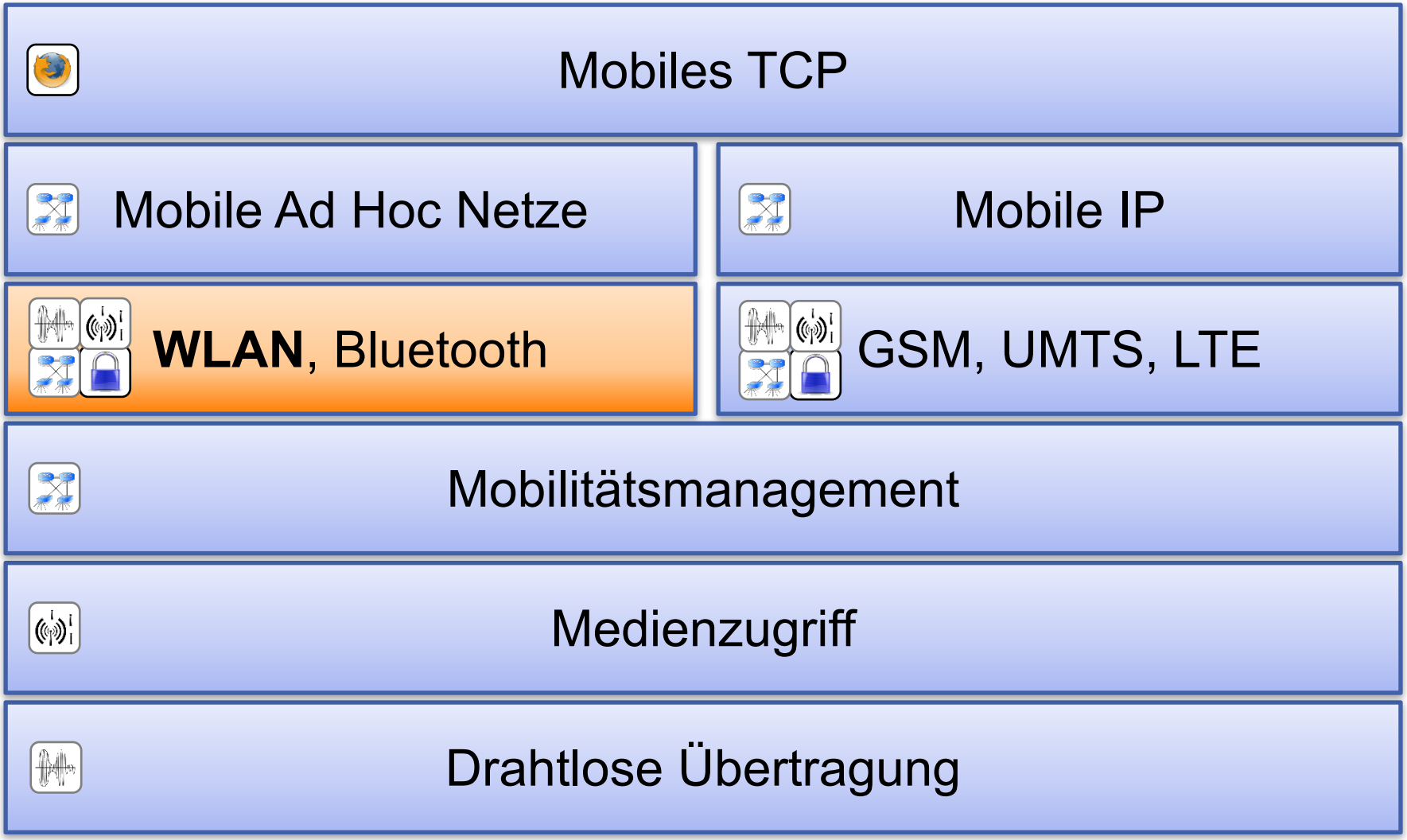
Karlsruher Institut für Technologie

Kapitel 5 – WLAN nach IEEE 802.11

Vorlesung Mobilkommunikation Wintersemester 2016/17
Prof. Dr. Oliver Waldhorst (HS Karlsruhe), Markus Jung

INSTITUT FÜR TELEMATIK

Gliederung


Mobiles TCP
Mobile Ad Hoc Netze
Mobile IP
WLAN, Bluetooth
GSM, UMTS, LTE
Mobilitätsmanagement
Medienzugriff
Drahtlose Übertragung

Charakteristika drahtloser lokaler Netze (Wireless Local Area Networks, WLAN)

- Vorteile
  - Keine Verkabelungsprobleme
    - z.B. historische Gebäude, Feuerschutz
  - Geringere Kosten für Inbetriebnahme
    - Ein Zugangspunkt wird von vielen Nutzern genutzt
  - Geräte räumlich flexibel platzierbar innerhalb eines Empfangsbereichs
  - Ad-hoc-Netze ohne vorherige Planung realisierbar
  - Robustheit gegenüber Beschädigungen
    - Katastrophen wie Erdbeben, Feuer - und unachtsame Benutzer

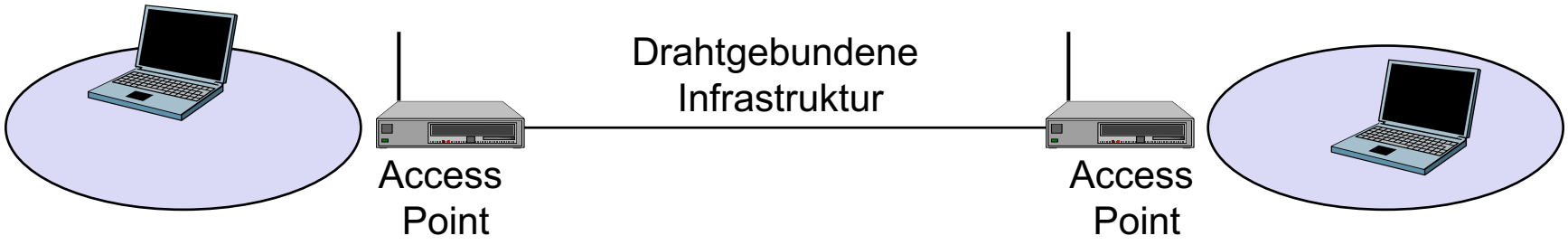
- Nachteile
  - Geringere Übertragungsraten als Festnetze
    - z.B. max. 54 Mbit/s bei IEEE 802.11a/g, max. 600 Mbit/s bei IEEE 802.11n
  - Geringere Dienstgüte
    - Übertragungsfehler, Verzögerung und Jitter größer
  - Sicherheit
    - Abhören der Luftschnittstelle leicht möglich

Entwurfsziele für drahtlose lokale Netze

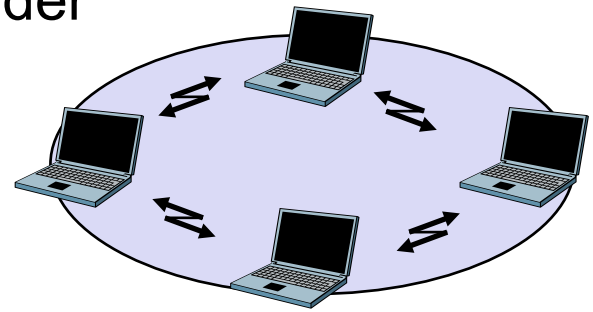
- Weltweite Funktion
- Betrieb ohne Sondergenehmigungen bzw. Lizenzen möglich
- Möglichst geringe Leistungsaufnahme wegen Batteriebetrieb
- Robuste Übertragungstechnik
- Vereinfachung der (spontanen) Zusammenarbeit bei Treffen
  - Einfache Handhabung und Verwaltung (Plug & Play)
- Schutz bereits getätigter Investitionen im Festnetzbereich
  - Interoperabilität zwischen LANs und WLANs
  - Transparenz für höhere Schichten
- Sicherheit hinsichtlich
  - Abhören vertraulicher Daten
  - Emissionen
    - z.B. keine Interferenzen mit Herzschrittmachern

Ausprägungsformen drahtloser LANs

- Infrastruktur-Netze
  - Geräte sind drahtlos über einen Zugangspunkt (AP - Access Point) mit der drahtgebundenen Infrastruktur verbunden



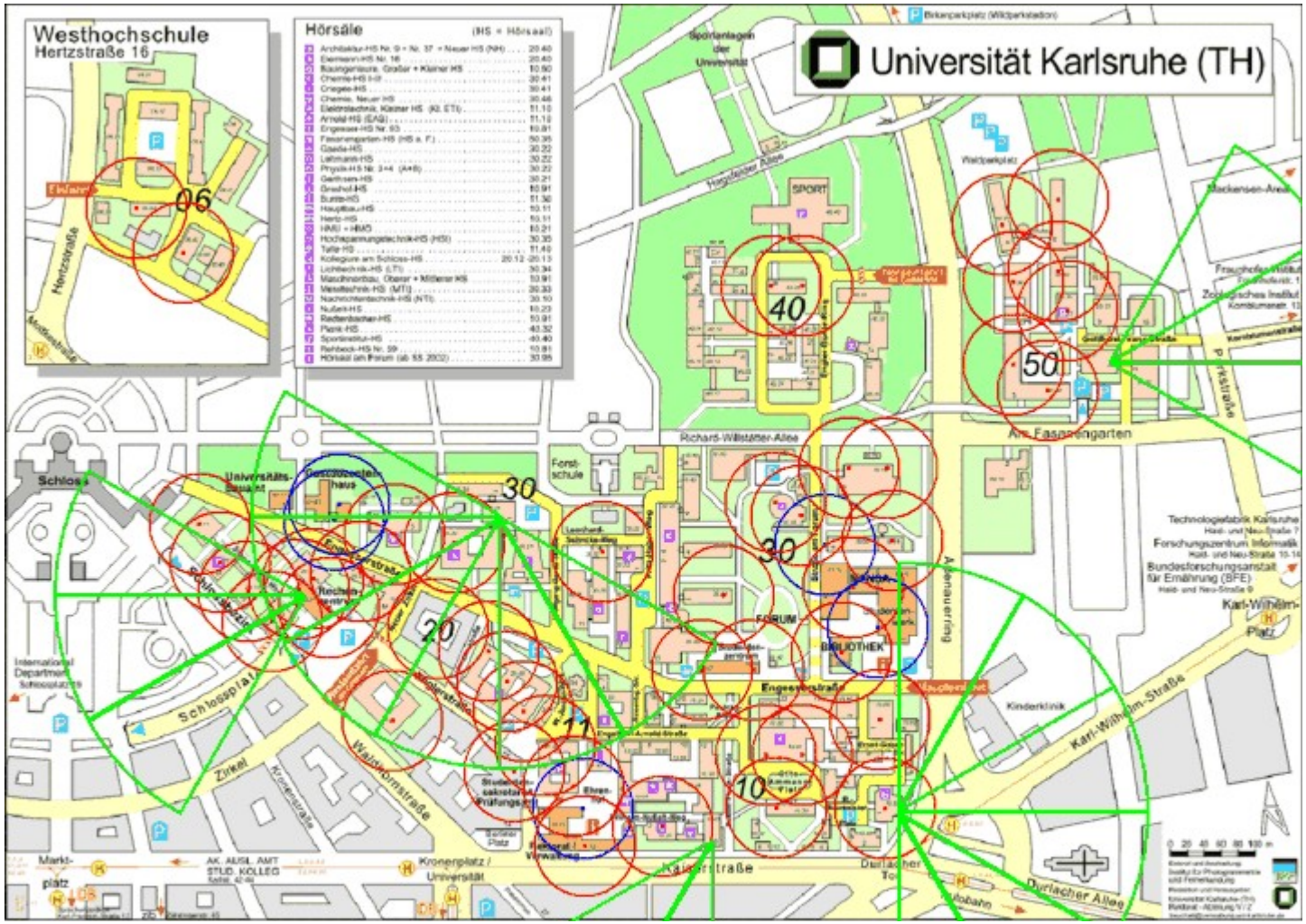
- Ad-hoc-Netze
  - Geräte kommunizieren ohne drahtgebundene Infrastruktur direkt miteinander



WLAN-Lösungen

- IEEE 802.11
  - Basisstandard wurde am 26.07.1997 verabschiedet
  - Erweiterungen der physikalischen Schicht (PHY-Schicht)
    - 802.11a/b/g/n
  - Erweiterungen der Medienzugriffsschicht-Schicht (MAC-Schicht)
    - 802.11h/e/i
  - Hohe Verbreitung (→ in diesem Kapitel behandelt)
- HIPERLAN – High Performance Radio Local Area Network
  - Europäischer Standard
  - Version 1: 23,529 Mbit/s im 5 GHz Band
  - Version 2: 54 Mbit/s im 5 GHz Band
  - Derzeit keine Produkte verfügbar
- HomeRF – Home Radio Frequency
  - Standardisierung durch Firmenkonsortium
    - u.a. Intel, Compaq, IBM, HP, Microsoft, Motorola
  - Speziell für Privatanwender konzipiert
    - Einfache Installation/geringe Kosten
  - Geringe Verbreitung
  - HomeRF Working Group hat sich im Januar 2003 aufgelöst

Beispiel: DUKATH



blau = Außenantennen

rot = Innenantennen

grün = Richtantennen

Aufbau:

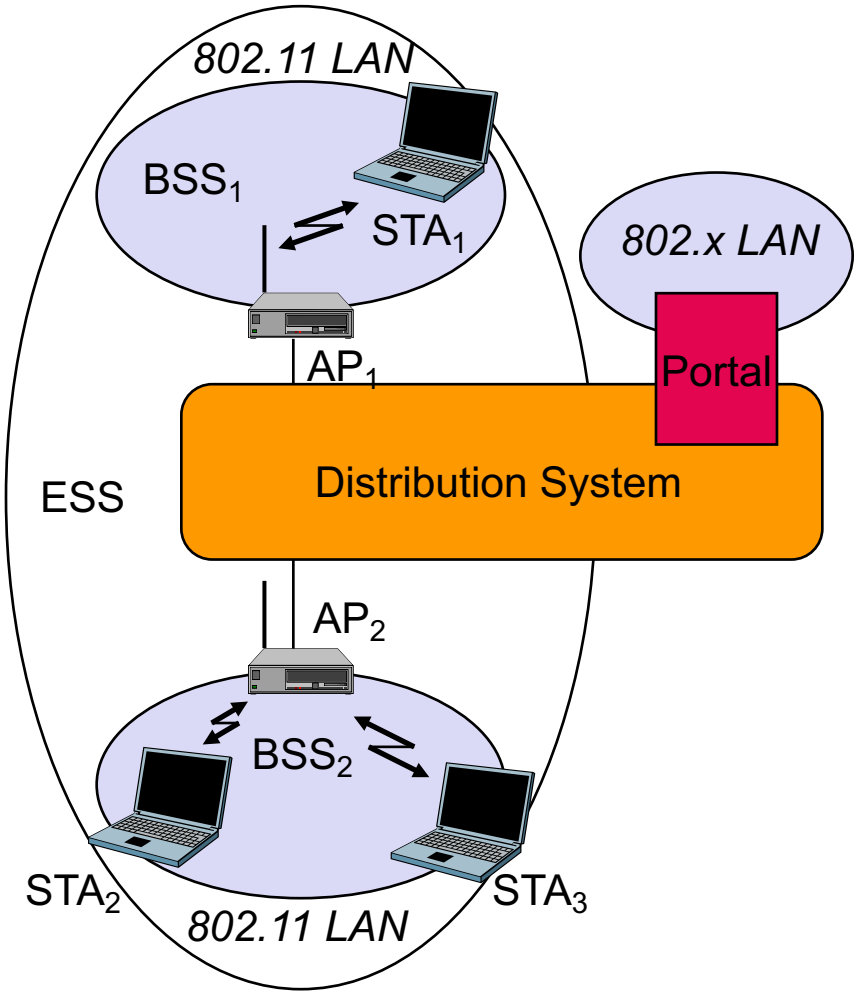
- ca. 210 Zugangspunkte
- IEEE 802.11 b/g

Abdeckung damals:

- ca. 80 % der Campusfläche
- 37 Hörsäle/Seminarräume

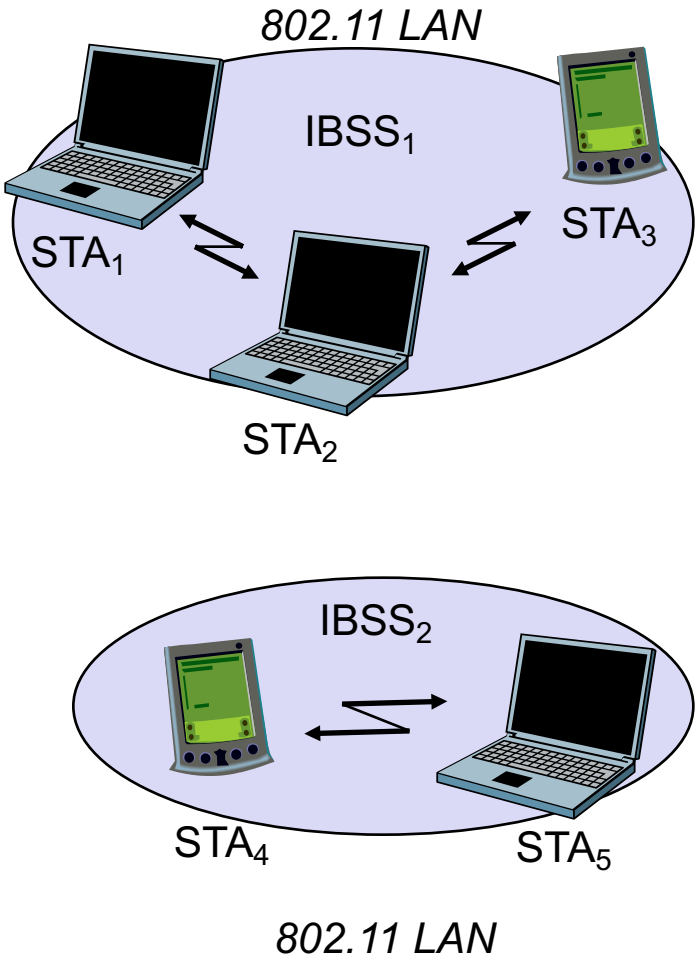
[5.6]

Architektur eines Infrastrukturnetzes



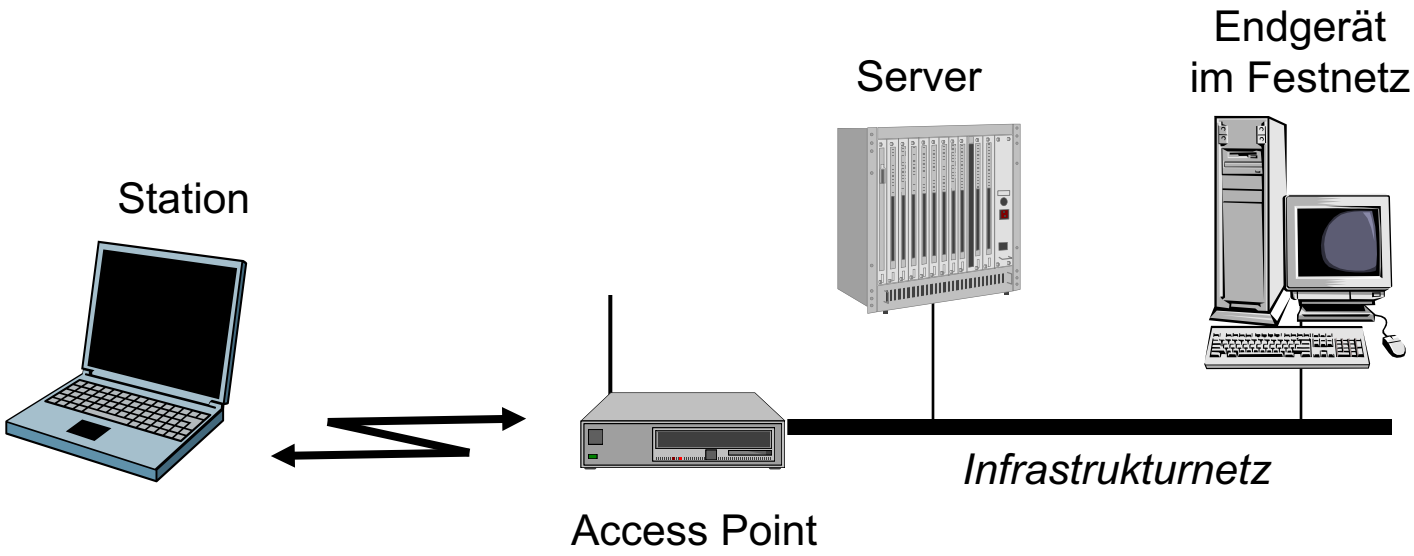
- Station (STA)
  - Endgeräte mit Zugriffsfunktion auf das drahtlose Medium und Funkkontakt zum Zugangspunkt (AP – Access Point)
- Basic Service Set (BSS)
  - Gruppe von Stationen + AP, die auf dem selben Kanal (Funkfrequenz) miteinander kommunizieren
- Access Point (AP)
  - Station, die sowohl an einem BSS als auch am Distribution System teilnimmt.
- Portal
  - Übergang in ein anderes Netz
- Distribution System (DS)
  - Verbindung mehrerer BSS zu einem Extended Service Set (ESS)
  - Architektur des Distribution System ist nicht Teil des Standards

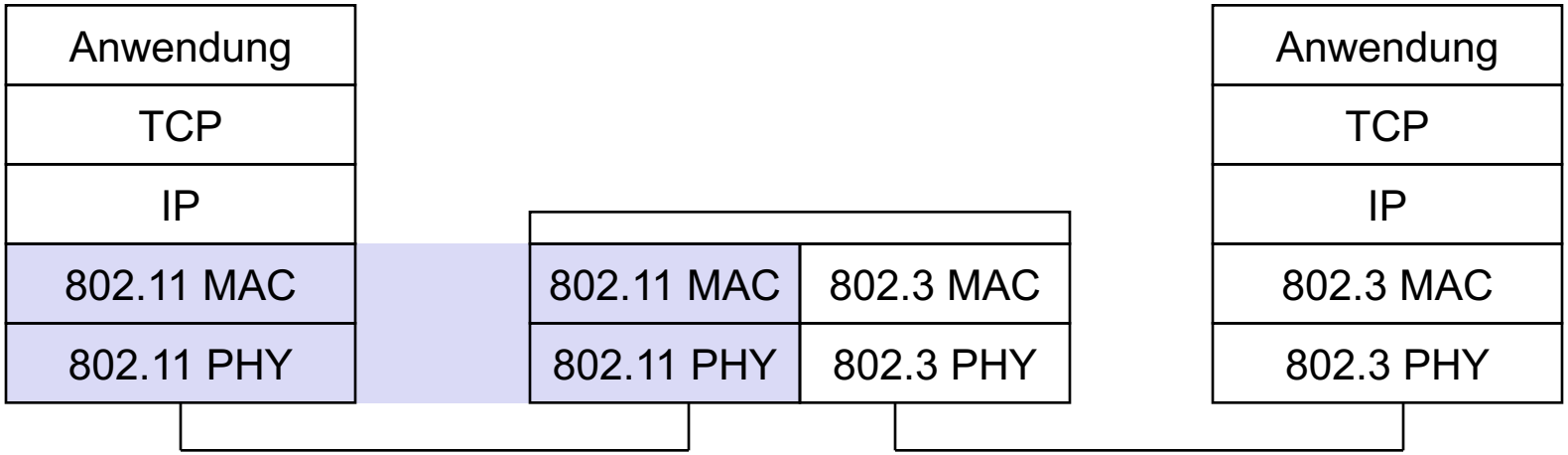
Architektur eines Ad-hoc-Netzs



- Direkte Kommunikation der Geräte
  - Begrenzte Reichweite
- Station (STA)
  - Endgerät mit Zugriffsfunktion auf das drahtlose Medium
- Independent Basic Service Set (IBSS)
  - Gruppe von Stationen, die auf dem selben Kanal (Funkfrequenz) miteinander kommunizieren
- Bildung verschiedener IBSSs
  - Nutzen unterschiedlicher Kanäle (Funkfrequenzen)
  - Raummultiplexen (genügend Abstand)
  - DSSS

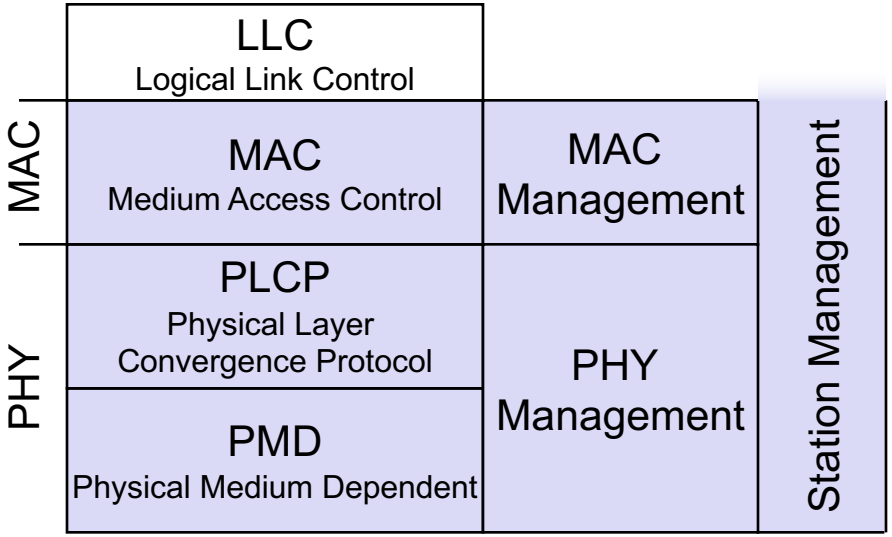
Protokollstack





Schichten und Funktionen

- MAC
  - Medienzugriff
  - Fragmentierung
  - Verschlüsselung
- MAC-Management
  - Synchronisation
  - Scanning
  - Association/Reassociation
  - Power-Management
  - Authentifizierung/ Verschlüsselung



- PLCP
  - Einheitlicher PHY-Zugangspunkt unabhängig von Übertragungstechnik
  - Clear Channel Assessment Signal
  - Signalschwelle für Carrier Sense
- PMD
  - Modulation
  - Codierung
- PHY Management
  - Kanalwahl
- Station Management
  - Koordination der Management-Funktionen

PHY-Schicht

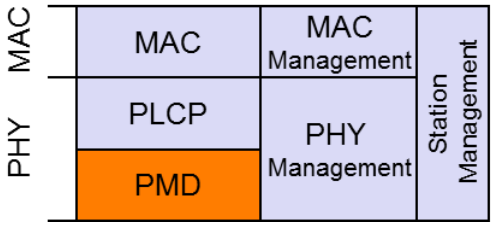
- Basisstandard definiert 3 Varianten
  - Direct Sequence Spread Spectrum (DSSS)
    - Datenraten von 1 – 2 Mbit/s
    - Weite Verbreitung
    - Heute noch in 802.11b/g-Komponenten enthalten
  - Frequency Hopping Spread Spectrum (FHSS)
    - Datenraten von 1 – 2 Mbit/s
    - Keine WLAN-Komponenten verfügbar, die FHSS verwenden
      - Aber: Bluetooth verwendet FHSS
    - … im Weiteren nur kurz berücksichtigt
  - Infrarot
    - Datenraten von 1 – 2 Mbit/s
    - Keine WLAN-Komponenten verfügbar, die Infrarot verwenden
      - Aber: IrDA verwendet Infrarot
    - … im Weiteren nicht berücksichtigt

DSSS in IEEE 802.11

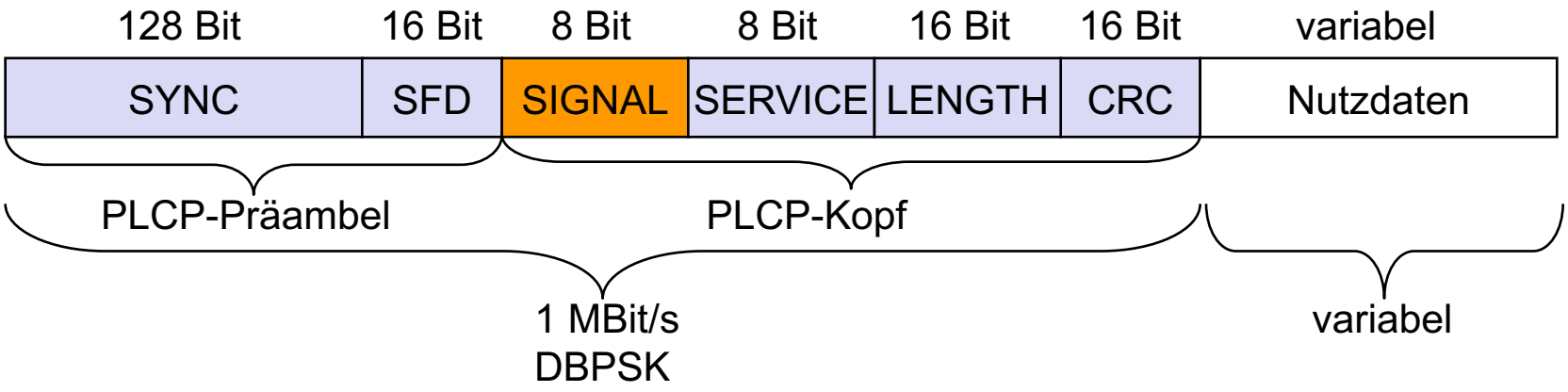
- Verwendung des 11-Chip Barker-Codes für die Spreizung im Basisstandard
  - Bei einer Datenrate von 1 oder 2 Mbit/s
    - Bei höheren Datenraten verwendet man andere Codes, s.u.

[5.11]

  - Code: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1
    - Konvention: +1 repräsentiert logische 0, -1 repräsentiert logische 1 → Code: 01001000111
    - Länge der Chipping-Sequenz ist 11
  - Konstante Symbolrate von 1 MSymbol/s
    - Achtung: In 802.11 ist Symbol die Wellenform für Übertragung einer Gruppe von Chips!
      - 11 oder 22 Chips bzw. 1 oder 2 Datenbits
    - Symbolrate im Sinn von Kapitel 2 ist in 802.11 Modulationsrate
      - Immer 11 MBd!
- Verwendete Modulationsverfahren
  - Differential Binary Phase Shift Keying (DBPSK)
    - 11 Chips/Symbol → 1 Bit/Symbol → Datenrate: 1 Mbit/s
  - Differential Quadrature Phase Shift Keying (DQPSK)
    - 22 Chips/Symbol → 2 Bit/Symbol → Datenrate: 2 Mbit/s



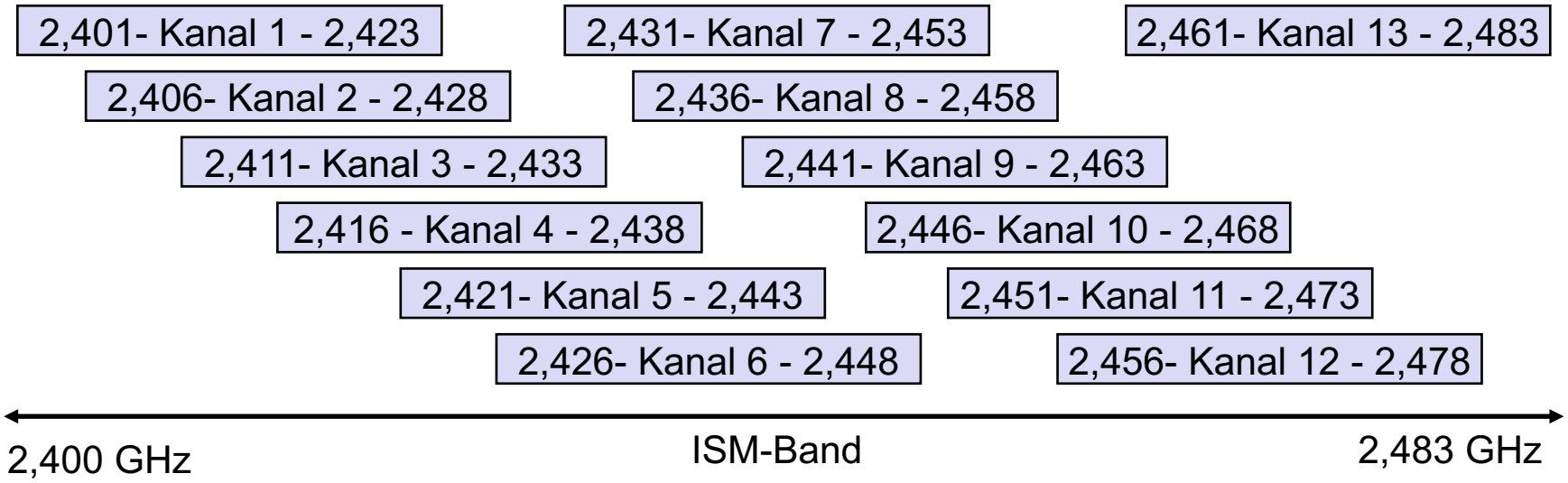
Format einer DSSS-Dateneinheit



- SYNC: Synchronisation
  - Synchronisation über die Bitfolge 101010....
- SFD: Start Frame Delimiter
  - Bitfolge 1111001110100000 kennzeichnet Ende der Präambel und Anfang vom PLCP-Kopf
- SIGNAL
  - Datenrate, mit der Nutzdaten übermittelt werden
  - Erleichtert Rückwärtskompatibilität
- SERVICE
  - Reserviert (wird z.B. von IEEE 802.11b/g verwendet)
  - 0x00 zeigt 802.11 Rahmen an
- LENGTH
  - Zeit [µs], die für die Übertragung der Nutzdaten benötigt wird
- CRC
  - Prüfsumme über den PLCP-Kopf
  - Prüfpolynom: ITU-T-CRC-16

DSSS-Kanalaufteilung

- WLAN verwendet das ISM-Band
  - Untergliederung in 13 Frequenzbänder/Kanäle im Bereich 2,4000 – 2,4835 GHz
    - Breite eines Frequenzbandes: 22 MHz
  - Max. 3 nicht überlappende Kanäle realisierbar
- Aufteilung



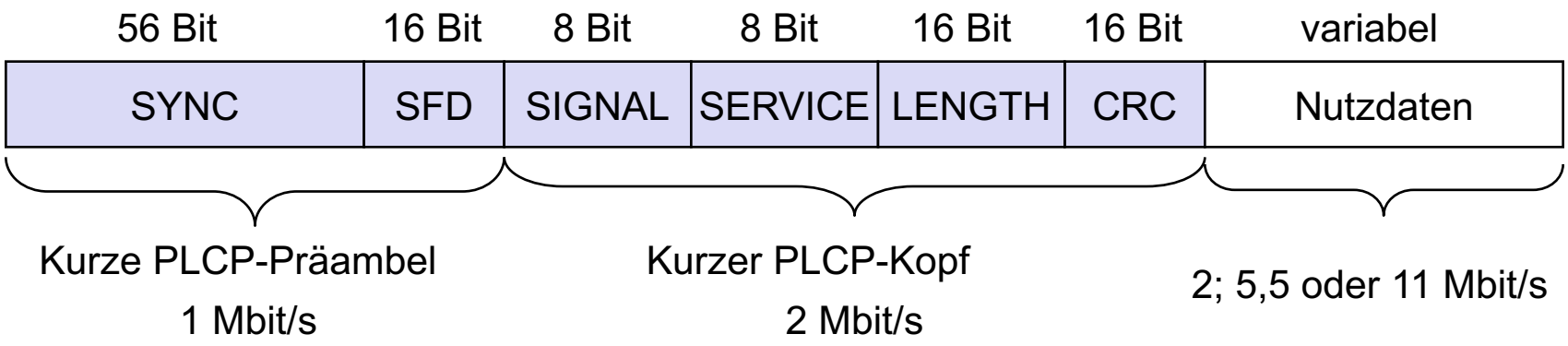
Erweiterungen

- IEEE 802.11b
  - Datenraten von 5,5 und 11 Mbit/s im 2,4 GHz-Band
  - Abwärtskompatibel zum Basisstandard
  - Einsatz von Complementary Code Keying (CCK)
  - Definition eines Formats für kurze Dateneinheiten
- IEEE 802.11g
  - Datenraten von 6 - 54 Mbit/s im 2,4 GHz-Frequenzbereich
  - Einsatz von OFDM
  - Abwärtskompatibel zu 802.11 und 802.11b
- IEEE 802.11a
  - Datenraten von 6 - 54 Mbit/s im 5 GHz-Frequenzbereich
  - Einsatz von OFDM
- IEEE 802.11n
  - Datenraten von bis zu 600 Mbit/s im 2.4 GHz- und 5 GHz Frequenzbereich
  - Einsatz von Multiple Input Multiple Output (MIMO) mit OFDM

IEEE 802.11b

- Verwendung eines 8 Bit langen Complementary Codes anstelle des 11 Bit langen Chip Baker Codes (Complementary Code Keying – CCK)
  - Modulationsrate bleibt bei 11 MBd
  - Neue Symbolrate = 1 MSymbol/s * 11 / 8 = 1,375 MSymbol/s
  - Chipping Sequence wird durch (einen Teil der) Nutzdaten bestimmt
    - d.h. durch verwendeten Spreizcode werden gleichzeitig Nutzdaten übermittelt
- Realisierung der höheren Datenraten
  - 4 Bit pro Symbol → Datenrate = 1,375 MSymbol/s * 4 Bit/Symbol = 5,5 MBit/s
    - 2 Bit werden über DQPSK moduliert
    - 2 Bit wählen einen von 4 komplexen Codes aus
  - 8 Bit pro Symbol → Datenrate = 1,375 MSymbol/s * 8 Bit/Symbol = 11 MBit/s
    - 2 Bit werden über DQPSK moduliert
    - 6 Bit wählen einen von 64 komplexen Codes aus
- Da Empfänger alle 4 bzw. 64 Codes kennt, kann er den verwendeten Code herausfinden und damit die Nutzdaten dekodieren

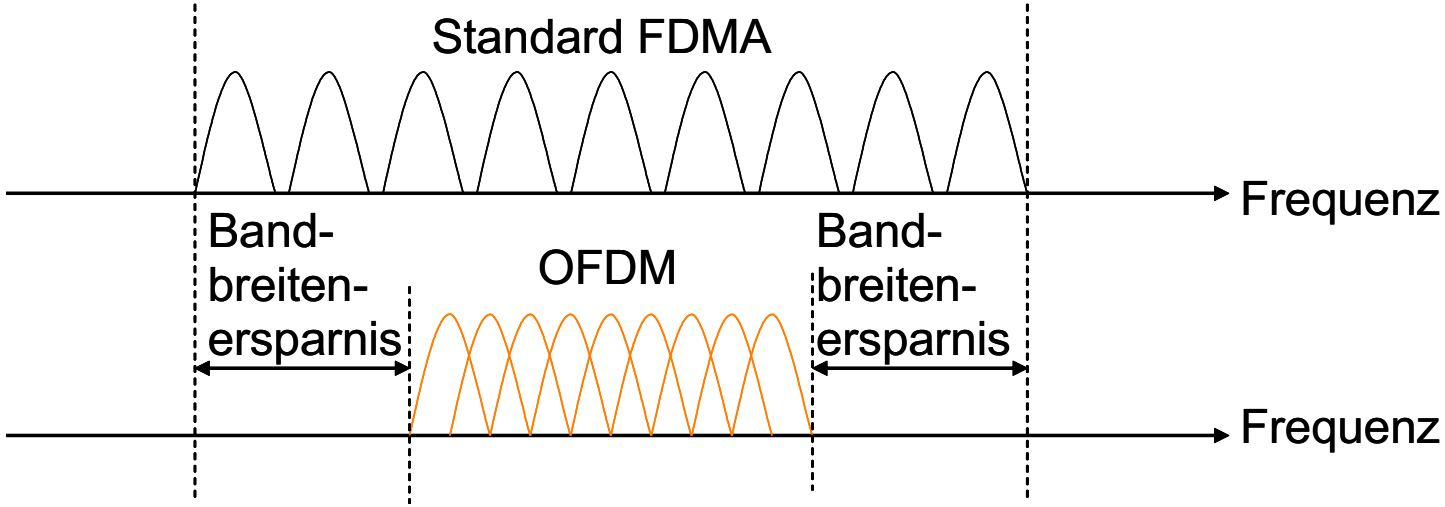
IEEE 802.11b - Kurze Dateneinheiten



- Format für kurze DSSS-Dateneinheiten
  - SYNC wird von 128 Bit auf 56 Bit reduziert
  - SFD zeigt statt 1111001110100000 den Wert 0000010111001111 an
    - Unterscheidung möglich
  - PLCP-Kopf wird mit 2 Mbit/s statt mit 1 Mbit/s übertragen
  - Ergebnis
    - Übertragung von Präambel und Kopf benötigt nur 96 µs statt 192 µs
      - Einsparung von 50%
  - Access Point zeigt ggf. in periodischen Beacons an, dass er das Format für kurze DSSS-Dateneinheiten unterstützt

IEEE 802.11g

- Datenraten von 6 bis 54 Mbit/s im 2,4 GHz Band
  - Vorteile
    - Weltweit lizenzfreies Frequenzband
    - Auswirkungen der Dämpfung geringer als im 5 GHz Band (vgl. IEEE 802.11a)
      - Geringere Sendeleistung erforderlich
- Verwendung von OFDM



IEEE 802.11g

- Abwärtskompatibel zu 802.11 und 802.11b
  - Extended Rate PHY
    - Verfahren, die Datenraten über 11 Mbit/s unterstützen
  - Non Extended Rate PHY
    - Verfahren, die Datenraten bis 11 MBit/s unterstützen (802.11, 802.11b)

- Erweiterung der MAC-Schicht
  - Abwärtskompatibilität zu 802.11 und 802.11b
    - Siehe MAC-Erweiterungen: Protection Mechanismus

IEEE 802.11a

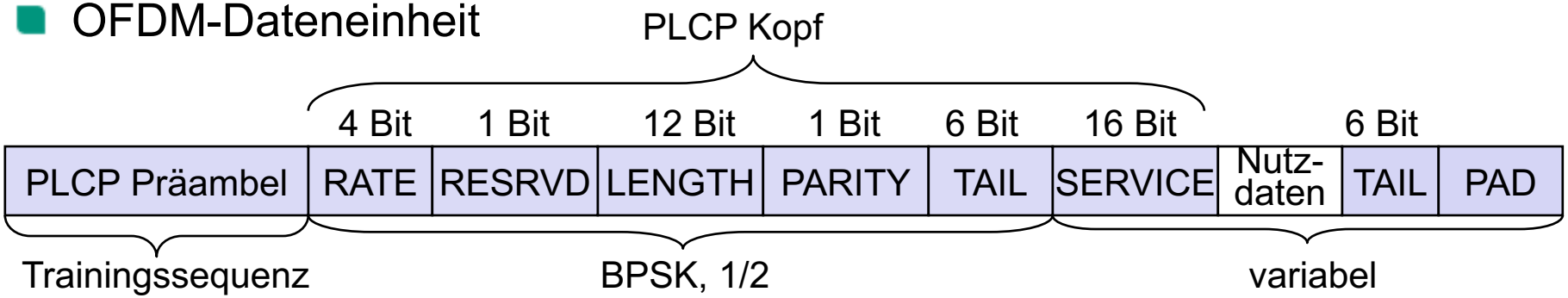
- Datenraten von 6 bis 54 Mbit/s im 5 GHz Band
- Verwendung von OFDM
- Forward Error Correction (FEC), um auftretende Fehler korrigieren zu können
  - FEC Rate = n/m
    - für n Netto-Bits müssen m Brutto-Bits gesendet werden

Modulation	FEC Rate	Datenrate
BPSK	1 / 2	6 Mbit/s (*)
BPSK	3 / 4	9 Mbit/s
QPSK	1 / 2	12 Mbit/s (*)
QPSK	3 / 4	18 Mbit/s
16-QAM	1 / 2	24 Mbit/s (*)
16-QAM	3 / 4	36 Mbit/s
64-QAM	2 / 3	48 Mbit/s
64-QAM	3 / 4	54 Mbit/s

(*) verpflichtend

IEEE 802.11a

- OFDM-Dateneinheit



- RATE
  - Datenrate mit der ab dem Service-Feld gesendet wird
- LENGTH
  - Länge der Nutzdaten
- PARITY
  - Gerade Parität des LENGTH-Feldes
- TAIL
  - 0-Bits; Empfänger stellt sich auf die geforderte Datenrate ein; Überführung des Faltungskodierers in den Ausgangszustand
- SERVICE
  - Reserviert für zukünftige Verwendung (9 Bits) und Synchronisation des Descramblers (7 Bits)
- PAD
  - Füllbits (OFDM spezifisch)

IEEE 802.11a

- Codierungsprozess
  - Trainingsphase
    - 1 x kurze Trainingssequenz
      - Kontrolle des Antennengewinns, Antennenauswahl, Taktgewinnung, Grobeinstellung der Empfängerfrequenz
    - 2 x lange Trainingssequenz
      - Kanalbestimmung, Feinabstimmung der Empfängerfrequenz
  - Scrambling
    - Verwürfeln der Daten (Service, Nutzdaten, Tail, Pad)
      - Vermeidung langer Folgen von Nullen und Einsen
  - Faltungskodierung (Service, Nutzdaten, Tail, Pad)
    - Hinzufügen von Redundanzbits für Vorwärtsfehlerkorrektur (immer Coderate 1/2)
  - Ggf. Punktierung (Service, Nutzdaten, Tail, Pad)
    - Gezieltes Verwerfen von Redundanzbits für Vorwärtsfehlerkorrektur
      - Notwendig um Coderaten von 2/3 und 3/4 erzeugen zu können
  - Interleaving-Prozess
    - Zusätzliche Verwürfelung
    - Umstellung der einzelnen Bits zwischen den Unterkanälen
    - Dient der Absicherung von Bündelfehlern

IEEE 802.11n

- Endgültige Fassung am 12. September 2009 von IEEE ratifiziert
- Maximale Bruttodatenraten bei 600 Mbit/s
  - Datenübertragung per Multiple Input Multiple Output (MIMO) Technik
    - Pro parallelem Datenpfad maximal 150 Mbit/s (brutto)
    - Für höhere Datenraten Bündelung mehrerer (bis zu vier) Datenpfaden
  - Orthogonal Frequency-Division Multiplexing (OFDM) als Basis-Modulation
    - Einzelträger je nach Qualität der Verbindung mittels BPSK, QPSK oder 16- bzw. 64-QAM
  - Verbreiterung der Übertragungskanäle von 20 MHz auf 40 MHz
- Arbeitet im 2,4-GHz- und im 5-GHz-Frequenzbereich
  - Kompatibel zu 802.11b- und 802.11g-Netzen
  - Koexistenz mit bestehenden 802.11a-Netzen
  - Kompatibilitätsmodus kann in manchen Implementierungen deaktiviert werden (sogenannter „Greenfield-Modus“)

Netto-Datenraten

Standard	Brutto-Datenrate	Netto-Datenrate
IEEE 802.11a	54 Mbit/s	20 – 22 Mbit/s
IEEE 802.11b	11 Mbit/s	5 – 6 Mbit/s
IEEE 802.11g	54 Mbit/s	20 – 22 Mbit/s
IEEE 802.11n	600 Mbit/s	100 – 120 Mbit/s

[5.12]

MAC Schicht

- Spezielle Anforderungen für WLANs
  - Medienzugriff
    - In drahtlosen LANs existiert das Problem der versteckten Endgeräte
      - → WLANs benötigen spezielles Medienzugriffsverfahren
  - Einfluss des drahtlosen Übertragungsmediums
    - Drahtlose LANs sind anfälliger für Störeinflüsse als drahtgebundene
      - Höhere Bitfehlerrate des Funkmediums
      - Frequenzbereich kann auch von anderen Technologien verwendet werden
      - → Automatic Repeat Request (ARQ) Verfahren auf MAC-Schicht sinnvoll
      - → Fragmentierung auf MAC-Schicht sinnvoll
    - Drahtlose LANs sind wesentlich leichter abhörbar als drahtgebundene
      - → Sicherheitsmechanismen auf MAC-Schicht erforderlich
  - Unterstützung mobiler Endgeräte
    - Geringe Batteriekapazität
    - Ständiges Abhören des Funkmediums würde zu viel Energie benötigen
    - → Power-Management-Mechanismen auf MAC-Schicht sinnvoll

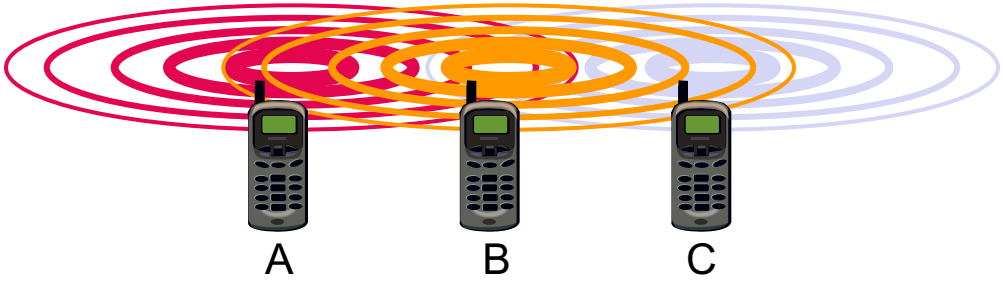
Medienzugriff in IEEE 802.11

- Distributed Coordination Function (DCF)
  - Dezentraler Ansatz
  - In Infrastruktur- und Ad-hoc-Netzen einsetzbar
  - In Wettbewerbsphase (Contention Period - CP) konkurrieren Stationen um Medienzugriff
    - Datenaustausch auf Best-Effort Basis
    - Broadcast und Multicast möglich
  - Jede IEEE 802.11 Station muss DCF unterstützen

- Point Coordination Function (PCF)
  - Zentraler Ansatz
  - Nur in Infrastruktur-Netzen einsetzbar
  - Point Coordinator kontrolliert innerhalb der wettbewerbsfreien Phase (Contention Free Period - CFP) den Medienzugriff
    - Medienzugriff kann Station für bestimmten Zeitraum garantiert werden
  - PCF muss nicht von jeder Station implementiert werden
    - Aktuelle Produkte unterstützen PCF in der Regel nicht

Distributed Coordination Function

- CSMA/CD-Verfahren (Carrier Sense Multiple Access/Collision Detection) von IEEE 802.3 einsetzbar?
  - Nein.
  - Kollisionserkennung findet bei CSMA/CD beim Sender statt
    - Station muss gleichzeitig senden und empfangen können
    - Bei WLAN vollständig getrennte Sende- und Empfangseinheit
      - Hardwareaufwand nicht gerechtfertigt
  - Kollisionserkennung muss bei WLAN beim Empfänger stattfinden
    - Vgl. Situation mit versteckten Endgeräten



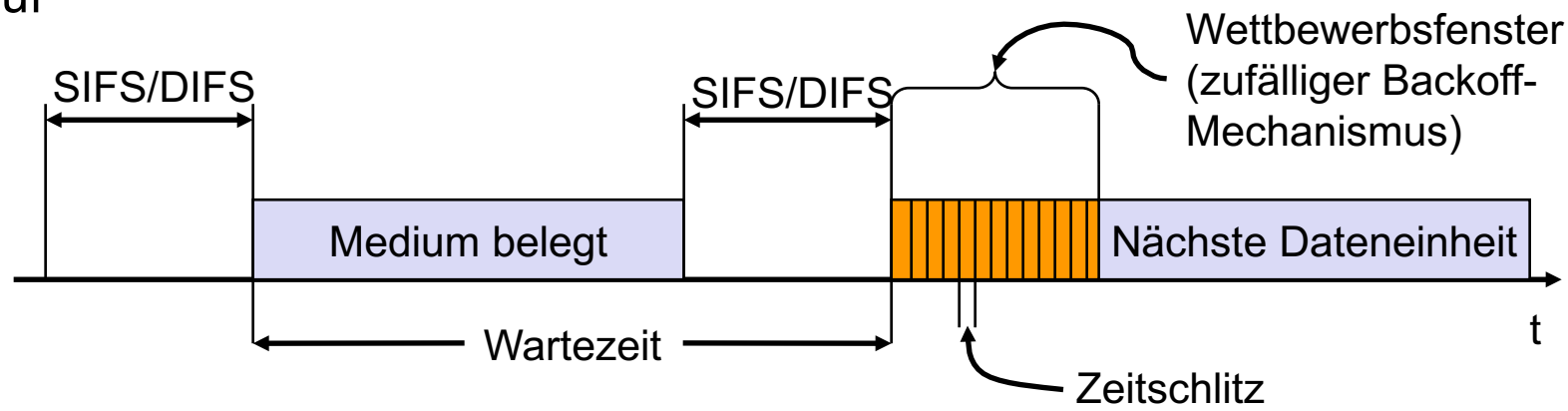
- IEEE 802.11 verwendet das CSMA/CA-Verfahren (Carrier Sense Multiple Access/Collision Avoidance) für den Medienzugriff
  - MACA-Verfahren, Wahrscheinlichkeit von Kollision wird minimiert

Distributed Coordination Function

- Physikalische Carrier-Sense-Funktion
  - Erkennen, ob Medium gerade von einer anderen Station belegt ist
- Virtuelle Carrier-Sense-Funktion
  - Medienreservierung auf Basis des Network Allocation Vectors (NAV)
    - In jeder MAC-Dateneinheit enthalten
    - Zeigt voraussichtliche Dauer der Medienbelegung an
- Unterschiedliche Wartezeiten (Inter Frame Spaces, IFS) nach Ablauf des NAV
  - Short Interframe Space (SIFS)
    - Höchste Priorität → geringste Wartezeit (10 µs)
  - Distributed (Coordination Function) Interframe Space (DIFS)
    - Geringste Priorität → längste Wartezeit (50 µs)
- Backoff-Algorithmus
  - Bestimmung einer zufälligen Wartezeit
  - *backoff_time* = random(*CW*) x *slot_time*
    - *CWmin* <= random(*CW*) <= *CWmax*
    - *CWmin* und *CWmax* bilden Wettbewerbsfenster (*CW* – Contention Window)
    - *slot_time* (Zeitschlitz): festgelegt von physikalischer Schicht (bei DSSS = 20 µs)

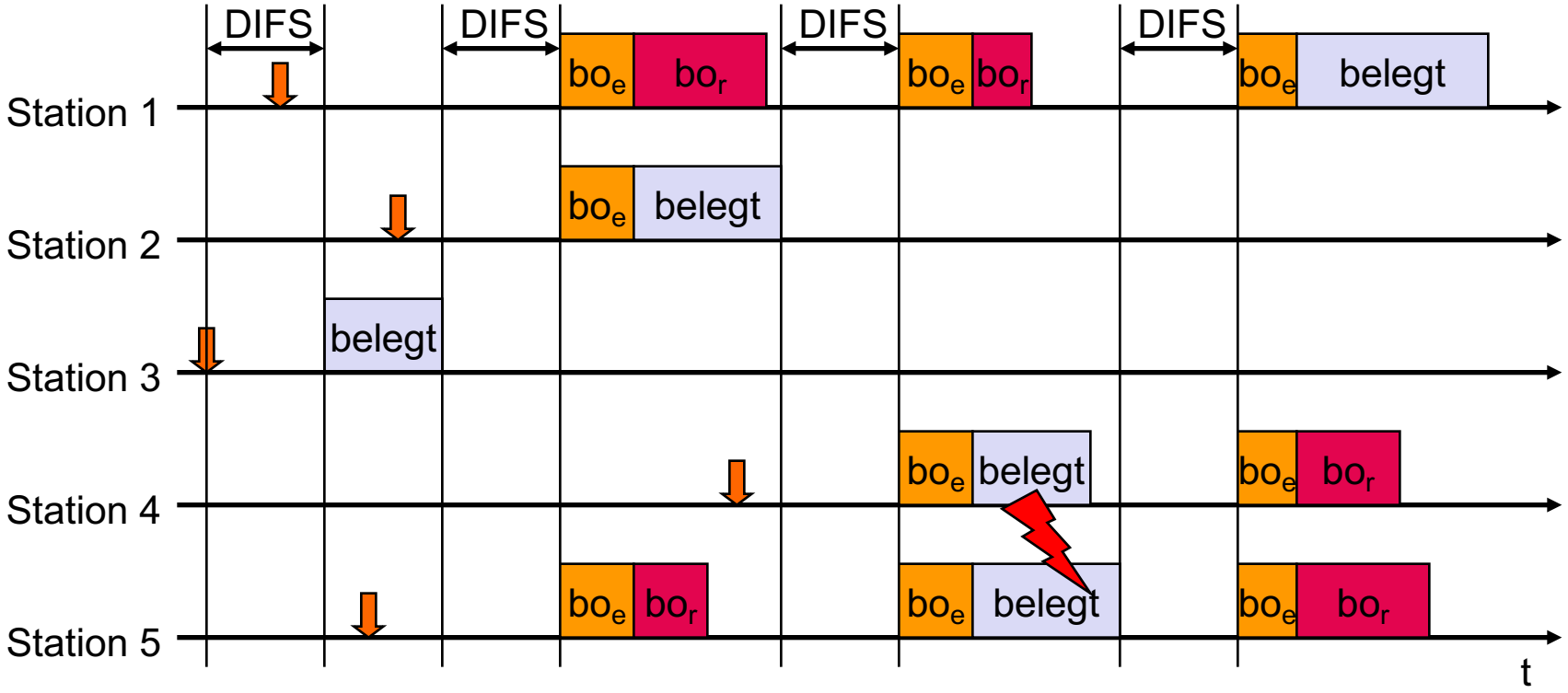
Distributed Coordination Function

- Ablauf



  - Sendewillige Station hört das Medium ab
  - Fall 1: Medium ist für die Dauer eines entsprechenden IFS frei
    - Daten werden versendet
  - Fall 2: Medium ist belegt
    - Warten bis das Medium für die Dauer des entsprechenden IFS frei ist
    - Zusätzlich wird das Versenden der Daten um eine zufällige Backoff-Zeit verzögert
    - Dynamische Anpassung des Wettbewerbsfensters
      - Bei fehlgeschlagenem Versuch werden *CWmin* und *CWmax* verdoppelt (bis Maximalwert)
      - Bei erfolgreichem Versuch werden *CWmin* und *CWmax* auf Minimalwert zurück gesetzt
    - Wird das Medium während der Backoff-Zeit von einer anderen Station belegt, wird der Backoff-Timer so lange angehalten

Stationen im Wettbewerb



belegt — Medium belegt

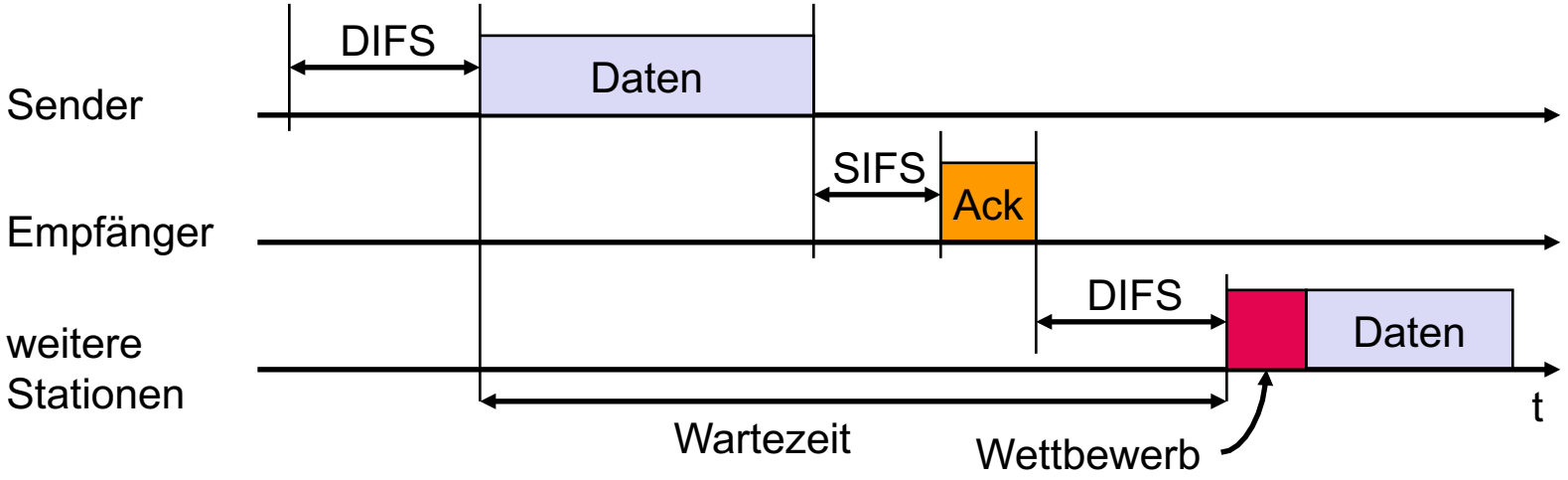
Sendewunsch liegt vor

bo_e — verstrichene Backoff-Zeit

bo_r — verbleibende Backoff-Zeit

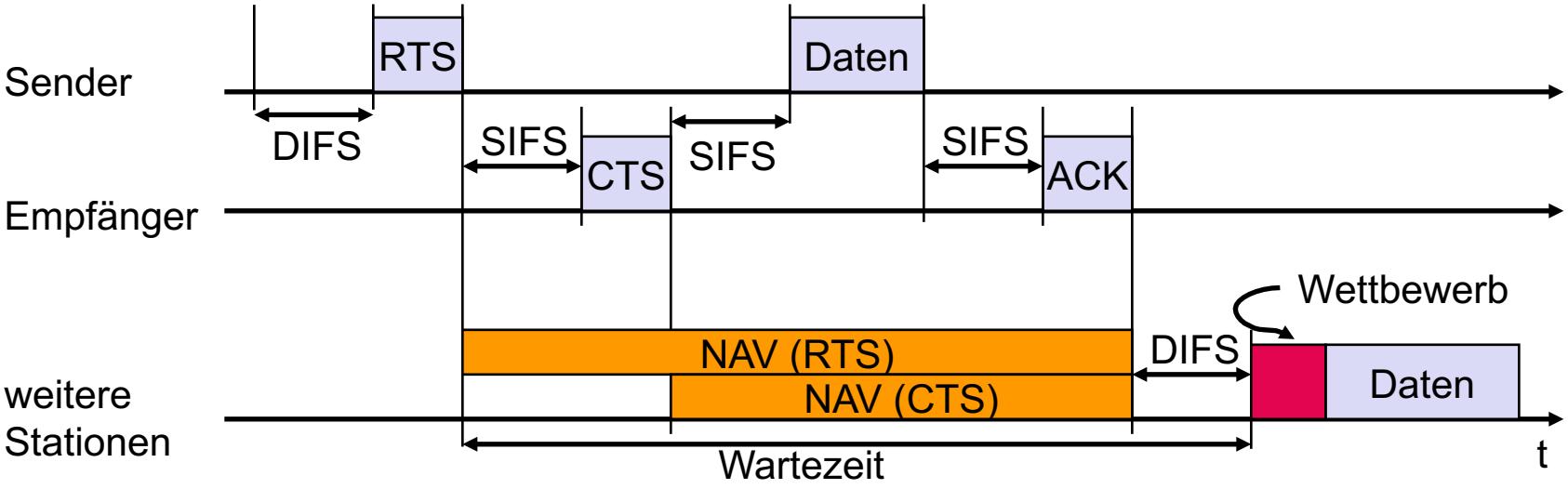
Senden von Unicast-Dateneinheiten

- Daten können nach Abwarten von DIFS gesendet werden
- Empfänger antworten nach SIFS mit einem ACK, falls die Dateneinheit korrekt empfangen wurde
  - Überprüfen der Korrektheit mittels CRC
- Im Fehlerfall wird die Dateneinheit vom Sender automatisch wiederholt
  - Station bewirbt sich erneut um das Medium
  - Neuer Backoff wird berechnet (*CWmin* und *CWmax* angepasst)



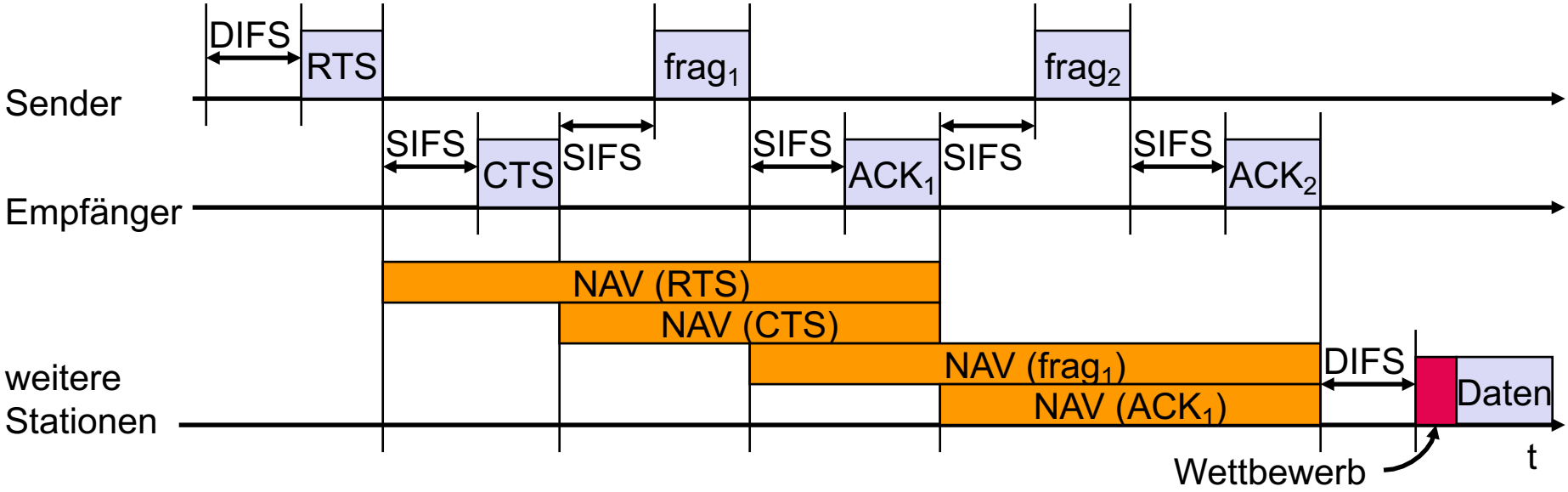
RTS/CTS-Erweiterung

- RTS/CTS-Erweiterung für Unicast-Dateneinheiten
  - RTS kann nach Abwarten von DIFS gesendet werden
    - Belegungsdauer als Parameter mit gesendet
  - Bestätigung durch CTS nach SIFS durch Empfänger
    - Enthält ebenfalls Belegungsdauer als Parameter
  - Sofortiges Senden der Daten nach SIFS möglich
    - Bestätigung wie gehabt mit ACK
  - Andere Stationen speichern Belegungsdauer im NAV (Net Allocation Vector)
    - Virtuelle Reservierung



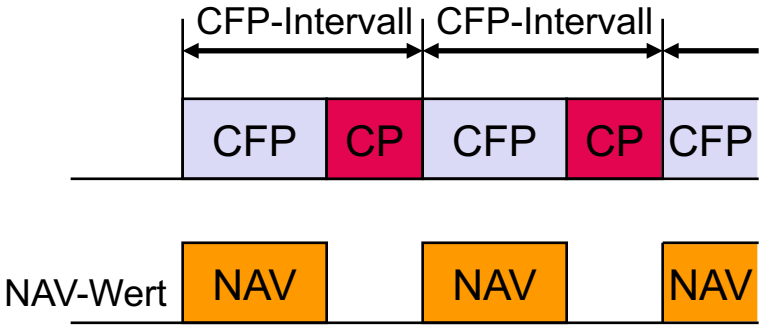
Fragmentierung

- Ziel
  - Übertragung längerer zusammenhängender Daten
- Vorgehensweise
  - Über Sequenznummern und Fragmentnummern gesteuert
  - Stop-and-Wait ARQ-Verfahren auf Fragmente angewendet
  - Weshalb ist der NAV-Wert nicht über die Sendung der gesamten Daten gesetzt?



Point Coordination Function

- Medienzugriff wird von Point Coordinator zentral gesteuert
- PCF ist optional, d.h. nicht jede Station muss PCF unterstützen, deshalb wird zwischen 2 Phasen unterschieden
  - Contention Period (CP) – Verwendung von DCF für den Medienzugriff
    - Auch Stationen die PCF nicht unterstützen können kommunizieren
  - Contention Free Period (CFP) – Verwendung von PCF für den Medienzugriff
    - Zentrale Steuerung ermöglicht Realisierung von zeitkritischen Diensten
- CFP-Intervall = CFP + CP
  - Vielfaches des Beacon-Intervalls
- Periodische Beacons des Access Points setzen NAV-Wert bei Stationen die kein PCF unterstützen



Point Coordination Function

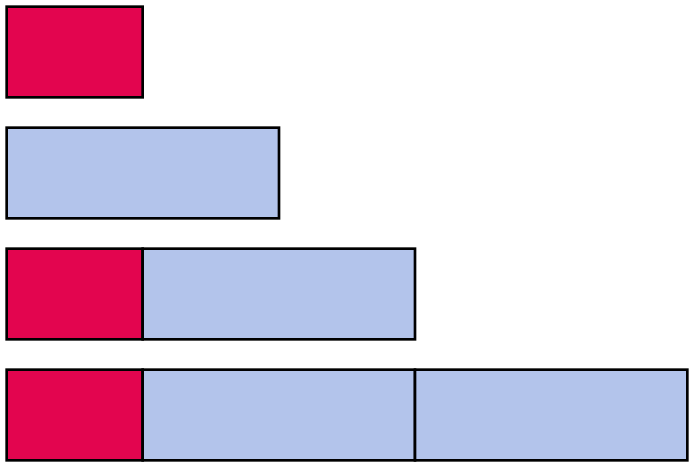
- Poll-Liste
  - Zugangspunkt führt eine Poll-Liste
    - Enthält alle PCF-fähigen Stationen
    - PCF-Fähigkeit wird bei Assoziierung mit dem WLAN von den Stationen bekannt gegeben
- Spezielle Wartezeit
  - Point (Coordination Function) Interframe Space (PIFS)
    - Mittlere Priorität
    - Berechnung:

SIFS (bei DSSS = 10 µs)

Slot Time (bei DSSS = 20 µs)

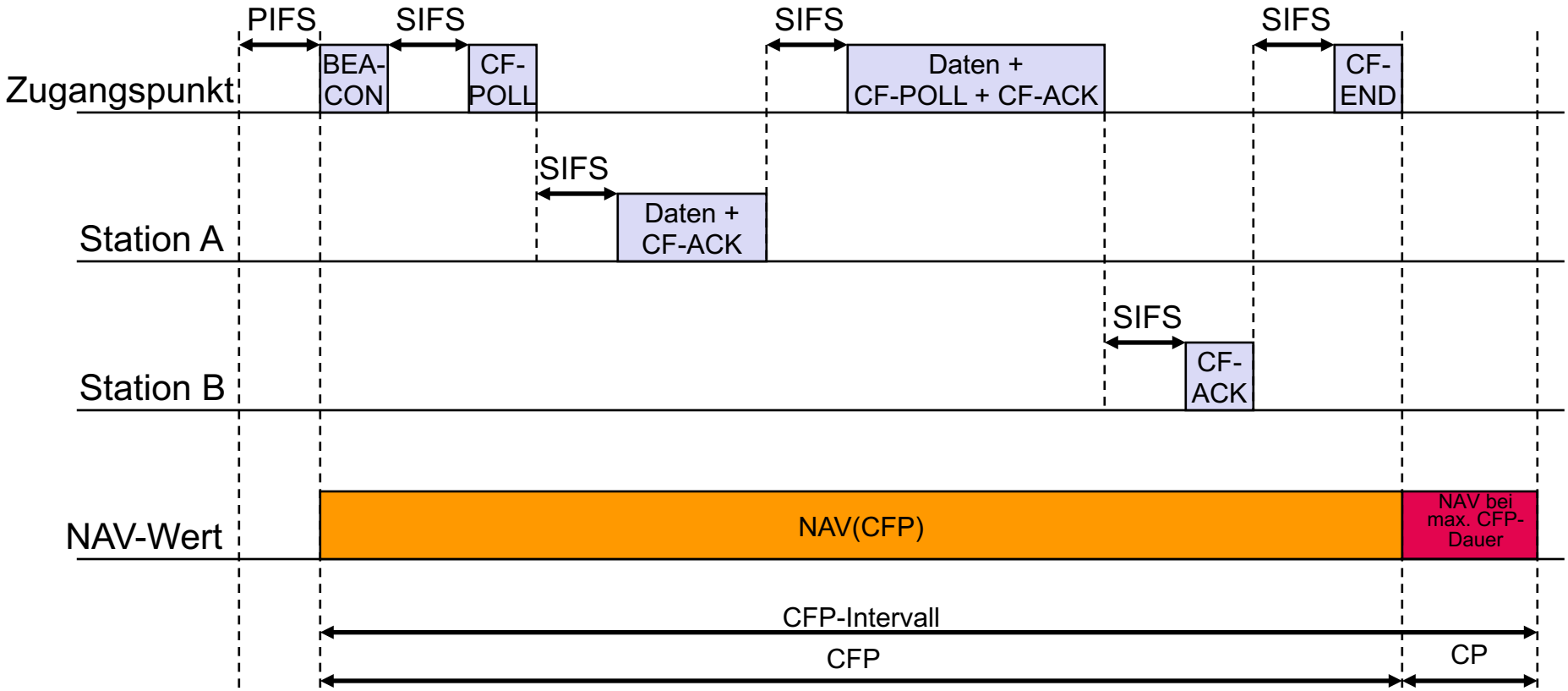
PIFS (bei DSSS = 30 µs)

DIFS (bei DSSS = 50 µs)



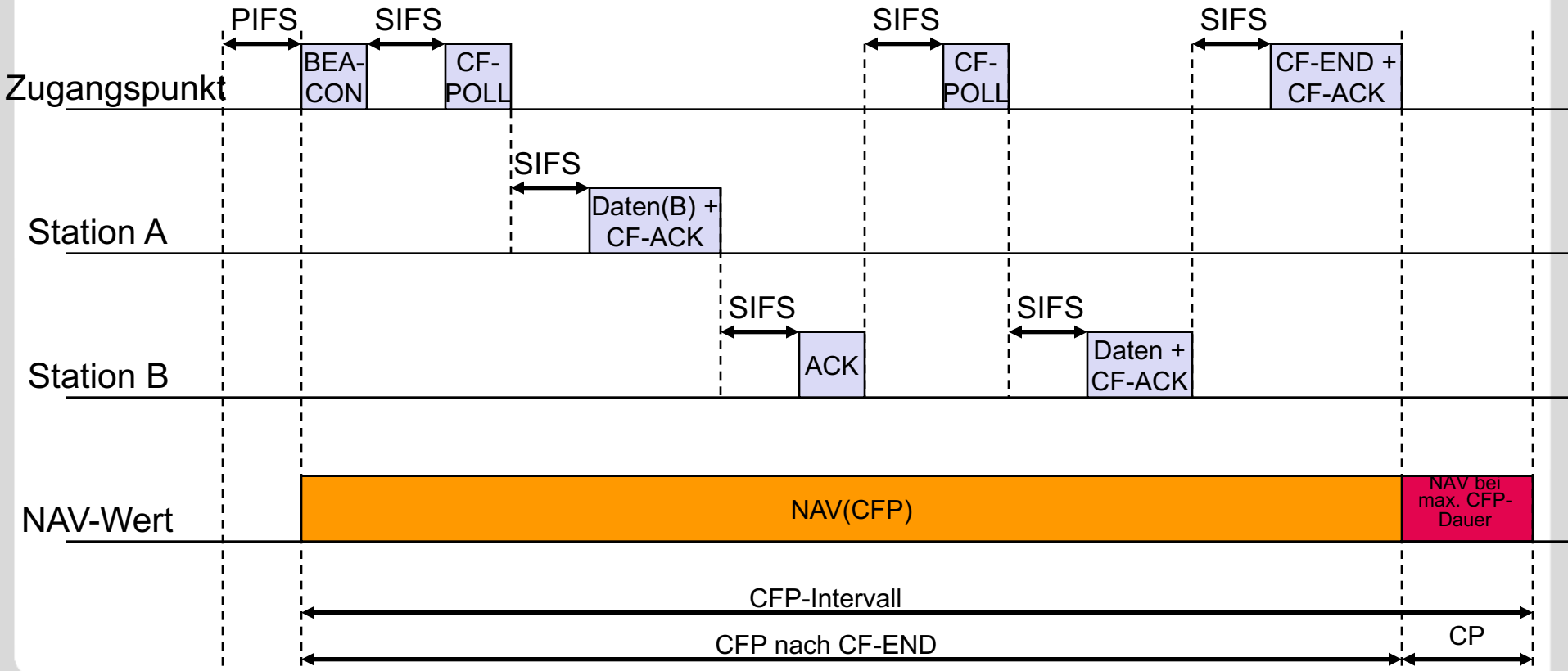
Kommunikation über Zugangspunkt

- Beispielablauf
  - Station A kommuniziert mit Station B über Zugangspunkt
    - Polling durch Zugangspunkt



Point Coordination Function

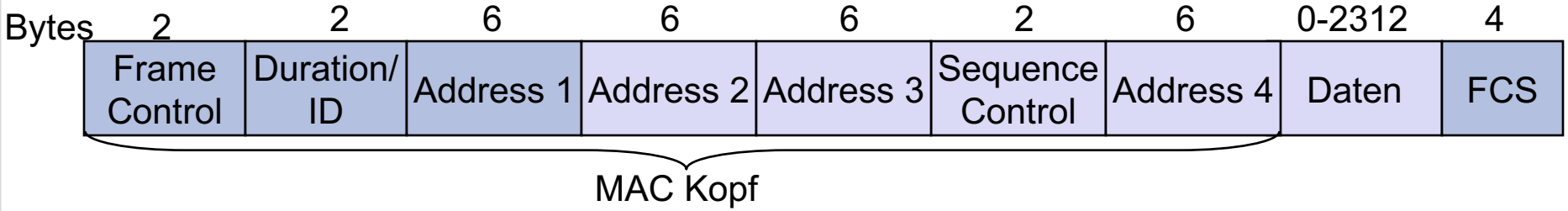
- Beispielablauf
  - Station A kommuniziert direkt mit Station B
- Vorteil
  - Geringere Belastung des Mediums



Format der MAC-Dateneinheiten

- Grundlegender Aufbau ähnlich dem bekannter MAC-Dateneinheiten
  - Kopf – Daten – Prüfsumme
- So in anderen MAC-Dateneinheiten nicht vorhanden
  - Bis zu vier Adressfelder
    - Länge des Kopfes variiert
  - Unterschiedliche Typen von MAC-Dateneinheiten
    - Daten-Dateneinheiten für den Transport von Nutzdaten
    - Kontroll-Dateneinheiten für die Steuerung des Medienzugriffs
    - Management-Dateneinheiten für das Management der Funkzelle
  - Duration/ID-Feld
    - Zeitangabe für die Datenübertragung
  - Sequenz-Kontroll-Feld
    - Fragmentnummer zur Kennzeichnung von Fragmenten
    - Sequenznummer zur Kennzeichnung von MSDUs

Generelles MAC-Format



- Felder
  - Duration/ID
    - Zeitangabe für Network Allocation Vector (NAV)
  - Sequence Control
    - Fragmentnummer (4 Bit) und Sequenznummer (12 Bit)
  - FCS: Frame Check Sequence
    - Prüfsumme
- Variable Länge des MAC-Headers
  - Felder Address 2, Address 3, Address 4, Sequence Control und Daten sind nur in bestimmten Dateneinheiten vorhanden

Frame-Control-Feld

Bits:	2	2	4	1	1	1	1	1	1	1	1
	Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order

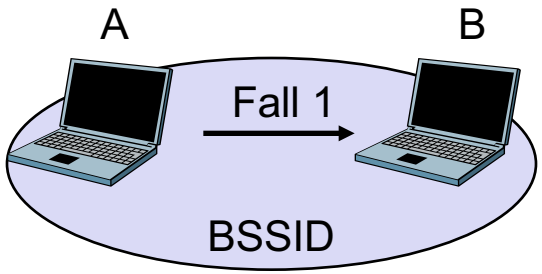
- Protocol-Version
  - Version des verwendeten Protokolls
- Type-Feld
  - Management-, Kontroll- oder Daten-Dateneinheit
- Subtype
  - Genauere Spezifikation der Dateneinheit
    - z.B. Type = Kontroll, Subtype = CTS
- ToDS/FromDS
  - Festlegung des Übertragungsweges
- More Fragment
  - Weitere Fragmente folgen
- Retry
  - Wiederholung einer Dateneinheit
- Power Management
  - Station wechselt in Passive Mode
- More Data
  - Weitere Daten stehen an
  - Station soll nicht in Passive Mode wechseln
- WEP
  - Dateneinheit ist verschlüsselt
- Order
  - Strikte Reihenfolgeerhaltung bei Fragmenten

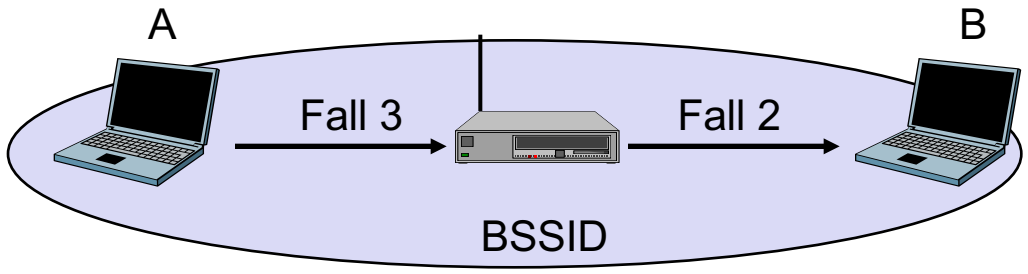
Adressen in MAC-Dateneinheiten

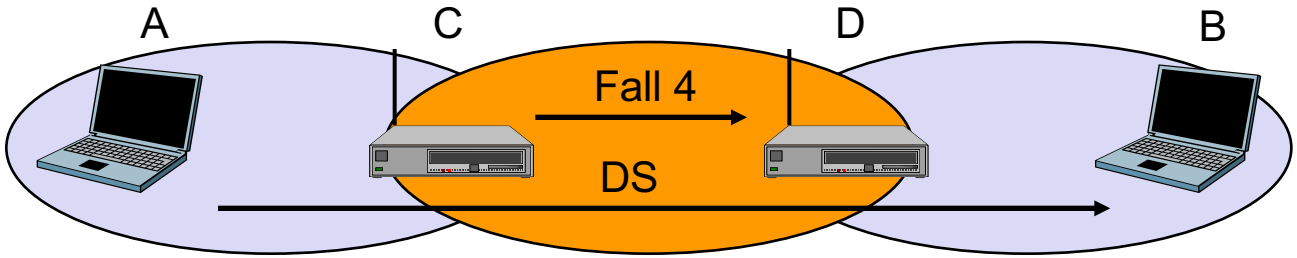
Physikalischer Empfänger

Physikalischer Sender

Fall	Beschreibung	To DS	From DS	Adresse			
				1	2	3	4
1	Ad-hoc-Netz	0	0	B	A	BSSID	-
2	Infrastruktur-Netz, von AP	0	1	B	BSSID	A	-
3	Infrastruktur-Netz, zu AP	1	0	BSSID	A	B	-
4	Infrastruktur-Netz, im DS	1	1	D	C	B	A



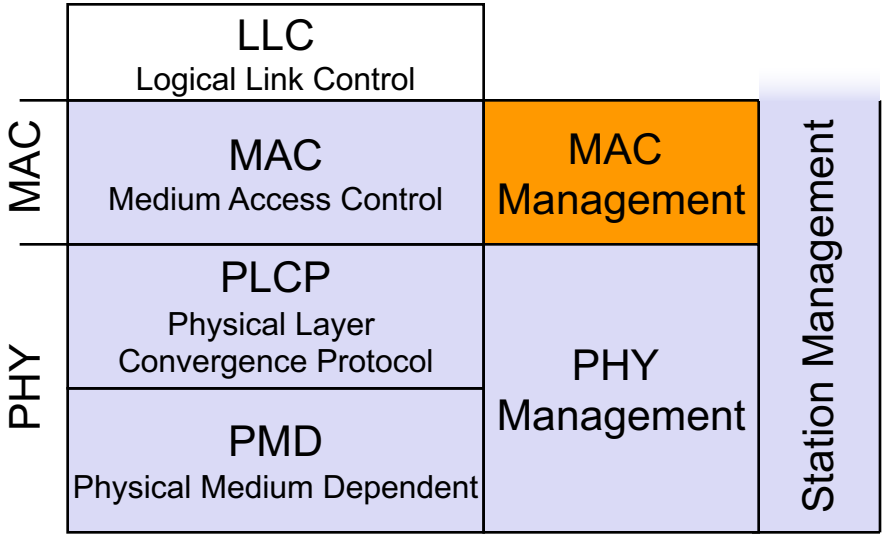




MAC Management

- Im Vergleich zu drahtgebundenen LANs wie IEEE 802.3 sind eine Reihe zusätzlicher Fragestellungen zu lösen. Zum Beispiel
  - Wie findet eine Station ein WLAN?
  - Wie wird eine Station Mitglied in einem WLAN?
  - Wie kann Energie durch „schlafen“ gespart werden?
  - Wie kann die drahtlose Kommunikation abgesichert werden?

→ Aufgaben des MAC Managements

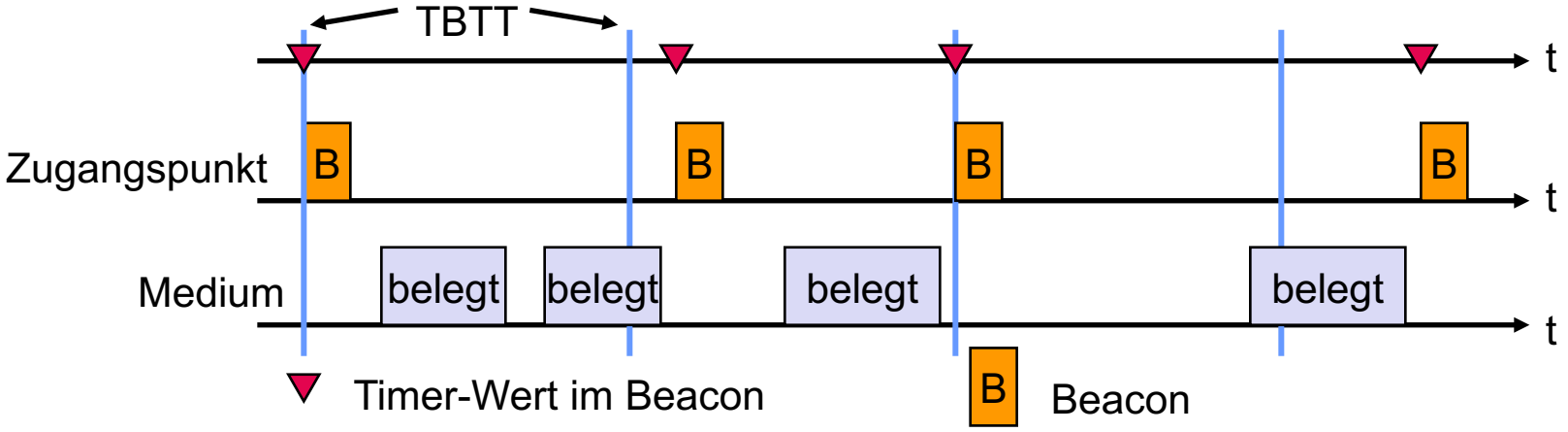


Synchronisation

- Problem
  - Für einige Aufgaben ist es erforderlich, dass die Stationen und Zugangspunkte über einen synchronisierten Timer verfügen, zum Beispiel:
    - Synchronisation der Sprungfolge bei FHSS
    - Power-Management
    - Koordination der PCF
- Timer Synchronisation Function (TSF)
  - Stationen und Zugangspunkte besitzen einen Timer
    - 64 Bit
    - 1 MHz
    - Genauigkeit: 25 ppm (Parts per million)
  - Synchronisation der Timer untereinander
    - Unterschiedliche Ansätze für Infrastruktur-Netz (BSS) und Ad-hoc Netz (IBSS)

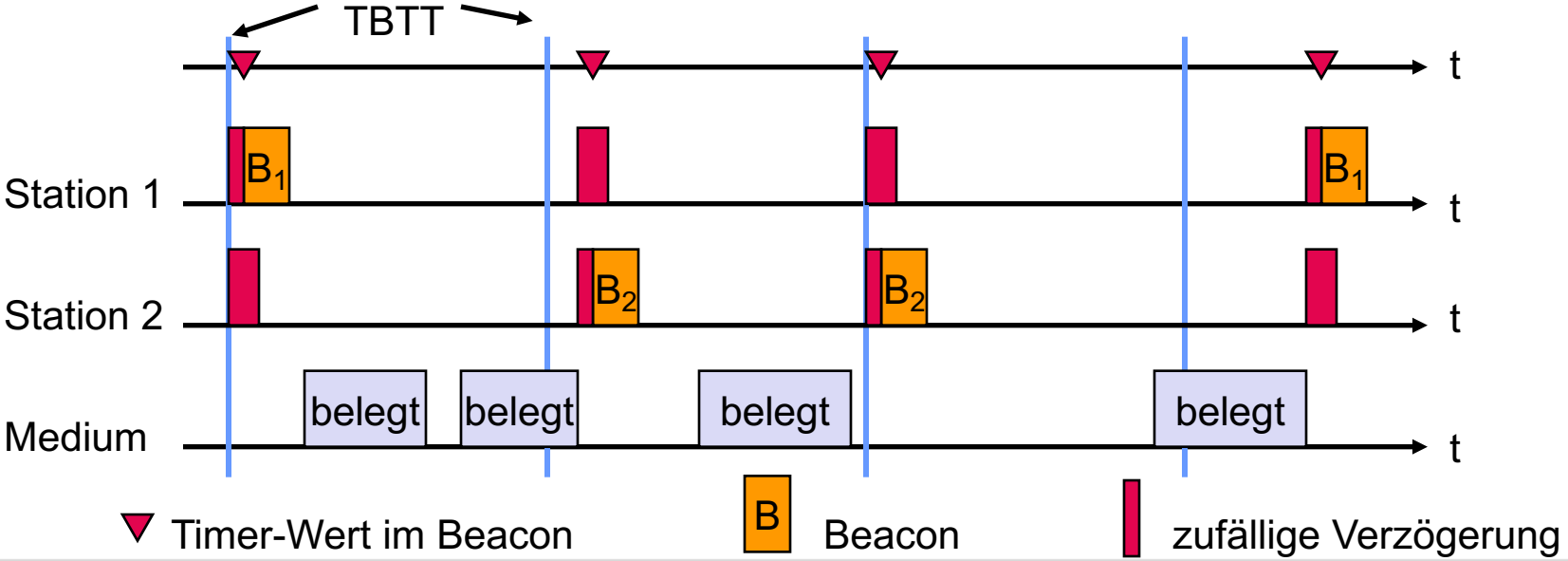
Timer-Synchronisation in einem BSS

- Zentraler Ansatz
  - Zugangspunkt sendet in regelmäßigen Abständen Beacons (Leuchtfeuer)
    - Broadcast-Dateneinheit
    - Enthält u.a. aktuellen Timer-Wert des Zugangspunkts
  - Target Beacon Transmission Time (TBTT)
    - Startzeitpunkt für das Aussenden eines Beacon
  - Wird beim Medienzugriff nicht anders behandelt als andere Dateneinheiten
    - Beacon kann verzögert werden
    - Timer-Wert im Beacon muss angepasst werden – repräsentiert echte Sendezeit
  - Stationen aktualisieren ihren Timer anhand der Informationen im Beacon



Timer-Synchronisation in einem IBSS

- Verteilter Ansatz
  - Nach Ablauf der TBTT bestimmt jede Station eine zufällige Verzögerung
  - Station sendet Beacon, wenn nach Ablauf der zufälligen Verzögerung noch kein Beacon empfangen wurde
  - Timer wird nur aktualisiert, falls Timer-Wert im Beacon größer war als eigener Wert
    - Synchronisation auf die am schnellsten laufende Uhr



Scanning

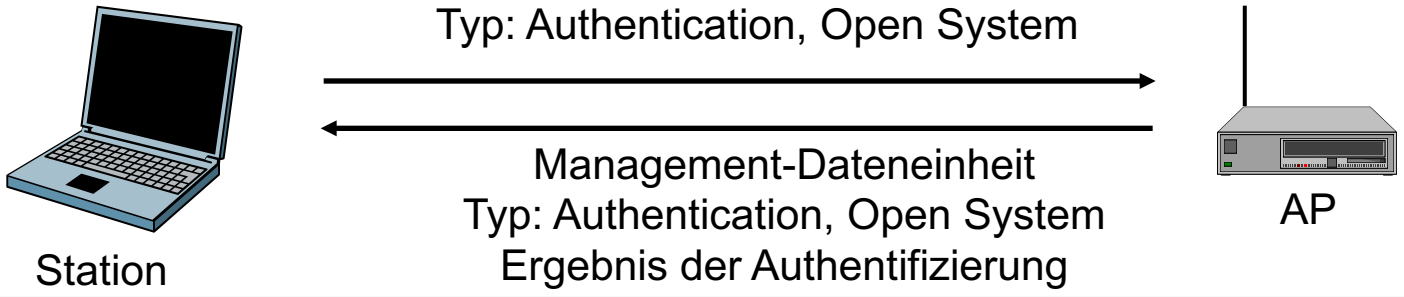
- Problem
  - Wie können vorhandene WLANs gefunden werden?
    - Stationen besitzen meist keine Information über vorhandene WLANs
- Identifikation eines WLANs
  - Service Set Identifier (SSID)
    - Zwischen 0 und 32 Byte langer Netzname
  - Zugangspunkte eines Infrastruktur-Netzes haben alle die gleiche SSID
- Möglichkeit 1: Passives Scanning
  - Zugangspunkt sendet in regelmäßigen Abständen ein Beacon
  - Station hört nacheinander alle Kanäle ab
    - Typischer Zeitraum für Abhören eines Kanals: 204,8 ms – 256 ms
  - Empfang eines Beacons signalisiert Existenz eines Zugangspunkts
  - Bei Empfang mehrerer Beacons wird der Zugangspunkt mit dem besten Empfangssignal ausgewählt

Scanning

- Möglichkeit 2: Aktives Scanning
  - Station sendet auf einem Kanal eine Probe-Request-Dateneinheit
    - SSID des gewünschten Netzes oder Broadcast-SSID (ANY)
  - Zugangspunkte mit entsprechender SSID antworten mit Probe-Response-Dateneinheit
    - Empfang mehrerer Antworten
      - Auswahl des Zugangspunkts mit dem besten Empfangssignal
    - Kein Empfang einer Antwort nach Wartezeit (Probe-Delay)
      - Senden von Probe-Request-Dateneinheit auf anderem Kanal
- In Ad-hoc-Netzen wird nur aktives Scanning eingesetzt
  - Station die, letztes Beacon gesendet hat, übernimmt die Rolle des Zugangspunkts

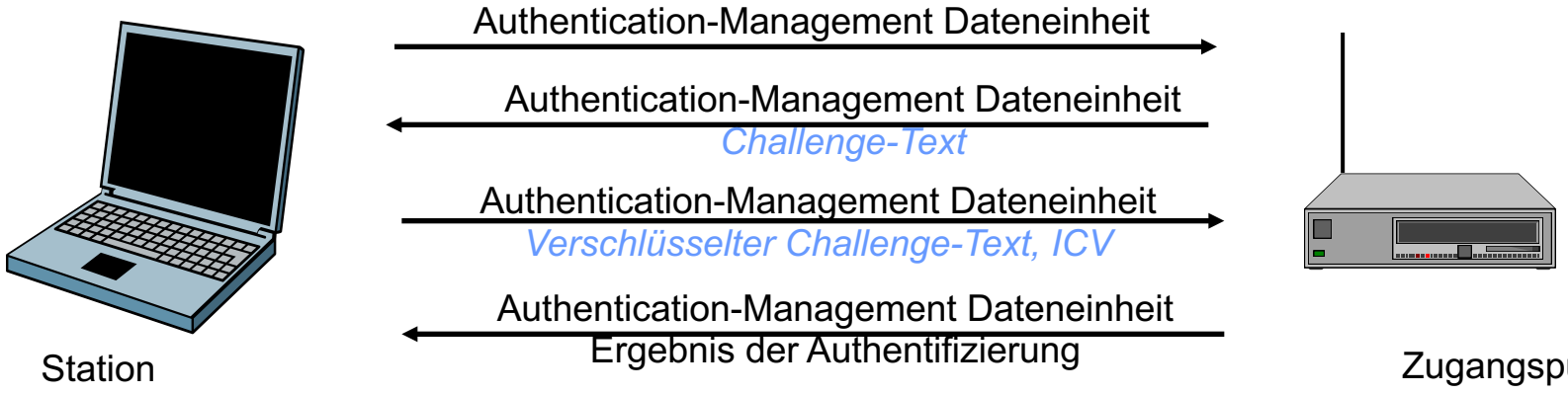
Authentifizierung

- Problem
  - Wer darf das WLAN nutzen?
    - Authentifizierung gegenüber dem Zugangspunkt
    - Authentifizierung zwischen zwei Stationen eines IBSS
- Möglichkeit 1: Open System Authentication
  - Keine tatsächliche Authentifizierung
  - WLAN von allen Stationen nutzbar die dies akzeptieren
  - Station sendet Dateneinheit zum Authentication-Management an AP
  - AP sendet Authentication-Management-Dateneinheit mit dem Ergebnis



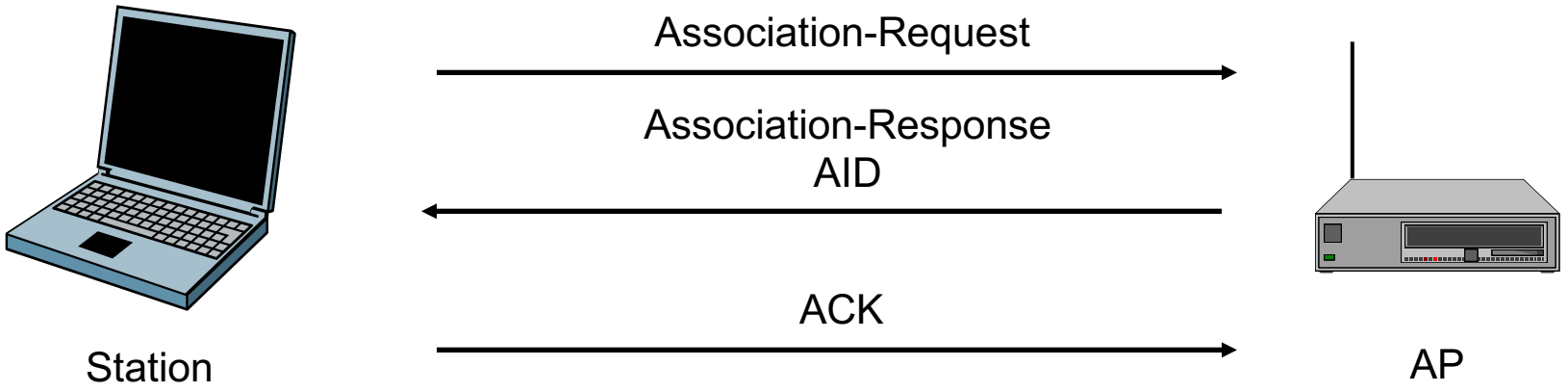
Authentifizierung

- Möglichkeit 2: Shared Key Authentication
  - Basiert auf Challenge-Response-Verfahren
    - Station sendet Authentication-Management Dateneinheit an Zugangspunkt
    - Zugangspunkt antwortet mit Authentication-Management Dateneinheit
      - enthält einen zufälligen, 128-Byte langen Challenge-Text
    - Station kopiert den erhaltenen Challenge-Text
      - Generiert Prüfsumme ICV (Integrity Check Vector) und neuen Initialisierungsvektor (IV)
      - verschlüsselt Challenge-Text und ICV mit ihrem geheimen WEP-Schlüssel
      - sendet Ergebnis samt IV an den Zugangspunkt
    - Zugangspunkt empfängt verschlüsselten Text und ICV
      - Entschlüsselt Text mit seinem geheimen WEP-Schlüssel
      - Prüft Übereinstimmung mit ursprünglichem Challenge-Text
    - Zugangspunkt sendet Authentication-Management-Dateneinheit, die Ergebnis enthält



Assoziierung

- Herstellung einer eindeutigen Verbindung zwischen Station und AP
  - Erfolgt im direkten Anschluss an Authentifizierung
  - Station sendet Association-Request Dateneinheit
  - Bei Erfolg antwortet AP mit Association-Response
    - Enthält Assocoiation-ID (AID) über die eine Station eindeutig identifiziert werden kann
      - Wird u.a. für Power-Management benötigt
  - Bei Fehlschlagen der Assoziierung antwortet AP mit Disassociation
  - Station bestätigt mit ACK den Empfang des Association-Response



Reassoziierung

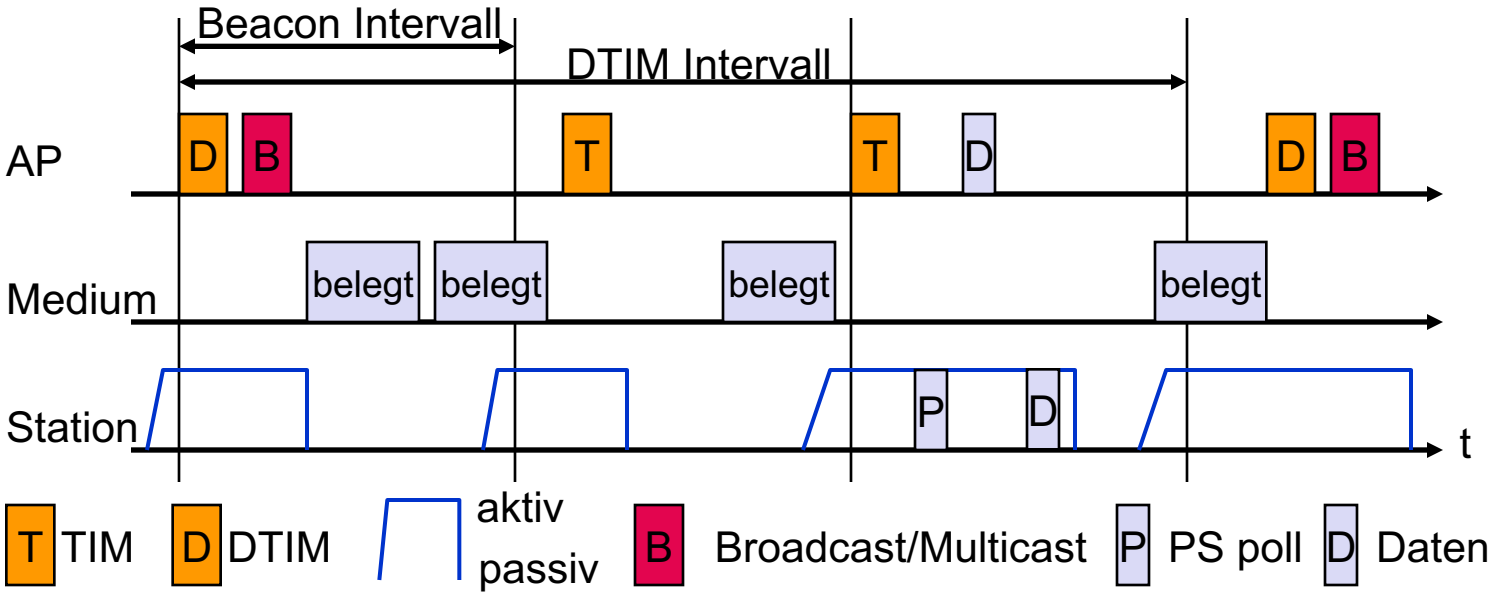
- Station führt Handover bei keiner oder schlechter Verbindung zum Zugangspunkt durch
  - Station führt Scanning nach neuem AP durch
  - Station sendet Reassociation-Request an neuen AP
    - Enthält die Adresse des alten Zugangspunkts
  - AP antwortet mit Reassociation-Response
    - Enthält neue AID, die für diesen Zugangspunkt gültig ist
  - Station bestätigt Empfang der Reassociation-Response mit ACK
  - AP informiert alle anderen Zugangspunkte des Distribution Systems über Reassoziierung
- Handoff auf Vermittlungsschicht bei Subnetzwechsel notwendig
  - Siehe Kapitel Mobiles Internet

Power-Management

- Ziel: Geringer Energieverbrauch
- Betriebsmodi bei IEEE 802.11
  - Active Mode (AM)
    - Sende-/Empfangseinheit aktiv
      - Daten können gesendet und empfangen werden
  - Power Save (PS)
    - Sende-/Empfangseinheit ausgeschaltet
      - Kein Empfang oder Senden von Daten möglich
      - Dateneinheiten für diese Station müssen zwischengespeichert werden
        - Infrastruktur-Netz: Zugangspunkt
        - Ad-hoc Netz: alle Stationen müssen zwischenspeichern können
      - Sender signalisiert Übergang in PS-Modus über das Power-Management-Feld einer Dateneinheit
- Grundsätzlicher Ablauf
  - Stationen befinden sich die meiste Zeit im PS-Modus
  - Zwischenspeicherung von Dateneinheiten durch Zugangspunkte
  - Stationen wechseln zu festgelegten Zeitpunkten in den AM-Modus
  - Stationen rufen zwischengespeicherte Dateneinheiten ab
  - Station wechselt zurück in den PS-Modus

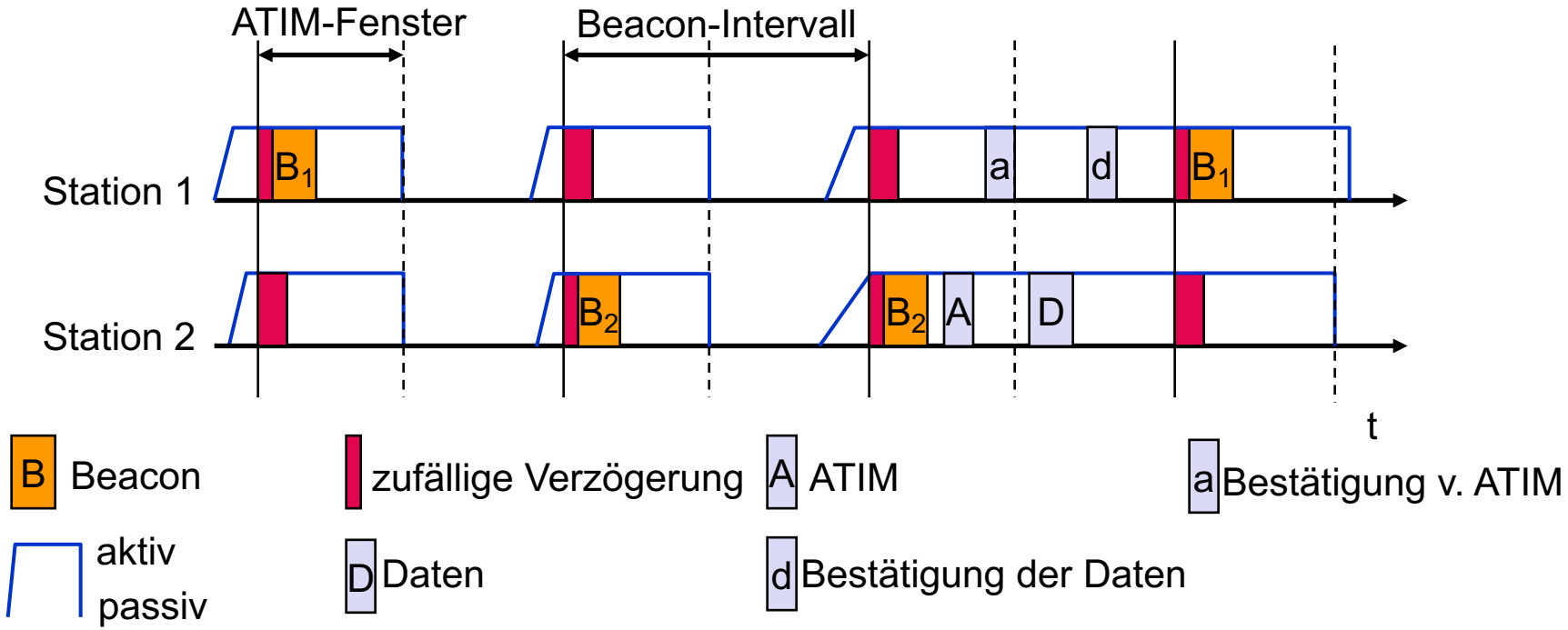
Power-Management in einem BSS

- Zugangspunkt für Zwischenspeicherung von Dateneinheiten verantwortlich
  - Annahme: verfügt über eine Stromversorgung und deshalb immer aktiv
- Traffic Indication Map (TIM)
  - Bekanntgabe von zwischengespeicherten Dateneinheiten (AIDs)
  - Kann in einem Beacon enthalten sein
- Delivery TIM Interval (DTIM-Intervall)
  - Intervall für zwischengespeicherte Broadcast/Multicast Dateneinheiten
    - Entspricht drei Beacon Intervallen
  - Werden nur einmalig an alle Stationen gesendet
- Abruf zwischengespeicherter Dateneinheiten mit Power Save Poll (PS-Poll)



Power-Management in einem IBSS

- Ad-hoc Traffic Indication Message (ATIM)
  - ATIM-Fenster
    - In diesem Zeitraum können alle Stationen Daten empfangen
    - Es können nur Beacons oder ATIMs gesendet werden
    - Kollisionen von ATIMs möglich (Skalierbarkeit?)
  - Bekanntgabe von Empfängern durch die sendende Station

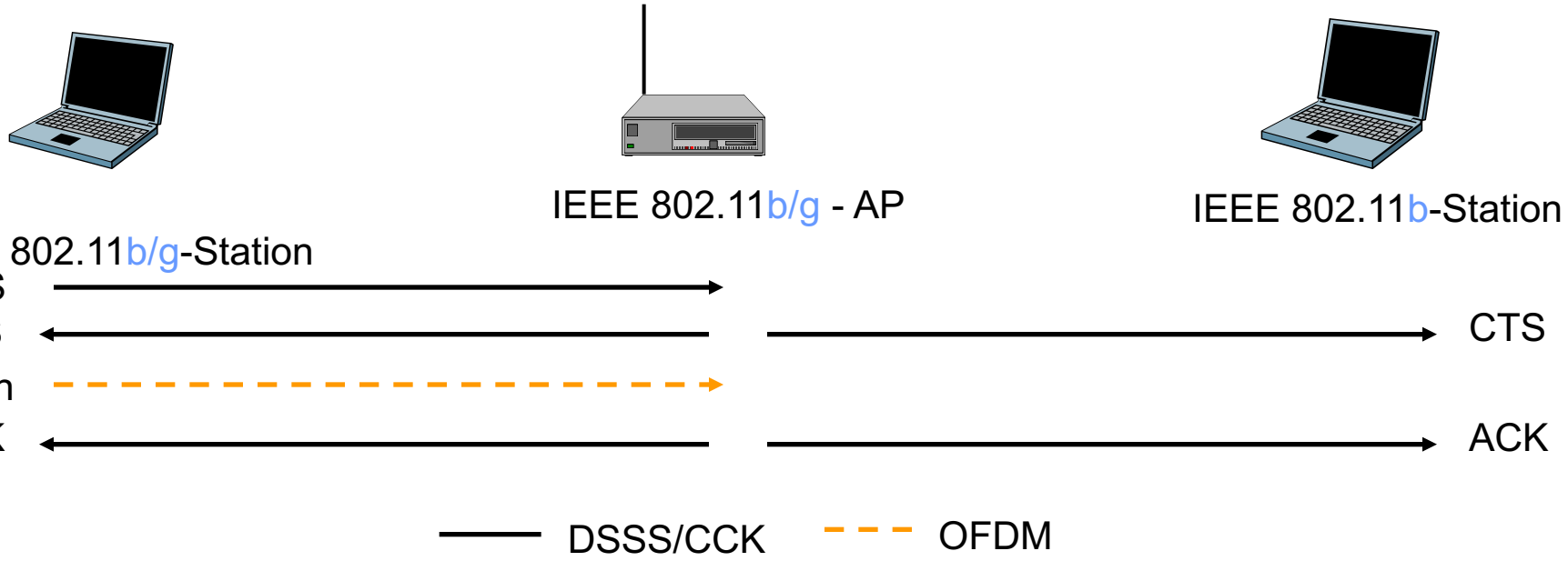


Erweiterungen der MAC-Schicht

- Protection-Mechanismus
  - Definiert in IEEE 802.11g
  - Koexistenz von 802.11, 802.11b und 802.11g im 2.4 GHz-Band
- Transmit Power Control
  - Definiert in IEEE 802.11h
  - Automatische Anpassung der Sendeleistung im 5 GHz-Band
- Dynamic Frequency Selection
  - Definiert in IEEE 802.11h
  - Automatischer Kanalwechsel im 5 GHz-Band
- Quality of Service (QoS)
  - Definiert in IEEE 802.11e
  - Bereitstellung von QoS-Fähigkeiten

Protection-Mechanismus

- Ziel
  - Koexistenz von 802.11, 802.11b und 802.11g im 2.4 GHz-Band
- Vorgehensweise
  - Beacons werden immer mit DSSS bzw. CCK gesendet
  - Anpassung des RTS/CTS-Mechanismus
    - Notwendig falls sich 802.11 oder 802.11b Stationen im BSS befinden



Protection-Mechanismus

[5.13]

- Maximaler Durchsatz einer TCP-Verbindung

Distance (Feet)	*802.11b (Mbps)*	*802.11a (Mbps)*	*802.11g-only (Mbps)*	*802.11g Mixed Environment with CTS-to-self (Mbps)*	*802.11g Mixed Environment with RTS/CTS (Mbps)*
10	5.8	24.7	24.7	14.7	11.8
50	5.8	19.8	24.7	14.7	11.8
100	5.8	12.4	19.8	12.7	10.6
150	5.8	4.9	12.4	9.1	8.0
200	3.7	0	4.9	4.2	4.1
250	1.6	0	1.6	1.6	1.6
300	0.9	0	0.9	0.9	0.9

© Dell Computer

Transmit Power Control - TPC

- Ziel
  - Automatische Anpassung der Sendeleistung
    - Festgelegte maximal zulässige Sendeleistung nicht überschreiten
    - Bestimmung der minimal notwendigen Sendeleistung
- Vorgehensweise
  - Während Assoziierung/Reassoziierung
    - Austausch über minimal und maximal zulässige Sendeleistung
    - Assoziierung/Reassoziierung einer Station wird ggf. verweigert
  - Beacons von Zugangspunkt (BSS) / Station (IBSS) enthalten maximal zulässige Sendeleistung eines Kanals
  - Dynamische Anpassung der Sendeleistung
    - Kommunizierende Stationen tauschen Verbindungsinformationen aus
      - TPC-Request/TPC-Response-Dateneinheiten
    - Algorithmus zur Anpassung der Sendeleistung ist nicht spezifiziert
      - Herstellerspezifische Lösungen

Dynamic Frequency Selection

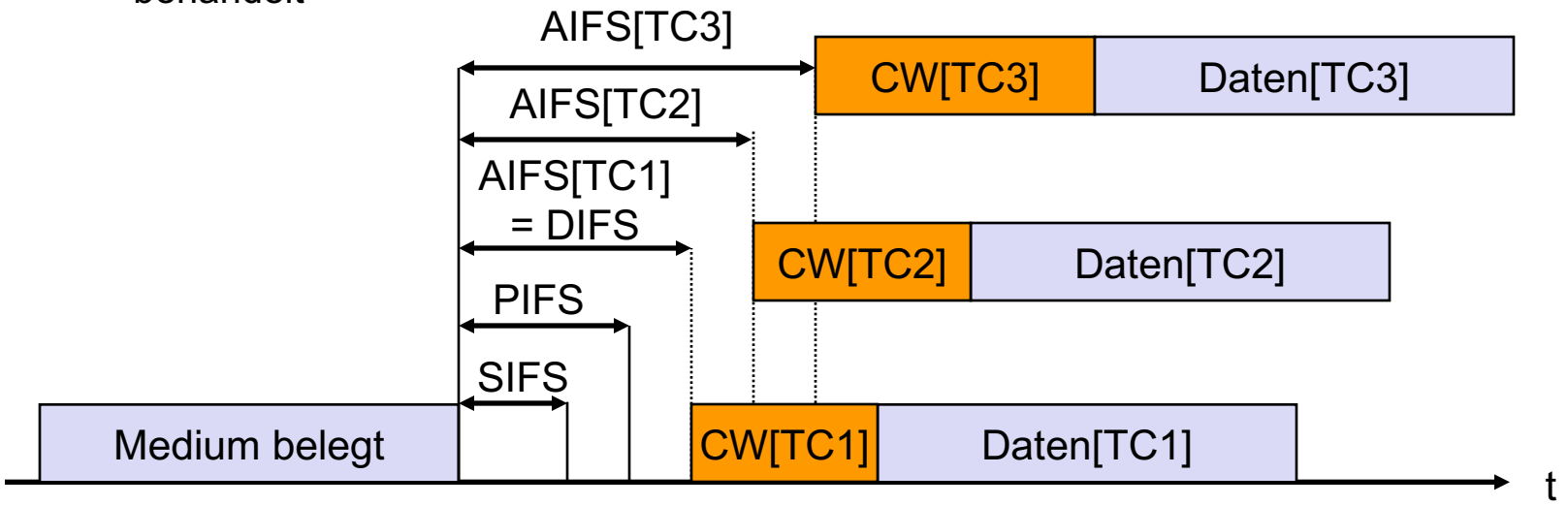
- Ziel
  - Automatischer Kanalwechsel im 5 GHz Band
    - Koexistenz mit Radar- und HIPERLAN/2 Systemen im gleichen Frequenzband
- 3 Alternative Vorgehensweisen
  - Kanal wird für eine gewisse Zeit (10 Sekunden) „ruhig gestellt“
    - Überprüfung des Kanals auf Verwendung durch andere Systeme
    - Über Beacons initiiert
    - Kriterien zur Erkennung eines anderen Systems nicht standardisiert
  - Medium wird in Sendepausen (SIFS/DIFS) nach anderen Systemen abgehört
  - Beauftragung anderer Stationen zur Überprüfung eines bestimmten Kanals
    - Senden von Measurement-Request-/Measurement-Response-Dateneinheiten
  - Fremdes System auf Kanal erkannt
    - Signalisierung eines Kanalwechsels
      - Beacons, Channel-Announcement-Dateneinheiten

Quality of Service

- Ziel
  - Bereitstellung von QoS-Fähigkeiten für zeitkritische Daten (z.B. VoIP)
    - QBSS = Funkzelle die QoS bereitstellt
- Vorgehensweise
  - Einführung von zwei neuen Medienzugriffsverfahren
    - Enhanced Distributed Coordination Function (EDCF)
      - Basiszugriffsverfahren in QBSS (ersetzt DCF)
      - Nur in CP (Contention Period) möglich
    - Hybrid Coordination Function (HCF)
      - Zentrale Verwaltung der QBSS
      - Hybrid Coordinator (HC) steuert Medienzugriff (ersetzt PCF)
      - Sowohl in CP als auch CFP möglich
  - Block-Acknowledgement-Mechanismus
    - Station kann bis zu 64 Dateneinheiten im Abstand von SIFS senden
    - Nach letzter Dateneinheit sendet die Station ein Block-ACK-Request
    - Empfänger antwortet mit Block-ACK-Response

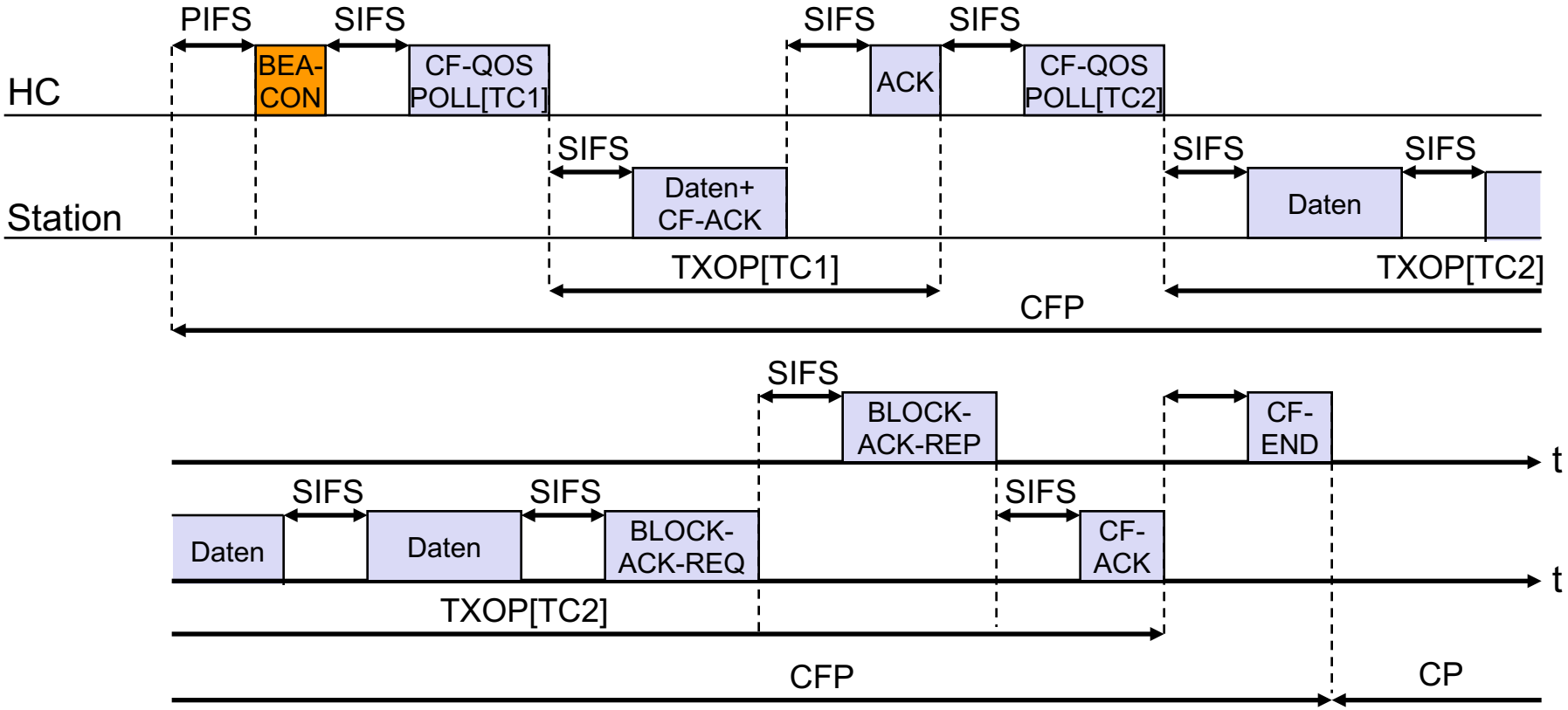
Enhanced Distributed Coordination Function

- Priorisierung von Daten durch 8 unterschiedliche Traffic Categories (TC)
- Höhere Priorität resultiert in geringerer Wartezeit beim Medienzugriff
  - Arbitration Interframe Space (AIFS)
    - Abhängig von verwendeter TC
  - Unabhängiger Backoff-Algorithmus für jede TC
    - Unterschiedliche Wertebereiche für das Wettbewerbsfenster (CW)
  - Interner Scheduler
    - Bei virtuellen Kollisionen werden Dateneinheiten mit höherer TC bevorzugt behandelt



Hybrid Coordination Function

- Transmission Opportunity (TXOP)
  - Zeitintervall für eine bestimmte Traffic Category
- Station teilen Hybrid Coordinator (HC) mit, für welche Stationen TXOPs benötigt werden
- HC leitet über QoS-Poll CFP für bestimmte TXOP ein



Zusammenfassung I

- WLAN (802.11) hat sich als drahtloses lokales Netzwerk durchgesetzt
  - Betreibbar sowohl im Infrastruktur-Modus als auch Ad-hoc Modus
- Physikalische Schicht
  - Einsatz von DSSS im Basisstandard
  - Einsatz von OFDM in neueren Lösungen mit höherer Datenrate
  - Varianten sowohl für 2,4 GHz als auch für 5 GHz Band
  - Dateneinheiten beinhalten Information über die gewünschte Datenrate
    - Anfang wird immer mit langsamster Variante gesendet
    - Rückwärtskompatibilität
    - Längenangabe in Form einer Zeitangabe

Zusammenfassung II

- Medienzugriff
  - CSMA/CA-Verfahren
    - CSMA/CD nicht anwendbar
      (versteckte Endgeräte, gleichzeitiges Senden und Empfangen …)
  - Zwei Zugriffsarten
    - Distribution Coordination Function (dezentral)
    - Point Coordination Function (zentral)
  - ARQ-Verfahren, Fragmentierung und Sicherheitsmechanismen in der MAC-Schicht
  - MAC-Dateneinheiten
    - Komplexer als z.B. bei Ethernet
    - Variable Kopflänge, Zeitangabe, mehrere Adressen
    - Frame-Controll Feld mit zusätzlicher Information
- MAC-Management
  - Synchronisation
  - Sicherheit (z.B. Authentifikation)
  - Scanning
  - Assoziierung/Reassoziierung
  - Power-Management

Erweiterungen in IEEE 802.11

- Inzwischen: zahlreiche Erweiterungen

IEEE Standard	Beschreibung
802.11	WLAN für 1-2 Mbit/s im 2,4 GHz-Band
802.11a	WLAN bis 54 Mbit/s im 5 GHz-Band
802.11b	Erweiterung von 802.11 bis 11 Mbit/s im 2,4 GHz Band
802.11d	Anpassung an nationale Regelungen
802.11e	MAC-Erweiterung zu 802.11a und b, um Quality of Service und verbessertes Power Management zu ermöglichen
802.11f	Kommunikation zwischen den Access Points (IAPP, Inter Access Point Protocol)
802.11g	Höhere Datenraten (bis 54 Mbit/s) im 2,4 GHz-Band
802.11h	Höhere Datenraten auf dem 5 GHz-Band mit automatischer Leistungsregelung und dynamischer Frequenzwahl
802.11i	MAC-Erweiterung, um verbessertes Sicherheits- und Authentifizierungsmechanismen zu ermöglichen

Aktuelle IEEE 802.11 Arbeitsgruppen

Arbeits-gruppe	Beschreibung
802.11j	Spezielles WLAN für Japan im 4,9 GHz und 5 GHz Band
802.11k	Interface für höhere Layer für Zugriff auf PHY- und MAC-Informationen
802.11n	„Next Generation WiFi“, Datenraten > 100 Mbit/s
802.11p	WiFi für Kommunikation zwischen Autos
802.11r	Minimierung der Verzögerung beim Wechsel der BSS
802.11s	Wireless Distribution System (WDS)
802.11t	Tests, Vergleiche und Einsatz von WLAN Geräten
802.11u	Spezifizierung der Informationen, die zwischen APs im DS ausgetauscht werden
802.11v	Interworking mit anderen Netzen

Übungen

5.1 Welche grundsätzlichen Organisationsformen gibt es für drahtlose lokale Netze?

5.1 Welche Modulationsverfahren kommen bei 802.11 DSSS zum Einsatz?

5.2 Mit welchen Verfahren werden in 802.11b verschiedene Datenraten erzielt?

5.3 Welche Probleme ergeben sich in drahtlosen LANS, die wir in drahtgebundenen LANs generell nicht haben?

5.4 Welche unterschiedlichen Medienzugriffsverfahren sind in 802.11 spezifiziert?

5.5 Welche konkrete Funktion erfüllt der Network Allocation Vector (NAV)?

5.6 Wie sind Sendeprioritäten in CSMA/CA realisiert?

5.7 Wie wird in WLAN Netzen Quality of Service sichergestellt?

Referenzen und weiterführende Literatur

[5.1] J. Rech, Wireless LAN – 802.11-WLAN-Technologien und praktische Umsetzung im Detail, Verlag Heinz Heise, 2004

[5.2] B. O'Hara, A. Petrick, The IEEE 802.11 Handbook – A Designers Companion IEEE, 1999

[5.3] J. Schiller, Mobilkommunikation; Addison-Wesley, 2003 (Kapitel 7)

[5.4] A. Chandra, V. Gummalla, J. Limb, Wireless Medium Access Control Protocols, IEEE Communications Surveys & Tutorials, www.comsoc.org/livepubs/surveys/public/2q00issue/gummalla.html, 6/2000

[5.5] I. Stojmenovic, ed., Handbook of Wireless Networks and Mobile Computing – Kapitel 6: Wireless Media Access Control, John Wiley & Sons, February 2002

[5.6] http://www.rz.uni-karlsruhe.de/rd/dukath.php

[5.7] C.-K. Toh, Ad Hoc Mobile Wireless Networks: Protocols and Systems, Prentice Hall, 2002

[5.8] C. Perkins, Ad-hoc Networking, Addison Wesley, 2000

[5.9] IETF MANET Working Group http://www.ietf.org/html.charters/manet-charter.html

[5.10] The MANET Bibliography http://www.antd.nist.gov/wctg/manet/manet_bibliog.html

[5.11] http://nostringsattachedshow.com/2012/01/06/dsss-with-802-11-prime-and-802-11b/

[5.12] Ernst Ahlers: Funk-Evolution. In: c't. Nr. 13, 2009, S. 86-89.

[5.13] http://www.dell.com/downloads/global/shared/broadcom_802_11_g.pdf