind die begrenzenden Faktoren für die Datenübertragungsrate.

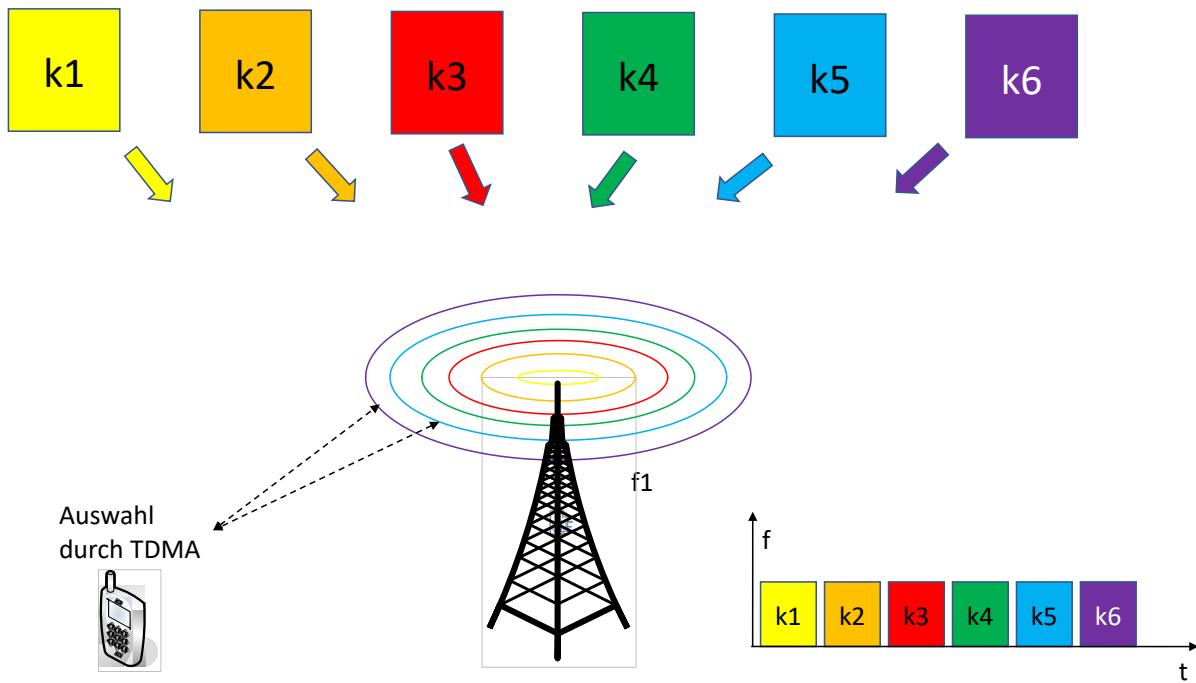


Abbildung 27: TDMA-Kanalauswahl

3.9.4 - CDMA

CDMA beruht auf dem Code Division Multiplexing (CDM).

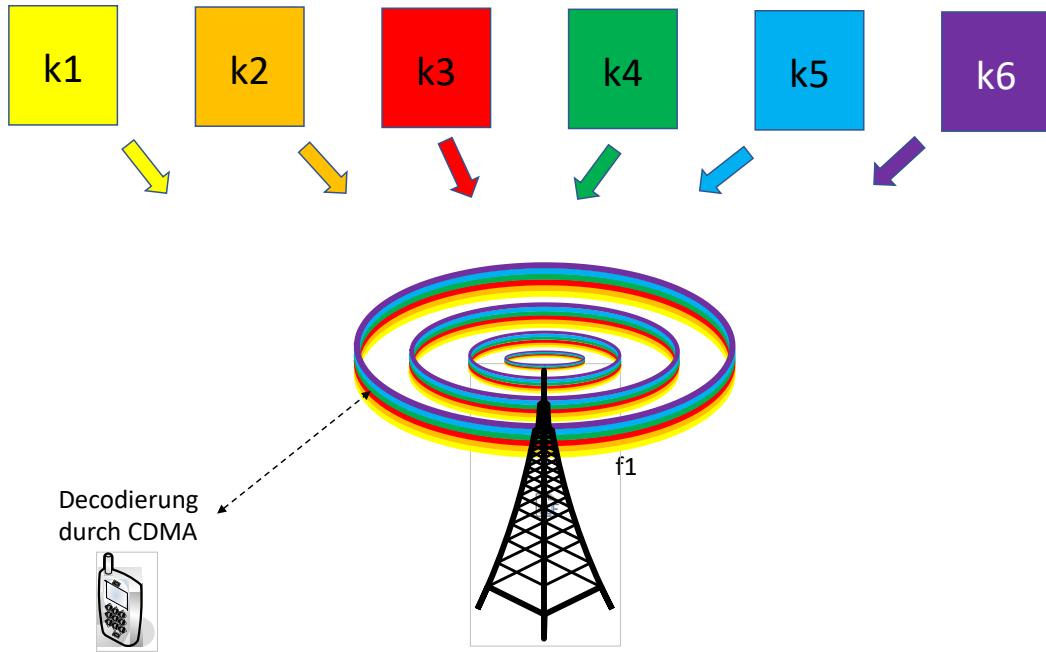


Abbildung 28: CDMA

Dabei wird jedem Kanal ein eigener Code zugewiesen und es kann auf der selben Frequenz zur selben Zeit gesendet werden. Durch die Entwicklung hochintegrierter Schaltungen wurde die Anwendung realisierbar. Durch die Anwendung des Bandspreizverfahrens ergibt sich eine gute Abhörsicherheit sowie eine geringe Störempfindlichkeit was allerdings den Aufwand für die Signaltrennung auf der Empfängerseite erhöht. Zwischen den Teilnehmern ist eine exakte Synchronisation erforderlich. Der Code des Senders muss dem Empfänger bekannt sein.

Jede Bitübertragungszeit wird in m kurze Intervalle namens Chips unterteilt.

Jede Station bekommt einen eindeutigen m -Bit-Code zugewiesen der auch Chipfolge genannt wird.

Wichtig ist, dass die Chipfolgen paarweise orthogonal sind. Das bedeutet, dass das normalisierte innere Produkt von zwei beliebigen Chipfolgen S und T (geschrieben als $S \bullet T$) 0 ist.

$$S \bullet T \equiv \frac{1}{m} \sum_{i=1}^m S_i T_i \quad (1)$$

Orthogonale Chipfolgen können mit einer Methode namens Walsh Code erzeugt werden.

Funktions-Beispiel:

Bei einer Versammlung von Personen können die Kommunikationspartner nahe beisammen stehen. Jeder spricht jeder nur so laut, dass der Partner ihn verstehen kann. Jede Kommunikationsbeziehung wird in einer anderen Sprache (einem anderen Code) durchgeführt. Dadurch sind die Kommunikationskanäle voneinander getrennt, denn andere Sprachen können nicht verstanden werden. Andere Sprachen werden nur als Hintergrundrauschen wahrgenommen. Problematisch dabei sind verwandte Sprachen mit geringen Unterschieden. Dabei ist dann der Störabstand zu gering. (z. B. Norwegisch und Schwedisch)

Umsetzungsbeispiel

- ➊ Sender A sendet ein Bit (A_d)
 - ◆ Daten: $A_d = 1$
 - ◆ Verwendeter Schlüssel $A_k = 010011$ (setze: „0“ = -1, „1“ = +1) = (-1, +1, -1, -1, +1, +1)
 - ◆ Resultierendes Sendesignal $A_s = A_d * A_k = (-1, +1, -1, -1, +1, +1)$ (d. h. A_k bleibt erhalten)

- ➋ Sender B sendet ein Bit (B_d)
 - ◆ Daten: $B_d = 0$
 - ◆ Verwendeter Schlüssel $B_k = 110101$ (setze: „0“ = -1, „1“ = +1) = (+1, +1, -1, +1, -1, +1)
 - ◆ Resultierendes Sendesignal $B_s = B_d * B_k = (-1, -1, +1, -1, +1, -1)$ (d. h. B_k wird negiert)

Beide Sendesignale werden additiv überlagert und über die Luft übertragen

- ➌ $C = A_s + B_s = (-2, 0, 0, -2, +2, 0)$

Empfänger C will Sender A hören und wendet dessen Schlüssel A_k bitweise an (inneres Produkt)

$$\text{➍ } A_s = C * A_k = (2, +0 + 0 + 2 + 2 + 0) = 6$$

Da das Ergebnis > 0 ist, wird das empfangene Bit = **1**

Empfänger D will Sender B hören und wendet dessen Schlüssel B_k bitweise an (inneres Produkt)

$$\text{➎ } B_s = C * B_k = -2, +0 + 0 - 2 - 2 + 0 = -6$$

Da das Ergebnis < 0 ist, wird das empfangene Bit = **0**

3.10 - Modulationsarten

Die bei der Funkübertragung genutzten Träger sind elektromagnetische Wellen. Sie können mit der folgenden Formel beschrieben werden:

$$S(t) = a(t) \cos(\omega_0 t + \varphi(t)) \quad (2)$$

Damit sind für eine Modulation folgende Variablen gegeben:

- Amplitude a
- Frequenz f = 1 / t
- Phase ϕ

Bei den WLANs wird im allgemeinen eine Mischung aus Amplitudenmodulation und Phasenmodulation verwendet.

Will man eine Modulation der Phase durchführen, kann man z. B. für die Kodierung einer „0“ den Phasenwinkel 0 nehmen und für die Kodierung einer „1“ den Phasenwinkel 180° dies führt zur Binary Phase Shift Keying (BPSK)

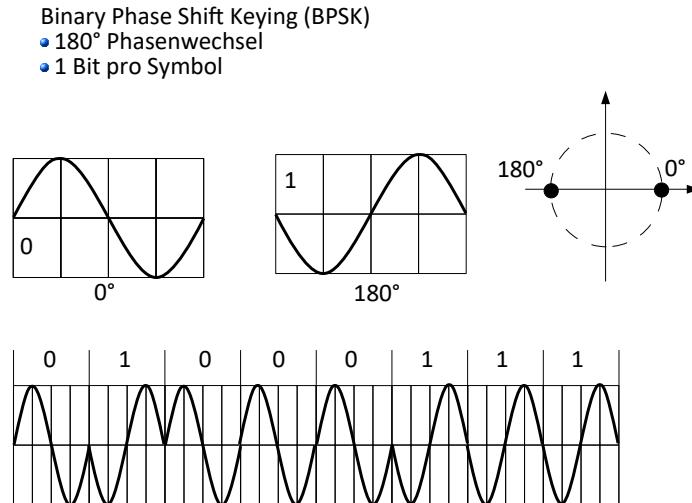


Abbildung 29: Modulationsart BPSK

Hierbei wechselt sich der Phasenwinkel um 180°, wenn ein Übergang von einer 1 auf eine Null oder umgekehrt übertragen wird.

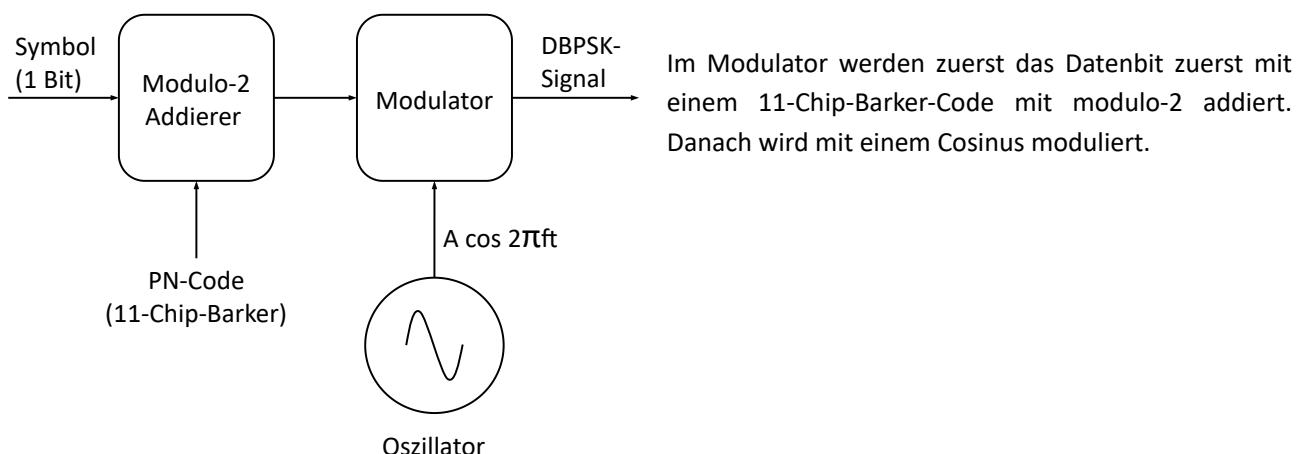


Abbildung 30: BPSK-Modulator

3.10.1 - QPSK

Quadrature Phase Shift Keying (QPSK)
 • 90° Phasenwechsel
 • 2 Bit pro Symbol

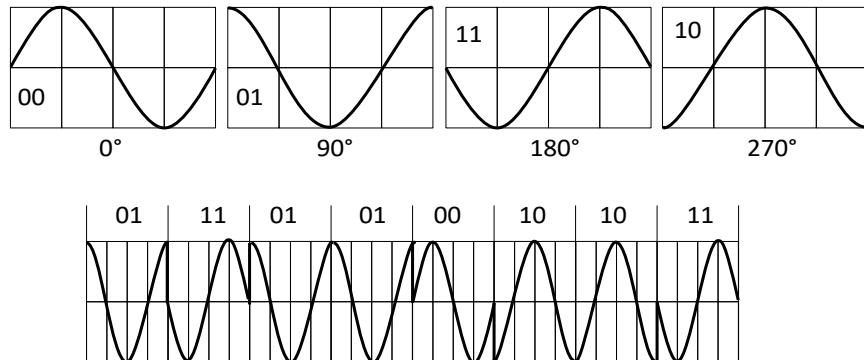
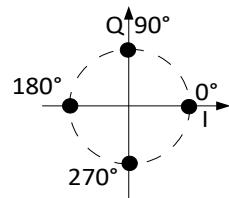
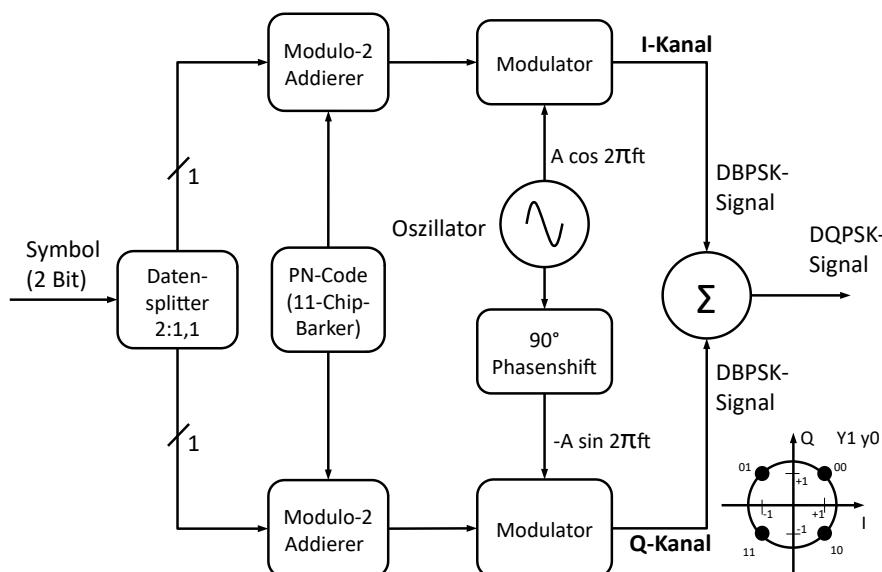


Abbildung 31: Modulationsart QPSK

Die Anzahl der verfügbaren Symbole / Punkte, in dieser komplexen Ebene, wird mit deren Zahl ausgedrückt. Beispielsweise in der Angabe 4-QAM für eine QAM mit einem Umfang von 4 Symbolen. In diesem Fall können pro Symbol 2 Bit übertragen werden.



Im Modulator werden zuerst die 2 Datenbits der Symbole auf 2 Wege aufgeteilt, die getrennt mit einem 11-Chip-Barker-Code mit modulo-2 addiert werden.

Danach werden sie einmal mit einem Sinus und das andere Mal mit einem Cosinus moduliert.

Nach der Modulation werden die beiden DBPSK-Signale addiert bevor sie auf die Antenne gegeben werden.

Abbildung 32: QPSK-Modulator

3.10.2 - CCK

Sobald mehr als 2 Bits zu modulieren sind wird das Complementary Code Keying (CCK) eingesetzt. Hierbei wird bei der Aufteilung der Bits am Anfang in 3 Teile aufgeteilt. Jeweils ein Bit für die Erstellung des I-Kanals für den Realteil und den Q-Kanal für den Imaginärteil. Die restlichen Bits (in Abbildung 33 sind das 6 Bits) werden für die Auswahl eines komplexen Codes, bestehend aus einem Realteil und einem Imaginärteil, herangezogen. Der Rest verläuft dann wie bei der QPSK.

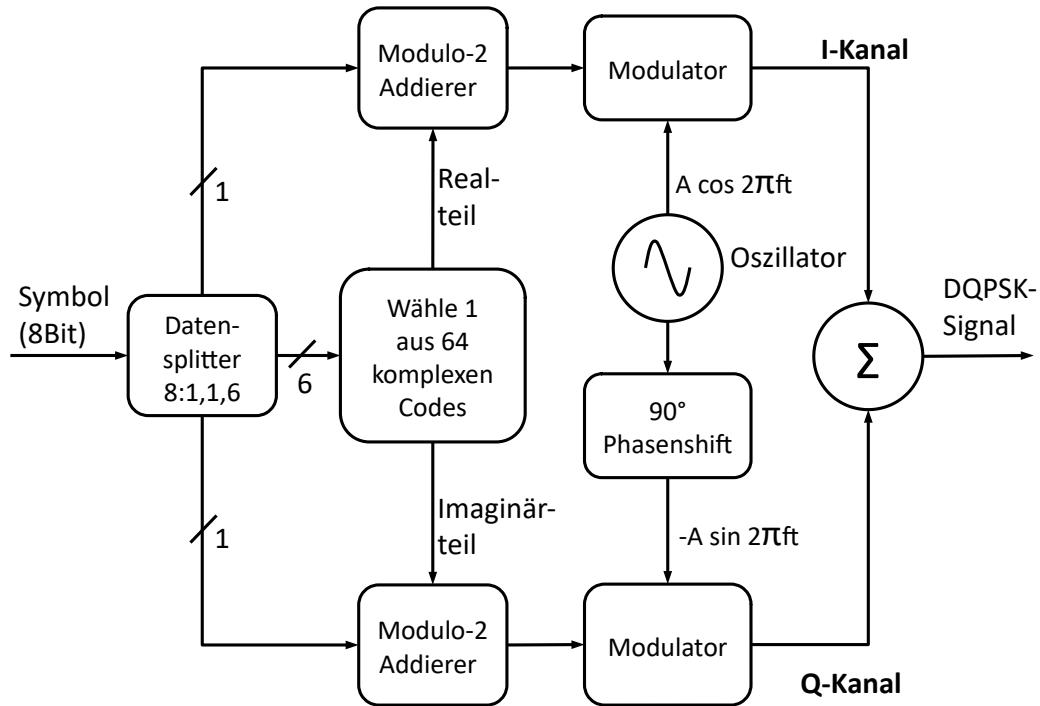


Abbildung 33: CCK-Sendestufe

Dieses Verfahren wird bei IEEE-802.11g angewendet.

3.10.3 - QAM-Modulation

Ein anderer Ansatz um 2 und mehr Bits pro Daten-Symbol zu übertragen, bietet die Quadrature-Amplitude-Modulation (QAM).

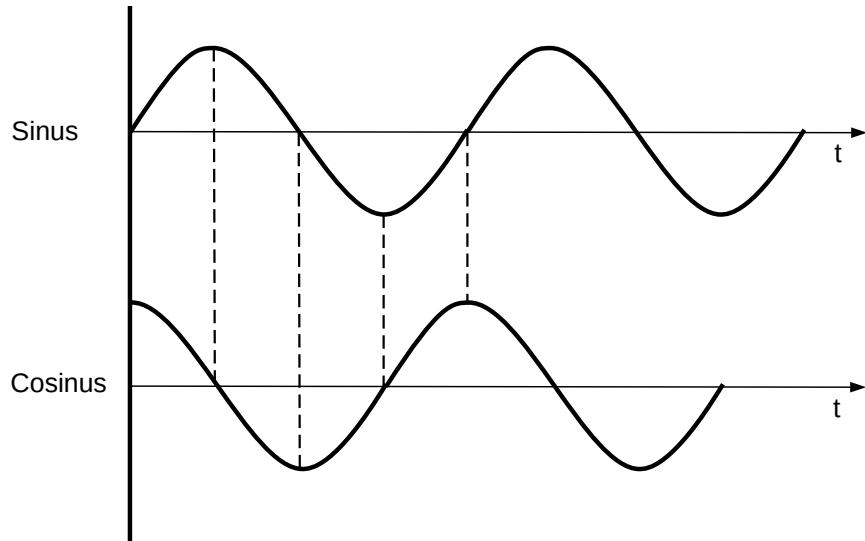


Abbildung 34: QAM Quadrature-Amplitude-Modulation

Dafür stehen die beiden Basisbandsignale I (Inline) und Q (Quadrature) orthogonal aufeinander, was die Darstellung der Symbole in der komplexen Ebene in Form eines Konstellationsdiagramms erlaubt.

Man nutzt zwei um 90° verschobene Schwingungen. Verwendet man eine Sinus- und eine Cosinus-Schwingung fällt auf, dass bei jedem Nulldurchgang die andere Schwingung ein Maximum (positiv oder negativ) hat.

3.10.4 - 16-QAM

Zusätzlich zur Phasenumtastung wurde noch eine Amplitudenumtastung durchgeführt. Beim 16-QAM steigt die Anzahl der Symbole auf 16. Damit lassen sich 4 Bit codieren. Im folgenden Beispiel wurde noch zusätzlich eine Gray-Codierung der Werte vorgenommen. Damit ändert sich bei jedem Übergang zu einem anderen Symbol nur ein Bit. Damit ist der Hamming-Abstand = 1.

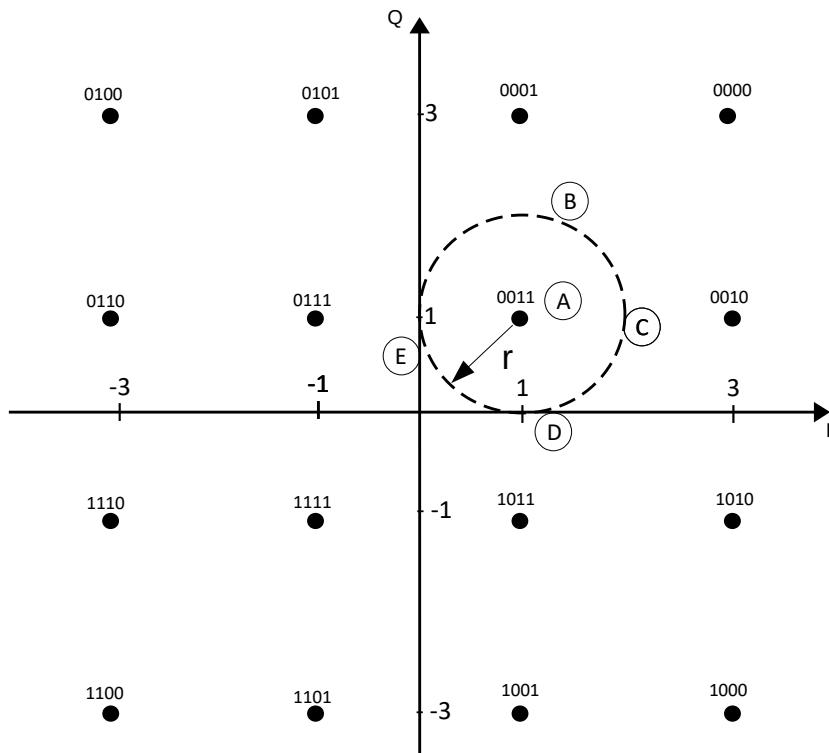


Abbildung 35: 16-QAM Gray-codiert

Im obigen Beispiel sieht man die Auswirkungen falls die Erkennung der Phase und / oder der Amplitude gelingt oder fehlschlägt.

Tabelle 5 Mögliche Bitfehler

Punkt	Decodiert	Bitfehler
A	0011	0
B	0001	1
C	0010	1
D	1011	1
E	0111	1

Innerhalb des Radius r kann das Symbol erkannt werden und es findet kein Bitfehler statt.

In den Fällen B bis E wird immer ein Bitfehler erkannt, da das erkannte Symbol außerhalb des Radius r liegt.

3.10.5 - 64-QAM

Beim 64-QAM-Verfahren werden 6 Bits pro Daten-Symbol transportiert. Die ersten 3 Bits (b_0, b_1 und b_2) werden dazu verwendet um eine von 8 Phasenlagen im I-Kanal darzustellen. Die höherwertigen Bits (b_3, b_4 und b_5) werden dazu verwendet die 8 möglichen Amplituden im Q-Kanal zu adressieren.

Tabelle 6 I- Und Q-Codierung

Bits ($b_0b_1b_2$)	I-Out	Bits ($b_3b_4b_5$)	Q-Out
000	-7	000	-7
001	-5	001	-5
011	-3	011	-3
010	-1	010	-1
110	1	110	1
111	3	111	3
101	5	101	5
100	7	100	7

Ordnet man die Werte einem Signalzustandsdiagramm zu, ergibt sich die folgende Abbildung.

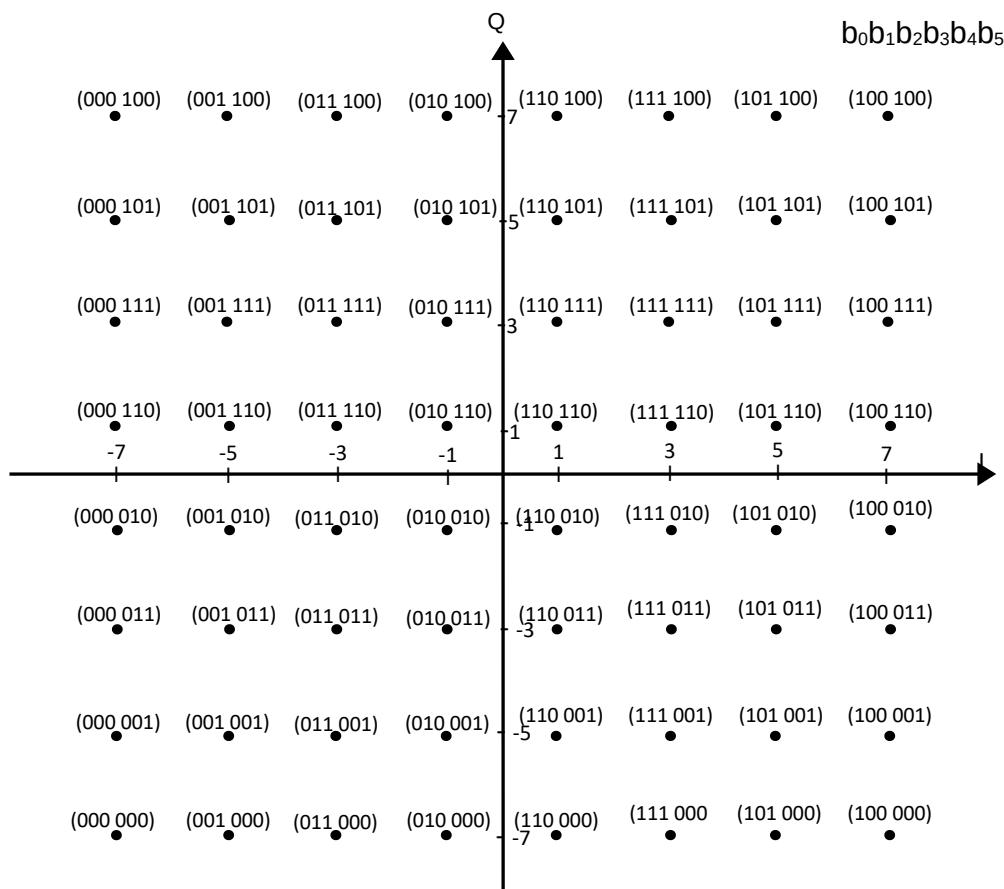
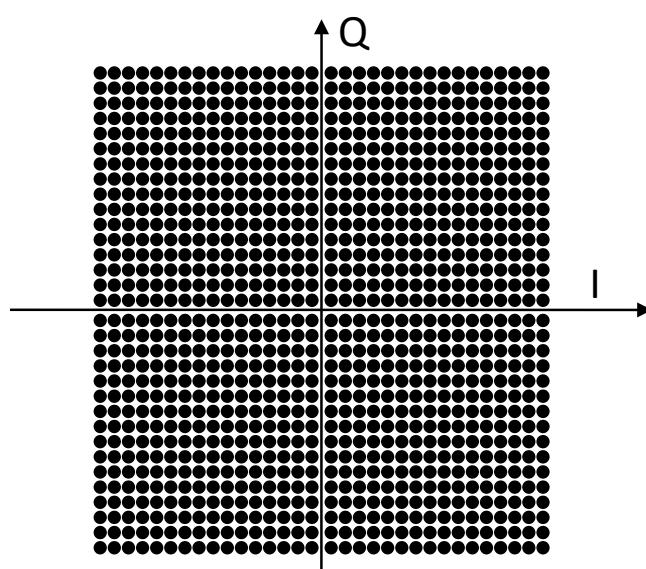


Abbildung 36: 64-QAM

3.10.6 - 1024-QAM

Spinnt man diese Entwicklung weiter landet man bei der Codierung von derzeit maximal 10 Bits bei 1024QAM.

Abbildung 37: 1024-QAM mit 10 Bit pro Codierung

4 - IEEE-802.11 im ISO-7-Schichtenmodell

4.1 - Aufteilung der Ebenen

IEEE-802.11 deckt im ISO-7-Schicht-Modell die unteren 2 Ebenen ab.

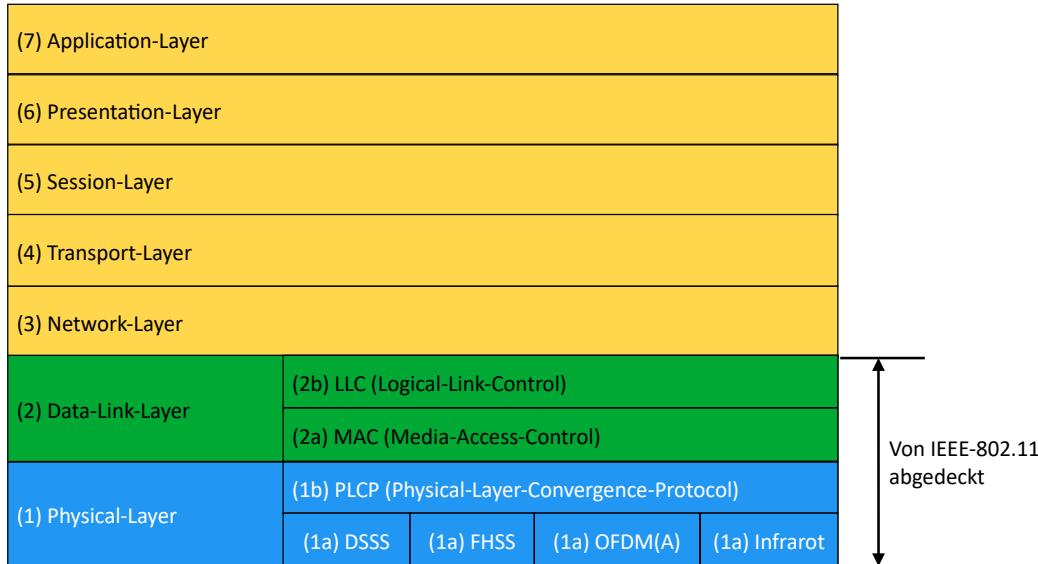


Abbildung 38: WLAN im ISO-7-Schichten-Modell

Die Ebene 1 (PHY-Layer) wird vom Standard komplett abgedeckt. In einer weiteren Unterteilung in 1a und 1b sind die Funktionen folgendermaßen verteilt:

- ➊ 1a
Modulation und Codierung. Hierbei sind die Realisierungen mit Frequency Hopping Spread Spectrum (FHSS) und Infrarot als historisch anzusehen und nicht mehr relevant. Direct Sequence Spread Spectrum (DSSS) hatte sich durchgesetzt. Aktueller Stand ist OFDM(A)
- ➋ 1b
Hier wird die Anpassung der MAC-Layer, die für alle Varianten gleich ist, und der individuellen Physical Media Dependent -Layer (PMD) (1a) vorgenommen. Zusätzlich wird das Clear Channel Assessment (CCA) abgehandelt

Die Ebene 2 (Data-Link-Layer) wird ebenso komplett abgedeckt und kann in 2 weitere Unterebenen aufgeteilt werden.

Die MAC-Ebene (2a) ist für die Adressierung und die Medien-Zugriffsprotokolle zuständig. Hier werden zwei unterschiedliche Verfahren angewendet:

- ➊ Der zentralistischen Ansatz mit der PCF (Point Coordination Function)
- ➋ Der dezentrale Ansatz mit der DCF (Distribute Coordination Function)
Im DCF wird als Basis-Zugriffsfunktion CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) angewendet.

Die Logical Link Control (LLC) - Ebene(2b) deckt Sicherungsmechanismen (Verschlüsselung) ab. Weiterhin wird hier noch die Fragmentierung abgehandelt.

In IEEE-802.11 sind Funktionen enthalten, die bei Ethernet auf den höheren Schichten angesiedelt sind. Dazu gehört:

- Fragmentierung und Reassembling. Bei Ethernet z. B. IP (Ebene 3)
- Paketwiederholungen. Bei Ethernet z. B. TCP (Ebene 4)
- Bestätigungen (z. B. ACK). Bei Ethernet z. B. TCP (Ebene 4)

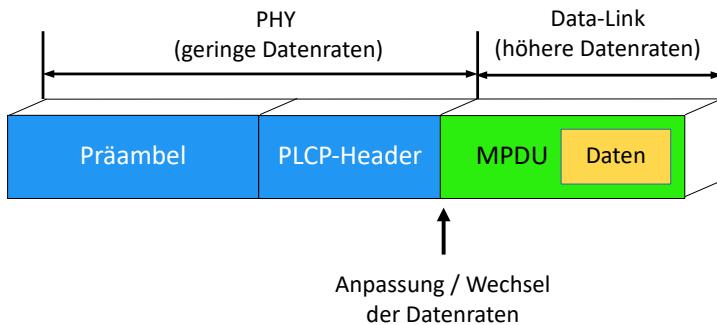


Abbildung 39: Grundsätzlicher Frame-Aufbau auf Ebene 1

Die Daten, die auf unterster Ebene ausgetauscht werden, sind die PPDUs. Das beinhaltet die Präambel, den PLCP-Header und die MPDU.

Die Daten, die auf Ebene 2 ausgetauscht werden, sind demnach die MPDUs.

Auf der Ebene 1 werden nach Abbildung 38 die Präambel und der PLCP-Header ausgetauscht. Die Datenrate für die Präambel ist immer 1 Mbps um sicher zu stellen, dass die Information auf alle Fälle beim Kommunikationspartner verstanden wird. Auch der PLCP-Header wird mit einer geringen Datenrate gesendet. Bei diversen Standards können hier schon Abweichungen zur Präambel-Datenrate auftreten.

Die MPDUs können mit höheren Datenraten übertragen werden. Welche Datenrate zum Zug kommt, wird im PLCP-Header mitgeteilt.

Damit muss zwischen dem PLCP-Header und der MPDU eine Umschaltung der Datenübertragungsrate stattfinden. Hierfür sind in den Standards entsprechende Zeitspannen vorgesehen.

Das Aussehen der Präambel und des PLCP-Headers ist je nach verwendetem Standard unterschiedlich und muss im jedem Einzelfall besonders betrachtet werden.

Dagegen ist der Aufbau der MPDU bei allen Standards gleich.

4.2 - Layer-Management

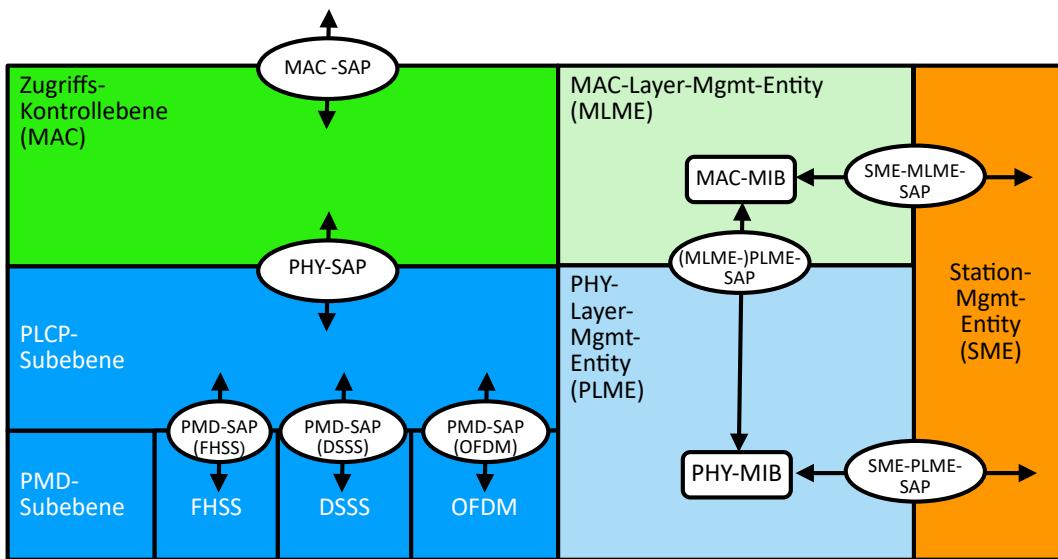


Abbildung 40: Layer-Management

Für jede Station gibt es eine übergeordnete Verwaltungseinheit, die so genannte Station-Management-Entity (SME). Diese Einheit ist unabhängig von den Ebenen in denen die einzelnen Aktivitäten abgehandelt werden.

Bei den einzelnen Ebenen gibt es für die MAC- und die PHY-Ebene Verwaltungseinheiten die so genannten Layer-Management-Entities (LME).

Für die MAC-Ebene gibt es damit eine MAC-Layer-Management-Entity (MLME) und für die Physikalische Ebene gibt es eine Physical-Layer-Management-Entity (PLME).

Informationen werden in den jeweiligen MIBs (Management-Information-Base) verwaltet.

Der Management-Zugriff der SME auf die Ebenen erfolgt waagerecht über SAPs (SME-MLME-SAP und SME-PLME-SAP) mit diversen Primitiven (GET und SET) um die Management-Funktionen durchzuführen. So wird z. B. der Layer-Status von den Management-Einheit verwaltet.

Zwischen MLME und PLME können über den MLME-PLME-SAP mittels den GET- und SET-Primitiven Informationen ausgetauscht werden.

Weiterhin kann eine Ebene einer ihr überlagerten Ebene Dienste (also senkrecht) über SAPs zur Verfügung stellen. Genauso kann die überlagerte Ebene die Dienste der unterlagerten Ebene über die SAPs in Anspruch nehmen.

Auch hier erfolgt der Zugriff über SAPs mittels den Dienste-Primitiven. (MAC-SAP, PHY-SAP und PMD-SAP) MAC-SAP und PHY-SAP ist für alle Technologien gleich. Die PMD-Subebene ist für jede Technologie unterschiedlich und damit auch der PMD-SAP. Die Anpassung an die unterschiedlichen Technologien wird in der PLCP-Subebene vorgenommen.

Der SME-PLME-SAP und der MLME-PLME-SAP unterstützen die selben Primitive und können als ein SAP, den PLME-SAP angesehen werden. Die Nutzung erfolgt durch die MLME selbst, oder durch die MLME im Auftrag der SME.

Die Management-Primitive GET und SET gibt es als Anforderung (REQUEST) und zugehöriger Antwort (CONFIRM)

Z. B.

- XX-GET.request(MIBattribute) fordert den Wert einer MIB-Variablen an.
- XX-GET.confirm(MIBattribute) gibt den Wert der MIB-Variablen zurück.
- XX-SET.request(MIBattribute, MIBattributevalue) setzt die Variablen (MIBattribute) auf den Wert (MIBattributevalue). Wenn MIBattribute eine Aktion impliziert wird dadurch die Durchführung der Aktion angestoßen.
- XX-SET.confirm(status, MIBattribute) gibt eine Rückmeldung zum XX-SET.request(x,x)
Ist status = „success“ wird zurückgemeldet, dass die Variable auf den gewünschten Wert gesetzt wurde.
Falls nicht, wird ein Fehlercode übergeben. War durch den XX-SET.request() eine Aktion angestoßen worden zeigt status = „success“ an, dass die Aktion erfolgreich durchgeführt wurde. Falls nicht, wird im Status ein Fehlercode übergeben.

Wobei XX für den SAP steht der angesprochen wird. (z. B. SME-MLME, oder MLME)

Folgende Primitive stellt der PHY-SAP zur Verfügung.

Clear Channel Assessment (CCA)

Damit wird die Carrier-Sense-Bearbeitung für CSMA durchgeführt

- PHY-CCARESET.request
Damit fordert die MAC-Ebene die unterlagerte Ebene auf den CS/CCA-Automaten zurückzusetzen.
Dieses Primitiv wird nach Ablauf des NAV-Timers generiert und erlaubt der Station wieder auf das Medium zuzugreifen.
- PHY-CCARESET.confirm
Rückmeldung nachdem der CS/CCA-Automat auf einen PHY-CCARESET.request hin zurückgesetzt wurde.
- PHY-CCA.indication(STATE)
Hiermit wird der Zustand (idle oder busy) im Parameter STATE zurückgemeldet. Von der physikalischen Ebene wird jede Zustandsänderung des Mediums an die MAC-Ebene mitgeteilt.

Senden einleiten

- PHY-TXSTART.request(TXVECTOR)
Damit teilt die MAC-Ebene der PHY-Ebene mit, dass sie MPDU übertragen will. Diese Primitive ist nur möglich wenn das Ergebnis (STATE) von PHY-CCA.indication(STATE) = Idle ist. Der TXVECTOR enthält die eine Parameterliste die die MAC-Ebene bereitstellt. Die Liste muss die Datenrate und die MPDU-Länge enthalten. Evtl. werden noch weitere PHY-spezifische Informationen mitgegeben.
- PHY-TXSTART.confirm
Die PHY-Ebene teilt der MAC-Ebene dadurch mit, dass sie bereit ist eine MPDU zu übertragen.

Daten Senden

- PHY-Data.request(DATA)
Damit wird ein Daten-Byte (im Parameter DATA) von der MAC-Ebene hinunter zur PHY-Ebene übertragen. Dieses Primitiv kann nur nach erfolgtem PHY-TXSTART.confirm erfolgen.
- PHY-Data.indication(DATA)
Damit wird ein Daten-Byte (im Parameter DATA) von der PHY-Ebene hoch zur MAC-Ebene übertragen.
- PHY-DATA.confirm
Damit bestätigt die PHY-Ebene dass ein Frame von der MAC-Ebene auf die PHY-Ebene übertragen wurde.
Es ist die Antwort auf ein PHY-Data.request(DATA).

Daten Empfangen

- ➊ PHY-RXSTART.indication(RXVECTOR)

Damit teilt die PHY-Ebene der MAC-Ebene mit, dass sie einen PLCP-Header erfolgreich empfangen hat. RXVECTOR enthält eine Parameterliste welche von der PHY-Ebene bereitgestellt wird. Darin muss die Datenrate und die Länge (aus dem PLCP-Header) enthalten. Evtl. werden noch weitere technologie-spezifische Informationen mitgegeben.

- ➋ PHY-RXEND.indication(RXERROR)

Die PHY-Ebene teilt der MAC-Ebene, dass der Empfang der MPDU, die gerade übertragen wird, beendet ist. Der Parameter RXVECTOR zeigt einen oder mehrere Fehler:

- ➌ NoError

Zeigt an, dass kein Fehler aufgetreten ist.

- ➌ FormatViolation

Zeigt an, dass ein fehlerhaftes Frameformat übertragen wurde.

- ➌ CarrierLost

Zeigt an, dass während der Übertragung des Frames kein Empfang mehr möglich war und die Übertragung abgebrochen wurde.

- ➌ UnsupportedRate

Zeigt an, dass die Datenrate des empfangenen Frames von der PHY-Ebene nicht unterstützt wird.

Sende-Ende

- ➊ PHY-TXEND.request

Dies ist eine Aufforderung der MAC-Ebene an die PHY-Ebene die Übertragung der MPDU zu beenden. Wird von der MAC-Ebene erzeugt wenn das letzte PHY-DATA.confirm von der PHY-Ebene empfangen wurde.

- ➋ PHY-TXEND.confirm

Bestätigung der PHY-Ebene an die MAC-Ebene dass die Übertragung der MPDU beendet ist.

Der PLCP basiert auf 3 Statusmaschinen. Eine für den Daten-Empfang, eine für das Daten-Senden und eine für das Clear Channel Assessment (CCA)

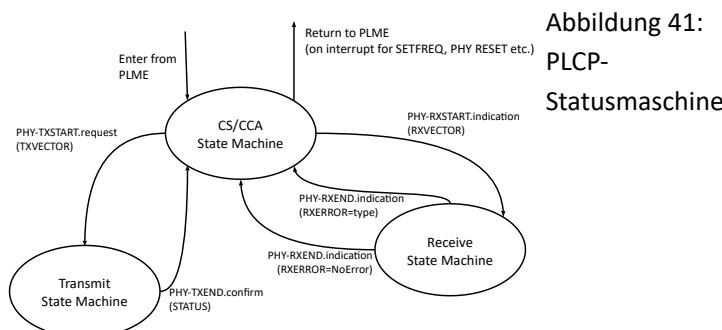


Abbildung 41:
PLCP-
Statusmaschine

Sobald der PLCP von der MAC-Layer ein PHY-START.request(TXVECTOR) empfängt beginnt er mit dem CCA.

Das Senden wird mit einem PHY TXSTART.request (TXVECTOR) eingeleitet.

Das Empfangen wird durch die PHY RXSTART.indication(RXVECTOR) initialisiert.

4.3 - Ausgetauschte Dateneinheiten

Wie bereits in der Vorlesung Netztechnik I im Kapitel 3 Schichtenmodelle beschrieben müssen bei der Betrachtung der ausgetauschten Dateneinheiten zwei Sichtweisen unterschieden werden:

- ➊ Dienste-Sicht
- ➋ Protokoll-Sicht

Die Schichten stellen über die SAPs Dienste (Services) zur Verfügung die mit den Dienste-Primitiven genutzt werden können. Die Daten die Dabei ausgetauscht werden sind die PDUs und die SDUs

Bei der Dienste-Sicht werden in der senkrechten Verbindung ICIs und SDUs ausgetauscht. Die Daten sind in den SDUs (Service Data Units) hinterlegt, die Information zur Steuerung der anderen Schicht in den ICIs (Interface Control Information). Natürlich müssen die Daten von der untersten Schicht in Form von PDUs auf dem Medium transportiert werden.

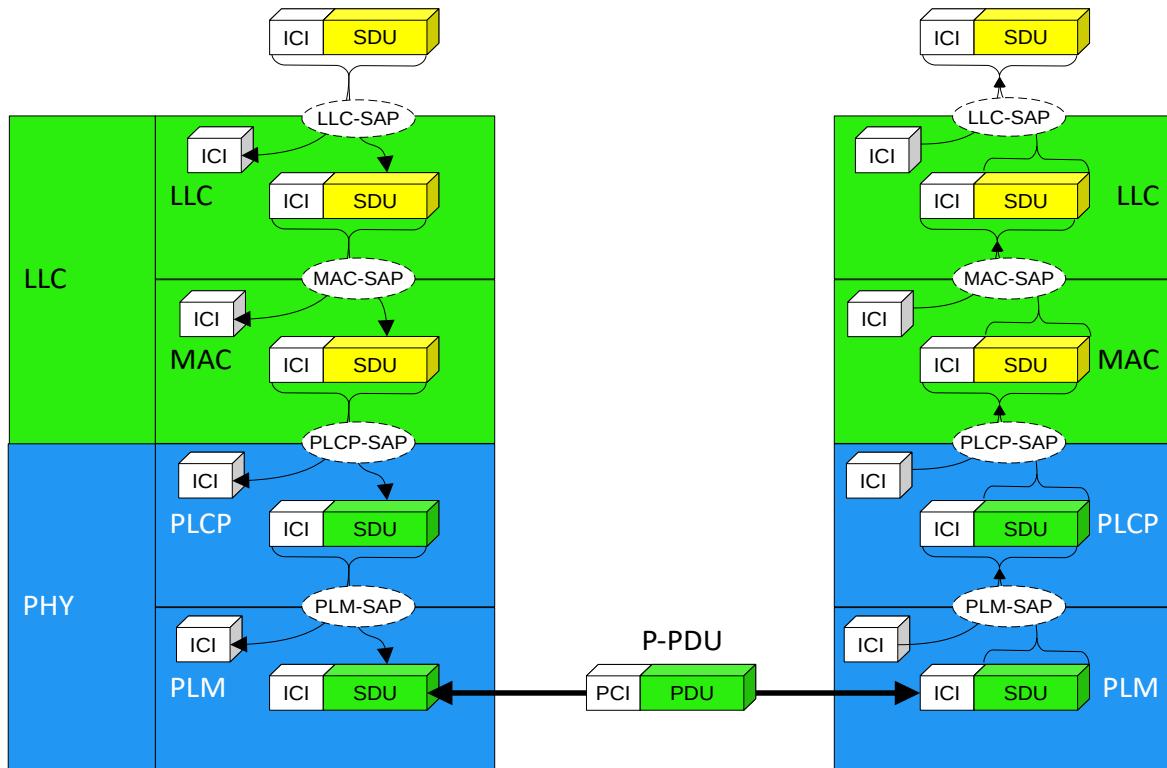


Abbildung 42: Dienste (Service) - Sicht des Schichtenmodells für WLANs

Bei der Protokoll-Sicht werden in der waagerechten Verbindung PCIs und PDUs ausgetauscht. Die Daten sind in den PDUs (Protocol Data Units) hinterlegt, die Information zur Steuerung der anderen Seite in den PCIs (Protocol Control Information).

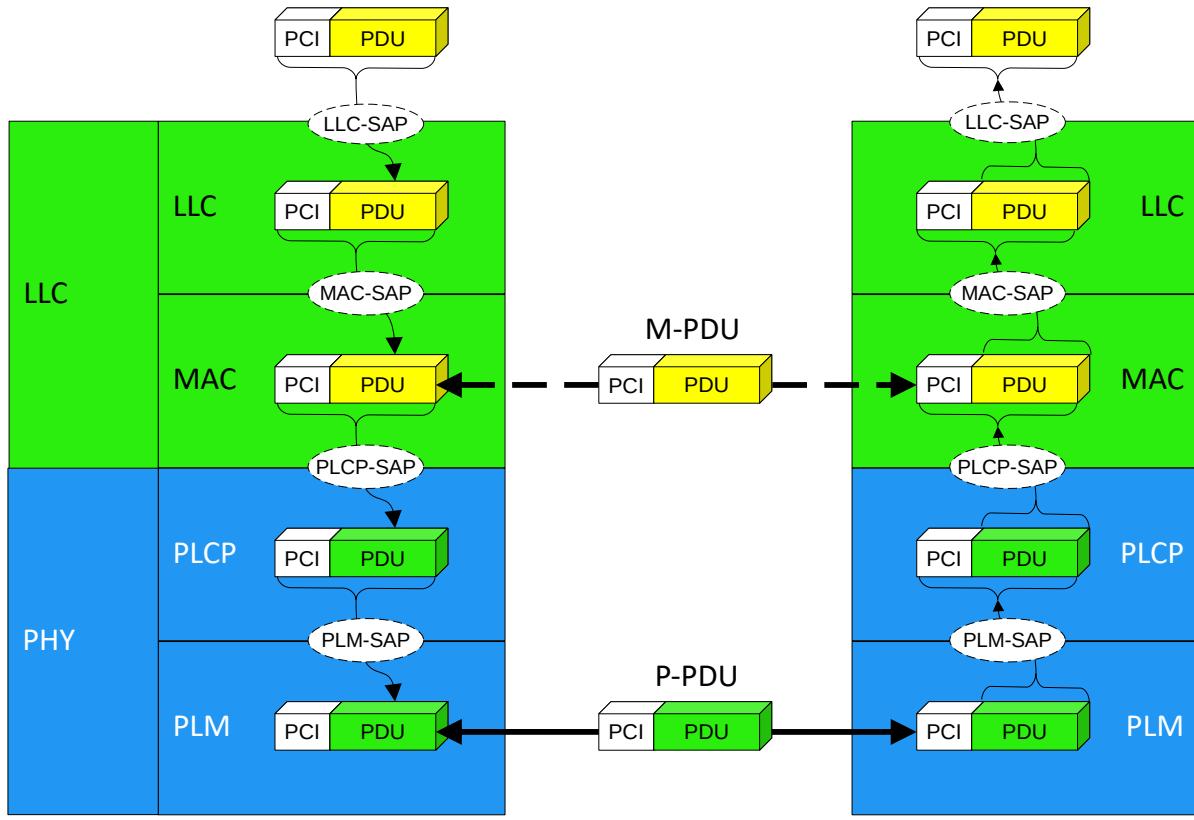


Abbildung 43: Protokoll (Protocol) - Sicht des Schichtenmodells für WLANs

4.4 - PHY-Layer

Auf der untersten Ebene werden die physikalischen Gegebenheiten, die eine Datenübertragung ermöglichen abgehandelt. Als Physical Media Dependent (PMD) wurden die folgenden Verfahren spezifiziert:

- ➊ Infrarot
- ➋ FHSS
- ➌ DSSS
- ➍ OFDM
- ➎ OFDMA

Die ersten 3 Verfahren sind mittlerweile als historisch zu betrachten. Deshalb soll hier nur kurz darauf eingegangen werden, denn in anderen Funktechniken werden diese Verfahren durchaus noch eingesetzt. (z. B. FHSS bei Bluetooth)

Jeder Standard - und damit auch jede Standard-Erweiterung - ist auf dieser Ebene unterschiedlich. Hier sind die unterschiedlichen Ausprägungen zu den Themen Modulationsverfahren, Datenraten, Antennenanzahl, usw. vertreten.

Da das Protokoll auf Ebene 2 für alle Standards einheitlich ist, wird eine Anpassung an die unterschiedlichen PMDs erforderlich. Dies wird in der Physical Layer Convergence Procedure (PLCP) gemacht. Die PLCP definiert Methoden um die Daten der MAC-Layer (2), die MAC Protocol Data Units (MPDUs), den unterschiedlichen PMDs zur Verfügung zu stellen und die Managementinformationen zwischen MAC und PMD auszutauschen. Das Management der PMD erfolgt über die PMD-SAPs (Service Access Points)

4.4.1 - PMD

Funkwellen werden auf ihrem Weg vom Sender zum Empfänger mit diversen Problemen konfrontiert. So können sie an Hindernissen reflektiert werden. Dies führt dazu, dass ein ausgesendetes Signal über unterschiedliche Wege zum Empfänger gelangen kann. (Mehrwegeproblem)

Durch die Atmosphäre oder beim Durchgang durch Hindernisse können Signale gedämpft oder verzerrt werden. So ist das Signal beim Durchgang durch massive Wassermengen (auch Menschen) stark gedämpft. Der Durchgang durch Regen, Nebel oder Schnee ist fast problemlos möglich. Je nachdem, ob innerhalb oder außerhalb von Gebäuden, ist mit den unterschiedlichsten Hindernissen und somit auch Signaldämpfungen zu rechnen.

Zusätzlich zu den Dämpfungsproblemen kommen noch Störungen in Form von Geräten, die ebenfalls Signale auf den genutzten Frequenzen emittieren. Diese Störungen kommen in Form von Rauschen beim Empfänger an. Selbst der Empfänger ist mit seinen Bauteilen nicht frei von Rauschen. Wichtig ist hierbei, dass das Nutzsignal aus dem Rauschen herausgefiltert werden kann

Um Funksignale vor Störungen zu schützen, wurden anfänglich so genannte Bandspreizverfahren angewendet. Dabei wird die Bandbreite künstlich vergrößert. In der folgenden Abbildung ist links das ursprüngliche Signal zu sehen. Auf der rechten Seite ist zu sehen, dass die Bandbreite verbreitert (also vergrößert) wurde. Allerdings ist dadurch das Nutzsignal in seiner Amplitude reduziert worden.

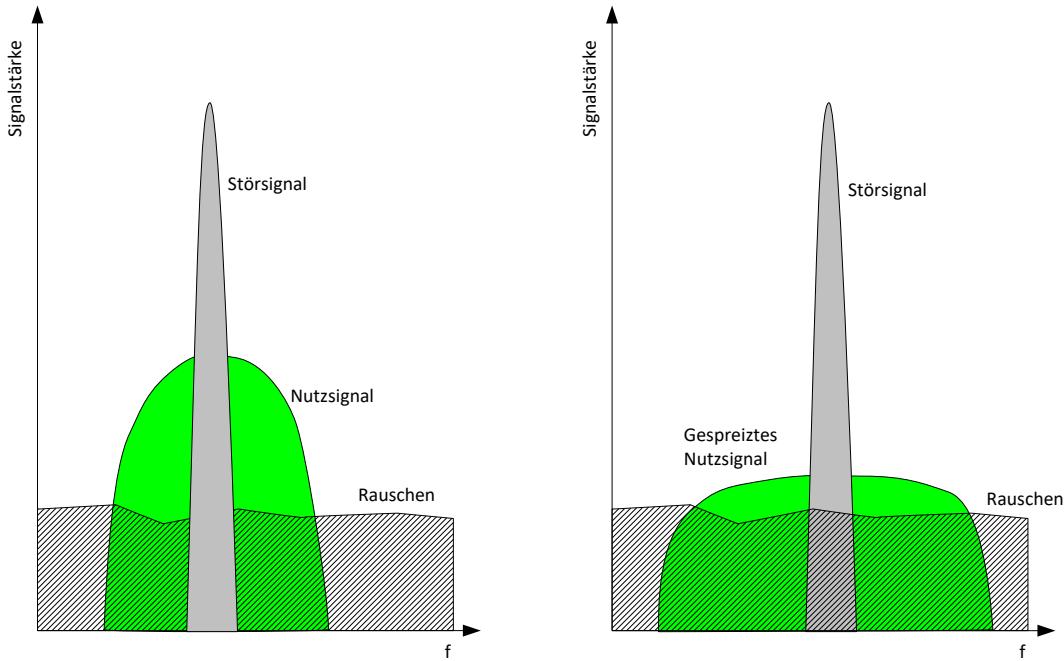


Abbildung 44: Signalspreizung

Dies lässt sich so lange treiben, bis das Nutzsignal im Rauschen verschwindet. Im militärischen Bereich wird das angewendet um ein Signal im Rauschen zu verstecken.

Bei der Satelliten-Kommunikation wird das Verfahren angewendet, um sehr kleine Nutzsignale von weit entfernten Satelliten aus dem Rauschen zu extrahieren.

Wird das Wechseln der Bänder durch die Codesequenz gesteuert, spricht man von Frequency-Hopping CDMA. Durch die Signalspreizung wird mehr Bandbreite benötigt!

4.4.2 - Bandspreizverfahren

4.4.2.1 - FHSS

Einzel angewandte Multiplexverfahren führen nicht immer zu optimalen Ergebnissen. Deshalb werden Kombinationen verschiedener Multiplexverfahren angewandt. Hier ein Beispiel zu einer Kombination aus FDMA und TDMA.

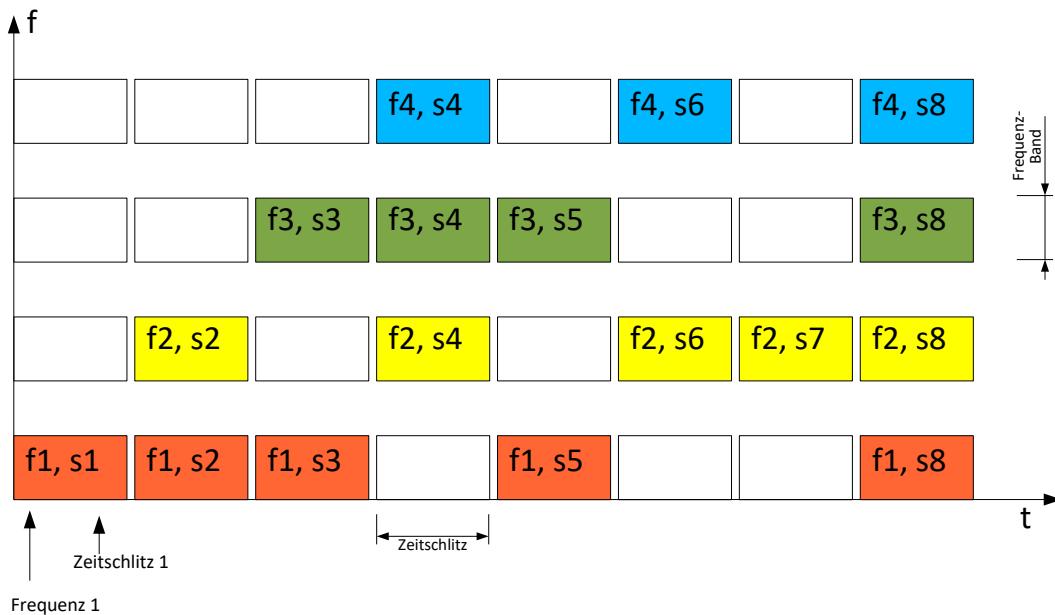


Abbildung 45: TDMA in Kombination mit FDMA

Damit kann eine Verbesserung bei der Ressourcen-Ausnutzung erreicht werden. Die frei werdenden Zeitschlüsse können für weitere Verbindungen genutzt werden.

Treten nun schmalbandige Störungen (also nur auf einem Frequenzband) auf, ist der Kanal und damit die Verbindung gestört. Durch einen zyklischen Kanalwechsel kann der Datentransport weiter gewährleistet werden.

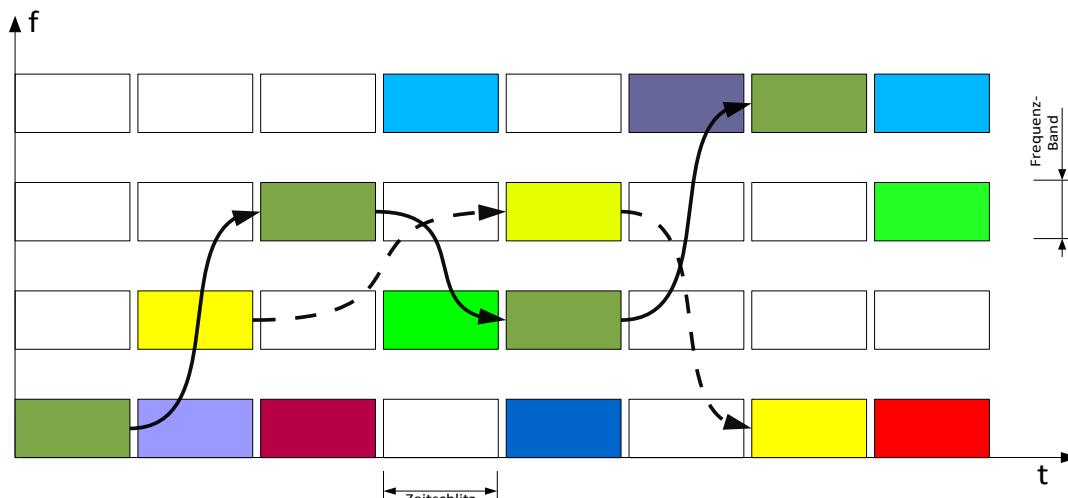


Abbildung 46: Frequency-Hopping

Dadurch benötigt ein Signal mehrere Frequenzbänder was einer Bandspreizung entspricht.

Eine konsequente Anwendung dessen, also ein ständiges Springen zwischen den Frequenzen wird beim Frequency-Hopping, wie z. B. bei IEEE-802.11 in einer ursprünglichen Variante, Bluetooth oder GSM gemacht.

4.4.2.1.1 - FHSS-Technologie

Die Bandbreite von 2,4000 GHz bis 2,4835GHz wird in 79 Frequenzunterbänder mit je 1 MHz aufgeteilt. Jedes der 79 Frequenzbänder stellt einen Kanal (2 – 80) bereit, die im Wechsel genutzt werden. Die Wechsel werden über die Hopping-Sequenz gesteuert. Sender und Empfänger wechseln gleichzeitig den Kanal. Durch ETSI festgelegt müssen (mit Ausnahme von Frankreich und Spanien) die Bänder nach 400 ms gewechselt werden. Das bedeutet, dass innerhalb einer Sekunde 2,5 Wechsel stattfinden. Der Abstand zwischen zwei nacheinander verwendeten Bändern muss mindestens 6 MHz betragen. Der Kanalwechsel muss innerhalb 224 µs erfolgen.

Damit nicht alle Teilnehmer die selben Kanäle verwenden gibt es in Europa (mit Ausnahme von Frankreich und Spanien) 3 Hopping-Sets:

1. Set: $x = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75\}$
2. Set: $x = \{1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 55, 58, 61, 64, 67, 70, 73, 76\}$
3. Set: $x = \{2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 38, 41, 44, 47, 50, 53, 56, 59, 62, 65, 68, 71, 74, 77\}$

Der genutzte Kanal einer Hopping-Sequenz lässt sich nach der Formel berechnen:

$$fx(i) = (b(i) + x) \bmod (79) + 2 \quad (3)$$

wobei $fx(i)$ die Kanalnummer, x eine Zahl des verwendeten Hopping-Sets, i der Index für den nächsten Kanal und $b(i)$ der folgenden Tabelle entnommen werden kann.

Tabelle 7 FHSS-Hopping-Sequenzen

i	b(i)										
1	0	15	52	29	37	43	41	57	65	71	55
2	23	16	63	30	10	44	74	58	50	72	35
3	62	17	26	31	34	45	32	59	56	73	53
4	8	18	77	32	66	46	70	60	42	74	24
5	43	19	31	33	7	47	9	61	48	75	44
6	16	20	2	34	68	48	58	62	15	76	51
7	71	21	18	35	75	49	78	63	5	77	38
8	47	22	11	36	4	50	45	64	17	78	30
9	19	23	36	37	60	51	20	65	6	79	46
10	61	24	71	38	27	52	73	66	67	-	-
11	76	25	54	39	12	53	64	67	49	-	-
12	29	26	69	40	25	54	39	68	40	-	-
13	59	27	21	41	14	55	13	69	1	-	-
14	22	28	3	42	57	56	33	70	28	-	-

Beispiel:

Berechnet man mit der oben genannten Formel aus der Hopping-Zahl 0 des ersten Hopping-Sets den 75., 76. und 77. Kanal, so erhält man:

$$fx(75) = [44 + 0] \bmod (79) + 2 = 46$$

$$fx(76) = [51 + 0] \bmod (79) + 2 = 53$$

$$fx(77) = [38 + 0] \bmod (79) + 2 = 40$$

Es zeigt sich, dass bis zu 13 unabhängige FSHH-Systeme innerhalb eines Empfangsbereichs arbeiten können, ohne dass der Datendurchsatz durch gehäufte Kollisionen beeinträchtigt wird.

Die durch IEEE-802.11 festgelegte FHSS-PHY-Layer ermöglicht Datenraten von 1 und 2 Mbps. Um das zu verbessern, müsste die Kanal-Bandbreite oder die Anzahl der Kanäle bzw. Frequenzunteränder erhöht werden. Dies würde jedoch die Anzahl der Bänder reduzieren, was eine Häufung der Kollisionen zur Folge hätte.

Die Implementierung ist einfach, was einen geringen Stromverbrauch und geringe Herstellungskosten zur Folge hat.

Dieser Vorteil wird durch ein aufwändiges Handover erkauft. Soll eine Zelle gewechselt werden, muss jeder der 79 Kanäle abgehört werden, denn ein gleichzeitiges Senden und Empfangen ist nicht möglich!

Da bei Bluetooth die Zelle nicht ständig gewechselt wird findet FHSS dort Anwendung.

4.4.2.1.2 - FHSS-Modulationsverfahren

Als Modulationsverfahren wird ein Frequency Shift Keying (FSK) angewendet. Da hierbei beide Seitenbänder verwendet werden müssen ist die benötigte Bandbreite relativ groß. Bei dieser Modulationsart handelt es sich um die Gaussian Frequency Shift Keying Modulation, kurz GFSK.

Für die Übertragung von 1Mbps wird die 2GFSK (2-Level Gaussian Frequency Shift Keying) Modulation eingesetzt. Sollen 2 Mbps übertragen werden, wird die 4GFSK (4-Level Gaussian Frequency Shift Keying) Modulation eingesetzt. Generell gilt, dass bei FHSS-Systemen pro Zeiteinheit 10^6 Symbole übertragen werden.

4.4.2.1.2.1 - 2GFSK

Bei der 2GFSK hat ein Symbol eine Länge von einem Bit und pro Zeiteinheit wird ein Bit übertragen. Somit kommt man auf 1 Mbps.

Die Symbole werden bei 2GFSK folgendermaßen dargestellt:

0 ergibt sich aus der Sendefrequenz = Center Frequenz -110 kHz bis -160 kHz

1 ergibt sich aus der Sendefrequenz = Center Frequenz +110 kHz bis +160 kHz

4.4.2.1.2.2 - 4GFSK

Bei der 4GFSK hat ein Symbol eine Länge von 2 Bit. Pro Zeiteinheit werden damit 2 Bit übertragen. Somit kommt man auf 2 Mbps.

Die Symbole werden bei 4GFSK folgendermaßen dargestellt:

- 00 ergibt sich aus der Sendefrequenz = Center Frequenz -202,5 kHz bis -216 kHz
- 01 ergibt sich aus der Sendefrequenz = Center Frequenz -67,5 kHz bis -72 kHz
- 10 ergibt sich aus der Sendefrequenz = Center Frequenz +202,5 kHz bis +216 kHz
- 11 ergibt sich aus der Sendefrequenz = Center Frequenz +67,5 kHz bis +72 kHz

Der FHSS-Empfänger muss eine Empfindlichkeit von -80dBm aufweisen. Das gilt sowohl für 1Mbps- als auch für die 2 Mbps-Variante. Bei einer PSDU-Länge von 400 Bytes muss eine maximale Frame Error Rate (FER) von 3% garantiert werden.

4.4.2.1.3 - FHSS-Frameformat

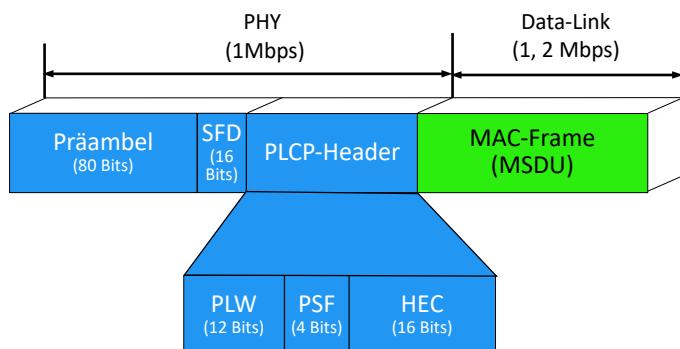


Abbildung 47: FHSS-PLCP-Frameformat

- Die Präambel besteht aus einem 80 Bit langen String mit abwechselnd 0 und 1 beginnend mit 0.
- Der 16 Bit lange Start-Frame-Delimiter (SFD) hat das Bitmuster 0000 1100 1011 1101 beginnend mit 0.
- Das PSDU Length Word (PLW) ist 12 Bit lang und legt die Länge des MAC-Frames in Bytes fest.
- Das PLCP Signaling Field (PSF) ist 4 Bit lang und legt die Datenrate des Frames fest. Obwohl der Standard Datenraten von 1 bis 4,5 Mbps vorsieht wurden nur Datenraten von 1 Mbps oder 2 Mbps realisiert.
- Das 16 Bit lange Header Error Control Feld (HEC) ist ein CRC-16 Test für den PLCP-Header. Damit können Fehler im PLW und PSF erkannt werden.

Tabelle 8 FHSS-Datenraten im PSF

B0 (res.)	b1	b2	b3	Data-Rate
0	0	0	0	1,0Mbps
0	0	0	1	1,5Mbps
0	0	1	0	2,0Mbps
0	0	1	1	2,5Mbps
0	1	0	0	3,0Mbps
0	1	0	1	3,5Mbps
0	1	1	0	4,0Mbps
0	1	1	1	4,5Mbps

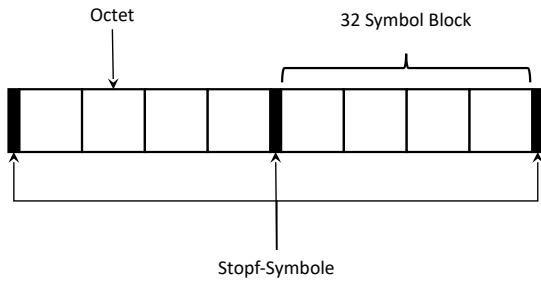


Abbildung 48: FHSS Scrambled PSDU

Der MAC-Frame (PSDU) wird gescrambelt. Das dient dazu den Gleichspannungsanteil zu reduzieren.

Dazu dient ein 127-Bit-Wort mit dem folgenden Inhalt:

00001110-11110010-11001001-00000010-00100110-00101110-10110110-00001100-11010100-11100111-10110100-00101010-11111010-01010001-10111000-1111111.

Das 127-Bit-Wort wird über die polynomiale Funktion $S(x) = x^7 + x^4 + 1$ erzeugt und mit den Daten als als Binärstrom XOR-Verknüpft.

Abschließend werden die Daten über eine 32/33-Codierung in 32-Bitlange Blöcke unterteilt und ein 32-Symbol-Block Stopf-Symbole angefügt, um einen Überhang von Nullen oder Einsen zu eliminieren, was bei den folgenden Prozessen unerwünschte Effekte haben kann.

Tabelle 9 Charakteristische FHSS-Parameter [Rech-WLAN-2012]

Parameter	Wert
aSlotTime	50 µs
aSIFSTime	28µs
aCCATime	27µs
aMPDUMaxLength	4095 Bytes
aCWmin	15
aCWmax	1023
Dauer für Präambel	96µs
Dauer für PLCP-Header	32µs

4.4.3 - DSSS

4.4.3.1 - DSSS-Signalspreizung

Ein weiteres Signalspreiz-Verfahren um die Kommunikation gegen Störungen resistent zu machen ist das Direct Sequence Spread Spectrum Verfahren (DSSS). Direct Sequence deutet darauf hin, dass immer nur eine Frequenz genutzt wird.

Dabei wird das Signal, mit einer so genannten Chipsequenz abgetastet. Die Frequenz der Chipsequenz ist höher als das abgetastete Signal. Danach erfolgt eine XOR-Verknüpfung des abgetasteten Signals mit einem Chipcode.

Dadurch wird das Signal im Verhältnis zum Rauschen kleiner, ist jedoch, selbst bei großem Rauschen, wieder zu ermitteln. Bleibt man dabei auf dem selben Band, spricht man von Direct Sequence CDMA.

Durch die Signalspreizung wird mehr Bandbreite benötigt!

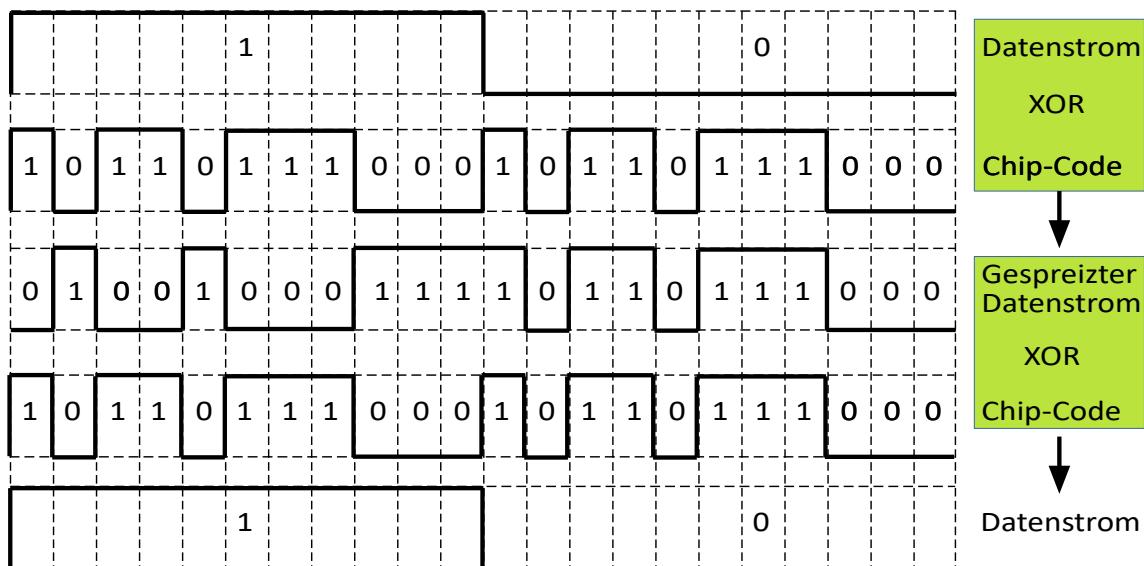


Abbildung 49: Direct Sequence CDMA

Als Spreizsequenz kann entweder ein PN-Code (Pseudo Noise – Code), oder ein festes binäres Codewort verwendet werden. Bei IEEE-802.11 wird für die Spreizsequenz ein Barker-Code mit 11 Chips verwendet. Das dadurch entstandene Spreizsignal hat in diesem Fall eine Frequenz von 11MHz.

Für die Codierung wird die folgende Chip-Sequenz verwendet. $+1, -1, +1, +1, -1, +1, +1, +1, -1, -1$.

4.4.3.2 - DSSS-Modulation

Bei IEEE-802.11 sind für DSSS zwei Modulations-Verfahren festgelegt worden, die mit 11MChips/s betrieben werden:

- BPSK (Binary Phase Shift Keying) Dabei wird zwischen zwei Symbolen unterschieden, die sich in der Phasenlage um 180° verschieben. Damit lässt sich pro Symbol genau ein Bit codieren. Bei einer Chiprate von 11 Mchips/s und einer Spreizsequenz von 11 Chips Länge lässt sich eine Datenrate von 1 Mbps erreichen.
- QPSK (Quadrature Phase Shift Keying) Bei QPSK wird eine Phasenverschiebung von 90° angewendet. Damit lassen sich 4 Symbole bei 2 Bits codieren. Daraus folgt, dass sich bei einer Chiprate von 11MChips/s und einer Spreizsequenz von 11 Chips Länge eine Datenrate von 2 Mbps erreichen lässt.

4.4.3.3 - DS-SSS-Frameformat

Da hierbei nur der kleinste gemeinsame Nenner zwischen unterschiedlichsten Herstellern und Anforderungen erreicht wurde, waren viele Freiheitsgrade offen geblieben. Deshalb war die Interoperabilität der Produkte unterschiedlicher Hersteller oft nicht gegeben. Die Weiterentwicklungen wurden weltweit von unterschiedlichen Herstellern betrieben. Leider sind hierbei auch nationale Gegebenheiten zu berücksichtigen. Dies führte dazu, dass die unterschiedlichen Weiterentwicklungen zeitlich versetzt auf den Markt kamen. Sie wurden in verschiedenen Ländern mit unterschiedlichen Ausprägungen, wie z. B. Sendeleistungen, auf den Markt gebracht.

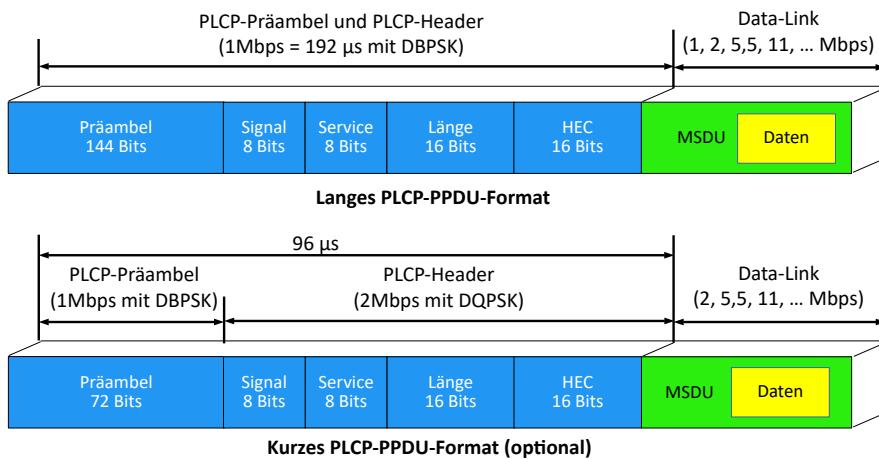


Abbildung 50: Die 2-PLCP-Frameformate bei DS-SSS

Tabelle 10 Charakteristische DS-SSS-Parameter [Rech-WLAN-2012]

Parameter	Wert
aSlotTime	20 µs
aSIFSTime	10µs
aCCATime	< 15µs
aMPDUMaxLength	4095 Bytes
aCWmin	31
aCWmax	1023
Dauer für Präambel	144 / 72µs
Dauer für PLCP-Header	48 / 24µs

Tabelle 11: DS-SSS-Empfänger-Empfindlichkeit [Rech-WLAN-2012]

Datenrate	Empfindlichkeit laut Standard	Typischer Wert von Produkten
1 MBit/s	Nicht definiert	-94 dBm
2 MBit/s	-80 dBm	-93 dBm
5,5 MBit/s	Nicht definiert	-92 dBm
11 MBit/s	-76 dBm	-90 dBm

4.4.4 - OFDM

OFDM (Orthogonal Frequency Division Multiplexing) wurde erstmals von ETSI beim HIPERLAN/2-Standard verwendet. Es ist keine simple Modulationstechnik sondern ein komplexes mehrstufiges Verfahren zur Signalsynthetisierung. [NI-2002-08]

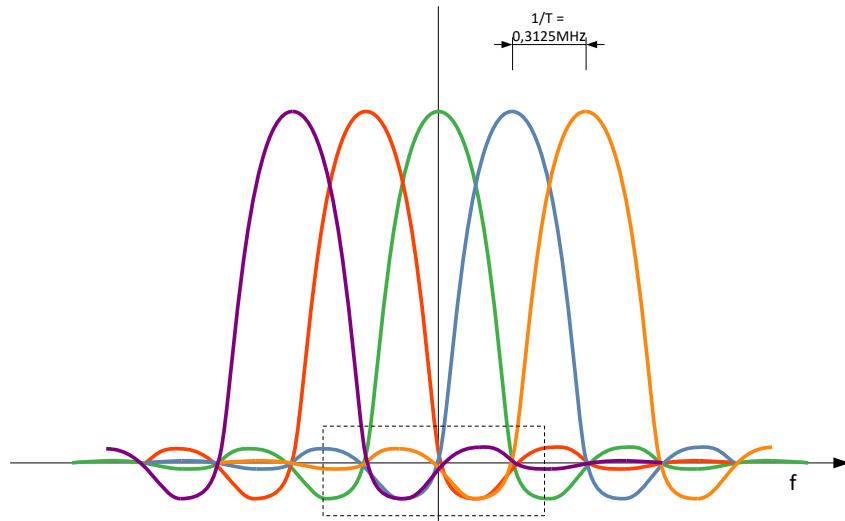


Abbildung 51: OFDM-Signalüberlagerung

Bei FHSS und DS-SS werden die Frequenzen der Kanäle weit auseinander gehalten um die einzelnen Teilnehmer sauber voneinander zu trennen.

Im Gegensatz dazu, werden bei OFDM die Unterträger so weit zusammengeschoben, dass die Seitenbänder der Unterträger sich gegenseitig eliminieren und dadurch keine Beeinflussung stattfindet.

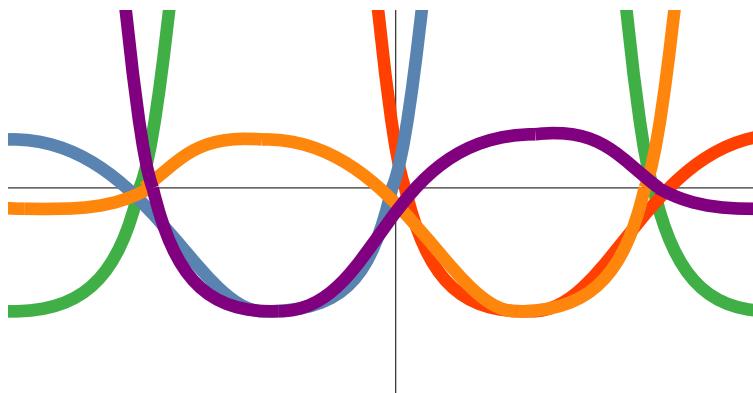


Abbildung 52: Detail: Nulldurchgänge der Nachbar-Unterträger bei Maximum

Orthogonal bedeutet in diesem Zusammenhang nicht, dass die Kanäle senkrecht aufeinander stehen, sondern, dass sie sich gegenseitig nicht stören. Das wird in der Abbildung 52 deutlich. Hier sieht man, dass, da wo das grüne Signal sein Maximum hat, die Nachbarn (rot und blau) ihren Nulldurchgang haben.

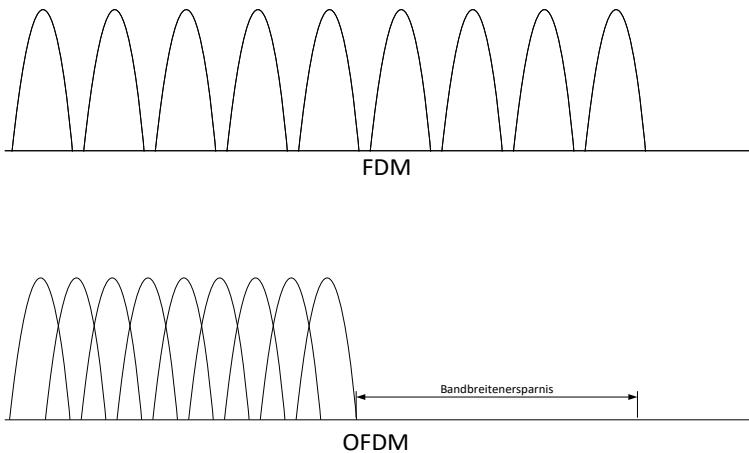


Abbildung 53: OFDM-Bandbreitenersparnis

Durch das Zusammenschieben der Unterträger kann ca. 50% Bandbreite eingespart werden, die wiederum für weitere Unterträger genutzt werden kann.

Bei OFDM im 5GHz-Band ist der zur Verfügung stehende Frequenzbereich in 53 Unterträger aufgeteilt. Die Unterkanäle -21, -7, 7 und 21 werden als Pilotkanäle genutzt und stehen nicht zum Datentransport zur Verfügung. In den Pilotkanälen werden die Referenzphasen übermittelt. Der Kanal 0 wird ebenfalls nicht verwendet. Damit stehen für den Datentransport 48 Unterträger zur Verfügung. Die Symbolrate ist 0,25 MSymbole/s.

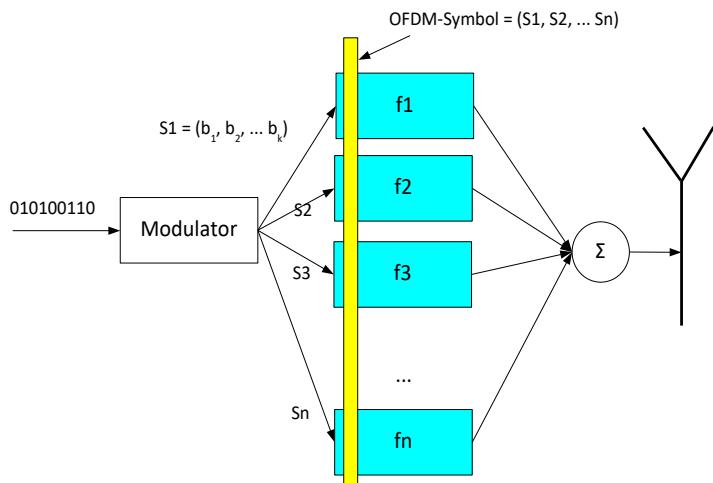


Abbildung 54: OFDM Datenübertragung

Auf jeden der 48 Unterträger wird ein Signal in Form einer Amplitude oder Phasenverschiebung aufgeprägt. Dazu bieten sich BPSK, QPSK und die QAM-Verfahren an.

Bei OFDM wird ein Symbol nicht seriell mit hoher Datenübertragungsrate sondern parallel mit einer niedrigeren Datenübertragungsrate auf die 48 Unterträger verteilt und gesendet.

FDMA (Frequency Division Multiple Access) wird bei FHSS oder DSSS dazu benutzt um mehrere Nutzer gleichzeitig zu übertragen. Bei OFDM wird von **einem** Nutzer einfach über die 48 Unterträger gleichzeitig und somit mehr an Daten übertragen.

4.4.4.1 - Beschreibung der verwendeten Parameter

Die Datenrate bei OFDM lässt sich folgendermaßen berechnen:

$$\text{Datenrate} = \text{Symbolrate} * \text{Bits pro Unterkanal} (\text{N}_{\text{BPSC}}) * \text{Anz. der Unterkanäle} * \text{Coderate} \quad (4)$$

$$\text{Datenrate} = \text{Symbolrate} * \text{Bits pro Unterkanal} (\text{N}_{\text{BPSC}}) * \text{Anzahl der Unterkanäle} * \text{Coderate}$$

Wobei:

Symbolrate: Ist die Rate in der die Symbole erzeugt werden. Bei OFDM ist das 0,25 MSymbole / s

Bits pro Unterträger (Number Bits Per Sub Carrier) : Bei 64-QAM sind das z. B. 6 Bits

Anzahl der Unterkanäle: Bei OFDM stehen 48 Unterkanäle für die Datenübertragung zur Verfügung

Die Coderate gibt das Verhältnis von Daten-Bits pro Symbol zu codierten Bits pro Symbol an

Die Datenrate von 48 Mbit/s errechnet sich mit:

$$0,25 \text{ MSymbole/s} * 6 \text{ Bits / Unterkanal} * 48 \text{ Unterkanäle} * 2/3$$

Tabelle 12: OFDM-Datenraten

Datenrate [Mbit/s]	Modulation	Coderate	Codierte Bits pro Unterträger [N _{BPSC}]	Codierte Bits pro OFDM-Symbol [N _{CBPS}]	Daten-Bits pro OFDM-Symbol [N _{DBPS}]
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

Dies bedeutet, in Abhängigkeit von der Übertragungsqualität werden

- 4 Modulationsarten
- Faltungscode mit drei Codearten eingesetzt.

Dies ergibt dann Datenraten von 6 bis 54 Mbps. Netto sind dies maximal 20 – 30 Mbps.

Tabelle 13: Datenraten nach Modulationsarten

	BPSK	QPSK	16-QAM	64-QAM	256-QAM	1024-QAM
Bits pro Symbol pro Kanal	1	2	4	6	8	10
Datenrate / Kanal [Mbit/s]	0,25	0,5	1	1,5	2	2,5
Bits pro OFDM Symbol	48	96	192	288	384	480
Datenrate [Mbit/s]	12	24	48	72	96	120

4.4.4.2 - Übersicht des Sendevorgangs in der PHY-Schicht

Die gesamte Verarbeitung kann man im folgenden Blockschaltbild sehen.

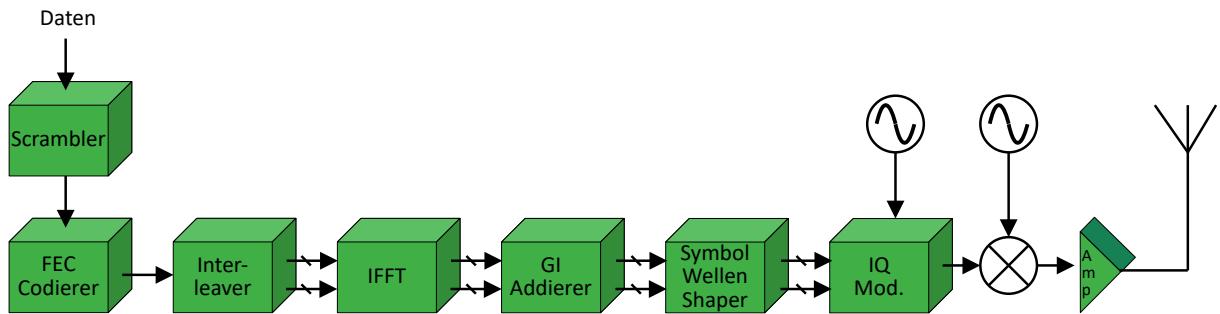


Abbildung 55: Blockschaltbild eines OFDM-Senders

Betrachtet man das Blockschaltbild des Senders in Abbildung 55 von links nach rechts, sieht man als erste Einheit den Scrambler, der dafür sorgt, dass es keine langen Einser- oder Null-Folgen gibt.

Der folgende Faltungscodierer fügt redundanten Bits ein, um den Faltungscode für die Forward Error Correction (FEC) zu erzeugen.

Der folgende Interleaver verwürfelt die Daten so, dass auf der Empfängerseite Burst-Störungen zu korrigierbaren Einzelfehlern gemacht werden können.

Ab dem Interleaver werden die Daten für jeden Unterträger getrennt bearbeitet.

Im Anschluss folgt die Inverse-Fast-Fourier-Transformation (IFFT) um für jeden Unterträger ein Ausgangssignal zu synthetisieren. Die IFFT liefert Koeffizienten, aus denen sich das Subframe mit der Dauer T_{FFT} zusammensetzt. Die Koeffizienten stellen Spektrallinien dar, die den Daten, Pilotträgern und Trainingssequenzen entsprechen.

Danach werden die Guard-Intervalle in den Datenfluss eingefügt.

Vor der IQ-Modulation werden die Signalwellen mittels eines Symbol Wellen Shapers in eine optimale Form gebracht.

4.4.4.3 - Übersicht des Empfangsvorgangs in der PHY-Schicht

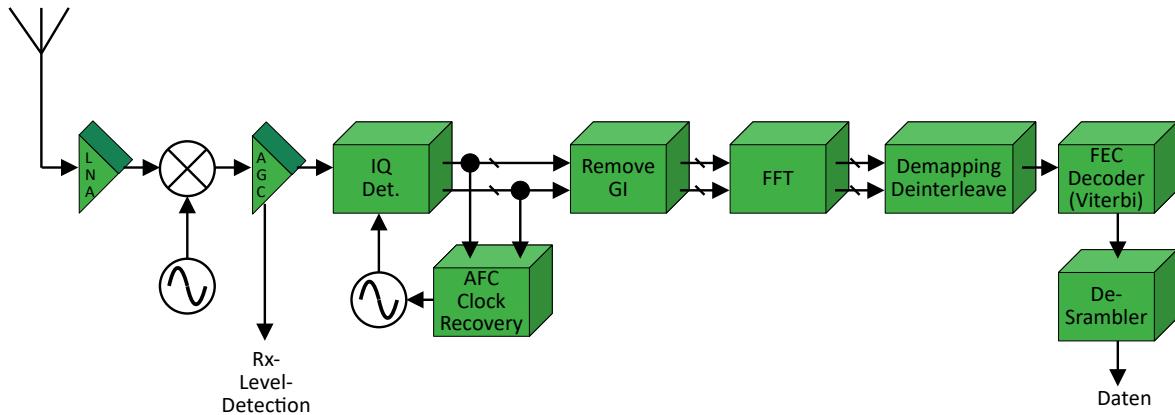


Abbildung 56: Blockschaltbild eines OFDM-Empfängers

Beim Empfänger Abbildung 56 durchlaufen die Informationen die Blöcke in umgekehrter Reihenfolge als beim Senden.

Zuerst werden jedoch die Signale verstärkt und auf eine Zwischenfrequenz gemischt.

Danach kommt ein Verstärker mit automatischer Verstärkungskontrolle (Automatic Gain Control). Daraus wird auch die Information für die Signalstärke abgeleitet.

Der folgende IQ-Diskriminatior wird mit einer steuerbaren Zwischenfrequenz aus der AFC-Baugruppe (Automatic Frequency Control) gemischt. Gleichzeitig wird der Takt aus dem Signal gewonnen.

Die nächste Baugruppe entfernt das Guard-Intervall.

Danach kann die Fast-Fourier-Transformation aus dem zusammenhängenden Signal ein Spektrum von Einzelsignalen erzeugen, die den Informationen der OFDM-Unterträger entsprechen.

Der Deinterleaver bringt die Informationen in die richtige Reihenfolge.

Der FEC-Decoder arbeitet mit einem Viterbi-Algorithmus. Es nähert die Information an das bestmögliche Ergebnis an und entfernt die redundanten Datenbits.

Als Letztes werden im Descrambler lange Null- oder Einser-Folgen wieder hergestellt.

4.4.4.4 - Scrambler

Mit dem Scrambler wird sicher gestellt, dass es keine langen Nullen- oder Einsen-Folgen gibt. Es handelt sich um selbst synchronisierende (multiplikative) Scrambler. Dabei wird das Generatorpolynom $S(x) = x^7 + x^4 + 1$ verwendet.

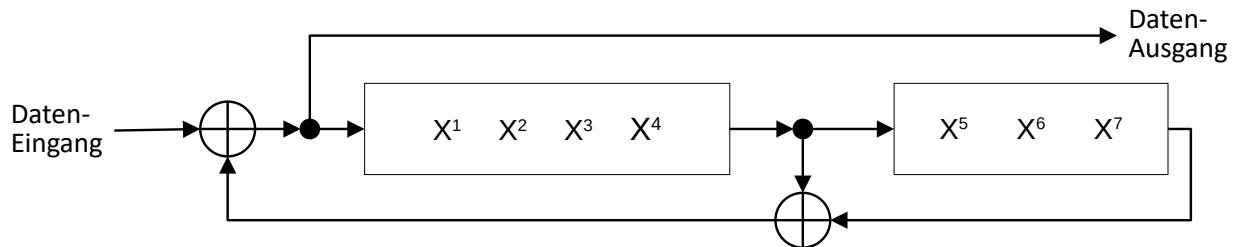


Abbildung 57: Scrambler

Auf der Empfängerseite wird die umkehrende Funktion mit dem selben Generatorpolynom durchgeführt.

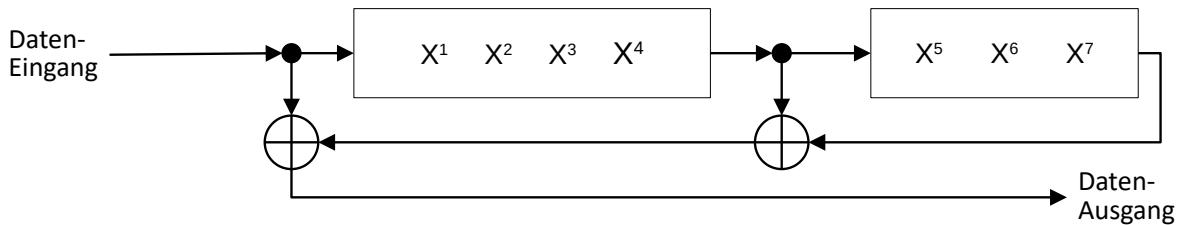


Abbildung 58: Descrambler

4.4.4.5 - Faltungscodierer

Nach dem Scrambler folgt ein nicht rekursiver Faltungscodierer. [Rech-WLAN-2012] Er fügt der Information Bits hinzu, um auf der Empfängerseite Fehler erkennen und beheben zu können. Da die Informationen vor der Übertragung bearbeitet werden, spricht man von einer Vorwärts-Fehlerkorrektur (Forward Error Correction = FEC)

Bei IEEE801.11a hat man sich auf einen Faltungscodierer mit 6 Schieberegistern geeinigt. Für die Initialisierung des Schieberegisters werden die 6 Tail-Bits aus dem Signal-Feld des PLCP-Headers verwendet.

Die Coderate (R) eines Faltungscodierers errechnet sich aus:

$$R = \text{Anzahl der Informationsbits (K)} / \text{Anzahl der erstellten Codebits (N)} = \text{Netto-Bits} / \text{Brutto-Bits} = K / N$$

Eine Coderate R von $1 / 2$ entspricht einer Übertragung der Datenbits + 100% Redundanz-Bits. Es wird also die Anzahl der zu übertragenen Bits verdoppelt.

Der resultierende Code wird allgemein mit (N, K, M) beschrieben. In dem in Abbildung 59 gezeigten Faltungscodierer ergibt das $(2,1,6)$, denn die Symbolspeichertiefe M durch die Anzahl der Speicherelemente definiert ist.

Der Faltungscodierer verwendet zwei Generatorpolynome nach dem ESA-NASA-Satellite-Standard-Code. Sie entsprechen $g_0 = 133_{(8)}$ und $g_1 = 171_{(8)}$.

Dies entspricht $g_0 = 1 + x^2 + x^3 + x^5 + x^6$ und $g_1 = 1 + x + x^2 + x^3 + x^6$ oder binär $g_0 = 1011011_{(2)}$ und $g_1 = 1111001_{(2)}$.

Der Aufbau entspricht einem linearen Schieberegister. Verschiedene Schieberegisterausgänge werden zwei Knotenpunkten zugeführt, wo sie Modulo-2 addiert werden. Die Ergebnisse der Knoten (A, B) werden einem Multiplexer zugeführt, der das Ergebnis auf einem Ausgang zusammenführt.

Welche Schieberegisterausgänge zu den Knotenpunkten zugeführt werden, lässt sich an der Binärschreibweise am besten erkennen. Ausgang A entspricht dem Generatorpolynom g_0 und Ausgang B entspricht dem Generatorpolynom g_1 . Bei einer Eins wird der Schieberegisterausgang dem Knoten zugeführt, bei einer Null nicht.

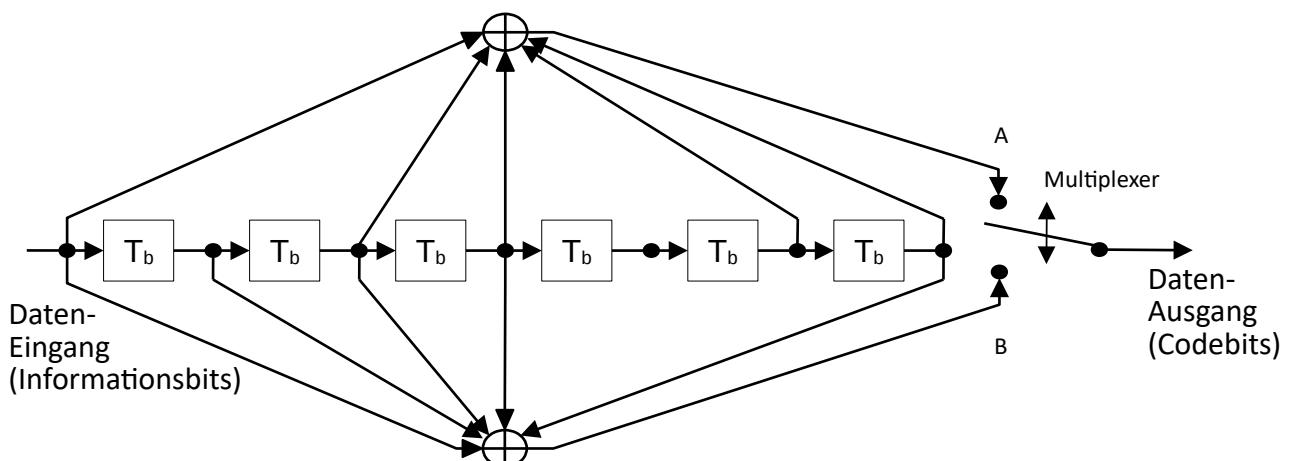


Abbildung 59: Faltungscodierer

In dem linearen Faltungscodierer liegt eine Symbolspeichertiefe von $M = 6$ vor. Das Codewort am Ausgang wird von 7 Bits ($M + 1$) beeinflusst. Damit wird die Einflusslänge zu $L_c = (M + 1) * K = (6 + 1) * 1 = 7$ Bit ermittelt.

Auf der Empfängerseite wird ein Viterbi-Decoder für Fehlererkennung und deren Behebung eingesetzt. Damit kann das empfangene Signal nicht errechnet werden sondern es wird bestmöglich geschätzt.

4.4.4.6 - Punktierung

Um nicht in allen fällen die Datenrate durch einen Faltungscodierer zu verdoppeln gibt es die Möglichkeit Zwischenstufen der Coderaten zu erzeugen. (Z. B. $R = 3 / 4$)

Um das zu erreichen werden, nach der Verdopplung der Bits durch die Faltung, mit einem so genannten Punktierungsmuster einige Bits wieder aus dem Ergebnis entfernt.

So können Coderate von $R = 2 / 3$ oder $R = 3 / 4$ erreicht werden.

Das Beispiel in der folgenden Abbildung zeigt eine Punktierung um die Coderate $3 / 4$ zu erzeugen.

Die A-Bits (A_0 bis A_8) und die B-Bits (B_0 bis B_8) werden zu einem Block von 18 Bits zusammengefasst.

Die Bits B_1, A_2, B_4, A_5, B_7 und A_8 werden punktiert, also gestrichen.

Damit entstehen am Ausgang $18 - 6 = 12$ Bits. Setzt man den Eingang des Faltungscodierers und den Ausgang der Punktierung in ein Verhältnis so entsteht das Verhältnis von $9 / 12$. Um 3 gekürzt ergibt sich $3 / 4$.

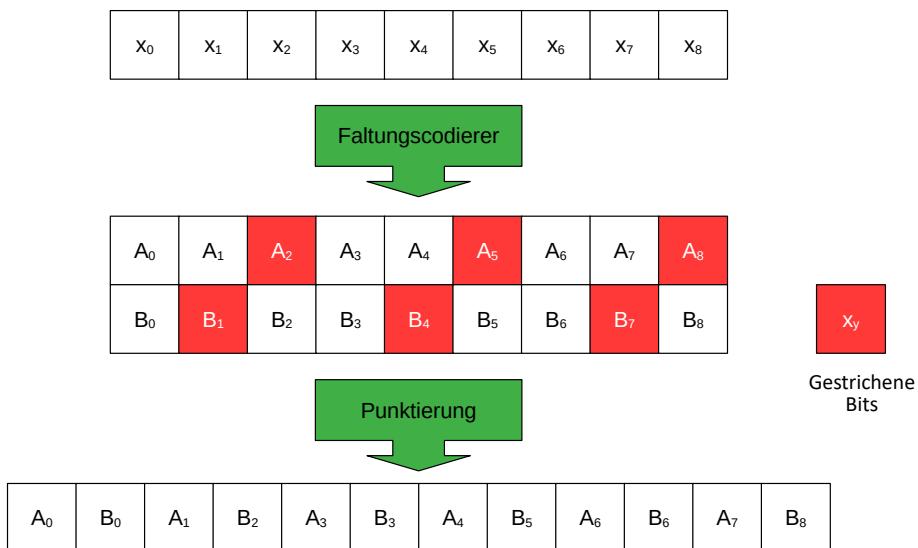


Abbildung 60: Beispiel einer Punktierung mit der Coderate $R = 3 / 4$

Auf der Empfängerseite müssen die punktierten Bits wieder mit Dummies aufgefüllt werden .

Damit ist die Coderate $R = 1 / 2$ die einzige Coderate, die unpunktiert ist.

4.4.4.7 - Beispiel für Faltungscodierung und Punktierung

Die Faltungscodierung und die Punktierung soll anhand eines Beispiels nochmals verdeutlicht werden. Der Faltungscodierer aus Abbildung 59 soll hierbei angewendet werden. Es soll die folgende Bitfolge bearbeitet werden:

$$D_0=1, D_1=1, D_2=0, D_3=1, D_4=1, D_5=1, D_6=0, D_7=1; D_8=0$$

In den folgenden Tabellen kann man sehen wie die Bits mit jedem Takt i weiter von links nach rechts durchgeschoben werden. Die roten Spalten sind nur der Vollständigkeit halber dargestellt um zu sehen wie die Bits durchgeschoben werden. Bei der Molulo-2 Addition werden die roten Spalten nicht mitgezählt.

Zu Beginn der Codierung wurden die Register mit Nullen zurückgesetzt.

Tabelle 14: Ausgang A

i	D_i	D_{i-1}	D_{i-2}	D_{i-3}	D_{i-4}	D_{i-5}	D_{i-6}	$A_i = \text{Modulo-2}$
0	1	0	0	0	0	0	0	1
1	1	1	0	0	0	0	0	1
2	0	1	1	0	0	0	0	1
3	1	0	1	1	0	0	0	1
4	1	1	0	1	1	0	0	0
5	1	1	1	0	1	1	0	1
6	0	1	1	1	0	1	1	0
7	1	0	1	1	1	0	1	0
8	0	1	0	1	1	1	0	0

Tabelle 15: Ausgang B

i	D_i	D_{i-1}	D_{i-2}	D_{i-3}	D_{i-4}	D_{i-5}	D_{i-6}	$B_i = \text{Modulo-2}$
0	1	0	0	0	0	0	0	1
1	1	1	0	0	0	0	0	0
2	0	1	1	0	0	0	0	0
3	1	0	1	1	0	0	0	1
4	1	1	0	1	1	0	0	1
5	1	1	1	0	1	1	0	1
6	0	1	1	1	0	1	1	0
7	1	0	1	1	1	0	1	0
8	0	1	0	1	1	1	0	0

Tabelle 16: Zusammenfassung der beiden Blöcke (A und B)

I	0	1	2	3	4	5	6	7	8
A	1	1	1	1	0	1	0	0	0
B	1	0	0	1	1	1	0	0	0

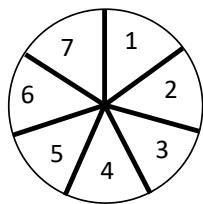
Tabelle 17: Nachfolgende Punktierung

I	0	1	2	3	4	5	6	7	8
A	1	1	1	1	0	1	0	0	0
B	1	0	0	1	1	1	0	0	0

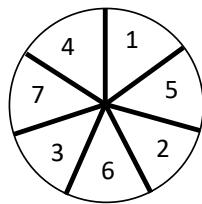
Der codierte Datenstrom am Ausgang ergibt sich damit ist 11-10-11-01-00-00.

4.4.4.8 - Interleaving

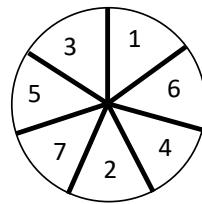
Um die Fehleranfälligkeit weiter zu verbessern werden, nach dem Faltungscodierer, die Daten verschachtelt, damit ein Burstfehler, der bei der Übertragung auftritt, beim Empfänger ausgeglichen werden kann. [Wikipedia-Interleaving] [Rech-WLAN-2012]



Nicht interleaved
(interleaved mit Faktor 1)



Interleaved
mit Faktor 2



Interleaved
mit Faktor 3

Abbildung 61: Interleaving

Interleaving kommt eigentlich aus der Festplatten-Technologie. Da früher die Platten schneller als das Schreiben und Lesen der Daten aus den / in die Caches war, musste die Platte mehrfach unter dem Schreiblese-Kopf gedreht werden bevor alle Daten gelesen waren. Deshalb wurde das Schreiben bzw. Lesen Blockweise versetzt. Der Interleave-Faktor gibt an, wie oft die Platte sich drehen muss, bis alle Daten gelesen wurden

In Abbildung 61 ist auf der linken Seite eine Platte mit 8 Sektoren zu sehen. In der Mitte wird Bei der Datenübertragung wird Interleaving dazu benutzt Burstfehler zu korrigierbaren Einzelfehlern zu machen. Beispiel:

Zu übertragende Daten:

aaaabbbbccccddddeeeeefffffggg.

Bei einer Übertragung ohne Interleaving wird folgendes übertragen:

aaaabbbbccccddddeeeeefffffggg .

Tritt nun ein Burst-Fehler auf, kann das Ergebnis folgendermaßen aussehen:

aaaabbbbccc ____ deeeeefffffggg .

Bei Interleaving werden die Daten folgendermaßen umgestellt:

abcdefgabcdefgabcdefgabcdefg.

Tritt bei der Datenübertragung ein Burstfehler auf, sieht die Information beim Empfänger so aus:

abcdefgabcd ____ bcdedefgabcdefg.

Nach einem De-Interleaving auf der Empfängerseite sieht die Information so aus:

aa _ abbbbccccddde _ eef _ ffg _ gg.

Damit wurde aus einem nicht korrigierbaren Burstfehler 4 korrigierbare Einzelfehler gemacht.

Bei OFDM wird das Interleaving in einer zweistufigen Permutation durchgeführt.

In der ersten Permutation werden Blöcke der Größe N_{CBPS} (Bits pro OFDM-Symbol) verschachtelt.

Die Ableitung erfolgt durch:

$$i = (N_{CBPS}/16) * (k \bmod 16) + \text{floor}(k/16) \quad (5)$$

Wobei gilt:

- $k = 0, 1, \dots, N_{CBPS} - 1$
- N_{CBPS} ist die Anzahl der codierten Bits pro OFDM-Symbol.
Mögliche Werte sind 48, 96, 192, 288.
- Die floor-Funktion bildet eine reelle Zahl (R) auf die nächst kleiner Ganzzahl (Z) ab.
Z. B. $Z = \text{floor}(3,6) = 3$ oder $Z = \text{floor}(-3,6) = -4$

Die zweite Permutation wird folgendermaßen abgeleitet:

$$j = s * \text{floor}(i/s) + [i + N_{CBPS} - \text{floor}(16 * i / N_{CBPS})] \bmod s \quad (6)$$

Wobei gilt:

- $i = 0, 1, \dots, N_{CBPS}$
- $s = \max(N_{BPSC} / 2, 1)$
- N_{BPSC} ist die Anzahl der Bits pro Subcarrier. Mögliche Werte sind 1, 2, 4, 6.
- Die max-Funktion ermittelt den maximalen Wert von zwei Werten.

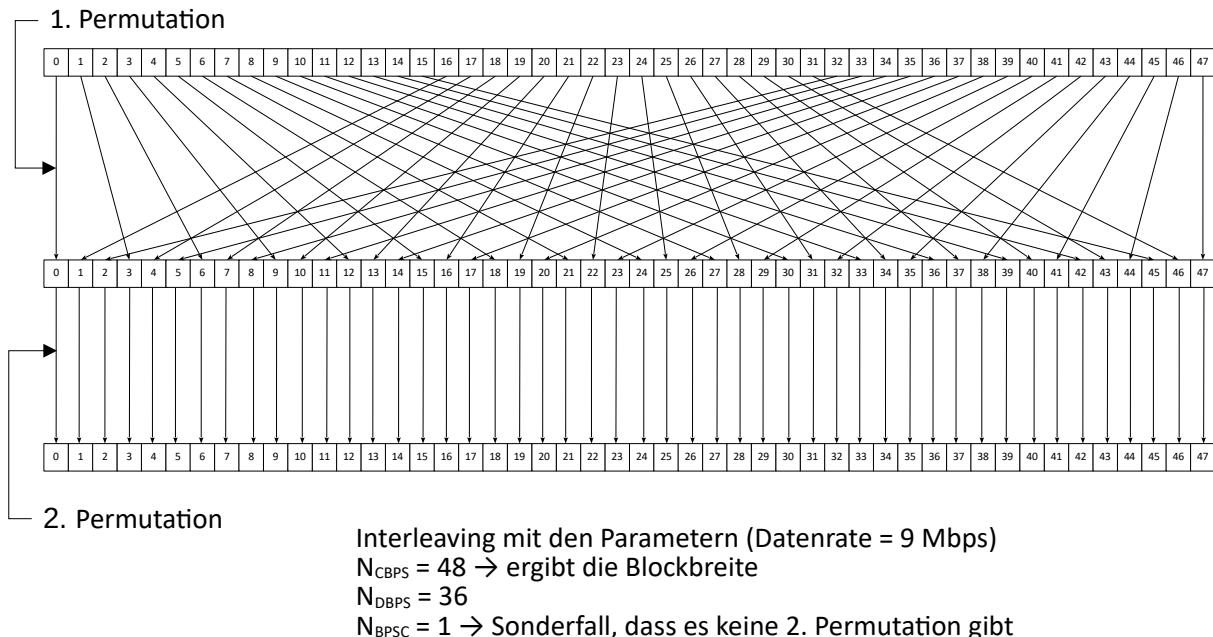


Abbildung 62: Interleaving bei einer Datenrate von 9Mbps

Interessant an der 2. Permutation ist, dass sie erst ab einer Anzahl von 4 Bits pro Subcarrier relevant wird. Siehe hierzu auch Abbildung 62.

Auf der Empfängerseite durchlaufen die Daten zuerst einen Deinterleaver, der die Bits der Unterträger wieder in die ursprüngliche Reihenfolge bringt.

Dabei werden wieder zwei Permutationen durchgeführt.

Die Erste Permutation auf der Empfängerseite ergibt sich aus:

$$i = s * \text{floor}(j/s) + [j + \text{floor}(16 * j / N_{CBPS})] \bmod s \quad (7)$$

Wobei gilt:

$$j = 0, 1, \dots, N_{BPS} - 1$$

Die zweite Permutation auf der Empfängerseite ergibt sich aus:

$$k = 16 * i * (N_{CBPS} - 1) * \text{floor}(16 * i / N_{CBPS}) \quad (8)$$

Wobei gilt:

$$i = 0, 1, \dots, N_{CBPS} - 1$$

Bevor die Daten dem Faltungscodierer zugeführt werden, müssen die durch die Punktierung entfernten Bits mit Füllbits (Dummies) eingefügt werden. Siehe hierzu auch Abbildung 63.

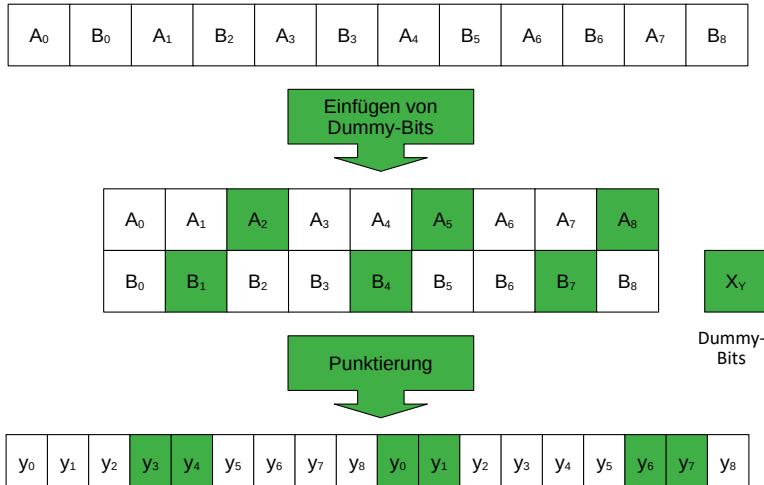


Abbildung 63: Wiederauffüllung der punktierten Bits auf der Empfängerseite

Auf der Empfängerseite wird die Faltung durch einen Viterbi-Algorithmus nicht errechnet, sondern die wahrscheinlichste Bitfolge ermittelt. Das ist die Bitfolge, die über den gesamten Verlauf den kleinsten Hamming-Abstand aufweist.

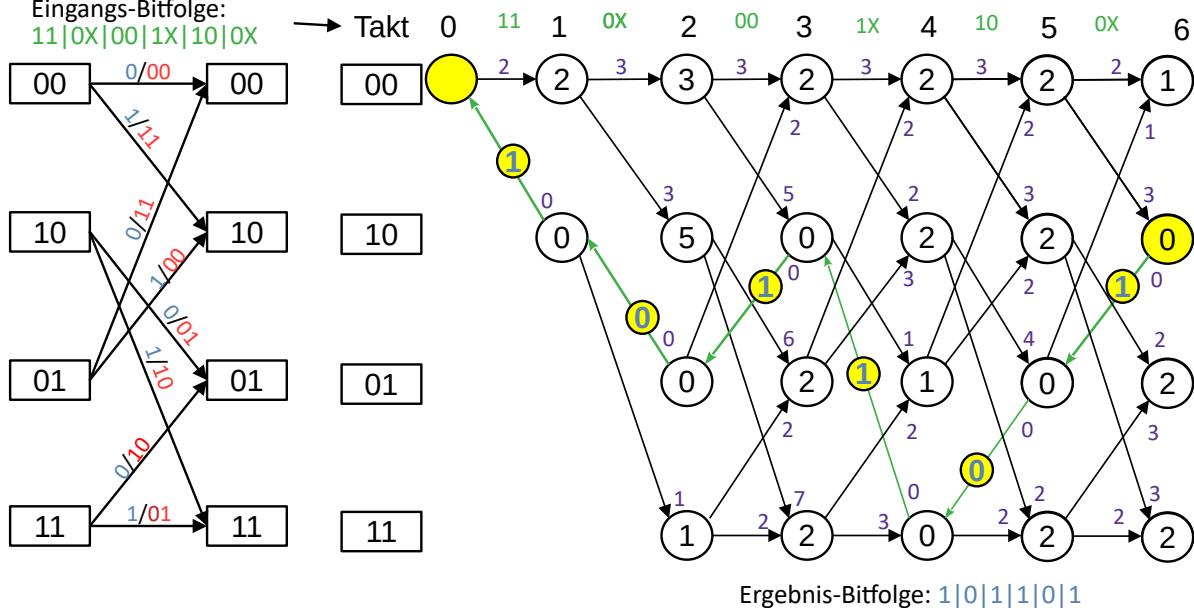


Abbildung 64: Beispiel: Viterbi-Algorithmus

Die einzelnen OFDM-Unterträger sind noch unabhängig von der Datenrate zu modulieren. Dabei werden die Modulationsverfahren BPSK, QPSK, 16-QAM, 64-QAM usw. angewendet. Vorher sind sie in zwei Gruppen mit der Größe N_{BPSC} (1, 2, 4, 6, usw.) aufzuteilen und in komplexe Zahlen zu konvertieren um die xx-QAM-Konstellationspunkte (Q und I) zu repräsentieren. Die Konversion sollte mit Gray-codierten Konstellations-Abbildungen wie in Abbildung 35 erfolgen.

Schließlich werden die komplexen Werte (Q und I), abhängig vom Modulationsverfahren, mit einem Normalisierungsfaktor (K_{MOD}) normalisiert um das Leistungsniveau für alle Teile eines Frames gleich zu halten. Dies ist erforderlich, weil die Modulationsart innerhalb eines Frames (zwischen Signal und Data) wechseln kann.

Tabelle 18 Normalisierungsfaktor (K_{MOD}) je Modulationsverfahren

Modulationsverfahren	Normalisierungsfaktor (K_{MOD})
BPSK	1
QPSK	$1 / \sqrt{2}$
16-QAM	$1 / \sqrt{10}$
64-QAM	$1 / \sqrt{42}$
256-QAM	$1 / \sqrt{170}$

Zum Schluss wird der Strom der komplexen Zahlen in Gruppen von je 48 komplexen Zahlen aufgeteilt, um den Unterträgern zugeführt werden zu können.

4.4.4.9 - Kanalabschätzung mit Trainingssequenzen

Bei der drahtlosen Übertragung von Daten über eine Funkstrecke breiten sich die Funkwellen in allen Richtungen aus. Dabei gibt es eine direkte Verbindung, die so genannte Line of Sight (LOS), zwischen Sender und Empfänger und weitere Ausbreitungswege, die über Reflexionen und Streuungen auch zum Empfänger führen. Allerdings haben die Reflexionen und Streuungen einen weiteren Weg zurückzulegen und kommen damit später beim Empfänger an. Außerdem werden sie durch den längeren Weg auch mehr gedämpft, als bei der direkten Verbindung. Weiterführende Literatur ist unter [BOSBOS-Math] zu finden.

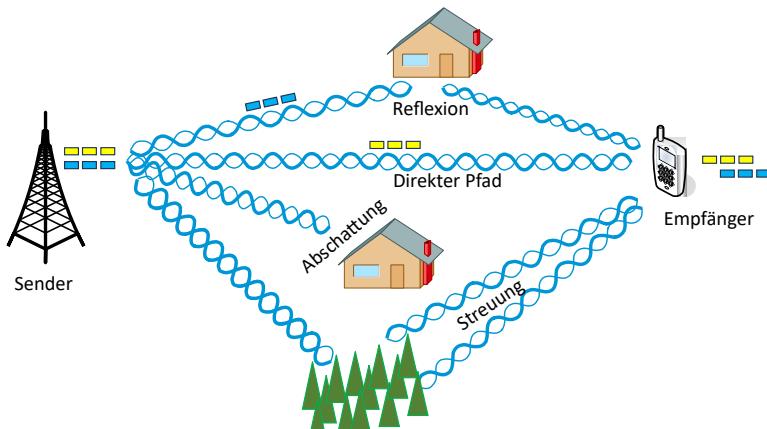


Abbildung 65: Mehrwegeausbreitung

Wenn also das k-te Bit auf dem direkten Weg eintrifft, kann es sein, dass gleichzeitig Bits, die früher gesendet wurden, auf einem anderen Weg auch beim Empfänger eintreffen und sich an der Empfangsanzeige überlagern. Die Überlagerung von Symbolen wird Intersymbolinterferenz genannt.

Bei GSM dauert die Übertragung von einem Bit $T_{\text{bit}} = 3,59 \mu\text{s}$. Durch viele Messungen hat man herausgefunden, dass die maximale Umweglaufzeit $16 \mu\text{s}$ betragen kann. Damit ist es möglich, dass beim Empfänger die Bits k, k-1, k-2, k-3 und k-4 gleichzeitig eintreffen und sich überlagern. Im schlimmsten Fall löschen sich die Symbole gegenseitig aus, was man Signalschwund nennt. Man kennt nur die Summe der Signale und damit nicht die Summanden.

Es gilt also die Anzahl der Pfade, die unterschiedlichen zeitversetzten Symbole und die Dämpfung der Symbole zu ermitteln. Dazu muss der Kanal abgeschätzt werden. Um einen Kanal abzuschätzen, muss beim Senden ein Teil der Nachricht dem Empfänger schon bekannt sein. Diesen Teil der Nachricht nennt man Trainingssequenzen. Mit den beim Empfänger bekannten Trainingssequenzen, kann eine Kanalabschätzung für jeden Frame gemacht werden und so bei einem bewegten Sender oder Empfänger die Kanaleigenschaften ständig angepasst werden.

Bei den Trainingssequenzen sollen n binäre Symbole $(s_0, s_1, \dots, s_k, \dots, s_{n-1})$ von der Basisstation zum Empfänger gesendet werden. Außerdem wird angenommen, dass die Symbole anstatt $\{0, 1\}$ nun $s_i \in \{-1, +1\}$ sind. Dabei gilt:

$$\begin{aligned} 0 &= -1 \\ 1 &= +1 \end{aligned}$$

Bei der mathematischen Operation der Multiplikation gilt:

$$\begin{aligned} -1 \cdot -1 &= +1 \\ -1 \cdot +1 &= -1 \\ +1 \cdot -1 &= -1 \\ +1 \cdot +1 &= +1 \end{aligned}$$

Für unterschiedliche Funkstandards gibt es eine Fülle von Trainingssequenzen. Im folgenden Beispiel soll eine Trainingssequenz aus dem GSM-Standard Verwendung finden. Bei GSM gibt es 8 unterschiedliche Trainingssequenzen mit 16 Bits, von denen eine je nach Land und Provider zum Einsatz kommt. Für das folgende Beispiel soll die folgende Trainingssequenz herangezogen werden:

$(-1, +1, -1, -1, +1, +1, +1, +1, -1, +1, +1, +1, -1, +1, +1, +1)$

Zuerst werden die 16 Bits um weitere 10 Bits erweitert. Dabei werden die ersten 5 Bits hinten angehängt und die letzten 5 Bits vorne vorangestellt.

Damit ergibt sich die folgende Bitfolge:

$+1, +1, -1, +1, +1, -1, +1, -1, -1, +1, +1, +1, +1, -1, +1, +1, -1, +1, +1, -1, +1, -1, -1$

Diese Sequenz mit der Länge von 26 Bit wird als Trainingssequenz gesendet. Auf der Empfängerseite wird die 16Bit große Trainingssequenz an der erweiterten Trainingssequenz schrittweise vorbeigeschoben die Korrelation für jedes Bit ermittelt. Bei jedem Schritt wird die Multiplikation komponentenweise durchgeführt und das Ergebnis aufsummiert.

Schritt -5:

$$\begin{array}{r} +1 +1 -1 +1 +1 -1 +1 -1 -1 +1 +1 +1 +1 -1 +1 +1 +1 -1 +1 -1 -1 \\ -1 +1 -1 -1 +1 +1 +1 -1 +1 +1 +1 -1 +1 +1 +1 +1 \\ \hline -1 +1 +1 -1 -1 +1 -1 +1 +1 +1 +1 -1 -1 +1 +1 = 0 \end{array}$$

Schritt -4:

$$\begin{array}{r} +1 +1 -1 +1 +1 -1 +1 -1 -1 +1 +1 +1 +1 -1 +1 +1 +1 -1 +1 -1 -1 \\ -1 +1 -1 -1 +1 +1 +1 -1 +1 +1 +1 -1 +1 +1 +1 +1 \\ \hline -1 -1 -1 -1 +1 +1 -1 -1 +1 +1 +1 +1 +1 +1 +1 = 0 \end{array}$$

Schritt -3:

$$\begin{array}{r} +1 +1 -1 +1 +1 -1 +1 -1 -1 +1 +1 +1 +1 -1 +1 +1 +1 -1 +1 -1 -1 \\ -1 +1 -1 -1 -1 +1 +1 +1 -1 +1 +1 +1 -1 +1 +1 +1 \\ \hline +1 +1 -1 +1 -1 -1 -1 +1 +1 +1 +1 -1 -1 +1 +1 +1 = 0 \end{array}$$

Schritt -2:

$$\begin{array}{r} +1 +1 -1 +1 +1 -1 +1 -1 -1 +1 +1 +1 +1 -1 +1 +1 +1 -1 +1 -1 -1 \\ -1 +1 -1 -1 -1 +1 +1 +1 -1 +1 +1 +1 -1 +1 +1 +1 \\ \hline -1 +1 +1 -1 +1 -1 -1 +1 +1 +1 -1 +1 -1 +1 +1 -1 = 0 \end{array}$$

Schritt -1:

$$\begin{array}{r}
 +1 +1 -1 +1 +1 -1 +1 -1 -1 +1 +1 +1 +1 +1 -1 +1 +1 -1 +1 -1 -1 \\
 -1 +1 -1 -1 +1 +1 +1 -1 +1 +1 +1 -1 +1 +1 = 0
 \end{array}$$

Schritt 0:

$$\begin{array}{r}
 +1 +1 -1 +1 +1 -1 -1 -1 +1 +1 +1 +1 +1 -1 +1 +1 -1 +1 -1 -1 \\
 -1 +1 -1 -1 +1 +1 +1 -1 +1 +1 +1 -1 +1 +1 = 16
 \end{array}$$

An der Stelle an der die Trainingssequenz mit der gesendeten Trainingssequenz übereinstimmt, ergibt die Korrelation für jede Komponenten den Wert 1, was im Summe 16 ergibt.

Das kann so weiter gemacht werden, bis alle Korrelationen erfolgt sind. Das Ergebnis wird für die noch fehlenden Korrelationen wird auch 0 sein.

Schritt +1:

$$\begin{array}{r}
 +1 +1 -1 +1 +1 -1 +1 -1 -1 +1 +1 +1 +1 +1 -1 +1 +1 -1 +1 -1 -1 \\
 -1 +1 -1 -1 +1 +1 +1 -1 +1 +1 +1 -1 +1 +1 = 0
 \end{array}$$

Schritt +2:

$$\begin{array}{r}
 +1 +1 -1 +1 +1 -1 -1 -1 +1 -1 +1 +1 +1 +1 -1 +1 +1 -1 +1 -1 -1 \\
 -1 +1 -1 -1 +1 +1 +1 -1 +1 +1 +1 -1 +1 +1 = 0
 \end{array}$$

Trägt man die Korrelationswerte über die Zeitverschiebung auf, kommt man auf die folgende Abbildung.

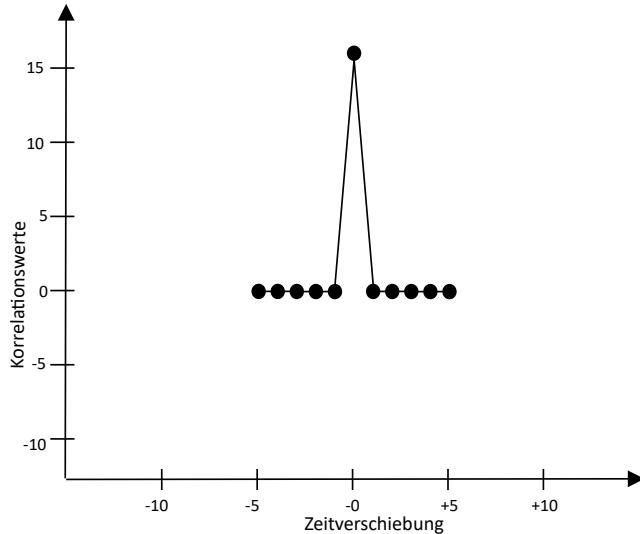


Abbildung 66: Korrelation mit der Trainingssequenz

Erweitert man die Trainingssequenz vorne und hinten nicht um 5 sondern um 14 Stellen, ergibt sich folgende Korrelation.

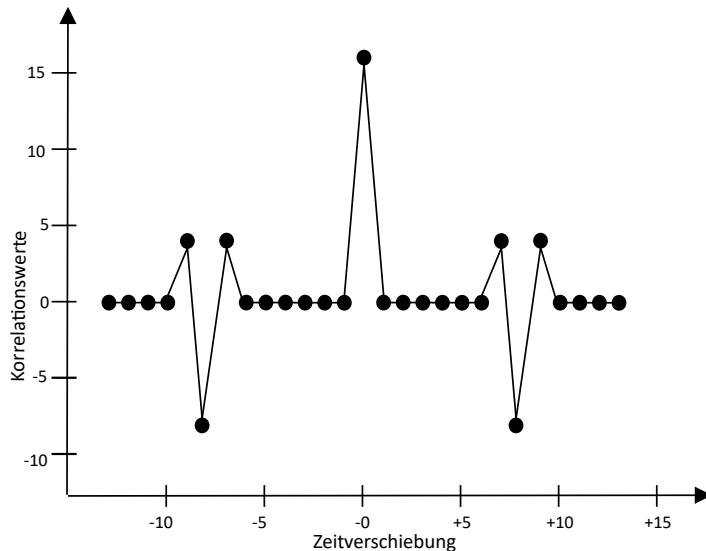


Abbildung 67: Korrelation mit nochmals erweiterter Trainingssequenz

Auch hier zeigt sich, dass die größte Korrelation in der Mitte bei einer Zeitverschiebung von 0 auftritt.

Bei GSM z. B. hat ein Symbol die Zeitliche Dauer $T_s = 3,69\mu s$. Zusammen mit der Lichtgeschwindigkeit kommt man auf eine Ausbreitungslänge von 1,103 km bei einem Symbol. Im flachen Gelände werden die Reflexionen andere sein, als in den Bergen. Doch durch viele Feldstudien wurde ermittelt, dass die maximale Ausbreitungsverzögerung 4 Symbole beträgt. Damit ist es ausreichend mit 4 Symbolen Verzögerung zu rechnen. Leider ist noch ein weiterer Effekt bei der Kanalabschätzung zu berücksichtigen. Jedes reflektierte Signal wird aufgrund der längeren Laufzeit eine größere Dämpfung aufweisen, als die direkte Verbindung. (die übrigens auch eine Dämpfung hat, was für die Berechnungen hier vernachlässigt werden soll)

Mathematisch kann man die Dämpfung eines Signals mit einer Multiplikation des Signals mit einem Faktor a mit $0 \leq a \leq 1$ darstellen.

$$y_k = s_k + a_1 * s_{k-1} + a_2 * s_{k-2} + a_3 * s_{k-3} + a_4 * s_{k-4}$$

Im folgenden Beispiel wird angenommen, dass es zwei Signale mit einer Verzögerung gibt. Die Faktoren für die Dämpfung sollen $a_1 = \frac{1}{4}$ und $a_2 = \frac{1}{8}$ sein. Beim direkten Signal s_k wird der Faktor = 1 angenommen.

$$y_k = s_k + \frac{1}{4} * s_{k-1} + \frac{1}{8} * s_{k-2}$$

$$(1) \ * \ +1 \ +1 \ -1 \ +1 \ +1 \ -1 \ +1 \ -1 \ -1 \ +1 \ +1 \ +1 \ +1 \ -1 \ +1 \ +1 \ -1 \ +1 \ +1 \ \dots \\ (\frac{1}{4}) \ * \ \quad +1 \ +1 \ -1 \ +1 \ +1 \ -1 \ +1 \ -1 \ -1 \ +1 \ +1 \ +1 \ +1 \ -1 \ +1 \ +1 \ +1 \ -1 \ +1 \ +1 \ \dots \\ (\frac{1}{8}) \ * \ \quad +1 \ +1 \ -1 \ +1 \ +1 \ -1 \ +1 \ -1 \ -1 \ +1 \ +1 \ +1 \ +1 \ -1 \ +1 \ +1 \ +1 \ -1 \ +1 \ +1 \ \dots$$

$$y_0 \ y_1 \ y_3 \dots$$

Beginnend mit y_0 empfängt man also:

$$-5/8, 7/8, 9/8, -5/8, 7/8, -7/8, -9/8, -11/8, 5/8, 9/8, 11/8, 11/8, -5/8, 7/8, 9/8, 11/8, -5/8, 7/8, 9/8, -5/8, 7/8, -7/8, -9/8, -11/8$$

Lässt man der Übersicht halber die Nenner weg entsteht:

$$-5, +7, +9, -5, +7, -7, -9, -11, +5, +9, +11, +11, -5, +7, +9, +11, -5, +7, +9, -5, +7, -7, -9, -11$$

Schiebt man die bekannte Trainingssequenz daran vorbei und beginnt die Korrelation bei y_0 erhält man:

$$(-1)(-5) + (1)(7) + (-1)(9) + (-1)(-5) + (-1)(7) + (1)(-7) + (1)(-9) + (1)(-11) + (1)(5) + (-1)(9) + (1)(11) + (1)(11) + (1)(-5) + (-1)(7) + (1)(9) + (1)(11)$$

$$= 5 + 7 - 9 + 5 - 7 - 7 - 9 - 11 + 5 - 9 + 11 + 11 - 5 - 7 + 9 + 11 = 0$$

Auch wenn man bei y_1 und y_2 beginnt wird das Ergebnis = 0 sein. Beim Start bei y_3 ergibt sich erstmals ein anderes Bild:

$$\begin{array}{r} -5 \quad +7 \quad -7 \quad -9 \quad -11 \quad +5 \quad +9 \quad +11 \quad +11 \quad -5 \quad +7 \quad +9 \quad +11 \quad -5 \quad +7 \quad +9 \\ -1 \quad +1 \quad -1 \quad -1 \quad +1 \quad +1 \quad +1 \quad -1 \quad +1 \quad +1 \quad +1 \quad -1 \quad +1 \quad +1 \\ \hline +5 \quad +7 \quad +7 \quad +9 \quad +11 \quad +5 \quad +9 \quad +11 \quad +11 \quad +5 \quad +7 \quad +9 \quad +11 \quad +5 \quad +7 \quad +9 \end{array} = 128$$

Der Wert von 128 geteilt durch 8 ergibt 16. Da dies der Wert ohne Dämpfung sein soll entspricht der ermittelte Wert 16/16. Somit ergibt sich auch der Wert von 16 für die weiteren Nenner bei den Dämpfungsberechnungen.

Beim Start bei y_4 ergibt sich:

$$\begin{array}{r} +7 \quad -7 \quad -9 \quad -11 \quad +5 \quad +9 \quad +11 \quad +11 \quad -5 \quad +7 \quad +9 \quad +11 \quad -5 \quad +7 \quad +9 \quad -5 \\ -1 \quad +1 \quad -1 \quad -1 \quad -1 \quad +1 \quad +1 \quad +1 \quad -1 \quad +1 \quad +1 \quad +1 \quad -1 \quad +1 \quad +1 \\ \hline -7 \quad -7 \quad +9 \quad +11 \quad -5 \quad +9 \quad +11 \quad +11 \quad -5 \quad -7 \quad +9 \quad +11 \quad -5 \quad -7 \quad +9 \quad -5 \end{array} = 32$$

Der Wert von 32 geteilt durch 8 ergibt 4, was 4/16 entspricht und bedeutet, dass dieser Pfad mit dem Faktor $\frac{1}{4}$ gedämpft ist.

Beim Start bei y_5 ergibt sich.

$$\begin{array}{r} -7 \quad -9 \quad -11 \quad +5 \quad +9 \quad +11 \quad +11 \quad -5 \quad +7 \quad +9 \quad +11 \quad -5 \quad +7 \quad +9 \quad -5 \quad +7 \\ -1 \quad +1 \quad -1 \quad -1 \quad -1 \quad +1 \quad +1 \quad +1 \quad -1 \quad +1 \quad +1 \quad +1 \quad -1 \quad +1 \quad +1 \\ \hline +7 \quad -9 \quad +11 \quad -5 \quad -9 \quad +11 \quad +11 \quad -5 \quad +7 \quad -9 \quad +11 \quad -5 \quad +7 \quad -9 \quad -5 \quad +7 \end{array} = 16$$

Das Ergebnis von 16 geteilt durch 8 ergibt 2 was 2/16 bedeutet, und dass dieser Pfad mit dem Faktor $\frac{1}{8}$ gedämpft ist.

Beim Start bei y_6 ergibt sich.

$$\begin{array}{r} -9 \quad -11 \quad +5 \quad +9 \quad +11 \quad +11 \quad -5 \quad +7 \quad +9 \quad +11 \quad -5 \quad +7 \quad +9 \quad -5 \quad +7 \quad -7 \\ -1 \quad +1 \quad -1 \quad -1 \quad -1 \quad +1 \quad +1 \quad +1 \quad +1 \quad -1 \quad +1 \quad +1 \quad +1 \quad -1 \quad +1 \quad +1 \\ \hline +9 \quad -11 \quad -5 \quad -9 \quad -11 \quad +11 \quad -5 \quad +7 \quad +9 \quad -11 \quad -5 \quad +7 \quad +9 \quad +5 \quad +7 \quad -7 \end{array} = 0$$

Ab hier ergibt sich also keine Dämpfung mehr.

4.4.4.10 - OFDM-Übertragungsverfahren

Mit der folgenden Gleichung kann die komplexe Übertragung im Basisband beschrieben werden:

$$r_{RF}(t) = R_e \{ r(t) \exp(j 2 f_c t) \} \quad (9)$$

Wobei der linke Term das zu übertragende Radiofrequenzsignal mit der Zeit und der rechte Teil der Realteil Re {...} der in den geschweiften Klammern angegebenen komplexen Zahl ist. Der Term f_c steht für die Mittenfrequenz des Trägers.

Das übertragene Basissignal setzt sich aus mehreren OFDM-Symbolen zusammen und entspricht der Gleichung:

$$r_{Packet}(t) = r_{Preamble}(t) + r_{Signal}(t - t_{Signal}) + r_{Data}(t - t_{Data}) \quad (10)$$

Wobei:

- ➊ t_{Signal} mit $16\mu\text{s}$
- ➋ t_{Data} mit $20\mu\text{s}$

anzusetzen ist.

Die Koeffizienten stellen die Daten, die Pilotträger und Trainigssymbole dar.

$$r_{\text{SUBFRAME}}(t) = w_{\text{TSUBFRAME}}(t) \sum_{K=-N_{\text{ST}}/2}^{N_{\text{ST}}/2} C_K \exp(j 2 \pi k \Delta_f)(t - T_{\text{Guard}}) \quad (11)$$

Wobei gilt:

- C_K = Koeffizienten
- N_{ST} = 52 (Anzahl der Subcarrier)
- Δ_f = 0,3125 MHz (Frequenzbandabstand der Subcarrier)
- K = Index
- $w_{\text{TSUBFRAME}}(t)$ = Window Funktion

Tabelle 19 Timing Parameter

Parameter	Wert
Gesamtanzahl der Unterträger	52 ($N_{\text{SD}} + N_{\text{SP}}$)
Anzahl der Daten-Unterträger	48
Anzahl der Pilot-Unterträger	4
Frequenzabstand zwischen Unterträgern	0,3125MHz (= 20MHz / 64)
TFFT / FFT / FFT Perle	3,2 μs (1 / Δ_f)
Dauer der PLCL Präambel	16 μs ($T_{\text{SHORT}} + T_{\text{LONG}}$)
Dauer des Signal OFDM-Symbols	4,0 μs ($T_{\text{GI}} + T_{\text{FFT}}$)
Dauer des Guard-Intervalls (GI)	0,8 μs ($T_{\text{FFT}} / 4$)
Dauer des GI im Training-Symbol	1,6 μs ($T_{\text{FFT}} / 2$)
Symbol Intervall	4 μs ($T_{\text{GI}} + T_{\text{FFT}}$)
Dauer der kurzen Trainingssequenz	8 μs (10 * $T_{\text{FFT}} / 4$)
Dauer der langen Trainingssequenz	8 μs ($T_{\text{GI2}} + 2 * T_{\text{FFT}}$)

Die Window Funktion ist eine Rechteckschwingung, die das Fenster nur zu dem gewünschten Intervall öffnet und sonst Null ist, wenn das Fenster geschlossen ist. Der Summenterm führt also nur bei geöffnetem Fester zu einem Ergebnis. Das Zeitfenster kann sich über mehrere Perioden erstrecken und bedeutet das Zeitfenster für das Zeitmultiplexverfahren (TDM) des OFDM-Verfahrens.

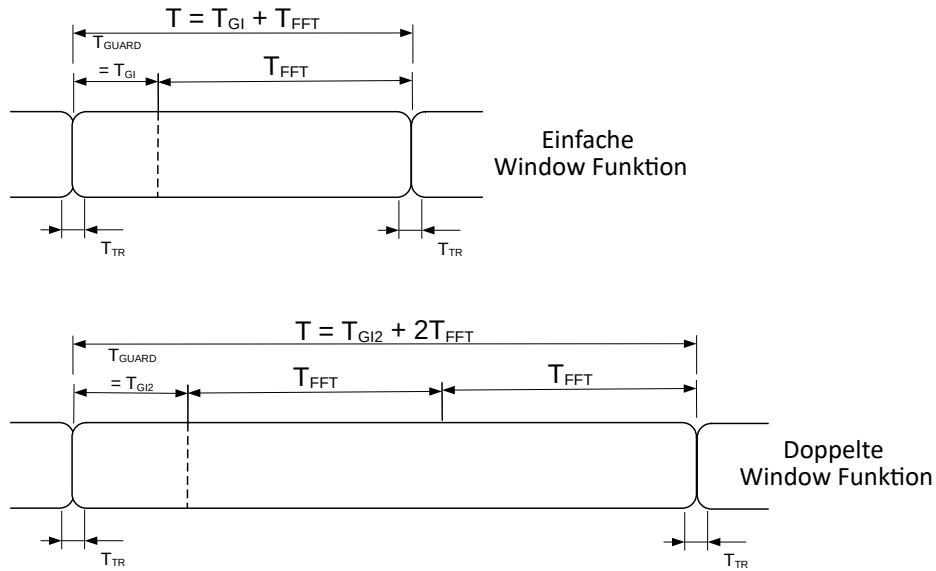


Abbildung 68: Window Funktion in einfacher und doppelter Form

In Abbildung 68 wird ersichtlich, dass das Fenster sich nicht über die Periodendauer erstreckt sondern noch um das Guard-Intervall (GI) verlängert wird. Damit sollen die Einwirkungen von evtl. auftretenden Mehrwegausbreitungen kompensiert werden.

Damit ist die eigentliche Dauer eines OFDM-Symbols:

$$T = T_{GI} + T_{FFT} \quad (12)$$

Reflexionen die kürzer als T_{GI} sind, können keine Symbolinterferenz (ISI) verursachen. Bei IEEE wurde die Dauer von $T_{GI} = T_{FFT}/4$ festgelegt. Da $T_{FFT} = 3,2\mu s$ beträgt, ist die Dauer von $T_{GI} = 800\text{ns}$. Die Gesamtdauer beträgt damit 4 μs .

Wie in Abbildung 69 dargestellt, besteht die PLCP-Präambel aus 10 kurzen Symbolen und zwei langen Trainingssymbolen.

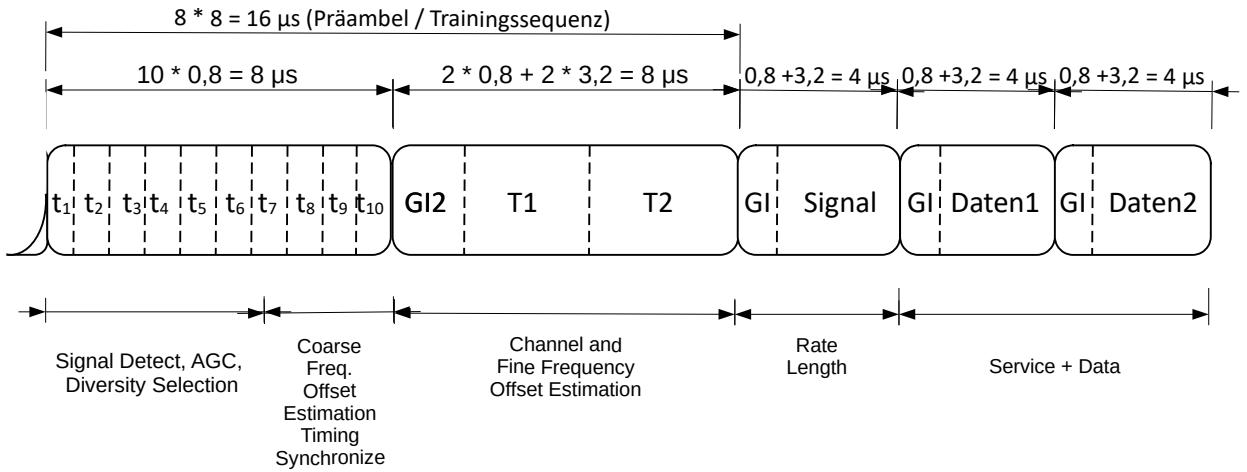


Abbildung 69: OFDM-Trainingsstruktur in der PLCP-Präambel

Beim kurzen Trainingssymbol werden 12 Unterträger mit der folgenden Sequenz verwendet:

$$S_{-26,26} = \sqrt{13/6} * \{0, 0, 1+j, 0, 0, -1-j, 0, 0, 0, 1+j, 0, 0, 0, -1-j, 0, 0, 0, -1-j, 0, 0, 0, 1+j, 0, 0, 0, 0, 0, 0, -1-j, 0, 0, 0, -1-j, 0, 0, 1+j, 0, 0, 0, 1+j, 0, 0, 0, 1+j, 0, 0\}$$

Der Faktor $\sqrt{13/6}$ dient zur Normalisierung der durchschnittlichen Leistung des gesendeten OFDM-Symbols.

Das Signal wird nach der folgenden Gleichung erzeugt:

$$r_{SHORT}(t) = w_{TSHORT}(t) \sum_{k=-N_{ST}/2}^{N_{ST}/2} S_k \exp(j 2\pi k \Delta_F t) \quad (13)$$

Beim langen Trainingssymbol werden alle 53 Unterträger mit der folgenden Sequenz verwendet:

$$L_{-26,26} = \{1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 1, -1, -1, 1, 1, -1, 1, 1, 1, 1, 1, 0, 1, -1, -1, 1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, -1, -1, -1, 1, 1, -1, 1, -1, 1, -1, 1, 1, 1, 1\}$$

$$r_{LONG}(t) = w_{TLONG}(t) \sum_{k=-N_{ST}/2}^{N_{ST}/2} L_k \exp(j 2\pi k \Delta_F (t - t_{GI2})) \quad (14)$$

Die gesamte Trainingssequenz ist 16μs lang.

Nach der Präambel kommt das Signal-Feld. Abbildung 70 Das Signal-Feld besteht aus 24 Bits. Es wird nicht verwürfelt und es soll als einzelnes OFDM-Symbol mit BPSK-Modulation und einer 1 / 2 – Rate gesendet werden.

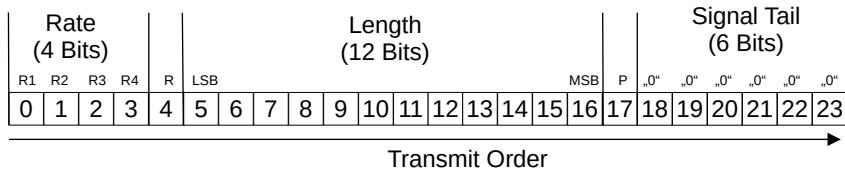


Abbildung 70: Signal-Feld

Das Rate-Feld enthält die Datenrate. Das Bit 4 dient als Reserve.

Tabelle 20 OFDM-Datenraten (Rate-Feld)

R0	R1	R2	R3	Datenrate [Mbps]
1	1	0	1	6
1	1	1	1	9
0	1	0	1	12
0	1	1	1	18
1	0	0	1	24
1	0	1	1	36
0	0	0	1	48
0	0	1	1	54

Die 12 Bits für die Länge beschreiben die Länge des TXVECTORs. Damit sind Werte von 0 bis 4095 möglich. Die 6 Tail-Bits am Ende dienen zur Initialisierung der Faltungscodierer.

Die komplexe Zahl, die zu einem Unterträger k des OFDM-Symbols n korrespondiert ergibt sich zu:

$$d_{k,n} = d_{k+N_{SD}xn}, k=0, \dots, N_{SD}-1, n=0, \dots, N_{SYM}-1 \quad (15)$$

wobei:

N_{SD} = Anzahl Subcarrier für Daten

N_{SYM} = Anzahl der OFDM-Symbole

Ein OFDM-Symbol ist dann definiert als:

$$r_{DATA,n}^{(t)} = w_{T_{SYM}}^{(t)} \sum_{k=0}^{N_{SD}-1} d_{k,n} \exp(j2\pi M(k)\Delta_F(t-T_{GI})) + P_{n+1} \sum_{k=-N_{ST}/2}^{N_{ST}/2} P_k \exp(j2\pi k\Delta_F(t-T_{GI})) \quad (16)$$

wobei:

Die Funktion $M(k)$ ist eine Abbildung vom logischen Unterträger mit der Zahl 0 – 47 auf die Indexe der Frequenzoffsets von -26 bis 26.

Die Pilot-Unterträger und die Center-Frequenz - also der Unterträger mit der Nummer 0 - werden ausgelassen.

Somit gilt für $M(k)$:

$$M(k) = \begin{cases} k-26 & 0 \leq k \leq 4 \\ k-25 & 5 \leq k \leq 17 \\ k-24 & 18 \leq k \leq 23 \\ k-23 & 24 \leq k \leq 29 \\ k-22 & 30 \leq k \leq 42 \\ k-21 & 43 \leq k \leq 47 \end{cases} \quad (17)$$

Berücksichtigt man die zuvor dargestellte Ansteuerung der Pilot Kanäle, so ergibt sich für die Verkettung von OFDM-Symbolen (N_{SYM}) folgende Funktion:

$$r_{DATA}(t) = \sum_{n=0}^{N_{SYM}-1} r_{DATA,n}^{(t-nT_{SYM})} \quad (18)$$

4.4.4.11 - PLCP Sendeprozedur

Um Daten zu übertragen müssen die folgenden Aktivitäten durchgeführt worden sein:

- PHY-CCA.indicate sollte freien Kanal anzeigen
- PHY-TXSTART.request(TXVECTOR)
- PHY muss in den Sendezustand gehen
- PLME muss Frequenz richtig einstellen

Im TXVECTOR wurden die Parameter für Datenrate, Service, Länge, und Sendeleistung mitgegeben. Damit kann die PHY-PLCP mit den Primitiven PMD-TXPWRLLV und PMD-RATE die PMD konfigurieren.

Danach sendet die PHY-PLCP ein PMD-TXSTART.request und kann danach damit beginnen den Header aufzubauen.

Sobald die Übertragung der Präambel begonnen hat, muss die PHY die Datenverwürfelung und die Codierung anstoßen.

Die PHY fährt dann mit dem Prozess der PSDU-Übertragung fort indem sie eine Anzahl von Oktetten von der MAC übernimmt. Die PLCP-Header, das SERVCE-Feld und die PSDU werden mit dem Faltungscodierer verschlüsselt.

Auf der PMD-Teilschicht werden dann die Daten oktettweise gesendet. Die Übertragung kann von der MAC nach dem Senden des letzten Oktetts (gemäß der Angabe in Length-Field) mit dem Primitiv PHY-TXEND.request beendet werden.

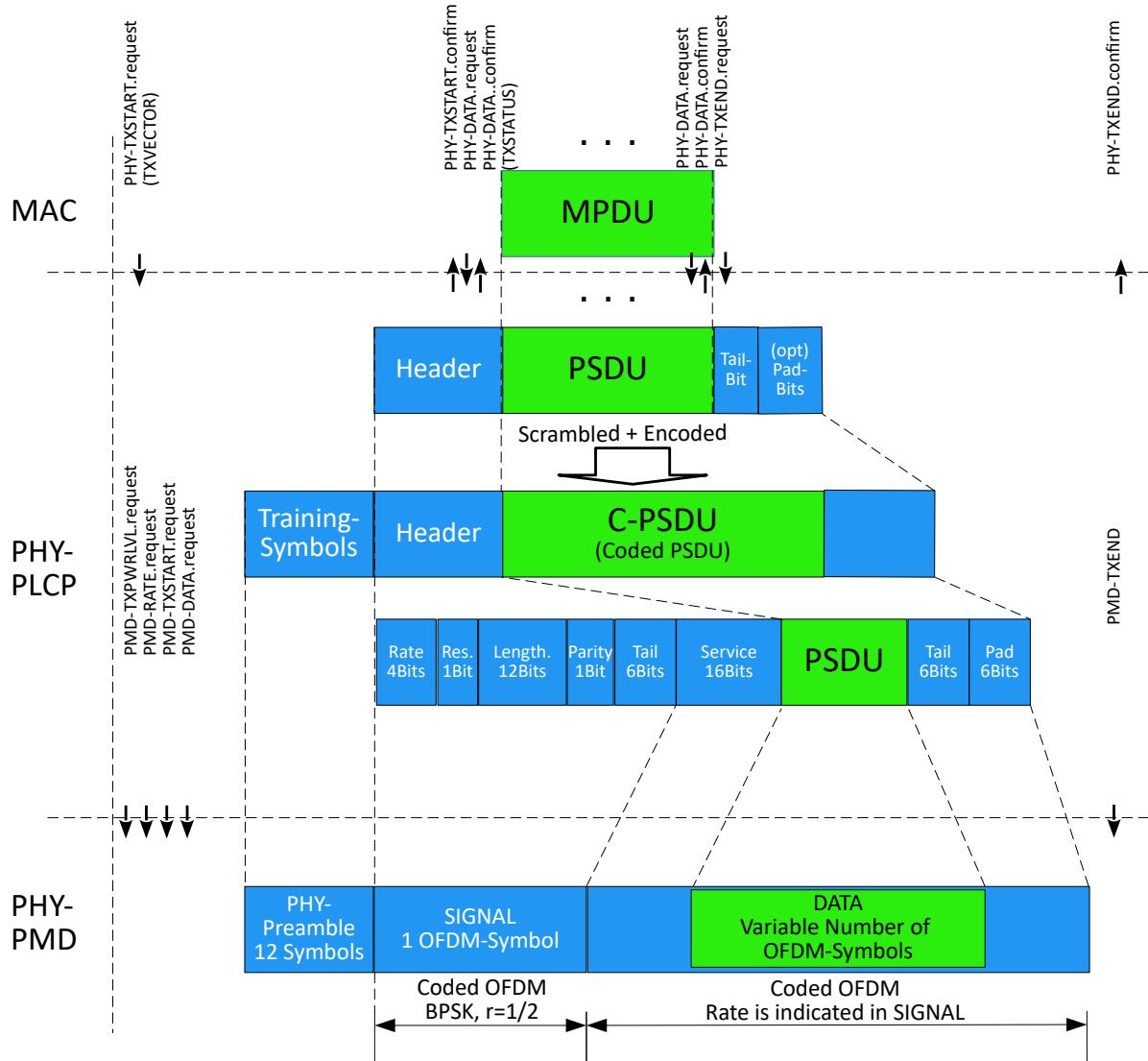


Abbildung 71: Transmit-PHY

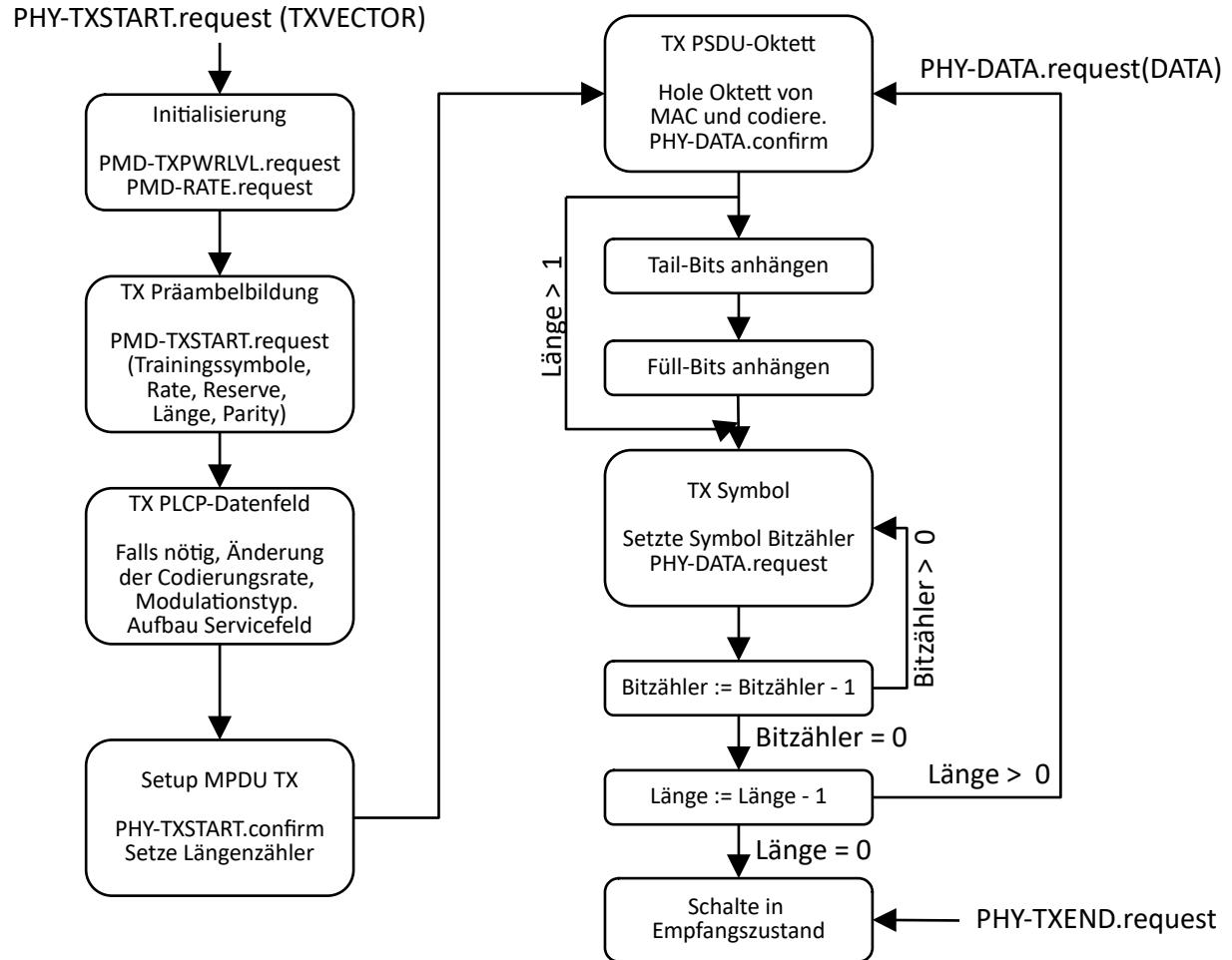


Abbildung 72: Endlicher Kontrollautomat Senden

4.4.4.12 - PLCP Empfangsprozedur

Angestoßen wird die Empfangsbearbeitung durch die PHY-CCA.indication.

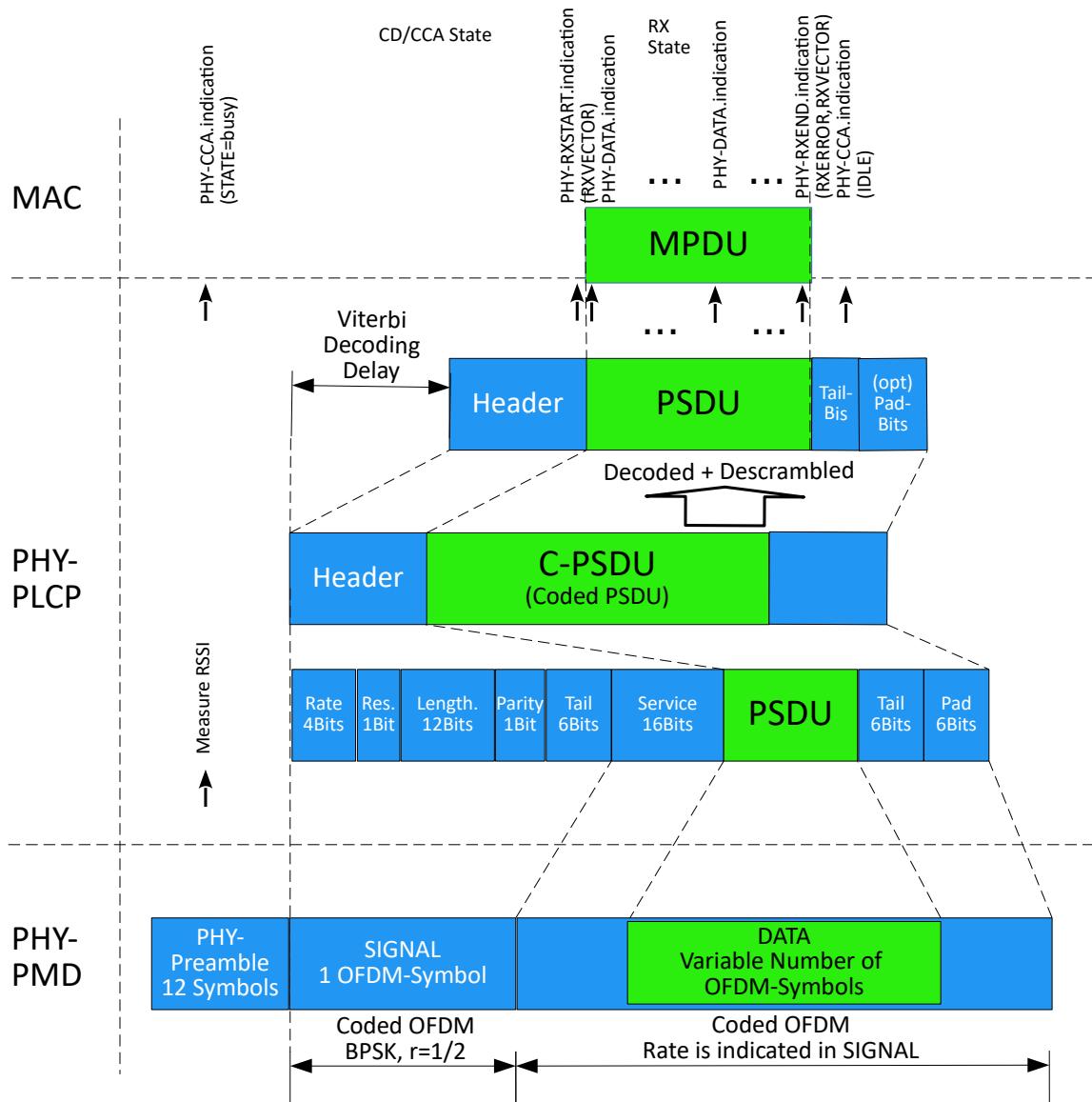


Abbildung 73: Receive-PHY

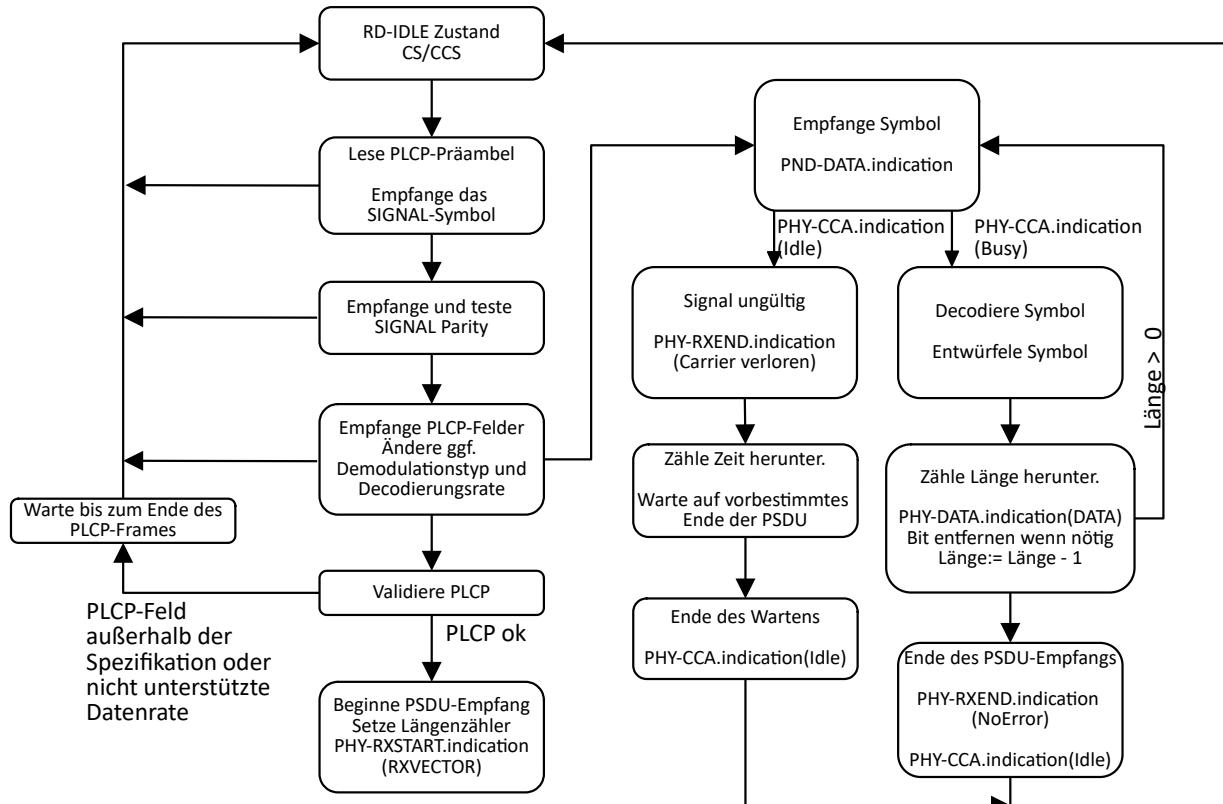


Abbildung 74: Endlicher Kontrollautomat Empfangen

Tabelle 21 Charakteristische OFDM-Parameter [Rech-WLAN-2012]

Parameter	Wert
aSlotTime	9 µs
aSIFSTime	16µs
aCCATime	< 4µs
aMPDUMaxLength	4095 Bytes
aCWmin	15
aCWmax	1023
Dauer für Präambel	20µs
Dauer für PLCP-Header	4µs

Tabelle 22 OFDM-Empfänger-Empfindlichkeit [Rech-WLAN-2012]

Datenrate	Empfindlichkeit
6 MBit/	-82 dBm
9 MBit/s	-81 dBm
12 MBit/s	-79 dBm
18 MBit/s	-77 dBm
24MBit/'s	-74 dBm
36 MBit/s	-70 dBm
48 MBit/s	-66dBm
54 MBit/s	-65 dBm

4.4.5 - Vergleich von FHSS DSSS und OFDM

In der ursprünglichen Definition der WLANs (IEEE802.11) waren FHSS und DSSS festgelegt worden um die Übertragung der Daten gegen Störungen zu schützen.

DSSS hat sich bei der weiteren Entwicklung noch länger halten können. Moderne Verfahren setzen alle auf OFDM

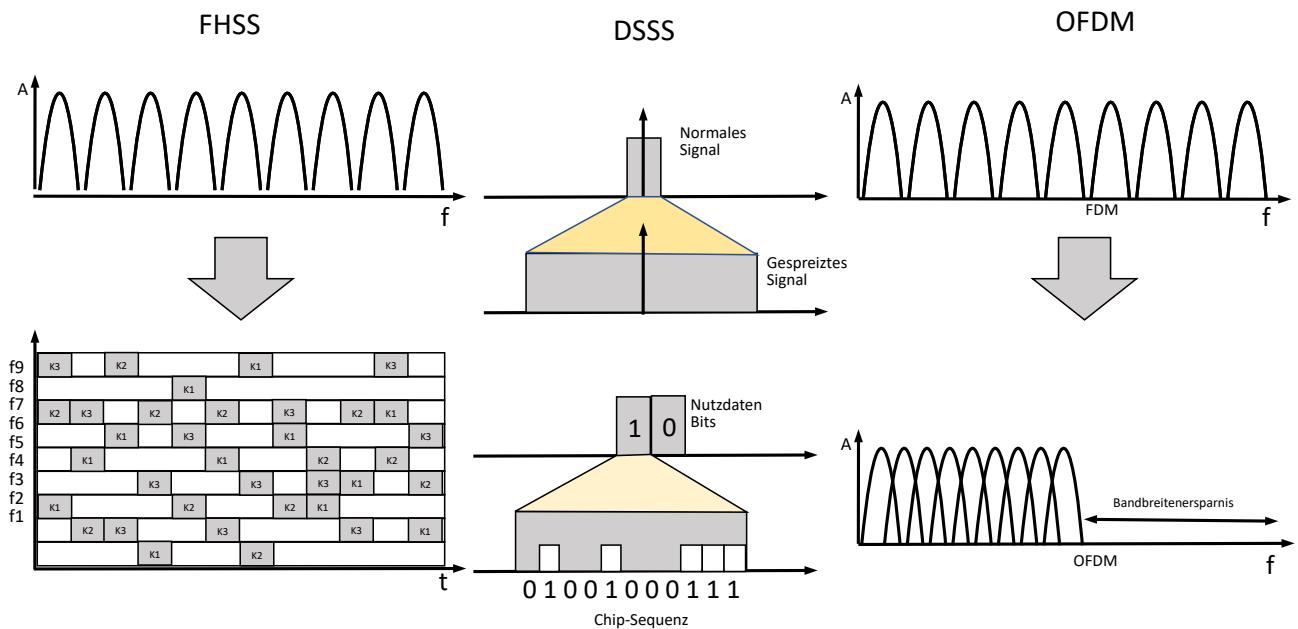


Abbildung 75: Vergleich von FHSS, DSSS und OFDM
da sich damit höhere Datenübertragungsraten erzielen lassen.

Tabelle 23 Zusammenfassung der 802.11-PHY-Implementierungen [Rech-WLAN-2012] (erweitert)

Standard	Übertragungsverfahren	Frequenzband	Datenrate
802.11	FHSS	2,4 GHz	1 und 2 MBit/s
802.11	DSSS	2,4 GHz	1 und 2 MBit/s
802.11	Optisch	850 nm	1 und 2 MBit/s
802.11b	DSSS	2,4 GHz	5,5 und 11 MBit/s
802.11b	PBCC	2,4 GHz	5,5 und 11 MBit/s
802.11a	OFDM	5 GHz	6, 9, 12, 18, 24, 36, 48, und 54 MBit/s
802.11g	OFDM	2,4 GHz	6, 9, 12, 18, 24, 36, 48, und 54 MBit/s
802.11g	PBCC	2,4 GHz	22 und 33 MBit/s
802.11n	OFDM	2,4 GHz oder 5 GHz	Bis 600 MBit/s
802.11ac	OFDM	5 GHz	Bis 6,9333 GBit/s
802.11ad	SC oder OFDM	60 GHz	Bis 6,75675 GBit/s
802.11ax	OFDMA	2,4 / 5 / 6 GHz	Bis 9,6 GBit/s

4.5 - MAC-Ebene

Wie auf der PHY-Ebene sind auch auf der MAC-Ebene bei diversen Standard-Erweiterungen Änderungen erfolgt. In diesem Kapitel geht es um die grundsätzlichen Mechanismen die auf der MAC-Ebene abgehandelt werden. Die Änderungen werden dann bei den jeweiligen Standards abgehandelt.

Im Gegensatz zu kabelgebundenen LANs sind WLANs zusätzlichen Störeinflüssen ausgesetzt. Dazu zählen z. B. Bluetooth, Bewegungsmelder, Mikrowellenherde und Wetterradar. Weiterhin ist Funk ein Shared Medium und deshalb muss ein Zugriffsverfahren zum Einsatz kommen, um den Medium-Zugriff der teilnehmenden Stationen zu koordinieren.

Wie beispielsweise bei Ethernet werden bereits auf MAC-Ebene Prüfsummen eingeführt, um möglichst schon auf dieser Ebene fehlerhafte Übertragungen zu verwerfen. Zusammen mit den eingeführten Quittungen, die im Fehlerfall ausbleiben, können die erforderlichen Wiederholungen angestoßen werden. Oberstes Ziel bei der Datenübertragung ist, möglichst viele Daten fehlerfrei in kürzester Zeit zu übertragen. Wiederholungen von Übertragungen können nicht ausgeschlossen werden, sind jedoch so weit wie möglich zu vermeiden.

Die Wahrscheinlichkeit einer Störung steigt bei wachsender Länge der Datenübertragung. In WLANs sind Datenteile mit einer Größe von bis zu 4095 Bytes vorgesehen. Je mehr Daten in einem Block übertragen werden sollen desto länger dauert die Datenübertragung und desto größer ist die Wahrscheinlichkeit, dass die Übertragung einer Störung zum Opfer fällt. Deshalb wurde bereits auf der MAC-Ebene eine Fragmentierung eingeführt.

Auf MAC-Ebene werden bei WLANs die folgenden Themen behandelt:

- ➊ Adressierung. Je nach Konstellation
- ➋ Medien-Zugriffsverfahren (CSMA/CA)
- ➌ Bildung von Prüfsummen (CRC)
- ➍ Quittierung (ACK)
- ➎ Fragmentierung und Reassemblierung

4.5.1 - MPDU-Header-Aufbau

In Abbildung 76 ist der MPDU-Aufbau dargestellt. In ihm werden die oben aufgeführten Themen abgehandelt.

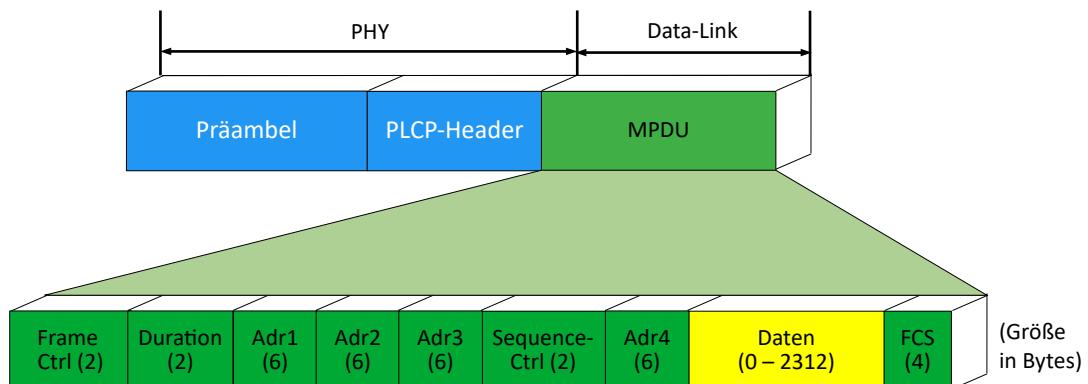


Abbildung 76: IEEE-802.11-MPDU-Header-Format

4.5.1.1 - Frame-Control-Feld

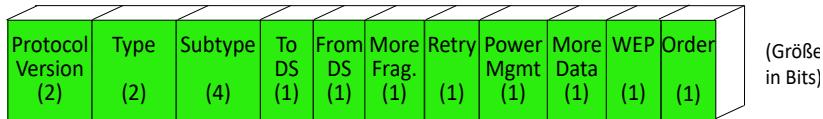


Abbildung 77: MPDU-Control-Feld

Tabelle 24 Frame-Control-Feld

Subfield-Name	Größe in Bits	Bedeutung	Werte
Protocol-Version (b1, b0)	2	Momentan nicht genutzt	00
Type (b3, b2)	2	Unterscheidung von Subtype in Management, Control, Data und Extension	00 = Management 01 = Control 10 = Data 11 = Extension
Subtype (b7, b6, b5, b4)	4	Bei Type = 00 = Management	0000 = Association Request 0001 = Association Response 0010 = Reassociation Request 0011 = Reassociation Response 0100 = Probe Request 0101 = Probe Response 0110 = Timing Advertisement 0111 = Reserved 1000 = Beacon 1001 = ATIM 1010 = Disassociation 1011 = Authentication 1100 = Deauthentication 1101 = Action 1110 = Action No Ack (NACK) 1111 = Reserved
		Bei Type = 01 = Control	0000, 0001 = Reserved 0010 = Trigger 0100 = Beamforming Report Poll 0101 = VHT / HE NDP Announcement 0110 = Control Frame Extension 0111 = Control Wrapper 1000 = Block ACK Request (BAR) 1001 = Block ACK (BA) 1010 = PS-Poll 1011 = RTS 1100 = CTS 1101 = ACK 1110 = CF-End 1111 = CF-End + CF-ACK
		Bei Type = 10 = Data	0000 = Data 0001 = Data + CF-ACK 0010 = Data + CF-Poll 0011 = Data + CF-ACK + CF-Poll 0100 = Null (no data) 0101 = CF-ACK (no data) 0110 = CF-Poll (no data) 0111 = CF-ACK+ CF-Poll (no data) 1000 = QoS Data 1001 = QoS Data + CF-ACK 1010 = QoS Data + CF-Poll 1100 = QoS Null (no data) 1101 = Reserved 1110 = QoS CF-Poll (no data) 1111 = QoS CF-ACK + CF-Poll (no data)
		Bei Type = 11 = Extension	0000 = DMG Beacon

Subfield-Name	Größe in Bits	Bedeutung	Werte
			0001 – 1111 Reserved
To DS	1	Zielbestimmung	0 = Daten sind nicht für das Distributionssystem bestimmt 1 = Daten sind für das Distributionssystem bestimmt
From DS	1	Herkunftsbestimmung	0 = Daten sind nicht vom Distributionssystem 1 = Daten sind vom Distributionssystem
More Fragments	1	Fragmente	0 = weitere Fragmente werden nicht folgen 1 = weitere Fragmente werden folgen
Retry	1	Wiederholung	0 = Frame ist kein Teil einer Wiederholung 1 = Frame ist ein Teil einer Wiederholung
Power-Management	1	Power-Management-Information	0 = Wechsel in den Energiesparmodus 1 = Station bleibt aktiv
More Data	1	Weitere Daten folgen	0 = nein 1 = ja
Protected Frame (WEP)	1	Datenverschlüsselung mittels WEP	0 = aus 1 = ein
+HTC/Order	1	Verlangt Weitergabe an das übergeordnete Protokoll in der Sender-Reihenfolge	0 = aus 1 = ein

4.5.1.2 - Duration-Feld

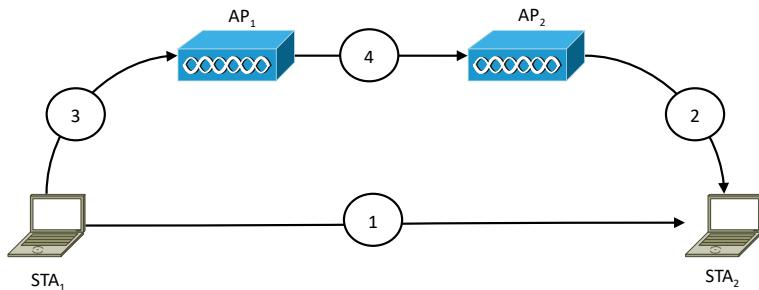
Die unterschiedliche Verwendung des 16 Bit lange Duration-Feldes wird in Bit 15 und 14 festgelegt.

Tabelle 25 Duration-Feld

Bit 15	Bit 14	Bit 13 - 0	Verwendung
0	0 – 32767		Anzeige der Zeit für die benötigte Übertragung
1	0	0	Fester Wert für Frames, die während der CFP übertragen werden
1	0	1 - 16383	Reserviert
1	1	0	Reserviert
1	1	1 - 2007	AID innerhalb eines PS-Poll-Frames
1	1	2008 – 16383	Reserviert

4.5.1.3 - Adress-Felder

Die Adressierung mit MAC-Adressen ist in WLANs aufwändiger als in kabelgebundenen LANs. In Abbildung 76 sieht man nach dem Control- und dem Duration-Feld die ersten 3 MAC-Adressen. Nach dem Sequenzzähler kommt dann noch eine 4. MAC-Adresse.



Auffällig beim MPDU-Header ist die Verwendung von 4 Adressfeldern für die MAC-Adresse.
Für alle möglichen Fälle der Kommunikation zwischen APs und Stationen wird unterschieden.

Abbildung 78: Verwendung der 4 MAC-Adressen

Es gilt folgender Zusammenhang:

Fall	To DS	From DS	Adr. 1 (Empfänger)	Adr. 2 (Sender)	Adr. 3	Adr. 4
1	0	0	MAC-Adr.	MAC-Adr.	BSSID	N / A
2	0	1	MAC-Adr.	BSSID (MAC-AP)	Source. MAC-Adr.	N / A
3	1	0	BSSID (MAC-AP)	MAC-Adr.	Dest. MAC-Adr.	N / A
4	1	1	Receiver-Adr.	Transmitter-Adr.	Dest. MAC-Adr.	Source. MAC-Adr.

Die BSSID entspricht der MAC-Adr. des APs und ist eine eindeutige Zuordnung zu einer Funkzelle.

Fall 1

Kommunikation verläuft innerhalb der Funkzelle zwischen zwei Stationen (von STA₁ zu STA₂) im Ad-hoc-Modus in einem IBSS.

Multicasts und Broadcasts werden nur an die höheren Schichten weiter geleitet, wenn die BSSID übereinstimmt um zu vermeiden, dass sie in einer fremden IBSS empfangen und fälschlicherweise interpretiert werden. Das Feld Adr. 4 wird nicht genutzt.

Fall 2

Hier sendet ein AP (AP₂) einen Frame aus einem Distributionsnetzwerk an eine Station (STA₂). Im Feld Adr. 3 steht die MAC-Adresse des Gerätes, das die Daten ursprünglich erzeugt hat. Das Feld Adr. 4 wird nicht genutzt.

Fall 3

Hier sendet eine Station (STA₁) einen Frame an einen AP (AP₁), der den Frame über ein Distributionsnetz weiter leitet. Im Feld Adr. 3 steht die MAC-Adresse des eigentlichen Ziels. Das Feld Adr. 4 wird nicht genutzt.

Fall 4

Hier werden zwei LANs über ein WLAN miteinander verbunden. Das entspricht einer Richtfunkstrecke und in der Abbildung 4 dem Bridge-Modus. Adr.2 entspricht der Sender Adresse (AP₁). Die Adr.1 entspricht der Empfänger Adresse (AP₂). Die MAC-Adresse des ursprünglichen Senders (STA₁) steht im Feld Adr.4 und die MAC-Adresse des eigentlichen Ziels (STA₂) steht im Feld Adr.3.

4.5.1.4 - Sequence-Feld

Mit diesem Feld wird die Steuerung der Fragmentierung durchgeführt. Siehe auch hierzu das Kapitel Fragmentierung

4.5.1.5 - Daten-Feld

Im Datenteil kommt als erstes der LLC-SNAP-Header. Er wird benötigt, um Ethernet-Pakete über Nicht-Ethernet-Medien zu transportieren. Er benötigt 8 Byte.

Dann folgt das eigentliche Ethernet-Frame mit maximal 2304 Byte und die Prüfsumme mit 4 Byte.

IEEE-802.11 hat drei Frameformate festgelegt.

Die Frames werden im Type-Feld voneinander unterschieden:

- Management Frames

Bei den Management-Frames sind die Header etwas kürzer geraten. Sie dienen zum Aufbau der Service-Sets (Funkzellen), die An- und Abmeldung von Clients an den AP sowie der Synchronisation der Clients untereinander.

Zusätzlich sind die so genannten Beacons auch Management-Frames. In ihnen werden detaillierte Informationen der jeweiligen Funkzelle übertragen. Diese Frames werden nicht verschlüsselt.

- Control Frames

Control-Frames sind die kürzesten Frames. Sie besitzen keine MSDU. Zu den Control-Frames zählen z. B. ACK-, RTS- und CTS-Frames. Diese Frames werden nicht verschlüsselt.

- Daten Frames

Wie der Name schon sagt, dienen die Datenframes zur Datenübertragung. Datenframes sind die einzigen Frames, die verschlüsselt übertragen werden. Dazu wird die MSDU nach WEP verschlüsselt und um 8 Bytes verlängert.

4.5.1.6 - Frame Check Sequence – Feld (FCS)

Das 4 Byte lange Feld beinhaltet die CRC-Prüfsumme welche über den Frame-Header und die Frame-Daten gebildet werden. Das verwendete Generatorpolynom lautet:

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1 \quad (19)$$

4.5.2 - Kanalzugriff

Da es sich bei allen Funknetzen immer um ein Shared Media handelt, ist auch ein Kanalzugriffsverfahren anzuwenden. Als besondere Schwierigkeit gilt hier, dass eine Kollision nicht wie bei Ethernet erkannt werden kann. Das liegt daran, dass beim Senden ein gleichzeitiges Abhören der Luftschnittstelle dazu führt, dass man man sich nur selbst erkennen kann. Kollisionen können also nicht direkt erkannt werden. Nur durch Prüfsummen oder ähnliche Mechanismen werden Probleme erkannt und die Frames verworfen. Wegen der fehlenden Quittungen werden dann die Frames wiederholt.

4.5.2.1 - Zugriffsverfahren

Es gibt zwei Zugriffsverfahren:

- DCF (Distributed Coordination Funktion)

Hierbei wird das Zugriffsverfahren über alle Teilnehmer verteilt realisiert

- ◆ Mit CSMA/CA (obligatorisch)
- ◆ Mit RTS/CTS (optional)

- PCF (Point Coordination Function) mit QoS-Unterstützung

Hierbei wird das Zugriffsverfahren an einer zentralen Stelle (also dem AP) realisiert

4.5.2.2 - Erweiterungen zu DCF und PCF

Mit IEEE-802.11e wurden für die Nutzung von zeitkritischen Sprach und Videodaten Erweiterungen eingeführt die eine Priorisierung unterschiedlicher Daten ermöglicht. Mit der Enhanced Distribution Channel Access Function (EDCAF) wurde DCF erweitert und mit der Hybrid Coordination Function (HCF) wurde die PCF ergänzt. Näheres siehe Seite: 188] (QoS-Erweiterungen) oder [IEEE-802.11e-2005]

Für die Koordinierung des Medienzugriffs bei vermaschten Strukturen wurde die Mesh Coordination Function (MCF) definiert. Siehe auch [IEEE-802.11-2016].

4.5.2.3 - DCF

Normalerweise verwendet IEEE-802.11 und die darauf aufbauenden Standards als Zugriffsverfahren CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance). Dort ist es im Rahmen der DCF (Distributed Coordination Funktion) realisiert. Wie im Namen bereits hinterlegt, handelt es sich um eine verteilte Funktion, bei der die Stationen selbstständig den Medienzugriff abhandeln. Deshalb lassen sich damit sowohl Ad-hoc-Netzwerke als auch Infrastruktur-Netzwerke aufbauen.

Nach dem Senden eines Frames muss für die Dauer eines so genannten Inter Frame Spaces (IFS) gewartet werden, bevor mit dem Medien-Zugriffsverfahren begonnen werden kann.

IFS werden zu verschiedenen Funktionen herangezogen. (Näheres im folgenden Kapitel)

Mit dem Start von CSMA/CA verläuft vorerst alles wie bei CSMA/CD. Bevor gesendet werden kann, muss der Kanal zuerst abgehört (CS = Carrier Sense) werden ob er frei ist. Bei den IEEE-802.11-WLANs wird das im Rahmen des Clear Channel Assessments (CCA) abgehandelt.

Ist der Kanal frei, dann können alle Stationen gleichberechtigt auf den Kanal zugreifen (MA = Multiple Access).

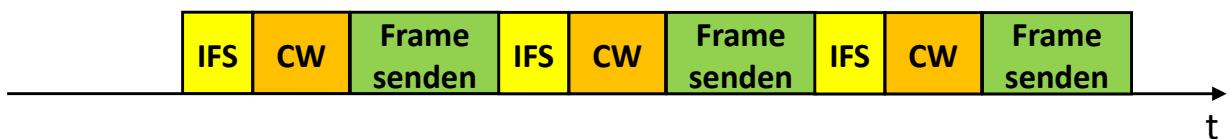


Abbildung 79: CSMA/CA

Wollen nun mehrere Stationen gleichzeitig senden, gilt es Kollisionen zu vermeiden. (Collision Avoidance = CA). Deshalb stehen sie vorerst für die Zeit eines Contention Window (CW) in einem Wettbewerb um den Medium-Zugriff.

4.5.2.3.1 - Backoff-Time

Dabei ermittelt jede Station aus einem Intervall eine zufällige Backoff-Time (BO):

$$\text{Backoff Time} = \text{Random}() \times a\text{SlotTime} \quad (20)$$

Wobei Random() eine Funktion zur Ermittlung einer integer Pseudo-Zufallszahl aus dem Intervall [0, CW] ist. CW ist ein Integer-Wert innerhalb der PHY-spezifischen Werte aCWmin und aCWmax. Ebenso ist aSlotTime von der PHY abhängig.

Die Station, bei der die Backoff-Time als erstes abgelaufen ist, kann mit dem Senden beginnen.

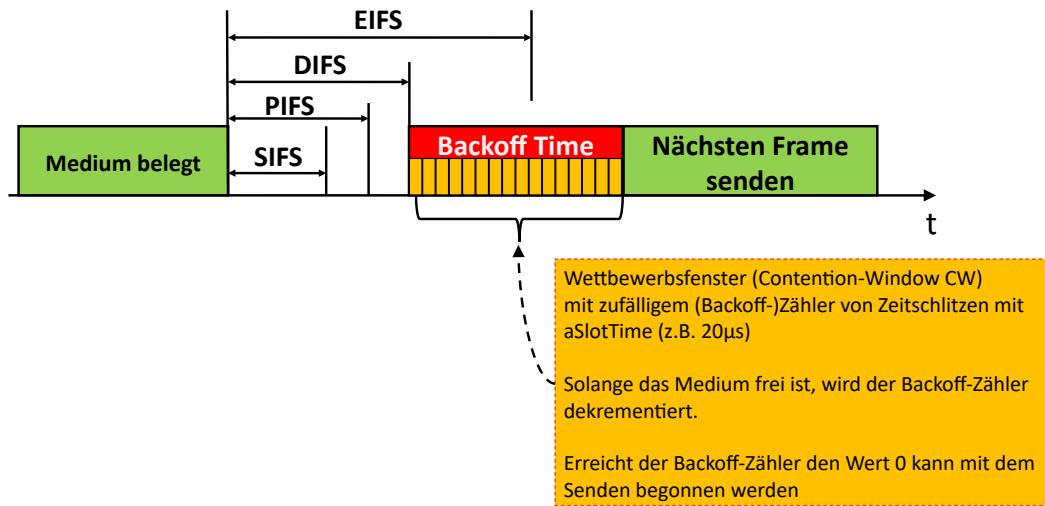
Alle anderen Stationen bekommen mit, dass eine Station mit dem Senden begonnen hat. Aus dem Header des gerade gesendeten Frames können sie die Zeit bis zum Ende des Sendevorgangs (mitsamt Quittung) entnehmen. Mit dieser Information setzen sie bei sich den Network Allocation Vector (NAV). Erst nach Ablauf des NAV startet ein neuer Sendeversuch mit einem neuen CW.

4.5.2.3.2 - Inter Frame Spaces (IFS)

Eine Station ermittelt mit dem Clear Channel assessment (CCA), ob ein Kanal belegt ist, oder nicht. Die Zeitspanne zwischen zwei Frames nennt man Inter Frame Space (IFS). Im Zusammenhang mit WLANs wurden 10 unterschiedliche IFSs definiert, um unterschiedliche Prioritätsstufen für den Medium-Zugriff zur Verfügung zu stellen:

- RIFS Reduced IFS
- SIFS Short IFS
- PIFS PCF IFS
- DIFS DCF IFS
- AIFS Arbitration IFS (für QoS)
- EIFS Extended IFS
- SBIFS Short Beamforming IFS
- BRPIFS Beam Refinement Protocol IFS
- MBIFS Medium Beamforming IFS
- LBIFS Long Beamforming IFS

Die Zuordnung der Zeiten werden in den Primitiven PHY-TXEND.confirm, PHY-TXSTART.confirm, PHYRXSTART.indication und PHY-RXEND.indication vorgenommen.



In Abbildung 80 sind die Zusammenhänge der gängigsten IFS dargestellt. Die anderen aktuellen IFS-Typen werden im entsprechenden Kapitel erläutert.

- ➊ RIFS (Reduced Inter Frame Spacing) entspricht einem SIFS und wurde bei IEEE-802.11 eingeführt.
- ➋ SIFS (Short Inter Frame Spacing)

Dies ist im ursprünglichen Standard das kürzeste und damit auch das Zeitintervall mit der höchsten Priorität. Es wird als Wartezeit vor dem Senden der folgenden Informationen verwendet:

- ➌ Quittung (ACK) auf ein Daten-Frame. Damit ist sichergestellt, dass Frames unmittelbar nachdem sie gesendet wurden, vom Empfänger quittiert werden können
- ➍ CTS als Sendeberechtigung nach Sendeberechtigungsanforderung mittels RTS
- ➎ Zweite und folgende MSDU aus einem Fragment Burst
- ➏ PIFS (PCF IFS)

Mittlere Priorität, für zeitbegrenzte Dienste mittels PCF. PIFS ist kürzer als das DIFS. Damit kommt die PCF früher zum Zug als die DCF. PIFS wird berechnet mit:

$$PIFS = aSIFSTime + aSlotTime \quad (21)$$

- ➐ DIFS (DCF Inter Frame Spacing)

DIFS hat die niedrigste Priorität und dient den Stationen die CSMA/CA verwenden zur Koordinierung des Medienzugriffs bei der DCF. Unter der DCF entspricht es der Zeit, die nach dem Senden eines Frames verstreichen muss, bevor eine Station senden darf. DIFS wird berechnet mit:

$$DIFS = aSIFSTime + 2 \times aSlotTime \quad (22)$$

- ➑ EIFS (Extended Inter Frame Spacing)

EIFS wird bei Stationen angewandt die im DCF-Modus arbeiten. Sind die von der MAC-Ebene übergebenen Daten nicht korrekt wird die Aussendung von der PHY abgebrochen. In diesem Fall wird der Kanal wieder nach dem Ablauf des EIFS freigegeben und es muss nicht auf den Ablauf der Zeit bis zum Duration/ID-Feld im NAV-Feld gewartet werden. Damit kann eine empfangende Station genug Zeit, eine negative Quittung senden. EIFS wird berechnet mit:

$$EIFS = aSIFSTime + DIFS + (8 \times ACK - Länge) + Präambel - Länge + PLCP - Header - Länge \quad (23)$$

Tabelle 26 PHY-abhängige IFS-Werte

PHY-Typ	SIFS [μs]	PIFS [μs]	DIFS [μs]	EIFS [μs]
FHSS	28	78	128	396
DSSS	10	30	50	364
DSSS (Short Frame)	10	30	50	268
802.11a/h (OFDM)	16	25	34	186
802.11g (OFDM) (nur ERP)	16	25	34	186
802.11g (OFDM) (ERP und nonERP)	10	30	50	268
Infrarot 1 MBit/s	10	18	26	185

4.5.2.3.3 - Quittungen

Broadcasts und Multicasts werden nicht quittiert. Unicasts können nach Ablauf von SIFS quittiert werden.

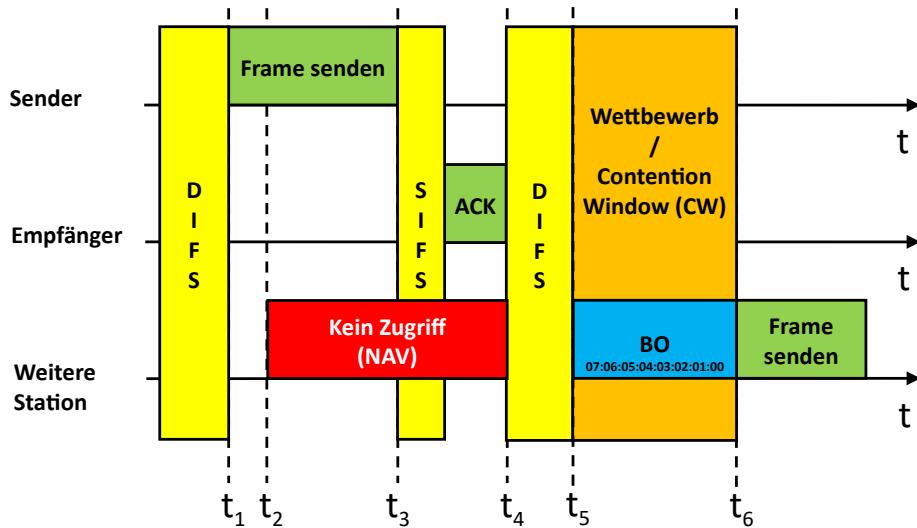


Abbildung 81: Unicast-Quittungen

- t₁ Wurde für einen Zeitraum länger als DIFS nicht gesendet, kann sofort gesendet werden, wenn der Back-off Timer = 0 ist.
- t₂ Eine weitere Stationen will Daten senden. Vor dem Senden muss sie prüfen, ob der Kanal belegt ist. Sie kann den gerade gesendeten Frame auch empfangen und aus dem Header die benötigte Sendezeit extrahieren. Mit diesem Wert kann sie die Wartezeit, bis der Kanal wieder frei ist im Network Allocation Vector (NAV) hinterlegen und so lange warten.
- t₃ Nachdem der erste Frame gesendet wurde muss für SIFS gewartet werden, bevor eine Quittung gesendet werden kann.
- t₄ Nach dem Senden der Quittung können die anderen Stationen nicht sofort senden. Es muss für den Zeitraum DIFS gewartet werden, bevor die anderen Stationen um den Kanal in Konkurrenz treten können.
- t₅ Nach dem Ablauf von DIFS beginnt das Contention-Window, in dem die sendewilligen Stationen um den Kanalzugriff konkurrieren können. Die weitere Station hat einen Backoff Timer von 7 ermittelt. Da der Kanal gerade frei ist läuft der Timer ab.
- t₆ Sobald der Backoff-Timer abgelaufen ist, kann sie mit dem Senden begonnen werden.

Mit einem ACK-Frame kann der Empfänger dem Sender mitteilen, dass die Datenübertragung erfolgreich war.
Abbildung 82 zeigt den Aufbau.

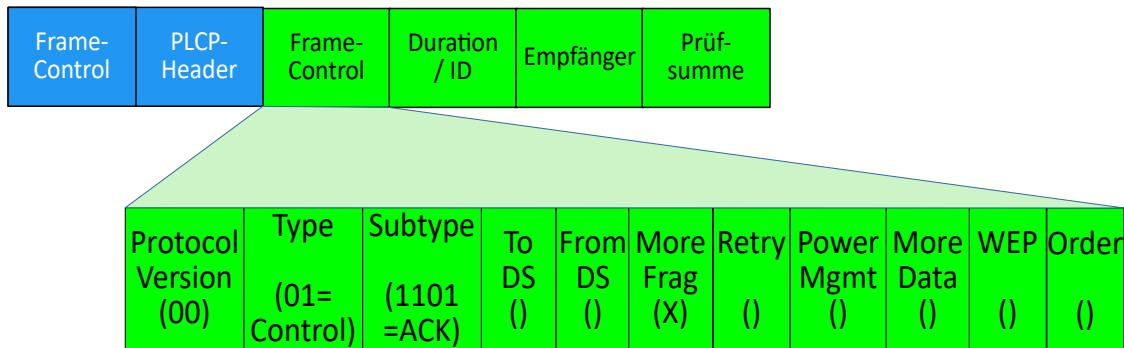


Abbildung 82: ACK-Frame-Format

Das Type-Feld zeigt mit dem Wert 10 an, dass es sich um ein Control-Frame handelt und der Subtype von 1101 zeigt an, dass es sich um ein ACK-Frame handelt.

Das Duration/ID-Feld ist von den zu quittierenden Daten abhängig.

Wurde ein Daten-Frame übertragen ist der Wert 0, denn mit dem ACK-Frame ist die Datenübertragung abgeschlossen und es kann nach einem DIFS mit einem CW für die nächste Datenübertragung weiter gemacht werden.

Wird ein Fragment quittiert, steht im Duration/ID-Feld die Dauer für die Übertragung der Fragmente.

4.5.2.3.4 - DCF Ablaufbeispiel

Die oben beschriebenen Zusammenhänge sollen nochmals in folgenden Ablaufbeispiel erklärt werden.

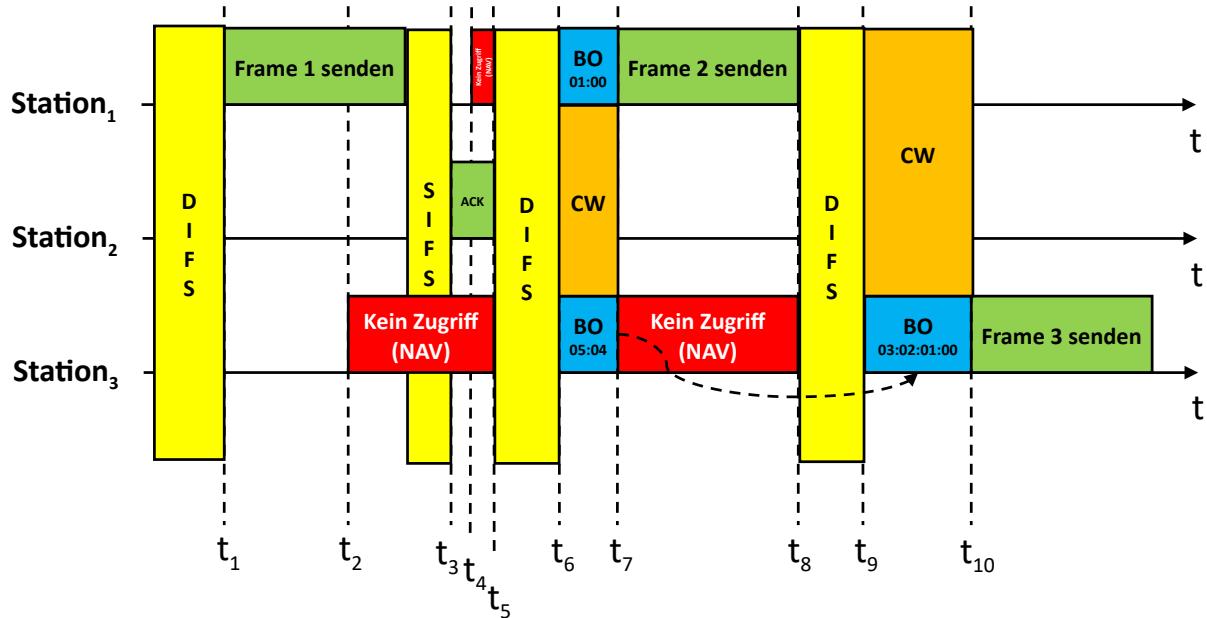


Abbildung 83: Ablaufbeispiel

Zeitpunkt

- t₁ Sta₁ will einen Frame an Sta₂ senden und stellt fest, dass der Kanal länger als DIFS nicht genutzt wurde und der Backoff-Zähler = 0 ist. Daher kann Station₁ sofort mit dem Senden beginnen.
- t₂ Sta₃ möchte Daten senden und stellt fest, dass bereits Daten gesendet werden. Nun muss gewartet werden bis das Senden der Daten abgeschlossen wurde. Dazu setzt Sta₃ den NAV und wartet. In der Zwischenzeit errechnet Sta₃ den Backoffwert (5)
- t₃ Sta₁ hat das Senden der Daten abgeschlossen und nach dem Ablauf von SIFS sendet der Empfänger (Sta₂) einen Quittung (ACK = Acknowledge)
- t₄ Noch während die Quittung gesendet wird möchte Sta₁ die nächsten Daten senden, muss jedoch warten. In der Zwischenzeit errechnet Station₁ den Backoffwert (1)
- t₅ Die Quittung ist abgeschlossen. Danach kann jedoch nicht sofort gesendet werden. Erst muss DIFS ablaufen.
- t₆ Nach dem Ablauf von DIFS startet das Contention Window (CW). In dieser Zeit laufen die Backoff-Timer der wartenden Stationen ab.
- t₇ Der Backoff-Timer von Station₁ ist als erster abgelaufen und der Kanal ist noch frei. Daher kann Sta₁ mit dem Senden eines Broadcasts (Frame 2) beginnen. Station₃ erkennt das Senden von Sta₁ und hält das Herunterzählen seines Backoff-Timers an. Zusätzlich wird der NAV gesetzt.
- t₈ Sta₁ hat das Senden eines Broadcasts beendet. Darauf muss nicht auf eine Quittung gewartet werden. Deshalb kommt hier kein SIFS sondern DIFS als nächstes.

- t₉ Nach Ablauf von DIFS startet das nächste CW. Nun ist der Kanal wieder frei und es läuft die Restzeit des Backoff-Timers von Station₃ ab.
- t₁₀ Der Backoff-Timer von Station₃ ist abgelaufen und der Kanal ist noch frei. Daher kann Sta₃ jetzt mit dem Senden beginnen.

Dieses Verfahren kann nicht vermeiden, dass Kollisionen entstehen. Eine Kollisionserkennung kann in Funknetzen nur durch einen Rückkanal erfolgen. Deshalb wird ein Unicast-Paket vom Empfänger immer nach einem SIFS mit ACK quittiert. Bleibt eine Quittung aus, wird der Sendevorgang wiederholt. Dies geschieht bis zu einer maximalen Anzahl von Übertragungsversuchen. Ist dann immer noch keine Quittung eingetroffen, wird das Paket verworfen.

Beispiel:

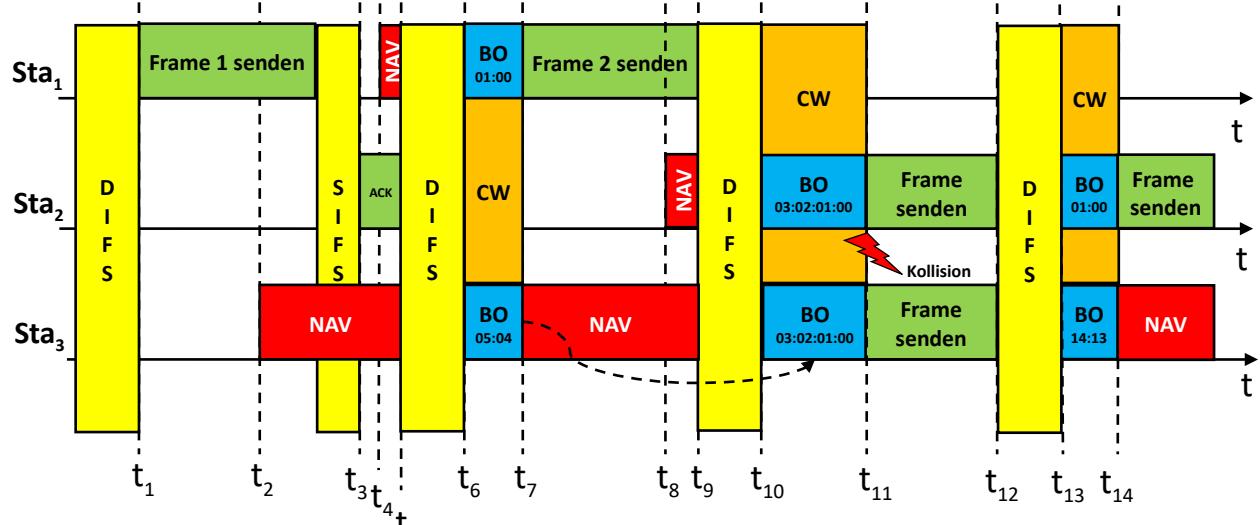


Abbildung 84: WLAN-Kollision und deren Auflösung

Ausgehend von Abbildung 83 ergibt sich zum Zeitpunkt t_8 eine Änderung.

- t_8 Angenommen während Sta_1 den zweiten Frame, einen Broadcast, sendet will Sta_2 noch einen Frame senden. Da der Kanal belegt ist kann kein Zugriff erfolgen und es wird NAV gesetzt und ein Back off-Zähler (3) ermittelt. Dies ist jedoch zufällig der selbe wert, die auch Sta_3 noch als Rest-Backoff-Zähler hat.
- t_9 Nach dem Senden von Frame 2 ist noch für die Zeit von DIFS zu warten bevor das CW losläuft.
- t_{10} Sobald das CW losläuft, zählen sowohl Sta_2 als auch Sta_3 den Backoff-Zähler herunter, da der Kanal frei ist.
- t_{11} Zufällig erreichen beide Zähler gleichzeitig den Wert 0. Der Kanal ist gerade frei und beide Stationen (Sta_2 und Sta_3) beginnen zu senden. Dadurch kommt es zur Kollision!
- t_{12} Eigentlich müssten jetzt Quittungen nach Ablauf eines SIFS erfolgen. Da diese jedoch ausbleiben werden noch vor Ablauf von DIFS jeweils eine neue Backoff-Zähler ermittelt. ($Sta_2 = 1$, $Sta_3 = 14$)
- t_{13} Mit Beginn des CWs laufen die BO-Zähler wieder herunter.
- t_{14} Der BO-Zähler von Sta_2 läuft als erster ab. Da der Kanal frei ist kann der Frame der Sta_2 gesendet werden. Sta_3 muss den BO-Zähler anhalten, NAV setzen und warten.

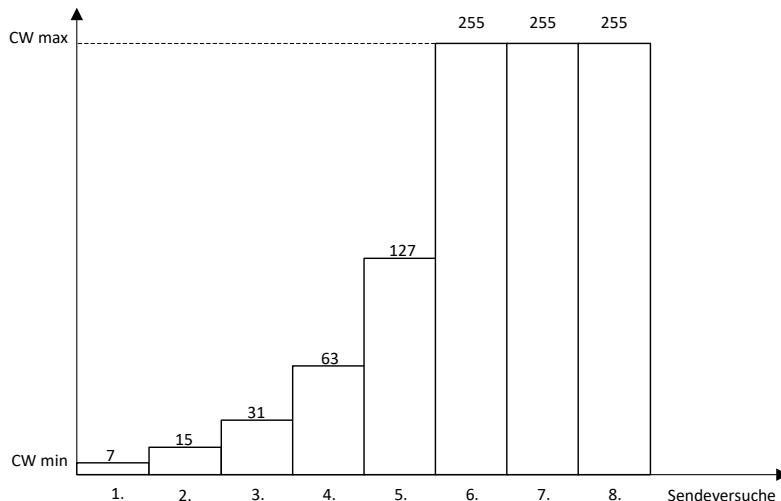


Abbildung 85: Exponentieller Backoff

Sollte es durch Probleme oder großen Sendeandrang mehrere Zugriffsversuche benötigen um ein Paket zu senden, dann wird bei jedem erneutem Sendeversuch die Backoff Time aus einem exponentiell wachsenden Intervall ermittelt. Damit wird die Backoff Time im statistischen Mittel exponentiell ermittelt.

Dies geschieht indem die Obergrenze des Intervalls bei jedem erneuten Sendeversuch exponentiell bis zum Wert CW_{max} vergrößert wird.

Ist CW_{max} erreicht, bleibt es bei dieser maximalen Intervall-Größe.

Die Anzahl der Sende-Wiederholversuche wird in zwei Zählern überwacht. Sie werden STA short retry count (SSRC) und STA long retry count (SLRC) genannt.

Welcher Zähler bei einem misslungenen Sendeversuch hochgezählt wird hängt von der Framelänge ab. Die Aufteilung in kurze und lange Frames wird über den Parameter RTS-Threshold vorgenommen. Ist bei einem Fehlversuch die Länge der PSDU kleiner oder gleich RTS-Threshold wird SSRC hochgezählt. Ist die Länge größer als RTS-Threshold, wird SLRC hochgezählt.

Damit kann auf Probleme bei der Übertragung selektiv zwischen kurzen und langen Frames unterschieden werden. Die Zähler werden zurückgesetzt falls ein ACK- oder CTS-Frame empfangen wurde. Das Maximum der Wiederholversuche wird im Parameter dot11ShortRetryLimit und dot11LongRetryLimit festgelegt.

IEEE-802.11 schlägt für die Tabelle Dot11OperationEntry als Default die folgenden Werte vor:

Tabelle 27: Default Werte für die Obergrenzen bei den Wiederholungen

Parameter	Wert
dot11RTSThreshold	65535
dot11ShortRetryLimit	7
dot11LongRetryLimit	4

4.5.2.3.5 - Einstellung von RTS/CTS

Mit dem Wert für Dot11RTSThreshold lässt sich auch das Verhalten einer Station bezüglich RTS/CTS beeinflussen. Mit dem Wert 0 wird RTS/CTS eingeschaltet, denn das würde bedeuten, dass bereits beim ersten Sendeversuch das Ergebnis mit einem Sendeabbruch beendet wäre. Das ist auch nicht notwendig da es bei RTS/CTS keine Fehlversuche beim Medienzugriff gibt.

Mit einem Wert größer als der maximalen PSDU-Größe wird RTS/CTS ausgeschaltet, denn dann könnten selbst kurze Frames bis zum Wert für dot11RTSThreshold wiederholt werden. Mit dem Default-Wert von 65535 wird RTS/CTS ausgeschaltet.

4.5.2.3.6 - Hidden-Station-Problem

Beim Hidden-Station-Problem (auch Hidden-Terminal-Problem genannt) kann es vorkommen, dass Stationen in einem Funknetz aufgrund von Hindernissen oder Reichweite-Problemen nicht alle Teilnehmer in einem Funknetz erkennen können.

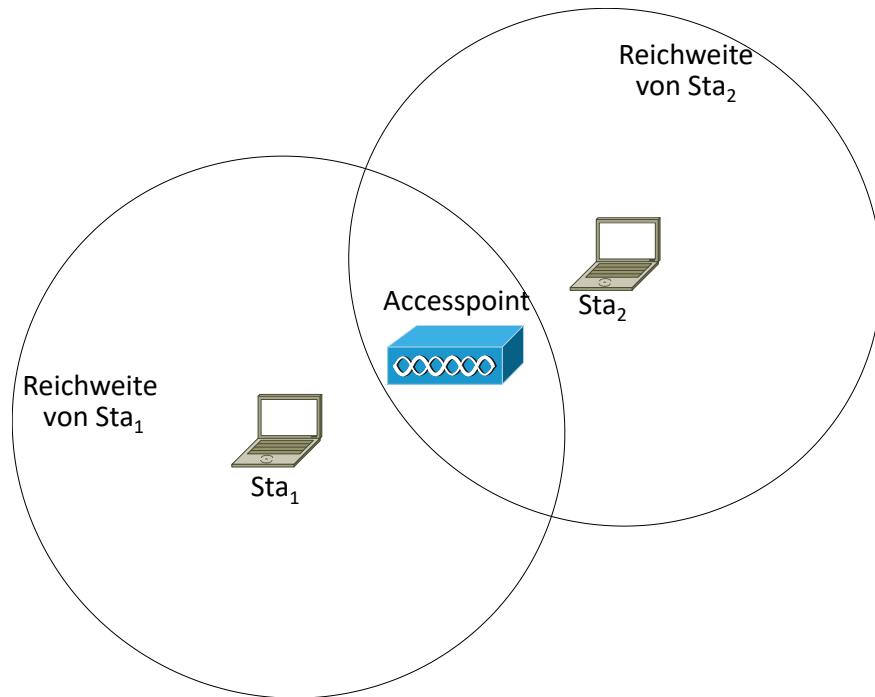


Abbildung 86: Hidden Station Problem

Sta₁ kann zwar den Accesspoint sehen, jedoch aufgrund von zu geringer Reichweite die Sta₂ nicht.

Umgekehrt kann Sta₂ auch den Accesspoint sehen jedoch die Sta₁ nicht.

Dies führt dazu, dass beide Stationen gleichzeitig anfangen zu senden, denn sie können nicht erkennen, dass der Kanal bereits belegt ist.

Die Daten der beiden Stationen überschneiden sich am Accesspoint und führen dort zur Kollision.

Durch Erhöhung oder Verminderung der Sendeleistung der Stationen kann das Problem nicht grundsätzlich gelöst werden.

Abhilfe bei diesem Dilemma kann die Konfiguration von RTS/CTS auf den Geräten herbeiführen.

RTS / CTS (Request to send / Clear to Send)

Es handelt sich hierbei um Kontrollpakete. Ein RTS-Paket wird vorab mit der Längeninformation des folgenden Pakets gesendet.

Bei erfolgreicher Übertragung antwortet der Empfänger mit einem Bestätigung (CTS).

Die Funktionen im Zusammenhang mit RTS/CTS müssen vom Administrator manuell vorgegeben werden.

Dazu ist der Wert von RTS-Threshold geändert. Im Default Fall steht er auf 65536. Damit ist RTS/CTS ausgeschaltet. Werte zwischen 1 und 65535 werden dazu genutzt die Zähler für die Wiederholungen von kurzen und langen Frames auseinander zu halten. Ein Wert von 0 schaltet RTS/CTS ein. Die Einstellung ist an jeder Station vorzunehmen.

Dies gilt damit ebenfalls für die Fragmentierung da dort RTS/CTS auch genutzt wird.

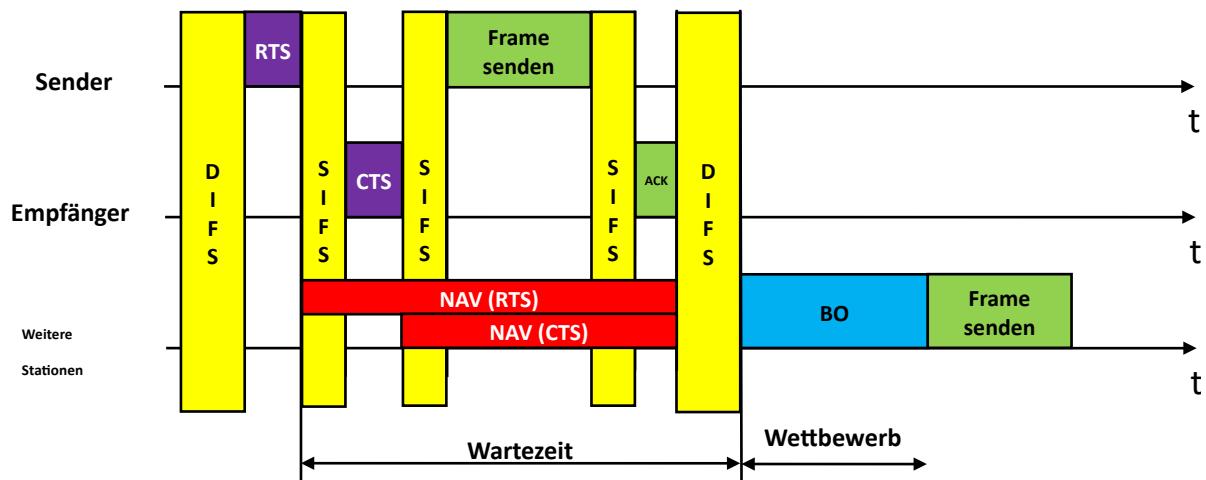


Abbildung 87: RTS/CTS

Diese Funktionen sind nur für niedrige bis mittlere Last effizient.

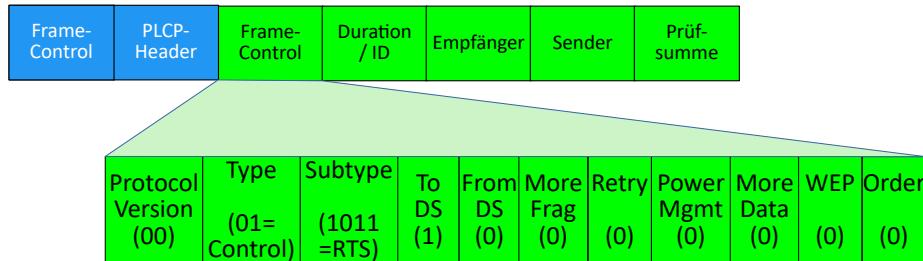


Abbildung 88:
RTS-Frame-Format

Beim RTS handelt es sich um so genannte Control-Frames. Daher ist das Type-Feld auf 10 gesetzt. Im Subtype wird mit 1011 angegeben, dass es sich um einen RTS-Frame handelt.

Im Duration Feld gibt der Sender an wie lange das Senden der Daten, inklusive der Quittung und der IFS, dauern wird. (Daten senden, CTS senden, ACK senden plus 3 * SIFS warten)

Mit der Dauer aus dem RTS-Frame setzen dann alle Stationen im Sendebereich des APs ihren NAV-Wert.

Ist der Empfänger bereit sendet er das CTF-Frame (Type = 10, Subtype = 1100) um seine Daten-Empfangsbereitschaft zu signalisieren.

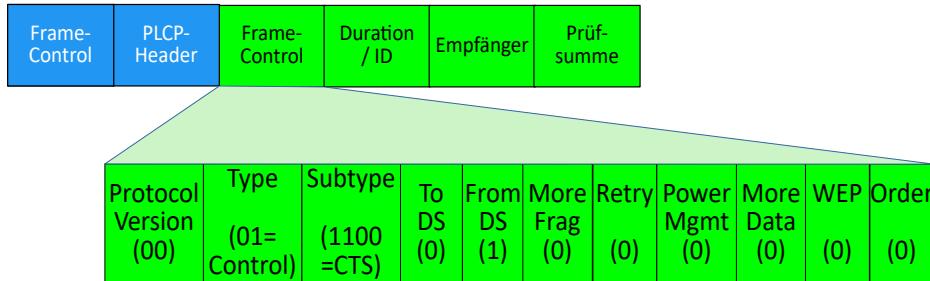


Abbildung 89: CTS-Frame-Format

Mit der Dauer aus dem CTS-Frame können dann alle Stationen im Sendebereich des APs ihren NAV-Wert setzen. Da sowohl vom Sender als auch vom Empfänger der RTS/CTS-Frames die Dauer gesetzt wird, können alle Stationen in den jeweiligen Reichweiten ihre NAV-Werte setzen.

4.5.2.3.7 - Exposed-Station-Problem

Beim Exposed-Station-Problem (auch Exposed-Terminal-Problem, oder Exposed-Node-Problem genannt) will Sta₂ an Sta₃ senden, stellt jedoch fest, dass der Kanal belegt ist weil gerade Sta₁ an Sta₄ sendet.

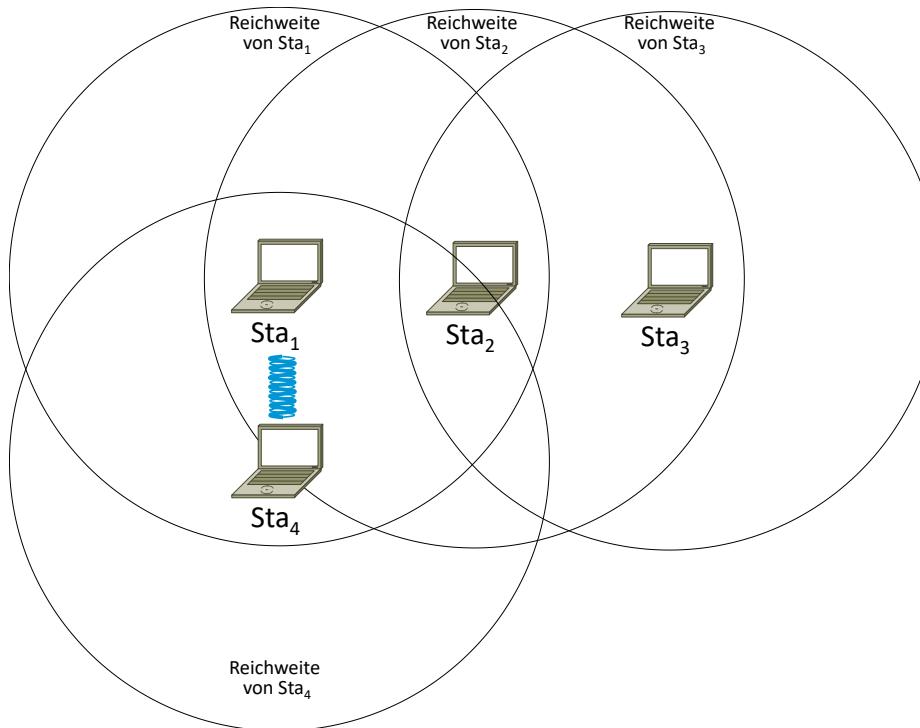


Abbildung 90: Exposed-Terminal-Problem

Eigentlich könnte Sta₂ an Sta₃ senden, denn Sta₃ ist außerhalb der Reichweite von Sta₄. Sta₂ muss warten bis der Kanal frei ist. Damit wird eine Übertragungsmöglichkeit verschwendet.

Auch bei diesem Problem könnte mit RTS/CTS eine Verbesserung der Situation herbeigeführt werden.

Voraussetzung ist hierbei natürlich wieder, dass die Stationen synchronisiert sind und gleiche Paketgrößen und Datenraten einhalten.

4.5.2.4 - PCF

Zusätzlich zu DCF ist noch ein Polling-Verfahren bei IEEE-802.11e spezifiziert. Es ist ein zentralisiertes Verfahren um zeitkritische oder asynchrone Dienste zu unterstützen. Bei PCF ist QoS möglich und es kann parallel zu DCF betrieben werden.

Mit der optionalen PCF (Point Coordination Function) entfällt der Wettbewerb um das Senderecht und somit auch das Kollisionsthema. Hierfür ist immer ein AP notwendig. Er fungiert als Point Coordinator (PC). Dies bedeutet, dass dieses Verfahren in Ad-Hoc-Netzwerken nicht möglich ist!

Durch Priorisierung vor der DCF übernimmt durch die PCF der AP die Koordinierung des Zugriffs auf den Kanal. Dies erreicht die PCF dadurch, dass nicht auf den Ablauf von DIFS sondern nur auf PIFS gewartet wird.

Der Medienzugriff wird innerhalb eines Superrahmens in zwei Phasen, die Contention Free Period (CFP) und Contention Period (CP) unterteilt.

Pro CFP wird jeder am AP entsprechend assoziierten Station einmal eine Datenübertragung garantiert. Alle Stationen setzen den NAV (Net Allocation Vector), und können in dieser Zeit keine Daten von sich aus übertragen. Die nicht entsprechend assoziierten Stationen können nach Ablauf der CFP, also während der CP, in einem Wettbewerb wie bei DCF um das Senderecht konkurrieren.

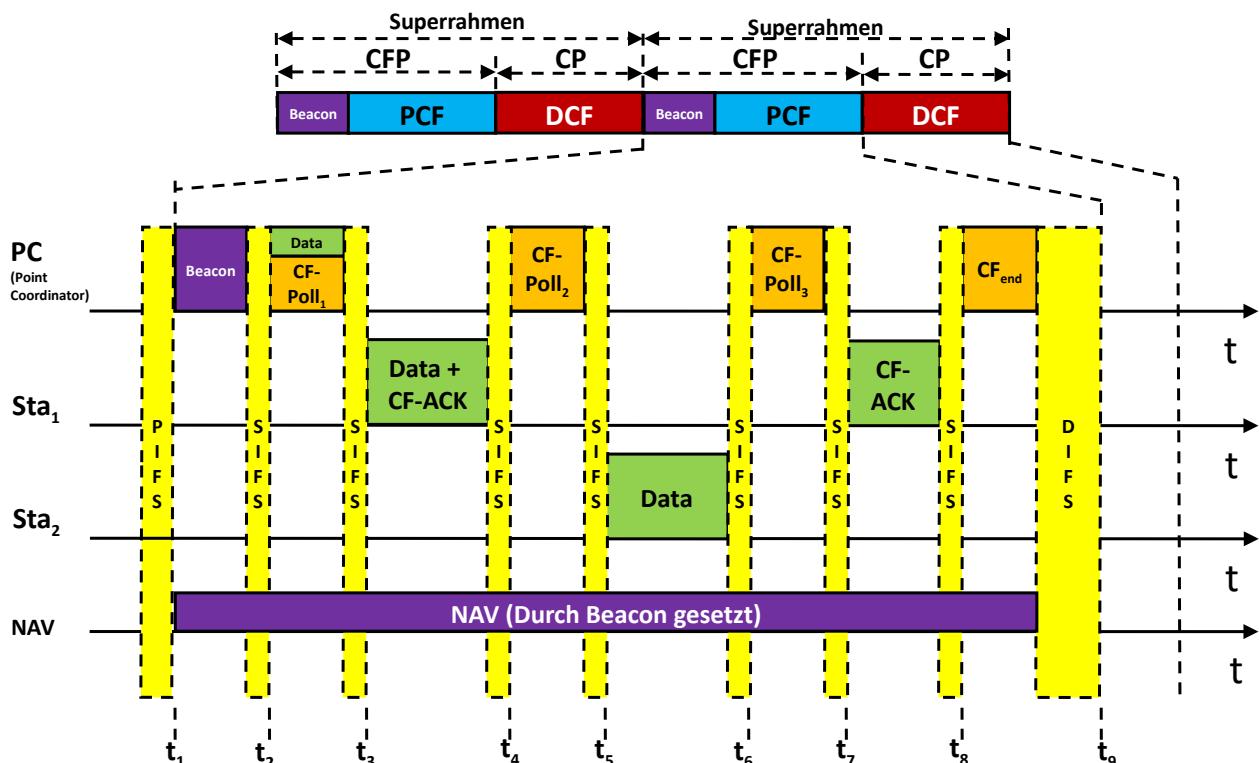


Abbildung 91: PCF

- t₁ Nach dem Ablauf der PIFS-Periode drängelt sich der Point Coordinator (PC) dadurch vor indem er den Beacon-frame aussendet und im CF-Parameter-Set die Informationen für die CFP verteilt. Alle Stationen setzen darauf hin den NAV auf den im CFPMaxDuration-Wert gefundenen Wert. Damit ist die Dauer der CFP gesetzt. Die Stationen werden ab jetzt von sich aus nicht mehr versuchen den Kanal zu belegen.
- t₂ Der Point Coordinator übernimmt nun die Kontrolle über den Kanal. Alle Stationen die sich bei ihm während der Assoziationsphase angemeldet haben werden nun der Reihe nach angesprochen. Als erstes sendet er einen Daten+CF-Poll₁-Frame aus. Damit sendet er Daten an Sta₁ und übergibt ihr gleichzeitig das Senderecht auf den Kanal. Über dieses Piggyback-Verfahren wird der Overhead reduziert.
- t₃ Sta₁ darf nun Daten Senden und tut dies auch. Gleichzeitig quittiert sie mit dem CF-ACK den Empfang der Daten vom AP (PC).
- t₄ Der PC hat den CF-ACK von Sta₁ empfangen und übergibt mit dem CF-Poll₂-Frame das Senderecht an die Sta₂.
Wenn der Point Coordinator keinen ACK-Frame vom Empfänger erhält, kann er den Frame nach Ablauf eines PIFS-Intervalls innerhalb der wettbewerbsfreien Periode nochmals aussenden.
Ein Point Coordinator kann individuelle, Broadcast und Multicast-Frames an alle Stationen schicken, auch an solche, die zurzeit im Power-Safe-Modus vor sich hin dösen.
- t₅ Sta₂ sendet Daten an Sta₁.
- t₆ Der PC übergibt mit dem CF-Poll₃-Frame das Senderecht an Sta₁
- t₇ Sta₁ quittiert mit einem CF-ACK-Frame den Empfang des Frames von Sta₂
- t₈ Nachdem alle Stationen gesendet und quittiert haben sendet der PC ein CF-End um die CFP abzuschließen. Danach stehen alle Stationen wieder untereinander im Wettbewerb um den Kanal.
Nach einem DIFS kann die Kommunikation wie unter der DCF beschrieben weiterlaufen.

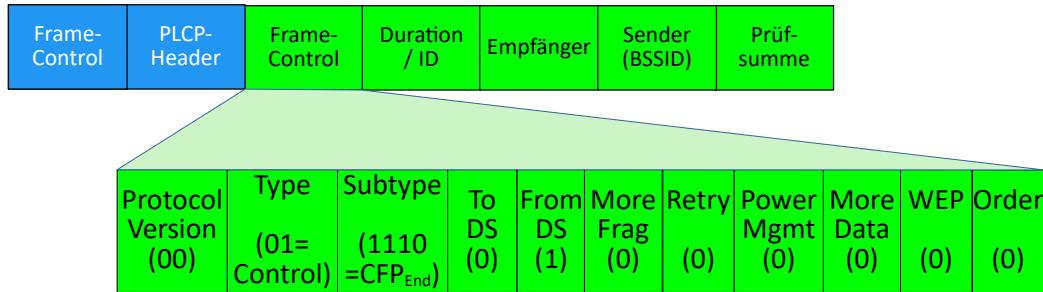


Abbildung 92: CFP-End-Frame-Format

Mit dem Type =10 und dem Subtype=1110 wird der CFP-End-Frame gekennzeichnet.

Im Duration/ID-Feld steht 0 da das Ende der CFP damit angezeigt wird und die CP nach einem DIFS eingeleitet wird. Die Empfängeradresse ist die Broadcast-Adresse, da die Information an alle Stationen der BSS gehen soll. Die Senderadresse enthält die BSSID.

Das CFP-End + CF-ACK-Frame hat die selbe Funktion wie das CFP-End-Frame. Es wird allerdings noch zusätzlich das letzte Datenframe quittiert. Zur Unterscheidung ist der Subtype dafür auf 1111 gesetzt.

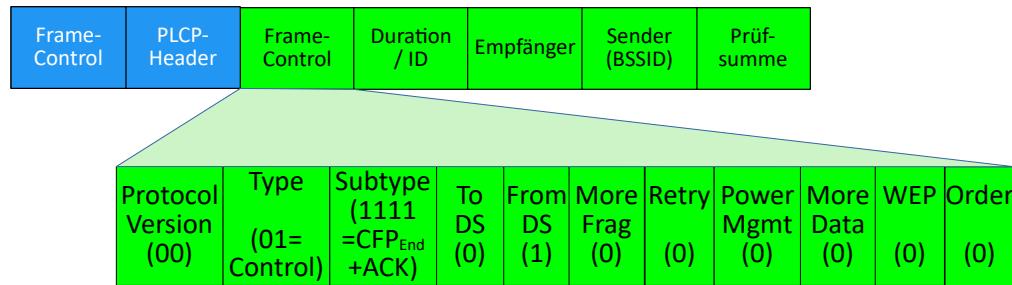


Abbildung 93: CFP-End + ACK - Frame-Format

4.5.3 - Fragmentierung

Um die Wahrscheinlichkeit einer fehlerfreien Übertragung zu erhöhen, können Frames in kleinere Frames fragmentiert werden.

Der Administrator muss die für die Fragmentierung relevante Paketgröße, ab der fragmentiert wird, auf den Stationen konfigurieren. Dazu muss er in der Tabelle Dot11OperationEntry den Wert des Feldes dot11FragmentationThreshold ändern. Der Default-Wert ist auf 65535 gesetzt, was bedeutet, dass es per Default keine Fragmentierung gibt.

Für die Steuerung der Fragmentierung wird das Sequence-Control-Feld im Frame-Header herangezogen. Sieh hierzu Abbildung 76.

Das 16 Bit lange Sequence-Control-Feld ist in 2 Teile aufgeteilt. Mit den ersten 4 Bits wird die Fragment-Nummer angegeben und die folgenden 12 Bits dienen zur Angabe der zugehörigen Sequenz.

Die Fragment-Nummer wird beim ersten Fragment auf 0 gesetzt und bei jedem weiteren Fragment um 1 erhöht. Bei Wiederholungen wird die Fragment-Nummer nicht inkrementiert und das Retry-Bit gesetzt.

Die erste Sequenznummer ist 0. Weitere Sequenznummern werden Modulo 4096 gebildet.

Die Fragmente werden einzeln mit einem ACK direkt nach einem SIFS bestätigt. Damit haben die Quittungen die höchste Priorität beim Medienzugriff. Für die einzelnen Fragmente gilt dasselbe. Direkt nach einem ACK und einem SIFS kann das nächste Fragment gesendet werden, ohne dass eine andere Station sich dazwischen drängelt. Dies ist möglich, da bei jedem Fragment und bei jedem ACK der NAV-Wert erneut gesetzt wird.

Da der priorisierte Fragment-Transport sicher gestellt ist, muss der NAV-Wert nicht über den Zeitraum für die Übertragung aller Fragmente gesetzt werden. Das wäre bei einem Abbruch der fragmentierten Übertragung schädlich, denn alle müssten auf den NAV-Ablauf warten. Stattdessen wird durch jedes Fragment und jedes ACK der NAV erneut gesetzt.

Es ist auch möglich die Koordinierung mittels des RTS/CTS-Mechanismus vorzunehmen. Dann leitet der Sender mittels eines RTS den Vorgang ein. Wie oben erfolgt die Kanalbelegung danach bei jedem Fragment und jedem ACK erneut.

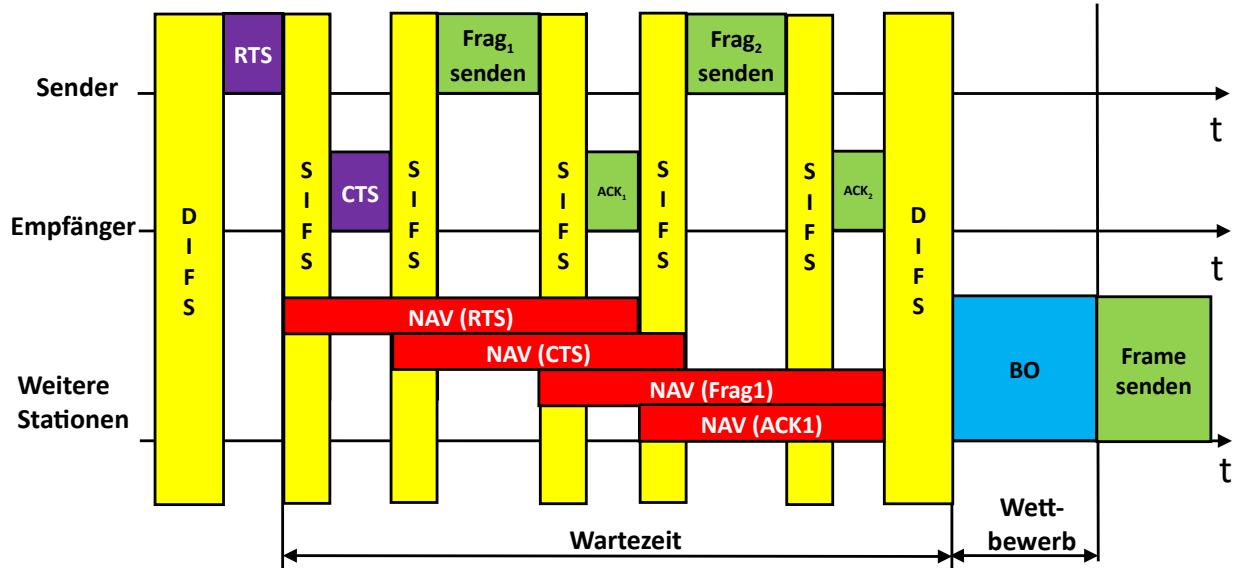


Abbildung 94: Fragmentierung

Über das More-Fragment-Bit (= 1) wird angezeigt, dass weitere Fragmente folgen. Ist das More-Fragment-Bit wieder auf 0 gesetzt, wird angezeigt, dass es sich um das letzte Fragment handelt und der ursprüngliche Frame zusammengesetzt werden kann.

4.5.4 - Synchronisation der Stationen

Im Infrastruktur-Modus werden für den Frequenzwechsel bei 802.11-FHSS sowie für die PCF und Stromsparfunktionen in bestimmten Zeitabständen Beacon-Frames mit einem Zeitstempel vom Accesspoint ausgesendet. Dies wird im Rahmen der Timing Synchronisation Function (TSF) durchgeführt.

Ist der Kanal in dem Moment, an dem Beacon-Frame fällig wäre belegt, wird das Senden des Beacon-Frames mit einem korrigierten Zeitstempel entsprechend verschoben. Sie Stationen synchronisieren sich damit auf den Takt des APs.

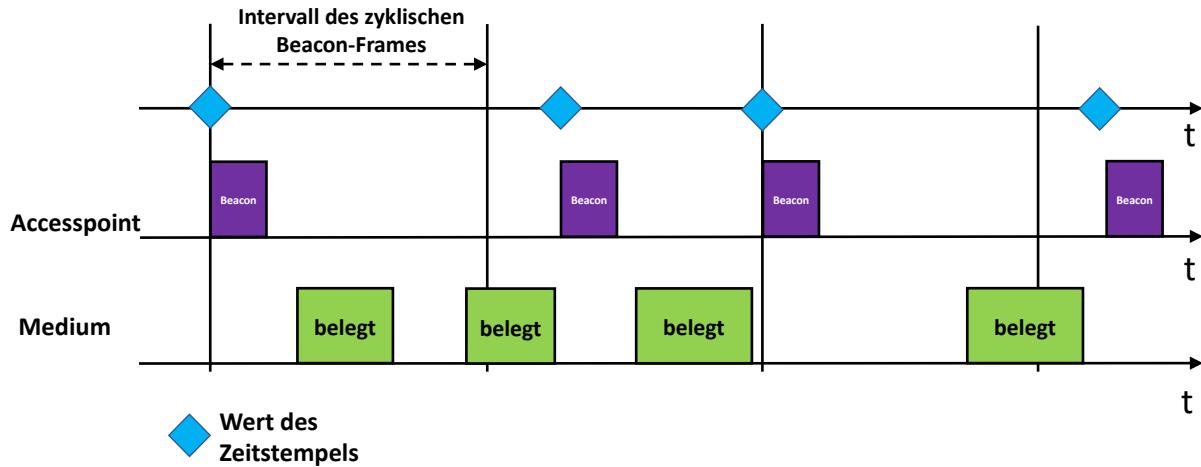


Abbildung 95: TSF im Infrastruktur-Modus

Im Ad-hoc-Modus führen die Stationen eine Timer-Synchronisierung für Frequenzwechsel bei 802.11-FHSS sowie für die Stromsparfunktionen auch die Timing Synchronisation Function (TSF) aus.

Die Stationen senden in bestimmten Abständen Beacon-Frames aus. Ist das Medium belegt, wird das Senden des Beacon-Frames verschoben. Alle Empfänger synchronisieren sich damit auf einen gemeinsamen Takt.

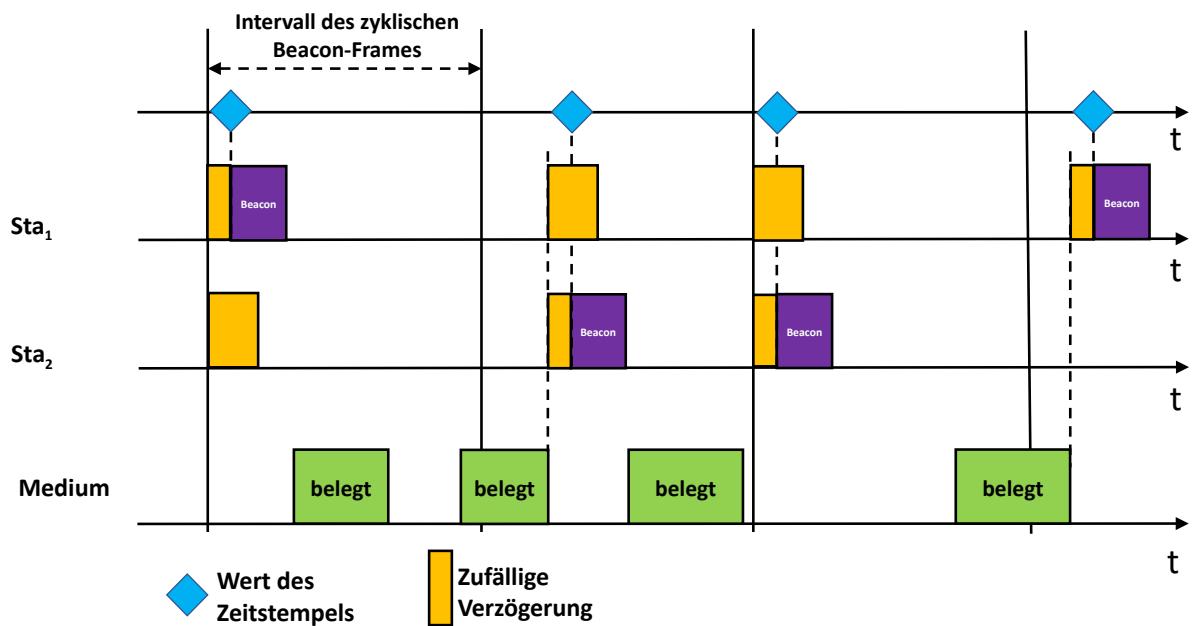


Abbildung 96: TSF im Ad-hoc-Modus

Damit nicht alle Stationen gleichzeitig den Beacon-Frame aussenden, wird der Sendebeginn um eine zufällige Zeit verschoben. So kommen im Mittel alle Stationen dran.

4.5.5 - Steuerung der Leistungsaufnahme

Um Strom zu sparen, können die Empfangs und Sendeeinheiten der Stationen ausgeschaltet werden. Stationen können damit den Zustand „schlafend“ oder „wach“ annehmen. Um sicher zu stellen, dass alle Stationen zur gleichen Zeit aufwachen, wird die Timing Synchronisation Function (TSF) genutzt.

Im Infrastruktur-Modus führt jeder AP eine Liste von Stationen für die Unicast-Frames. Die Liste wird mit Traffic Indication Map (TIM) bezeichnet und periodisch im Beacon-Frame versandt. Für Broadcasts (BC) und Multicasts (MC) wird die Delivery Traffic Indication Map (DTIM) von den APs ausgesandt.

Die Stationen wachen regelmäßig auf. Die dafür erforderliche Zeitsynchronisation erfolgt durch die Timing Synchronisation Function (TSF). TIM und DTIM werden regelmäßig im Beacon-Frame übertragen. Darin werden die Stationen, für die Daten vorliegen angekündigt.

Wenn Daten für eine Station vorliegen kann sie diese mit einem Polling anfordern. Liegen Daten zum Versenden vor können diese während der Wachperiode gesendet werden.

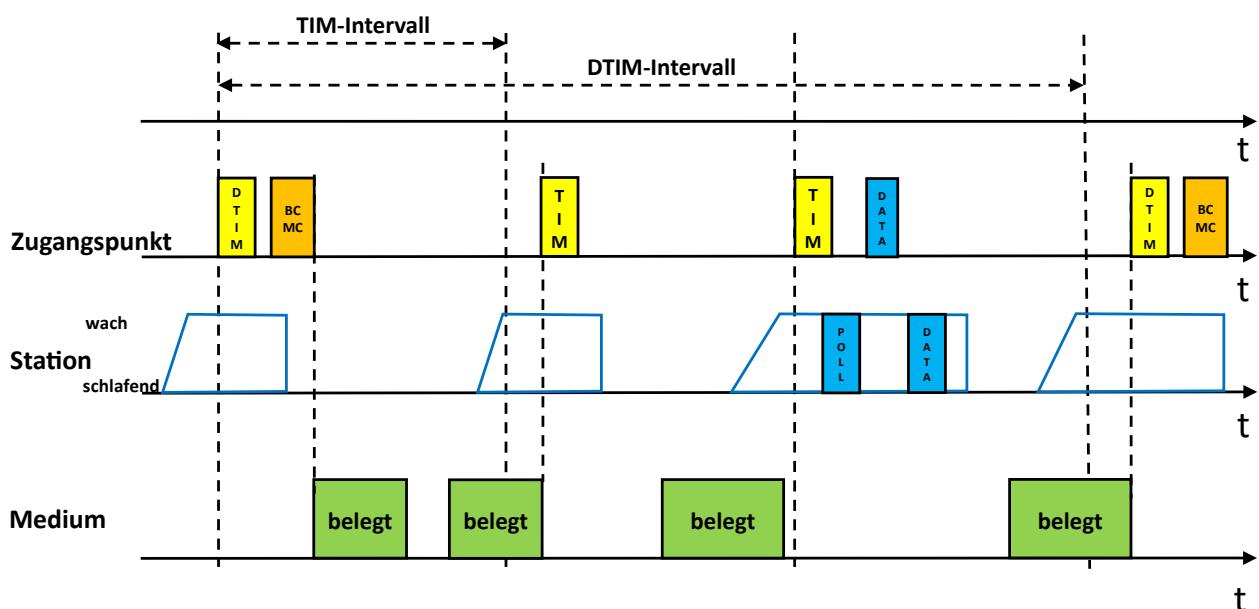


Abbildung 97: TIM / DTIM im Infrastruktur-Modus

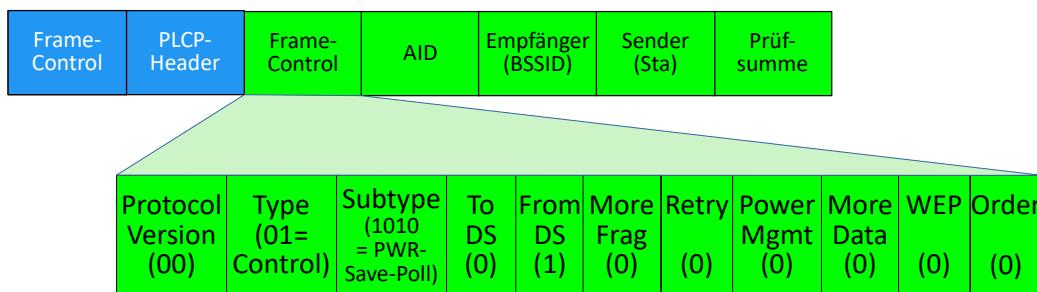


Abbildung 98: Power-Save-Poll-Frame-Format

Anstelle des Duration/ID-Feldes steht hier das AID-Feld, welches die Association-ID (AID) der Station beinhaltet, die ihre Daten beim AP abrufen möchte.

Im Ad-hoc-Modus ist die Bearbeitung komplexer, da eine zentrale Steuerung fehlt. Verwaltet werden die Empfänger in der Ad-hoc Traffic Indication Map (ATIM). Kollisionen von ATIMs sind möglich.

Der Beacon-Frame wird regelmäßig während der Bearbeitung von CSMA/CA übertragen. ATIM-Frames werden nach dem Beacon-Frame als Unicast nach dem CSMA-CA-Verfahren gesendet. Dabei wird angekündigt, dass Daten vorliegen.

Die Stationen wachen regelmäßig gleichzeitig auf und hören den Beacon-Frame sowie die ATIMs ab. Wurden Daten angekündigt, können diese mittels Polling angefordert werden.

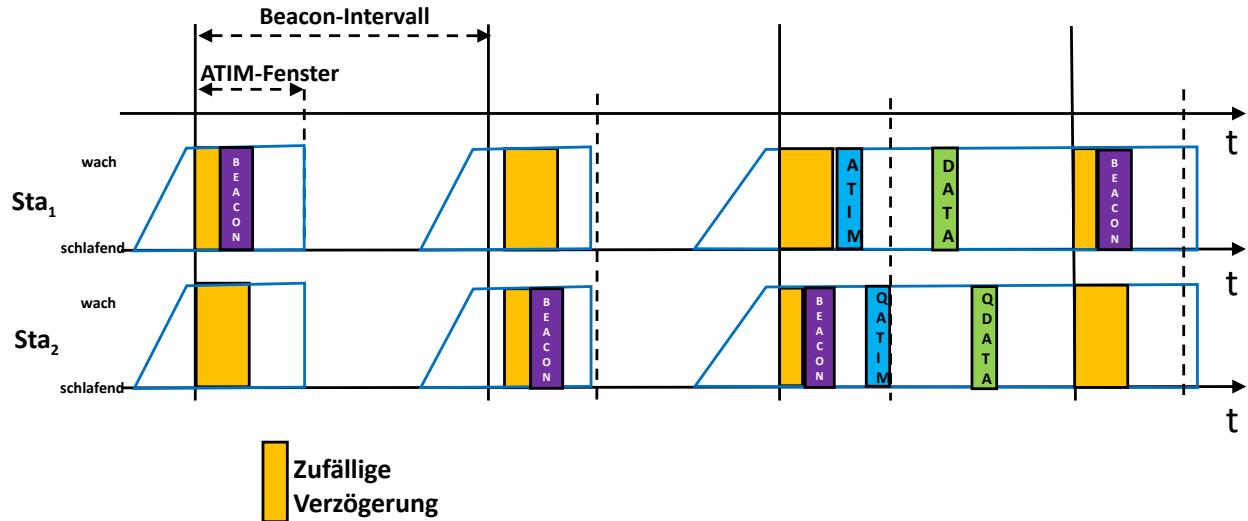


Abbildung 99: ATIM

4.5.6 - Management-Frames

Mit Management-Frames werden diverse Funktionen abgehandelt. Dazu zählen :

- Auffinden eines APs
- An- und Abmelden einer Station an einem Funkzelle (BSS)
- Datenverwaltung während des Stromsparmodus

In den Management-Frames werden die ersten 3 Adressfelder verwendet:

1. Feld: Ziel-MAC-Adresse
2. Feld: Quell-MAC-Adresse

Feld: BSSID der Funkzellen. Nur passende BSS-IDs werden von der MAC-Layer bearbeitet.

Im Control-Feld ist das Type-Feld mit 00 zur Kennzeichnung der Management-Frames belegt. Siehe hierzu auch Abbildung 77 und Tabelle 24. Der Inhalt des Duration/ID-Feldes ist auf 32768 gesetzt, falls das Frame innerhalb einer CFP-Phase übertragen wird.

Innerhalb einer CP-Phase gibt es drei unterschiedliche Fälle:

1. Wird an eine Gruppe von Empfängern mittels eines Multicast (MC) oder Broadcasts (BC) gesendet, ist das Duration/ID-Feld = 0, denn es wird keine Bestätigung erwartet.
2. Wird der Frame mit einem Unicast (UC) gesendet und ist das More Fragment-Bit = 0, entspricht das Duration/ID-Feld der Zeit die für das Senden eines ACK-Frames und einem SIFS benötigt wird.
3. Wird der Frame mit einem Unicast (UC) gesendet und ist das More Fragment-Bit = 1, entspricht das Duration/ID-Feld der Zeit die für das Senden eines Fragments, einem ACK-Frame und 3 SIFS benötigt wird.

Im Subtyp wird die Funktion des Management-Frames festgelegte

Tabelle 28: Management-Frames von Typ 00

Subtyp (b7, b6, b5, b4,)	Subtyp-Bezeichnung	Beschreibung
0000	Association Request	Frames zur An- und Abmeldung am AP
0001	Association Response	
0010	Reassociation Request	
0011	Reassociation Response	
0100	Probe Request	Frames zum Auffinden von Stationen und APs. Die APs senden in regelmäßigen Abständen Beacon-Frames aus, in denen sie die Attribute der Zelle bekannt machen.
0101	Probe Response	
0110	Timing Advertisement	
0111	Reserviert	
1000	Beacon	
1001	ATIM	
1010	Disassociation	
1011	Authentication	
1100	Deauthentication	Frames zum Authentifizieren von Stationen
1101	Action	
1110	Action (NO ACK)	
1111	Reserviert	

Die Übertragung der eigentlichen Information erfolgt abhängig vom Subtyp in Feldern mit fester und variabler Länge.

4.5.6.1 - Authentication-Algorithm-Feld

Das Feld hat eine Länge von 16 Bits und legt den Algorithmus zur Authentifizierung fest. Momentan gibt es zwei Werte

0 = Open-System-Verfahren

1 = Preshared-Key-Verfahren

4.5.6.2 - Authentication-Transaction.Sequence-Number-Feld

In diesem 16 Bit langen Feld wird der aktuelle Status bei der Authentifizierung hinterlegt

4.5.6.3 - Beacon-Interval-Feld

Dieses Feld hat eine Länge von 16 Bits und gibt die Anzahl der Time Units (TU) an, die zwischen den Target Beacon Transmission Times (TBTT) vorhanden sind.

4.5.6.4 - Capability-Infomation-Feld

Diese Feld hat eine Länge von 16 Bit. Die einzelnen Bits repräsentieren Informationen die bei Anfragen oder Bekanntgaben ausgetauscht werden.

Tabelle 29: Bedeutung der Bits des Capability-Feldes

Bit-Nr.	Bezeichnung	Bedeutung
0	ESS	Es handelt sich um ein Infrastruktur-Netzwerk (Dabei ist IBSS = 0)
1	IBSS	Es handelt sich um ein Ad-hoc-Netzwerk (Dabei ist ESS = 0)
2	CF Pollable	CF-Pollable und CF-PollRequest werden immer zusammen verwendet und sind in den folgenden Tabellen beschrieben.
3	CF Poll request	
4	Privacy	Datenframes werden verschlüsselt
5	Short Preamble	Erweiterung für 802.11b: Innerhalb des BSS wird die kurze Präambel und damit das kurze Frame-Format verwendet
6	PBCC	Erweiterung für 802.11b/g: Es wird das Packet Binary Convolutional Code (PBCC) - Verfahren verwendet. Siehe hierzu auch Kapitel IEEE-802.11b Seite: 123
7	Channel Agility	Erweiterung für 802.11b: Agility-Option wird genutzt. Dabei wird wie beim FHSS-Verfahren regelmäßig der Kanal gewechselt um Probleme zu vermeiden.
8	Spectrum Management	Erweiterung für 802.11h: Ist das Bit gesetzt wird DFS und TPC bei Nutzung des 5GHz-Bandes verwendet. Siehe hierzu auch Kapitel IEEE-802.11h Seite: 122
9	QoS	Erweiterung für 802.11e: Ist das Bit gesetzt wird angezeigt, dass QoS unterstützt wird
10	Short Slot Time	Erweiterung für 802.11e: Ist das Bit gesetzt wird angezeigt, dass die kurze Slot Time von 9 µs unterstützt wird. Die gilt nur wenn sich keine Non ERP Stationen in der gesamten BSS befinden. Mit der ersten Non ERP-Station setzt der AP den Wert auf 0
11	Robust Security Network (RSN)	Erweiterung für 802.11i: Ist das Bit gesetzt wird angezeigt, dass die neuen Sicherheitsverfahren unterstützt werden.
12	Reserviert	
13	DSSS-OFDM	Erweiterung für 802.11g: Ist das Bit gesetzt wird angezeigt, dass DSSS-OFDM verwendet wird um Datenraten bis zu 54 Mbit/s erreicht werden können.
14	Delayed Block-ACK	Erweiterung für 802.11e: Ist das Bit gesetzt wird angezeigt, dass die Quittierung mit den Blockverfahren erfolgt.
15	Immediate Block-ACK	

Tabelle 30: Bedeutung von CF-Pollable und CF-PollRequest auf AP-Seite

CF-Pollable	CF-PollRequest	Bedeutung
0	0	Keine Point Coordination Function (PCF) durch den AP
0	1	Point Coordination Function (PCF) durch den AP, jedoch nur zur Aussendung von Daten
1	0	Vollständige Point Coordination Function (PCF) durch den AP
1	1	Reserviert

Tabelle 31: Bedeutung von CF-Pollable und CF-PollRequest auf Stations-Seite

CF-Pollable	CF-PollRequest	Bedeutung
0	0	Station kann über das Poll-Verfahren nicht abgefragt werden
0	1	Frames dieser Station können über das Poll-Verfahren abgerufen werden, jedoch soll die Station nicht in die Poll-Liste des APs aufgenommen werden.
1	0	Frames dieser Station können über das Poll-Verfahren abgerufen werden und die Station soll in die Poll-Liste des APs aufgenommen werden.
1	1	Station lässt sich über das Poll-Verfahren abfragen, Requests sollen jedoch nicht abgefragt werden

4.5.6.5 - Current-AP-Feld

Das Feld ist 6 Bytes lang und gibt die Adresse des APs an, mit dem die Station verbunden ist.

4.5.6.6 - Listen-Interval-Feld

Das Feld ist 16 Bit lang. Damit gibt eine Station dem AP bekannt in welchen Zeitabständen sie in den Empfangsmodus geht. Daraus kann der AP ableiten wie lange er Frames für diese Station zwischenspeichern muss.

4.5.6.7 - Reason-Code-Feld

Der Reason-Code ist 16 Bit lang. Damit lassen sich 65535 verschiedene Codes angeben von denen 65 genutzt werden. Darin werden die Gründe aufgelistet, warum eine Station von einer Funkzelle getrennt, oder die Authentifizierung abgelehnt wurde. Näheres hierzu siehe [IEEE-802.11-2016]

4.5.6.8 - Association-ID-Feld

In dem 16 Bit langen Feld wird die Association ID (AID) angegeben. Damit verwaltet ein AP eine Station. Die beiden höchsten Bits sind auf 1 gesetzt. Die restlichen 14 Bits enthalten die AID (1 -2007)

4.5.6.9 - Status-Code-Feld

Das 16 Bit lange Feld gibt Auskunft über Erfolg oder Misserfolg der letzten Operation. Der Wert 0 steht für eine erfolgreiche Operation. Andere Werte geben den Fehlergrund an. Näheres hierzu siehe [IEEE-802.11-2016]

4.5.6.10 - Timestamp-Feld

Mit dem 64 Bit langen Feld erfolgt die Zeitsynchronisation im Rahmen der Time Synchronization Function (TSF) statt. Der Master sendet innerhalb der Beacon-Frames die Zeitinformation der TSFTimer aus. Der TSFTimer kann 2^{64} Werte in Schritten von 1 μ s annehmen. Wird das Maximum erreicht, wird der Zähler (nach 580000 Jahren) zurückgesetzt.

4.5.6.11 - Informations-Elemente

Felder mit variabler Länge, die auch dem Informationsaustausch dienen, werden in der Tabelle Element-IDs verwaltet. Diese setzen sich aus einer 1 Byte langen Element-ID, einem 1 Byte langen Length-Feld (gibt die

Informationslänge in Bytes an) und deinem variablen Informationsanteil mit maximal 255 Bytes zusammen. Näheres hierzu siehe in [IEEE-802.11-2016] Tabelle 9-77-Element-Ids.

4.5.6.12 - Herstellerspezifische Informationselemente

Hier können Hersteller Informationen hinterlegen, die nicht dem Standard entsprechen

5 - Der IEEE-802.11 - Standard

5.1 - Übersicht

Seit seiner ersten Veröffentlichung im Jahre 1997 hat der Standard IEEE-802.11 bereits mehrere Verbesserungen durchlaufen. Dabei sind folgende Ausprägungen entstanden.

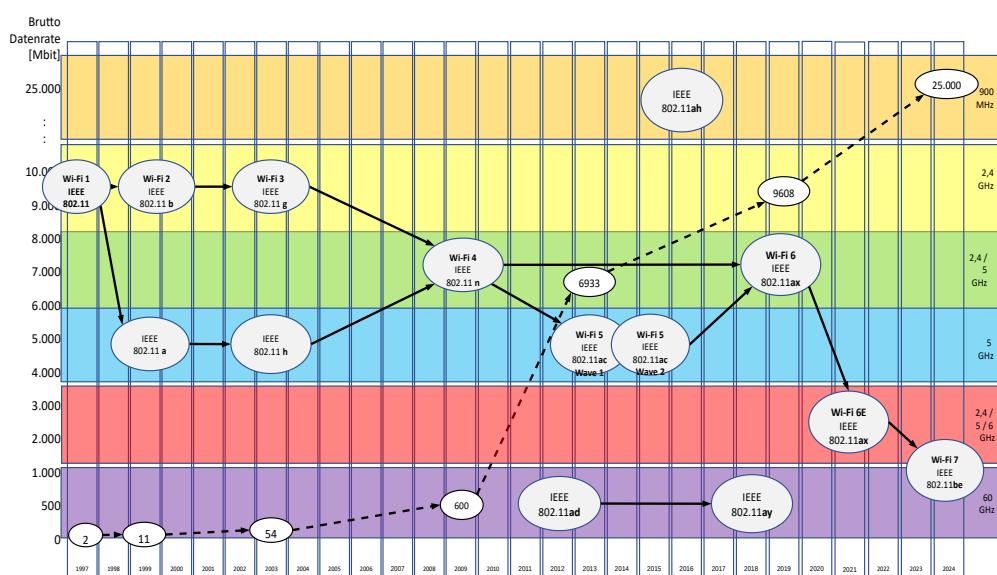


Abbildung 100: WLAN:
Historische
Entwicklung

Die von der IEEE-802.11-Familie verwendeten Frequenzbereiche sind in ISM(Industrial- Scientific-Medical)-Bändern bei 900MHz, 2.4 GHz, 5GHz, 6GHz sowie bei 60 GHz. Dies hat den Vorteil, dass keine Lizenzen erforderlich sind.

Ursprünglich wurden nur die 2,4 GHz-Bänder genutzt. Um die Bandbreite zu erhöhen mussten weitere Bänder (900MHz, 5GHz, 6GHz und 60 GHz) herangezogen werden. Dabei wurde die die Brutto-Datenrate von anfänglich 1Mbps bis auf 9.6Gbps gesteigert.

Nachdem mehrere Innovationszyklen die Normen etwas unübersichtlich gemacht hatten, einigte man sich im Jahre 2018 auf eine Vereinfachung bei der die Generationen von WLAN-Standards durchnummierter werden. So wurde aus dem ersten Standard (IEEE-802.11) die Bezeichnung Wi-Fi-1, bis man für IEEE-802.11ax bei Wi-Fi-6 ankommt.

2021 wurde mit der Freigabe des 6 GHz-Bandes der IEEE-802.11ax-Standard zu Wi-Fi-6E. Funktional hatte das keine Auswirkungen!

5.2 - Anfänge von IEEE-802.11

5.2.1 - Eigenschaften

Name: Wi-Fi 1

Frequenzband: 2,4GHz

Anzahl der Kanäle: 13 (überschneidungsfrei nur 3)

Kanalbreite: 22MHz

Multiplex-Verfahren: DSSS oder FHSS

Modulation: BPSK

Maximale Brutto-Datenrate: 2Mbps

Der erste Standard von 1997 sah Datenraten von < 2 Mbps mit Signalspreizung vor. Mit dem Frequency Hopping Spread Spectrum (FHSS) und dem Direct Sequence Spread Spectrum (DSSS) waren 2 unterschiedliche Spreizverfahren der Frequenzbandnutzung möglich. Siehe hierzu auch Abbildung 75. Als Medien-Zugriffsverfahren wurde CSMA/CA verwendet. Dies funktioniert recht zuverlässig, bildet jedoch auch bei den folgenden Standards den Flaschenhals. Die Bandbreite eines Kanals liegt bei 22MHz.

Für IEEE-802.11 stehen 13 Kanäle (11 in den USA) im 2,4 GHz-Band zur Verfügung, die sich allerdings überlappen. (siehe hierzu auch Abbildung 14)Die Überlappung entsteht durch die 22MHz Bandbreite, die ein Kanal belegt. Dies ist jedoch weitaus mehr als die 5 MHz, die ein Kanal per Definition breit ist. Es können somit nur 3 Kanäle (1, 7, 13) ohne Überlappung und 4 Kanäle (1, 5, 9, 13) mit leichter Überlappung gleichzeitig betrieben werden. Dies macht eine flächendeckende Planung erschwert und eine 3-dimensionale Planung (über mehrere Stockwerke) fast unmöglich.

Da jedoch von manchen Herstellern die Kanäle 1, 7 und 13 bevorzugt behandelt werden (schnelleres Handover), ist es sinnvoll diese Kanäle zu wählen, wenn optimale Datenübertragung gefordert ist.

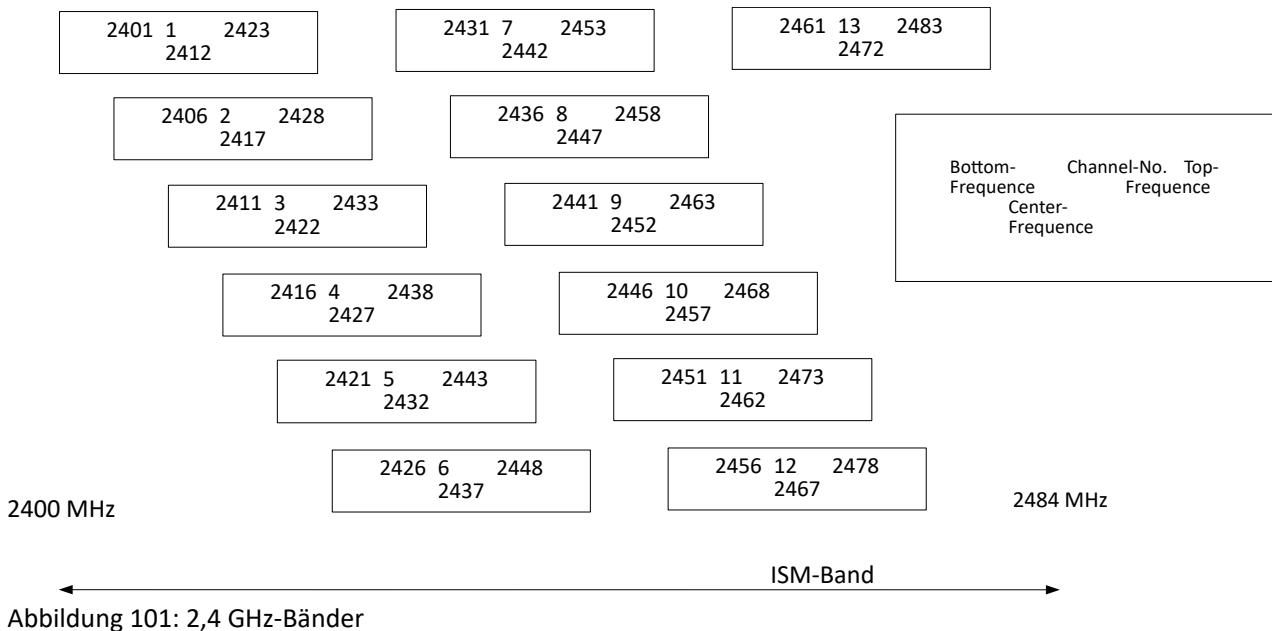


Abbildung 101: 2,4 GHz-Bänder

Beim Betrieb eines Hotspots kann es erforderlich werden, die Verwendung der Kanäle 1,6 und 11 zu planen, wenn Gäste aus den USA auch den Hotspot nutzen sollen. Die Chipsätze für die USA haben in der Firmware nur 11 Kanäle hinterlegt obwohl die Hardware 13 Kanäle unterstützt.

Da hierbei nur der kleinste gemeinsame Nenner zwischen unterschiedlichsten Herstellern und Anforderungen erreicht wurde, waren viele Freiheitsgrade offen geblieben. Deshalb war die Interoperabilität der Produkte unterschiedlicher Hersteller oft nicht gegeben. Die Weiterentwicklungen wurden weltweit von unterschiedlichen Herstellern betrieben. Leider sind hierbei auch nationale Gegebenheiten zu berücksichtigen. Dies führte dazu, dass die unterschiedlichen Weiterentwicklungen zeitlich versetzt auf den Markt kamen. Sie wurden in verschiedenen Ländern mit unterschiedlichen Ausprägungen, wie z. B. Sendeleistungen, auf den Markt gebracht.

Ein weiteres Problem war, dass die Sicherheit anfänglich vernachlässigt worden war. Erst mit der Einführung von WPA wurde am Markt eine Akzeptanz geschaffen.

5.2.2 - WLAN-Frame nach IEEE-802.11

Wie bei Ethernet gibt es eine Präambel zur Synchronisation. Die Präambel wird immer mit 1Mbps übertragen. Die Größe der Präambel variiert je nach Standard.

Danach folgt der PLCP-Header. In ihm werden die PHY-spezifischen Eigenschaften adressiert.

Danach folgt der so genannte MAC-Frame der die Ebene-2 und die folgenden Ebenen beinhaltet.

In ihm wird die Adressierung mittels MAC-Adressen vorgenommen.

Das Frameformat wurde von Ethernet abgeleitet. Allerdings können wesentlich mehr Daten in einem Frame übertragen werden. Während ein Ethernet-Frame maximal 1518 Byte haben darf, kann das Ethernet-Frame über WLAN 2304 Byte beinhalten. Damit reduziert sich die Anzahl der Header und damit erhöht sich der Durchsatz.

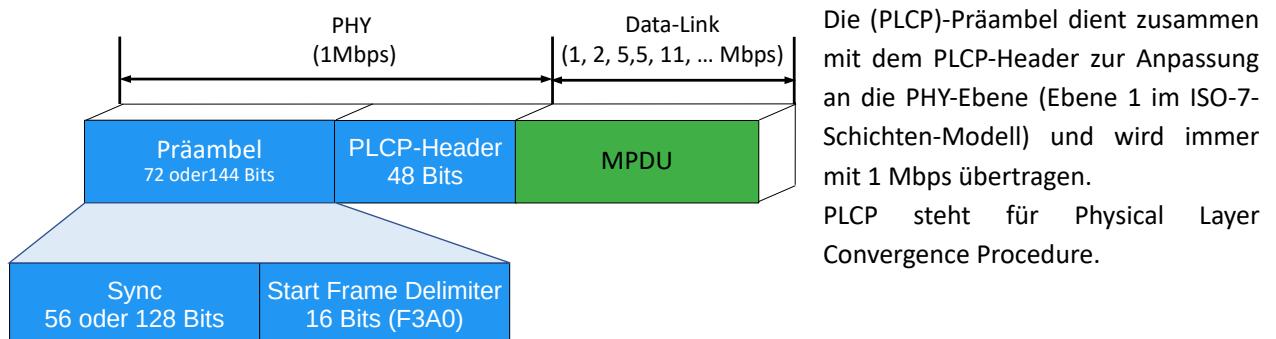


Abbildung 102: WLAN-Präambel und SFD

Hierbei wird auch schnell klar warum, bei einer Datenrate von 11Mbps, nur etwa 5 bis 6 Mbps als Netto-Übertragungsrate zustande kommt. Mit ein Grund hierfür ist, dass die Präambel sowie der PLCP-Header immer nur mit 1Mbps übertragen werden.

Um hierbei eine Optimierung zu erreichen kann die Präambel verkürzt werden. Die Präambel hat dann nur eine Länge von 72 Bits.

Die lange Version ist Standard. Wird die verkürzte Version verwendet, muss das von allen teilnehmenden Geräten unterstützt werden! Den Abschluss bildet ein Start Frame Delimiter (SFD).

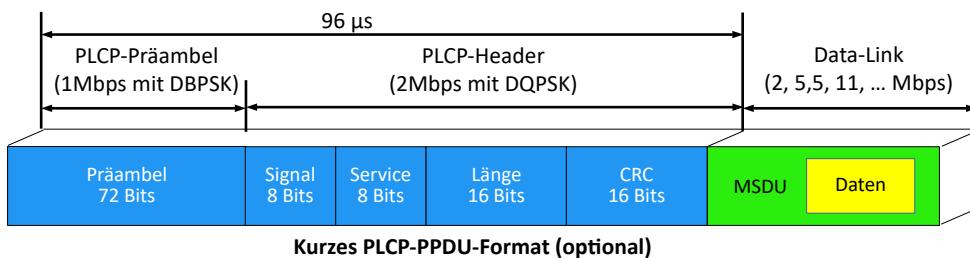
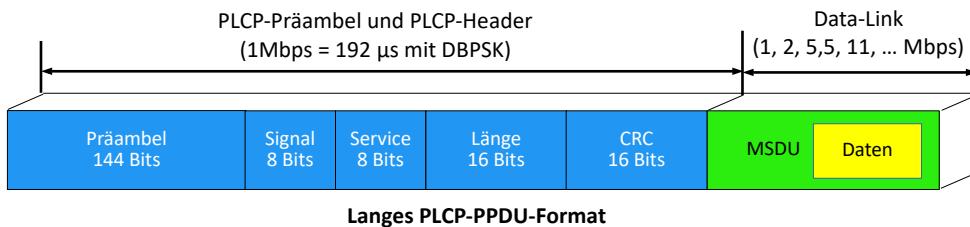


Abbildung 103: PLCP-Formate

Der PLCP-Header legt die Modulationsart und damit die Datenrate der MPDU (MAC-PDU) fest

Er besteht aus 4 Feldern:

Mit dem Signal-Feld wird die Datenrate festgelegt:

- 0A hex = 1 Mbps
- 14 hex = 2 Mbps
- 37 hex = 5,5 Mbps
- 6E hex = 11 Mbps
- DC hex = 22 Mbps (ERP-PBCC)
- 21 hex = 33 Mbps (ERP-PBCC)
- 1E hex = DSSS-OFDM-Datenraten
- ...

Im Service-Feld werden die folgenden Themen abgehandelt:

- Bit 0 = reserviert 0
- Bit 1 = reserviert
- Bit 2 = Locked clocks (0 = not locked / 1 = TX-Frequency and symbol clocks are locked)
- Bit 3 = Modulatiopn Selection (0 = NoERP-PBSS / 1 = ERP-PBCC)
- Bit 4 = reserviert
- Bit 5 = Length Extension for ERP-PBCC
- Bit 6 = Length Extension for ERP-PBCC
- Bit 7 = Length Extension for PBCC

Das Längenfeld gibt die Länge der MSDU an.

Im CRC wird die Prüfsumme über den MSDU abgelegt.

5.3 - Verbesserungen

Im Jahr 1999 wurden die beiden Standards IEEE-802.11a und IEEE-802.11b veröffentlicht. Es handelt sich hierbei um zwei völlig unterschiedliche Weiterentwicklungen, die in unterschiedlichen Frequenzbereichen mit unterschiedlichen Verfahren, z. B. Modulationsarten, arbeiten.

5.3.1 - IEEE-802.11a/h

Eigenschaften

Frequenzband: 5GHz

Anzahl der Kanäle: 53 - 140

Kanalbreite: 20MHz

Multiplex-Verfahren: Orthogonal Frequency Division Multiplexing (OFDM)

Modulation: Max. 64-QAM

Maximale Brutto-Datenrate: 54Mbps

Trotz der größeren Datenrate setzte sich IEEE-802.11a zuerst nicht durch. Erst 2002 wurden die zugehörigen Frequenzbänder in Deutschland freigegeben. Zusätzlich werden die Frequenzbänder von Flugzeugen und Wetterradar professionell genutzt und die Sendeleistung des WLANs ist daran anzupassen. Das wurde 2003 mit der Ergänzung um IEEE-802.11h erreicht. Dabei wird mit Transmission Power Control (TPC) und der Dynamic Frequency Selection (DFS) erreicht, dass die professionellen Nutzer vor allem im Outdoor-Bereich nicht gestört werden.

5.3.2 - IEEE-802.11b

Eigenschaften

Name: Wi-Fi 2

Frequenzband: 2,4GHz

Anzahl der Kanäle: 13 (3 überschneidungsfreie Kanäle)

Kanalbreite: 22MHz

Multiplex-Verfahren: HR-DSSS

Modulation: BPSK, QPSK

Maximale Brutto-Datenrate: 11Mbps

Die erste Verbesserung im 2,4GHz-Band bot eine Erhöhung der Datenübertragungsrate durch Ersatz von DSSS durch High-Rate-DSSS (HR-DSSS). Dabei wird der feste Barker-Code durch eine komplementäre Sequenz aus 8 Chips ersetzt. CCK (Complementary Code Keying)

Damit ergibt sich eine Datenrate von:

$$\text{Datenrate} = (\text{Chiprate}/\text{Codelänge}) \times \text{Anzahl codierter Bits} \quad (24)$$

$$\text{Datenrate} = 11 \text{ Mchips/s} / 8 \text{ Cips} * 4 \text{ Bits} = 5,5 \text{ Mbits/s}$$

Damit 11 Mbps übertragen werden können, wird die Anzahl der codierten Bits durch eine Erhöhung der Spreizsequenzen auf 8 Bit erhöht.

Bei IEEE-802.11b ist zwar eine Bitfehler-Korrektur mittels FEC (Forward Error Correction) vorgesehen, jedoch ist der im Standard als PBCC (Packet Binary Convolutional Coding) bezeichnete Mechanismus optional und in den meisten Produkten nicht implementiert.

Deshalb geht man bei Störungen auf robustere Spreizsequenzen zurück und halbiert damit jedes Mal die Datenrate von 11Mbps über 5,5Mbps über 2Mbps bis zu 1Mbps.

Da die Bitfehler auf physikalischer Ebene (Ebene1) nicht korrigiert werden können, sind die Daten auf MAC-Ebene (Ebene2) zu wiederholen.

5.3.3 - IEEE-802.11g

Eigenschaften

Name: Wi-Fi 3

Frequenzband: 2,4 GHz

Anzahl der Kanäle: 13. (Überschneidungsfrei 3)

Kanalbreite: 22MHz

Multiplex-Verfahren: ERP-OFDM, ERP-PBCC und DSSS-OFDM

Modulation: Max. 64-QAM

Maximale Brutto-Datenrate: 54Mbps

Hierbei handelt es sich um eine physikalische Übertragungsebene, die abwärts kompatibel zu IEEE-802.11b ist und im 2,4 GHz-Band arbeitet. Der Standard wurde im Juni 2003 verabschiedet.

Als Modulationsarten wird sowohl Orthogonal Frequency Division Multiplexing (OFDM), wie bei IEEE-802.11a, als auch CCK (Complementary Code Keying), wie bei IEEE-802.11b, verwendet. Datenraten von 6, 9, 12, 18, 24, 36, 48 und 54 Mbit/s sind möglich. Mindestens die Datenraten von 6, 9, 12, 18 und 24 Mbit/s sollen übertragen werden können. Die Datenraten 36, 48 und 54 Mbit/s sind optional. Weiterhin sind mit PBCC22 22MBit/s und mit PBCC33 33MBit/s möglich.

Allerdings sind nur 3 Kanäle (wie bei IEEE-802.11b) für den parallelen Betrieb nutzbar.

Mit der Einführung von IEEE-802.11g auf Basis des 2,4GHz-Bandes sind 2 unterschiedliche PHY-Typen zu unterscheiden:

- ➊ ERP (Extended Rate PHY)
Erweiterter PHY der im 2,4GHz-Band die höheren Datenraten unterstützt
- ➋ NonERP (non Extended Rate PHY)
PHY um mit den DSSS- und CCK-Verfahren Datenraten von 1Mbit/s bis zu 11MBit/s nach 802.11 und 802.11b zu ermöglichen

Dazu wurden 4 Betriebsmodi definiert:

- ➊ ERP-DSSS/CCK
Erweiterter PHY der das DSSS- und CCK-Verfahren unterstützt. Dabei wird das kurze Header-Format verwendet.
- ➋ ERP-OFDM
Entspricht einem PHY der im 2,4GHz-Band mit OFDM arbeitet
- ➌ ERP-PBCC
Dieser Modus wurde als Option aufgenommen und arbeitet mit dem PBCC22 und PBCC33-Verfahren
- ➍ DSSS-OFDM
Dabei wird sowohl das DSSS als auch das OFDM-Verfahren unterstützt. Vor die OFDM-Daten wird ein DSSS-Header gesetzt. Der Teil am Anfang wird mittels DSSS (mit 1 oder 2 Mbit/s) übertragen und der folgende Teil wird mit OFDM (mit 6 bis 54MBit/s) übertragen. Damit wird eine Koexistenz von 802.11, 802.11b und 802.11g in einer Funkzelle ermöglicht. Dadurch wird jedoch ein Overhead erzeugt, der die geringere Netto-Datenrate im Vergleich zu 802.11a/h erklärt.

Neben der Möglichkeit vor die OFDM-Daten einen Header zu setzen, gibt es noch einen so genannten Protection-Mechanismus. Mit entsprechenden Management-Informationen wird der Schutzmechanismus in der MAC-Ebene abgehandelt. Dabei wird ein weiterer Protokoll-Overhead im Vergleich zu 802.11a/h generiert. Der Protection-Mechanismus ist nicht für PBCC- und DSSS-OFDM-Verfahren erforderlich.

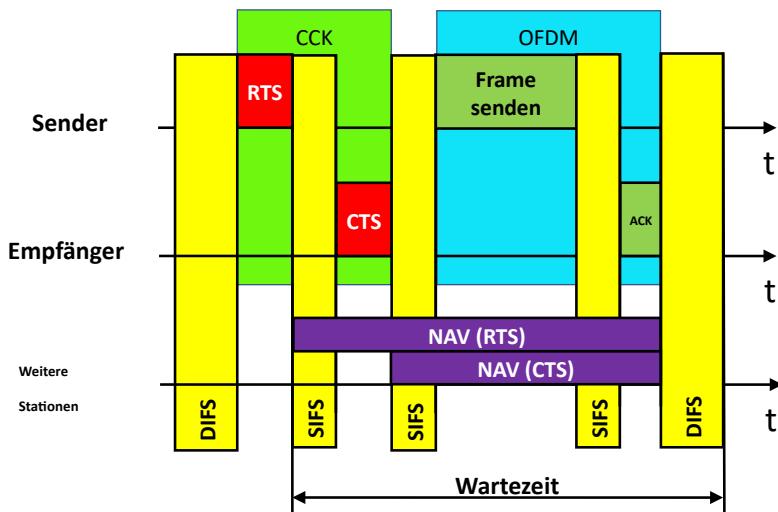


Abbildung 104: IEEE-802.11g - Protection-Mechanismus

Mit dem IEEE-802.11g-Standard wurde eine Optimierung des Frame-Formats vorgenommen. Dabei wird mittels RTS/CTS die Umschaltung zwischen CCK-Modus und OFDM-Modus geregelt.

Die Übertragung der Daten kann damit sowohl im CCK-Modus als auch im OFDM-Modus erfolgen.

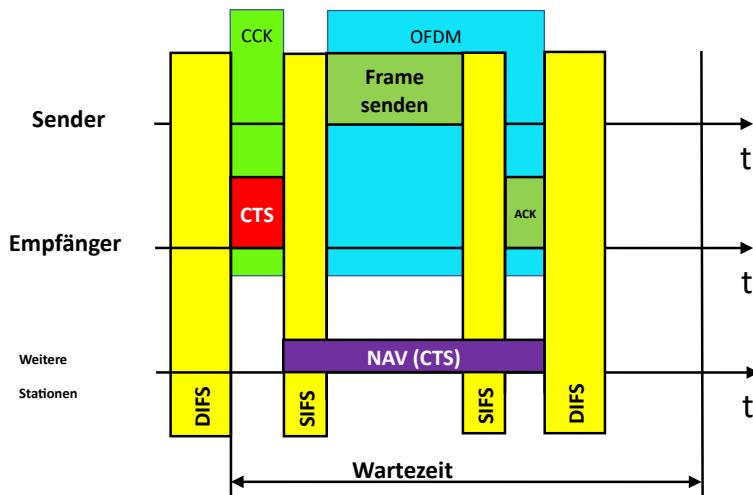


Abbildung 105: CTS to Self

Da dies einen erhöhten Organisationsaufwand mit einem ordentlichen Overhead bedeutet wurde eine Abkürzung des RTS/CTS eingeführt.

Mit dem „CTS to self“ werden im CCK-Modus Übertragungen angekündigt. Das Ziel ist der Sender selbst. Die Datenübertragung kann dann im OFDM-Modus erfolgen. Als Problem gilt hier, dass wie beim Hidden-Station-Problem nicht alle Stationen das „CTS to Self“ empfangen.

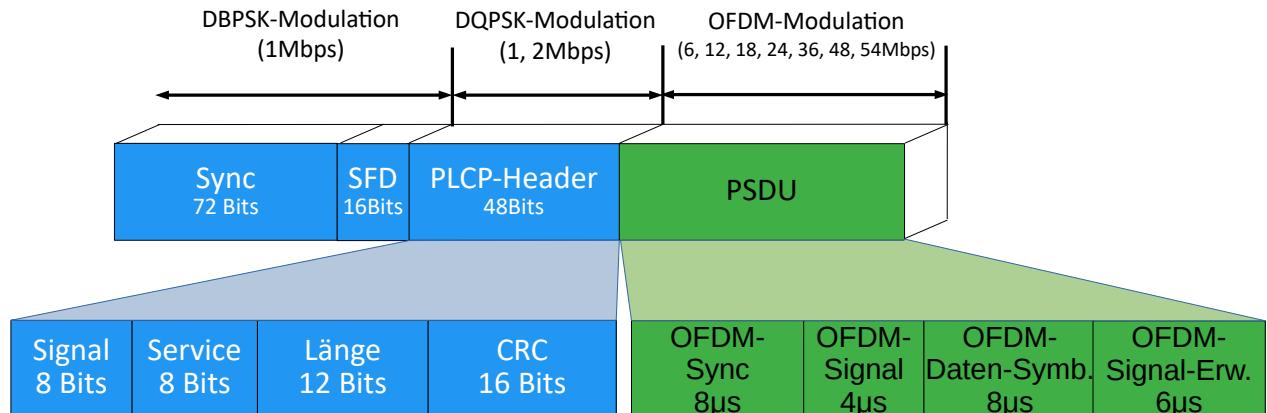


Abbildung 106: DS-SS-OFDM-Frameformat nach 802.11g

Tabelle 32 Charakteristische OFDM-Parameter [Rech-WLAN-2012]

Parameter	Wert
aSlotTime	Lang = 20 µs (falls ERP und NonERP innerhalb der BSS) kurz 9 µs (falls nur ERP und innerhalb der BSS)
aSIFSTime	10µs
aCCATime	< 15µ für lange Slottime < 4 µs für kurze Slottime
aMPDUMaxLength	4095 Bytes
aCWmin	15
aCWmax	1023
Dauer für Präambel	20µs (falls nur ERP), 72 µs (falls ERP und NonERP)
Dauer für PLCP-Header	4µs(falls nur ERP), 24 µs (falls ERP und NonERP)

5.3.4 - IEEE-802.11n

5.3.4.1 - Eigenschaften

Name: Wi-Fi 4

Frequenzband: 2,4 und 5 GHz

Anzahl der Kanäle: 13 im 2,4 Ghz-Band (Überschneidungsfrei 3) / 8 im 5GHz-Band

Kanalbreite: 22MHz

Multiplex-Verfahren: Orthogonal Frequency Division Multiplexing (HT-OFDM)

Modulation: Max. 64-QAM

Maximale Reichweite: 100m

Maximale Antennenanzahl: 4*4

MIMO-Streams: 1 bis 4

Maximale Brutto-Datenrate: 600 Mbps

Typische Netto-Datenrate: 40 – 150 Mbps

Der Standard, der Datenübertragungsraten von bis zu 600 MBit/s ermöglichen soll, wurde vom EWC-Konsortium (Enhanced Wireless Consortium) entwickelt. Dazu gehören unter anderen die Firmen Apple, Atheros, Broadcom, Buffalo, Cisco, [Conexant](#), [D-Link](#), Foundry, [Intel](#), [Lenovo](#), [Linksys](#), [Netgear](#), [Sanyo](#), [Sony](#), [Ralink](#) und [Toshiba](#). Bisher waren zwei Gruppen (TGnSync und WWiSE = World-Wide Spectrum Efficiency) mit der Definition eines Standards 802.11n für höhere Datenraten (Enhancements for Higher Throughput) beschäftigt.

Um die erhöhten Datenübertragungsraten auszuweisen wird bei einigen Begriffen HT vorangestellt. HT steht dabei für High Throughput. z. B. HT-OFDM.

Für die hohen Datenraten wurde eine neue PHY-Layer mit diversen Neuigkeiten eingeführt:

- ➊ Multiple Input Multiple Output (MIMO)
- ➋ Selection Combining (Antenne mit dem besten Signal-Rausch-Verhältnis wird verwendet)
- ➌ Maximal Ration Combining (Bei SIMO-Systemen kann der Diversity Gewinn weiter erhöht werden, indem man die Empfangssignale beider Antennen linear kombiniert. Durch separates Kombinieren der Signale kann auch einer Mehrwegeausbreitung der entgegengewirkt werden.)
- ➍ Transmit Beamforming
- ➎ Adaptives Beamforming
- ➏ Raum-Zeit-Codes
- ➐ Raum-Multiplex-Verfahren
- ➑ Zusätzliche Coderate 5/6
- ➒ Verkürztes Guard-Intervall
- ➓ Kanäle mit 40MHz Bandbreite
- ➔ 52 anstelle von 48 Unterträger

5.3.4.2 - MIMO

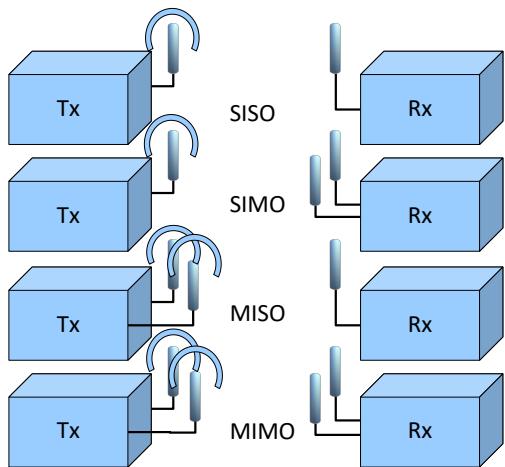


Abbildung 107: MIMO im Vergleich zu SISO, SIMO und MISO

Eine der wichtigsten neu eingeführten Verfahren ist das das MIMO - Übertragungsverfahren (**M**ultiple **I**nput **M**ultiple **O**utput) bei der Datenübertragung. Damit sind mehrere Empfangs- und Sendeeinheiten mit den zugehörigen Antennen gemeint.

Die Betrachtung, was Input oder Output ist wird aus der Sicht des Übertragungsmediums gemacht. Damit ist die Sendeseite der Input und die Empfangsseite der Output. Systeme nach IEEE- 802.11a, b oder g sind demnach SISO-Systeme (**S**ingle **I**nput **S**ingle **O**utput).

Dies ist die Grundlage für das Space-Time-

Coding, bei dem nicht nur die zeitliche sondern auch die räumliche Dimension zur Informationsübertragung genutzt wird.

5.3.4.3 - Selection Combining

Bei den Standards 802.11b/g wurden bereits 2 Antennen nach dem MISO-Konzept eingesetzt. Dabei wurden sie nach dem Switched-Antenna-Diversity-Funktion genutzt, bei der die Antenne mit dem bestem Signal-Rausch-Verhältnis genutzt wird. Die Auswahl der Antenne erfolgt während der Präambel-Testmessung.

Eine Steigerung der Empfangsleistung lässt sich erreichen wenn man die Signale auf den Empfangsantennen kombiniert. Dies reduziert auch das Problem der Mehrwegeausbreitung. Die intelligente Signalkombination erfolgt über Addierer, Multiplizierer und Verzögerer, deren Funktion auf den Einfallsinkel der auf der Antenne eintreffenden Wellenfront angepasst werden können. Dies entspricht einer speziellen Diversity-Form von Diversity und wird Maximal-Ration Combining (MRC) genannt. Auf der Seite der Empfänger mit mehreren Antennen greifen spezielle MRC-Algorithmen, die dafür sorgen, dass die empfangenen Signale optimal kombiniert werden und unter dem Strich ein verbessertes Signal erstellen. Der große Aufwand lohnt sich denn bei einer Antennenverdopplung ergibt sich ein Gewinn von 3dB, was einer Verdopplung entspricht.

Damit MRC eine hohe Effizienz liefert ist es erforderlich, dass die einzelnen Antennen jeweils ein unterschiedliches Signal empfangen können. Die unterschiedlichen Signale werden durch Störungen und Interferenzen hervorgerufen. Damit die Signale wirklich unterschiedlich sind, müssen die Antennen mindestens einen Abstand von $\lambda/2$ aufweisen, was 6,25cm entspricht.

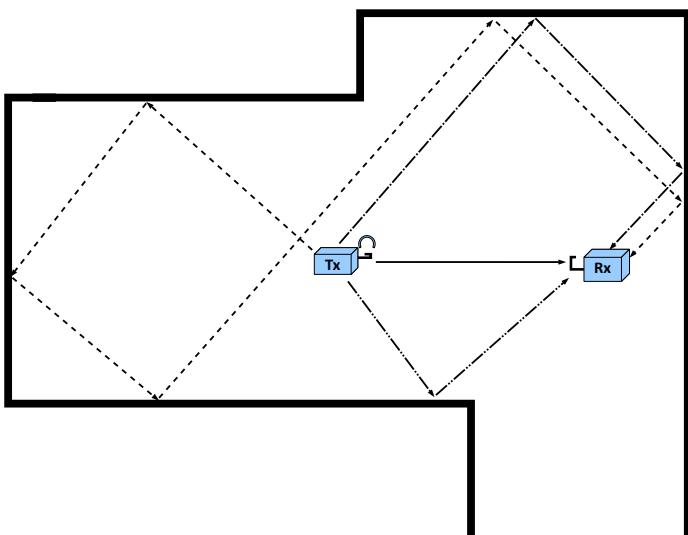


Abbildung 108: Multipath

Ein ausgesendetes Signal kam bei den bisherigen WLAN-Standards auf unterschiedlichen Wegen mit unterschiedlicher Signalstärke, zeitlich versetzt beim Empfänger an und führte dort zu Problemen bei der Signalerkennung. Zum einen wird auf direktem Weg über die Line of Sight (LOS) das stärkste Signal empfangen. Zusätzlich kommt das Signal über unterschiedliche Reflexionen zeitversetzt über die Non Line of Sight (NLOS) beim Empfänger an.

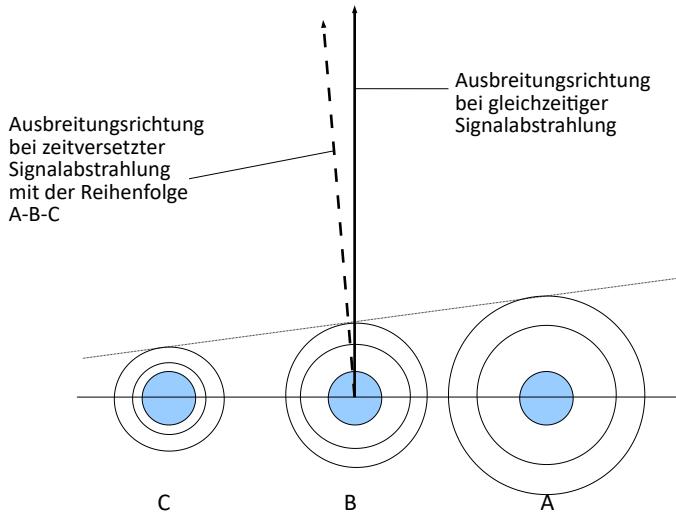
Bisher mussten die Effekte der Multipathübertragung heraus gefiltert werden. Dies geschah durch die Auswahl der besseren Antenne bei einer Diversity-Antenne (2 Antennen am Access Point).

Die störenden Reflexionen, hervorgerufen durch Wände, Personen usw. werden beim IEEE-802.11n-Standard als unterschiedliche nutzbare Kanäle verwendet. Durch die Verwendung mehrerer Antennen kann die dazu notwendige Information über die Einfallsrichtung der Funkwellen ermittelt werden.

Obwohl die Signale im selben Kanal übertragen werden lässt sich dadurch eine räumliche Signatur (Spatial Signature) zweier Signale ermitteln und voneinander unterscheiden. Dadurch wird die Kanalkapazität gesteigert.

Am besten funktioniert das, wenn die Signale möglichst unterschiedliche Wege also auch eine unterschiedlich lange Laufzeit haben. Bei idealen Empfangsbedingungen, wenn also jede Empfangsantenne das ungestörte Summensignal der Sendeantennen empfangen kann entsteht nur ein einziger Bitstrom. Damit wäre die Kapazität des Übertragungskanals nicht besser als bei SISO.

5.3.4.4 - Transmit Beamforming



Durch die Verwendung mehrerer Antennen und das zeitlich versetzte Abstrahlen eines Signals kann eine Richtwirkung erzielt werden.

Dies nennt sich Beamforming. Peilt man mehrere Empfänger mittels Beamforming an, spricht man von räumlichem Multiplexgewinn (Spatial Multiplexing).

Die derzeit verfügbaren Chipsätze unterstützen in der Regel zwei Streams und sind in der Lage mehr als zwei Sender und Empfänger zum Transport des Streams zu verwenden.

Abbildung 109: Beamforming

Allerdings funktioniert das nur bei Unicasts. Be Multicasts und Broadcasts kann das Transmit-Beamforming nicht durchgeführt werden da evtl. alle Stationen im Umfeld eines APs erreicht werden müssen. Damit kann also eine Funkzelle nicht vergrößert werden. Am Rand einer Funkzelle kann allerdings für einzelne Geräten die Datenrate erhöht werden.

5.3.4.5 - Adaptives Beamforming

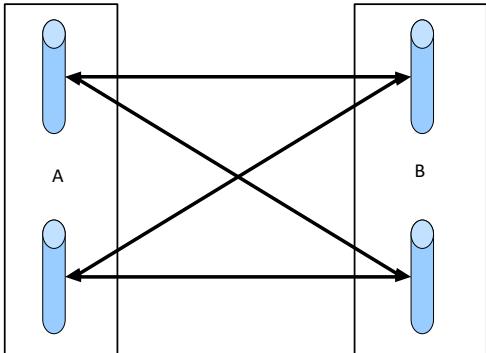
Wenn mehrere Signale über mehrere Antennen abgestrahlt werden, können diese Signale beim Empfänger kombiniert werden. Allerdings sind die Signale evtl. in der Phase verschoben. Daher muss beim Senden die Phasenlage angepasst werden um die maximale Summe der Signale beim Empfänger zu erreichen. Damit muss der Empfänger dem Sender mitteilen wie gut das Signal angekommen ist und bei jedem Frame muss ein Feintuning stattfinden, um Änderungen von Hindernissen oder bei der Empfängerposition auszugleichen.

5.3.4.6 - Raum-Zeit-Codes

Signale, die über unterschiedliche Wege beim Empfänger ankommen, haben auch einen unterschiedlichen Signalschwund (Fading) erfahren. Dadurch können sie auseinandergehalten werden. So kann die sogenannte Raum-Zeit-Block-Codierung (Space-Time Block Coding, kurz STBC) zum Tragen kommen. Damit kann neben der zeitlichen und spektralen Komponente noch eine räumliche Komponente das Multiplexen der Datenströme verwendet werden. Bei STBC wird aus zeitlich aufeinander folgenden Symbolen zu einem Block zusammengefasst, aus dem eine Matrix gebildet wird deren Spalten der Zeit entsprechen und die Zeilen den Antennen. STBC bietet sich vor allem an, wenn es senderseitig viele Antennen und Empfangsseitig wenige, oder nur eine Antenne gibt.

5.3.4.7 - Raum-Multiplex-Verfahren

Bei MIMO-Systemen kann der Datenstrom durch mehrere Antenne auf Sender- und Empfängerseite auf mehrere getrennte Datenströme aufgeteilt werden. Dies entspricht einem Raum-Multiplex (Spatial Multiplexing). In diesem Fall ist der Abstand der Antennen für die Aufteilung in unterschiedliche Datenströme verantwortlich im Gegensatz zur Multipath-Ausbreitung.



Es werden mindestens 2 und maximal 4 Antennen, im Abstand einer halben Wellenlänge der Trägerfrequenz, verwendet. Dadurch können mehrere Verbindungen gleichzeitig betrieben werden.

Bei zwei Antennen können, wie im linken Beispiel, gleichzeitig 4 Kanäle betrieben werden.

Bei n Sende- und m Empfangsantennen entspricht die Übertragung in einem MIMO-Kanal einem Gleichungssystem mit m Gleichungen und n Unbekannten.

Abbildung 110: Kanalanzahl bei mehreren Antennen

Mathematisch kann ein solches Gleichungssystem mit $r = H * s + u$ beschrieben werden. Mit s ist der Sendevektor und mit r wird der Empfangsvektor beschrieben. Mit u wird ein Vektor bezeichnet, der das statisch unabhängige Rauschen beschreibt. H ist eine $(n*m)$ -Matrix die den Übertragungskanal beschreibt.

Damit können maximal $k \leq \min(n,m)$ unabhängige Bitströme, die so genannten Spacial Streams erzeugt werden.

Auf der Empfängerseite kann sich die Beschreibungsmatrix H ständig ändern, da sich der Empfänger bewegen kann, oder Hindernisse sich verschieben können. Eigentlich müsste die Beschreibungsmatrix für jede Übertragung neu ermittelt werden.

Bei IEEE-802.11n wird für jeden Spatial Stream ein zeitlich von einander getrenntes Trainingssignal gesendet, so dass der Empfänger für jede Antennenpaarung (Position in der Beschreibungsmatrix) den Übertragungskanal schätzen kann. Leider erhöht sich dadurch der Overhead bei der Übertragung.

Im deutschsprachigen Raum werden die Spacial Streams als Senderzüge und Empfangszüge bezeichnet.

Die unterschiedlichen Kanäle lassen sich bei der selben Frequenz nutzen!

Das Raum-Multiplex-Verfahren setzt auf der Empfängerseite Kenntnis über den Kanal voraus, denn dort werden mittels einer intelligenten, echtzeitfähigen Signalverarbeitung aus den überlagerten Signalen die Teilströme detektiert.

Die Kanalkenntnisse können über Pilot-Symbole oder durch Abschätzung ermittelt werden.

Die Pilotsymbole werden in den Datenstrom eingestreut, was diesen unterbricht und Übertragungszeit für die Daten verloren geht. Dafür ist die Implementierung einfach und zuverlässig.

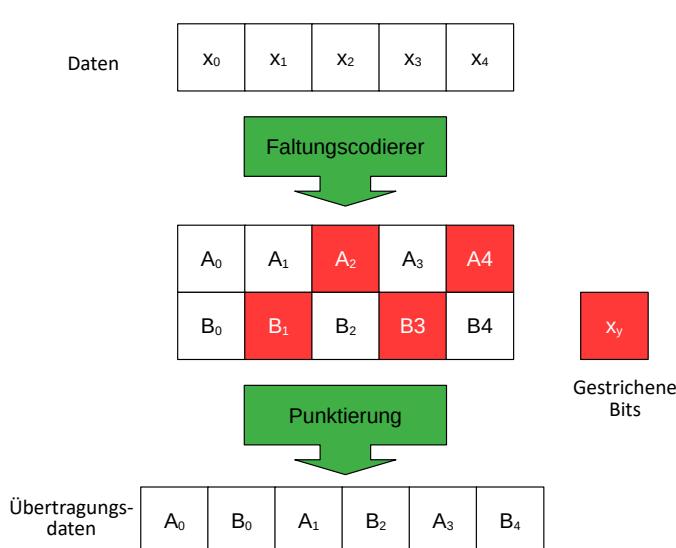
Bei der Abschätzung (blinde Kanalabschätzung) werden nur Datensignale übertragen und die Kanalabschätzung über statistische Eigenschaften der Übertragung ermittelt. Damit ist die Signalaufbereitung auf der Empfängerseite aufwändiger, jedoch wird der Datenstrom nicht unterbrochen.

Der Sender übermittelt dem Empfänger regelmäßig Informationen, mit denen der Empfänger sich dynamisch auf die Charakteristik der Übertragungspfade einstellen kann.

Bei den bisher verwendeten Standards mit OFDM-Nutzung waren die Kanäle 20 MHz breit. Mit dieser Bandbreite ließen sich eigentlich 64 anstelle der genutzten 53 Unterträger unterbringen. Bei 802.11n werden 57 Unterträger verwendet, die von -28 bis 28 durchnummeriert werden. Der Unterträger 0 werden wieder nicht genutzt und die Unterträger -21, -7, 7 und 21 werden ebenso wieder als Pilotkanäle verwendet. Für die Datenübertragung werden damit 52 Unterträger im Vergleich zu bisher 48 Unterträgern genutzt.

Die Pilotkanäle leisten beim Thema Raum-Multiplex keinen Beitrag, sondern werden für die Bezugscodierung benötigt.

5.3.4.8 - Zusätzliche Coderate



Bei den bisherigen Standards wurden Coderaten von $1/2$, $2/3$ oder $3/4$ verwendet. Im Standard 802.11n wurde im Rahmen des HT-OFDM-Verfahrens eine Effizienzsteigerung durch Einführung der Coderate $R = 5/6$ erreicht.

Abbildung 111: Punktierung für die Coderate $R = 5/6$

5.3.4.9 - Verkürztes Guard-Intervall

Bisher wurde für das Guard-Intervall (GI) 800ns und daraus resultierend eine Gesamtsymbollänge von $4\mu s$ verwendet. Damit ergibt sich für die Symbolrate 0,25 MSymbole/s.

Für die HT-OFDM wurde für 802.11n ein verkürztes Guard-Intervall von 400ns eingeführt. Damit ergibt sich für die Gesamtsymbollänge $3,6 \mu s$, was einer Symbolrate von 0,778 Msymbole/s entspricht.

5.3.4.10 - Verdopplung der Kanalbandbreite von 20 MHz auf 40MHz

Eine weitere Verbesserungsmaßnahme sind 40MHz breite Kanäle, wobei die Kanäle nebeneinander liegen müssen. Damit sind 108 Unterkanäle verfügbar. (also mehr als die Verdoppelung von 52 Unterträgern)

Die verwendbaren Unterträger sind von -58 bis -2 und von 2 bis 58 durchnummeriert. Die Unterträger -1, 0 und 1 werden nicht verwendet. Die Unterträger -53, -25, -11, 11, 25 und 53 werden wieder als Pilotkanäle verwendet. Welcher Kanal als zweiter Kanal verwendet wird, gibt die MAC-Ebene durch das Secondary-Offset-Element vor. Dabei kann nur der vorhergehende oder nachfolgende Kanal festgelegt werden.

Im 2,4GHz-Band stößt die Kanalbündelung schnell an Grenzen, da es nur 3 überschneidungsfreie Kanäle gibt. Obwohl es im 802.11n-Standard definiert ist, wird es von der Wi-Fi-Alliance nicht erlaubt.

Im 5GHz-Band ist das einfacher.

5.3.4.11 - Low Density Parity-Check

Bisher war die Dotierung von Information mit zusätzlichen Bits zur Durchführung der Forward Error Correction (FEC) mit Faltungscodierern (Binary Convolutional Code (BCC)) durchgeführt worden.

Ab einer Datenrate von 300 Mbit/s wird der Faltungscodierer zwei Mal durchlaufen um der Störanfälligkeit bei höheren Datenraten gerecht zu werden.

Optional ist für HT-OFDM der Low Density Parity-Check (LDPC) als Codierung anstelle der BCC-FEC mit darauffolgender Punktierung vorgesehen um eine Performance-Steigerung zu erzielen.

Dabei werden mit einer linearen Blockcodierung Parity-Bits hinzugefügt. Die Paritätsbits werden bei der LDPC-Codierung durch die eingehenden Bits aus einer Matrix ausgewählt.

802.11n sieht 3 unterschiedliche Codeblock-Längen mit 648, 1296 und 1944 Bits vor. Bei der Codierung werden die Daten in Blöcke einer bestimmten Länge unterteilt und diese Blöcke werden zu einem Codewort-Block umgewandelt. Mit LDPC wandelt x eingehende Bits in y ausgehende Bits um indem y-x Paritätsbits hinzugefügt werden. Beispielweise werden bei einem LDPC(864, 1296)-Codierer 864 Bits mit 432 zusätzlichen Bits zu einem 1296Bit großen Codewort umgewandelt. Das Verhältnis von eingehender Blocklänge zu Codewort-Blocklänge ergibt die Coderate. Je kleiner die Coderate ist desto mehr Paritäts-Information wird hinzugefügt.

Tabelle 33: [IEEE-802.11-2016]

Coding-Rate [R]	LDPC Informationsblock Länge [Bits]	LDPC Codewortblock Länge [Bits]
1/2	972	1944
1/2	648	1296
1/2	324	648
2/3	1296	1944
2/3	864	1296
2/3	432	648
3/4	1458	1944
3/4	972	1296
3/4	486	648
5/6	1620	1944
5/6	1080	1296
5/6	540	648

5.3.4.12 - Zusammenfassung der Schritte zur Verbesserungen der Datenübertragungsraten

Die Änderung bis zu einer Datenübertragungsrate von 600Mbit/s wurden in vielen kleinen Schritten vollzogen ohne die Modulationsart zu verändern:

- ➊ Anstatt der Verwendung von OFDM mit 48 parallelen Unterträgern wurden 52 Unterträger verwendet. Dies führt zu einer Steigerung der Datenübertragungsrate von 54 Mbit/s auf 58,5 Mbit/s.
- ➋ Durch die FEC-Rate von 5:6 konnte eine weitere Steigerung auf 65 Mbit/s erreicht werden.
- ➌ Durch die Verkürzung des Guard Intervalls (Sicherheitsabstand) von 800ns auf 400ns zwischen zwei OFDM-Symbolen werden schließlich 72,2 Mbit/s erreicht.
- ➍ Durch die Verbreiterung der genutzten Kanalbandbreite von 20 MHz auf 40MHz können 108 Unterträger verwendet werden. Damit steigert sich die Datenübertragungsrate auf einem spatial Stream auf 150Mbit/s.
- ➎ Durch die Verwendung von bis zu 4 spacial Streams können Datenübertragungsraten von bis zu 600Mbit/s erreicht werden.

Tabelle 34: Vergleich der erzielbaren Datenrate OFDM und HT-OFDM mit einem Spacial Stream

Modulation	Code-Rate	Datenrate [MBit/s]				
		OFDM		HT-OFDM		
		48 Unterträger	52 Unterträger GI = 800ns	52 Unterträger GI = 400ns	108 Unterträger GI = 800ns	108 Unterträger GI=400ns
BPSK	1/2	6	6,5	7,2	13,5	15
QPSK	1/2	12	13	14,4	27	30
QPSK	3/4	18	19,5	21,7	40,5	45
16-QAM	1/2	24	26	28,9	54	60
16-QAM	3/4	36	39	43,3	81	90
64-QAM	2/3	48	52	57,8	108	120
64-QAM	3/4	54	58,5	65	121,5	135
64-QAM	5/6	-	65	72,2	135	150

5.3.4.13 - Vergleich der spektrale Effizienzsteigerung

Vergleicht man die Standards bezüglich der möglichen Datenübertragungsraten und benötigter Bandbreite, kommt an zur folgenden Übersicht.

Tabelle 35 Spektrale Effizienz der 802.11-Standards [GAST-ASG-2012]

PHY	Spektrale Effizienz [Mbps/MHz]
802.11 (FHSS / DSSS)	0,09
802.11b	0,5
802.11a/g	2,7
802.11n (20MHz, MCS15)	6,5
802.11n (40MHz, MCS15)	6,75

5.3.4.14 - Modulation Coding Scheme (MCS)

Bei den bisherigen WLAN-Standards war die Ermittlung der Datentransferrate vom Funkkanal abhängig. Je besser der Funkkanal ist, desto höher ist die Datentransferrate.

Bei IEEE-802.11n wurde statt dessen das Modulation Coding Scheme (MCS) eingeführt. MCS definiert eine Reihe von Variablen wie z. B. die Anzahl der spatialen Streams, Datenrate und Modulation jedes Datenstroms, Interferenzen oder Bewegung des Senders. Während der Datenübertragung wird für jeden Stream der optimale MCS ermittelt und angewendet. Als Basis dienen die jeweiligen Kanalbedingungen.

Im Standard IEEE-802.11n in der Version V2 vom März 2007 werden 77 MCS (0 – 76) definiert, von denen jedes Gerät 8 unterstützen muss. Dabei werden die Modulationsarten und Code-Raten nach unterschiedlichen Randbedingungen (Kanalbandbreite, Guard-Intervall) in einer Tabelle zusammengefasst.

Tabelle 36: Erzielbare HT-OFDM-Datenraten mit MCS 0 bis MCS 7 bei 20MHz-Kanalbreite

MCS	Modulation	Bits/Unterkanal (N _{BPSCS})	Bits / OFDM- Symbol (N _{CBPS})	FEC-Code- Rate (R)	Datenbits/OFDM- Symbol (N _{DBPS})	Datenrate [MBit/s]	
						GI=800ns	GI=400ns (optional)
0	BPSK	1	52	1/2	26	6,5	7,2
1	QPSK	2	104	1/2	52	13	14,4
2	QPSK	2	104	3/4	78	19,5	21,7
3	16-QAM	4	208	1/2	104	26	27,9
4	16-QAM	4	208	3/4	156	39	43,3
5	64-QAM	6	312	2/3	208	52	57,8
6	64-QAM	6	312	3/4	234	58,5	65
7	64-QAM	6	312	5/6	260	65	72,2

Aus der Tabelle 36 können die Datenrate wie folgt berechnet werden:

$$\text{Datenrate} = \text{Symbolrate} \times \text{Bits/Unterkanal}(N_{BPSCS}) \times \text{Anz. Unterkanäle} \times \text{Coderate}(R) \times \text{Sender- und Empfängerzüge} \quad (25)$$

Beispiel:

Bei einem Guard-Interval von 800ns werden für die Übertragung 4μs benötigt was einer Symbolrate von 0,25MSymbole/s entspricht.

Die Datenrate von 58.5MBit/s = 0,25MSymbole/s * 6 Bits/Unterkanal * 52 Unterkanäle * ¾ Coderate * 1 Sender- und Empfangszüge

Die MCS 8 bis 15 beziehen sich auf 2 Sender- und Empfangszüge, sowie den Durchlauf einer BCC-FEC-Codierung.

Tabelle 37: Erzielbare HT-OFDM-Datenraten mit MCS 8 bis MCS 15 bei 20MHz-Kanalbreite

MCS	Modulation	Bits pro Unterkanal (N _{BPSCS})	Bits pro OFDM-Symbol (N _{CBPS})	FEC-Code- Rate (R)	Datenbits pro OFDM-Symbol (N _{DBPS})	Datenrate [MBit/s]	
						GI=800ns	GI=400ns (optional)
8	BPSK	1	52	1/2	52	13	14,4
9	QPSK	2	104	1/2	104	26	28,9
10	QPSK	2	104	3/4	156	39	43,3
11	16-QAM	4	208	1/2	208	52	57,8
12	16-QAM	4	208	3/4	312	78	86,7
13	64-QAM	6	312	2/3	416	104	115,6
14	64-QAM	6	312	3/4	468	117	130
15	64-QAM	6	312	5/6	520	130	144,4

5.3.4.14.1 - MCS 32

MCS 32 nimmt eine Sonderstellung ein. Dabei wird zwar mit einer Kanalbreite von 40MHz gearbeitet, jedoch werden bei jedem 20MHz-Band 8 Unterträger als Pilotkanäle genutzt, wodurch sich die Anzahl der Unterträger von 108 auf 96 reduziert. MCS32 wird für die Erzielung eine Datenübertragungsrate von 6MBit/s verwendet und stellt damit die robusteste OFDM-Version dar.

Tabelle 38MCS32

MCS	Modulation	Bits pro Unterkanal (N _{BPSCS})	Bits pro OFDM- Symbol (N _{CBPS})	FEC-Code- Rate (R)	Datenbits pro OFDM- Symbol (N _{DBPS})	Datenrate [MBit/s]	
						GI=800ns	GI=400ns (optional)
32	BPSK	1	48	1/2	24	6	6,7

Die MCS-Varianten 33 bis 76 sind für 2, 3 oder 4 Sender- und Empfangszüge spezifiziert.

5.3.4.14.2 - Verwaltung der MCS-Varianten

Welche MCS unterstützt wird auf der MAC-Ebene im so genannten Supported-MCS-Set-Feld verwaltet, das eine Länge von 128 Bits hat. Unter anderem enthält dieses Feld eine 77 Bit lange RX-MCS-Bitmaske, über die die eingangsseitige Unterstützung der MCS angezeigt wird. Zudem wird die maximal unterstützte Datenrate in 1 MBit/s-Schritten zwischen 1 und 1023 MBit/s angezeigt.

5.3.4.15 - IEEE-802.11n-PPDU-Formate

Für den Betrieb der MIMO-Geräte stehen 3 Modi zur Verfügung:

- Legacy -Mode / Non HT-Mode (802.11a,b,g)
- HT-Mixed-Mode (802.11a,b,g und 802.11n)
- HT-Greenfield-Mode (nur 802.11n)

Damit die alten Standards noch bedient werden können wurden 3 unterschiedliche Gerätetypen definiert:

- 20/40 HT 802.n-Systeme, die sowohl 20MHz als auch 40MHz breite Kanäle unterstützen
- 20 HT 802.n-Systeme, die nur 20MHz breite Kanäle unterstützen
- Non-HT Systeme, die nur 802.11a/h oder b/g unterstützen.

HT steht in diesem Zusammenhang für High Throughput. Nur für die HT-Geräte stehen der Greenfield- und der Mixed-Mode zur Verfügung.

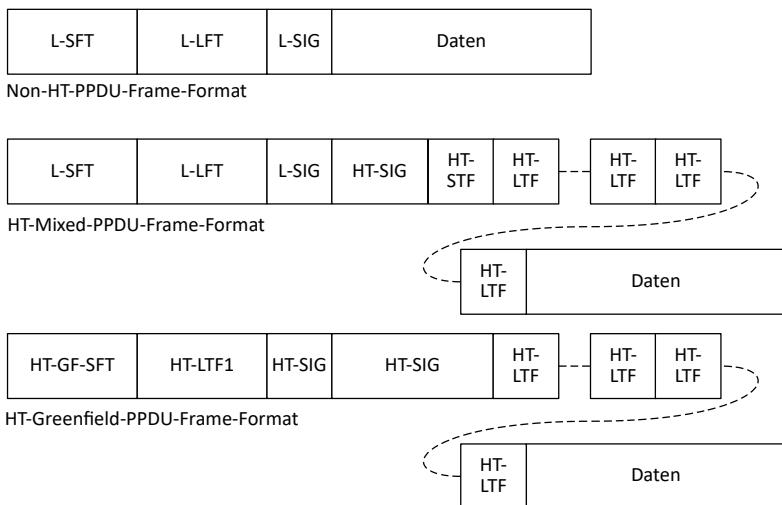


Abbildung 112: IEEE-802.11n-PPDU-Formate

Die Felder haben keine neuen Funktionen, sondern nur neue Namen bekommen

- L-SFT (Non HT Short Training Field) entspricht der kurzen Trainingssequenz.
- L-LTF (Non HT Long Training Field) entspricht der langen Trainingssequenz.
- L-SIG (Non HT SIGNAL Field) entspricht dem Signal-Feld
- HT-SIG (HT SIGNAL Field) entspricht dem Signalfeld eines HT-OFDM-Frames
- HT-STF (HT Short Trainings Field) entspricht einer 4 µs langen Trainingssequenz zur Einschätzung der Automatic Gain Control (AGC) eines MIMO-Systems. Bei Nutzung eines 20MHz-Kanals entspricht das Feld dem von 802.11a/g. Bei 40MHz Kanalbreite wird die 20MHz-Variante von der Frequenz her verdoppelt und in der Phase 90° verschoben.
- HT-LTF (HT Long Trainings Field) besteht aus zwei Teilen. Der erste Teil (HT-LTF1) entspricht einem HT-Long-Training-Field oder einer Folge von bis zu 4 HT-STFs und wird für die Demodulation des Datenteils (PSDU) benötigt. Deshalb wird er auch als Data HT-LTF bezeichnet. Der zweite Teil des HT-LTF ist optional und beinhaltet 0 bis 4 HT-LTFs, die für die Hervorhebung von zusätzlichen räumlichen Dimensionen eines MIMO-Kanals genutzt werden können. Diese HT-LTFs werden auch als Extension HT-LTFs bezeichnet.
- HT-GF-STF (HT-Greenfield Short Training Field) steht am Anfang eines GT-Greenfield-Frames. Es hat eine spezielle Wellenform, deren Länge jeweils 0,8µs beträgt. Da 10 Signalperioden genutzt werden, ergibt sich für HT-GF-STF eine Dauer von 8 µs.

5.3.4.16 - HT-Signal-Felder

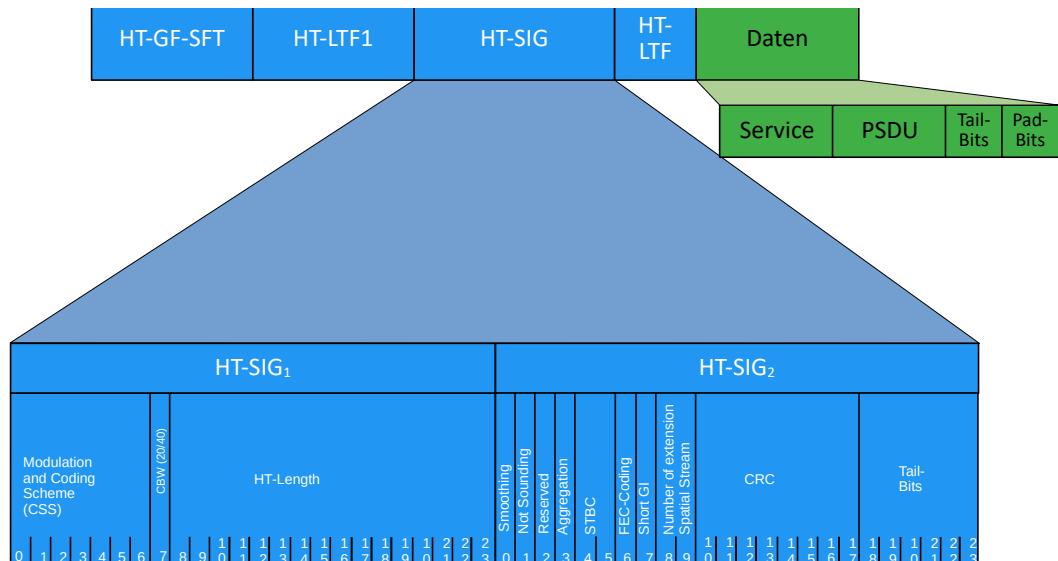


Abbildung 113: HT-SIGNAL- Felder

- HT-SIG₁-Felder
 - MCS (Modulation and Coding Scheme) Die 7 Bits entsprechen dem verwendeten MCS-Index
 - CBW (Channel Band Width (20 oder 40 MHz)
 - 16 Bit langes Feld das die Länge der PSDU-Bytes enthält. (0 bis 65535)
 - HT-SIG₂-Felder
 - Smoothing: 1 Bit langes Feld mit Methode zur Kanalabschätzung (0 = Die Unterträger werden unabhängig voneinander betrachtet. 1 = Kanalabschätzung erfolgt über den gesamten Kanal)
 - Not Sounding 1 Bit langes Feld für das PPDU-Format. 0 = Sounding Frame zur Aussendung von Transmit Beamforming Frames zur Kalibrierung / 1 = kein Sounding Frame)
 - Aggregation (0 = PPDU ist kein A-MPDU / 1 = Es handelt sich bei PPDU um eine A-MPDU)
 - STBC Unterschied zwischen Raum-Zeit-Strömen und Sender- und Empfängerzügen falls nicht = 00)
 - FEC-Coding (0= BCC-FEC / 1 = LDPC-FEC)
 - Short GI 1 = Nach HT-Trainingsintervalle folgen kurze Guard Intervalle)
 - Number of extension Spatial Streams (2 Bits für Anzahl der erweiterten Sender- und Empfängerzüge)
 - CRC Prüfsumme über die Bits 0 bis 23 im HT-SIG₁
 - Tail-Bits 6 Bits dienen dem Initialisieren des Faltungscodierers mit einem definierten Nullstatus

5.3.4.17 - Sendeleistung

Es gelten nach wie vor die festgelegten Sendeleistungen mit 100mW im 2,4GHz-Band und 200mW/1W im 5GHz-Band.

5.3.4.18 - CCA-Empfindlichkeit

Bei 20MHz breiten Kanälen gilt die bisherige Empfindlichkeit von OFDM.

Der Beginn eines gültigen OFDM-Symbols liegt vor, wenn für $4 \mu\text{s}$ ein Signal das größer oder gleich 90% der kleinsten Empfängerempfindlichkeit ist, anliegt.

Die kleinste Empfängerempfindlichkeit ist bei einer Datenrate von 6MBit/s -82dBm. Weiterhin zeigt die CCA-Prozedur ein belegtes Medium an sobald ein beliebiges Signal mit -62dBm anliegt.

Bei 40MHz gilt, dass ein Signal anliegt, sobald der Empfänger für $4\mu\text{s}$ ein Signal mit 90% der geringsten Empfängerempfindlichkeit von -79dBm empfängt.

5.3.4.19 - Empfängerempfindlichkeit

Die Empfängerempfindlichkeit ist von der verwendeten Modulationsart, der Coderate und der Kanalbreite abhängig.

Tabelle 39: Mindest-Empfängerempfindlichkeit bei 802.11n

Modulations-Verfahren	Code-Rate	Empfängerempfindlichkeit bei 20MHz Kanalbandbreite [dBm]	Empfängerempfindlichkeit bei 40MHz Kanalbandbreite [dBm]
BPSK	1/2	-82	-79
QPSK	1/2	-79	-76
QPSK	3/4	-77	-75
16-QAM	1/2	-74	-71
16-QAM	3/4	-70	-67
64-QAM	2/3	-66	-63
64-QAM	3/4	-65	-62
64-QAM	5/6	-64	-61

5.3.4.20 - 802.11n-MAC

Zur Effizienzsteigerung wurden auch auf dieser Ebene einige Verbesserungen vorgenommen.

5.3.4.20.1 - Reduced IFS

Mit der Reduced Inter Frame Space (RIFS) wurde ein neuer kleinster IFS eingeführt. Er kann angewendet werden, wenn die Frames von einer Station ausgesendet werden und keine andere mit SIFS abgetrennte Frameaussendung erwartet wird.

Bei 802.11n ist der RIFS mit 2µs und der SIFS mit 16 µs definiert.

5.3.4.20.2 - Aggregationsverfahren

Bei 802.11n gibt es zwei Aggregationsverfahren. (A-MPDU oder A-MSDU) Beide führen zu einer Reduzierung des Overheads indem für eine Datenaussendung nur eine Präambel übertragen wird. Voraussetzung ist, dass alle Frames die selbe Empfängerstation haben und die selbe QoS-Klasse angewendet wird. Weiterhin ist die maximale Framelänge, die ausgesendet werden kann von der Coherence Time abhängig. Die Dauer einer fehlerfreien Frame-Übertragung muss kleiner als die Coherence Time sein. Die Channel Coherence Time ist davon abhängig, wie schnell sich die Übertragungsbedingungen ändern, also wie schnell sich Sender, Empfänger und Hindernisse bewegen. Je schneller sich die Situation ändert desto kürzer ist die maximale Framelänge da die Datenrate reduziert wird und damit die Dauer der Frame-Übertragung zwangsläufig steigt. Eine Empfangsstation gibt über das A-MPDU-Length-Exponent-Feld oder Maximum-A-MSDU-Capability-Feld bekannt wie lange die A-MPDU oder A-MSDU sein darf.

5.3.4.20.2.1 - A-MPDU

Bei den MPDUs handelt es sich um Daten die von der MAC-Ebene an den PLCP übergeben werden. Das sind komplette Frames inklusive MAC-Header. Damit wird bei der A-MPDU komplettete Frames aneinandergereiht und übertragen. Eine A-MPDU enthält einen oder mehrere Subframes. Die Gesamtlänge eines A-MPDUs darf bis zu 65535 Bytes entsprechen. Eine MPDU kann bis zu 4096 Bytes enthalten. Ein Subframe enthält einen MPDU-Delimiter und die MPDU. Mit Ausnahme des letzten Subframes können die Subframes 0 bis 3 Padding-Bytes angehängt bekommen, damit die Subframe-Länge immer einem Vielfachen von 4 Bytes entspricht. Der A-MPDU-Delimiter enthält 4 Felder. (Reserved, MPDU Length, CRC und Delimiter-Signatur)

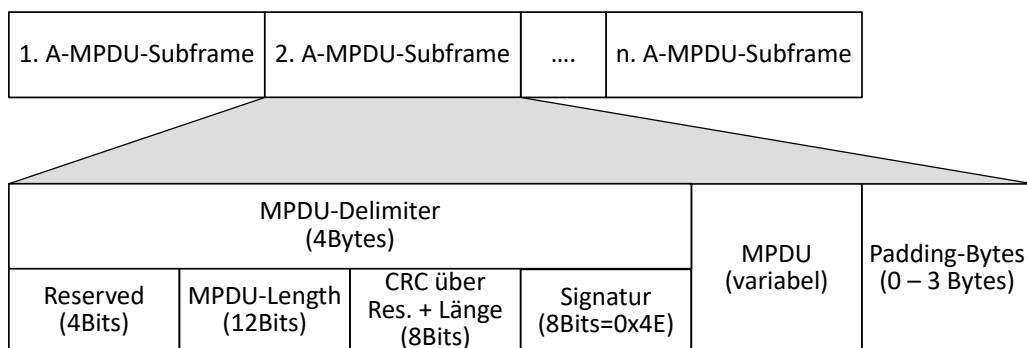


Abbildung 114: A-MPDU-Frame und Subframes

5.3.4.20.2.2 - A-MSDU

Bei den MSDUs handelt es sich um den Datenteil eines MAC-Frames. Mit einer A-MSDU werden mehrere MSDUs als Subframes zusammengefasst und übertragen.

Mit Ausnahme des letzten Subframes können die A-MSDU-Subframes 0 bis 3 Padding-Bytes angehängt bekommen, damit die Subframe-Länge immer einem Vielfachen von 4 Bytes entspricht.

Ein A-MSDU-Subframe-Header ist 14 Bytes groß und enthält die 6 Byte großen Quell- und Ziel-Adressen sowie die Länge. Damit entspricht ein A-MSDU-Frame einem Ethernet-Frame nach IEEE802.3. Die Quell- und Zieladressen können unterschiedlich sein solange die A-MSDU-Frames zwischen den denselben WLAN-Stationen ausgetauscht werden. Damit können Ethernet-Frames ganz einfach über eine WLAN-Funkstrecke mittels A-MSDUs transportiert werden. Die maximale A-MSDU-Länge beträgt 3839 oder 7935 Bytes. Wird eine A-MSDU in einem A-PDU übertragen ist die maximale a-MSDU-Länge 4065 (= 4095 – MPDU-Overhead).

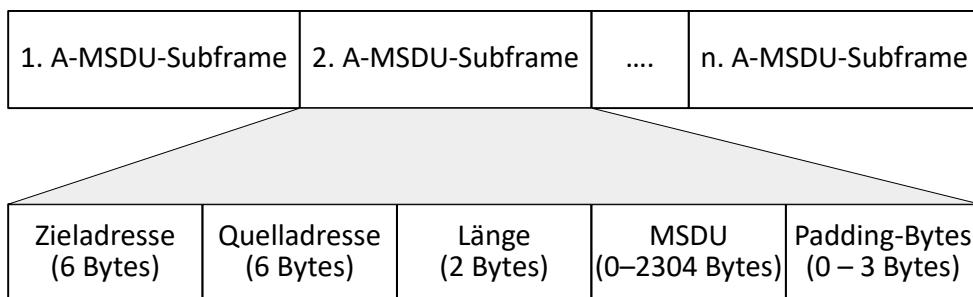


Abbildung 115: A-MSDU und Subframes

Vergleicht man A-MPDU und A-MSDU miteinander, ist das A-MSDU-Verfahren effektiver da die MAC-Header in den Subframes sich negativer auswirken. Durch Verschlüsselung wird das Missverhältnis sogar noch verschärft.

5.3.4.20.3 - Block-Acknowledgement

Jeder Unicast-Frame wird im ursprünglichen Standard mit einem ACK quittiert. Mit dem 802.11e-Standard wurde ein Block-Acknowledge-Verfahren (BlockACK) eingeführt, womit mehrere Frames zusammen bestätigt werden können. Dies reduziert den Overhead.

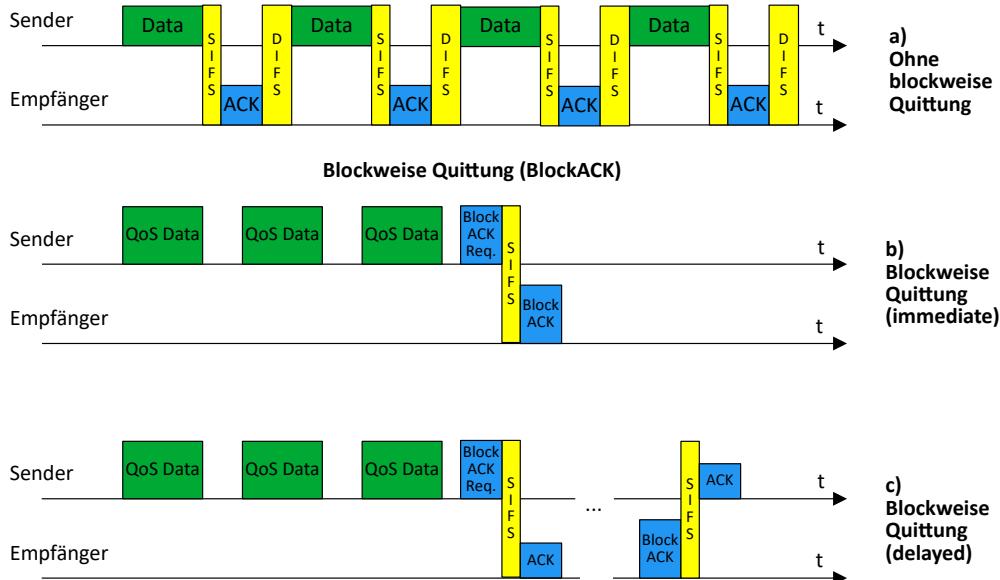


Abbildung 116: BlockACK

In Abbildung 116 a) ist der Ablauf ohne eine blockweise Bearbeitung dargestellt. Dabei wird jedes Datenframe mit einem ACK nach SIFS quittiert.

Bei der blockweisen Quittierung wird wie bei TCP mit einem Window-Verfahren agiert. Es wird für jedes Frame innerhalb des Fensters eine Quittung im BlockACK gesendet. Geht bei Abbildung 116 b) der zweite QoS-Data-Frame verloren so wird nur der erste und dritte Frame quittiert. Damit kann selektiv der zweite QoS-Data-Frame wiederholt werden.

Beim BlockACK-Verfahren gibt es zwei Varianten. (immediate / delayed)

- ➊ Beim Immediate BlockACK wird sofort nach einem SIFS quittiert.
- ➋ Beim Delayed BlockACK wird nur die Aufforderung zur Quittierung nach einem SIFS quittiert. Der eigentliche Block-ACK erfolgt dann später.

Der Vorteil dieser Vorgehensweise ist eine schnellere Bearbeitung da weniger Protokoll-Overhead abzuhandeln ist. So werden z. B. einige SIFS eingespart. Der Nachteil der Vorgehensweise ist, dass der Sender die Daten länger vorhalten muss, da er erst nachdem alle QoS-Data-Frames eines Blocks positiv quittiert wurden die Frames aus dem Speicher entfernen kann. Dies gilt vor allem für die Delayed-Variante.

5.3.4.20.4 - BlockACK-Frame-Format

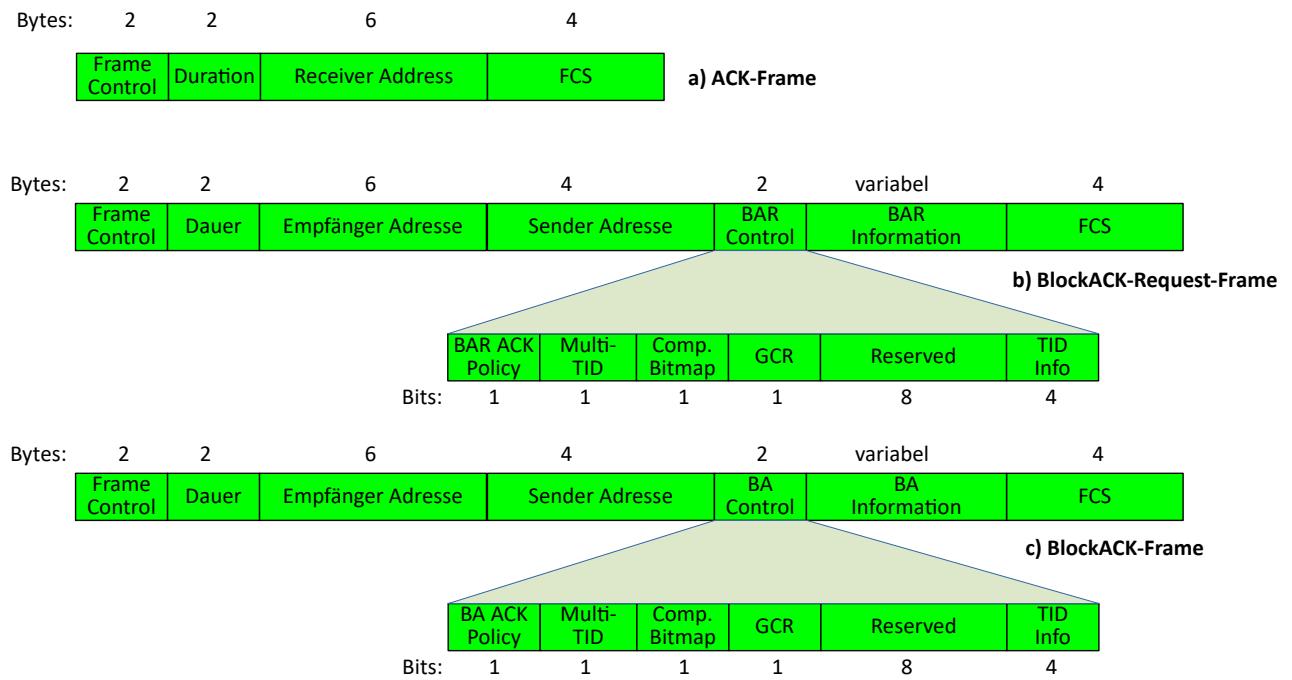


Abbildung 117: Aufbau der ACK und BlockACK - Frames

5.3.4.20.4.1 - BlockACK-Request

Siehe hierzu Abbildung 117 b).

Die Bedeutung der BAR-Control-Feldes (BAR = BlockAckReq) ist folgender:

BAR-ACK-Policy (0 = Kein Immediate BlockACK gewünscht → Delayed BlockACK / 1 = Immediate ACK gewünscht)

Die nächsten drei Bits wählen die Block-ACK-Request-Variante aus:

Tabelle 40: BlockACK-Varianten

Multi-TID-Feld	Compressed-Bitmap-Feld	GCR-Feld	BlockAck-Req. Variante
0	0	0	Basic BlockAckReq (obsolete)
0	1	0	Compressed BlockAckReq
1	0	0	Extended Compressed BlockAckReq
1	1	0	Multi-TID BlockAckReq
0	0	1	Reserved
0	1	1	GCR BlockAckReq
1	0	1	Reserved
1	1	1	Reserved

5.3.4.20.4.1.1. Basic BlockACK-Request Variante

Diese Variante ist obsolet und wir nicht weiter gewartet.

Das TID-Info-Sub-Feld im BAR-Control-Feld enthält die TID, für das der BlockACK-Frame angefordert wird. TID steht für Traffic Identifier. Es gibt 16 Werte. 8 identifizieren Traffic Categories (TCs) und 8 identifizieren einen konfigurierten Traffic Stream (TS).

Hier besteht das BAR-Information-Feld aus 2 Sub-Feldern:

- ➊ Fragment-Nummer (wir hier auf 0 gesetzt)
- ➋ Sequenznummer (enthält die Start-Sequenznummer der ersten MSDU für die dieser BlockACK-Request gesendet wird)

5.3.4.20.4.1.2. Compressed BlockACK-Request Variante

Das TID-Info-Sub-Feld im BAR-Control-Feld enthält die TID, für das der BlockACK-Frame angefordert wird.

Hier besteht das BAR-Information-Feld aus 2 Sub-Feldern:

- ➊ Fragment-Nummer (wir hier auf 0 gesetzt)
- ➋ Sequenznummer (enthält die Start-Sequenznummer der ersten MSDU oder A-MSDU, für die dieser BlockACK-Request gesendet wird)

5.3.4.20.4.1.3. Extended Compressed BlockACK-Request Variante

Das TID-Info-Sub-Feld im BAR-Control-Feld enthält die TID, für das der BlockACK-Frame angefordert wird.

Hier besteht das BAR-Information-Feld aus 2 Sub-Feldern:

- ➊ Fragment-Nummer (wir hier auf 0 gesetzt)
- ➋ Sequenznummer (enthält die Start-Sequenznummer der ersten MSDU oder A-MSDU, für die dieser BlockACK-Request gesendet wird)

5.3.4.20.4.1.4. Multi-TID BlockACK-Request Variante

Das TID-INFO-Sub-Feld des BAR-Control-Feldes verweist auf die Anzahl (+1) der TIDs im BAR-Information-Feld. So bedeutet ein Wert von 2, dass es im BAR-Information-Feld um drei TIDs geht.

Hier besteht das BAR-Information-Feld aus 2 Sub-Feldern (Wird für jede TID wiederholt):

- ➊ Per TID-Info (Bit 0 bis Bit11 = Reserviert, Bit 12 bis Bit 15 = TID)
- ➋ BlockAck Starting Sequence Control.

5.3.4.20.4.1.5. GCR BlockACK-Request Variante

(GCR = groupcast with Retries)

Das TID-INFO-Sub-Feld des BAR-Control-Feldes ist auf 0 gesetzt.

Hier besteht das BAR-Information-Feld aus 2 Sub-Feldern:

- ➊ Bit 0 bis Bit 15: BlockAck Starting Sequence Control.
 - ➌ Fragment-Nummer (wir hier auf 0 gesetzt)
 - ➌ Sequenznummer (enthält die Start-Sequenznummer der ersten MSDU oder A-MSDU, für die dieser BlockACK-Request gesendet wird)
- ➋ Bit 16 bis Bit 63: GCR Group Adresse

5.3.4.20.4.2 - BlockACK Frame

Siehe hierzu Abbildung 117 c).

Im Feld Empfänger-Adresse ist die Station hinterlegt, welche die Block-Quittung angefordert hat.

Die Bedeutung der BA-Control-Feldes (BA = BlockAck) ist folgender:

BAR-ACK-Policy (0 = Kein Immediate BlockACK gewünscht → Delayed BlockACK / 1 = Immediate ACK gewünscht)

Die nächsten drei Bits wählen die Block-ACK-Variante aus. Siehe hierzu Tabelle 40.

5.3.4.20.4.2.1. Basic BlockACK Variante

Diese Variante ist obsolet und wir nicht weiter gewartet.

Das TID-Info-Sub-Feld im BA-Control-Feld enthält den TID, für den der BlockACK-Frame angefordert wurde.

TID steht für Traffic Identifier. Er gibt 16 Werte. 8 identifizieren Traffic Categories (TCs) und 8 identifizieren einen konfigurierten Traffic Stream (TS).

Hier besteht das BA-Information-Feld aus 2 Sub-Feldern:

- ➊ BlockACK-Starting-Sequence Control
- ➋ Die BlockACK-Bitmap besteht aus 128 Bytes und dient dazu den Status von bis zu 64 **MPDUs** zu signalisieren. Die Bit-Position bezieht sich immer auf das BlockACK-Starting-Sequence-Control-Subfeld + n. Ist das Bit gesetzt wird signalisiert dass die MPDU angekommen ist und somit quittiert wird. Ist das Bit auf 0 gesetzt wird signalisiert, dass die MPDU nicht angekommen ist.

5.3.4.20.4.2.2. Compressed BlockACK Variante

Das TID-Info-Sub-Feld im BA-Control-Feld enthält den TID, für den der BlockACK-Frame angefordert wurde.

Hier besteht das BA-Information-Feld aus 3 Sub-Feldern:

- ➊ Fragment-Nummer (wir hier auf 0 gesetzt)
- ➋ BlockACK-Starting-Sequence Control
- ➌ Die BlockACK-Bitmap besteht aus 8 Bytes also 64 Bits und dient dazu den Status von bis zu 64 **MSDUs** zu signalisieren. Die Bit-Position bezieht sich immer auf das BlockACK-Starting-Sequence-Control-Subfeld + n. Ist das Bit gesetzt wird signalisiert dass die MSDU oder A-MSDU angekommen ist und somit quittiert wird. Ist das Bit auf 0 gesetzt wird signalisiert, dass die MSDU oder A-MSDU nicht angekommen ist.

5.3.4.20.4.2.3. Multi-TID BlockACK Varianten

Das TID-INFO-Sub-Feld des BA-Control-Feldes verweist auf die Anzahl (-1) der TIDs im BAR-Information-Feld. So bedeutet ein Wert von 2, dass es im BAR-Information-Feld um eine TID geht.

Hier besteht das BA-Information-Feld aus 3 Sub-Feldern (wird für jede TID wiederholt):

- ➊ Fragment-Nummer (wir hier auf 0 gesetzt)
- ➋ Per TID-Info (TID)
- ➌ BlockAck Starting Sequence Control. Enthält die Sequenznummer der ersten MSDU oder A-MSDU.
- ➍ Die BlockACK-Bitmap besteht aus 8 Bytes also 64 Bits und dient dazu den Status von bis zu 64 **MSDUs** zu signalisieren. Die Bit-Position bezieht sich immer auf das BlockACK-Starting-Sequence-Control-Subfeld + n. Ist das Bit gesetzt wird signalisiert dass die MSDU oder A-MSDU angekommen ist und somit quittiert wird. Ist das Bit auf 0 gesetzt wird signalisiert, dass die MSDU oder A-MSDU nicht angekommen ist.

5.3.4.20.4.2.4. Extended Compressed BlockACK Variante

Das TID-Info-Sub-Feld im BA-Control-Feld enthält den TID, für den der BlockACK-Frame angefordert wurde.

Hier besteht das BA-Information-Feld aus 3 Sub-Feldern:

- BlockAck Starting Sequence Control. Enthält die Sequenznummer der ersten MSDU oder A-MSDU.
- Die BlockACK-Bitmap besteht aus 8 Bytes also 64 Bits und dient dazu den Status von bis zu 64 **MSDUs** zu signalisieren. Die Bit-Position 0 entspricht der Sequenznummer im BlockAck-Starting-Sequence-Control-Feld. Ist das Bit gesetzt wird signalisiert dass die MSDU oder A-MSDU angekommen ist und somit quittiert wird. Ist das Bit auf 0 gesetzt wird signalisiert, dass die MSDU oder A-MSDU nicht angekommen ist.
- Das 1 Byte große RBUFCAP-Feld (Receiver Buffer Capability) enthält die Anzahl der MPDU-Puffer um MPDUs zu speichern.

5.3.4.20.4.2.5. GCR BlockACK Variante

Das TID-Info-Sub-Feld im BA-Control-Feld enthält den TID, für den der BlockACK-Frame angefordert wurde.

Das TID-INFO-Sub-Feld des BAR-Control-Feldes ist auf 0 gesetzt.

Hier besteht das BAR-Information-Feld aus 3 Sub-Feldern:

- Bit 0 bis Bit 15: BlockAck Starting Sequence Control.
 - ◆ Fragment-Nummer (wir hier auf 0 gesetzt)
 - ◆ Sequenznummer (enthält die Start-Sequenznummer der ersten MSDU oder A-MSDU, für die dieser BlockACK-Request gesendet wird)
- Bit 16 bis Bit 63: GCR Group Adresse
- 8 Byte BlockACK Bitmap für die Quittierung von 64 MSDUs oder A-MSDUs.

5.3.4.20.5 - PoE-Stromversorgung

Wegen der limitierten Leistungsübertragung von 12,95W bei IEEE802.3af dürfen bei diesem Standard nur einzügige APs verwendet werden. Sollen Mehrzügige APs über PoE mit Energie versorgt werden muss die Stromversorgung nach IEEE802.3at (PoE+) erfolgen da hier bis zu 25.5 W möglich sind.

Bei den Clients wirkt sich der 802.11n-Standard auch auf den Energieverbrauch und somit auf die Akkulaufzeit aus. Deshalb wurde mit dem 802.11n-Standard eine Power-Save-Funktion eingeführt. Dabei werden bei MIMO-Stationen alle Antennen bis auf eine deaktiviert. Sobald eine an sie adressierte Start-of-Frame-Sequenz von der Station empfangen wird, werden die anderen Antennen wieder aktiviert. Die Start-of-Frame-Sequenz wird dann an einen Zug gesendet sobald er sich im Power-Save-Modus befindet. Hier gibt es eine statische und eine dynamische Variante. Die verwendete Variante wird im SM-Power-Control-Fixed-Feld in Management-Frames übertragen.

Im statischen SM-Power-Save-Modus sendet eine Station dem AP eine Information und deaktiviert bis auf einen Zug alle Züge. Der AP wird, solange ihm keine Änderung mitgeteilt wird, nur auf dem noch aktiven Sende- und Empfangszug Frames übertragen. Die Mitteilung an den AP erfolgt über das SM-Power-Control-Fixed-Feld, das in diesem Fall Bestandteil eines SM-Power-Save-Action-Frame ist.

Im dynamischen SM-Power-Save-Modus deaktiviert eine Station bis auf einen alle Züge. Sobald ein Frame an die Station kommt kann sie kurzfristig in der Lage wieder alle Züge aktivieren. Kommen dann keine Frames mehr, werden die Züge wiederum bis auf einen deaktiviert. APs senden bevor sie einen Frame an eine Station senden ein RTS-Frame. Nachdem die Station alle züge aktiviert hat sendet sie ein CTS-Frame an den AP, der darauf hin seine Züge aktiviert und die Daten sendet.

5.3.4.20.6 - Protection Mechanismus

Ähnlich wie bei der Einführung von 802.11g muss dafür gesorgt werden, dass ältere Geräte die 802.11n nicht verstehen, auch in einem BSS betrieben werden können. Der Protection Mechanismus wird für die Übertragung von HT-PPDUs genutzt, sobald Stationen die nicht mit HT-Signalen umgehen können, vorhanden sind. Dazu dient ein CTS-to-Self-Verfahren und das Dual-CTS-to-Self-Verfahren. In den Beacon-Frames und in den Probe-Response-Frames sind dazu die Felder HT-Protection und Non-Greenfield vorhanden, die die Notwendigkeit für den Protection Mechanismus anzeigen.

5.3.4.20.7 - 20- und 40MHz-Betrieb

Eine BSS, die eine Bandbreite von 40 MHz belegt und durch einen HT-AP verwaltet werden soll ist eine 20/40MHz-BSS.

Der HT-AP zeigt die Bereitschaft an, dass er 40 MHz bereitstellen kann in dem er das Channel-Width-Feld des HT-Capability-Elementes auf einen Wert ungleich 0 setzt. Damit wird lediglich die Bereitschaft des APs signalisiert jedoch nicht, dass er 40 Mhz-Frames nutzt oder bereitstellt.

Für die Nutzung entscheidend ist der Inhalt des Secondary-Channel-Offset-Feldes. Mit dem Wert 3 wird angezeigt, dass der davor liegende Kanal als zweiter Kanal genutzt wird. Ein Wert von 1 zeigt an, dass der darauf folgende Kanal, als zweiter Kanal genutzt wird. Ein Wert von 0 zeigt an, dass nur 20MHz genutzt werden.

Der eigentliche Betriebsmodus des APs wird über ein so genanntes STA-Channel-Width-Feld angezeigt. Ein Wert ungleich 0 zeigt an, dass der AP mit einer Bandbreite von 40MHz arbeitet.

Bevor jedoch eine 20/40MHz-BSS betrieben wird, muss der AP zuvor sicherstellen, dass dies überhaupt möglich ist. Es ist auszuschließen, dass eine bereits vorhandene 20MHz- oder 20/40MHz -BSS beeinflusst wird.

Dazu muss der AP alle Kanäle in einem Overlapping-BSS-Scanning-Prozess abscannen. Der Scan kann entweder durch den AP selbst durchgeführt werden, oder an eine assoziierte Station delegiert werden. Die 40-Mhz-Bandbreite kann nur genutzt werden wenn der Scan eine Beeinflussung einer 20MHz- oder 20/40MHz -BSS ausschließt.

Es ist auch auszuschließen, dass sich die Bedingungen für die Nutzung von 40 MHz-Kanälen im laufenden Betrieb nicht ändern. Dazu kann ein AP, die an ihn assoziierten Stationen, beauftragen, den Status der Umgebung zu überprüfen. Erkennt eine Station, dass der Status sich geändert hat, kann sie mit dem Wert 1 im Forty-MHz-Intolerant-Feldes mitteilen.

Die Umschaltung zwischen dem 20MHz- und 40MHz-Betrieb kann durch die folgenden Ereignisse initiiert werden

- ➊ Es wird ein Beacon-Frame empfangen, der kein HT-Capability-Feld enthält
- ➋ Empfang eines 20/40MHz-Coexistence, Beacon-, Probe-Request- oder Probe-Response-Frame in dem das Forty-Mhz-Intolerant-Feld auf 1 gesetzt ist.
- ➌ 20/40MHz-Coexistence-Management-Frame, bei dem das 20MHz-BSS-Width-Feld auf 1 gesetzt ist.

5.3.4.20.8 - Phased Coexistence Operation (mittlerweile obsolet)

Trotz einem sauber aufgesetzten 40MHz-Betrieb kann es vorkommen, dass 20MHz-Stationen in der BSS koexistieren können, denn optional sieht 802.11n eine so genannten Phased Coexistence Operation (PCO) vor. Ist PCO bei einem AP aktiviert teilt er die Zeit in 20MHz- und 40MHz-Phasen ein, zwischen denen er umschaltet. Die 20MHz-Phase ist für die 802.11a/g-Stationen vorgesehen und die 40MHz-Phase steht für die 802.11n-Stationen zur Verfügung.

802.11a/g-Stationen können entweder im unteren oder oberen Bereich eines 40MHz-Kanals arbeiten, nutzen also wie bisher nur einen 20MHz-breiten Kanal.

Der AP reserviert das Übertragungsmedium für den 40MHz-Betrieb, indem er auf beiden 20MHz-Kanälen eines 40MHz-Kanals einen CTS-to-Self-Frame aussendet. In diesem CTS-to-Self-Frame wird die Zeit, bis zur Rückschaltung in den 20MHz-Betrieb, im Duration-Feld mitgeteilt.

Auf der 40MHz-Ebene wird die Übertragungsphase mit einem CF-End-Frame eingeleitet, das den NAV-Wert der 40MHz-Station zurücksetzt.

Ein Set-PCO-Phase-Frame beendet den 40MHz-Betrieb bei den 40MHz-Stationen. Das Ende der 40MHz-Phase wird bei den 20MHz-Stationen mit einem CF-End-Frame auf jedem 20MHz-Band mitgeteilt.

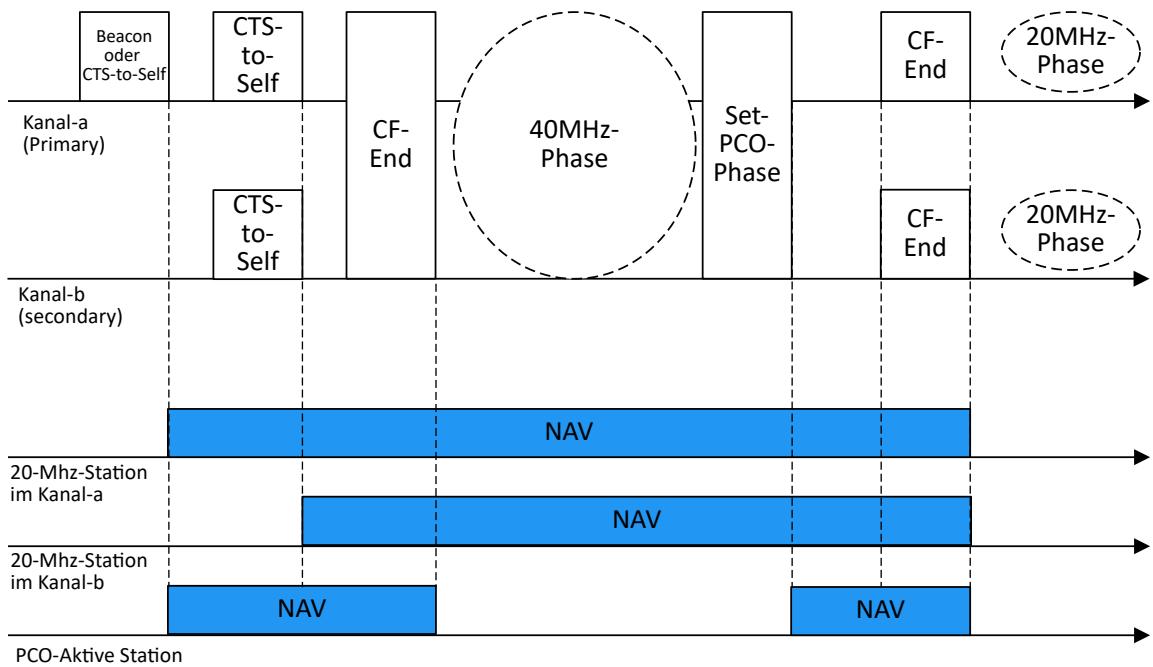


Abbildung 118: Phased Coexistence Betrieb

5.3.4.20.9 - Dual-CTS-to-Self-Verfahren

Sollte ein AP mit einem anderen Übertragungsverfahren arbeiten als eine Station, muss die Station trotzdem mitbekommen, dass sie gerade nicht senden darf. Dazu kann in den Beacon-Frames das Dual-CTS-to-Self-Feld genutzt werden.

Die Station leitet die Übertragung mit einem RTS ein. Der AP antwortet mit zwei CTS-Frames deren Format vom RTS-Frame abhängt.

- Wurde das RTS-Frame im bisherigen Format empfangen, wird das CTS-Frame mit der selben Datenrate (oder MCS), ohne Verwendung von STBC ausgesendet und das zweite CTS-Frame Basis-MCS unter Verwendung von STBC.
- Wurde dagegen das RTS-Frame als STBC-Frame empfangen, wird das CTS-Frame mit der Basis-MCS, unter Verwendung von STBC ausgesendet. Das zweite CTS-Frame mit geringster Basis-Service-Rate ohne Verwendung von STBC.

Alle CTS-Frames adressiert der AP an sich selbst. Darin ist das Duration-Feld auf den Wert gesetzt, der der Dauer der Übertragung entspricht. Damit können die Stationen den NAV-Wert setzen.

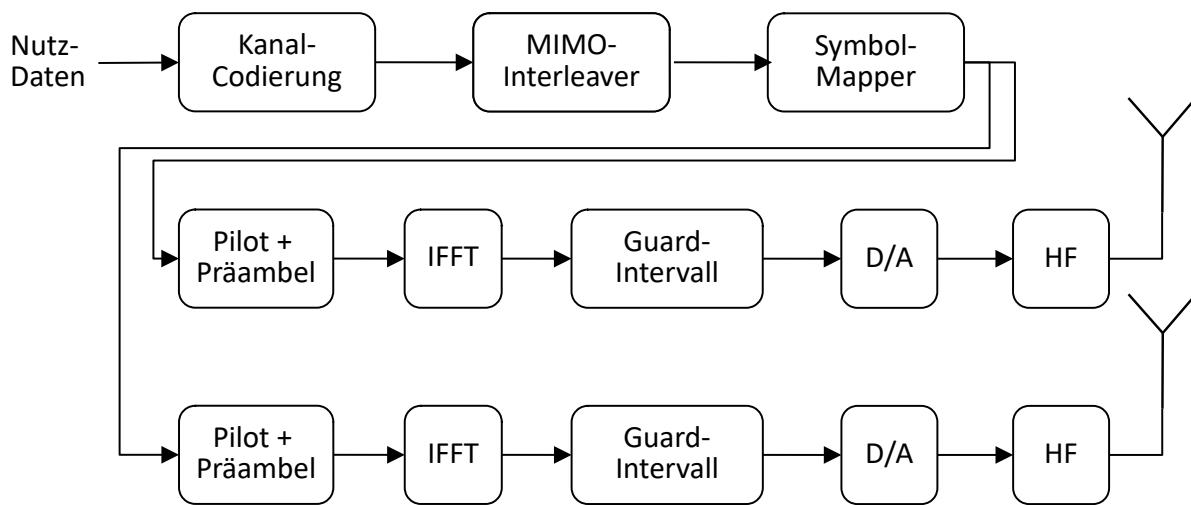


Abbildung 119: MIMO-Blockschaltbild

In Abbildung 119 ist das Blockschaltbild für 2 Antennen dargestellt. Nach dem Symbolmapper wird, für jede Antenne getrennt, die Bearbeitung durchlaufen, wie sie bereits bei den OFDM-Systemen abgehandelt wurden.

5.3.5 - IEEE-802.11ac

5.3.5.1 - Eigenschaften

Name: Wi-Fi 5

Frequenzband: 5 GHz

Anzahl der Kanäle: 16 (5GHz 20 MHz) / 7 (5GHz 40 MHz) / 3 (5GHz 80 MHz) / 1 (5GHz 160 MHz)

Kanalbreite: 20 MHz, 40 MHz, 80 MHz, 160 MHz (5GHz)

Multiplex-Verfahren: Orthogonal Frequency Division Multiplexing (OFDM)

Modulation: Max. 256-QAM

MIMO-Streams: 1 bis 8

Maximale Reichweite 50m

Maximale Brutto-Datenrate: 3,5 Gbps

Typische Netto-Datenrate: 0,24 – 1,1 Gbps

5.3.5.2 - Neuerungen

Seit 2008 arbeitete die TGac (Task Group ac bei IEEE). Der Standard wurde in 2 Waves verabschiedet. Die Unterschiede ergaben sich durch die Verfügbarkeit der Funktionen in den Chipsätzen auf dem Markt. Am 18.12.2013 wurde die erste Wave verabschiedet. Ende 2015 folgte die zweite Wave.

Um die nochmals erhöhten Datenübertragungsraten auszuweisen, wird bei den Begriffen VHT vorangestellt. VHT steht dabei für Very High Throughput. Deshalb wird eine Funkzelle mit 802.11ac-Unterstützung VHT-BSS genannt.

Um den Problemen im 2,4GHz-Band auszuweichen, arbeitet dieser Standard nur im 5GHz-Band. Damit galt der IEEE-802.11n-Standard weiterhin für den 2,4GHz-Bereich.

Im Prinzip wurden die bereits bei IEEE-802.11n eingeführten Verfahren konsequent weiter entwickelt.

- ➊ 2 neue MCS (Modulation and Coding Scheme) wurden eingeführt und mit dem Modulationsverfahren 256-QAM sowie Coderraten von 3 / 4 und 5 / 6 umgesetzt.
- ➋ Erhöhung der Kanalbandbreite (20 MHz*2-> 40Mhz, 20 MHz*4-> 80Mhz, 20 Mhz*8->160Mhz). Dazu benötigt es entsprechende Maßnahmen zur gleichzeitigen Koexistenz unterschiedlicher Bandbreiten.
- ➌ Erhöhung der Anzahl der Antennen und damit der Spatial Streams von maximal 4 auf bis zu 8.
- ➍ Multi User MIMO (MU-MIMO) Hier werden die bis zu 8 Spatial Streams auf unterschiedlichen Verbindungen aufgeteilt. (z. B. 2*4 Antennen für 2 unterschiedliche Verbindungen) Dies ist effizienter als die Verbindungen nacheinander zu bedienen, da die Wartezeiten zwischen den Paketen gespart werden können. Einschränkende Bedingung: Die Pakete der unterschiedlichen Verbindungen müssen gleich lang sein.

Tabelle 41: Parameter der 802.11ac-Waves (Quelle: Heise/IX 10/2015)

IEEE-802.11ac	Wave 1	Wave 2	Maximal
Kanalbreiten	20, 40, 80	20, 40, 80, 80 + 80, 160	20, 40, 80, 80 + 80, 160
Anzahl Streams	3	3 - 4	8
Mimo	SU	MU	MU
Max. Durchsatz	1,3Gbps	2,34 – 3,47 Gbps	6,9Gbps

In der folgenden Abbildung sind die Evolutionsstufen der WLAN-Bandbreiten dargestellt.

Mit IEEE-802.11n waren bereits Bandbreiten von 40 MHz eingeführt worden (blau).

Das gilt sowohl für den 2,4GHz-Bereich als auch für den 5MHz-Bereich (grün).

Im 5MHz-Bereich muss eine Kollision mit dem Wetterradar und Flugzeugen vermieden werden.

Mit dem IEEE-802.11ac-Standard wurden die Bandbreiten auf 80MHz, 80 + 80 MHz und 160MHz ausgeweitet.

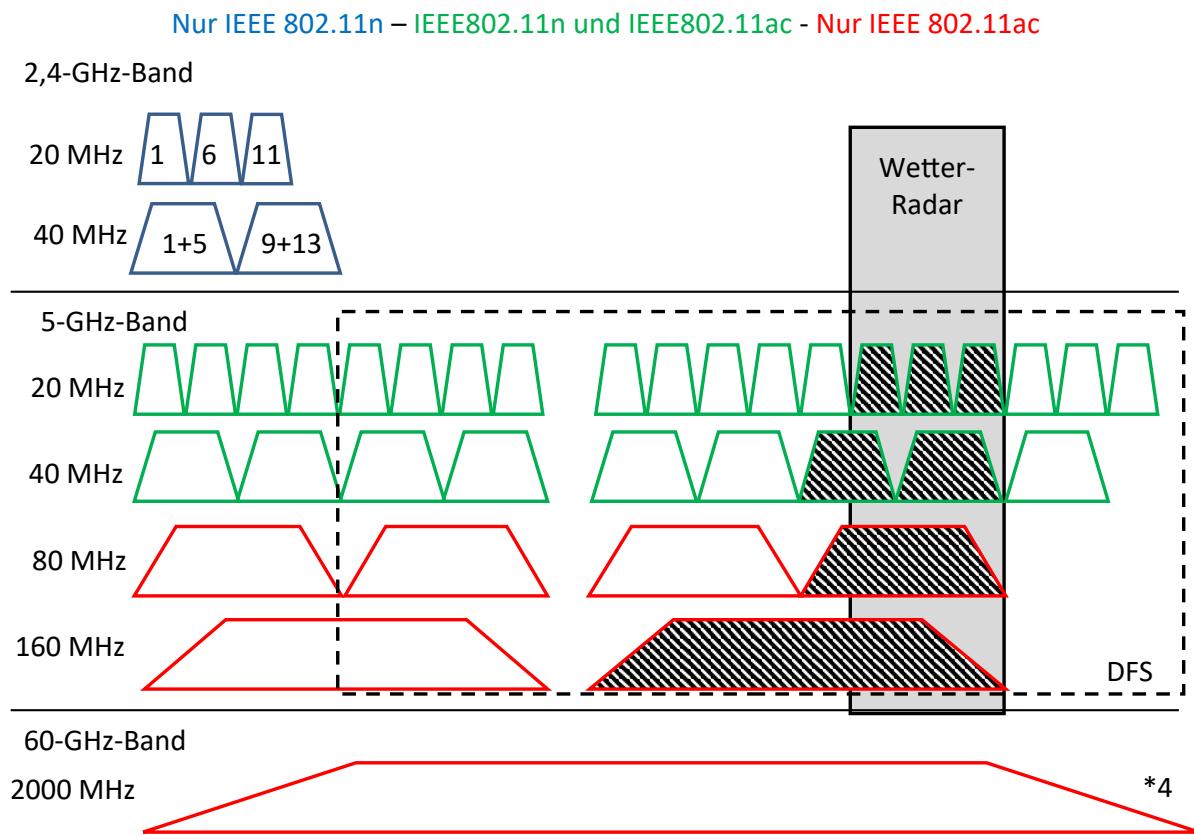


Abbildung 120: WLAN-Bandbreiten

Im 5GHz-Brech gibt es 3 zusammenhängende Bereiche von denen der untere für den Indoor-Bereich gedacht ist. Deshalb ist dort die DFS (Dynamic Frequency Selection) nicht erforderlich. Im Außenbereich muss DFS angewendet werden, da es dort passieren kann, dass die Primäruser unterwegs sind.

5.3.5.3 - 802.11ac-Beamforming

Für das Beamforming muss der Sender Kenntnisse über den Kanal-Status haben, um die Steuerungsmatrix für die Verbindungen zu den assoziierten Stationen aufbauen zu können.

Beim 802.11n-Standard, wurde das noch optionale Beamforming, mit dem Single Sounding also 1:1 abgehandelt. D. h. Es wurden regelmäßig Beamforming-Frames an die Stationen ausgesendet, die von den einzelnen Stationen mit Beamforming-Response-Frames beantwortet wurden. Mit dem 802.11ac-Standard wurde das Multi-Sounding und Feedback Beamforming eingeführt. (VHT-Sounding Protocol) Dabei werden die Beamforming Informationen mit mehreren Stationen ausgetauscht, um das auszusendende Signal weiter zu optimieren. Dies war durch die Einführung von Multi-User-MIMO (MU-MIMO) erforderlich geworden.

Für die Erstellung der Steuerungsmatrix wird mit einem VHT NDP (Null-Data-Packet) Announcement eine Sounding-Feedback-Sequenz initiiert. Innerhalb dieses Frames sind alle Stationen aufgelistet mit denen die Steuerungsmatrix abgeglichen werden soll. Von diesen Stationen erwartet der Sender, dass sie einen VHT-Compressed-Beamforming-Response-Frame vorbereiten.

Nach Ablauf eines SIFS und dem Senden eines NDP antwortet die erste Station mit ihrem VHT-Compressed-Beamforming-Response-Frame.

Nach einem weiteren SIFS wird im folgenden Beamforming-Report-Poll-Frame die nächste Station aufgefordert zu antworten, was sie dann auch tut. Dies wird so lange wiederholt, bis alle Stationen abgearbeitet sind.

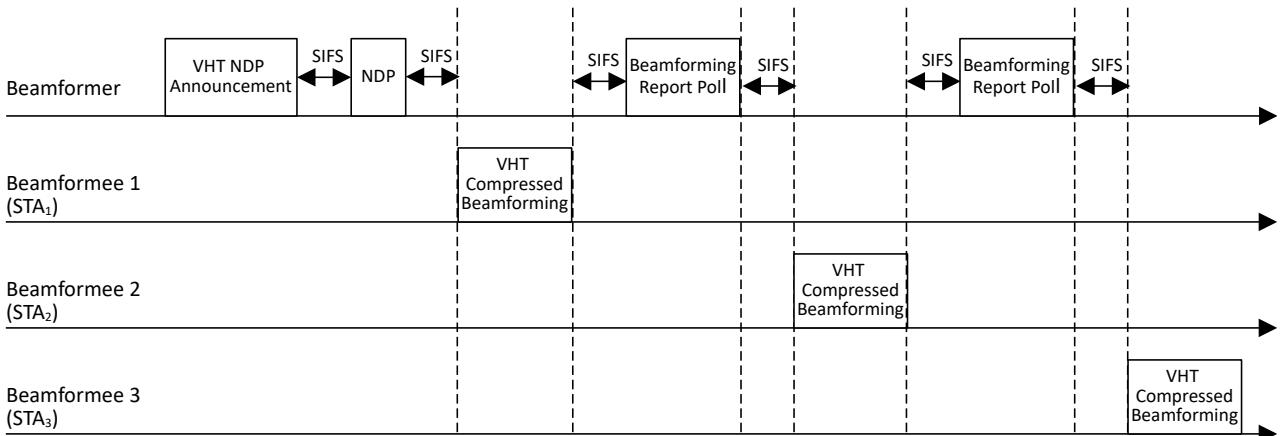


Abbildung 121: Sounding-Feedback-Sequenz mit mehreren Stationen

5.3.5.4 - Multi-User-MIMO

Besonders für Multimedia-Anwendungen interessant ist das Multi-User-MIMO. Dabei wird mit einer oder mehreren Antennen gleichzeitig Daten senden und empfangen können. Die Trennung der Daten erfolgt mit einer Raum-Zeit-Codierung (Space Time Block Coding = STBC). Optional ist ein Downstream-MU-MIMO vorgesehen bei dem eine Instanz zeitgleich an mehrere Stationen Daten aussendet.

5.3.5.5 - Kanalbündelung

Die Erhöhung der Datenraten beruht größtenteils auf der Bündelung mehrerer Kanäle mit der resultierenden Erhöhung der Anzahl der Unterträger. Diese Kanäle müssen nebeneinander liegen. Somit können die Pilot-Kanäle in ihrer Anzahl reduziert werden was bei einer Verdopplung der Bandbreite zu mehr als der doppelten Datenübertragungsrate führt, weil weniger Pilot-Kanäle erforderlich sind. Ein großer Vorteil des 5 GHz-Bandes ist, dass bis zu 19 überlappungsfreie Kanäle zur Verfügung stehen. Werden jedoch bis zu 8 20-MHz-Kanäle gebündelt und die VHT-BSS mit vielen Stationen besiedelt, sind die Grenzen wiederum schnell sichtbar. Bei der Bildung eines 160-Mhz-breiten Kanals sieht der 802.11ac-Standard deshalb 2 Lösungen vor.

Tabelle 42: Nutzung der Kanalbandbreite

Bandbreite [MHz]	Unterträger	Pilotträger	Träger für Centerfrequenz	Verbleibende Unterträger für Daten
20	57	4	1	52
40	115	6	1	108
80	243	8	1	234
80 + 80	243 + 243	8 + 8	1 + 1	234 + 234
160	485	16	1	468

Für die Betrachtung der Frequenzbereiche erfolgt die Verwaltung in Kanallisten. Das Element Primär beschreibt, dass die primären 20MHz belegt sind. Das Element Sekundär beschreibt, dass die sekundären 20MHz belegt sind. Das Element Sekundär 40 weist darauf hin, dass mindestens ein 20MHz-Bereich im sekundären 40MHz-Bereich genutzt wird. Das Element Sekundär 80 weist darauf hin, dass mindestens ein 20MHz-Bereich im sekundären

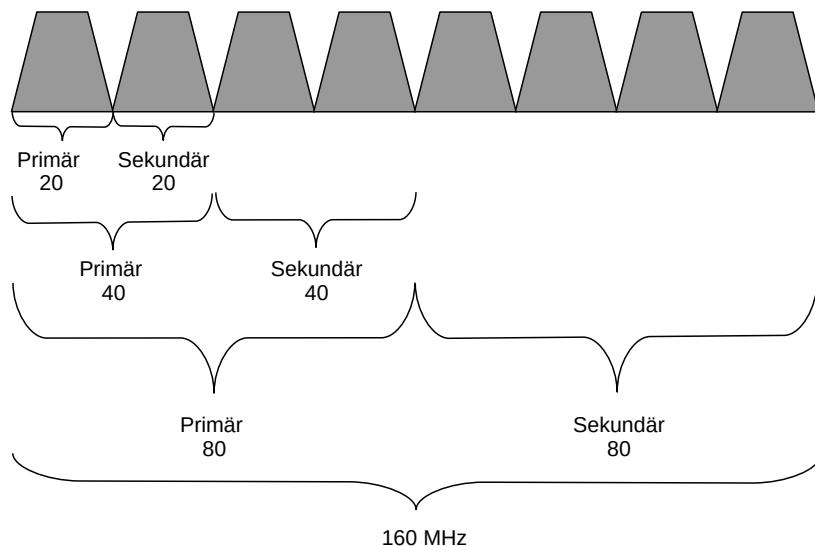


Abbildung 122: Zusammenhang Kanallistenelement und Frequenzband
80MHz-Bereich belegt ist.

Für den Medienzugriff prüft eine Station immer die Kanalliste. Ist diese leer kann sie von einem freien Übertragungsmedium ausgehen. Ansonsten werden über die Kanallisten die belegten Bereiche angezeigt.

Die NAV-Werte werden über das Duration-Feld/ID-Feld aktualisiert, das in der PPDU enthalten ist, die von einer Station auf dem Primären Kanal empfangen wurde. Dies entspricht beispielsweise bei einer 20MHz-PPDU dem primären 20MHz-Kanal und bei einer 80MHz-PPDU dem primären 80MHz-Kanal.

5.3.5.6 - CCA-Empfindlichkeit

Ein Kanal gilt als belegt wenn auf einem primären 20-Mhz-Kanal ein Signal mit der Mindestgröße von -62 dBm anliegt. Weiterhin gilt, wenn eine Nicht-HT-PPDU oder Nicht-VHT-PPDU mit der Signalstärke von -83 dBm oder mehr anliegt. Bei 40MHz gilt für diesen Wert -79 dBm, bei 80MHz gilt -76 dBm und bei 160MHz gilt -73 dBm.

5.3.5.7 - Empfängerempfindlichkeit

Die Empfängerempfindlichkeit ist von der verwendeten Modulationsart, der Coderate und der Kanalbreite abhängig. Voraussetzung ist eine Packet Error Rate (PER) von weniger als 10% bei einer PSDU-Länge von 4096 Bytes.

Tabelle 43: Mindest-Empfängerempfindlichkeit bei 802.11ac

MCS	Modulations-Verfahren	Code-Rate	Empfängerempfindlichkeit bei 20MHZ Kanalbandbreite [dBm]	Empfängerempfindlichkeit bei 40MHZ Kanalbandbreite [dBm]	Empfängerempfindlichkeit bei 80MHZ Kanalbandbreite [dBm]	Empfängerempfindlichkeit bei 160MHZ Kanalbandbreite [dBm]
0	BPSK	1/2	-82	-79	-76	-73
1	QPSK	1/2	-79	-76	-73	-70
2	QPSK	3/4	-77	-74	-71	-68
3	16-QAM	1/2	-74	-71	-68	-65
4	16-QAM	3/4	-70	-67	-64	-61
5	64-QAM	2/3	-66	-63	-60	-57
6	64-QAM	3/4	-65	-62	-59	-56
7	64-QAM	5/6	-64	-61	-58	-55
8	256-QAM	3/4	-59	-56	-53	-50
9	256-QAM	5/6	-57	-54	-51	-48

Bei 802.11ac gibt es 32 MCS-Tabellen mit unterschiedlichen Parametern.

Tabelle 44: Unterschiede der Brutto-Datenraten bei einem Sende- und Empfangszug

MCS	Modulation	Code-Rate	Datenrate bei 20Mhz	Datenrate bei 40Mhz	Datenrate bei 80Mhz	Datenrate bei 160Mhz
0	BPSK	1/2	7,2	15,0	32,5	65,0
1	QPSK	1/2	14,4	30,0	65,0	130,0
2	QPSK	3/4	21,7	45,0	97,5	195,0
3	16-QAM	1/2	28,9	60,0	130,0	260,0
4	16-QAM	3/4	43,3	90,0	195,0	390,0
5	64-QAM	2/3	57,8	120,0	260,0	520,0
6	64-QAM	3/4	65,0	135,0	292,0	585,0
7	64-QAM	5/6	72,2	150,0	325,0	650,0
8	256-QAM	3/4	86,7	180,0	390,0	780,0
9	256-QAM	5/6	-	200,0	433,3	866,7

Um von z. B. 72 Mbps (64-QAM, Coderate 5/6, und 20 Mhz Kanalbandbreite) auf 867Mbps (256-QAM, Coderate 5/6, und 160 Mhz Kanalbandbreite) zu kommen ist die Grenze des 10%igen Paketverlusts von -64dBm auf -48dBm zu erhöhen. Dies entspricht einer Erhöhung von 0,4 auf 16 Nanowatt.

Da die Regulierungsbehörde (in Deutschland die Bundesnetzagentur) eine Erhöhung der Sendeleistung nicht erlaubt, kann nur noch die Reichweite reduziert werden. Damit ist zur Ausleuchtung der gleichen Fläche mit etwa der doppelten Anzahl von Accesspoints zu rechnen.

5.3.5.8 - VHT-PPDU-Format

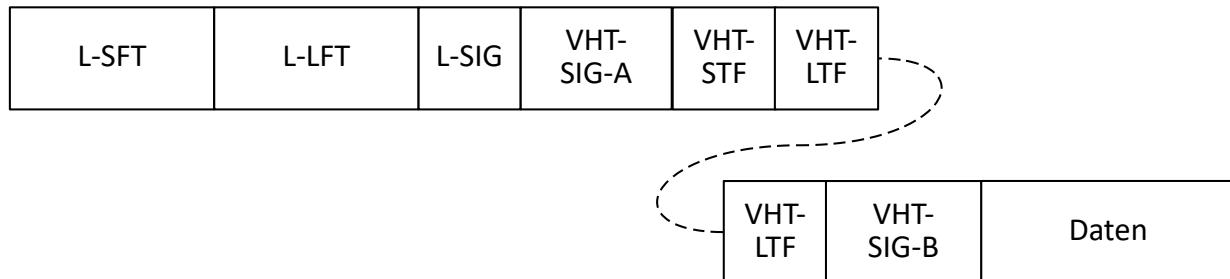


Abbildung 123: VHT-PPDU-Format

Das VHT-PPDU-Format ähnelt dem HT-PPDU-Format im Mixed Mode.

Eingeleitet wird das Frame mit den OFDM-Frame-Bestandteilen:

- L-SFT
- L-LFT
- L-SIG

Im Anschluss folgt das:

- VHT-SIG-A-Feld

gefolgt von den Trainingssequenzen

- VHT-STF
- VHT-LTF

als nächstes folgt das:

- VHT-SIG-B-Feld

Als letztes werden die:

- Daten

angehängt.

Das VHT-SIG-A-Feld hat im Detail die folgenden 24 Bits:

- Bit 0 und Bit 1 Bandwidth-Bits (00 = 20MHz, 01 = 40MHz, 10 = 80MHz, 11 = 160MHz oder 80MHz + 80MHz)
- Bit 2 ist reserviert und auf 1 gesetzt
- Bit 3 entspricht dem STPC-Bit. (1 = alle Signale basieren auf einer Raum-Zeit-Block-Codierung)
- Bit 4 bis Bit 9 Group-ID. Gibt an, für welche Gruppe der Frame bestimmt ist oder ob es sich um einen Broadcast-Frame handelt
- Bit 10 bis Bit 21 N_{sys} Anzahl der genutzten sende- und Empfangszüge und ob es sich um einen Single-User- oder Multi-User-Frame handelt.
- Bit 22 Power-Save-Modus (0 = nicht zugelassen, 1 = Zugelassen)
- Bit 23 ist reserviert und auf 1 gesetzt

Das VHT-SIG-B-Feld hat im Detail die folgenden 24 Bits:

- Bit 0 und Bit 1 Benutzung eines Short Guard-Intervalls
- Bit 2 und Bit 3 Codierung (Bit 2: 0 = BBC, 1 = LDPC / Bit 3: 1 = Bei LDPC falls mindestens eine empfängerbezogene PPDU in einem extra OFDM-Symbol mündet. Es ergibt sich, wenn sendeseitig die Anzahl der Datenbits nicht dem Vielfachen des OFDM-Symbols entspricht. Dann müssen bis zu 7 Füllbits den Datenbits hinzugefügt werden.)
- Bit 4 bis Bit 7 MCS-Index
- Bit 8 Art des Beamforming. 1 = Beamforming zu einer station, Andernfalls = 0)
- Bit 9 ist reserviert und auf 1 gesetzt
- Bit 10 bis Bit 17 CRC
- Bit 18 bis Bit 23 Tailbits. Werden für die Initialisierung des Faltungscodierers verwendet.

5.3.6 - IEEE-802.11ad

Eigenschaften

Frequenzband: 60 GHz

Anzahl der Kanäle: ?

Kanalbreite: 2160MHz

Multiplex-Verfahren: ?

Modulation: ?

Maximale Brutto-Datenrate: 6,75675GBit/s

Parallel zum IEEE-802.11ac gibt es eine TGad (Task Group ad bei IEEE), die WLANs bei 60 GHz ermöglichen soll. Dort muss man sich nicht mit anderen Nutzern beschäftigen und die Bandbreite bei 5 Millimeter Wellenlänge ist enorm. Der Standard wurde am 28.12.2012 veröffentlicht.

IEEE-802.11ad arbeitet mit einem 2160MHz breiten Funkkanal. Dass der atmosphärische Sauerstoff bei 60 GHz, zusätzlich zur regulären Dämpfung mit 20 db pro km dämpft, führt dazu, dass sich dieser Standard nur in geschlossenen Räumen, jedoch nicht darüber hinaus verwenden lässt. Mehr als 10m bis 20m sind bei Sichtverbindung nicht möglich. Deshalb war der Standard konzipiert worden um Geräte mit hohen Anforderungen an die Datenübertragungsrate über kurze Distanzen anzubinden. Damit sind z. B. Bildschirme oder Beamer in Konferenzräumen die klassischen Kandidaten für diesen Standard.

Es wird auf MIMO verzichtet, allerdings kommt Beamforming zum Einsatz.

5.3.7 - IEEE-802.11af

Eigenschaften

Frequenzband: 54MHz - 790MHz

Anzahl der Kanäle: 4

Kanalbreite: 6 / 7 / 8 MHz

Multiplex-Verfahren:

Modulation: Orthogonal Frequency Division Multiplexing (OFDM)

Maximale Brutto-Datenrate: 35,6 Mbps

Dieser Standard wurde im Februar 2014 verabschiedet und ist für die so genannten TV-Whitespaces gedacht und funktioniert im Sub-800 MHz-Bereich. Der Standard agiert somit im Bereich UHF- und VHF-Bereich zwischen 54MHz und 790MHz und basiert auf dem OFDM (Orthogonal Frequency Division Multiplexing). Es können bis zu 4 Kanäle zu einem oder 2 zusammenhängenden Blöcken gebündelt werden.

MIMO kann entweder für STBC (Space Time Block Code) oder MU-MIMO (Multi-User MIMO) genutzt werden.

Die erreichbare Datenrate pro Spatial Stream ist 26,7 Mbps bei Verwendung von 6/7MHz breiten Kanälen. Bei Verwendung von 8 MHz breiten Kanälen sind bis zu 35,6 Mbps möglich.

Tabelle 45: Theoretischer Durchsatz für einen Spatial Stream [Mbps]

MCS-Index	Modulationstyp	Coding Rate	6 / 7 MHz Channel		8 MHz Channel	
			6 µs GI	3µs GI	4,5 µs GI	2,25 µs GI
0	BPSK	1/2	1,8	2,0	2,4	2,7
1	QPSK	1/2	3,6	4,0	4,8	5,3
2	QPSK	3/4	5,4	6,0	7,2	8,0
3	16-QAM	1/2	7,2	8,0	9,6	10,7
4	16-QAM	3/4	10,8	12,0	14,4	16,0
5	64-QAM	2/3	14,4	16,0	19,2	21,3
6	64-QAM	3/4	16,2	18,0	21,6	24,0
7	64-QAM	5/6	18,0	20,0	24,0	26,7
8	256-QAM	3/4	21,6	24,0	28,8	32,0
9	256-QAM	5/6	24,0	26,7	32,0	35,6

5.3.8 - IEEE-802.11ah

Eigenschaften

Frequenzband: unter 990MHz

Anzahl der Kanäle: Je nach Region bis zu 32MHz (siehe Tabelle unten)

Kanalbreite: Je nach Region bis zu 16MHz (siehe Tabelle unten)

Multiplex-Verfahren: OFDM

Modulation: 256-QAM

Maximale Brutto-Datenrate: 8,67MBit/s

Im Zuge des IoT (Internet of Things) nutzen immer mehr Geräte WLAN-Verbindungswege. Allerdings sind die bisher verfügbaren WLAN-Standards nicht unbedingt für Geräte aus diesem Umfeld geeignet. So ist zum Beispiel die Anzahl, der mobilen Geräte pro Zelle, eher klein.

Deshalb wurde im Januar 2016 von der Wi-Fi-Alliance die Zertifizierung von Wi-Fi-HaLow angekündigt. Im Englischen klingt HaLow wie halo (dt. Heiligschein Strahlenkranz) was eher auf Marketingaktivitäten hinweist als auf die gemeinten Eigenschaften wie niedriger Stromverbrauch und niedrige Sende-Frequenz. (unter 900MHz).

Durch die Wahl des Frequenzbereichs ist eine große Ausbreitungsfläche möglich und wenn man jetzt noch Geräte mit geringem Bandbreitenbedarf (wie bei vielen IoT-Geräte) verwendet wird ersichtlich für welchen Anwendungsbereich dieser Standard gedacht ist.

Viele Teile Eigenschaften wurden vom IEEE-802.11ac übernommen. Es werden Reichweiten von bis zu 1km und über 8191 Endgeräte in einer hierarchischen Struktur pro Access Point (AP) versprochen. Für den niedrigen Energieverbrauch sorgt ein Power-Saving-Mode, der auch dazu führen kann, dass sich Geräte ganz abschalten.

Ein Nachteil des Standards ist, dass er auf unterschiedlichen Gebieten unterschiedliche Frequenzbereiche und unterschiedliche Sendeleistungen vorsieht. Dies steht einer globalen Einführung des Standards entgegen.

Tabelle 46: Vergleich der Funkpartner (IEEE-802.11ah)

Gebiet	Europa	USA	China	Korea	Japan
Frequenzband	863 – 868,6MHz	902 – 928MHz	755 – 787MHz	917 -923,5MHz	915,9 – 928,1MHz
Kanalbreite					
1MHz	5	26	32	6	11
2MHz	2	13	4	3	-
4MHz	-	6	2	1	-
8MHz	-	3	1	-	-
16MHz	-	1	-	-	-
Max. Sendeleistung (EIRP)	25mW	1W	5mW 10mW	3mW 10mW	1mW 20mW 250mW +3db Antennengewinn

Wie aus der obigen Tabelle ersichtlich ist gibt es Kanalbreiten von 1, 2, 4, 8 und 16MHz.

In Europa werden wahrscheinlich nur die 1MHz-breiten Kanäle genutzt, da sonst zwei Kanäle nutzbar wären, was den Verwendungsabstand sehr einschränkt. Im ETSI-Vorschlag TR 103 245 werden weitere Kanäle vorgeschlagen.

5.3.9 - IEEE-802.11ax

Eigenschaften

Name: Wi-Fi 6

Frequenzband: 2,4 GHz und 5GHz

Anzahl der Kanäle: 3 (2,4GHz) / 16 (5GHz 20 MHz) / 7 (5GHz 40 MHz) / 3 (5GHz 80 MHz) / 1 (5GHz 160 MHz)

Kanalbreite: 20, 40, 80, 160MHz

Multiplex-Verfahren: OFDMA

Modulation: Max. QAM1024

MIMO-Streams: 1 bis 8

Maximale Brutto-Datenrate: 9,6 Gbps

Typische Netto-Datenrate: 0,3 – 1,6 Gbps

Während die vorhergehenden Standards damit beschäftigt waren die Datenrate immer weiter in die Höhe zu treiben, bestand der Flaschenhals aus den Anfangstagen namens CSMA/CA als Medien-Zugriffsverfahren weiterhin. Die Distributed Coordination Function (DCF) funktioniert mit CSMA/CA als Zugriffsverfahren recht gut hat unter anderem jedoch den Nachteil bei vielen Teilnehmern in einer BSS zu schwächeln.

Im Hinblick darauf wurde unter dem Namen High Efficiency Wireless (HEW) nächste Standard entwickelt, was schon einen Hinweis auf den Schwerpunkt gibt. Den Parametern des Standards wird deshalb auch HE (High Efficiency) vorangestellt. Er wurde 2019 unter dem Namen IEEE-802.11ax (Wi-Fi-6) freigegeben.

Dabei wird die Datenrate zwar wiederum weiter entwickelt, jedoch liegt das Hauptaugenmerk darauf, möglichst vielen Stationen, eine Datenübertragung zu ermöglichen. 802.11ax hat das konstruktive Ziel, den mittleren Durchsatz pro Benutzer in dichten Umgebungen um den Faktor 4 zu erhöhen. Damit soll es z. B. in Stadien, Flughafenterminals und Zügen einen vernünftigen WLAN-Betrieb ermöglichen.

Dazu wurden diverse Verbesserungen eingeführt.

5.3.9.1 - Betriebsmodi für die Versorgung mehrerer User

Für den Multiuserbetrieb wurden unterschiedliche Modi spezifiziert.

- ➊ Single User Modus

Das wurde bereits mit DCF eingeführt. Die Stationen senden sequentiell nacheinander, sobald der Kanal frei ist.

- ➋ Multi-User-Modus

Damit ist der simultane Betrieb von Teilnehmer-Stationen gemeint, die nicht APs sind. Der Standard unterteilt hier noch in einen Uplink und einen Downlink.

- ➌ Multi-User-Downlink

Hier sind die Daten gemeint, die vom AP gleichzeitig an die Stationen gesendet werden.

- ➌ Multi-User-Uplink

Hierbei sind die Daten gemeint, die von mehreren Stationen gleichzeitig an einen AP gesendet werden. Der AP verwaltet die Verbindungen und triggert die simultane Übertragung der Daten an den AP.

Im Rahmen der Multiuser-Modi gibt es zwei Möglichkeiten der Abarbeitung. Multi-User-MIMO und OFDMA.

Bei beiden Verfahren steuert der AP zentral die Abläufe, ähnlich wie bei LTE, wo den Teilnehmern die RUs zugewiesen werden.

Wie bei IEEE-802.11ac kann durch Beamforming mit räumlich getrennten Stationen unterschiedliche Verbindungen aufgebaut werden. Näheres siehe Kapitel: Beamforming.

Bei OFDMA werden mit Triggerframes vom AP die Stationen aufgefordert ihre Daten an den AP zu senden. Der Quittiert den Empfang aller empfangenen Daten mit einer Quittung. Näheres siehe Kapitel OFDMA.

5.3.9.2 - OFDMA

Bei der Modulation ging man von OFDM auf OFDMA über.

Dabei wurde der Abstand der Unterträger (Subcarrier) von 312,5kHz auf 78,125kHz reduziert, was ein weiteres Zusammenschieben der Unterträger bedeutet. Damit mehr Unterträger in einem Frequenzband untergebracht werden.

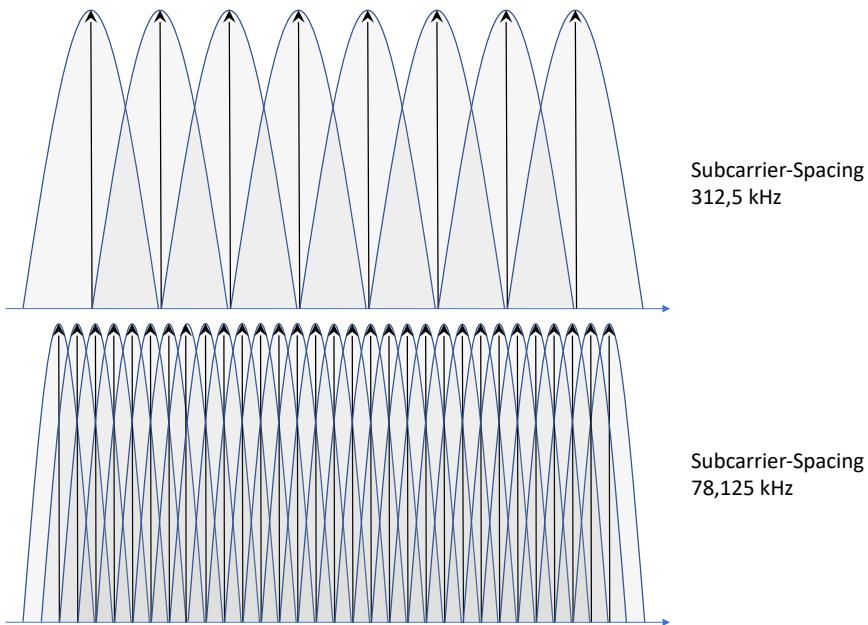


Abbildung 124: Subcarrier-Spacing

Bei den Vorgängern wurde OFDM zusammen mit Zeitmultiplex angewendet. D. h. es sendet immer nur eine Station. Bei OFDMA werden nicht wie bei OFDM alle Unterträger eines Bandes für ein WLAN-Paket zur Verfügung gestellt, sondern eine Menge von Resource-Units (RU). Damit haben einzelne User ein schmaleres Band zur Verfügung. Dafür können jedoch gleichzeitig mehrere User in einem Zeitslot übertragen werden, was den Durchsatz pro User deutlich erhöht. Dies gilt für den Uplink (UL) und den Downlink (DL).

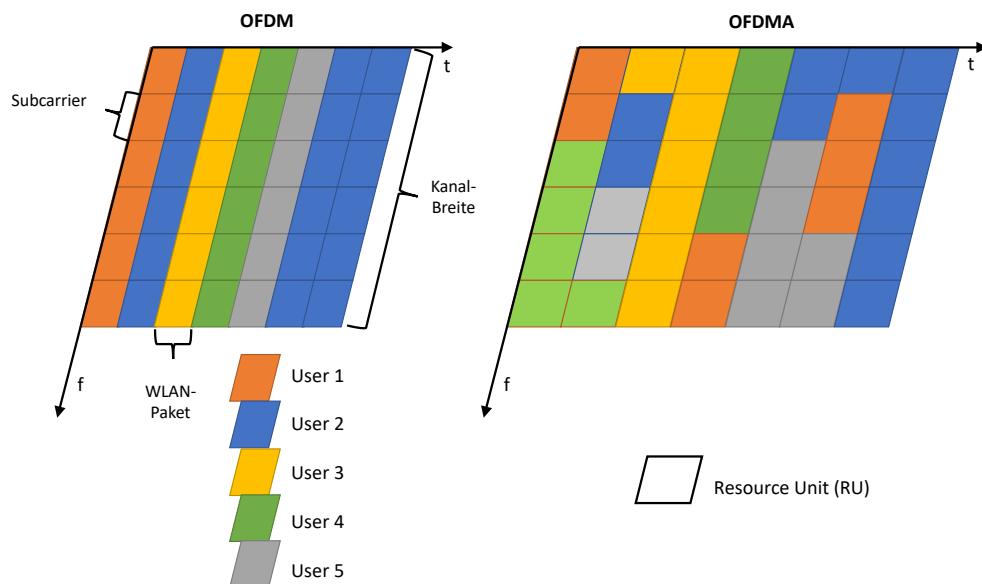


Abbildung 125: Unterschied OFDM / OFDMA

Durch das gleichzeitige Senden der Daten an mehrere Stationen reduziert sich die Anzahl der Präambeln und der Wartezeiten, was den Durchsatz erheblich steigert. Dies gilt vor allem bei kurzen Datenframes.

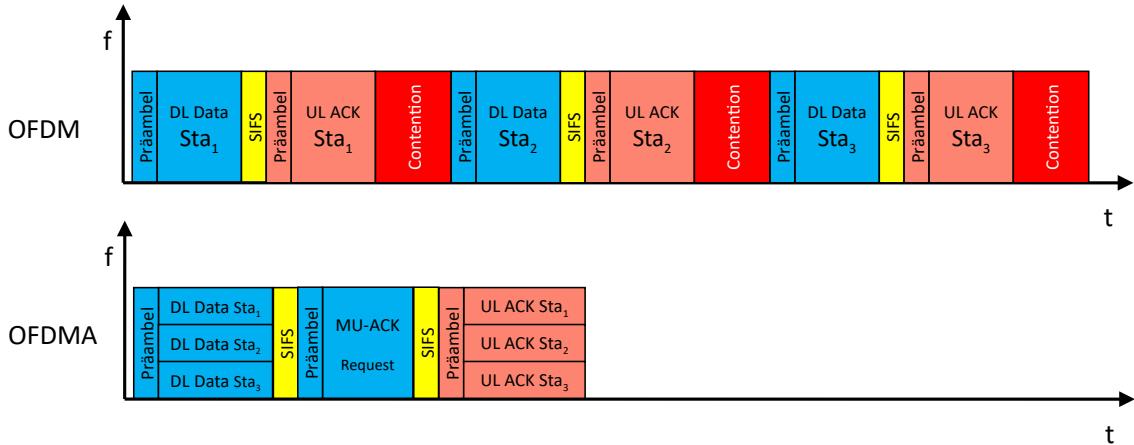


Abbildung 126: Reduzierung der Präambeln

Die Mechanismen für den Uplink und den Downlink müssen voneinander unterschieden werden. Dazu wurde die Distributed Coordination Funktion (DCF) erweitert. Hierbei greift der AP als koordinierende Instanz in das verteilte Medien-Zugriffsverfahren ein. Dazu wurden die Control-Frames neu definiert.

Das Senden der APs an mehrere Stationen wird mit einem Multi-User-RTS/CTS (MU-RTS / MU-CTS) koordiniert.

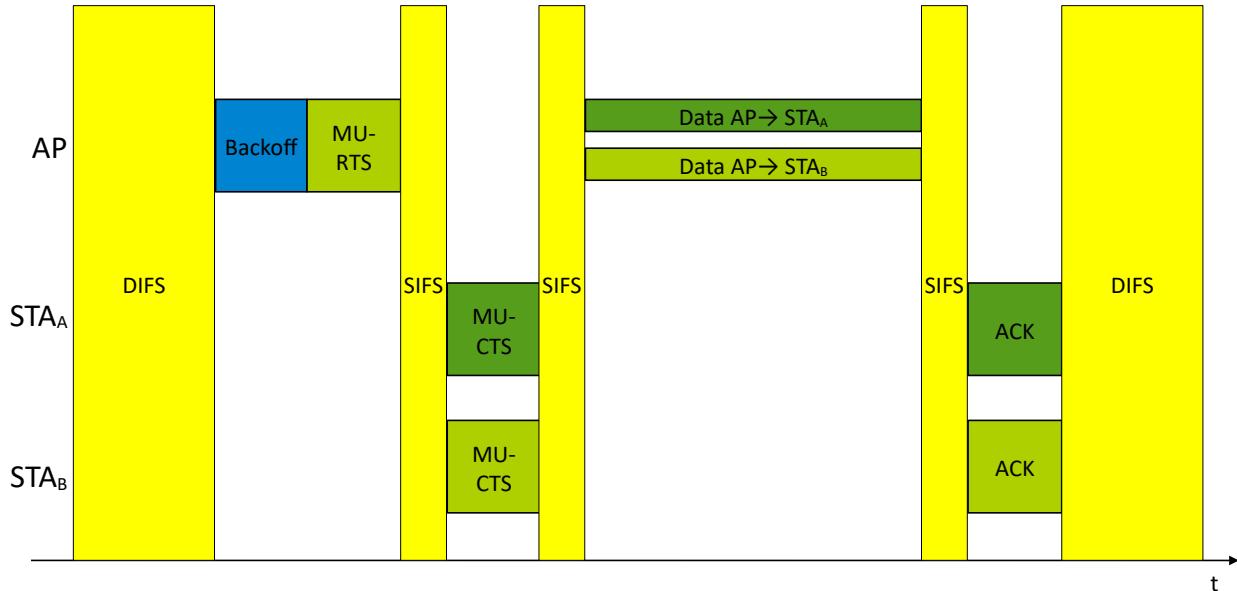


Abbildung 127: MU-Downlink

Das gleichzeitige Senden von Stationen an den AP wird mit Trigger-Frames durch den AP koordiniert. Der AP sendet an alle ax-Stationen einen Buffer Status Report Poll (BSRP). Die Clients antworten mit einem Buffer Status Report (BSR). Darin ist enthalten, ob und wie viele Daten sie senden wollen.

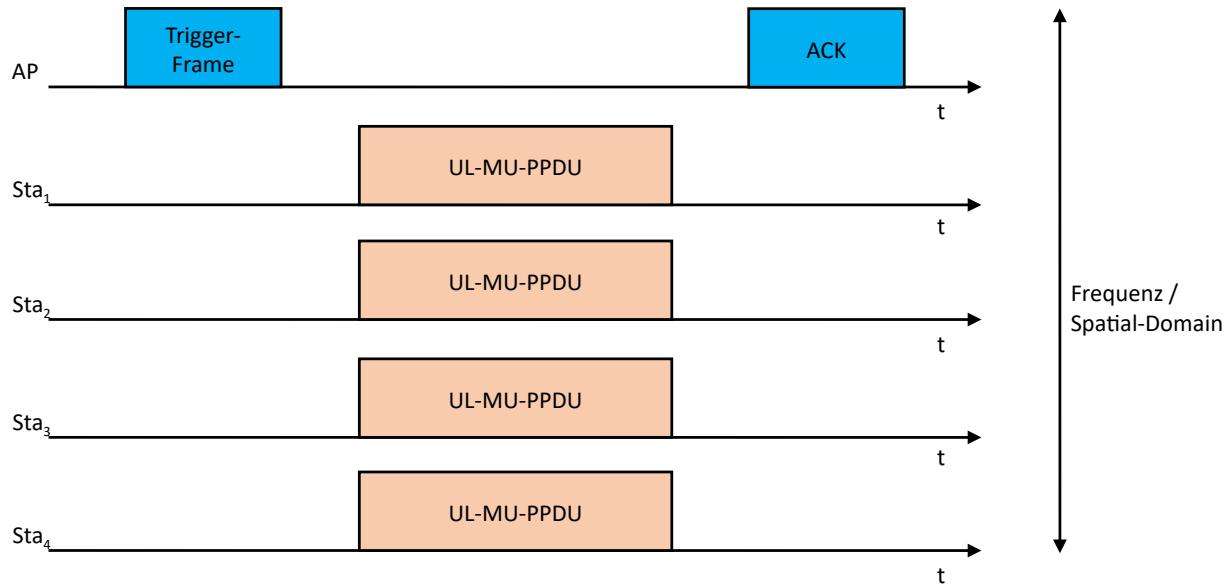


Abbildung 128: Verwaltung von MU-MIMO-Uplinks

Um die MU-MIMO-Daten für den Uplink von den Stationen abzurufen sendet der AP Trigger-Frames an alle Stationen. Darin werden die Anzahl der Spacial Streams und/oder die OFDMA-Zuordnungen zu Frequenz und RU-Größen für jeden Nutzer mitgeteilt.

Weiterhin sind auch Informationen zur Power-Control enthalten womit die Stationen ihre Sendeleistung anpassen können. Damit soll nicht Energie gespart werden, sondern die am AP ankommende Leistung aller Stationen, unabhängig von der Entfernung, möglichst gleich sein.

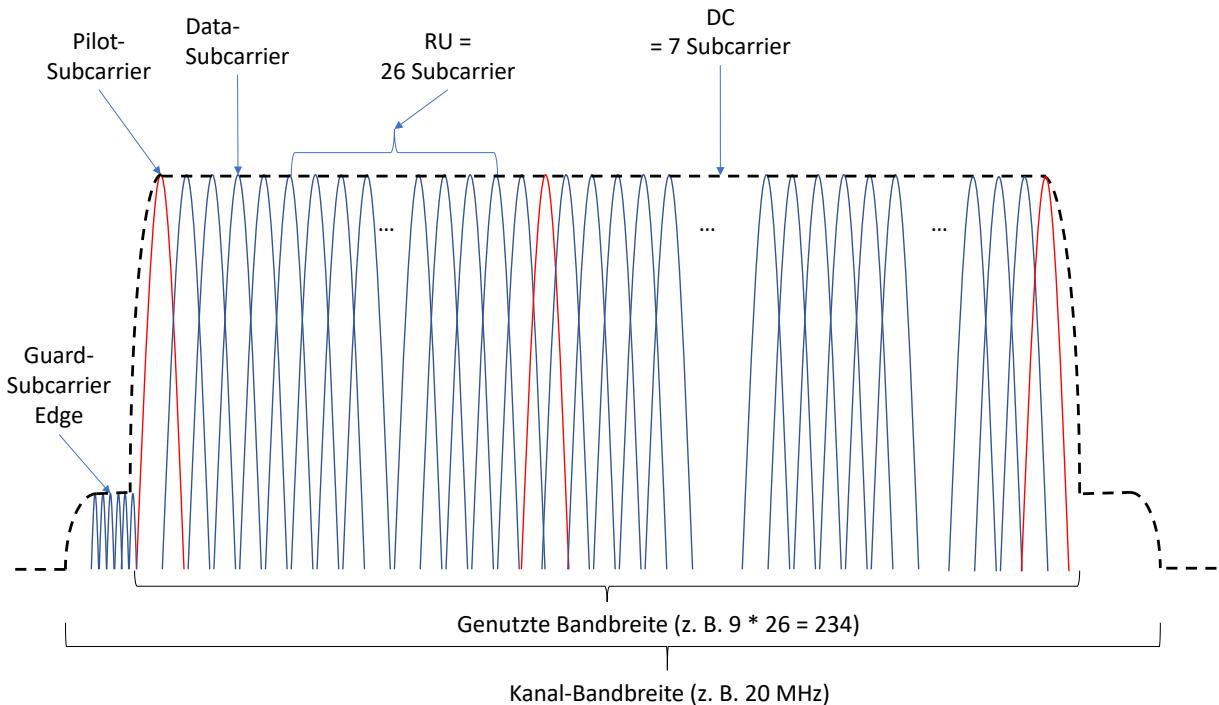
Im Trigger-Frame sind auch Informationen zum Beginn der Rückmeldungen (UL-MU-MIMO-PPDUs) und deren Dauer enthalten damit alle Stationen wissen, wann die Datenübertragung beendet werden muss.

Nachdem der AP alle Frames der Stationen empfangen hat sendet er ein ACK an alle Stationen.



Abbildung 129: OFDMA in gemischter Umgebung

Der Grundsätzliche Aufbau eines Frequenzbandes hat folgendes Aussehen:



Es gibt drei Nutzungsmöglichkeiten von Unterträgern:

- ➊ Daten-Unterträger. Diese Träger werden zu RUs zusammengefasst.
- ➋ Pilot-Unterträger. Diese Unterträger werden zur Bestimmung der Phasenlage bei OFDM benötigt.
- ➌ Ungenutzte Träger. Diese Unterträger sind als Trenner zwischen den RUs. Die DC-Subcarrier in der Mitte sind wichtig für die Rekonstruktion des OFDM-Signals.

Weiterhin gibt es am Randbereich noch die Guard-Subcarrier, welche die Frequenzbänder gegeneinander abtrennen

Das zur Verfügung stehende Frequenzband wird in unterschiedlich große RUs eingeteilt. RUs sind immer zusammenhängende Bereiche von Daten-Subcarriern.

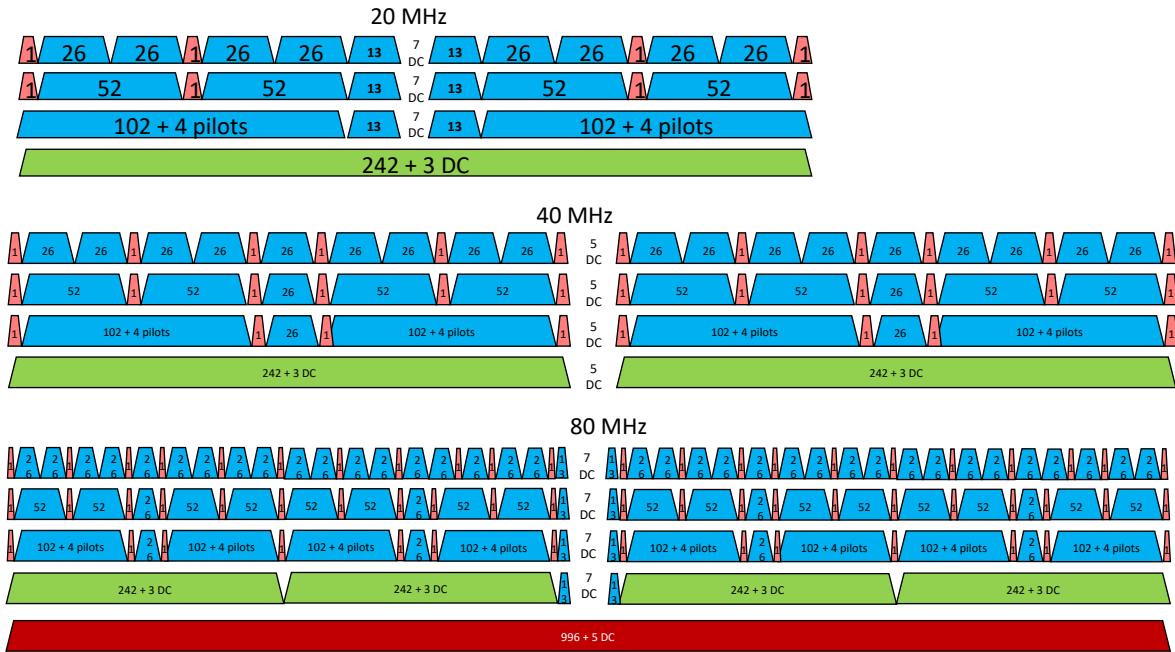


Abbildung 130: RUs bei unterschiedlichen Bändern

Es werden mindestens 26 (maximal 996) zusammenhängende Subcarrier einer RU zugewiesen.

Damit ergeben sich bei einem 20MHz breiten Kanal 9 User die gleichzeitig bedient werden können.
(siehe hierzu oberste Zeile in der obigen Abbildung)

Die DC-Subcarrier in der Mitte werden zur Vermeidung von Störungen ausgespart.

Bei Verwendung von 996 Subcarriern in einem 160MHz-Kanal sind 74 simultane User möglich.

Das Maximum, das einem einzelnen User zur Verfügung gestellt werden kann ist eine RU mit 242 Subcarriern.

Die folgende Tabelle zeigt die Anzahl der möglichen Benutzer in Abhängigkeit von Unterträger (Subcarrier) und Bandbreite (Channel Bandwidth)

Tabelle 47: Anzahl möglicher Benutzer nach Kanalbandbreite sortiert

RU-Typ	CBW 20	CBW 40	CBW 80	CBW 160
26 Subcarrier	9	18	37	74
52 Subcarrier	4	8	16	32
106 Subcarrier	2	4	8	16
242 Subcarrier	1-SU/MU-MIMO	2	4	8
484 Subcarrier	./.	1-SU/MU-MIMO	2	4

5.3.9.3 - Beamforming

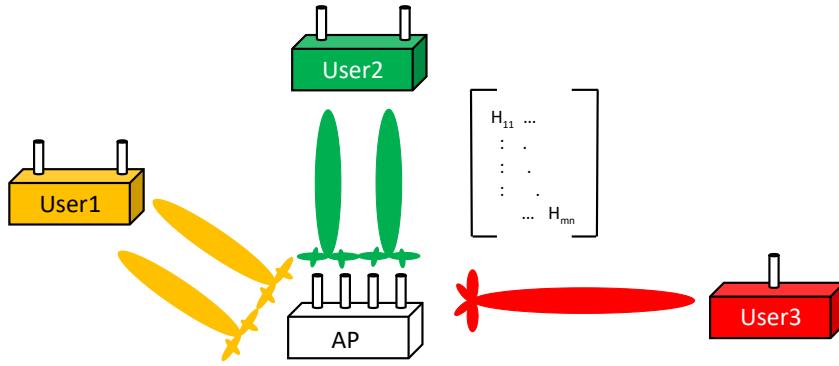


Abbildung 131: AP mit MU-MIMO sendet gerichtet an Stationen

Es wurde eine explizite Beamforming-Prozedur mit folgendem Ablauf eingeführt:

Der Beamformer (Trainer) initiiert mit einem Null-Paket die Prozedur zur Kanalprüfung.

Der Partner (Trainee) misst den Kanal und antwortet mit einem Beamforming-Feedback-Frame, der eine komprimierte Feedbackmatrix enthält.

Der Beamformer nutzt die Information zur Berechnung der Matrix H , die er dazu nutzt die Energie gezielt auf jeden Empfänger zu richten.

Wo bei IEEE-802.11ac noch 4 unterschiedliche Ziele von einem AP adressiert werden konnten sind es bei IEEE-802.11ax bis zu 8 unterschiedliche Ziele. Jede MU-MIMO-Verbindung kann ihre eigene Modulations, Codierungsmenge (MCS) und Spacial Streams haben. Senden Stationen auf einen Trigger-Frame hin simultan ihre Daten an den AP kann er durch Anwenden der Matrix die Daten der unterschiedlichen Verbindungen wieder herausfiltern.

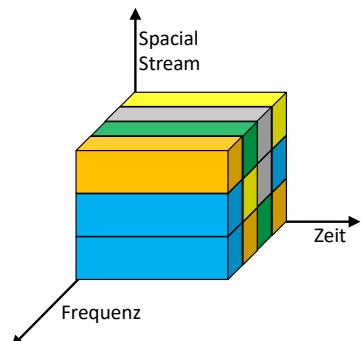


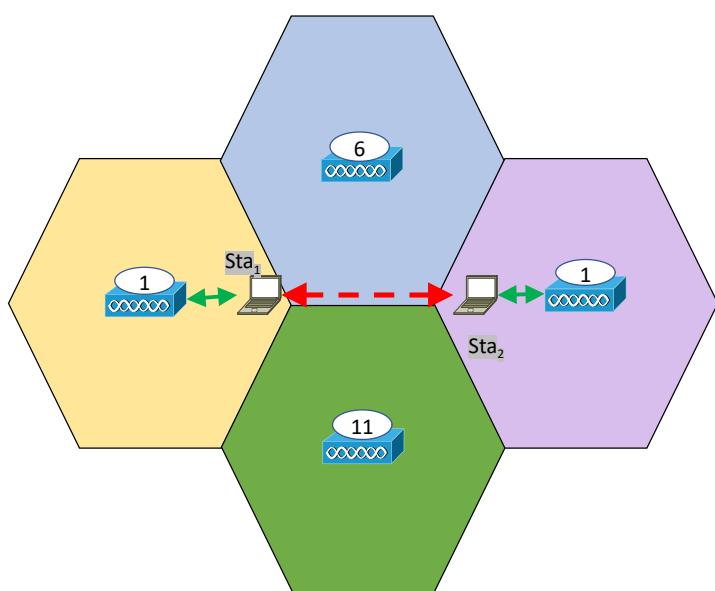
Abbildung 132: Zusammenhang:
Zeit - Spacial Stream - Frequenz

5.3.9.4 - BSS-Coloring

Bei einer sauberen Kanalplanung und Einhaltung des Mindestabstands sollte es nicht dazu kommen, dass eine Station mit zwei unterschiedlichen APs auf einem Kanal kommunizieren kann. Trotzdem kann es durch nicht sauber eingestellte Sendeleistungen oder durch unterschiedliche Betreiber von APs z. B. in einem Mehrfamilienhaus dazu kommen, dass eine Station auf einem Kanal mehrere APs zu sehen bekommt.

Selbst eine automatische Kanalwahl durch die APs gibt es keine Gewähr, dass immer ein freier Kanal gefunden wird und da das mittlerweile viele APs machen gibt es so gut wie nirgendwo noch freie Kanäle.

Wenn sich mehrere Geräte auf diesem Kanal beeinflussen sinkt die Übertragungsrate deutlich. Zur Lösung des Problems mit dem Mindestabstand bei z. B. 3 überschneidungsfreien Kanälen im 2,4GHz-Band wurde das BSS-Coloring eingeführt.



Obwohl die beiden Stationen (Sta_1 und Sta_2) im Kanal 1 senden beeinflussen sie sich nicht, da sie in unterschiedlich „eingefärbten“ Kanälen (gelb / lila) unterwegs sind.

Dazu ist im Header ein weiteres Feld eingeführt worden.

Abbildung 133: BSS-Coloring

Weiterhin gibt es noch die folgenden Verbesserungen:

- ➊ Höchste Modulation QAM1024
Das war zwar schon für IEEE-802.11ac vorgesehen, jedoch nicht umgesetzt worden
- ➋ Extended Range Preamble (ERP)
Hier wird mit einem speziellen Paketformat für Anwendungen im Freien
- ➌ OFDM-Symboldauer von $12,8\mu\text{s} + 0,8/1,6/3,2 \mu\text{s CP}$ (anstelle bisher $3,2\mu\text{s} + 0,8/0,4 \mu\text{s CP}$)
Dies verbessert vor allem im Outdoor-Bereich die Übertragungsqualität und damit die Datenrate.
- ➍ Zusätzlich zum 5GHz-Bereich wird der 2,4GHz-Bereich genutzt

Tabelle 48: Modulation and coding schemes for single spatial stream

MCS index[a]	Modulation type	Coding rate	Data rate (in Mb/s)[b]							
			20 MHz channels		40 MHz channels		80 MHz channels		160 MHz channels	
			1600 ns GI[c]	800 ns GI	1600 ns GI	800 ns GI	1600 ns GI	800 ns GI	1600 ns GI	800 ns GI
0	BPSK	1/2	8	8.6	16	17.2	34	36.0	68	72
1	QPSK	1/2	16	17.2	33	34.4	68	72.1	136	144
2	QPSK	3/4	24	25.8	49	51.6	102	108.1	204	216
3	16-QAM	1/2	33	34.4	65	68.8	136	144.1	272	282
4	16-QAM	3/4	49	51.6	98	103.2	204	216.2	408	432
5	64-QAM	2/3	65	68.8	130	137.6	272	288.2	544	576
6	64-QAM	3/4	73	77.4	146	154.9	306	324.4	613	649
7	64-QAM	5/6	81	86.0	163	172.1	340	360.3	681	721
8	256-QAM	3/4	98	103.2	195	206.5	408	432.4	817	865
9	256-QAM	5/6	108	114.7	217	229.4	453	480.4	907	961
10	1024-QAM	3/4	122	129.0	244	258.1	510	540.4	1021	1081
11	1024-QAM	5/6	135	143.4	271	286.8	567	600.5	1134	1201

Hinweise:

MCS 9 is not applicable to all channel width/spatial stream combinations.

A second stream doubles the theoretical data rate, a third one triples it, etc.

GI stands for the guard interval.

Quelle Wikipedia

Tabelle 49: Mindest-Empfängerempfindlichkeit bei 802.11ax

MCS	Modulations-Verfahren	Code-Rate	Empfängerempfindlichkeit bei 20MHz Kanalbandbreite [dBm]	Empfängerempfindlichkeit bei 40MHz Kanalbandbreite [dBm]	Empfängerempfindlichkeit bei 80MHz Kanalbandbreite [dBm]	Empfängerempfindlichkeit bei 160MHz oder 80+80MHz Kanalbandbreite [dBm]
0	BPSK	1/2	-82	-79	-76	-73
1	QPSK	1/2	-79	-76	-73	-70
2	QPSK	3/4	-77	-74	-71	-68
3	16-QAM	1/2	-74	-71	-68	-65
4	16-QAM	3/4	-70	-67	-64	-61
5	64-QAM	2/3	-66	-63	-60	-57
6	64-QAM	3/4	-65	-62	-59	-56
7	64-QAM	5/6	-64	-61	-58	-55
8	256-QAM	3/4	-59	-56	-53	-50
9	256-QAM	5/6	-57	-54	-51	-48
10	1024-QAM	3/4	-54	-51	-48	-45
11	1024-QAM	5/6	-52	-49	-46	-43

5.3.9.5 - PPDU-Formate

Die Einführung der neuen Funktionen erforderte auch die Einführung von vier neuen PPDU-Formaten wie die unteren vier Formate in Abbildung 134:

- High Efficiency Single-User PPDU (HE_SU). Damit werden Daten zu einem einzelnen User übermittelt.
- Multi User PPDU (HE_MU) Damit sollen die Daten für einen oder mehrere User transportiert werden.
- High Efficiency Extended Range Single-User(HE_EXT_SU) Damit sollen die Daten zwar immer noch nur an einen User übermittelt werden, jedoch soll die Reichweite wesentlich verbessert werden.
- HE Trigger based PPDU (HE_Trig) Dieses Frame-Format wird durch einen Trigger-Frame ausgelöst und transportiert die Daten einer Übertragung.

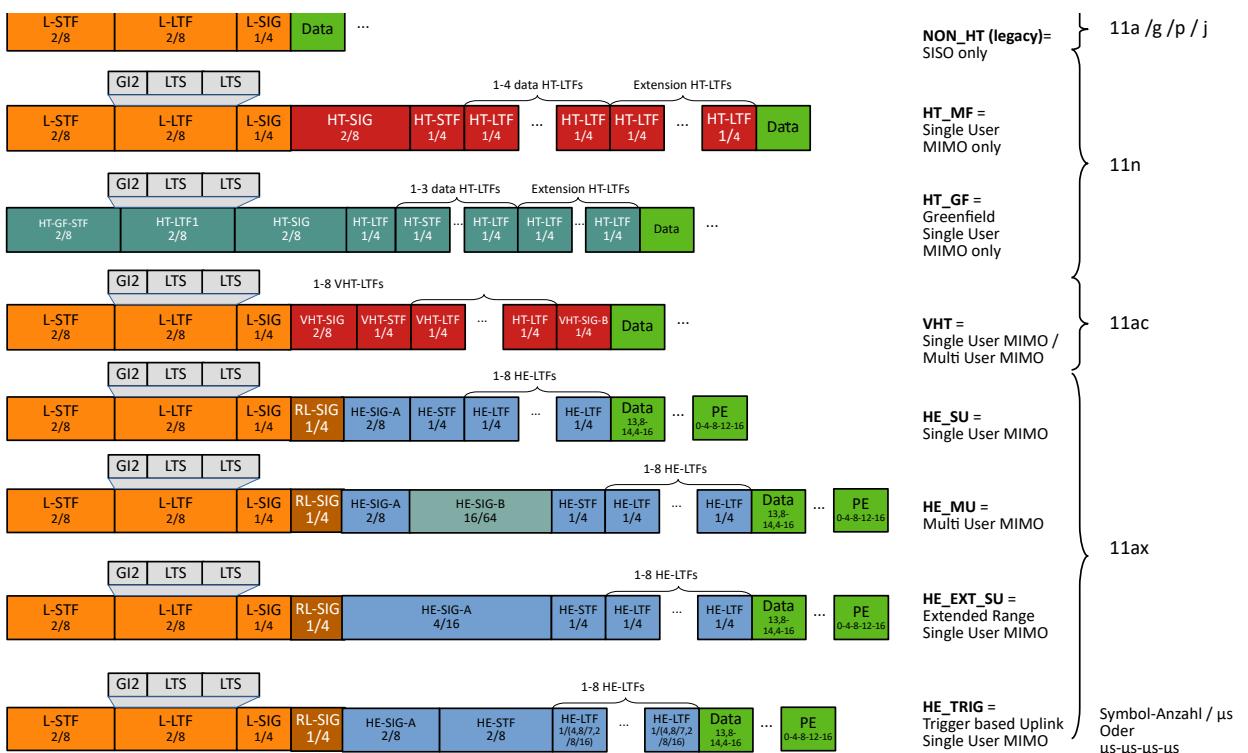


Abbildung 134: IEEE-802.11-PPDU-Formate

Tabelle 50: Beschreibung der PPDU-Felder

Feld	Bedeutung	Feld	Bedeutung
L-STF	Legacy Short Trainings Field	HE-STF	HE Short Trainings Field
L-LTF	Legacy Long Trainings Field	HE-LTF	HE Long Trainings Field
L-SIG	Legacy Signal Field	Data	Daten
RL-SIG	Repeated Legacy Long Trainings Field	PE	Packet Extension
HE-SIG-A	HE Signal Field A	GI	Guard Interval
HE-SIG-B	HE Signal Field B	LTS	Legacy Training Sequence

5.3.9.6 - Frame-Format-Details

Je nachdem, ob es sich um ein Uplink (UL) oder Downlink (DL) werden die neuen Teile des Frame-Formats genutzt. Weiterhin ist noch zwischen Single-User (SU) und Multi-User (MU) zu unterscheiden.

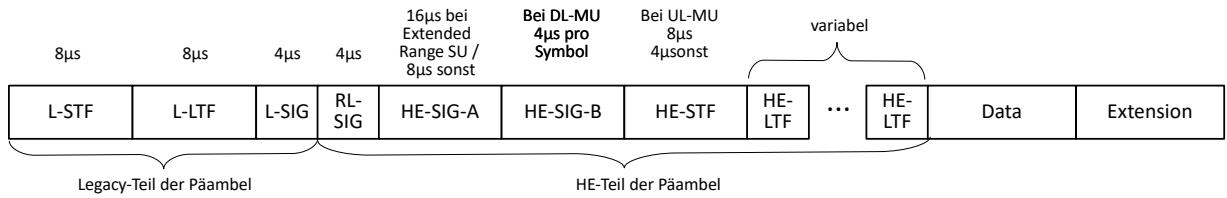


Abbildung 135: 802.1ax PHY Frame Format

Für jeden 20MHz Unterträger wird die Information kopiert.

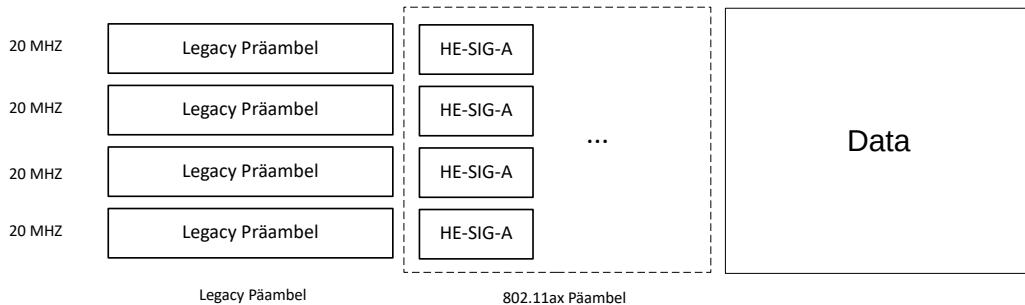


Abbildung 136: Duplizierung der Legacy und HE-Präambel

5.3.9.6.1 - HE-SIG-A

Die Information für das Sig-A-Feld wird verdoppelt.

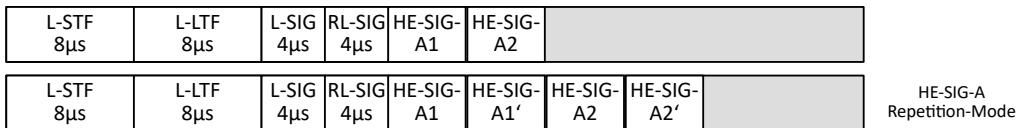


Abbildung 137: Wiederholung der HE-SIG-A Informationen

5.3.9.6.2 - HE-SIG-B

Das SIG-B Feld ist nur bei der Variante für DL-MU PPDU vorhanden.

Die SIG-B-Information teilt sich in zwei Bereiche auf:

- Common-Field.
- User-Specific-Field. Hier sind User-spezifische Informationen hinterlegt.

Tabelle 51: HE-SIG-B Common Teil mit deren Bedeutung

Feld	Anzahl Bits	Beschreibung
RU	N * 8	Beschreibt die RU Aufteilung innerhalb der Frequenz-Domäne. Siehe auch Tabelle 53 Zeigt die Anzahl der User die MU-MIMO nutzen an N = 1 bedeutet 20MHz und 40MHz HE-MU-PPDU N = 2 bedeutet 80 MHz HE-MU-PPDU N = 4 bedeutet 160/80+80 MHz HE-MU-PPDU
Center 26- tone RU	1	Nur bei voller 80-MHz- und 160/80+80-Mhz-Bandbreite 0 = Center-26-Tone RU ist nicht zugewiesen 1 = Center-26-Tone RU ist zugewiesen
CRC	4	Prüfsumme
Tail	6	Initialisierung für den Faltungscodierer (auf 0 gesetzt)

Tabelle 52: HE-SIG-B User-spezifischer Teil mit deren Bedeutung

Feld	Bedeutung
STA-ID	Niederwertigste 11 Bits der Assosiation-ID (AID) Ist die RU keiner Station zugeordnet, wird der Wert auf 2046 gesetzt
NSTS	Anzahl der Spatial Streams
TX-Beamforming	1 = TX-Beamforming wird durchgeführt / 0 = kein TX-Beamforming
MCS	Modulation and Coding Scheme: 0: BPSK 1 / 2 1: QPSK 1 / 2 2: QPSK 3 / 4 3: 16-QAM 1 / 2 4: 16-QAM 3 / 4 5: 64-QAM 1 / 2 6: 64-QAM 3 / 4 7: 64-QAM 5 / 6 8: 256-QAM 3 / 4 9: 256-QAM 5 / 6 10: 1024-QAM 3 / 4 11: 1024-QAM 5 / 6
DCM	Dual Carrier Modulation (0 = not used / 1 = used)
Coding	0 = Binary Convolutional Code / 1 = Low Density Parity Check

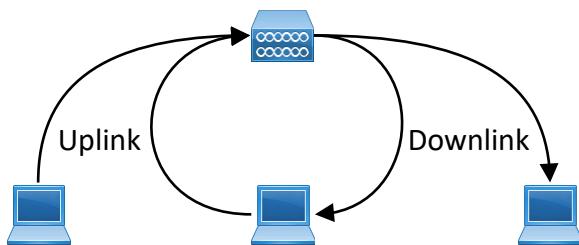
5.3.9.6.3 - Zuordnung der RUs zu den Tone-Segmenten

Die unterschiedlich breiten Kanäle können wie in der folgenden Tabelle zusammengefasst und den Stationen zugeordnet werden.

Tabelle 53: OFDMA RU-Zuordnung per 242-Tone-Segment

8-Bit b7 ... b0	#1	#2	#3	#4	#5	#6	#7	#8	#9													
00000000	26	26	26	26	26	26	26	26	26													
00000001	26	26	26	26	26	26	26	52														
00000010	26	26	26	26	26	52		26	26													
00000011	26	26	26	26	26	52		52														
00000100	26	26	52		26	26	26	26	26													
00000101	26	26	52		26	26	26	52														
00000110	26	26	52		26	52		26	26													
00000111	26	26	52		26	52		52														
00001000	52		26	26	26	26	26	26	26													
00001001	52		26	26	26	26	26	52														
00001010	52		26	26	26	52		26	26													
00001011	52		26	26	26	52		52														
00001100	52		52		26	26	26	26	26													
00001101	52		52		26	26	26	52														
00001110	52		52		26	52		26	26													
00001111	52		52		26	52		52														
00010000	52		52		-	106																
00011000	106				-	52		52														
00100000	26	26	26	26	26	106																
00101000	26	26	52		26	106																
00110000	52		26	26	26	106																
00111000	52		52		26	106																
01000000	106				26	26	26	26	26													
01001000	106				26	26	26	52														
01010000	106				26	52		26	26													
01011000	106				26	52		52														
01100000	106				-	106																
01110000	52	52		-	52	106																
01110001	242-tone RU empty																					
01110010	484-tone RU mit zero HE-SIG-B user-spezifisch mit zugehörigem HE-SIB-B content channel																					
01110011	996-tone RU mit zero HE-SIG-B user-spezifisch mit zugehörigem HE-SIB-B content channel																					
011101x ₁ x ₀	tbd.																					
011111x ₁ x ₀	tbd.																					
10000000	106			26	106																	
11000000	242																					
11001000	484																					
11010000	996																					
11011000	2 * 996																					
111x ₄ x ₃ x ₂ x ₁ x ₀	tbd.																					

5.3.9.7 - Multiuser-Betrieb



Mit dem 802.11ax-standard ist es erstmals möglich, dass mehrere Stationen gleichzeitig in in Uplink-Richtung Daten senden, oder in Downlink-Richtung Daten empfangen.

Abbildung 138: Gleichzeitige Datenübertragung in Uplink- oder Downlink-Richtung

5.3.9.8 - OFDMA-Padding

Alle User, die OFDMA nutzen, müssen zur selben Zeit mit dem Frame-Empfang starten und zur selben Zeit enden. Das ist erforderlich damit andere Stationen, die den Kanal abhören erkennen können, ob der Kanal belegt ist oder nicht. Das hat beim Multi-User-Downlink (MU-DL) zur Folge, dass kurze Frames, die zusammen mit langen Frames gesendet werden, aufgefüllt werden müssen.

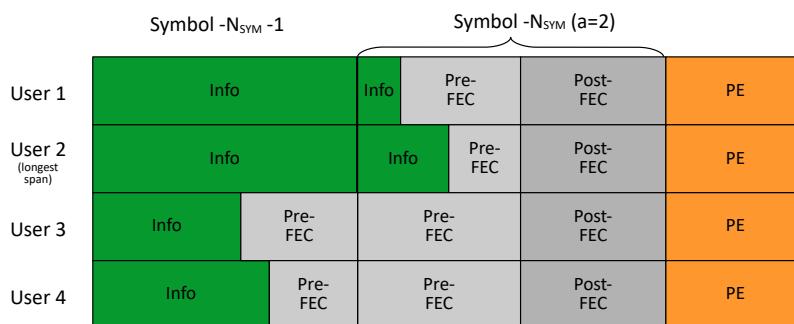


Abbildung 139: DL-OFDMA-Padding

In Gegenrichtung weiß der AP erst einmal nicht wie groß die Pakete der Stationen sind. Deshalb teilt er den angemeldeten Stationen mit dem Trigger-Frame eine Sendegröße zu.

5.3.9.9 - Wi-Fi 6E

Als zusätzliche Erweiterung der Frequenzbänder des IEEE-802.11ax Umfangs wurden am 24.4.2020 für die USA vier Frequenzbänder freigegeben.

Die US-amerikanische Regulierungsbehörde Federal Communications Commission (FCC) hat am 24. April 2020 weitere Frequenzbänder im 6GHz-Bereich freigegeben. Dabei handelt es sich um Bänder in der so genannten Unlicensed National Infomation Infrastructure (U-NII) :

- 5.925 – 6.425 MHz (U-NII-5)
- 6.425 – 6.525 MHz (U-NII-6)
- 6.525 – 6.875 MHz (U-NII-7)
- 6.875 – 7.125 MHz (U-NII-8)

Damit könnte eine Bandbreite von 1200 MHz für WLAN genutzt werden, womit eine theoretische Datenübertragungsrate von 60Gbit/s auf kurze Distanzen möglich wird. In den USA kann ein AP im Freien in den U-NII-Bändern 7 und 8 mit einer maximalen Sendeleistung von bis zu 4 Watt (EIRP) senden. Stationen dürfen mit maximal 1 Watt senden. Das gilt übrigens innerhalb von Gebäuden auch für APs. Weitere Länder sind Chile und Südkorea.

In Europa werden diese Frequenzen Länderweise freigegeben. In einem ersten Schritt wird das erste Band freigegeben. In den unterschiedlichen Ländern erfolgt die Freigabe durch die zuständigen Gremien, weshalb hier Wi-Fi 6E teilweise nur ein Marketing-Spruch ist. Freigabetermine:

- Deutschland (5,945 – 6,425 GHz ab 20.06.2021)
- Österreich (bis Ende 2021)
- Schweiz (geplant zum 01.01.2022)

Die höhere Dämpfung bei höheren Frequenzen reduziert das Signal bei gleicher Reichweite auf die Hälfte (3dB).

Damit ergeben sich zusätzliche 500 MHz (24 zusätzliche 20MHz-Kanäle) an Bandbreite für die WLAN-Nutzung, was das WLAN-Spektrum fast verdoppelt. Im neuen Band sind Low Power Indoor (LPI) und Very Low Power Devices (VLP).

Frequenzbereich [GHz]	Kanal-Anzahl bei 20MHz Kanalbreite	Maximale Sendeleistung [mW]	Einschränkungen
2,4 – 2,482	3	100	
5,150 – 5,250	4	200	Nur Indoor
5,250 – 5,350	4	200	Nur Indoor / DFS erforderlich
5,470 – 5,725	11	1.000	Indoor und Outdoor / DFS erforderlich
5,725 – 5,350	5	25	Short Range Devices (SRD)
5,925 – 6,425	24	200 (LPI) 25 (VLP)	Beschränkter Innenraumeinsatz, auch in Zügen mit metallbeschichteten Fenstern und Luftfahrzeugen. Kein Einsatz im Außenbereich. (Auch nicht in Straßenfahrzeugen) Indoor und Outdoor. Kein Einsatz im unbemannten Luftfahrzeugsystemen (UAS)

Es ist vorgesehen die Bänder U-NII-6 bis U-NII-8 in den nächsten Jahren freizugeben. Mit den zusätzlichen 700MHz könnten dann auch die in IEEE-802.11be (Wi-Fi 7) vorgesehenen 320MHz breiten Kanäle genutzt werden.

Um die Unterschiede zwischen Single-User-MIMO und Multi-User-MIMO zu veranschaulichen, soll Abbildung 140 dienen.

Pro AP stehen maximal 8 Spacial Streams zur Verfügung von denen 4 als Säulen dargestellt sind.

Bei 802.11ax man sehen, dass ein AP, einen Stream, durch unterschiedliche RU-Zusammensetzung und RU-Zuordnung zu Stationen, gleichzeitig mehrere Stationen in Uplink- und Downlink-Richtung bedienen kann.

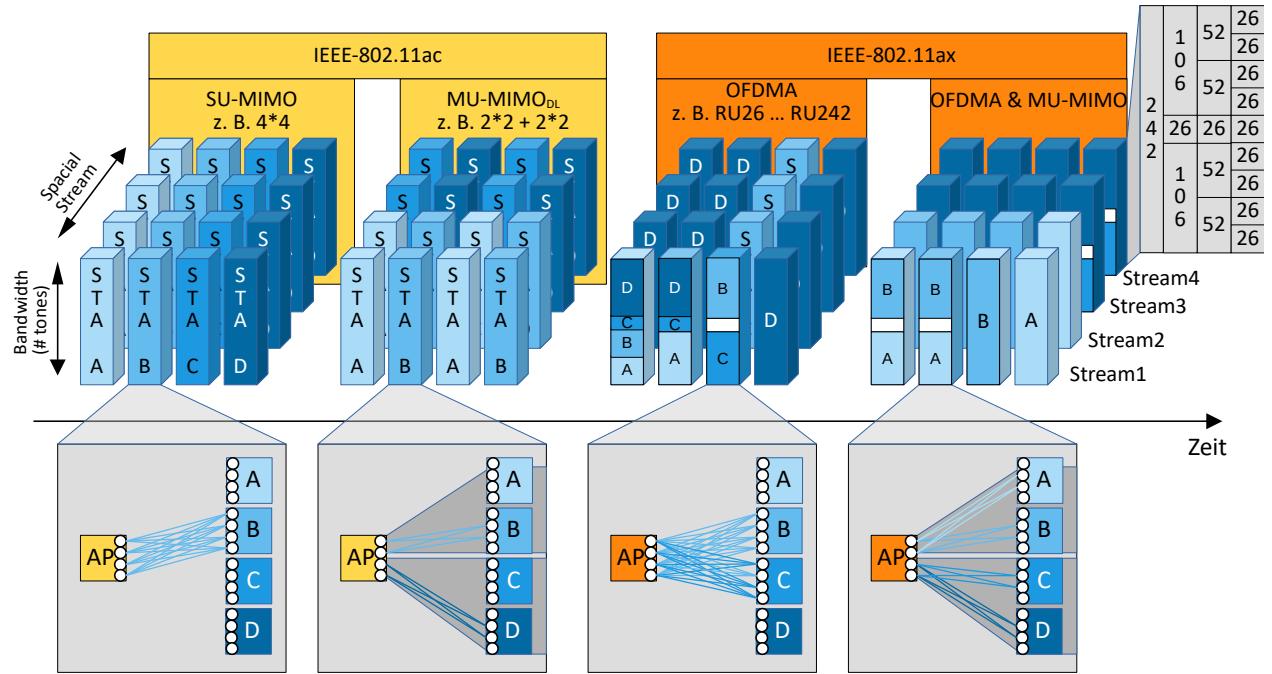


Abbildung 140: Vergleich IEEE-802.11ac und IEEE-802.11ax

5.3.10 - Künftiger Standard Wi-Fi-7 (IEEE802.11be)

Für Mitte 2024 wird die Verabschiedung des Standards IEEE802.11be (Wi-Fi-7) erwartet. Erste Geräte sind bereits seit Ende 2023 auf dem Markt.

Die wichtigsten Neuerungen sind:

- Multi-Link Operation (MLO). Damit kann gleichzeitig in bis zu drei Frequenzbändern (2,4GHz, 5GHz und 6GHz) gesendet werden.
- Mit der höchsten Modulationsstufe 4096-QAM (4kQAM) können pro Symbol 12 Bit übertragen werden.
- Die verwendbare Kanalbreite wird auf 320MHz verdoppelt.

Bei der maximalen Anzahl von 8 MIMO-Streams ändert sich nichts.

Eigenschaften

Name: Wi-Fi 7

Frequenzband: 2,4 GHz, 5GHz und 6GHz

Anzahl der Kanäle: 3 (2,4GHz) / 16 (5GHz 20 MHz) / 7 (5GHz 40 MHz) / 3 (5GHz 80 MHz) / 1 (5GHz 160 MHz)

Kanalbreite: 20, 40, 80, 160, 320MHz

Multiplex-Verfahren: OFDMA

Modulation: Max. 4096QAM (4kQAM)

MIMO-Streams 1 bis 8

Maximale Brutto-Datenrate: 23 Gbps

Typische Netto-Datenrate: 0,3 – 8 Gbps

Bei Wi-Fi-6e gab es auch schon die Möglichkeit für die Geräte auf 2,4GHz, 5GHz oder 6GHz zu senden und zu empfangen. Allerdings war das zu einem Zeitpunkt immer nur auf einem der Kanäle möglich. Bei Wi-Fi-7 gibt es erstmals die Möglichkeit gleichzeitig auf allen Kanälen Daten auszutauschen.

Für ein Endgerät, wie ein Notebook, ist es erst einmal nicht ersichtlich, ob es einen Access Point mit 3 Funkmodulen und 3 MAC-Adressen oder mit 3 Access Points mit je einem Funkmodul und einer MAC-Adresse vor sich hat.

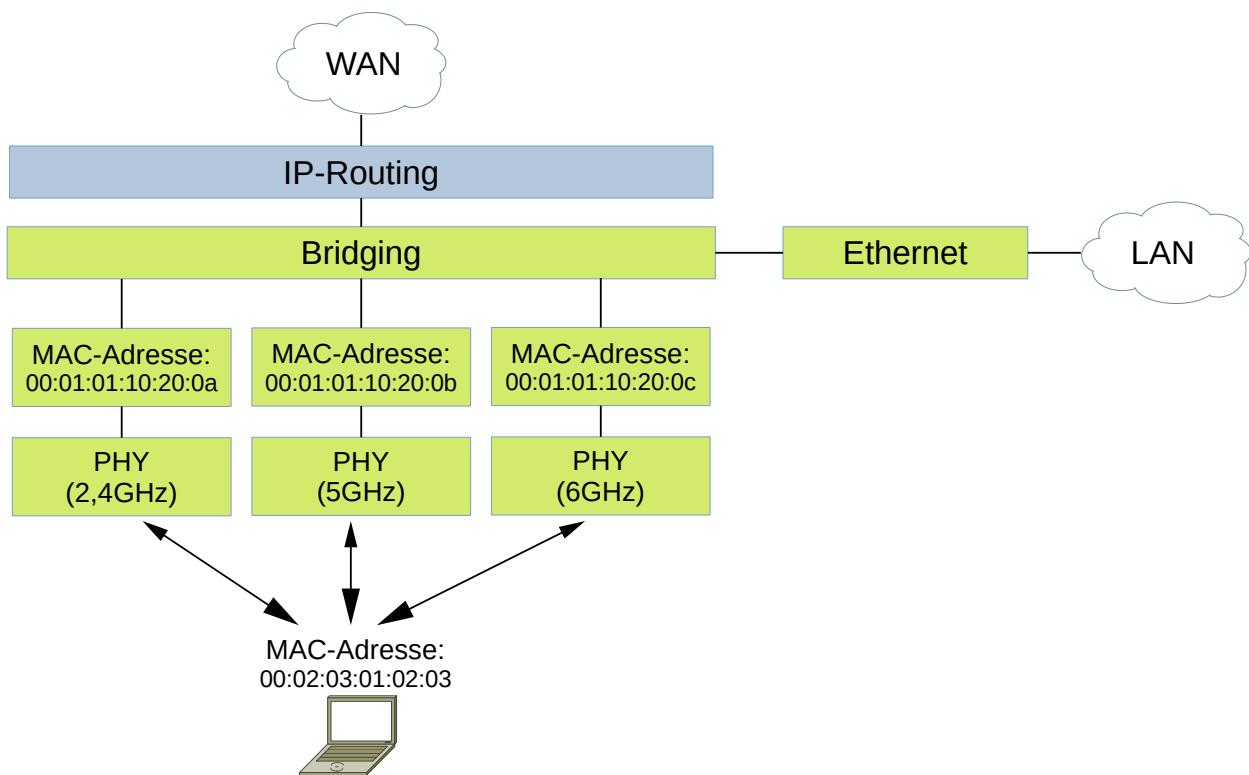


Abbildung 141: Wi-Fi-7: Router mit drei WLAN-Kanälen und Notebook mit 2 WLAN-Kanälen

5.3.10.1 - Multi-Link Operation (MLO)

Mit MLO-Funktion konnten folgende Verbesserungen erreicht werden.

- Durchsatz
- Latenzzeit
- Robustheit

Für unterschiedliche Anwendungsfälle wurden 4 Modi entwickelt, die für alle Möglichkeiten Verbesserungen bieten.

- Simultaneous Transmit and Receive (STR)

Hier kann auf allen drei möglichen Bändern gleichzeitig ein Datenaustausch stattfinden.

Für die Kommunikation mit Geräten, die nicht alle drei Kanäle bedienen können, weil Transceiver oder Antennen fehlen, wurden abgestuft nach den Möglichkeiten trotzdem noch Verbesserungen erreicht.

- Enhanced Multi-Link Multi Radio (EMLMR)
- Enhanced Multi-Link Single Radio (EMLSR)
- Multi-Link Single Radio (MLSR)

5.3.10.1.1 - Simultaneous Transmit and Receive (STR)

Um gleichzeitig auf mehreren Kanälen Daten auszutauschen, hat man bei IEEE auf der MAC-Ebene einen neuen Ebene die Upper-MAC-Layer eingeführt.

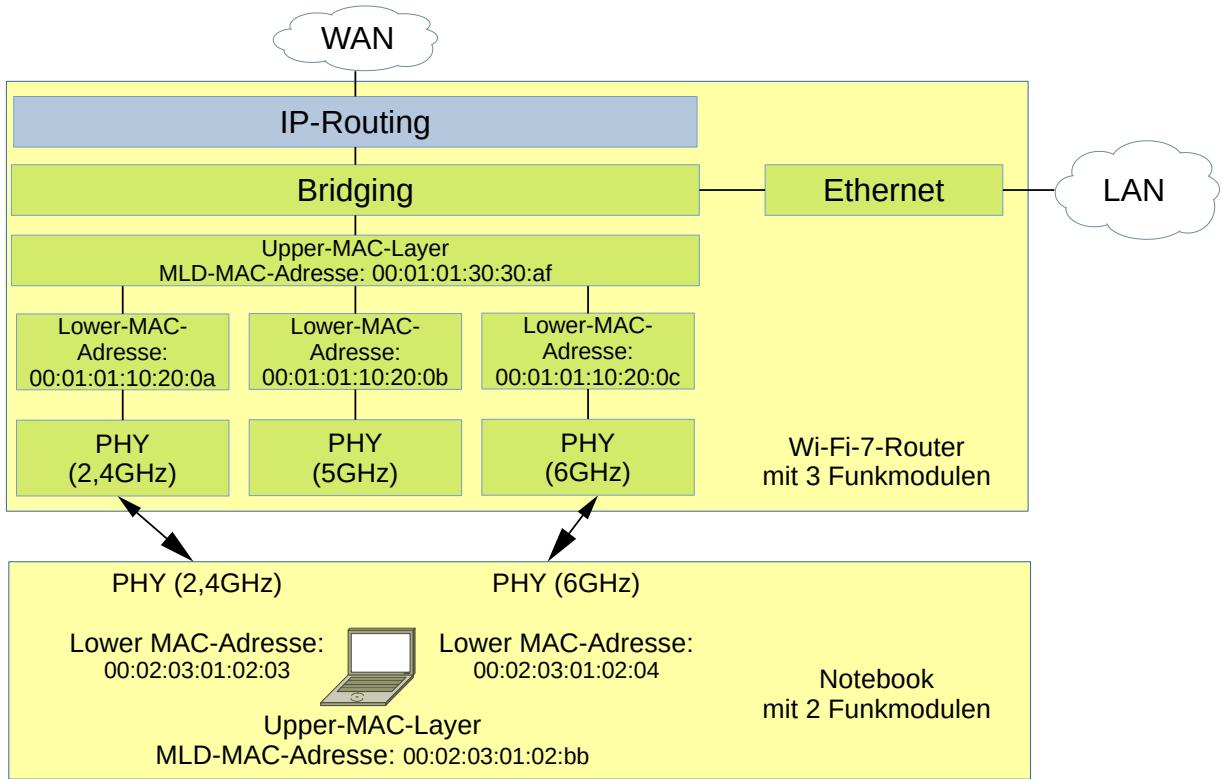


Abbildung 142: Wi-Fi 7: Gleichzeitiger Datenaustausch auf drei Kanälen

Mit der MLD-MAC-Adresse können die Kanäle gebündelt und gleichzeitig bedient werden. Eine MLD-MAC-Adresse muss es für jedes Gerät geben, das mehrere Kanäle parallel nutzen will.

Wie oben bereits ausgeführt waren die Ziele Steigerung des Durchsatzes, Reduzierung der Latenzzeit und Verbesserung der Robustheit den Entwicklern vorgegeben worden. Die Ziele konnten folgendermaßen erreicht werden. Allerdings können die Ziele nicht gleichzeitig erreicht werden da sie sich stellenweise gegenseitig ausschließen.

5.3.10.1.1.1 - Durchsatzsteigerung

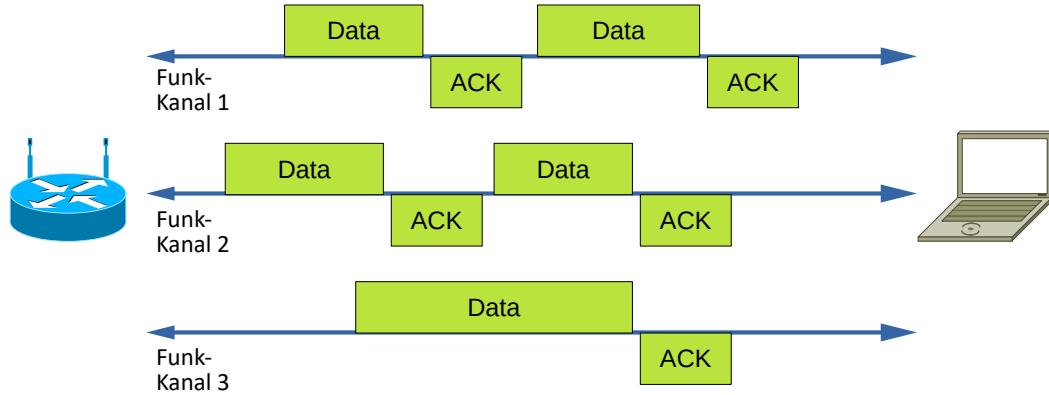


Abbildung 143: Wi-Fi-7: Durchsatzsteigerung

Durch die gleichzeitig zur Verfügung stehenden Kanäle können mehr Daten transportiert werden. Allerdings bedeutet die Koordinierung einen erheblichen Aufwand damit z. B. keine Überholvorgänge der Pakete eintreten. So sind unterschiedlich ausgelastete Kanäle unterschiedlich in der Lage, Daten schnell zu transportieren.

5.3.10.1.1.2 - Reduzierung der Latenzzeit

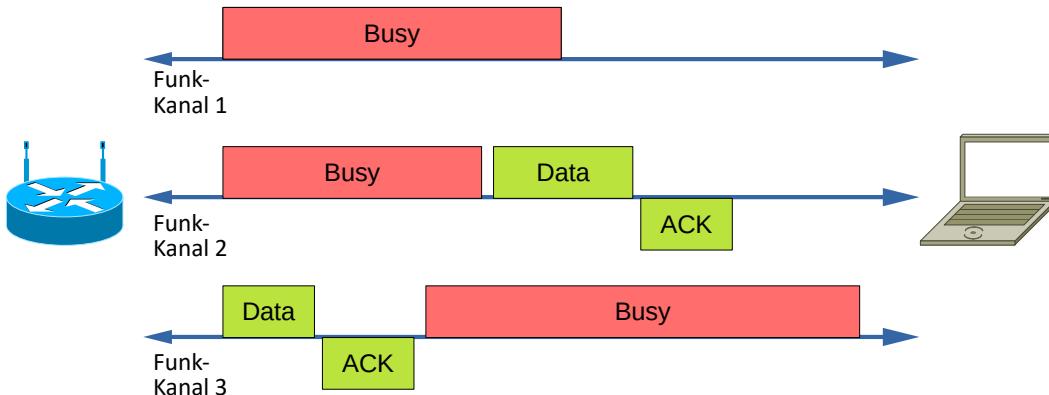


Abbildung 144: Wi-Fi-7: Reduzierung der Latenzzeit

Kanäle die von vielen Teilnehmern genutzt werden reduzieren den Durchsatz und erhöhen die Latenz. Ist dagegen ein anderer Kanal frei, kann er genutzt und die Latenzzeit reduziert werden.

5.3.10.1.1.3 - Robustheit

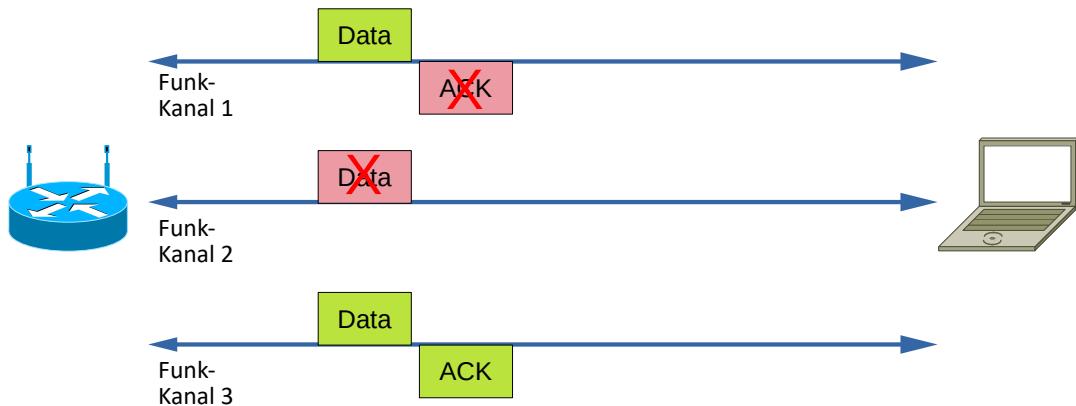


Abbildung 145: Wi-Fi-7: Robustheit

Ein Paket wird nicht nur auf einem Kanal, sondern auf drei Kanälen gesendet. Damit ist die Wahrscheinlichkeit, dass auf einem Kanal das Paket fehlerfrei übermittelt werden kann, größer.

Der Simultaneous Transmit and Receive Mode (STR) ist nur für Geräte möglich, die 3 Funkmodule eingebaut haben. Für Geräte, bei denen das nicht der Fall ist, wurden trotzdem Verbesserungen ermöglicht.

5.3.10.1.2 - Enhanced Multi-Link Multi Radio (EMLMR)

Gleich unter der Performance des STR-Modus ist der EMLMR-Modus angesiedelt. So haben z. B. Notebooks für das 5GHz-Band und das 6GHz-Band nur eine Kombiantenne. Deshalb können sie immer nur die Kombination von 2,4GHz und 5GHz oder 2,4GHz und 6GHz nutzen. Die Basis bestimmt welchen der beiden Varianten genutzt wird.

5.3.10.1.3 - Enhanced Multi-Link Single Radio (EMLSR)

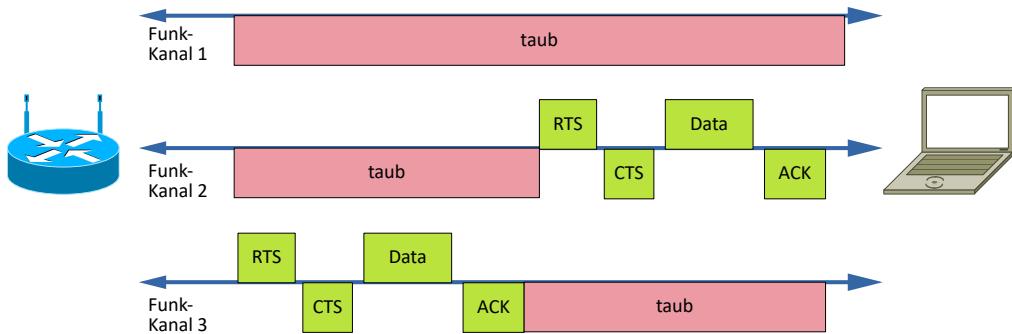


Abbildung 146: Enhanced Multi-Link Single Radio

Transceiver haben an den Rändern der Kanäle oft flach auslaufende Signale welche die Nachbarkanäle stören. Das war bisher kein Problem, da die Nachbarkanäle nicht genutzt wurden. Jetzt, da auch benachbarte Bänder genutzt werden sollen, beeinträchtigen sich die Bänder gegenseitig. Das wird auch Selbstinterferenz genannt. Für steilere Filter oder größere Antennenabstände ist z. B. in Mobiltelefonen kein Platz. Die Lösung zum Problem sieht folgendermaßen aus.

Der Client lauscht auf allen Kanälen mit einem robusten Modulationsverfahren. Das spart Strom und reicht für kurze Control-Frames wie RTS und CTS. Eine voll ausgebauten Basisstation sendet einen RTS. Der Client antwortet

mit einem CTS und schaltet auf ein höherwertiges Modulationsverfahren. Auf den anderen Kanälen ist der Client taub. Darauf hin sendet der AP seine Daten, die vom Client mit einem ACK quittiert werden. Danach lauscht er wieder mit niedriger Modulation auf einen RTS.

5.3.10.1.4 - Multi-Link Single Radio (MLSR)

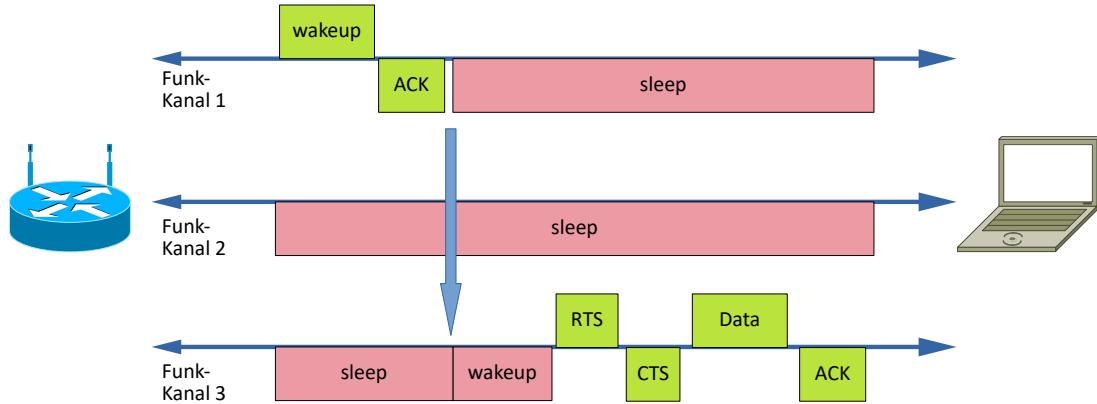


Abbildung 147: Multi-Link Single Radio

Dieses Verfahren ist gedacht für Clients, die nur einen Transceiver haben. Der Client wechselt schnell zwischen den Kanälen und meldet sich an allen Kanälen an und wartet auf einem Kanal.

Sobald der AP Daten zu senden hat weckt er den Client mit einem Wakeup-Frame auf. In der Quittung sendet der Client den Kanal, in dem er Daten empfangen will und fährt den in den Sleep Modus.

Der Client wechselt nun schnell auf den angegebenen Kanal und fährt den Transceiver hoch. Der AP sendet ein RTS und sobald der Client bereit ist, sendet er mit dem CTS den Startschuss für die Datenübertragung.

Ungenutzte Kanäle werden in den Sleep-Modus versetzt.

5.3.10.2 - Optimierungen am Medienzugriffsverfahren OFDMA

Die Mindestanzahl koordinierter Clients wurde gesenkt. Da die Koordinierung von Clients nur Gruppen von Daten verwalten kann musste auf die Daten von mindestens 2 Clients gewartet werden. So konnte es vorkommen, dass lange gewartet werden musste. Durch die Senkung auf nur einen Client pro Gruppe konnte beschleunigt werden.

Die Aufteilung eines Bandes ist unter Wi-Fi-7 noch feiner geworden und kann damit auf kleine zu übertragende Datenmengen besser reagieren.

5.4 - Vergleich der IEEE-802.11-Standards

Ein Vergleich der zur Zeit auf dem Markt befindlichen Standards kann in der folgenden Tabelle zusammengefasst werden.

	IEEE-802.11									
	Wi-Fi 1	Wi-Fi 2	Wi-Fi 3			Wi-Fi 4	Wi-Fi 5	Wi-Fi 6	Wi-Fi 6E	Wi-Fi 7
	a	b	g	a	h	n	ac	ax	ax + (6GHz)	be
Max. Brutto-Datenrate [Mbit/s]	1	11/5,5/2/1	54/ 48/ 36/ 24/ 18/ 12/ 9/6	54/ 48/ 36/ 24/ 18/ 12/ 9/6	54/ 48/ 36/ 24/ 18/ 12/ 9/6		6.900	9.600	9.600	23.000
Max. Reichweite (innen/außen) [m]	20/100	38/140	38/140	25/120	25/120	70/250 70/250	50/?	30/? 30/?	30/?	
Frequenz-Bänder [GHz]	2,4	2,4	2,4	5	5	2,4 / 5	5	2,4 / 5	2,4 / 5 / 6	2,4 / 5 / 6
Kanaleanz. bei 20MHz	3 (4)	3 (4)	3 (4)	4	19/8 (D), 8 (CH)			27	52	
FEC	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Sendeleistung EIRP		100 mW	100 mW	30 mW (D) 60 mW (CH)	200 mW, 1W (D) 200 mW (CH)	100mW (D)		100mW (D)		
Modulations-Verfahren	BPSK	BPSK / QPSK	BPSK / QPSK / QAM16 / QAM64	BPSK / QPSK / QAM16 / QAM64	BPSK / QPSK / QAM16 / QAM64	BPSK / QPSK / QAM16 / QAM64	BPSK / QPSK / QAM16 / QAM64 / QAM256	BPSK / QPSK / QAM16 / QAM64 / QAM256 / QAM1024	BPSK / QPSK / QAM16 / QAM64 / QAM256 / QAM1024	BPSK / QPSK / QAM16 / QAM64 / QAM256 / QAM4096
Multiplex-Verfahren	FHSS DSSS	HR-DSSS	OFDM	OFDM	OFDM	OFDM	OFDM	OFDMA	OFDMA	
Max. Datenrate bei 1 SS und 20MHz [Mbit/s]	1	11	54	54	54	75	87	144		
Max. Datenrate bei 2 SS und 20MHz [Mbit/s]	./.	./.	./.	./.	./.	144,4	173,3	286,8		
Max. Datenrate bei 2 SS und 40MHz [Mbit/s]	./.	./.	./.	./.	./.	300	400	573,5		
Max. Datenrate bei 2 SS und 80MHz [Mbit/s]	./.	./.	./.	./.	./.	./.	867	1201		
Max. Datenrate bei 2 SS und 160MHz [Mbit/s]	./.	./.	./.	./.	./.	./.	1733	2402		
Maximale Anz. Spatial Streams	1	1	1	1	1	4	8	8	8	8
MIMO	SU-SISO	SU-SISO	SU-SISO	SU-SISO	SU-SISO	SU-MIMO	DL-MU-MIMO	UL/DL-MU-MIMO	UL/DL-MU-MIMO	UL/DL-MU-MIMO

5.5 - Zusätzliche Entwicklungen für den IEEE-802.11-Standard

Zusätzlich zu den Standards, welche die Datenraten festlegen, sind parallel noch unterstützende Erweiterungen implementiert worden.

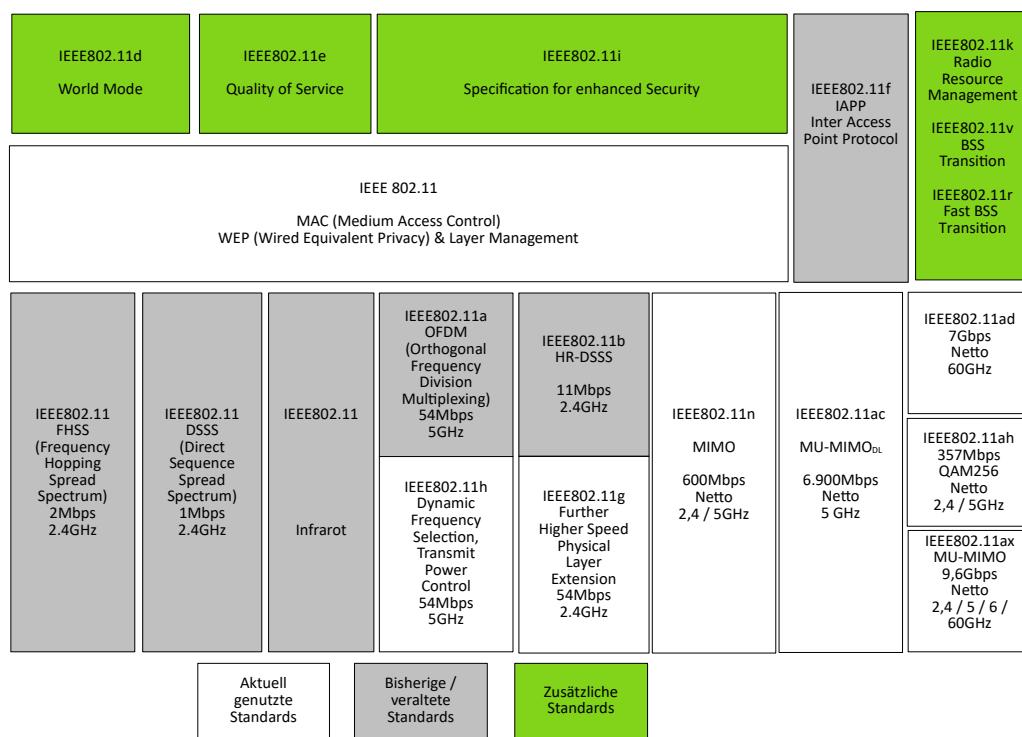


Abbildung 148:
IEEE-802.11 -
Übersicht

Mittlerweile sind auf der PHY-Ebene diverse Standards aus dem Verkehr gezogen worden. Neue Standards haben deren Funktion übernommen und verbessert. Zusätzlich sind noch diverse Hilfs-Standards hinzugekommen.

Darin werden vor allem die folgenden Themen abgehandelt:

- ➊ Regionale Unterschiede
- ➋ Quality of Service
- ➌ Security
- ➍ BSS-Übergang

5.5.1 - IEEE-802.11d

Um die Bearbeitung der regionalen Unterschiede zu vereinfachen wurden mit dem Standard IEEE802.11d die Ländercodes eingeführt. Diese werden aus dem ISO 3166-alpha-2 abgeleitet. Die Ländercodes werden z. B. in den Beacon-Frames verwendet in denen die APs ihre BSS propagieren. Die Frequenzdomäne und deren Eigenschaften werden im Beacon-Frame über das 6 Byte große Informationselement ID 7 spezifiziert. Die ersten beiden Bytes enthalten den Country-Code

Tabelle 54: Ländercodes

Ländercode	Länderkennung	Land
44 45	DE	Deutschland
46 52	FR	Frankreich
49 54	IT	Italien
55 53	US	USA

Das nächste Byte legt die Umgebung festgelegt

Tabelle 55: Umgebungscode

Ländercode	Umgebung
20	offen und geschlossen
49	geschlossen
4F	offen

Über das folgende 1 Byte große Starting-Channel-Feld wird die erste zu nutzende Kanalnummer festgelegt.

Danach folgt mit dem 1 Byte großen Number-of-Channel-Feld die Anzahl der zu nutzenden Kanäle.

Als letztes gibt das 1 Byte große Max-TX-Power-Feld die maximale zulässige Sendeleistung in dBm an.

5.5.2 - IEEE-802.11e

Mit IEEE-802.11e wird auf MAC-Ebene Quality of Service (QoS) ermöglicht.

Stationen die QoS-fähig sind werden in diesem Zusammenhang QoS Stations (QSTAs) und APs mit dieser Fähigkeit werden QoS Access Points (QAPs) genannt. Damit werden Basic Service Sets die QoS unterstützen QBSS genannt. Dazu werden Frames in 4 Kategorien, die so genannten Access Categories (ACs), eingeteilt:

Tabelle 56: Zuordnung von AC-Index (ACI) zu ACs und deren Bedeutung

ACI	AC	Description
0	AC_BE	Best Effort
1	AC_BK	Background
2	AC_VI	Video
3	AC_VO	Voice

QoS beinhaltet, dass der Transport von Frames unterschiedlicher QoS-Klassen neu organisiert wird. Für den Zugriff auf das Medium wurde der Enhanced Distributed Channel Access (EDCA) eingerichtet. Dabei ist der Zugriff auf das Medium zwar immer noch verteilt, jedoch werden die Frames bevor sie auf das Medium gegeben werden nach QoS-Klassen gruppiert, um dann mehr oder weniger priorisiert gesendet zu werden. Dafür verantwortlich ist die EDCA-Function (EDCAF). Die Verwaltung erfolgt in den EDCA-Parameter Set Elementen.

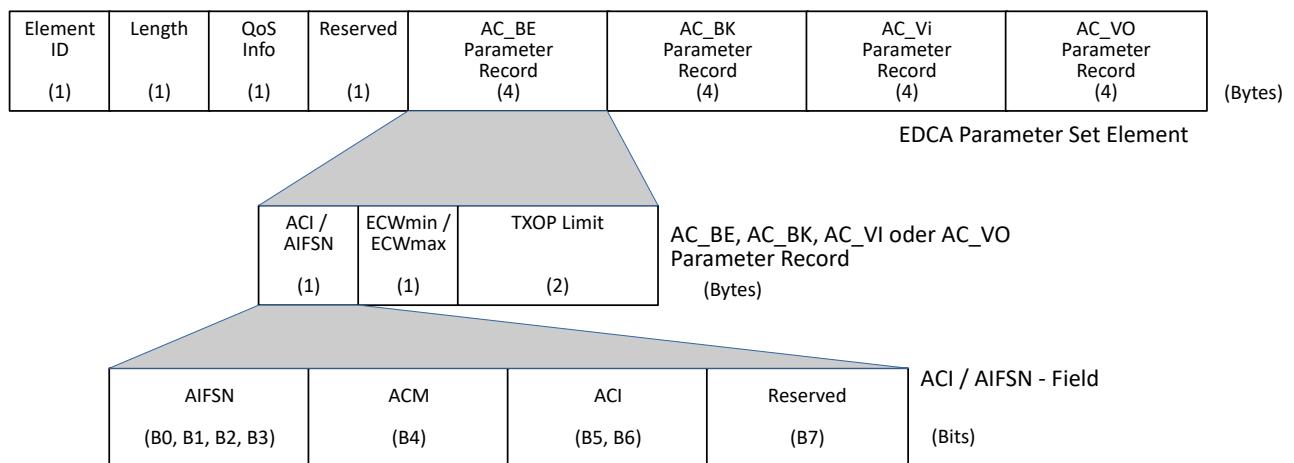


Abbildung 149: EDCA Parameter Set Element

Die ACs werden 8 User Priorities (UPs) zugeordnet.

Tabelle 57: Zuordnung von User Priority zu Access Category

Priority	User Priority (UP)	Access Category (AC)	Designation
Lowest	1	AC_BK	Background
	2	AC_BK	Background
	0	AC_BE	Best Effort
	3	AC_BE	Best Effort
	4	AC_VI	Video
	5	AC_VI	Video
	6	AC_VO	Voice
Highest	7	SC_VO	voice

Während der CP-Phase erhält jede AC für eine bestimmte Dauer eine Zugriffsberechtigung auf das Übertragungsmedium die Transmission Opportunity (TXOP) bezeichnet wird. Eine TXOP wird durch eine Anfangszeit und Dauer zeitlich begrenzt.

Für die Access Categories werden Warteschlangen bereitgestellt, in die die Frames eingesortiert werden. Für jede AC wird ein eigenständiger Backoff-Algorithmus bereitgestellt. Der IFS wird mit Arbitration Inter Frame Space (AIFS) bezeichnet.

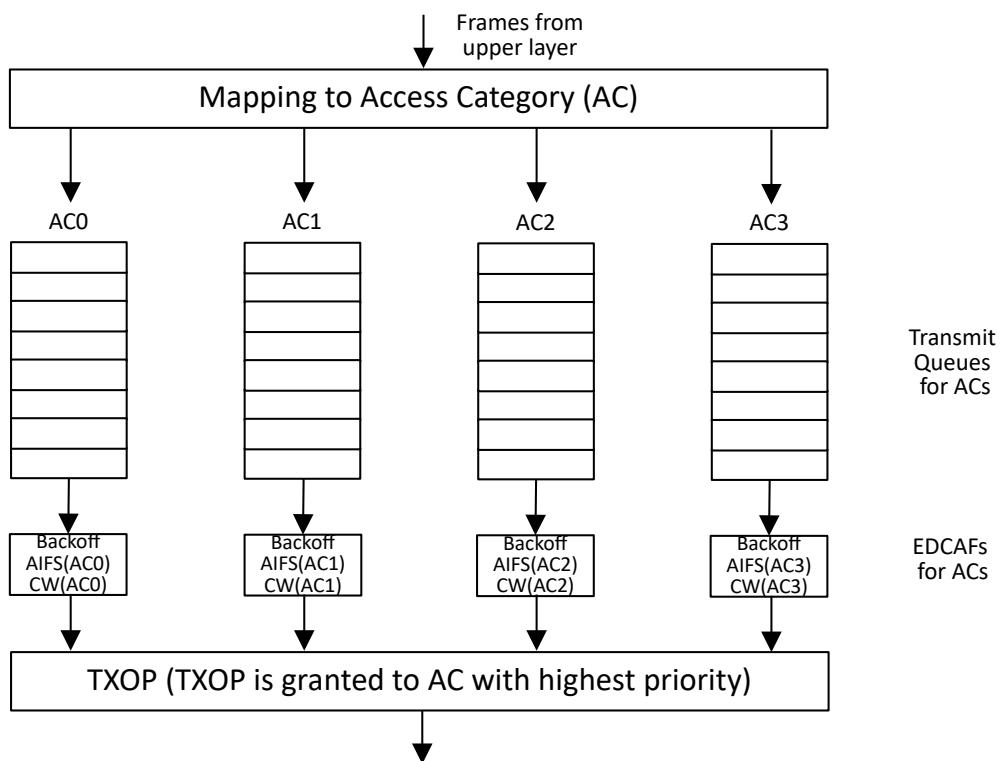


Abbildung 150: Umsetzung der Access Categories mit Warteschlangen

Den Backoffzeiten, und damit den unterschiedlichen Prioritäten, werden unterschiedliche CW zugeordnet. Die Backoff-Zeiten werden aus dem Intervall zwischen CWmin und CWmax ermittelt. War CWmin bisher bei 10 (802.11a/g) und 15 (802.11b) festgelegt, stehen mit 802.11e Werte von 0 bis 255 zur Verfügung. Der Wert von CWmax liegt zwischen CWmin und 1023.

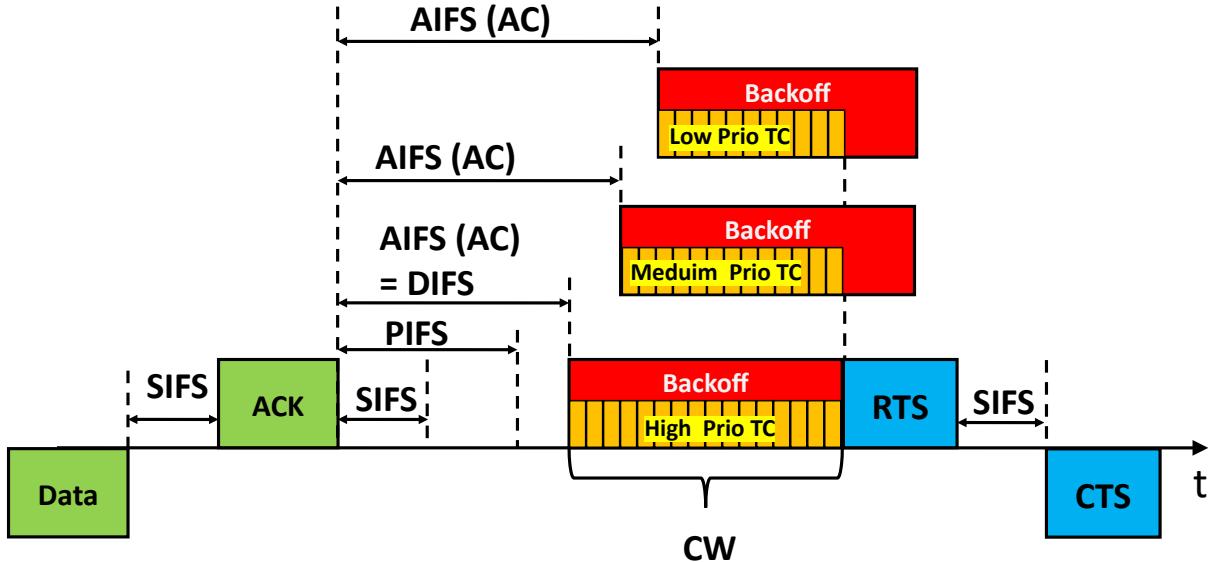


Abbildung 151: Medium-Zugriff der Access Classes

Ein AC mit der höchsten Priorität wird mit dem AIFS = DIFS. Ein AC mit einer niedrigen Priorität wird eine größere AIFS bekommen und damit später den Zugang zum Contention Window (CW).

Das bedeutet eine Abkehr vom Prinzip der Gleichberechtigung aller Stationen. Alle Stationen und der AP muss diese Technik unterstützen. Es wird ein Master/Slave-Schema eingeführt, bei dem die Kanalvorgabe dem AP obliegt.

Gleichzeitig bedeutet das auch eine Fortsetzung der VLAN-Technologie auf die Luftschnittstelle.

Vermischte Strukturen sind bei QoS nicht möglich! Siehe auch [IEEE-802.11-2016]

5.5.3 - IEEE-802.11f

Innerhalb eines großen drahtlosen Netzwerkes konnte eine Mobile Station ihren Standort über die Reichweite eines einzelnen Access Points (APs) hinaus nicht verändern.

Im Jahre 2003 wurde das Inter Access Point Protocol (IAPP) als Empfehlung verabschiedet, da es im IEEE-802.11-Standard nicht spezifiziert worden war. Der Standard soll ein standardisiertes schnelleres Handover zwischen AP's möglich machen. 2006 wurde der Standard wieder zurückgezogen.

Der übernehmende AP informiert per Multicast den ehemals bedienenden Access Point mit einem Handover Request. Der ehemalige AP, löscht daraufhin die Station aus seiner Stationstabelle.

Der neue Access Point übermittelt diese Information mit der Quell-MAC-Adresse der Station, sodass im LAN vorhandene Switches den neuen Leitweg erfahren und ihre Zuordnungstabelle aktualisieren können.

5.5.4 - IEEE-802.11i

Ursprünglich hatte IEEE-802.11 nur eine so genannte Wired Equivalent Privacy (WEP) vorgesehen. Damit sollte eine gleichwertige Sicherheit wie bei den kabelgebundenen LANs geschaffen werden. Leider nutzt WEP nur einen leicht zu ermittelnden Schlüssel, der auf allen Stationen einzusetzen ist. Siehe hierzu auch das Kapitel Sicherheit. Damit ergab sich vor allem im professionellen Umfeld keine Akzeptanz.

Zur Verbesserung der Sicherheit und somit der Akzeptanz wurde die Sicherheitsarchitektur WPA (Wi-Fi Protected Access) von der Wi-Fi Alliance (3Com, Cisco und RSA im Wesentlichen) entwickelt.

Die folgenden Anforderungen haben eine zentrale Bedeutung:

- Die Pakete müssen sowohl verschlüsselt, als auch authentifiziert sein
- Ein Schlüssel wird nur für ein einziges Paket benutzt
- Die Pakete müssen eine unveränderbare Sequenznummer tragen
- Die Kommunikationspartner müssen sich gegenseitig authentifizieren

Zusätzlich soll das neue Verfahren zu den bisherigen Verfahren abwärts kompatibel sein. Da dies nicht so einfach möglich ist, wurden 2 Verfahren festgelegt.

Die abwärts kompatible Lösung wurde mit dem Temporal-Key-Integrity-Protocol (TKIP) realisiert. Dabei sind die folgenden 4 Merkmale wichtig:

- Re-Keying. Dabei wird der Schlüssel automatisch so schnell/oft gewechselt, dass einem Angreifer nicht genügend Zeit bleibt, genügend Daten zu sammeln, um den Schlüssel zu ermitteln.
- Die Schlüssel-Information soll bei unterschiedlichen Datenpaketen an unterschiedlichen Stellen stehen. Dieses Verfahren wird auch Per-Paket-Mixing genannt.
- Die Reihenfolge der Datenpakete soll ständig vertauschbar sein. Dieses Verfahren wird Re-Sequencing genannt.
- Mit dem MIC (Message-Integrity-Check) – Verfahren soll verhindert werden, dass die Daten zwischen Sender und Empfänger manipuliert werden können.

Zusätzlich soll die Authentifizierung nach IEEE-802.1x, das von Microsoft entwickelt wurde, für eine sichere Kommunikation sorgen. Dafür wurde das EAP (Extensible Authentication Protocol) für eine zentrale Authentifizierung mit z. B. einem RADIUS-Server festgelegt.

Durch die Einführung von WPA2 wurde IEEE-802.11i vollständig übernommen. Das sieht auch den Einsatz einer Verschlüsselung nach dem AES (Advanced Encryption Standard) vor. Näheres zur Umsetzung der Forderungen siehe im Kapitel Sicherheit.

5.5.5 - IEEE-802.11k-v-r

Mit diesem Paket von Standards wurde unter anderem erreicht, dass der Wechsel einer Station von einem AP zu einem anderen AP optimiert von statten geht. Man spricht hierbei auch von einem Seamless Roaming.

5.5.5.1 - IEEE-802.11k

Mit dem Radio Ressource Management wurde erreicht, dass ein AP die Verbindungen zu den Stationen überwacht. Dabei wird überprüft, ob das Signal einer Station sich verändert. Schwächt es sich ab, wird davon ausgegangen, dass die Station sich entfernt. Fällt das Signal zu Rausch-Verhältnis unter einen Schwellwert wird davon ausgegangen, dass sich die Station vom AP entfernt und sich eventuell mit einem anderen AP verbinden sollte.

Damit kann ein AP den Anstoß für eine Station geben um sich mit einem anderen AP zu verbinden. Normalerweise geht der Anstoß zum AP-Wechsel immer von der Station aus.

5.5.5.2 - IEEE-802.11v

Mit diesem Standard wurden die folgenden Themen optimiert:

- ➊ BSS Transition-Verwaltung
- ➋ Disassociation imminent
- ➌ Directes Multicast Service (DMS)
- ➍ BSS-Max-Idle-Service

Bei der BSS Transition-Verwaltung geht es darum, dass die APs Informationen zu ihrer Nachbarschaft sammeln. Die Auslastung der APs ist darin genauso hinterlegt wie die nutzbaren Kanäle.

Erkennt ein AP über das in IEEE802.11k beschriebene Radio Ressource Management dass eine Station sich mit einem anderen AP verbinden sollte, informiert sie die Station über ein Disassociation imminent, also eine bevorstehende Abmeldung. Diese Information nutzt eine Station um beim AP eine Liste mit den Stationen in der Umgebung anzufordern. Die Liste wird vom AP an die Station gesendet. Darin ist auch vermerkt, wie es mit der Auslastung der APs aussieht. Mit dieser Information kann die Station sich mit dem optimalen AP verbinden.

Mit dem Direct Multicast Service wurde die Behandlung von Multicasts verbessert.

Der BSS-Max-Idle-Service wurde die Schlafenszeit der Stationen optimiert. Dies dient vor allem der Verlängerung der Akku-Laufzeit von Stationen.

5.5.5.3 - IEEE-802.11r

Im Jahre 2008 wurde dieser auch als Fast-BSS-Transition (FT) bekannte Standard verabschiedet, der ein schnelles Roaming ermöglichen soll.

Grundlage ist ein schnelles Authentifizierungsverfahren, das nicht mit IEEE-802.11i (WPA2) kollidiert. Der Übergang einer Station von einem AP zu einem anderen muss dabei unter 50ms erfolgen, um z. B. Beeinträchtigungen bei der Sprachübertragung mittels Voice over IP (VoIP) zu vermeiden.

5.6 - Betrieb von IEEE-802.11

Im Folgenden sollen die Aktivitäten im Zusammenhang mit dem normalen Betrieb von WLANs dargestellt werden. Die Steuerung des Betriebs erfolgt mit Management-Frames:

- ➊ Beacon-Frames
- ➋ Probe-Request-Frame
- ➌ Probe-Response-Frame
- ➍ Authentication-Frame
- ➎ Deauthentication-Frame
- ➏ Association-Request-Frame
- ➐ Association-Response-Frame
- ➑ Reassociation-Request-Frame
- ➒ Reassociation-Response-Frame
- ➓ Disassociation-Request-Frame
- ➔ Disassociation-Response-Frame
- ➕ Announcement-Traffic-Indication-Frame

Mit den Beacon-Frames werden die BSS-Parameter den Stationen mitgeteilt und Steuerungsfunktionen wahrgenommen (z. B. Zeitsynchronisierung)

Probe-Request-Frames und Probe-Response-Frames dienen der Verbindungsaufnahme zu anderen Stationen oder APs.

Sobald die Kommunikationspartner gefunden wurden, muss eine Authentifizierung stattfinden. Dazu dienen die Authentication- und Deauthentication-Frames.

Nachdem sich die Kommunikationspartner gegenseitig vertrauen müssen die Verbindungen noch etabliert, also assoziiert werden. Dazu dienen die Association-Frames mit ihren unterschiedlichen Ausprägungen.

Announcement-Traffic-Indication-Frames werden z. B. von APs dazu benutzt um mitzuteilen, dass ein Kanalwechsel stattfinden wird.

5.6.1 - Beacon-Frames

Das Kennzeichen einer WLAN-Funkzelle sind die Geräte, die über Funk miteinander in Kontakt treten. Dazu gehört, dass von einer zentralen Station zyklisch Beacon-Frames gesendet werden. Bei Infrastruktur-BSSs ist das ein Access Point (AP) und bei IBSSs sind das ausgewählte Stationen.

Das Beacon-Intervall wird in jedem Beacon-Frame in TU-Einheiten (Time Unit = TU) propagiert. Eine TU entspricht 1024µs. Ein typischer Wert für ein Beacon-Intervall ist 100 was 102,4ms entspricht. Damit wird etwa 10 mal in der Sekunde ein Beacon-Frame gesendet.

Die genaue Synchronisation der Zeit ist für die Einhaltung der Prozesse in einem WLAN extrem wichtig um einen reibungslosen Ablauf zu ermöglichen. In den Stationen wird die Zeit über die Time Synchronisation Function (TSF) vom Timestamp-Feld im Beacon-Frame abgeleitet.

Der Startzeitpunkt eines Beacon-Intervalls wird als Target Beacon Transmission Time (TBTT) bezeichnet. Er wird von der TSF vom Timestamp-Feld abgeleitet. Innerhalb des Beacon-Intervalls ist das der Zeitpunkt 0. Von da an werden die Beacon-Frames im Abstand des Beacon-Intervalls gesendet. Auch diese Zeitpunkte werden TBTT genannt.

Sollte das Medium zu Zeitpunkt des Aussendens eines Beacon-Intervalls belegt sein, wird das Beacon-Frame verzögert ausgesendet sobald das Medium wieder frei ist.

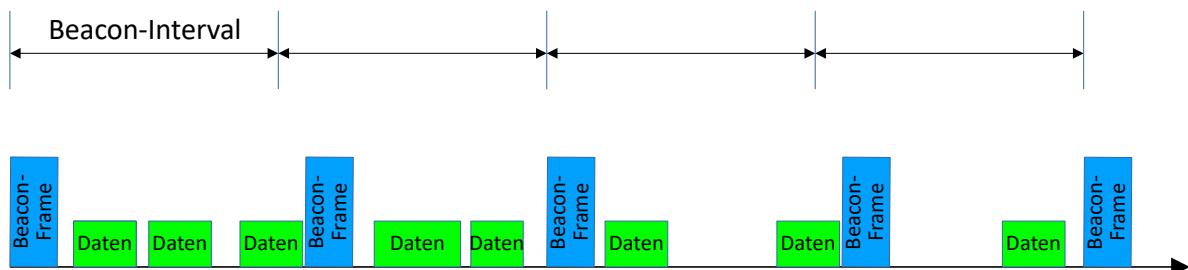


Abbildung 152: Beacon-Intervall teilweise belegt

In der Fassung des IEEE-802.11-standards von 2016 kann ein Beacon-Frame bis zu 68 Felder haben. Dabei gibt es feste Bestandteile und so genannte Informations-Elemente (IE). Je nach Konfiguration der WLAN-Umgebung können die Informations-Elemente eines Parameter-Sets zum Beacon-Frame hinzukommen. Die Informationselemente bestehen aus einer ein Byte langen Element-ID, einer ein Byte langen Längeninformation und aus einem bis zu 255 Byte langen variablen Informationsteil.

Tabelle 58: Ausgewählte Element-IDs und deren Bedeutung

Element-ID	Bezeichnung	Länge des Informations-teils [Bytes]	Bedeutung
0	0	0	0
1	Supported Rates	0	In den bis zu 8 Bytes kann jeweils ein Wert für eine unterstützte Datenübertragungsrate angegeben werden. Die angegebenen Werte sind mit 500kBit/s zu multiplizieren. Es ist zwischen Übertragungsraten zu unterscheiden die unterstützt werden müssen (MSB = 1; z. B. 2MBit/s = 0x84) und denen die optional sind (MSB = 0; z. B. 2MBit/s = 0x04).
2	0	3	Im Frequency-Hopping-Parameterset werden die Parameter: -Dwell Time (Dauer der Kanalbelegung bis zum nächsten Wechsel) -Hop-Set (Welches der 3 Hopping-Sets wird verwendet) -Hop-Pattern (Hopping Set aus dem Hopping-Muster wird verwendet) -Hop-Index (Damit wird der derzeit verwendete Kanalindex angegeben)
3	0	1	0
4	0	5	Im Contention-Free-Parameterset stehen folgende Parameter: -CFP Count (Zeit bis zur nächsten CFP angegeben) -CFPPeriod (Dauer der CFP-Intervalle) -CFPMaxDuration(Gibt die Maximale Dauer der CFP-Intervalle an) -CFP DurRemaining
5	0	0	Mit diesen Parametern können die Stationen die NAV-Werte setzen Die Traffic Indication Map dient im Power-Safe-Modus den APs dazu mitzuteilen für welche Stationen er Informationen zwischengespeichert hat. -DTIM-Count (Anzahl der Beacon-Frames (einschließlich diesem) bis zum nächsten DTIM) -DTIM-Period (Anzahl der Beacon-Intervalle bis nächste DTIM eintritt) -Bitmap-Control (Angabe ob Broadcasts oder Multicast im AP gespeichert sind) -Partial Virtual Bitmap (Angabe der Stationen für die Informationen gespeichert sind)
6	IBSS-Parameter	2	Informationen zum ATIM-Window im Ad-hoc-Modus (IBSS) Enthält die Zeitspanne, in der alle Stationen im aktiven Modus sein müssen, um Management-Frames zu empfangen.
7	0	6	Die Länder-Kennung enthält: -Country-Code (2 Byte Länderkennung nach ISO 3166-alpha-2 Ländercode; z. B. 0x4445 = DE = Deutschland) -Environment -Starting-Channel -Number-of-Channel -Max-TX-Power (Maximal zulässige Sendeleistung) Die Stationen können sich anhand dieser Informationen mit ihren Kanälen und Sendeleistungen einstellen
8	Power Constraint	1	Der Local-Power-Constraint Wert in dB definiert die Sendeleistung um die die Sendeleistung wegen TPC zu reduzieren ist
9	Channel Switch Announcement	3	Mit der Kanalwechsel-Anzeige kann ein AP (oder eine Station innerhalb eines IBSS) auf einen bevorstehenden Kanalwechsel hinweisen Channel-Switch-Mode (1 = Stationen dürfen bis zum Kanalwechsel keine weiteren Frames mehr senden) New-Channel-Number (Neuer Kanal in den übergegangen wird) Channel-Switch-Count (Anzahl der Target Beacon Transmission Times (TBTT) bis zum Kanalwechsel entspricht Zeitdauer bis zum Kanalwechsel. Ist der Wert = 0 dann erfolgt der Kanalwechsel unmittelbar)

Element-ID	Bezeichnung	Länge des Informations-teils [Bytes]	Bedeutung
10	0	4	Dient zur Spezifikation eines Zeitraums, in dem auf dem Kanal nicht gesendet werden darf. Felder: Quiet-Count: Anzahl der TBTTs bis zu dem Beacon-Intervall an dem die Senderuhe eintreten soll Quiet-Period: Anzahl der Beacon-Intervalle mit dem die sende-Verbotszeit beginnt Quiet Duration: Dauer der sendungsfreien Zeit Quiet-Offset: Zusätzliche Offset Zeit (in TU-Einheiten) über das Quiet-Count-Feld
11	0	9	0
13	ERP-Information	1	Hiermit kann angezeigt werden, dass sich innerhalb einer BSS Non-ERP-Stationen befinden, welche die erhöhten Datenraten ab 6MBit/s nicht unterstützen.
14	Extended Supported Rates	0	0
15	0	0	0

Im Anhang ist die komplette Liste zu finden.

5.6.2 - Verbindungsvorgang

Um Teilnehmer an einer Zelle zu werden muss man mit ihr in Verbindung treten. Dazu muss man erst einmal herausfinden, wo, also in welchen Frequenzband die Zelle agiert.

Um einen Station an ein WLAN anzubinden sind drei Phasen zu durchlaufen:

- Scanning
- Authentifizierung
- Assoziation

5.6.2.1 - Scanning

Angestoßen durch einen MLME-SCAN.request Primitiv versucht eine Station eine Verbindung zu einem AP aufzubauen. Sehe hierzu auch Abbildung 40. Die WLAN-Station muss dazu alle möglichen Kanäle durchsuchen. Es gibt Hersteller, die die Kanäle 1, 7 und 13 zur beschleunigten Suche bevorzugen. Bei der Kanalsuche wird die an der Station lokal definierte SSID mit der SSID der sendenden APs verglichen. Das Ergebnis des Scan-Vorgangs wird, in Form einer Liste der gefundenen APs, im MLME-SCAN.confirm Primitiv mitgeteilt.

Beim Scanning-Vorgang unterscheidet IEEE-802.11 zwei Methoden:

5.6.2.1.1.1 - Passive Scanning

Der AP sendet periodisch Beacon-Frames aus. Darin teilt er die Eigenschaften der Funkzelle mit. Man spricht dann von einem „Open System“.

Damit muss eine Station in jedem Kanal nur lange genug auf einen Beacon-Frame warten, um herauszufinden auf welchen Kanälen ein AP agiert. Die Wartezeiten werden durch MinChannelTime (typisch ist hier ein Wert von 200) und MaxChannelTime (hier ist ein Wert von 250 typisch). Mit den typischen Werten ergibt sich eine Zeitspanne von 204,8ms bis 256ms. Da ein Beacon-Frame normalerweise mit einem Beacon-Intervall von 200 gesendet wird, sollte eine Station jeden Kanal bis maximal MaxChannelTime abhören. Sollte ein AP auf dem Kanal arbeiten, kann er somit sicher erkannt werden, auch wenn der Beacon-Frame wegen einer aktuellen Kanalbelegung etwas verzögert gesendet wird.

Welche Kanäle abgehört werden, wird mit einer ChannelList, die vom PHY-Typ abhängig ist, festgelegt. Diese Liste ist auch von der ortsabhängigen Aufteilung des Frequenzbandes abhängig. In Deutschland sind z. B. für die DSSS-PHY 13 Kanäle im 2,4GHz-Band festgelegt.

Empfängt eine Station auf mehreren Kanälen einen Beacon-Frame, wird sie den mit dem stärksten Empfangssignal (SNR) auswählen.

5.6.2.1.1.2 - Active Scanning

Es gibt auf APs die Möglichkeit, das Senden der SSID in einem Beacon-Frame zu unterdrücken. Man spricht dann von einem „Closed System“. Dann kann eine Station einen empfangenen Beacon-Frame nicht interpretieren und muss selbst aktiv werden.

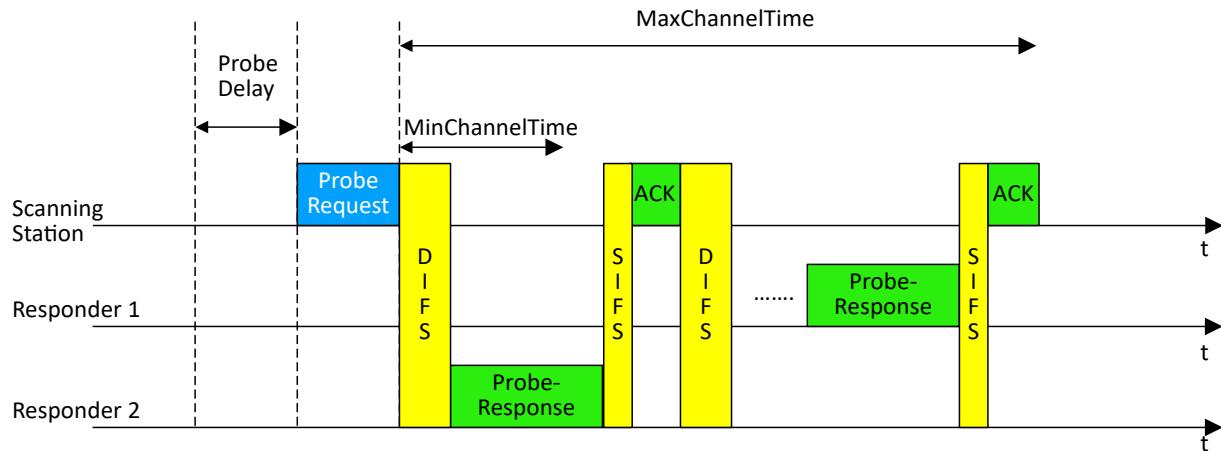


Abbildung 153: Probe-Request und -Response

Der Reihe nach wird jeder Kanal aus der ChannelList abgearbeitet. Um zu vermeiden, dass mehrere Stationen gleichzeitig einen Probe-Request senden und dadurch einen Kanal blockieren warten die Stationen eine kurze Wartezeit, die ProbeDelay genannt wird, ab. Danach sendet die Station einen Probe-Request-Frame aus und initialisiert einen Timer.

Im Probe-Request-Frame überträgt die Station die SSID, mit der sie sich verbinden möchte. Läuft der Timer vor der Zeit MinChannelTime ab und es ist keine PHY-CCA.indication (Busy) eingetroffen, wird mit dem nächsten Kanal weiter gemacht, denn bis dahin hätte sich ein AP melden müssen. Wurde allerdings ein Probe-Response-Frame empfangen, wird bis zum Ablauf von MaxChannelTime gewartet, denn es könnten ja noch weitere APs auf dem Kanal arbeiten und sich zurückmelden.

Wurden beim Scan der Kanäle mehrere APs mit der gewünschten SSID gefunden, dann wird der AP mit dem besten Empfangssignal (SNR) ausgewählt.

Sollte eine Station keinen AP finden, kann sie selbst eine IBSS aufbauen. Dazu verwendet sie den MLME-START.request Primitiv.

5.6.2.2 - Authentifizierung

5.6.2.2.1 - Stati

Eine Authentifizierung findet immer zwischen Peers , also gleichberechtigten Stationen statt. Davon kann eine Station natürlich ein AP sein. Eine Authentifizierung von Gruppen ist nicht gestattet. Nachdem eine Station gefunden wurde, kann die Verbindung zu ihr mit einem MLME-JOIN.request hergestellt werden.

Zu Beginn ist einer Station im Status 1 (Unauthenticated / Unassociated). Nach einer erfolgreichen Authentifizierung hat die Station den Status 2 (Authenticated / Unassociated). Ist die Authentifizierung nicht erfolgreich bleibt die Station im Status 1. Eine Deauthentifizierung führt aus allen Stati zurück in den Status 1.

Falls Station A in einem Infrastruktur BSS einen Klasse-2- oder Klasse-3-Frame von einer nicht authentifizierten Station B (Z. B. Ist Station B im Status1) empfängt, ist der Frame zu verwerfen. Falls der Frame eine individual Adresse im Adress-1-Feld hat, soll die MLME von Station A einen Deauthentication-Frame an Station B senden .

Eine Authentifizierung ist in einem IBSS optional. In einem Non-DMG-Infrastruktur-BSS ist eine Authentifizierung erforderlich. In einem DMG-Infrastruktur-BSS und PBSS wird die Open-system-Authentication nicht genutzt.

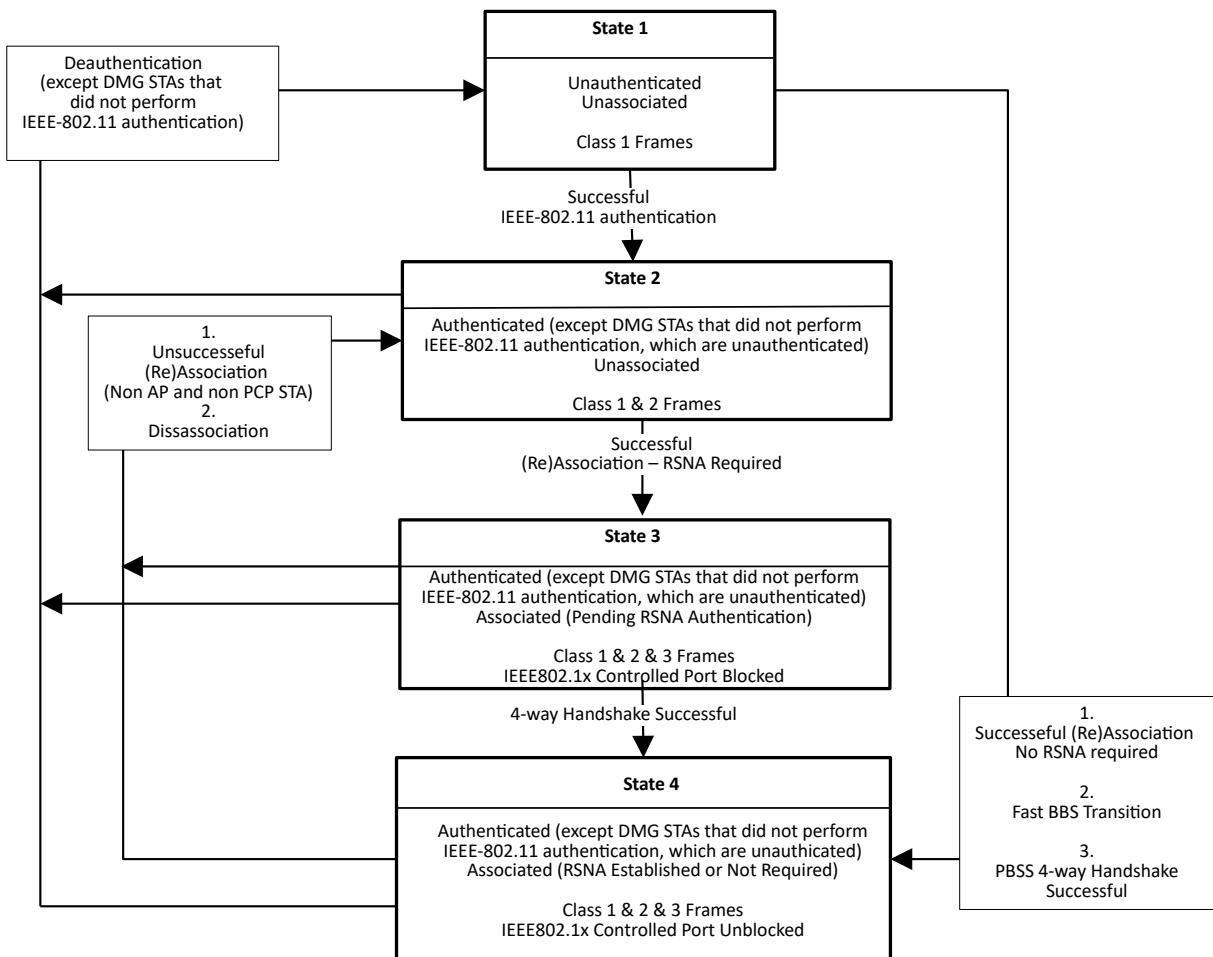


Abbildung 154: Beziehung von Status und Services zwischen Non-Mesh-Stationen

Der aktuelle Beziehungsstatus zwischen Empfänger und Sender von Frames entscheidet welcher Frametyp ausgetauscht werden kann. Die erlaubten Frametypen sind in Klassen gruppiert und den Status der Stationen zugeordnet.

Tabelle 59: Zuordnung von Status zu erlaubten Frame-Klassen

Status	Erlaubte Frame-Klasse
1	1
2	1 und 2
3 und 4	1, 2 und 3

Tabelle : Zuordnung von Frames und Frametypen zu Klassen

Klasse	Frame-Typ	Frame
1	1. Control-Frames	1. RTS 2. CTS 3. DMG Clear to Send (DMG CTS) 4. ACK 5. Grant 6. SSW 7. SSW-Feedback 8. SSW-Feedback 9. Grant ACK 10. CF-End + CF ACK 11. CF-End 12. In IBSS und in PBSS falls dot11RSNAActivated = false Block Ack 13. In IBSS und in PBSS falls dot11RSNAActivated = false Block Ack Request
	2. Management-Frames	1. Probe Request / Response 2. Beacon-Frame 3. Authentication 4. Deauthentication 5. ATIM 6. Public Action 7. Self-protected Action 8. In einem IBSS alle Action Frames und alle Action- und No Ack Frames 9. Unprotected DMG Action Frames 10. In einem DMG BSS Link Measurement Request und Link Measurement Report Frames 11. In einem PBSS falls dot11RSNAActivated = false alle Action- und No Ack Frames außer: - ADDTS Requests - ADDTS Response - DELTS
	3. Data-Frames	1. Data-Frames zwischen IBSS Stationen 2. Data-Frames zwischen Peers bei Nutzung von DLS 3. Daten-Frames innerhalb eines PBSS
	4. Extension-Frames	DMG Beacon
2	1. Management-Frames	1. Association Request / Response 2. Reassociation Request / Response 3. Disassociation
3	1. Data-Frames	1. Daten-Frames zwischen Stationen in einem Infrastruktur BSS oder in einem Mesh BSS (MBSS)
	2. Management-Frames	1. In einem Infrastruktur BSS, einem MBSS oder einem PBSS alle Action und Action No Ack Frames, außer solchen die zur Klasse 1 oder 2 gehören
	3. Control-Frames	1. PS-Poll 2. Poll 3. SPR 4. DMG DTS 5. Block Ack außer jenen die zu Klasse 1 gehören 6. Block Ack Request außer jenen die zu Klasse 1 gehören

5.6.2.2.2 - Ablauf

Die Station, welche die Authentifizierung anstößt nennt man Requester. Die angefragte Station nennt man Reaponder. Ein AP wird nie eine Authentifizierung anstoßen.

5.6.2.2.2.1 - Aus Sicht des Requesters

Nach dem Empfang eines MLME-AUTHENTICATE.request Primitiv authentifiziert sich eine Station bei der angezeigten Station nach der folgenden Vorgehensweise.

Erfolgt die Authentifizierung in einem IBSS, werden mittels eines MLME-DELETEKEYS.request die Keys PTKSA, GTKSA und IGTKSA gelöscht. Das sind die Verwaltungseinheiten für die Verschlüsselung von Daten.

Die eigentliche Authentifizierung erfolgt nach einer der beiden Vorgehensweisen:

- Open-System-Authentication
- Shared-Key-Authentication

Abweichende Bearbeitungsschritte sind bei einer Fast BSS Transition (FT) in einer ESS erforderlich.

Auch bei einer Simultaneous Authentication of Equals (SAE) in einer Infrastruktur BSS, IBSS oder MBSS ist eine abweichende Vorgehensweise durchzuführen.

War der Status vor der Authentifizierung auf 1 gesetzt, ist nach einer erfolgreichen Authentifizierung innerhalb des AuthenticationFailureTimeout der Status auf 2 zu setzen. War der Status vorher ungleich 1 bleibt die Station auf dem bisherigen Status. Die MLME erzeugt danach ein MLME-AUTHENTICATE.indication Primitiv um die SME über das Ergebnis zu informieren.

5.6.2.2.2.2 - Aus Sicht des Responders

Beim Empfang eines Authentication-Frame mit der Authentication-Transaction-Sequenznummer = 1 wird die Ziel-Station die anfragende Station mit der folgenden Prozedur Authentifizieren:

1. Informieren der SME über den Eingang einer Authentifizierungs-Anfrage mittels eines MLME-AUTHENTICATION.indication Primitiv
2. Falls eine FT Authentifizierung genutzt wurde werden zusätzlich die FT Authentifizierungs-Elemente informiert.
3. Falls eine SAE Authentifizierung genutzt wurde werden zusätzlich die SAE Authentifizierungs-Elemente informiert.
4. Ist die Station in einem IBSS und die Management-Frame-Protection wurde nicht ausgehandelt als die PTKSA(s) erstellt wurden löscht die SME mit einem MLME-DELETEKEYS.request Primitiv die PTKSA, GTKSA, IGTKSA und temporäre Schlüssel für die Kommunikation mit der Station.
5. War der Ergebnis-Code (Result-Code) nicht SUCCESS wird die MLME einen entsprechenden Authentication-Frame mit passendem Statuscode zurücksenden und den Status der Station nicht ändern.
6. War der Ergebnis-Code (Result-Code) SUCCESS wird die MLME einen entsprechenden Authentication-Frame mit dem Statuscode SUCCESS zurücksenden und den Status der Station auf 2 setzen falls er auf 1 war.

5.6.2.2.3 - Open-System-Authentifizierung

Die Open-System-Authentification ist der Default-Algoritmus für Pre-RSNA Stationen, denn diese Authentifizierung ist eine Null-Authentifizierung. Das bedeutet, sie ist immer erfolgreich.

Jede Nicht-DMG-Station, die eine Open-System-Authentifizierung anfragt, kann von der angefragten Station authentifiziert werden, sofern diese aktiviert ist. (Wenn dort in der Tabelle dot11AuthenticationAlgorithmsTable ein Eintrag mit openSystem und dot11AuthenticationAlgorithmActivatet = true existiert)

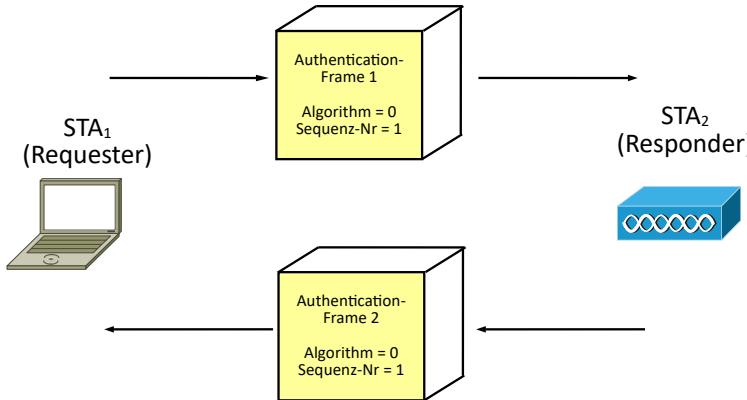


Abbildung 155: Open-System-Authentifikation

Die Authentifizierung besteht aus zwei Management-Frames vom Typ Authentication.

Die Station STA₁ möchte von der Station STA₂ authentifiziert werden. Damit ist STA₁ die anfragende Station (Requester) und STA₂ die angefragte Station (Responder).

Mit dem Erhalt eines MLME-AUTHENTICAT.request Primitiv erstellt der Requester einen Open-System-Authentification-Request (Authentication Algorithm Identification = 0 und Authentication Transaction Sequence Number = 1) und sendet ihn an den Responder.

Mit dem Eintreffen des Open-System-Authentification-Requests beim Responder ergibt sich folgender Ablauf:

1. Mit einem MLME-AUTHENTICATE.indication Primitiv wird die SME informiert, dass ein Authentication-Request eingetroffen ist.
2. Erstellung und Übertragung einer Antwort in einem Authentication-Frame. Bei einer positiven Antwort wird der zurückgegebene Wert auf „SUCCESS“ gesetzt.
3. Sind die entsprechenden Einträge auf der Responder-Seite nicht vorhanden darf der Wert für die Antwort nicht „SUCCESS“ sein.

Es findet nur eine administrative Anmeldung statt. Es ist kein gemeinsamer Schlüssel vorhanden.

5.6.2.2.4 - Shared-Key-Authentifizierung

Es werden 4 Management-Frames vom Typ Authentication ausgetauscht. In der folgenden Abbildung will eine Station sich beim Accesspoint (AP) authentifizieren.

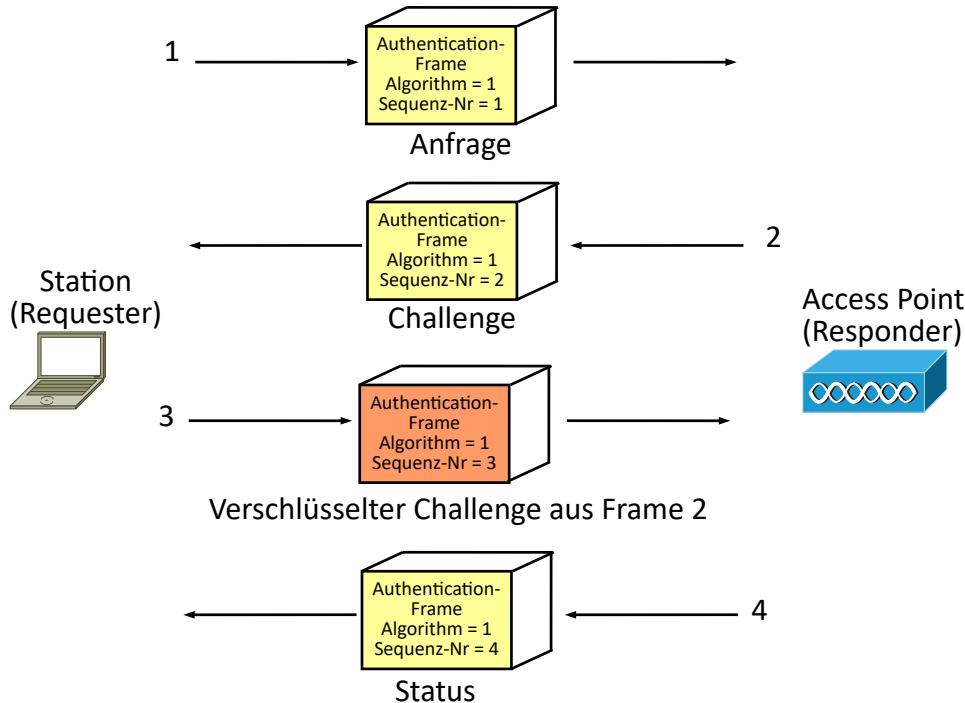


Abbildung 156: WLAN Shared-Key-Modus

In der Anfrage (1) erstellt die Station einen Authentication-Management-Fame mit folgendem Inhalt und sendet in an den AP:

- Algorithm-Identification = 1 (Shared-Key-Authentication)
- Authentication-Transaction-Sequence-Number = 1

Darauf hin erstellt der AP einen Authentication-Management-Fame mit folgendem Inhalt und sendet in an die Station (2):

- Algorithm-Identification = 1 (Shared-Key-Authentication)
- Authentication-Transaction-Sequence-Number = 2
- 128 Byte langer Challenge-Text mit zufälligem Inhalt

Die Station nimmt den erhaltenen Challenge-Text und generiert daraus eine Prüfsumme (ICV) und einen neuen Initialisierungs-Vektor (IV). Challenge-Texte und Prüfsumme werden mit dem WEP-Schlüssel verschlüsselt. Damit baut die Station einen Authentication-Management-Fame mit folgendem Inhalt und sendet in an den AP:

- Algorithm-Identification = 1 (Shared-Key-Authentication)
- Authentication-Transaction-Sequence-Number = 3
- Verschlüsselter Challenge-Text und Prüfsumme
- Initialisierungs-Vector

Der AP nimmt die verschlüsselten Daten (Challenge-Text und Prüfsumme) und entschlüsselt sie. Darauf hin wird der entschlüsselte Challenge-Text mit dem eigenen Challenge-Text verglichen. Bei Gleichheit kann der AP davon ausgehen, dass die Station über den selben WEP-Schlüssel verfügt wie er selbst. Damit kann die Authentifizierung der Station akzeptiert werden und der Zugriff auf das Netz für alle Klasse-2-Frame freigegeben.

Zum Schluss sendet der AP einen Authentication-Management-Fame mit folgenden Inhalt an die Station:

- Algorithm-Identification = 1 (Shared-Key-Authentication)
- Authentication-Transaction-Sequence-Number = 4
- Status Code = 0 (SUCCESS) oder Grund (siehe hierzu Anhang: Status-Codes)

Da diese Verschlüsselung kompromittierbar ist, sollte sie nicht verwendet werden. Es wird ein Klartext und das zugehörige Chiffrat ausgetauscht, dies ermöglicht es einem Angreifer die WEP-Verschlüsselung zu knacken. Es ist nur der zweite und der dritte Frame mitzulesen und der erste Eintrag im Schlüsselsequenz-Wörterbuch ist möglich, (siehe hierzu das Kapitel: Schlüsselsequenz-Wörterbuch).

Da ein Angreifer genau diese Authentisierung für sich selbst verwenden kann, ist diese Vorgehensweise katastrophal. Da die Wiederverwendung von Initialisierungsvektoren nicht verboten ist, kann dies beliebig oft weiter durchgeführt werden!

Die angewandte Authentifizierung ist nur einseitig, denn es wird nur eine Station von einer anderen oder einem AP authentifiziert. In der Gegenrichtung findet keine Authentifizierung statt. Dies ermöglicht es einem Angreifer bei der Authentifizierung als Man-in-the-Middle einem Client der sich anmelden will einen AP vorzugaukeln.

Ein weiterer Schwachpunkt dieser Authentifizierung ist, dass nur WLAN-Komponenten und nicht User authentifiziert werden können.

5.6.2.3 - Assoziation

Nach einer erfolgreichen Shared-Key- oder Open-System-Authentifizierung muss sich eine Station am Accesspoint assoziieren um eindeutig verwaltet werden zu können. Ohne eine Assozierung können keine Frames der Klasse 3 (also auch Daten) innerhalb einer Funkzelle ausgetauscht werden.

Dazu sendet die Station einen Association-Request-Frame an den AP, in dem sie ihre Parameter / Fähigkeiten mitteilt. Je nachdem, welche Fähigkeiten die Station unterstützt, sind die folgenden Elemente vorhanden, oder auch nicht:

- Supported Rates
- Extended Supported Rates
- Power Capability
- Supported Channels
- Robust Security Network (RSN)
- Quality of Service (QoS) Capability
- Radio Measurement (RM) Enabled Capabilities
- Mobility Domain
- Supported Operating Classes
- High Throughput (HT) Capabilities
- 20/40 BSS Coexistence
- Extended Capabilities
- QoS Traffic Capability
- TIM Broadcast Requests
- Interworking
- Multi-Band
- DMG Capabilities
- Multiple MAC-Sublayers
- VHT Capabilities
- Operating Mode Notification
- Vendor Specific

Als Antwort sendet der AP einen Association-Response-Frame an die Station zurück. Darin teilt sie ihrerseits ihre Fähigkeiten (also die obige Liste) und weitere Informationen mit:

- Statuscode = 0 (SUCCESS) oder Grund (siehe hierzu Anhang: Status-Codes)
- Association ID (AID)
- ...

War die Assozierung erfolgreich, quittiert die Station den Empfang des Association-Response-Frames mit einem ACK-Frame.

Am Ende schaltet der AP auch die Verbindung zum Distribution System (DS) für die Station frei. Damit können vom AP Frames der Klasse 3 für die Station transportiert werden.

5.6.2.4 - Reassoziation

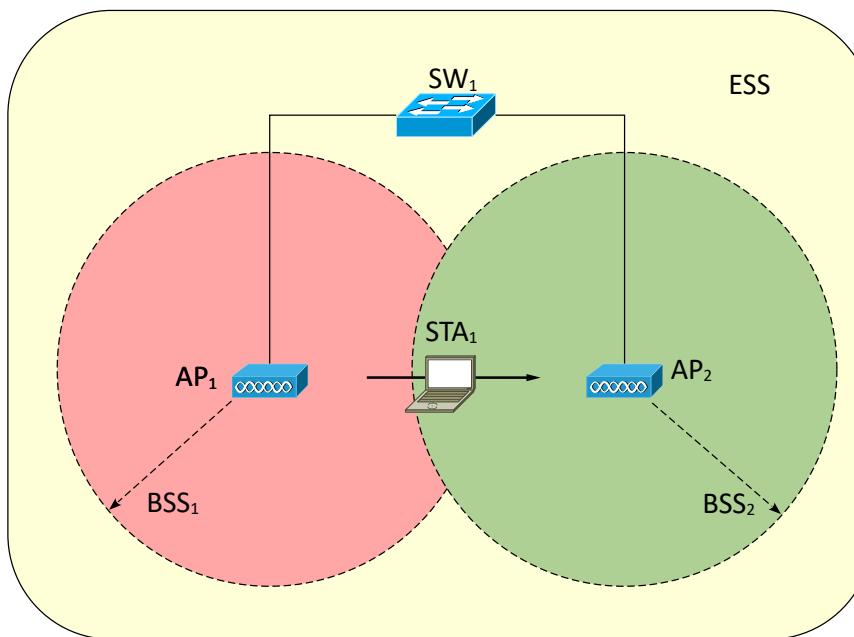


Abbildung 157: Reassozierung

STA₁ kann sich innerhalb der Funkzelle des AP₁ im BSS₁ frei bewegen.

Verlässt STA₁ die Funkzelle, kann sie sich mit einem anderen AP (hier AP₂) verbinden, falls BSS₁ mit der sie verbunden war, zu einem ESS gehört. Das ist in Abbildung 157 der Fall.

Dazu sendet die Station an den AP₂ einen Reassocation-Request-Frame (3). Darin ist die MAC-Adresse des letzten APs enthalten.

Der neue AP antwortet mit einem Reassocation-Response-Frame (4).

Falls der Status Code = „SUCCESS“ ist bekommt STA₁ ihre neue AID mitgeteilt unter der sie nun von AP₂ verwaltet wird.

Darauf hin sendet STA₁ einen ACK-Frame an den AP₂. AP₂ sendet am Ende noch die Information über die erfolgreiche Reassoziation an das Distribution System um alle APs über den neuen Zustand informieren. Dieser Frame wird Disassotiation-Frame genannt (5).

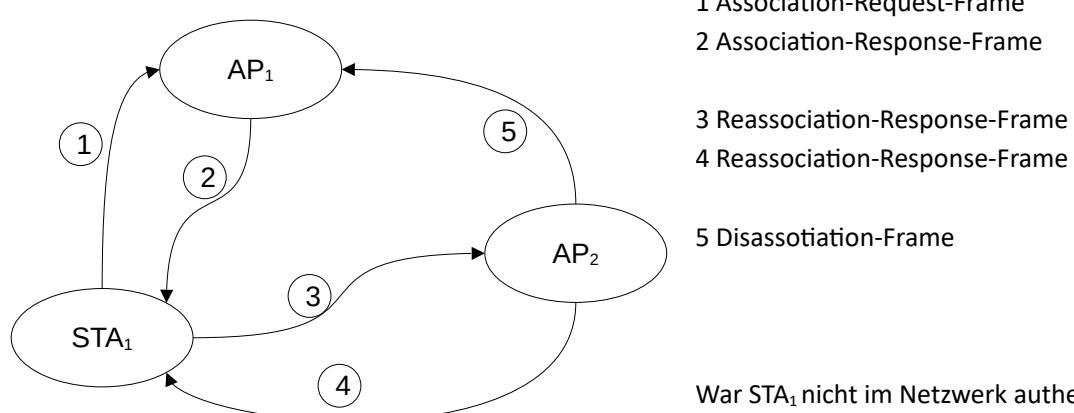


Abbildung 158: Assoziierung Reassozierung Disassozierung

War STA₁ nicht im Netzwerk authentifiziert beantwortet AP₂ den Reassocation-Request-Frame mit einem Deauthentication-Frame.

Der Ablehnungsgrund ist aus dem Reason-Code ersichtlich. Siehe hierzu auch Reason-Codes im Anhang.

5.6.3 - Dynamischer Schlüsselaustausch nach IEEE-802.1x

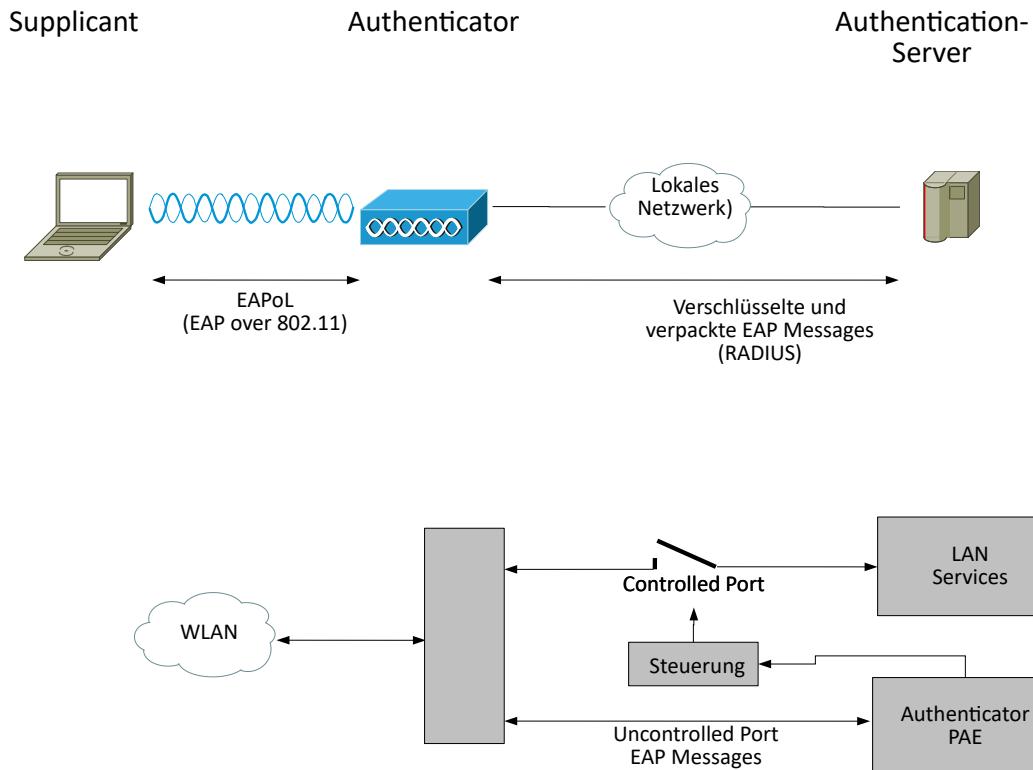


Abbildung 159: WLAN IEEE-802.1x

Der Standard wurde 2001 veröffentlicht. Das x steht für eine Unabhängigkeit von einer Topologie. Somit ist der Standard für Ethernet, Token Ring oder auch für WLANs verwendbar.

Über ein LAN wird ein Gerät (Authenticator), das den Port zur Verfügung stellt an einen Authentifizierungsserver angebunden.

Sobald nun ein weiteres Gerät im obigen Fall der Supplicant (deutsch: Bittsteller oder Station, die hereingelassen werden will) an das LAN über den Authenticator (deutsch: Wächter am Tor) an das WLAN angebunden werden will, ist zuerst der Authentisierungsprozess durchzuführen. Dazu wird das EAPoL (EAP over LAN) Protokoll verwendet. Der AP muss eine Kommunikationsbeziehung zum Authenticator-Server haben. Hier finden vermehrt RADIUS-Server Verwendung. Für die Kommunikation zwischen der Station und dem AP wird das EAP (Extensible Authentication Protocol) verwendet. EAP hat den Vorteil, dass es sich nicht auf einen bestimmten Authorisierungsalgorithmus festlegt und offen für Erweiterungen ist.

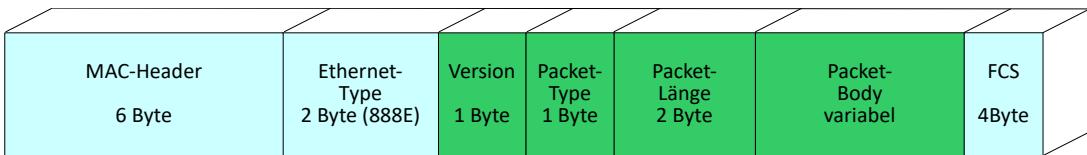


Abbildung 160: IEEE-802.1x (EAPoL)

- ➊ Type = 0 EAP-Paket das Body-Feld enthält den EAP-Frame
- ➋ Type = 1 EAPoL-Start
- ➌ Type = 2 EAPoL-Logoff
- ➍ Type = 3 EAPoL-Key, zur Schlüsselübermittlung
- ➎ Type = 4 EAPoL-Encapsulated-ASF-Alert, z. B. SNMP-Traps

Der AP kümmert sich nicht um den Authentisierungs-Prozess. Er verarbeitet keine unautorisierten Pakete, es sei denn Pakete, die zum Authentisierungsvorgang selbst gehören. Deshalb sendet er die empfangenen Anmelde-Informationen über eine gesicherte Verbindung an den Authentisierungsserver. Die Station kann in diesem Zustand keine Pakete in das LAN übermitteln. Erst wenn die Autorisierung erfolgreich abgeschlossen ist, kann mit den Basisdiensten wie DHCP oder DNS die Station an das LAN angebunden werden. Eine Verbindung zu anderen Stationen über den AP ist in diesem Zustand auch nicht möglich. Wenn eine erfolgreiche Assoziation im WLAN stattgefunden hat, kann man das mit einem Link-Up bei Ethernet vergleichen.

Diese Vorgehensweise bietet den Vorteil eine zentrale Benutzerverwaltung zu implementieren. Es ist evtl. nur an der Station oder am Authentisierungsserver eine Änderung vorzunehmen, wenn auf ein anderes Authentisierungsverfahren umgestellt werden soll.

Da EAP für eine Punkt zu Punkt-Verbindung entwickelt wurde, fehlt dem Protokoll eine Adressierung auf Ebene 2. Dies wird durch die Transportprotokolle EAPoL und RADIUS (Remote Authentication Dial In User Service) erledigt.

Da die Station anfänglich noch keine gültige IP-Adresse hat, wird die Kommunikation um den L2-Header (LLC) ergänzt und als MDSU ein EAPoL-Frame verwendet, der den EAP-Frame mit den Authentisierungsdaten kapselt.

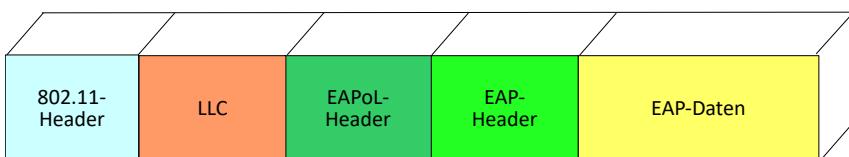


Abbildung 161: WLAN EAP-Stack

Die Kommunikation zwischen AP und Authentisierungsserver wird in der Regel ein Layer-3-Protokoll Verwendung finden, da der RADIUS-Server unter Umständen in einem gesonderten Netzwerk installiert ist. RADIUS verwendet UDP auf der Netzwerkschicht (Layer3) und ist im RFC 2865 beschrieben. Im RFC 2869 wurde dieses Protokoll um EAP erweitert. Im Prinzip ist es ein Client/Server-Protokoll und dient der zentralen Benutzerdatenverwaltung.

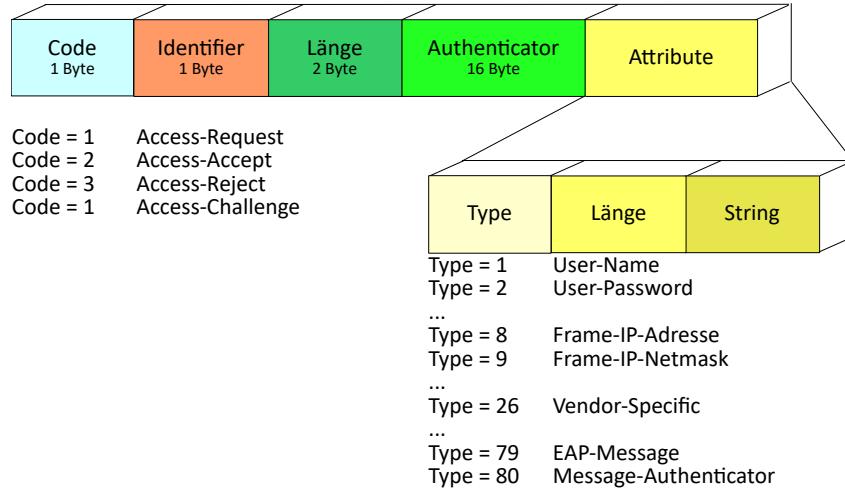


Abbildung 162: RADIUS-Frameformat

Die Station sendet zur Authentisierung einen EAPoL-Start-Frame.

Zusammen mit dem RADIUS-Server stellt der AP daraufhin weitere Anfragen, um die Verbindung schließlich mit einem EAP-Success-Frame zu etablieren. Mit einem EAPoL-Logoff-Frame beendet die Station die Kommunikationsbeziehung.

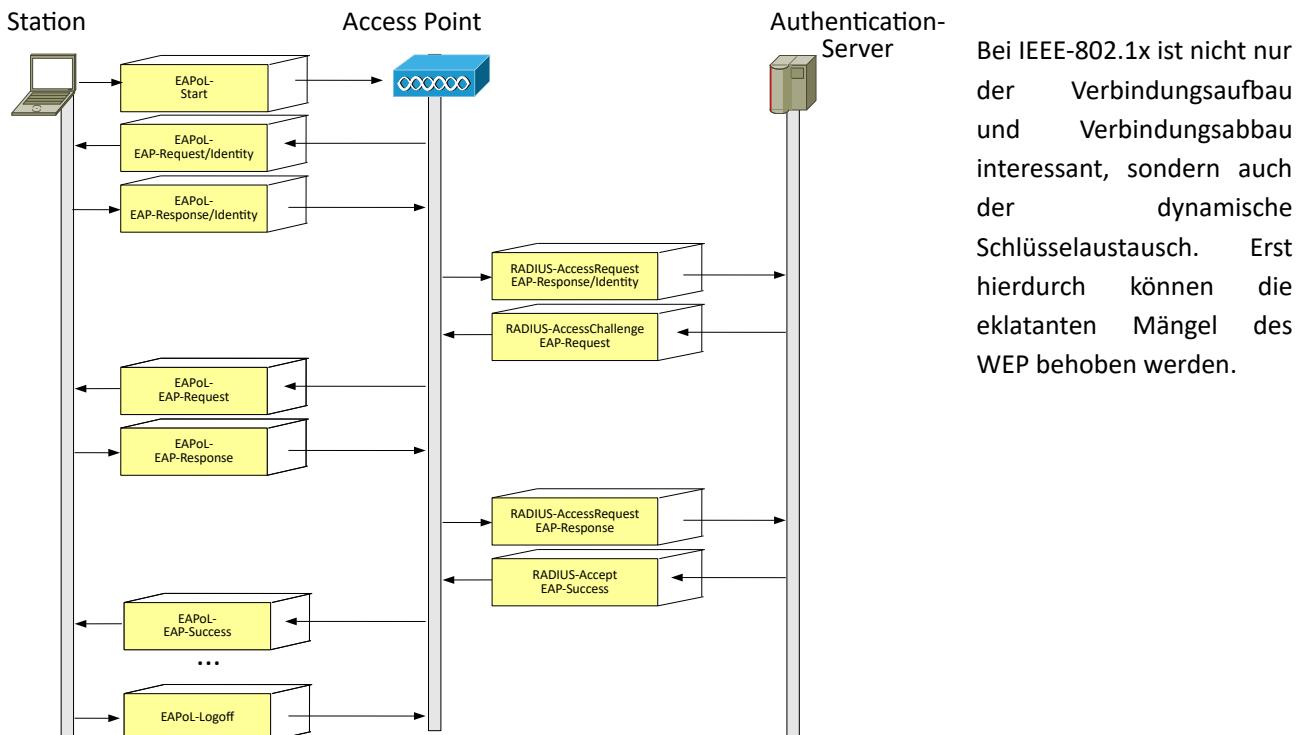


Abbildung 163: WLAN Authentisierung nach IEEE 802.1x

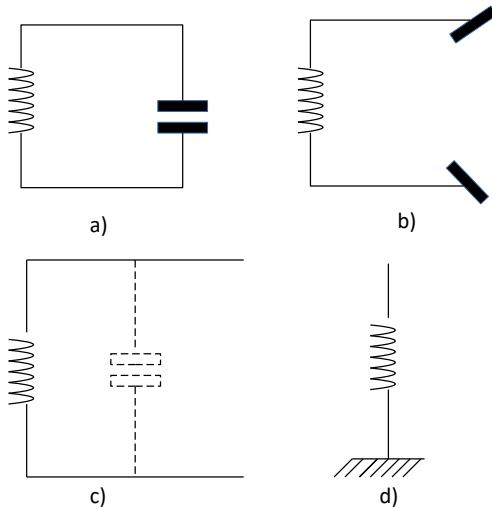
6 - WLAN-Antennen

6.1 - Allgemeines

Ein wesentliches Bauteil beim Aufbau von WLANs sind die Antennen. Je nach Bauform und ihrer Positionierung unterscheiden sie sich wesentlich in ihren Eigenschaften wie Reichweite oder Raum-Abdeckung.

6.2 - Einführung

Um Informationen über die Luft zu übertragen müssen auf der Senderseite die Wellen, die sich in einem LAN leitungsgebunden ausbreiten in eine so genannte Freiraumwelle umgewandelt werden. Auf der Empfängerseite muss die umgekehrte Wandlung vorgenommen werden. Man spricht deshalb auch bei Antennen von Wellentypwandlern.



Antennen strahlen elektromagnetische Wellen ab oder nehmen sie auf. Eine Antenne ist ein Grenzfall eines Schwingkreises wie er in Abbildung 164 a) dargestellt ist.

Öffnet man den Kondensator wie in Abbildung 164 b) immer weiter kommt man schließlich zu Abbildung 164 c). Dabei entsprechen die beiden parallelen Drähte dem Kondensator da zwischen ihnen ein elektrisches Feld besteht.

Bei einer Antenne wie in Abbildung 164 d) ist ein Draht mit der Erde verbunden und der andere Draht hängt frei in der Luft. Schaut man sich das Röntgenbild einer WLAN-Antenne, wie in Abbildung 166 an, kann man die Spule und die Drähte erkennen.

Abbildung 164: Vom Schwingkreis zur Antenne

In Abbildung 165 ist der Zusammenhang zwischen der halben Wellenlänge ($\lambda/2$) und der Antennenbauform ersichtlich. Solche Antennen werden z. B. bei APs im SOHO-Bereich verwendet. Siehe Abbildung 166.

Damit die elektromagnetischen Wellen abgestrahlt werden muss bei dem Dipol die Länge der beiden Drahtstücke der halben Wellenlänge ($\lambda/2$) entsprechen. Bei 2,4GHz ist das 6,14cm und bei 5GHz ist das 2,75cm.

Da diese Bauform von ihren Abmessungen her in mobilen Geräten oft schlecht einsetzbar ist verwendet man dort $\lambda/4$ -Antennen.

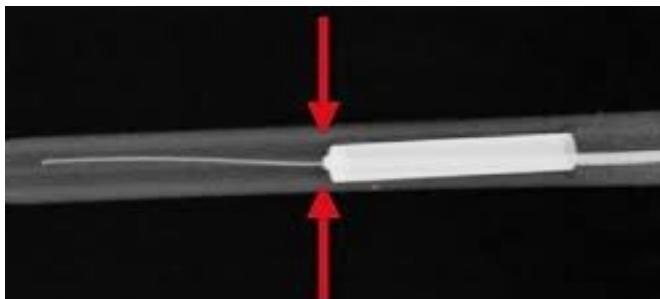


Abbildung 166: Röntgenbild WLAN-Antenne

Quelle: heise.de

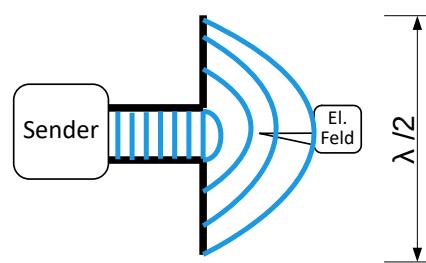
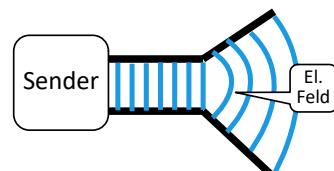
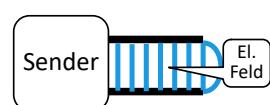


Abbildung 165: Halbwellendipol

6.3 - Grundlagen

Um Antennen zu bewerten, geht man von einer idealen Antenne mit optimalen Sende- und Empfangseigenschaften aus. Dafür nimmt man einen punktförmigen Strahler an, der in allen Raumrichtungen gleichmäßig arbeitet. Eine solche Antenne wird auch isotrope Antenne genannt.

Reale Antennen haben allerdings immer eine Richtcharakteristik. In der Richtung der Bündelung tritt eine Verstärkung auf, die als Antennengewinn bezeichnet wird. Da von einer isotropen Antenne ausgegangen wird, ist bei der Angabe der Verstärkungsleistung, die in dB angegeben wird, ein „i“ angehängt. Somit lautet die Angabe der Verstärkungsleistung „dB_i“. Eine isotrope Antenne mit einer gleichförmigen Abstrahlung (ohne Richtcharakteristik) hat keinen Antennengewinn und somit 0 dB_i.

6.4 - Antennenbauformen

Die in einem WLAN verwendete Antenne ist entscheidend für die Größe und Form einer Funkzelle verantwortlich. Im 2,4 GHz-Band sind die verschiedensten Bauformen möglich. Für die flächenförmige Abdeckung können folgende Antennen verwendet werden:

- Halbwellen-Dipole
- Dipol-Gruppen
- Patch-Antenne

6.5 - Richtantennen

Für eine gerichtete Verbindung (z. B. zwischen Gebäuden) im Freien werden folgende Antennen verwendet:

- Yagi-Antennen
- Parabol-Antennen

6.6 - Freiraumdämpfung

Im Freien breiten sich elektromagnetische Wellen wie Lichtwellen geradlinig aus. An der Grenzfläche zu leitenden Medien werden elektromagnetische Wellen reflektiert. Beim Durchgang durch nichtleitende Medien (Dielektrikum), wozu auch die Luft gehört, werden elektromagnetische Wellen gedämpft.

Die erreichbaren Reichweiten sind von der so genannten Freiraumdämpfung abhängig.

Die Freiraumdämpfung FSPL (Free Space Path Loss) berechnet sich bei:

- Entfernung = d in m
- Frequenz = f in Hz oder Wellenlänge (λ) in m
- Lichtgeschwindigkeit = c (299000000 m/s)

In der Literatur wird die Freiraumdämpfung auch mit A_F (Attenuation Free-Space-Path-Loss) abgekürzt.

$$A_F [dB] = FSPL [dB] = \frac{4 \times \pi \times d}{\lambda} = \frac{4 \times \pi \times d \times f}{c} \quad (26)$$

Dabei gilt der folgende Zusammenhang zwischen Frequenz und Wellenlänge:

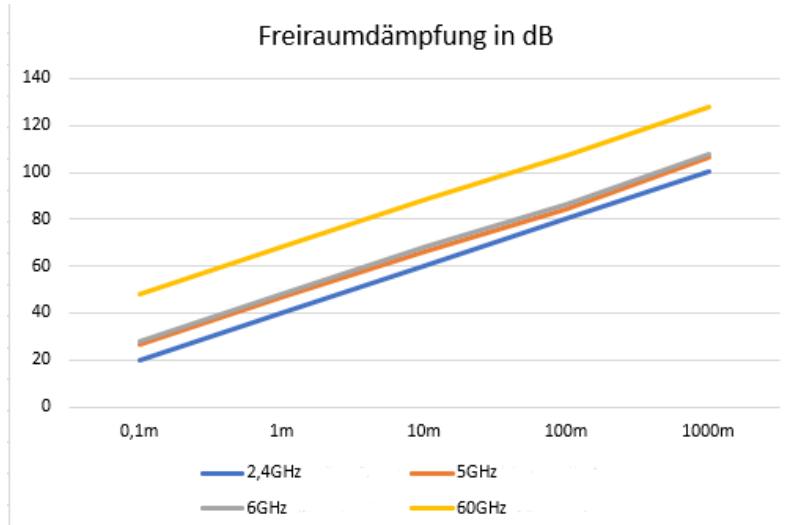
$$\lambda = \frac{c}{f} \quad (27)$$

Wobei gilt:

- Wellenlänge λ in m
- Frequenz in Hz (1/s)
- Lichtgeschwindigkeit 299.000.000 m pro Sekunde

Es gibt auch eine weit verbreitete logarithmische Berechnungsformel für die Freiraumdämpfung:

$$A_F [dB] = FSPL [dB] = 20 \times \log_{10}(d) + 20 \times \log_{10}(f) - 147,55 \quad (28)$$



Mit steigender Frequenz wird die Beeinflussung der Freiraumdämpfung auch größer.

Deshalb haben 5GHz-WLANS gegenüber 2,4GHz-WLANS bei gleicher Sendeleistung und gleichem Modulationsverfahren eine geringere Reichweite.

Abbildung 167: Freiraumdämpfung

Schaut man sich die Werte in Tabelle 60 pro Dekade an, fällt auf, dass die Freiraumdämpfung pro Dekade (1, 10, 100, 1000m) um immer 20dB zunimmt. Genauso fällt auf, dass bei einer Distanzverdopplung (100, 200, 400m) immer 6 dB dazu kommen.

Tabelle 60: Freiraumdämpfung in Abhängigkeit zur Frequenz und Distanz

Distanz [m]	Freiraumdämpfung bei 2,4GHz [dB]	Freiraumdämpfung bei 5GHz [dB]	Freiraumdämpfung bei 6GHz [dB]	Freiraumdämpfung bei 60GHz [dB]
1	40,2	47,16	48,01	68,01
10	60,2	67,16	68,01	88,01
100	80,2	87,16	88,01	108,01
200	86,22	93,18	94,03	114,03
400	92,24	99,2	100,05	120,05
1000	100,2	107,16	108,01	128,01

6.7 - Halbwellendipole

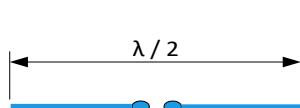
Halbwellendipole gibt es in offener, gefalteter und geschlossener Form. Für die in WLANs verwendeten Antennen werden Halbwellendipole verwendet. Diese Antennen haben die Länge der halben Wellenlänge ($\lambda / 2$).

Halbwellendipole haben einen theoretischen Antennengewinn von 2,2 dBi. Je nachdem, ob man das magnetische oder das elektrische Feld betrachtet, ergeben sich unterschiedliche Richtcharakteristiken:

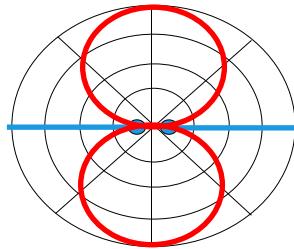
- Halbwellendipole haben in der Ebene des magnetischen Feldes (H-Ebene) eine Rundstrahlcharakteristik.
- In der Ebene des elektrischen Feldes (E-Ebene) haben sie eine Richtcharakteristik.

Für einen tatsächlichen Aufbau mit einer gewünschten Ausrichtung der Antenne gilt folgende Regel:

- Der Leiter der Antenne (Strahler) liegt in der E-Ebene
- Der Leiter der Antenne (Strahler) steht senkrecht auf der H-Ebene



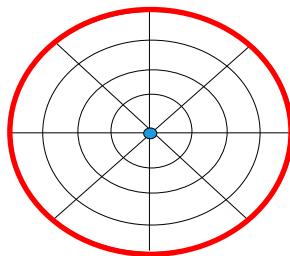
Offener Dipol



E-Ebene



Geschlossener Dipol



H-Ebene

Abbildung 168: Halbwellendipole und ihre Ausrichtung

6.8 - Stabantenne

Die Einfachste Form einer Antenne ist ein Halbwellendipol in Form einer Stabantenne. Die Ausbreitung von Funkwellen haben bei einer Stabantenne immer die Ausbreitung wie in Abbildung 169.



Abbildung 169: Ausführungen von Stabantennen

Dipolantennen weisen in der Regel keinen Antennengewinn auf. Sie sind anhand der Länge erkennbar, da sie etwas kürzer sind, als Antennen mit Gewinn. Siehe Abbildung 169 oben.

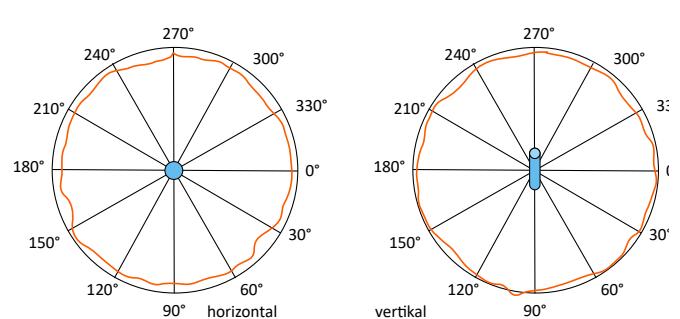


Abbildung 170: Strahlungsdiagramme einer Dipolantenne ohne Gewinn

6.9 - Dipolgruppen

Werden mehrere Dipole hintereinander (parallel) angeordnet, spricht man von einer Dipolreihe. Werden mehrere Dipole nebeneinander (kollinear) angeordnet spricht man von einer Dipollinie. Dies wird vor allem zur Verbesserung des Antennengewinns und somit auch der Richtcharakteristik gemacht. Je nach Anzahl und Abstand der Dipole ändern sich hier die Eigenschaften.

Eine Dipolreihe hat eine starke Richtwirkung in der H-Ebene und eine leichte Richtwirkung in der E-Ebene.

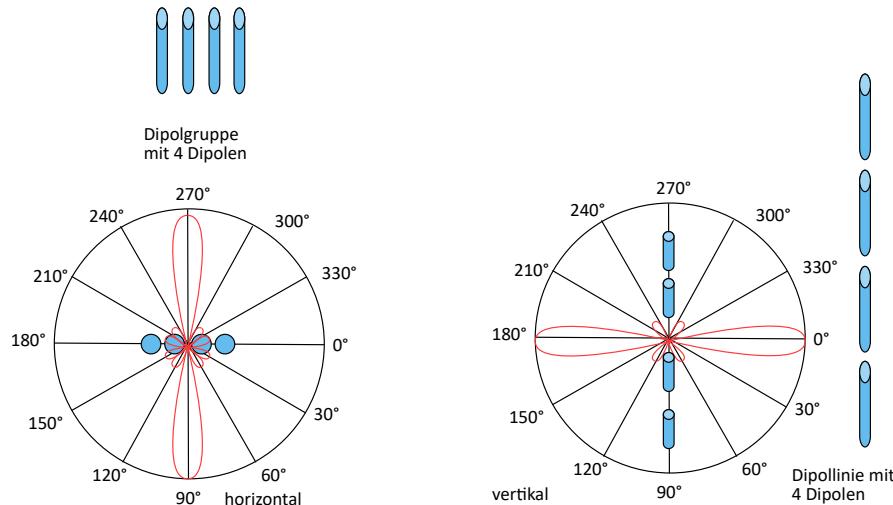
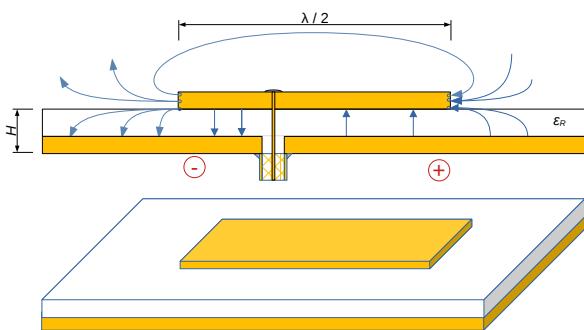


Abbildung 171: Dipolgruppe mit 4 Dipolen und Dipollinie mit 4 Dipolen

Kollinare Dipole haben nur in der E-Ebene eine Richtcharakteristik. In der H-Ebene haben sie eine Rundstrahlcharakteristik.

6.10 - Patchantennen



- a) Werden spezielle Materialien verwendet, kann eine sehr flache Bauweise der Antennen erreicht werden. Typischerweise haben sie eine rechteckige flache Form. Patchantennen haben eine verbesserte Abstrahlcharakteristik für Räume ca. 180° (Form einer Halbkugel). Sie werden hauptsächlich für die Wandmontage verwendet.
- b)

Abbildung 172: Patch-Antenne

6.11 - Richtantennen

Montiert man zwei Dipole im Abstand von $\lambda/4$ und speist sie mit einer Phasenverschiebung von 90° erhält man eine einseitige Charakteristik. Siehe Abbildung 174. Eine solche Bauform nennt man Reflektorantenne.

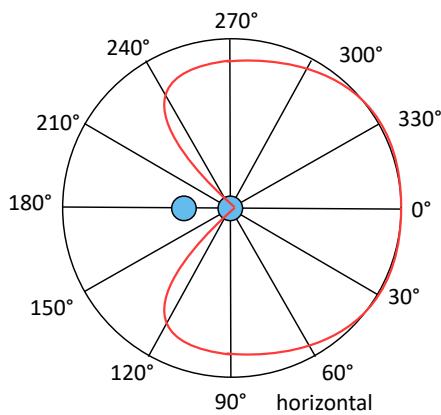


Abbildung 174: Dipolgruppe mit 2 Dipolen im Abstand von $\lambda/4$

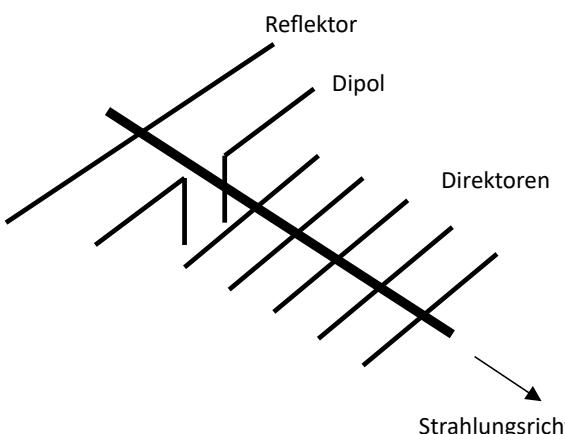


Abbildung 173: Yagi-Antenne

In Vorwärtsrichtung treffen Maxima des Reflektors auf die Maxima des Erregers und verstärken sich somit. In Rückwärtsrichtung treffen Maxima des Erregers auf Minima des Reflektors und werden damit ausgelöscht. Hinter dem Halbwellendipol sitzt ein etwas längerer Reflektor der das Strahlungsfeld in eine Vorzugsrichtung bündelt. Vor dem Dipol sind in Strahlungsrichtung die etwas kürzeren Direktoren montiert um das Feld weiter zu bündeln.

6.11.1 - Öffnungswinkel / Halbwertsbreite

Der Antennengewinn steht im direkten Zusammenhang mit dem Öffnungswinkel. Damit wird angegeben über welches Winkelsegment bei einer Antenne die Sendeleistung bevorzugt angegeben wird. Dies gilt natürlich auch für eine Empfangsantennen. Je größer die Richtfunkcharakteristik ist und damit der Antennengewinn, desto kleiner der Öffnungswinkel.

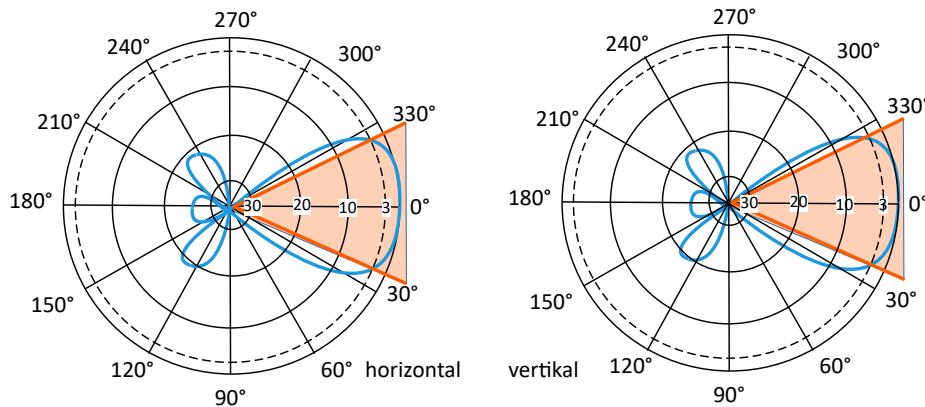


Abbildung 175: Richtungsdiagramme mit Öffnungswinkeln

Bei den Richtungsdiagrammen wird in Polar- oder Winkelkoordinaten angegeben wie groß die Sendeleistung in welcher Raumrichtung ist.

In den Richtungsdiagrammen normiert man die maximale Sendeleistung auf 0dB. Der Öffnungswinkel wird dadurch ermittelt, dass die Strahlungsleistung auf die Hälfte der maximalen Leistung abgesunken ist. Bei der Hälfte der Strahlungsleistung, das ist bei etwa 3 dB weniger als das Maximum, wird gemessen. Daher wird dieser Winkel als Halbwertsbreite oder Half Power Beam Width (HPBW) bezeichnet.

6.11.2 - Vor- Rückverhältnis

Bei Richtantennen gibt es nicht nur eine Keule in Senderichtung, sondern es sind noch kleinere Keulen in seitlicher und in der Rückwärtsrichtung messbar. Die Nebenkeulendämpfung des rückwärtigen Bereichs bezogen auf die Hauptkeule wird als Vor-Rück-Verhältnis (engl. Front-Back-Ratio (FBR)) bezeichnet.

$$FBR = 20 \times \log \left(\frac{r_{Vor}}{r_{Rück}} \right) \quad (29)$$

Im Indoor-Bereich ist das Vor-Rück-Verhältnis von besonderer Bedeutung wenn es darum geht begrenzte Bereiche auszuleuchten, denn damit kann auch die Reichweite von Antennen abgeschätzt werden.

6.12 - Fresnel-Zone

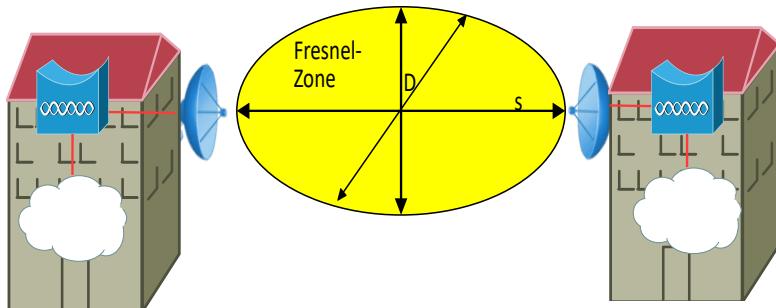


Abbildung 176: Fresnel-Zone

Beim Aufbau einer Richtfunkstrecke ist zu beachten, dass Hindernisse die Reichweite einer Funkzelle beeinflussen können. Dieses Phänomen wird durch die so genannte Fresnel-Zone beschrieben.

Darin ist nicht nur die direkte Sichtverbindung freizuhalten sondern auch ein Bereich um die so genannte Line of Sight (LoS) in Form einer Ellipse.

Dabei ist zu beachten, dass die Ellipse nicht nur nach oben und unten eine Ausdehnung (D) hat, sondern auch links und rechts. Zur Berechnung des Durchmessers in der Mitte der Ellipse kann folgende vereinfachte Formel verwendet werden.

$$D = \sqrt{s \times \lambda} \quad (30)$$

Um D an jeder beliebigen Stelle zu errechnen kann auf die folgende Formel zurückgegriffen werden.

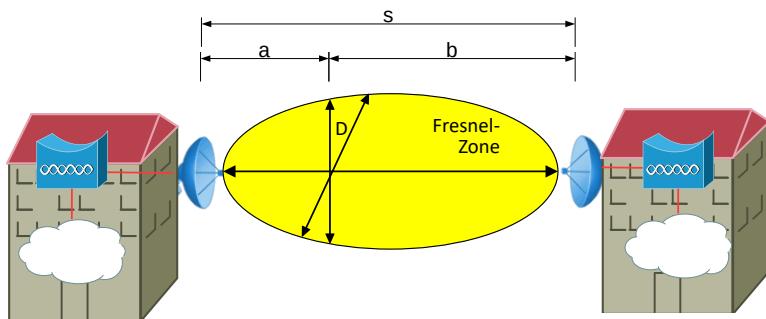


Abbildung 177: Berechnung von D an beliebiger Stelle

Dabei setzt sich die Strecke s aus den Teilstrecken a und b zusammen.

$$D = 2 \times \sqrt{\frac{a \times b \times \lambda}{s}} \quad (31)$$

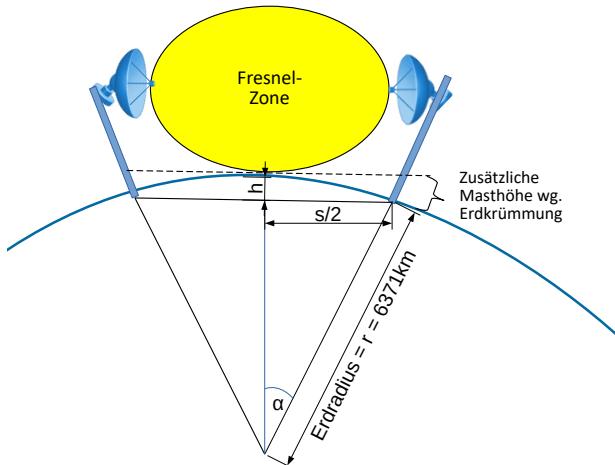


Abbildung 178: Fresnel-Zone mit Berücksichtigung der Erdkrümmung

Bei größeren Distanzen kommt die Erdkrümmung ins Spiel da sie in die Fresnel-Zone hineinragt und deshalb bei der Masthöhe berücksichtigt werden muss.

$$\arcsin \alpha = \left(\frac{s}{2} \right) \times \text{Erdradius} \quad (32)$$

$$h = \left(\frac{\text{Erdradius}}{\cos \alpha} \right) - \text{Erdradius} \quad (33)$$

Aus der folgenden Tabelle können die Antennenmasthöhen für verschiedene Distanzen ermittelt werden.

Tabelle 61: Ermittlung der Antennenmasthöhe bei 2,4GHz für verschiedene Distanzen

Distanz [km]	Durchmesser der Fresnel-Zone [m]	Höhe durch Erdkrümmung [m]	Mindesthöhe für Antennenmast [m]
0,5	4,5	0,0	2,36
1	6,65	0,02	3,34
5	14,87	0,49	7,92
10	21,03	1,96	12,47
20	29,73	7,85	22,72

Witterungseinflüsse spielen bei WLANs nach IEEE-802.11 kaum eine Rolle.

6.13 - Diversity-Antennen

Es gibt APs mit zwei Antennen bzw. mit zwei Antennenanschlüssen. Dies ist für eine Verbesserung der Störungseinflüsse durch Mehrwege-Ausbreitung sinnvoll. Dies ist vor allem in Gebäuden durch die unterschiedlichsten Reflexionen an Wänden und Gegenständen der Fall. Je nachdem, welche der beiden Antennen einen besseren Kontakt zum Kommunikationspartner hat, wird diese Antenne aktiviert.

6.14 - Antennenleitungen

Die Antennenleitungen vom AP zur Antenne haben einen großen Einfluss auf die Sendeleistung. Grundsätzlich gilt, je dünner die Leitung, desto größer ist die Dämpfung. Allerdings ist mit einer dünneren Leitung auch ein kleinerer Biegeradius beim Verlegen möglich. Um eine dicke Antennenleitung an eine kleine PCMCIA-Karten anzuschließen, gibt es so genannte Pigtails, welche nichts anderes als ein Adapterleitungen sind.

Tabelle 62: Antennenleitungen und die Auswirkung auf die Dämpfung

Kabeltyp	Durchmesser [mm]	Minimaler Biegeradius [mm]	Dämpfung in [dB / m] bei		
			2,4GHz	5,3GHz	5,7GHz
U.FL	1,13	5	3,43	4,6	5,13
RG178 A/U	1,85	19	2,5	n/a	n/a
RG316 A/U	2,5	15	1,5	n/a	n/a
RG316 D	2,5	15	1,54	2,51	2,66
ULA 168	2,95	20	0,656	n/a	n/a
ULA 196	2,95	20	0,863	n/a	n/a
LMR 200	2,95	20	0,554	n/a	n/a
LMR 195	3,07	20	0,625	n/a	n/a
Low-Loss	3,9	30	0,46	n/a	n/a
Low-Loss RF 195	4,95	25	0,58	n/a	n/a
RG214U	10,8	55	0,45	0,75	0,85
RG 223 U	5,4	30	0,76	1,35	1,43
Aircell7	7,3	25	0,356	~ 0,6	~ 0,64
HDF 400	7,24	30	0,265	n/a	n/a

6.15 - Equivalent Isotropically Radiated Power (EIRP)

Die so genannte äquivalente isotrope Strahlungsleistung ist eine Angabe der Regulierungsbehörden (in Deutschland die Bundesnetzagentur) welche die maximal zulässige Strahlungsleistung einer Sendeeinheit festlegt.

Dabei fließen die Senderleistung, die Dämpfung der Antennenleitung, sowie Stecker/Kupplungen und der Antennengewinn in die Berechnung mit ein.

$EIRP [dBm] = \text{Senderleistung [dBm]} - \text{Dämpfung durch Antennenleitung und Stecker/Kupplungen [dB]} + \text{Antennengewinn [dBi]}$.

Zulässige Werte für die Frequenzbereiche in Deutschland sind:

Frequenzband [GHz]	Kanal	EIRP [mW]	EIRP [dBm]
2,4	1 - 13	100	20
5GHz	36 – 64	200	23
5GHz	100 – 140	1.000	30
5GHz	149 – 165	25	14
6GHz	alle	200	23

6.16 - Reichweite

Bei der Betrachtung der überbrückbaren Distanzen ist zuerst die im Frequenzband geltende Freiraumdämpfung A_F zu ermitteln.

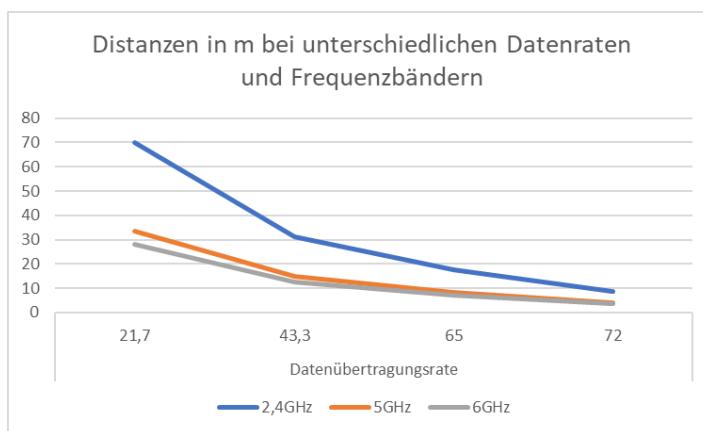
Dabei gilt für die zu verwendenden Frequenzen (f) in [m]:

- 2,4GHz → $0,124913534 \approx 12,5$ cm
- 5GHz → $0,059958492 \approx 6$ cm
- 6GHz → $0,04996541 \approx 5$ cm

$$A_F [dB] = 20 \times \log \frac{4 \times \pi \times d}{\lambda} \quad (34)$$

Daraus lässt sich die überbrückbare Distanz (d) ermitteln:

$$d [m] = 10^{\frac{A_F}{20}} \times \left(\frac{\lambda}{4 \times \pi} \right) \quad (35)$$



Bei vergleichbaren Verhältnissen (20MHz Kanalbreite Coderate = 2/3) ergeben sich für unterschiedlichen Bänder unterschiedlichen Reichweiten.

Abbildung 179: Reichweiten unterschiedlicher Bänder

Zur Ermittlung der maximalen Reichweite eines WLANs sind die folgenden Faktoren relevant:

Tabelle 63: Faktoren zur Berechnung der Reichweite

Faktor	Auswirkung [positiv / negativ]	Einheit
Sendeleistung des Senders	positiv	dBm
Antennengewinn der Sendeantenne	positiv	dBi
Verlust in Antennenkabeln auf der Senderseite	negativ	dB
Verlust in Steckern auf der Senderseite	negativ	dB
Verlust in der Sendeanlage	negativ	dB
Reguläre Dämpfung über die Funkstrecke	negativ	dB
Zusätzliche Dämpfung durch Hindernisse (z.B.Wände)	negativ	dB
Zusätzliche Dämpfung durch Störsignale	negativ	dB
Verlust in der Empfangsanlage	negativ	dB
Verlust in Steckern auf der Empfängerseite	negativ	dB
Verlust in Antennenkabeln auf der Empfängerseite	negativ	dB
Antennengewinn der Empfängerantenne	positiv	dBi
Leistungsreserve	negativ	dB

Bis auf die Antennengewinne und die Sendeleistung sind die Werte negativ zu berechnen. Da die Werte meistens Annahmen unter günstigen Bedingungen sind ist noch eine Leistungsreserve anzusetzen.

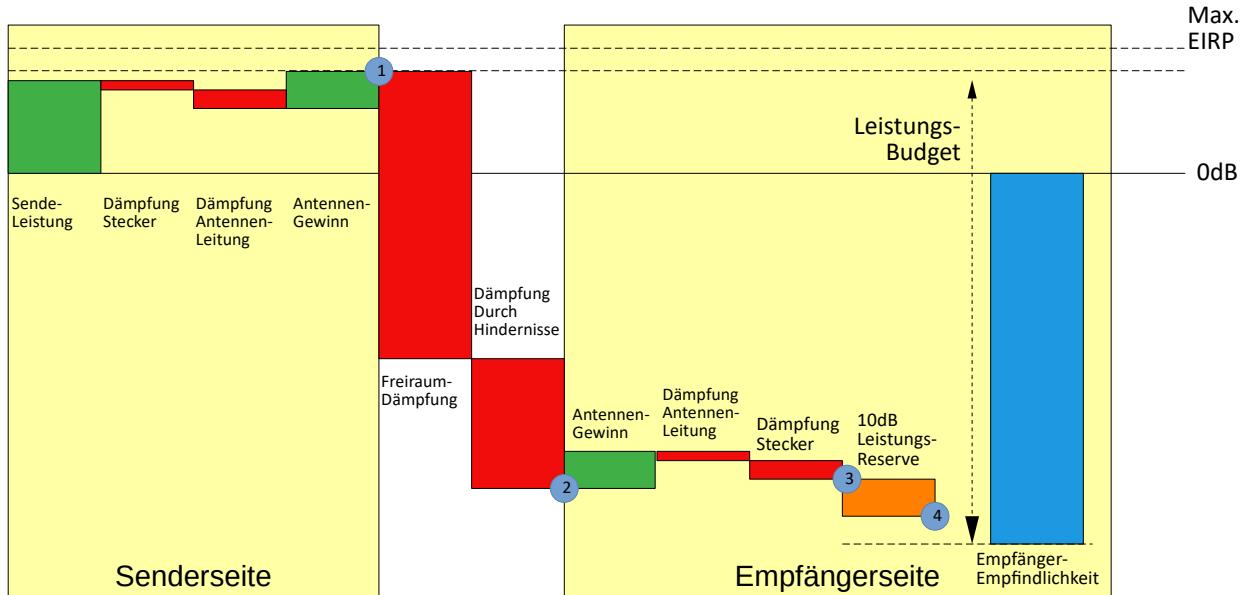


Abbildung 180: WLAN-Leistungsbudget zur Ermittlung der Reichweite

Wichtig ist, dass die auf Senderseite abgestrahlte Leistung die EIRP nicht übersteigt. Evtl. muss um die Einhaltung des EIRP-Wertes zu gewährleisten, zusätzlich zu den Steckern und Antennenleitung, noch ein Dämpfungsglied eingefügt werden.

Beispiel:

Auf der Sendeseite steht ein AP mit externer Antenne, der mit 35mW (15dBm) im 2,4GHz-Band sendet. Die Antenne hat einen Gewinn von 6dBi. Die Antennenleitung ist 4 m lang und eine Dämpfung von 0,4dB/m (= 4 * 0,4dB = 1,6dB). An den Enden der Antennenleitung ist je ein Stecker mit 0,2dB Dämpfung (= 2 * 0,2dB = 0,4dB)

Nach 25m Distanz steht auf der Gegenseite ein Notebook. Zwischen AP und Notebook stehen 3 Wände mit je 10dB Dämpfung.

Damit ergibt sich in der obigen Abbildung am Punkt 1 für das Sendesystem:

$$15\text{dBm} + 6\text{dBi} - 1,6\text{dB} - 0,4\text{dB} = 19\text{dB}$$

Da im 2,4GHz-Bereich die maximal zulässige Sendeleistung bei 20dBm liegt, wird der zulässige EIRP-Wert eingehalten.

Auf der Empfängerseite wird inklusive Dämpfung 0dB veranschlagt.

Die Freiraumdämpfung beträgt bei 25m 68,2dB.

Dazu kommen noch die 3 Wände mit insgesamt 30dB

Insgesamt erhält man also:

$$19\text{dB} + 0\text{dB} - 68,2\text{dB} - 30\text{dB} = -79\text{dB}$$

Das liegt an der Grenze Empfindlichkeit der Empfänger. Je nach gewünschter Datenrate ist die Empfindlichkeit des Empfängers nicht ausreichend. Wenn dann noch Störungen durch andere Sender hinzu kommen, kann es vorkommen, dass die Verbindung mit niedrigeren Datenraten zustande kommt.

7 - Sicherheit

7.1 - Einführung

Da ein WLAN immer ein „Shared Media“ ist, kann es leicht abgehört werden. Um die Sicherheitsanforderungen Vertraulichkeit, Zugangskontrolle und Datenintegrität zu gewährleisten, wurde bei IEEE-802.11 das Wired Equivalence Privacy (WEP) -Verfahren implementiert. Damit sollen die Sicherheitsanforderungen durch Verschlüsselung und Authentifizierung, wie bei verkabelten Netzwerken, abgehandelt werden.

Als Verschlüsselungsverfahren wird bei WEP RC4 verwendet. Es handelt sich hierbei um ein symmetrisches Verfahren, das zu den Stromchiffrierern gehört. Wie der gemeinsame Schlüssel auf die Geräte kommt, ist nicht festgelegt. WEP nimmt an, dass auf allen Teilnehmern eines BSS ein gemeinsamer (meist von Hand) konfigurierter Schlüssel ist. Bei WEP sind Schlüssellängen von 64 und 128 Bit möglich. Allerdings sind davon noch 24 Bit für den Initialisierungsvektor (IV) abzuziehen. In proprietären Lösungen werden auch 256 Bit für die Verschlüsselung verwendet.

7.1.1 - Verschlüsselung

Die Verschlüsselung der MAC Service Data Unit (MSDU) erfolgt pro Paket. Der verschlüsselte Text (Chiffrat) ergibt sich aus der XOR-Verknüpfung der Schlüssel-Sequenz und dem Klartext.

Die Entschlüsselung erfolgt auf dem umgekehrten Weg. Das Chiffrat wird mit derselben Schlüssel-Sequenz in einer XOR-Verknüpfung in den Klartext überführt.

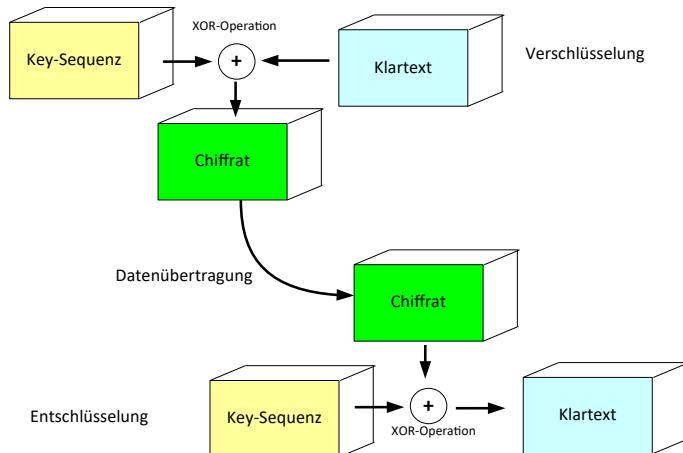


Abbildung 181: Grundsätzliche WLAN Verschlüsselung

Damit die beiden Pseudo-Zufallszahlen gleich sind, müssen sie mit dem selben Startwert(Seed) initialisiert werden. Der Startwert wird aus dem geheimen Schlüssel berechnet, der bei beiden Kommunikationspartnern vorliegen muss.

Ein Angreifer kann zwar die Datenübertragung belauschen. Es ist ihm jedoch nicht möglich, die Klartexte zu ermitteln, solange er den Startwert nicht kennt.

Ein Problem entsteht erst, wenn der gleiche Startwert für eine weitere Datenübertragung verwendet wird.

Bei der Verwendung von RC4 ist also die geschickte Konstruktion des Startwerts ausschlaggebend für die Sicherheit. Wichtig ist also: „Niemals den selben Schlüsselstrom verwenden“. Leider ist das bei WEP nicht gegeben!

Das liest sich bis hierhin noch ganz entspannt und man kann sich fragen, was die Hysterie um die WLAN-Verschlüsselung soll. Doch zwei Probleme liegen schon jetzt auf der Hand.

7.1.2 - Probleme

Schafft ein Angreifer es zwei verschlüsselte Texte abzufangen, die mit dem selben Schlüssel verschlüsselt wurden, kann er über die XOR-Operation die beiden Klartexte ermitteln.

Hat er die Klartexte, kann er über eine weitere XOR-Operation die Schlüssel-Sequenz ermitteln.

Dieses Verfahren ist deshalb so leicht, weil bei den Protokollen, die über das WLAN transportiert werden, immer wieder die selben Informationen, wie z. B. Header, an der selben Position zu übertragen sind. Daher sind ganze Textpassagen leicht zu erraten.

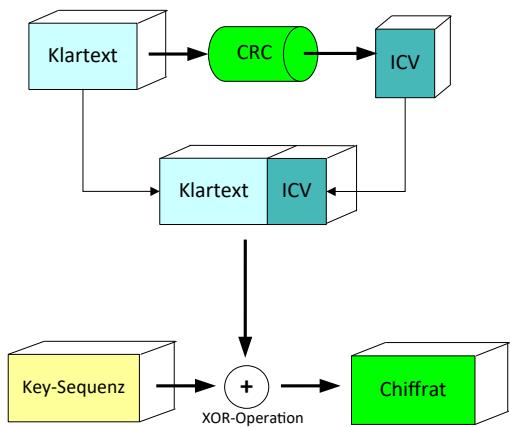
7.1.3 - Datenverfälschung

Zusätzlich ist es immer noch möglich, ein Bit im Chiffrat zu verändern. Genau dieses Bit wird im Klartext bei der Entschlüsselung ebenfalls gekippt. Dies funktioniert, ohne dass der Schlüssel oder der Originaltext bekannt sein muss.

7.2 - Verschlüsselung

Um die Datenintegrität zu verbessern, wurde der Originaltext ($M = \text{Message}$) mit einer 32 Bit langen Checksumme dem Integrity Check Value (ICV) verlängert. Zusammen bilden sie den Klartext ($M \parallel ICV$).

Damit sollen veränderte Klartexte erkannt werden und vom Empfänger verworfen werden.



Ungeschickterweise wird bei WEP ein CRC (Cyclic Redundancy Check) verwendet. Dieses Verfahren ist optimal für die Erkennung von Bitfehlern bei der Übertragung von Daten. Es ist jedoch gänzlich ungeeignet, um Daten kryptographisch abzusichern. Der Grund liegt in der Linearität von CRCs bezüglich der XOR-Operation.

$$\text{CRC}(a \oplus b) = \text{CRC}(a) \oplus \text{CRC}(b)$$

Dies bedeutet, dass leicht ein Verfahren entwickelt werden kann, um für veränderte Klartexte eine entsprechende Checksumme zu erhalten. Da der ICV grundsätzlich an die verschlüsselten Daten hinten angehängt wird und er immer die gleiche Länge hat, ist es einfach ihn zu manipulieren.

Abbildung 182: WLAN WEP-Verschlüsselung mit CRC

Damit hat der Empfänger keine Möglichkeit mehr, einen gefälschten Klartext zu erkennen.

Damit von Paket zu Paket nicht derselbe Initialisierungswert für RC4 verwendet wird, gibt es noch einen 24 Bit langen zufälligen Initialisierungsvektor(IV). Der Schlüssel mit 40 oder 104 Bit Länge und der IV bilden zusammen den Startwert (WEP-Seed) für den Schlüsselstrom RC4($K \parallel IV$).

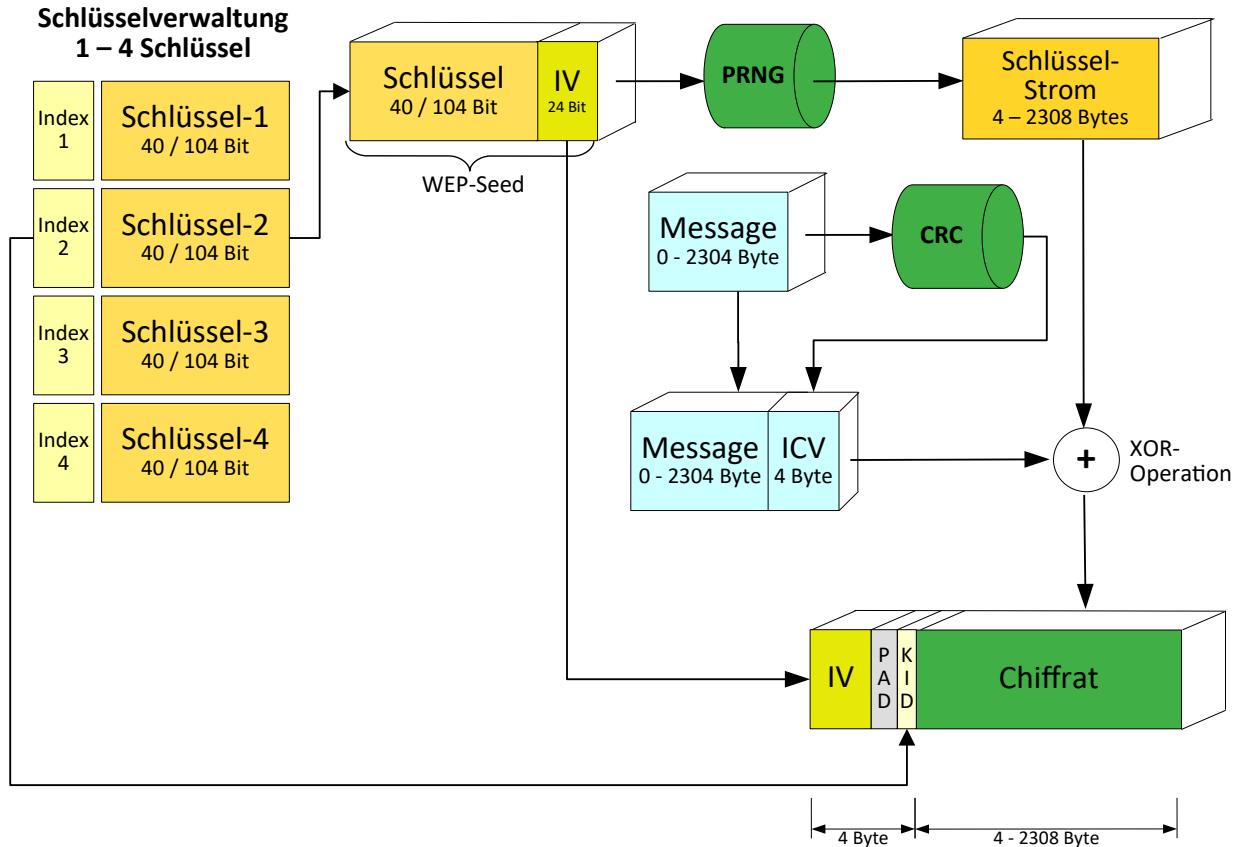


Abbildung 183: WLAN Gesamte WEP-Verschlüsselung

Als letzter Schritt erfolgt die Erzeugung des Chiffrauts (C) durch XOR-Verknüpfung des Klartextes mit dem Schlüsselstrom:

$$C = (M \parallel ICV) \oplus RC4(K \parallel IV) \quad (36)$$

Mit der Forderung, dass ein Schlüssel nur ein einziges Mal verwendet werden darf, kann mit dem Initialisierungsvektor der Schlüssel ca. 16 Millionen Mal variieren. Das reicht bei einem gut ausgelasteten AP nur wenige Stunden. Danach müsste ein neuer WEP-Schlüssel verwendet werden. Dies ist unabhängig von der Schlüssellänge mit 40 Bit oder 104 Bit. Da bietet der Standard jedoch nichts.

Damit der Empfänger weiß, welcher Wert für den IV verwendet wurde, wird er im Header des MAC-Pakets im Klartext mit übertragen.

Da bei der Konfiguration der Schlüssel von Hand bis zu 4 mögliche Schlüssel eingebbar sind, muss die Key-ID (KID) aus dem Schlüsselspeicher ebenfalls im Paket-Header mit übertragen werden. Da zwischen IV und KID noch Platz ist, wird mit einem Pad aufgefüllt.

7.3 - Entschlüsselung

Alles was der Empfänger benötigt und noch nicht hat, bekommt er im Datenpaket unverschlüsselt geliefert. Das ist der Initialisierungs Vektor (IV) und die Key-ID (KID).

Damit kann der Empfänger den benötigten Schlüsselstrom $RC4(K \parallel IV)$ aufbauen und die Entschlüsselung vornehmen:

$$C \oplus RC4 = (M \parallel ICV) \oplus RC4 \oplus RC4 = (M \parallel ICV) \oplus (RC4 \oplus RC4) = (M \parallel ICV) \quad (37)$$

Hierbei gilt: $RC4 = RC4(K \parallel IV)$ Ein mit WEP verschlüsseltes Datenpaket sieht folgendermaßen aus.

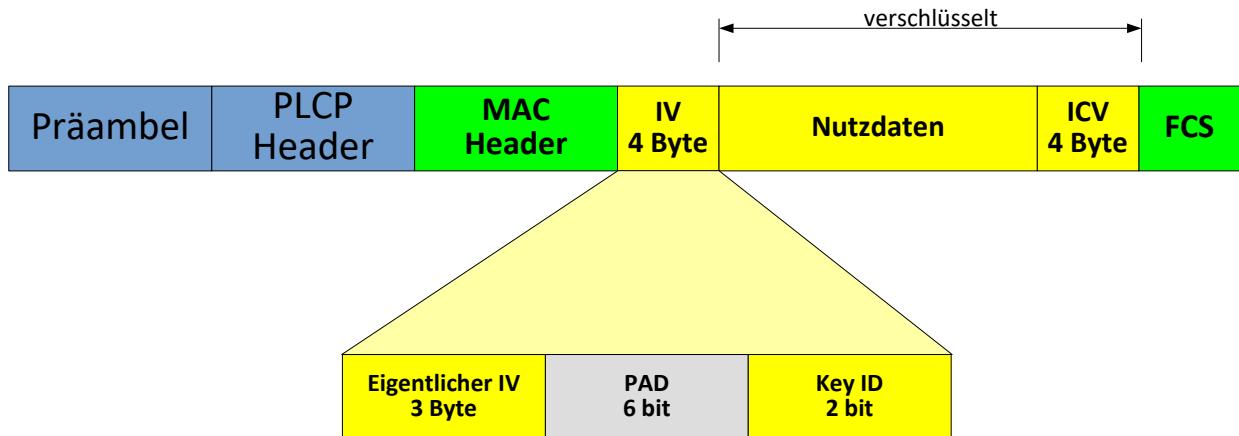


Abbildung 184: WEP-Paketformat

Der symmetrische Schlüssel ist mit frei verfügbaren Tools wie z. B. Airsnort ermittelbar. Ist dieser bekannt, kann der gesamte Datenverkehr mit einem Protokollanalysator im Klartext aufgezeichnet werden!

7.4 - Zusammenfassung der WEP-Probleme

- ➊ Dreh- und Angelpunkt aller Sicherheitsprobleme ist das fehlende Schlüssel-Management.
- ➋ Verschlüsselte Frames können nachträglich verändert werden ohne dass der Empfänger eine Möglichkeit hat, dies zu erkennen.
- ➌ Mit einer Schlüsselsequenz kann man die zugehörige Nachricht entschlüsseln. Den eigentlichen RC4-Schlüssel braucht man nicht.
- ➍ Zu jedem IV gehört genau eine Schlüsselsequenz. D. h. man kann die verwendete Schlüsselsequenz im MAC-Header erkennen.
- ➎ Bereits verwendete Schlüssel können wieder verwendet werden.
- ➏ Bereits gesendete Frames können nochmals gesendet werden. Es gibt keinen Schutz vor Wiederholungen.
- ➐ Es werden nur die Datenframes verschlüsselt.

7.5 - Wi-Fi Protected Access (WPA)

Offensichtlich sind die Sicherheitsmechanismen bei WEP nicht als ausreichend anzusehen. Bei IEEE wurde mit der Arbeitsgruppe IEEE-802.11i an einer Verbesserung gearbeitet, die allerdings Zeit in Anspruch nahm.

Da eine Verbesserung der Situation auf dem bisherigen Standard aufzubauen waren eine schnelle Lösung nicht zu machen. Deshalb waren in einem ersten Ansatz Lösungen aus höheren Schichten wie VPNs oder der Einsatz von Secure Shell (SSH) ergriffen worden.

Um WLANs vor allem im professionellen Umfeld zu retten, wurde der Zwischenzeit von der Wi-Fi-Alliance eine Verbesserung der Sicherheit unter dem Namen Wi-Fi Protected Access (WPA) definiert. Treibende Kraft war dabei die Firma Intersil (HP) die auch die ersten Produkte auf dem Markt bracht. Parallel dazu wurden durch andere Firmen Lösungen erarbeitet:

- ➊ WEPplus von Agere Systems Inc. (HP). Dabei werden schwache Initialisierungs Vektoren (IVs) verworfen.
- ➋ Fast Packet Keying (FPK) zur Erzeugung von dynamischen WEP-Schlüsseln von RSA

Die Produkte haben sich zwar nicht durchgesetzt, allerdings sind Teile aus diesen Verfahren bei WPA2 und IEEE-802.11i verwendet worden.

WPA sollte die WEP-Schwachstellen bereinigen und die wichtigsten Schutzziele Vertraulichkeit, Integrität und Authentizität erreichen. Trotzdem sollte es auf der bisherigen Lösung aufbauen, um die alten Geräte weiter verwenden zu können und zum künftigen IEEE-802.11i-Standard kompatibel sein. Deshalb bot es sich an, das was für IEEE-802.11i bis Oktober 2003 bereits entwickelt war, zu übernehmen. Dazu zählen Sicherheitsmechanismen wie das Temporary Key Integrity Protocol (TKIP) und IEEE-802.1x.

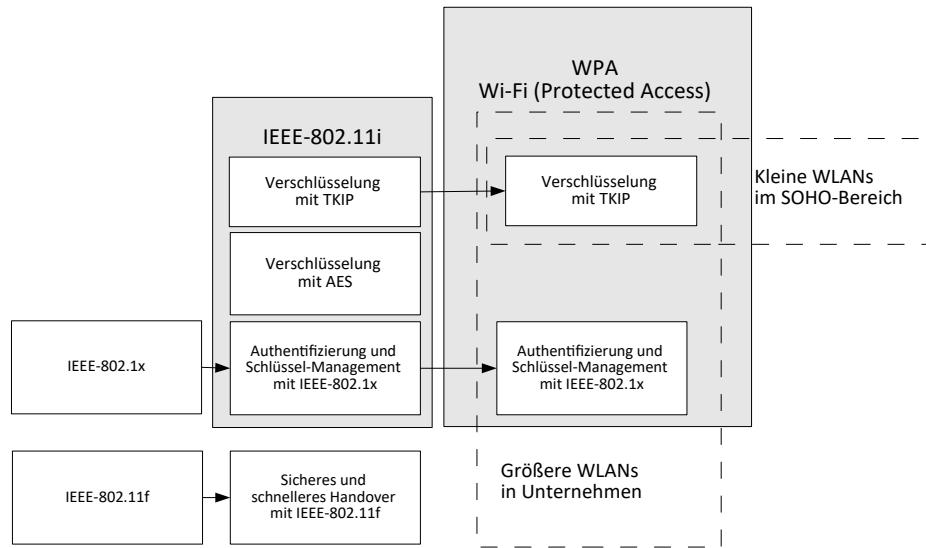


Abbildung 185: Zusammenhänge der Sicherheitsaktivitäten

Je nachdem, ob ein kleines SOHO (Small Office / Home Office) erstellt werden soll, oder ein großes Firmennetzwerk, wird bei WPA unterschieden, welche Bestandteile von IEEE-802.11i übernommen werden sollen.

- ➊ Die Verschlüsselung mit TKIP ist in beiden Fällen vorgesehen. Bei kleinen WLANs bleibt es bei den Preshared Keys. Das ist immer noch besser als bei WEP.
- ➋ Bei großen WLANs in Unternehmen kann mit einem RADIUS-Server und EAP die Schlüssel-Verwaltung nach IEEE-802.1x durchgeführt werden. In diesem Bereich sind auch diverse proprietäre Lösungen wie LEAP (Lightweight EAP) von Cisco angesiedelt.

AES bleibt bei WPA nicht berücksichtigt. WPA ist leider auch nur für den Infrastruktur-Modus spezifiziert.

7.6 - WPA 2

7.6.1 - Einführung

IEEE-802.11i war am 24. Juni 2004 verabschiedet worden. Im September 2004 legte die Wi-Fi Alliance mit einem Wi-Fi Protected Access 2 (WPA 2) nach, bei dem IEEE-802.11i weitgehend übernommen worden war. Die Verschlüsselung entspricht dem IEEE-802.11i-Standard. Nur in der Detailbetrachtung gibt es Unterschiede.

Um existierende Hardware – zumindest kurzfristig – weiterhin verwenden zu können, wurden zwei unterschiedliche Basisprotokolle für die Verschlüsselung und Integritätssicherung im 802.11i-Standard definiert:

- ➊ Ein auf dem Advanced Encryption Standard (AES) basierendes Verfahren namens CTR/CBC-MAC Protocol (CCMP)
- ➋ Das Temporal Key Integrity Protocol (TKIP)

Wie bei WPA gibt es zwei Modi, den Enterprise-Mode und den Personal-Mode. Der Personal-Mode unterscheidet sich vom Enterprise-Mode in beiden Versionen dadurch, dass der Enterprise-Mode auf einem Authentifizierungsserver basiert und der Personal-Mode auf Preshared Keys (PSK)

Tabelle 64: WPA-Versionen und deren verwendete Schlüssel bei unterschiedlichen Modi

WPA-Variante		WPA	WPA 2
Personal-Mode	Authentifizierung	PSK	PSK
	Verschlüsselung	TKIP / MIC	AES-CCMP
Enterprise-Mode	Authentifizierung	IEEE-802.1x	IEEE-802.1x
	Verschlüsselung	TKIP / MIC	AES-CCMP

Die in IEEE-802.11i vorgestellte Sicherheitsarchitektur war komplett neu und wird als Robust Security Network (RSN) bezeichnet. Diese Bezeichnung ist später auch im IEEE-802.11 Standard aufgenommen worden. Die wichtigsten Elemente der RSN-Sicherheitsarchitektur sind die Mechanismen zur Verschlüsselung, Integritätssicherung und Authentifizierung.

Wie man in Tabelle 64 sehen kann, wurde die größte Änderung im Bereich der Verschlüsselung vorgenommen. Deshalb soll im folgenden erst einmal das Schlüsselmanagement erläutert werden.

Als Grundlage wurde eine mehrstufige Schlüsselhierarchie eingeführt.

7.6.2 - Master Key

Ein Benutzer muss sich zuerst authentifizieren damit er einen Zugriff auf eine Ressource erlangen kann. Dies macht er indem er nachweist, dass er Kenntnis von einem Geheimnis hat, das zwischen beiden Parteien vereinbart worden ist. Das Geheimnis ist ein Schlüssel, bei dessen Erzeugung besondere Sorgfalt aufgewendet werden muss, denn von ihm hängen alle anderen Schlüssel ab. Wegen seiner wichtigen Funktion wird dieser Schlüssel als Master Key genannt. Es soll so selten wie möglich genutzt werden. Deshalb wird er in der RSN-Architektur nur zur Erzeugung der temporären Schlüssel verwendet. Dagegen wurde bei WEP, wo es kein Schlüsselmanagement gibt, nur der Master Key, sowohl für die Authentifizierung, als auch die Datenverschlüsselung, eingesetzt.

7.6.3 - Transient Key

Mit dem Master Key werden in Echtzeit temporäre (transient) Schlüssel erzeugt, mit denen dann die verschiedenen Dienste genutzt werden können. Damit hat der Administrator nur die Aufgabe beim Einrichten einer Station, oder eines APs, den Master Key anzulegen. Den Rest übernimmt das Schlüsselmanagement automatisch was die Akzeptanz dieser Lösung fördert.

7.6.4 - Schlüsselarten

Neben der Trennung der Schlüssel in Master Key und Transient Key gibt es eine weitere Aufteilung die auf der Art des Datenaustauschs basiert. Es werden unterschiedliche Schlüssel für Unicasts und Multicasts /Broadcast angewandt.

Zum sicheren Datenaustausch zwischen zwei Stationen muss ein Schlüssel verwendet werden der nur den beiden Stationen bekannt ist. Man spricht hierbei von paarweisen Schlüsseln denn nur den beiden Partnern ist der Schlüssel bekannt. Typischerweise kommuniziert eine Station immer mit dem AP. Damit muss die Station einen paarweisen Schlüssel speichern, während ein AP für alle Stationen einen paarweisen Schlüssel halten muss.

Soll ein verschlüsseltes Datenpaket von einem Sender an mehrere oder alle Stationen einer BSS gesendet werden, muss der Schlüssel natürlich allen bekannt sein. Man spricht hierbei von Trusted Groups, also einer Gruppe von Stationen, die sich untereinander vertrauen. Dieser Gruppen-Schlüssel ist kleiner und somit nicht so sicher wie ein Unicast-Schlüssel. Da die Anwendung von Multicasts und Broadcasts eingeschränkt ist, ist sie auch nicht so sensibel. Multicasts werden nur von APs gesendet. Will eine Station einen Multicast senden, muss sie zuerst einen Unicast an den AP senden, der die Information als Multicast weiter leitet.

In der RSN-Sicherheitsarchitektur werden für die oben beschriebenen Schlüsselarten zwei Schlüsselhierarchien definiert.

- ➊ Für die Unicasts die paarweise Schlüsselhierarchie
- ➋ Für die Multicasts die Gruppenschlüsselhierarchie

Beide Schlüsselhierarchien können sowohl auf CCMP als auch auf TKIP angewendet werden.

7.6.5 - Verfahren zur Erzeugung von Zufallszahlen

Für den Aufbau von Schlüsselhierarchien werden Zufallszahlen benötigt die mit unterschiedlichen Methoden erzeugt werden können.

7.6.5.1 - Pseudo-Random Number Generator (PRNG)

Mit Hilfe eines PRNGs können, sowohl auf Softwarebasis als auch auf spezielle Hardware, Zufallszahlen erzeugt werden die von kryptographischer Qualität sind. Das heißt bei allen möglichen Werten haben alle die selbe Wahrscheinlichkeit. Damit benötigt ein Angreifer bei 2^n möglichen Werten $2^{n/2}$ Versuche um den richtig Wert zu erraten. Da PRNGs deterministisch vorgehen, erzeugen sie bei gleichen Eingabewerten immer gleiche Ausgabewerte. Deshalb kommt dem Eingabe- bzw. Startwert besondere Bedeutung zu. Er ist anhand von möglichst vielen zufallsabhängigen Daten zu erzeugen, um eine ausreichende Zufälligkeit zu generieren.

7.6.5.2 - Pseudo-Random Function (PRF)

Mit dieser Funktion kann ein n Bit langer zufälliger Ausgabewert erzeugt werden. Als Eingabewert dient die gewünschte Länge des Ausgabewerts sowie drei weitere in ihrer Länge nicht näher festgelegte Parameter. Sie dürfen nur 128 Bytes nicht überschreiten. Die Parameter sind folgende:

Geheimer Schlüssel (K) , oder ersatzweise ein Zufallswert

Beschreibung (A) der Funktion, für die der Aufruf der PRF dient. (Z. B. „Pairwise key expansion“)

Bytefolge, bestehend aus MAC-Adresse und Zeit-Rahmen

Gewünschte Länge (n)

Damit gilt:

$$PRF-n(K, A, B) = PRF(K, A, B, n) \quad (38)$$

Zweck dieser Funktion ist einen pseudozufälligen Wert mit vorgegebener Länge zu erzeugen, der unabhängig von der Länge der Eingabewerte ist und von dem nicht auf die Eingabewerte geschlossen werden kann.

Verwendet wird dafür der Hashed Message Authentication Code (HMAC) in Kombination mit dem Secure Hash Algorithmus (SHA)-1 kurz HMAC-SHA-1. Damit kann ein 20 Byte langer Hashwert erzeugt werden.

Werden längere Werte benötigt wird der Algorithmus mit einem jeweils um 1 inkrementierten Eingabewert angewendet. Am Ende wird die Zufallszahl (Z) aus den ersten n Bits, die durch diese Funktion erzeugt wurde, verwendet.

7.6.6 - Paarweise Schlüssel

Ganz oben in der Hierarchie der paarweisen Schlüssel (also für Unicasts) steht der 256 Bit lange Pairwise Master Key (PMK). Er muss auf beiden Seiten zuerst eingerichtet werden. Dazu gibt es zwei Möglichkeiten:

- ➊ Manuelle Eingabe eines Pre-Shared Key auf beiden Seiten. Das ist wegen des manuellen Aufwands nur in kleinen WLANs sinnvoll.
- ➋ Verwendung von IEEE-802.1x. Siehe hierzu auch Abbildung 159. Dabei wird der PMK von einem AAA-Key abgeleitet, der das Ergebnis eines asymmetrischen Verschlüsselungsverfahrens ist und zwischen Supplicant und Authentifizierungsserver ausgehandelt wird. Danach wird der PMK vom Authentifizierungsserver an den Authenticator (also den AP) gesendet. Wichtig ist dabei, dass der PMK niemals über die WLAN-Schnittstelle gesendet wird und somit von einem Angreifer nicht abgefangen werden kann.

AAA steht für Authentifizierung (des Users) / Autorisierung (was darf der Benutzer) / Accounting (welche Ressourcen hat der User verwendet)

In der Hierarchie an zweiter Stelle steht der so genannten Pairwise Transient Key (PTK). Bei TKIP ist dieser Schlüssel 512 Bit lang. Bei CCMP hat der Schlüssel nur eine Länge von 384 Bits.

Der PTK wird mit der PRF aus dem PMK, der MAC-Adresse des Authenticators, und einerNonce (Zufallszahl) gebildet. DieNonce wird aus einerNonce des Authenticators (ANonce) und einerNonce des Supplicants (SNonce) mittels einerPRF-256 nach der folgenden Formel gebildet:

$$\text{Nonce} = \text{PRF-256}(\text{Zufallszahl}, \text{Init Counter}, \text{MAC-Adresse} \parallel \text{Zeit}) \quad (39)$$

Damit die beiden Nonce-Werte sowohl auf dem Client als auch auf dem Authenticator zur Berechnung des PTK vorliegen müssen diese mittels eines 4-Wege-Hanshakes ausgetauscht werden:

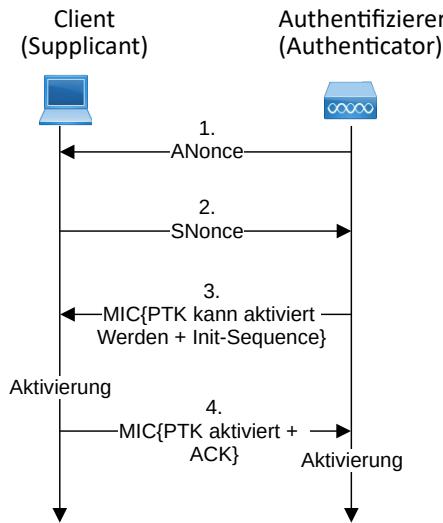


Abbildung 186: 4-Wege-Handshake zum Austausch der Nonce-Werte

1. Zuerst sendet der Authenticator den ANonce an den Supplicant. Dies erfolgt im Klartext. Damit kann der Client seinen PTK zusammenbauen und verwenden.
 2. Danach sendet der Supplicant den SNonce an den Authenticator. Dies erfolgt wiederum unverschlüsselt jedoch erfolgt mit Hilfe des zuvor berechneten EAPOL MIC-Schlüssels vorher ein Integritätscheck.
 3. Der Authenticator sendet nun eine mit MIC verschlüsselte Nachricht „Aktivierung der PTKs kann vorgenommen werden“ + Sequenznummer der künftigen MPDUs
 4. Der Supplicant bestätigt mit einer MIC-verschlüsselten Nachricht an den Authenticator die erfolgreiche Schlüsselerzeugung und aktiviert ihn.
- Nach dem Empfang und MIC-Prüfung der Nachricht aktiviert der Authenticator ebenfalls seinen PTK.

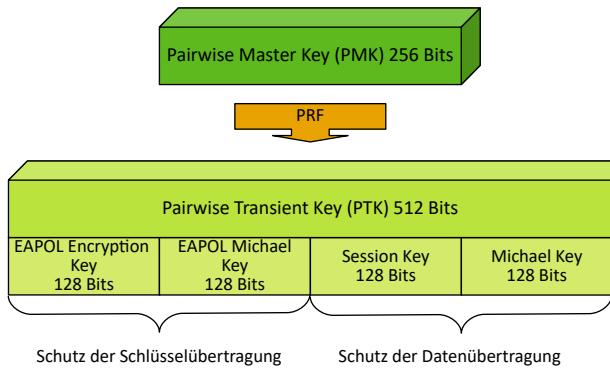
Nach dem erfolgreichen Ablauf des 4-Wege-Handshakes haben die Teilnehmer die erforderlichen temporären Schlüssel (PTKs) aktiviert. Der Standard bezeichnet diesen Status auch als Pairwise Transient Key Security Association (PTKSA) und Group Transient Key Security Association (GTKSA).

Die eigentliche Erstellung der PTKs erfolgte mit einer PRF-512 für TKIP und PRF-384 für CCMP. Sowohl die MAC-Adressen als auch die Nonce-Werte werden in aufsteigend sortierter Reihenfolge verkettet. Beim Aufruf der entsprechenden PRF kommt noch der PMK und ein Textstring dazu der darauf hinweist dass es sich um eine Erweiterung des PMK zum PTK handelt.

$$PTK = PRF - n(PMK, \text{Pairwise key extension}, MAC\ 1 \| MAC\ 2 \| \text{Nonce}\ 1 \| \text{Nonce}\ 2) \quad (40)$$

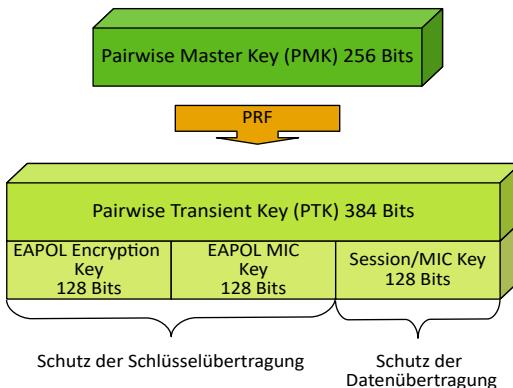
Mit der nun sicheren Verbindung kann die Erstellung der Gruppenschlüssel vorgenommen werden

Der PTK wird anschließend zur Erzeugung von 4 temporären Schlüsseln bei TKIP und 3 temporären Schlüsseln bei CCMP zerlegt. Bei beiden Fällen werden die ersten beiden Schlüssel zur Integritätssicherung von EAPOL (EAP over LAN) und damit zum Schutz der Schlüsselübertragung genutzt.



Bei TKIP werden für die Datenübertragung zwei 128 Bit lange Schlüssel (Session Key und Michael Key) verwendet. Der Michael Key wird hier nochmals in zwei 64 Bit lange Teile zerlegt. Der erste Teil dient den Stationen welche die Authentifizierung übernommen haben (im allgemeinen sind das die APs, somit der Authenticator). Der zweite Teil wird von den anfragenden Stationen (Suplicants) verwendet.

Abbildung 187: TKIP - Pairwise Key Hierarchie



Bei CCMP kommt nur ein 128 Bit langer Schlüssel für die Datenübertragung zum Einsatz. Deshalb ist der PTK kürzer.

Abbildung 188: CCMP - Pairwise Key Hierarchie

7.6.7 - Gruppenschlüssel

Wie der Pairwise Master Key (PMK) wird nur der Group Master Key (GMK) erstellt. Die Erstellung gestaltet sich nun einfacher, da bereits sichere Verbindungen über die Pairwise Keys vorhanden sind. Sie wird vom Authenticator vorgenommen.

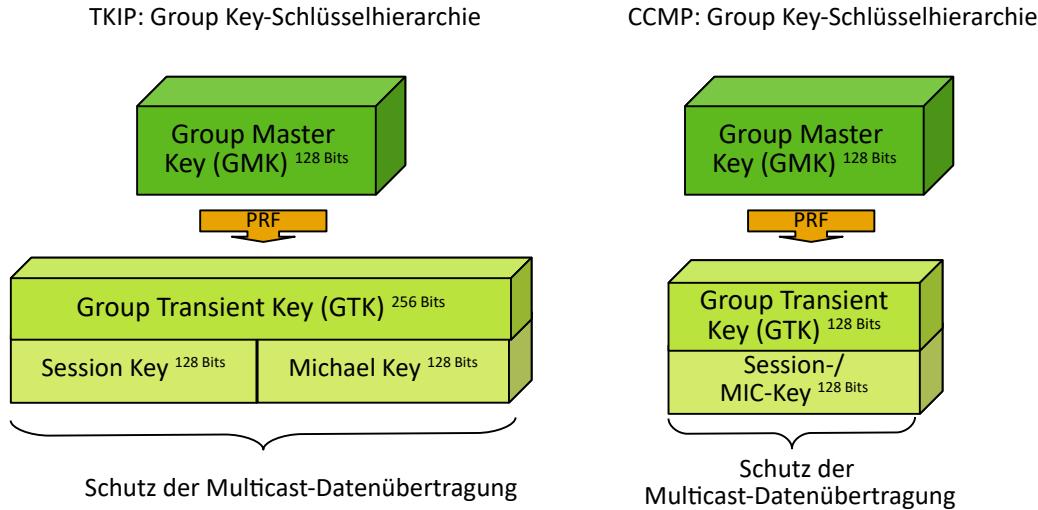


Abbildung 189: Group Key Schlüsselhierarchie

So benötigt der Aufbau der Group Key Schlüsselhierarchie nur einen 2-Wege-Handshake.

7.6.8 - Schlüsselwechsel

Verlässt ein Client ein Netzwerk, teilt er das dem AP mit, der daraufhin das Senden an den Client einstellt und den paarweisen Schlüssel für den Client löscht. Auf Clientseite ist keine Aktivität erforderlich.

Problematisch wird es hingegen beim Gruppenschlüssel. Auch nach dem Abmelden des Clients kann er ihn noch nutzen. Deshalb muss er vom AP neu erstellt und an die Clients verteilt werden. Da dies zentral vom AP gemacht wird hält sich der Aufwand in Grenzen. Allerdings kann bei erhöhter Fluktuation von Clients ein Problem entstehen. Solange die Gruppenschlüssel verteilt werden können die Clients keine Multicasts und Broadcasts empfangen. Erst wenn der letzte Client den neuen Gruppenschlüssel hat, können alle Clients wieder mit dem neuen Gruppenschlüssel arbeiten. Dieses Problem wird mit einer alten WEP-Eigenschaft gelöst, bei der bis zu 4 Schlüssel mittels einer Key-ID (KID) verwaltet werden konnten. Der auf dem Client gespeicherte Gruppenschlüssel hat die KID = 0. Damit sind 3 weitere Gruppenschlüssel möglich. Während der AP die neuen Gruppenschlüssel verteilt sendet er Multicasts und Broadcasts noch mit dem alten Gruppenschlüssel. Sobald der neue Gruppenschlüssel verteilt ist sendet er mit dem neuen Schlüssel und deaktiviert den alten Gruppenschlüssel bei sich und den Clients. Dies sorgt dafür, dass vor allem bei Audio- und Videostreaming-Diensten keine Beeinträchtigungen erfolgen.

7.6.9 - Temporal Key Integrity Protocol (TKIP)

Bei der Einführung von IEEE-802.11 war das Thema Sicherheit zwar betrachtet und abgehandelt worden, jedoch war die Implementierung schlecht gelungen. Das führte schnell zur Aufdeckung von Sicherheitsrisiken und in der Folge zu Akzeptanzproblemen. Die Industrie war also an einer schnellen Lösung interessiert, die vor allem auf der bisherigen Hardware implementiert werden konnte und somit einen Investitionsschutz bot. Im ersten Wurf, beim Wi-Fi Protected Access (WPA) war TKIP zentraler Bestandteil der Sicherheitsarchitektur.

TKIP wurde aus Gründen der Weiterverwendung alter Hardware als Option auch im IEEE-802.11i eingeführt. TKIP sollte deshalb auf der neuen RSN-Hardware nur für den Mischbetrieb verwendet werden.

7.6.10 - Verschlüsselung mit TKIP

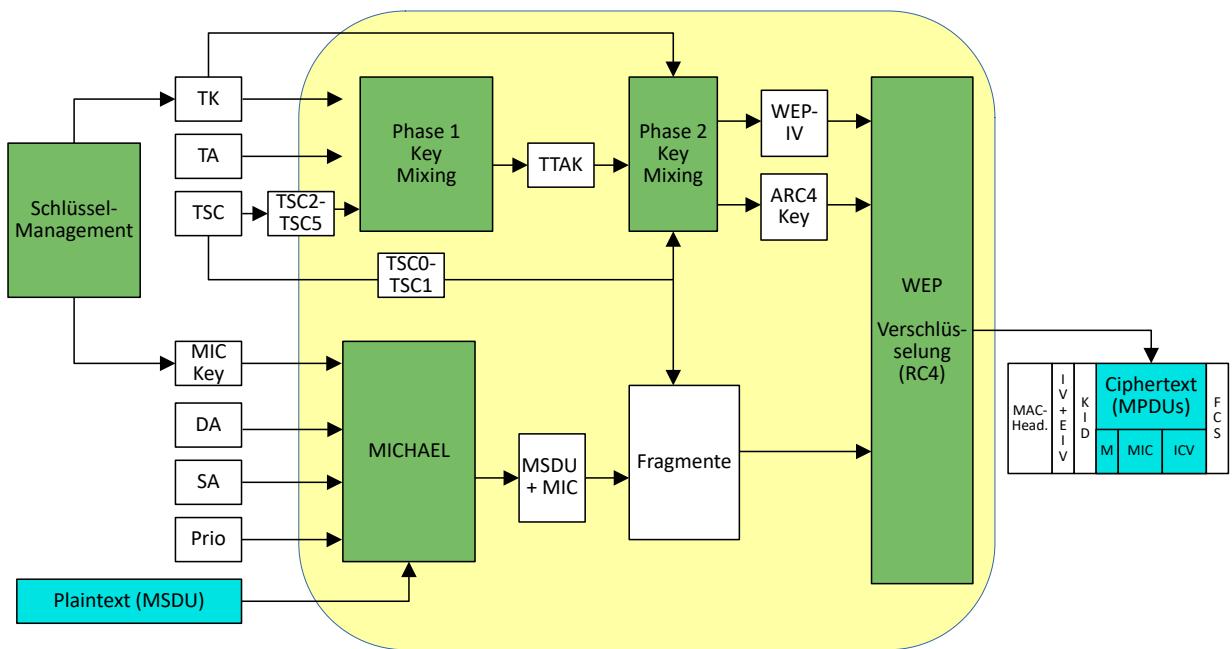


Abbildung 190: TKIP-Verschlüsselung

Das Schlüsselmanagement stellt den Michael Key (MIC Key) und den Session Key (TK) zur Verfügung. Der Michael Key dient zur Sicherung der Datenintegrität während der TK der Datenverschlüsselung dient. Die zu übertragenden Daten werden in Form der MSDU zugeführt. Mithilfe der Source-MAC-Adresse (SA), der Destination-MAC-Adresse (DS), der Priorität wird zusammen mit dem Michael Key mittels der Michael-Hash-Funktion der TKIP Message Integrity Code (MIC) errechnet und an die MSDU angehängt. Der MIC verlängert die MSDU um 8 Bytes, was zu einer zusätzlichen Fragmentierung führen kann.

TKIP sorgt mit dem 6 Byte großen TKIP Sequence Counter (TSC) dafür, dass die Fragmente eine aufsteigende Reihenfolge haben. Damit kann dem Einfügen von Paketen durch Angreifer entgegengewirkt werden. Der TSC wird im Header im Klartext im IV und im EIV gesendet. Siehe hierzu auch Kapitel Transport der Daten-Bits mit TKIP.

Die Erstellung des Schlüssels erfolgt in zwei Phasen.

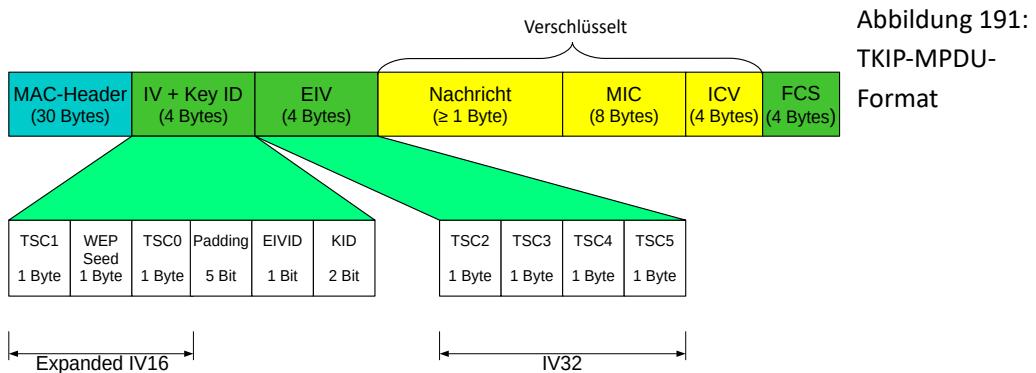
In der ersten Phase wird aus dem Session Key (TK), der Transmitter Adresse (TA) und dem IV32-Teil (höherwertiger Teil) des TSC ein Zwischenschlüssel mit 80 Bits ($5 * 16$ Bit) namens TKIP-mixed transmit address and key (TTAK) erzeugt. Der TTAK-Zwischenschlüssel kann bis zum Ende der Session beibehalten werden. Es gibt jedoch auch Gründe für eine Neuberechnung.

Für jede zu erzeugende MPDU wird in einer zweiten Phase ein eigener Schlüssel, der so genannte Per Packet Key (PPK) erstellt, der sich aus dem PRNG-ARC4-Key und dem IV16-Teil des TSC zusammensetzt. Da zur Erzeugung

des ARC4-Key nur der IV16-Teil (niederwertiger Teil) des TSCs inkrementiert wird, kann er auf Vorrat errechnet und zwischengespeichert werden. Bei einem Überlauf ist der höherwertige Teil TSC zu inkrementieren.

Die eigentliche Verschlüsselung erfolgt dann nach dem bekannten WEP-Verfahren (RC4).

7.6.11 - Transport der Daten-Bits mit TKIP



Bei TKIP wird der IV (IV16) um einen Extended IV (EIV) mit 32 Byte ergänzt (IV32), der zwischen dem IV und der verschlüsselten MPDU eingefügt wird.

Zusätzlich ist im verschlüsselten Teil der 8 Byte große Message Integrity Code (MIC) zwischen Nachricht (MSDU) und dem Integrity Check Value (ICV) eingefügt.

Um zu erkennen, ob ein EIV eingefügt wurde, musste eine Kennung dafür geschaffen werden. Dafür wurde aus dem 6 Bit großen Padding ein Bit namens EIVID spendiert. Ist es auf 1 gesetzt, ist ein EIV eingefügt. Hat die EIVID den Wert 0, handelt es sich um einen mit WEP verschlüsselten Frame.

Ist der Wert der Key-ID (KID) = 0 handelt es sich um ein pairwise verschlüsselten Frame für einen Unicast. Bei den Werten 1 bis 3 handelt es sich um Gruppenschlüssel.

Das erste und dritte Byte des IV sowie die vier Bytes des EIV werden zur Übermittlung des TSC verwendet. Dabei werden die 6 Bytes des TSC nach steigender Signifikanz der Bits eingefügt. Nur TSCO und TSC1 werden im IV getauscht um schwachen RC4-Schlüsseln entgegen zu wirken.

Das zweite Byte im IV (WEP Seed) wird nicht für Erstellung des TSC verwendet und ist nur eine Kopie von TSC1 bei der Bit B0 immer auf 0 und Bit B6 immer auf 1 gesetzt werden. WEP-Seed = (TSC1 | 0x20) & 0x7F.

7.6.12 - Entschlüsselung mit TKIP

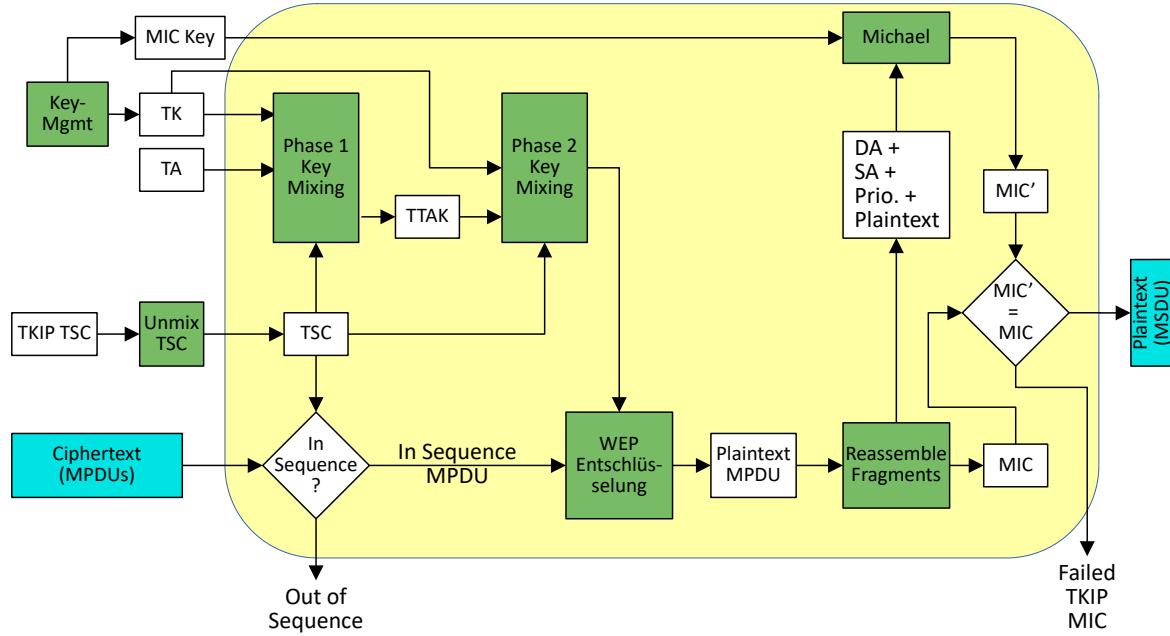


Abbildung 192: TKIP Entschlüsselung

Zuerst wird aus dem IV und dem EIV der TSC ermittelt und überprüft ob er aufsteigend ist. Bei Unstimmigkeiten wird der Frame verworfen.

Wie bei der Verschlüsselung wird bei der Phase 1 aus dem Session Key (TK), der Transmitter Adresse (TA) und dem TKIP Sequence Counter (TSC) der TTAK erzeugt.

Das Ergebnis der Phase 2 ist der WEP Seed (WEP IV und ARC4 Key). Der WEP Seed wird zusammen mit dem MPDU für die Entschlüsselung verwendet. Das Entschlüsselungs-Ergebnis sind MPDUs die evtl. noch fragmentiert sind. Deshalb schließt sich eine evtl. erforderliche Reassemblierung an.

Die Reassemblierten Frames (DA, SA, Priorität und der der Plaintext MSDU) werden im Michael-Verfahren zusammen mit dem MIC Key zu einem MIC'.

Am Ende vergleicht die MIC-Überprüfung den MIC aus den reassemblierten Daten und den MIC'. Sind beide gleich, werden die Daten als MSDU an die überlagerte Schicht übergeben. Sind MIC und MIC' ungleich werden die Daten verworfen.

7.6.13 - MIC-Fehler

Wird innerhalb von 60 Sekunden mehr als ein MIC-Fehler erkannt, wird eine Attacke angenommen und es deassoziiieren sich die Stationen oder der AP deassoziiert die betroffene Station. Das ist abhängig von der Senderichtung und somit von dem Gerät, das die MIC-Fehler erkennt.

Wurde ein MIC-Fehler von einer Station erkannt, sendet sie einen MIC-Failure-Report-Frame an den AP. Wurden wiederholte MIC-Fehler vom AP erkannt, werden die PTK und der GTK verworfen. Damit müssen sich alle Stationen neue authentifizieren.

Der neue GTK wird erst nach 60 Sekunden wieder freigegeben.

Nun kann es jedoch sein, dass es tatsächlich Übertragungsfehler gab, die als MIC-Fehler interpretiert werden. Um das auszuschließen, werden vor der MIC-Überprüfung die FCS, der ICV und der TSC einer MPDU überprüft. Sind bereits hierbei Fehler erkennbar, handelt es sich um einen Übertragungsfehler und es wird kein MIC-Fehler registriert.

Leider kann mit der forcierten Erzeugung von MIC-Fehlern ein DoS-Angriff durchgeführt werden. Wer es schafft den TSC richtig zu inkrementieren und zusätzlich einen MIC-Fehler zu erzeugen, kann den Zugriff auf einen AP für 60 Sekunden zu unterbinden. (Die TSC-Überprüfung läuft vor der MIC-Überprüfung)

7.7 - CCMP

Das TKIP-Verfahren war von Anfang an eine temporäre Zwischenlösung um alte Hardware weiter betreiben zu können. TKIP wurde dazu in Form von Treibern, also als Softwarelösung, realisiert. Mit dem erhöhten Software-Aufwand wurde zwar die Sicherheit verbessert, jedoch auch die Performance beeinträchtigt.

Das darauf hin als Ziel anvisiertes Verschlüsselungsverfahren für IEEE-802.11i ist der Advanced Encryption Standard (AES) den das National Institute of Standards and Technology (NIST) im November 2001 mit einem aufwändigen Auswahlverfahren ausgewählt hatte. AES verwendet zur Verschlüsselung den Rijndael-Algorithmus. Das ist eine Block-Chiffre, die Blöcke mit unterschiedlichen Längen verschlüsseln kann. Es sind auch Schlüssel mit unterschiedlichen Längen möglich. Im 802.11i-Standard wurde sowohl die Blocklänge, als auch die Schlüssellänge, auf 128 Bit festgelegt. RC4 verschlüsselt dagegen Bitweise.

Die Daten die bei WLANs zu verschlüsseln sind haben eine Länge zwischen 64 und 1500 Bytes. Daher müssen die Daten vor der Verschlüsselung in Blöcke aufgeteilt werden. Dazu gibt es wiederum verschiedene Modi.

Die für WLANs festgelegte Modi sind der Counter-Modus (CTR) zusammen mit dem Cipher Block Chaining – Message Authentication Code (CBC-MAC) für die Integritätssicherung kurz CCM-Mode festgelegt. CCM ist im RFC 3610 beschrieben. Das damit realisierte Protokoll heißt CCM Protocol (CCMP) (Ausgeschrieben CTR/CBC-MAC Protocol). CCM gibt es bei 802.11i in zwei Ausprägungen mit je 2 Parametern

Tabelle 65: CCM-Parameter

	Parameter	
CCM-Version	M	L
CCM-128	8 = MIC hat eine Länge von 8 Bytes	2 = MPDU-Längen-Feld ist 2 Bytes groß
CCM-256	16 = MIC hat eine Länge von 16 Bytes	2 = MPDU-Längen-Feld ist 2 Bytes groß

Wegen den unterschiedlichen M-Parameter ist die Länge des MIC-Feldes im verschlüsselten Teil einer CCMP-MPDU variabel und hat eine Länge von 8 oder 16 Bytes.

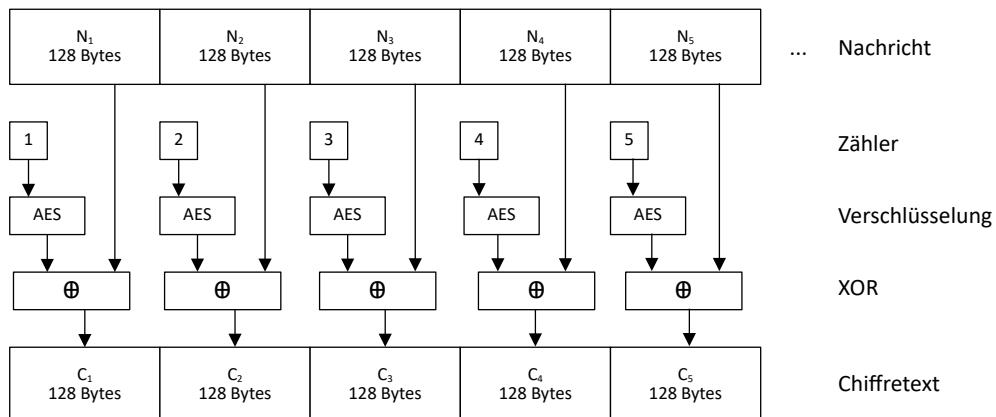


Abbildung 193: CCMP-CTR-Mode

Der CTR-Mode hat seinen Namen von einem Zähler (Counter) auf den die AES-Verschlüsselung angewendet wird. Es wird also nicht die Nachricht mit AES verschlüsselt, sondern ein Zähler. Das Ergebnis der Verschlüsselung wird dann mit einem Nachrichten-Block mit XOR-Verknüpft. Der Zähler wird mit einem Nonce-Wert initialisiert der im Kapitel Verschlüsselung mit CCMP beschrieben wird.

Das Chiper-Block-Chaining übernimmt die Aufgabe des Message Authentication Code (MAC). Bei IEEE-802.11i wurde allerdings aus MAC, um eine Verwechslung mit einer MAC-Adresse zu vermeiden, der Message Integrity Code (MIC).

7.7.1 - Verschlüsselung mit CCMP

Im Gegensatz zu TKIP wird die Verschlüsselung nicht auf MSDU-Ebene sondern auf MPDU-Ebene durchgeführt. Deshalb muss eine evtl. erforderliche Fragmentierung vorher durchgeführt werden.

Während TKIP für die Daten-Verschlüsselung und die Sicherung der Datenintegrität zwei Schlüssel verwendet, wird bei CCMP nur ein temporärer Schlüssel (TK) für beide Vorgänge verwendet. Das stellt aus kryptographischer Sicht eine Schwachstelle dar. Um das Problem zu beheben fließt in die Verschlüsselung ein 13 Byte langer Nonce-Wert ein. Entscheidend ist, dass der Nonce-Wert während einer Sitzung einmalig ist. Deshalb wird er aus der Sender-MAC-Adresse, der Priorität und einer Sequenznummer, die Packet Number (PN) genannt wird, gebildet.

Die PN ist ein 48 Bit lange positive Integer-Zahl welche die Basis für den Replay-Schutz bildet. Der PN darf sich während der Nutzung eines temporären Schlüssels auf einer Übertragungsrichtung niemals wiederholen. Deshalb wird die PN vom Sender auf den Startwert 1 gesetzt sobald der temporäre Schlüssel initialisiert oder erneuert wird und bei jeder MPDU um 1 inkrementiert.

Zum Schutz vor Replay-Attacken wird für jede Pairwise Transient Key Security Association (PTKSA), Group Transient Key Security Association (GTKSA) und Station To Station Key Security Association (STKSA) ein eigener PN-Counter geführt und mit den zugehörigen MPDUs inkrementiert.

Der PN-Counter wird bei der Schlüsselinitialisierung auf 0 gesetzt. Es wird von einem wiederholt empfangenen Frame ausgegangen wenn die empfangene PN geringer oder gleich dem aktuellen Wert des PN-Counters ist.

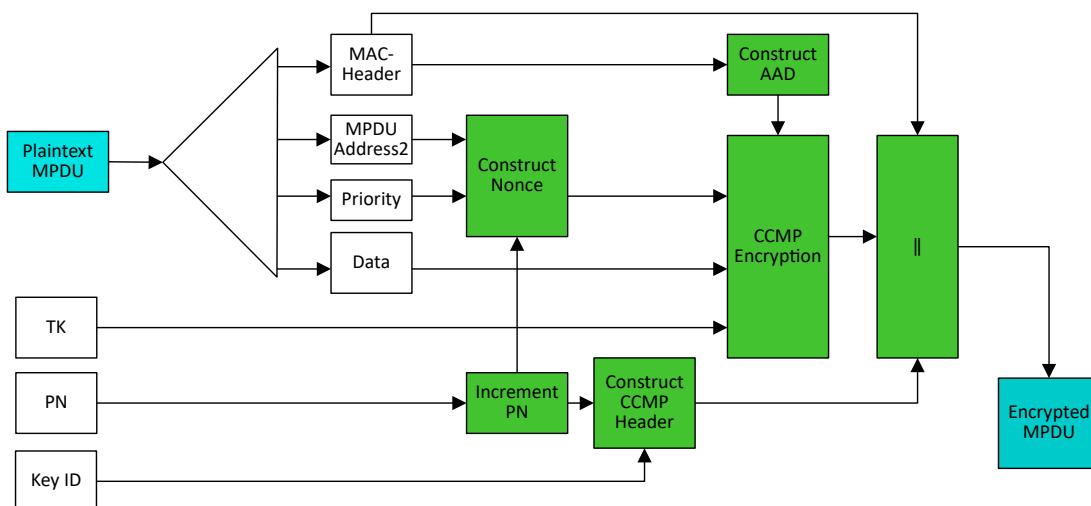


Abbildung 194: CCMP - Verschlüsselung

7.7.1.1 - Ablauf der Verschlüsselung

1. Packet-Number-Counter (PN) wird für jede MPDU inkrementiert.
2. Erstellung des Additional Authentication Data (AAD) für das CCM-Verfahren. (Siehe unten CCMP-MIC-Berechnung)
3. Erstellung des Nonce-Blocks aus der Sender-MAC-Adresse, der Priorität und dem PN.
4. Erstellung des CCMP-Headers aus dem PN und der Key-ID (KID).
5. Aus dem temporären Schlüssel (TK), der AAD, dem Nonce und den MPDU-Daten wird der Ciphertext und der MIC mit der CCMP Encryption erzeugt.
6. Aus dem Original-MPDU-Header, dem CCMP-Header und den verschlüsselten Daten wird die verschlüsselte MPDU erzeugt.

7.7.1.2 - CCMP-MIC-Berechnung

Die MIC-Berechnung erfolgt mit dem Cipher-Block-Chaining (CBC-MAC)-Verfahren. Dazu werden die Daten in 128 Bit lange Blöcke aufgeteilt. Teile des MPDU-Headers werden vorher zu den Additional Authentication Data (AAD) zusammengesetzt und bei der MIC-Berechnung berücksichtigt. Mit den AAD wird die Authentizität der MPDU sichergestellt. Die Teile des MPDU-Headers, die sich bei einer wiederholten Frame-Übertragung ändern würden werden auf 0 gesetzt.

Aus Abbildung 195 kann entnommen werden welche Teile des MPDU-Headers für die AAD verwendet werden. Je nachdem, welche Felder Verwendung finden, hat die AAD eine Länge von 22 bis 28 Bytes.

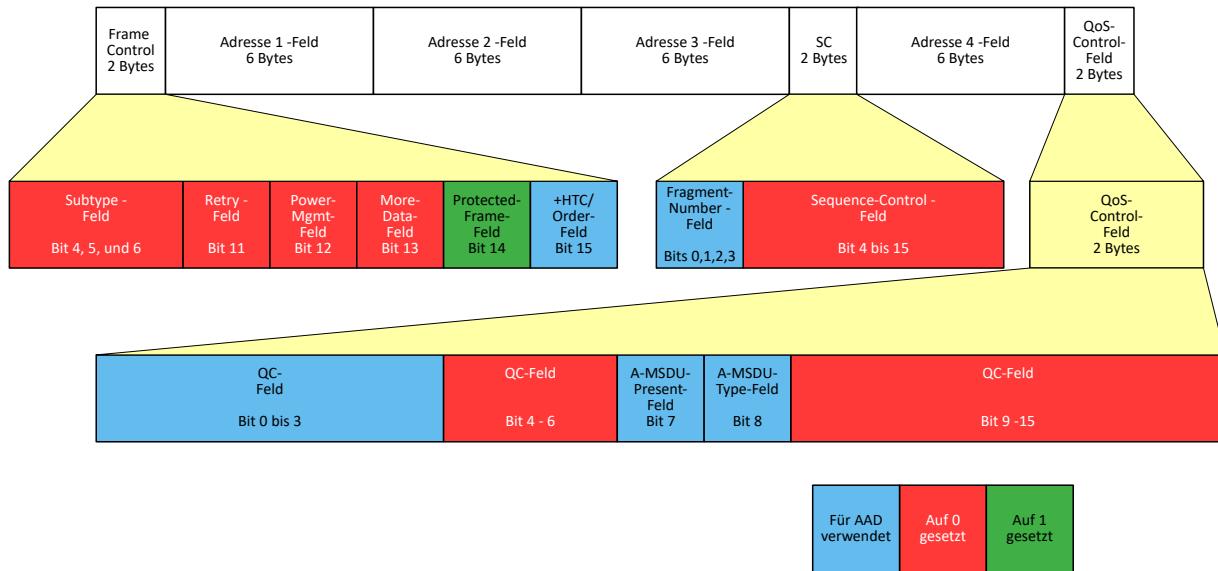


Abbildung 195: Verwendung des MPDU-Headers für den Aufbau der AAD

Die MIC-Berechnung erfolgt, indem der erste Block mit AES verschlüsselt wird. Das Ergebnis wird mit dem zweiten Block XOR-verknüpft. Danach wird das mit AES verschlüsselt und so weiter. Siehe hierzu auch Abbildung 196.

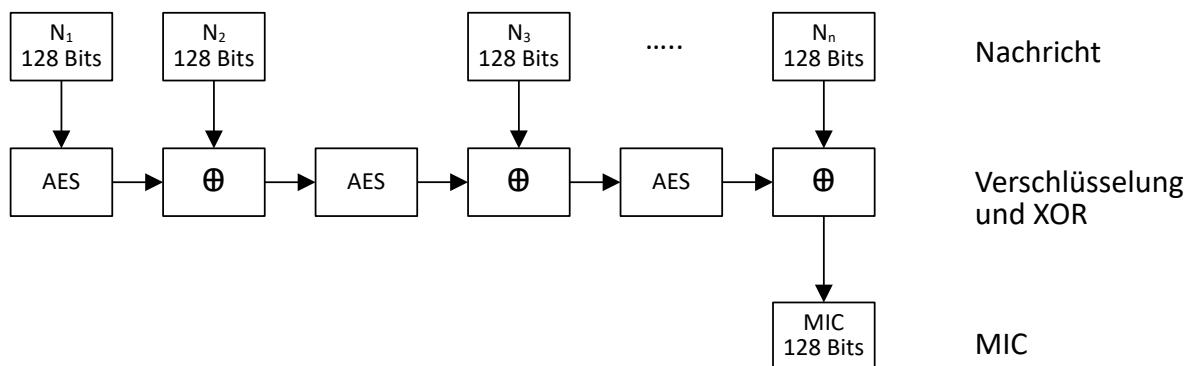


Abbildung 196: CCMP-MIC-Berechnung

7.7.2 - Transport der Daten mit CCMP

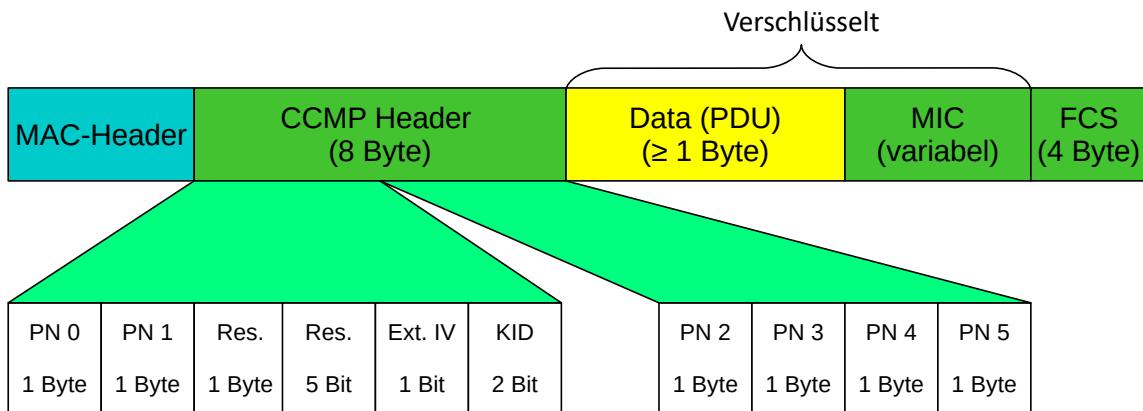


Abbildung 197: CCMP-MAC-Frame

Je nachdem welche CCM-Verschlüsselung vorgenommen wurde, hat das MIC-Feld eine Länge von 8 oder 16 Bytes. Sieh hierzu auch Tabelle 65.

7.7.3 - Entschlüsselung mit CCMP

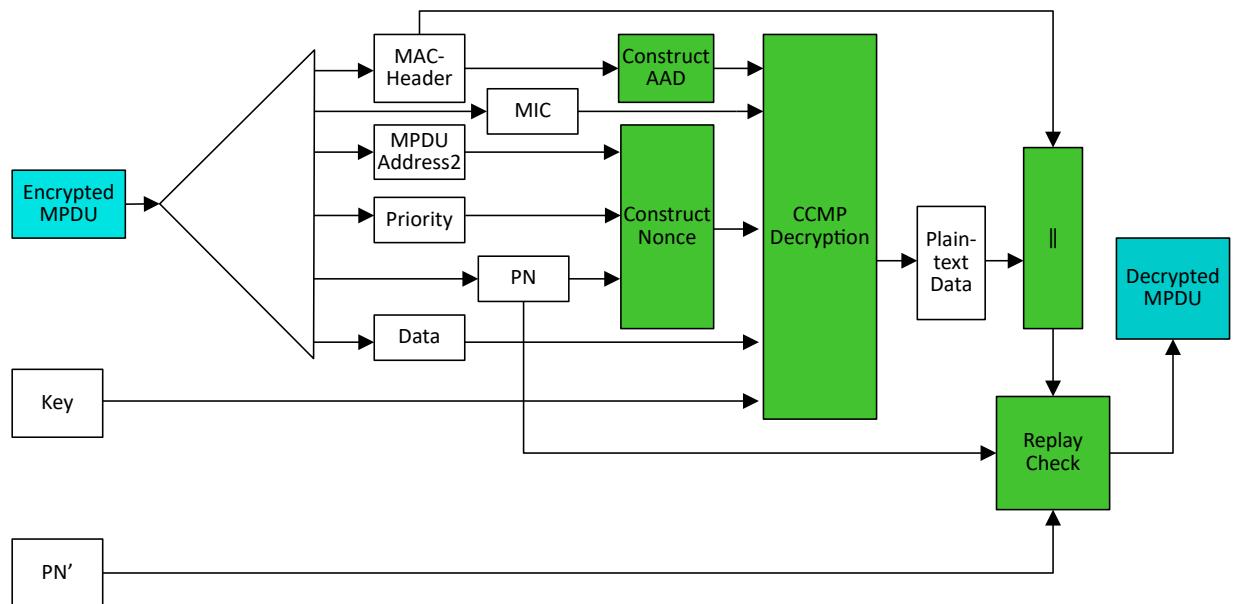


Abbildung 198: CCMP - Entschlüsselung

Der Ablauf der Entschlüsselung ist folgender:

1. Aus der verschlüsselten MPDU werden die AAD, der Nonce, der MIC und die PN ermittelt.
2. Bei der CCMP-Entschlüsselung wird der Plaintext ermittelt sowie der Integrity-Check durchgeführt.
3. Danach wird der MAC-Header vorangestellt.
4. Am Ende findet mit dem PN und dem selbst verwalteten PN' ein Replay-Check statt.
5. Verläuft der Replay-Check erfolgreich, werden die MPDU ausgeliefert.

7.7.4 - Broadcast / Multicast Integrity Protocol (BIP)

Für Frames, die mit Gruppenschlüsseln gesichert werden, erfolgt ein ähnlicher Ablauf wie bei den Frames die mit Pairwise Keys gesichert wurden. Allerdings ist hierbei etwas weniger aufwand erforderlich. Die Verwaltung läuft über die Integrity Group Temporal Key Security Association (IGTKSA)

7.8 - WPA3

Nachdem WPA2 viele Jahre ein sicherer Standard war wurde im Jahre 2017 mit der KRACK-Sicherheitslücke eine Schwachstelle offen gelegt.

Am 25. Juni 2018 wurde als nächster Schritt bei der Verbesserung der Sicherheit WPA3 vorgestellt. WPA3 setzt mit der Implementierung des sogenannten Dragonfly-Protokolls als Verschlüsselungsmethode Simultaneous Authentication of Equals (SAE) ein. Damit muss nicht nur ein Client sich beim AP authentifizieren, sondern auch der AP beim Client, was einen Man-in-the-Middle-Angriff beim Verbindungsauftbau ausschließt.

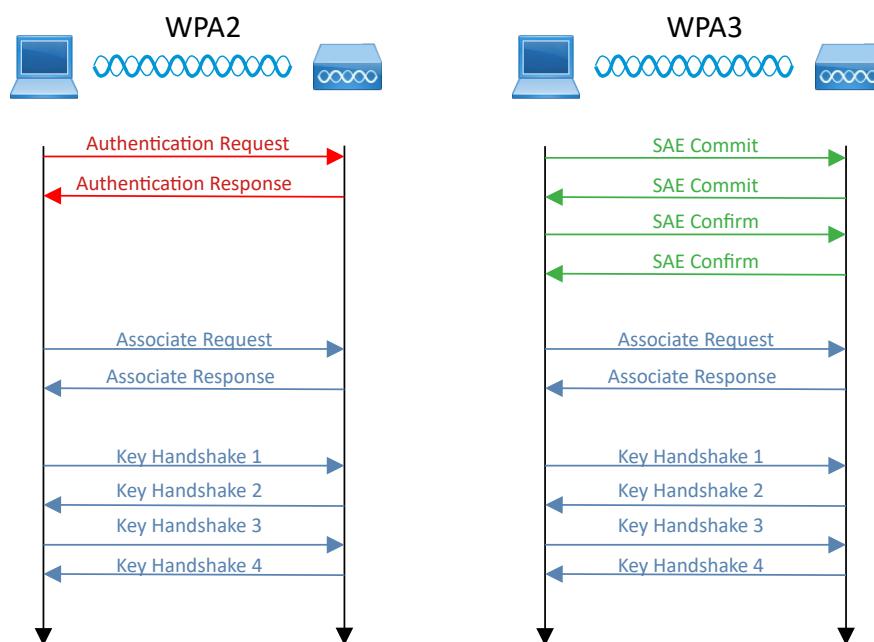


Abbildung 199: Vergleich WPA2 mit WPA3

Zusätzlich wird durch Protected Management Frames (PMF) eine erhöhte Sicherheit beim Anmeldevorgang geschaffen. PMFs waren bei einigen Herstellern schon optional bei WPA2 möglich und ist nun verpflichtend. Damit können Management Frames nicht mehr gefälscht werden.

Wie bei den Vorgängerversionen von WPA3 gibt es auch hier einen Personal-Mode und einen Enterprise-Mode. Im Enterprise Mode gibt es WLAN-User mit individuellem Passwort und es kommt eine stärkere Verschlüsselung mit 192 Bit-Schlüsseln zum Einsatz.

Allerdings ist WPA3 nicht das Ende der Fahnenstange. Anfang April 2019 demonstrierten die Forscher Mathy Vanhoef (NYUAD) und Eyal Ronen (Tel Aviv University & KU Leuven) in ihrem Paper „Dragonblood: A Security Analysis of WPA3's SAE Handshake“ mehrere Schwachstellen, wie etwa eine Downgrade-Attacke mit denen sich die neuen Funktionen umgehen lassen. Weiterhin ließen sich Schwachstellen des Dragonfly Protokolls selbst ausnutzen.

7.9 - Angriffs-Szenarien

7.9.1 - Daten-Umleitung

Mit den oben aufgeführten Methoden können z. B. IP-Header verändert werden. Damit ist es möglich die Ziel-IP-Adressen zu verändern. Die veränderte Ziel-IP-Adresse kann die IP-Adresse eines bereits kompromittierten Rechners sein. Selbst eine Firewall bietet in einem solchen Fall keinen Schutz, da ausgehender Verkehr normalerweise nicht gefiltert wird.

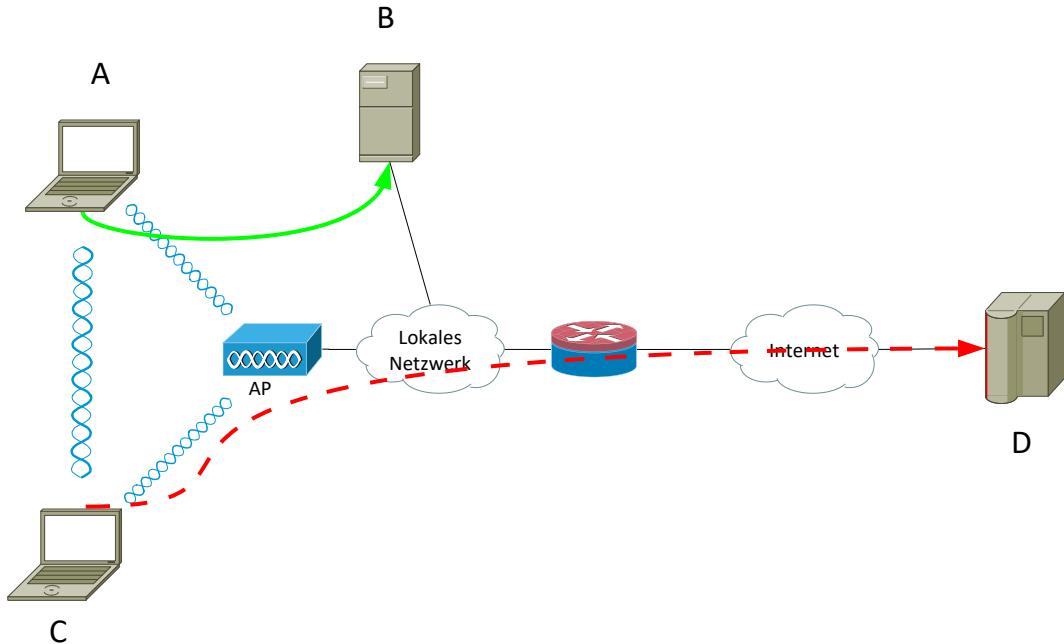


Abbildung 200: WLAN Daten-Umleitung

Im obigen Beispiel sendet das Notebook A an den Server B Daten (grüne durchgehende Linie). Der Spion mit dem Notebook C kann diese Daten mitlesen und modifizieren. Über einen vorhandenen Router werden anschließend die Daten an einen komromittierten Router im Internet weiter geleitet (rote gestrichelte Linie). Dies geschieht unter Ausnutzung der vorhandenen WLAN-Infrastruktur.

7.9.2 - Replay (Wiederholung von Paketen)

IEEE-802.11 kennt keine Mechanismen zum Schutz vor Wiederholungen. In diesem Fall braucht ein Angreifer die Daten nicht einmal zu entschlüsseln. Es reicht aus, die Daten noch einmal zu senden, um große Verwirrung zu stiften. So kann eine wiederholte Druckausgabe in einem unbeobachteten Moment vertrauliche Informationen zutage bringen.

7.9.3 - Wörterbuch mit Schlüsselsequenzen

Um Daten zu entschlüsseln, reicht die Schlüsselsequenz aus. Da zu jeder Schlüsselsequenz ein eindeutiger Initialisierungsvektor gehört, kann man sich vorstellen, dass ein Angreifer sich ein Wörterbuch mit folgendem Inhalt zusammenstellt:

IV1	-	Schlüsselsequenz 1
IV2	-	Schlüsselsequenz 2
IV3	-	Schlüsselsequenz 3
..	-	..

Dies ist durchaus realistisch, wenn man lange genug Zeit dazu hat. Sobald die Schlüsselsequenz nochmals Verwendung findet, kann das Chiffrat direkt entschlüsselt werden.

Dagegen kann nur durch einmalige Verwendung der Schlüsselsequenz vorgegangen werden. Die Schlüssel sind dazu, möglichst automatisch, ständig auszutauschen.

7.9.4 - Known-Plain-Text Angriff

Eine Schlüssel-Sequenz kann durch eine einfache XOR-Operation aus dem Chiffrat und dem Klartext ermittelt werden. Sobald der Angreifer in den Besitz eines Klartextes kommt, hat er keine Probleme die IV bereits gewonnen.

Im folgenden Beispiel hat der Angreifer C es geschafft, einen Klartext auf dem Server C abzulegen. Jetzt muss er nur noch A dazu bringen, den Text vom Server zu laden. Sobald A dies tut, wird der Text als Chiffrat über das WLAN übertragen. Hier kann der Angreifer den verschlüsselten Text wieder abgreifen. Da er nun den Klartext und das Chiffrat kennt, kann leicht durch die XOR-Operation die Schlüsselsequenzen ermitteln und Wörterbücher für Schlüsselsequenzen anlegen.

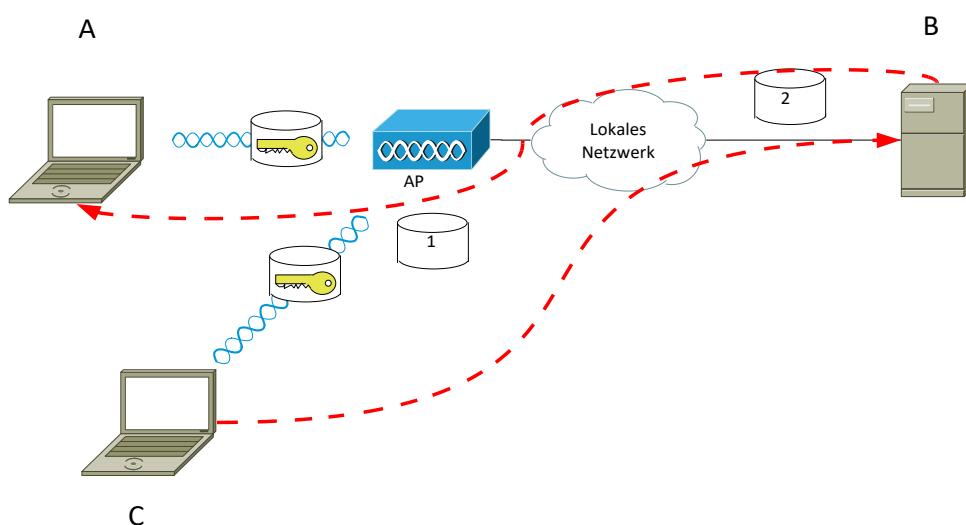


Abbildung 201: WLAN Known-Plain-Text Angriff

7.9.5 - Schwache Schlüssel

Leider gibt es beim RC4-Algorithmus 256 so genannte „schwache Schlüssel“. Eine Schlüsselsequenz ,die mit einem solchen Schlüssel erzeugt wurde, kann Rückschlüsse auf den Schlüssel selbst ermöglichen. WEP vermeidet diese schwachen Schlüssel nicht.

In einem Papier von Fluhrer, Mantin und Shamir wird nachgewiesen, dass aus den ersten beiden Bytes eines Chiffrats der geheime Schlüssel zurückgerechnet werden kann. Nach wenigen Stunden kann der geheime Schlüssel entdeckt werden. Danach kann der gesamte verschlüsselte Datenverkehr mit gelesen und sogar vom Angreifer selbst verschlüsselt werden. Dieses Verfahren wird z. B. von

<http://sourceforge.net/projects/wepcrack>

verwendet.

Am einfachsten wäre es nun, diese Schlüssel einfach zu vermeiden und erst gar nicht zu verwenden. Eine automatisierte Schlüsseländerung wäre ebenfalls ein gutes Mittel dagegen. Dann könnte ein geknackter Schüssel nur dazu verwendet werden, den bereits aufgezeichneten Datenverkehr rückwirkend zu entschlüsseln.

Hersteller wie Enterasys haben mit WEPplus auf die Verwendung verzichtet, was übrigens immer noch standardkonform ist.

7.9.6 - IV-Kollisionen

Im Standard ist keine Aussage darüber gemacht, wie der IV zu initialisieren ist. Die meisten Hersteller beginnen deshalb bei Null den Zähler zu realisieren. Deshalb starten diese Stationen nach jedem Reset mit den gleichen IVs. Dies ist der Grund für eine große Wahrscheinlichkeit für die Verwendung kleiner IVs. Wenn nun mehrere Stationen mit dieser Vorgehensweise hintereinander mit dem Datenverkehr beginnen, dann werden über einen längeren Zeitraum immer wieder die gleichen RC-4-Schlüssel verwendet. Dies macht es einem Angreifer sehr leicht, mit wenigen Schlüsselsequenzen den gesamten Datenverkehr abzuhören. Man spricht dann von IV-Kollisionen.

7.9.7 - Einschleusen von Nachrichten

Da der Standard Wiederholungen von Schlüsseln nicht untersagt, kann eine einmal entschlüsselte Schlüsselsequenz jederzeit wieder verwendet werden. Jeder Empfänger wird eine damit verschlüsselte Nachricht akzeptieren. Dies ist zwar mit einer Modifikation von Treibersoftware verbunden, jedoch nicht unmöglich. Einzelne Datenpakete zu erstellen und vorhersehbare Reaktionen eines Netzwerks , wie z. B. DNS-Anfragen, können leicht damit bewerkstelligt werden.

7.9.8 - Denial-of-Service

Bereits mit ein Mikrowellenofen, der einen Defekt in der Isolation aufweist, reicht aus, um ein WLAN im 2,4 GHz-Band zu stören.

Management- oder Controlframes werden nicht verschlüsselt. Dies führt dazu, dass sie durch die Empfänger nicht authentisiert werden können. Mit CTS-Frames ohne vorausgegangene RTS-Anforderungen kann das WLAN-Zugangsverfahren korrumptiert werden. Allerdings ist auch hier die Sendersoftware zuvor zu modifizieren.

7.9.9 - Man-in-the-Middle

Damit lassen sich Pakete mitschreiben. Ein Angreifer gibt sich einem Client gegenüber als AP aus . Dem AP gegenüber gibt sich hierbei der Angreifer als Client aus.

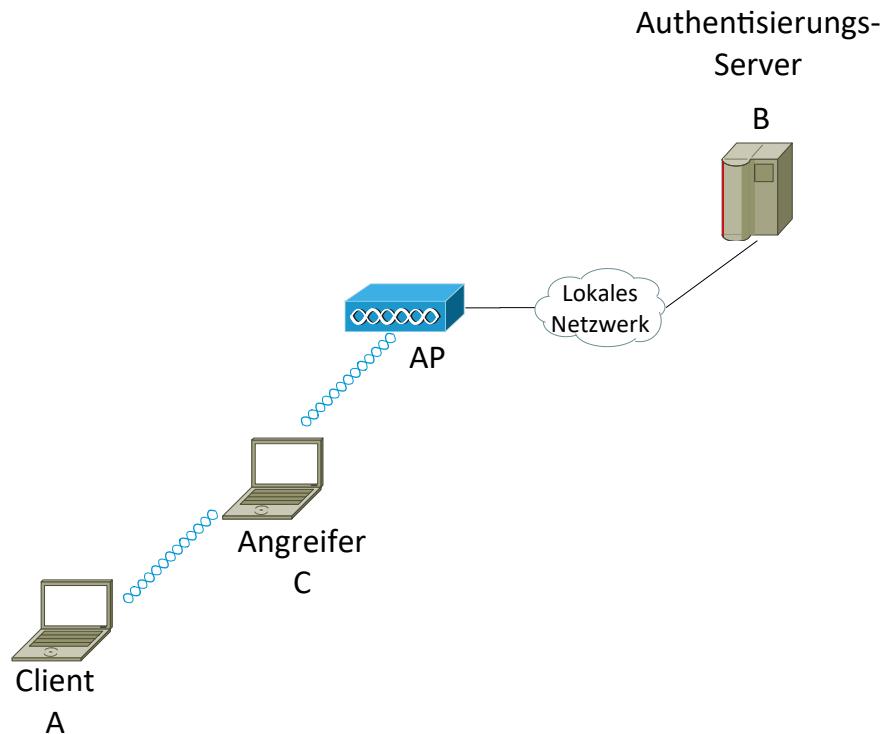


Abbildung 202: WLAN Man-in-the-Middle

7.9.10 - Session Hijacking

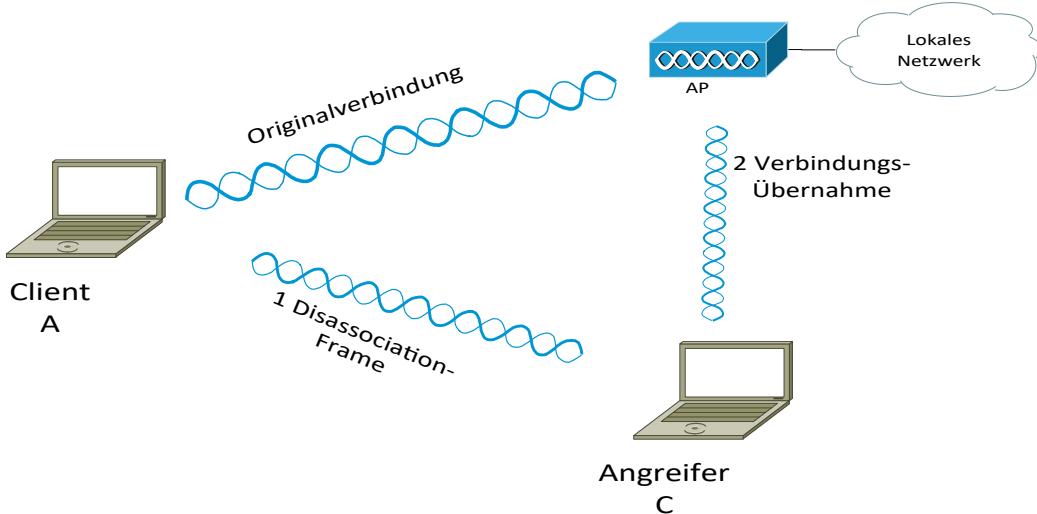


Abbildung 203: WLAN Session Hijacking

Der Angreifer C wartet hier, bis A eine Verbindung mit dem AP aufgebaut hat. Dadurch braucht er sich um das Anmelde-Prozedere nicht zu kümmern.

Zuerst sendet der Angreifer eine Disassociation-Nachricht an den Client. Der Client verliert dadurch seine Verbindung zum AP.

Der AP hingegen kennt den Client immer noch als eine Station, die mit ihm verbunden ist. Der Angreifer kann unter Verwendung der MAC-Adresse des Clients A weiter in Verbindung mit dem lokalen Netzwerk bleiben. Dies beinhaltet auch alle Rechte, die der Client A hatte!

Glücklicherweise ist dieses Szenario nicht mit Standardmitteln zu bewerkstelligen und daher eher theoretischer Natur.

7.9.11 - Deauthentication

Mit einem Deauthentication oder Disassociation Managementframe kann ein Angreifer einen Client beim AP abmelden. Jeder AP wird einen solchen Frame nur mit einem ACK-Frame beantworten und dann die Verbindung bei sich löschen. Dies stellt einen typischen Denial-of-Service dar.

8 - Planungsgrundlagen

8.1 - Einleitung

Das Ziel ist hier, einen Raum mit überlappenden Funkzellen so auszustatten, dass ein in diesem Raum sich bewegender Client immer den Kontakt zu seinen Kommunikationspartnern halten kann.

Da für alle Clients nur ein „Shared Media“ zur Verfügung steht, ist bei einer großen Anzahl von Clients dafür zu sorgen, dass immer noch ausreichend Bandbreite für einen Client bereit gestellt wird.

Dies hat Auswirkungen bei der Funkzellen-Planung. Hierbei spielt die Auswahl der Antennen, der Sendeleistung sowie der Kanäle eine zentrale Rolle.

Damit sind folgende Festlegungen relevant:

- Festlegung der Anschlussmöglichkeiten von Antennen an APs
- Auswahl der Antennen nach Charakteristik und Antennengewinn
- Festlegung der Antennen-Positionen
- Festlegung der AP-Sendeleistung
- Festlegung der Zellgröße und Zellüberlappung
- Zuordnung der Funkkanäle zu APs
- Festlegung der Basic Rates (Übertragungsgeschwindigkeiten) an allen Stationen
- Festlegung von SSIDs

Da hierbei bereits bei einigen Herstellern Grenzen erreicht werden, kann die Produktauswahl sehr eingeschränkt sein.

8.2 - Konfigurationsbeispiele

8.2.1 - Erweiterung des vorhandenen LANS um ein WLAN

Im Normalfall wird man ein bestehendes LAN um ein WLAN erweitern, wenn neue Geräte schwierig zu verkabeln wären. Dies kann aus den unterschiedlichsten Gründen der Fall sein.

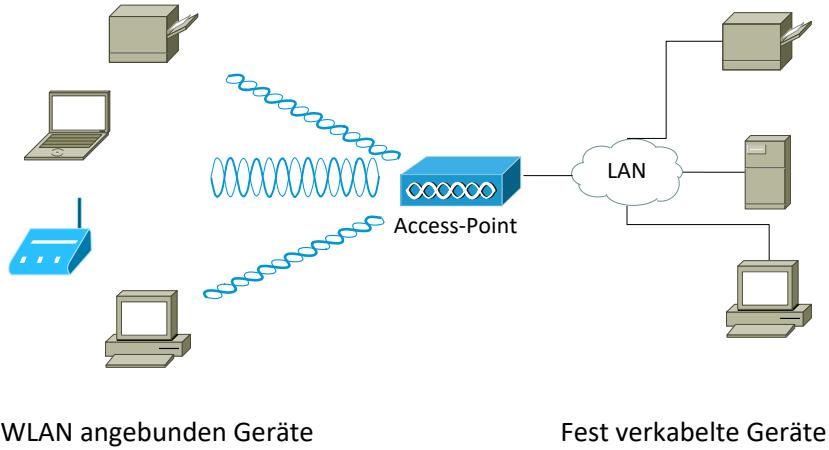


Abbildung 204: LAN um WLAN erweitert

8.2.2 - Überdeckung einer großen Fläche mit einem WLAN

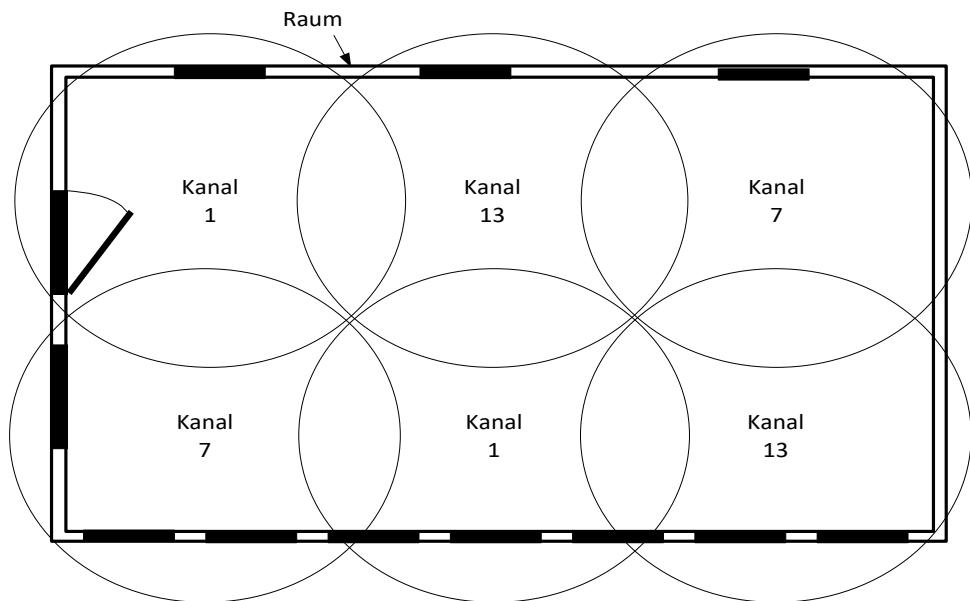


Abbildung 205: Überdeckung einer großen Fläche

Da durch die Interferenzen nicht immer der gleiche Kanal ausgewählt werden kann, muss auf die im Frequenzband zur Verfügung stehenden Frequenzen zurückgegriffen werden.

Die Kanäle 1, 7 und 13 werden hierzu standardmäßig bei IEEE-802.11b/g verwendet. Mit der Verwendung von IEEE-802.11a/h und Folgende kann hier Abhilfe geschaffen werden. In diesen Standards sind weitere Kanäle möglich.

8.2.3 - Viele Clients im selben WLAN

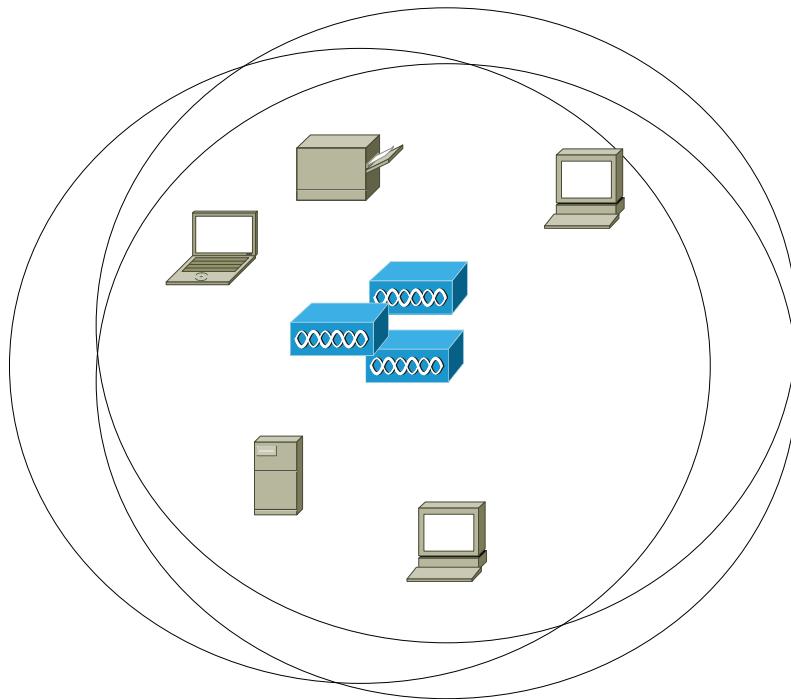


Abbildung 206: WLAN mit vielen Clients

Es kann vorkommen, dass die zur Verfügung stehende Bandbreite nicht ausreicht. Hier kann durch eine Überlagerung von bis zu 3 WLANs Abhilfe geschaffen werden. Natürlich ist auf überschneidungsfreie Kanäle zu achten.

Dadurch werden die Clients auf verschiedene WLANs verteilt und somit kann die 3fache Bandbreite erreicht werden.

8.2.4 - Ausfallsicherheit und Redundanz

Wie oben bei der Erhöhung der Bandbreite kann auch die Ausfallsicherheit und somit die Verfügbarkeit dadurch erhöht werden, dass man mehrere WLANs übereinander legt.

8.2.5 - Funkverbindung zwischen zwei LANs

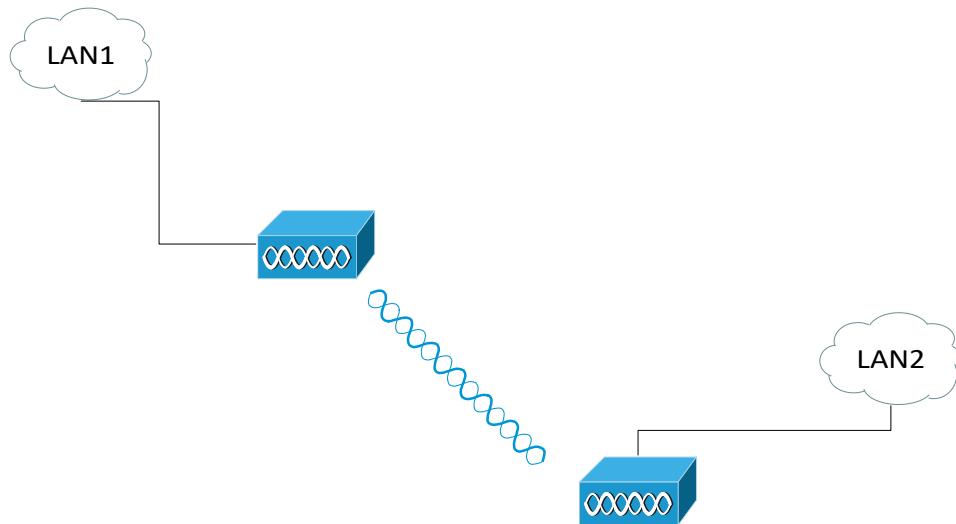


Abbildung 207: WLAN verbindet LANs

Dazu müssen die APs im Bridge-Modus betrieben werden.

Beide APs arbeiten im selben WLAN auf dem selben Funkkanal. Zusätzliche Clients können hier die verfügbare Bandbreite reduzieren.

Sollen die LANs in unterschiedlichen Gebäuden verbunden werden, kommen Richtantennen zum Einsatz.

8.3 - Antennenbeispiele

8.3.1 - Flächenabdeckung mit omnidirektionalen Antennen

Abbildung 205 zeigt wie mit rundum abstrahlenden Antennen eine flächendeckende WLAN Abdeckung erreicht werden kann.

8.3.2 - Flächenabdeckung mit Dipol-Antennen

Durch Verwendung von Patch- oder Yagi-Antennen kann durch gerichtete Antennen eine Abdeckung des WLANs erreicht werden.

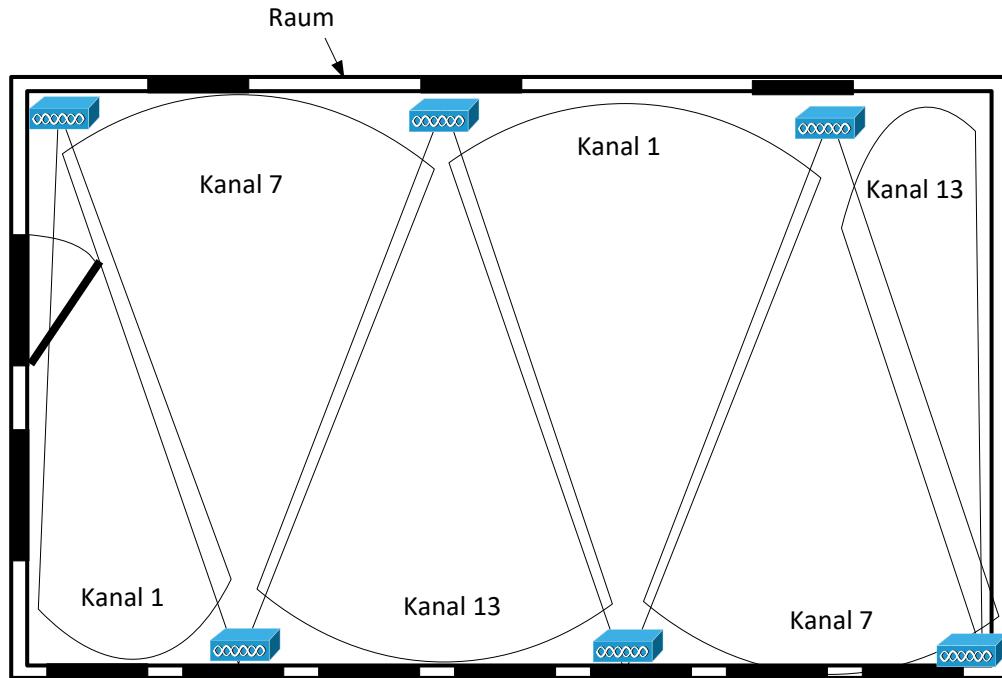


Abbildung 208: WLANs Flächenabdeckung mit gerichteten Antennen

Es kann vorkommen, dass zum Beispiel eine LAN-Verkabelung nur an den Wandseiten eines Gebäudes möglich ist. In einem solchen Fall kann man mit gerichteten Antennen arbeiten.

9 - WLAN-Geräte

9.1 - Clients

WLAN ist heutzutage für die meisten Geräte verfügbar. Vor allem mobile Systeme haben meist auch eine WLAN-Schnittstelle. Unterschiede bestehen in den verwendeten Chipsätzen.

Einerseits soll eine möglichst einfache Handhabung der Geräte durch Plug-and-play bei den meisten Benutzer zu großer Akzeptanz führen. Andererseits sind z. B. in industriellen Umgebungen detaillierte Anpassungen an die Umgebung erforderlich. Hier kommt es auf die Treiber an, welche eine mehr oder weniger detaillierte Anpassung der Geräte an die Gegebenheiten ermöglichen.

Weitere Unterschiede bestehen in der Verbindung mit der WLAN-Adapter an das System angeschlossen sind. Je nachdem, ob ein WLAN-Adapter fest verbaut ist, als Modul auf das Motherboard gesteckt, oder als USB-Adapter daherkommt ist es möglich, von neuen Standards zu profitieren.

Im allgemeinen reicht es bei einer Station aus den Schlüssel für die gewünschte SSID einzugeben. Damit kann eine Verbindung zu einem AP aufgebaut werden. Soll jedoch nur einen temporären Verbindung zu einer anderen Station aufgebaut werden ist z. B. in den Ad-hoc-Modus umzuschalten. Siehe hierzu auch das Kapitel Fehler: Verweis nicht gefunden.

9.2 - WLAN-Telefon

Ein WLAN-Gerät, mit dem man nur telefonieren kann war eine Zeit lang besonders in Firmen eine gute Alternative zu einer DECT-Telefonanlage da mit Voice over WLAN (VoWLAN) ein bestehender AP mit genutzt werden kann. Die erforderliche Sprachqualität kann über QoS sicher gestellt werden.

9.3 - Access Points (APs)

APs sind aus WLAN-Sicht erst einmal Stationen. Allerdings sind sie mit zusätzlichen Fähigkeiten ausgestattet, welche z. B. eine Koordinierung mehrerer Stationen innerhalb einer Funkzelle durchführt um einen geregelten Betrieb sicher zu stellen. Einige Funktionen sind nur mit APs realisierbar, da sie eine zentrale Verwaltungsinstantz voraussetzen.

Die AP-Funktionen sind bei den entsprechenden Standards beschrieben.

9.4 - WLAN-Controller

Diese Geräte sollen das Management von WLANs zentralisieren und damit vereinfachen. Sie unterscheiden sich vor allem in der Anzahl der verwaltbaren APs und SSIDs. Sinnvoll ist es WLAN-Controller und APs vom selben Hersteller zu beziehen, um den größtmöglichen Funktionsumfang nutzen zu können. So wie bei einer kabelgebundenen Vernetzung ist es auch bei WLANs oft wünschenswert einzelne Benutzergruppen in VLAN's zusammenzufassen. Dazu sollte die Verwaltung mehrerer SSIDs möglich sein. Auf der kabelgebundenen Seite sollte es möglich sein unterschiedliche VLANs anzuschließen. Damit kann die Idee der VLANs in SSIDs abgebildet und weiter geführt werden.

Hier eine Auswahl möglicher Funktionen:

- Zentrales Management der WLAN-Funktionen
- VPN-Gateways
- Firewall
- Wireless Intrusion Detection System (IDS)
- Interface Monitoring
- Trennung/Verwaltung von Benutzergruppen (VLANs durch unterschiedlichen SSIDs)
- Verwaltung von Quality of Service
- Subnetzübergreifende Online-Mobilität über IP-Tunnel

9.5 - WLAN-Switches

Anfänglich sind WLANs oft kleine Funkzellen. Mit der Anforderung nach Anbindungen an andere Netzwerke kommen schnell Switches ins Spiel mit denen APs an die Außenwelt angebunden werden können.

Einige Hersteller hatten dann unter dem Marketing-Begriff WLAN-Switches Geräte auf den Markt gebracht die einige sinnvolle Funktionen möglich machten. Dadurch wurden die APs von zentralen Aufgaben entlastet.

Mittlerweile wurden die WLAN-Switches durch WLAN-Controller abgelöst. Switches spielen jedoch noch eine Rolle bei der Stromversorgung von APs mittels PoE.

10 - Gesundheitliche Aspekte

Gerade im Funkbereich sind die Gegner der Technik zahlreich. Hier herrscht eine große Unsicherheit in Bezug auf die möglichen Schäden. Besonders die Langzeitbelastung und deren Auswirkungen sind nicht ausreichend geklärt.

Alle bisherigen Studien konnten keine abschließende Klarheit schaffen. Das eigentliche Problem ist, dass eine solche Studie einen Negativbeweis erbringen müsste. Dies ist jedoch nicht möglich.

Der Gesetzgeber, insbesondere das Bundesamt für Strahlenschutz, hat bisher keine Ergebnisse geliefert, welche die Schädlichkeit von Mobilfunk untermauern würde. In der Pressemitteilung 18 vom 11.3.2002 wird dies nochmals bekräftigt.

Unstrittig ist jedoch, dass elektromagnetische Strahlung mit hoher Leistung immer gefährlich ist. Dies ist im Zusammenhang mit den Radar-“Unfällen” kürzlich wieder bestätigt worden.

Vermutete Schäden sind:

- Chromosomen-Schäden
- Genmutation
- DNA-Schäden

Im Vergleich zu bestehenden Funknetzen wie z. B. das D-Netz liegt die Leistung von WLANs um den Faktor 10 darunter.

Wie kann jedoch mit diesem Thema umgegangen werden?

Ein vorsichtiger Umgang mit dem Thema ist grundsätzlich angebracht. Es sollte bewusst und vorsichtig mit den Ängsten und Bedenken von Mitarbeitern umgegangen werden. Bereits bei der Planung sollten alle möglichen Beteiligten mit einbezogen werden. Hierbei sind Betriebsrat, Werksarzt, Management sowie Sicherheitsbeauftragte usw. von Bedeutung.

11 - Abkürzungsverzeichnis

Abkürzung	Ausgeschriebene Form	Bedeutung
5G	5. Generation	Mobilfunkstandard der 5. Generation
AA	Authenticator Address	
AAA	Authentication, Authorization and Accounting	
AC	Access Category	Überträgt Queues für Geräte die 802.11e (QoS) unterstützen
ACI	Access Category Index	
ACK	Acknowledge	Quittung / Bestätigung
AES	Advanced Encryption Standard	Verschlüsselungsstandard, der auf dem Rijndael-Algorithmus basiert
AES-CCM	Advanced Encryption Standard CTR/CBC MAC	von 802.11i unterstützter Verschlüsselungsstandard
AGC	Automatic Gain Control	Automatische Verstärkungssteuerung
AID	Accociation Identifier	Identifier für die Verwaltung einer Station auf einem AP
AIFS	Arbitration Inter Frame Space	
AP	Access Point	Zentraler WLAN-Kommunikationspartner.
ATIM	Ad-hoc Traffic Indication Map	Leistungsaufnahme-Sparfunktion in Ad-hoc-Umgebung
ATM	Asynchronous Transfer Mode	Datenübertragungs-Standard
BA	Block Acknowledge	
BAN	Body Area Network	Netzwerk mit einer Ausdehnung bis zu einem Meter
BAPT	Bundesamt für Post und Telekommunikation	
BAR	Block Achnowledge Request	
BC	Broadcast	Ein Frame wird an alle Geräte in einem BSS gesendet
BEC	Backward Error Correction	Fehlerbehandlungsverfahren mit Quittungen
BF	Beamforming	
BFWA	Broadband Fixed Wireless Access	
Bluetooth SIG	Bluetooth Special Interest Group	Bluetooth Normierungsgremium

Abkürzungsverzeichnis

BO	Back Off Time	Wartezeit beim Medienzugriff
BPSK	Binary Phase Shift Keying	Modulationsverfahren
BSS	Basic Service Set	Basis-Sendeeinheit
BSR	Buffer Status Report	Buffer-Status-Report für MU-Uplink
BSRP	Buffer Status Report Poll	Aufforderung einen Buffer-Status-Report zu senden
CA	Collision Avoidance	Kollisionsvermeidung beim Medium-Zugriff
CBC	Cipher Block Chaining	Verschlüsselungsverfahren
CCK	Complementary Code Keying	Signal-Spreizverfahren
CCM	CTR / CBC-MAC	Verschlüsselungsverfahren für WPA2
CCMP	CCM Protocol	Verschlüsselungsprotokoll für WPA2
CDMA	Code Division Multiplexing Access	Multiplexverfahren das auf Codierung basiert
CEPT	Conference Européenne des Administration des Postes et des Télécommunications	Europäisches Normierungsgremium
CFP	Contention Free Period	Zeitfenster ohne Wettbewerbssituation beim Medien-Zugriff
CRC	Cyclic Redundancy Check	Prüfsummenverfahren
CTR	Counter	
CTS	Clear To Send	Sende-Genehmigung
CP	Contention Period	Wettbewerbssituation beim Medienzugriff
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance	Medienzugriffsverfahren für WLANs
CW	Contention Window	Zeitfenster mit Wettbewerbssituation beim Medien-Zugriff
DA	Destination Address	(in Form der Destination-MAC-Adresse)
dB	Dezibel	
dBm	Dezibel bezogen auf 1mWatt	
dBi	Dezibel bezogen auf isotopen Strahler	
dBr	Dezibel (relativ) bezogen auf Grundlinie	
DCF	Distributed Coordination Function	Verteiltes Medien-Tugriffsverfahren
DECT	Digital Enhanced Cordless Telephone	Standard für schnurlose Telefone
DFS	Dynamic Frequency Selection	Dynamische Frequenzauswahl
DHCP	Dynamic Host Configuration Protocol	Protokoll zu Vergabe von Parametern wie IP-Adressen
DIFS	DCF Inter Frame Spacing	Wartezeit beim Medienzugriff

Abkürzungsverzeichnis

DL	Downlink	Daten-Senderichtung AP → Station
DMG	Directional Multi-Gigabit	
DNS	Domain Name Service	
DS	Distribution System	Verteilungs-System. Zur Erstellung von ESSen
DSSS	Direct Sequence Spread Spectrum	Datenübertragungsverfahren.
DTIM	Delivery Traffic Indication Map	Leistungsaufnahme-Sparfunktion
EAP	Extensible Authentication Protocol	
EAPoL	EAP over LAN	
ECC	Electronic Communication Commision	Regulierungs- / Normungsbehörde
EDCA	Enhanced Distributed Channel Access	Definition von Kanälen für unterschiedliche QoS-Prioritäten
EDCAF	Enhanced Distributed Channel Access Function	
EIFS	Extended Inter Frame Spacing	Wartezeit beim Medienzugriff
EIRP	Equivalent Isotropically Radiated Power	Sendeleitung eines fiktiven Kugelstrahlers
EIV	Extended IV	Erweiterung des Initialisierungsvektors
EIVID	EIV Identiy	Kennung für die Verwendung des EIV
ETSI	European Telecommunications Standard Institute	Europäische Telekommunikations-Normungsinstitut
ESS	Extended Service Set	Erweiterte Sendeinheit (Zusammenschluss mehrerer BSS)
FCS	Frame Check Sequence	Prüfsumme
FDD	Frequency Division Duplex	Multiplexverfahren, das auf unterschiedlichen Frequenzen basiert
FDMA	Frequency Division Multiple Access	Multiplexverfahren, das auf unterschiedlichen Frequenzen basiert
FEC	Foreward Error Correction	Vorwärts Fehlerbehandlungsverfahren
FFT	Fast Fourier Transformation	Mathematisches Verfahren
FHSS	Frequency Hopping Spread Spectrum	Datenübertragungsverfahren. Wird bei Bluetooth angewendet.
FPK	Fast Packet Keying	Erzeugung von dynamischen WEP-Schlüsseln durch von der Firma RSA
FSPL	Free Space Path Loss	Freiraumdämpfung

Abkürzungsverzeichnis

FT	Fourier Transformation	Mathematisches Verfahren
	Fast-BSS-Transition	
GCR	Groupcast Retries	
GI	Guard Intervall	Schutzintervall bei OFDM
GPRS	General Packet Radio Service	Mobilfunkstandard
GSM	Global System for Mobile Communications	Mobilfunkstandard
GTKSA	Group Temporal Key Security Association	
HEC	Header Error Control	Prüfsumme für Header
HSPA	Hight Speed Packes Access	UMTS Beschleunigung
HT	High Throughput	
HT-LTF	High Throughput Long Training Field	
HT-SIG	High Throughput SIGNAL Field	
HT-STF	High Throughput Short Training Field	
IAPP	Inter Access Point Protocol	Protokoll für ein schnelles Handover
IBSS	Independent Basic Service Set	Unabhängige Basis-Sendeeinheit
ICI	Interface Control Information	
ICV	Integrity Check Value	Integritäts-Prüfsummer für WEP
IDS	Intrusion Detection System	Erkennung von Angreifern in einem WLAN
IE	Information Element	
IFS	Inter Frame Spacing	Wartezeit beim Medienzugriff
IFT	Inverse Fourier Transformation	Mathematisches Verfahren
IFFT	Inverse Fast Fourier Transformation	Mathematisches Verfahren
IGTKSA	Integrity Group Temporal Key Security Association	Verwaltung der Verschlüsselung von Broadcasts und Multicasts
ISI	Inter Symbol Interferenz	Gegenseitige Beeinflussung von benachbarten Symbolen.
ISM	Industrial Scientific Medical	Frequenzband für industrielle wissenschaftliche und medizinische Nutzung
IoT	Internet of Things	
IV	Initialisierungs Vector	
KID	Key Identity	Schlüssel-ID beim WEP-Verfahren
LAN	Local Area Network	Netzwerk mit Verkabelung

Abkürzungsverzeichnis

LLC	Logical Link Control	Datensicherungsschicht (Ebene 2b)
LoS	Line of Sight	Verbindungsleitung mit Sichtkontakt
LTE	Long Term Evolution	Mobilfunkstandard der 4. Generation
L-LTF	NonHT Long Trainings Field	
L-SFT	NonHT Short Trainings Field	
L-SIG	NonHT SIGNAL Field	
MAC	Media Access Control	Medien-Zugriffs-Steuerung. Wird mit MAC-Adresse adressiert. MAC-Ebene = Ebene 2a
MAP	Mesh Access Point	AP zum Zugriff von Clients auf ein Mesh
MBSS	Mesh Basic Service Set	Zu einem Mesh zusammengeschlossene Einheit von APs
MC	Multicast	Ein Frame wird an eine Gruppe von Empfängern gesendet
MCF	Mesh Coordination Function	
MCS	Modulation and Coding Scheme	
MIC	Message Integrity Code	
MIMO	Multiple In Multiple Out	
MISO	Multiple In Single Out	
MP	Mesh Point	AP für den Weitertransport von MSDUs innerhalb eines Mesh
MPDU	MAC Protocol Data Unit	Daten der MAC-Layer an die unterlagerte Schicht.
MPP	Mesh Portal (.)	AP innerhalb eines Mesh der die Verbindung zu einem anderen Netzwerk erbringt
MSDU	MAC Service Data Unit	Über SAP an MAC-Ebene übergebene Daten
MU	Multi User	Gleichzeitige Bearbeitung mehrerer Stationen
MU-DL	Multi User Downlink	Gleichzeitiges Senden von Daten vom AP → Stationen
MU-MIMO	Multi User MIMO	
MU-UL	Multi User Uplink	Gleichzeitige Senden mehrerer Stationen zum AP
NAV	Net Allocation Vector	Belegungsdauer des Sendekanals
N _{BPSC}	Number of Bits per Sub-Carrier	Bits die pro Unterträger aufmoduliert werden.
N _{CBPS}	Number of Coded Bits per Symbol	Anzahl der Bits die je Symbol codiert werden.
N _{DBPS}	Number of Data Bits per Symbol	Anzahl der Bits die pro Abtastung erzeugt wurde.
		Dies sind die letztendlich zu transportierenden Daten.
NDP	Null Data Packet	(Test)-Paket ohne Daten

Abkürzungsverzeichnis

NIST	National Institute of Standards and Technology	Standardisierungsgremium für Sicherheitsthemen
OBSS	Overlapping Basic Service Set	Management von APs mit überlappenden BSS auf dem selben Kanal
OFDM	Orthogonal Frequency Division Multiplexing	Datenübertragungsverfahren.
OFDMA	Orthogonal Frequency Division Multiple Access	Datenübertragungsverfahren.
PBCC	Packet Binary Convolutional Code	
PBSS	Personal BSS	
PCF	Point Coordination Function	Medien-Zugriffsverfahren mit einem AP als Koordinator
PCF IFS	Entspricht PIFS	
PCI	Protocol Control Information	
PDU	Protocol Data Unit	Zwischen Schichten gleicher Ebene ausgetauschte Daten
PER	Packet Error Rate	Paket-Fehler-Rate
PHY	Physical Layer	Physikalische Schicht (Ebene 1)
PIFS	PCF Inter Frame Spacing	Wartezeit beim Medienzugriff
PLCP	Physical Layer Convergence Protocol	Anpassung der MAC-Layer an die PMD.
PLW	PSDU Length Word	Länge der PSDU
PMF	Protected Management Frames	Sicherheit beim Anmeldevorgang bei WPA3
PMD	Physical Media Dependent	Von der Physik abhängige Übertragungsebene. Im allgemeinen werden hier die Daten in Form von Einsen und Nullen auf einem Medium übertragen.
PMK	Pairwise Master Key	
PPK	Per Packet Key	
PoE	Power over Ethernet	Stromversorgung von APs über die Ethernetanbindung
PRF	Pseudo Random Function	
PRNG	Pseudo Random Number Generator	
PSDU	PLCP Service Data Unit	Daten die über SAP an PLCP übergeben werden
PSF	PLCP Signaling Field	
PTK	Pairwise Temporal Key	
PTKSA	Pairwise Transient Key Security Association	

Abkürzungsverzeichnis

QAM	Quadrature Amplitude Modulation	Modulationsverfahren
QAP	QoS AP	AP mit QoS Funktionalität
QBSS	QoS BSS	
QoS	Quality of Service	
QPSK	Quadrature Phase Shift Keying	Modulationsverfahren
QSTA	QoS STA	Station mit QoS Funktionalität
RADIUS	Remote Authentication Dial In User Service	Authorisierungsverfahren
RBUFCAP	Receive Buffer Capability	Empfangspufferkapazität für MPDUs
RC4	Rivet Cipher 4	Verschlüsselungsverfahren von Ronald Linn Rivest
RegTP	Regulierungsbehörde für Telekommunikation und Post	
RSSI	Received Signal Strength Indication	
RTR	Rundfunk und Telekom Regulierungs-GmbH	Österreichische Behörde zur Vergabe von Frequenzbändern
RTS	Request To Send	Sende-Anforderung
SA	Source Address	(in Form der Source-MAC-Adresse)
SAE	Simultaneous Authentication of Equals	Verschlüsselungsmethode bei WPA3
SAP	Service Access Point	Zugriffspunkt für die Dienste-Primitive, um die Datenübertragung und Steuerung der unterlagerten Schichten abzuhandeln.
SDMA	Space Division Multiple Access	Multiplexverfahren, das auf räumlicher Trennung basiert
SDU	Service Data Unit	Zwischen Protokollschichten über den SAP ausgetauschte Daten
SFD	Start Frame Delimiter	
SIFS	Short Inter Frame Spacing	Wartezeit beim Medienzugriff
SISO	Single In Single Out	Datenübertragung mittels einer Sendeantenne und einer Empfangsantenne
SNR	Signal to Noise Ratio	Nutzsignalstärke im Vergleich zum Störsignal
SOHO	Small Office Home Office	Kleine und Heimbüros. Darin kommen Geräte aus der Konsumer-Line zum Einsatz
SRD	Short Range Device	
SS	Single Stream	Datenübertragung auf nur einem Kanal
STA	Station	Station / Gerät / Kommunikationspartner

Abkürzungsverzeichnis

STBC	Space Time Block Coding	
STK	STSL transient Key	
STKSA	STSL transient Key Security Association	
STSL	Station To Station Link	Verbindung zwischen zwei Stationen
SU	Single User	
SU-SISO	Single User – SISO	SISO–Datenübertragung mit einzelner Station
SU-MIMO	Single User – MIMO	MIMO-Datenübertragung mit einzelner Station
TC	Traffic Categoriy	
TTAK	TKIP-mixed transmit address and key	Zwischenschlüssel bei der TKIP-Verschlüsselung
TBTT	Target Beacon Transmission Time	Startzeitpunkt des Beacon-Intervalls
TDD	Time Division Duplex	Multiplexverfahren, das auf Zeit-Rahmen und -Schlitzen basiert
TDM	Time Division Multiplexing	
TDMA	Time Division Multiple Access	Multiplexverfahren, das auf Zeit-Rahmen und -Schlitzen basiert
TETRA	Trans European Trunked Radio	Bündelfunk für Taxi, Busse, Polizei
TID	Traffic Identifier	
TIM	Traffic Indication Map	Leistungsaufnahme-Sparfunktion
TK	Temporal Key	Temporärer Schlüssel bei CCMP
TKIP	Temporal Key Management Protocol	
TPC	Transmission Power Control	Steuerung der Sendeleistung
TS	Traffic Stream	
TSC	TKIP Sequence Counter	
TSF	Timing Synchronisation Function	
TTAK	TKIP mixed transmit address and key	Zwischenschlüssel beim TKIP-Verschlüsselungs-Verfahren
TU	Time Units	
TXOP	Transmit Opporunity	
TXVECTOR	Transmit Vector	Sende Parameter und Danten
UC	Unicast	Ein Frame wird an eine Station gesendet
UDP	User Datagram Protocol	
UL	Uplink	Daten-Senderichtung Station → AP
UMTS	Universal Mobile Telecommunications System	Mobilfunkstandard

Abkürzungsverzeichnis

VHT	Very High Throughput	Präfix für Parameter bei IEEE802.11ac
VHT-BSS	Very High Throughput Basic Service Set	
VoIP	Voice over IP	
VoWLAN	Voice over WLAN	
WDS	Wireless Distribution System	Verteilnetz auf WLAN-Basis
WECA	Wireless Compatibility Alliance	
WEP	Wireless Equivalent Privacy	Ursprüngliches Verschlüsselungsverfahren für WLANs
WEPplus	Wireless Equivalent Privacy plus	Erweiterung von WEP von HP
WiFi	Wireless Fidelity	
WLAN	Wireless Lokal Area Network	Netzwerk mit einer Ausdehnung bis zu 100 Meter
WMAN	Wireless Metropolitan Area Network	Netzwerk mit einer Ausdehnung bis zu 30km
WPA	Wi-Fi Protected Access	Sicherheitssystem für wireless LANs
WPAN	Wireless Personal Area Network	Netzwerk mit einer Ausdehnung bis zu 10 Meter
WWAN	Wireless Wide Area Network	Netzwerk mit einer Ausdehnung bis zu 50 km

IT-Security

Einleitung

Das Thema IT-Sicherheit ist nicht erst im Zusammenhang mit der Nutzung des Internets wichtig geworden. Seit Informationen in Firmen ein schützenswertes Gut darstellen sind zu deren Schutz besondere Maßnahmen erforderlich. Allerdings hat das Internet, mit all seinen Möglichkeiten, auch viele zusätzliche Probleme, wie Viren und Würmer, mitgebracht.

Bevor auf einzelne Probleme und deren Lösung eingegangen werden kann, sind einige Begriffe zu erklären.

Begriffe und Definitionen

IT-System

Darunter versteht man ein technisches System mit der Fähigkeit zur Speicherung und Verarbeitung von Informationen. Diese Systeme können einen offenen oder geschlossenen Charakter haben.

Bei den geschlossenen Systemen sind meist nur proprietäre homogene Technologien eines Herstellers in Verwendung. Diese Systeme haben meist keine Schnittstellen zu anderen Systemen. Dadurch ist die räumliche Ausdehnung und die Anzahl der Teilnehmer oft beschränkt. Solche Systeme lassen sich einfach zentral verwalten.

Typisch für offene Systeme ist eine dezentrale, also eine verteilte, Verwaltung. Ein gesamtes System kann aus unter lagerten Teilsystemen bestehen die offen für die Kommunikation zu anderen Teilsystemen sind. Es kann ein Informationsaustausch mit anderen Systemen über standardisierte Schnittstellen erfolgen.

Es liegt auf der Hand, dass geschlossenen Systeme einfacher zu verwalten und somit auch zu schützen sind. Offene Systeme sind aufgrund der vielen möglichen Schnittstellen einfacher zu manipulieren und bedürfen somit einem erhöhten Schutz-Aufwand.

Soziotechnisches System

IT-Systeme sind Bestandteile von soziotechnischen Systemen. Dies bedeutet, dass sie in unternehmerischen, gesellschaftlichen und politischen Strukturen eingebettet sind.

Damit ist eine Abhängigkeit, zu den Zwecken zu denen sie genutzt werden, zu berücksichtigen. Weiterhin sind unterschiedlichste Nutzer mit unterschiedlichen technischen Kenntnissen zu betrachten. Je nach Umfeld ist die Akzeptanz sowie die Nutzbarkeit der Systeme unterschiedlich zu bewerten. Eine Sekretärin ist zufrieden wenn eine Firewall nur den E-Mail-Dienst ermöglicht. Damit kann sie mit Outlook ihre E-Mails senden und die Termine des Chefs verwalten. Ein Entwickler wird immer alle technischen Möglichkeiten offen haben wollen und bei jeder Einschränkung eines Dienstes protestieren.

Weiterhin sind unterschiedliche Anforderungen, Vorschriften und organisatorische Regelungen zu beachten.

Objekte

IT-Systemen verarbeiten und speichern Informationen in Form von Daten bzw. Objekten. Es gibt passive Objekte wie Dateien oder Datenbank-Einträge und aktive Objekte wie Prozesse die in der Lage sind die Informationen zu

Abbildungsverzeichnis

bearbeiten und zu speichern. Bei diesen Informationen spricht man von von schützenswerten Gütern (engl. asset)

Informationen

Informationen sind immer zusammen mit einer Interpretationsvorschrift zu sehen. So kann ein Integer-Datenobjekt eine Temperatur, ein Datum oder eine Längenangabe sein.

Weiterhin kann ein und dieselbe Information in unterschiedlichen Datenobjekten untergebracht sein. Ein Passwort kann als Binärzeichenfolge auf der Festplatte in einem IP-Paket oder als Eingabe im Tastatur-Puffer stehen.

Will man eine Information schützen, ist es wichtig zu wissen in welchen Datenobjekten die Information steht. Nur durch eine adäquate Vorgehensweise, kann die Information richtig geschützt werden.

Subjekte

Datenobjekte sind durch Operationen oder Methoden von anderen Objekten eines Systems oder von der Umwelt nutzbar. Zur Umwelt gehören vor allem die Benutzer. Die Benutzer eines Systems sowie alle Objekte, die im Auftrag eines Benutzers aktiv sind (Prozesse, Prozeduren, ..), werden als Subjekte bezeichnet.

Autorisierung

Eine Interaktion zwischen einem Subjekt und einem Objekt, die einen Informationsfluss zur Folge hat, nennt man Zugriff auf die Information. Damit ist ein Zugriff auf ein Datenobjekt auch ein Zugriff auf Information. Deshalb ist für jeden Zugriff auf ein Datenobjekt, bzw. auf die dadurch repräsentierte Information Zugriffsrechte festzulegen.

Hat ein Subjekt die Berechtigung auf ein Datenobjekt zuzugreifen spricht man davon, dass das Subjekt für den Zugriff autorisiert ist.

Verlässlichkeit

Unter Verlässlichkeit (engl. dependability) eines Systems versteht man die Eigenschaft keine unzulässigen Zustände anzunehmen (siehe Funktionssicherheit) und zu gewährleisten, dass die spezifizierten Funktionen zuverlässig (engl. reliability) erbracht werden.

Informationskanäle

Informationen werden in einem System über Speicherkanäle (legitime und verdeckte Kanäle) transportiert.

Speicherkanäle

Speicherkanäle sind zum Beispiel Dateien in denen Informationen zwischengespeichert werden können.

Legitime Informationskanäle

Über legitime Kanäle tauschen Subjekte normalerweise Informationen aus. Hierzu zählen Parameter bei Operationsaufrufen oder Nachrichten.

Verdeckte Informationskanäle

Verdeckte Kanäle (engl. covert channel) sind solche Kanäle die nicht für den Informationsaustausch vorgesehen sind. Die Veränderung einer Programm-Ausführungszeit kann eine Information an jemand übermitteln, der sich um Programm-Ausführungszeiten kümmert. Solche Kanäle sind in den heutigen Systemen vielfach vorhanden und sie lassen sich leider auch nur schwer überwachen. Es kann nur dafür gesorgt werden, dass die Bandbreite eines solchen verdeckten Kanals möglichst klein ist.

Sicherheit

Allgemeines

Vor der Betrachtung der unterschiedlichen Ausprägungen zum Thema Sicherheit sollen hier noch ein paar allgemeine Aussagen zur Sicherheit erläutert werden.

Sicherheit nimmt mit der Zeit tendenziell ab.

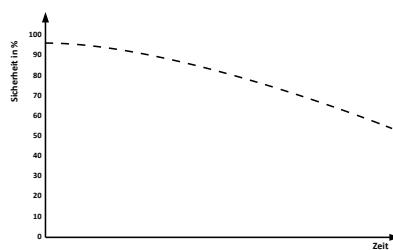


Abbildung 209 : Sicherheit über der Zeit

Ein einmal erreichtes Sicherheitsniveau bleibt nicht konstant. Es nimmt durch neue Angriffsarten und Bedrohungen wieder ab. Um ein erreichtes Niveau zu halten ist es somit erforderlich kontinuierlich Aufwand in die Erhaltung der Sicherheit zu investieren.

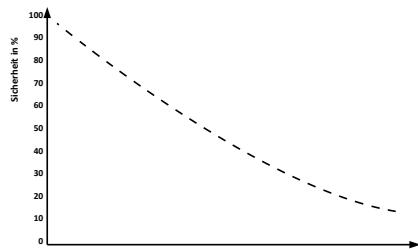


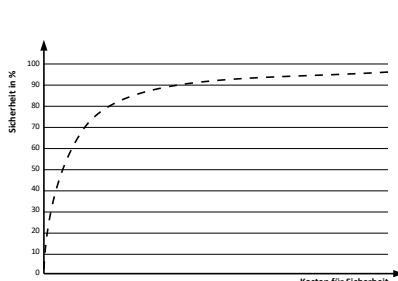
Abbildung 210 : Sicherheit in Abhängigkeit von der Umgebung

Sicherheit ist von der Umgebung abhängig.

Ein in Benutzung befindliches System wird durch ständige Änderungen immer wieder beeinflusst.

Diese Änderungen können sich auf Benutzer-Anzahl, Protokolle, Services usw. beziehen.

Z. B. bei der Einführung eines neuen Users kann durch eine fehlerhafte Rechte-Vergabe ein großes Sicherheitsrisiko entstehen.



Sicherheit kostet Geld.

Bereits mit einem kleinen finanziellen Aufwand kann ein großes Maß an Sicherheit geschaffen werden.

Wer jedoch möglichst nahe an die maximal erreichbare Sicherheit kommen will, muss mit einem großen finanziellen Aufwand rechnen.

Eine 100 percentige Sicherheit kann nicht erreicht werden.

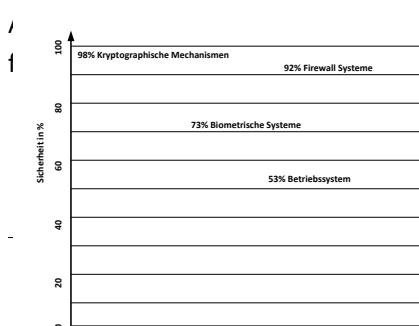


Abbildung 212 : Sicherheit in Abhängigkeit von Mechanismen

Unterschiedliche Sicherheitsmechanismen bieten einen unterschiedlichen Sicherheitsgrad.

Hierbei sind natürlich, je nach Hersteller, wiederum Unterschiede möglich.

Funktionssicherheit

Unter Funktionssicherheit (engl. safety) eines Systems versteht man, dass die ursprünglich spezifizierte SOLL-Funktionalität mit der IST-Funktionalität übereinstimmt. Ein funktionssicheres System nimmt keine unzulässigen Zustände ein. Ein funktionssicheres System funktioniert unter (normalen) Betriebsbedingungen.

Informationssicherheit

Die Informationssicherheit (engl. security) ist die Eigenschaft eines funktionssicheren Systems nur solche Systemzustände anzunehmen, die zu keiner unautorisierten Informationsveränderung oder -Gewinnung führen.

Datensicherheit

Die Datensicherheit ist die Eigenschaft eines funktionssicheren Systems nur solche Zustände anzunehmen, die zu keinem unautorisiertem Zugriff auf System-Ressourcen und Daten führen. Hier ist auch das Thema Datensicherung (engl. backup) anzusiedeln.

Datenschutz

Der Begriff Datenschutz (engl. privacy) beschreibt die Fähigkeit eines Systems einer natürlichen Person die Weitergabe von persönlichen Informationen zu kontrollieren. Hier hat der deutsche Gesetzgeber das informationelle Selbstbestimmungsrecht gesetzt.

Schutzziele

Authentizität

Damit ist die Echtheit bzw. die Glaubwürdigkeit eines Subjekts oder eines Objekts zu verstehen. Geprüft wird dies anhand einer eindeutigen Identität und charakteristischen Eigenschaften.

Authentifikation

Die Authentizität eines Subjekts oder Objekts wird durch Maßnahmen der Authentifikation (engl. authentication) überprüft. Dabei wird die vorgegebene Identität mit den charakteristischen Eigenschaften des Subjekts oder Objekts verglichen. Z. B. ein Passwort oder ein Fingerabdruck.

Subjekt-Authentifikation

Normalerweise handelt es sich hierbei um die Authentifikation von Benutzern. Dazu ist für jeden Benutzer eine eindeutige Identifikation zu vergeben. Dies geschieht durch die Vergabe einer Benutzer-Kennung (engl. account). Für die charakteristischen Eigenschaften wird normalerweise ein Passwort verwendet, dessen Kenntnis der Benutzer beim Systemzugang nachweisen muss. Anstelle des Passworts können auch biometrische Merkmale wie Fingerabdruck, Stimme oder Augen-Netzhaut verwendet werden. Damit sind jedoch wiederum neue Themen relevant. So ist bei einem Fingerabdruck wichtig zu wissen ob der Finger an einem lebenden Körper ist oder nicht.

Objekt-Authentifikation

Durch offene Systeme ist es erforderlich, die Authentizität von Objekten (WEB-Server, Access-Points) nachzuweisen. Dabei wird im allgemeinen auf kryptographische Verfahren zurückgegriffen um die Echtheit zu

überprüfen. Ein Ursprungs- oder Urhebernachweis reicht derzeit noch aus. Eine Aussage über die Funktionalität ist derzeit noch nicht im Einsatz. Die Mobilität von Daten wird in Zukunft hier noch zu entsprechenden Verfahren führen. Bedenkt man, dass Java-Applets in wichtigen Systemen eingesetzt werden sollen, ist eine Objekt-Authentifikation unumgänglich.

Datenintegrität

Datenintegrität ist gewährleistet, wenn Subjekte nur autorisiert auf zu schützende Daten zugreifen kann. Eine unbemerkt unautorisierte Zugriff auf Daten ist von sicheren Systemen zu unterbinden. Erreicht wird dies durch die Vergabe von Zugriffsrechten auf die Objekte. Z. B. Schreib- oder Leserechte auf Dateien.

Vertraulichkeit

Wird keine unautorisierte Informationsgewinnung ermöglicht, spricht man von einem System das Vertraulichkeit (engl. confidentiality) gewährleistet. Durch die Vergabe und Überwachung von Berechtigungen für die Informationsflüsse zwischen den Subjekten soll ein System gewährleisten dass keine Informationen zu unautorisierten Subjekten durchsickert. Dieses Problem wird Confinement-Problem genannt.

Verfügbarkeit

Ein System gewährleistet die Verfügbarkeit (engl. availability), wenn autorisierte Benutzer nicht durch unautorisierte Benutzer beeinträchtigt werden. Dies ist vor dem Hintergrund von Time-Sharing Betriebssystemen, an denen mehrere Benutzer gleichzeitig Ressourcen wie CPU, Speicher oder Festplattenplatz nutzen, wichtig.

Verbindlichkeit

Die Verbindlichkeit bzw. Zuordenbarkeit (engl. non repudiation) einer Aktion eines Subjekts darf im Nachhinein nicht bestreitbar. Diese Eigenschaft ist vor allem im Zusammenhang mit elektronischen Handel (engl. Electronic Business) wichtig. Erreicht werden diese Anforderung durch elektronische Signaturen.

Abrechenbarkeit

Erst durch die Verbindlichkeit ist die Abrechenbarkeit (engl. accountability) möglich geworden. Durch eine entsprechende Überwachung (engl. audit) und eine Protokollierung (engl. logging) kann die Abrechnung (engl. billing) erfolgen.

Anonymität

Durch die Vernetzung ist die Forderung nach Sicherheit durch Unkenntlichkeit, also Anonymität, gewachsen. Dabei werden personenbezogene Daten so verändert, dass sie nicht mehr oder nur mit großem Aufwand, auf eine bestimmbarer natürliche Person zurückzuführen sind. Ziel ist dabei Aufenthaltsorte und Kommunikationsbeziehungen so zu verschleiern, dass keine Bewegungs-, Kommunikations- oder Zugriffsprofile durch Dritte erstellt werden können. Damit soll die Privatsphäre (engl. privacy) des geschützt werden.

Pseudomisierung

Eine abgeschwächte Form der Anonymisierung ist die Pseudomisierung. Dabei werden die personenbezogenen Daten nach einer Zuordnungsvorschrift verändert. Damit ist die Identität eines Subjekts zwar einem vertrauenswürdigem Kommunikationspartner bekannt, jedoch nicht allen anderen.

Informationelle Selbstbestimmung

Beim Versenden einer E-Mail ist es zwar wünschenswert, dass der Empfänger die Sender-E-Mail-Adresse zu sehen bekommt, jedoch nicht die zuletzt vom Sender besuchte Homepage. Es ist das Recht einer jeden Person auf informationelle Selbstbestimmung Informationen von sich an Dritte weiterzugeben. 1983 wurde dies im Rahmen der Volkszählung vom Bundesverfassungsgericht festgelegt.

Schwachstelle

Eine Schwachstelle (engl. weakness) ist eine Stelle im System an dem es verwundbar werden kann.

Verwundbarkeit

Eine Verwundbarkeit ist eine Schwachstelle über welche die Sicherheitsdienste des Systems umgangen, getäuscht oder unautorisiert modifiziert werden können.

Bedrohungen

Eine Bedrohung (engl. threat) zielt darauf ab, eine oder mehrere Schwachstellen oder Verwundbarkeiten auszunutzen um einen Verlust der Datenintegrität, der Informationsvertraulichkeit oder der Verfügbarkeit zu erreichen.

Risiko

Unter dem Risiko (engl. risk) versteht man die Wahrscheinlichkeit oder relative Häufigkeit des Eintritts eines Schadensereignisses sowie die Höhe des potentiellen Schadens.

Gewichtung

Innerhalb einer Bedrohungs- oder Risiko-Analyse werden folgende Schritte durchgeführt. Je nach Umgebung ist eine Bedrohung unterschiedlich zu bewerten. Zur Bestimmung der tatsächlichen Gefährdung ist zunächst das Risiko zu bewerten. Dabei werden die zu schützenden Güter (engl. assets) bewertet. Daran anschließend kann das potentielle Schadenspotential ermittelt werden. Nach einer Berücksichtigung der Eintrittswahrscheinlichkeit eines Schadensereignisses .

Angriff

Mit einem Angriff (engl. attack) ist ein unautorisierte Zugriff oder auch nur der Versuch eines Zugriffs auf ein System gemeint. Es gibt passive und aktive Angriffe. Bei den passiven Angriffen steht die unautorisierte Informationsgewinnung im Vordergrund. Bei den aktiven Angriffen wird auf eine Veränderung von Informationen sowie einen Verlust der Verfügbarkeit abgezielt.

Passiver Angriff

Hauptsächlich ist hierbei das Abhören (engl. eavesdropping) von Datenleitungen in vernetzten Systemen gemeint. In kupferverkabelten Systemen ist dazu ein Zugriff auf eine Anschlussdose oder eine Datenleitung notwendig. Dies kann mit einem Netzwerk-Management sowie z. B. VLANs relativ einfach eingeschränkt werden. Bei drahtlosen Kommunikationssystemen ist diese Einschränkung nicht so einfach durchführbar. Hier kann das Abhören so gut wie nicht unterbunden werden. Deshalb sind hier zusätzlich Verschlüsselungstechniken einzusetzen.

Sniffer

Der Sniffer (deutsch: Schnüffler) ist ein häufig eingesetztes Hilfsmittel. Es handelt sich hierbei um Software die einen Rechner in die Lage versetzt, die auf der Netzwerkschnittstelle anstehenden Daten mitzulesen und zu decodieren. Eine Entschlüsselung ist allerdings nicht möglich. Ursprünglich zur Erkennung und von Fehlern auf fast allen Ebenen des ISO-RM wird mittlerweile die original Sniffer-Software von der Firma NAI weiterentwickelt. Hierbei sind hilfreiche Expertensysteme für den Netzwerk-Administrator entstanden. die Im Internet sind leistungsfähige Open-Source - Sniffer, wie Ethereal oder Packetizer verfügbar.

Aktiver Angriff

Ein Beispiel hierfür ist das Verändern oder Entfernen von Informationen aus einem Datenstrom. Auch das Wiedereinspielen von aufgezeichneten Daten gehört hierzu.

Spoofing

Beim Spoofing wird eine falsche Identität vorgespiegelt. Zum Beispiel ist das Vorgeben einer falschen E-Mail-Absenderadresse ein solcher Vorgang. Damit kann evtl. der Empfänger der E-Mail dazu veranlasst sensible Informationen preis zugeben. Eine weitere Möglichkeit ist der Versuch einen Rechnernamen zu übernehmen (DNS-Name-Spoofing). Dabei wird die eigene IP-Adresse einem vertrauenswürdigen Rechnernamen in einem DNS-Server zugeordnet. Damit kann einem Client eine falsche Information auf seine Anfrage zurückgeliefert werden.

Denial of Service (DoS)

Hierbei wird die Verfügbarkeit eines Dienstes oder einer Systemkomponente reduziert. Dies kann z. B. durch Überfluten eines Rechners mit Anfragen geschehen. Dadurch kann das System legitime Anfragen nicht mehr bearbeiten und beantworten.

Social Engineering

Hierbei geht es um Angriffe nichttechnischer Art. Beim Social Engineering, das auch Social Hacking genannt wird, gibt sich der Angreifer am Telefon z. B. als Administrator aus der gerade mal das Passwort des Opfers für eine wichtige administrative Aufgabe braucht. Da dies unpersönlich geschieht, liegt es am Sicherheitsbewusstsein des Opfers. Ist es gutgläubig teilt das Opfer das Passwort mit. Der Phantasie und der Dreistigkeit der Angreifer sind hier keine Grenzen gesetzt.

Viren

In der Biologie ist ein Virus ein Mikroorganismus der auf eine lebende Wirtszelle angewiesen ist. Er besitzt keinen eigenen Stoffwechsel und ist fähig sich zu reproduzieren.

Ein Computervirus ist kein selbstständig ablaufähiges Programm. Er benötigt ein Wirtsprogramm um ausgeführt zu werden. Computerviren sind zur Reproduktion fähig. Bei der Ausführung wird eine Kopie (Reproduktion) oder modifizierte Version (mutierender Virus) in einen Speicherbereich geschrieben (Infektion), der noch nicht infiziert ist. Weiterhin besitzt ein Computervirus noch einen Schadensteil. Dieser kann bedingt oder unbedingt durch einen Auslöser aktiviert werden. Dies kann durch Social Engineering dadurch geschehen, dass ein E-Mail-Empfänger durch eine Aufforderung dazu gebracht wird einen Anhang zu öffnen und damit das Wirtsprogramm aktiviert.

Viren waren früher nur destruktiv angelegt. Neuerdings werden Viren zum Sammeln von Passworten oder zum Verändern von Systemdateien eingesetzt.

Viren verbreiten sich z. B. in E-Mails als Anhänge.

Als Gegenmaßnahmen kann auf administrativer Seite folgendes gemacht werden:

- ➊ Beschränkung von Schreibrechten
- ➋ Verschlüsselung von Daten
- ➌ Verschlüsselung von Programmcode (ein infiziertes Programm wird vor der Ausführung entschlüsselt. Durch das Entschlüsseln wird der Virus zerstört. Das ausführbare Programm ist durch den Virus zerstört, doch eine weitere Verbreitung des Virus und der Schadensteil funktionieren nicht mehr)
- ➍ Erstellung eines digitalen Fingerabdrucks (engl. digest) eines Programms. Es handelt sich dabei um einen Bitstring fester Länge der durch eine kryptographische Hash-Funktion erzeugt wird. Eine Veränderung des Programmcodes würde zu einem anderen Fingerabdruck führen.

Zusätzlich sollten VirensScanner eingesetzt werden. Diese Scanner untersuchen die ausführbaren Dateien auf bestimmte Virenkennungen oder spezifische Bytemuster. Mutierte Viren können mit heuristischen Verfahren erkannt werden. Dabei werden Codesequenzen gesucht die auf Virenaktivitäten hinweisen wie z. B. das kopieren von Code.

Würmer

Würmer sind, im Gegensatz zu Viren, selbstständig ablauffähig. Sie sind zur Reproduktion fähig. Die Verbreitung findet vorzugsweise über Netzwerke statt. Dabei kopiert sich der Wurm auf einen anderen Rechner im Netzwerk. Dabei nutzt der Wurm bekannte Schwachstellen in Programmen aus die ständig oder zyklisch immer wieder laufen. Durch das Ausnutzen eines Puffer-Überlaufs (engl. Buffer-Overflow) kann sich ein Wurm sich in einem weiteren Rechner einnisten. So nutzte z. B. 2001 der Code-Red Wurm einen Puffer-Überlauf im Microsoft Internet Information Service (IIS) aus um sich zu verbreiten.

Kann ein Puffer-Überlauf in einem System-Prozess erzeugt werden kann ein Angreifer uneingeschränkte Rechte über den gesamten Rechner erlangen.

Durch Würmer wird die Integrität, Vertraulichkeit und die Verfügbarkeit eines Systems bedroht.

Als Reaktion auf den ersten Wurm mit bedrohlicher Funktionalität gründete die U.S. Defense Advanced Research Projects Agency (DARPA) das erste Computer Emergency Response Team (CERT). Es hat die Aufgabe sich mit Sicherheitsfragen rund um das Internet zu beschäftigen. Aktuelle Informationen über Sicherheitslücken und Problembereiche werden von CERT regelmäßig veröffentlicht. Hier werden auch Maßnahmen sowie Patches zur Verfügung gestellt.

Trojaner

Ein Trojanisches Pferd ist ein Programm dessen implementierte Ist-Funktionalität nicht mit der Soll-Funktionalität übereinstimmt. Es erfüllt zwar die Soll-Funktionalität, besitzt darüber hinaus jedoch noch weitere Funktionalität. Damit ist nicht fehlerhafte Software gemeint. Ein Trojanisches Pferd manipuliert zusätzlich Daten oder zeichnet diese verbotener weise in einem Speicherbereich. Beispiele dafür sind Editoren, Textverarbeitungsprogramme manipulierte Datenbanken oder Login-Prozesse.

Als Gegenmaßnahmen können die Rechte von Benutzern beschränkt werden. Sensible Daten wie Passworte sollten nicht im Klartext auf Speichermedien, wie Festplatten abgelegt werden. Programme können digital signiert werden und vor der Ausführung auf Korrektheit der Signatur überprüft werden.

Trojanische Pferde werden über Würmer, Viren oder Puffer-Überläufe verbreitet.

Abwehr von Angriffen

Passive Angriffe sind z. B. bei einem WLAN sehr schwer zu unterbinden. Da hierzu auch die Nutzung von verdeckten Kanälen zählt, kann nur versucht werden die Bandbreite eines solchen Kanals zu reduzieren.

Verschlüsselung

Eine Möglichkeit die Angriffsfläche zu reduzieren ist die Verschlüsselung. Mit kryptographischen Verfahren kann man sich bei den sog. Sniffer-Angriffen schützen. Verschlüsselt übertragene Passwörter können nicht mehr ausgespäht werden. Allerdings kann ein aufgezeichnetes verschlüsseltes Passwort immer noch für die Authentifizierung verwendet werden. Um sich vor solchen Angriffen zu schützen sind weitere Maßnahme bei der Authentifizierung erforderlich.

Rechte-Reduzierung

Aktive Angriffe können durch eine restriktive Rechte-Vergabe zumindest reduziert werden.

Monitoring

Eine kontinuierliche Überwachung des Datenverkehrs auf den Netzwerken mit so genannten Intrusion Detection Systemen (IDS) (deutsch: Einbruchs-Erkennungssystem) oder Intrusion Prevention Systemen (IPS) (deutsch:

Abbildungsverzeichnis

Einbruchs-Vermeidungssystem) schafft einen Überblick über die aktuelle Bedrohung und hilft bei der Analyse von Einbruchsversuchen. Allerdings ist die Parametrierung gerade bei den IPS eine diffizile Angelegenheit.

Angreifer Typen

Hacker

Hacker waren während den Anfängen des Internets technisch versierte, begnadete Programmierer die einen möglichst optimalen Programmcode entwickeln wollten. Ein guter Hack war ein möglichst kurzer Programmcode mit dem möglichst viel erreicht werden sollte.

Heutzutage sind Hacker Personen, die es darauf angelegt haben in fremde Systeme einzudringen. Dort hinterlassen sie dann ihre Duftmarke. Dies gelingt ihnen in der Regel durch die Entwicklung eines Exploits. Dies ist ein Stück Software mit der ein Angriff durchgeführt werden kann. Hacker wenden sich mit diesen Exploits an die Öffentlichkeit oder an die Betreiber der betroffenen Systeme. Normalerweise ziehen die Hacker aus diesem Tun weder persönlichen Vorteile noch schaden sie dadurch Dritten. Obwohl sich die Hacker an eine Hacker-Ethik halten, verwenden sie illegale Mittel für ihre Aktionen.

Cracker

Cracker sind, wie die Hacker technisch versierte Programmierer und gehen wie sie vor. Allerdings versucht ein Cracker mit seinem Tun für sich einen Vorteil oder dem Angegriffenen einen Nachteil zu verschaffen.

Skript-Kiddie

Während Hacker und Cracker noch mit viel Know-how ihre Angriffe durchführen, ist bei Skript-Kiddies kein technisches Wissen vorhanden. Sie verwenden im Internet frei verfügbare Software (Exploits) um ihre Angriffe durchzuführen. Ihre Motivation besteht eher aus Neugier und Spieltrieb als der Absicht zu schaden.

Rechtliche Rahmenbedingungen

Die Vielfalt der Gesetze, die sich mit IT-Sicherheit beschäftigen, lassen schnell den Eindruck entstehen, dass man sich ohne eine juristische Ausbildung nur im Paragraphen-Dschungel verirren kann. Die Einstellung, dann ganz auf die Beachtung der Rechtslage zu verzichten ist allerdings ein Fehler denn Unwissenheit schützt nicht vor Strafe.

Relevante Gesetze

Bundes Datenschutzgesetz (BDSG)

§3 Grundsatz der Datenvermeidung

§4 Verbot der Erhebung personenbezogener Daten

§5 Festlegung des Datengeheimnisses

§9 Notwendige technische und organisatorische Maßnahmen

§28 Datenerhebung für eigene Zwecke

Telekommunikationsgesetz (TKG)

§ 85 Fernmeldegeheimnis

Betriebsverfassungsgesetz (BetrVG)

§ 87 Abs. 1 Mitbestimmungsrechts bei Content-Scanning

§ 87 Abs. 1 Nr. 6 Technische Überwachungseinrichtung

Strafgesetzbuch (StGB)

§ 201 StGB Verletzung der Vertraulichkeit des Wortes

§ 202a StGB Ausspähen von Daten

§ 206 StGB Post- und Fernmeldegeheimnis

§ 303a StGB Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

§ 303b Computersabotage

(1) Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, dass er

1. eine Tat nach § 303a Abs. 1 begeht oder

2. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

Bürgerliches Gesetzbuch (BGB)

§§ 823, 1004 BGB Unterlassungsansprüche

Gesetz zur Kontrolle und Transparenz im Unternehmen (KonTraG)

Mit Einführung des Gesetzes zur Kontrolle und Transparenz im Unternehmen (KonTraG) im Mai 1998 sind Aktiengesellschaften sowie Tochterfirmen (unabhängig von ihrer Gesellschaftsform) zur Implementierung eines unternehmensweiten Früherkennungssystems für bestandsgefährdende Risiken sowie eines entsprechenden Überwachungssystems verpflichtet. Dies betrifft auch die IT Landschaft.

Wer nicht einführt, haftet **persönlich**.

Aktiengesetz (AktG)

Im Aktiengesetz ist festgelegt, dass ein Vorstand persönlich haftet, wenn er Entwicklungen, die zukünftig ein Risiko für das Unternehmen darstellen könnten, nicht durch ein Risiko-Management überwacht und durch geeignete Maßnahmen vorbeugt (§ 91 Abs. 2 und § 93 Abs. 2 AktG).

GmbH-Gesetz (GmbHG)

Geschäftsführern einer GmbH wird im GmbH-Gesetz "die Sorgfalt eines ordentlichen Geschäftsmannes" auferlegt (§ 43 Abs. 1 GmbHG).

Haftung

Gerichtsurteile

Manager haften persönlich

"ARAG-Garmenbeck"-Entscheidung des BGH v. 21.04.1997

Schadensersatz bei Verbreitung eines Computervirus

- LG Hamburg, Urteil vom 18.07.2001, Az: 401 O 63/00

Schadensersatz bei Serverausfall

Amtsgericht Charlottenburg 208 C 192/01

usw.

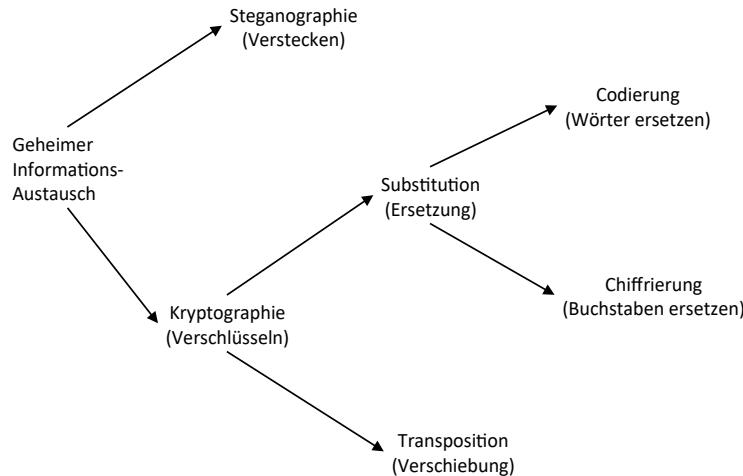
Hieraus lassen sich konkrete Verpflichtungen für die Gewährleistung eines angemessenen IT-Sicherheitsniveaus im eigenen Unternehmen ableiten.

Für bestimmte Berufsgruppen gibt es darüber hinaus noch höhere Anforderungen, bis zu Regelungen im Strafgesetzbuch (§ 203). Ein fahrlässiger Umgang mit Informationstechnik kann diesen Tatbestand bereits erfüllen.

Abbildungsverzeichnis

Auch Banken berücksichtigen, bei der Kreditvergabe IT-Risiken des Kreditnehmers - mit unmittelbaren Auswirkungen auf die angebotenen Konditionen (Basel II).

Geheimer Datenaustausch

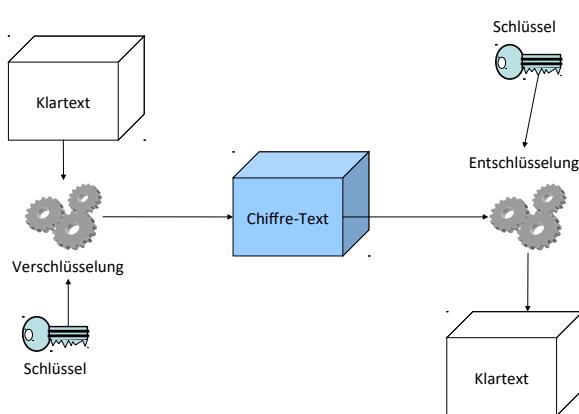


Für die Geheimhaltung von Daten wurden im Laufe mehrerer Jahrhunderte unterschiedliche Verfahren entwickelt. Besonders erfolgreich waren hierbei die Steganographie (griechisch: steganos = bedeckt, graphein = schreiben) mit unsichtbarer Tinte und dem verstecken von Texten in Bildern und die Kryptografie (griechisch: Kryptos = verbergen) mit den Verschlüsselungstechniken.

Abbildung 213 : Geheimhaltung

Verschlüsselung

Für die Problematik eines sicheren Datenaustauschs sind verschiedene Verschlüsselungsverfahren entwickelt worden. Dabei wird grundsätzlich ein lesbaren Text (Klartext-Nachricht) mit einer Verschlüsselungsfunktion in eine nicht mehr lesbaren Text (Chiffre-Text-Nachricht oder auch Chiffrat) umgewandelt. Diese Daten können dann über unsichere Transportwege zum Empfänger der Nachricht transportiert werden. Selbst wenn unterwegs die Daten mit geschrieben werden kann niemand mit dem Text etwas anfangen da er unlesbar ist.



Der Empfänger der Nachricht kann mit dem übertragenen Text zunächst ebenfalls nichts anfangen. Erst wenn er auf das Chiffrat eine Entschlüsselungsfunktion anwendet entsteht wieder der ursprüngliche Klartext. Sind die Daten beim Empfänger angekommen muss ein Sicherheitssystem auch sicherstellen, dass diese Daten nicht schon einmal übertragen wurden.

Abbildung 214 : Verschlüsselung

Bei den Verschlüsselungsverfahren ist Verschlüsselungsmechanismus offen gelegt. Die Geheimhaltung wird durch die Verwendung des geheimen Schlüssels erreicht. Wer den Schlüssel hat, der hat auch die Möglichkeit den Chiffre-Text zu entschlüsseln, bzw. gefälschte Chiffre-Texte zu verfassen.

Kryptographie

Die Kunst der geheimen Kommunikation wird auch als Kryptographie bezeichnet.

Kryptoanalyse

Die Kunst geheime, also verschlüsselte Texte zu entziffern wird als Kryptoanalyse bezeichnet. Hierbei wurden verschiedene Methoden entwickelt.

Statistische Kryptoanalyse

Hierbei wird die Häufigkeit der verwendeten Zeichen mit der Wahrscheinlichkeit des Auftretens innerhalb einer Sprache verwendet.

Verfahren die nur eine Verschiebungschiffre oder eine Substitutionschiffre verwenden können mit dieser Analysemethode geknackt werden.

DES und alle folgenden Verfahren können nicht mit einer statistischen Kryptoanalyse geknackt werden da die Methoden von Shannon zur Diffusion und Konfusion verwendet wurden.

Differentielle Kryptoanalyse

Hierbei wird die Auswirkung von Unterschieden im Klartext auf die entsprechenden Geheimtext-Paare untersucht. Die Unterschiede werden eingesetzt um den möglichen Schlüsseln Wahrscheinlichkeiten zuzuweisen. Damit wird der wahrscheinlichste Schlüssel gefunden. Dieses Verfahren wurde 1990 erstmalig von Murphy beschrieben.

Lineare Kryptoanalyse

Hierbei wird versucht eine lineare Approximation zu finden die auf den Transformationen basieren welche ein Verschlüsselungsverfahren mit dem Klartext durchführt.

Kryptoregulierung

Der Einsatz kryptographischer Methoden für die geheime Übertragung von Daten ist in den Augen der Regierungen ein Problem bei der Verbrechensbekämpfung. Besonders die USA wollen die im Einsatz befindlichen kryptographischen Verfahren begrenzen um auf die Klartexte noch einen Zugriff zu haben. Das organisierte Verbrechen oder der Terrorismus soll sich mit den Verschlüsselungstechniken keine Vorteile gegenüber den staatlichen Organen verschaffen können.

Die Vorstellung die hierbei verfolgt wird ist die Hinterlegung der Schlüssel (engl. key escrow) an einem sicheren Ort an dem auch die gesetzlichen Vertreter im Notfall einen Zugriff haben. Eine Hinterlegung eines Schlüssels läuft allerdings den Grundgedanken einer Verschlüsselung zuwider. Ein Schlüssel sollte nur einmal bei seinem Besitzer hinterlegt sein. Nur so kann garantiert werden dass bei Verwendung von digitalen Signaturen der Sender einer Signatur auch wirklich die richtige Person ist.

Außerdem wären solche Pools in denen die Schlüssel hinterlegt wären ein lohnendes Angriffsziel.

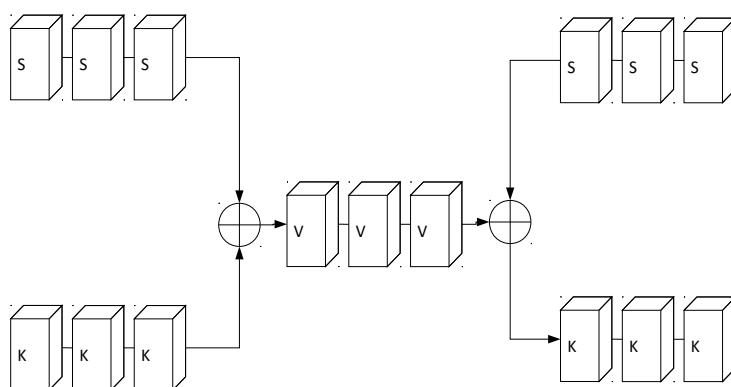
In Deutschland bestehen erhebliche verfassungsrechtliche Bedenken gegen eine Kryptoregulierung. Die Grundrechte auf wirtschaftliche Entfaltungsfreiheit aus Art. 12 Abs. 1, Art. 2 Abs. 1 GG, der Vertraulichkeit der Kommunikation aus Art. 10 GG sowie des informationellen Selbstbestimmungsrechts aus Art. 2 Abs. 1, Art. 1 Abs. 1 GG würden verletzt werden.

Deshalb dürfen nach einer Entscheidung des Bundeskabinetts vom 2. Juni 1999 Verschlüsselungsverfahren und -produkte ohne Restriktionen entwickelt, hergestellt, vermarktet und genutzt werden.

Chiffrierer

Die Chiffrierung kann mit zwei unterschiedlichen Methoden realisiert werden. Die Daten können als Strom also ein Bit nach dem anderen verschlüsselt oder blockweise aufbereitet werden.

Stromchiffrierer

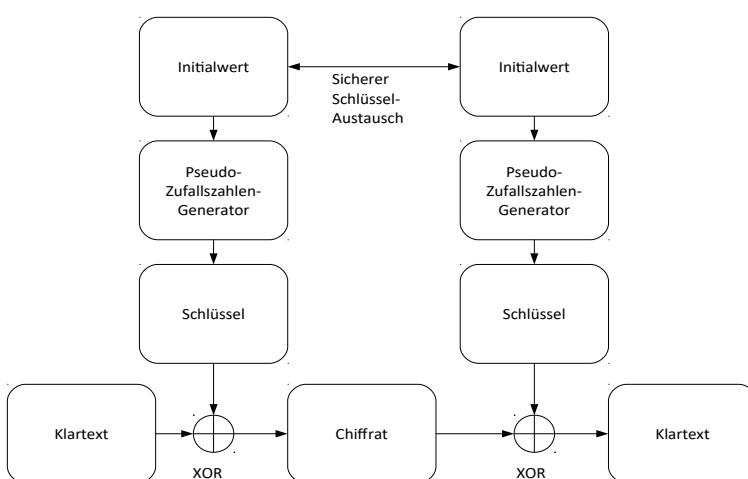


Hierbei wird sowohl für das Verschlüsseln als auch das Entschlüsseln der gleiche Schlüssel verwendet.

Sowohl der Klartext als auch der Schlüssel wird als Datenstrom verstanden und bearbeitet.

Die zu verschlüsselnden Daten werden bitweise mit einer XOR-Funktion mit dem Schlüsselstrom verknüpft.

Abbildung 215 : Stromchiffrierer



Um die Schlüsselübertragung abzusichern wird der Schlüssel mittels eines Pseudo-Zufallszahlen-Generators erzeugt.

Damit beide Pseudo-Zufallszahlen-Generatoren synchron arbeiten und den gleichen Schlüssel erzeugen sind sie mit einem Initialisierungswert, auch Initialisierungsvektor genannt, vom Administrator zu versorgen. Hierbei ist natürlich voraus zu setzen, dass der Initialisierungsvektor sicher verwaltet und transportiert wird.

Abbildung 216 : Stromchiffrierer Funktionen

Somit ist nicht mehr der gesamte Schlüsselstrom sondern nur noch der Initialisierungsvektor beim Schlüsselaustausch zu übertragen.

Blockchiffrierer

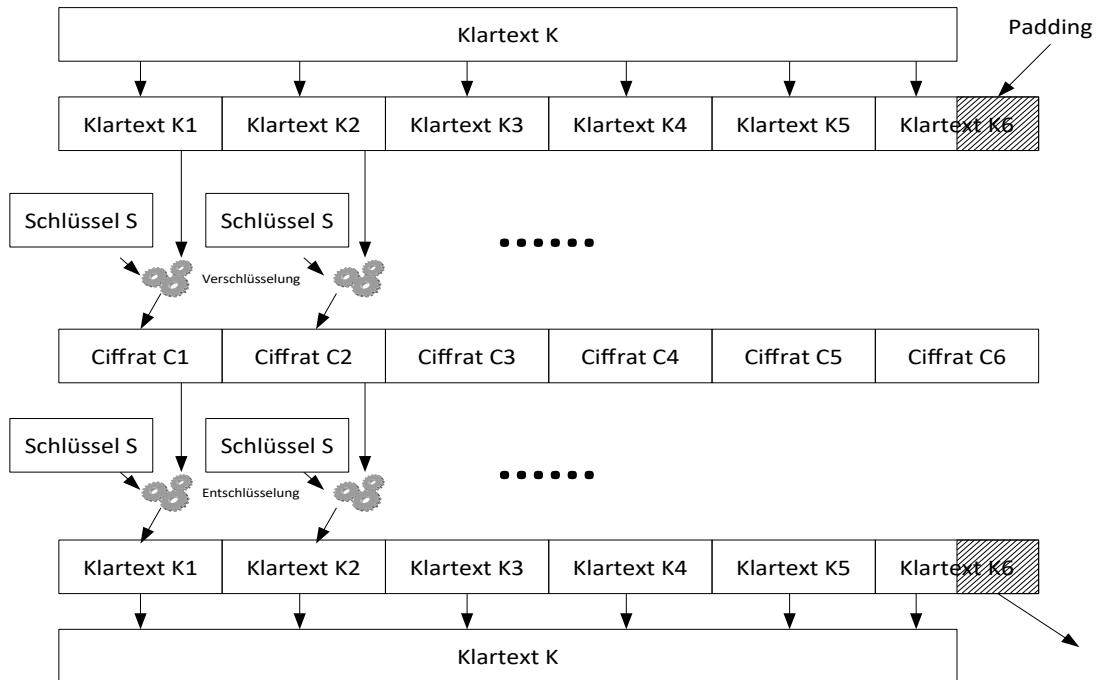


Abbildung 217 : Blockchiffrierer im ECB-Modus

Hierbei wird der Klartext zuerst in Blöcke von 64 Bit Länge zerlegt. Entspricht der Klartext nicht genau einem Vielfachen von 64 Bit wird der letzte Klartextblock mit einem Bitmuster (Padding) aufgefüllt. Die Länge des Klartextanteils ist im letzten Block zu kodieren.

Bei der Blockverschlüsselung gibt es zwei Modi:

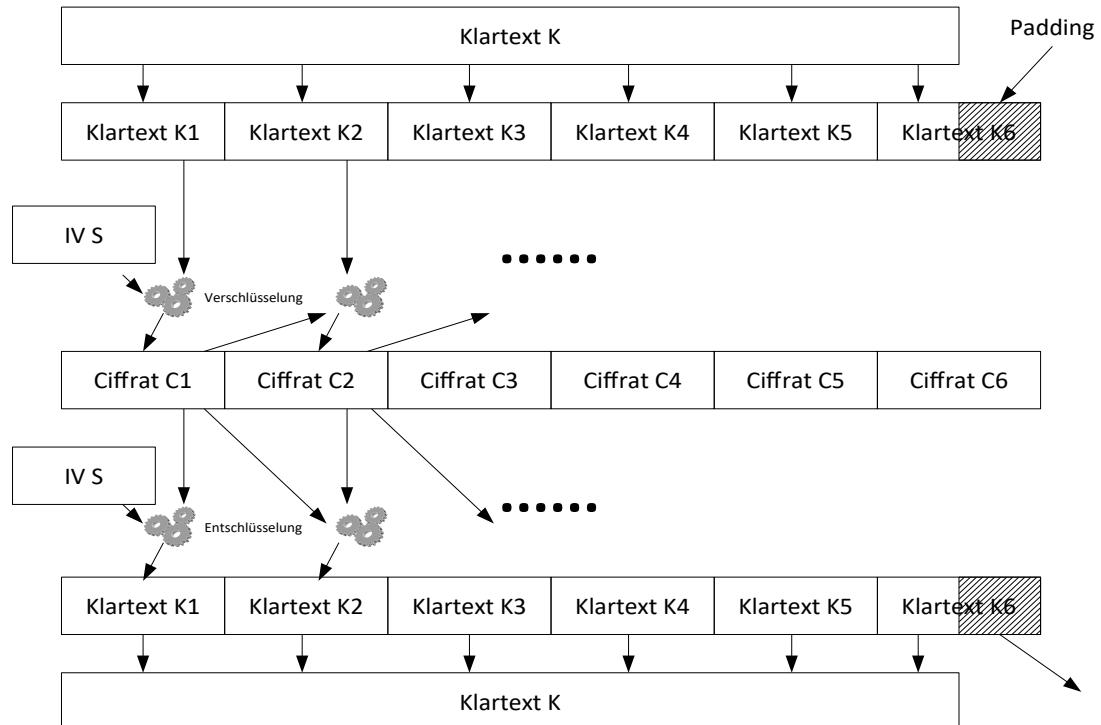
- ➊ ECB-Modus
- ➋ CBC-Modus

ECB-Modus

Im ECB-Modus (Electronic Code-Book) wird jeder Block unabhängig von den anderen Blöcken verschlüsselt. Dadurch wird bei der Verschlüsselung auf jeden Klartextblock der gleiche Schlüssel zur Verschlüsselung angewendet.

CBC-Modus

Beim CBC-Modus (Cipher-Block-Chaining) ist das Ergebnis einer Blockchiffrierung vom Ergebnis der letzten Blockchiffrierung abhängig. Das Problem einer Fehlerfortpflanzung ist hier gravierend. Sobald ein Chiffretext fehlerhaft übertragen wird ist der restliche Text nicht mehr zu entschlüsseln.



Wird bei der Erzeugung eines Schlüsselstroms als Pseudo-Zufallszahlen-Generator ein Blockchiffre eingesetzt, kann aus einem Blockchiffre-Verfahren ein Stromchiffre-Verfahren gemacht werden.

Hierzu gibt es zwei unterschiedliche Verfahren:

- ➊ Output-Feedback-Modus (OFB-Modus)
- ➋ Cipher-Feedback Modus (CFB-Modus)

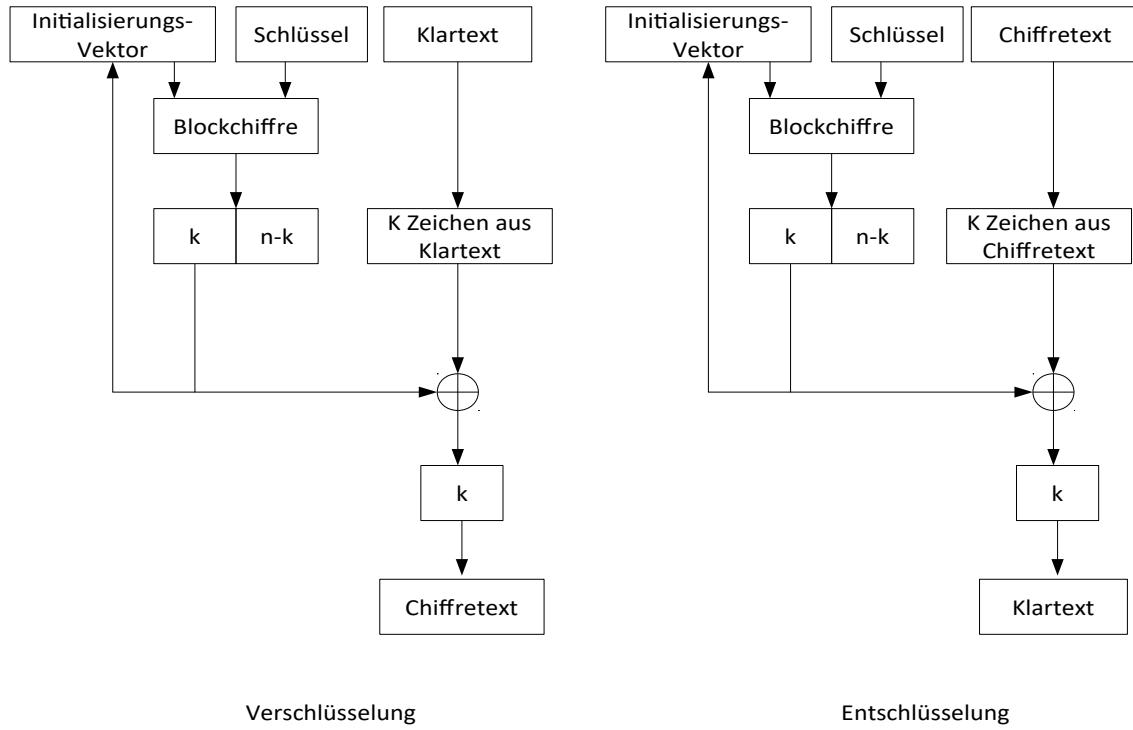


Abbildung 219 : OFB-Modus

In beiden Fällen wird der Blockchiffre als Pseudozufallszahlengenerator verwendet. Sowohl beim Verschlüsseln als auch beim Entschlüsseln erzeugt der Blockchiffre den Schlüsselstrom der mit dem Klartext/Chiffretext mit einer XOR-Funktion verknüpft wird.

Der vorher auszutauschende Schlüssel dient als Initialisierungsvektor und ist auf beiden Systemen vom Administrator einzubringen.

Der CFB-Modus arbeitet ähnlich wie der OFB-Modus. Der Unterschied ist, dass für das Ersetzen von k -Bits des Eingabeblocks der Blockchiffre nicht auf einen Teil des Ausgabeblocks sondern auf die erzeugten Chiffretextzeichen zurückgegriffen wird.

In beiden Modi kann nach dem Auftreten eines Übertragungsfehlers nicht weiter Entschlüsselt werden.

Schlüsselverfahren

Symmetrische Schlüsselverfahren

Bei diesem Verfahren wird nur ein Schlüssel verwendet. Er dient gleichermaßen zum Ver- und Entschlüsseln der Nachrichten. Diese Verfahren sind schnell, haben aber den Nachteil, dass die Schlüssel bevor sie angewendet werden können sowohl beim Sender als auch beim Empfänger vorliegen müssen. Damit entsteht das Problem des Schlüsselaustauschs. Es wird im Allgemeinen dadurch gelöst, dass die symmetrischen Schlüssel, über eine bereits über asymmetrische Schlüssel aufgebaute Verbindung, ausgetauscht werden.

Asymmetrische Schlüsselverfahren

Bei den asymmetrischen Schlüsselverfahren werden 2 unterschiedliche Schlüssel verwendet. Ein Schlüssel dient zum Verschlüsseln und wird öffentlich vergeben (public key). Deshalb wird dieses Verfahren auch Public Key Verfahren genannt. Jeder der dem Empfänger eine verschlüsselte Nachricht zukommen lassen will kann diesen Schlüssel zum Verschlüsseln verwenden. Der Schlüssel zum Entschlüsseln (private key) bleibt im Privatbesitz des Empfängers. Beide Schlüssel sind einander zugeordnet. Asymmetrische Schlüssel sind sicherer als symmetrische Schlüssel, jedoch sind sie in der Verarbeitung wesentlich aufwändiger und somit langsamer. Deshalb werden sie im allgemeinen nicht für die Verschlüsselung von Daten sondern für den Austausch symmetrischer Schlüssel verwendet.

Public Key Verfahren zur Verschlüsselung

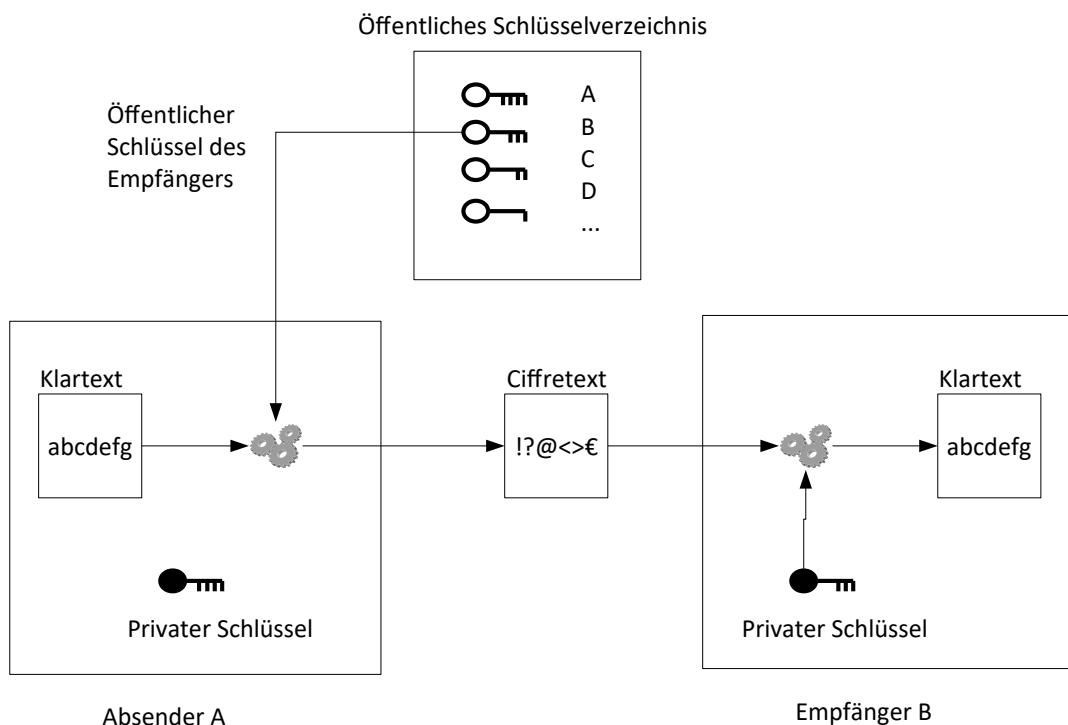


Abbildung 220 : Verschlüsselung mit dem Public Key Verfahren

Ein weiterer Vorteil des Verfahrens ist, dass nicht nur die Daten verschlüsselt werden können, sondern die Authentizität des Absenders überprüft werden kann.

Dazu wird eine Nachricht mit dem privaten Schlüssel verschlüsselt und übertragen. Der Empfänger kann mit dem öffentlichen Schlüssel die Nachricht wieder entschlüsseln. Eine erfolgreiche Entschlüsselung kann als Beweis dafür verwendet werden, dass wirklich diese Person die Daten verschlüsselt hat. Da dieser Vorgang einer Unterschrift in digitaler Form gleich kommt wird dieses Vorgehen auch digitale Signatur genannt.

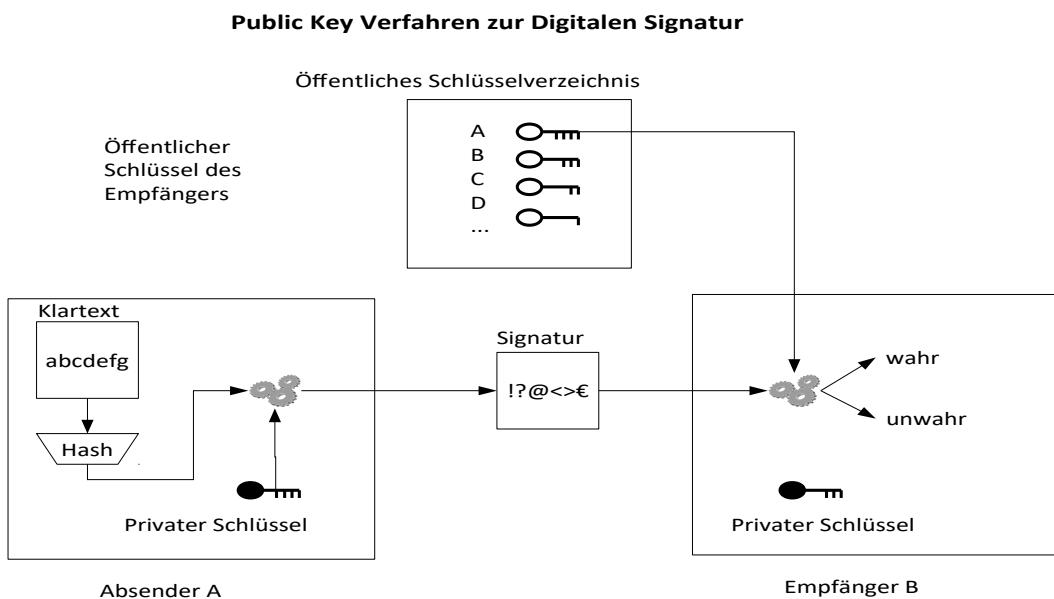


Abbildung 221 : Digitale Signatur

Mit dem Public Key Verfahren kann sowohl ein geheimer Datenaustausch durchgeführt, als auch eine digitale Signatur durchgeführt werden.

Zusätzlich ist mit diesem Verfahren ein einfaches Schlüssel-Management möglich. Mit diesem asymmetrischen Verfahren können symmetrischen Schlüssel sicher ausgetauscht werden. Damit ist das Problem des Schlüsselaustauschs von symmetrischen Schlüsseln lösbar.

Da dieses Verfahren sehr rechenintensiv ist, wird es zum Austausch großer Datenmengen nicht verwendet. Große Datenmengen werden mit symmetrischen Schlüsseln verschlüsselt da diese Schlüssel einfach zu implementieren sind und keine große Rechenkapazität benötigen.

Übersicht über Schlüsselverfahren

	<i>Symmetrisch</i>	<i>Asymmetrisch</i>
Operation	Shift, XOR	Ganzzahlige Exponenten, Log
Geschwindigkeit	schnell	Langsam
Schlüssel-Länge	100-256Bit	2000 Bit 2047 Bit 2048 Bit
Benötigte Schlüssel-Anzahl	$N * (n - 1) / 2 \approx n^2$	n
Anwendung	Datenverschlüsselung	Schlüsselaustausch
Algorithmus	DES, 3DES, IDEA, AES	RSA, Diffie-Hellmann

Verschlüsselungsstandards

Verwendete Methoden

S-Boxen

Die Daten werden in Tabellenform abgelegt. Danach wird mit den Daten eine nichtlineare Substitution durchgeführt.

Byte-Umstellung

Die Diffusion (Umstellung von Bytes) wird einer MDS—Matrix (Maximum Distance Separable) durchgeführt. Dabei wird eine Multiplikation mit der Matrix durchgeführt.

Pseudo-Hadamard-Transformation (PHT)

PHT ist eine Mischung von zwei 32-Bit-Zahlen nach folgenden Gleichungen.

$$a' = a + b \bmod 2^{32}$$

$$b' = a + 2b \bmod 2^{32}$$

Transformation / Verschiebungschiffre

Hierbei wird das ABC um n Zeichen verschoben interpretiert. Diese Verschlüsselung wird auch Verschiebungschiffre genannt. Beim Spezialfall mit n = 3 spricht man auch von der Cäsar-Verschlüsselung da diese Methode bereits von Julius Cäsar angewandt wurde. Dabei wird der erste Buchstabe A zu D der zweite Buchstabe B wird zu E usw.

Beispiel mit n=4. Dabei wird der erste Buchstabe A zu E der zweite Buchstabe B wird zu F usw. :

Buchstaben	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Verschlüsselte Buchstaben	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

Da es nur 26 Schlüssel gibt ist die Verschlüsselung ist leicht zu knacken. Nach spätestens 25 Versuchen ist der Schlüssel gefunden. Damit erfüllt die Cäsar-Chiffre nicht Kerckhoffs-Prinzip nach dem die Sicherheit eines kryptographischen Verfahrens nur vom verwendeten Schlüssel abhängen sollte. Damit ein Angreifer nicht durch einfaches ausprobieren den Schlüssel finden kann ist ein wesentlich größerer Schlüsselraum erforderlich.

Beispiel:

Zuerst wird jedem Buchstaben im Alphabet eine Ziffer zugeordnet.

Buchstabe	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Position für Umsetzung	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Nun kann ein Klartext verschlüsselt werden.

Klartext	D	A	T	E	N	U	E	B	E	R	G	A	B	E	M	O	R	G	E	N
Umgesetzter Klartext	3	0	19	4	13	20	4	2	4	17	6	0	1	4	12	14	17	6	4	13
Schlüssel	2																			
Chiffrettext	5	2	21	6	15	22	6	4	6	19	8	2	3	6	14	16	19	8	6	15
Übertragener Chiffrettext	F	C	V	G	P	W	G	E	G	T	I	C	D	G	O	Q	T	I	G	P

Substitutionschiffre

Bei dieser Verschlüsselung wird jedes Zeichen des ABC's einem anderen Zeichen zugeordnet. Infolgedessen stellt der Schlüssel statt einer ganzen Zahl eine Permutation dar.

Im folgenden Beispiel wird der Buchstabe A zu M, der Buchstabe B zu S usw.

Buchstabe	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Umsetzung	M	S	Q	C	N	D	J	R	T	E	B	W	U	K	A	X	L	O	Z	F	Y	H	V	G	P	I

Da ein Schlüsselplatz aus allen möglichen 26 Symbolen bestehen kann gibt es $26!$ mögliche Permutationen. Dies bedeutet maximal $26!$ Versuche um den Schlüssel zu knacken.

Für das obige Beispiel ergibt sich nun die folgende Umsetzung.

Klartext	D	A	T	E	N	U	E	B	E	R	G	A	B	E	M	O	R	G	E	N
Chiffretext	C	M	F	N	K	Y	N	S	N	O	J	M	S	N	U	A	O	J	N	K

Symmetrische Verschlüsselungsstandards

DES (Data Encryption Standard)

Dieser Standard wurde Mitte der 70er Jahre von IBM entwickelt. Es handelt sich um ein Blockchiffre-Verfahren. Es wird ein 64-Bit-Klartext-Block mit einem 64-Bit-Schlüssel-Block, in einen 64-Bit-Ausgabe-Block verschlüsselt. Jedes 8. Bit des Schlüssels dient der Paritätsprüfung und trägt somit nichts zur Verschlüsselung bei. Damit hat der Schlüssel eigentlich nur 56 Bit. Als Verschlüsselungstechniken werden folgende Techniken verwendet:

- ➊ Bitpermutation (Transposition)
- ➋ Substitution
- ➌ bitweise Addition modulo 2

DES kann in den folgenden Modi betrieben werden:

- ➊ ECB
- ➋ CBC
- ➌ CFB
- ➍ OFB

TripleDES / 3DES

Hierbei wird DES drei Mal hintereinander angewendet. Dabei werden 3 Schlüssel verwendet die zusammen eine Schlüssellänge von 168 Bit ergibt. Durch mögliche Meet-in-the-Middle Angriffe reduziert sich die effektive Schlüssellänge auf 108 Bit. 3DES lässt sich analog zu DES im CBC-Modus betreiben.

Verschlüsselung: $\text{DES}(\text{DES}^{-1}(\text{DES}(X, K^1), K^2), K^3)$

Entschlüsselung: $\text{DES}^{-1}(\text{DES}(\text{DES}^{-1}(X, K^3), K^2), K^1)$

International Data Encryption Algorithm (IDEA)

Da die restriktiven Schlüsselverwaltungsauflagen der USA zu starke Einschränkungen der Sicherheit boten wurden weltweit weitere Verschlüsselungsverfahren entwickelt. Hierzu gehört das Anfang der 90er Jahre vorgestellte IDEA. Es ist ein Blockchiffre-Verfahren bei dem Blöcke von 64 Bit mit Schlüsseln von 128 Bit verschlüsselt werden. Zur Verschlüsselung werden folgende Funktionen verwendet:

- ➊ Addition
- ➋ Multiplikation
- ➌ XOR-Verknüpfungen

IDEA kann, wie DES in den folgenden Modi betrieben werden:

- ➊ ECB
- ➋ CBC
- ➌ CFB
- ➍ OFB

Blowfish

Blowfish wurde 1993 von Bruce Schneider entwickelt. Es ist ein Blockchiffre-Verfahren. Dabei werden jeweils 64 Bit des Klartextes mit einem variablen Schlüssel von bis zu 448 Bits verschlüsselt. Blowfish ist frei verfügbar und sehr schnell. Die verwendeten mathematischen Operationen sind:

Addition

Index-Operation

XOR-Verknüpfung

Es werden 16 Runden durchlaufen in denen je 2 Blöcke von 32 Bit einer Permutation und einer Substitution unterworfen werden.

RC4

RC4 wurde 1987 von Ron Rivest entwickelt und lange geheim gehalten. RC4 ist ein Schlüsselstrom-Verfahren. Der Schlüssel wird aus einem 64 Byte großen Feld erstellt. Aus diesem Feld wird der Schlüsselstrom über einige Additionen und eine Substitution erstellt.

RC4 ist sehr schnell. Da jedoch viele „schwache Schlüssel“ erzeugt werden ist RC4 nicht mehr zeitgemäß.

RC4 wird bei der ursprünglichen WEP-Verschlüsselung bei WLANs sowie bei der SSL-Verschlüsselung von Browsern eingesetzt.

AES

1997 begann die Suche nach einem Nachfolger für DES. 3DES bietet zwar mit einem Schlüssel von 108 Bit eine ausreichende Sicherheit, benötigt jedoch auch die 3fache Zeit wie DES.

Das National Institute of Standards (NIST) in den USA veröffentlichte hierzu eine Ausschreibung. Bis 1999 wurden für den neuen Standard AES (Advanced Encryption Standard) 15 Bewerbungen eingereicht. Diese Bewerbungen wurden Kryptologen und anderen Interessenten zur Begutachtung übergeben. Am 2. Mai 2000 wurde Ergebnis der Begutachtung, eine Reduzierung auf die folgenden 5 Kandidaten bekannt gegeben:

- ➊ MARS (IBM)
- ➋ RC6 (RSA Laboratories)
- ➌ Rijndael (Universität Leuven)
- ➍ Serpent (Universität Cambridge und San Diego)
- ➎ Twofish (Bruce Schneider)

Am 2. Oktober wurde vom NIST Rijndael als Sieger bekannt gegeben. Damit ist Rijndael von Joan Daemen und Vincent Rijmen das neue AES und damit der Nachfolger von DES. AES ist frei von Patenten und wird deshalb eine schnelle Verbreitung finden.

Rijndael ist ein Blockchiffre-Verfahren. Die zu verschlüsselnde Blocklänge kann 128, 192 oder 256 Bit betragen. Die Schlüssellängen können genauso gewählt werden. Die Anzahl der zu durchlaufenden Runden beträgt je nach Block- und Schlüssellänge 10, 12 oder 14.

	Blocklängen		
Schlüssellängen	128	192	256
128	10	12	14
192	12	12	14
256	14	14	14

1. Der erste Rundenschlüssel wird mit XOR mit dem Block verknüpft.

2. Bei jeder Runde werden folgende 4 Einzelschritte durchlaufen:

➊ Substitution

Jedes Byte des Blocks wird durch eine S-Box-Eintrag ersetzt.

➋ Permutationen

Die Bytes des Blockes werden in Shift-Row-Transformationen permutiert. Dabei werden die Bytes in den Zeilen des zweidimensionalen Feldes state zyklisch verschoben.

➌ Diffusion

Es wird eine Mix-Column-Transformation durchgeführt. Hierbei wird spaltenweise eine Multiplikation mit einem festgelegten Polynom durchgeführt. Dies bewirkt, dass jedes Byte der Spalte mit jedem anderen Byte der Spalte in Wechselwirkung tritt. Die Polynome sind so gewählt, dass mittels Shift und XOR effizient gearbeitet werden kann.

➍ Schlüssel-Verknüpfung

Der Block wird mit dem Rundenschlüssel mit XOR verknüpft.

3. In der abschließenden Runde wird die Mix-Column-Transformation der regulären Runden ausgelassen.

Bei AES sind im Gegensatz zu DES keine schwachen Schlüssel bekannt. AES ist hochperformant. Eine Referenz-Implementierung mit 500 Zeilen C-Code ist unter <http://www.nist.gov/aes> zu finden. Weitere Informationen sind unter http://csrc.nist.gov/encryption/aes/aes_home.htm zu finden.

Asymmetrische Verschlüsselungsstandards

Diffie-Hellmann

Es ist das erste Verfahren mit asymmetrischen Schlüsseln und wurde 1976 von Whitfield Diffie und Martin Hellmann entwickelt.

Das Verfahren beruht auf der Tatsache, dass eine Potenzierung von großen Zahlen viel einfacher ist als deren Umkehrfunktion der Logarithmus. Damit ist es möglich einen Schlüssel geheim auszutauschen auch wenn der Datenverkehr mit gelesen wird.

Vorgehensweise:

Beide Partner einigen sich auf eine große Primzahl n und eine natürliche Zahl g . Beide Zahlen (g und n) können nun gefahrlos über ein unsicheres Netzwerk ausgetauscht werden.

Jeder Partner wählt jetzt eine geheime Zahl. Partner A wählt x und Partner B wählt y .

Der Besitzer von x , also Partner A, führt folgende Operation aus:

$$x = g^x \bmod n$$

x wird von Partner A an den Partner B gesendet.

Der Partner B führt die folgende Operation durch:

$$y = g^y \bmod n$$

und sendet y an den Partner A.

Nach dem Empfang von y berechnet Partner A

$$K = y^x \bmod n$$

Der Partner B berechnet:

$$K' = x^y \bmod n$$

Als Ergebnis erhalten beide das Gleiche:

$$K = K' = g^{xy} \bmod n$$

Damit sind K und K' der geheime Schlüssel.

Mit dieser Methode kann auch ein Schlüsselpaar mit geheimen und öffentlichem Schlüssel erstellt werden. Die Primzahl n und die natürliche Zahl g muss allen Teilnehmern bekannt sein. Jeder Teilnehmer wählt per Zufallsgenerator einen geheimen Schlüssel x .

Der zugehörige öffentliche Schlüssel wird mit:

$$x = g^x \bmod n$$

berechnet.

Will ein Teilnehmer Nachrichten verschlüsselt senden, ermittelt er aus seinem geheimen Schlüssel und dem öffentlichen Schlüssel eines Empfängers den symmetrischen Schlüssel K . Diesen Schlüssel kann der Empfänger ebenso ermitteln und den Chiffretext in einen Klartext umwandeln.

RSA

Dieses Verfahren beruht auf dem Verfahren von Diffie und Hellmann. Es wurde von Ron Rivest, Adi Shamir und Howard Adleman die mit den Anfangsbuchstaben ihrer Namen dem Verfahren seinen Namen gaben.

Schlüsselberechnung:

1. 2 große Primzahlen p und q werden zufällig ausgewählt.
2. Es wird das Produkt der beiden Primzahlen durch die Berechnung $n = p * q$ ermittelt.
1. p und q werden gelöscht.
2. der öffentliche Schlüssel besteht aus n und einem Chiffrierschlüssel e der durch einen Zufallszahlengenerator ermittelt wird. Es muss ein e gefunden werden das zu $(p-1)(q-1)$ prim ist. D. h. Es gibt keinen gemeinsamen Teiler.
3. Der Private Schlüssel d berechnet sich aus $d = e^{-1} \text{ mod } ((p-1)(q-1))$.

Bei der Verschlüsselung werden die Klartextblöcke b mit dem öffentlichen Schlüssel n und e in verschlüsselte Blöcke v umgesetzt:

$$v = b^e \text{ mod } n$$

Die Entschlüsselung geschieht mit dem privaten Schlüssel:

$$b = v^d \text{ mod } n$$

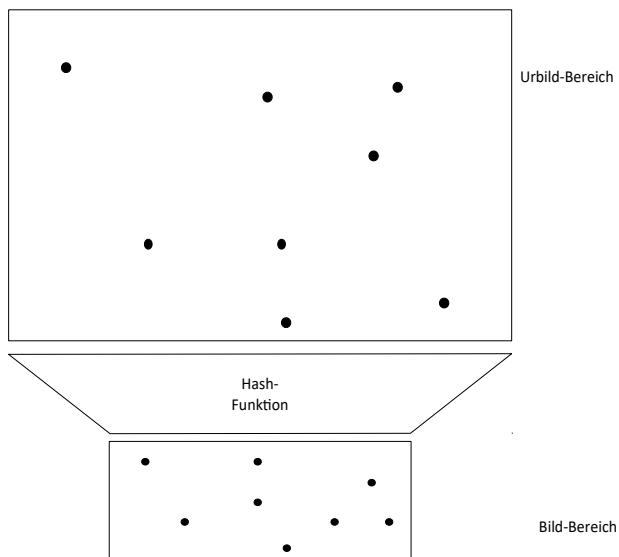
Ein Angreifer kann den privaten Schlüssel d aus den öffentlich bekannten Teilern e und n nur dann ermitteln wenn er p und q kennt.

Heutzutage werden für p und q große Zahlen mit 1024 oder 2048 Bit verwendet. Ein Brute Force Angriff durch ausprobieren aller Möglichkeiten

$$n = p * q$$

ist nicht sehr erfolgversprechend.

Hash-Funktionen

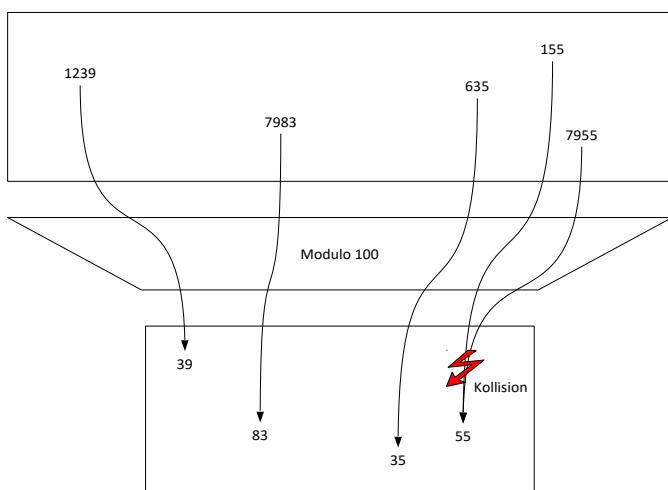


Hash-Funktionen werden im Datenbank-Umfeld bei schnellen Such- und Zugriffsverfahren eingesetzt. Mit einer Hash-Funktion werden weit verstreute Daten aus einem Urbildbereich, auch Universum genannt in eng beieinander liegende Daten in einen Bildbereich, der in der Regel wesentlich kleiner ist überführt. Es wird also aus einer Eingabe mit beliebiger Länge, eine Ausgabe fester, meist kürzerer Länge erzeugt. Realisiert wird dies mit einer Modulo-Rechnung bezogen auf eine Primzahl.

Abbildung 222 : Hash-Funktionen

Ein Hashwert kann auch als so genannter digitaler Fingerabdruck verwendet werden. Wenn z. B. ein Programmcode das Hash-Verfahren durchläuft wird ein Bitstring erzeugt. Dieser Bitstring wird an einer sicheren Stelle hinterlegt. Wenn ein Administrator sicher sein will, dass ein Programm nicht verändert wurde kann er seinen Programmcode mit dem Hash-Verfahren bearbeiten und dann den erzeugten Hashwert gegen den gesicherten Hashwert vergleichen.

Hash-Verfahren werden auch bei digitalen Signaturen verwendet. Dort wird die zu signierende Nachricht mit dem Hash-Verfahren auf einer festen Länge gekürzt bevor die Verschlüsselung erfolgt.

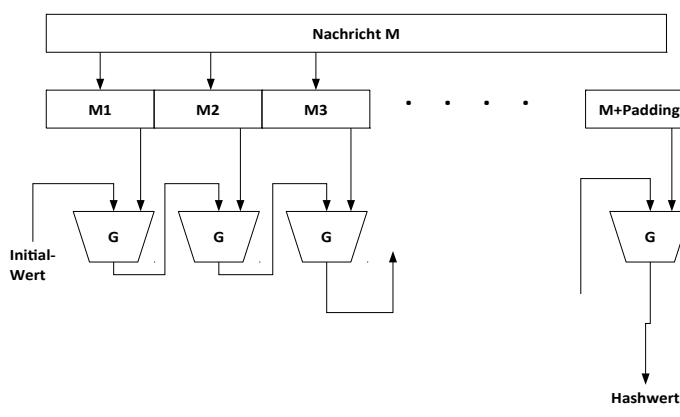


Eine Hash-Funktion ist erst dann brauchbar wenn sie weitestgehend frei von Kollisionen ist. Dies bedeutet, dass es praktisch unmöglich sein muss zwei Nachrichten x und x' aus dem Universum zu finden, für die $x \neq x'$ aber $h(x) = h(x')$.

Eine Kollision bedeutet, dass für zwei unterschiedliche Nachrichten aus dem Urbildbereich die gleichen Werte im Bildbereich über die Hash-Funktion ermittelt werden.

Abbildung 223 : Kollision bei Hash-Funktion

Hashwerte mit einer Länge von 64 Bit werden als „Schwache Hashwerte“ angesehen. „Starke Hashwerte“, welche als kollisionsresistent angesehen werden, haben eine Länge von 128 bis 192 Bit.



Eine beliebig lange Nachricht wird in einzelne Blöcke zerlegt.
 Die Blöcke werden der Kompressions-Funktion zur Verarbeitung übergeben.
 Zusätzlich zu den Nachrichten-Blöcken wird der Kompressions-Funktion G ein Initialisierungswert verarbeitet.
 Das Ergebnis der ersten Kompression wird als Initialisierungswert für den zweiten Kompressions-Durchlauf verwendet usw.
 Das Ergebnis des letzten Kompressions-Durchlaufs ist der Hashwert.

Abbildung 224 : Erzeugung eines Hashwertes

MD5

Die MD-Verfahren (Message Digest) wurden 1990 von R. Rivest mit dem MD4 vorgestellt und mit MD5 weiter entwickelt.

MD5 erzeugt einen 128-Bit Hashwert. Es werden, wie bei SHA-1 512-Bit große Eingabeblocks verarbeitet die in 32-Bit Worte zerlegt werden.

Jeder 512-Bit Block wird in 4 Runden vollständig bearbeitet. In jeder Runde werden 16 Verarbeitungsschritte durchgeführt bei denen jeweils 32-Bit Worte des Eingabeblocks verarbeitet werden.

Da die 4 Initialisierungswerte bekannt sind kann eine Kollision durch eine erschöpfenden Suche (exhaustive search) gefunden werden. Deshalb sollte MD5 in seiner ursprünglichen Form nicht verwendet werden. Statt dessen sollten SHA-1 oder MD5 als HMAC verwendet werden.

SHA / SHA-1

Der Secure Hash Algorithm (SHA) wurde 1993 vom NIST entwickelt. Die überarbeitete Version SHA-1 wurde 1995 veröffentlicht. Mit dem SHA-1 Algorithmus wird ein Wert kleiner 2^{64} Bits in einen Hashwert von 160 Bits umgewandelt.

RIPEMD-160

Im Rahmen des EU Projekts RIPE (Race Integrity Primitives Evaluation) wurde RIPEMD als Variante von MD5 entwickelt. Die sicherere Version RIPEMD-160 wurde 1996 von Hans Dobbertin, Antoon Bosselaers und Bart Preneel entwickelt.

Dabei wird eine Nachricht beliebiger Länge in einen 160 Bit Hashwert umgesetzt.

Tiger

Die Tiger-Hash-Funktion wurden von Ross Anderson und Ali Biham entwickelt. Der Algorithmus ist für 64-Bit Prozessoren optimiert.

Es wird eine Eingabe beliebiger Länge in einen Hashwert mit der Länge von 192 Bits umgesetzt. Daher stammt der Name Tiger/192. Es gibt noch die Varianten Tiger/128 mit einer Hashwert-Länge von 128 Bits und Tiger/160 mit einer Hashwert-Länge von 160 Bits.

Vergleich der beschriebenen Hash-Funktionen

Da MD5 den kleinsten Hashwert mit 128 Bit liefert, wird MD5 als unsicher eingestuft. Besser ist hier SHA-1, RIPEMD-160 mit einer Hashwert-Länge von 150 Bit. Am besten wird Tiger mit den 192 Bit Hashwert eingestuft. Hinsichtlich der Anzahl zum Auffinden einer Kollision notwendigen Nachrichten gelten folgende Werte.

Hash-Funktion	Ungefährre Anzahl von notwendigen Nachrichten zum Auffinden einer Kollision
MD5	$2^{64} \sim 1,8 * 10^{19}$
SHA-1	$2^{80} \sim 1,2 * 10^{24}$
RIPEMD-160	$2^{80} \sim 1,2 * 10^{24}$
Tiger	$2^{96} \sim 8,0 * 10^{28}$

MAC

Hash-Funktionen werden zur Sicherstellung der Unverfälschtheit von Daten herangezogen. Da die Hash-Funktionen bekannt sind und von Jedermann auf ein Datum angewendet werden können ist nicht sichergestellt, dass der Absender auch der Richtige ist. Um dies zu erreichen kann der Message Authentication Code zur Sicherstellung des authentischen Ursprungs der Daten verwendet werden.

Es handelt sich hierbei um eine Hash-Funktion mit Einweg-Eigenschaften, die noch einen zusätzlichen Schlüssel verwendet. Der geheim auszutauschende Schlüssel wird MAC-Geheimnis genannt.

Die Verwendung von DES zur Erstellung eines MAC ist weit verbreitet. Im einfachsten Fall werden die zu authentifizierenden Daten mit einem DES-Schlüssel unter Verwendung des CBC-Modus verschlüsselt. Der MAC der Nachricht ist der letzte Krypto-Block, also ein 64-Bit Wert.

Bei SSL oder IPsec wird das MAC-Verfahren mittels MD5 als dedizierte Hash-Funktion verwendet und mit einem Schlüssel ergänzt. Dieses Verfahren wird auch „Keyed MD5“ genannt.

HMAC

Bei HMAC wird ein Schlüssel für den Initialwert der Kompressionsfunktion verwendet. Die verwendete Hash-Funktion wird als Black Box angesehen und wird daher bei der Verwendung nicht modifiziert.

Public Key Infrastructure (PKI)

Um die öffentlichen Schlüssel von natürlichen oder juristischen Personen zu bescheinigen werden Zertifikate verwendet. Ein Zertifikat lässt weder Rückschlüsse auf den Inhalt der Dokumente noch auf die Vertrauenswürdigkeit der signierenden Person zu. Eine Person oder ein Objekt dem man vertraut (trusted) muss keineswegs vertrauenswürdig (engl. trustworthy) sein.

Für die Erzeugung sowie die Verwaltung von Zertifikaten werden spezielle Infrastrukturen eingesetzt. Bei den asymmetrischen Kryptosystemen hat sich der Begriff der Public Key Infrastructure (PKI) etabliert. Dazu wurden Standards entwickelt. Bei der IETF hat sich die PKIX Working Group mit dem Thema beschäftigt. Im Herbst 1995 wurde eine für X.509 entwickelte PKI vorgestellt und im RFC 2459 und RFC 2510 beschrieben.

Zertifikate

Heutzutage werden Zertifikate mit dem X.509-Standard als Bestandteil des X.500 Authentifikations-Frameworks verwendet. Mittlerweile sind die X.509-Zertifikate in der Version v3 verfügbar. Dabei wird folgende Struktur festgelegt:

Inhalt	Erläuterung
Versionsnummer	Beschreibung des Zertifikat-Formats
Seriенnummer	Eindeutiger Identifikator
Signatur	Verwendete Algorithmen und Parameter
Zertifikatsaussteller	Name der ausstellenden Instanz
Gültigkeitsdauer	Angabe eines Zeitintervalls
Benutzername	Eindeutiger Name des Benutzers
Schlüssel-Informationen	Schlüssel des Benutzers und Algorithmen
Eindeutiger Identifikator	In den Versionen v2 und v3
Erweiterungen	In den Versionen v2 und v3 (siehe auch RFC 2459)

Komponenten einer PKI

Zu einer PKI gehören folgende Komponenten:

- ➊ Zertifizierungsstelle (CA Certification Authority)

In dieser Stelle werden die Schlüssel-Paare erzeugt und verwaltet. Also herausgegeben und ggf. wieder zurückgerufen (revoziert).

- ➋ Registrierungsinstanz (RA Registration Authority)

Diese Instanz bürgt für die Verbindung zwischen dem öffentlichen Schlüssel und Identitäten sowie Attributen der Zertifikats-Inhaber.

- ➌ Policy

Die Regeln nach denen das Trust Center die Zertifikate ausstellt und verwaltet sind in der Zertifikatspolicy, einem CPS (Certification Practice Statement) festgelegt. Hier sind die rechtlichen und finanziellen Rahmenbedingungen sowie der Ablauf der Authentifikation von Zertifikatbesitzern sowie die Kriterien zum Schutz des Trust Centers festgeschrieben.

- ➍ CRL

In der Sperrliste (CRL Certificate Revocation List) werden die Zertifikate hinterlegt, die gesperrt wurden. Hier sind die Nummern, der vor dem Ablauf der Gültigkeit zurückgezogenen Zertifikate aufgelistet.

Als Alternative zur Sperrliste gibt es das OCSP (Online Certificate Status Protocol). Damit kann der Status eines Zertifikats online abgefragt werden.

- ➎ Verzeichnis

Ausgestellte Zertifikate und Sperrlisten werden in einem Verzeichnis zur Verfügung gestellt.

Virtuelle Private Netzwerke (VPN)

Ein VPN ist eine Kommunikationsumgebung bei der Verbindungen unter Kommunikationspartnern nur dann erlaubt sind, wenn diese zu einer bestimmten Gruppe gehören. Ist dies der Fall, wird ein sicherer Datentransport zwischen den Kommunikationspartnern über unsichere Netzwerke hinweg gewährleistet. Die Voraussetzungen für sicheren Datentransport ist die zweifelsfreie Identifikation des Kommunikationspartners, die Unveränderbarkeit der Daten während des Transports sowie eine von außen nicht lesbare Datenübertragung. Möglich sind VPNs auf verschiedenen Transport-Technologien.

- ATM und Frame Relay bieten hierbei noch die Möglichkeit die garantierte Laufzeit, max. Verzögerung und die max. Verlustrate festzulegen. Diese Techniken sind nicht weltweit verfügbar. Es gibt auch keine Möglichkeit der Einwahl für mobile Nutzer.
- Eine so genannte Standard Festverbindung (SFV) ist auch eine Art von VPN. Die Multiprotokoll-Fähigkeit sowie ein geringer Konfigurationsaufwand sprechen dafür. Allerdings ist sie teuer und bietet auch keine Einwahlmöglichkeit für mobile User.
- IP-VPN mit dem Internet als Transportmedium. Das Internet ist global verfügbar und erlaubt verschiedene Einwahl-Prozeduren bei hoher Verfügbarkeit und geringen Kosten. Allerdings besteht hier ein massives Sicherheitsproblem.

Unterschiedliche Tunnel-Protokolle

Ein Tunnel nennt man das einpacken (engl: encapsulation) eines Protokolls in ein anderes Protokoll, das zum Transport verwendet wird, dem Transport-Protokoll.

Layer-2-Tunnelprotokolle

Hierbei wird ein Layer-2-Protokoll wie PPP über ein Layer-3-Protokoll wie etwa IP transportiert.

Beispiele:

- Layer-2-Forwarding Protocol (L2P)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer-2-Tunneling Protocol (L2TP)

Es gibt unterschiedliche Möglichkeiten einen Tunnel zwischen einem Einwahl-Client und einem Firmen-Netzwerk aufzubauen.

Voluntary Tunneling

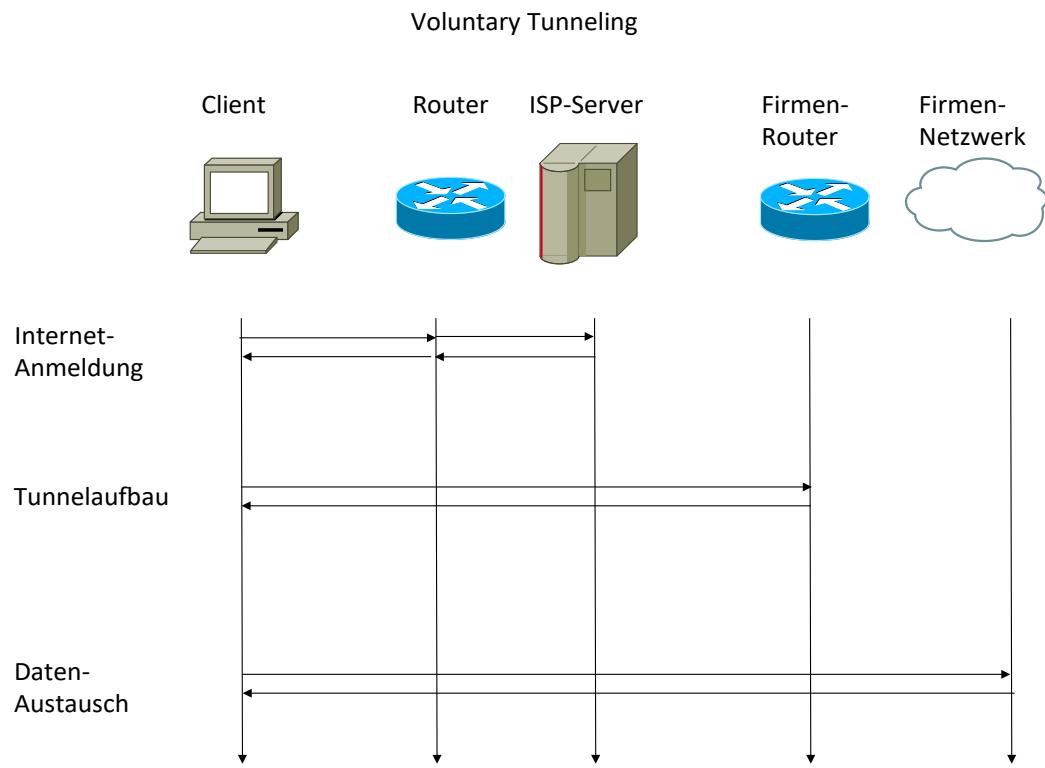


Abbildung 225 : Voluntary Tunneling

Hierbei baut der Client den Tunnel auf. Er wählt sich bei seinem ISP (Internet Service Provider) ein . Nachdem er sich authentifiziert hat bekommt er seine IP-Adresse, DNS-Server-Adresse usw. Danach ist der Client mit dem Internet verbunden. Er kann jetzt selbstständig mit dem Firmen-Gateway eine Verbindung aufbauen. Die Tunnelendpunkte sind Client und Firmen-Gateway. PPTP und L2TP unterstützen diesen Modus:

Vorteile:

- Es muss sich bei dem Firmen-Netzwerk nicht unbedingt um ein IP-Netzwerk handeln. IPX wäre auch möglich.
- Da der Provider nicht am Tunnel-Aufbau beteiligt ist besteht freie Providerwahl.
- Ein Transport über mehrere Provider-Netzwerke ist möglich da der Tunnel für die Provider transparent ist.
- Der Client kann alle Firmen sowie Internet-Dienste nutzen.

Nachteile:

- Der Client ist den Angriffen aus dem Internet ausgesetzt.
- Keine garantierte Bandbreite da der Provider keinen Einfluss auf den Tunnel hat.
- Software ist auf dem Client notwendig
- 2-maliges Anmelden ist notwendig (ISP, Firmen-Router).

Compulsory Tunneling

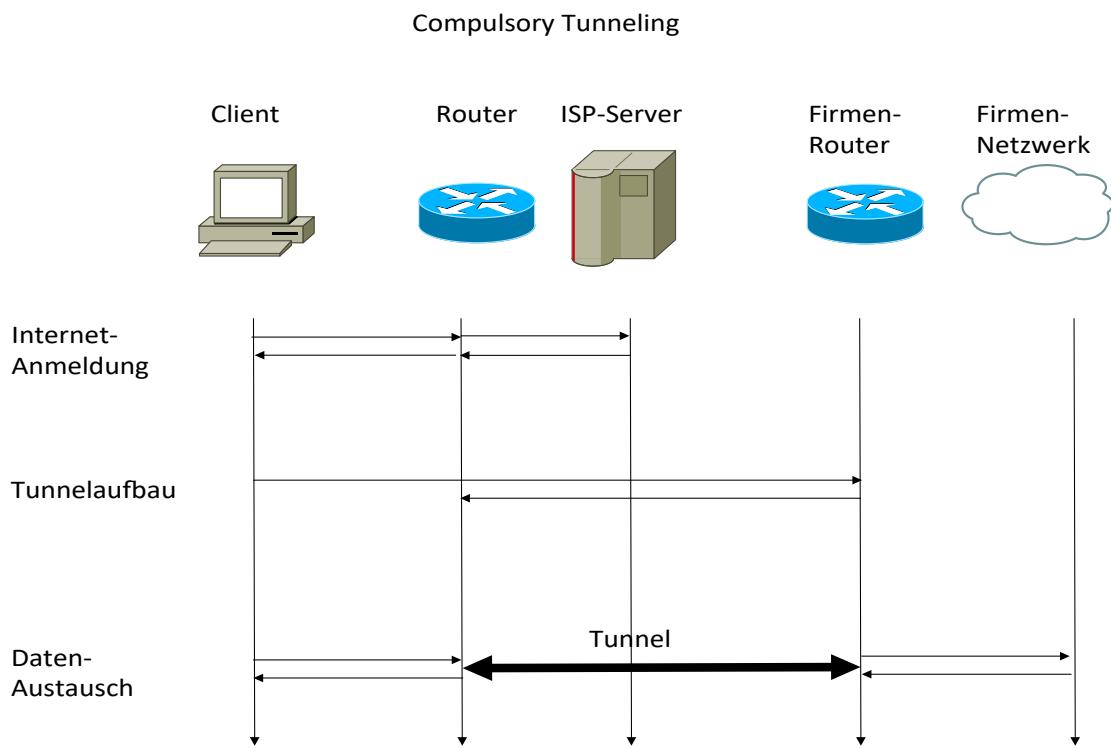


Abbildung 226 : Compulsory Tunneling

Der Tunnel-Aufbau ist nur beim vertraglich festgelegten ISP der Firma möglich. Die NAS (Network Access Server = Einwahl-Router beim ISP) bauen automatisch einen Tunnel zum Firmen-Gateway auf.

Dieses Tunneling wird von L2F, PPTP und L2TP unterstützt. L2F und L2TP haben keine Verschlüsselung. PPTP erlaubt Verschlüsselung. Für die Zugangskontrolle wird PAP (Passwort Authentication Protocol) oder CHAP (Challenge Handshake Protocol) verwendet. Die Verschlüsselung wird mit Rivest's Cipher4 (RC4) und Data Encryption Standard (DES) durchgeführt. PPTP ist nach neueren Erkenntnissen durch die schwache Verschlüsselung und Authentifizierung als nicht sicher anzusehen.

Nachteile:

- Es sind nur bestimmte Einwahlpunkte für den Client möglich.
- Normalerweise kein Internet-Zugriff möglich.

Vorteile:

- Es sind keine Angriffe aus dem Internet möglich.
- Eine Bandbreiten-Reservierung ist möglich.
- Der Client braucht keine spezielle Software zur Anmeldung.
- Der Client meldet sich nur einmal an.

Layer-3-Tunnelprotokolle

Dabei geht es darum Layer-3-Protokolle wie z. B. IPX über ein anderes Layer-3-Protokoll zu transportieren.

Beispiele:

IP-in-IP

Die Tunnel-Steuerung erfolgt Out of Band mittels ICMP-Meldungen. Die Tunnel sind vom Administrator auf den Routern manuell einzurichten. Eine Authentisierung oder eine Sicherung der Daten ist nicht realisiert. Eine automatische Tunnel-Konfiguration ist nicht möglich.

Generic Routing Encapsulation (GRE)

Dieses Protokoll wurde von Cisco entwickelt. Der Weg der Datenpakete, durch die anzusteuernden Router-IP-Adressen, kann vorgegeben werden. Die Authentisierung erfolgt über einen vorher verteilten Schlüssel. Die Daten sind nicht ausreichend geschützt. Eine unveränderbare Prüfsumme fehlt.

Internet Protocol Security (IPSec)

Ist in den RFC 2401 bis RFC 2409 beschrieben. Der Standard wurde ursprünglich für IPv6 entwickelt. IPSec ist kein eigenes Protokoll, sondern eine Zusammenfassung mehrerer Protokolle.

- AH (Authentication Header) dient zur Sicherstellung der Datenintegrität.
- ESP (Encapsulation Security Payload) dient zur Verschlüsselung der Daten.

IPSec kann in zwei verschiedenen Modi betrieben werden.

- Transportmodus. Die Daten werden verschlüsselt. Die Header werden nicht verschlüsselt.
- Tunnelmodus. Die Daten und der Header werden verschlüsselt.

Der Schlüsselaustausch erfolgt über 3 verschiedene Verfahren.

- Senden eines öffentlichen Schlüssels und dessen fernmündliche Kontrolle (am Telefon)
- Austausch von digitalen öffentlichen Schlüsseln einer CA (Certification Authority) (deutsch: Zertifizierungsstelle)
- Manuell verteilte Schlüssel (Preshared Keys)

IPSec Key Exchange (IKE)

IKE dient beim Austausch von Schlüsseln um folgende Bearbeitungen durchzuführen:

- ➊ Enkapsulierung
- ➋ Authentifizierung
- ➌ Verschlüsselung
- ➍ Kompression

Mit IKE wird eine Security Association (SA) (deutsch: Sicherheitsverbindung) zwischen 2 Knoten ausgehandelt. Dazu verwendet IKE UDP-Pakete (Port 500) was bedeutet, dass es eine geroutete Verbindung zwischen den beteiligten IKE-Knoten geben muss. Der System-Administrator hat eine Reihe von Festlegungen zu treffen die aus einer Palette von Auswahlmöglichkeiten entnehmen kann. Dabei hat er Abhängigkeiten zwischen Sicherheit, Bequemlichkeit Vertrauen und Effektivität zu beachten. Die Festlegungen, die der Administrator hier trifft sind Teil der Policy.

IKE geht bei der Schlüssel-Verwaltung in 2 Phasen vor . In der ersten Phase wird eine ISAKMP-SA aufgebaut. Das Internet Security Association Key Management Protocol (ISAKMP) ist im RFC2408 beschrieben. Damit werden die Schlüssel zwischen zwei IKE-Partnern gesichert ausgetauscht. Das Aushandeln einer ISAKMP-SA wird auch IPSec-Phase1 genannt. Hierbei können 2 unterschiedliche Modi verwendet werden.

➊ Main Mode

Es werden insgesamt 6 Nachrichten ausgetauscht. Verschlüsselte Übertragung von IDs und Zertifikaten. Beim Einsatz von Preshared Keys müssen alle Keys gleich sein. Dies bedeutet eine Schwächung der Authentisierung

➋ Aggressive Mode

Insgesamt 3 Nachrichten werden ausgetauscht. Es erfolgt keine Verschlüsselung der IDs und der Zertifikate. Die Übertragung erfolgt im Klartext! Wird verwendet wenn der Client sich über einen Provider ein wählt.

Dabei werden asymmetrische Schlüssel verwendet. Dies ist aufwändiger als mit symmetrischen Schlüsseln jedoch wesentlich sicherer. Sobald mit Abschluss der Phase 1 ein gesicherter Schlüsselaustausch möglich ist, kann mit der Phase 2 begonnen werden. Für die Verschlüsselung der Daten werden symmetrische Schlüssel verwendet. Diese sind performanter als asymmetrische Schlüssel. Da der Schlüsselaustausch für die Symmetrischen Schlüssel über eine bereits bestehende sichere Verbindung erfolgt ist diese Methode ebenfalls sicher.

RADIUS (Remote Authentication Dial In User Service)

Allgemeines

Hierbei handelt es sich um ein Protokoll mit dem die Themen Authentifizierung, Autorisierung und Abrechnung abgehandelt werden können. Seit in letzter Zeit das Thema WLAN mit dem Protokoll IEEE 802.1x einen Boom erfährt, ist auch der dazu notwendige RADIUS-Server in das Blickfeld der Administratoren gerückt.

- Bei der Authentifizierung handelt es sich darum festzustellen, ob der User der sich einloggen will auch derjenige ist für den er sich ausgibt.
- Bei der Autorisierung geht es um die Zuteilung von Ressourcen wie den Zugriff auf Dienste und Leistungen etwa eine Festplatte und die dazugehörigen Schreib- oder Leserechte.
- Bei der Abrechnung wird ein ISP ebenfalls durch einen RADIUS-Server unterstützt.

Bei RADIUS handelt es sich um ein Client-Server-Protokoll. Dabei wird UDP verwendet. Es wird bewusst auf TCP mit den Möglichkeiten einer Stateful-Bearbeitung verzichtet.

Im Juni 2000 wurde RADIUS in den RFCs 2865 und 2866 beschrieben. Der Datenaustausch wird über die Ports 1812 für die Authentifizierung und 1813 für das Accounting durchgeführt. In älteren Versionen werden die Ports 1645 und 1646 verwendet. Diese Konstellation kollidiert jedoch evtl. mit anderen Applikationen.

Bevor zwischen einem RADIUS-Client und einem RADIUS-Server Daten ausgetauscht werden können, müssen sie einen Preshared Key oder auch Shared Secret (vorher ausgetauschter symmetrischer Schlüssel) vereinbart haben. Damit werden die ausgetauschten Daten verschlüsselt und die Antworten des Servers authentifiziert.

Für den Datenaustausch wird ein sehr einfach gehaltenes Protokoll verwendet.

Der Code beschreibt den Paket-Typ

Code 1 Byte	ID 1 Byte	Länge 2 Byte	
Authenticator 16 Byte			
A-Nr 1 Byte	A-Len 1 Byte	A-Val 2 Byte	

Die ID wird für eine eindeutige Zuordnung der Anfrage zur Antwort verwendet

Die Länge gibt die gesamte Paketlänge einschließlich der Attribute an.

Das Authenticator-Feld wird vom Client auf einen zufälligen Wert gesetzt.

Die Attribut-Nummer, Attribut-Länge und Attribut-Werte sind in den RFCs 2865 bis 2869 beschrieben.

Abbildung 227 : RADIUS-Paket-Aufbau

Die möglichen Codes haben folgende Bedeutung:

Code	Paket-Typ
1	Access Request
2	Access Accept
3	Access Reject
4	Accounting Request
5	Accounting Response
11	Access Challenge
12	Status Server (experimental)
13	Status Client (experimental)
255	Reserved

Ablauf einer Authentifizierung

In der folgenden Abbildung ist ein typischer Ablauf aufgezeichnet. In diesem Beispiel ist der RADIUS-Server in einer DMZ durch eine Firewall geschützt. Der Einwahl-Router, auch NAS (Network Application Service) bekommt von einem Homeoffice-User eine Verbindungsanforderung. Der Benutzer meldet sich dabei mit User-Name und Passwort am NAS an. Daraufhin sendet der NAS als RADIUS-Client an den RADIUS-Server einen Access Request (Code = 1).

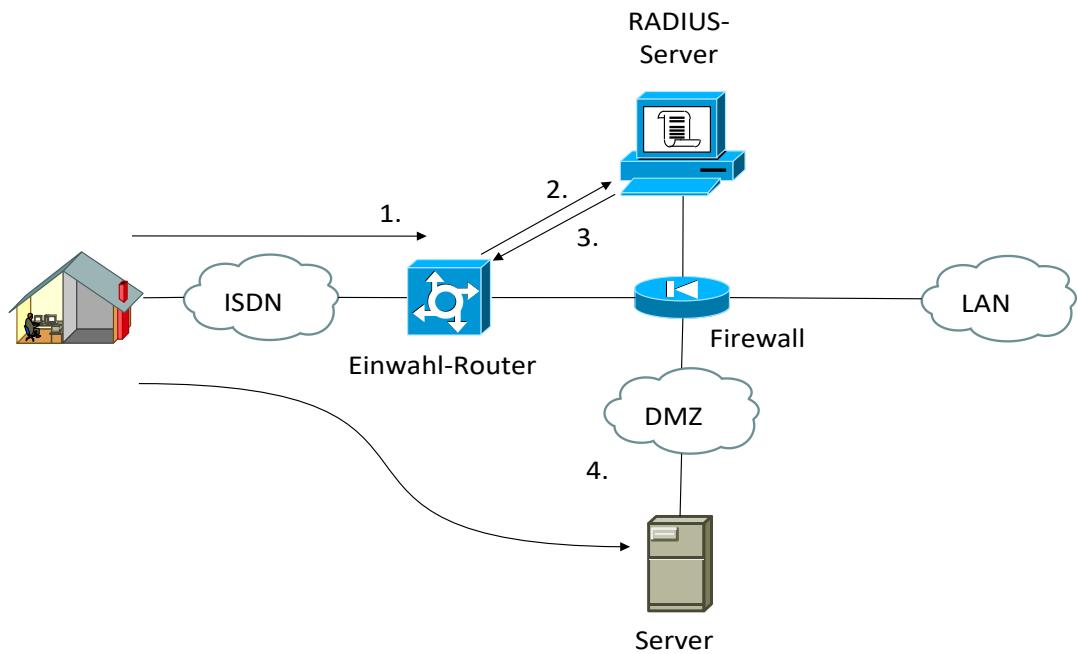


Abbildung 228 : Ablauf RADIUS-Einwahl

Der RADIUS-Server wird daraufhin mit einem Access Accept (Code = 2) oder einem Access Reject (Code = 3) antworten. Als ID wird die ID des Request-Paketes verwendet.

Um sicherzustellen, dass das Paket auch vom richtigen RADIUS-Server kommt, berechnet der Server den MD5-Hash-Wert aus dem kompletten Paket und dem Shared Secret. Damit kann der Client erkennen, ob das Paket von einem Server kommt. Nur wer den Shared Secret kennt, kann den MD5-Wert richtig berechnen. Damit sind jedoch nur Maßnahmen zum Schutz der Integrität und der Authentizität durchgeführt, denn die für die Vertraulichkeit erforderliche Verschlüsselung des gesamten Pakets wird mit Ausnahme des Passworts nicht durchgeführt.

Für die Attribute und ihre Bedeutung folgt hier eine kleine Auswahl:

1	User-Name (Benutzername für Anmeldung)
2	User-Password (Verschlüsseltes Passwort für PAP)
3	CHAP-Password (Antwort auf Challenge bei CHAP)
19	Callback-Number (hinterlegte Rufnummer für Rückruf)
26	Vendor Specific (herstellerspezifische Erweiterungen)
40	Account-Status-Type (Accounting Start / Stop / Update)
60	CHAP Challenge (hier oder im Feld Authenticator)
79	EAP-Message bei Nutzung des Extensible Authentication Protocol

Hierbei ist besonders das Attribut mit der Nummer 26 interessant. Mit diesem Attribut kann jeder NAS-Hersteller eigene Attribute spezifizieren und so das RADIUS-Protokoll für seine Zwecke erweitern. Eine 4 Byte große Hersteller-ID leitet das herstellerspezifische Attribut ein. Im ersten Byte ist ein Nullbyte. Die drei folgenden Bytes werden aus der weltweit eindeutigen Hersteller-ID, welche bei www.iana.org/assignments/enterprise-numbers nachzulesen sind, gebildet.

Authentifizierungsprotokolle bei RADIUS

PAP

Das Attribut 2 zieht die Authentifizierung mit dem Password Authentication Protocol nach sich. Der Client sendet dem Server das Passwort in verschlüsselter Form zu. Dazu wird ein MD5-Hash über das Passwort gebildet welches an den Server gesendet wird. Dort liegt das Passwort nur als MD5-Hash-Wert vor. Sollte der Server kompromittiert werden ist das Passwort selbst nicht ermittelbar. Obwohl das Passwort verschlüsselt übertragen wird gilt PAP als nicht sicheres Verfahren da ein Passwort übertragen wird. Dieses Passwort könnte mit entsprechendem Aufwand entschlüsselt werden.

CHAP

Das Challenge Response Authentication Protocol hat die 3 als Attribut-Nummer. Der NAS generiert eine zufällige Zeichenfolge (Challenge) und sendet sie dem Server. Der verarbeitet die Zeichenfolge zusammen mit dem Passwort zu einem Hash-Wert den er an den NAS zurück sendet. Hierbei wird das Passwort zwar nicht übertragen, jedoch liegt es als Klartext auf dem Server. Im Falle einer Kompromittierung des Servers sind die Passworte auf dem Server ungeschützt.

EAP

Das Extensible Authentication Protocol ist eigentlich eine erweiterbare Familie von Protokollen wie PEAP, LEAP, EAP-MD5, EAP-TLS, oder EAP-TTLS und nutzt fortgeschrittene Verfahren bis hin zu Zertifikaten

Externe Benutzerdaten

Die meisten RADIUS-Produkte können auf die Benutzerdaten von Betriebssystemen wie UNIX, Linux, Windows und Novell sowie die Benutzer-Verzeichnisse (Active Directory, Windows-Domain-Controller, LDAP-Directory, NIS/NIS+ oder SQL-Datenbanken) zugreifen.

Accounting

Der RADIUS-Client versorgt den RADIUS-Server mit den notwendigen Informationen um die Abrechnungsdaten auf dem Server zu verwalten. Dazu werden Accounting-Request-Pakete (Code = 4) an den Server der die Pakete mit Accounting-Response-Paketen (Code = 5) beantwortet. Mit dem Status-Account-Type 40 werden die Accounting-Informationen an den Server übergeben.

Attribut-Nr.	Bedeutung
1	Start
2	Stop
3	Interim Update
7	Accounting on
8	Accounting off

Am Ende einer Verbindung (Code = 2 oder bei einem Update (Code = 3) können weitere Attribute für die Anzahl der übertragenen Bytes (Attribut 42 und 43) übergeben werden.

Ausblick auf die weitere Entwicklung

Nur Cisco hat derzeit mit TACACS+ eine Alternative zu RADIUS. Im Zusammenhang von WLANs mit dem IEEE 802.1x-Protokoll erfährt RADIUS derzeit einen regelrechten Boom. Eine Weiterentwicklung findet nicht mehr unter dem Namen RADIUS-V2 statt, sondern unter dem Namen Diameter (deutsch: Durchmesser = 2 * Radius). Hierbei sollen Kompatibilitätsprobleme ausgemerzt werden sowie auf TCP aufgesetzt werden.

Quellen

- | | |
|--------------------------|--|
| FreeRadius | www.freeradius.org |
| OpenRadius | www.openradius.org |
| GNU Radius | www.gnu.org/software/radius/ |
| Cistron RADIUS Server | www.radius.cistron.nl |
| IAS | www.microsoft.com/windows2000/technologies/communications/ias |
| Funk Steel Belted Radius | www.funk.com |
| TACACS | www.cisco.com/warp/public/480/10.html |

Abbildungsverzeichnis

Abbildung 1: Wi-Fi-Logo.....	1
Abbildung 2: Abgrenzung zwischen WPAN, WLAN, WMAN und WWAN.....	5
Abbildung 3: Allgemeiner Funknetzaufbau.....	8
Abbildung 4: WLAN-Modi.....	9
Abbildung 5: Ad-hoc-Modus unter Windows10.....	10
Abbildung 6: Mesh-WLAN.....	12
Abbildung 7: BSS in der einfachsten Ausprägung.....	13
Abbildung 8: Independent Basic Service Set (IBSS).....	14
Abbildung 9: Infrastruktur BSS.....	15
Abbildung 10: Extended Service Set.....	16
Abbildung 11: Unterschied zwischen Handover und Roaming.....	17
Abbildung 12: Mobile IP.....	18
Abbildung 13: WLAN Allgemeiner Aufbau.....	19
Abbildung 14: Der 2.4 GHz-Bereich.....	21
Abbildung 15: Spektralmaske für einen Sender mit 20MHz Bandbreite im 2,4GHz-Band.....	22
Abbildung 16: Regionale Unterschiede bei den Frequenzbändern und die Konsequenzen.....	22
Abbildung 17: Spektralmaske für einen Sender mit 20MHz Bandbreite im 5GHz-Band.....	24
Abbildung 18: Überlappungsfreie Kanäle im 5GHz-Band.....	24
Abbildung 19: WLAN – Reichweiten-Vergleich.....	26
Abbildung 20: FDD / TDD.....	27
Abbildung 21: Multiplexverfahren.....	28
Abbildung 22: SDMA.....	29
Abbildung 23: Wiederverwendungsabstand.....	30
Abbildung 24: FDMA.....	31
Abbildung 25: FDMA-Kanalauswahl.....	31
Abbildung 26: TDMA.....	32
Abbildung 27: TDMA-Kanalauswahl.....	32
Abbildung 28: CDMA.....	33
Abbildung 29: Modulationsart BPSK.....	35
Abbildung 30: BPSK-Modulator.....	35
Abbildung 31: Modulationsart QPSK.....	36
Abbildung 32: QPSK-Modulator.....	36
Abbildung 33: CCK-Sendestufe.....	37
Abbildung 34: QAM Quadrature-Amplitude-Modulation.....	38
Abbildung 35: 16-QAM Gray-codiert.....	39
Abbildung 36: 64-QAM.....	40
Abbildung 37: 1024-QAM mit 10 Bit pro Codierung.....	41
Abbildung 38: WLAN im ISO-7-Schichten-Modell.....	42
Abbildung 39: Grundsätzlicher Frame-Aufbau auf Ebene 1.....	43
Abbildung 40: Layer-Management.....	44
Abbildung 41: PLCP-Statusmaschine.....	46

Abbildung 42: Dienste (Service) - Sicht des Schichtenmodells für WLANs.....	47
Abbildung 43: Protokoll (Protocol) - Sicht des Schichtenmodells für WLANs.....	48
Abbildung 44: Signalspreizung.....	50
Abbildung 45: TDMA in Kombination mit FDMA.....	51
Abbildung 46: Frequency-Hopping.....	51
Abbildung 47: FHSS-PLCP-Frameformat.....	54
Abbildung 48: FHSS Scrambled PSDU.....	55
Abbildung 49: Direct Sequence CDMA.....	56
Abbildung 50: Die 2-PLCP-Frameformate bei DSSS.....	57
Abbildung 51: OFDM-Signalüberlagerung.....	58
Abbildung 52: Detail: Nulldurchgänge der Nachbar-Unterträger bei Maximum.....	58
Abbildung 53: OFDM-Bandbreitenersparnis.....	59
Abbildung 54: OFDM Datenübertragung.....	59
Abbildung 55: Blockschaltbild eines OFDM-Senders.....	61
Abbildung 56: Blockschaltbild eines OFDM-Empfängers.....	62
Abbildung 57: Scrambler.....	63
Abbildung 58: Descrambler.....	63
Abbildung 59: Faltungscodierer.....	64
Abbildung 60: Beispiel einer Punktierung mit der Coderate $R = 3 / 4$	65
Abbildung 61: Interleaving.....	67
Abbildung 62: Interleaving bei einer Datenrate von 9Mbps.....	68
Abbildung 63: Wiederauffüllung der punktierten Bits auf der Empfängerseite.....	69
Abbildung 64: Beispiel: Viterbi-Algorithmus.....	70
Abbildung 65: Mehrwegeausbreitung.....	71
Abbildung 66: Korrelation mit der Trainingssequenz.....	73
Abbildung 67: Korrelation mit nochmals erweiterter Trainingssequenz.....	74
Abbildung 68: Window Funktion in einfacher und doppelter Form.....	78
Abbildung 69: OFDM-Trainingsstruktur in der PLCP-Präambel.....	79
Abbildung 70: Signal-Feld.....	80
Abbildung 71: Transmit-PHY.....	83
Abbildung 72: Endlicher Kontrollautomat Senden.....	84
Abbildung 73: Receive-PHY.....	85
Abbildung 74: Endlicher Kontrollautomat Empfangen.....	86
Abbildung 75: Vergleich von FHSS, DSSS und OFDM.....	88
Abbildung 76: IEEE-802.11-MPDU-Header-Format.....	89
Abbildung 77: MPDU-Control-Feld.....	90
Abbildung 78: Verwendung der 4 MAC-Adressen.....	93
Abbildung 79: CSMA/CA.....	96
Abbildung 80: IFS.....	97
Abbildung 81: Unicast-Quittungen.....	99
Abbildung 82: ACK-Frame-Format.....	100
Abbildung 83: Ablaufbeispiel.....	101
Abbildung 84: WLAN-Kollision und deren Auflösung.....	103
Abbildung 85: Exponentieller Backoff.....	104
Abbildung 86: Hidden Station Problem.....	105

Abbildung 87: RTS/CTS.....	106
Abbildung 88: RTS-Frame-Format.....	107
Abbildung 89: CTS-Frame-Format.....	107
Abbildung 90: Exposed-Terminal-Problem.....	108
Abbildung 91: PCF.....	109
Abbildung 92: CFP-End-Frame-Format.....	111
Abbildung 93: CFP-End + ACK - Frame-Format.....	111
Abbildung 94: Fragmentierung.....	113
Abbildung 95: TSF im Infrastruktur-Modus.....	114
Abbildung 96: TSF im Ad-hoc-Modus.....	114
Abbildung 97: TIM / DTIM im Infrastruktur-Modus.....	115
Abbildung 98: Power-Save-Poll-Frame-Format.....	115
Abbildung 99: ATIM.....	116
Abbildung 100: WLAN: Historische Entwicklung.....	122
Abbildung 101: 2,4 GHz-Bänder.....	123
Abbildung 102: WLAN-Präambel und SFD.....	124
Abbildung 103: PLCP-Formate.....	125
Abbildung 104: IEEE-802.11g - Protection-Mechanismus.....	129
Abbildung 105: CTS to Self.....	129
Abbildung 106: DSSS-OFDM-Frameformat nach 802.11g.....	130
Abbildung 107: MIMO im Vergleich zu SISO, SIMO und MISO.....	132
Abbildung 108: Multipath.....	133
Abbildung 109: Beamforming.....	134
Abbildung 110: Kanalanzahl bei mehreren Antennen.....	135
Abbildung 111: Punktierung für die Coderate $R = 5/6$	136
Abbildung 112: IEEE-802.11n-PPDU-Formate.....	141
Abbildung 113: HT-SIGNAL-Felder.....	142
Abbildung 114: A-MPDU-Frame und Subframes.....	144
Abbildung 115: A-MSDU und Subframes.....	145
Abbildung 116: BlockACK.....	146
Abbildung 117: Aufbau der ACK und BlockACK - Frames.....	147
Abbildung 118: Phased Coexistence Betrieb.....	153
Abbildung 119: MIMO-Blockschaltbild.....	154
Abbildung 120: WLAN-Bandbreiten.....	156
Abbildung 121: Sounding-Feedback-Sequenz mit mehreren Stationen.....	157
Abbildung 122: Zusammenhang Kanallistenelement und Frequenzband.....	158
Abbildung 123: VHT-PPDU-Format.....	160
Abbildung 124: Subcarrier-Spacing.....	166
Abbildung 125: Unterschied OFDM / OFDMA.....	166
Abbildung 126: Reduzierung der Präambeln.....	167
Abbildung 127: MU-Downlink.....	167
Abbildung 128: Verwaltung von MU-MIMO-Uplinks.....	168
Abbildung 129: OFDMA in gemischter Umgebung.....	168
Abbildung 130: RUs bei unterschiedlichen Bändern.....	171
Abbildung 131: AP mit MU-MIMO sendet gerichtet an Stationen.....	172

Abbildung 132: Zusammenhang: Zeit - Spacial Stream - Frequenz.....	172
Abbildung 133: BSS-Coloring.....	173
Abbildung 134: IEEE-802.11-PPDU-Formate.....	176
Abbildung 135: 802.1ax PHY Frame Format.....	177
Abbildung 136: Duplizierung der Legacy und HE-Präambel.....	177
Abbildung 137: Wiederholung der HE-SIG-A Informationen.....	177
Abbildung 138: Gleichzeitige Datenübertragung in Uplink- oder Downlink-Richtung.....	181
Abbildung 139: DL-OFDMA-Padding.....	181
Abbildung 140: Vergleich IEEE-802.11ac und IEEE-802.11ax.....	183
Abbildung 141: Wi-Fi-7: Router mit drei WLAN-Kanälen und Notebook mit 2 WLAN-Kanälen.....	185
Abbildung 142: Wi-Fi-7: Gleichzeitiger Datenaustausch auf drei Kanälen.....	186
Abbildung 143: Wi-Fi-7: Durchsatzsteigerung.....	187
Abbildung 144: Wi-Fi-7: Reduzierung der Latenzzeit.....	187
Abbildung 145: Wi-Fi-7: Robustheit.....	188
Abbildung 146: Enhanced Multi-Link Single Radio.....	188
Abbildung 147: Multi-Link Single Radio.....	189
Abbildung 148: IEEE-802.11 - Übersicht.....	191
Abbildung 149: EDCA Parameter Set Element.....	193
Abbildung 150: Umsetzung der Access Categories mit Warteschlangen.....	194
Abbildung 151: Medium-Zugriff der Access Classes.....	195
Abbildung 152: Beacon-Intervall teilweise belegt.....	199
Abbildung 153: Probe-Request und -Response.....	203
Abbildung 154: Beziehung von Status und Services zwischen Non-Mesh-Stationen.....	204
Abbildung 155: Open-System-Authentifikation.....	208
Abbildung 156: WLAN Shared-Key-Modus.....	209
Abbildung 157: Reassoziiierung.....	212
Abbildung 158: Assoziiierung Reassoziiierung Disassoziiierung.....	212
Abbildung 159: WLAN IEEE-802.1x.....	213
Abbildung 160: IEEE-802.1x (EAPoL).....	214
Abbildung 161: WLAN EAP-Stack.....	214
Abbildung 162: RADIUS-Frameformat.....	215
Abbildung 163: WLAN Authentisierung nach IEEE 802.1x.....	216
Abbildung 164: Vom Schwingkreis zur Antenne.....	217
Abbildung 165: Halbwellendipol.....	217
Abbildung 166: Röntgenbild WLAN-Antenne Quelle: heise.de.....	217
Abbildung 167: Freiraumdämpfung.....	219
Abbildung 168: Halbwellendipole und ihre Ausrichtung.....	221
Abbildung 169: Ausführungen von Stabantennen.....	222
Abbildung 170: Strahlungsdiagramme einer Dipolantenne ohne Gewinn.....	222
Abbildung 171: Dipolgruppe mit 4 Dipolen und Dipollinie mit 4 Dipolen.....	222
Abbildung 172: Patch-Antenne.....	223
Abbildung 173: Yagi-Antenne.....	223
Abbildung 174: Dipolgruppe mit 2 Dipolen im Abstand von $\lambda/4$	223
Abbildung 175: Richtungsdiagramme mit Öffnungswinkeln.....	224
Abbildung 176: Fresnel-Zone.....	225

Abbildungsverzeichnis

Abbildung 177: Berechnung von D an beliebiger Stelle.....	225
Abbildung 178: Fresnel-Zone mit Berücksichtigung der Erdkrümmung.....	226
Abbildung 179: Reichweiten unterschiedlicher Bänder.....	228
Abbildung 180: WLAN-Leistungsbudget zur Ermittlung der Reichweite.....	229
Abbildung 181: Grundsätzliche WLAN Verschlüsselung.....	231
Abbildung 182: WLAN WEP-Verschlüsselung mit CRC.....	232
Abbildung 183: WLAN Gesamte WEP-Verschlüsselung.....	233
Abbildung 184: WEP-Paketformat.....	234
Abbildung 185: Zusammenhänge der Sicherheitsaktivitäten.....	235
Abbildung 186: 4-Wege-Handshake zum Austausch der Nonce-Werte.....	240
Abbildung 187: TKIP - Pairwise Key Hierarchie.....	241
Abbildung 188: CCMP - Pairwise Key Hierarchie.....	241
Abbildung 189: Group Key Schlüsselhierarchie.....	242
Abbildung 190: TKIP-Verschlüsselung.....	243
Abbildung 191: TKIP-MPDU-Format.....	244
Abbildung 192: TKIP Entschlüsselung.....	245
Abbildung 193: CCMP-CTR-Mode.....	247
Abbildung 194: CCMP - Verschlüsselung.....	248
Abbildung 195: Verwendung des MPDU-Headers für den Aufbau der AAD.....	249
Abbildung 196: CCMP-MIC-Berechnung.....	249
Abbildung 197: CCMP-MAC-Frame.....	250
Abbildung 198: CCMP - Entschlüsselung.....	250
Abbildung 199: Vergleich WPA2 mit WPA.....	251
Abbildung 200: WLAN Daten-Umleitung.....	252
Abbildung 201: WLAN Known-Plain-Text Angriff.....	253
Abbildung 202: WLAN Man-in-the-Middle.....	255
Abbildung 203: WLAN Session Hijacking.....	256
Abbildung 204: LAN um WLAN erweitert.....	258
Abbildung 205: Überdeckung einer großen Fläche.....	259
Abbildung 206: WLAN mit vielen Clients.....	260
Abbildung 207: WLAN verbindet LANs.....	261
Abbildung 208: WLANs Flächenabdeckung mit gerichteten Antennen.....	262
Abbildung 209 : Sicherheit über der Zeit.....	278
Abbildung 210 : Sicherheit in Abhängigkeit von der Umgebung.....	278
Abbildung 211 : Sicherheit und finanzieller Aufwand.....	278
Abbildung 212 : Sicherheit in Abhängigkeit von Mechanismen.....	278
Abbildung 213 : Geheimhaltung.....	293
Abbildung 214 : Verschlüsselung.....	293
Abbildung 215 : Stromchiffrierer.....	296
Abbildung 216 : Stromchiffrierer Funktionen.....	296
Abbildung 217 : Blockchiffrierer im ECB-Modus.....	298
Abbildung 218 : Blockchiffrierer im CBC-Modus.....	299
Abbildung 219 : OFB-Modus.....	300
Abbildung 220 : Verschlüsselung mit dem Public Key Verfahren.....	301
Abbildung 221 : Digitale Signatur.....	302

Abbildungsverzeichnis

Abbildung 222 : Hash-Funktionen.....	311
Abbildung 223 : Kollision bei Hash-Funktion.....	311
Abbildung 224 : Erzeugung eines Hashwertes.....	312
Abbildung 225 : Voluntary Tunneling.....	317
Abbildung 226 : Compulsory Tunneling.....	318
Abbildung 227 : RADIUS-Paket-Aufbau.....	321
Abbildung 228 : Ablauf RADIUS-Einwahl.....	322

Literaturverzeichnis

IEEE802.11-2016

IEEE Computer Society Wireless LAN Medium Access Control(MAC) and Physical Layer (PHY) Specifications , 2016

GAST-ASG-2012

Gast, Mattew S., 802.11n A Survival Guide, 2012, ISBN:978-1-449-31204-6

IEEE-802.11e-2005

Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, 2005

BOSBOS-Math

Bossert, Martin / Bossert, Sebastian, Mathematik der digitalen Medien, 2017, ISBN:978-3-8007-4456-5

Wikipedia-Interleaving: , Wikipedia-Interleaving, 2019

NI-2002-08

Netzwerk-Insider 2002-08: OFDM - Der Signalligator, 2002

Rech-WLAN-2012

Rech, Jörg, Wireless LANs, 2012, ISBN:978-3-936931-75-4

KAUF-WLANS-2002

Kauffels, Franz-Joachim, Wireless LANs, 2002, ISBN:3-8266-0955-7

IEEE-802.11-2016

IEEE Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2018

Stichwortverzeichnis

2,4 GHz-Band.....	21	Asymmetrische Schlüsselverfahren.....	301
4096-QAM.....	184	Asymmetrische Verschlüsselungsstandards.....	309
4kQAM.....	184	ATM.....	316
5 GHz-Band.....	23	attack.....	284
Abrechenbarkeit.....	282	Aufbau.....	8
Abrechnung.....	282, 321	Ausfallsicherheit.....	260
Abrechnungsdaten.....	326	authentication.....	280
AC.....	193	Authentication.....	209
AC-Index.....	193	Authentication Header.....	319
Access Categories.....	193	Authenticaton-Server.....	213
Access Point.....	1, 11, 15, 19, 163, 195, 199, 263	Authenticator.....	213
account.....	280	Authentifikation.....	280
accountability.....	282	Authentifizierung.....	19, 202, 204, 287, 321
Accounting-Information.....	326	Authentizität.....	280, 324
Accounting-Request-Paket.....	326	Autorisierung.....	277, 321
Accounting-Response-Paket.....	326	availability.....	282
ACI.....	193	BA.....	149
ACK.....	94	Backbone-System.....	16
ACK-Frame.....	256	Backoff-Time.....	96
Active Scanning.....	203	backup.....	280
Ad-hoc-Modus.....	9, 14	BAKOM.....	20
Advanced Encryption Standard.....	236, 247	Bandbreite.....	260
AES.....	235f., 247, 307	BAR.....	147
AH.....	319	Barker-Code.....	56
AIFS.....	194	Basel II.....	292
AktG.....	291	Basic BlockAckReq.....	147
Aktiengesetz.....	291	Basic Service Set.....	13
Allgemeines.....	278	Basisstation.....	8
Angreifer.....	255	BC.....	117
Angriff.....	284	BDSG.....	290
Angriffs-Szenarien.....	252	Beacon-Frame.....	199, 202
ANonce.....	239	Beacon-Intervall.....	199
Anonymisierung.....	282	Beacons.....	94
Anonymität.....	282	Bedrohungen.....	284
Antennenbeispiele.....	262	Benutzerdatenverwaltung.....	215
Antennengewinn.....	222	Betriebsverfassungsgesetz.....	290
AP.....	1, 11, 15, 19, 163, 195, 199, 263	BetrVG.....	290
Arbitration Inter Frame Space.....	194	BFWA.....	23
asset.....	276, 284	BGB.....	291
Assoziation.....	202, 211	Bildbereich.....	311

billing.....	282	Cipher-Block-Chaining.....	299
Binary Phase Shift Keying.....	56	Cipher-Feedback Modus.....	299
Bitfehler-Korrektur.....	127	Clear to Send.....	106
BlockAck.....	149	Closed System.....	203
BlockAckReq.....	147	Code Division Multiple Access.....	28
Blockchiffre.....	306	Codesequenz.....	50
Blockchiffrierer.....	298	Coherence Time.....	144
Blowfish.....	307	Collision Avoidance.....	96
Bluetooth.....	21, 51	Complementary Code Keying.....	37, 127
BNetzA.....	20	Compulsory Tunneling.....	318
BO.....	96	Computer Emergency Response Team.....	287
BPSK.....	56	confidentiality.....	282
Bridge-Modus.....	11	Confinement-Problem.....	282
Broadband Fixed Wireless Access.....	23	Contention Window.....	96
Brute Force Angriff.....	310	Controller.....	8
BSS.....	13f, 199	covert channel.....	277
BSS-Transition.....	16f.	Cracker.....	289
Bundes Datenschutzgesetz.....	290	CRC.....	232
Bundesnetzagentur.....	20	CSMA/CA.....	7, 42, 96
Bürgerliches Gesetzbuch.....	291	CTR/CBC-MAC Protocol.....	236
CA.....	96, 319	CTS.....	94, 106
Carrier Sense Multiple Access / Collision Avoidance ..	42,	CW.....	96
96		Cyclic Redundancy Check.....	232
CBC.....	306	DARPA.....	287
CBC-Modus.....	298f.	Data Encryption Standard.....	318
CCK.....	37, 127	Daten-Umleitung.....	252
CCM.....	247	Datenaustausch.....	293
CCM Protocol.....	247	Datenintegrität.....	232, 282
CCMP.....	236, 247	Datenschutz.....	280
CDMA.....	28	Datensicherheit.....	280
CEPT.....	23	Datenverfälschung.....	232
CERT.....	287	DCF.....	42, 96, 109
Certification Authority.....	319	DCF Inter Frame Spacing.....	98
CFB.....	306	Deauthentication.....	256
CFB-Modus.....	299	DECT.....	7
Challenge Handshake Protocol.....	318	Defense Advanced Research Projects Agency.....	287
Challenge Response Authentication Protocol.....	324	Denial of Service.....	285
Challenge-Texte.....	209	Denial-of-Service.....	254, 256
CHAP.....	318, 324	dependability.....	277
Checksumme.....	232	DES.....	313, 318
Chiffrat.....	231, 253, 293	DES (Data Encryption Standard).....	306
Chiffretext.....	293	Destination-MAC-Adresse.....	243
Chiffrierer.....	296	DFS.....	7, 23, 119, 126
Chips.....	56	DHCP.....	18, 214
Chipsequenz.....	56	Differentielle Kryptoanalyse.....	295

Diffie-Hellmann.....	309	Electronic Code-Book.....	298
DIFS.....	98	Encapsulation Security Payload.....	319
digitale Signatur.....	302	Enhanced Distributed Channel Access.....	193
digitalen Signaturen.....	311	ESP.....	319
digitaler Fingerabdruck.....	311	Ethereal.....	285
Dipol-Antenne.....	262	ETSI.....	7
Dipolgruppen.....	222	EWC-Konsortium.....	131
Dipolreihe.....	222	Exploit.....	289
Direct Sequence CDMA.....	56	Extended Inter Frame Spacing.....	98
Direct Sequence Spread Spectrum.....	56	Extended Service-Set.....	16
Directional Multi-Gigabit.....	13	Extensible Authentication Protocol.....	213, 325
Disassociation-Nachricht.....	256	Faltungscode.....	61
Distributed Coordination Funktion.....	96	Faltungscodierer.....	64, 80
Distribution System.....	211	Einflusslänge.....	64
Diversity-Antennen.....	227	ESA-NASA-Satellite-Standard-Code.....	64
DMG.....	13	Symbolspeichertiefe.....	64
DNS.....	214	Viterbi-Decoder.....	64
DNS-Name-Spoofing.....	285	Fast-BSS-Transition.....	197
DoS.....	285	FCS.....	94
Downlink.....	27	FDD.....	27
DS.....	211	FDMA.....	28, 51, 59
DSSS.....	56	FEC.....	61, 64, 127, 138
Dynamic Frequency Select.....	23	FHSS.....	
Dynamic Frequency Selection.....	126	Header Error Control.....	54
E-Ebene.....	221	HEC.....	54
EAP.....	213, 325	PLCP Signaling Field.....	54
EAP over LAN.....	213	PLW.....	54
EAP-MD5.....	325	Präambel.....	54
EAP-TLS.....	325	PSDU.....	55
EAP-TTLS.....	325	PSDU Length Word.....	54
EAPoL.....	213, 215	PSF.....	54
eavesdropping.....	284	SFD.....	54
ECB.....	306	Start-Frame-Delimiter.....	54
ECB-Modus.....	298	Firewall.....	19
ECC.....	23	Forward Error Correction.....	61, 64, 127
EDCA.....	193	Fragmentierung.....	89
EDCA-Function.....	193	Frame Relay.....	316
EDCAF.....	193	Free Space Path Loss.....	219
EIFS.....	98	Frequency Division Duplex.....	27
Einschleusen von Nachrichten.....	254	Frequency Division Multiple Access.....	28, 59
Eintrittswahrscheinlichkeit.....	284	Frequency-Hopping.....	51
EIRP.....	25, 182	Frequency-Hopping CDMA.....	50
EIV.....	244	Frequenz-Bänder.....	20
EIVID.....	244	Frequenzband.....	30
Electronic Business.....	282	FSPL.....	219

Stichwortverzeichnis

FT.....	197	IBSS.....	199
Funkkanäle.....	257	ICI.....	47
Funknetz.....	8	ICV.....	232, 244
Funktionssicherheit.....	280	IDEA.....	306
Funkzelle.....	8, 16, 94, 257	Identifikation.....	316
GCR.....	148	IDS.....	264, 287
Generic Routing Encapsulation.....	319	IEEE 802.1x.....	321
Gerichtsurteile.....	291	IEEE-802.11.....	123
Gesetz zur Kontrolle und Transparenz im Unternehmen	291	IEEE-802.11a.....	26, 126
Gewichtung.....	284	IEEE-802.11ac.....	155
GmbH-Gesetz.....	291	IEEE-802.11af.....	162
GmbHG.....	291	IEEE-802.11ah.....	163
GMK.....	242	IEEE-802.11ax.....	164
GPRS.....	4	IEEE-802.11b.....	1, 26, 126
GRE.....	319	IEEE-802.11e.....	193
Group Master Key.....	242	IEEE-802.11f.....	195
GSM.....	51	IEEE-802.11g.....	128
Guard Intervall.....	138	IEEE-802.11h.....	7
H-Ebene.....	221	IEEE-802.11i.....	196, 236
Hacker.....	289	IEEE-802.11n.....	131
Hacker-Ethik.....	289	IEEE-802.11s.....	11
Haftung.....	291	IEEE-802.1x.....	19, 196, 213, 235, 239
Halbwelldipole.....	221	IEEE802.11be.....	184
Halbwertsbreite.....	224	IFFT.....	61
Half Power Beam Width.....	224	IFS.....	96
HaLow.....	163	IGTKSA.....	251
Handover.....	16f., 123	IKE.....	320
Hash-Funktion.....	311	Aggressive Mode.....	320
Hash-Funktionen.....	311	Main Mode.....	320
HE.....	164	Phase 1.....	320
Hersteller-ID.....	324	Phase 2.....	320
Hidden-Station-Problem.....	105	Informationelle Selbstbestimmung.....	283
High Efficiency.....	164	Informationskanäle.....	277
High Throughput.....	131	Informationssicherheit.....	280
Hiperlan2.....	7	Informationsveränderung.....	280
HMAC.....	313	Informationsvertraulichkeit.....	284
HomeRF.....	7	Infrarot.....	7
Hotspot.....	1, 124	Infrastruktur BSS.....	15
HPBW.....	224	Infrastruktur-Modus.....	11
HT.....	131	Initialisierungs-Vektor.....	209
HT-Greenfield-Mode.....	141	Initialisierungsvektor.....	231, 233, 253, 296
HT-Mixed-Mode.....	141	Initialisierungswert.....	233
HT-OFDM.....	131	Initialwert.....	313
IAPP.....	195	Integrity Check Value.....	232
		Inter Access Point Protocol.....	195

Inter Frame Spaces.....	96	Layer-2-Forwarding Protocol.....	316
Interface Control Information.....	47	Layer-2-Tunneling Protocol.....	316
Interferenzen,.....	30	Layer-2-Tunnelprotokolle.....	316
Interleaver.....	61	Layer-3-Tunnelprotokolle.....	319
International Data Encryption Algorithm.....	306	LEAP.....	325
Internet Protocol Security.....	319	Legacy -Mode.....	141
Internet Service Provider.....	317	Legitime Informationskanäle.....	277
Intersymbolinterferenz.....	71	Line of Sight.....	11, 71, 225
Intrusion Detection System.....	264, 287	Lineare Kryptoanalyse.....	295
Intrusion Prevention System.....	287	logging.....	282
Inverse-Fast-Fourier-Transformation.....	61	LoS.....	225
IoT.....	163	LOS.....	11, 71
IP.....	316	LTE.....	4
IP-in-IP.....	319	MAC.....	247, 313
IP-Mobile.....	18	MAC Protocol Data Unit.....	49
IPS.....	287	MAC-Adresse.....	11
IPSec.....	319	MAC-Geheimnis.....	313
IPv6.....	319	Man-in-the-Middle.....	255
IPX.....	317	Management-Frame.....	209
ISM.....	122	Master Key.....	237
ISM-Bänder.....	20	MC.....	117
ISP.....	317f	MCF.....	95
IT-System.....	275	MCS.....	139, 155
IV.....	209, 231, 233	MD5.....	312f.
IV-Kollisionen.....	254	MD5-Hash.....	324
IV16.....	244	Medien-Zugriffsverfahren.....	89
IV32.....	244	Meet-in-the-Middle Angriff.....	306
Kanal.....	123	Mehrwegeproblem.....	49
Kanäle.....	260	Mesh.....	
Kanalsuche.....	202	Access Point.....	12
Kanalzugriff.....	95	AP.....	12
Keyed MD5.....	313	IEEE-802.11s.....	11
KID.....	244	MAP.....	12
Klartext.....	232, 253, 293	MBSS.....	11
Known-Plain-Text Angriff.....	253	MCF.....	11
Kollision.....	311	Mesh Access Point.....	12
Kommunikationsbeziehungen.....	282	Mesh Coordination Function.....	11
Konfigurationsbeispiele.....	258	Mesh Point.....	12
KonTraG.....	291	Mesh Portal.....	12
Kryptoanalyse.....	295	Mesh-BSS.....	11
Kryptographie.....	295	MP.....	12
Kryptoregulierung.....	295	MPP.....	12
L2F.....	318	MSDU.....	11
L2P.....	316	QoS.....	11
L2TP.....	316ff.	Mesh Coordination Function.....	95

Mesh-WLAN.....	11	Packet Binary Convolutional Coding.....	127
Message Authentication Code.....	247, 313	Packet Error Rate.....	159
Message Integrity Code.....	243, 247	Packetizer.....	285
MIC.....	196, 243f., 247	Pairwise Master Key.....	239
Michael.....	243	Pairwise Transient Key.....	239
Mikrowellen-Öfen.....	21	PAP.....	318, 324
MIMO.....	132, 162	Passive Scanning.....	202
Empfangszüge.....	135	Passiver Angriff.....	284
Senderzüge.....	135	Password Authentication Protocol.....	324
MLO.....	184	Passwort.....	287
Mobilstation.....	8	Passwort Authentication Protocol.....	318
Modulation Coding Scheme.....	139	Patchantennen.....	223
Modulations-Verfahren.....	56	patial Stream.....	135
MPDUS.....	49	PBCC.....	127
MSDU.....	231	PBSS.....	14
MU-DL.....	181	PCF.....	42, 109
MU-MIMO.....	157, 162	PCI.....	48
Multi-Link Operation.....	184	PDU.....	47
Multi-Sounding.....	157	PEAP.....	325
Multi-User-Downlink.....	181	PER.....	159
Multi-User-MIMO.....	157	Per Packet Key.....	243
NAS.....	324	Per-Paket-Mixing.....	196
National Institute of Standards and Technology.....	247	Personal BSS.....	14
NAV.....	96	PHY.....	96
NDP.....	157	PHY-Layer.....	42
Network Allocation Vector.....	96	Physical Layer Convergence Procedure.....	49
Netzwerk-Management.....	284	Physical Media Dependent.....	49
NIST.....	247	Planung.....	257
non repudiation.....	282	PLCP.....	49
Nonce.....	239	PMD.....	49
Null-Data-Packet.....	157	PMK.....	239
Objekt-Authentifikation.....	280	PoE.....	264
OFB.....	306	Point Coordination Function.....	109
OFB-Modus.....	299	Point-to-Point Tunneling Protocol.....	316
OFDM.....	58, 138, 162	Polling-Verfahren.....	109
GI.....	78	PPK.....	243
Guard-Intervall.....	78	PPP.....	316
ISI.....	78	PPTP.....	316ff.
Symbolinterferenz.....	78	Preshared Key.....	235, 319
Tail-Bit.....	80	PRF.....	238
TXVECTOR.....	80	Primärnutzer.....	23
Open System.....	202	privacy.....	280, 282
Open-System-Authentication.....	207	private key.....	301
Orthogonal Frequency Division Multiplexing.....	58	Privatsphäre.....	282
Output-Feedback-Modus.....	299	PRNG.....	238

Produktauswahl.....	257	RADIUS-Server.....	324, 326
Protocol Control Information.....	48	Raum-Multiplex-Verfahren.....	29
Protocol Data Units.....	48	RC4.....	231, 254, 307, 318
Protokollierung.....	282	Re-Keying.....	196
Prüfsumme.....	89	Re-Sequencing.....	196
Pseudo-Random Number Generator.....	238	Rechte-Reduzierung.....	287
Pseudo-Random Function.....	238	Reduced Inter Frame Spacing.....	98
Pseudo-Zufallszahlen-Generatoren.....	296	Reflexionen.....	71
Pseudomisierung.....	282	Registriereinheit.....	8
PTK.....	239	RegTP.....	23
public key.....	301	reliability.....	277
Puffer-Überlauf.....	287	Remote Authentication Dial In User Service.....	214
QAP.....	15, 193	Replay.....	253
QBSS.....	15, 193	Request to send.....	106
QoS.....	7, 109, 193	RFC 2401.....	319
QOS.....	15	RFC 2409.....	319
QoS Access Point.....	193	RFC 2865.....	215
QoS Station.....	193	RFC 2869.....	215
QPSK.....	56	Richtantennen.....	15
QSTA.....	193	Richtcharakteristik.....	221f.
Quadrature Phase Shift Keying.....	56	Richtwirkung.....	222
Quality of Service.....	193	RIFS.....	98
Quittungen.....	89	RIPEMD-160.....	312
RadioLAN.....	7	Risiko.....	284
RADIUS.....	19, 213ff., 235, 321	Risiko-Management.....	291
Access Accept.....	322	risk.....	284
Access Challenge.....	322	Rivest's Cipher4.....	318
Access Reject.....	322	Roaming.....	18
Access Request.....	322	Robust Security Network.....	236
Accounting Request.....	322	RSA.....	310
Accounting Response.....	322	RSN.....	236
Attribut.....	321	RTR.....	20
Attribut-Länge.....	321	RTS.....	94, 106
Attribut-Nummer.....	321	Rundstrahlcharakteristik.....	221
Authenticator-Feld.....	321	SA.....	320
Authentizität.....	324	safety.....	280
Code.....	321	SAP.....	49
DMZ.....	322	Scanning.....	202
ID.....	321	Schadensereignis.....	284
NAS.....	322	Schadenspotential.....	284
Preshared Key.....	321	Schlüssel.....	208, 231
RADIUS-Client.....	322	Schlüssellänge.....	233
RADIUS-Server.....	322	Schlüsselsequenz.....	234, 253
Shared Secret.....	321	Schlüsselsequenz-Wörterbuch.....	210
RADIUS-Client.....	326	Schlüsselstrom-Verfahren.....	307

Stichwortverzeichnis

Schlüsselverfahren.....	301	Speicherkanäle.....	277
Schutzziele.....	280	Spoofing.....	285
Schwache Hashwerte.....	311	Spreizsequenz.....	56, 127
schwache Schlüssel.....	307	SRD.....	23
Schwache Schlüssel.....	254	SSL.....	307
Schwachstelle.....	284	Standard Festverbindung.....	316
SDU.....	47	Starke Hashwerte.....	311
security.....	280	Startwert.....	231
Seed.....	231	Statistische Kryptoanalyse.....	295
Sekundärnutzer.....	23	STBC.....	162
Service Access Points.....	49	StGB.....	290
Service Data Units.....	47	Strafgesetzbuch.....	290f.
Service-Sets.....	13, 94	Streuungen.....	71
Session Hijacking.....	256	Stromchiffrierer.....	296
SFV.....	316	Subjekt-Authentifikation.....	280
SHA / SHA-1.....	312	Subjekte.....	277
SHA-1.....	312	Substitution.....	306f.
Shared Media.....	231, 257	Supplicant.....	213
Shared Medium.....	27, 89	Symmetrische Schlüsselverfahren.....	301
Shared Secret.....	324	Symmetrische Verschlüsselungsstandards.....	306
Shared-Key-Authentication.....	207	Systemzustände.....	280
Shared-Key-Authentifizierung.....	209	Target Beacon Transmission Time.....	199
Short Inter Frame Spacing.....	98	Target Beacon Transmission Times.....	119
Short Range Device.....	23	TBTT.....	119, 199
Sicherheit.....	231, 278	TC.....	148f.
Sicherheitsniveau.....	291	TDD.....	27
Sicherheitsprobleme.....	234	TDM.....	78
Sichtverbindung.....	11	TDMA.....	28, 32, 51
SIFS.....	98	Telekommunikationsgesetz.....	290
Signalschwund.....	71	Temporal Key Integrity Protocol.....	236
Single Sounding.....	157	Temporal-Key-Integrity-Protocol.....	196
SISO.....	132	Text.....	293
Skript-Kiddie.....	289	threat.....	284
Small Office / Home Office.....	235	TID.....	148f.
Small Office Home Office.....	1	Tiger.....	312f.
Sniffer.....	285, 287	Time Division Duplex.....	27
SNonce.....	239	Time Division Multiple Access.....	28
SNR.....	202	Time Division Multiplexing.....	32
Social Engineering.....	285	Time Synchronisation Function.....	199
SOHO.....	1, 21, 235	Time Synchronization Function.....	120
Source-MAC-Adresse.....	243	Time Unit.....	199
Soziotechnisches System.....	275	Time Units.....	119
Space Division Multiple Access.....	29	TK.....	248
Spacial Streams.....	183	TKG.....	290
Spatial Multiplexing.....	134	TKIP.....	196, 235f.

TKIP Sequence Counter.....	243, 245	Wirtszelle.....	286
TKIP-mixed transmit address and key.....	243	Virtuelle Private Netzwerke.....	316
Topologien.....	13	Virus.....	286
TPC.....	7, 23, 119, 126	VLAN.....	284
Trainingssequenzen.....	71	Voice over IP.....	197
Transmission Opportunity.....	194	VoIP.....	197
Transmission Power Control.....	23, 126	Voluntary Tunneling.....	317
Transposition.....	306	VPN.....	316
TripleDES / 3DES.....	306	WDS.....	11
Trojaner.....	287	weakness.....	284
Trojanisches Pferd.....	287	WEP.....	231, 235, 307
TS.....	148f.	WEP-Verschlüsselung.....	210
TSC.....	243	Wi-Fi.....	17
TSF.....	120, 199	Wi-Fi Protected Access.....	235
TTAK.....	243	Wi-Fi-7.....	184
TU.....	119, 199	Wi-Fi-Alliance.....	235
Tunnel-Aufbau.....	318	Wiedereinspielen.....	285
TXOP.....	194	WiMAX.....	3
Übertragungsgeschwindigkeiten.....	257	Window Funktion.....	78
UC.....	117	Wired Equivalence Privacy.....	231
UDP.....	215	Wireless Distribution System.....	11
UMTS.....	4	Wireless Ethernet.....	17
Umweglaufzeit.....	71	Wireless Personal Area Networks.....	3
Universum.....	311	WLAN.....	287
Unveränderbarkeit.....	316	5G.....	4
Uplink.....	27	Access-Points.....	2
Urbildbereich.....	311	Ad-hoc Traffic Indication Map.....	116
Verändern.....	285	Ad-hoc-Modus.....	114
Verbindlichkeit.....	282	Advanced Encryption Standard.....	196
Verdeckte Informationskanäle.....	277	AES.....	196
Verfügbarkeit.....	282, 284	AP.....	2, 109
Verlässlichkeit.....	277	ATIM.....	116
Vermittlungsnetzwerk.....	8	Beacon-Frame.....	114
Verschlüsselung.....	231, 287	Broadcast.....	115
Verschlüsselungsverfahren.....	231, 293	CFP.....	109
Vertraulichkeit.....	282	Contention Free Period.....	109
Verwundbarkeit.....	284	Contention Period.....	109
Very High Throughput.....	155	CP.....	109
VHT.....	155	Delivery Traffic Indication Map.....	115
VHT-BSS.....	155	Distributions-System.....	16
VHT-Sounding Protocol.....	157	DS.....	16
Viren.....		DTIM.....	115
Infektion.....	286	EAP.....	196
Reproduktion.....	286	ESS.....	16
Schadensteil.....	286	Extensible Authentication Protocol.....	196

Stichwortverzeichnis

Funkzelle.....	8, 30	Wi-Fi Alliance.....	196
IBSS.....	14	Wi-Fi Protected Access.....	196
IEEE-802.11.....	1, 51, 196	Wired Equivalent Privacy.....	196
IEEE-802.11a.....	126	Wireless Compatibility Alliance.....	1
IEEE-802.11h.....	126	Wireless Fidelity.....	1
IEEE802.16.....	3	Wireless Metropolitan Area Network.....	3
IFS.....	97	WMAN.....	3
Independent Basic Service-Set.....	14	WPA.....	196
Infrastruktur-Modus.....	114	WPA2.....	196
Inter Frame Spaces.....	97	WLAN-Antennen.....	217
Interoperabilität.....	1	WLAN-Controller.....	264
Mobilfunkstandards.....	4	WLAN-Switches.....	264
Multicast.....	115	WLAN-Telefon.....	263
NAV.....	109	Wörterbuch mit Schlüsselsequenzen.....	253
Net Allocation Vector.....	109	WPA.....	235
PC.....	109	WPA 2.....	236
PCF.....	95, 98	WPAN.....	
PCF IFS.....	98	BAN.....	3
Physical Layer Convergence Procedure.....	124	Body-Area-Networks.....	3
PIFS.....	98	IEEE-802.15.....	3
PLCP.....	124	WPANs.....	3
Point Coordination Function.....	95	Würmer.....	287
Point Coordinator.....	109	Reproduktion.....	287
SDMA.....	28f.	Verbreitung.....	287
Shared Media.....	2	WWiSE.....	131
Space Division Multiple Access.....	28	XOR-Funktion.....	296, 300
Synchronisation.....	114	XOR-Operation.....	232
TIM.....	115	XOR-Verknüpfung.....	231
Timing Synchronisation Function.....	114f.	Yagi-Uda-Antenne.....	11
Traffic Indication Map.....	115	Zellgröße.....	257
TSF.....	114f.	Zellüberlappung.....	257
Unicast.....	115	Zugriffsprofile.....	282
WECA.....	1	Zuordenbarkeit.....	282
WEP.....	196	Zuordnungsvorschrift.....	282
Wi-Fi.....	1		

3 - Anhänge

3.1 - Beacon-Frame-Informationen

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability Information	
4	Service Set Identifier (SSID)	If dot11MeshActivated is true, the SSID element is the wildcard value as described in 9.4.2.2.
5	Supported Rates and BSS	Membership Selectors
6	DSSS Parameter Set	The element is optionally present. The DSSS Parameter Set element is present within Beacon frames generated by STAs using Clause 15, Clause 16, and Clause 18 PHYs. The element is present within Beacon frames generated by STAs using a Clause 19 PHY in the 2.4 GHz band.
7	CF Parameter Set	The CF Parameter Set element is present only within Beacon frames generated by APs supporting a PCF. This element is not present if dot11HighThroughputOptionImplemented is true and the Dual CTS Protection field of the HT Operation element is 1.
8	IBSS Parameter Set	The IBSS Parameter Set element is present only within Beacon frames generated by IBSS STAs.
9	Traffic indication map (TIM)	The TIM element is present only within Beacon frames generated by APs or mesh STAs.
10	Country	The Country element is present if dot11MultiDomainCapabilityActivated is true or dot11SpectrumManagementRequired is true or dot11RadioMeasurementActivated is true.
11	Power Constraint	The Power Constraint element is present if dot11SpectrumManagementRequired is true and is optionally present if dot11RadioMeasurementActivated is true.
12	Channel Switch Announcement	Channel Switch Announcement element is optionally present if dot11SpectrumManagementRequired is true.
13	Quiet	The Quiet element is optionally present if dot11SpectrumManagementRequired is true or dot11RadioMeasurementActivated is true.
14	IBSS DFS	IBSS DFS element is present if dot11SpectrumManagementRequired is true in an IBSS.
15	TPC Report	The TPC Report element is present if dot11SpectrumManagementRequired is true or dot11RadioMeasurementActivated is true.
16	ERP	The ERP element is present within Beacon frames generated by STAs using extended rate PHYs (ERPs) defined in Clause 18 and is optionally present in other cases.

17	Extended Supported Rates and BSS Membership Selectors	The Extended Supported Rates and BSS Membership Selectors element is present if there are more than eight supported rates, and it is optional otherwise.
18	RSN	The RSN is present within Beacon frames generated by STAs that have dot11RSNAActivated equal to true.
19	BSS Load	The BSS Load element is present if dot11QosOptionImplemented and dot11QBSSLoadImplemented are both true.
20	EDCA Parameter Set	The EDCA Parameter Set element is present if dot11QosOptionImplemented is true, and dot11MeshActivated is false, and the QoS Capability element is not present.

Order	Information	Notes
21	QoS Capability	The QoS Capability element is present if dot11QosOptionImplemented is true, and dot11MeshActivated is false, and EDCA Parameter Set element is not present.
22	AP Channel Report	If dot11RMAPChannelReportActivated is true, one AP Channel Report element is present for each operating class that has at least 1 channel to report.
23	BSS Average Access Delay	The BSS Average Access Delay element is present if dot11RMBSSAverageAccessDelayActivated is true and the value of the AP Average Access Delay field is not equal to 255 (measurement not available); otherwise, the BSS Average Access Delay element is optionally present if dot11RMBSSAverageAccessDelayActivated is true.
24	Antenna	The Antenna element is present if dot11RMAntennaInformationActivated is true and the value of the Antenna ID field is not equal to 0 (unknown antenna); otherwise, the Antenna element is optionally present if dot11RMAntennaInformationActivated is true.
25	BSS Available Admission Capacity	The BSS Available Admission Capacity element is present if dot11RMBSSAvailableAdmissionCapacityActivated is true with the following exceptions: 1) when Available Admission Capacity Bitmask equals 0 (Available Admission Capacity List contains no entries), or 2) when the BSS Load element is present and the Available Admission Capacity Bitmask states that only AC_VO is present in the Available Admission Capacity List field.
26	BSS AC Access Delay	The BSS AC Access Delay element is present if dot11RMBSSAverageAccessDelayActivated is true and at least one field of the element is not equal to 255 (measurement not available); otherwise, the BSS AC Access Delay element is optionally present if dot11RMBSSAverageAccessDelayActivated is true.
27	Measurement Pilot Transmission	The Measurement Pilot Transmission element is present if dot11RMMeasurementPilotActivated is a value between 2 and 7.
28	Multiple BSSID	One or more Multiple BSSID elements are present if dot11RMMeasurementPilotActivated is a value between 2 and 7 and the AP is a member of a multiple BSSID set (see 11.11.14) with two or more members, or if dot11MultiBSSIDActivated is true, or if dot11InterworkingServiceActivated is true and the AP is a member of a multiple BSSID set with two or more members and at least one dot11GASAdvertisementID exists.

Anhänge

29	RM Enabled Capabilities	RM Enabled Capabilities element is present if dot11RadioMeasurementActivated is true.
30	Mobility Domain	The Mobility Domain element (MDE) is present if dot11FastBSSTransitionActivated is true.
31	DSE registered location	The DSE Registered Location element is present if dot11LCIDSERequired is true.
32	Extended Channel Switch Announcement	The Extended Channel Switch Announcement element is optionally present if dot11ExtendedChannelSwitchActivated is true.

Order	Information	Notes
33	Supported Operating Classes	The Supported Operating Classes element is present if dot11ExtendedChannelSwitchActivated is true. The Supported Operating Classes element is optionally present if dot11TVHTOptionImplemented is true.
34	HT Capabilities	The HT Capabilities element is present when dot11HighThroughputOptionImplemented is true.
35	HT Operation	The HT Operation element is included by an AP and a mesh STA when dot11HighThroughputOptionImplemented is true.
36	20/40 BSS Coexistence	The 20/40 BSS Coexistence element is optionally present when the dot112040BSSCoexistenceManagementSupport is true.
37	Overlapping BSS Scan Parameters	The Overlapping BSS Scan Parameters element is optionally present if dot11FortyMHzOptionImplemented is true.
38	Extended Capabilities	The Extended Capabilities element is present if any of the fields in this element are nonzero.
39	FMS Descriptor	The FMS Descriptor element is present if dot11FMSActivated is true.
40	QoS Traffic Capability	The QoS Traffic Capability element is optionally present if dot11ACStationCountActivated is true.
41	Time Advertisement	The Time Advertisement element is present every dot11TimeAdvertisementDTIMInterval if dot11UTCTSFOffsetActivated is true.
42	Interworking	The Interworking element is present if dot11InterworkingServiceActivated is true.
43	Advertisement Protocol	Advertisement Protocol element is present if dot11InterworkingServiceActivated is true and at least one dot11GASAdvertisementID MIB attribute exists.
44	Roaming Consortium	The Roaming Consortium element is present if dot11InterworkingServiceActivated is true and the dot11RoamingConsortiumTable has at least one entry.
45	Emergency Alert Identifier	One or more Emergency Alert Identifier elements are present if dot11EASActivated is true and there are one or more EAS message(s) active in the network.
46	Mesh ID	The Mesh ID element is present if dot11MeshActivated is true.
47	Mesh Configuration	The Mesh Configuration element is present if dot11MeshActivated is true.
48	Mesh Awake Window	The Mesh Awake Window element is optionally present if dot11MeshActivated is true.
49	Beacon Timing	The Beacon Timing element is optionally present if both dot11MeshActivated and dot11MBCAActivated are true.
50	MCCAOP Advertisement Overview	The MCCAOP Advertisement Overview element is optionally present if both dot11MeshActivated and dot11MCCAActivated are true.

Anhänge

51	MCCAOP Advertisement	One or more MCCAOP Advertisement elements are optionally present if both dot11MeshActivated and dot11MCCAActivated are true.
52	Mesh Channel Switch Parameters	The Mesh Channel Switch Parameters element is present when dot11MeshActivated is true and either Channel Switch Announcement element or Extended Channel Switch Announcement element is present.
53	QMF Policy	Indicates the QMF policy parameters of the transmitting STA. The QMF Policy element is present when dot11QMFAActivated is true and the transmitting STA is an AP or a mesh STA. This element is not present otherwise.

Order	Information	Notes
54	QLoad Report	The QLoad Report element is present every dot11QLoadReportIntervalDTIM DTIMs if dot11QLoadReportActivated is true.
55	HCCA TXOP Update Count	The HCCA TXOP Update Count element is present if both dot11PublicHCCATXOPNegotiationActivated is true and an HC is collocated with the AP.
56	Multi-band	The Multi-band element is optionally present if dot11MultibandImplemented is true.
57	VHT Capabilities	The VHT Capabilities element is present when the dot11VHTOptionImplemented is true.
58	VHT Operation	The VHT Operation element is present when the dot11VHTOptionImplemented is true; otherwise, it is not present.
59	Transmit Power Envelope element	One Transmit Power Envelope element is present for each distinct value of the Local Maximum Transmit Power Unit Interpretation subfield that is supported for the BSS if both of the following conditions are met: — dot11VHTOptionImplemented or dot11ExtendedSpectrumManagementImplemented is true; — Either dot11SpectrumManagementRequired is true or dot11RadioMeasurementActivated is true. Otherwise, this parameter is not present.
60	Channel Switch Wrapper element	The Channel Switch Wrapper element is optionally present if dot11VHTOptionImplemented or dot11ExtendedSpectrumManagementImplemented is true and at least one of a Channel Switch Announcement element or an Extended Channel Switch Announcement element is also present in the Beacon frame and the Channel Switch Wrapper element contains at least one subelement.
61	Extended BSS Load element	The Extended BSS Load element is optionally present if dot11QosOptionImplemented, dot11QBSSLoadImplemented, and dot11VHTOptionImplemented are true.
62	Quiet Channel	Either one Quiet Channel element containing an AP Quiet Mode field equal to 0 or, in an infrastructure BSS, one or more Quiet Channel elements each containing an AP Quiet Mode field equal to 1 are optionally present if dot11VHTOptionImplemented is true, and either dot11SpectrumManagementRequired or dot11RadioMeasurementActivated is true.
63	Operating Mode Notification	The Operating Mode Notification element is optionally present if dot11OperatingModeNotificationImplemented is true.
64	Reduced Neighbor Report	The Reduced Neighbor Report element is optionally present if dot11TVHTOptionImplemented is true.

Anhänge

65	TVHT Operation	The TVHT Operation element is present for a TVHT STA when the dot11TVHTOptionImplemented is true; otherwise it is not present.
66	Estimated Service Parameters	The Estimated Service Parameters element is present if dot11EstimatedServiceParametersOptionImplemented is true.
67	Future Channel Guidance	The Future Channel Guidance element is optionally present if dot11FutureChannelGuidanceActivated is true.
Last	Vendor Specific	One or more vendor-specific elements are optionally present. These elements follow all other elements.

3.2 - Status-Codes

Status code	Name	Meaning
0	SUCCESS	Successful.
1	REFUSED, REFUSED_REASON_UNSPECIFIED	Unspecified failure.
2	TDLS_REJECTED_ALTERNATIVE _ PROVIDED TDLS	wakeup schedule rejected but alternative schedule provided. 3 TDLS_REJECTED TDLS wakeup schedule rejected.
4	Reserved.	
5	SECURITY_DISABLED	Security disabled.
6	UNACCEPTABLE_LIFETIME	Unacceptable lifetime. 7 NOT_IN_SAME_BSS Not in same BSS.
8–9	Reserved.	
10	REFUSED_CAPABILITIES_MISMATCH	Cannot support all requested capabilities in the Capability Information field.
11	DENIED_NO_ASSOCIATION_EXISTS	Reassociation denied due to inability to confirm that association exists.
12	DENIED_OTHER_REASON	Association denied due to reason outside the scope of this standard.
13	UNSUPPORTED_AUTH_ALGORITHM	Responding STA does not support the specified authentication algorithm.
14	TRANSACTION_SEQUENCE_ERROR	Received an Authentication frame with authentication transaction sequence number out of expected sequence.
15	CHALLENGE_FAILURE	Authentication rejected because of challenge failure.
16	REJECTED_SEQUENCE_TIMEOUT	Authentication rejected due to timeout waiting for next frame in sequence.
17	DENIED_NO_MORE_STAS	Association denied because AP is unable to handle additional associated STAs.
18	REFUSED_BASIC_RATES_MISMATCH	Association denied due to requesting STA not supporting all of the data rates in the BSSBasicRateSet parameter, the Basic HT-MCS Set field of the HT Operation parameter, or the Basic VHT-MCS and NSS Set field in the VHT Operation parameter.
19	DENIED_NO_SHORT_PREAMBLE _ SUPPORT	Association denied due to requesting STA not supporting the short preamble option.
20	Reserved.	
21	Reserved.	
22	REJECTED_SPECTRUM _ MANAGEMENT_REQUIRED	Association request rejected because Spectrum Management capability is required.
23	REJECTED_BAD_POWER_CAPABILITY	Association request rejected because the information in the Power Capability element is unacceptable.
24	REJECTED_BAD_SUPPORTED_CHANNELS	Association request rejected because the information in the Supported Channels element is unacceptable.
25	DENIED_NO_SHORT_SLOT _ TIME_SUPPORT	Association denied due to requesting STA not supporting the Short Slot Time option.

Status code	Name	Meaning
26	Reserved.	
27	DENIED_NO_HT_SUPPORT	Association denied because the requesting STA does not support HT features.
28	ROKH_UNREACHABLE	ROKH unreachable.
29	DENIED_PCO_TIME_NOT_SUPPORTED	Association denied because the requesting STA does not support the phased coexistence operation (PCO) transition time required by the AP.
30	REFUSED_TEMPORARILY	Association request rejected temporarily; try again later.
31	ROBUST_MANAGEMENT_POLICY_VIOLATION	Robust management frame policy violation.
32	UNSPECIFIED_QOS_FAILURE	Unspecified, QoS-related failure.
33	DENIED_INSUFFICIENT_BANDWIDTH	Association denied because QoS AP or PCP has insufficient bandwidth to handle another QoS STA.
34	DENIED_POOR_CHANNEL_CONDITIONS	Association denied due to excessive frame loss rates and/ or poor conditions on current operating channel.
35	DENIED_QOS_NOT_SUPPORTED	Association (with QoS BSS) denied because the requesting STA does not support the QoS facility.
36	Reserved.	
37	REQUEST_DECLINED	The request has been declined.
38	INVALID_PARAMETERS	The request has not been successful as one or more parameters have invalid values.
39	REJECTED_WITH_SUGGESTED_CHANGES	The allocation or TS has not been created because the request cannot be honored; however, a suggested TSPEC/DMG TSPEC is provided so that the initiating STA can attempt to set another allocation or TS with the suggested changes to the TSPEC/DMG TSPEC.
40	STATUS_INVALID_ELEMENT	Invalid element, i.e., an element defined in this standard for which the content does not meet the specifications in Clause 9.
41	STATUS_INVALID_GROUP_CIPHER	Invalid group cipher.
42	STATUS_INVALID_PAIRWISE_CIPHER	Invalid pairwise cipher.
43	STATUS_INVALID_AKMP	Invalid AKMP.
44	UNSUPPORTED_RSNE_VERSION	Unsupported RSNE version.
45	INVALID_RSNE_CAPABILITIES	Invalid RSNE capabilities.
46	STATUS_CIPHER_OUT_OF_POLICY	Cipher suite rejected because of security policy.
47	REJECTED_FOR_DELAY_PERIOD	The TS or allocation has not been created; however, the HC or PCP might be capable of creating a TS or allocation, in response to a request, after the time indicated in the TS Delay element.
48	DLS_NOT_ALLOWED	Direct link is not allowed in the BSS by policy.
49	NOT_PRESENT	The Destination STA is not present within this BSS.
50	NOT_QOS_STA	The Destination STA is not a QoS STA.
51	DENIED_LISTEN_INTERVAL_TOO_LARGE	Association denied because the listen interval is too large.
52	STATUS_INVALID_FT_ACTION_FRAME	Invalid FT Action frame count.

Status code	Name	Meaning
53	_COUNT	
54	STATUS_INVALID_PMKID	Invalid pairwise master key identifier (PMKID).
55	STATUS_INVALID_MDE	Invalid MDE.
56	STATUS_INVALID_FTE	Invalid FTE.
57	REQUESTED_TCLAS_NOT_SUPPORTED	Requested TCLAS processing is not supported by the AP or PCP.
58	INSUFFICIENT_TCLAS_PROCESSING_RESOURCES	The AP or PCP has insufficient TCLAS processing resources to satisfy the request.
59	TRY_ANOTHER_BSS	The TS has not been created because the request cannot be honored; however, the HC or PCP suggests that the STA transition to a different BSS to set up the TS.
60	GAS_ADVERTISEMENT_PROTOCOL_NOT_SUPPORTED	Advertisement Protocol not supported.
61	NO_OUTSTANDING_GAS_REQUEST	No outstanding GAS request.
62	GAS_RESPONSE_NOT_RECEIVED	Response not received from the Advertisement Server.
63	_FROM_SERVER_GAS	
64	GAS_QUERY_TIMEOUT	STA timed out waiting for GAS Query Response.
65	GAS_QUERY_RESPONSE_TOO_LARGE	GAS Response is larger than query response length limit.
66	REJECTED_HOME_WITH_SUGGESTED_CHANGES	Request refused because home network does not support request.
67	SERVER_UNREACHABLE	Advertisement Server in the network is not currently reachable.
68	Reserved.	
69-71	REJECTED_FOR_SSP_PERMISSIONS	Request refused due to permissions received via SSPN interface.
72	REFUSED_UNAUTHENTICATED_ACCESS_NOT_SUPPORTED	Request refused because the AP or PCP does not support unauthenticated access.
73	INVALID_RSNE	Invalid contents of RSNE.
74	U_APDS_COEXISTANCE_NOT_SUPPORTED	U-APSD coexistence is not supported.
75	U_APDS_COEX_MODE_NOT_SUPPORTED	Requested U-APSD coexistence mode is not supported.
76	BAD_INTERVAL_WITH_U_APDS_COEX	Requested Interval/Duration value cannot be supported with U-APSD coexistence.
77	ANTI_CLOGGING_TOKEN_REQUIRED	Authentication is rejected because an Anti-Clogging Token is required.
78	UNSUPPORTEDFINITECYCLICGROUP	Authentication is rejected because the offered finite cyclic group is not supported.
79	CANNOT_FIND_ALTERNATIVE_TBTT	The TBTT adjustment request has not been successful because the STA could not find an alternative TBTT.
80	TRANSMISSION_FAILURE	Transmission failure.
81	REQUESTED_TCLAS_NOT_SUPPORTED	Requested TCLAS Not Supported.
	TCLAS_RESOURCES_EXHAUSTED	Resources Exhausted.

82	REJECTED_WITH_SUGGESTED _BSS_TRANSITION	Rejected with Suggested BSS transition.
83	REJECT_WITH_SCHEDULE	Reject with recommended schedule.
84	REJECT_NO_WAKEUP_SPECIFIED	Reject because no wakeup schedule specified.
85	SUCCESS_POWER_SAVE_MODE	Success, the destination STA is in power save mode.
86	PENDING ADMITTING FST SESSION	FST pending, in process of admitting FST session.
87	PERFORMING_FST_NOW	Performing FST now.
88	PENDING_GAP_IN_BA_WINDOW	FST pending, gap(s) in block ack window.
89	REJECT_U-PID_SETTING	Reject because of U-PID setting.
90–91	Reserved.	
92	REFUSED_EXTERNAL_REASON	(Re)Association refused for some external reason.
93	REFUSED_AP_OUT_OF_MEMORY	(Re)Association refused because of memory limits at the AP.
94	REJECTED_EMERGENCY_SERVICES _NOT_SUPPORTED	(Re)Association refused because emergency services are not supported at the AP.
95	QUERY_RESPONSE_OUTSTANDING	GAS query response not yet received.
96	REJECT_DSE_BAND	Reject since the request is for transition to a frequency band subject to DSE procedures and FST Initiator is a dependent STA.
97	TCLAS_PROCESSING_TERMINATED	Requested TCLAS processing has been terminated by the AP.
98	TS_SCHEDULE_CONFLICT	The TS schedule conflicts with an existing schedule; an alternative schedule is provided.
99	DENIED_WITH_SUGGESTED _BAND_AND_CHANNEL	The association has been denied; however, one or more Multi-band elements are included that can be used by the receiving STA to join the BSS.
100	MCCAOP_RESERVATION_CONFLICT	The request failed due to a reservation conflict.
101	MAF_LIMIT_EXCEEDED	The request failed due to exceeded MAF limit.
102	MCCA_TRACK_LIMIT_EXCEEDED	The request failed due to exceeded MCCA track limit.
103	DENIED_DUE_TO_SPECTRUM _MANAGEMENT	Association denied because the information in the Spectrum Management field is unacceptable.
104	DENIED_VHT_NOT_SUPPORTED	Association denied because the requesting STA does not support VHT features.
105	ENABLEMENT DENIED	Enablement denied.
106	RESTRICTION FROM AUTHORIZED GDB	Enablement denied due to restriction from an authorized GDB.
107	AUTHORIZATION DEENABLED	Authorization deenabled.
108–	Reserved.	

65 535

3.3 - Reason-Codes

Reason Name	Meaning
code	
0 Reserved	
1 UNSPECIFIED_REASON	Unspecified reason
2 INVALID_AUTHENTICATION	Previous authentication no longer valid
3 LEAVING_NETWORK_DEAUTH	Deauthenticated because sending STA is leaving (or has left) IBSS or ESS
4 REASON_INACTIVITY	Disassociated due to inactivity
5 NO_MORE_STAS	Disassociated because AP is unable to handle all currently associated STAs
6 INVALID_CLASS2_FRAME	Class 2 frame received from nonauthenticated STA
7 INVALID_CLASS3_FRAME	Class 3 frame received from nonassociated STA
8 LEAVING_NETWORK_DISASSOC	Disassociated because sending STA is leaving (or has left) BSS
9 NOT_AUTHENTICATED	STA requesting (re)association is not authenticated with responding STA
10 UNACCEPTABLE_POWER_CAPABILITY	Disassociated because the information in the Power Capability element is unacceptable
11 UNACCEPTABLE_SUPPORTED_CHANNELS	Disassociated because the information in the Supported Channels element is unacceptable _CHANNELS
12 BSS_TRANSITION_DISASSOC	Disassociated due to BSS transition management
13 REASON_INVALID_ELEMENT	Invalid element, i.e., an element defined in this standard for which the content does not meet the specifications in Clause 9
14 MIC_FAILURE	Message integrity code (MIC) failure
15 4WAY_HANDSHAKE_TIMEOUT	4-way handshake timeout
16 GK_HANDSHAKE_TIMEOUT	Group key handshake timeout
17 H ANDSHAKE_ELEMENT_MISMATCH	Element in 4-way handshake different from (Re)Association Request/Probe Response/Beacon frame
18 REASON_INVALID_GROUP_CIPHER	Invalid group cipher
19 REASON_INVALID_PAIRWISE_CIPHER	Invalid pairwise cipher
20 REASON_INVALID_AKMP	Invalid AKMP
21 UNSUPPORTED_RSNE_VERSION	Unsupported RSNE version
22 INVALID_RSNE_CAPABILITIES	Invalid RSNE capabilities
23 802_1X_AUTH_FAILED	IEEE 802.1X authentication failed
24 REASON_CIPHER_OUT_OF_POLICY	Cipher suite rejected because of the security policy
25 TDLS_PEER_UNREACHABLE	TDLS direct-link teardown due to TDLS peer STA unreachable via the TDLS direct link
26 TDLS_UNSPECIFIED_REASON	TDLS direct-link teardown for unspecified reason
27 SSP_REQUESTED_DISASSOC	Disassociated because session terminated by SSP request
28 NO_SSP_ROAMING AGREEMENT	Disassociated because of lack of SSP roaming agreement
29 BAD_CIPHER_OR_AKM	Requested service rejected because of SSP cipher suite or AKM requirement

Anhänge

30 N	OT_AUTHORIZED_THIS_LOCATION	Requested service not authorized in this location
31 S	ERVICE_CHANGE_PRECLUDES_TS	TS deleted because QoS AP lacks sufficient bandwidth for this QoS STA due to a change in BSS service characteristics or operational mode (e.g., an HT BSS change from 40 MHz channel to 20 MHz channel)
32	UNSPECIFIED_QOS_REASON	Disassociated for unspecified, QoS-related reason
33	NOT_ENOUGH_BANDWIDTH	Disassociated because QoS AP lacks sufficient bandwidth for this QoS STA
34	MISSING_ACKS	Disassociated because excessive number of frames need to be acknowledged, but are not acknowledged due to AP transmissions and/or poor channel conditions
35	EXCEEDED_TXOP	Disassociated because STA is transmitting outside the limits of its TXOPs

Reason Name	Meaning
code	
36 STA_LEAVE	Requesting STA is leaving the BSS (or resetting)
37 END_TS	Requesting STA is no longer using the stream or session
END_BA	
END_DLS	
38 UNKNOWN_TS	Requesting STA received frames using a mechanism for which a setup has not been completed
UNKNOWN_BA	
39 TIMEOUT	Requested from peer STA due to timeout
45 PEERKEY_MISMATCH	Peer STA does not support the requested cipher suite
46 PEER_INITIATED	In a DLS Teardown frame: The teardown was initiated by the DLS peer In a Disassociation frame: Disassociated because authorized access limit reached
47 AP_INITIATED	In a DLS Teardown frame: The teardown was initiated by the AP In a Disassociation frame: Disassociated due to external service requirements
48 REASON_INVALID_FT_ACTION _FRAME_COUNT	Invalid FT Action frame count
49 REASON_INVALID_PMKID	Invalid pairwise master key identifier (PMKID)
50 REASON_INVALID_MDE	Invalid MDE
51 REASON_INVALID_FTE	Invalid FTE 52 MESH-PEERING-CANCELED Mesh peering canceled for unknown reasons
53 MESH-MAX-PEERS	The mesh STA has reached the supported maximum number of peer mesh STAs
54 MESH-CONFIGURATION-POLICY -VIOLATION	The received information violates the Mesh Configuration policy - configured in the mesh STA profile
55 MESH-CLOSE-RCVD	The mesh STA has received a Mesh Peering Close frame requesting to close the mesh peering.
56 MESH-MAX-RETRIES	The mesh STA has resent dot11MeshMaxRetries Mesh Peering Open frames, without receiving a Mesh Peering Confirm frame.
57 MESH-CONFIRM-TIMEOUT	The confirmTimer for the mesh peering instance times out.
58 MESH-INVALID-GTK	The mesh STA fails to unwrap the GTK or the values in the wrapped contents do not match
59 MESH-INCONSISTENT- PARAMETERS	The mesh STA receives inconsistent information about the mesh parameters between mesh peering Management frames
60 MESH-INVALID-SECURITY- CAPABILITY	The mesh STA fails the authenticated mesh peering exchange because due to failure in selecting either the pairwise ciphersuite or group cipher suite
61 MESH-PATH-ERROR-NOPROXY- INFORMATION	The mesh STA does not have proxy information for this external destination.
62 MESH-PATH-ERROR- NOFORWARDING-INFORMATION	The mesh STA does not have forwarding information for this destination.
63 MESH-PATH-ERROR- DESTINATION-UNREACHABLE	The mesh STA determines that the link to the next hop of an active path in its forwarding information is no longer usable.

- 64 MAC-ADDRESS-ALREADYEXISTS- IN-MBSS The Deauthentication frame was sent because the MAC address of the STA already exists in the mesh BSS. See 11.3.6.
 - 65 MESH-CHANNEL-SWITCH-REGULATORY-REQUIREMENTS The mesh STA performs channel switch to meet regulatory requirements.
 - 66 MESH-CHANNEL-SWITCH-UNSPECIFIED The mesh STA performs channel switching with unspecified reason.
 - 67- Reserved
- 65 535

Quelle: [IEEE802.11-2016]

4 - Formelanhang

4.1 - DB-Leistungsverhältnisse

Steigerung

Steigerung	0	1	3	6	10	12	20	30
Faktor	*1	*1,25	*2	*4	*10	*16	*100	*1000

Reduzierung

Reduzierung	0	-1	-3	-6	-10	-12	-20	-30
Faktor	*1	*0,8	*0,5	*0,25	*0,1	*0,06	*0,01	*0,001

4.2 - dbw

Entspricht einem Vergleich mit 1 W Leistung

$$\text{Sendeleistung [dBw]} = 10 \times \log_{10} \left(\frac{\text{Senderleistung [Watt]}}{1 \text{W}} \right) \quad (41)$$

4.3 - dbm

Entspricht einem Vergleich mit 1 mW Leistung

$$\text{Sendeleistung [dBm]} = 10 \log_{10} \left(\frac{\text{Senderleistung [mw]}}{1 \text{mW}} \right) \quad (42)$$

Tabelle 66: Umrechnung von dBm in mW

dBm	0	1	3	6	7	10	12	13	15	17	20	30	40
mW	1	1,25	2	4	5	10	16	20	32	50	100	1.000	10.000

dBm	0	-1	-3	-6	-7	-10	-12	-13	-15	-17	-20	-30	-40
mW	1	0,8	0,5	0,25	0,2	0,1	0,06	0,05	0,03	0,02	0,01	0,001	0,0001