

Netzwerke II

Kapitel 2 – Drahtlose Netzwerke

Prof. Dr. L. Wischhof <wischhof@hm.edu>

Fakultät 07 – Hochschule München

Einführung

Motivation

- Stark steigender Anteil **mobiler, drahtloser** Sprach- und Datenübertragung in den letzten 25 Jahren

Beispiele:

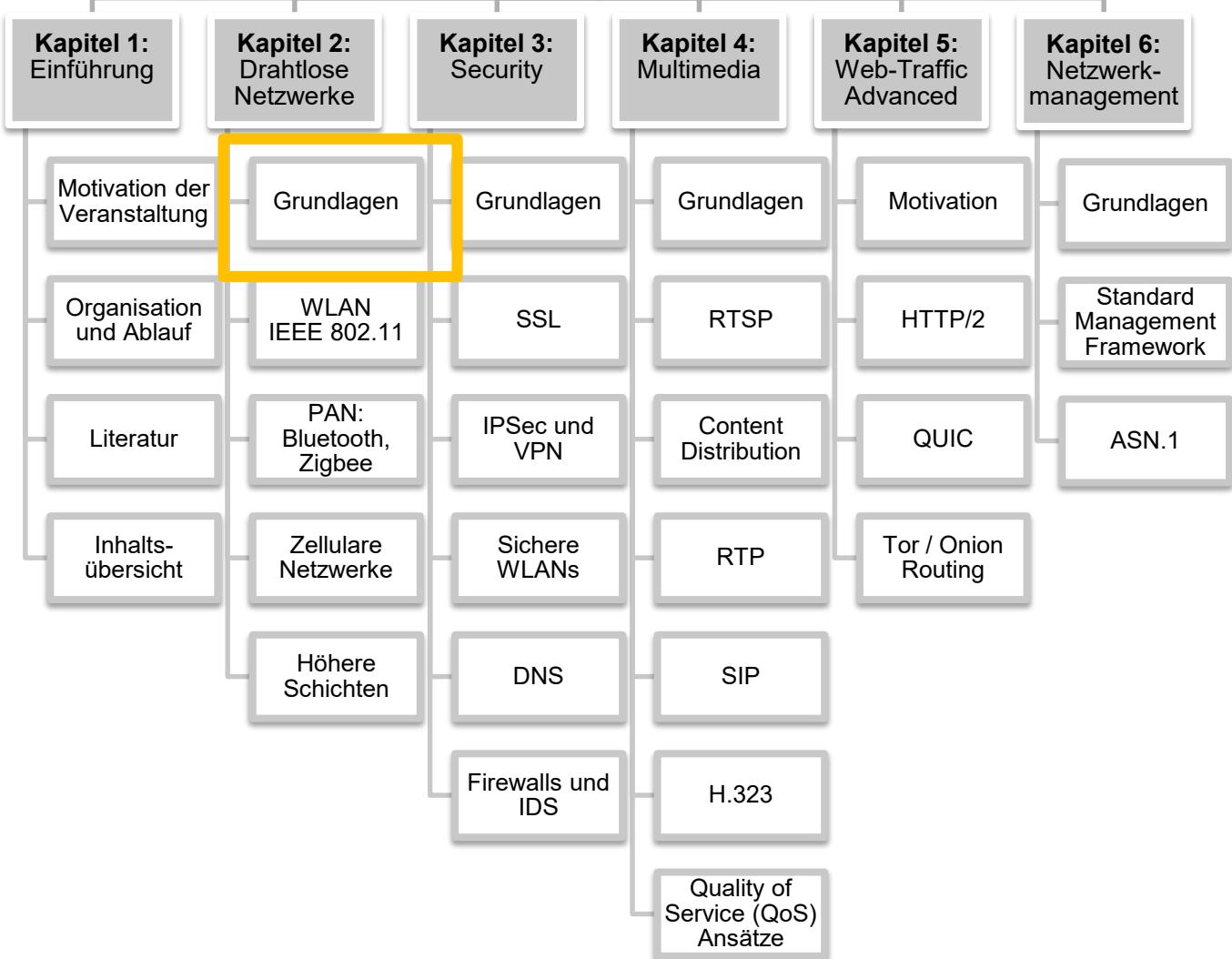
Verhältnis Mobiltelefonie zu Festnetztelefonie: ca. 5:1 !,
mehr als die Hälfte aller Internet-Teilnehmer drahtlos angebunden

- **Wichtigkeit drahtloser Netzwerke** nimmt zu
- Neue Herausforderungen für Datenübertragung
- ABER: viele im Internet eingesetzte Verfahren/Protokolle ursprünglich für **drahtgebundene** Netze entworfen!

Unterscheidung zweier Arten von Herausforderungen

- (1) Drahtloser Übertragungskanal (wireless link)
- (2) Mobilität des Nutzers bzw. Endgeräts

Netzwerke II



Einführung

Ziele dieses Kapitels

Die Datenübertragung über drahtlose und mobile Netzwerke zeichnet sich durch besondere Eigenschaften und Herausforderungen aus.

Im Folgenden soll ein Grundverständnis hierfür sowie für die aktuell verwendeten Übertragungsverfahren und Protokolle erzielt werden.

Grundlagen

Elemente in drahtlosen Netzwerken

Drahtloser Teilnehmer (wireless host)

- Endsystem auf dem die Applikation läuft
- Stationär oder mobil
- Beispiele: Notebook, Smartphone, Desktop mit WLAN-Karte

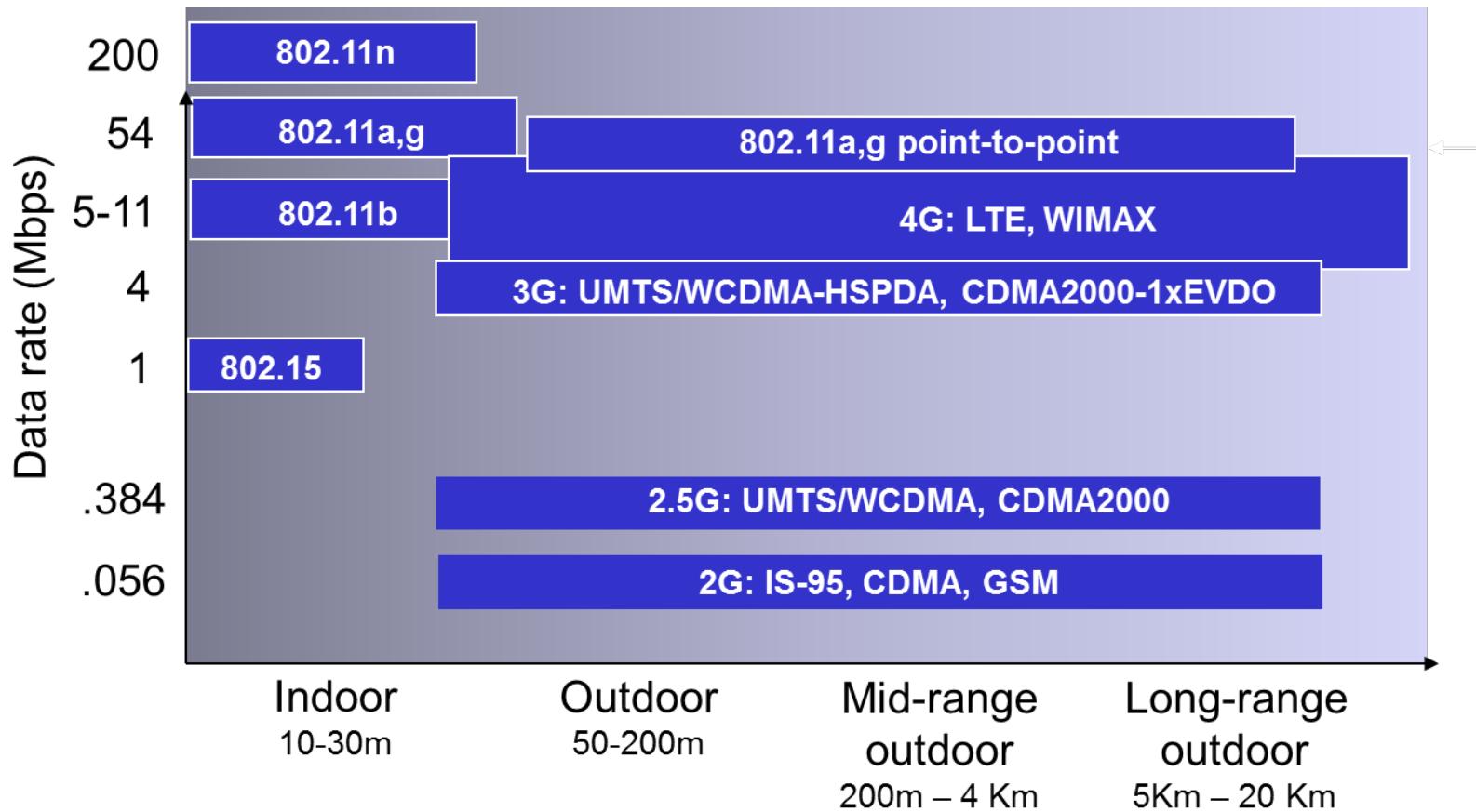
Drahtlose Verbindung (wireless link)

- Verbindet Teilnehmer mit Basisstation oder (falls erlaubt) direkt mit anderem Teilnehmer
- Zentrale Eigenschaften:
 - Abdeckung (coverage area)
 - Datenrate



Grundlagen

Abdeckung und Datenrate typischer Standards



Quelle: [1], Seite 543

Grundlagen

Elemente in drahtlosen Netzwerken

Basisstation (base station)

- Teil der Netzwerkinfrastruktur
- Meist selbst mit drahtgebundenem Netz verbunden
- Agiert als Relay: Übertragung von Datenpaketen zwischen drahtlosem und drahtgebundenem Netzwerk in abgedecktem Gebiet
- Beispiele: WLAN Access Point, UMTS Basisstation (NodeB)

Unterscheidung zweier drahtloser Netzwerkarten

- (1) Infrastruktur-basiert
 - Netzwerketeilnehmer über Basisstation mit Netz verbunden
- (2) Ad-Hoc Netzwerk
 - Keine Infrastruktur (Basisstationen), Teilnehmer erbringen Netz

Grundlagen

Elemente in drahtlosen Netzwerken

Unterscheidung nach Anzahl drahtloser Übertragungen

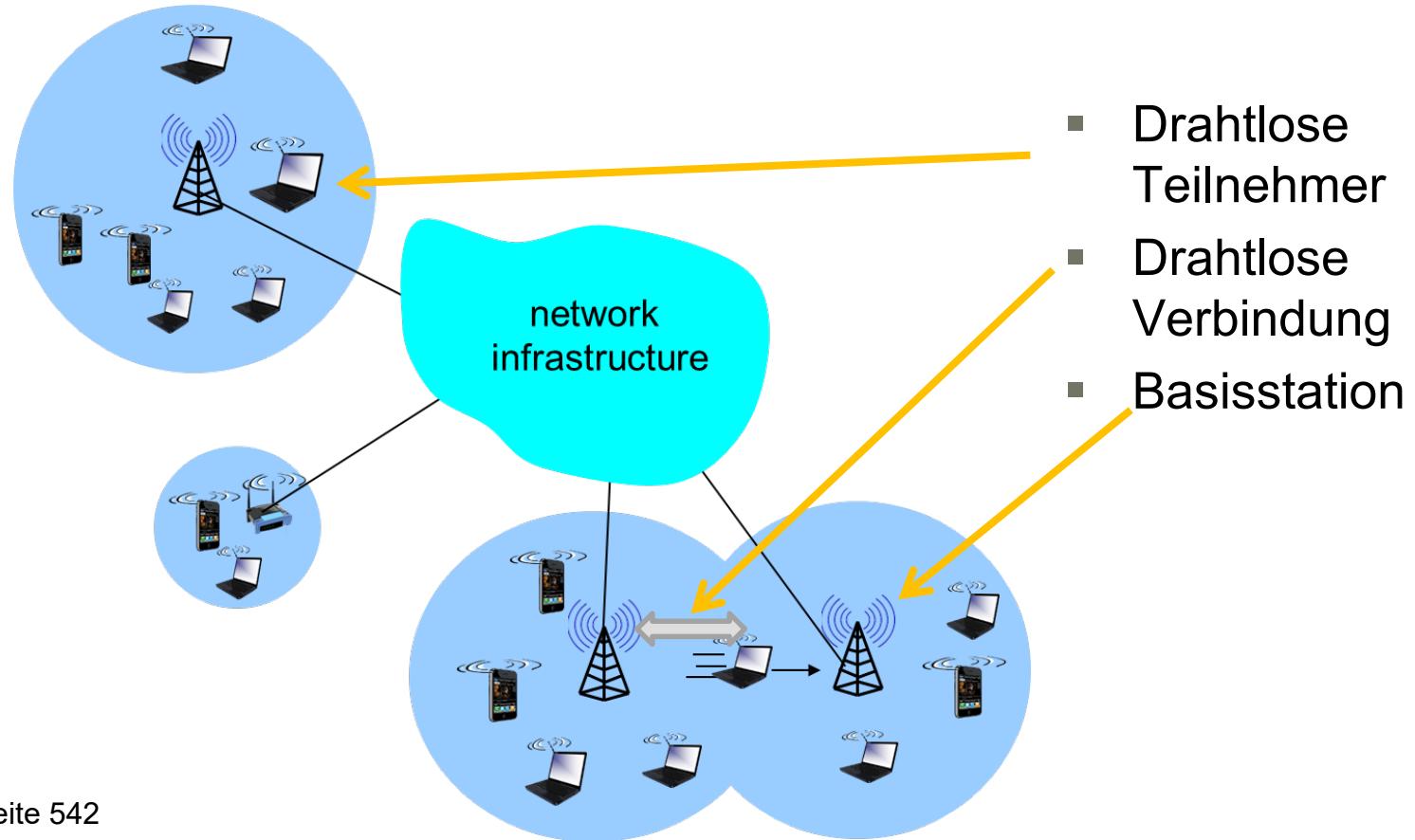
- (1) **Single-hop**: genau ein drahtloser Link
- (2) **Multi-hop**: Übertragung auch über mehrere drahtlose Links in Folge

	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: <i>mesh net</i>
no infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET

Quelle: [1]

Grundlagen

Elemente in drahtlosen Netzwerken – Beispiel



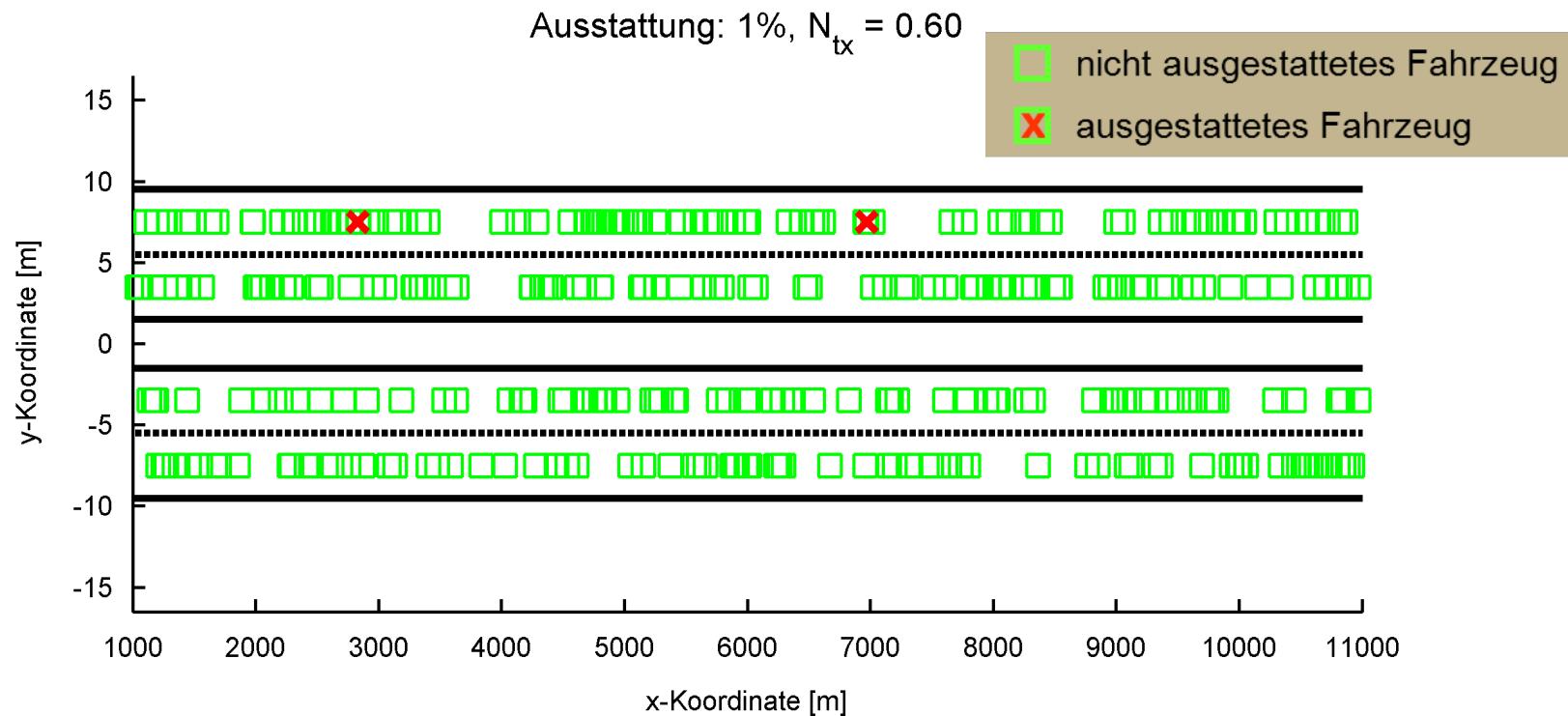
Quelle: [1], Seite 542

Grundlagen

Beispiel: Vehicular Ad Hoc Network (VANET)

Hochdynamisches drahtloses Netz, Eigenschaften stark abhängig von

- Funkreichweite, Fahrspuren, Verkehrsdichte, Ausstattungsgrad
⇒ N_{tx} mittlere Zahl anderer Fahrzeuge in Funkreichweite



Grundlagen

Drahtloser Übertragungskanal (1/3)

Drahtloser Kanal unterscheidet sich von drahtgebundenem in wesentlichen Eigenschaften

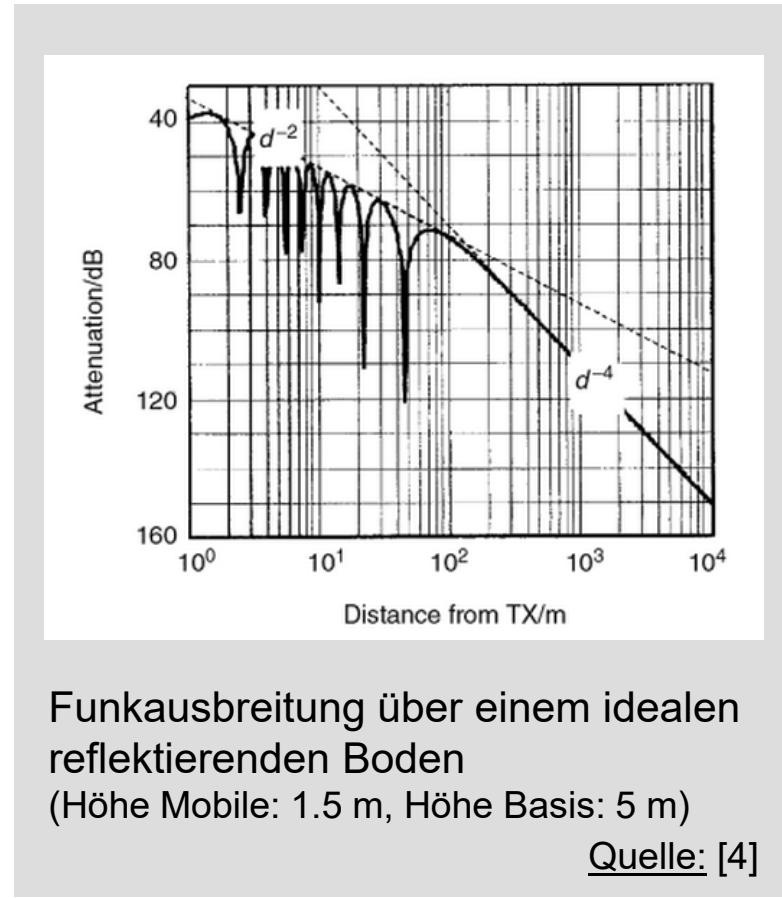
- **Dämpfung** (path loss)
 - Elektromagnetische Strahlung wird durch Luft, Wände etc. gedämpft → Signalstärke sinkt mit steigender Entfernung
- **Beeinträchtigung durch Störer** (interference)
 - Andere Sender (z.B. im ISM Band bei 2.4 GHz)
 - Elektrische Geräte (Motoren, Mikrowelle, etc.)
- **Mehrwegeausbreitung** (multipath)
 - Signal wird an unterschiedlichsten Objekten reflektiert
 - Am Empfänger überlagern sich unterschiedlich zeitlich verschobene Versionen des Sendesignals
→ konstruktive aber auch destruktive Überlagerung möglich!



Grundlagen

Drahtloser Übertragungskanal (2/3)

- Funkkanal in der Regel **unzuverlässiger** als drahtgebundener Kanal
- Mehrere Nutzer (teilweise, z.B. in ISM Bändern, sogar unterschiedliche Techniken!) teilen sich den Kanal („**shared medium**“)
- **zeit- und ortsvariantes Verhalten**
⇒ jeder Nutzer sieht „einen Kanal mit anderen Eigenschaften“
- **Mobilität** der Nutzer
⇒ Änderung der Umgebungs-/Abschattungssituation



Grundlagen

Drahtloser Übertragungskanal (3/3)

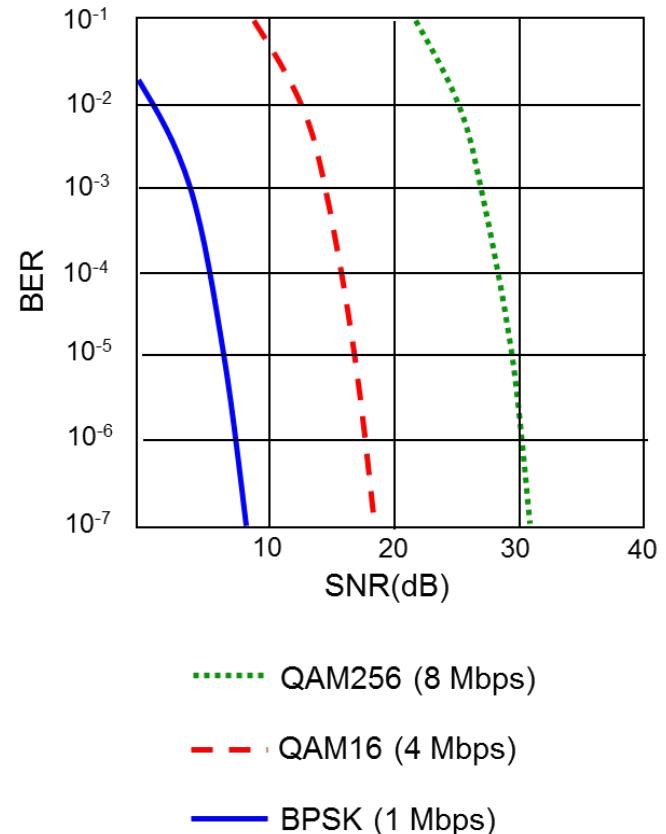
- Nutzsignal (Daten) wird vor der Übertragung **moduliert**
 - ➔ Daten werden durch Änderung eines Trägersignals einer bestimmten Trägerfrequenz dargestellt
 - Unterschiedlichste **Modulationsarten**
 - Änderung der Amplitude: Amplitudenmodulation
 - Änderung der Frequenz: Frequenzmodulation
 - Änderung der Phase: Phasenmodulation
 - oder auch Kombinationen davon, z.B. Änderung von Amplitude und Phase, z.B. Quadraturamplitudenmodulation (QAM)
- ➔ Übertragung von Symbolen, wobei ein Symbol die Information eines oder mehrerer Bits codieren kann
- ➔ Höhere Modulationsart überträgt mehr Bit/Symbol ist aber in der Regel fehleranfälliger



Grundlagen

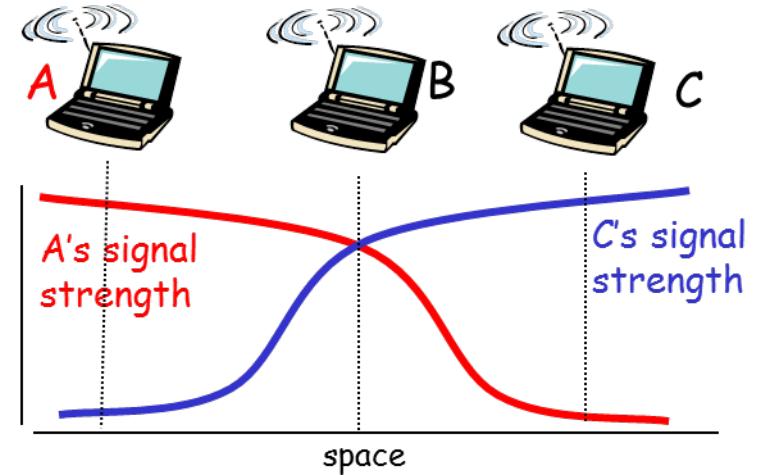
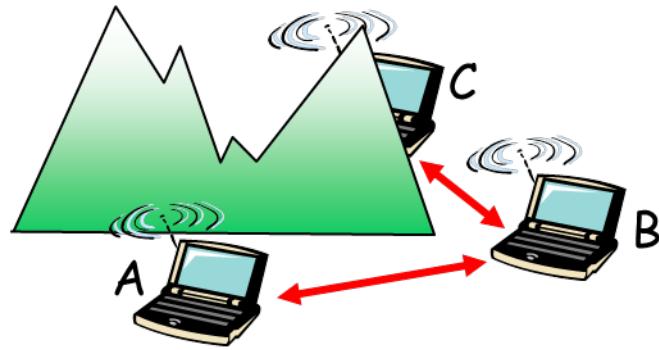
Signal-zu-Rausch Verhältnis (signal-to-noise ratio, SNR)

- Empfänger sieht Mischung aus gedämpften, durch Ausbreitung verändertem Sendesignal und Störungen
- SNR beschreibt Verhältnis von Stärke des empfangenen Signals zu Störungen/Rauschen
- Größeres SNR → Signal leichter zu empfangen → höhere Modulation kann eingesetzt werden
- Bit-Error-Rate (BER): Wahrscheinlichkeit, dass ein übertragenes Bit fehlerhaft empfangen wird



Grundlagen

Hidden Terminal Problem



- A und B hören sich
- B und C hören sich
- ABER: A und C hören sich nicht → bemerken nicht, dass sie sich bei gleichzeitiger Übertragung an B gegenseitig stören!

Quelle: [1], Seite 548

Was könnte man tun, um das Problem zu beseitigen/zu mindern?

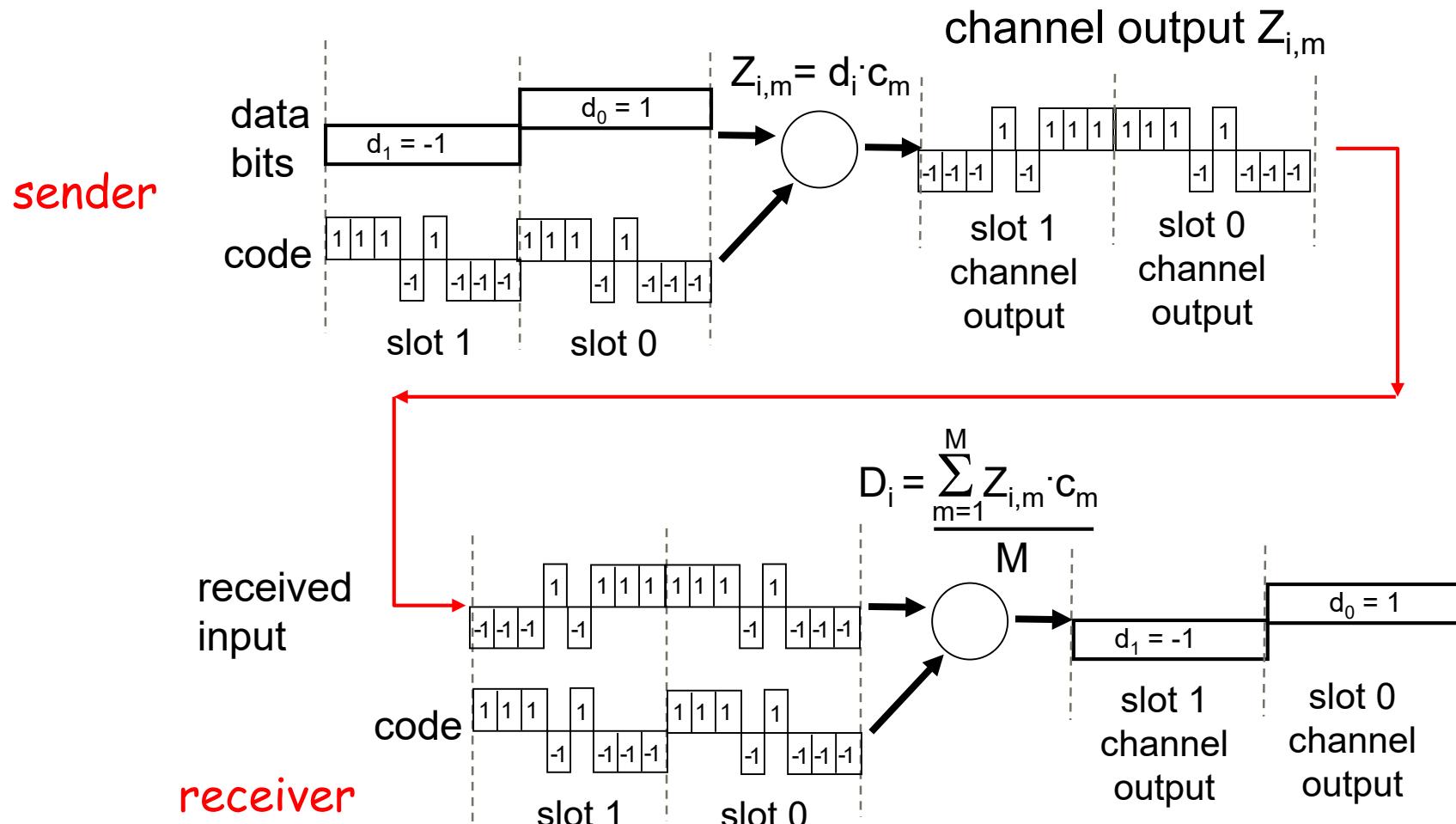
Grundlagen

Code-Division Multiple Access (CDMA)

- aus Netzwerke I sind verschiedene Verfahren zum Zuteilen von Ressourcen auf einem Kanal bekannt (TDMA, FDMA)
- In vielen drahtlosen Netzen wird weiteres Verfahren genutzt:
Code-Division Multiple Access (CDMA)
 - Teilnehmern werden unterschiedliche (orthogonale) Codes zugeordnet
 - Zu sendende Daten werden mit Code multipliziert („gespreizt“), zu übertragende Ergebnisbits werden **Chips** genannt
 - Mehrere Teilnehmer übertragen **zur gleichen Zeit im gleichen Band**
 - ➔ eigene Daten werden bitweise Multiplikation mit dem Code zurückgewonnen
 - ➔ andere Teilnehmer wirken als (zusätzliches) Rauschen
 - zusätzliche Teilnehmer: Signal-zu-Rausch Abstand (Signal-to-Noise Ratio, SNR) verringert sich, Sendeleistung muss erhöht werden

Grundlagen

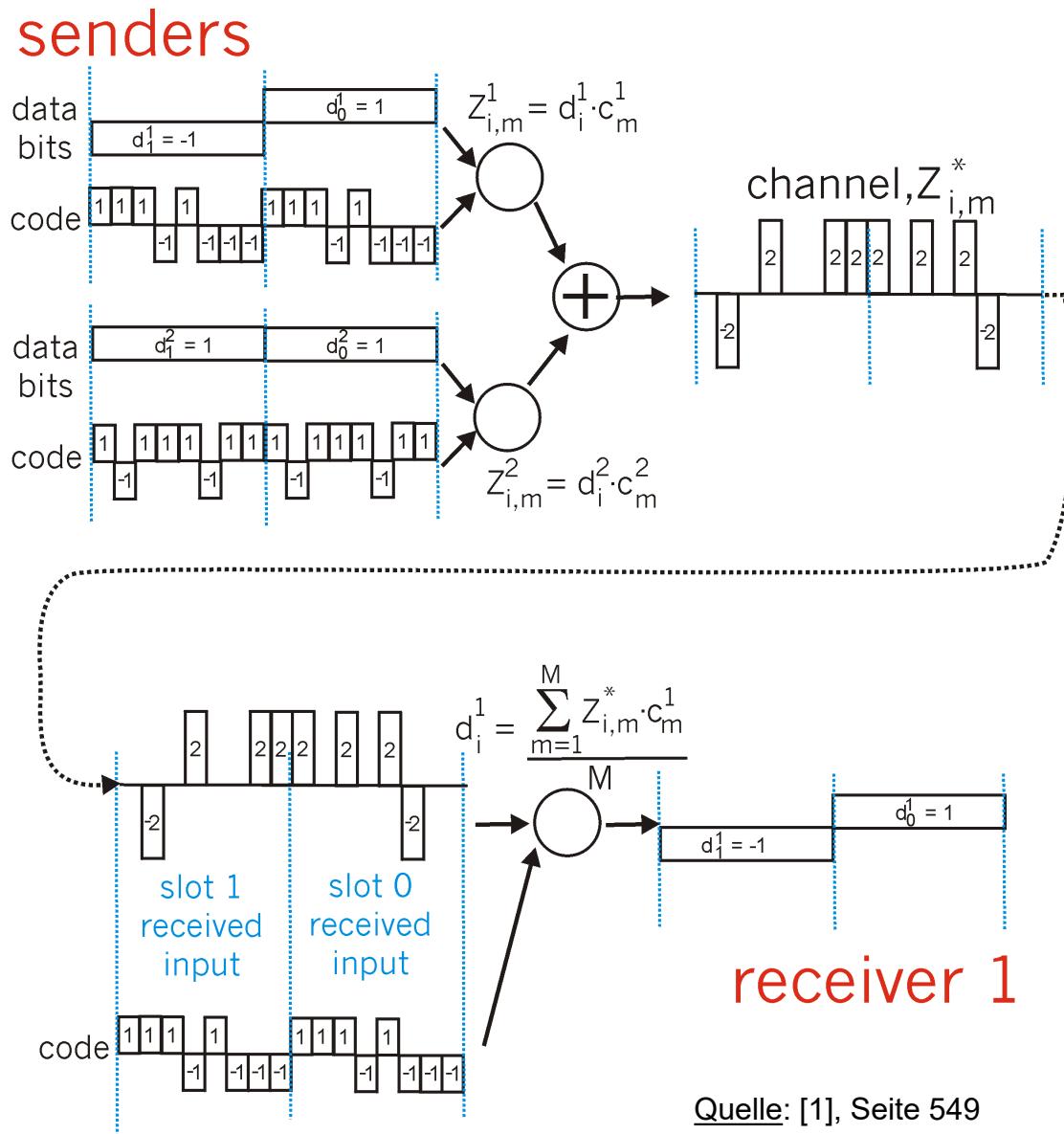
CDMA – Beispiel zur Kodierung/Dekodierung



Grundlagen

CDMA – Beispiel mit zwei Sendern

- Empfänger kann gesendetes Signal durch Multiplikation mit passendem Spreizcode zurückgewinnen

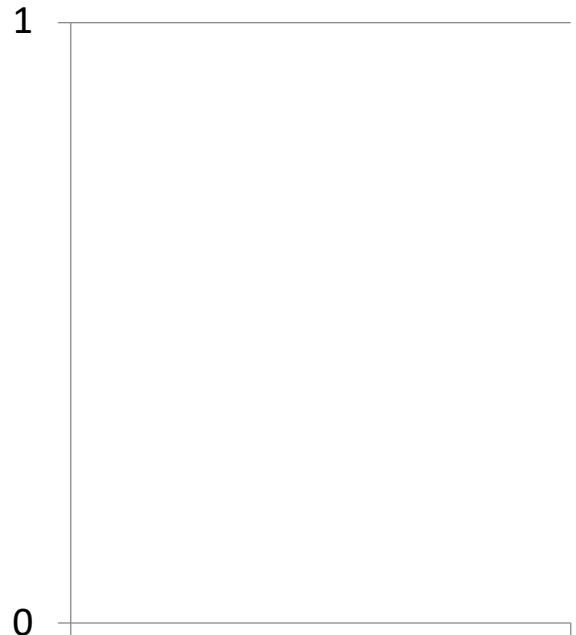


Wiederholung: Netzwerkarten

Beim LRZ-WLAN hier an der Hochschule handelt es sich um ein Infrastruktur-basiertes multi-hop Ad-Hoc Netzwerk.

- A) Ja
- B) Nein

ID = wischhof@hm.edu
Umfrage noch nicht
gestartet



Umfrage starten

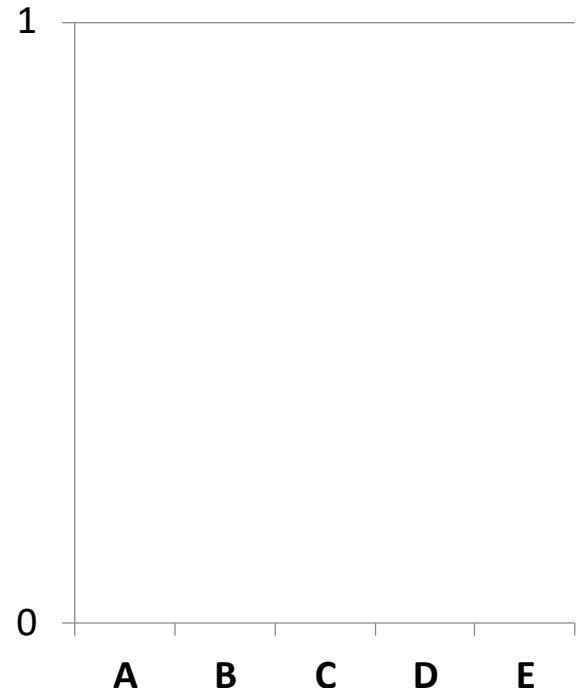
Wiederholung: SNR und BER

Ihre drahtlose Netzwerkkarte festgestellt, dass die BER zu hoch ist, um Pakete erfolgreich zu übertragen. Ursache ist ein geringes SNR.

Was kann helfen, um die Übertragung der Daten zu verbessern?

- A) Erhöhung der Sendeleistung
- B) Niedrigere Modulationsart,
z.B. QAM-16 statt QAM-256
- C) Höhere Modulationsart,
z.B. QAM-256 statt QAM-16
- D) A und B
- E) A und C

ID = wischhof@hm.edu
Umfrage noch nicht
gestartet



Umfrage starten

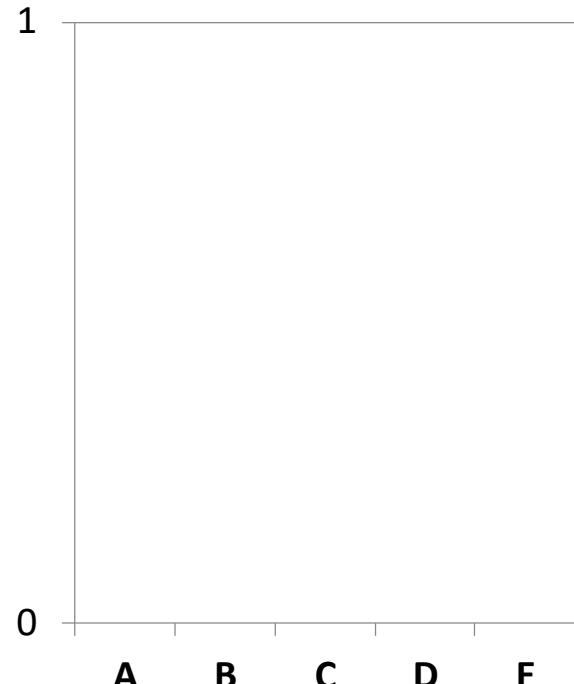


Wiederholung: Hidden Terminal Problem

Was versteht man unter dem Hidden Terminal Problem?

- A) Signal des einen Senders ist durch CDMA Verfahren für anderen nicht sichtbar
- B) Empfänger kann nicht empfangen wenn er gleichzeitig sendet
- C) Signale zweier Sender, welche sich gegenseitig nicht empfangen können, kollidieren am Empfänger
- D) Leistungsunterschied im Sendesignal zweier Sender
- E) Keine Ahnung

ID = wischhof@hm.edu
Umfrage noch nicht gestartet



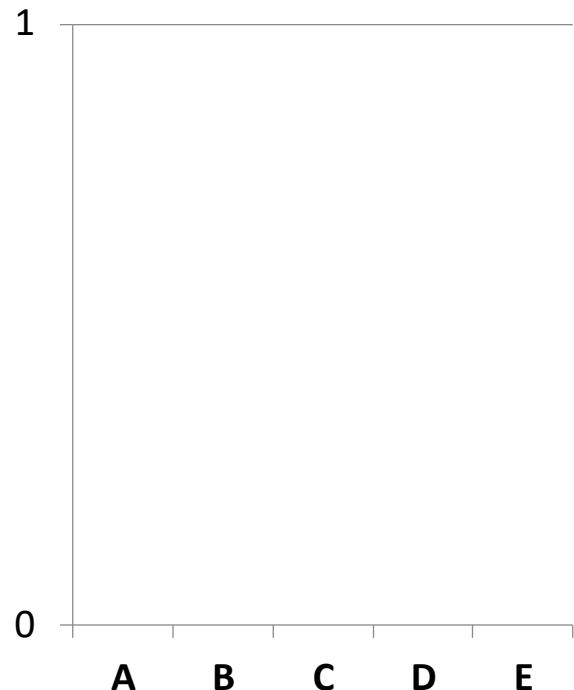
Umfrage starten

Wiederholung/Transfer: CDMA

Wie wirkt sich ein längerer Spreizcode beim CDMA Verfahren aus?

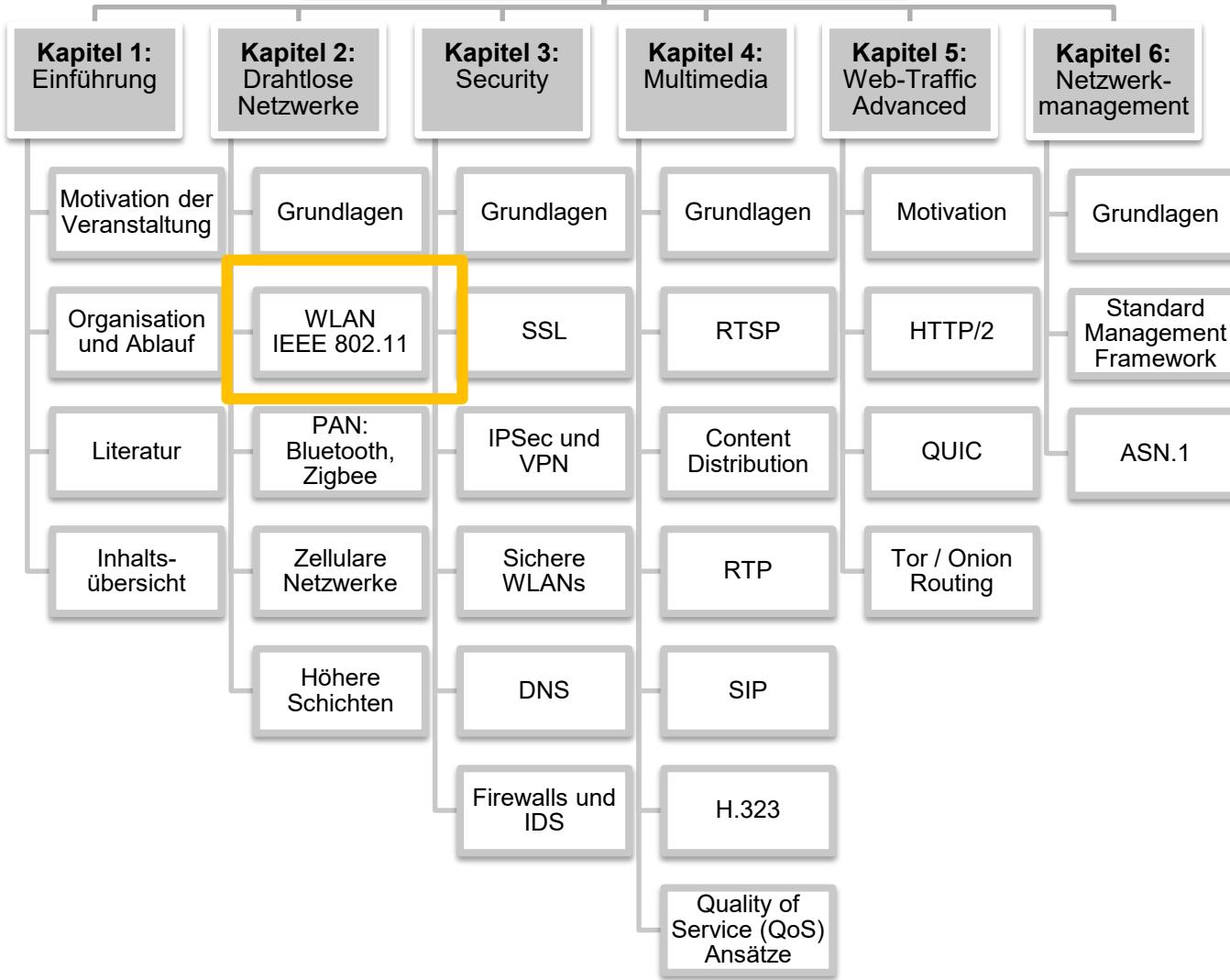
- A) Die Datenrate steigt
- B) Die Datenrate sinkt
- C) Es können mehr Sender gleichzeitig senden ohne sich zu stören
- D) Übertragung ist weniger störanfällig
- E) B, C und D

ID = wischhof@hm.edu
Umfrage noch nicht gestartet



Umfrage starten

Netzwerke II



Wireless Local Area Networks

Motivation

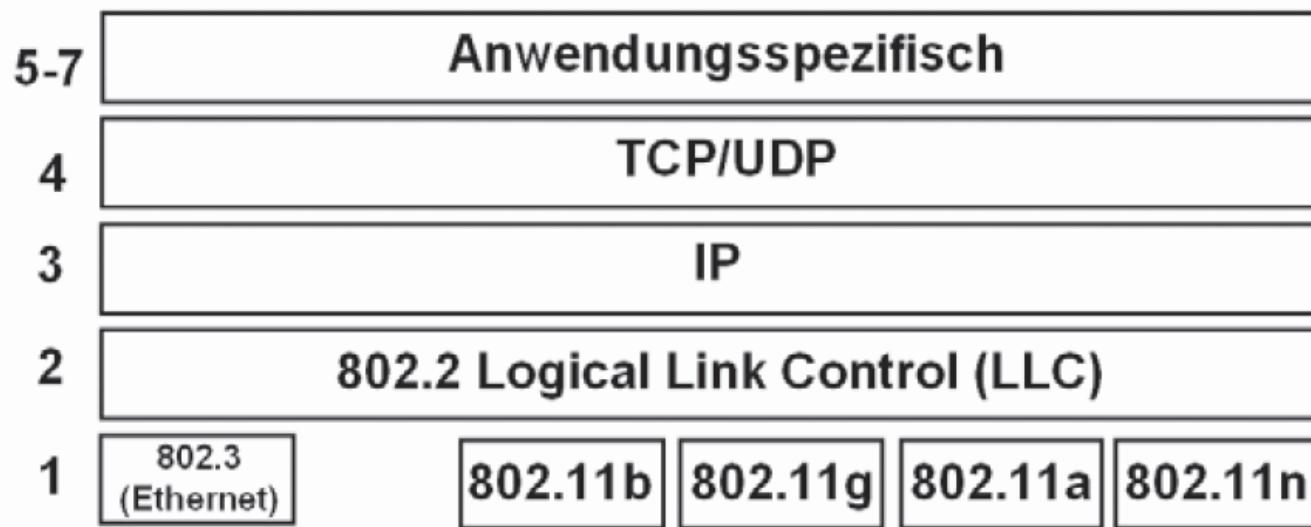
- Datenkommunikation über Mobilfunknetze ist nur über Nutzung eines Mobilfunkanbieters möglich (→ Lizensierung der Frequenz)
 - Kosten für Vertrag
 - SIM Karte für jeden Teilnehmer
 - Beschränkung der Datenrate und des Datenvolumens
- Alternativen für lokale (drahtlose) Kommunikation?

Idee: Übertragung des LAN Standards (802.X, Ethernet) in den drahtlosen Bereich, in einem nicht-lizenzierten Frequenzband.

- Nutzung eines freien ISM (Industrial, Scientific, Medical) Frequenzbandes
- Nutzer selbst für Bereitstellung der Infrastruktur verantwortlich
- Kostengünstige Access Points und Endgeräte

Wireless Local Area Networks

Grundlagen: Protokollstack



Quelle: [4], S. 338

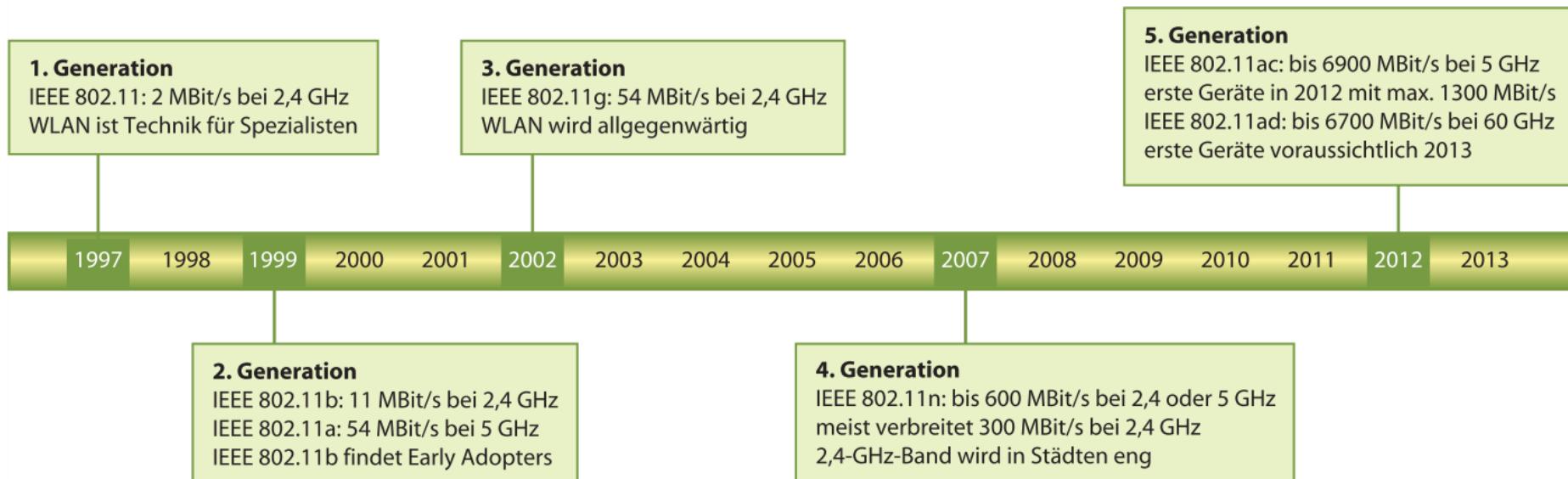
Wireless Local Area Networks

Grundlagen: Standards

Standard	Frequenzband	Geschwindigkeit	Beschreibung
802.11	2,4 GHz	1 – 2 MBit/s	Ursprungsstandard, 1997, FHSS/DSSS
802.11b	2,4 GHz	1 – 11 MBit/s	1999, DSSS
802.11a	5 GHz	6 – 54 MBit/s	1999, OFDM
802.11g	2,4 GHz	6 – 54 MBit/s	2003, OFDM
802.11n	2,4 / 5 GHz	6 – 600 MBit/s	2009, OFDM, MIMO
802.11p	5,9 GHz	3 – 27 MBit/s	2010, Inter-Vehicle Communication, OFDM
802.11ac	5 GHz	Bis 6,93 GBit/s	2014, MU-MIMO im Downlink (DL)
802.11ad (WiGig)	60 GHz	> 7 GBit/s	2016, Punkt-zu-Punkt
802.11ax	2,4 / 5 GHz (1-7 GHz)	11 GBit/s	2019, bis 1024-QAM, MU-MIMO in UL und DL
802.11ay	60 GHz	20 – 40 GBit/s	2019, Nachfolger von ad

Wireless Local Area Networks

Grundlagen: Standards - Überblick



Quelle: Heise Online, 15.10.2013



Wireless Local Area Networks

Grundlagen

Basic Service Set (BSS)

- Stationen, die (innerhalb eines geographischen Bereiches) auf dem gleichen Übertragungskanal Daten austauschen

Extended Service Set (ESS)

- Zusammenschluss mehrerer BSS zu einem Kommunikationsnetz, in dem Roaming von einem BSS zum nächsten erfolgt

Service Service Set ID (SSID)

- Name des Netzwerkes



Wireless Local Area Networks

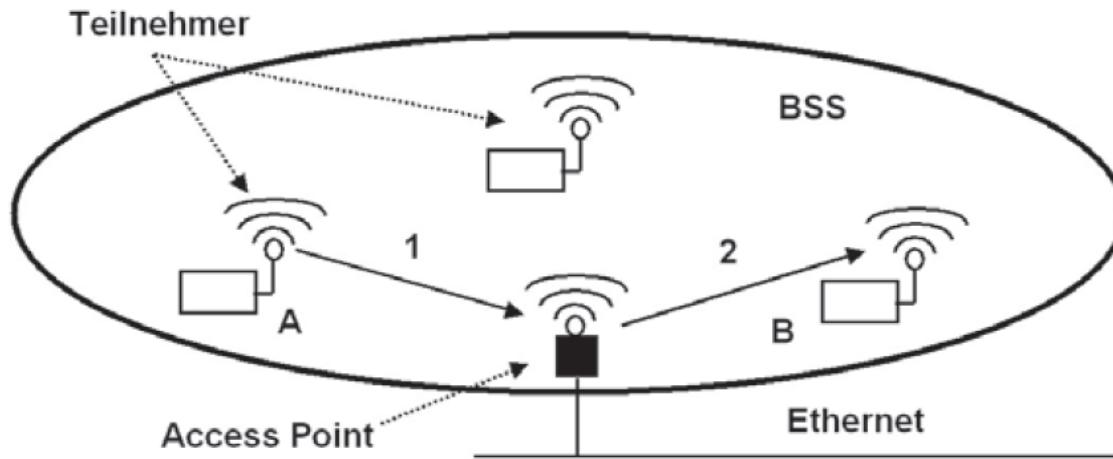
Modi

Ad-Hoc Mode / Independent BSS (IBSS)

- Alle Stationen sind gleichberechtigt, kein Access Point

Infrastructure BSS

- Geräte kommunizieren über Access Point (AP)
- AP ist in der Regel zudem Übergang in drahtgebundenes Netz

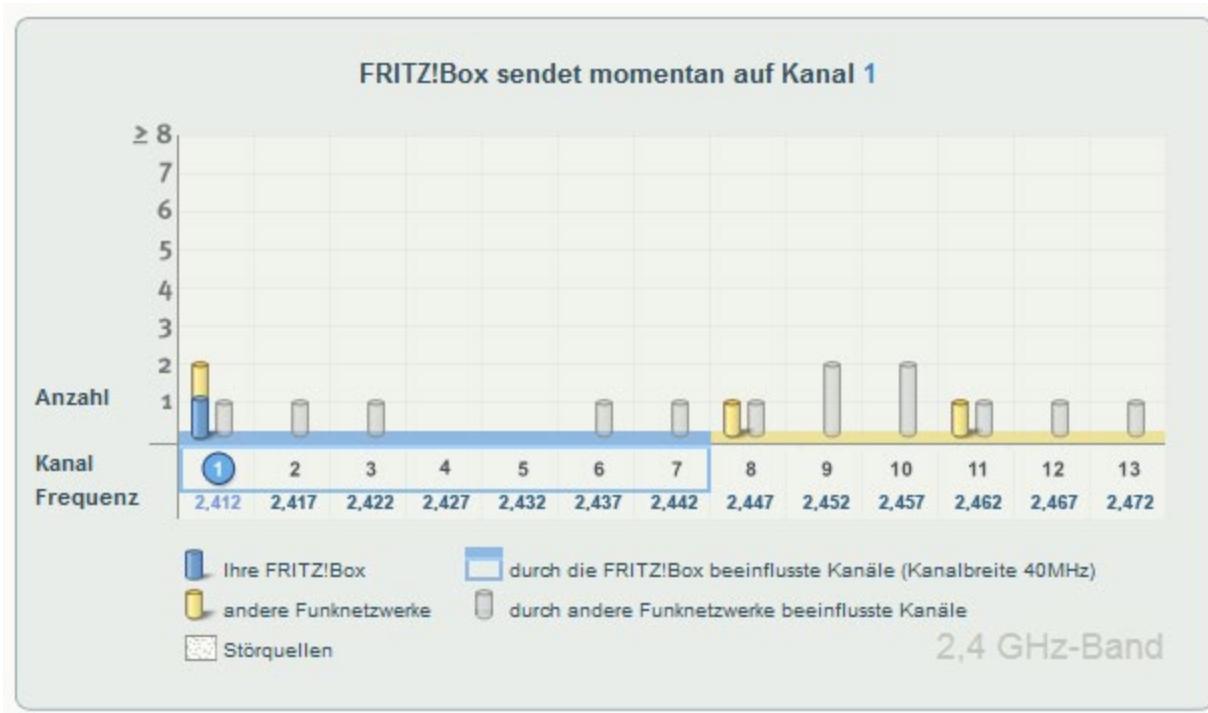


Quelle: [4], S. 342

Wireless Local Area Networks

Kanäle

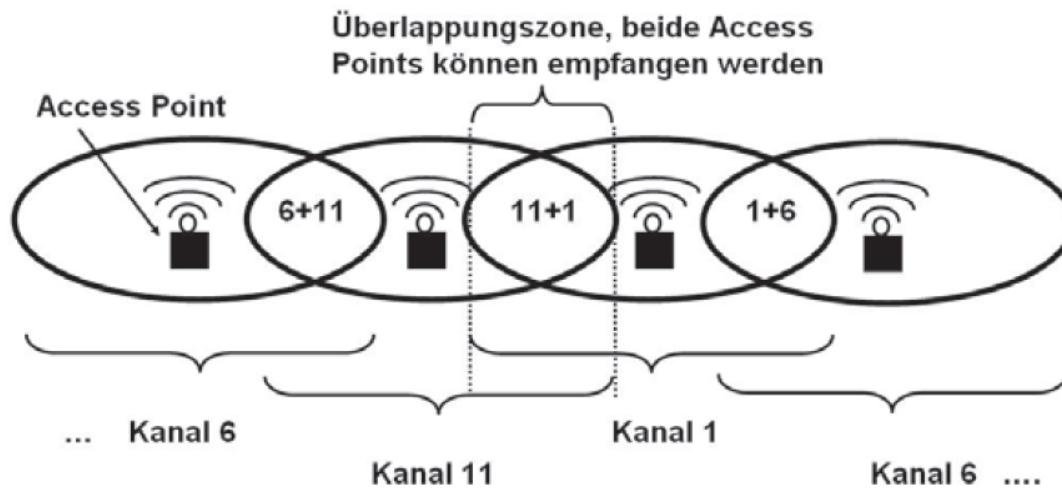
*Sie kennen doch sicher folgendes Bild
(oder das eines ähnlichen Access Points):*



Wireless Local Area Networks

Kanäle

- Definition von (je nach Land) bis zu 13 Kanälen mit je 5 MHz im Bereich 2410 MHz bis 2483 MHz
- Breite 22MHz bei DSSS, 20 MHz/40 MHz bei OFDM ohne/mit Kanalbündelung
→ Störungsfreier Betrieb nur bei passendem Abstand (→ 5 Kanäle bei DSSS)



Quelle: [4], S. 346

Wireless Local Area Networks

Assoziation mit AP

- Im Infrastrukturmodus ist vor der Übertragung von Nutzdaten eine **Assoziation mit einem Access Point** notwendig

Wie erkennt die Wireless Station welche APs in Reichweite sind?

- AP sendet periodisch sogenannte Beacon Frames
 - Spezieller Rahmen der SSID und MAC Adresse enthält

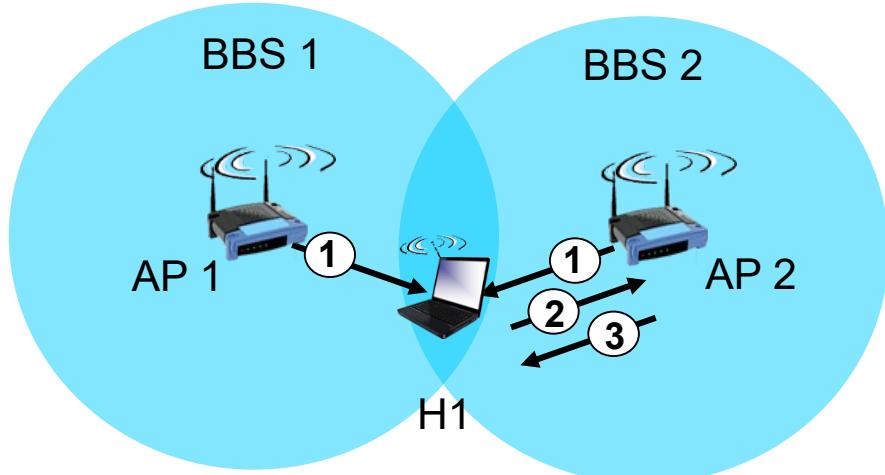
Typischer Ablauf

- Wireless Station scannt Kanäle und sucht nach Beacon Frames
- Wählt einen verfügbaren AP aus (je nach Einstellung, Signalstärke)
- Führt Authentifizierung durch (falls notwendig)
- Erhält IP-Adresse über DHCP (siehe Netze I, falls keine feste IP)



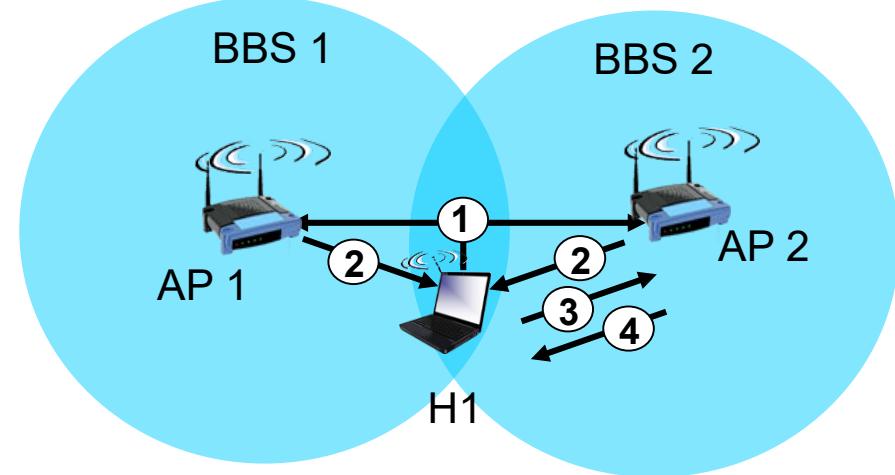
Wireless Local Area Networks

Passives und aktives Scannen



Passives Scannen

- Host H1 ist passiv, hört Kanal ab
- APs senden Beacon Frames
- H1 sendet Association Request an ausgewählten AP (hier: AP 2)
- AP 2 sendet Association Response an H1



Quelle: [1], Seite 557

Aktives Scannen

- H1 sendet Probe Request
- APs senden Probe Response
- H1 sendet Association Request an ausgewählten AP (hier: AP 2)
- AP 2 sendet Association Response an H1



IEEE 802.11 WLANs

Bestätigungen auf Schicht 2 (Link Layer ACKs)

- Übertragung über Luftschnittstelle ist **unzuverlässig**
 - Interferenz von anderen Teilnehmern, anderen Netzen, Geräten
 - Schwächung des Signals durch Fading etc.
- Im Gegensatz zu drahtgebundenem Ethernet ist dem Sender **keine Kollisionserkennung** (Collision Detection, CD) möglich
 - Gleichzeitiges Senden und Empfangen einer Funksignals aufgrund der unterschiedlichen Signalstärken am Sender nicht möglich
 - Durch Hidden Terminal Problem verursachte Kollisionen können ohnehin nicht erkannt werden

→ Abhilfe: Bestätigungen (ACKs) auf Schicht 2

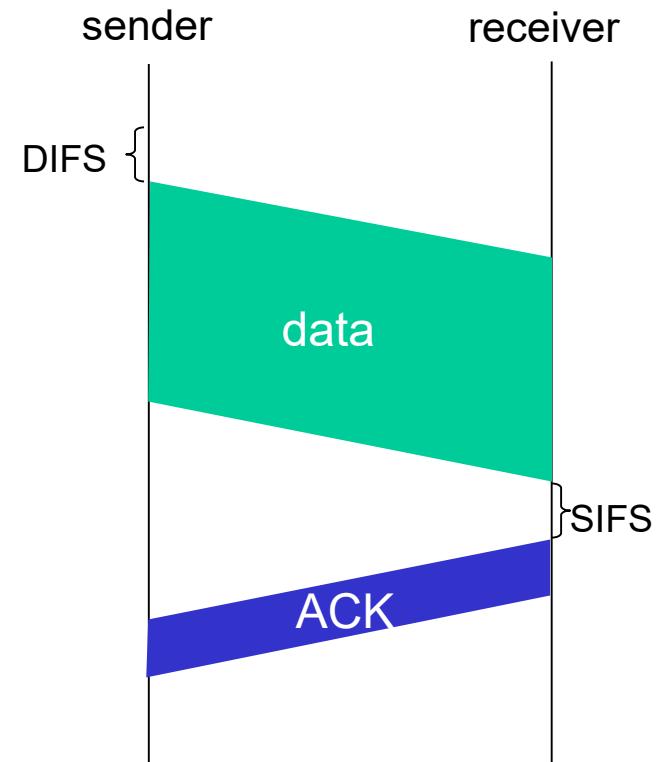


IEEE 802.11 WLANs

Bestätigungen auf Schicht 2 (Link Layer ACKs)

Vereinfachter Ablauf

1. Sender wartet eine vom Standard vorgegebene Zeitspanne (DIFS) in der das Medium frei sein muss
2. Sender überträgt kompletten Rahmen (keine CD)
3. Empfänger prüft empfangenen Rahmen mit Hilfe des CRC
4. Empfänger sendet ACK, falls Rahmen korrekt empfangen wurde



Quelle: [1], Seite 559

IEEE 802.11 WLANs

Medienzugriff

Verfahren basiert auf zwei unterschiedlichen Zeitspannen

Short Interframe Spacing (SIFS)

- Sehr kurzer zeitlicher Abstand zwischen einem Datenframe und dem zugehörigen ACK
- Durch kurze Dauer kann kein normaler Frame vorher gesendet werden.

Distributed Coordination Function Interframe Spacing (DIFS)

- Längerer zeitlicher Abstand, der zwischen normalen Frames eingehalten werden muss.

Anmerkung: QoS Erweiterung 802.11e variiert DIFS je nach Datenklasse, d.h. höhere Prioritäten haben schnelleres Zugriffsrecht.



IEEE 802.11 WLANs

Medienzugriff

Verfahren:

Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)

Sender:

- Sender belauscht erst den Kanal (Carrier Sense)
 - Wenn frei für eine Zeit von einem DIFS: Zufällige Backoff-Zeit im aktuellen Contention Window würfeln, nach Ablauf Frame übertragen
 - Wenn busy:
 - Warten bis Kanal frei (\rightarrow Network Allocation Vector, NAV), Wann immer der Kanal länger als DIFS frei ist (idle), zähle den Backoff-Timer runter
 - Bei Auslaufen des Backoff-Timers: Frame übertragen
- Falls kein ACK erfolgt: Backoff-Intervall verdoppeln (binary exponential backoff, wie von Ethernet bekannt), erneut versuchen

Empfänger:

- Bei Empfang eines korrekten Frames: sende ACK nach SIFS

IEEE 802.11 WLANs

Ansätze zu Kollisionsvermeidung

Problem:

- Senden eines Datenrahmens dauert lange
- eine Kollision wird vom Sender beim Senden nicht erkannt
- ➔ hoher Zeitverlust im Falle einer Kollision
- ➔ muss möglichst vermieden werden

Ansätze:

1. Im Gegensatz zu CSMA/CD sendet Station bei belegtem Kanal nicht sofort wenn Kanal länger als Inter-Frame Spacing (IFS) wieder frei wird sondern erst **nach DIFS und zufälligem Backoff**
➔ wartet mehr als eine Station startet meist eine zu erst
ABER: hilft nicht bei Hidden Terminal
2. Kann Kollision nicht vermieden werden, dann **besser eine Kollision bei kurzen Kontrollpaketen als bei langen Datenpaketen**
➔ Request-To-Send/Clear-To-Send (RTS/CTS) Verfahren

IEEE 802.11 WLANs

RTS/CTS Verfahren (1/2)

Idee:

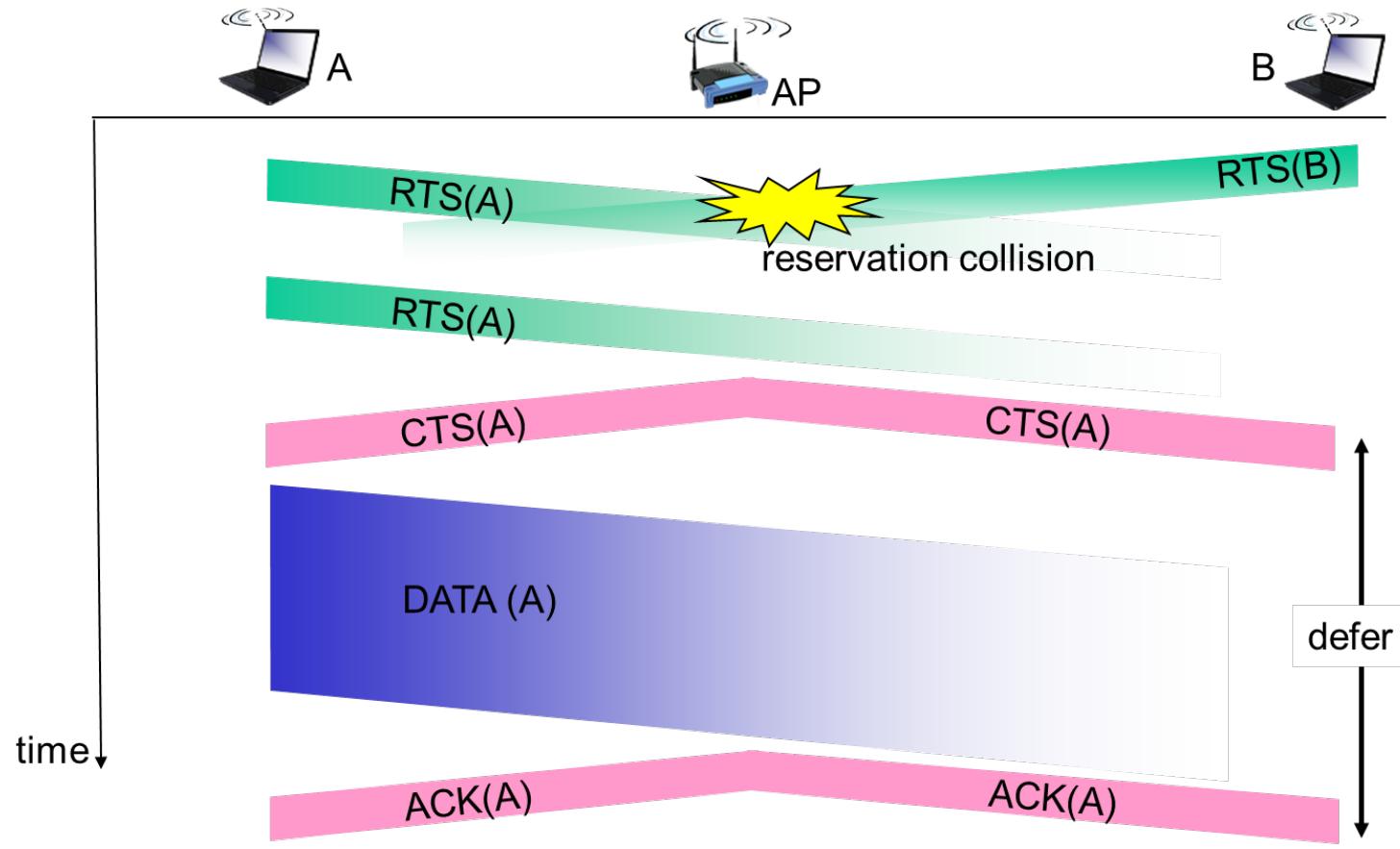
Kurze **Kontrollpakete zur Reservierung** des Kanals
→ Vermeidung von Kollisionen bei langen Datenpaketen

Ablauf:

1. Sender sendet erst kurzes Request-To-Send Paket (RTS) um den Kanal zu reservieren
 - Kollisionen können dabei auftreten sind aber weniger „schlimm“ als bei Datenpaketen (da kurzes RTS-Paket)
 2. Empfänger antwortet mit Clear-To-Send Paket (CTS)
 3. Andere Stationen empfangen RTS/CTS ebenfalls
→ berücksichtigen dass Kanal belegt ist
 4. Sender sendet Datenpaket
- Kollision von Datenpaketen kann vermieden werden
→ Funktioniert auch bei Hidden Terminal da dieses CTS empfängt

IEEE 802.11 WLANs

RTS/CTS Verfahren (2/2)

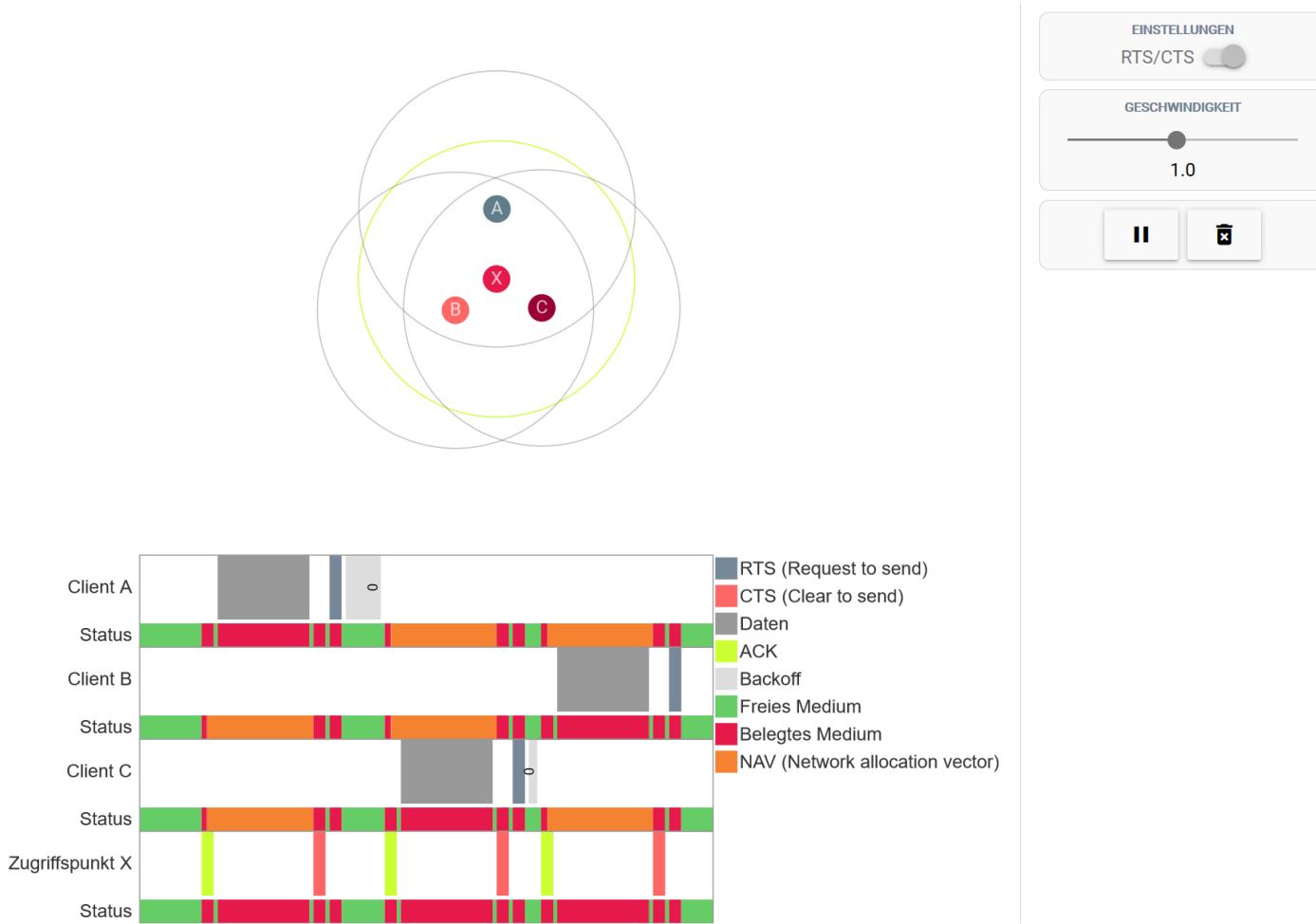


Quelle: [1], Seite 562

CSMA/CA bei IEEE 802.11

Animation: 3 Teilnehmer (keine Hidden Terminals)

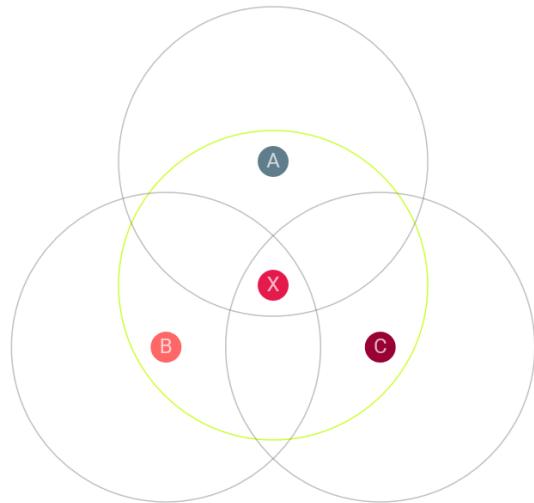
<https://www.sam.cs.hm.edu/#/animation/hidden-node-problem>



CSMA/CA bei IEEE 802.11

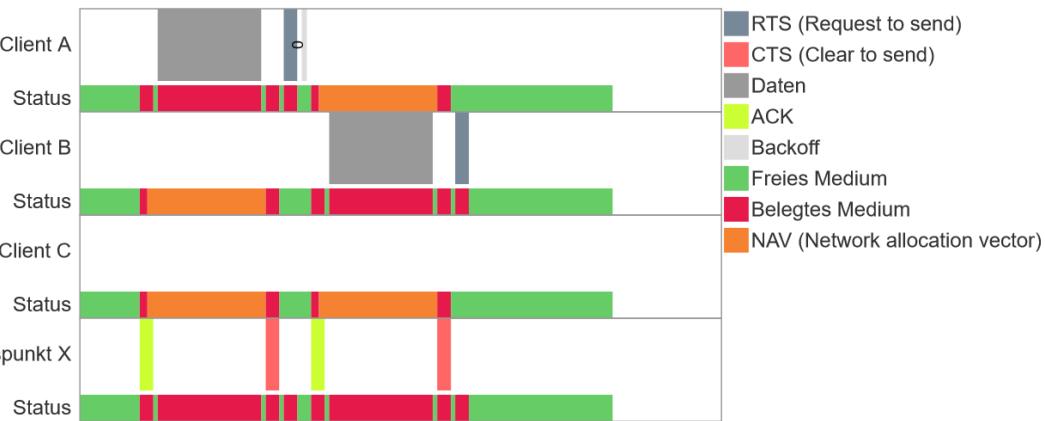
Animation: 3 Teilnehmer (Hidden Terminals)

<https://www.sam.cs.hm.edu/#/animation/hidden-node-problem>



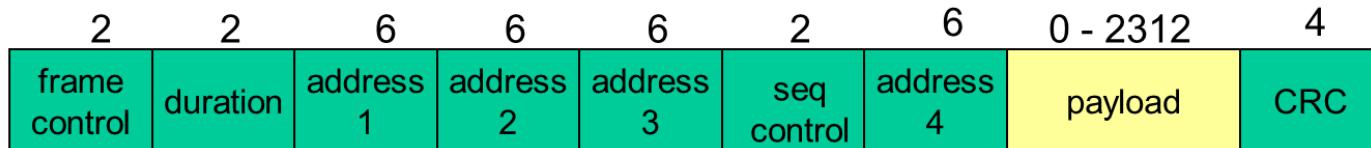
EINSTELLUNGEN
RTS/CTS

GESCHWINDIGKEIT
1.0



IEEE 802.11 WLANs

Rahmenformat



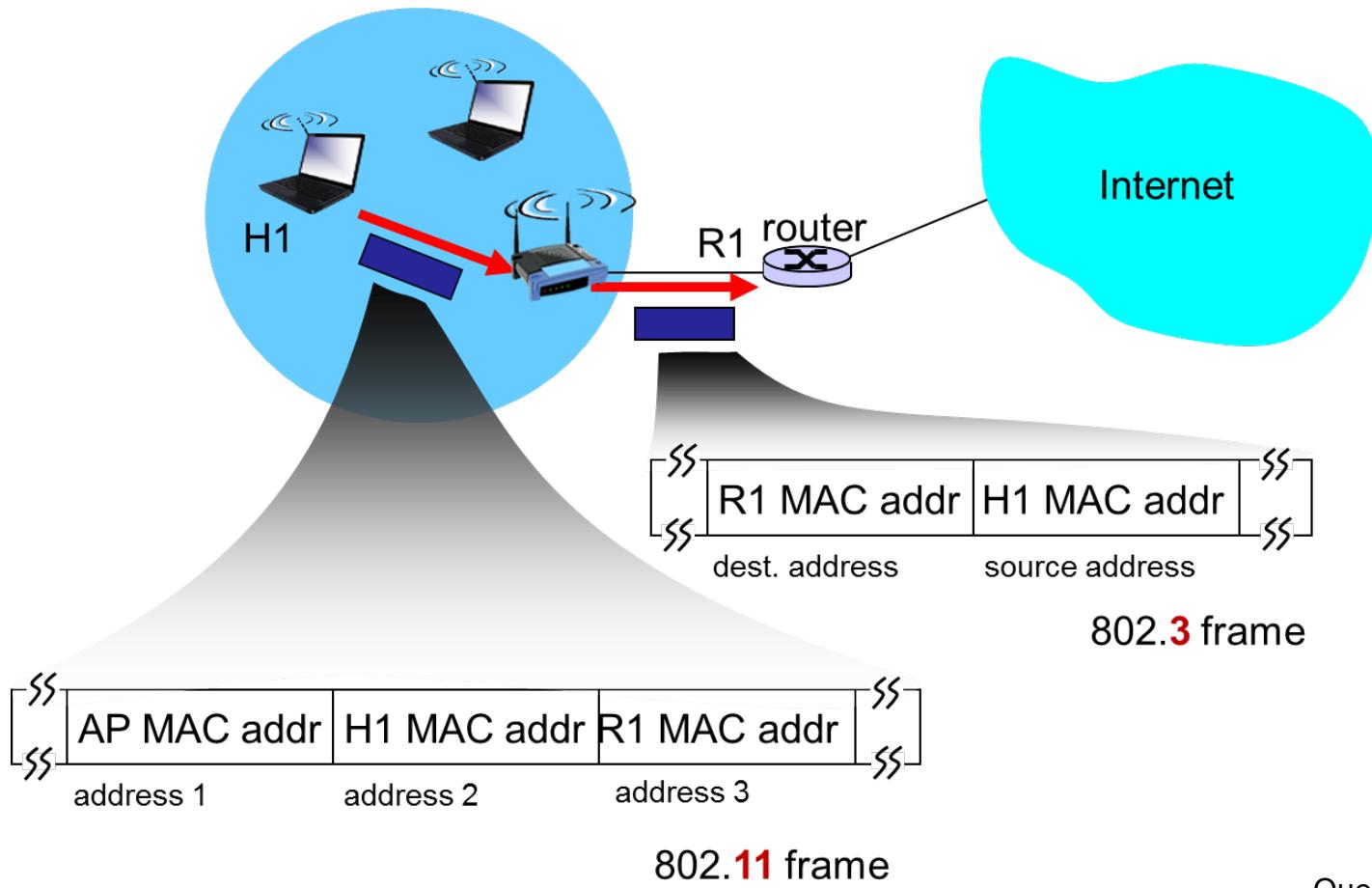
- Maximal 2312 Bytes an Nutzdaten (payload, typisch: < 1500 Bytes)
- Dritte Adresse erlaubt die Umsetzung des Rahmens auf einen Ethernet-Rahmen mit der passenden Zieladresse

Bedeutung der Adressfelder variiert je nach Funktion, angezeigt über ToDS, FromDS Bits (DS: Distribution System) in Frame Control:

Funktion	ToDS	FromDS	Add. 1	Add. 2	Add. 3	Add. 4
IBSS	0	0	destination	source	BSSID	unused
To AP	1	0	BSSID	source	destination	unused
From AP	0	1	destination	BSSID	source	Unused
WDS (bridge)	1	1	receiver	transmitter	destination	source

IEEE 802.11 WLANs

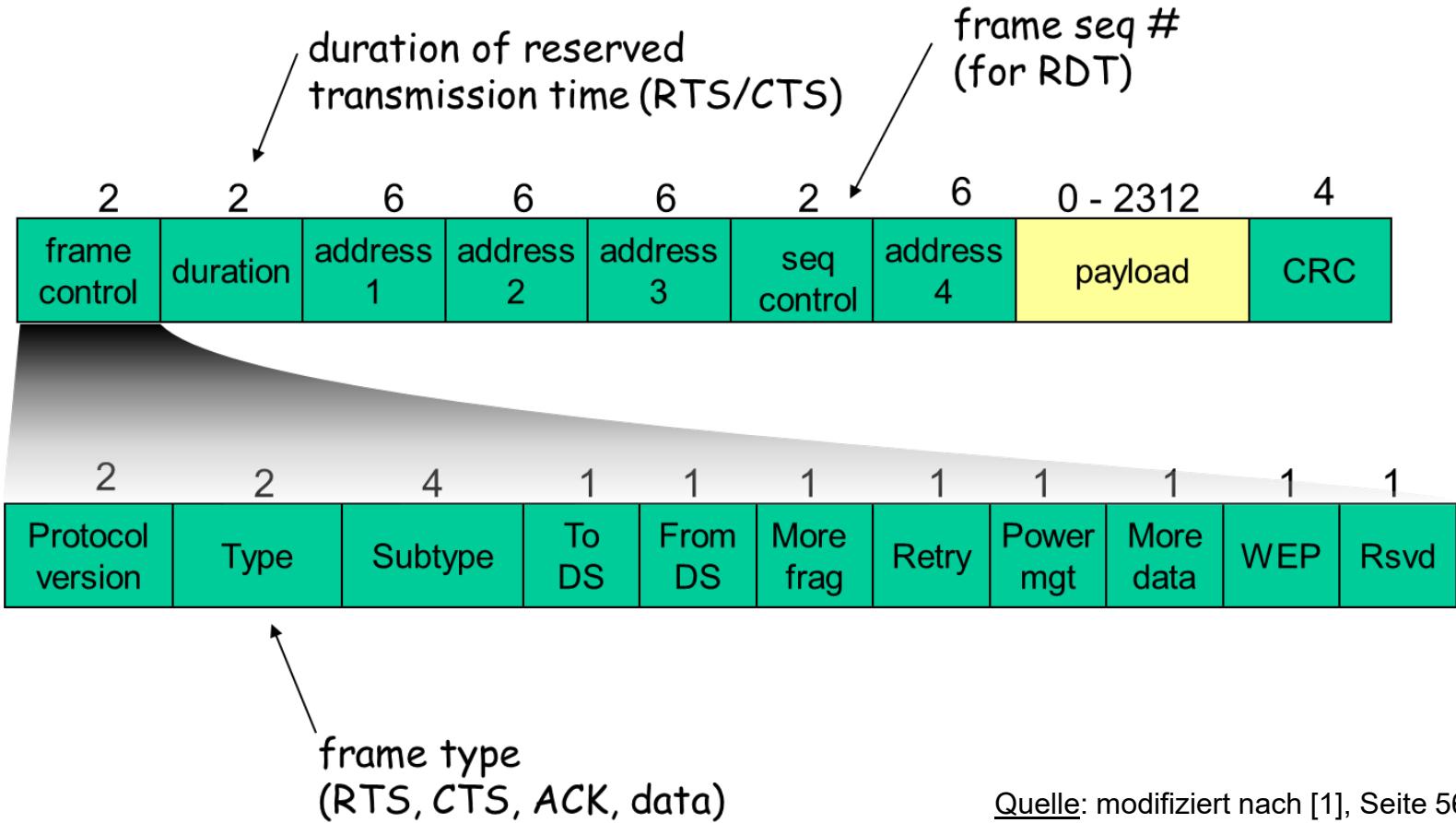
Rahmenformat - Beispiel



Quelle: [1], Seite 565

IEEE 802.11 WLANs

Rahmenformat: Aufbau Frame Control (2 Byte)



Quelle: modifiziert nach [1], Seite 564

IEEE 802.11 WLANs

Vergrößerung der Reichweite (Coverage)

Problem:

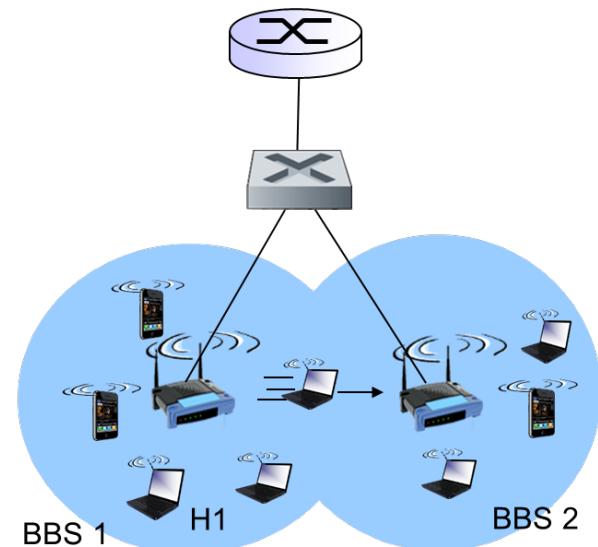
Regulierung begrenzt Sendeleistung im ISM Band auf 100mW (EIRP)
→ Reichweite je nach Umgebung auf wenige Meter begrenzt

Lösungsansatz: Mehrere überlappende BSSs in einem IP Subnetz

- IP Adresse bleibt erhalten
(da selbes IP Subnetz)
- Station H1 wechselt von AP 1 zu AP 2

Woher erfährt Switch den aktuell zuständigen Access Point?

- Selbstlernender Switch merkt sich auf welchen Port er den letzten Rahmen von H1 gesehen hat



Wiederholung: CSMA/CA

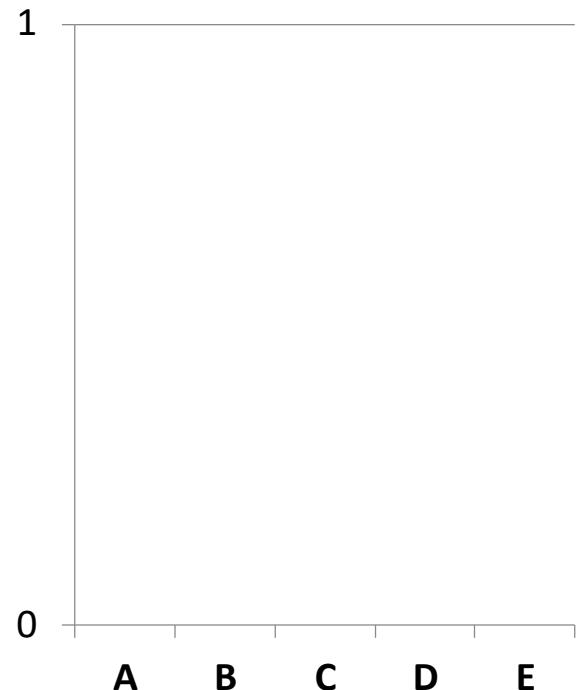
Vergleichen Sie CSMA/CA und CSMA/CD:

Welche Unterschiede gibt es?

Der Ablauf von CSMA/CA bei WLANs nach IEEE 802.11 unterscheidet sich vom CSMA/CD bei drahtgebundenem Ethernet

- A) gar nicht
- B) In einem Punkt
- C) In zwei Punkten
- D) In drei Punkten
- E) In mehr als drei Punkten

ID = wischhof@hm.edu
Umfrage noch nicht gestartet



Umfrage starten

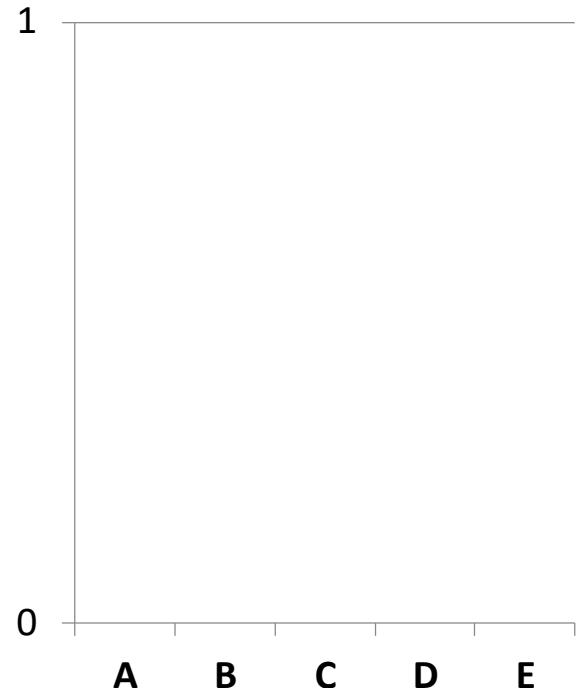
WLAN Reichweite und Datenrate

Kunden beschweren sich beim Betreiber eines WLANs, dass die erzielte Übertragungsrate zu gering sei.

Was sollte er tun?

- A) Andere Kanäle einstellen
- B) Sendeleistung der APs erhöhen
- C) Sendeleistung der APs verringern
- D) Mehr APs aufstellen und Sendeleistung verringern
- E) Mehr APs aufstellen und Sendeleistung erhöhen

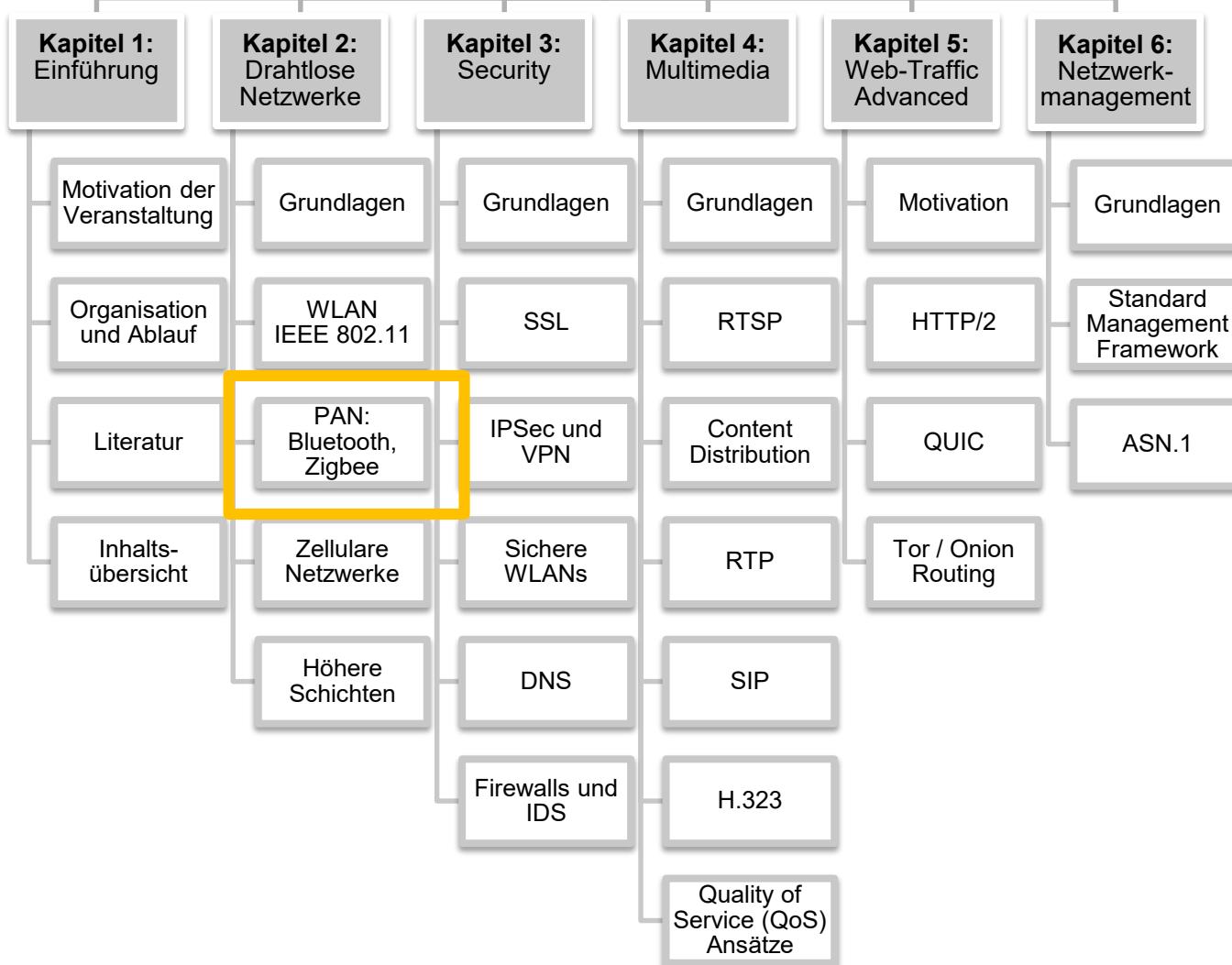
ID = wischhof@hm.edu
Umfrage noch nicht
gestartet



Umfrage starten



Netzwerke II



Personal Area Networks

Einführung

- (Ad Hoc) Netzwerk aufgebaut von Kleingeräten in der näheren Umgebung (z.B. Smartphone zu Headset, Smartphone zu Navi)
- Drahtlos oder drahtgebunden
- Reichweite oft nur wenige Meter

Typische drahtlose Standards

- Bluetooth (IEEE 802.15.1)
- Zigbee (basierend auf IEEE 802.15.4)



Bluetooth (IEEE 802.15.1)

Überblick



Ziele

- Geringer Stromverbrauch/Sendeleistung → kleine Reichweite
- Geringe Kosten

Eigenschaften

- Frequenzband: 2,4 GHz ISM Band
- 79 Kanäle, jeweils 1 MHz breit
- Modulation: Gaussian FSK
- Mehrfachzugriff mit TDMA, Länge der Zeitslots 625 µs
- Frequenzsprungverfahren (Frequency Hopping Spread Spectrum, FHSS) mit 1600 hops/s: wählt anderen Kanal nach jedem Zeitslot, pseudo-zufällige Sprungfolge → Robustheit gegen Störer





Bluetooth (IEEE 802.15.1)

Geräteklassen, Versionen

Klasse	Max. Leistung	Reichweite
Class 1	100 mW	ca. 100 m
Class 2	2,5 mW	ca. 10 m
Class 3	1 mW	ca. 1 m

Übersicht über die wichtigsten Bluetooth-Spezifikationen

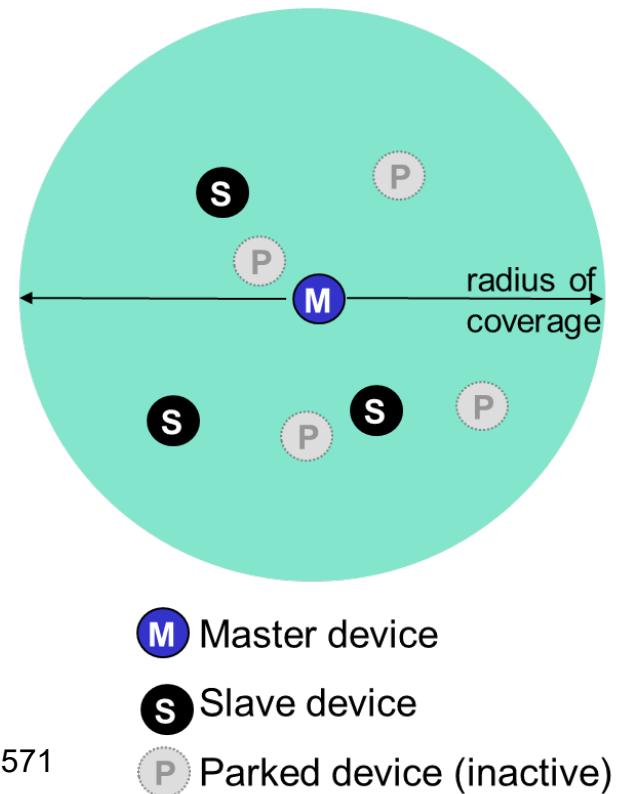
Version	Kommentare
1.0	Erschienen 1999, bis 732,2 kbit/s
1.2	2003, bis 1 Mbit/s
2.0	2004, bis 2,1 Mbit/s (Enhanced Data Rate, EDR)
2.1	2007, Secure Simple Pairing (SSP), Quality of Service (QoS)
3.0	2009, Bluetooth über WLAN (+HS) mit bis 24 Mbit/s
4.0	2010, Bluetooth Low Energy/Smart als zusätzlichen Stack
4.1	2013, Integration mit LTE, „Internet der Dinge“ (IoT)
4.2	2014, Erweiterung Bluetooth Low Energy/Smart, Sicherheit
5.0	2016, Verbesserte Reichweite, Datenrate, IoT Erweiterungen



Bluetooth (IEEE 802.15.1)

Netzstruktur: Piconet

- Ad Hoc Netzwerk → keine Infrastruktur
- Bis zu acht Geräte aktiv, bis zu 255 geparkte Geräte
- Ein Gerät wird zum Master bestimmt
 - Gibt Zeit vor
 - Gewährt Slaves das Recht zu senden
 - Aktiviert geparkte Slaves



Quelle: [1], Seite 571



Bluetooth (IEEE 802.15.1)

Kernspezifikation und Profile

Bluetooth Spezifikation zweigeteilt:

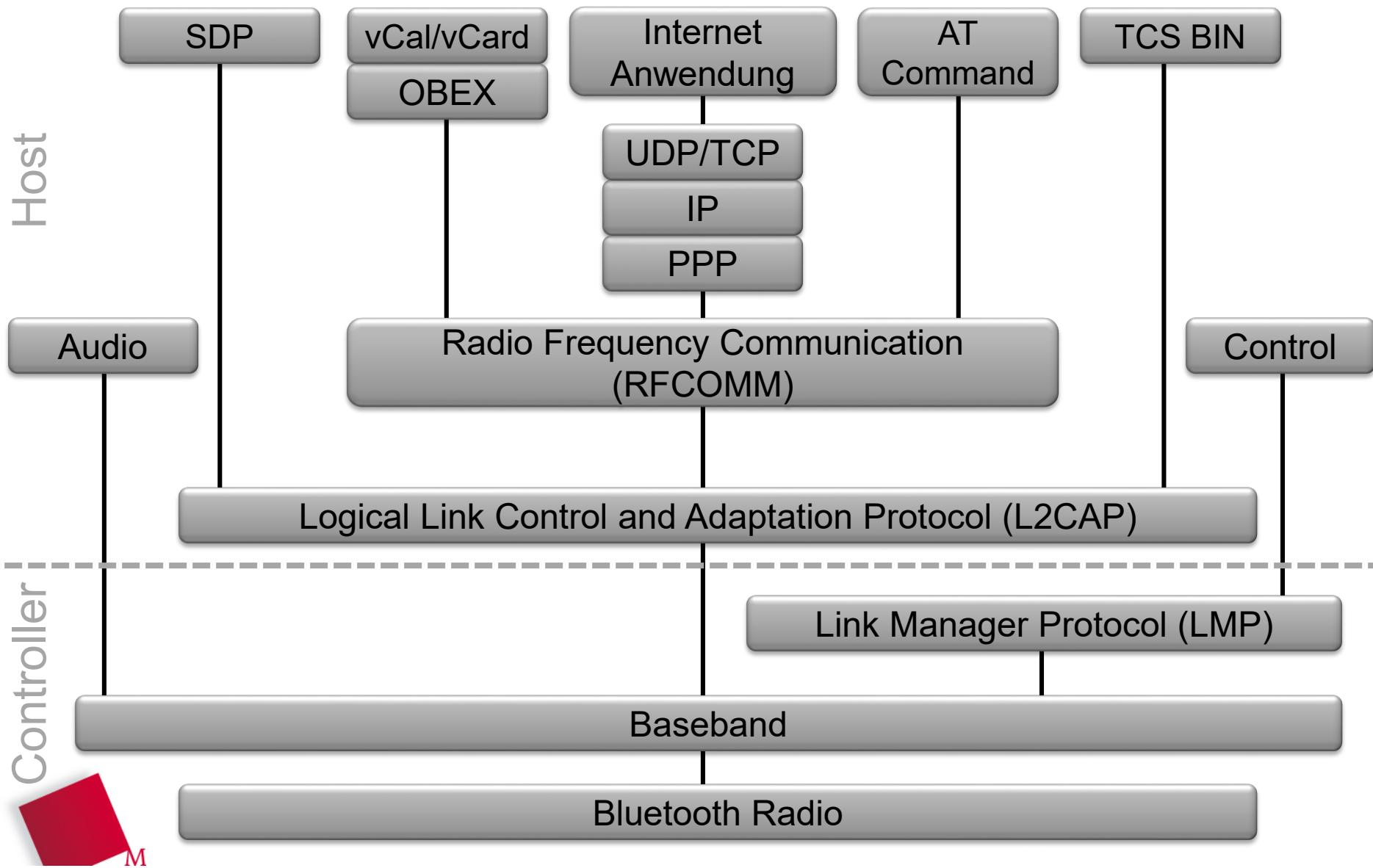
1. Kernspezifikation (Core)
2. Profile

Bluetooth Profil

- Profil spezifiziert die Anwendung von Bluetooth für einen bestimmten Zweck
- Beispiele
 - Serial Port Profile (SPP): serielle Datenübertragung
 - Hands Free Profile (HFP): Freisprechverbindung im Auto
 - Health Device Profile (HDP): Verbindung medizinischer Geräte
 - Dialup Networking Profile (DUN): Internet Einwahl
 - Advanced Audio Distribution Profile (A2DP): Musikwiedergabe
 - Object Exchange (OBEX): generischer Datenaustausch

Bluetooth (IEEE 802.15.1)

Protocol Stack



Bluetooth (IEEE 802.15.1)

Übersicht wichtiger Abkürzungen (1/2)

AT Kommando	AT tention – Kommandos zur Modemsteuerung, z.B. Anwahl, Abfrage Signallevel, etc.
Baseband	Basisband, Verbindungsaufbau im Piconet, Adressierung, Paketformate, Power Control
LMP	Link Manager Protocol , Aufbau eines Bluetooth-Links, Link Management (Authentifizierung, Verschlüsselung)
L2CAP	Logical Link Control and Adaptation Protocol , Adaptionsschicht zwischen Baseband und höheren Protokollschichten, bietet verbindungslose und verbindungsorientierte Dienste
OBEX	OBject EXchange Protocol , Austausch beliebiger Datenobjekte
PPP	Point-to-Point Protocol , für Verbindung zum Provider

Bluetooth (IEEE 802.15.1)

Übersicht wichtiger Abkürzungen (2/2)

RFCOMM	Radio Frequency COMMunications , Bereitstellung virtueller serieller Verbindungen, Emulation mehrerer serieller Ports (Kabelersatz), Basis z.B. für Serial Port Profile (SPP)
SDP	Service Discovery Protocol , zur selbstständigen Erkennung vorhandener Dienste
TCS BIN	Telephony Control Specification – BINary
vCal	virtual Calender – Austauschformat für Kalenderdaten
vCard	virtual Card – Austauschformat für virtuelle Visitenkarten

Bluetooth (IEEE 802.15.1)

Health Device Profile (HDP)

Problem

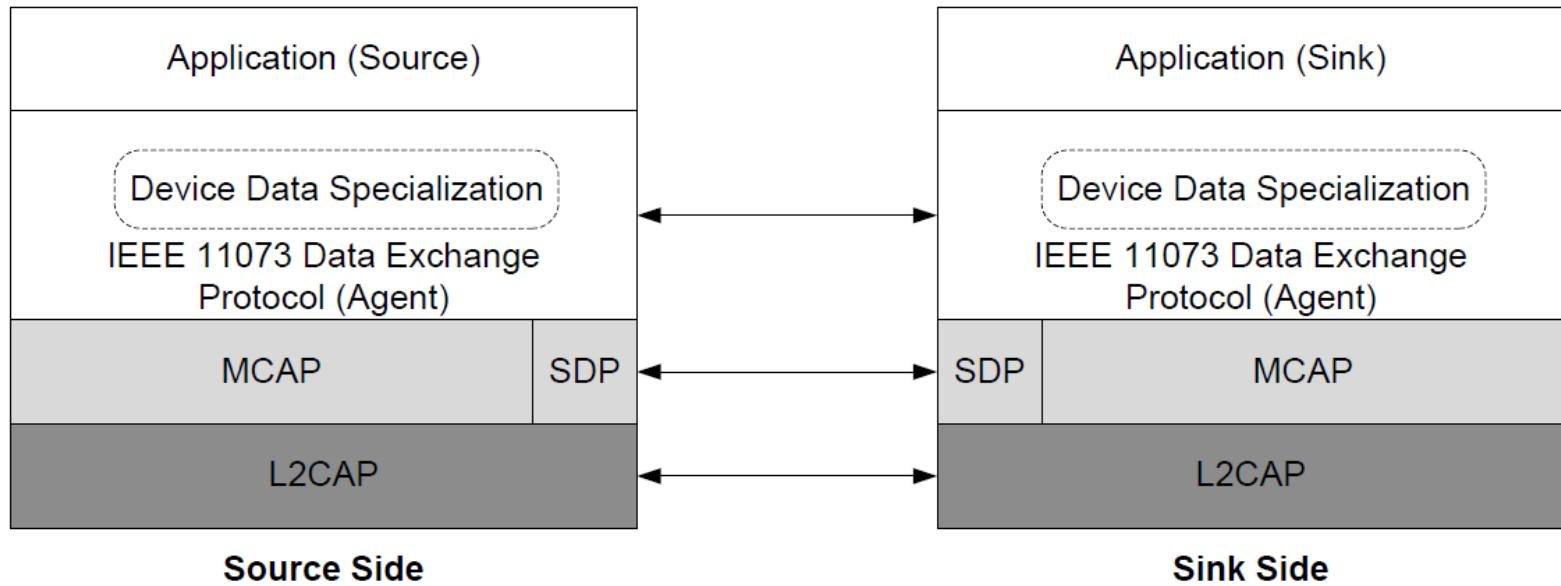
- Historisch viele Geräte/Sensoren auch im Gesundheitsbereich über Serial Port Profile (SPP) basierend auf RFCOMM angebunden
→ keine Interoperabilität!

Lösungsansatz

- Medical Working Group of Bluetooth Special Interest Group (SIG) verabschiedete im Juni 2008 das Health Device Profile (HDP)
→ Sicherung der Interoperabilität durch Standardisierung
- Zwei Rollen: Source (Datenquelle, z.B. Waage, Thermometer) und Sink (Datensenke, z.B. Smartphone)
- Kernfunktionen: Verbindungsauf-/abbau von Kontrollkanal und Datenkanälen (gesichert/streaming), Wiederaufbau abgebrochener Verbindungen, Synchronisation der Uhren

Bluetooth (IEEE 802.15.1)

Protocol Stack for HDP



Erläuterungen:

MCAP

Multi-Channel Adaptation Protocol, stellt einen Kontrollkanal (MCL) und mehrere Datenkanäle (MDL) bereit

IEEE 11073

Protokoll zum Austausch der Vitaldaten (IEEE 11073-20601)



Bluetooth (IEEE 802.15.1)

Bluetooth 4.0 / Bluetooth Smart



- Sensoren (z.B. Pulsmesser, Thermometer) sollen lange Laufzeit (→geringen Stromverbrauch) aufweisen, bisher oft über proprietäre Protokolle wie ANT+ (von Garmin) angebunden
- Bluetooth ab Version 4.0 beinhaltet „Bluetooth Smart“: Low Energy Profil extra für Anwendungsbereiche wie Fitness/Sport, etc.
 - Ab Android 4.3 (Jelly Bean) von Smartphones unterstützt
 - Sensoren (z.B. Pulsmesser) bereits ab ca. 30€ für Endkunden
- Basis ist Generic Attribute Profile (GATT)
<https://developer.bluetooth.org/gatt/profiles/Pages/ProfilesHome.aspx>



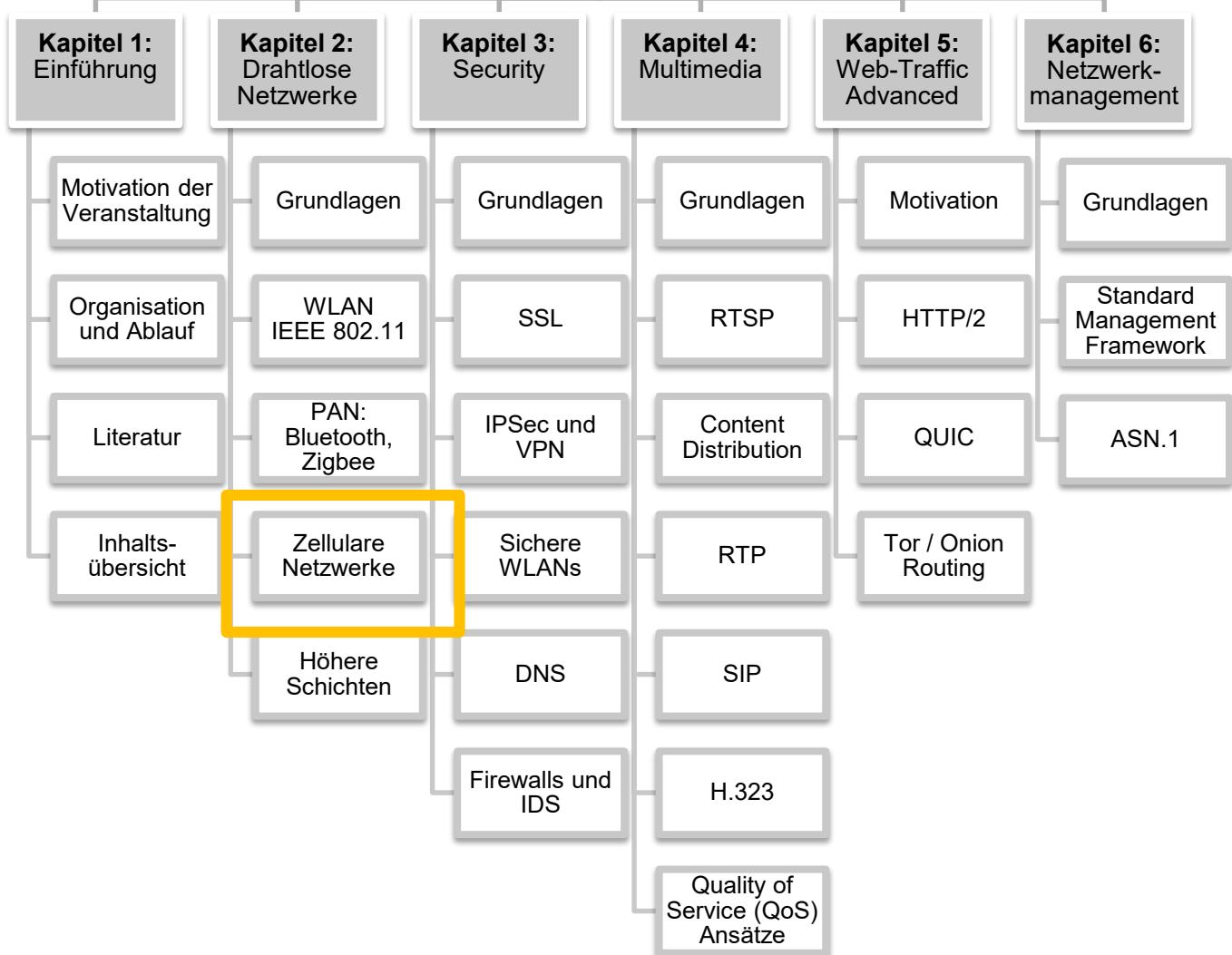
ZigBee

Überblick

- Basiert auf IEEE 802.15.4
- Getrieben von ZigBee Alliance (<http://zigbee.org/>)
- Zielsetzung: drahtlose Datenübertragung bei geringem Stromverbrauch
 - geringe Datenrate (20-250 kbit/s)
 - selten aktiv (low duty-cycle)
- Typische Anwendungsfälle
 - Übertragung von Sensordaten/Überwachung von Gütern
 - Heim- und Gebäudeautomatisierung
- Gerätearten
 1. **Endgerät** (Reduced Function Device, RFD), implementiert nur einen Teil der ZigBee Protokolle, geringe Komplexität/Kosten
 2. **Router** (Full Function Device, FFD), kann Daten weiterleiten
 3. **Koordinator** gibt zusätzlich Parameter vor, koordiniert dieses PAN



Netzwerke II



Zellulare Netzwerke

Einführung und Motivation

Problem: geringe Reichweite eines WLAN APs
→ flächendeckender Internet-Zugang kaum realisierbar

Lösung: Für Mobiltelefonie bereits flächendeckendes drahtloses Netzwerk vorhanden → nutzbar auch für mobilen Internetzugang

Fokus im Folgenden: **Überblick über zellulare Netzarchitektur**

Hinweis: Gründliche Behandlung dieses komplexen Themas in einer eigenen Lehrveranstaltung: „Mobile Netze“ (Master Informatik)



Mobilfunk

Überblick über die technische Entwicklung

- **1. Generation Mobilfunk (1G):**
analog (A-Netz, B-Netz, C-Netz)
- **2. Generation Mobilfunk (2G):**
GSM (digital), ab ca. 1992
 - Erweiterung um paketbasierte Daten mit GPRS (2.5G)
 - Effizientere Modulationsverfahren für Daten: EDGE (2.75G)
- **3. Generation Mobilfunk (3G):**
UMTS, ab ca. 2003
 - Höhere Datenübertragungsraten mit HSPA (3.5G)
 - Höhere Datenübertragungsraten durch OFDM, Übergang zu Netzen der 4. Generation mit LTE (3.9G)
- **4. Generation Mobilfunk (4G):**
LTE Advanced, ab ca. 2014 (abwärtskompatibel zu LTE)
- **5. Generation Mobilfunk (5G):**
ab ca. 2021, Ziel: Skalierbarkeit (→ IoT), Latenz < 1ms

Global System for Mobile Communication (GSM)

Einführung: GSM Überblick als Film



Global System for Mobile Communication (GSM)

Standards

- International Telecommunication Union (ITU)
u.a.: Signalling System #7 (SS-7)
- European Telecommunication Standards Institute (ETSI)
ETSI GSM Standards: Technical Specifications (TS)

Internationalisierung von GSM:

- 3rd Generation Partnership Project (3GPP)

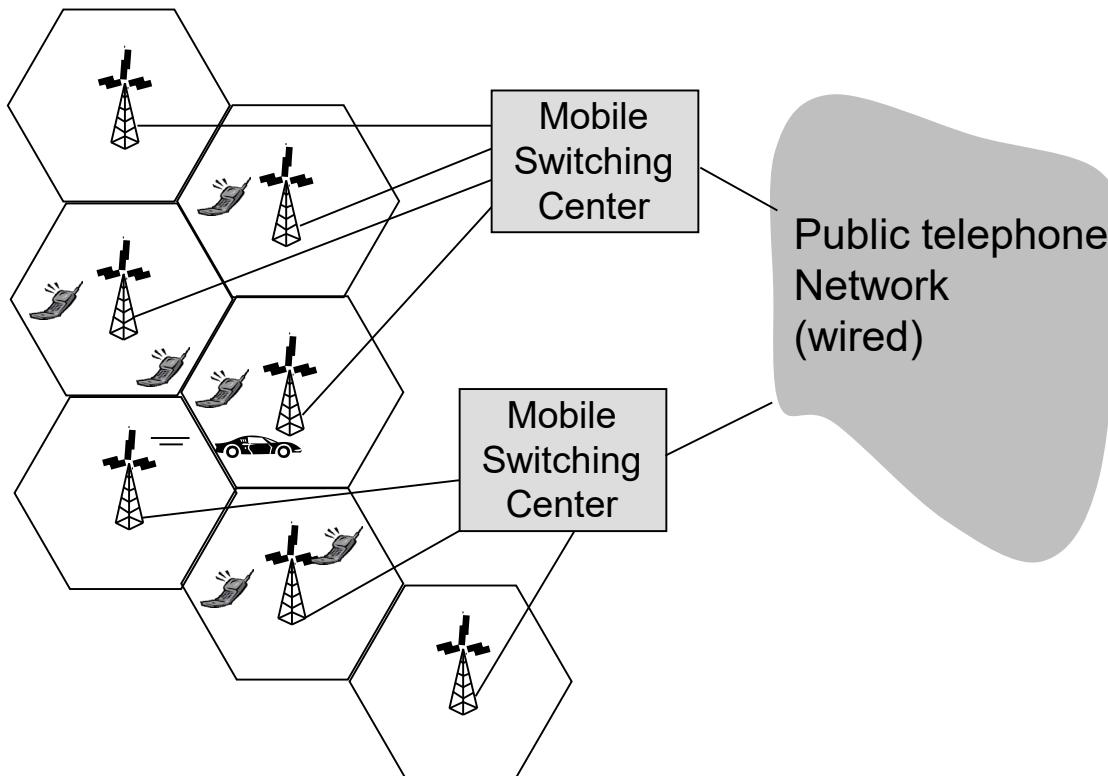
Spezifikationen können (kostenlos!) abgerufen werden:

<http://www.3gpp.org>
<ftp://ftp.3gpp.org>



Zellulare Netzwerke

Zellulare Netzwerkarchitektur



Quelle: [1], Seite 575

Mobilfunkzelle

Von einer Base Transceiver Station (BTS) abgedeckter Bereich

Air-Interface

Untere zwei Netzwerkprotokoll-schichten zwischen Mobile Station (MS) und BTS

Mobile Switching Center (MSC)

Anrufauf-/abbau,
Verbindung ins Festnetz
Mobilitätsmanagement
(dazu später mehr)

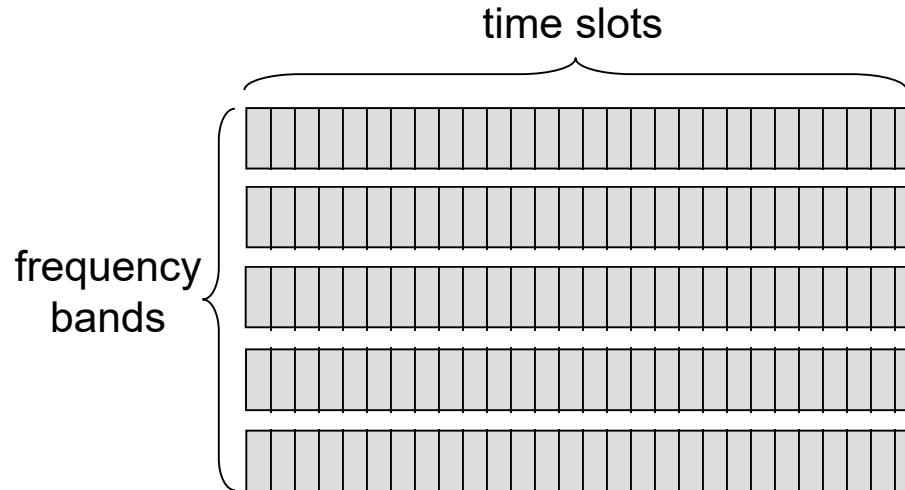


Zellulare Netzwerke

Ressourcenzuteilung in der Zelle

Variante 1: Kombination von FDMA und TDMA (GSM)

- Verfügbares Spektrum wird in einzelne Frequenzkanäle aufgeteilt
- Jeder Frequenzkanal wird wiederum in einzelne Zeitschlüsse geteilt



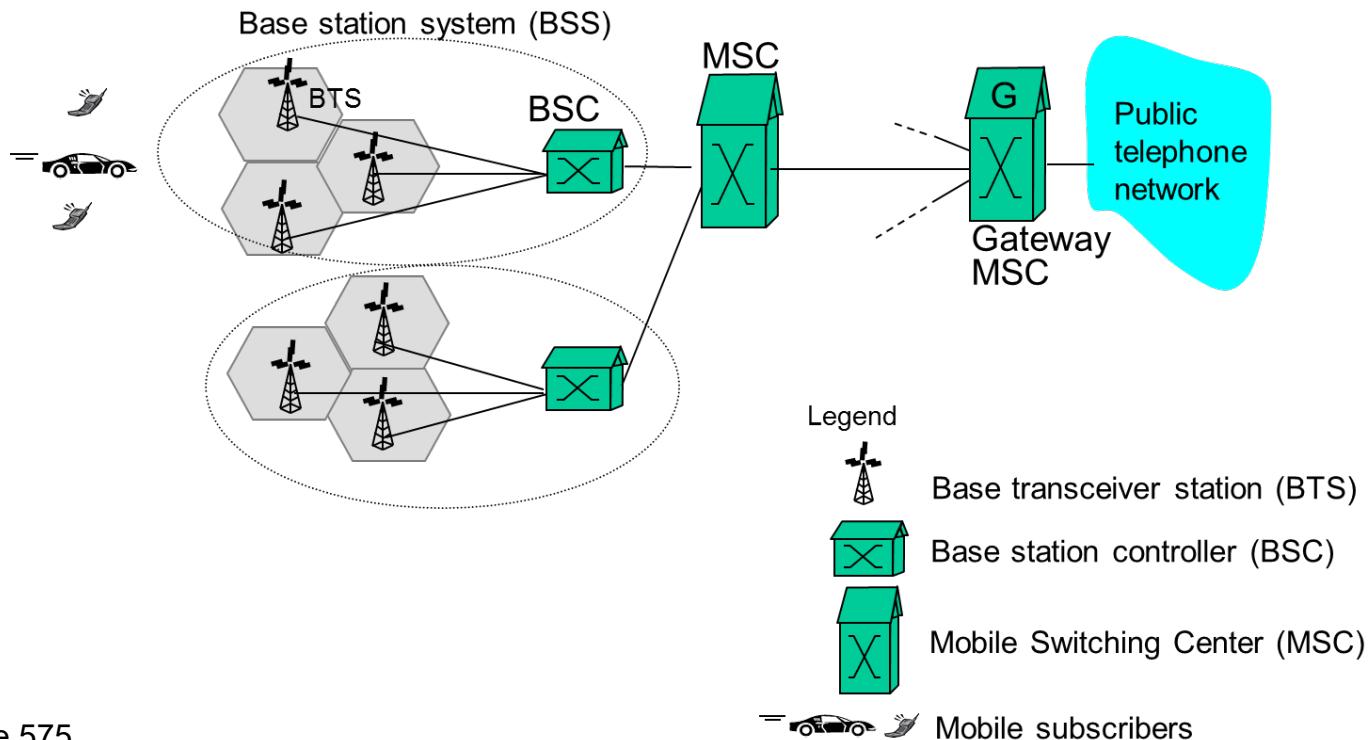
Variante 2: CDMA Verfahren (2G in USA, Asien, UMTS)

- Zuordnung unterschiedlicher Codes zu unterschiedlichen Nutzern

Zellulare Netzwerke

2G Netzarchitektur (Sprache, leitungsvermittelte Daten)

- Base Station Controller (BSC) übernimmt Ressourcenzuweisung und Mobilitätsmanagement in einem Base Station Subsystem (BSS)

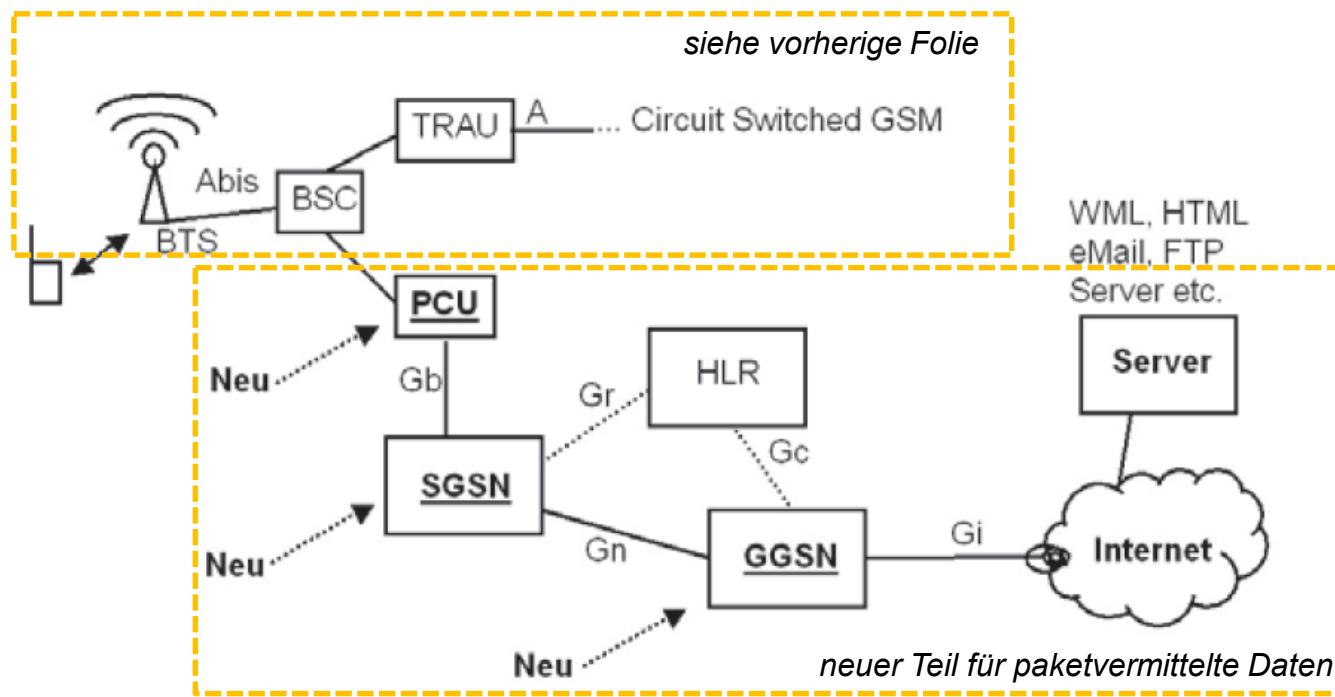


Quelle: [1], Seite 575

Zellulare Netzwerke

2G Netzarchitektur (Sprache, paketvermittelte Daten)

- Mit GPRS erstmals paketvermittelte Datendienste
→ paralleles Datennetzwerke, welches BTS mitbenutzt (Kostenersparnis!)



Packet Control Unit (PCU)
Verteilung von Ressourcen (timeslots)

Serving GPRS Support Node (SGSN)
Zustellung von Paketen im Bereich eines BSC (Pendant zu MSC)

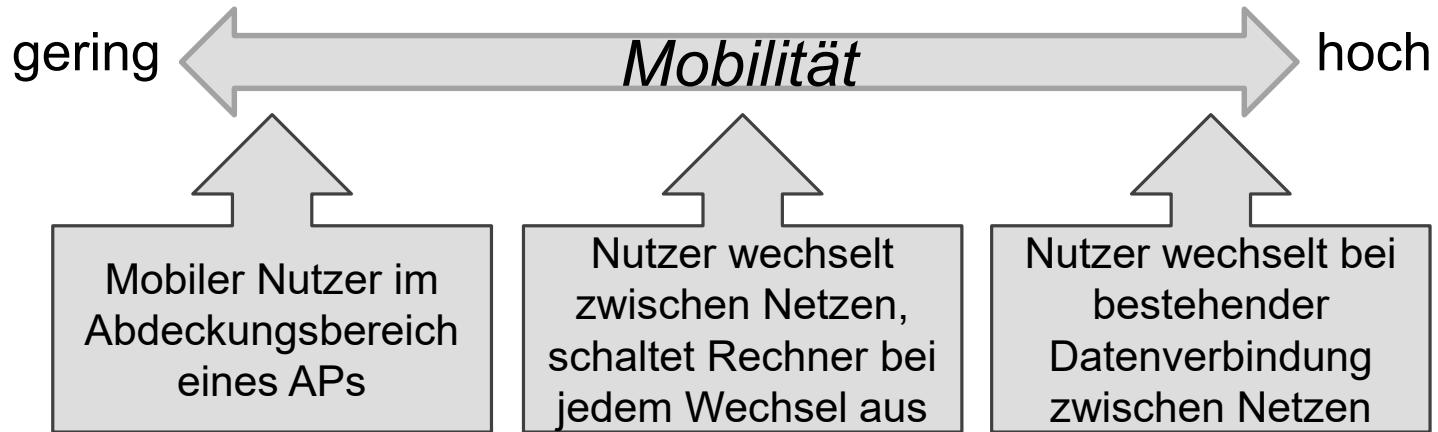
Gateway GPRS Support Node (GGSN)
Weiterleitung ins Internet

Quelle: [4], S. 117

Zellulare Netzwerke

Mobilitätsmanagement - Einführung

Wie mobil ist ein Nutzer (aus Sicht der Netzwerkschicht)?



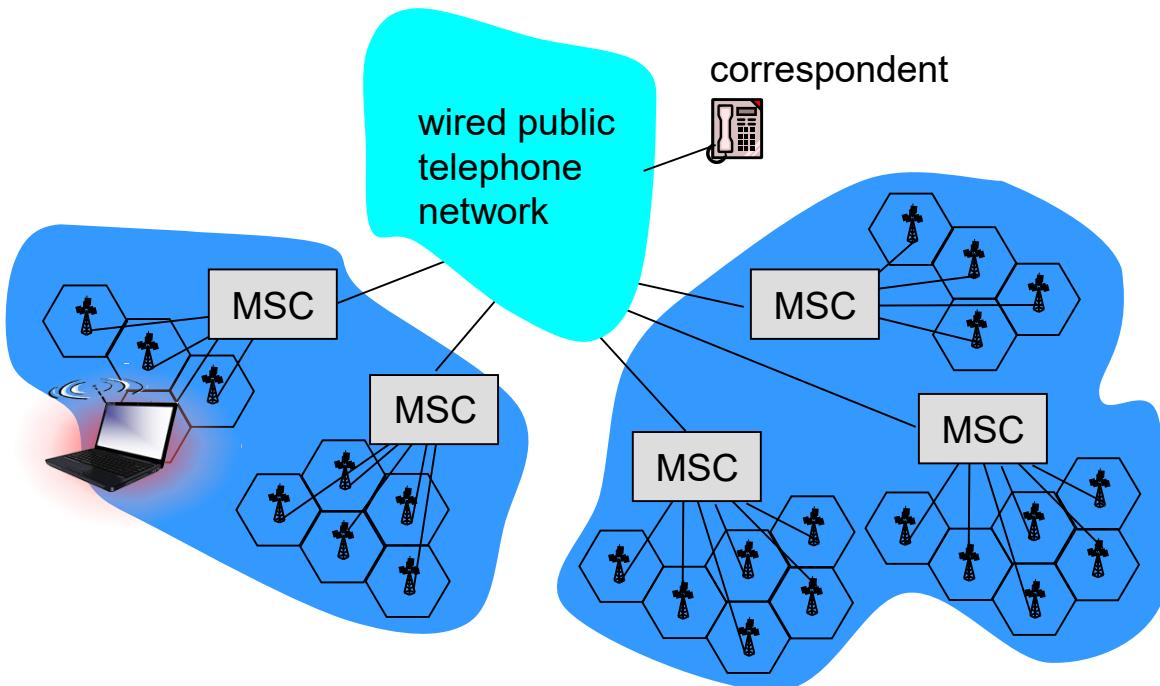
Fragen:

- Muss der Nutzer seine IP-Adresse beibehalten?
- Welche Netzwerkinfrastruktur wird benötigt?

Zellulare Netzwerke

Mobilitätsmanagement

Nutzer kann sich zwischen Zellen verschiedener Mobile Switching Center (MSC) – auch unterschiedlicher Provider – bewegen:



Quelle: modifiziert nach [1], Seite 595

Zellulare Netzwerke

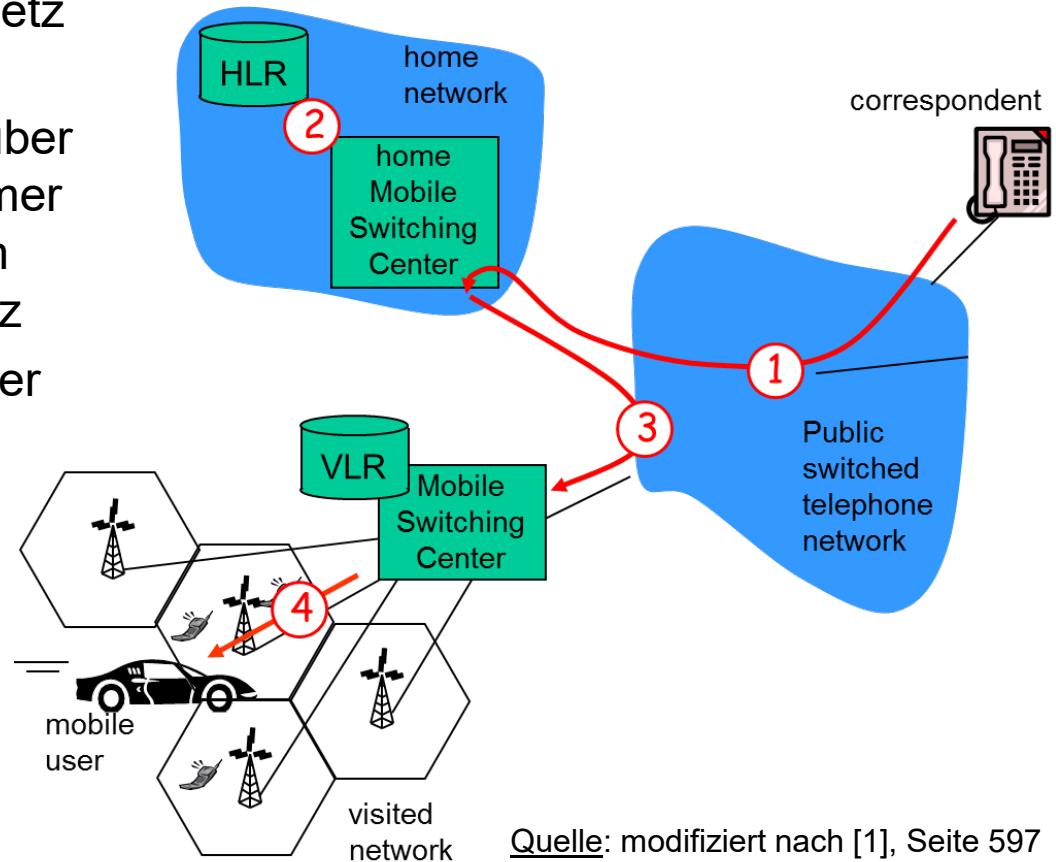
Mobilitätsmanagement: Konzept bei GSM

- Provider des Teilnehmers (Heimatnetz) hat **Home Location Register (HLR)**
 - Datenbank mit Informationen zum Nutzer, dessen Rufnummer/IMSI sowie dessen zuletzt bekanntem Aufenthaltsort
 - Besuchtes Netzwerk hat **Visitor Location Register (VLR)**
 - Datenbank mit Informationen zu allen Nutzern, die sich aktuell im vom MSC bedienten Bereich befinden (Kopie aus HLR)
 - Wird Teilnehmer angerufen, so wird zunächst HLR nach aktuellem Ort befragt. Dann wird Anruf über VLR/MSC im besuchten Netz aufgebaut
 - Falls gerade keine Verbindung zum Nutzer besteht: Broadcast Nachricht über alle Basisstationen im Bereich der MSC („Paging“)
- Indirektes Routing

Zellulare Netzwerke

Mobilitätsmanagement: Ablaufbeispiel

1. Anruf trifft im Heimatnetz des Nutzers ein
2. Heimat-MSC erfährt über HLR temporäre Nummer (Roaming Number) im aktuell besuchten Netz
3. Anruf wird zu besuchter MSC weitergeleitet
4. Teilnehmer wird gerufen, ggf. wird vorher noch ein Paging durchgeführt



Zellulare Netzwerke

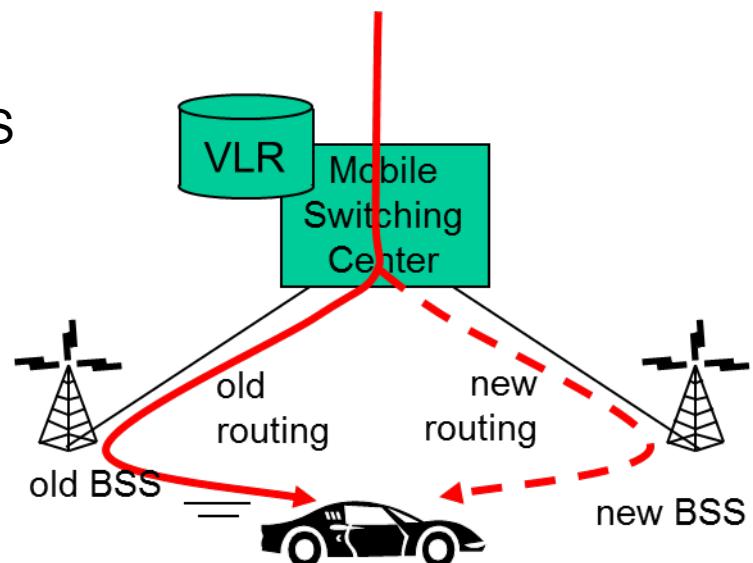
GSM: Handover (gleiche MSC/Inter-BSC Handover)

Handover:

Mobilgerät wechselt **bei bestehender Verbindung** von einer Basisstation zu einer anderen

Mögliche Ursachen

- Bewegung des Nutzers
→ stärkeres Signal von anderer BSS
- Aktuelle Zelle ist überlastet

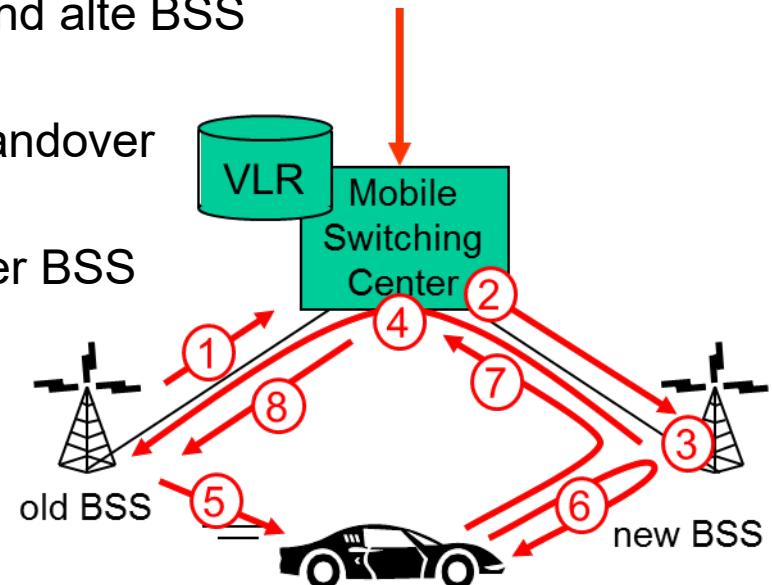


Quelle: [1], Seite 599

Zellulare Netzwerke

GSM: Inter-BSC Handover – vereinfachter Ablauf

1. Altes BSS informiert MSC über anstehendes Handover
2. MSC reserviert Ressourcen zu neuer BSS
3. Neue BSS reserviert Zeitslot
4. Neue BSS signalisiert an MSC und alte BSS Bereitschaft zum Handover
5. Alte BSS weist Mobilgerät an, Handover zu neuer BSS durchzuführen
6. Mobilgerät aktiviert Kanal in neuer BSS
7. Mobilgerät bestätigt Handover an MSC, diese leitet Daten um
8. MSC weist alte BSS an, Ressourcen des Mobilgeräts freizugeben



Quelle: [1], Seite 600

Zellulare Netze

Handover (siehe [4] und [3GPP TS 23.009](#))

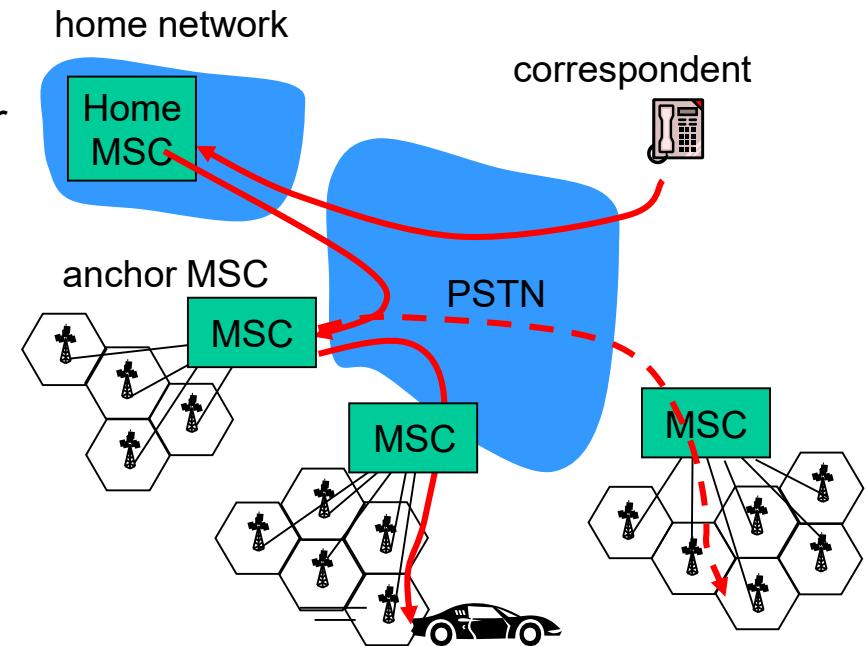
Unterscheidung von

- **Intra BSC Handover**
Aktuelle und neue Zelle gehören zum selben BSC
- **Inter BSC Handover**
Aktuelle und neue Zelle gehören zu unterschiedlichen BSC (sind aber dem gleichen MSC zugeordnet)
- **Inter MSC Handover**
Aktuelle und neue Zelle sind unterschiedlichen MSC zugeordnet
- **Subsequent Inter MSC Handover**
Teilnehmer wechselt nach Inter MSC Handover in Zelle eines dritten MSC
- **Subsequent Handback**
Teilnehmer wechselt nach Inter MSC Handover wieder zurück in das Gebiet der ersten MSC

Zellulare Netzwerke

GSM: Inter-MSC Handover – vereinfachter Ablauf

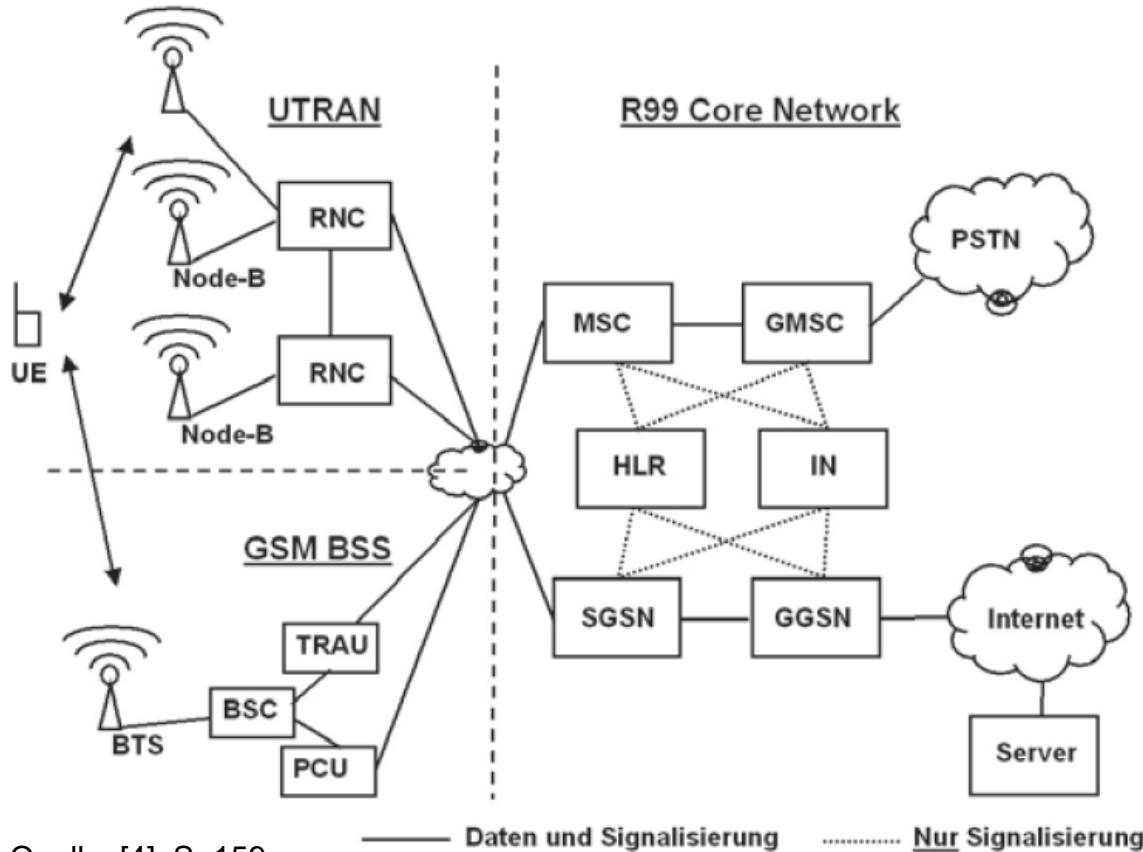
- **Anker-MSC** (Anchor MSC)
erste MSC während eines Anrufs
- Daten/Anruf wird zunächst an Anker-MSC geleitet
- Dann Weiterleitung zu aktueller MSC



Quelle: [1], Seite 600

Zellulare Netzwerke

3G Netzarchitektur (Sprache, paketvermittelte Daten)



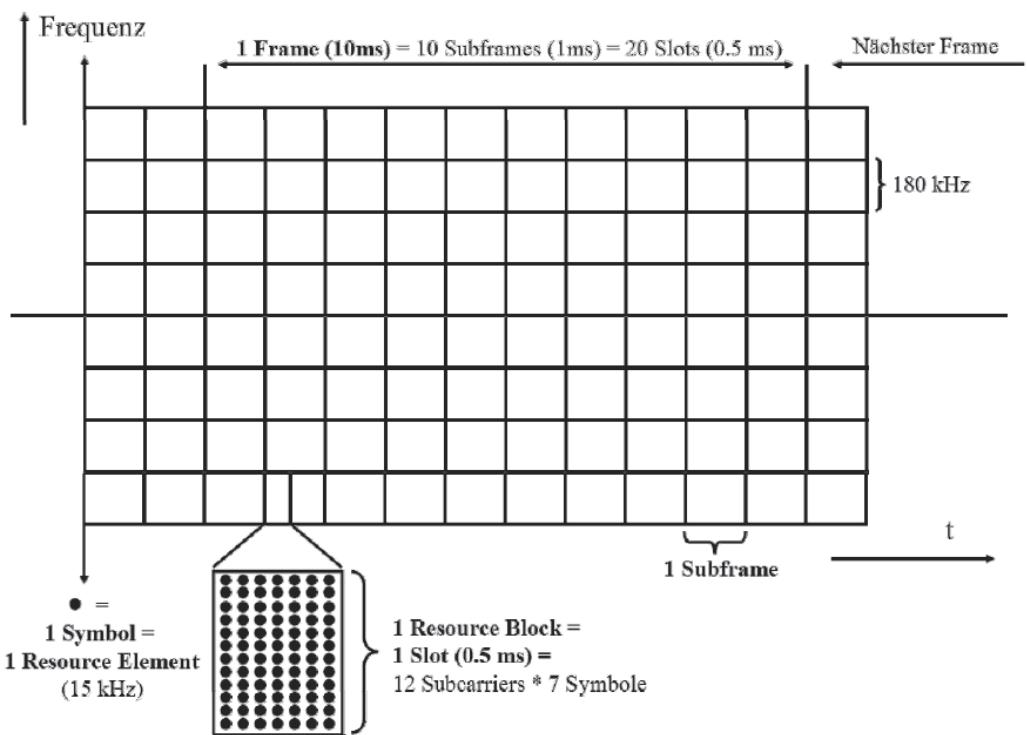
Quelle: [4], S. 159

- Mit UMTS (Release 99) neues Air-Interface **Universal Terrestrial Radio Access Network (UTRAN)**
- basierend auf Wideband-CDMA (W-CDMA)
- Ab UMTS (Release 4): Umstellung des Kernnetzes auf IP basierte Kommunikation (Sprache und Daten!)

Zellulare Netzwerke

LTE und LTE Advanced (4G)

- Umstellung auf **Orthogonal Frequency Division Multiplexing (OFDM)** als Übertragungstechnik, flexible Bandbreiten von 1.25 bis 20 MHz
- LTE Endgerät muss Mehrantennenverfahren (Multiple Input Multiple Output, **MIMO**) unterstützen
- LTE Kernnetz ist **rein paketbasiert** (Sprache über IMS / VoIP oder 3G/2G Fallback)



Quelle: [4], S. 300

Long Term Evolution (LTE, LTE-A)

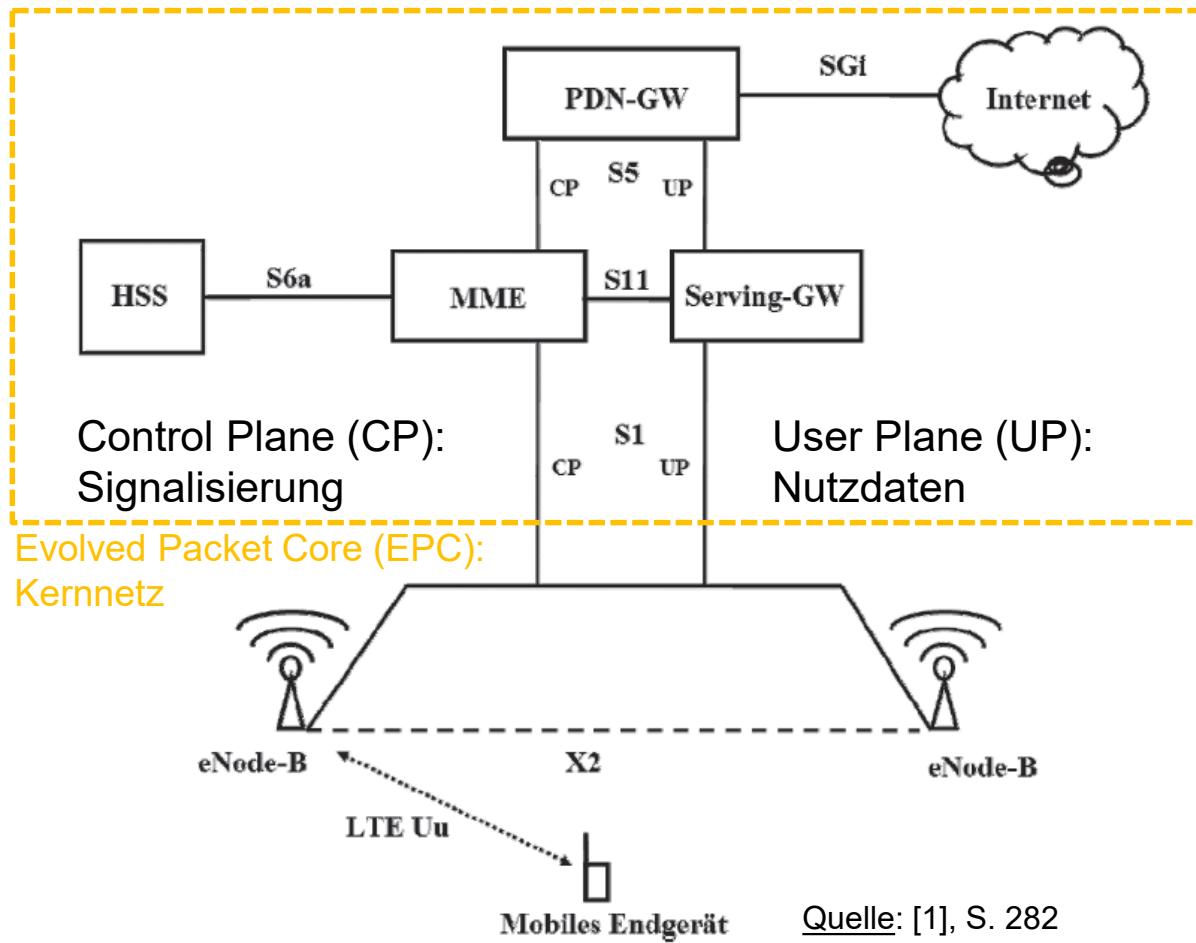
Einführung

- LTE beginnt mit 3GPP Release 8,
spätere Releases spezifizieren weitere Features:
 - Release 10: LTE Advanced (LTE-A, LTE+), bis 3 Gbit/s DL, 1,5 Gbit/s UL,
Bündelung von bis zu fünf Carriern mit 20 MHz (Carrier Aggregation, CA)
 - Release 13, 14: LTE Advanced Pro (LTE-A Pro): CA von bis zu 32
Carriern (→ mehr als 3 Gbit/s), Nutzung von lizenziertem und
unlizenziertem Spektrum (License Assisted Access), 256-QAM, Massive
MIMO, LTE Narrow-Band Internet-of-Things (NB-IoT)
- Geeignete Protokolle/Interfaces zur Interaktion mit GSM,
GPRS/EDGE und UMTS Netzen
- 5G Standardisierung läuft gerade:
 - Release 15: 5G Phase 1 (New Radio, 5G Standalone, 2018 fertiggestellt)
 - Release 16: 5G Phase 2 (offen, aktuell geplantes end date 20.12.2020)



Long Term Evolution (LTE)

Überblick Netzwerk-Architektur



Packet Data Network Gateway (PDN-GW)
Schnittstelle ins Internet

Mobility Management Entity (MME)
Mobilitätsmanagement

Serving-GW
Weiterleitung von Nutzdaten im Kernnetz

Home Subscriber Service (HSS)
entspricht HLR bei GSM

evolved Node-B (eNode-B)
Basisstation

5G

Motivation und Anwendungsfelder

Drei Dienstkategorien motivieren den Wechsel zu 5G

1. **Enhanced Mobile Broadband (eMBB)**
Hohe Datenraten z.B. für HD-Video, Virtual/Augmented Reality
2. **Massive Machine Type Communications (mMTC)**
Internet-of-Things (IoT) Anwendungen, z.B. Smart City, Grid, etc.
3. **Ultra-Reliable and Low-Latency Communication (uRLLC)**
Anwendungen in Industrie und Verkehr, z.B. drahtlose Vernetzung in der Produktion, automated driving (C-V2X)

5G Netz soll dafür verglichen mit der Vorgängertechnologie bieten:

- 1000x höheres Datenvolumen pro Fläche
- 10-100x mehr verbundene Geräte
- 10-100x typische Datenrate eines Nutzers
- Ende-zu-Ende Latenz von < 1ms

5G

Überblick über technische Neuerungen

Neuerungen in der Luftschnittstelle (Air Interface): 5G New Radio

OFDM-basiert (wie LTE) aber skalierbar auf höhere Bandbreiten (>100 MHz), flexible und kürzere Slotzeiten (<1 ms), Massive MIMO (Nutzung mehrerer Antennen), Nutzung der mmWave-Bänder (24-30 GHz)

Neuerungen in der Architektur: Service-Driven 5G Architecture

Höhere Flexibilität durch Software-Defined Networking (SDN) und Network Function Virtualization (NFV), eigenständige Zuteilung einzelner virtueller Netze auf einer gemeinsamen physikalischen Infrastruktur (Network Slicing)

Umsetzung in zwei Phasen:

1. 5G-Zellen mit LTE-Kernnetz (non-standalone 5G systems): Nutzung gängiger Mobilfunkbänder, nur ca. 2-3 Gbit/s erreichbar
2. 5G mit 5G-Kernnetz (standalone 5G systems): 5G-Vollausbau, mmWave-Bänder, z.B. 26 GHz Band

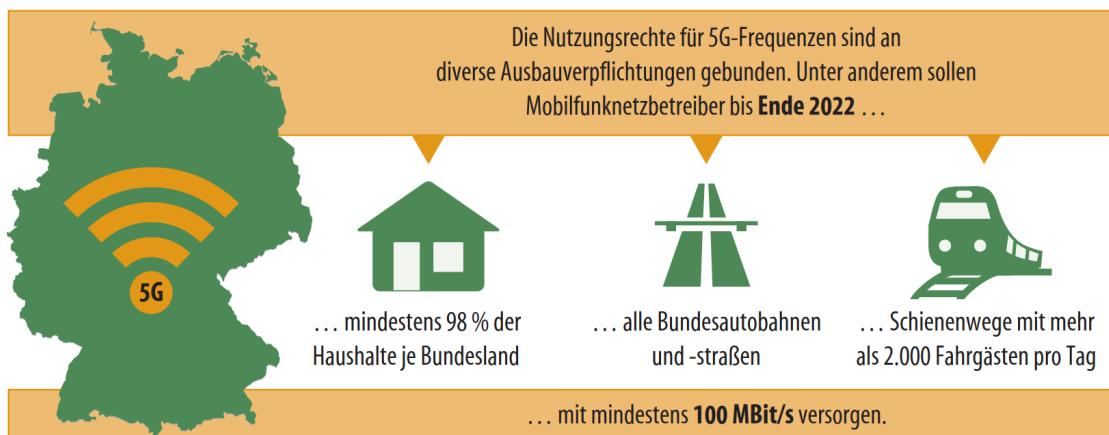
5G

Geplante Markteinführung in Deutschland

- Erste 5G Anwendungen ab Ende 2019:
- Ausbauverpflichtungen:

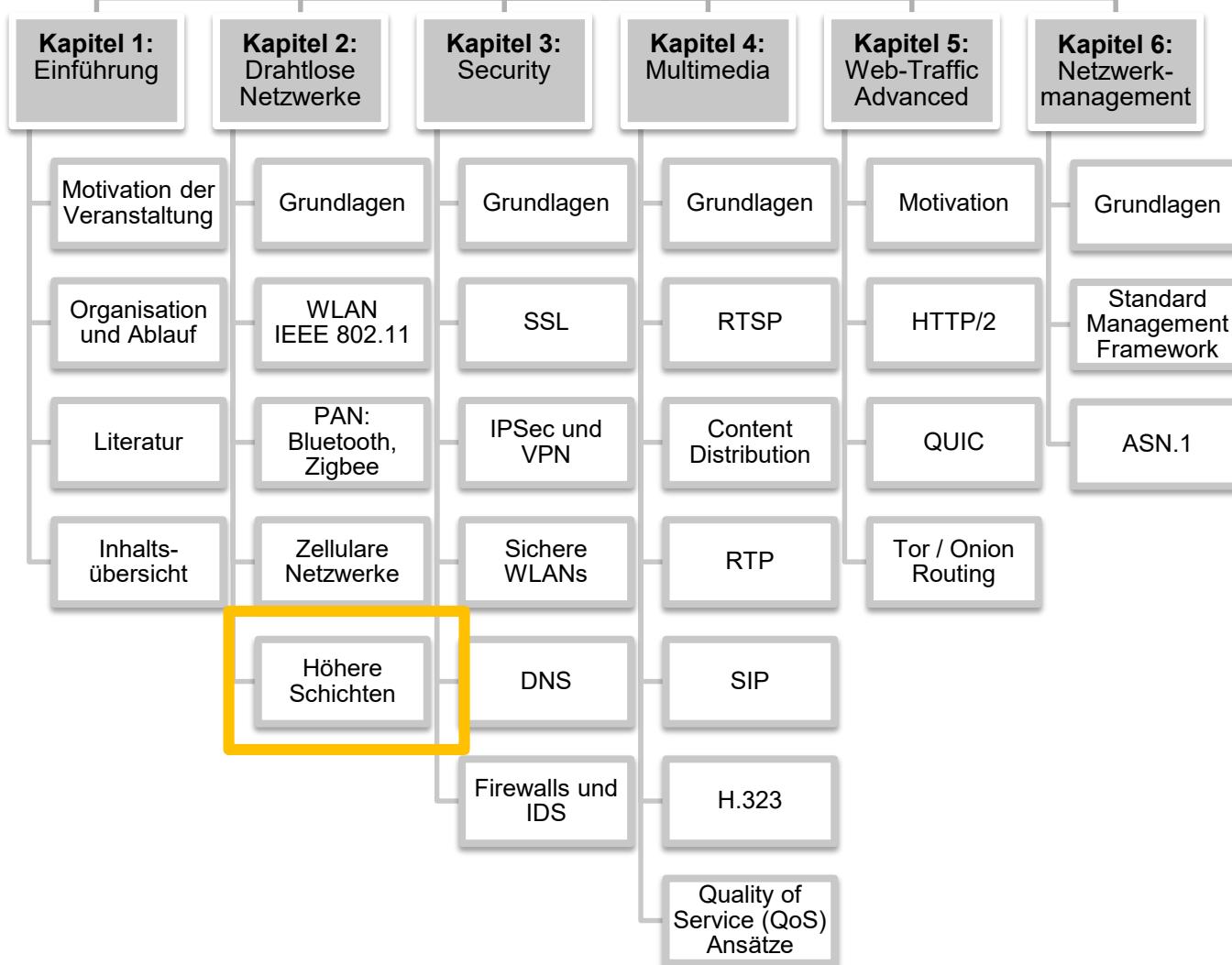
5G-Feldversuche	2018
Versteigerung bundesweiter Frequenzen	März 2019
Versteigerung lokaler Frequenzen	Ende 2019
Netzausbau bundesweit	ab Mitte 2019
schneller Surfen	ab Ende 2019
Edge-Computing	ab 2020
Nutzung lokaler Frequenzen	ab 2020
Auto-Vernetzung mit V2V	ab 2020
C-V2X-Verkehrssteuerung	ab 2025

Quelle: c't 2019, Heft 8, S. 59



Quelle: c't 2019, Heft 8, S. 60

Netzwerke II



Drahtlose Netzwerke

Auswirkung auf höhere Schichten

Zusammenfassung dieses Kapitels: **Ersetzen der unteren zwei Schichten (Link Layer, Physical Layer) durch drahtlose Varianten**

- Nach Schichtenkonzept sollten Auswirkungen minimal sein
- Weiterhin best-effort, TCP und UDP funktionieren weiterhin

ABER: Auswirkungen auf Performance

- **Paketverluste und -verzögerungen** durch Bitfehler auf dem drahtlosen Link und Mobilität/Handover
- **Fehlinterpretation von Paketverlusten seitens TCP:**
 - wird als Indiz für Netzüberlast gewertet
 - Congestion Window wird verringert, Datenrate sinkt
- Verzögerungen durch Link Layer Retransmissions
 - Auswirkungen auf Realtime-Applikationen
- Drahtloser Link hat zudem in der Regel geringere Datenrate

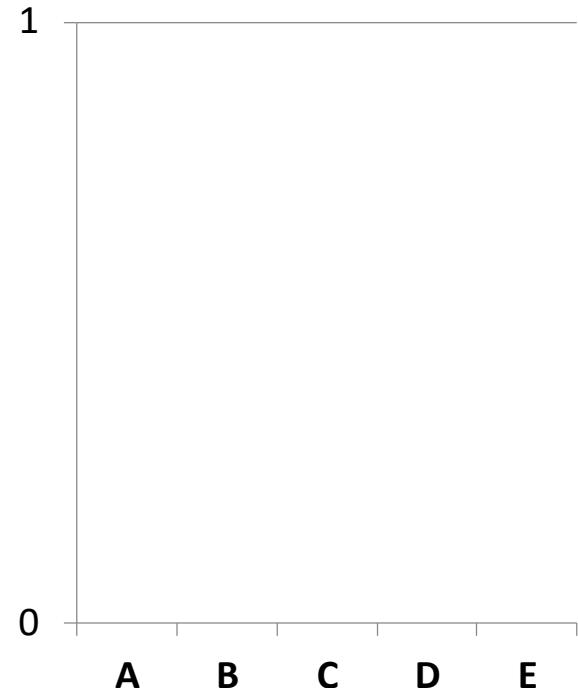


Drahtlose Netzwerke – Abschlussfrage 1

ID = wischhof@hm.edu
Umfrage noch nicht
gestartet

Sie nutzen einen Internetzugang über GSM mittels GPRS. Um welche Art der Ressourcenzuteilung handelt es sich?

- A) FDMA
- B) TDMA
- C) CDMA
- D) FDMA+TDMA
- E) FDMA+CDMA



Umfrage starten

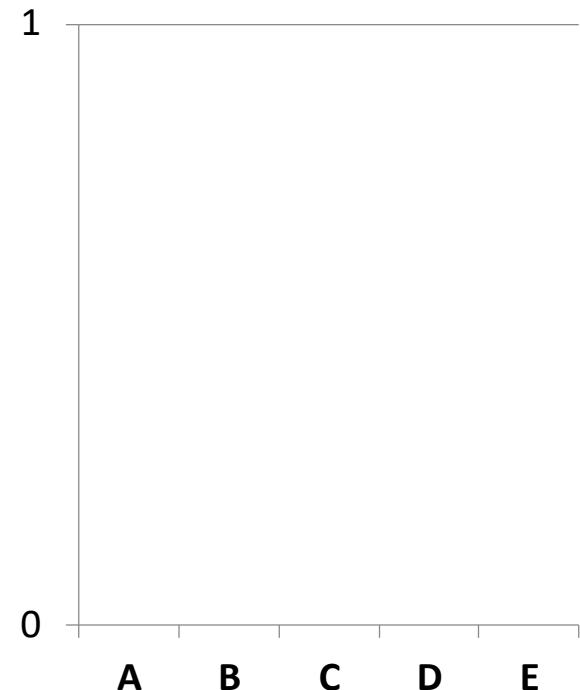
Drahtlose Netzwerke – Abschlussfrage 2

Ein Nutzer betreibt auf einem Notebook einen FTP Server. Er nutzt einen UMTS-Stick zum Internetzugriff, es läuft gerade der Upload einer Datei.

Da sich der Nutzer bewegt, kommt es zu einem Inter-BSC Handover. Läuft der Upload weiter?

- A) Nein, er muss neu gestartet werden
- B) Ja
- C) Ja, aber nur wenn Mobile IP aktiv ist
- D) Ja, aber nur wenn beide BSC die gleich Zelle nutzen

ID = wischhof@hm.edu
Umfrage noch nicht
gestartet



Umfrage starten

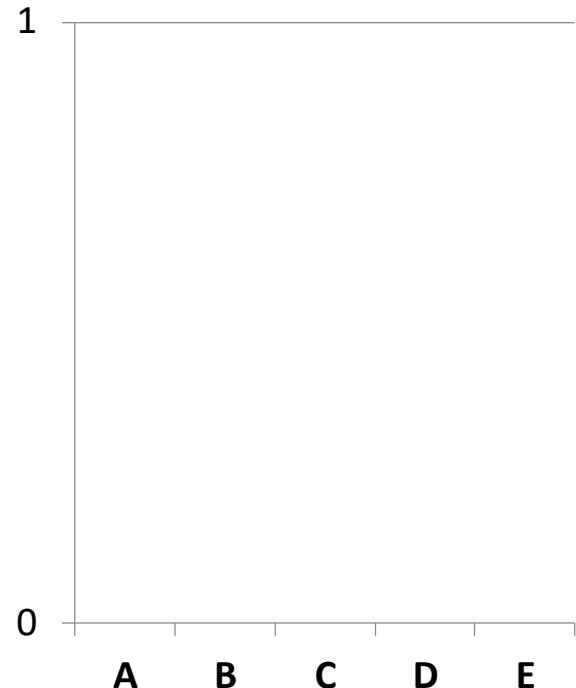


Drahtlose Netzwerke – Abschlussfrage 3

Sie nutzen Mobile IP und betreiben in Ihrem Heimnetz einen Home Agent. Aktuell sind Sie im Ausland in einem fremden Netz der Firma A. Ist es möglich, Sie unter Ihrer Heimat-Internetadresse (Permanent Address) zu erreichen – auch wenn Firma A keinen Foreign Agent betreibt?

- A) Ja
- B) Nur für Rechner innerhalb des fremden Netzes
- C) Nur für Rechner im Heimnetz
- D) Nein

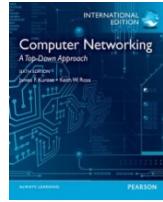
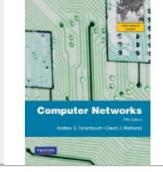
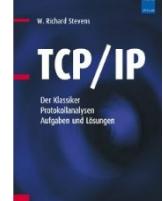
ID = wischhof@hm.edu
Umfrage noch nicht
gestartet



Umfrage starten

Quellen

Empfohlene Literatur und weitere Informationen

[1]	<p>James F. Kurose, Keith W. Ross Computer Networking – A Top-Down Approach Prentice Hall International; ISBN-13: 978-0273768968 <i>im Wesentlichen Stoff aus Kapitel 6 bis Kapitel 9</i></p>	
[2]	<p>Andrew S. Tanenbaum, David Wetherall Computer Networks Prentice Hall International; ISBN-13: 978-0132553179</p>	
[3]	<p>W. Richard Stevens, Ian Travis (Übersetzer) TCP/IP: Der Klassiker. Protokollanalyse. Aufgaben und Lösungen Vde Verlag GmbH; ISBN-13: 978-3800732234</p>	
[4]	<p>Martin Sauter Grundkurs Mobile Kommunikationssysteme Vieweg+Teubner; ISBN-13: 978-3-8348-1407-4 Im Netz der Hochschule/VPN online unter: http://link.springer.com/book/10.1007/978-3-8348-9828-9/page/1</p>	