HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

WLAN

Wireless Local Area Network

Prof. Dr.-Ing. habil. Lutz Winkler
Fakultät Elektro- und Informationstechnik
https://www.telecom.hs-mittweida.de
lutz.winkler@hs-mittweida.de

2012-11

Ziel und Inhalt der Vorlesung

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

- Ziel

  Kennenlernen aktueller WLAN-Technologien, basierend auf IEEE 802.11, bezüglich ihrer Funktionsweise, Parameter, Protokolle, Anwendung, Sicherheit.

- Inhalt

Übersicht

WLAN unterstützt:	• für Direktverbindung (peer-to-peer) zwischen Endgeräten (Laptop's, PC's), • für Indirektverbindungen, die Endgeräte kommunizieren über Infrastrukturnetze auf die sie durch Access Points Zugang erhalten.
WLAN sind Technologien der OSI-Schichten 1 und 2, es ist nur geregelt:	• wie Bits per Funk übertragen werden (Physical), • wie mehrere Endgeräte auf ein gemeinsames Medium zugreifen (MAC - Medium Access Control) und Zugriffskonflikte vermieden werden sollen,
Funkzellengröße	• 10m bis 100m, mit Richtantennen einige km. • Zell-Größe = f(Datenrate, Umgebung,Sendeleistung,Antenne)
Datenraten	• 600 Mbit/s • geplant einige Gbit/s
Sendeleistung	• 100-4000 mW international • 100-1000mW in Europa
Mehrere lokale Funknetztechnologien	• WLAN, standardisiert in IEEE[1)]-802.11 • WPAN (Wireless Personal Area Network), IEEE-802.15, hervorgegangen aus Bluetooth
Schwerpunkt des Scripts	• IEEE-802.11 und Erweiterungen.

[1)] IEEE - The Institute of Electrical and Electronics Engineers, auch IE^3 (I-triple-E)

Übersicht: **Entwicklung der IEEE[1)]-WLAN-Standards**

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

1997	Erster WLAN-Standard →802.11 • Drei Ph-Layer: Infrarot, Frequency Hopping Spread Spectrum (FHSS), Direct-Sequence-Spread-Spectrum-Verfahren (DSSS). →Vü: 1,2 Mbps. • FHSS und DSSS über lizenzfreies 2,4-GHz-ISM-Band (Industrial-Scientific-Medical-Band)
1999	Erweiterung von 802.11 auf 802.11b • Nur noch DSSS für 1|2 Mbit/s und "Complimentary Code Keying" (CCK) für Datenraten von 5,5 und 11 Mbit/s. • Nutzung des ISM-Bandes (2,4 GHz): 13 Kanäle zu 22MHz, die sich überlappen.
1999	Erweiterung durch 802.11a • Nutzung des ebenfalls lizenzfreien 5,2 GHz-Bandes: 19 Kanäle zu 20MHz nichtüberlappend. • Als Spreizverfahren wird OFDM (Orthogonal Frequency Division Multiplexing) verwendet. Je nach FEC-Code (Forward Error Correcting Code) und Modulationsverfahren werden bis 108 Mbps erreicht.
2004	Erweiterung von 802.11b auf 802.11g • Freigabe für OFMD, auch im ISM-Band (2,4 GHz).

2006	Erweiterung 802.11n
	• Bis 300/600 Mbit/s mittels MIMO (Multiple Input Multiple Output) im 5,2 oder 2,4-GHz-Band.
	• In einem Kanal werden durch mehrere Sende- und Empfangsantennen
	  • das Signal-Rausch-Verhältnis verbessert: größere Reichweite, höherwertige Modulation möglich
	  • oder gleichzeitig mehrere Bitströme übertragen (orthogonale Ausbreitungspfade).

Aktuell	Erweiterung 802.11ac • im 5-GHz-Band, Kanalbandbreiten von 80/160 MHz, OFDM und MIMO, Datenraten bis 7Gbit/s.

[1)] IEEE - The Institute of Electrical and Electronics Engineers, auch IE^3 (I-triple-E)

Übersicht: **Vor- und Nachteile drahtloser Netze** /Sch2000/

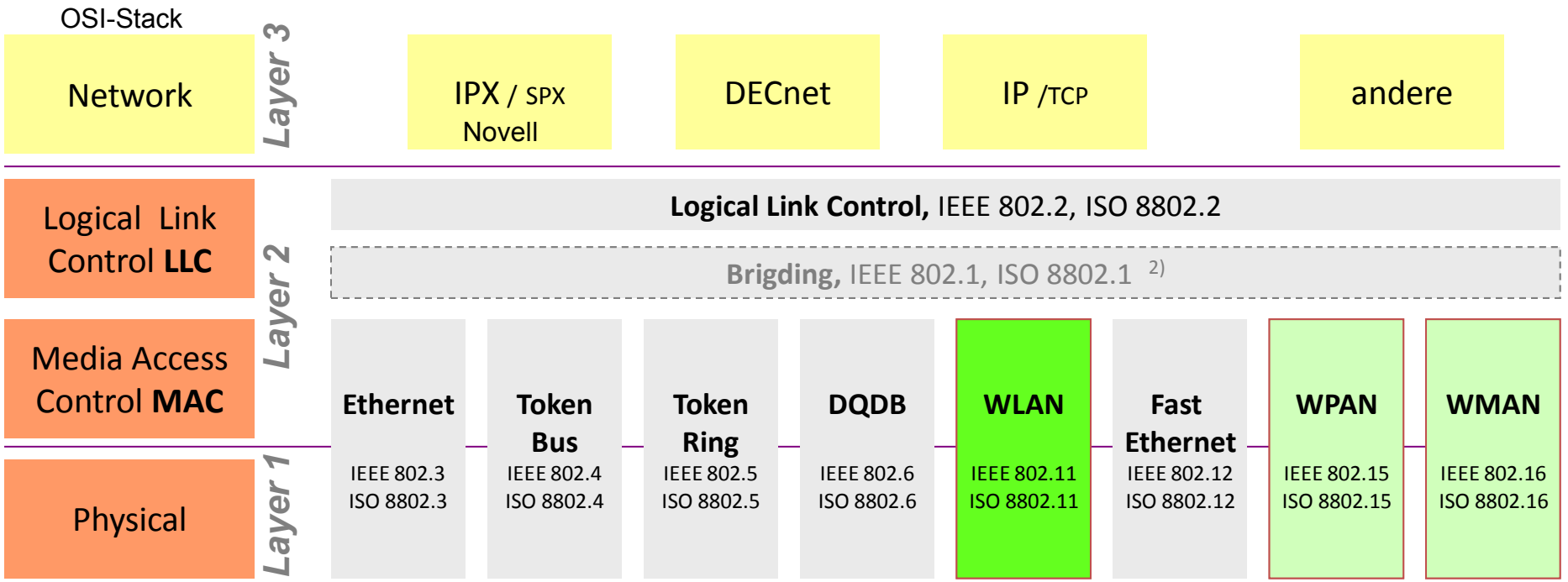
HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

Vorteile	Nachteile
Größere Flexibilität • Gute Anpassbarkeit an bauliche Gegebenheiten (historische Gebäude), • Technik kann versteckt werden (Zwischendecken, Blenden), kaum bauliche Eingriffe (z.B. Brandmauerdurchbrüche)	**Dienstgüte** von WLAN's ist **deutlich schlechter** • Datenraten um Faktor 10 kleiner gegenüber Fest-LAN, • Fehlerrate Funk/Kabel wie 10-1 .. 10-3 / 10-4 ..10-9,
Geringere Kosten für Netzprovider • z.B. in Bildungseinrichtungen reichen ein oder zwei Access Points für einen Hörsaal, • Verkabelung jedes Platzes ist teuer	**Funklösungen sind oft proprietäre Lösungen** • Standardisierung dauert lange, unterschiedliche Zulassungsregelungen in den Ländern, • unterschiedliche Vergabe und Nutzbarkeit von Frequenzbändern.
Robustheit gegenüber drahtgebundener Technik (Katastrophen)	**Sicherheitsprobleme** • Mithören, unberechtigte Nutzung von Access Points • Störung sensibler Infrastrukturen (Krankenhäuser, Flugzeuge, andere Funknetze).

Übersicht: **Entwurfsziele von WLAN-Technologien** /Sch2000/

Weltweite Standardisierung	• damit Produkte mit Festnetztechnologien kostenmäßig mithalten können, • damit auf Geschäftsreisen Kommunikation unterwegs und am Ziel möglich sind.
Niedrige Leistungsaufnahme	• Nur Batteriebetrieb erlaubt größtmögliche Flexibilität, • Geräte müssen Energiesparmodus (Sendeleistung, Inaktivitätskontrolle) unterstützen.
Lizenzfreier Betrieb	• Der Betrieb der meisten Mobilfunknetze ist genehmigungspflichtig, • Für WLAN nicht praktikabel →deshalb lizenzfreie Bänder →aber kleine Sendeleistung →Störungen durch andere.
Robuste Übertragungstechnik	• Funkkanäle unterliegen Störungen (Haushaltgeräte, Fahrzeuge), Netze sind nicht optimiert, • Kommunikation soll trotzdem möglich sein.
Einfachheit der Nutzung	• keine komplexen Administrationsvorgänge in Endgeräten (Plug & Play), • WLAN-Nutzung (Firma, zu Hause, Unterwegs) →keine verschieden Einstellungen.

IEEE[1)]802.11-Grundlagen: **Übersicht 802-LAN-Standards**



http://grouper.ieee.org/groups/802/index.html

- IEEE 802.11, Wireless-LAN
- IEEE 802.15, WPAN – Wireless Personal Area Network, niedrige Bandbreite, Reichweite bis 10 m, basierend auf Bluetooth
- IEEE 802.16, WMAN – Wireless Metropolitan Area Network, breitbandiger Zugang im Stadtbereich (bis 50 km)

1) IEEE - The Institute of Electrical and Electronics Engineers, auch IE[3] (I-triple-E)
2) Gibt es nur in in Brücken bzw. Multiport-Brücken, nicht in Endgeräten!

IEEE802.11-Grundlagen: **802.11- Aktivitäten**

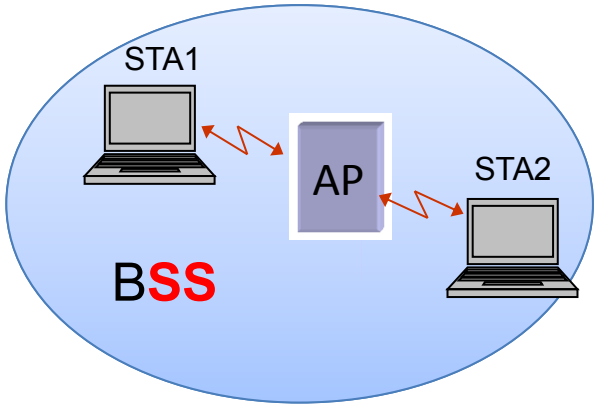
HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

IEEE	WLAN
802.11	**1|2 Mbit/s, im 2,4-GHz-ISM[1)]-Band** →1997 Basisstandard
802.11b	5,5|11 Mbit/s, im 2,4-GHz-ISM[1)]-Band, →2000 Erweiterung 802.1b - CCK, 22-MHz-Kanäle
802.11a	6…54 Mbit/s, im 5-GHz-Band, →2000 Erweiterung 802.11a – OFDM, 20-MHz-Kanäle
802.11g	6…54 Mbit/s, im 2,4-GHz-Band, →2003 Erweiterung 802.11g – OFDM, 20-MHz-Kanäle
802.11n	bis 600 Mbit/s im 2,4-GHz-Band →2007 Erweiterung 802.11n – 40-MHz-Kanäle, MIMO (Multiple Input Multiple Output), bis 600 Mbit/s im 5-GHz-Band →2007 Erweiterung 802.11n – 40-MHz-Kanäle, MIMO (Multiple Input Multiple Output),
802.11ac	Gigabit-WLAN
802.11e	Erweiterungen der 802.11-MAC-Subschicht, zur Bereitstellung von QoS z.B. durch Zugriffspriorisierung u.a., 2005
802.11f	Protokoll zwischen Access Points (Inter Access Point Protocol). Erlaubt Roaming zwischen AP´s verschiedener Hersteller.
802.11h	Ergänzung zu 802.11a: Für Europa zur Leistungsregelung und dynamische Frequenzselektion um Störungen ziviler Radar- und Navigationssysteme zu vermeiden, 2003
802.11i	Verbesserungen von 802.11 (WEP) betreffend Authentikation, Integrität, Verschlüsselung, 2004
802.11w	Erweiterung von 802.11i bezüglich der Authentizität und Integrität von Managementpaketen, 2008
802.11s	Funk-Paketübertragung über mehrere APs →2008 sogenannte Meshed Networks, man benötigt kein drahtgebundenes Distribution System mehr

[1)] ISM- Band (Industrial, Scientific, Medical), lizenzfreies Band, nutzbare Bandbreite länderspezifisch

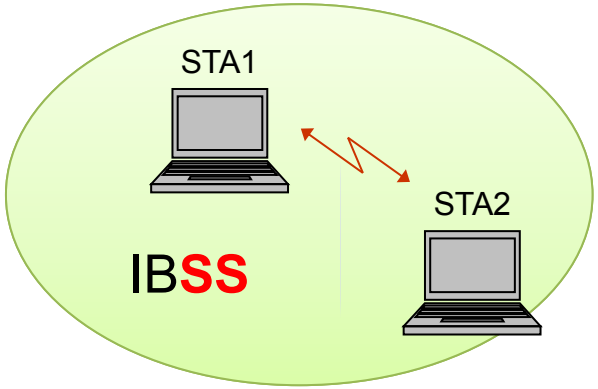
BSS (basic service set):

- **STA**s (stations) sind Mitglieder eines BSS.
- **AP**s (access points) realisieren die Kommunikation zwischen den STAs.
- BSS können räumlich entfernt sein, sich überlappen, oder überdecken.



IBSS (independent BSS):

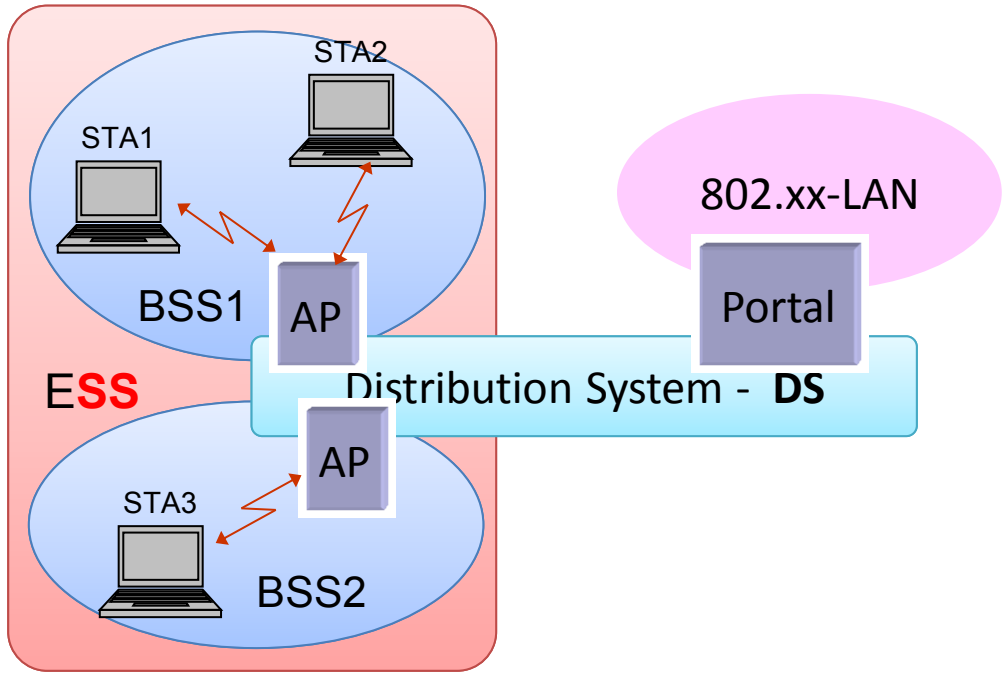
- **STA's** kommunizieren direkt miteinander.
- Eine STA übernimmt quasi "AP-Rolle".



ESS (extended service set):

- Bindung mehrer BSS über ein DS (distribution system).
- Das DS realisiert die Kommunikation zwischen APs, stellt Datenbasis für Roaming (welche STA ist über welchen AP erreichbar?).
- AP's nutzen zwei Medien: **WM** (wireless medium), **DSM** (distributed system medium) und verwenden dabei zwei verschiedene MAC-Adressen..

Portal realisiert Übergang zu anderen LAN-Typen



- **SSID, jeder Service Set (BSS, IBSS, ESS) hat einen Namen (OnAir, MeineFunke, …)**
  - Im Falle eines BSS, ESS wird dieser im AP, bzw. den AP's eingestellt.
  - Im Falle eines IBSS ist das der STA-Name.
  - Mittels SSID kann man WLAN-Netze unterscheiden und STAs können sich gezielt anmelden.

- **BSSID (Basic Service Set Identifier)**
  - Ein Access Point benötigt zwei MAC-Adressen.
  - eine auf der Funkseite zu den STA's: diese nennt man BSSID
  - eine auf der Infrastrukturseite, die auf dem sogenannten "distributed system medium" verwendet wird. →Verwendung der Adressen: siehe Folie.
  - Die Funk-MAC-Adresse ist eine lokal erzeugte, die zur Infrastrukturseite vom Hersteller festgelegt und programmiert.

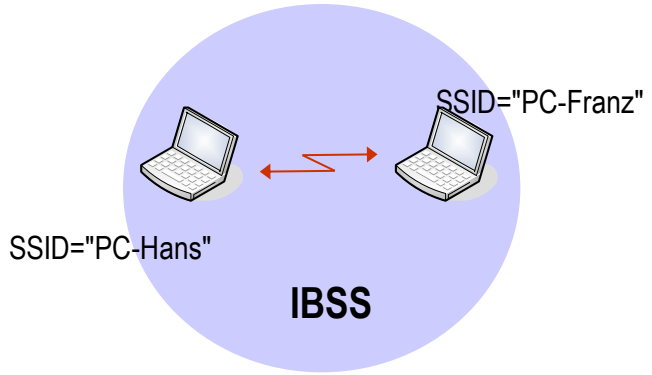
- **Beachte:**
  - SSID ist der Name von Funknetzen und selber wähl- und einstellbar.
  - BSSID ist eine lokal erzeugte MAC-Adresse, die ein AP auf der Funkseite zu Kommunikation verwendet.

Netzwerkname (SSID) /nach BSI2006/

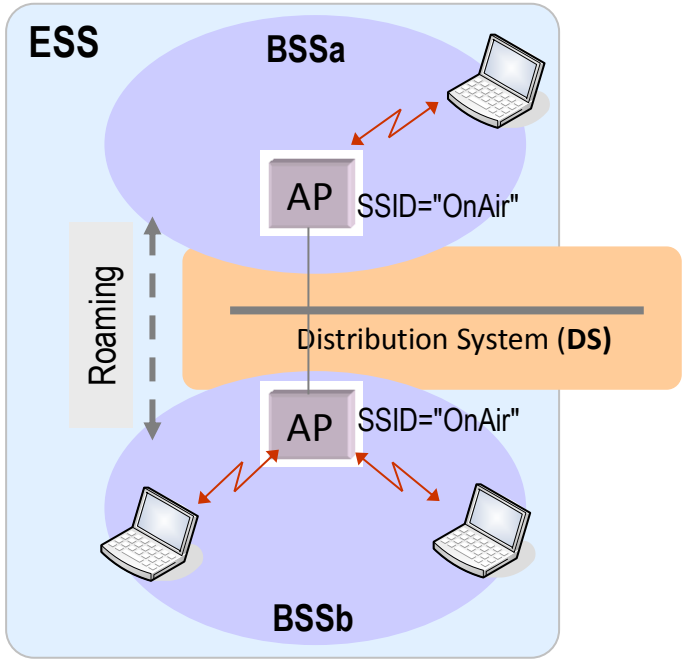
- Der Service Set Identifier (SSID) dient der Identifikation eines ESS, IBSS, BSS.
- Bei Anmeldung an einem WLAN, beim Handover zwischen zwei benachbarten Funkzellen dient der SSID dazu, den nächsten Access Point zu finden.
- Maximale SSID-Länge 32 Byte. Der SSID wird auf Client und Access Point konfiguriert.
- Die Client-Software unterstützt üblicherweise mehrere Profile, damit kann sich der Rechner automatisch z.B. zu Hause oder in der Firma anmelden, ohne das der Nutzer jedes mal den Funkadapter administrieren muss.

- Die Übertragung des SSID erfolgt auf Layer 2 als Parameter im Beacon Frame (Funkfeuer). Dieser Mechanismus wird auch als SSID-Broadcast bezeichnet.
- In dem Beacon Frame übermittelt ein Access Point oder eine STA neben dem SSID die wesentlichen Übertragungsparameter inklusive der Sicherheitseinstellungen, wie z.B. das zu verwendende Verschlüsselungsverfahren.
- Alternativ kann ein Client explizit erfragen, ob ein Access Point mit einem gewissen SSID erreichbar ist. Hierzu sendet der Client unter Angabe des gewünschten SSID ein spezielles Layer-2-Paket (Probe Request) und ein Access Point passender SSID antwortet mit einem Probe-Response-Paket. Verwendet der Client dabei den so genannten Broadcast SSID (ein SSID der Länge 0), bedeutet dies, dass der Client mit einem beliebigen Access Point kommunizieren möchte. Sofern es in der Konfiguration eines Access Point nicht unterdrückt wird, antwortet ein Access Point auf ein Probe Request mit Broadcast SSID durch ein Probe-Response-Paket mit dem SSID des Access Point.
- Für nicht-öffentliche WLAN sollte an einem Access Point die Antwort auf eine Anfrage mit Broadcast-SSID unterdrückt werden. Da der SSID unverschlüsselt gesendet wird, kann ein Angreifer ihn mit einfachen Mitteln in Erfahrung bringen.
- Einige Access Points bieten die Möglichkeit, die Aussendung des SSID im Funkfeuer zu unterbinden. Ein Client muss den SSID explizit erfragen.

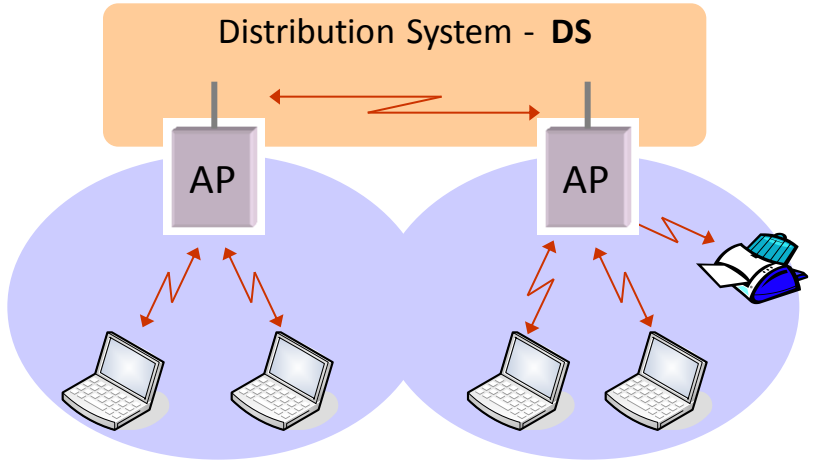
- Typ1: IBSS (auch ad-hoc-network, peer-to-peer (P2P)), 802.11/15
  - benötigen keine zusätzliche Infrastruktur, STA's kommunizieren direkt miteinander
  - Endgeräte müssen den Medienzugriff und Konfliktauflösung beherrschen



- Typ2: ESS (auch Infrastrukturnetz, Portable-to-fixed-Network), 802.11/16
  - ESS besteht aus mindestens zwei BSS.
  - STA´s kommunizieren über AP´s und das DS.
  - DS realisiert Mobilität der STA's.
  - Die Zusammenarbeit zwischen AP's über das DS wird durch IEEE-802.11f geregelt.

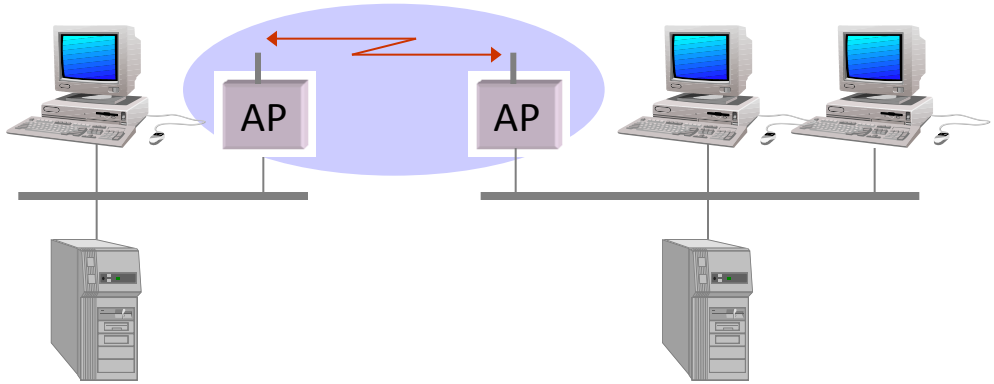


- Typ3: Funk-Infrastrukturnetze
  - Direkte Verbindung zwischen APs verschieder Hersteller →802.11f
  - Schneller und flexibler Aufbau von Netzen für Meetings
  - Access-Points relativ komplex durch zusätzliche Funktionalität (Bridge/Router, Roaming)



- Typ4: Funkverbindung zwischen Infrastrukturnetzen, 802.11/16
  - Verbindung drahtgebundener Netze über AP-Verbindung
  - über Richtantennen bis 5 km.
  - erspart kostenintensive und genehmigungspflichtige Kabelverlegung.

Funkverbindung zwischen Infrastrukturnetzen

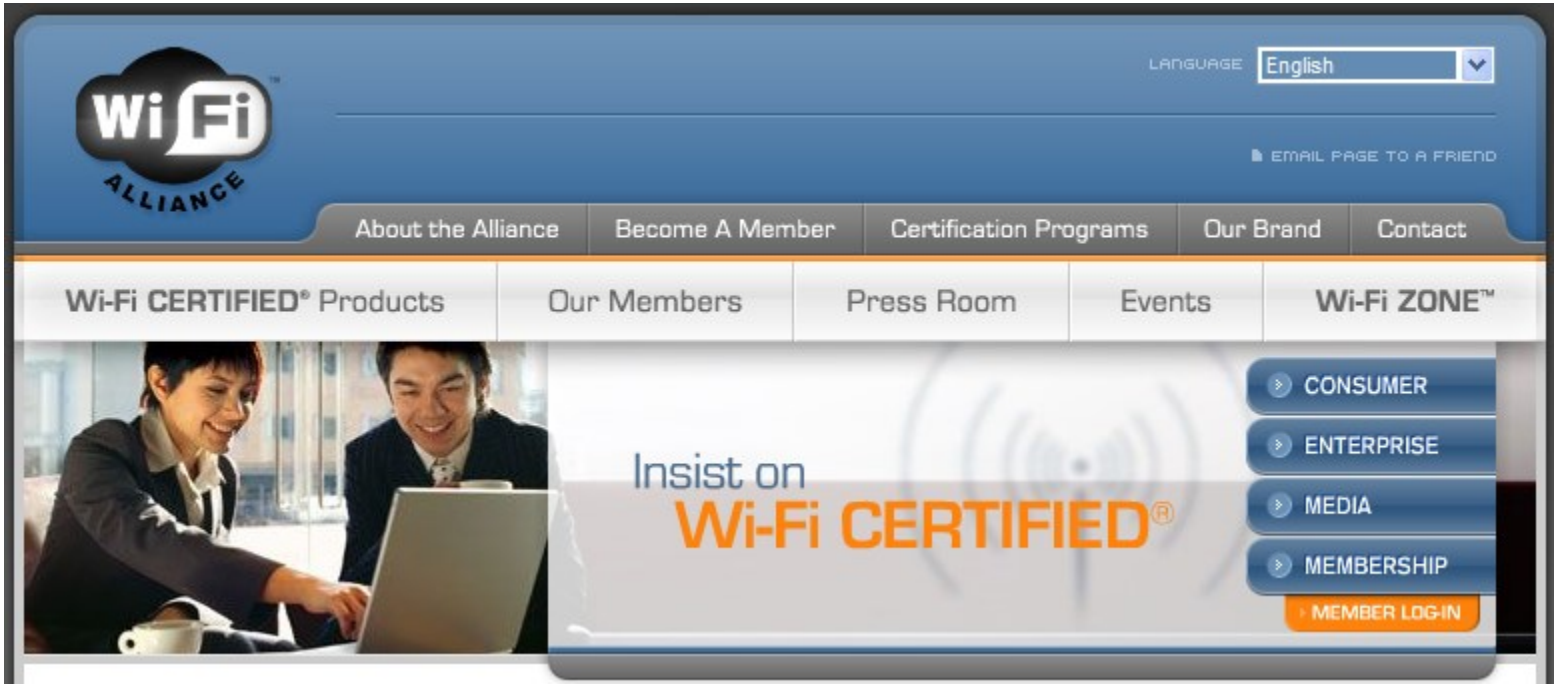


Technik: **Wireless Netzwerkadapter und Router**

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

- Netzwerkadapter gibt es als PCI-Karte, PC-Karte, mit USB-Anschluss.
- Router gibt es mit externen/internen Antennen.

Technik: **Wi-Fi** http://www.wi-fi.org/



The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification. Currently the Wi-Fi Alliance has 205 member companies from around the world, and 903 products have received Wi-Fi® certification since certification began in March of 2000. The goal of the Wi-Fi Alliance's members is to enhance the user experience through product interoperability.

Funk-Datenübertragung in WLANs hat u.a. zwei Probleme zu lösen:

(1) Vermeidung von Mehrfachzugriffskonflikten,

(2) Unterdrückung von Störquellen (in der Regel schmalbandig und kurzzeitig auftretend) und Mehrwegeausbreitung.

(1) Vermeidung von Mehrfachzugriffskonflikten

- Öffentliche Funknetze unterliegen einer Planung (Frequenznutzung, Ausleuchtung),
- WLAN's entstehen spontan →Mehrfachzugriffskonflikte auf Medium sind vorprogrammiert!
- Mehrfachzugriffskonflikte kann man regeln über:
  - TDMA (Time Division Multiple Access),
  - FDMA (Frequency Division MA),
  - CDMA (Code Division MA)
- In 802.11 werden FDMA- sowie FDMA/TDMA-Verfahren genutzt. →*siehe MAC-Schicht*

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

(2) Unterdrückung von (schmalbandigen, kurzzeitigen) Störungen durch Bandspreiztechniken.

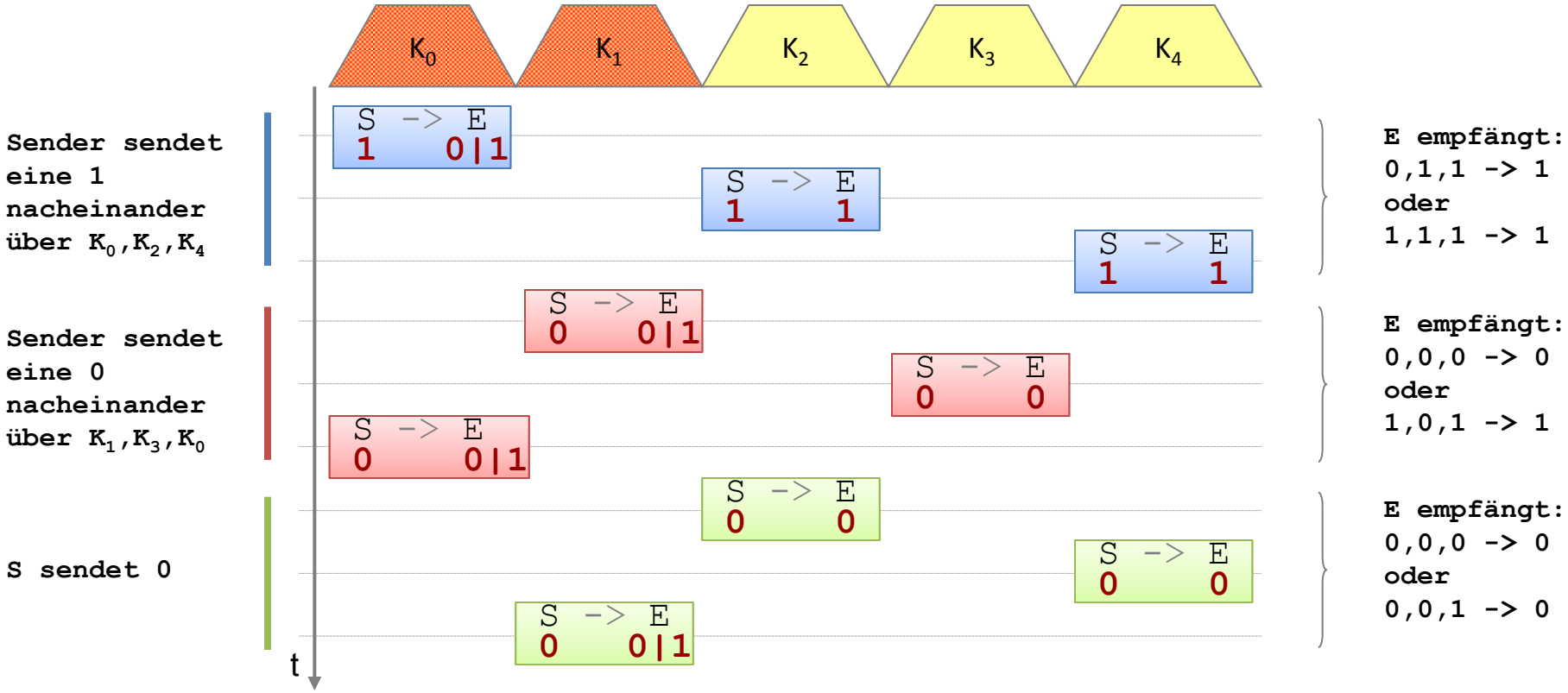
- Das “schmalbandige" Nutzsignal wird durch ein Spreiz-Spektrum-Verfahren (Spread Spectrum Technology) breitbandig gesendet.
- Das gespreizte Nutzsignal ist unempfindlicher gegen schmalbandige, kurzzeitige Störer.

- Verwendete Spreiztechniken in WLANs sind:
  - **FHSS** (Frequency Hopping Spread Spectrum) – Spreizung durch Frequenzsprungverfahren,
  - **DSSS** (Direct Sequence Spread Spectrum) – Spreizung mit fixen 11-stelligen Barkercode,
  - **CCK** (Complementary Code Keying) Spreizung mit 8-stelligen Code, ausgewählt aus einer Tabelle,
  - **OFDM** (Orthogonal Frequency Division Multiplexing) – Spreizung durch Aufteilung der Sendedaten auf mehrere orthogonale Teilbänder.

Bandspreiztechnik: **Störer mittels FHSS "unterdrücken"**

- Bei FHSS (Frequency Hopping Spread Spectrum) wird ein Bit über mehrere Funkkanälen übertragen. Man kann solange Daten übertragen, wie gilt: *Anzahl gestörter Kanäle < Anzahl ungestörter Kanäle*
- **Bsp.**: Ein FHSS-System nutze 5 disjunkte Frequenzkanäle K_0 …K_4. Jedes Bit werde über drei verschiedene Kanäle übertragen. Die Kanäle ***K_0 und K_1 seien gestört***. Die Kanalnutzung beginne mit K_0 und ergebe sich aus:

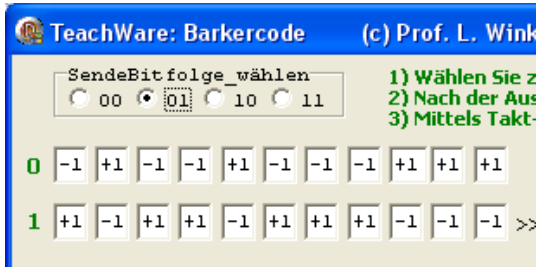
$$K_{t+1} = \mathrm{mod}_5(K_t + 2) = K_0, K_2, K_4, K_1, K_3, K_0, \ldots$$

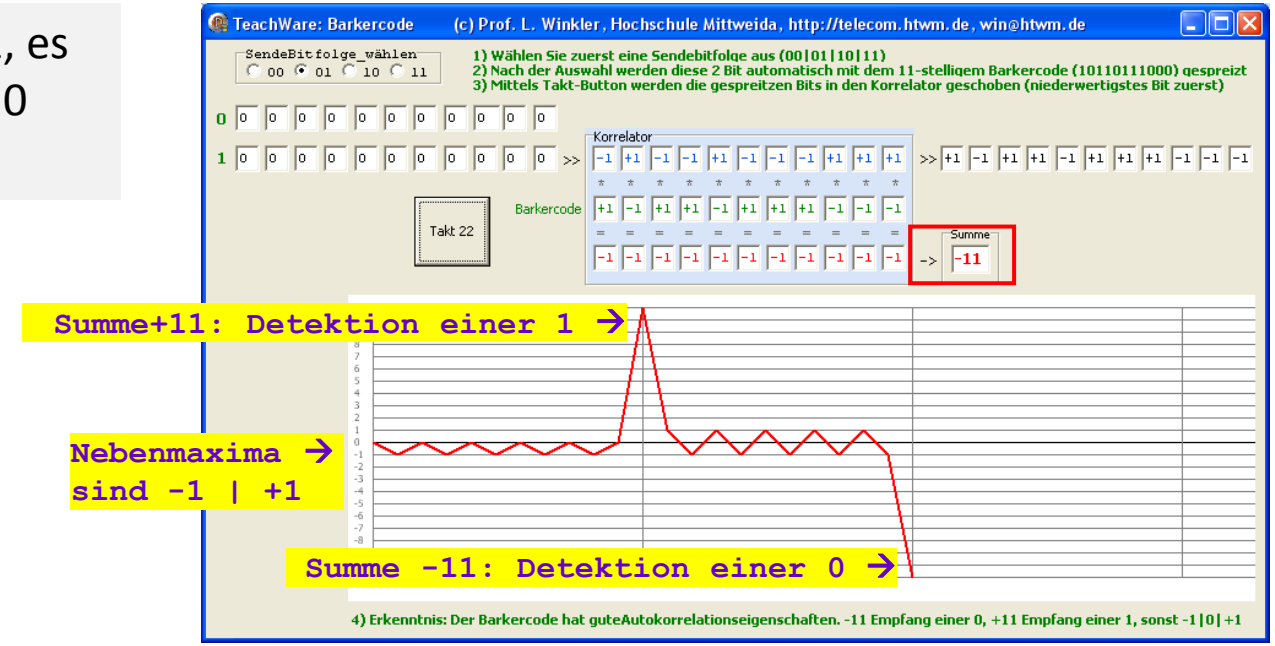


Bandspreiztechnik: **Störer mittels DSSS "unterdrücken"**

- Bei DSSS wird ein Bit mittels eines Chipcodes codiert (gespreizt). Verwendet man z.B. einen 11-stelligen Chipcode, sendet man pro Bit (0|1) 11 Bit. Dazu benötigt man aber auch die 11-fache Bandbreite.
- Wie DSSS funktioniert, soll anhand der Teachware "Barkercode" ermittelt werden. Laden und starten Sie:
  https://www.telecom.hs-mittweida.de/fileadmin/verzeichnisfreigaben/telecom/winkler/teachware/barkercode.exe

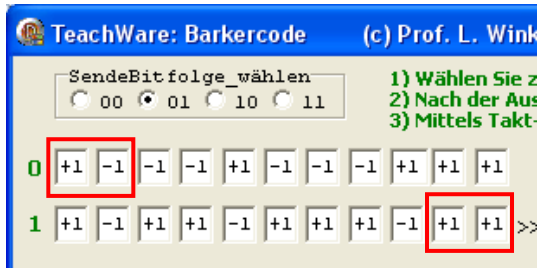
- Wählen Sie Sendebitfolge 01, es wird erst die 1 und dann die 0 gespreizt gesendet.

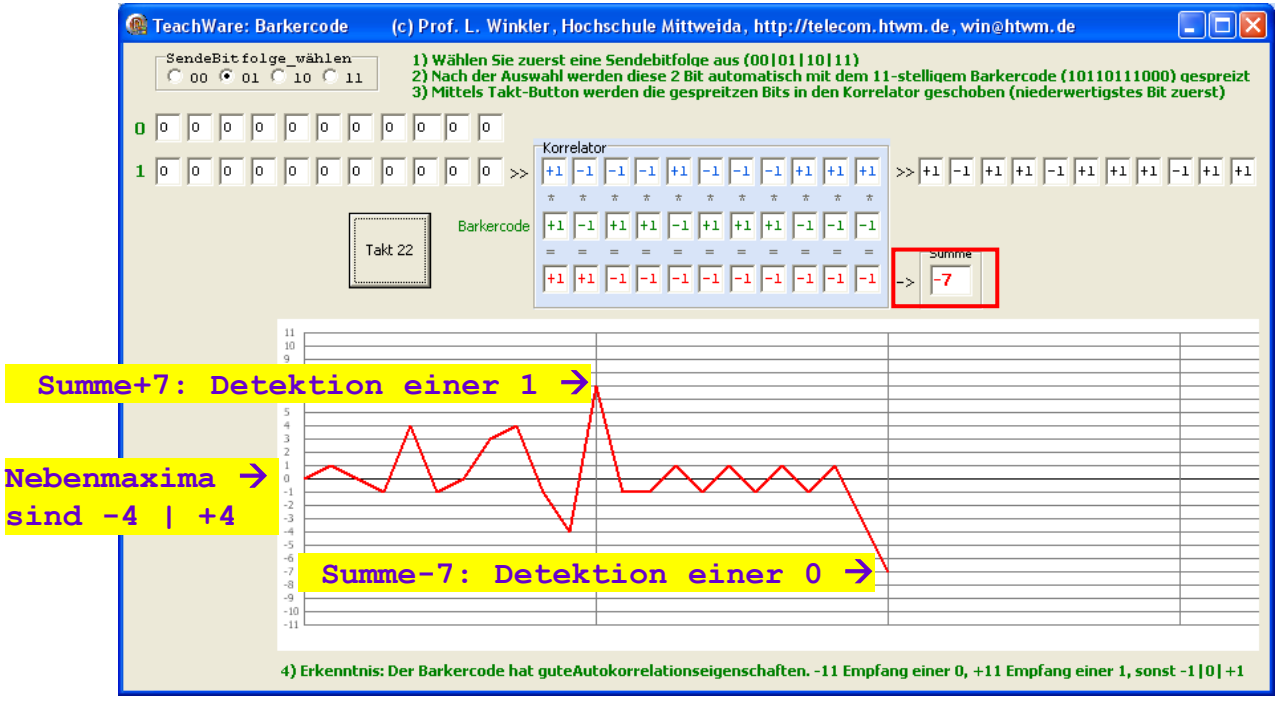




Bandspreiztechnik: **Störer mittels DSSS "unterdrücken"**

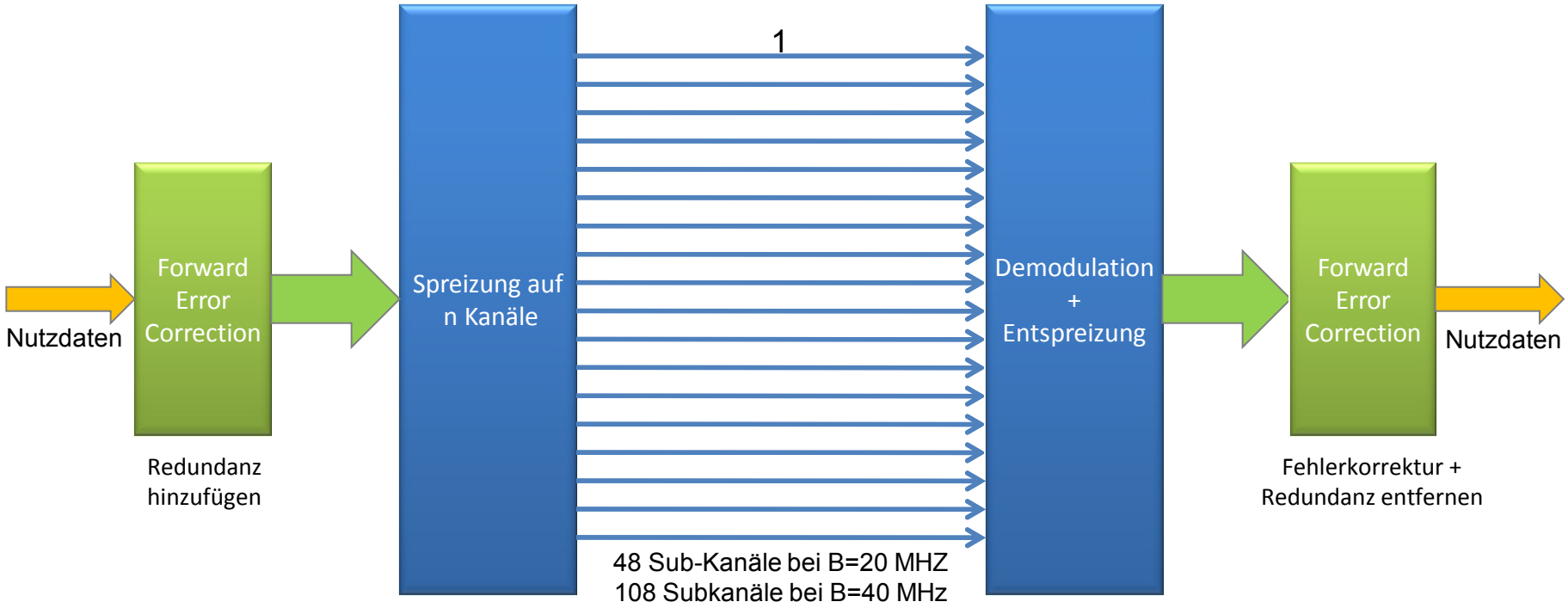
- Wählen Sie wieder die Sendebitfolge 01. In jeder Spreizfolge werden jetzt aber 2 Bit verfälscht (Kurzzeitstörung)



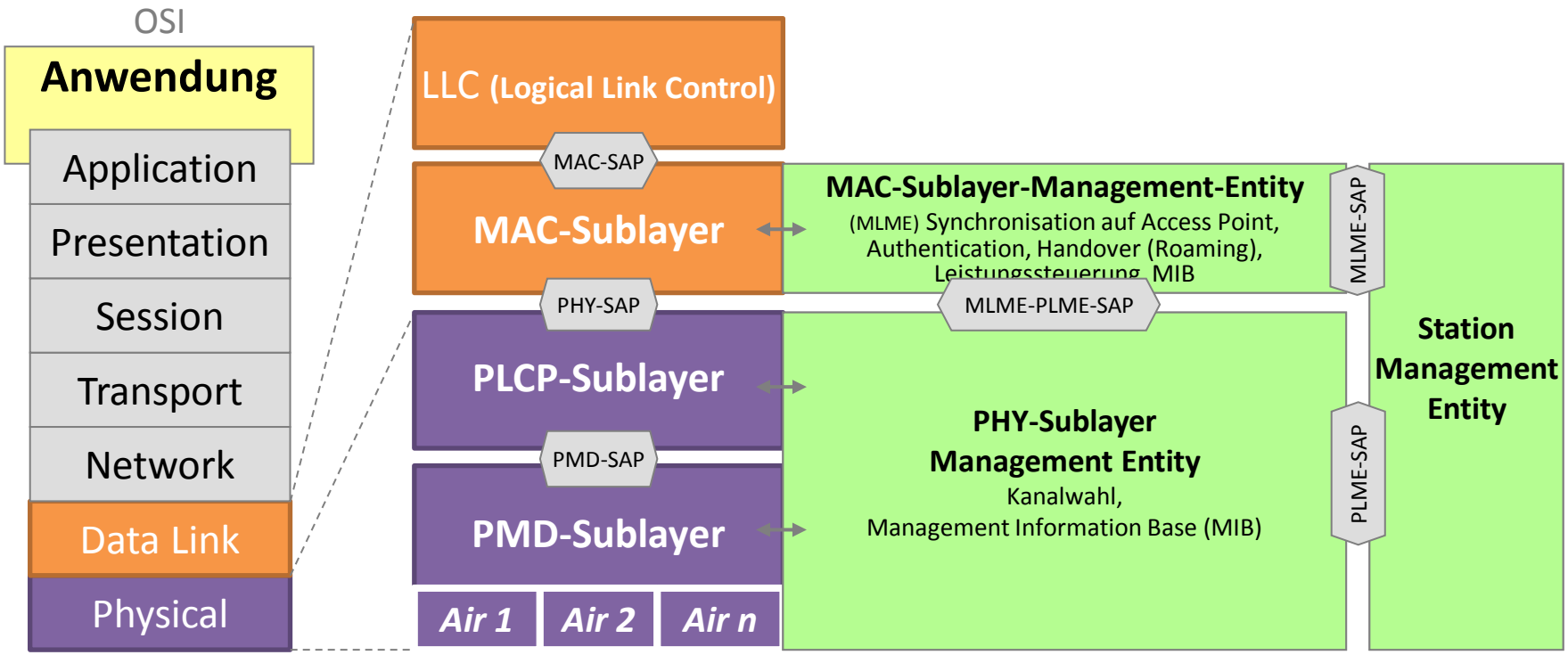


Bandspreiztechnik: **Störer mittels OFDM "unterdrücken"**

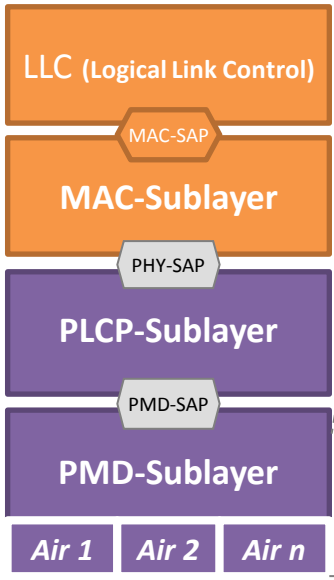
- Bei OFDM (orthogonal frequency division multiplexing) wird ein serieller Bitstrom auf n parallele Träger gespreizt.
  - Dadurch vermindert sich die Schrittgeschwindigkeit, d.h. die Symboldauer ist groß, wodurch kurzzeitige Störungen und Mehrwegeausbreitung beherrschbar werden.
  - Durch eine Vorwärtsfehlerkorrektur-Kanalcodierung des Nutzdatenstrom wird zusätzlich eine Fehlerkorrektur möglich.



- MAC: Medienzugriffssteuerung, Fragmentierung, Verschlüsselung,
- PLCP (Physical Layer Convergence Protocol): stellt MAC ein einheitliches Interface bereit:
  - Verdeckt die verschiedenen Spreiz- und Modulationsverfahren,
  - liefert CCA (Clear Channel Assessment (Bescheid, Benachrichtigung)).
- PMD (Physical Media Dependent) Modulation, Demodulation.



IEEE802.11-PHY: **Datenraten, Medien, Modulationsverfahren**



Mbps	802.11 2,4 –GHz-Band B=22MHz		802.11.b 2,4-GHz-Band B=22MHz	802.11.a 5,2-GHz-Band B=20 MHz	802.11.g 2,4-GHz-Band B=20 MHz
1	FHSS	DSSS/BPSK			
2	FHSS	DSSS/QPSK			
5,5			CCK/QPSK		
6				OFDM/BPSK	OFDM/BPSK
9				OFDM/BPSK	OFDM/BPSK
11			CCK/QPSK		
12				OFDM/QPSK	OFDM/QPSK
16				OFDM/QPSK	OFDM/QPSK
24				OFDM/16-QAM	OFDM/16-QAM
36				OFDM/16-QAM	OFDM/16-QAM
48				OFDM/64-QAM	OFDM/64-QAM
54				OFDM/64-QAM	OFDM/64-QAM

Spreizverfahren:
CCK - Complementary Code Keying
DSSS - Direct Sequence Spread Spectrum,
FHSS - Frequency Hopping Spread Spectrum,
OFDM - Orthogonal Frequency Division Multiplexing

Modulationsverfahren:
BPSK - Binary Phase Shift Keying
QPSK- Quadrature Phase Shift Keying
QAM - Quadrature Amplitude Modulation

IEEE802.11-PHY: **Frequenzbereiche in DE für WLANs**

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

- Frequenzbereiche werden durch die Bundesnetzagentur festgelegt.
- Es erfolgt eine Allgemeinzuteilung.
  Bisher wurden 2 Frequenzbereiche freigegeben:
  - **WLAN 2,4 GHz** Allgemeinzuteilung
    Frequenzbereich 2400,0 - 2483,5 MHz
  - **WLAN 5 GHz** Allgemeinzuteilung
    Frequenzbereichen 5150 MHz - 5350 MHz und 5470 MHz - 5725 MHz

- WLAN-Funkanwendungen können ohne Antrag und förmliche Genehmigung auf diesen Frequenzen genutzt werden.
- Bei privater oder firmeninterner Nutzung entstehen dem Anwender durch die Frequenznutzung keine Kosten in Form von Gebühren und Beiträgen.
- Mit WLAN Funkverbindungen dürfen Grundstücke miteinander verbunden werden.
- Es ist keine bestimmte Reichweite vorgeschrieben. Diese wird ausschließlich durch die maximale Strahlungsleistung der Funkanlage bestimmt.
- Die maximale Strahlungsleistung EIRP[1)] wird für Teilbänder länderspezifisch festgelegt.

1) Die EIRP (Equivalent Isotropic Radiated Power) gibt an, mit welcher Sendeleistung man einen isotropen (richtungsunabhängigen) Kugelstrahler speisen müsste, um im Fernfeld dieselbe Leistungsflussdichte zu erreichen wie mit einer bündelnden Richtantenne in ihrer Hauptsenderichtung.

IEEE802.11-PHY: **2,4-GHz-Band**

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

- ISM-Band (Industrial, Scientific, Medical)
  - lizenzfreies, gebührenfreies Band,
  - unterschiedliche Bandbreite und zulässige Sendeleistung,
  - für WLAN wird genutzt:

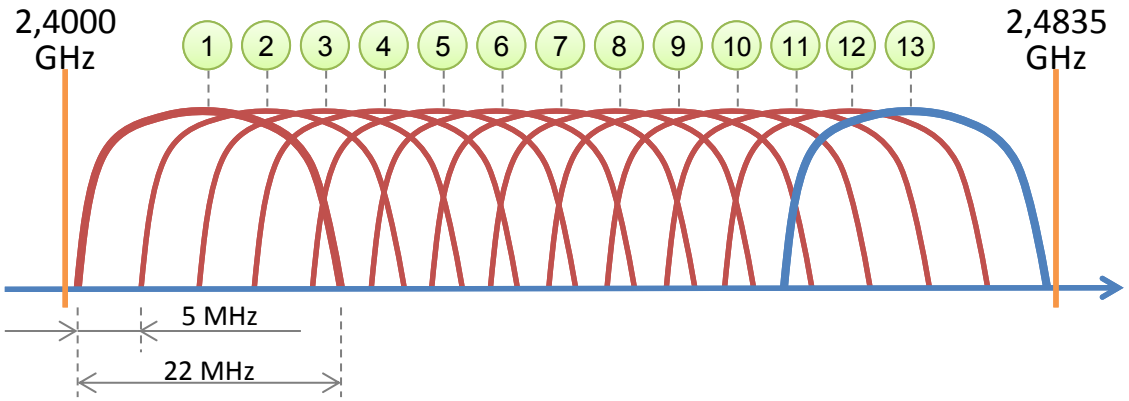
Region	Frequenzbereich GHz	B in MHz	1-MHz-Bereiche bei FHSS	Max. Sendeleistung
USA	2,4000-2,4835	83,5	79	1000 mW
Deutschland	2,4000-2,4835	83,5	79	100 mW
Japan	2,4710-2,4970	26,0	23	100 mW
Frankreich	2,4465-2,4835	47,0	27	100 mW
Spanien	2,4450-2,4750	30,0	35	100 mW

- ISM-Band-Nutzung:
  - 802.11**b**: Kanäle mit einer Bandbreite von 22 MHz,
  - 802.11**g**: Kanäle mit einer Bandbreite von 20 MHz,
  - 802.11**n**: Kanäle mit einer Bandbreite von 40 MHz.

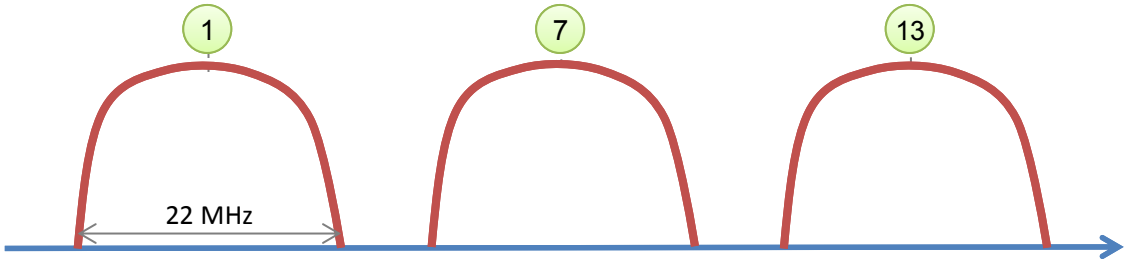
IEEE802.11-PHY: 2,4-GHz-Band-Nutzung bei →802.11 b

- **802.11**: Im Band von 2,4-2,4835 GHz werden in Europa 13 Kanäle gebildet. Deren Mittenfrequenzen in GHz:

  2,412 Kanal 1
  +0,005 = **2,417** Kanal 2
  +0,005 = **2,422** Kanal 3
  …
  2,472 Kanal 13



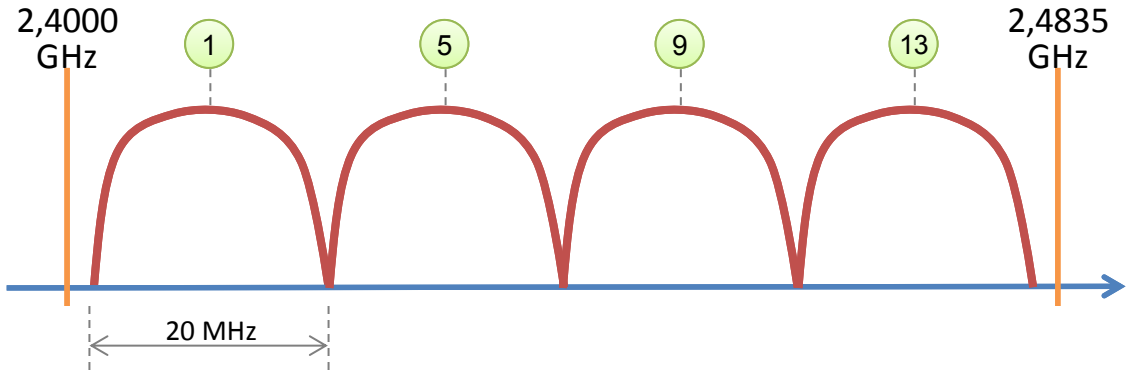
- **802.11b-Nutzung**: In Europa[1)] sollen die Mittenfrequenzen der genutzten Kanäle 30 MHz auseinanderliegen. Das sind die Kanäle **1, 7, 13**.
- Mittenfrequenzabstand USA →25 MHz. Damit gilt für die USA:
  (1, 6, 11) | (2, 7, 12) | (3, 8, 13)



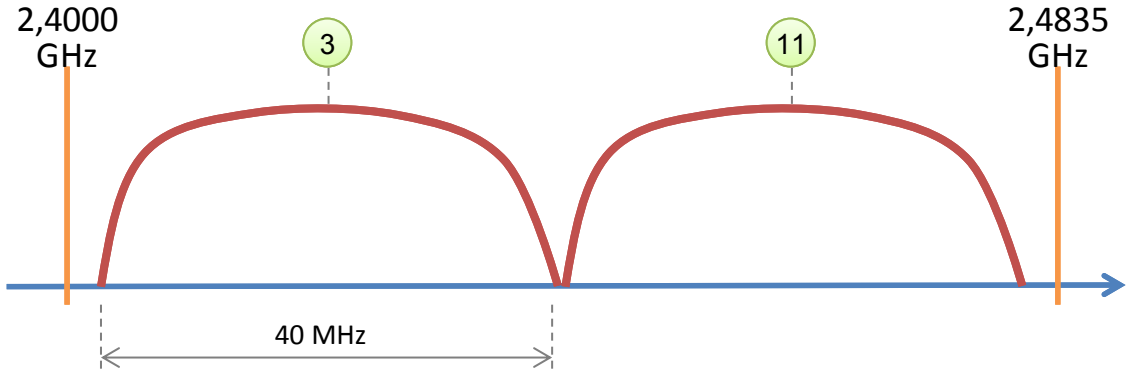
[1)] außer Frankreich und Spanien

IEEE802.11-PHY: **2,4-GHz-Band-Nutzung bei →802.11g,n**

- **802.11g,n-Nutzung**:
  OFDM bei einer Kanalbandbreite von **20 MHz**.
  Damit kann man im europäischen ISM-Band 4 disjunkte Kanäle bilden, mit den Mittenfrequenzen:
  2,412, 2432, 2452, 2472 GHz.



- **802.11g,n-Nutzung**:
  OFDM bei einer Kanalbandbreite von **40 MHz**.
  Damit kann man im europäischen ISM-Band 2 disjunkte Kanäle bilden mit den Mittenfrequenzen:
  2,422 GHz, 2462 GHz.



IEEE802.11-PHY: **Das 5,2-GHz-Band**

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

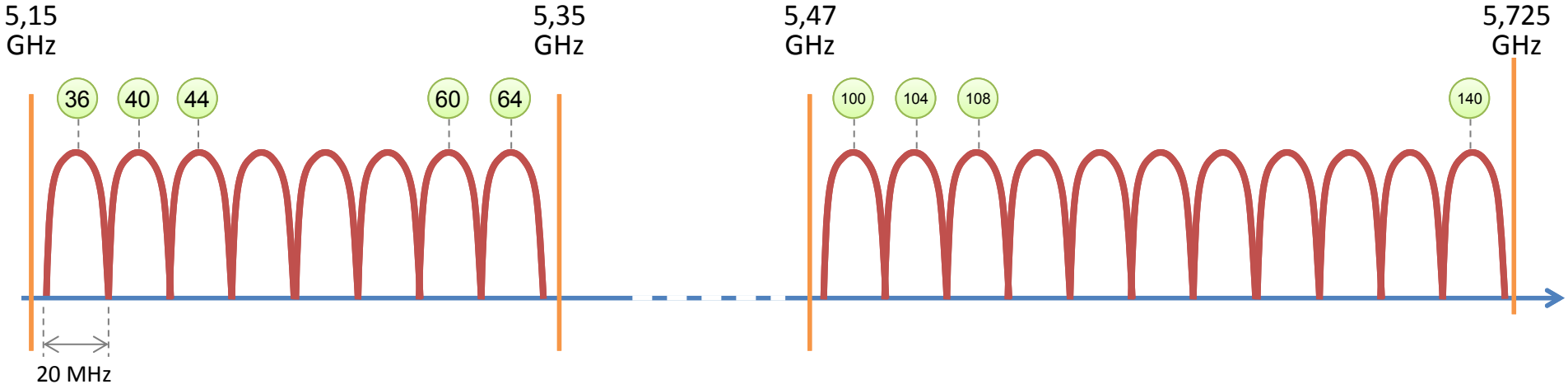
- Weiteres lizenzfreies Band, unterschiedliche B und Sendeleistungen.
  - Kanalraster im Abstand von →20MHz, Kanalbandbreite → 20MHz
  - Kanalraster im Abstand von →40MHz, Kanalbandbreite → 40MHz
  - Sendeleistungen von 50mW bis 4W

Region	Frequenzbereich GHz	B in MHz	Kanäle mit je 20 MHz	Max. Sendeleistung für (innen/außen)
USA	5,150 - 5,250	100	1 - 4	50/200 mW (innen/außen)
	5,250 - 5,350	100	5 - 8	250/1000 mW (innen/außen)
	5,725 - 5,825	100	9 - 12	1000/4000 mW (innen/außen)
Deutschland	5,150 - 5,350	200	1 - 8	200 mW (Nutzung nur innen erlaubt)
	5,470 - 5,725	255	9 -19	1000 mW (innen/außen)

- **Im 5-GHz-Band**
  werden bei 802.11a in DE 19 Kanäle mit einer Bandbreite von 20 MHz genutzt.
  Diese Kanäle sind nicht überlappend !!!

IEEE802.11-PHY: Das 5,2-GHz-Band-Nutzung in Europa 802.11h

- Europa: 5,2-GHz-Bandes wird auch für andere Zwecke[1)] genutzt. Deshalb 802.11h:
  - DFS (Dynamic Frequency Selektion): WLAN-Systeme müssen z.B. Radarsignale erkennen und bei Bedarf einen Kanalwechsel durchführen.
  - TCP (Transmitter Power Control): STAs senden Empfangsreport an AP, dieser entscheidet über Sendeleistungsanpassung. AP misst Empfangsleistung/Bitfehlerrate von STAs und sendet ggf. ein Power Control Command.

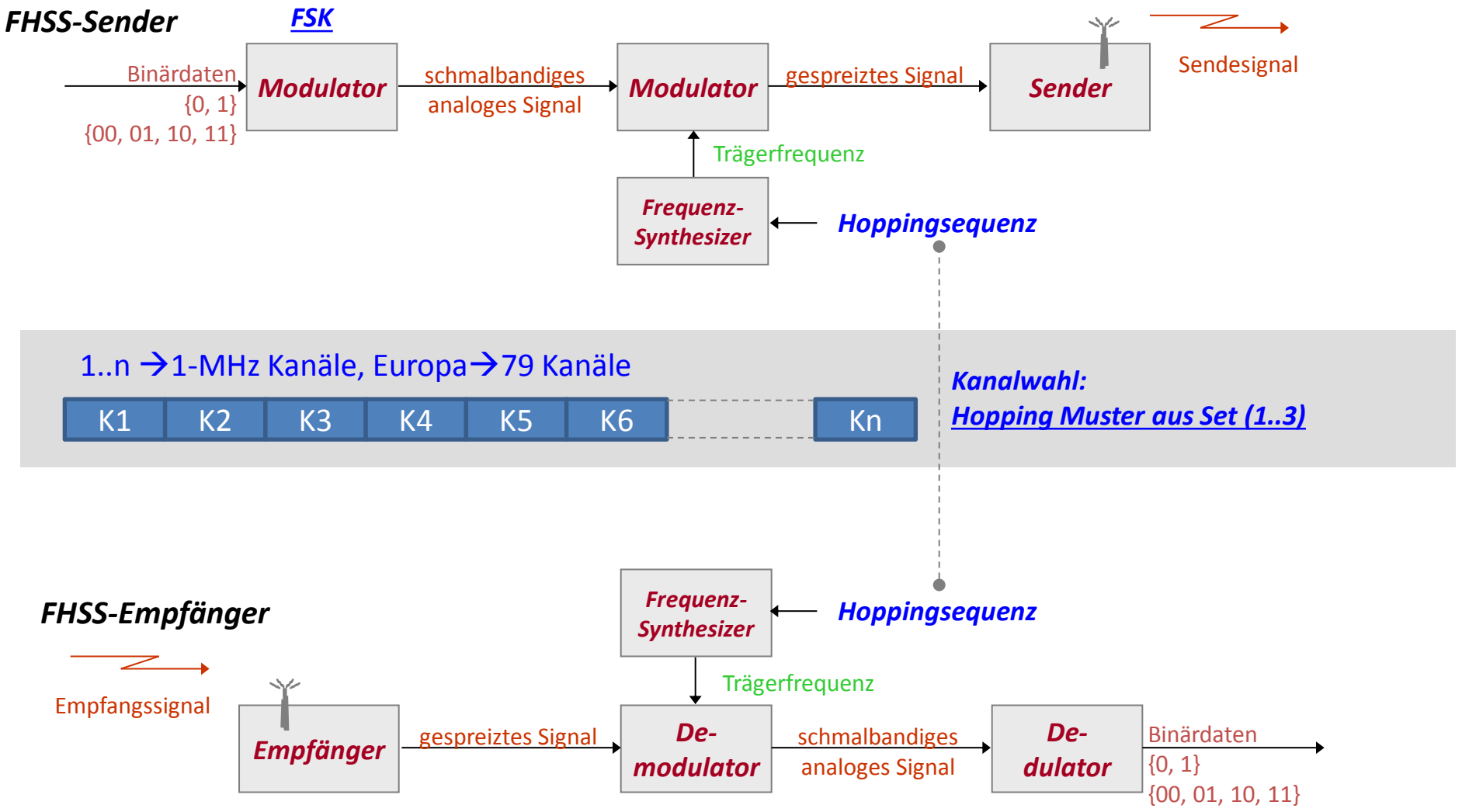


Nutzung innen				Nutzung innen mit DFS und TPC			
200 mW							
Mittenfrequenzen in GHz							
5,18	5,20	5,22	5,24				5,32

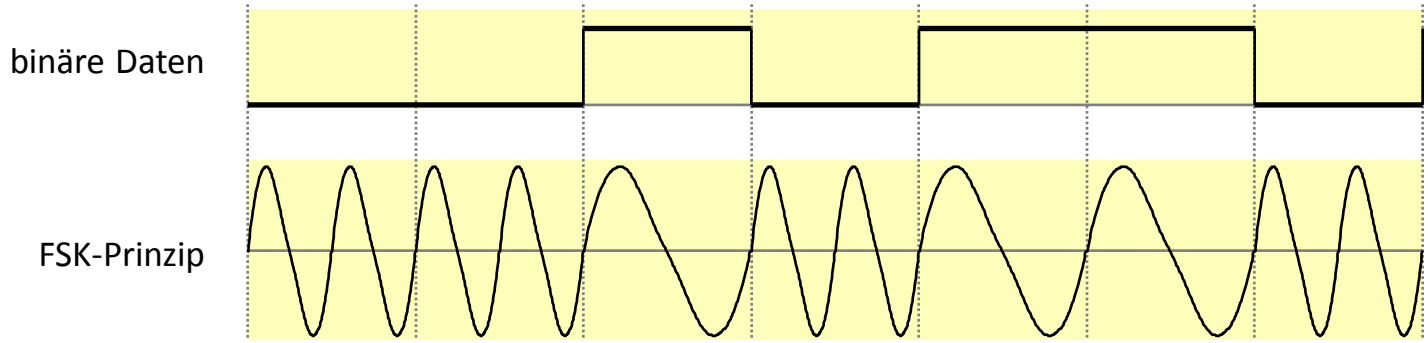
Nutzung innen und außen mit DFS und TPC										
1000 mW										
Mittenfrequenzen in GHz										
5,50	5,52	5,54							5,68	5,70

[1)] Militär, Satellitenfunk usw.

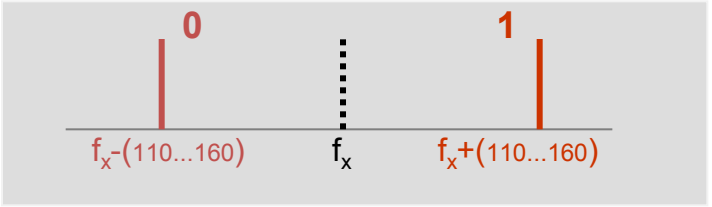
IEEE802.11-PHY: FHSS - Sender-Empfänger-Prinzip

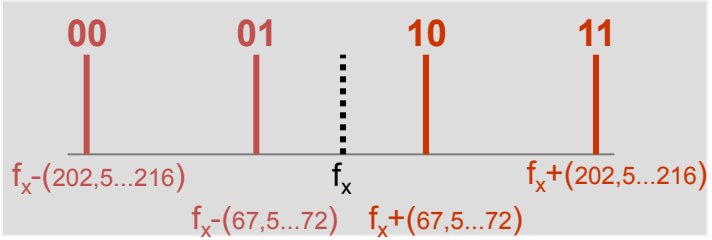


- FHSS verwendet FSK[1)], mit einer Schrittgeschwindigkeit Vs=1 MBaud.



- 2 Übertragungsraten:
  - 1 Mbit/s: es wird 1 Bit/Schritt übertragen,
    - (0)B → Mittenfrequenz−110...160 kHz
    - (1)B → Mittenfrequenz+110...160 kHz
  - 2 Mbit/s: es werden 2 Bit/Schritt übertragen.
    - (00)B → Mittenfrequenz−202,5...216 kHz
    - (01)B → Mittenfrequenz− 67,5... 72 kHz
    - (11)B → Mittenfrequenz+ 202,5...216 kHz
    - (10)B → Mittenfrequenz+ 67,5... 72 kHz





[1)]FSK – Frequency Shift Keying

IEEE802.11-PHY: **FHSS - Hopping**

- Aufteilung der Bandbreite in bis zu 79 1-MHz-Bereiche (DE, USA). Diese bilden DÜ-Kanäle, nummeriert von 2 bis 80. → Bei weniger B, weniger Kanäle.
  - Kanal-2-Mittenfrequenz: 2,402 GHz, Kanal-80-Mittenfrequenz: 2,480 GHz.
  - Ein Rufkanal dient zum Verbindungsaufbau. Nachdem ein Verbindungswunsch erkannt wurde, legt die Basisstation die Sprungsequenz fest.
  - Hopping-Sequenz: Sender und Empfänger springen synchron von Kanal zu Kanal:
  - Kanalnutzungsdauer max. 400 ms,
  - Sprungabstand: mind. 6 MHz.
- → 3 Hopping-Sets (26-stelliges Muster) wurden festgelegt:

Set	x-Werte
1	{0,3,6, 9,12,...,69,72,75}
2	{1,4,7,10,13,...,70,73,76}
3	{2,5,8,11,14,...,71,74,77}

IEEE802.11

- Jeder Sender/Empfänger nutzt aus einem der drei Sets ein Hopping-Muster:
  - Set 1, Muster 0; Set 1, Muster 3; ...;Set 3, Muster 77.
- Mithin gibt es 78 verschiedene Muster. Nur FHSS-Systeme, die das gleiche Muster verwenden, können Daten austauschen.

IEEE802.11-PHY: **FHSS - Hopping-Sequenztabelle, Berechnung**

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

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

Table 42, IEEE 802.11

fx (i) = [b(i) + x] mod (79) + 2	in North America and most of Europe, with b(i) defined in Table 42 (IEEE 802.11).
fx (i) = [b(i) + x] mod (27) + 47	in Spain with b(i) defined in Table 43 (IEEE 802.11).
fx (i) = [b(i) + x] mod (35) + 48	in France with b(i) defined in Table 44 (IEEE 802.11).

IEEE802.11-PHY: FHSS - Hopping: Berechnung der Sequenz

- Welche Kanäle das sind, berechnet sich aus:

$$f_x(i) = (b(i) + x) \bmod 79 + 2$$

x	verwendetes Hopping-Muster aus Set 1 bis 3
i	aktueller Schritt im Bereich von 1 bis 79
b(i)	Pseudo-Zufallswert aus Tabelle 42 (IEEE 802.11)

- **Beispiel 1**
  Set 1, Muster 0,
  die ersten 3 benutzten Kanäle:

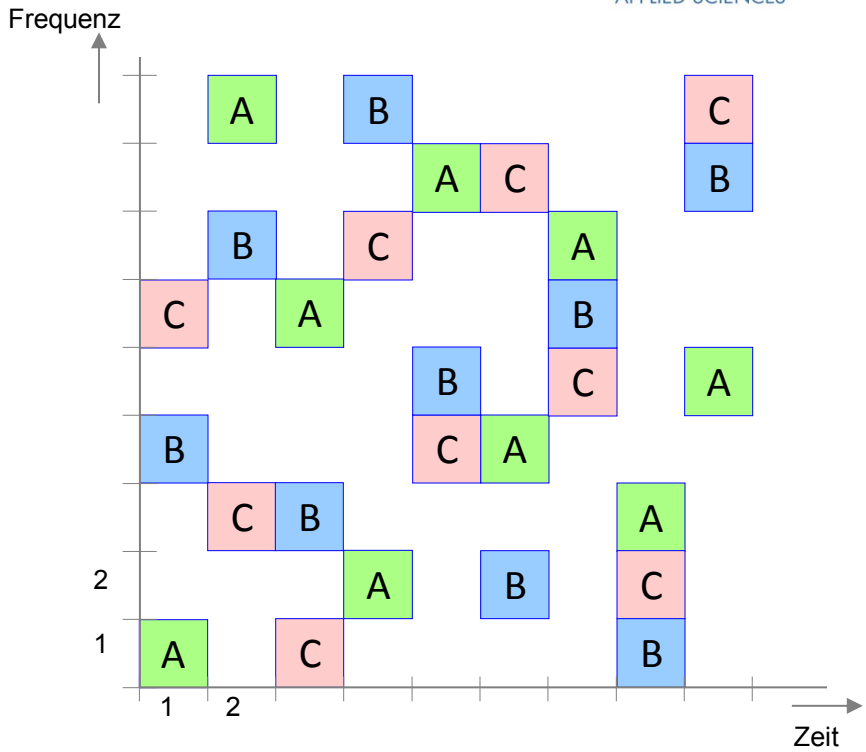
i	$f_x(i) = (b(i)+x) \bmod 79 + 2$
1	$f_0(1) = (0 + 0) \bmod 79 + 2 = 2$
2	$f_0(2) = (23 + 0) \bmod 79 + 2 = 25$
3	$f_0(3) = (62 + 0) \bmod 79 + 2 = 64$

- **Beispiel 2**
  Set 3, Muster 77,
  die ersten 3 benutzten Kanäle:

i	$f_x(i) = (b(i)+x) \bmod 79 + 2$
1	$f_{77}(1) = (0 + 77) \bmod 79 + 2 = 79$
2	$f_{77}(2) = (23 + 77) \bmod 79 + 2 = 23$
3	$f_{77}(3) = (62 + 77) \bmod 79 + 2 = 62$

IEEE802.11-PHY: **FHSS - Hopping**

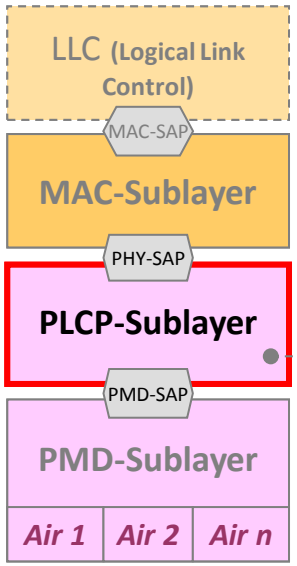
- Mehrfachzugriff (Multiple Access):
  - gemischtes FDMA-TDMA-Verfahren.
  - Jeder Sender benutzt ein, von den anderen disjunktes Frequenzsprungmuster.
  - Dieses Muster wird mit den Empfängern abgestimmt.
- Wenn alle Stationen exakt zeitsynchron wären
  - könnten 79 Sender-Empfänger-Relationen innerhalb eines Empfangsbereiches störungsfrei arbeiten.
  - Es gäbe nie zwei oder mehr Stationen, die die gleiche Frequenz benützten.



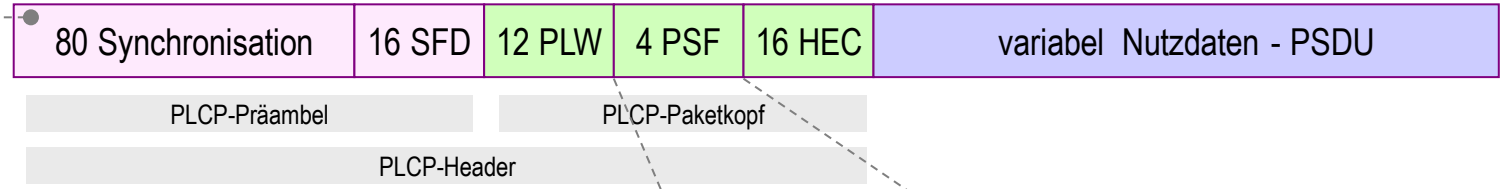
Konfliktfreies Frequenzsprungmuster am Beispiel von 3 Stationen

- Da aber keine Zeitsynchronisation besteht, treten Kollisionen auf. Die Kollisionshäufigkeit hängt von der Anzahl gleichzeitig arbeitender FHSS-Systeme im gleichen geografischen Gebiet ab.
- FHSS soll hinreichend funktionieren, wenn **nicht mehr als 13 Systeme** im gleichen Empfangsbereich arbeiten.

IEEE802.11-PHY: **FHSS - Schicht-1-Rahmen (PPDU)**



- Rahmenstruktur:
  - SFD – Start Frame Delimiter (0000 1100 1011 1101),
  - PLW – PLCP-PDU Length Word (0 bis 4095) $(000)_H$ bis $(FFF)_H$,
  - PSF – PLCP Signalling Field (Datenrate für PSDU)[1)],
  - HEC – Header Error Check,

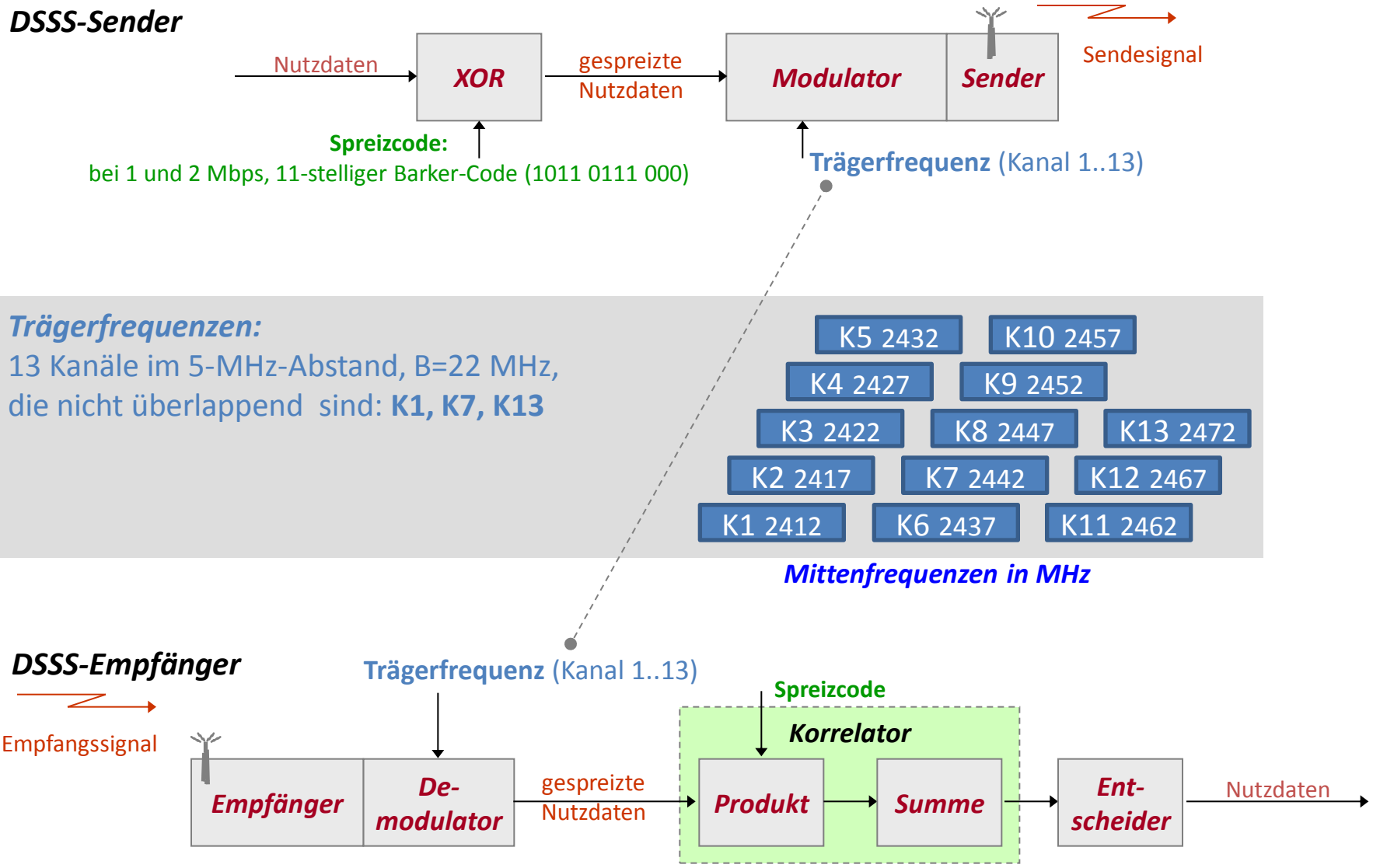


- 1)Der PLCP-Header wird immer mit 1 Mbit/s gesendet → im Header steht Geschwindigkeit mit der dann die PSDU gesendet wird. 8 $V_ü$ sind standardisiert, es werden aber nur 1 oder 2 Mbit/s verwendet

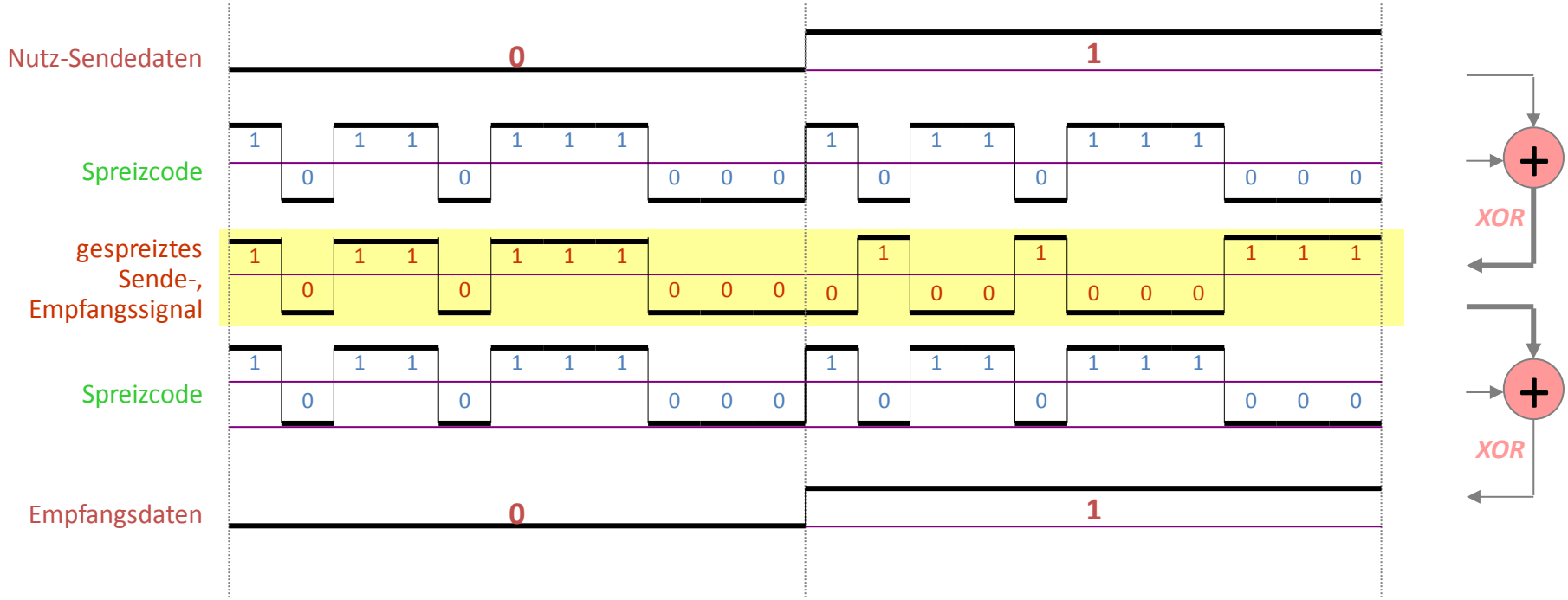
Bit 3	Bit 2	Bit 1	Bit 0	Datenrate Mbit/s
0	0	0	0	1,0
0	0	0	1	1,5
0	0	1	0	2,0
0	0	1	1	2,5
0	1	0	0	3,0
0	1	0	1	3,5
0	1	1	0	4,0
0	1	1	1	4,5

PLCP - Physical Layer Convergence Protocol
PMD - Physical Media Dependent

IEEE802.11-PHY: DSSS - Sender-Empfänger-Prinzip



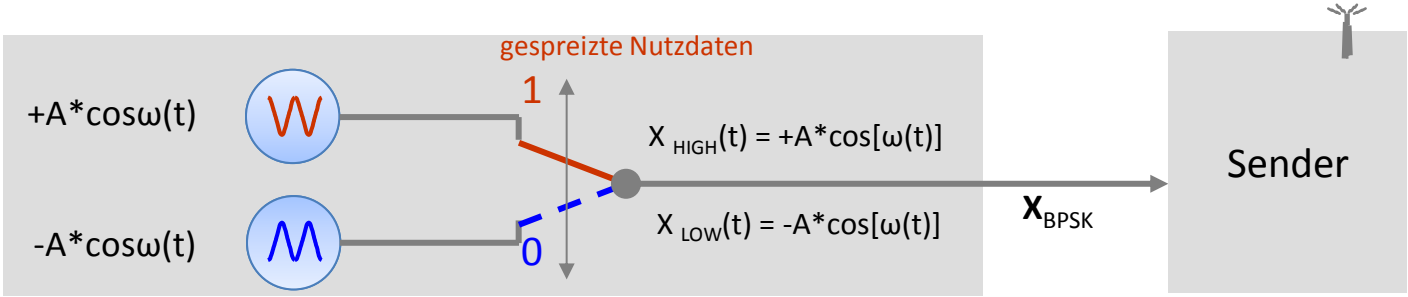
- Nutzdaten werden mit feststehendem Chipcode gespreizt[1)]
  - Für 1 und 2 Mbps kommt der **Barkercode mit 11 Chips** zur Anwendung.
  - Barkercode: (1 0 1 1 0 1 1 1 0 0 0)$_B$
  - **So wird eine 1 gesendet** (+1,−1,+1,+1,−1,+1,+1,+1,−1,−1,−1)
  - **So wird eine 0 gesendet** (−1,+1,−1,−1,+1,−1,−1,−1,+1,+1,+1)

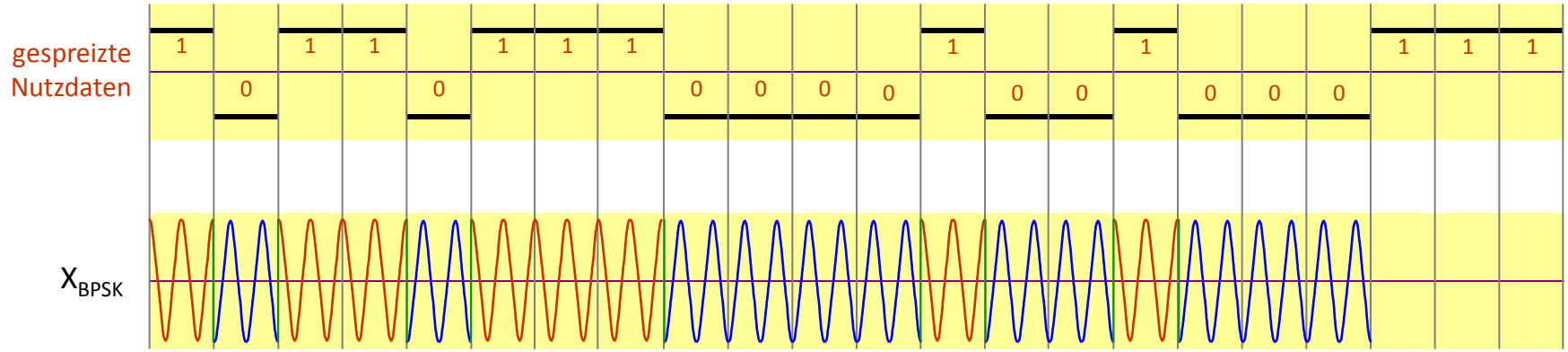


[1)] Spreizfaktoren von 10-100 (normale Anwendungen) bis 10000 (Militär), Spreizfaktor s= tb/ts , (tb ist die Bitdauer des Nutzsignals, ts ist die Bitdauer des Spreizsignals), Bandbreite des gespreizten Signals ist s-mal größer als die des Nutzsignals

- Schrittgeschwindigkeit Vs = 11 MBd.
- **Durch** die **Spreizung** erhält man:
  - bei **$V_ü$ = 1 Mbps → 11 Mbps**, Modulationsverfahren BPSK (Binary Phase Shift Keying),
  - bei **$V_ü$ = 2 Mbps → 22 Mbps**, Modulationsverfahren QPSK (Quadrature Phase Shift Keying).

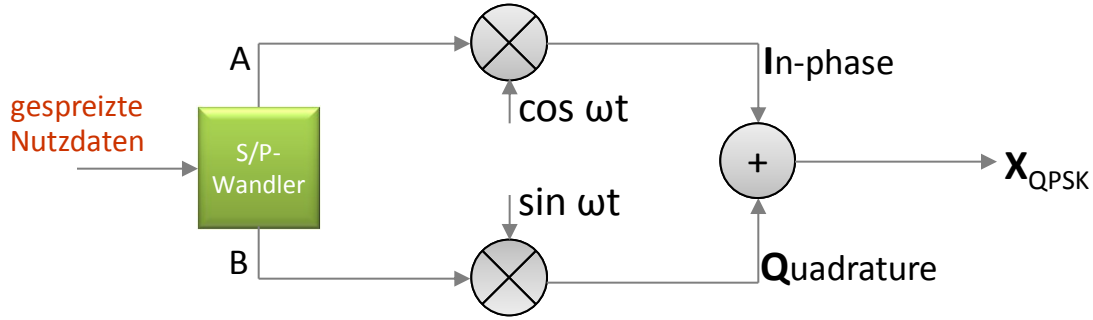
- Prinzip BPSK-Modulator

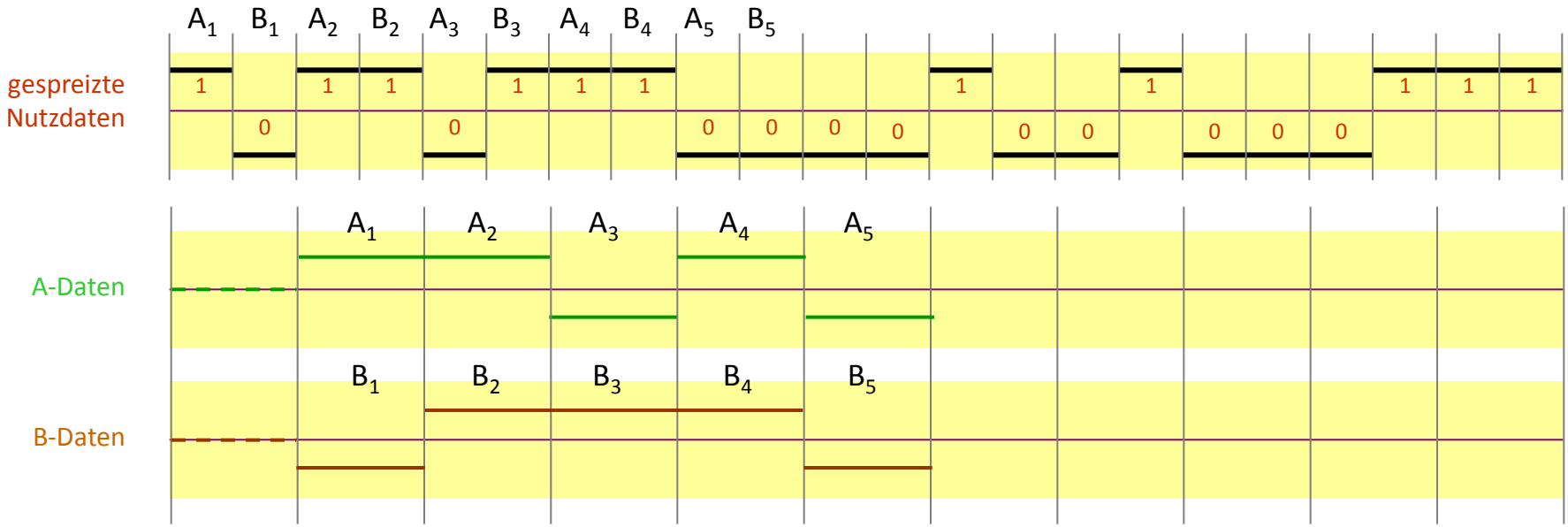




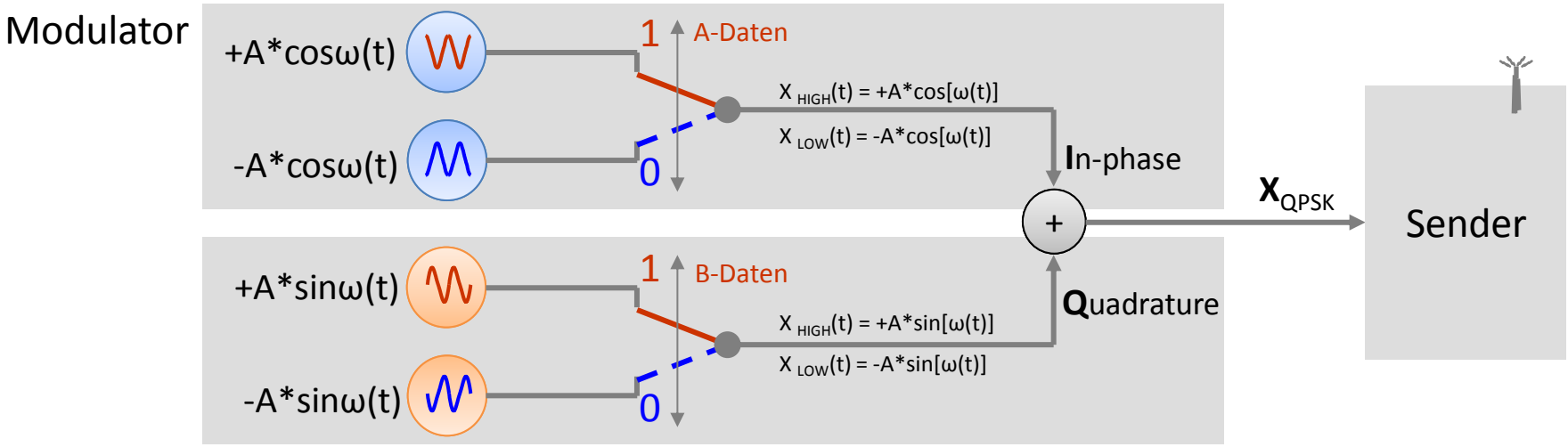
IEEE802.11-PHY: **DSSS - QPSK-Modulation**

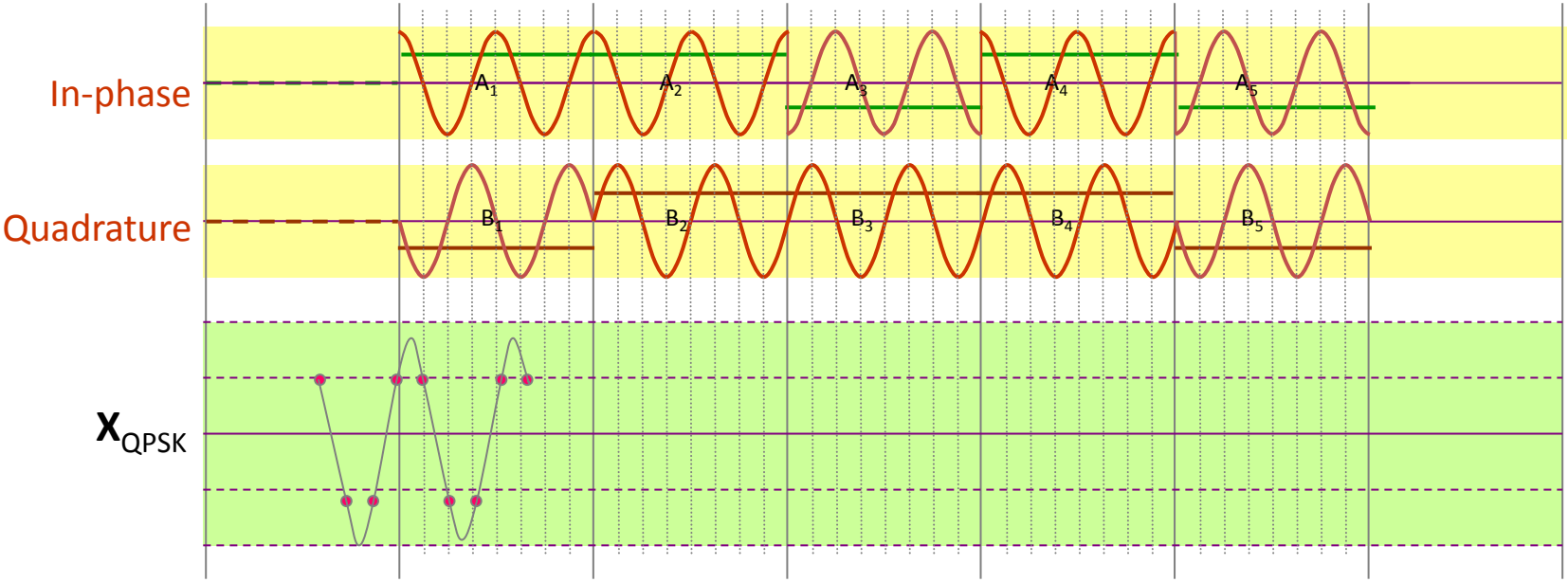
- Bei 2 Mbps wird eine QPSK-Modulation verwendet →2 orthogonale Träger.
- Das gespreizte 22 Mbps-Signal wird S-P-gewandelt → 2 * 11 Mbps.
- QPSK-Prinzip (Quadrature Phase Shift Keying)





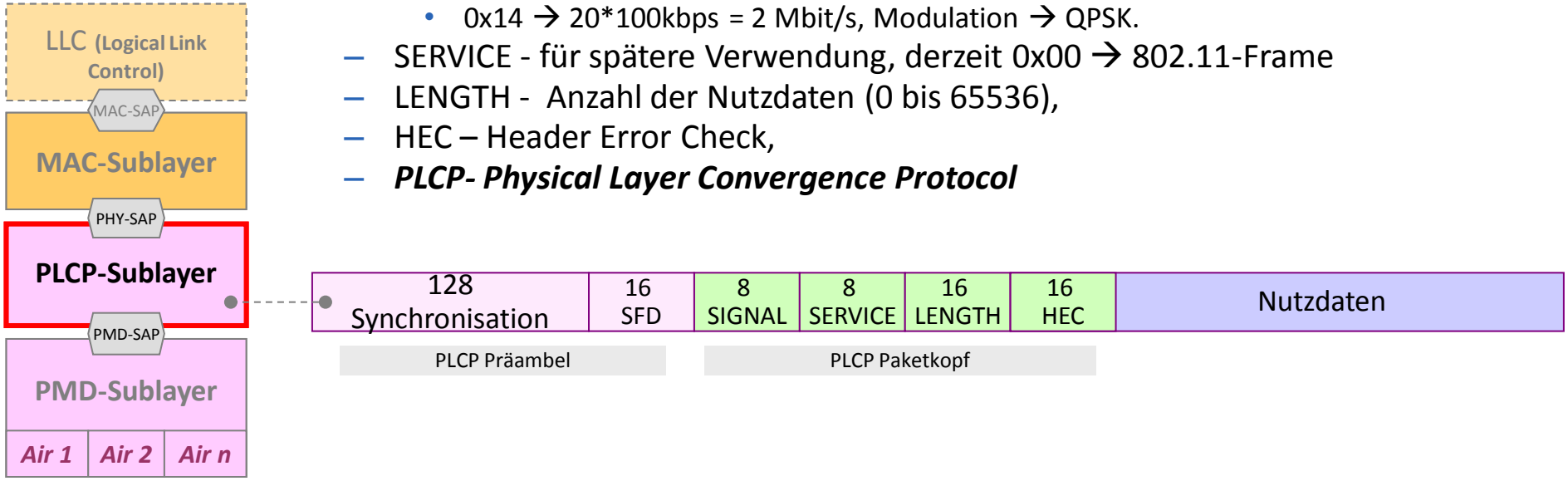
IEEE802.11-PHY: **DSSS - QPSK-Modulation**





IEEE802.11-PHY: DSSS - Schicht-1-Rahmen (PPDU)

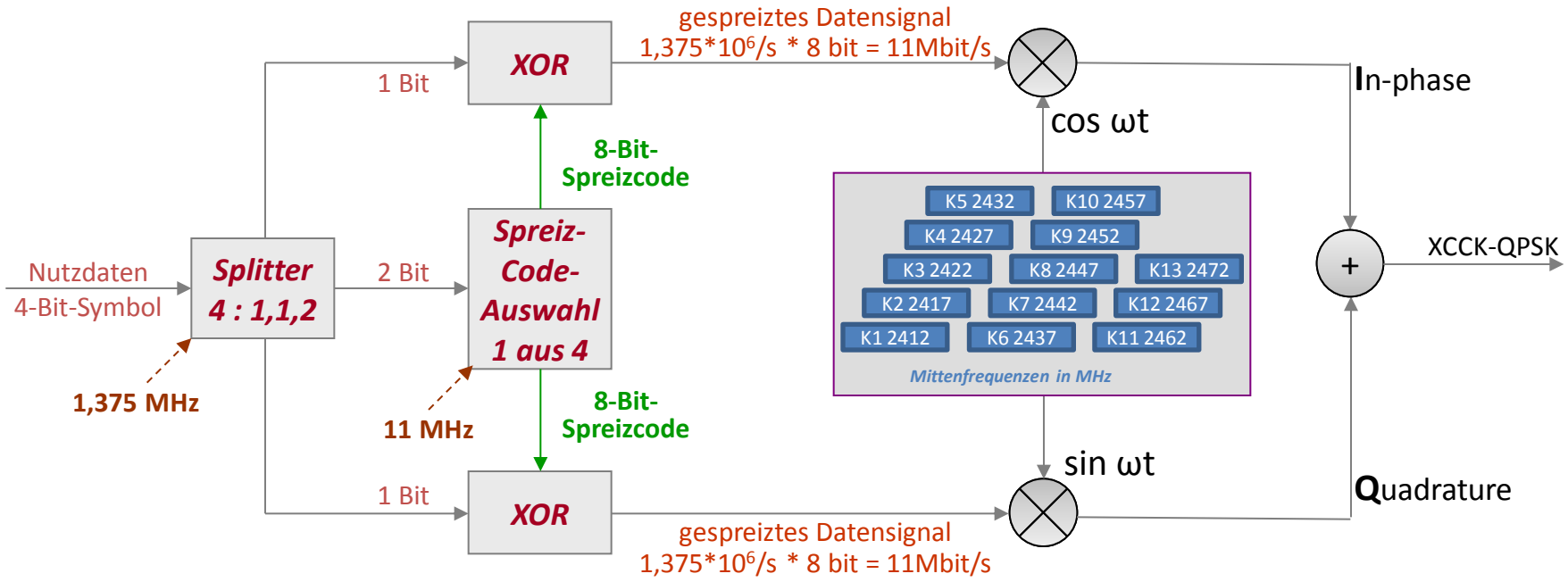
- Rahmenstruktur:
  - 128 Bit zur Synchronisation
  - SFD - Start Frame Delimiter (1111 0011 1010 0000),
  - SIGNAL - zur Angabe der verwendeten Datenrate für die Nutzdaten
    - 0x0A → 10*100kbps = 1 Mbit/s, Modulation → BPSK,
    - 0x14 → 20*100kbps = 2 Mbit/s, Modulation → QPSK.
  - SERVICE - für spätere Verwendung, derzeit 0x00 → 802.11-Frame
  - LENGTH - Anzahl der Nutzdaten (0 bis 65536),
  - HEC – Header Error Check,
  - ***PLCP- Physical Layer Convergence Protocol***



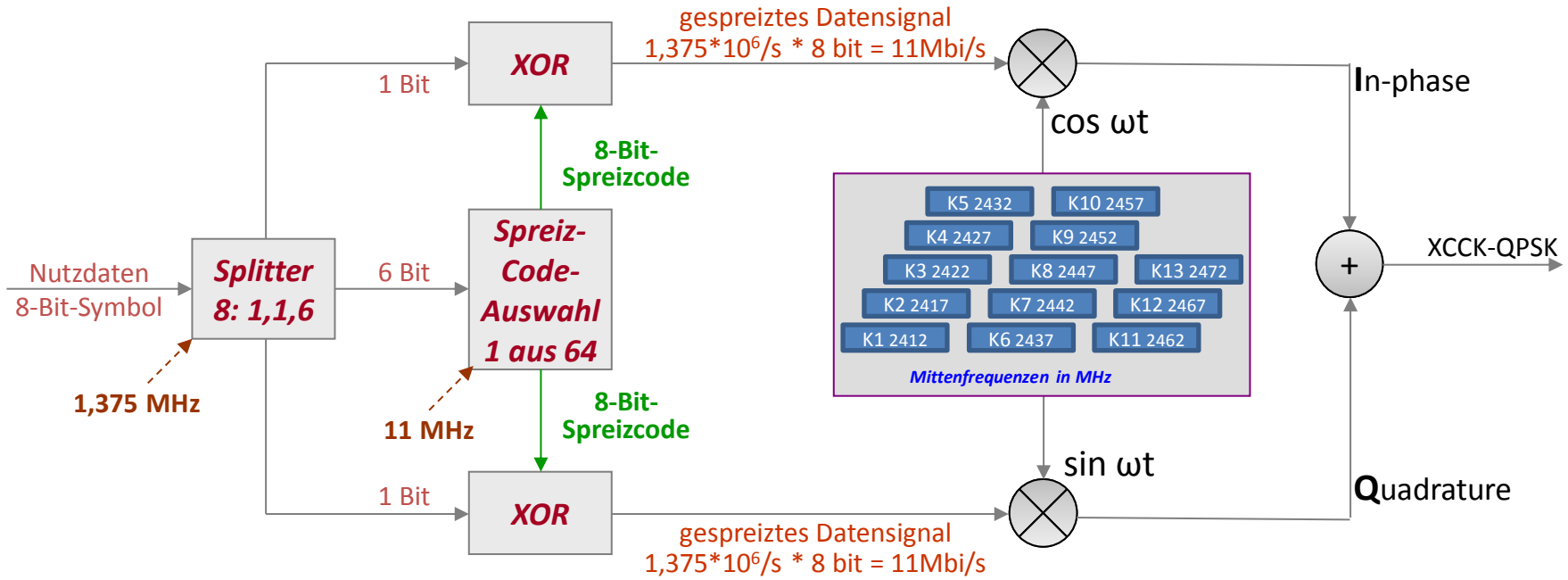
- Wie bei FHSS wird auch hier der PLCP-Header einheitlich mit 1 Mbit/s gesendet.
- Die verwendete Datenrate und das Modulationsverfahren für die Nutzdatenübertragung (1 / 2 / 5,5 / 11 Mbit/s) geht aus dem SIGNAL-Feld hervor.

PLCP - Physical Layer Convergence Protocol
PMD - Physical Media Dependent

- Bei 5,5 und 11 Mbps wird einer von 4 möglichen 8-Bit-Spreizcodes genutzt.
- CCK-QPSK-Sender für 5,5 Mbps:
  - je ein Bit wird über einen 8-Bit-Code gespreizt und QPSK-moduliert. Im 8-Bit-Spreizcode selber sind 2 Bit codiert. Es werden Chipcodes mit großer Distanz verwendet.
  - Daraus folgt eine Datenrate von: (1 + 1 + 2) bit * 1,375*10^6/s = 5,5 Mbit/s.
- Auf Empfängerseite wird das demodulierte Signal 4 Korrelatoren zugeführt.



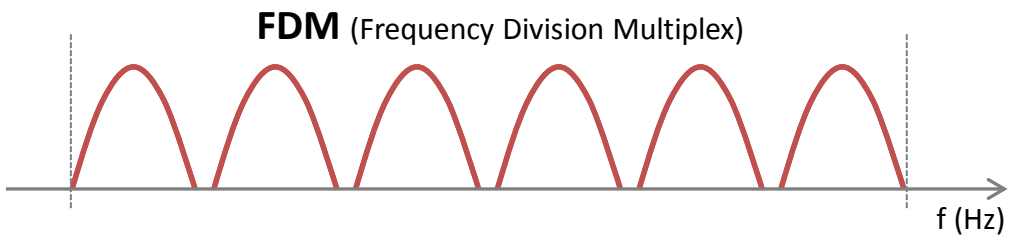
- CCK-QPSK-Sender für 11 Mbps:
  - je ein Bit wird über einen 8-Bit-Code gespreizt und QPSK-moduliert. Im 8-Bit-Spreizcode selber sind 6 Bit codiert.
  - Daraus folgt eine Datenrate von: (1 + 1 + 6) bit * 1,375*106/s = 11 Mbit/s.
- Auf Empfängerseite wird das demodulierte Signal 64 Korrelatoren zugeführt.



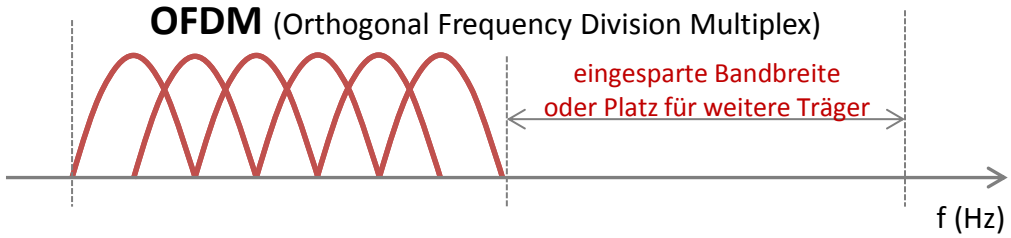
IEEE802.11a/g: **Übersicht – OFDM** (Orthogonal Frequency Division Multiplexing)

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

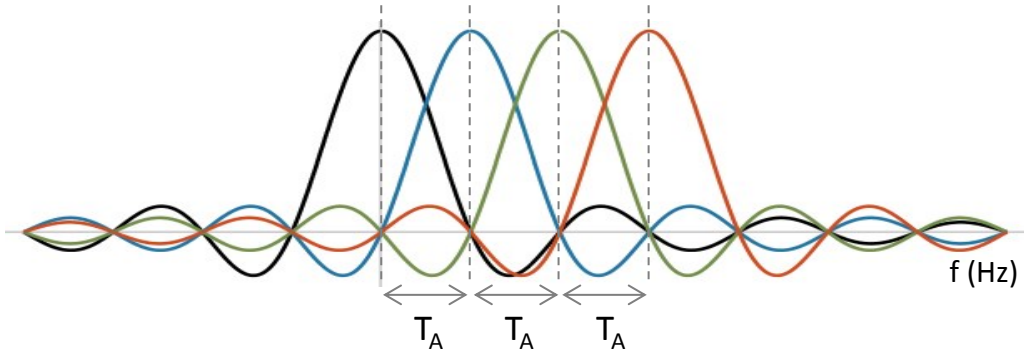
- Bisherige Bereitstellung orthogonaler Träger durch FDM:
  - Sicherheitsabstand zwischen den Bändern garantiert die Unabhängigkeit.
  - Aber, schlechte Nutzung der Bandbreite.



- Bereitstellung orthogonalen Träger durch OFDM:
  - Entspricht der Trägerabstand T_A dem Kehrwert der Symbolperiode T_S, liegt Orthogonalität vor.
  - Die Bandbreite kann etwa doppelt so gut genutzt werden.



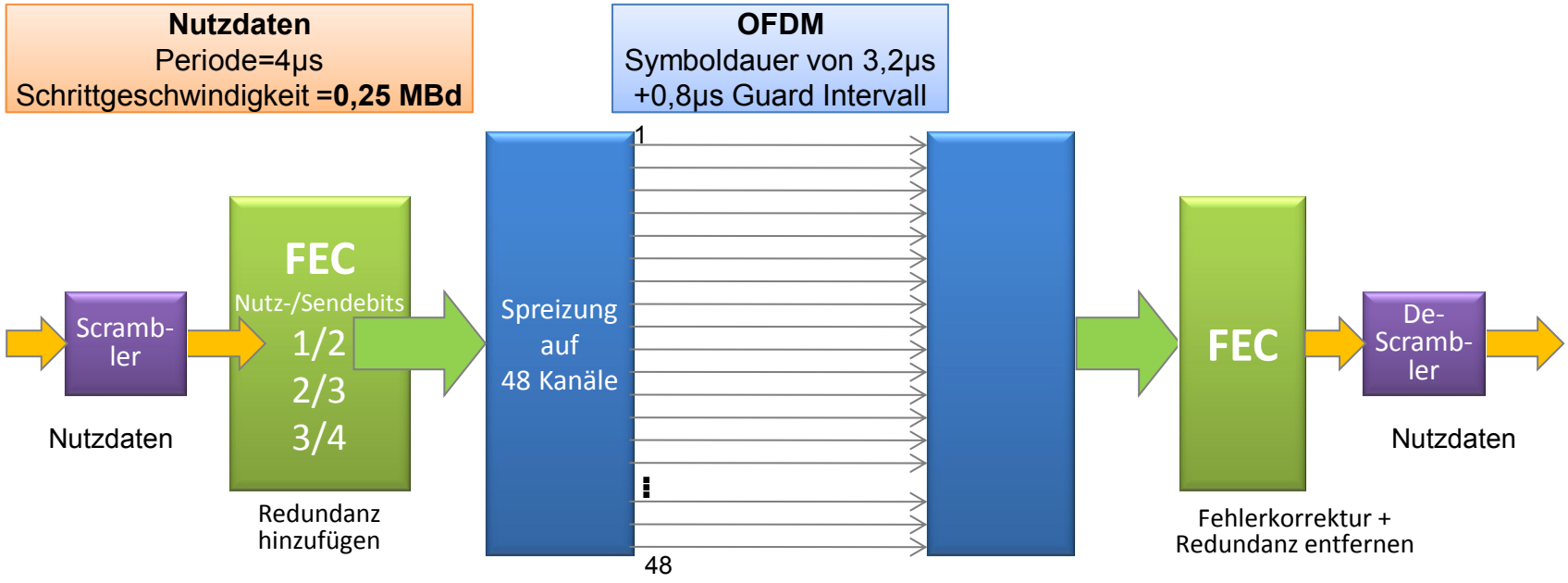
- **Beispiel**: OFDM-Signal mit vier Trägern im Frequenzbereich.



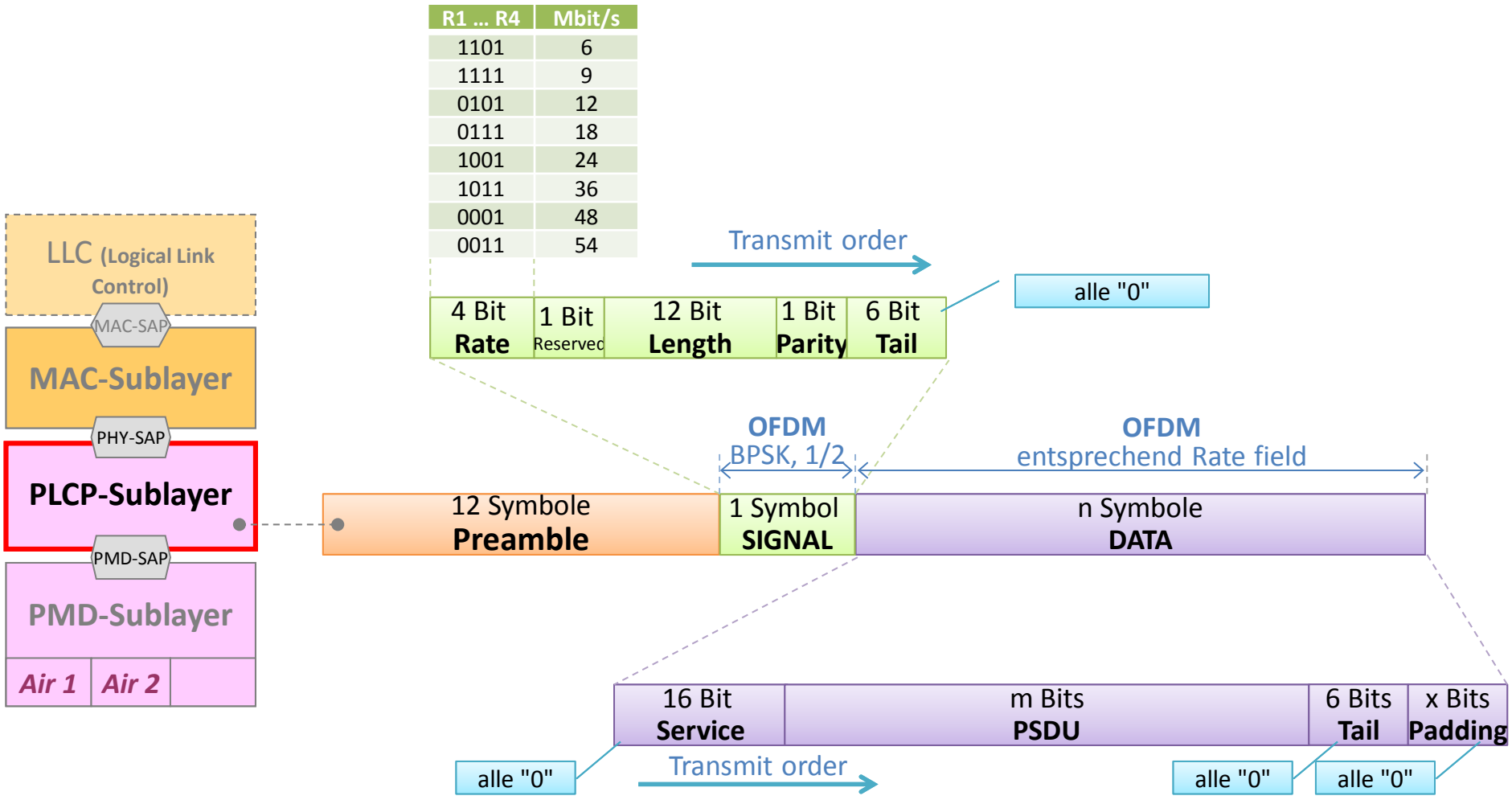
- In 802.11g wird beispielsweise eine Symbolperiode von 3,2 µs genutzt.
  - Daraus folgt der Trägerabstand T_A
    $T_A = 1/T_S$ = 1/3,2 µs= 312500 Hz = **312,5 kHz**

IEEE802.11a/g: **Übersicht – OFDM, 20-MHz-Kanal**

	Bemerkungen	Nummerierung
64	**Gesamtzahl der Träger**. Trägerabstand $T_A = 1/T_S = 1/3{,}2\ \mu s =$ **312,5 kHz**	**-32**, -31, ..,30, **31**
48	**Träger werden zur Datenübertragung genutzt**	± {1,..,6, 8,..,20, 22,..26}
4	Träger dienen zur Übertragung der Referenzphasen(Pilotträger)	± {7, 21}
1	Träger (Centerfrequenz) bleibt ungenutzt	0
11	Träger dienen als Schutz gegenüber den Nachbarkanälen	oben 5 {27,..31} unten 6 {-32,..,27}

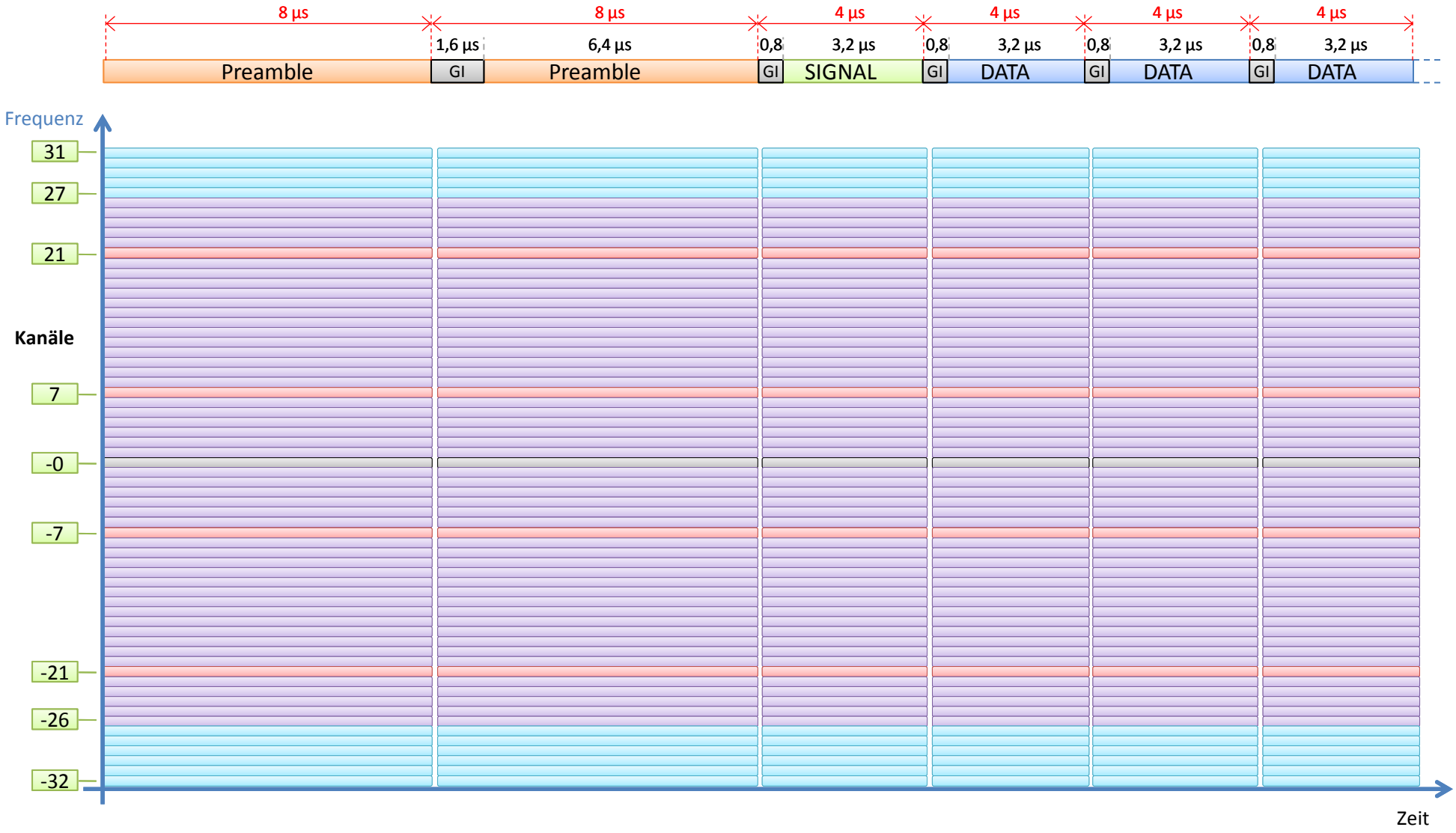


IEEE 802.11a: **OFDM – PLCP-PDU**

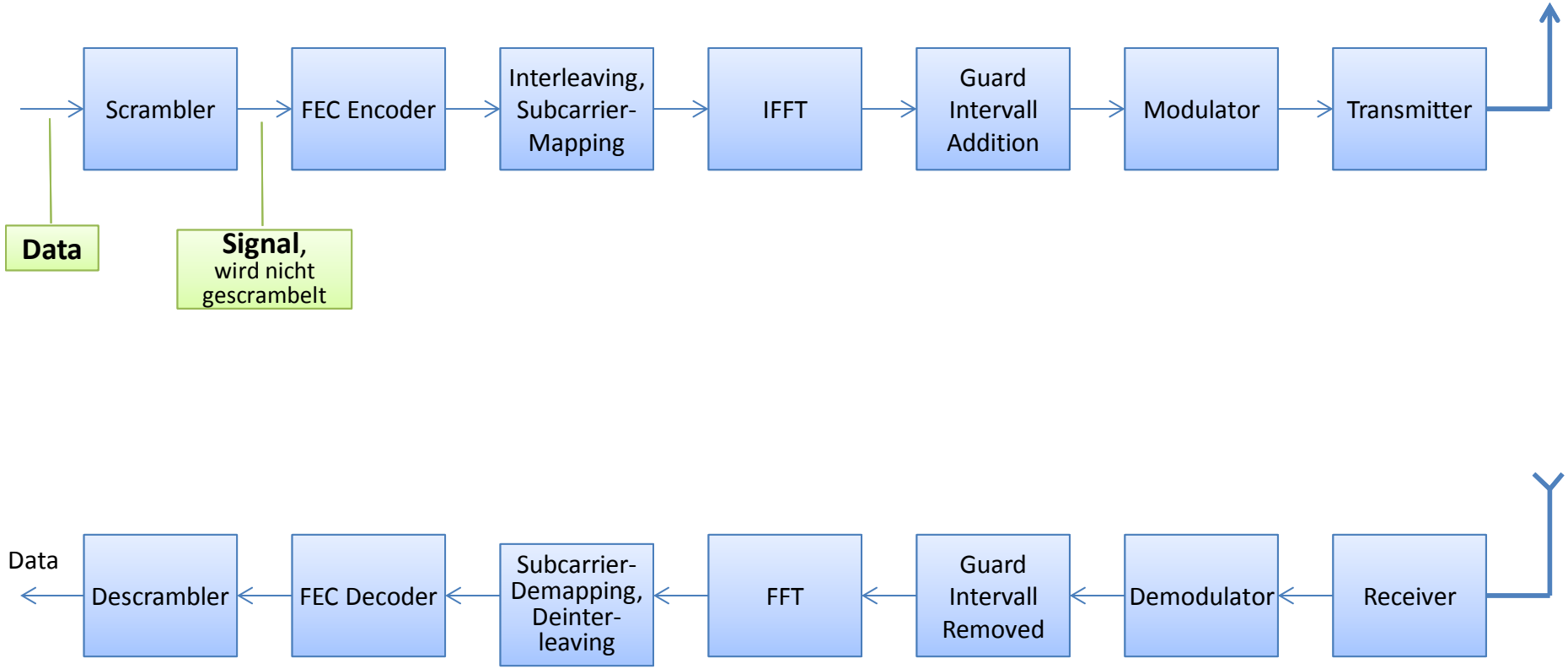


PLCP - Physical Layer Convergence Protocol
PMD - Physical Media Dependent

IEEE 802.11a/g: **OFDM – Frame**



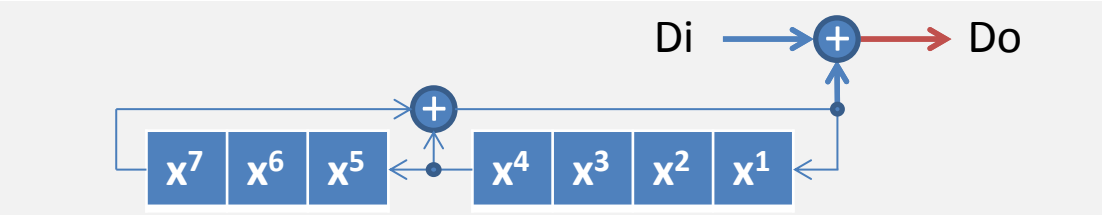
IEEE 802.11a: **OFDM – Blockschaltung Sender/Empfänger**



- Generatorpolynom für Scrambler/Descrambler: **$S(x) = x^7 + x^4 + 1$**
- Ist der Initialzustand $(1111111)_B$ erhält man folgende 127-Bit-Folge:

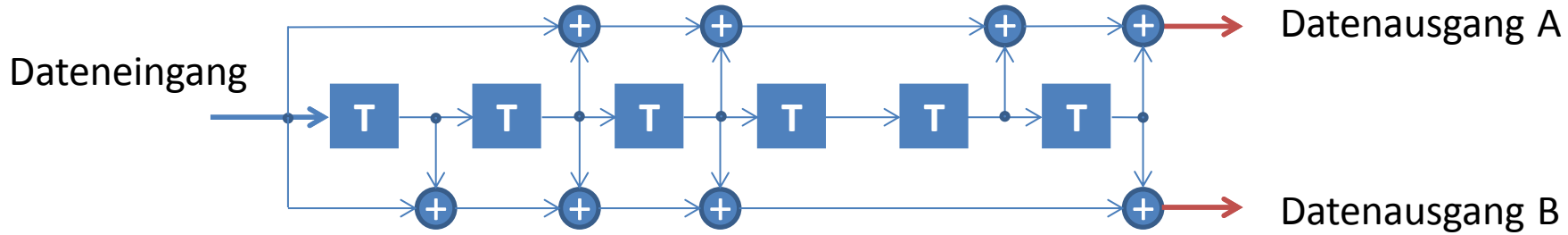
```
00001110 11110010 11001001 00000010 00100110 00101110 10110110 00001100
11010100 11100111 10110100 00101010 11111010 01010001 10111000 1111111
```

- Zum Scrambeln nutzt man einen Zufallswert, der aber nicht $(0000000)_B$ sein darf.



1	1	1		1	1	1	1	
1	1	1		1	1	1	0	0
1	1	1		1	1	0	0	0
1	1	1		1	0	0	0	0
1	1	1		0	0	0	0	0
1	1	0		0	0	0	1	1
1	0	0		0	0	1	1	1
0	0	0		0	1	1	1	1
0	0	0		1	1	1	0	0
0	0	1		1	1	0	1	1
0	1	1		1	0	1	1	1
1	1	1		0	1	1	1	1
1	1	0		1	1	1	1	1
1	0	1		1	1	1	0	0
0	1	1		1	1	0	0	0

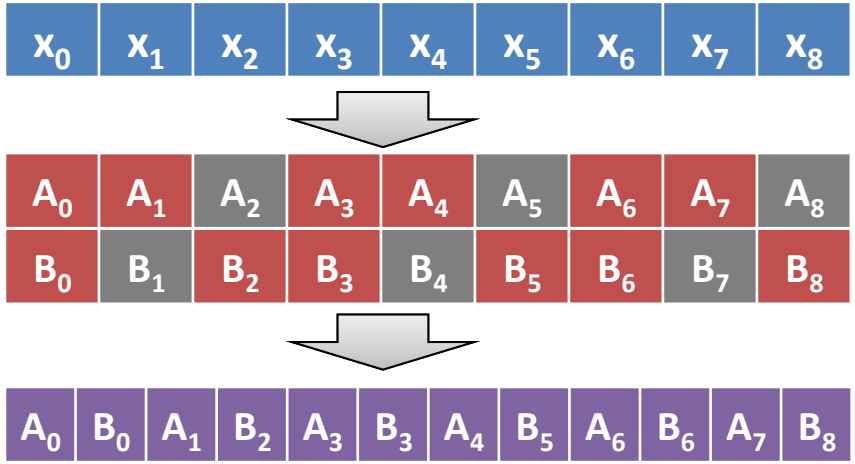
- Kanalkodierung erfolgt mittels eines Faltungscoders.
- Aus jedem Eingangsbit entstehen zwei gedächtnisbehaftete Ausgangsbits.
- Die Tail-Bits (alles 0) bringen den Coder in einen initialen Zustand.



- Die Coderate R nach dem Faltungscoder beträgt R = 1/2.
- Jedem Eingangsbit wird ein Redundanzbit hinzugefügt.
- Faltungscoder werden beschrieben durch (n,k,m)
  - n=Anzahl der Ausgangsbits
  - k=Anzahl der Eingangsbits
  - m=Speicheranzahl
- Für den verwendeten Coder gilt (n,k,m)=(2,1,6).

- Durch Weglassen bestimmter Bits - diesen Vorgang nennt man **Punktierung** – verringert man die Redundanz und kommt damit auf Coderaten R = 2/3 | 3/4.

- Zur **Erreichung der Coderate R = 3/4** werden aus 18 A-/B-Datenbits 6 Bits nach einem festliegendem Muster gestrichen.
- 9 Eingangsbits haben damit 12 Ausgangsbits zur Folge: R = 9/12 = 3/4
- Bei der Decodierung werden die gelöschten Bits nicht berücksichtigt.
- Durch Punktierung wird die Vorwärtskorrekturfähigkeit gemindert.

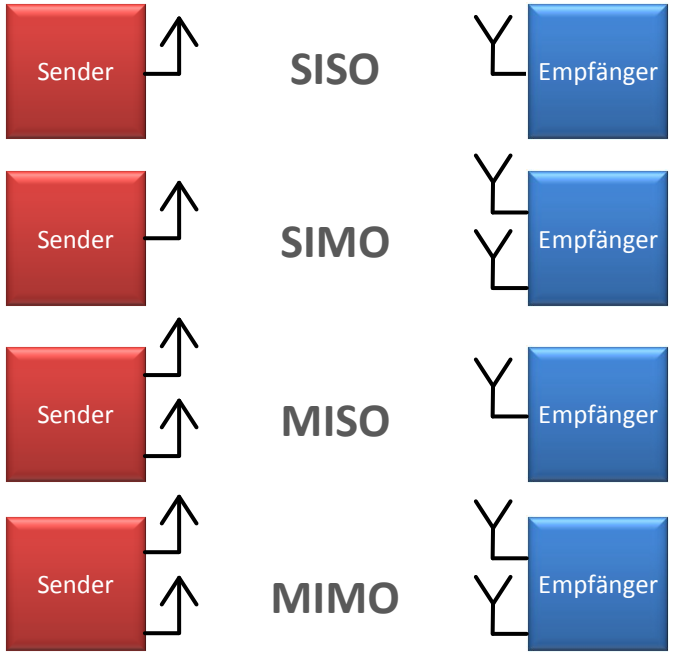


- Durch die Faltungscodierung wird R =1/2. Daraus resultieren die Datenraten 6, 12, 24 Mbps.
- Die anderen Datenraten werden durch Punktierung erreicht.

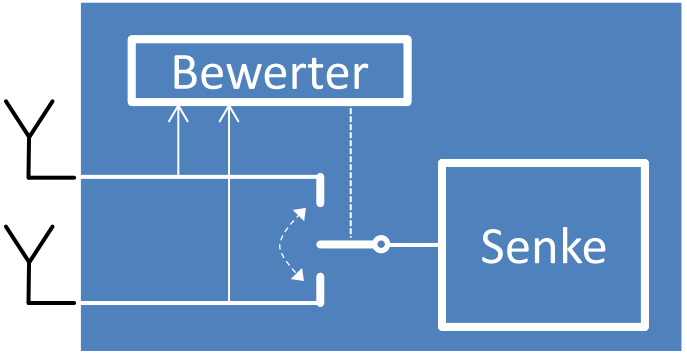
Modulations -verfahren	Bits pro Subkanal	FECCR -Forward Error Correction Coderate	Bits je OFDM-Symbol	Datenbits je OFDM-Symbol	Datenrate in Mbps	
BPSK	1	**1/2**	48	24	**6**	24 bit*0,25*10^6/s
BPSK	1	3/4	48	36	**9**	36 bit*0,25*10^6/s
QPSK	2	**1/2**	96	48	**12**	
QPSK	2	3/4	96	72	**16**	
16-QAM	4	**1/2**	192	96	**24**	
16-QAM	4	3/4	192	144	**36**	
64-QAM	6	2/3	288	192	**48**	
64-QAM	6	3/4	288	216	**54**	54 bit*0,25*10^6/s

- 802.11n wird neben OFDM durch **Mehrantennensysteme** geprägt.
- Baugleiche Antennen, angesteuert über intelligente Signalverarbeitungsalgorithmen, haben eine wesentliche **Verbesserung der Sende- und Empfangseigenschaften** zur Folge:
  - wodurch der **Signal-Rauschabstandes größer** wird,
  - was **höhere Datenraten** oder **höhere Reichweiten** erlaubt.

- Mehrantennensysteme werden aus Sicht der Empfangsseite klassifiziert:
  - **SISO** (Single Input, Single Output):
    ein Sendesignal hat ein Empfangssignal zur Folge.
  - **SIMO** (Single Input, Multiple Output) :
    ein Sendesignal hat zwei Empfangssignale zur Folge.
  - **MISO** (Multiple Input, Single Output) :
    zwei Sendesignale haben ein Empfangssignal zur Folge.
  - **MIMO** (Multiple Input, Multiple Output):
    zwei Sendesignale haben zwei Empfangssignale zur Folge.



- Aktuelle 802.11n-Produkte nutzen alle Methoden, von SISO bis MIMO.
- SIMO-Anwendung →Switched-Antenna-**Diversity**[1)]-Verfahren:
  - Beim Empfang der Präambel entscheidet der Bewerter, welches Antennensignal genutzt wird.



- SIMO-Anwendung →Maximal-**Ratio-Combining**-Verfahren:
  - Die Empfangssignale werden technisch aufwändig kombiniert, wodurch aber die Empfangsleistung deutlich erhöht wird
  - und gleichzeitig Interferenzen durch eine Mehrwegeausbreitung unterdrückt werden.
- MIMO-Anwendung
  - Aufteilung des Datenstromes auf mehrere Sendersysteme - **Spatial Multiplexing**.
  - Auf der Empfängerseite werden die überlagerten Signale separiert und die einzelnen Datenströme wieder zusammengefügt.
  - Verfahren erfordern Aufwand: n Sende-/Empfangssysteme, leistungsfähige Signalverarbeitung.

[1)] Vielfalt

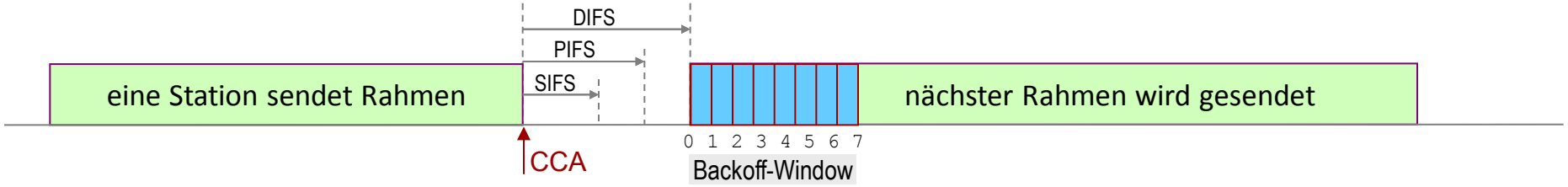
IEEE 802.11-MAC: Media Access Control

- MAC-Aufgaben sind: Media Access, Roaming, Authentication, Power Management.
- Es werden zwei Medien-Zugriffsarten unterstützt:
  - **(1) Asynchronous Data Service**
    - Stationen greifen bei Bedarf auf Kanal zu,
    - versuchen aber eine Kollision zu vermeiden, CA (Collision Avoidance[2)]).
    - Nutzbar bei Adhoc- und Infrastrukturnetze, kein garantierter Durchsatz.
  - **(2) Time Bounded Service,** nur bei Infrastrukturnetzen, zwei Zeitabschnitte der Kanalnutzung:
    - wettbewerbsfreie Periode:
      - der AP pollt/selektiert Stationen, damit diese Daten senden oder empfangen können,
      - garantierter Durchsatz aber auch Zeitverschwendung möglich.
    - Wettbewerbsperiode →wie (1).

- Drei MAC-Verfahren DFWMAC (Distributed Foundation Wireless Medium Access Control) wurden spezifiziert:
  - *Basis:* **DFWMAC** mittels CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance[2)]). Dieses Verfahren müssen alle Stationen beherrschen.
  - *Erweiterung:* **DFWMAC mit RTS/CTS-Erweiterung**, wird zusätzlich verwendet, wenn Gefahr verdeckter Endgeräte besteht.
  - *Erweiterung:* **DFWMAC-PCF**[1)] mit Polling, wenn man z.B. Mindestdurchsatz garantieren will.

[1)]PCF – Point Coordination Function
[2)]Vermeidung

IEEE 802.11-MAC: **DFWMAC-Basiskonzepte** /nach Sch2000/

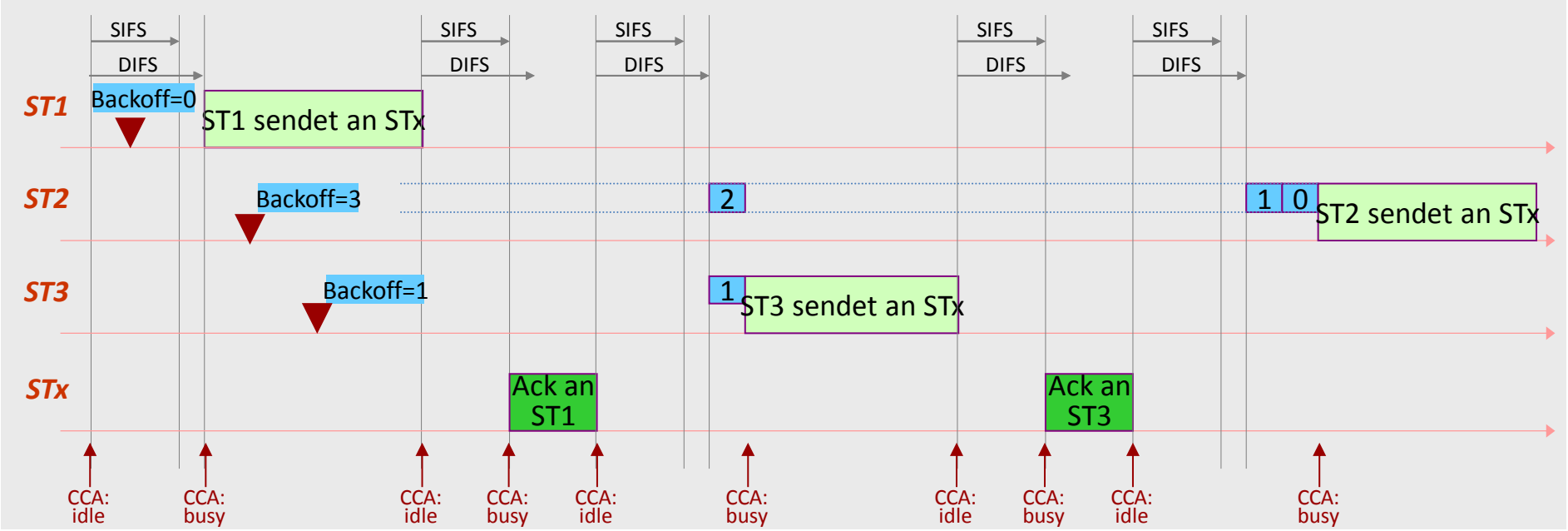


- **CCA-Signal** (Clear Channel Assessment), PHY zeigt MAC Medienzustand an (frei, belegt).
  - Bei Medium-Frei-Meldung beginnt die Zeitmessung in den Stationen.
- **Drei Zeiten**:
  - **SIFS (Short Inter-frame Spacing):**
    - Kürzeste Wartezeit für STAs, z.B. zur Quittierung von Daten oder auf RTS mit CTS reagieren .
  - **PIFS (PCF2 - Inter-frame Spacing) → synchrone Dienste:**
    - Wartezeit für eine Masterstation (AP). Nach dieser Zeit kann das Pollen beginnen.
    - Stationen, die den Zeitraum DIFS warten müssen, unterliegen.
  - **DIFS (DCF1- Inter-frame Spacing) → asynchrone Dienste:**
    - Wartezeit für Stationen die asynchrone Daten senden wollen.
    - Mittels eines Wettbewerbsfensters wird zusätzlich entschieden, wer zuerst Daten senden darf.
- **Backoff-Mechanismus:** Erhält eine Station einen Sendeauftrag und das Medium ist in dem Moment besetzt, "würfelt" es einen Backoff-Wert, z.B. zwischen 0 ... 7.
  - Ist DIFS vergangen, wartet sie noch 0|1|2| ...|7 Slot's und beginnt zu senden, wenn CCA immer noch ein freies Medium signalisiert.
  - Treten Kollisionen auf, wird das Wettbewerbsfenster jeweils verdoppelt , 0 ... 15, 0... 31, usw. (kleinere Zeitinkremente).

[1] DCF - Distributed Coordination Function, wird verteilt in jeder Station realisiert und erlaubt nur asynchrone Dienste.

[2] PCF - Point Coordination Function, wird im AP verwendet und erlaubt asynchrone und zeitbeschränkte Dienste.

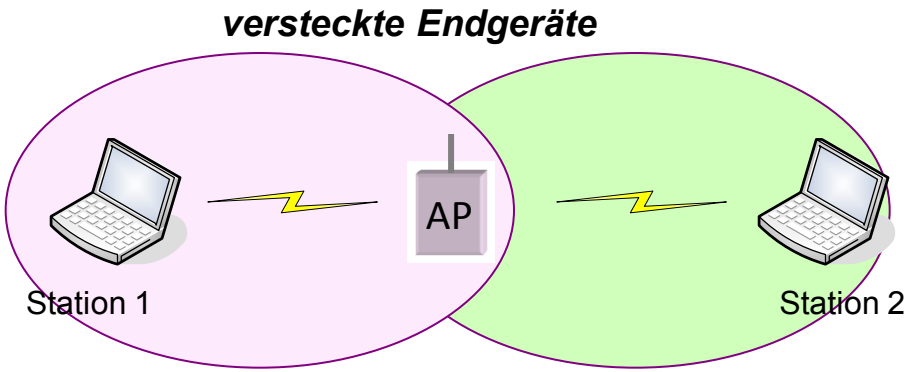
- Beispiel: ST1 bis ST3 wollen asynchron Daten an STx senden.
  - MAC-Layer von ST1 bekommt DataRq (▼), würfelt Backoff-Wert=0
  - ST2 und ST3 erhalten ein DataRq (▼) und würfeln Backoff-Wert von 3 bzw. 1

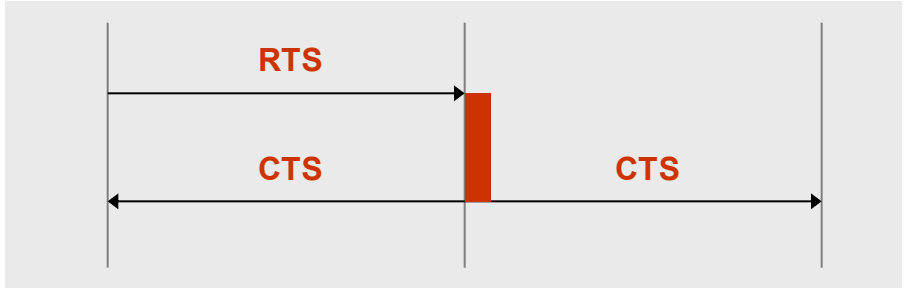


- ST1 beginnt nach Ablauf von DIFS zu senden,
- STx will Datenempfang quittieren, muss nur SIFS warte.
- Nach DIFS wartet ST3 noch ein Timeslot (Backoff=1) und beginnt dann zu senden. ST2 dekrementiert Backoff.
- Nach SIFS sendet STx Quittung an ST3.
- Nach SIFS wartet ST2 noch zwei Timeslots und beginnt dann zu senden.

IEEE 802.11-MAC: **DFWMAC mit RTS/CTS-Erweiterung**

- Nicht alle Endgeräte „hören“ sich untereinander → **versteckte Endgeräte**.
  - AP empfängt ST1 und ST2, aber ST2 empfängt nicht ST1
  - Wenn ST1 und ST2 Daten zu AP senden wollen, gibt es ein Problem.
  - ST1 beginnt zu senden, ST2 bemerkt dies nicht und beginnt auch zu senden.

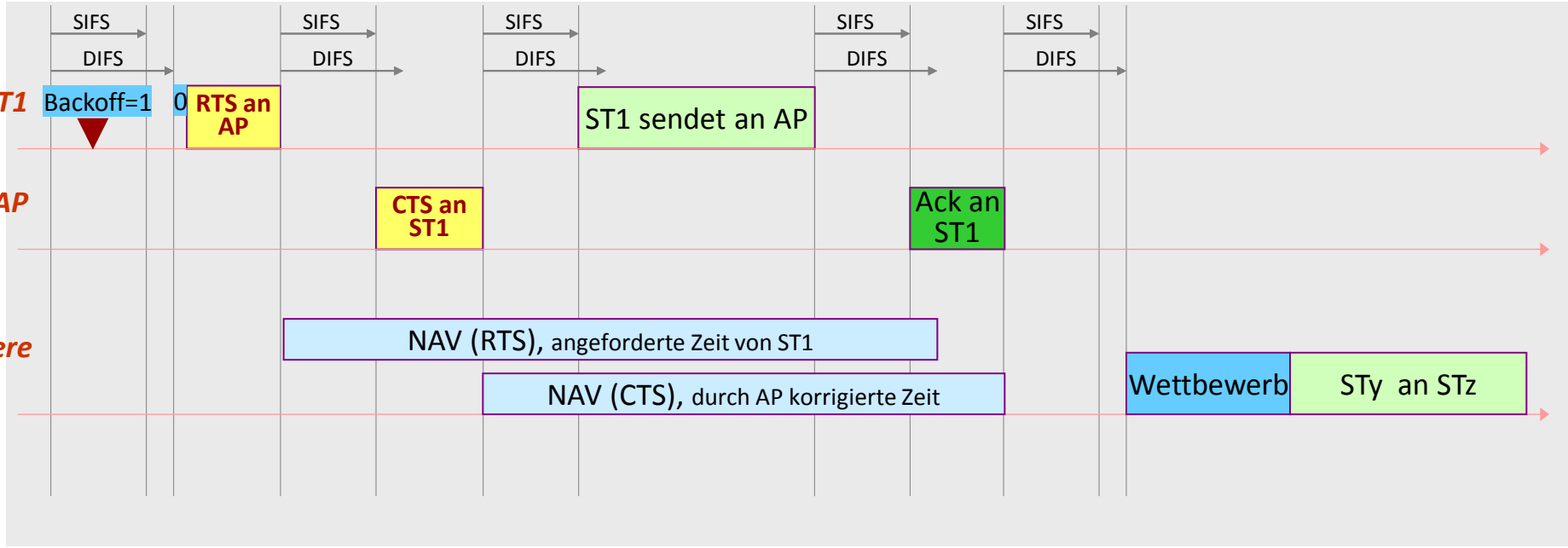




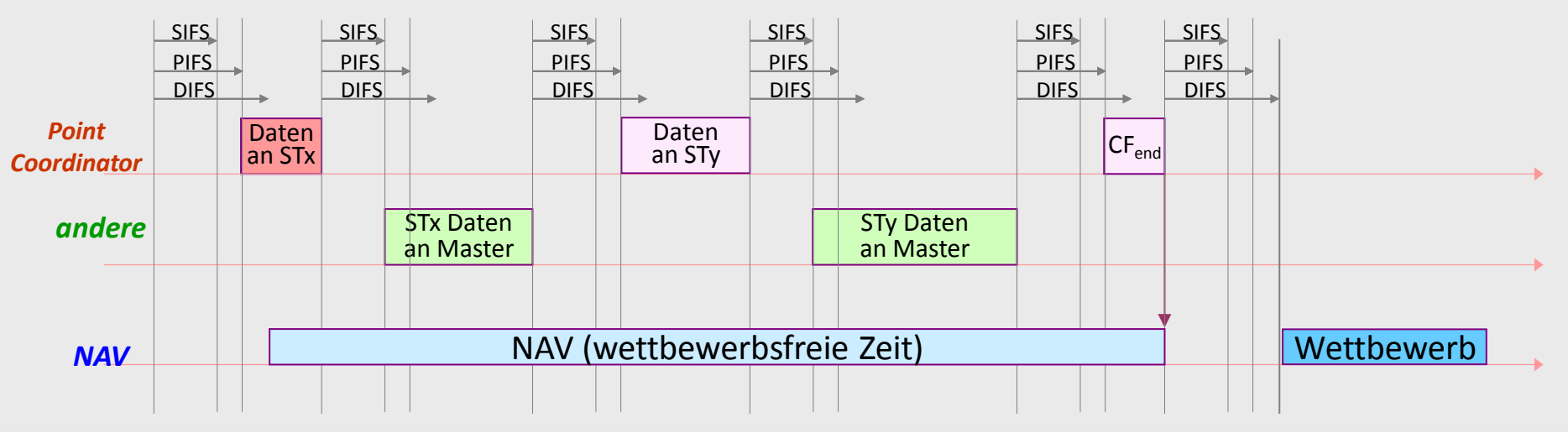
- **Lösung**: Vor der eigentlichen Datensendung tauscht man zwei relativ kurze Managementrahmen aus (RTS-CTS-Mechanismus):
  - RTS: Request-to-Send,
  - CTS: Clear-to-Send.
- In den RTS/CTS-Paketen stehen Dest.-MAC-Address, Sour.-MAC-Address und der Sendezeitbedarf (net allocation vector).
- Während der angeforderten/bestätigten Allokationszeit bleiben andere STA passiv.
- Ab welcher Datenpaketgröße RTS-CTS-Präambeln verwendet werden, kann man im AP administrieren.

IEEE 802.11-MAC: **DFWMAC mit RTS/CTS** /nach Sch2000/

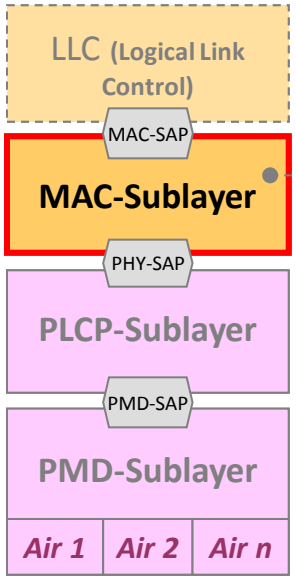
- Verwendet werden RTS-/CTS-Rahmen.
  - Im RTS-Rahmen steht die angeforderte Übertragungszeit inklusive die Zeit für die Quittung.
  - In CTS wird die korrigierte Zeit angegeben.
- Diese Zeit tragen die Stationen in den NAV (Network Allocation Vector) ein. Sie gibt den frühestmöglichen Zeitpunkt an, wo Stationen einen Zugriff versuchen dürfen.

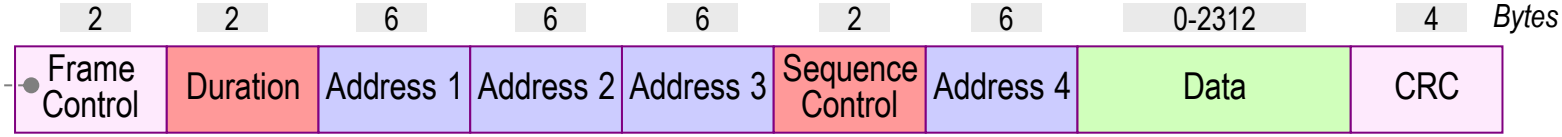


- Der **PointCoordinator** teilt Nutzungszeit ein in: Wettbewerb/-sfrei.
- Point Coordinator (**PCo**):
  - Nach PIFS sendet PCo Daten (**CF-Poll+Data**) an STx oder pollt ihn (**CF-Poll**).
  - STx sendet nach SIFS Daten an den PCo.
  - Antwortet STx nicht nach SIFS, pollt der Master nach PIFS nächste Station.
- Das CF_{end}-Paket (Contention Free, streitfrei) zeigt Stationen Ende der streitfreien Zeit an.



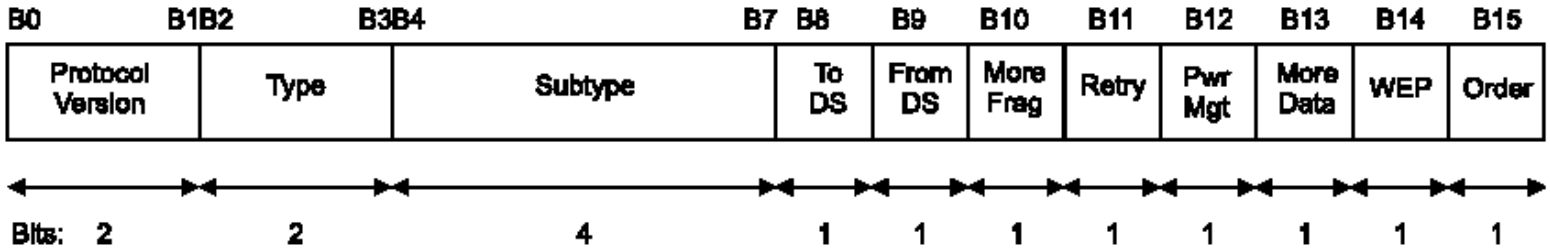
IEEE 802.11-MAC: **Rahmenstruktur**





- Frame Control: Protokollversion, Rahmen-Typ (Verwaltung, Steuerung, Daten),Verschlüsselungsinformationen, 2 DS-Bits
- Duration: geforderte Belegungsdauer bei RTS/CTS-Mechanismus → NAV - Net Allocation Vector
- Sequence Control: Folgenummerierung von Datenrahmen
- CRC: 32-Bit-Prüfsumme
- Addresses 1-4: 48-Bit-Adresse → Bedeutung wird von DS-Bits (Distribution System) im Frame-Control-Feld bestimmt.

- Frame Control Field:



IEEE 802.11-MAC: **Rahmentypen** (Auswahl)

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

Typ	*Des-cription*	*Subtype*	*Subtype description*	
00	Manag.	0000	**AssociationRq**	Zum Anmelden an einem AP
00	Manag.	0001	**AssociationRs**	Anmeldeantwort
00	Manag.	0100	**ProbeRq**	Aktives Scannen aller SS (Broadcast) oder bestimmtes SS.
00	Manag.	0101	**ProbeRs**	Antwort auf ProbeRq
00	Manag.	1011	**Authentication**	Authentication-Mechanismus (einzelne Schritte werden numeriert)
00	Manag.	1000	**Beacon**	Funkfeuer, ausgesendet durch STAs im Ad-hoc-mode oder APs. Beacon enthält u.a. (Zeitstempel, SSID, Parameter). Die Aussendung des SSID kann unterdrückt werden.
01	Control	1011	**Request To Send (RTS)**	Anfordern von Sendezeit bei verdeckten Endgeräten
01	Control	1100	**Clear To Send (CTS)**	Quittung auf RTS und Korrektur der Zeit
01	Control	1101	**Acknowledgment (ACK)**	Quittierung von Data
01	Control	1110	**Contention Free End**	*nur bei PCF:* AP teilt STA‘s Ende der streitfreien Zeit mit
10	Data	0000	**Data**	Daten in Wettbewerbszeit
10	Data	0001	**CF-Ack + Data**	*nur bei PCF:* Ack-Frame von STA an AP mit Daten
10	Data	0010	**CF-Poll + Data**	*nur bei PCF:* Poll-Frame mit Daten an STA
10	Data	0101	**CF-Ack (no data)**	*nur bei PCF:* Antwort von STA an AP ohne Daten
10	Data	0110	**CF-Poll (no data)**	*nur bei PCF:* AP pollt STA

IEEE802.11, 1999 Edition, Table 1: Valid type and subtype combinations

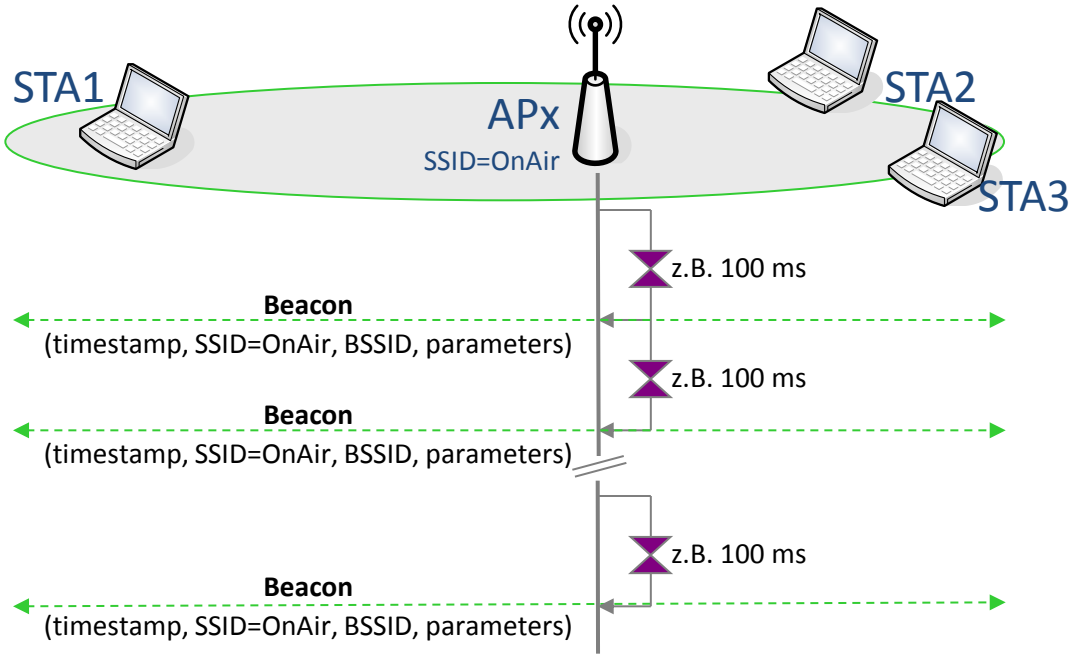
IEEE 802.11-MAC: **Management**

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

- **Powermanagement** →für batteriebetriebene Geräte lebenswichtig:
  - Sender wird bei Bedarf eingeschaltet, Empfänger →Sleep- oder Awake-Modus.
  - STA‘s müssen deshalb Sendedaten für momentan Schlafende zwischenspeichern.
  - Alle Stationen gehen in definierte Wachphase →Sendewünsche werden mitgeteilt.
  - Liegt Sendewunsch vor →muss STA bis zum Empfang der Daten wach bleiben.
- **Roaming**, gemeint ist Handover
  - Bewegt sich ein Nutzer in einem ESS (Extended Service Set) soll Handover erfolgen.
  - Stellt STA zu geringe Feldstärke fest, wird passiv oder aktiv gescannt:
    - passiv: STA hört Kanäle auf Beacon-Frames ab,
    - aktiv: Senden einer “Probe“ in die Kanäle →Warten auf Antwort.
  - Beaconframe als auch Antwort enthalten Informationen zur Nutzung eines AP.
  - Anhand der Feldstärke →Auswahl des AP:
    - STA sendet AssociateRequest an AP, wird im Erfolgsfall mit AssociateResponse bestätigt.
    - AP teilt Wechsel an DS mit →Aktualisierung der DS-Datenbasis: STAx von APm zu APn.
    - DS informiert APm über Wechsel →Ressourcenfreigabe
- **Zeitsynchronisation**: exakte Einstellung einer lokalen Uhr gegenüber anderen STA‘s:
  - zur Steuerung der Sprungfolge bei FHSS,
  - zur Steuerung des Powermanagements
  - zur Einhaltung der Zeiten SIFS, DIFS, PIFS usw.

- BSS senden zyklisch Broadcast-Leuchtfeuer (Beacon). Ein Beacon-Frame enthält:
  - Absendezeitstempel und Beacon-Intervall (typisch um 100 ms).
  - Capability Informations: AP oder STA, Point Coordination: Y|N, WEP: Y|N
  - SSID-Parameter (Name des AP), z.B. "OnAir"
  - Supported Rates: z.B. 1(B), 2(B), 5,5(B), 11(B), 6, 9, 12, 18, 24, 36, 48, 54
  - DS-Parameters: z.B. Channel 11

BEISPIEL: 3 STAs empfangen z.Zt das Funkfeuer von APx



Legende:
- MAC-Broadcast
- MAC-Unicast

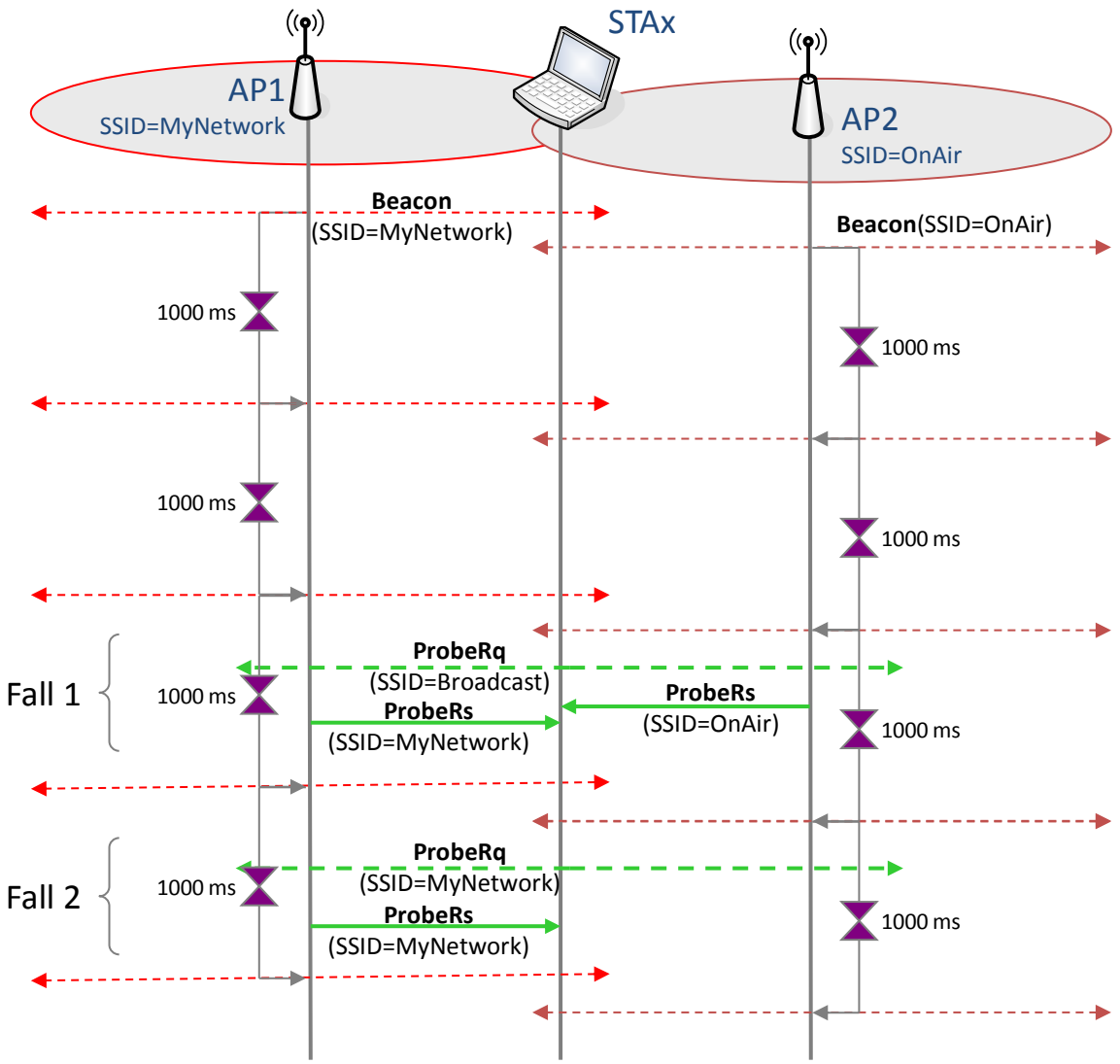
IEEE 802.11-MAC: **Aktives Scannen mittels ProbeRq/Rs**

BEISPIEL: →Aktives Scannen
STAx hört die Funkfeuer von AP1 und AP2. Beide Funkfeuer wurden z.B. auf 1000 ms eingestellt.

Fall 1: Überblick verschaffen, welche APs sind verfügbar? →erfolgt beim Aktivieren des Adapters.
Station STAx sendet per MAC-Broadcast ein ProbeRq(SSID=Broadcast), →aktives Scannen. Alle APs antworten per MAC-Unicast mit ProbeRs(SSID=ServiceSetName).

Fall 2: Eine STA scannt zielgerichtet ein Netz →erfolgt bei Verbindungsaufnahme.
Im ProbeRq (mittels MAC-Broadcast gesendet) wird nur das gewünschte Zielnetz angegeben, z.B. MyNetwork. STA erhält jetzt per MAC-Unicast nur noch ein ProbeRs von MyNetwork.

Legende:
- MAC-Broadcast
- MAC-Unicast

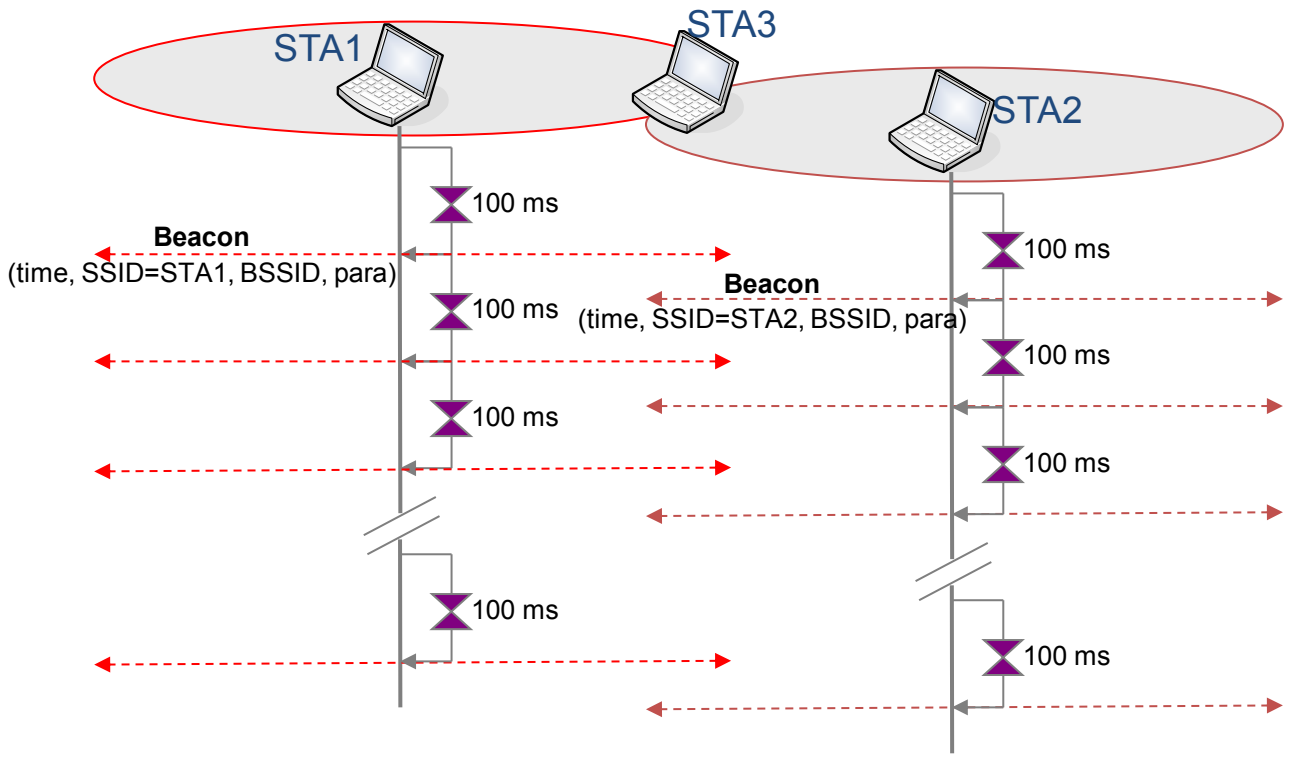


IEEE 802.11-MAC: **Beacon-Frames in Ad-hoc-Netzen**

- Ad-Hoc-Netze:
  - Alle Interfaces im Ad-Hoc-Modus senden Beacons (Funkfeuer).
  - Tritt eine Station einem IBSS bei, sendet diese kein Beacon mehr.

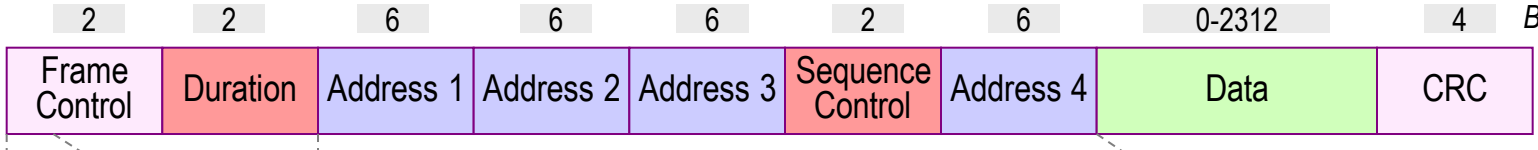
BEISPIEL:

- STA3 ist z.B. STA1 beigetreten, sendet deshalb kein eigenes Funkfeuer.
- STA3 hört aber die Funkfeuer von STA1 und STA2.
- Wäre STA3 ungebunden, würden STA1/2/3 Funkfeuer senden:
  - STA1 würde STA3 hören,
  - STA2 würde STA3 hören,
  - STA3 würde STA1/2 hören.



Legende:
- MAC-Broadcast
- MAC-Unicast

- Erfolgt über 4 Adressenfelder und 2 Bit im Frame Control Field

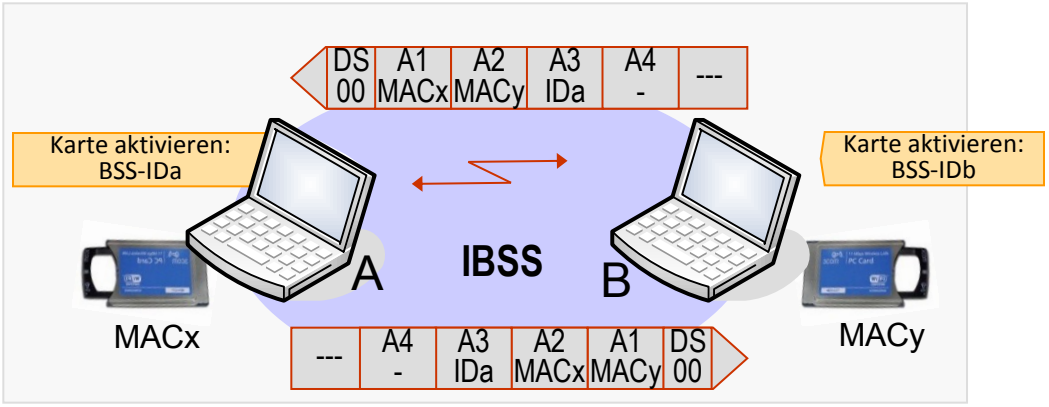


zu DS	von DS	Address 1	Addresse 2	Address 3	Address 4
0	*0*	DA	SA	BSS-ID	-
0	*1*	DA	BSS-ID	SA	-
1	*0*	BSS-ID	SA	DA	-
1	*1*	RA	TA	DA	SA

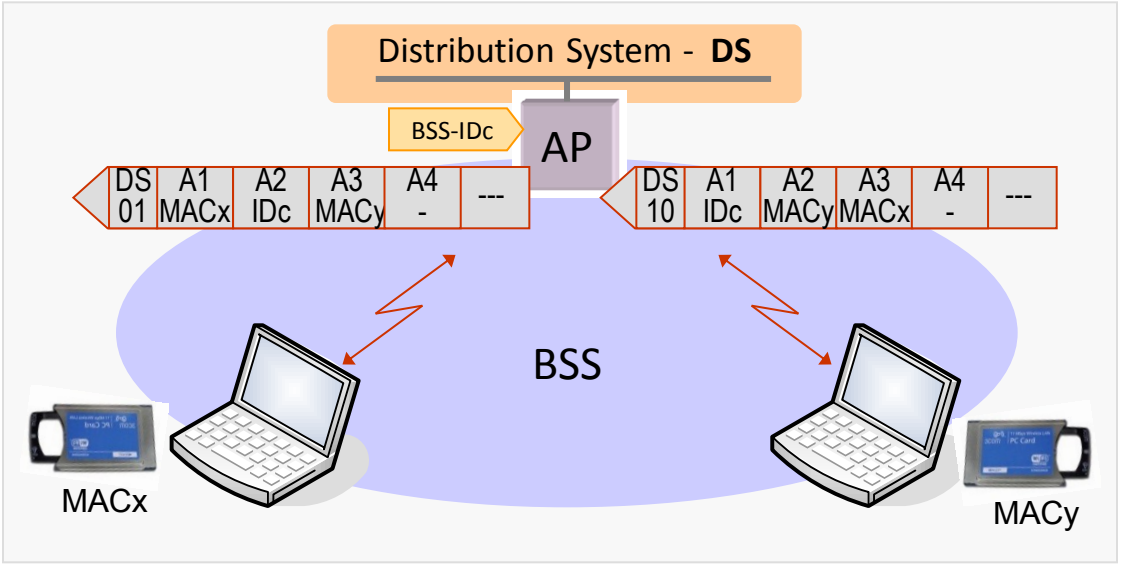
BSSID	MAC-Adresse der Funkseite (MAC-Adr.)
DA	Destination Address (MAC-Adr., Funkadapter)
SA	Source Address (MAC-Adr., Funkadapter)
RA	Receiver Address (MAC-Adr.eines AP im DS)
TA	Transmitter Address (MAC-Adr. eines AP im DS)

IEEE 802.11-MAC: **Adressierung**

- **Ad-hoc-Netz**:
  - A1 (DA): phys. MAC-Zieladresse,
  - A2 (SA): phys. MAC-Absenderadresse
  - A3 (BSS-ID1)): <log. Adresse, 46-Bit-Zufallszahl, die in jeder STA eingetragen wird. Dieser ID macht die BSS unterscheidbar und bestimmt die Zugehörigkeit von STA‘s zu einer IBSS.
  - Nimmt ein Computer in einem IBSS eine Verbindung zu einem anderen auf, haben beide den gleichen IBSS-ID

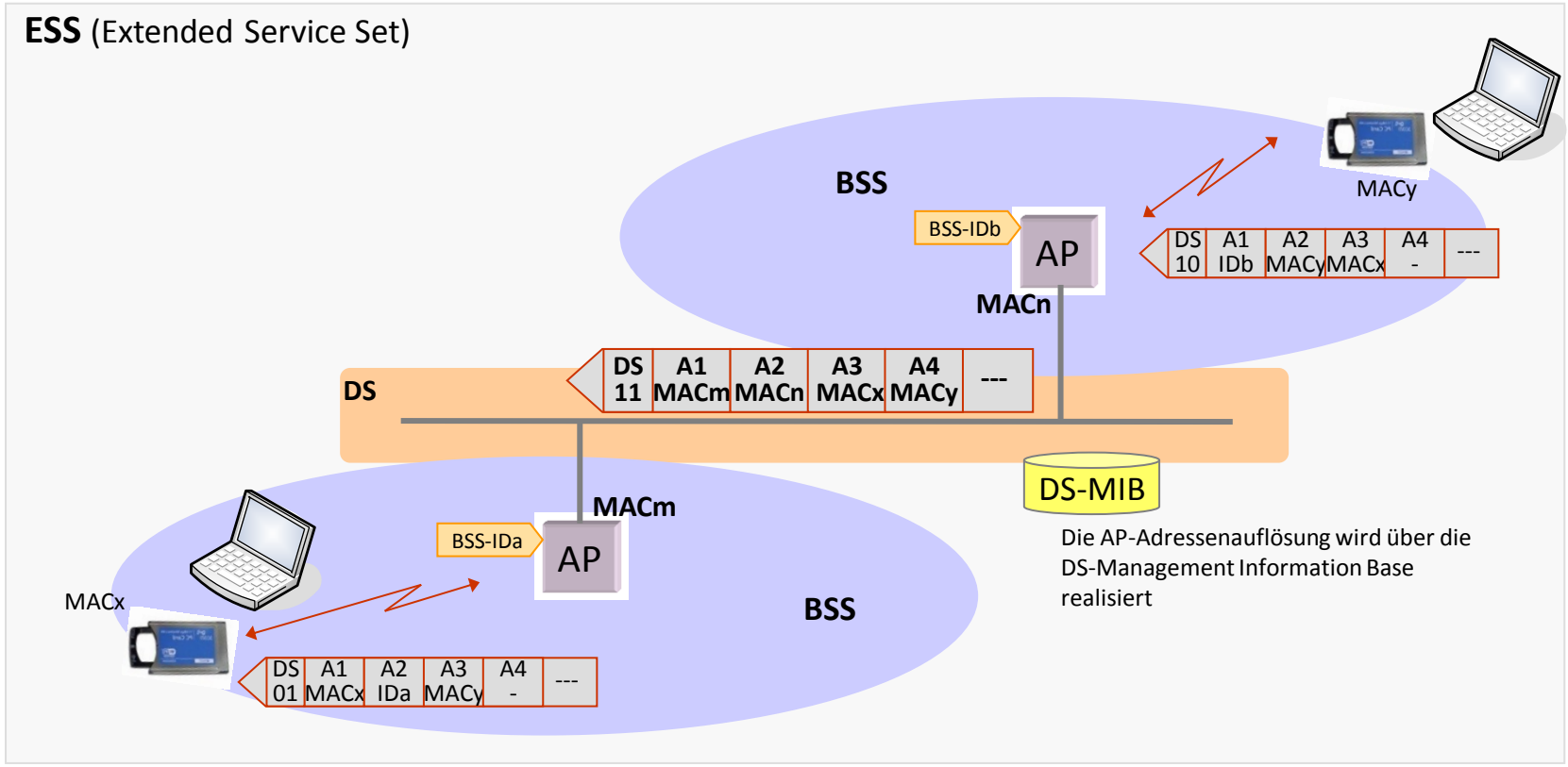


- **Infrastruktur-Netz**-Beispiel:
  - Paket wird von MACy für MACx an AP gesendet.
  - AP leitet Paket an MACx weiter.

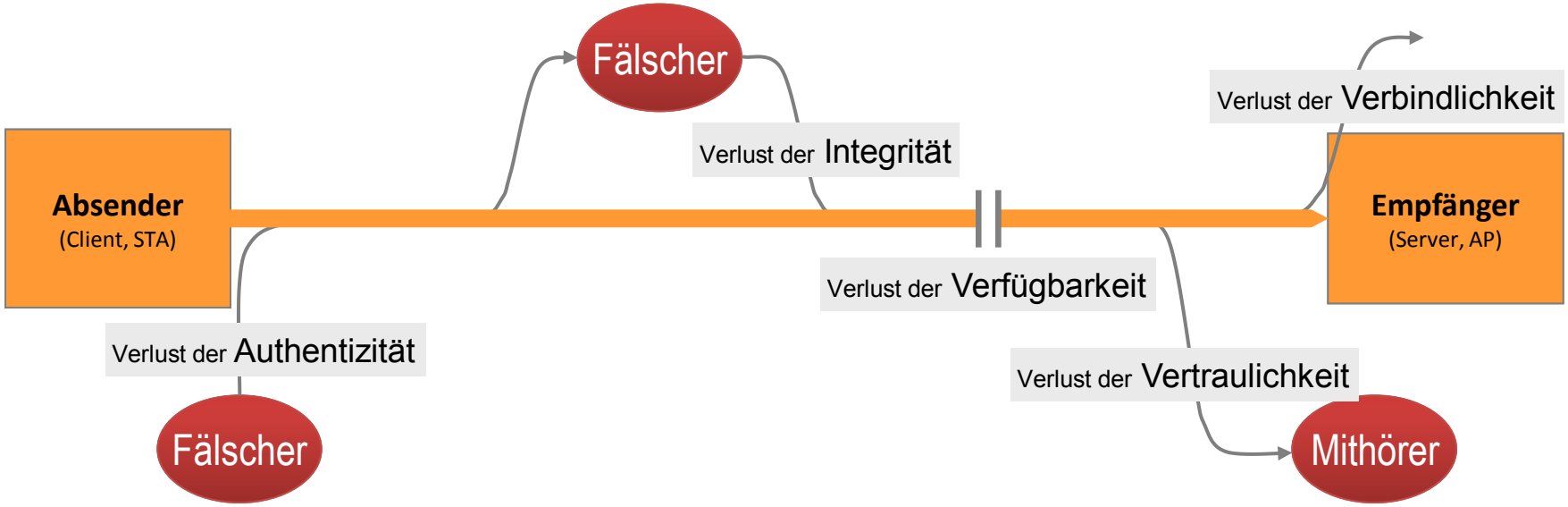


1) Der ID hat das gleiche Format wie eine MAC-Adresse

- Infrastruktur-Netz-Beispiel:
  - Paket wird von MACy für MACx an AP gesendet.
  - AP leitet Paket an MACx weiter.
  - Für die Weiterleitung werden die MAC-Adressen der beiden AP‘s verwendet. Damit erspart man sich ein Tunnelprotokoll.



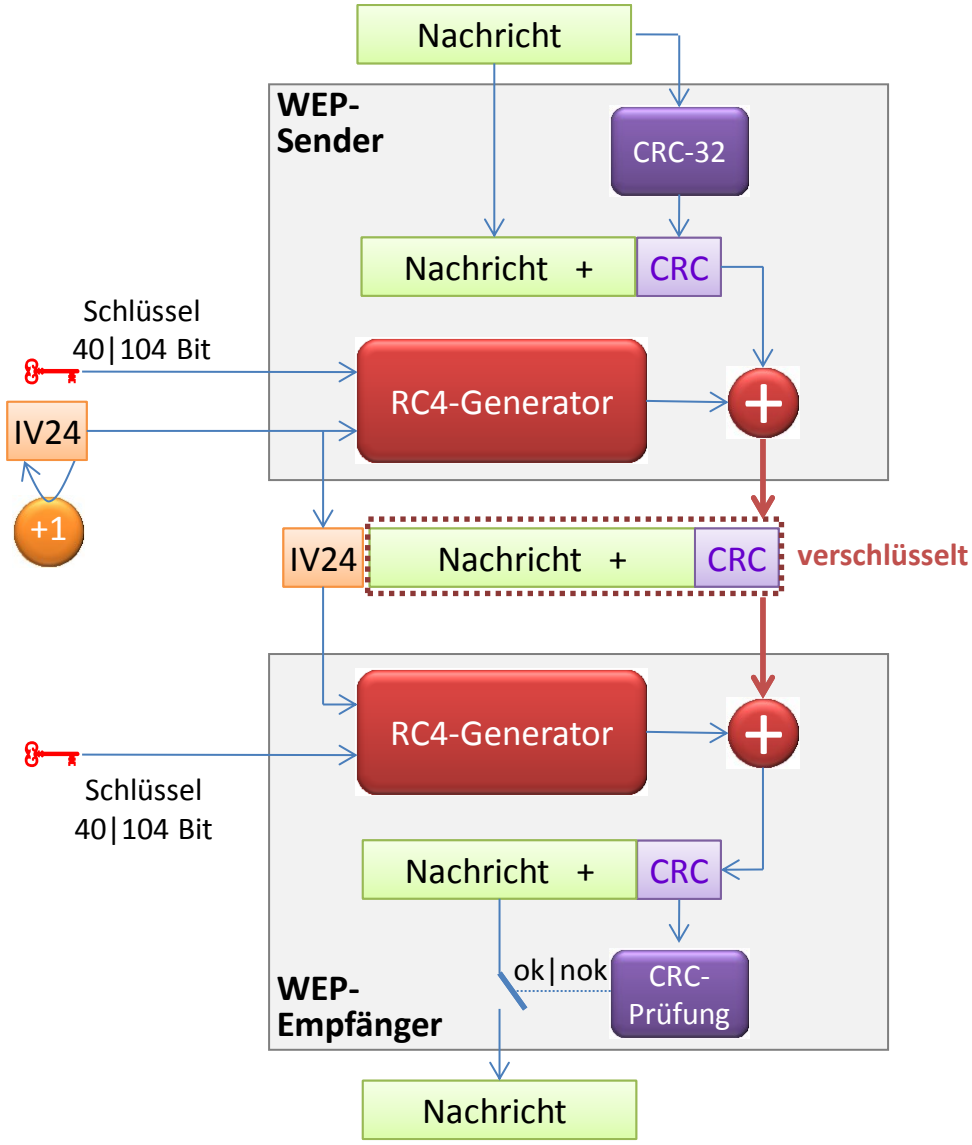
Sicherheit: Allgemeine Aspekte



- Sicherheitsziele sind Herstellung/Bewahrung von:
  - **Authentizität** (authenticity): Echtheit, Glaubwürdigkeit des Absenders garantieren.
  - **Integrität** (integrity) Unversehrtheit der Nachricht garantieren.
  - **Vertraulichkeit** (privacy): Nachricht vor "mitgehören/mitlesen" sichern.
  - **Verfügbarkeit** (availability): Dienst|Daten sind verfügbar.
  - **Verbindlichkeit**: Absender kann nicht das Absenden, Empfänger nicht den Empfang bestreiten.

- Vertraulichkeit, Integrität und Authentizität wurden im IEEE 802.11 durch einen als Wired Equivalent Privacy (**WEP**) bezeichneten Mechanismus gesichert.
- WEP ist mittlerweile vollständig kompromittiert.
- **WEP-Vertraulichkeit** basiert:
  - auf einem **Stromchiffre RC4**, mit der Klardaten paketweise abhängig von einem **Schlüssel und einem Initialisierungsvektor** (IV) in Chiffredaten umgewandelt werden.
  - Schlüssel ist eine Zeichenkette von 40 oder 104 Bit. Dieser muss allen STAs und APs vorab zur Verfügung gestellt werden.
  - Der IV wird vom Absender gewählt und sollte für jedes übertragene Datenpaket unterschiedlich sein. Dieser wird unverschlüsselt übertragen.
- **WEP-Integrität**
  - Für jedes zu übertragene Datenpaket wird eine 32-Bit CRC-Checksumme berechnet. Anschließend wird das Datenpaket und die angehängte Checksumme verschlüsselt.
  - Der Empfänger entschlüsselt das Datenpaket und überprüft die Checksumme. Ist die Checksumme korrekt, wird das Datenpaket angenommen, andernfalls wird es verworfen.
  - *Das verwendete Verfahren eignet sich zwar zur Erkennung von Bitfehlern durch Übertragungsstörungen, es ist jedoch für die Abwehr systematischer Paketfälschungen und damit für die Sicherstellung der Integrität ungeeignet.*

- WEP-Vertraulichkeit/-Integrität basiert zusammengefasst auf:
  - einem geheimen Schlüssel K, 40 | 104 Bit →allen STA's und den APs bekannt.
  - einem Initialisierungsvektor (IV), 24 Bit, der durch den Absender zufällig erzeugt werden sollte und für jede Übertragung inkrementiert wird.
  - Aus K und IV wird nach einem RC4-Algorithmus eine pseudozufällige Bitfolge erzeugt.
  - Die Daten der MSDU werden mit dieser Bitfolge XOR verknüpft.
  - Über MSDU wird mittels CRC-32 Mechanismus ein Integrity Check (IC) realisiert.
  - Der IV wird als Klartext in jeder PDU mitgeschickt, damit Decodierung möglich wird.



IEEE 802.11-Sicherheit: **WEP - Prinzip der Chiffrierung**

- Aus IV und K wird mittels RC-4 eine Pseudozufallsfolge von ***n*** Bits erzeugt.
- Annahme: ***n*** sei hier 8 und die RC-4-ermittelte Folge: **1001 0111**
- Es soll der ISO-8859-1-Text: **HTWM ≡ (48 54 57 4d)$_h$** verschlüsselt werden.

Codierung

MSDU-Text	H	T	W	M
MSDU-Bin	0100 1000	0101 0100	0101 0111	0100 1101
Schlüssel K	1001 0111	1001 0111	1001 0111	1001 0111
MSDN XOR K	1101 1111	1100 0011	1100 0000	1101 1010
entspräche	ß	Ã	À	Ú

Decodierung

MSDN XOR K	1101 1111	1100 0011	1100 0000	1101 1010
Schlüssel K	1001 0111	1001 0111	1001 0111	1001 0111
MSDU-Bin	0100 1000	0101 0100	0101 0111	0100 1101
MSDU-Text	H	T	W	M

XOR	
00	0
01	1
10	1
11	0

- **Authentisierung**: Es kann zwischen zwei Authentisierungsmodi gewählt werden:
  - **„Open“** (hierbei findet keine Authentisierung statt) und
  - **„Shared Key“**. Für die Authentisierung im „Shared Key“-Modus wird ein so genanntes Challenge-Response-Verfahren durchgeführt:
    - Der Access Point generiert 128 zufällige Bytes und sendet diese in einem Datenpaket unverschlüsselt an einen Client (Challenge).
    - Der Client verschlüsselt das Datenpaket und sendet es zurück zum Access Point (Response).
    - Der Client hat sich erfolgreich authentisiert, wenn der Access Point die Response zur Challenge entschlüsseln kann.
    - Der Authentisierungsprozess ist nur einseitig: der Access Point muss sich gegenüber den Clients nicht authentisieren. Zum Authentisieren wird derselbe Schlüssel verwendet wie zur Verschlüsselung der Nutzdaten.
  - Probleme:
    - Schlüsselverteilung muss händisch erfolgen,
    - Viele kennen Schlüssel.
    - Große Netze →schlechte Lösung,
    - kleine Netze→OK!

→WEP verschlüsselt die übertragenen Nutzdaten und die Integritäts-Checksumme. Management- und Steuersignale (Management Frames und Control Frames) werden auf der Funk-Schnittstelle jedoch nicht verschlüsselt.

IEEE 802.11-Sicherheit: **WEP - Authentisierung**

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

BEISPIEL: Anmelde- und Assoziierungsvorgang von STAx am AP1 (vereinfacht), wenn der AP1 ein "**Open System**" ist. Beacon-Frames werden nicht dargestellt (Übersichtlichkeit).

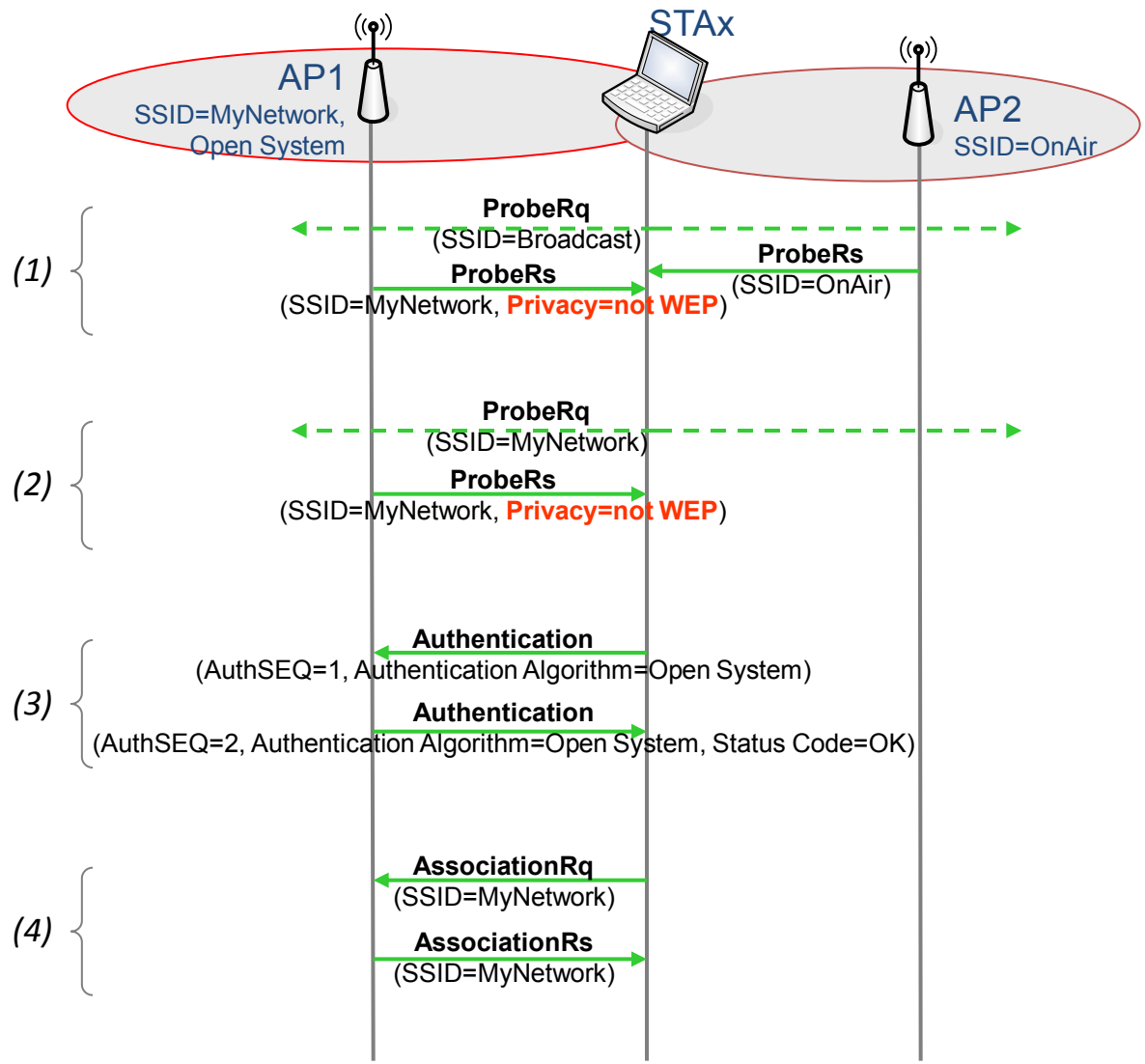
Der Ablauf:

(1) allgemeiner ProbeRq(SSID=Broacast)
→alle aktiven APs antworten mit ProbeRs.

(2) selektives ProbeRq(SSID=MyNetwork)
→nur AP1 (SSID=MyNetwork) antwortet.

(3) Authentication gegenüber AP1, der als "Open System" administriert wurde.

(4) Assoziation zwischen STAx und AP1 herstellen



Legende:
- MAC-Broadcast
- MAC-Unicast

IEEE 802.11-Sicherheit: **WEP - Authentisierung**

BEISPIEL: Anmelde- und Assoziierungsvorgang von STAx am AP1 (vereinfacht), wenn der AP1 ein „WEP-SharedKey-System" ist. Beacon-Frames werden nicht dargestellt (Übersichtlichkeit).

Der Ablauf:

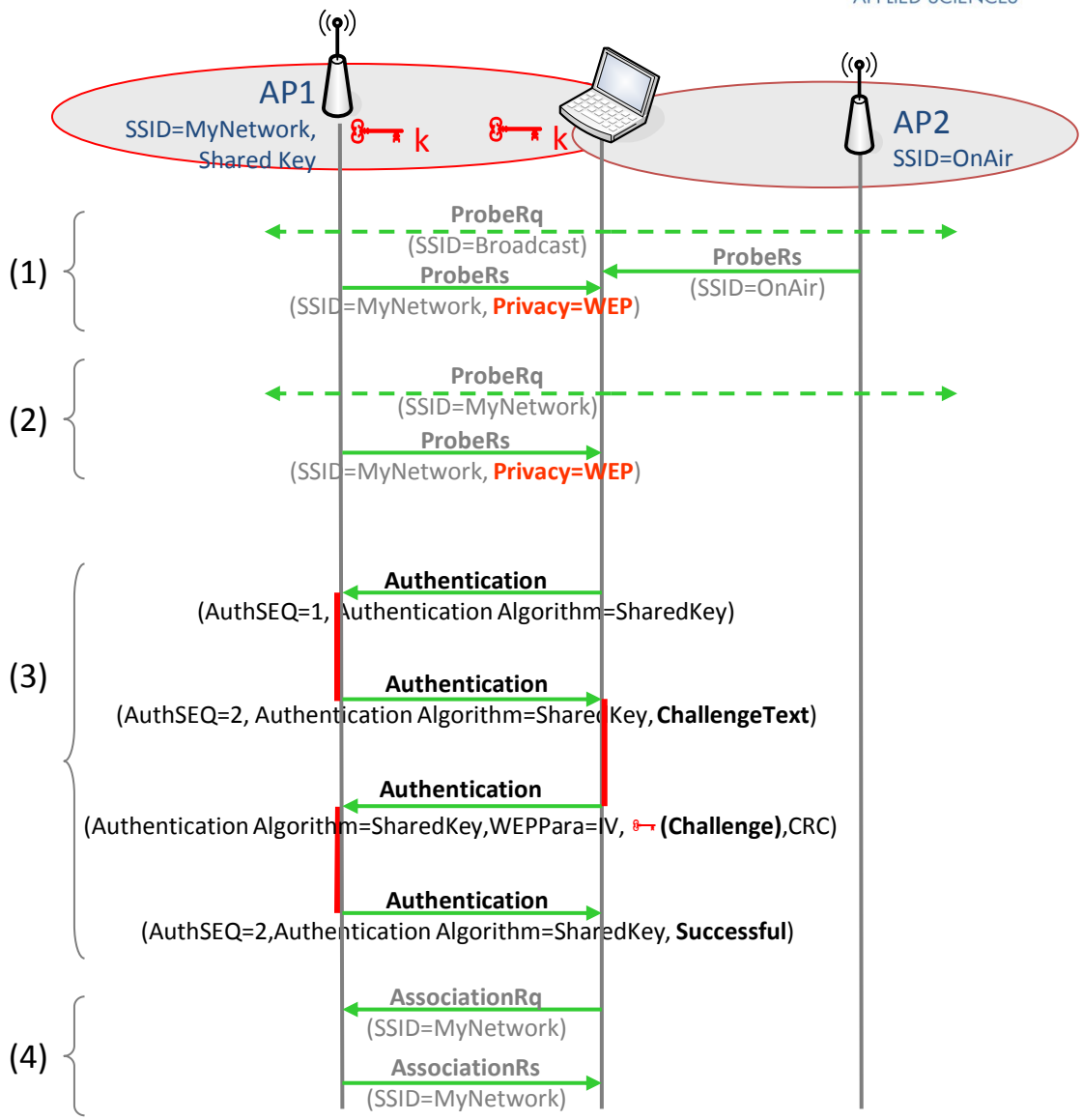
(1) allgemeiner ProbeRq(SSID=Broacast)
→alle aktiven APs antworten mit ProbeRs.

(2) selektives ProbeRq(SSID=MyNetwork)
→nur AP1 (SSID=MyNetwork) antwortet.

(3) Authentication mittels Chared Key:
•AP1 sendet ChallengeText (128 Byte).
•Dieser wird mittels Key k in der STA verschlüsselt und zurück gesendet.
•AP entschlüsselt verschlüsselten Text. Entspricht dieser dem ChallengeText →STA hat den Schlüssel →Zugang erlauben!

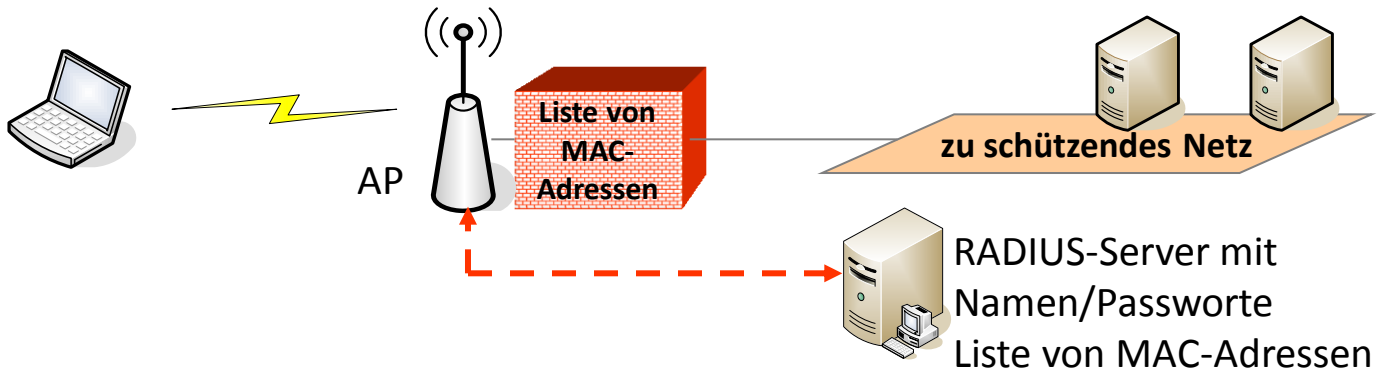
(4) Assoziation zwischen STAx und AP1 herstellen

Legende:
- MAC-Broadcast
- MAC-Unicast



IEEE 802.11-Sicherheit: WEP - Zugangskontrolle über MAC-Adresse

- APs unterstützen eine Zugangskontrolle über MAC-Adressen:
  - Man kann Positivliste oder Negativliste von MAC-Adressen führen
  - AP-Benutzung ist nur dann möglich, wenn die MAC-Adresse der STA in der Liste steht bzw. nicht steht. Die händische Pflege von MAC-Adressen ist nur für kleine Netze OK.
- APs unterstützen i.d.R. die Verwendung des "Remote Authentication Dial-In User Service" (RADIUS). RADIUS ist ein Client-Server-Protokoll
  →zur Authentifizierung (Nutzername/Passwort) →Zugangskontrolle.
  Account und MAC-Adressen werden auf einem zentralen RADIUS-Server gepflegt.



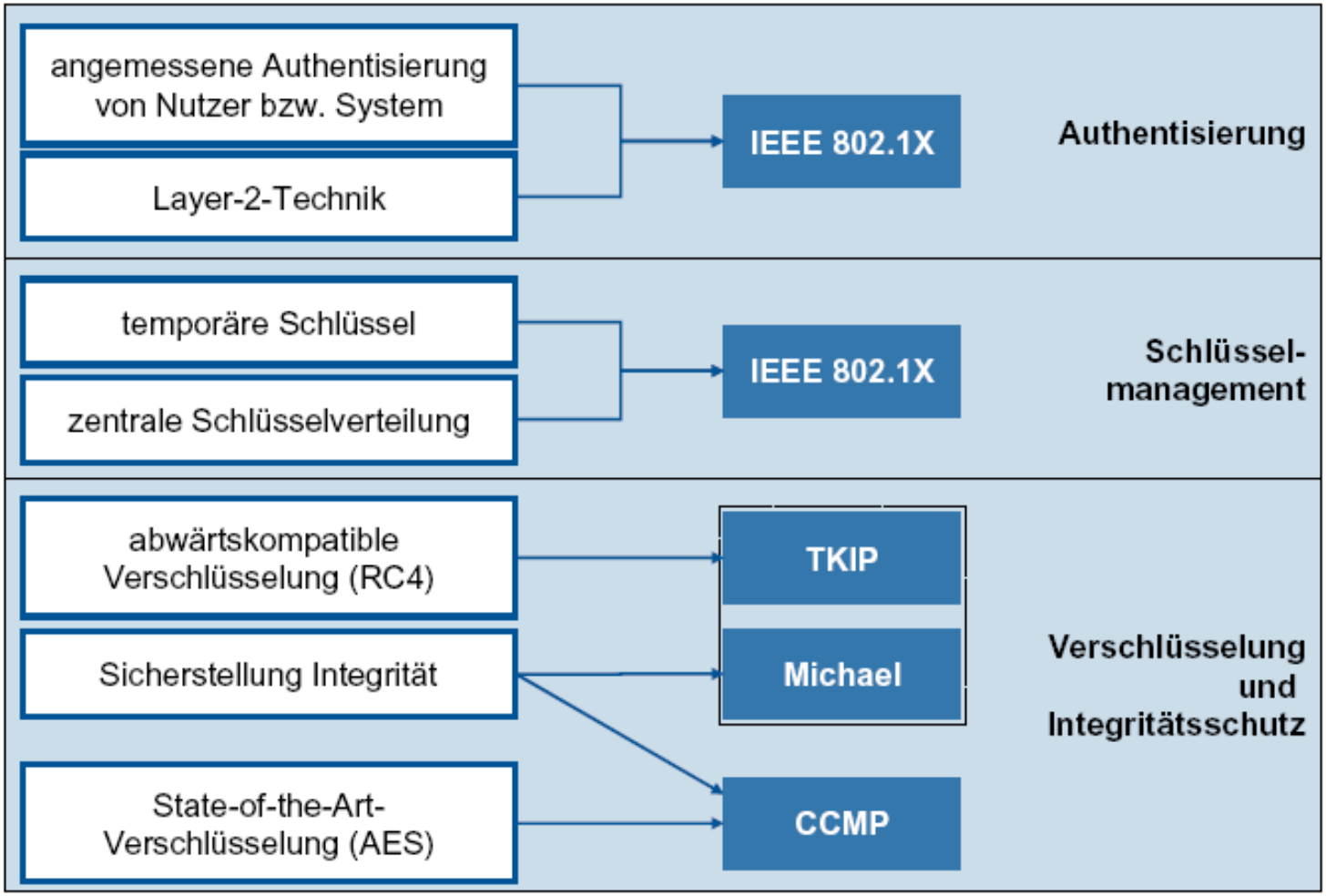
- Mangel dieses Verfahrens:
  - Viele Funkadapter lassen ein Überschreiben der originalen MAC-Adresse zu.
  - Ein Angreifer kann nach Abhören, berechtigte MAC-Adresse verwenden →Verlust der Authentizität.

802.11i-Sicherheit: **Überblick** /BSI2006/

- Die Erweiterung IEEE 802.11i entstand, um die aufgetretenen Sicherheitslücken von WEP zu schließen. IEEE 802.11i umfasst die Bereiche:
  →Verschlüsselung, →Authentisierung und →Schlüsselmanagement.
- Da die in IEEE 802.11i verabschiedete Lösung abwärtskompatibel zu WEP sein musste, umfasst sie zwei verschiedene Verschlüsselungsverfahren:
  - Temporal Key Integrity Protocol (TKIP) mit Integritätsprüfung Michael. TKIP ist eine als Temporärlösung aufzufassende abwärtskompatible Lösung, die sich insbesondere zur verbesserten Absicherung bereits bestehender WLANs eignet.
  - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). CCMP ist eine langfristige Lösung, die neue Hardware erfordert.
- Die Authentisierung erfolgt entweder
  - über IEEE 802.1X (in diesem Fall erfolgt das Schlüsselmanagement auch über IEEE 802.1X) oder
  - Pre-Shared Keys.

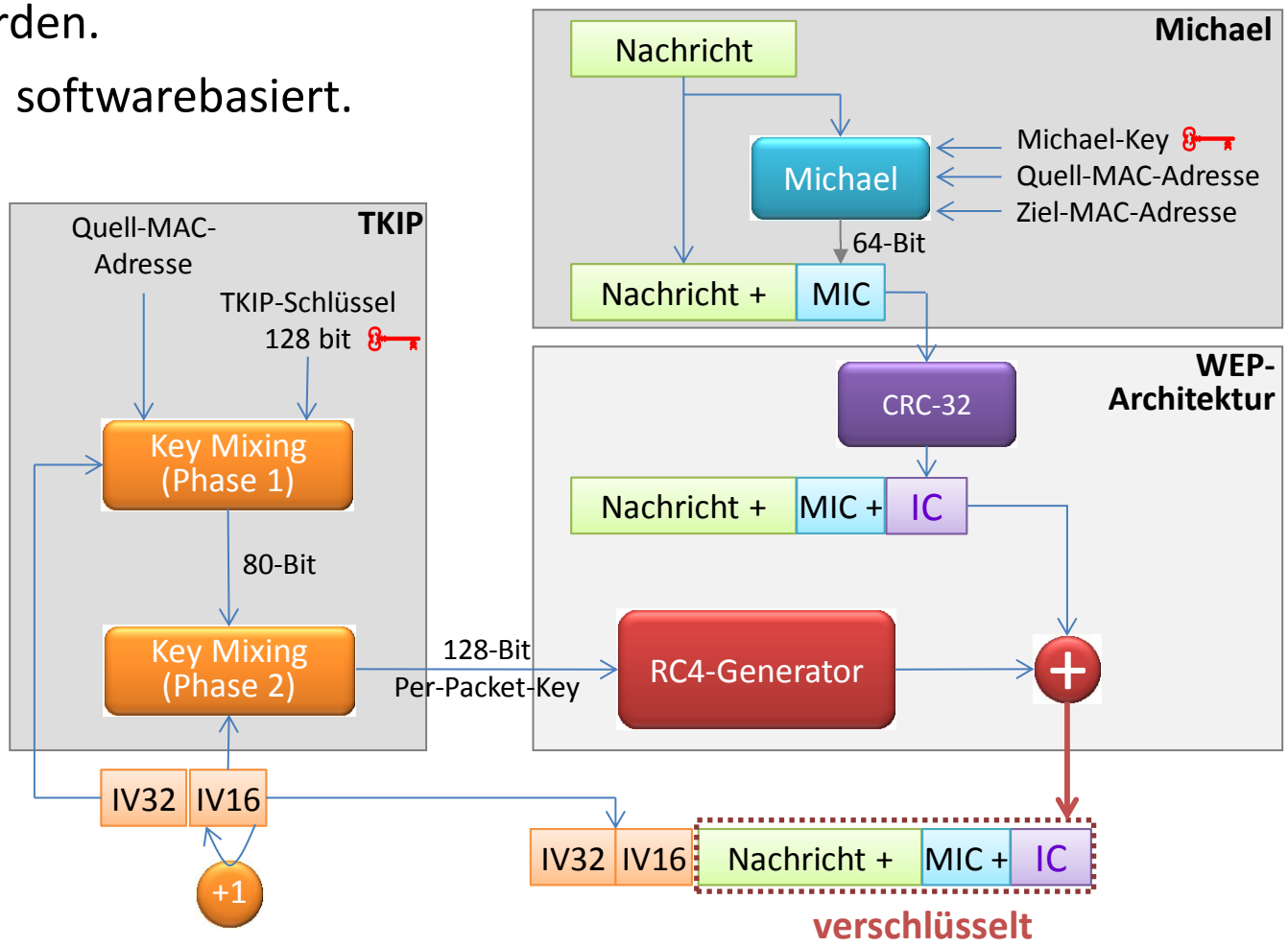
WPA-Variante		WPA	WPA2
Personal Mode	Authentifizierung	PSK	PSK
	Verschlüsselung	TKIP/MIC	AES-CCMP
Enterprise Mode	Authentifizierung	802.1X/EAP	802.1X/EAP
	Verschlüsselung	TKIP/MIC	AES-CCMP

802.11i-Sicherheit: **Überblick** /BSI2006/



AES ..... Advanced Encryption Standard ist ein symmetrisches Kryptosystem
CCMP ..... Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
IEEE 802.1X ..... Methode für die Authentifizierung und Autorisierung in IEEE 802-Netzen
Michael ..... Algorithmus zur Erzeugung des Message IntegrityCode (MIC)
TKPI ..... Temporal Key Integrity Protocol

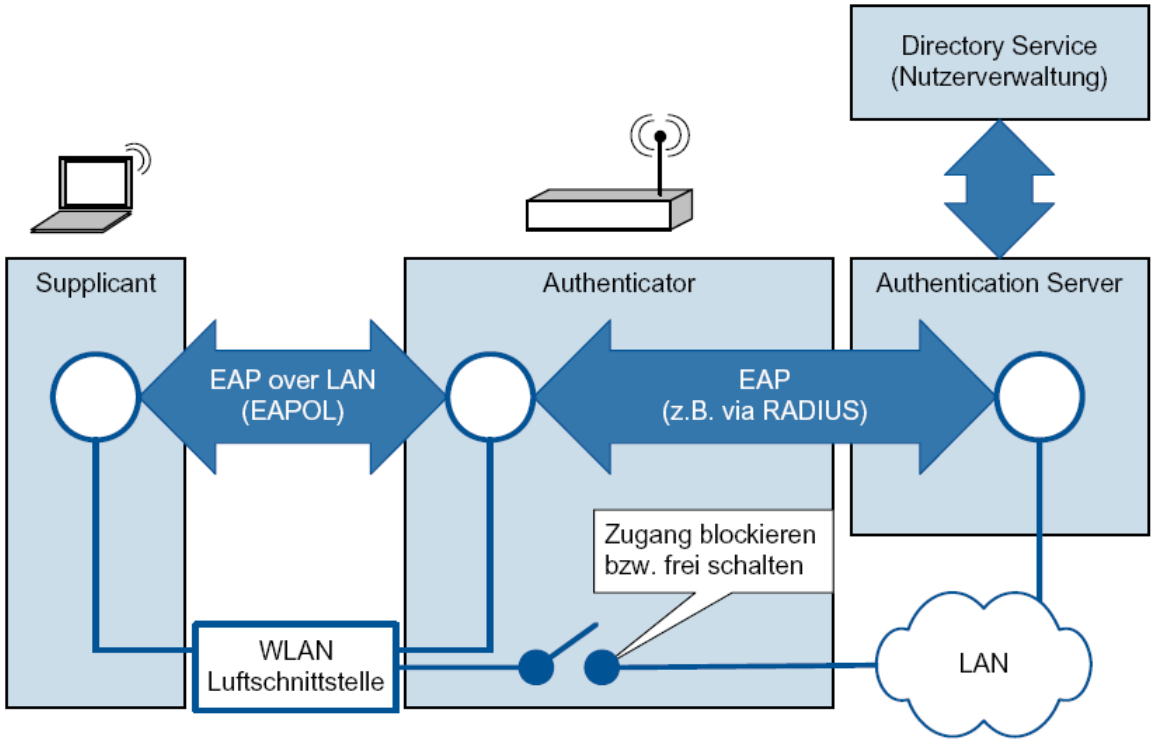
- WPA kann auch auf WEP-basierender Hardware genutzt werden.
- Michael und TKIP sind softwarebasiert.



IV	Initialisierungsvektor
MIC	Message Integrity Check
Michael	Verfahren zur Integritätssicherung
RC4	Pseudo-Zufallsgenerator
TKIP	Temporal Key Integrity Protocol

802.11i-Sicherheit: **IEEE 802.1X** /BSI2006, Abb. A-9/

- **Supplicant** ist Software auf Client, gibt es für alle Betriebssysteme.
- **Authenticator** ist der AP.
- **Authentication Server** ist üblicherweise ein RADIUS-Server
- **Extensible Authentication Protocol** (EAP) unterstützt mehrere Authentikations-verfahren und dient auch zur Schlüsselverteilung vom Authenticator zum Supplicant.



EAPOL - Extensible Authentication Protocol over LAN

IEEE 802.11i-Sicherheit: **Zusammenfassung**

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

Bezeichnung	Authentizität	Integrität	Vertraulichkeit
802.11→ WEP wired equivalency privacy	Beim Zugang einer STA zum AP wird geprüft, ob diese im Besitz des aktuellen Schlüssels Ki ist. Der AP erzeugt Zufallstext, für STA. Diese verschlüsselt Text mit Schlüssel Ki und sendet an AP. AP prüft, ob Text mit aktuellem Ki verschlüsselt wurde. Ja, Zugang erlaubt.	Die Sendedaten werden vor der Verschlüsselung mit einer 32-Bit-Prüfsumme (CRC) versehen. Der Empfänger prüft, ob Inhalt und Prüfsumme zusammenpassen. Ja, Inhalt vermutlich integer.	Die Daten mit Prüfsumme werden mittels eines Stromchiffre kodiert. Dazu wird aus dem Schlüssel Ki (40 oder 104 Bit) und einem zufälligen 24-Bit-Wert (Initialisierungsvektor, IV) eine Pseudozufallsfolge nach einem RC-4-Algorithmus erzeugt und mit den Datenbits EXOR verknüpft. Der Schlüssel Ki wird händisch verteilt.
802.11.i → WPA WPA=WiFi Protected Access, ist ein Profil aus 802.11.i	Zwei Möglichkeiten (1) Wie bei WEP (2) Nach 802.1X: Die STA muss <user> und <pwd> an AP senden. AP lässt prüfen. Wenn <user> und <pwd> zusammenpassen →Zugang	Hier kommt ein zweistufiges Verfahren zur Anwendung: (A) Über Sendedaten, Michael-Schlüssel, Ziel- und Absender-MAC-Adresse wird Hashwert als Integritätsschutz gebildet. (B) Danach erfolgt die übliche WEP-Prüfsummenbildung	Die Daten mit der zweistufigen Prüfsumme werden mittels eines Stromchiffre kodiert. Die Schlüsselbildung ist bedeutend komplexer. Jedes Paket wird mit einem anderen Schlüssel kodiert. Die Schlüsselverteilung erfolgt über ein Verfahren TKPI (Temporal Key Integrity Protocol)
802.11.i → WPA2	Anmeldung nur noch mittels 802.1X	Hier werden Integrität und Vertraulichkeit durch ein mächtigeres Verschlüsselungsverfahren realisiert → CCMP - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol	

Literatur

Fachbücher/Fachaufsätze	
/Rech2008/	J. Rech: Wireless LANs, Heise 2008, ISBN 978-3-936931-51-8
/Sch2000/	J. Schiller: Mobilkommunikation, Addison-Wesley, 2000, ISBN 3-8273-1578-6
/BSI2006/	Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte, Bundesamt für Sicherheit in der Informationstechnik, 2006. http://www.bsi.de/literat/doc/drahtkom/drahtkom.pdf
Taschenbuch	
/STEIN/	Taschenbuch Rechnernetze und Internet, Fachbuchverlag Leipzig, 2004, ISBN 3-446-22573-0
Standards	
/IEEE802.11/	IEEE 802.11 Second edition 2005-08-01: Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications (Includes IEEE Std 802.11, 1999 Edition; IEEE Std 802.11a.-1999; IEEE Std 802.11b.-1999; IEEE Std 802.11b.-1999/Cor 1-2001; and IEEE Std 802.11d.-2001) ISO/IEC 8802-11 IEEE Std 802.11 Second edition 2005-08-01
Tools	
/NetStumbler/	Anzeige drahtloser Netze im Empfangsbereich und deren Einstellungen, http://stumbler.net/
/WireShark/	OpenSource Netzwerkanalyse-Tool, http://www.wireshark.org/
URLs	
/ELKO/	Elektronik-Kompendium, 2006, http://www.elektronik-kompendium.de/sites/net/0610051.htm
/FreiFunk/	Freie funkbasierte Netze, 2006, http://freifunk.net/downloads/freifunk-praesentation_v11_060804_03_jpn.pdf
/Brenner/	Wireless topics, http://www.sss-mag.com/wlstopics.html
/Murphy/	OFDM http://www.wirelesstrainingsolutions.com/class/mod/forum/discuss.php?d=13 (14, 15)