Rechnernetze II

SoSe 2020

Roland Wismüller
Betriebssysteme / verteilte Systeme
roland.wismueller@uni-siegen.de
Tel.: 0271/740-4050, Büro: H-B 8404

Stand: 25. Mai 2020

Rechnernetze II

SoSe 2020

3 Drahtlose Netze

Inhalt

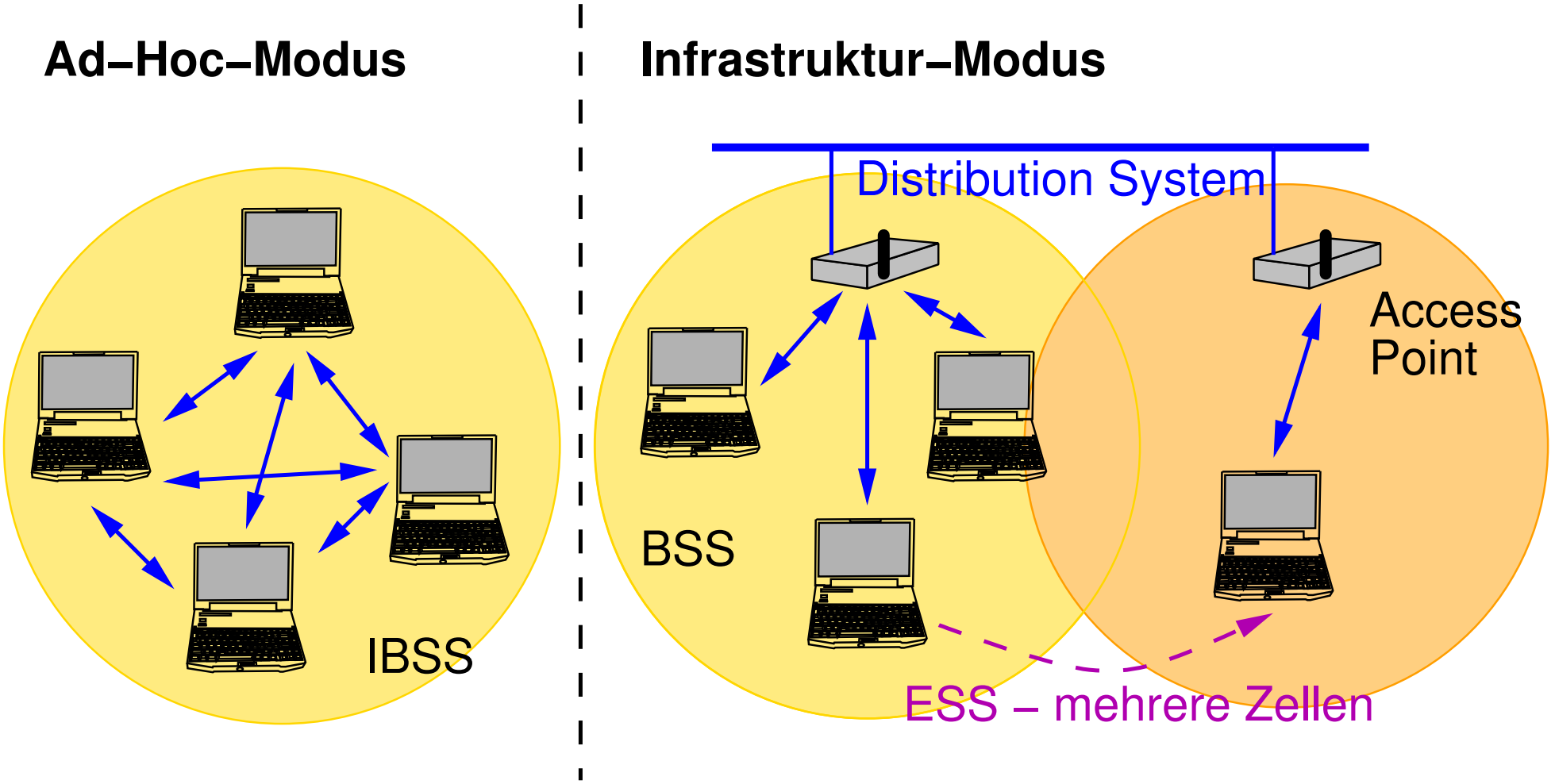
- WLAN (IEEE 802.11)
- Bluetooth (IEEE 802.15)

- Tanenbaum, Kap. 1.5.4, **4.4**, **4.6**
- Peterson, Kap. **2.8**
- Axel Sikora: Wireless LAN, Addison Wesley, 2001.
- Jörg Rech: Wireless LANs, 2. Auflage, Heise Verlag, 2006.
- Edgar Nett, Michael Mock, Martin Gergeleit: Das drahtlose Ethernet, Addison-Wesley, 2001.

Hintergrund

- Drahtlose Netzanbindung von mobilen Geräten
- Sicherungsschicht kompatibel zu Ethernet
- Unterstützung für zwei Betriebsmodi:
  - Ad-Hoc-Modus: Endgeräte kommunizieren direkt
    - IBSS (*Independent Basic Service Set*)
  - Infrastruktur-Modus: Kommunikation über *Access Point*
    - BSS (*Basic Service Set*): eine Funkzelle
    - ESS (*Extended Service Set*): mehrere Funkzellen, über ein anderes Netz (z.B. Ethernet oder auch WLAN) verbunden

WLAN-Betriebsmodi



802.11 Protokollstack

Höhere Schichten					
Logical Link Control (802.2, wie bei Ethernet)					
MAC–Teilschicht: CSMA/CA, MACAW					
802.11 IR / 2.4 GHz FHSS/DSSS 2 Mb/s	802.11a 5 GHz OFDM 54 Mb/s	802.11b 2.4 GHz HR–DSSS 11 Mb/s	802.11g 2.4 GHz OFDM 54 Mb/s	802.11n 2.4/5 GHz OFDM/MIMO – 600 Mb/s	802.11ac 5 GHz OFDM/MIMO – 1.69 Gb/s

Siche–
rungs–
schicht

Bitüber–
tragungs–
schicht

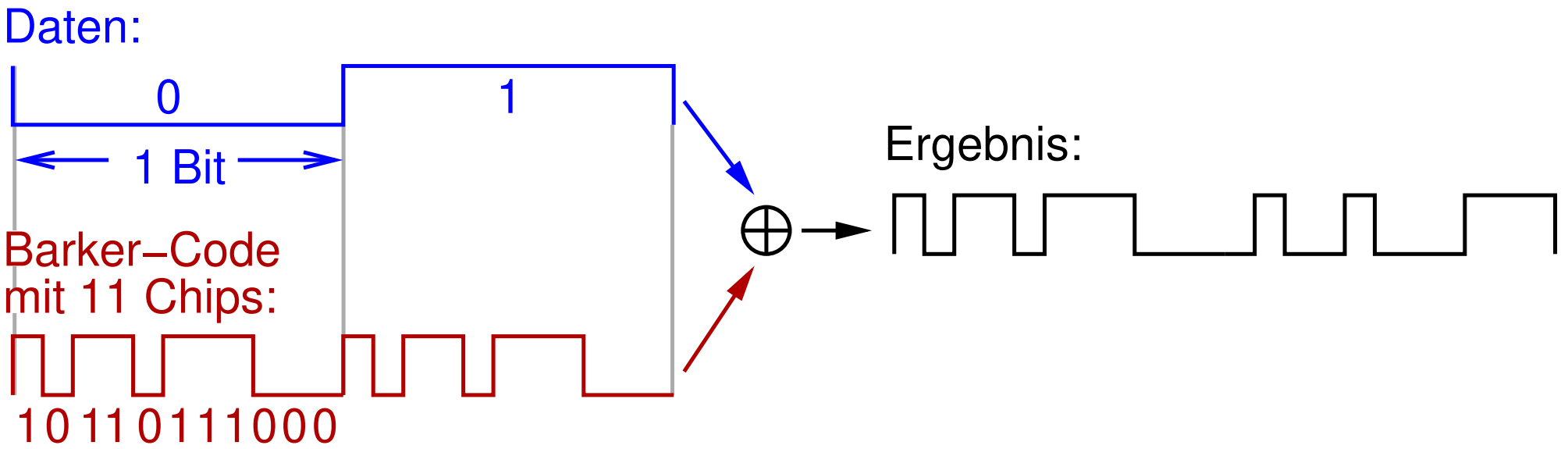
➥ Im Folgenden: Schwerpunkt auf 802.11b und 802.11g

Basis der Funkübertragung: Spreizbandtechnik

- Problem: 802.11 arbeitet in feigegebenen ISM-Bändern
  - ISM: Industrial, Scientific, Medical
  - 2,4 GHz und 5 GHz
- Maßnahme gegen Funkstörungen:
  - Übertragung in möglichst breitem Frequenzband
  - Störungen sind meist schmalbandig
- Techniken:
  - FHSS (*Frequency Hopping Spread Spectrum*)
    - viele Kanäle, Frequenz wechselt pseudozufällig
  - OFDM (*Orthogonal Frequency Division Multiplexing*)
    - im Prinzip ähnlich zu DMT (☞ **1.6**: ADSL)

Basis der Funkübertragung: Spreizbandtechnik ...

- Techniken ...:
  - DSSS (*Direct Sequence Spread Spectrum*)
    - Sendedaten werden mit (fester!) Pzeudozufallsfolge höherer Bitrate XOR-verknüpft
    - Muster leicht aus verrauschtem Signal „herauszuhören“

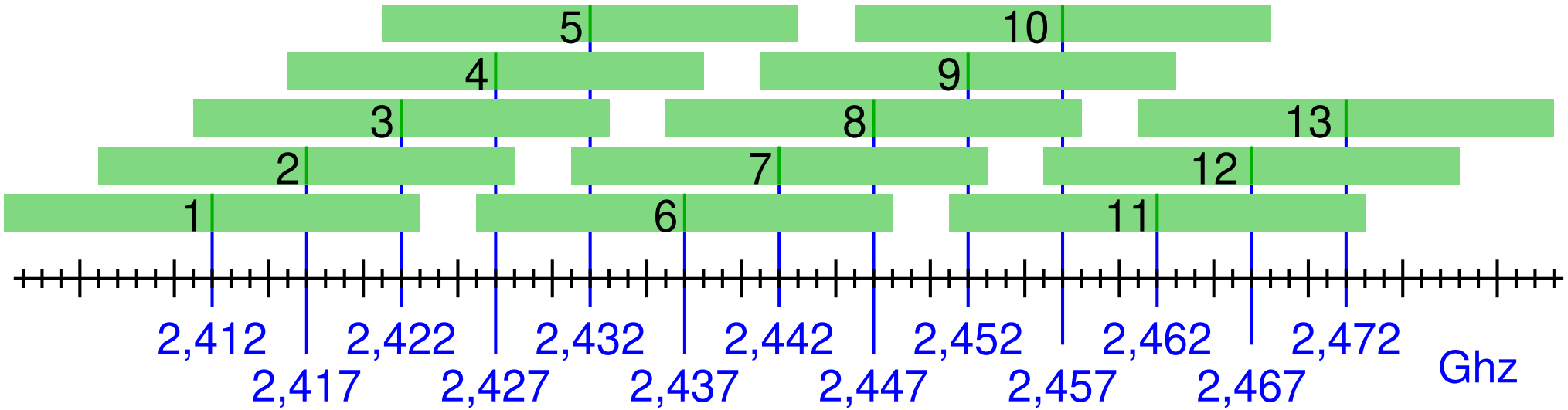


Basis der Funkübertragung: Spreizbandtechnik ...

- Techniken ...:
  - HR-DSSS (*High Rate DSSS*)
    - verkürzte Codelänge: 8 Chips
    - QPSK-artige Modulation
      - 4 Bit / Symbol (für 5.5 Mb/s)
      - 8 Bit / Symbol (für 11 Mb/s)
    - benötigt höheren Rauschabstand

Frequenzbänder im 2.4 GHz Band

- 13 Kanäle (Europa)
- Bandbreite eines Kanals bei 802.11b: 22 MHz
- Kanäle überlappen!
  - bei 802.11b max. 3 nicht überlappende Kanäle möglich



WLAN nach IEEE 802.11g

- Bruttodatenrate bis 54 Mbit/s (netto max. 50%)
- Verwendet OFDM wegen Mehrfachempfang durch Reflexionen
  - Problem verschärft sich bei höherer Bitrate
  - daher: parallele Übertragung auf mehreren (48) Unterkanälen
- Unterschiedliche Modulationsarten (z.B. QAM-16, QAM-64)
  - Symbolrate: 250 kHz
- Vorwärts-Fehlerkorrektur
  - Code-Rate 1/2, 2/3 oder 3/4 (Nutzdaten / Gesamtdaten)
- Zur Kompatibilität mit 802.11b:
  - 802.11g-Geräte unterstützen i.d.R. auch DSSS

Medienzugriffssteuerung (MAC)

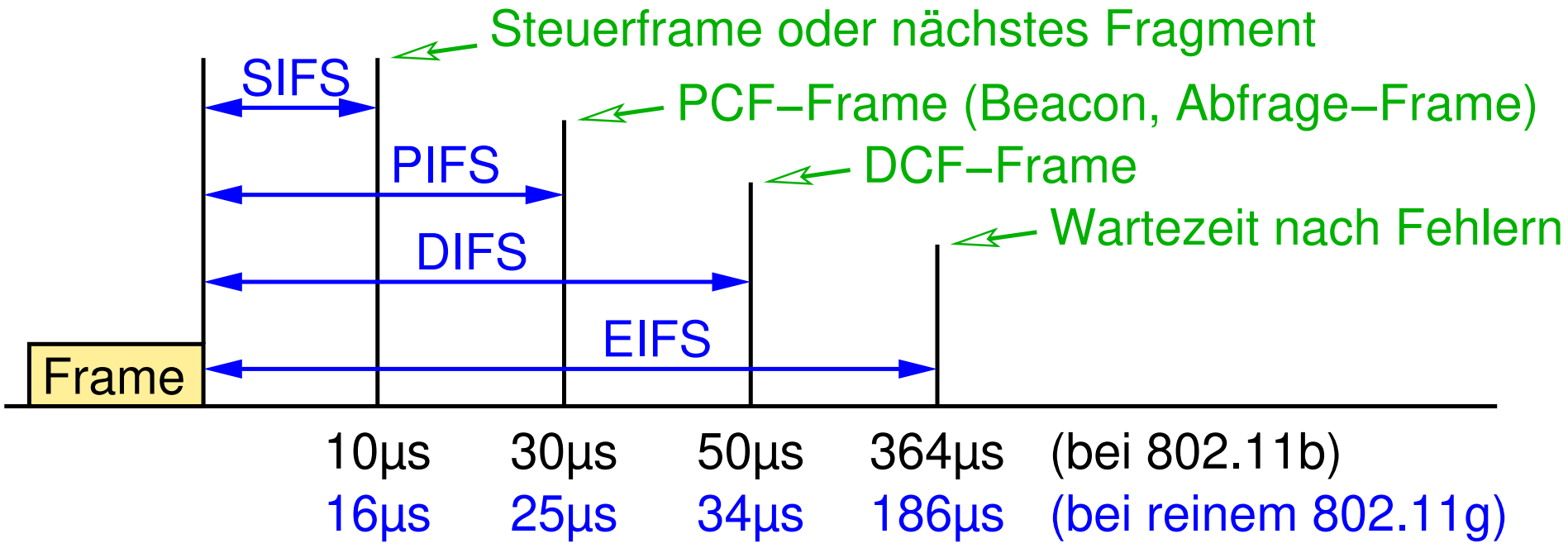
- CSMA/CD ist nicht möglich
  - Funkgeräte arbeiten im Halbduplex-Modus
  - während des Sendens kein Mithören möglich
  - nur Empfänger „erkennt“ Kollision (durch Prüfsumme)
- In IEEE 802.11 zwei Modi für Zugriffssteuerung:
  - DCF (*Distributed Coordination Function*)
    - dezentrales Verfahren (CSMA/CA, MACAW)
  - PCF (*Point Coordination Function*)
    - zentrale Steuerung durch den *Access Point*
  - beide Modi können gleichzeitig genutzt werden

DCF: CSMA/CA

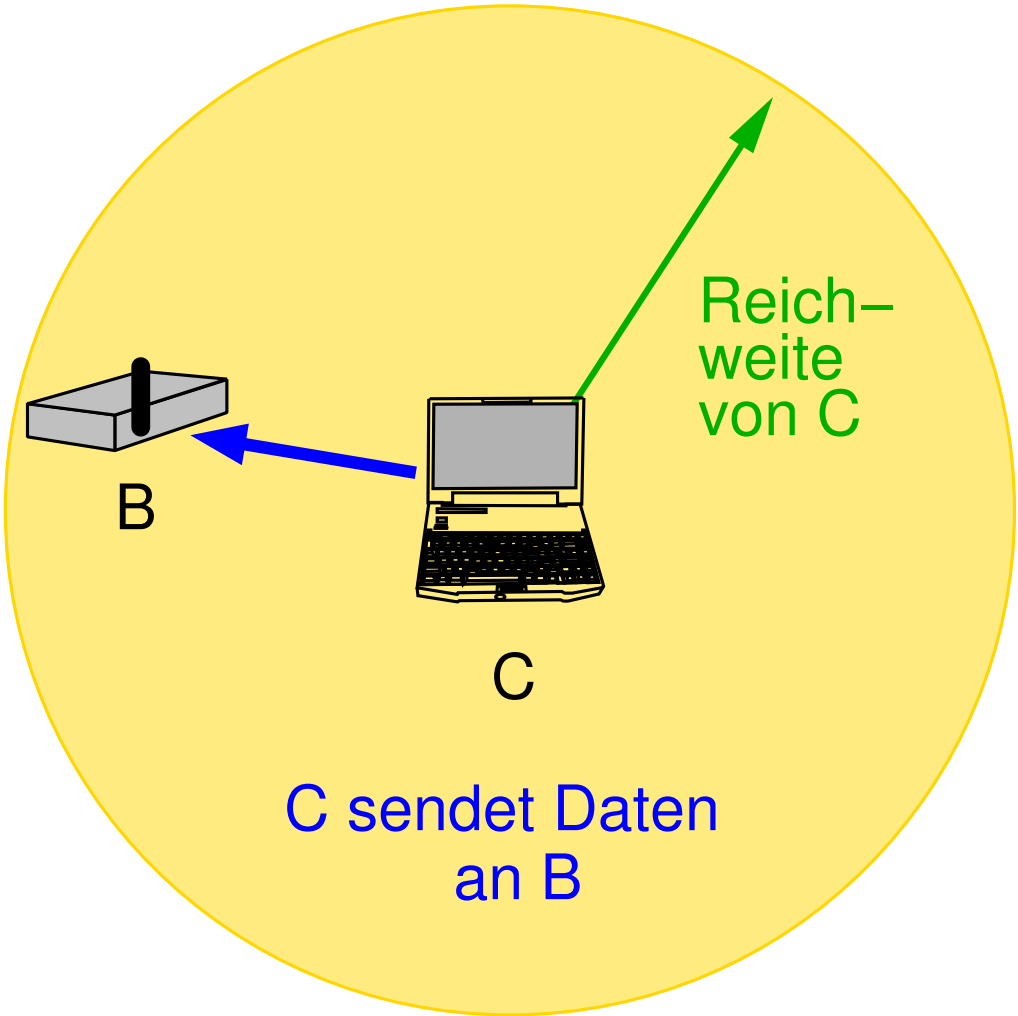
- *Carrier Sense Multiple Access / Collision Avoidance*
  - *Avoidance* heißt hier: **möglichst** vermeiden
  - Kollisionen sind aber immer noch möglich
- Vorgehen im Prinzip wie bei CSMA/CD:
  - Abhören des Mediums, senden sobald Medium frei
- Unterschiede:
  - keine Kollisionserkennung beim Senden
    - Empfänger muß jeden Frame bestätigen (ACK-Frame)
  - vor dem Senden muß das Netz immer mindestens für eine bestimmte Zeit abgehört und als frei erkannt werden:
    - IFS (*Interframe Spacing*)
  - Medium belegt: zufällige Wartezeit zur Kollisionsvermeidung

Interframe Spacing (IFS)

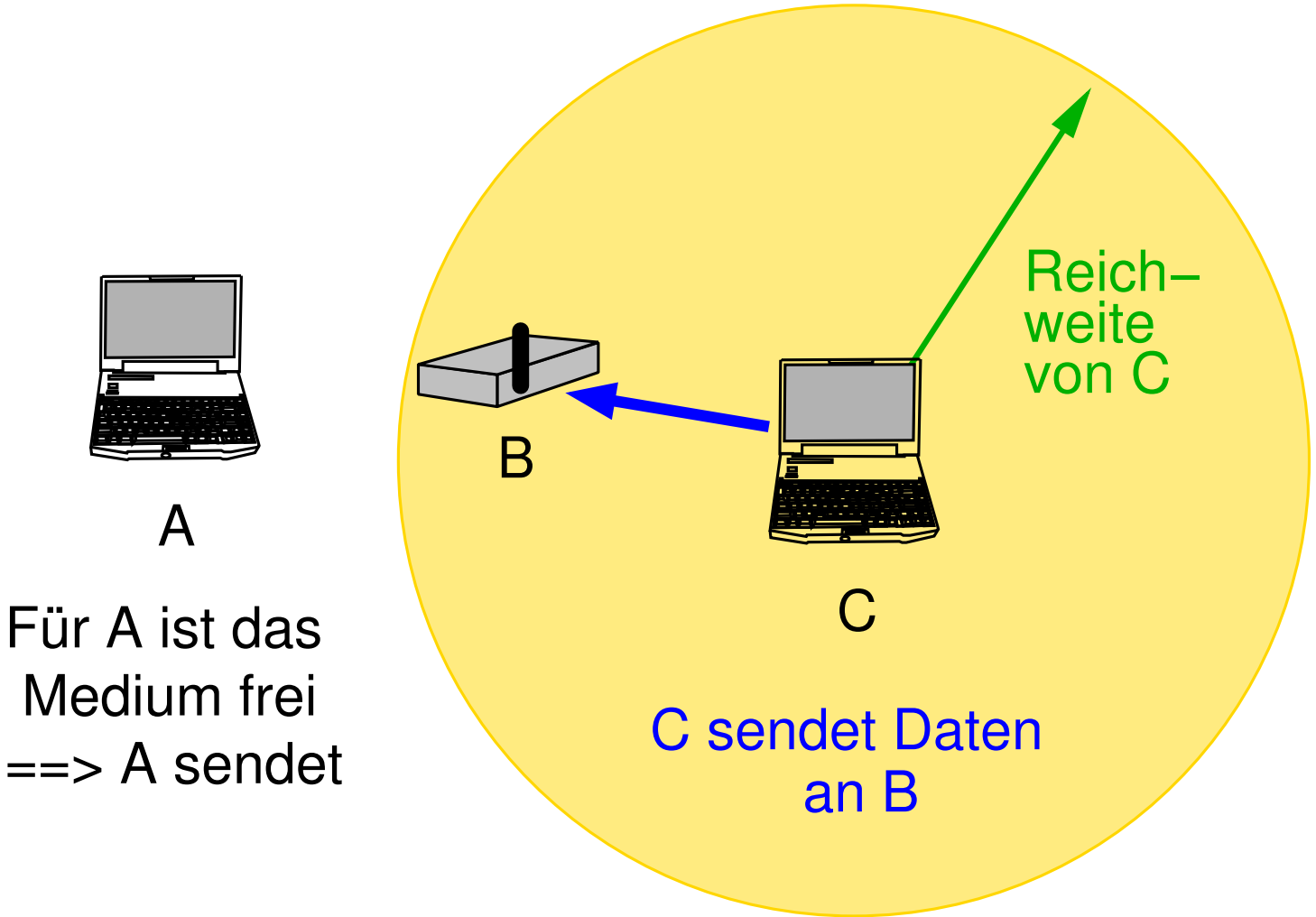
- Gibt an, wie lange eine Station das Medium mindestens als frei erkennen muß, bevor sie senden darf
- Unterschiedliche IFS-Zeiten für verschiedene Frame-Typen
  - damit: Realisierung unterschiedlicher Prioritäten



Das Hidden-Station-Problem

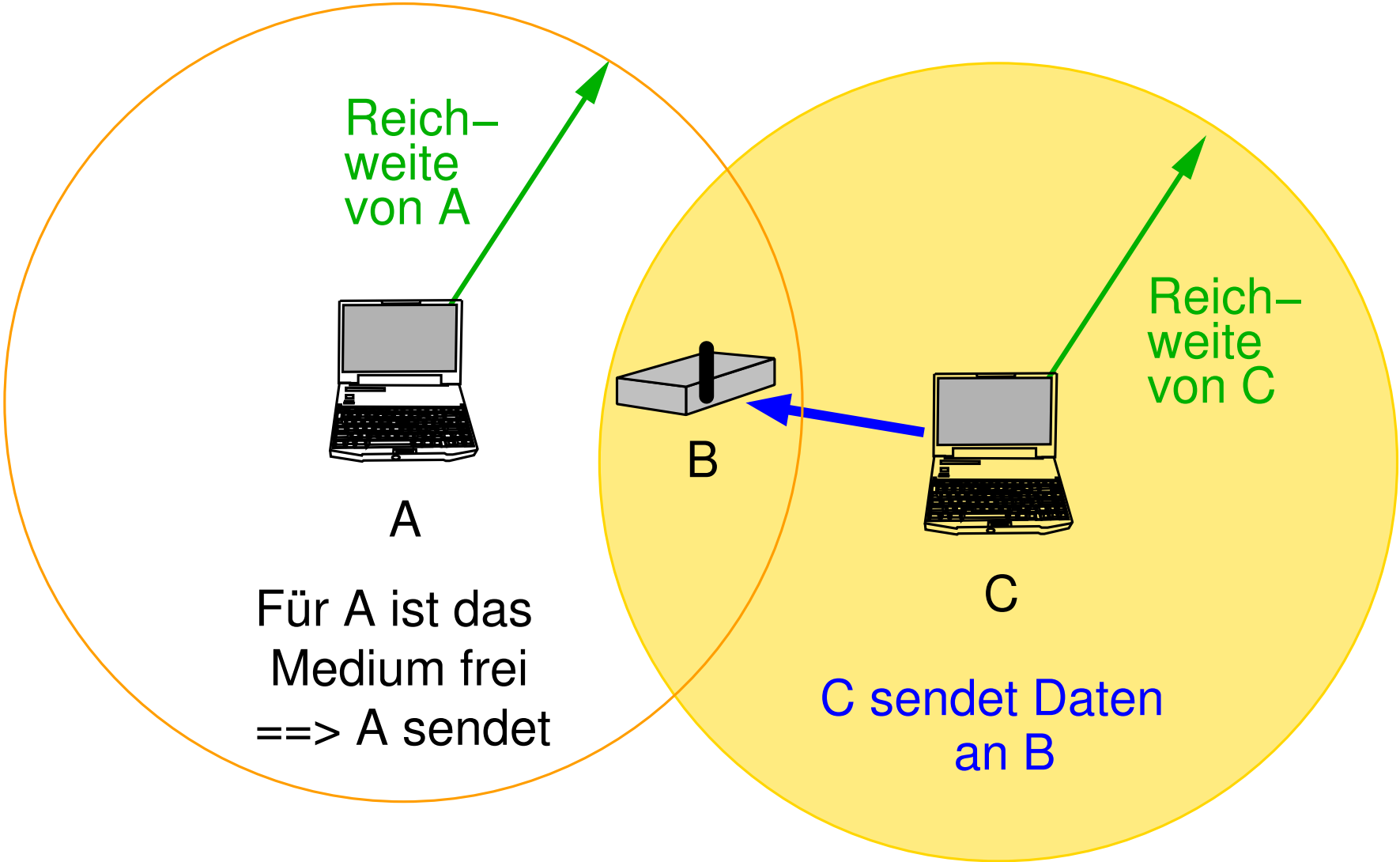


Das Hidden-Station-Problem

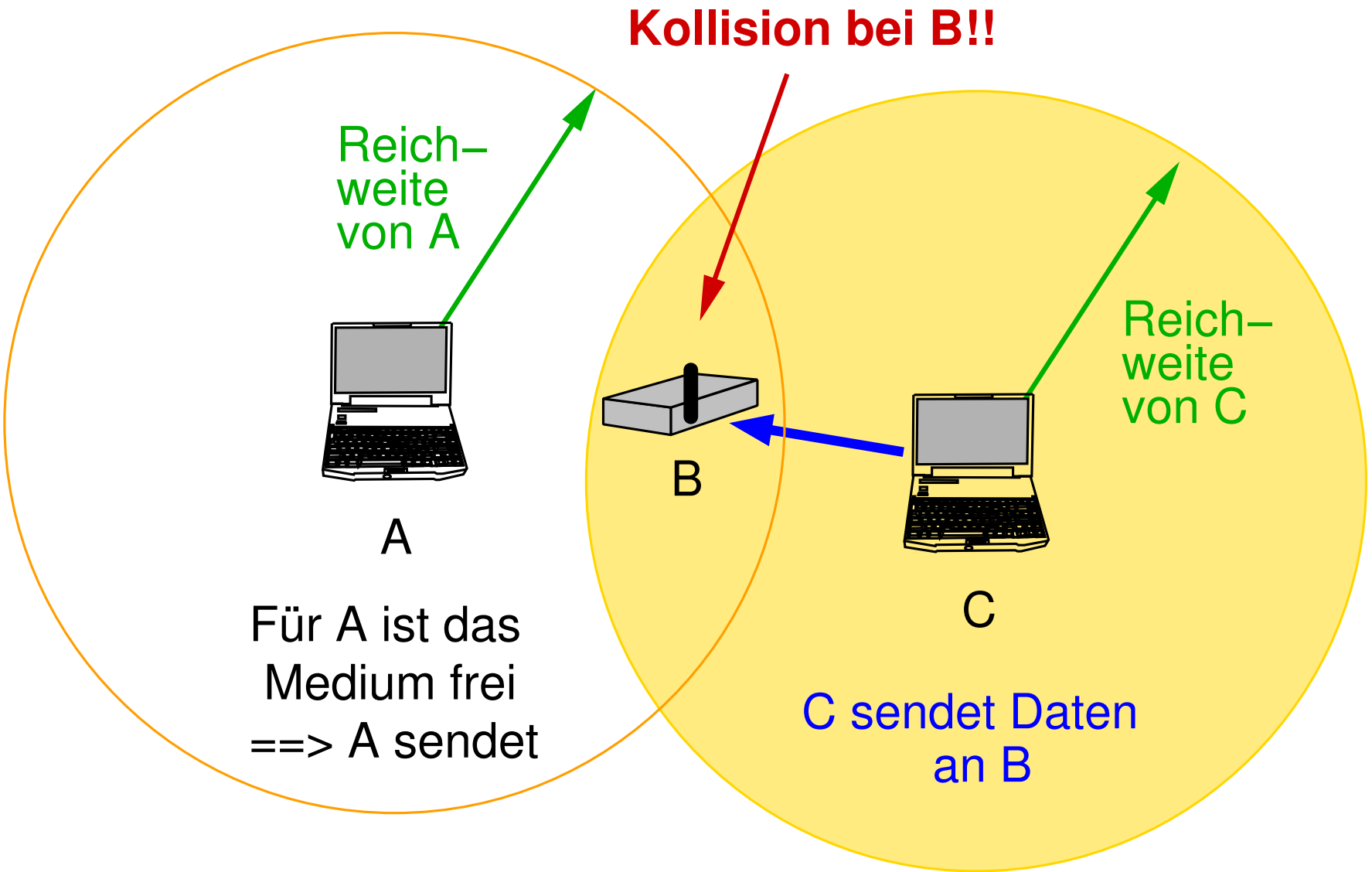


Für A ist das
Medium frei
==> A sendet

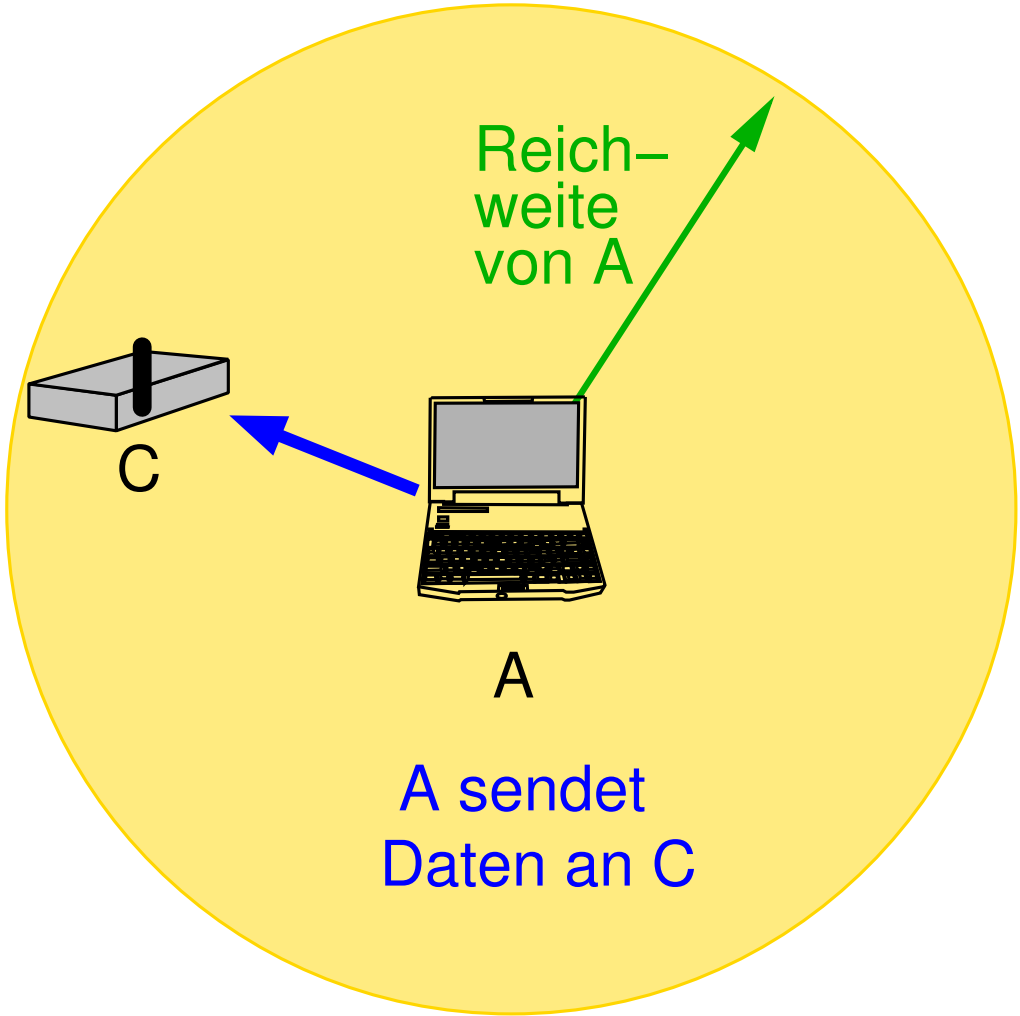
Das Hidden-Station-Problem



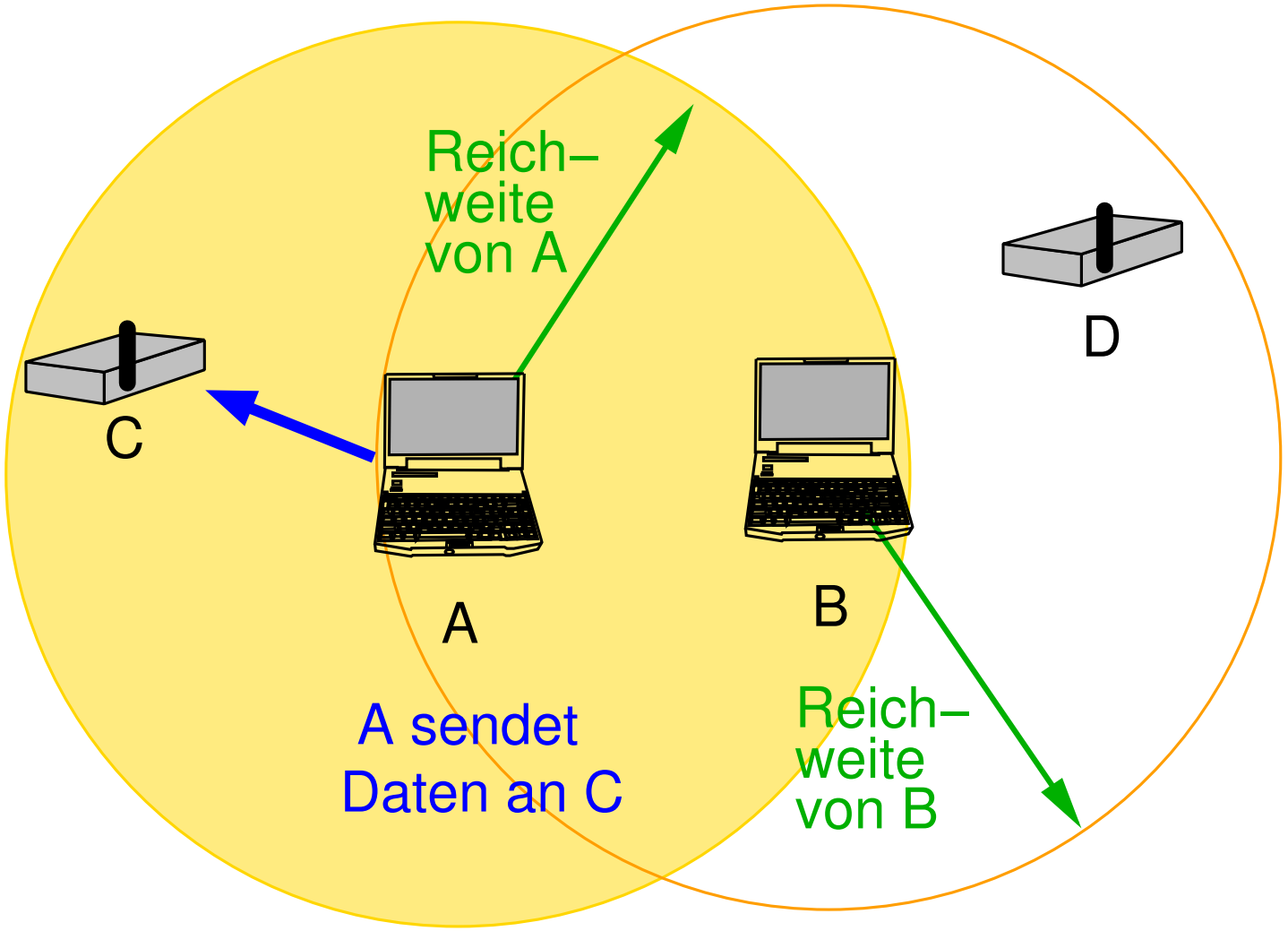
Das Hidden-Station-Problem



Das Exposed-Station-Problem



Das Exposed-Station-Problem



B will an D senden, glaubt aber, daß dies eine Kollision hervorruft

Das MACA - Protokoll (*Multiple Access, Collision Avoidance*)

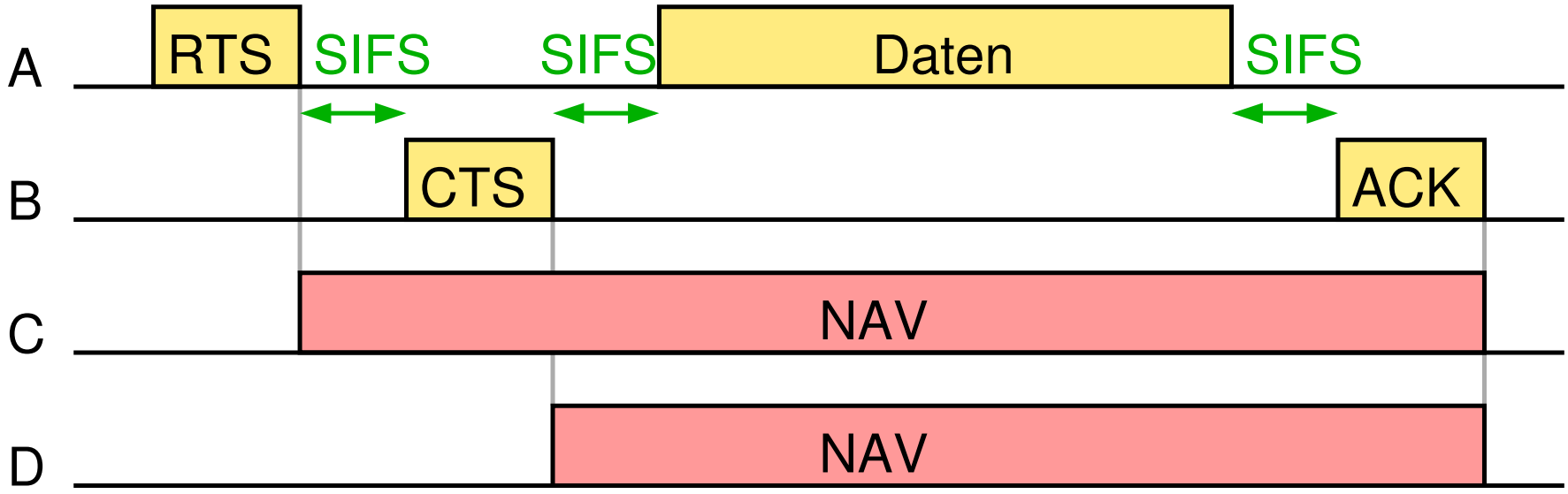
1. Sender sendet RTS (*Request To Send*) an Empfänger
2. Empfänger antwortet mit CTS (*Clear To Send*)
   - ➥ CTS-Frame enthält Dauer der Übertragung
3. Sender sendet Daten

- ➥ Wer RTS hört, sendet nicht, bis CTS übertragen sein sollte
  - ➥ Zeit ergibt sich aus Framelängen und Signallaufzeit
- ➥ Wer CTS hört, sendet nicht vor Ablauf der Übertragungsdauer
  - ➥ löst *Hidden Station* Problem
- ➥ Wer CTS nicht hört, kann gleichzeitig senden
  - ➥ löst *Exposed Station* Problem
- ➥ Wenn zwei RTS kollidieren, kommt kein CTS $\Rightarrow$ *Backoff*

MACAW - Erweiterung von MACA für WLAN

- Einführung von ACKs, um Neuübertragung durch Sicherungsschicht zu ermöglichen
  - schneller, da kürzere Timeouts als z.B. bei TCP
- Modifikationen gegenüber MACA:
  - Empfänger bestätigt Empfang der Daten mit ACK
  - Station, die RTS hört, darf nicht senden, bis ACK übertragen wurde
    - Übertragung könnte mit ACK kollidieren
  - auch RTS-Frame enthält Dauer der Übertragung
- 802.11 verwendet MACAW zum Versenden längerer Frames
  - für kurze Frames: einfaches CSMA/CA

MACAW - Beispiel

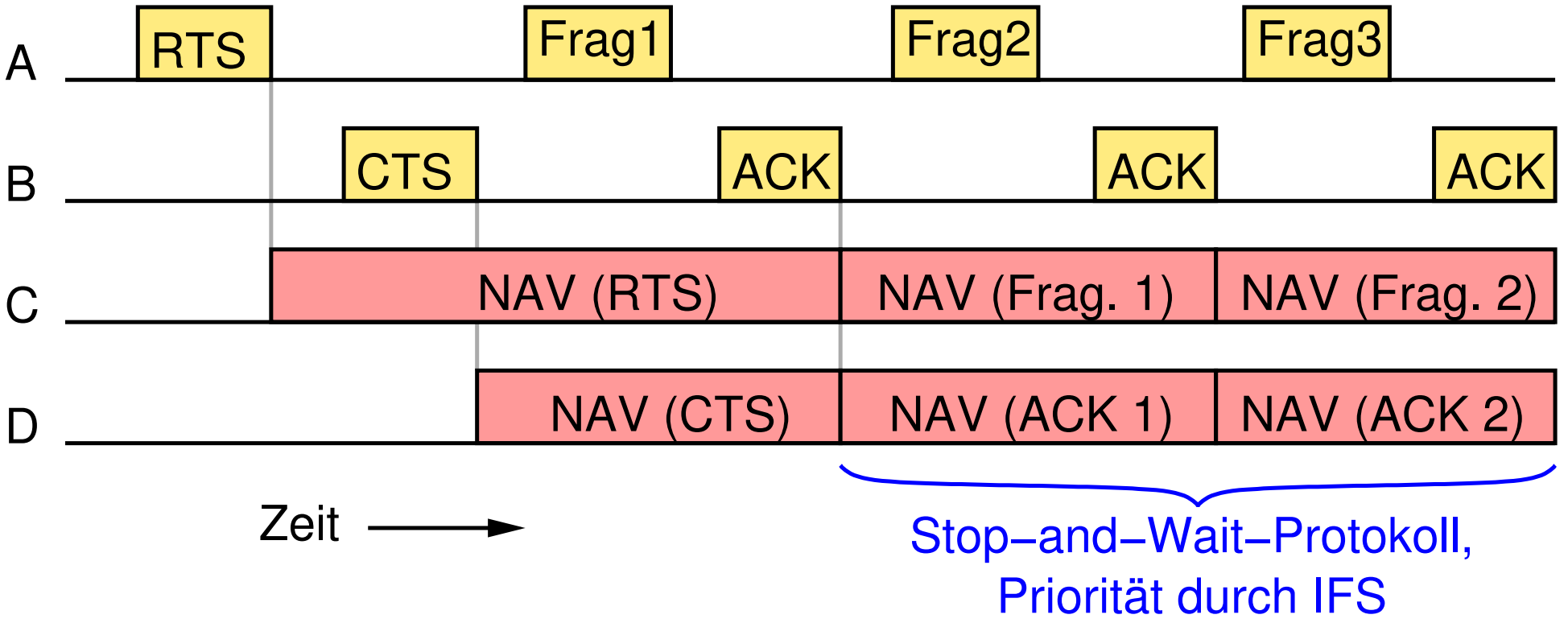


B und C sind in Reichweite von A, D nicht

NAV: *Network Allocation Vector* (Netz ist belegt, kein Senden)

Fragmentierung

- Frames können in mehreren Fragmenten übertragen werden
  - erhöht Effizienz bei hoher Bitfehlerrate

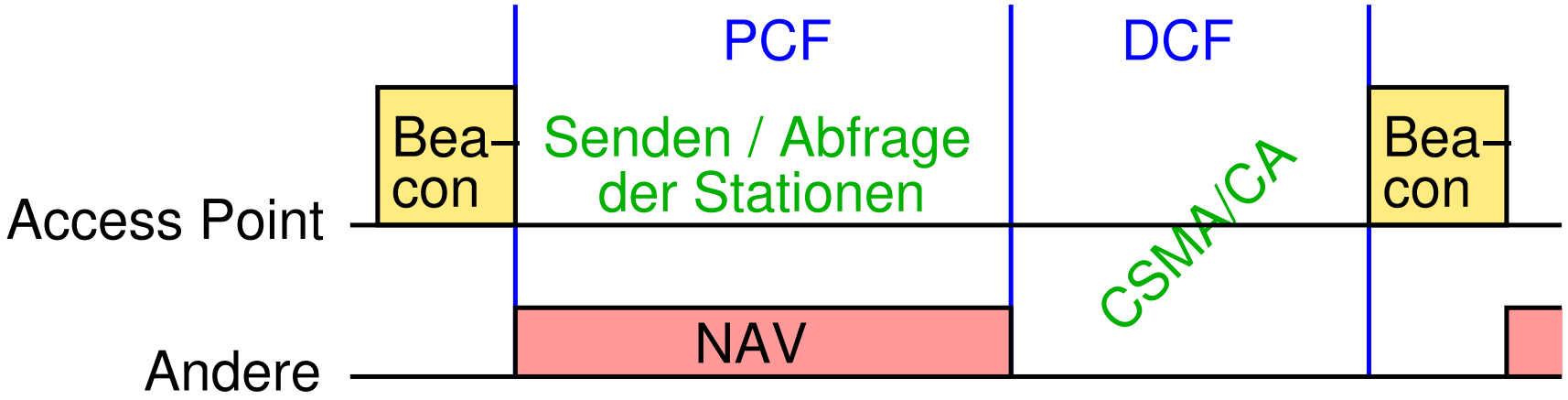


Koexistenz von 802.11b und 802.11g

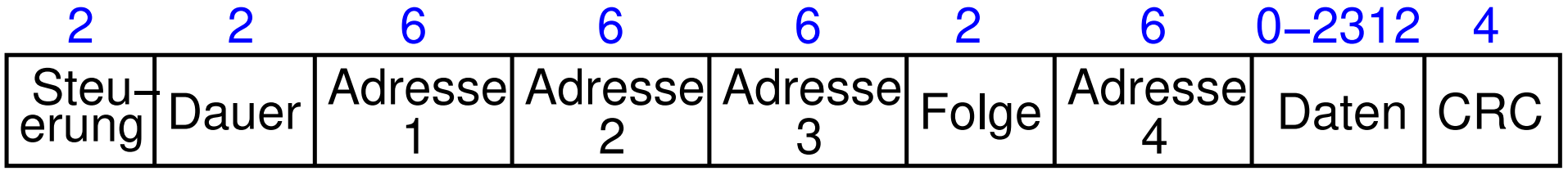
- Problem: 802.11b-Station erkennt nicht, daß 802.11g-Station sendet
- Lösung: *Protection*-Mechanismus
  - wird vom *Access-Point* aktiviert, wenn dieser eine 802.11b-Station erkennt
- Zwei Verfahren:
  - **CTS-to-Self:** 802.11g-Station sendet vor der eigentlichen Übertragung ein CTS mit DSSS, das das Medium reserviert
  - **RTS/CTS:** RTS, CTS und ACK werden mit DSSS übertragen, nur Datenframes werden mit OFDM gesendet
- Nachteil: Nutzdatenrate sinkt deutlich ($\sim$ 10-15 Mbit/s)

PCF: TDMA (*Time Division Multiple Access*)

- *Access Point* sendet regelmäßig *Beacon*-Frame als Broadcast
  - enthält verschiedene Systemparameter
  - kann Medium für bestimmte Zeit reservieren (über NAV)
    - in dieser Zeit: Stationen, die sich für PCF angemeldet haben, werden vom *Access Point* einzeln abgefragt
  - danach: normaler DCF-Betrieb bis zum nächsten *Beacon*



Frame-Format (für Daten-Frames)



- **Steuerung**: Frame-Typ, Frame von/an *Distribution System*, Verschlüsselung, *Power Management*, ...
- **Dauer**: für Belegung des Kanals über NAV
- **Adresse 1-4**: IEEE 802 MAC-Adressen
  - Quell- und Ziel-Rechner
  - BSS-ID bzw. Quell- und Ziel-*Access-Point*
- **Folge**: Numerierung von Fragmenten

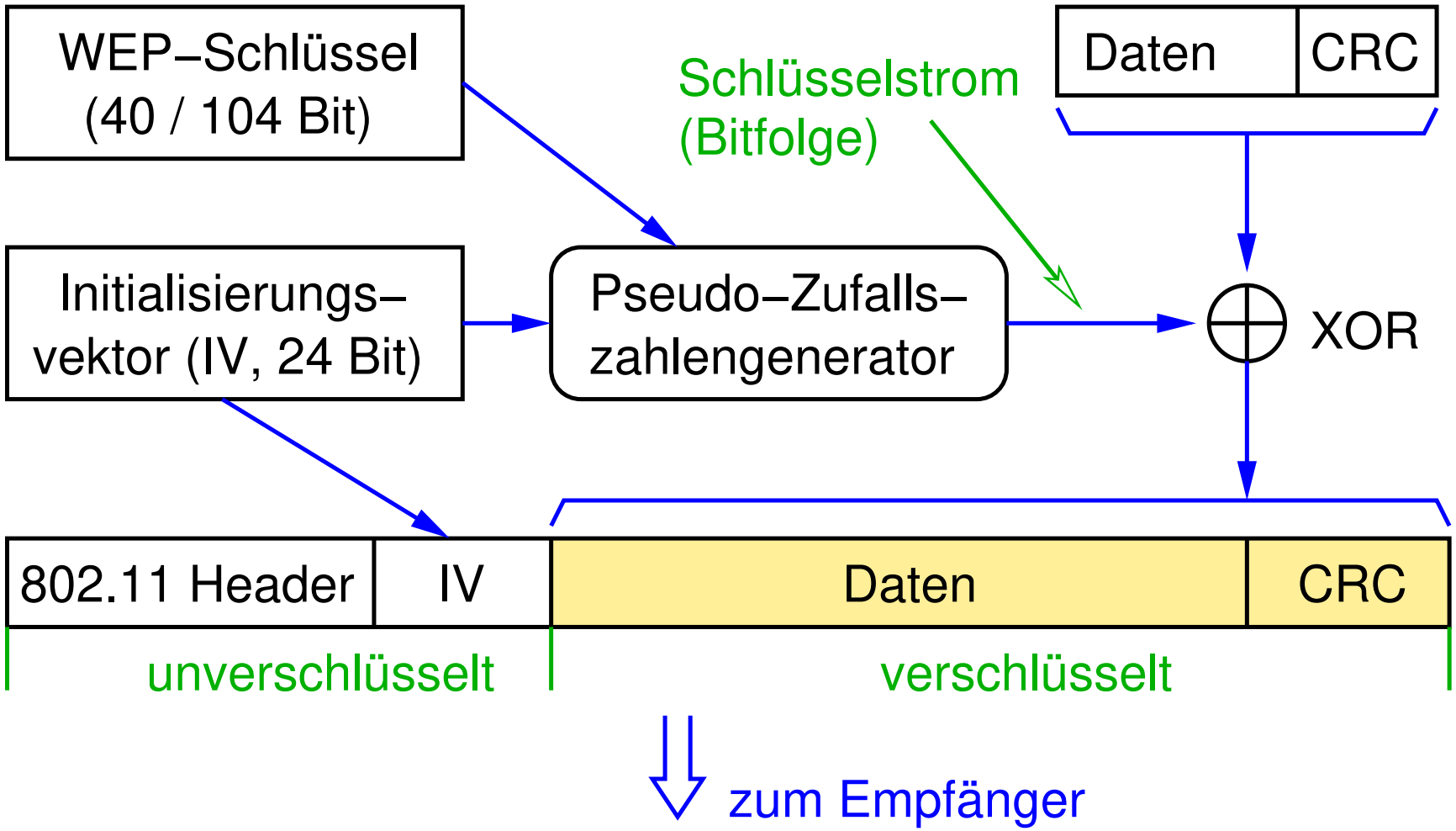
Sicherheitsmechanismen

- ESSID (*Extended Service Set IDentifier*): Name des Netzes
  - muß i.a. zum Anmelden an *Access Point* bekannt sein
  - wird i.d.R. vom *Access Point* im *Beacon*-Frame mitgesendet
  - viele WLAN-Karten akzeptieren auch „*any*“
- Authentifizierung über MAC-Adresse
  - Basisstation hat Liste der erlaubten MAC-Adressen
  - viele WLAN-Karten erlauben Änderung der MAC-Adresse!
- Verschlüsselung
  - WEP (*Wire Equivalent Privacy*, IEEE 802.11)
    - 40 (bzw. 104) Bit Schlüssel, veraltet
  - WPA und WPA2 (*Wi-Fi Protected Access*, IEEE 802.11i)
    - deutlich bessere Sicherheit als WEP

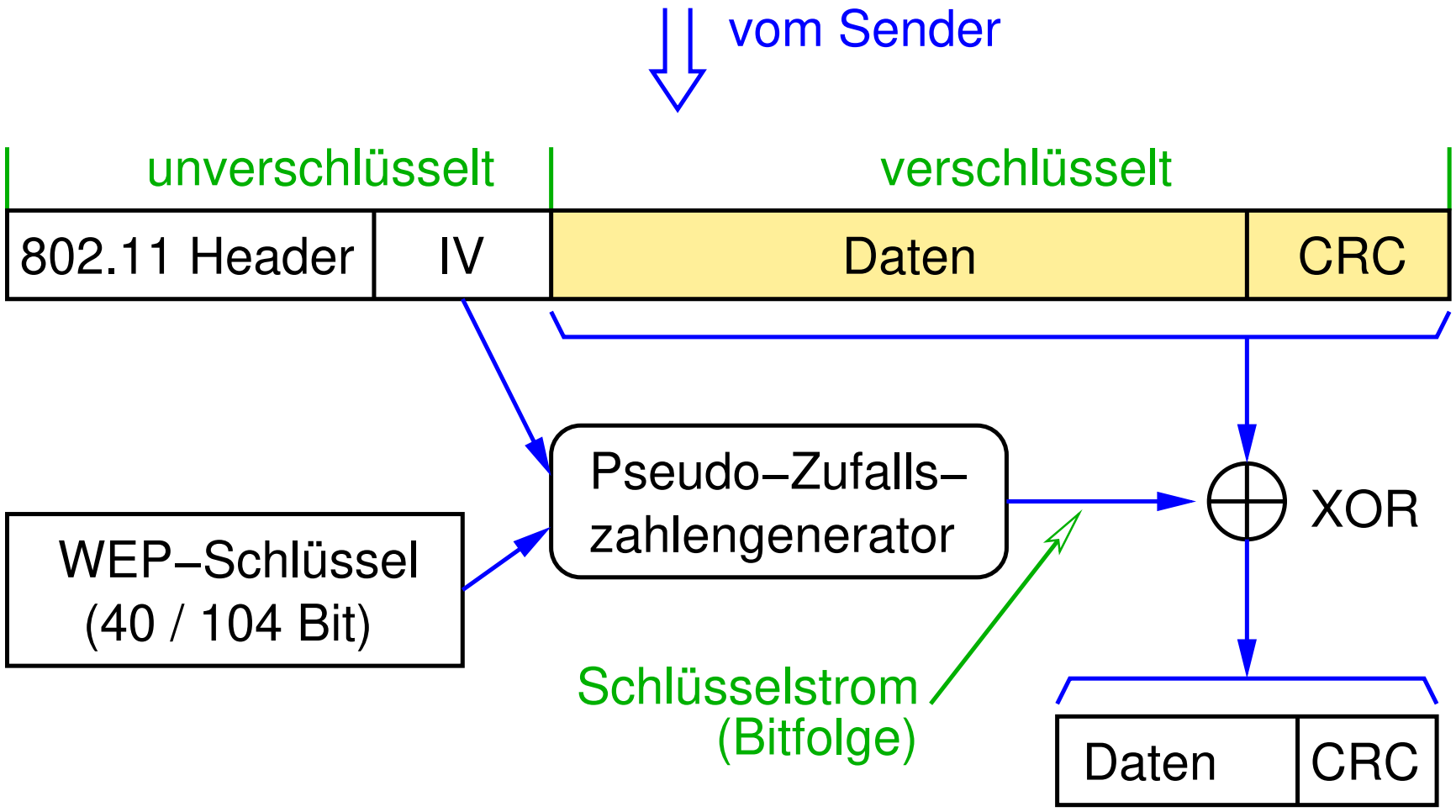
WEP: Funktionsweise

- Basis: symmetrische Verschlüsselung mit RC4 Stromchiffre
  - Daten werden mit Pseudozufalls-Bitfolge EXOR-verknüpft
  - Bitfolge kann aus Schlüssel und Initialisierungsvektor (IV) eindeutig bestimmt werden
  - Schlüssel (40 bzw. 104 Bit) muß allen Stationen bekannt sein
  - Initialisierungsvektor wird für jede Übertragung neu gewählt und (unverschlüsselt) mitübertragen
- Authentifizierung der Teilnehmer durch *Challenge-Response* - Protokoll

WEP-Verschlüsselung beim Sender



WEP-Entschlüsselung beim Empfänger



WEP: Schwachstellen

- Verschlüsselung ist angreifbar (Problem: Schlüsselerzeugung)
- Verschlüsselung erfolgt immer direkt mit WEP-Schlüssel
  - macht Schlüssel durch Kryptoanalyse angreifbar
- CRC ist bezüglich $\oplus$ linear $\Rightarrow$ Angreifer kann nach Manipulation der Daten verschlüsselten CRC neu berechnen
- IV ist zu kurz: wiederholt sich nach wenigen Stunden
  - wiederholte Verwendung desselben Schlüsselstroms
  - Schlüsselstrom kann durch Klartextangriff ermittelt werden
    - *Challenge-Response* - Protokoll bei Authentifizierung!
- WEP ist unsicher! $\Rightarrow$ WPA bzw. WPA2 verwenden!!!

IEEE 802.11i: verbesserte Sicherheitsstandards

- Bessere Verschlüsselung als WEP, sichere Integritätsprüfung
  - Ziel: schrittweiser Übergang unter Weiterverwendung vorhandener Hardware
  - daher Übergangslösung über Firmware-Update
    - ersetze WEP-Verschlüsselung durch TKIP
    - zusätzlich: Integritätsprüfung über Hash-Funktion
      - MIC: *Message Integrity Check*
  - endgültige Lösung (erfordert neue Hardware)
    - AES-CCMP (*Advanced Encryption Standard*)
- Verbesserte Authentifizierung (inkl. Schlüsselmanagement)
  - über Authentifizierungsserver (IEEE 802.1X, EAP)
  - oder über *Pre-Shared Key* (PSK)

WPA, WPA2: Quasi-Standard der Wi-Fi Alliance

- Die IEEE-Standardisierung dauerte zu lange ...
  - WPA entspricht (in etwa) Übergangslösung von IEEE 802.11i
  - WPA2 entspricht (in etwa) IEEE 802.11i
- Jeweils zwei Modi: *Personal* und *Enterprise*

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

Authentifizierung mit 802.1X und EAP

- 802.1X: Authentifizierung über einen zentralen Server
  - RADIUS-Server (*Remote Authentication Dial-In User Service*)
  - Vorteil: zentrale Administration des Zugangs

- EAP: *Extensible Authentication Protocol* (RFC 2284)
  - zum Austausch der Authentifizierungsnachrichten

Ablauf von Authentifizierung und Schlüsselaustausch

- Client muß gegenüber Authentifizierungsserver seine Identität nachweisen
  - Challenge/Response, z.B. mit Paßwort oder X.509 Zertifikat
- Dabei gleichzeitig: Aushandlung eines Schlüssels
  - PMK: *Pairwise Master Key*
  - wird vom Server auch an *Access Point* geschickt
- Client und *Access Point* bilden aus PMK einen nur ihnen bekannten Schlüssel für diese Sitzung
  - PTK (*Pairwise Transient Key*), für Punkt-zu-Punkt-Kommunik.
- *Access Point* sendet an Client einen Gruppenschlüssel
  - GTK (*Group Transient Key*), verschlüsselt mit PTK
  - für Broadcast- und Multicast-Kommunikation

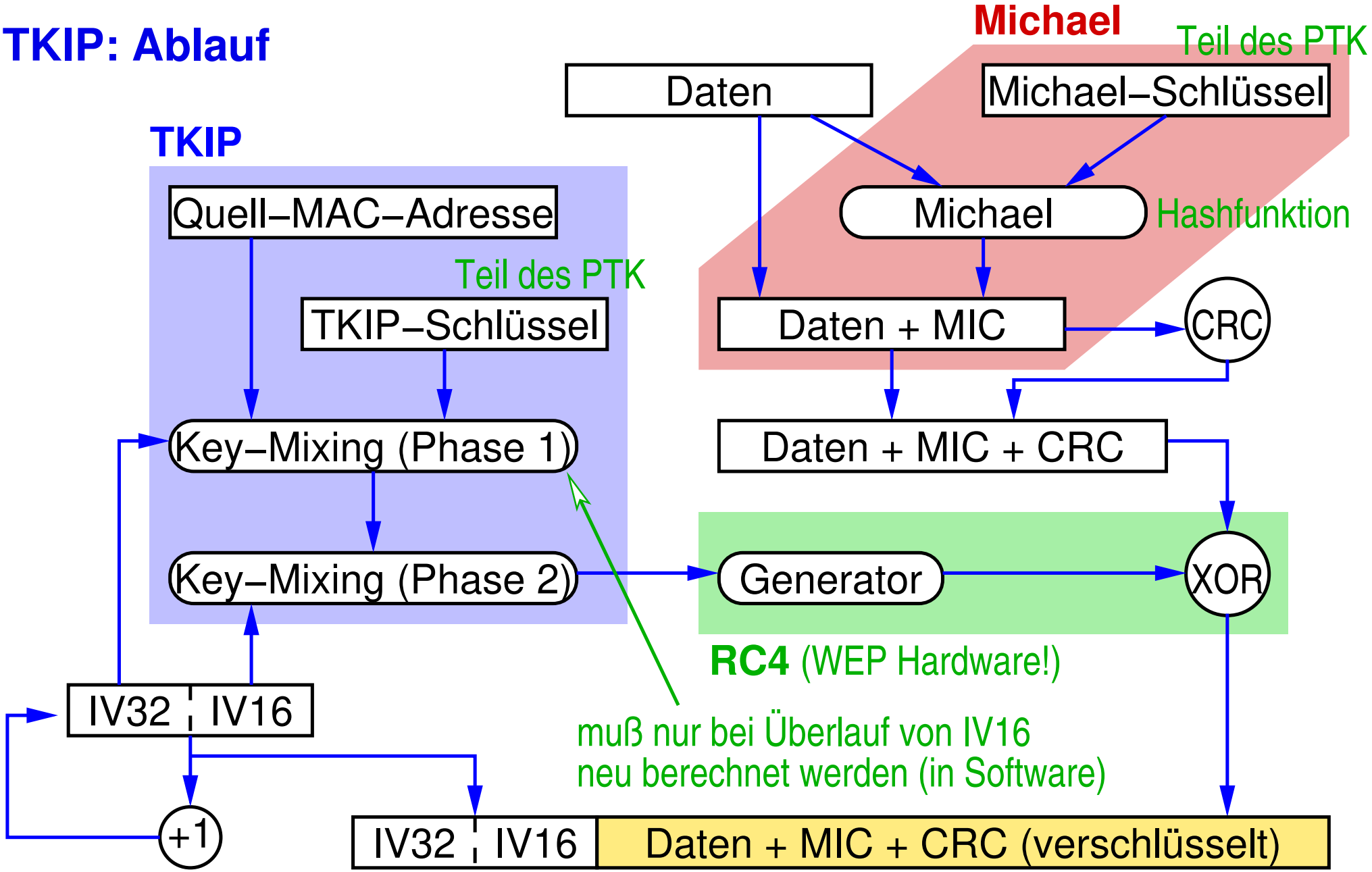
Authentifizierung mit PSK (*Pre-Shared Key*)

- PSK wird über Hashfunktion aus Passphrase und SSID gebildet
  - Passphrase wird auf allen Stationen manuell eingetragen
- PSK übernimmt die Rolle des PMK bei Auth. über 802.1X/EAP
  - d.h., Client und *Access Point* bilden aus PSK den PTK
    - unter Einbeziehung von MAC-Adresse und Zufallszahlen
- Nur, wenn Client und *Access Point* denselben PSK besitzen, erhalten sie denselben PTK und können kommunizieren
- PSK wird nicht für die Kommunikation verwendet
  - weniger Angriffspotential, um PSK zu ermitteln
  - trotzdem ist bei Kenntnis des PSK ein Entschlüsseln der Kommunikation anderer Clients möglich
    - Voraussetzung: Schlüsselaustauch wird abgehört

TKIP *Temporary Key Integrity Protocol*

- Übergangslösung für Verschlüsselung
  - Verwendung der WEP-Hardware mit neuer Software
- RC4 Verschlüsselung wie bei WEP
- Unterschiede:
  - Initialisierungsvektor (IV) mit 48 Bit
  - IV wird nach jedem Paket inkrementiert, Empfänger prüft Sequenz (Replayschutz)
  - 128 Bit langer TKIP-Schlüssel (Teil des PTK)
    - unterschiedliche Schlüssel für jeden Client
    - zusätzlich: Quell-MAC-Adresse fließt in RC4-Seed mit ein
  - Integritätsschutz (MIC): Hashfunktion mit Schlüssel (Michael)
    - getrennte Schlüssel je Übertragungsrichtung

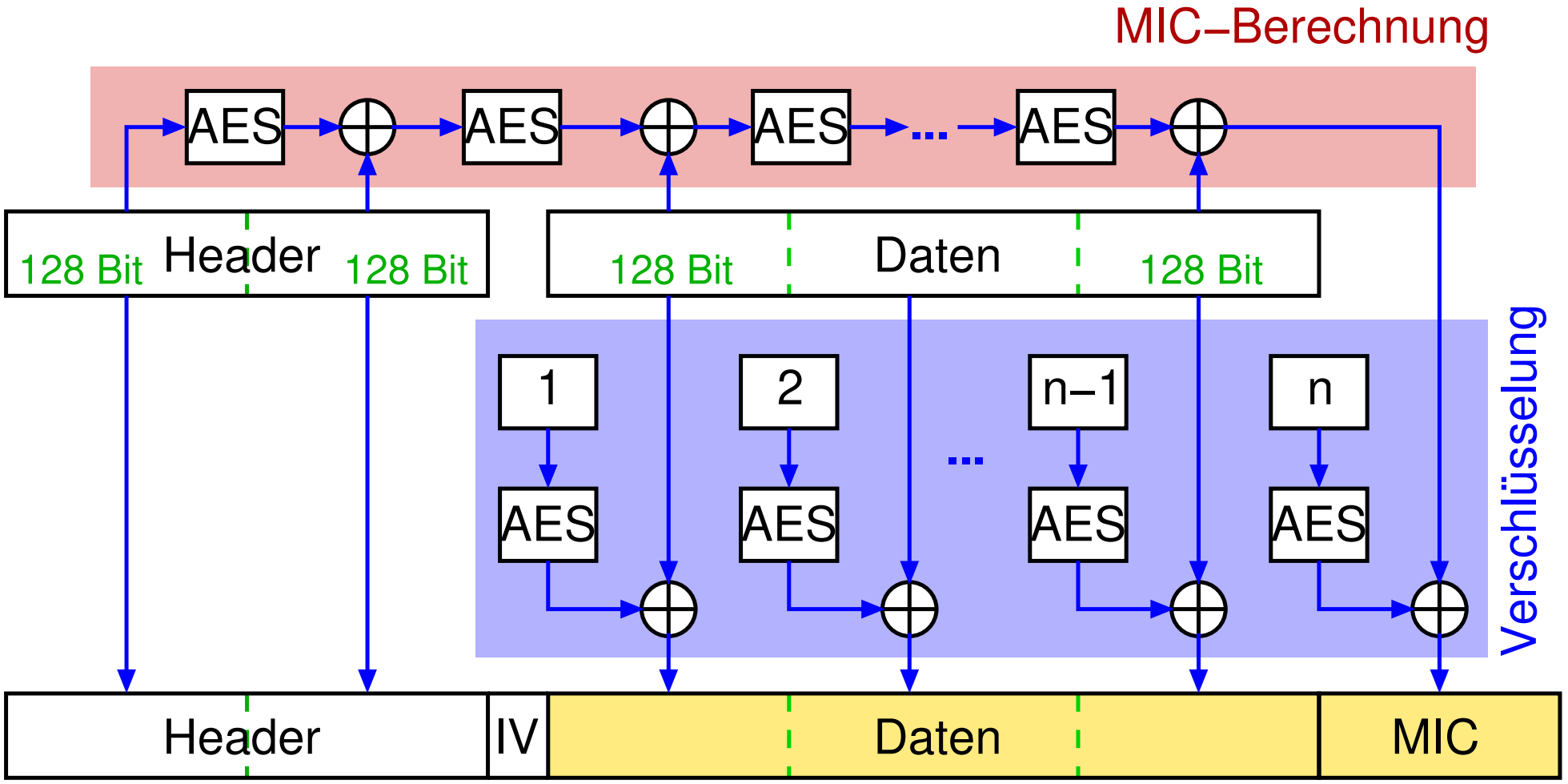
TKIP: Ablauf


Michael
Teil des PTK
Daten
Michael–Schlüssel
TKIP
Quell–MAC–Adresse
Michael
Hashfunktion
Teil des PTK
TKIP–Schlüssel
Daten + MIC
CRC
Key–Mixing (Phase 1)
Daten + MIC + CRC
Key–Mixing (Phase 2)
Generator
XOR
RC4 (WEP Hardware!)
IV32
IV16
muß nur bei Überlauf von IV16
neu berechnet werden (in Software)
+1
IV32
IV16
Daten + MIC + CRC (verschlüsselt)

AES-CCMP

- AES: vom NIST standardisiertes Verschlüsselungsverfahren
- AES-CCMP = AES *CTR/CBC-MAC Protocol*
  - AES im Zähler-Modus, MIC mittels *Cipher Block Chaining*
  - Integritätsprüfung (Datenteil + Teile des Headers) und Verschlüsselung (Datenteil + MIC)
    - ein gemeinsamer Schlüssel mit 128 Bit
  - benötigt neue Hardware
- 48 Bit Paketzähler mit Sequenzprüfung beim Empfänger
  - Sequenznummer geht mit Quell-MAC-Adresse in Verschlüsselung und Integritätsprüfung mit ein
  - Replayschutz

AES-CCMP: Ablauf (vereinfacht)



1 = Zähler

AES = AES–Verschlüsselung
(Quell–Mac und Sequenznummer IV gehen mit ein)

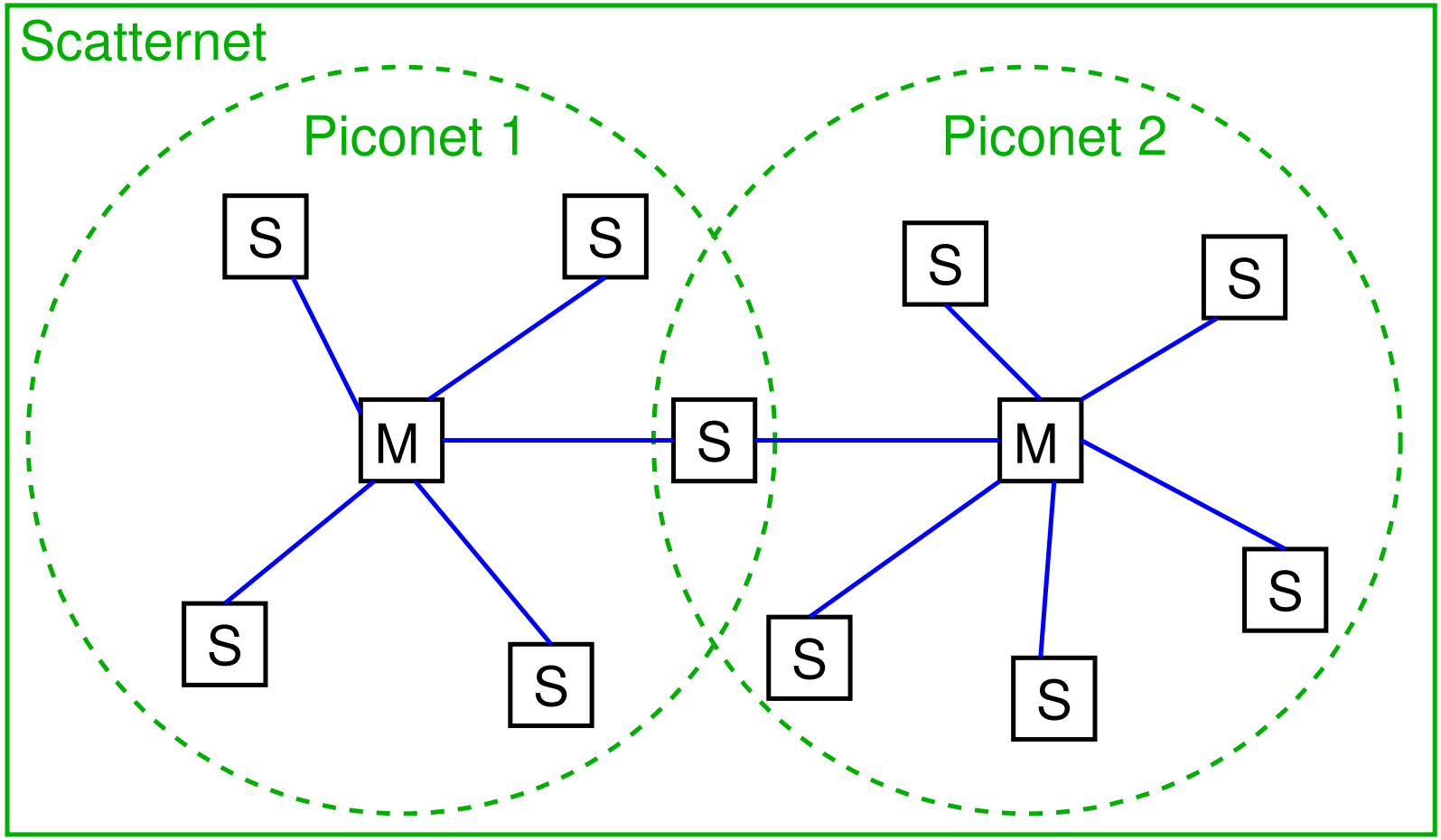
WPA / WPA2 / IEEE 802.11i: Fazit

- AES-CCMP: Sicherheit nach Stand der Technik
- TKIP und Michael: Zwischenlösung für alte Hardware
  - bessere Verschlüsselung als WEP
    - paarweise geheime Schlüssel + Gruppenschlüssel, regelmäßiger Schlüsselwechsel, längerer IV
  - verbesserter Integritätsschutz (Hashwert mit Schlüssel)
  - Replayschutz (durch IV als Sequenznummer)
- PSK: für private / kleine WLANs
  - einfache Nutzung, aber Zugangsberechtigung nicht mehr ohne weiteres entziehbar
- IEEE 802.1X / EAP: für professionellen Einsatz
  - zentrale, flexible Benutzerverwaltung

3.2.1 Bluetooth Classic

- Ursprüngliches Ziel: Verbindung von Mobiltelefonen mit anderen Geräten (PDA, ...)
  - geringer Stromverbrauch ist wesentlich
  - geringe Reichweite (10 m)
- Definition durch Gruppe mehrerer Unternehmen (1994 -)
  - untere Schichten in IEEE Standard 802.15 übernommen
- Bluetooth definiert Protokollstapel bis zur Anwendungsschicht
  - Zusammenarbeit der Geräte auf Anwendungsebene!
  - Profile für verschiedene Anwendungsbereiche
- benannt nach König Harald II. Blaatand (940-981)
  - vereinte Dänemark und Norwegen

Architektur eines Bluetooth-Netzes

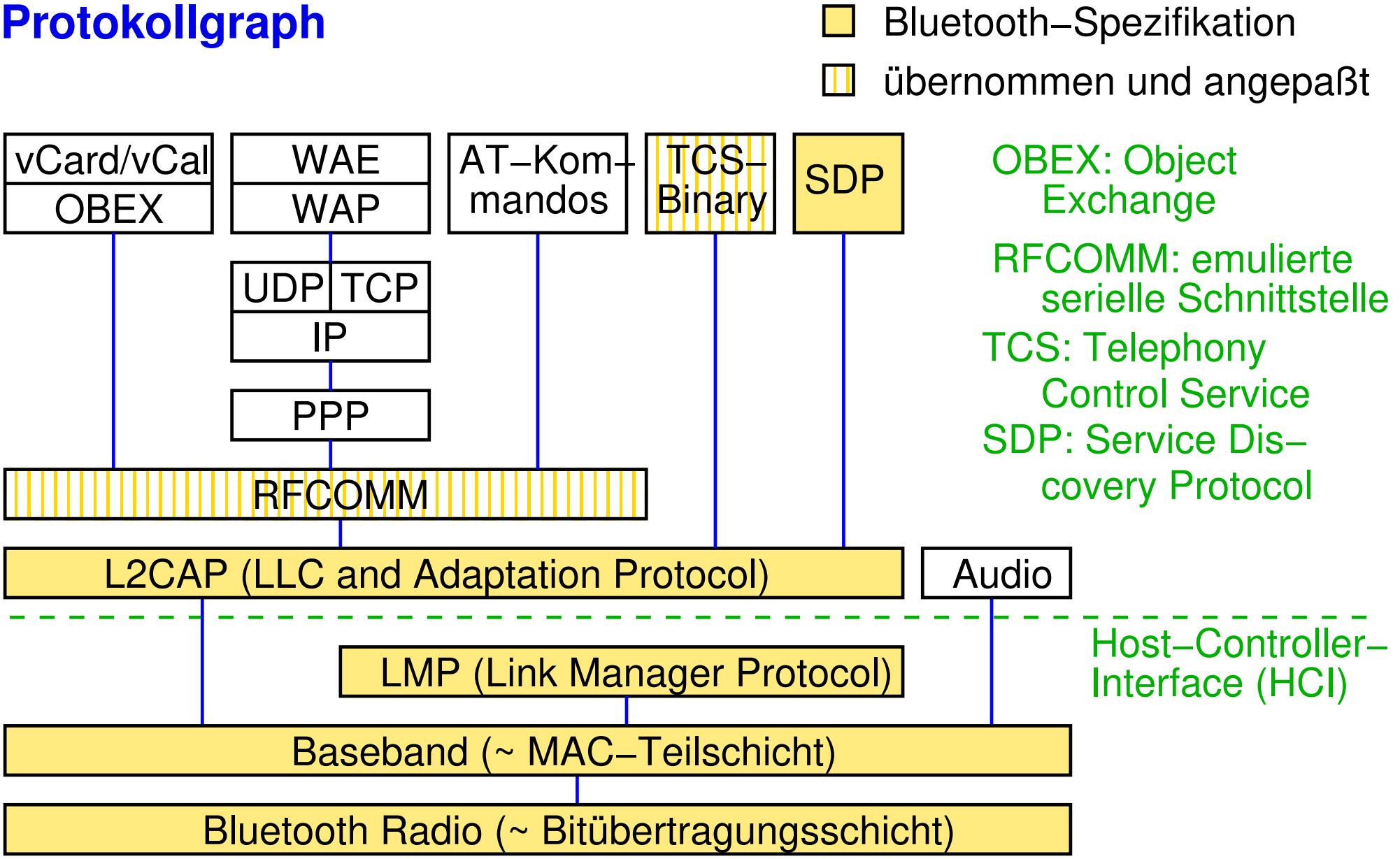


M: Master S: Slave

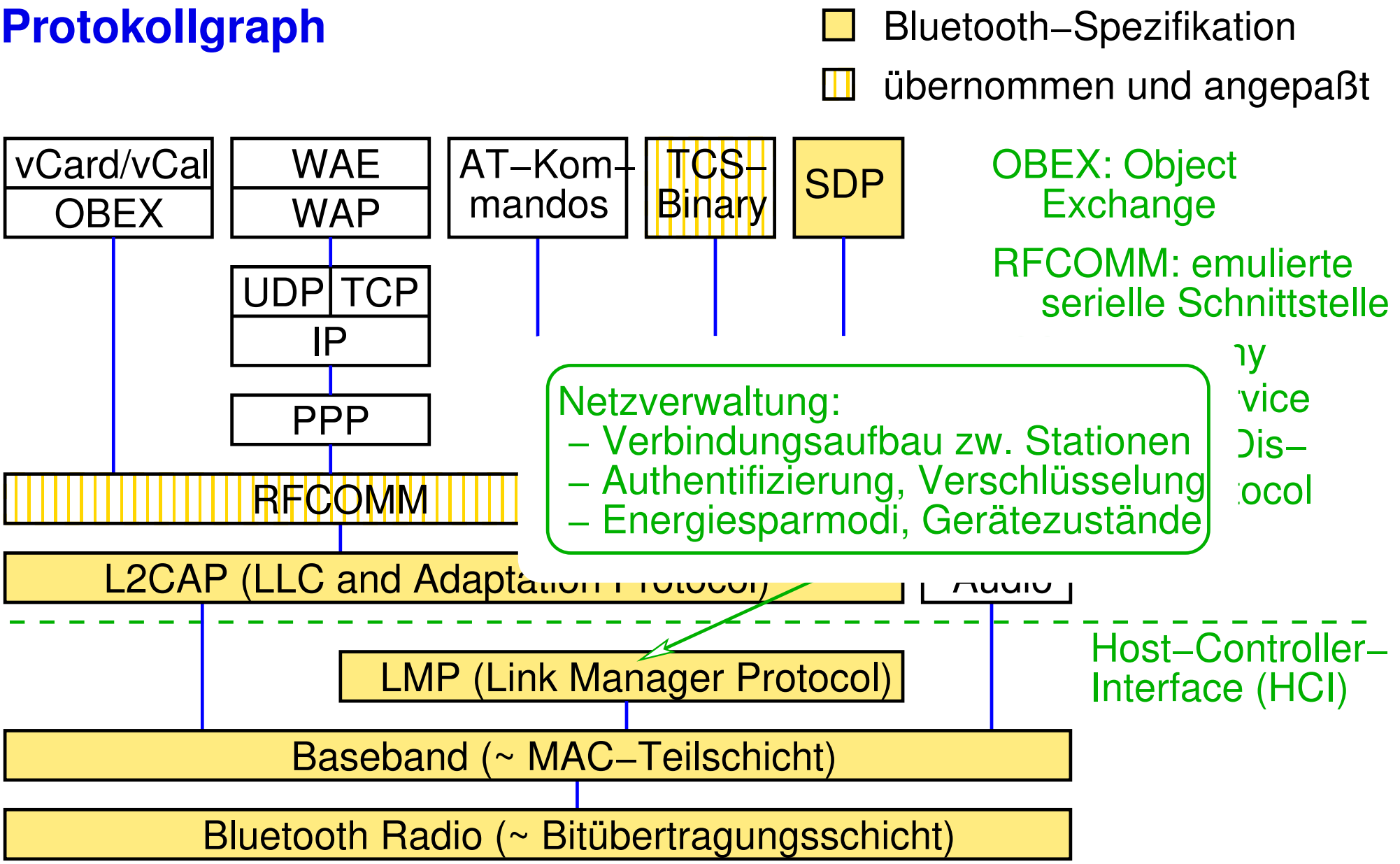
Architektur eines Bluetooth-Netzes ...

- Grundstruktur: Piconet
  - ein Master, bis zu 7 aktive Slaves
  - zusätzlich bis zu 255 „geparkte“ Slaves (Stromspar-Modus)
  - Medienzugang vollständig durch Master gesteuert (Zeitmultiplex)
- Mehrere Piconets können zu Scatternet verbunden werden
  - Verbindung über gemeinsamen Slave-Knoten als Bridge

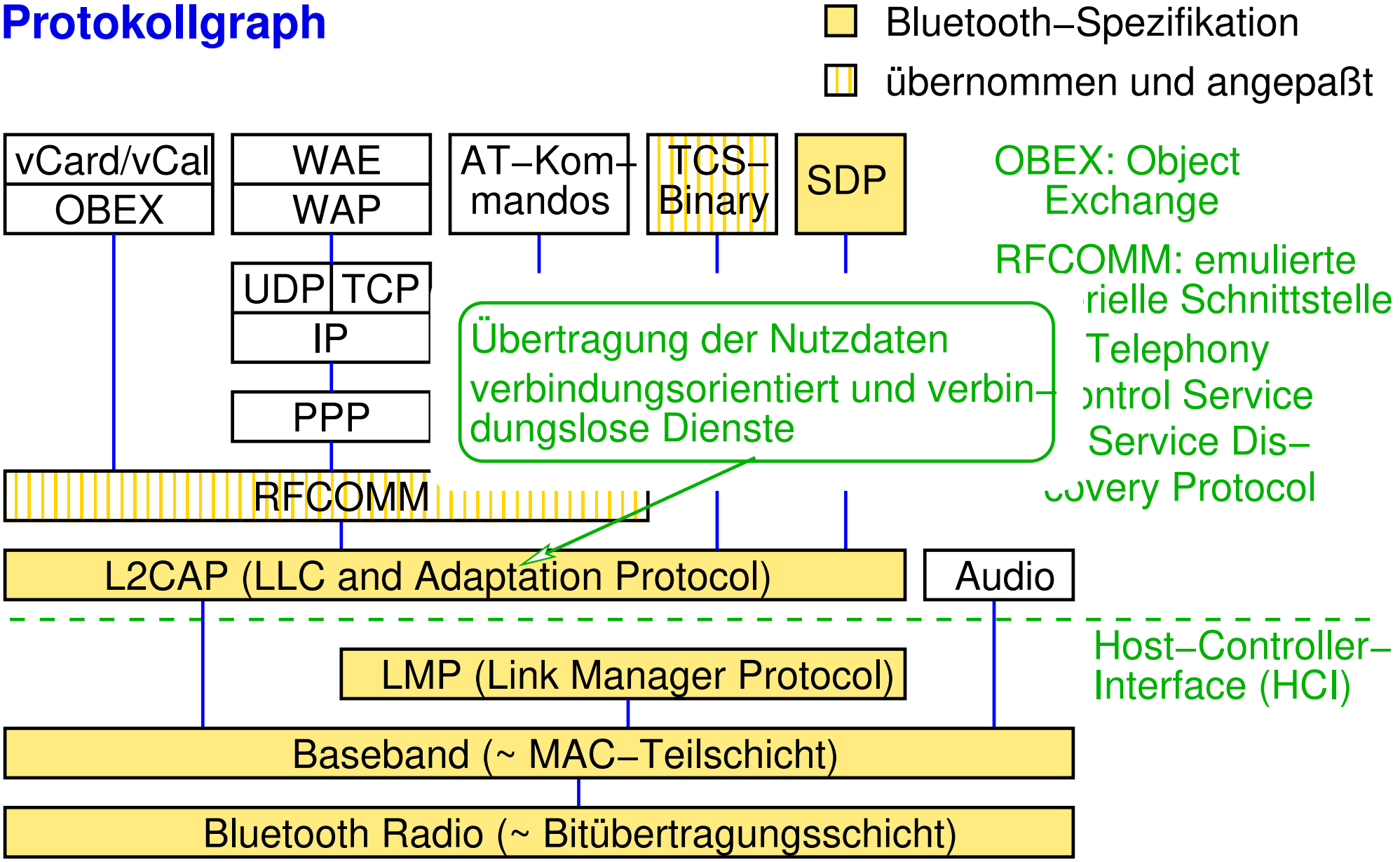
Protokollgraph



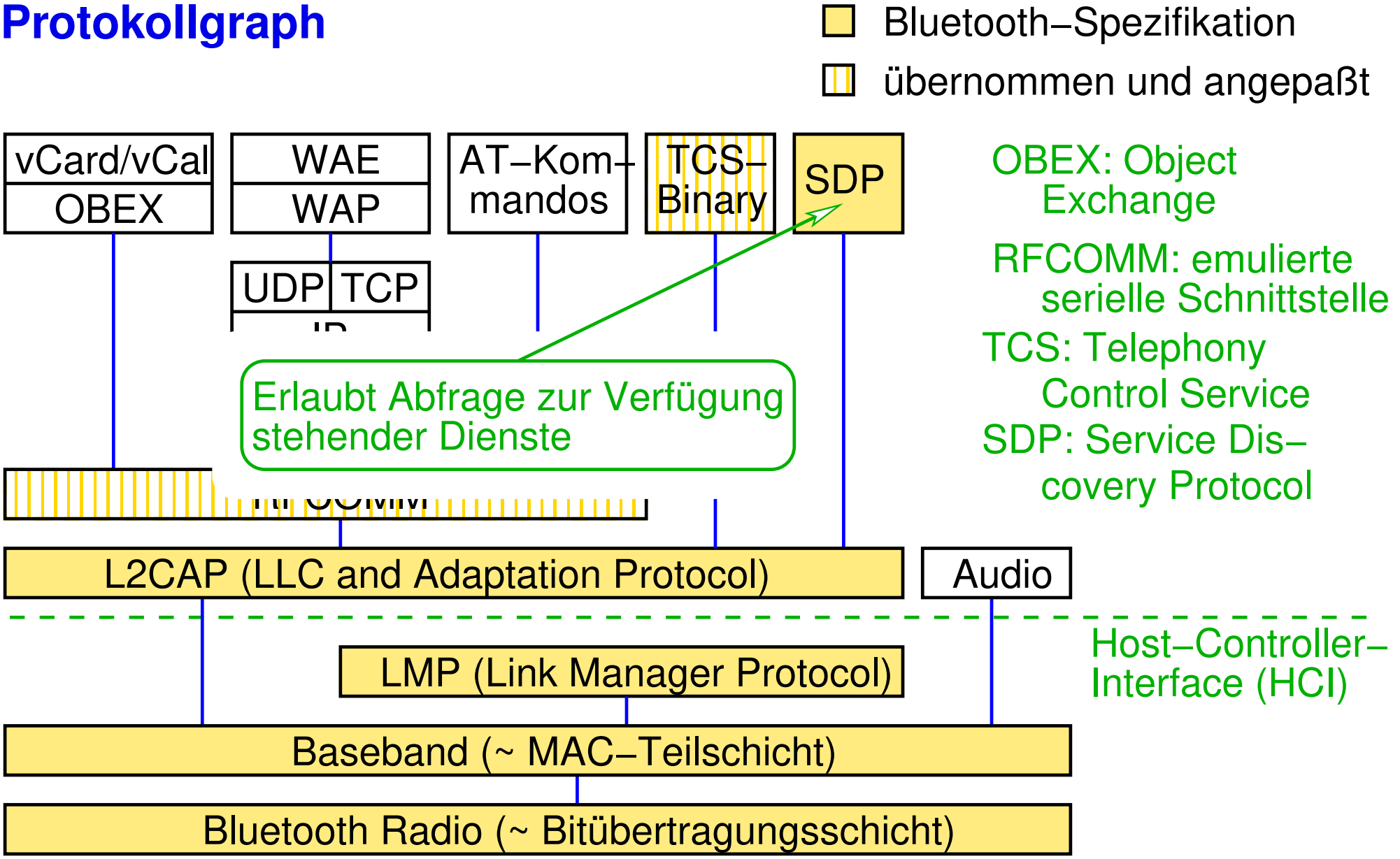
Protokollgraph



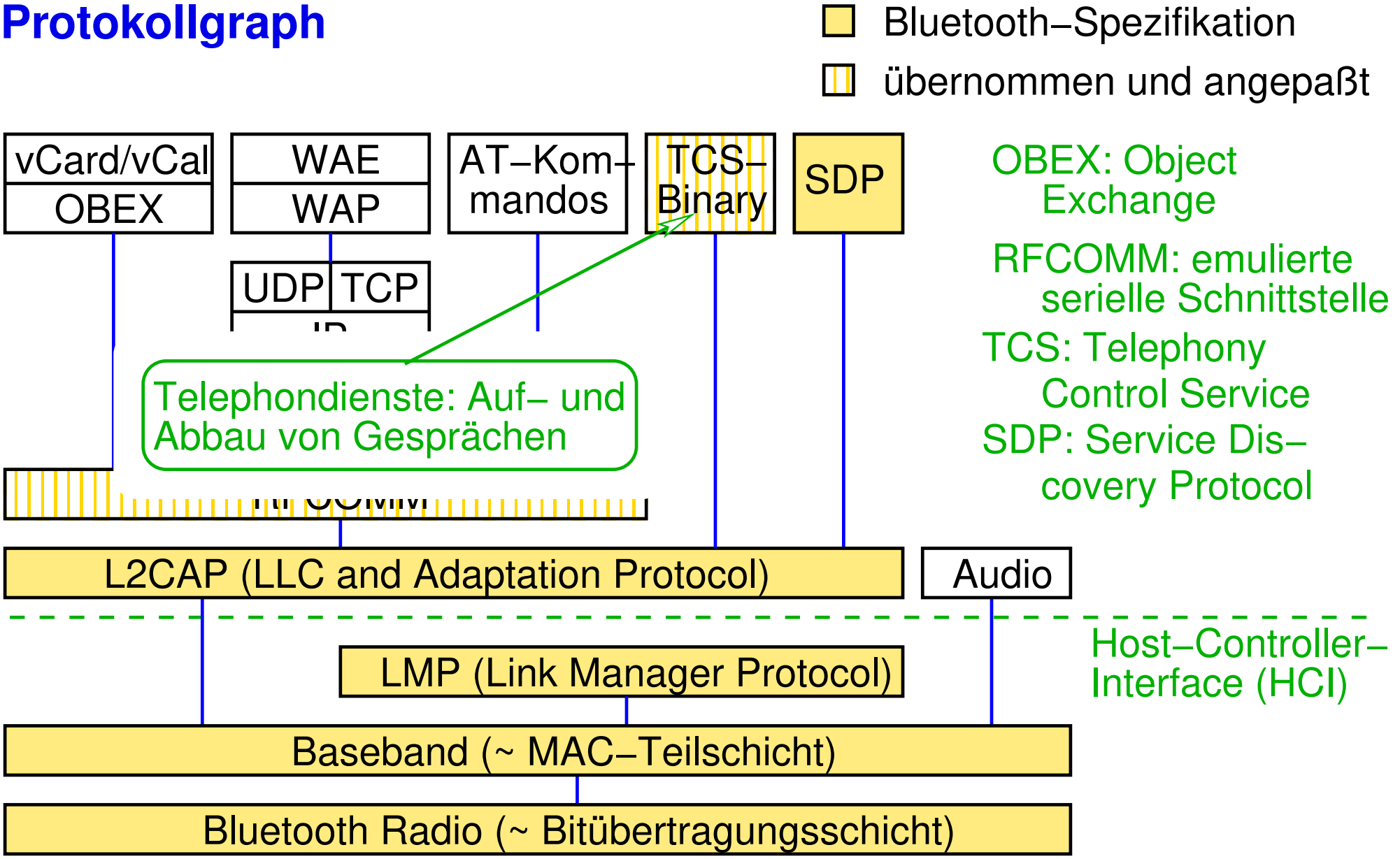
Protokollgraph



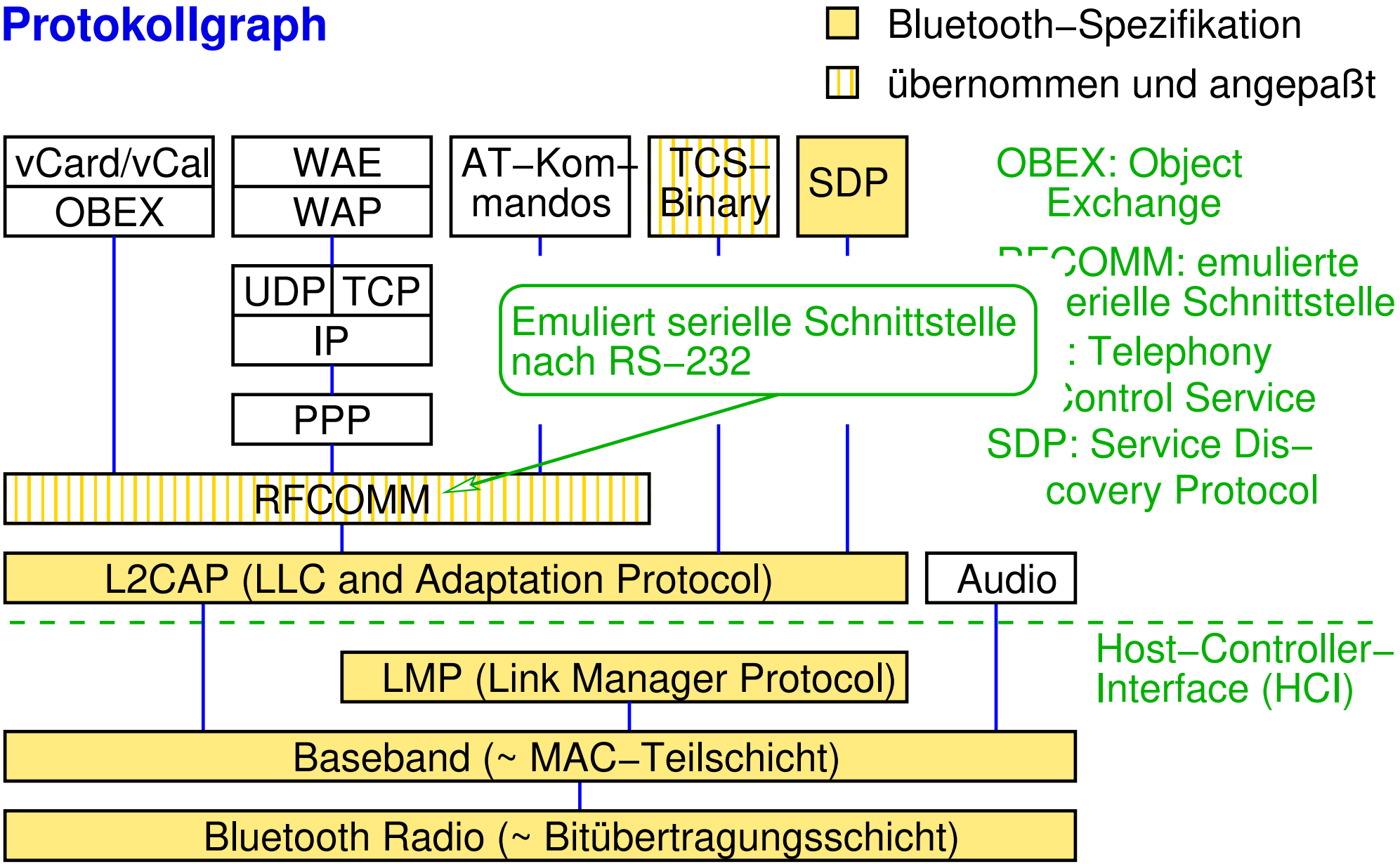
Protokollgraph



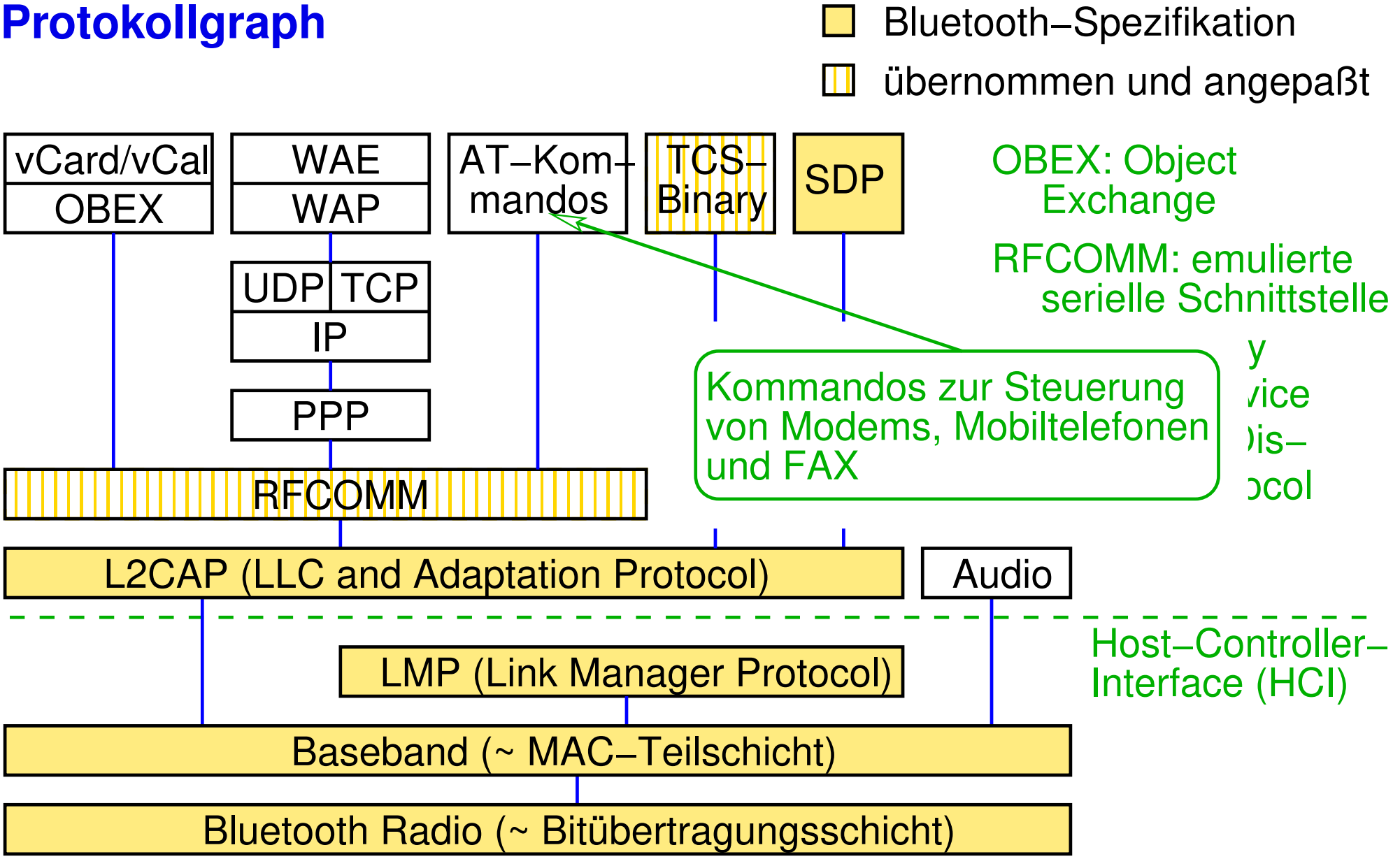
Protokollgraph



Protokollgraph



Protokollgraph



Funkschicht

- 2,4 GHz ISM Band
- 79 Kanäle á 1 MHz
- Frequenzsprungverfahren (FHSS)
  - 1600 Umschaltungen/s (alle 625 μs)
  - Sprungfolge wird vom Master vorgegeben
- Frequenzmodulation, Brutto-Datenrate 1 Mbit/s
- Auch 802.11b/g/n verwendet 2,4 GHz Band
  - gegenseitige Störungen!

Basisband-Schicht (MAC)

- Zeitmultiplex-Verfahren
  - Master beginnt Senden in geraden Zeitschlitzen
  - Slaves beginnen in ungeraden Zeitschlitzen
    - nur nach Erhalt eines Frames vom Master
  - Frames können 1, 3 oder 5 Zeitschlitze lang sein
    - 240 Bit Nutzdaten bei 1 Zeitschlitz
    - 2744 Bit bei 5 Zeitschlitzen
      - mehr als 5 * 240 Bit wegen Übergangszeit bei Frequenzwechsel und Frame-Header

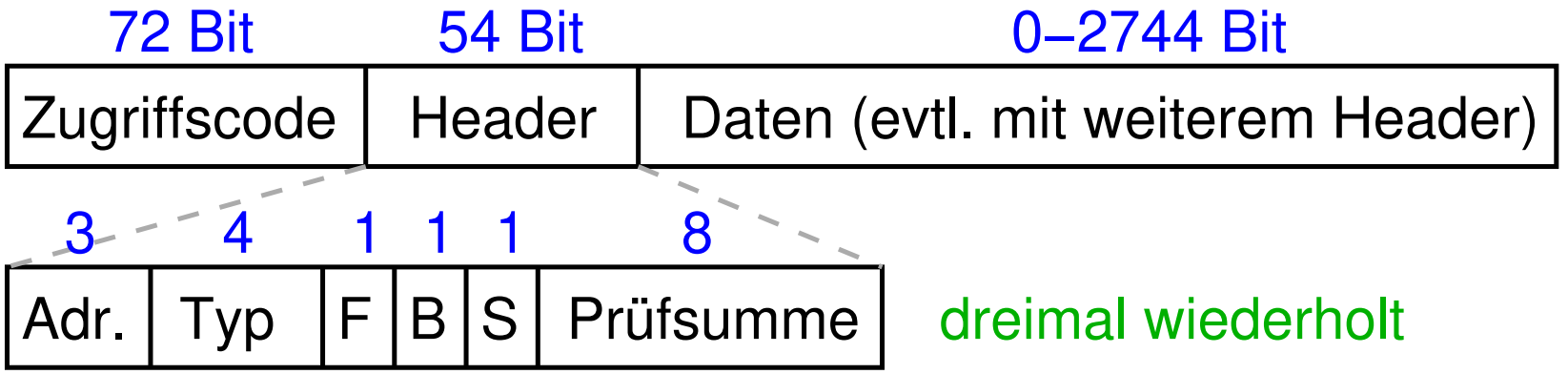
Basisband-Schicht (MAC)

- Übertragung über logische Kanäle (*Links*)
  - ACL (*Asynchronous Connectionless Link*)
    - paketvermittelte Daten, *best effort*
    - pro Slave max. 1 Link
  - SCO (*Synchronous Connection Oriented*)
    - für Echtzeitdaten (Telefonie)
    - feste Zeitschlitze für jede Richtung
    - Vorwärts-Fehlerkorrektur, keine Neuübertragung
      - Code-Raten 1/3, 2/3 und 3/3 (Nutz- / Gesamtdaten)
      - bei 1/3: Daten werden dreimal wiederholt, *Voting*
    - pro Slave max. 3 Links, 64000 Bit/s pro Link
    - Duplex-SCO-Link mit max. Redundanz lastet Netz aus!

L2CAP-Schicht

- *Logical Link Control Adaptation Protocol*
- Fragmentierung und Wiederzusammenbau von Paketen
  - Pakete bis 64 KB
- Multiplexen und Demultiplexen
  - Weitergabe von Paketen an höhere Protokolle
- Aushandlung / Verwaltung von Dienstgüte-Anforderungen
  - z.B. maximale Paketgröße

Frame-Format



- **Zugriffscode** identifiziert Master (d.h. Piconet)
- 3-Bit **Adresse** (7 Slaves + Broadcast durch Master)
- **Typ**: ACL, SCO, Polling, Fehlerkorrektur, Zeitschlitze, ...
- **F**: Flußkontrolle (Empfangspuffer ist voll)
- **B**: Bestätigung (ACK)
- **S**: Sequenzbit (*Stop-and-Wait*-Verfahren)

Sicherheit

- 3 Modi: keine Sicherheit, Sicherheit auf Diensteebene, Authentifizierung und Verschlüsselung auf Link-Ebene
- Bei erster Verbindungsaufnahme: *Pairing*
  - beide Geräte benötigen identische PIN (1-16 Bytes, fest installiert bzw. Benutzereingabe)
- Aus PIN werden Schlüssel berechnet: 8(!) - 128 Bit
- Authentifizierung und Verschlüsselung mit unterschiedlichen Chiffren (SAFER+ bzw. E0-Stromchiffre)
- Schwächen:
  - feste Geräteschlüssel möglich (für alle Verbindungen)
  - nur Geräte-, keine Benutzer-Authentifizierung
  - kein Replay-Schutz

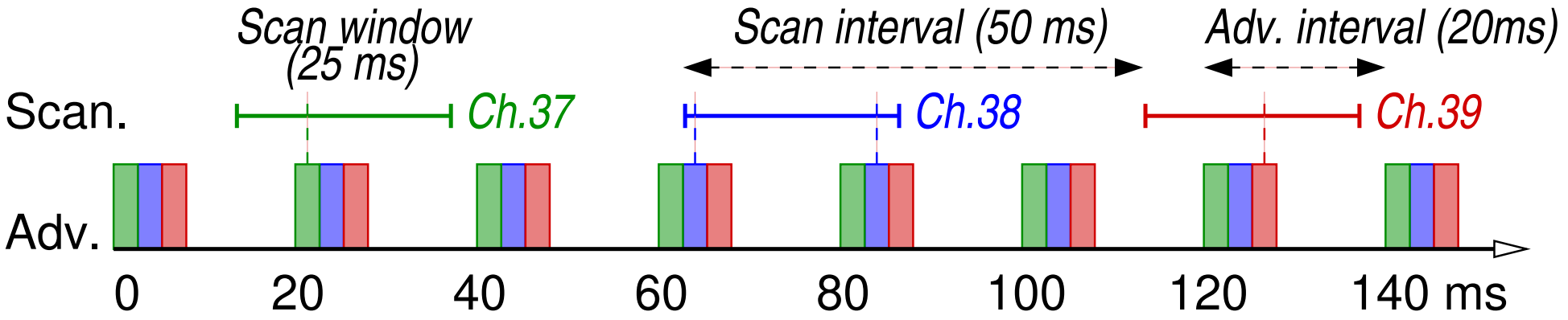
3.2.2 Bluetooth Smart (BT Low Energy, BT 4.x)

- Entwicklung seit 2001 durch Nokia, seit 2007 Bluetooth SIG
- Nicht kompatibel mit 2.x und 3.x, als Ergänzung
- Ziel: möglichst geringer Energieverbrauch, preisgünstig
- Kurze Nachrichten (max. 20 Byte), Datenrate max. 1 Mb/s
- Einfache Sterntopologie (keine Scatternets)
- Anwendungen z.B.:



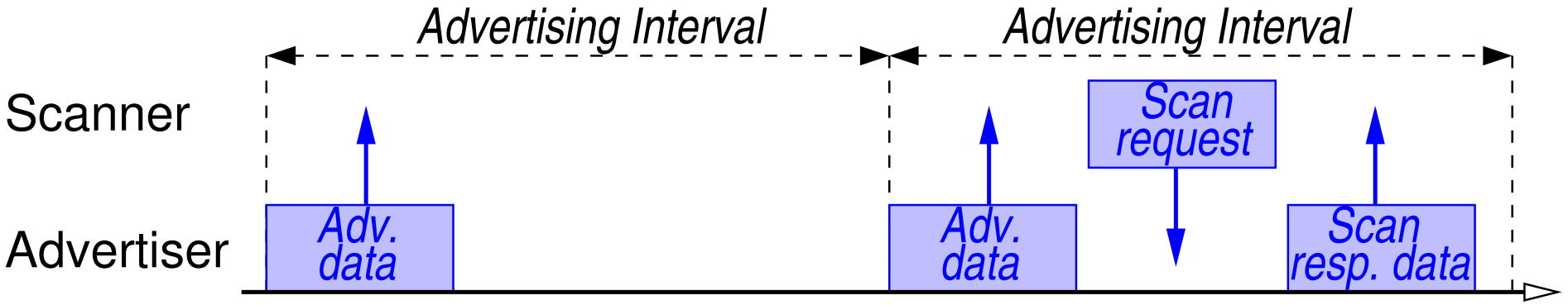

Sicherungsschicht

- Ziel: Funkgerät ist nur möglichst kurz eingeschaltet
  - Energieverbrauch: Empfangsbereitschaft ≈ Senden!
- *Advertising* und *Scanning*
  - Peripheriegerät (*Advertiser*) sendet periodisch Broadcasts
    - auf 3 reservierten Kanälen
    - Intervall: 20ms - 10,24s; mit oder ohne Nutzdaten / Adresse
  - *Scanner* hört Kanäle periodisch ab



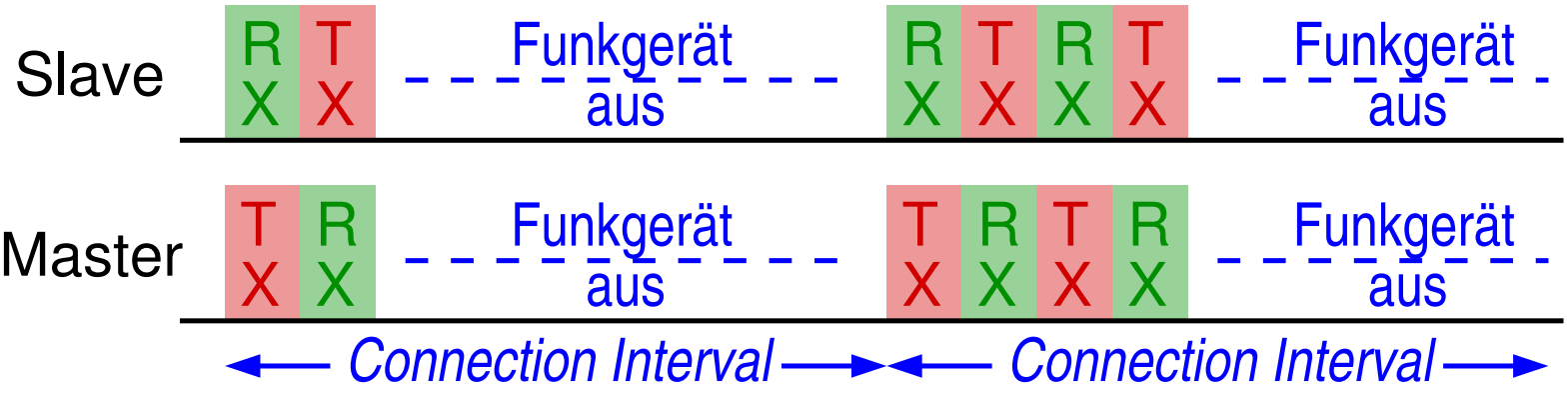
Sicherungsschicht ...

- Aktives Scannen
  - *Advertiser* bleibt nach Versenden der *Advertising*-Daten noch kurz empfangsbereit
  - *Scanner* kann so noch weitere Daten anfordern
  - aber: keine Übertragung von Nutzdaten zum *Advertiser*



Sicherungsschicht ...

- Verbindungsaufbau
  - erlaubt weiteren Datenaustausch, insbes. vom *Scanner* zum *Advertiser*
  - *Scanner* antwortet auf *Advertising*-Paket mit *Connection Request*, u.a. mit
    - Sprungfolge für *Frequency Hopping* (37 Kanäle)
    - *Connection Interval*: wann wird Funkgerät eingeschaltet?



  - Verschlüsselung möglich (bis 128 Bit AES)

Attribut-Protokoll und Attribut-Profil

- Server geben Attribute an Clients bekannt
  - Größe max. 20 Bytes
- Attribute werden über UUIDs (16 bzw. 128 Bit) identifiziert
- Operationen:
  - *Discover*/*Find*, Lesen, Schreiben, Benachrichtigung
- *Generic Attribute Profile*: höhere Abstraktion
  - Profil definiert Menge von *Services*
    - z.B. *Heart Rate Profile*: *Heart Rate* + *Dev. Info. Service*
  - *Service* enthält *Characteristics*
  - *Characteristic* enthält Wert und Metadaten (Eigenschaften, Beschreibung)

WLAN (IEEE 802.11)

- LLC-Teilschicht identisch zu Ethernet
- Ad-hoc und Infrastruktur-Modus
- Spreizbandtechnik
  - *Frequency Hopping*, *Orthogonal Frequency Division Multiplexing*, *Direct Sequence*
  - Ziel: Reduzierung der Störempfindlichkeit
- 802.11b: Überlappende Kanäle im 2,4 GHz ISM-Band
- Zwei MAC Varianten:
  - verteilte Kontrolle: CSMA/CA-Protokolle (MACAW)
  - zentrale Kontrolle: Zuteilung von Zeitschlitzen

WLAN (IEEE 802.11)

- *Hidden / Exposed Station* Probleme
- MACAW
  - MACA: RTS / CTS-Protokoll
    - Reservierung des Mediums für bestimmte Zeit (NAV)
  - MACAW: Einführung von Bestätigungsframes
- IFS zur Priorisierung von Frameklassen
- Sicherheit:
  - WEP: veraltet, kein ausreichender Schutz
  - WPA und v.a. WPA2 bieten gute Sicherheit
- Aktuell: IEEE 802.11n, MIMO-System, max. 600 Mbit/s; bzw. 802.11ac, MIMO-System, max. 1.69 Gbit/s pro Verbindung

Bluetooth

- Vernetzung mobiler Geräte (Handy, PDA), Kabelersatz
- Piconet: Master + max. 7 aktive Slaves
- definiert vollständigen Protokollstapel + Anwendungsprofile
- Funkschicht: 2,4 GHz ISM Band, Frequenzsprungverfahren
- MAC: Zeitmultiplex, zentral durch Master gesteuert
- Vorwärtsfehlerkorrektur, hohe Redundanz
- Sicherheit: optional, ausreichend, aber (theoretisch) angreifbar
- Bluetooth Smart: energiesparende Datenübertragung von „Sensorknoten“