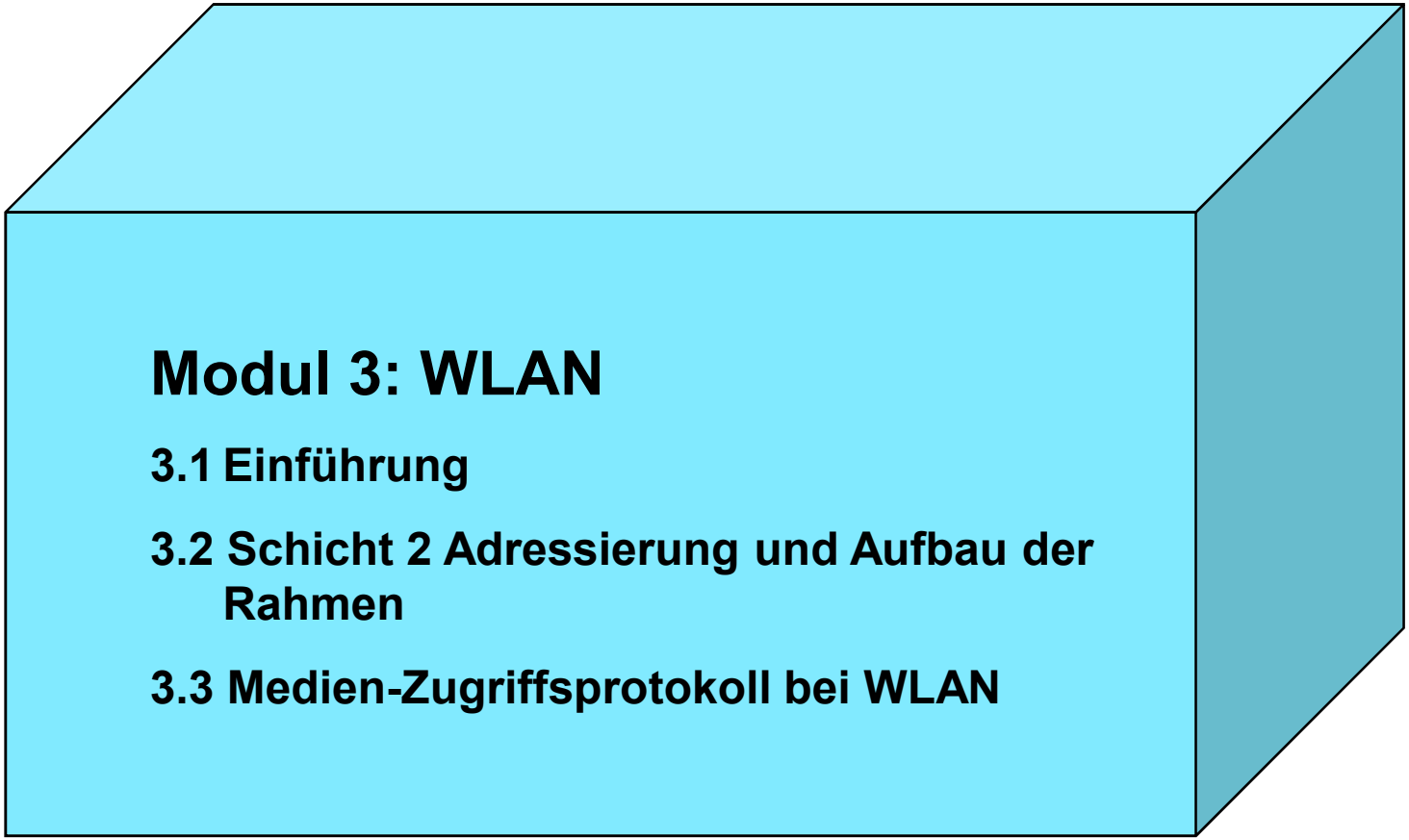
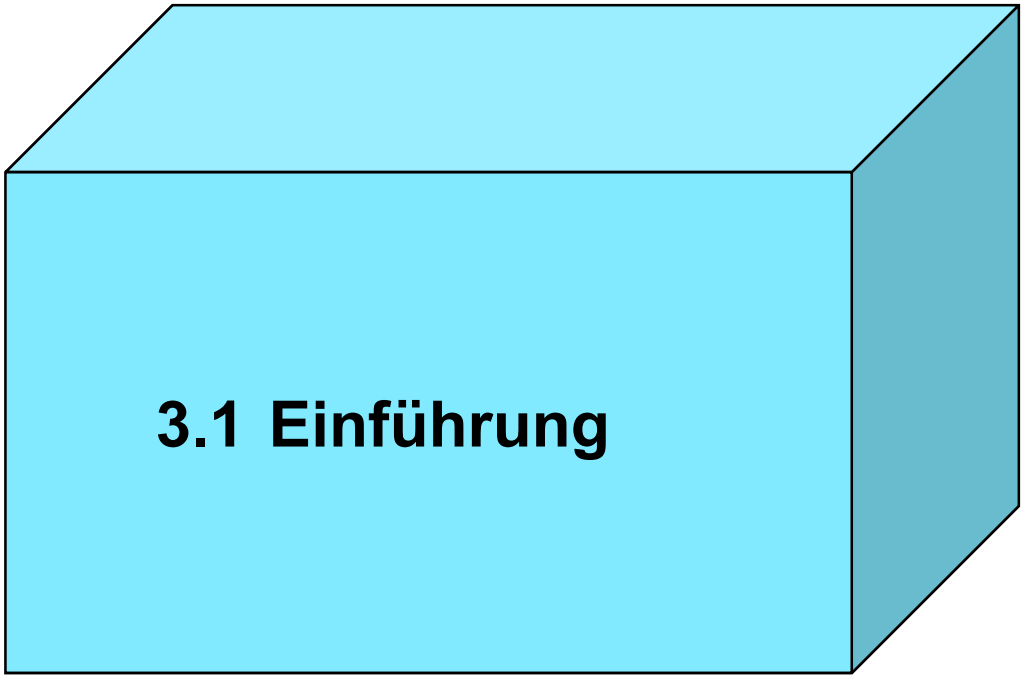


Modul 3: WLAN

3.1 Einführung

3.2 Schicht 2 Adressierung und Aufbau der Rahmen

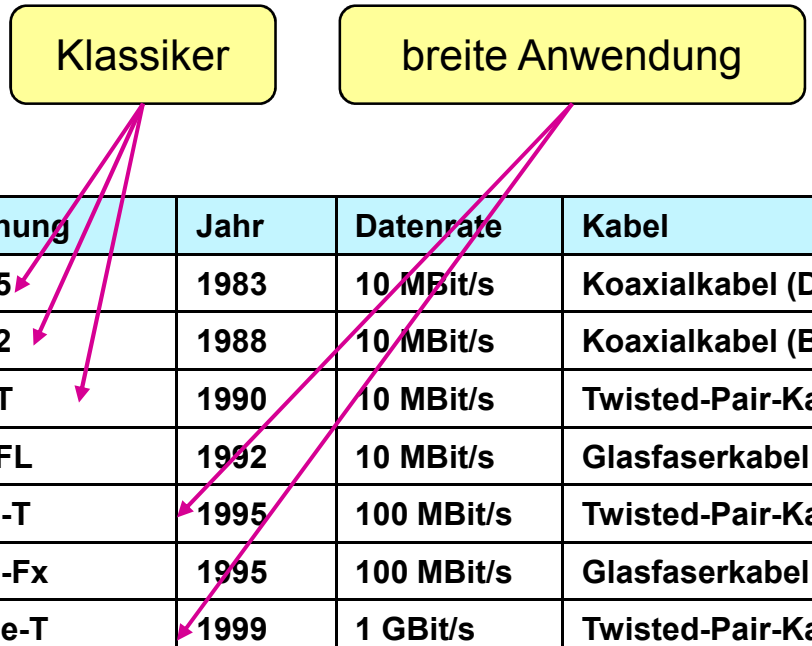
3.3 Medien-Zugriffsprotokoll bei WLAN


3.1 Einführung

Wichtige Technologien im LAN Bereich

- IEEE Standard 802.3 (Ethernet):
  - Kabelgebundene Übertragung von Daten in lokalen Netzen
  - Mit verschiedenen Kabeltypen/ Varianten in der Schicht 1 werden unterschiedliche Bitraten erzielt.
  - Im ursprünglichen Standard wurde als Topologie eine Busstruktur mit dezentralem Medienzugriffsverfahren verwendet.
  - Inzwischen ist eine sternförmige Verkabelung mit einem „Switch“ üblich.
- IEEE Standard 802.11 (WLAN = wireless LAN):
  - Drahtlose Übertragung von Daten in lokalen Netzen
  - Mit verschiedenen Übertragungsverfahren/ Varianten der Schicht 1 sind mittlerweile Bitraten bis zu 6,9 Gbit/s möglich.
  - Der Zugriff der Teilnehmer auf den „Funkkanal“ erfolgt nach wie vor mit einem dezentralen, stochastischen Medienzugriffsverfahren, das vom Zugriffsverfahren des Ethernet Standards abgeleitet wurde.

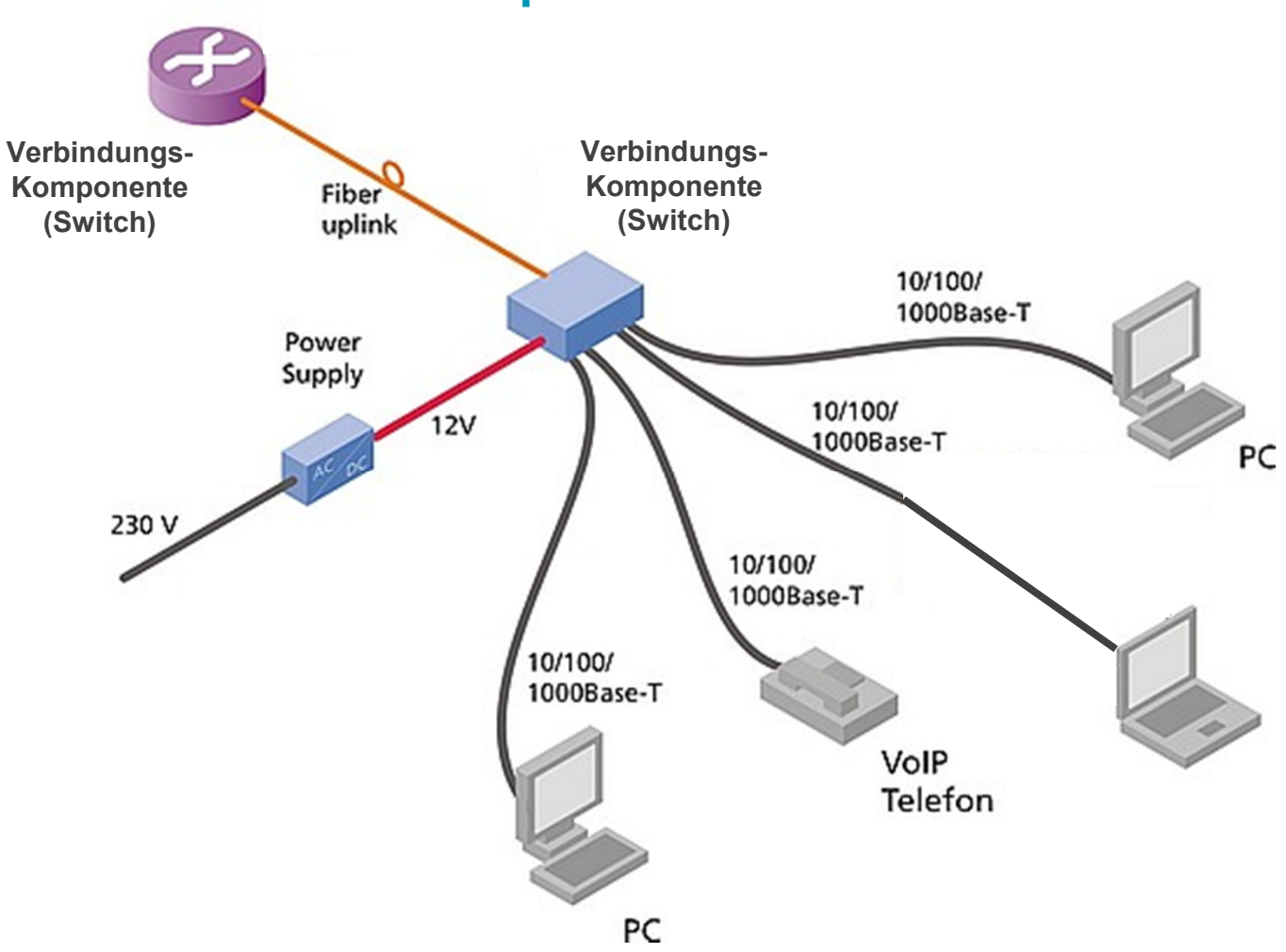
Überblick Ethernet-Standards (IEEE 802.3)



IEEE-Standard	Bezeichnung	Jahr	Datenrate	Kabel
802.3, Clause 8	10Base-5	1983	10 MBit/s	Koaxialkabel (DIX/AUI), 500 m
802.3, Clause 2	10Base-2	1988	10 MBit/s	Koaxialkabel (BNC), 185 m
802.3, Clause 14	10Base-T	1990	10 MBit/s	Twisted-Pair-Kabel (RJ-45), 100 m
802.3, Clause 18	10Base-FL	1992	10 MBit/s	Glasfaserkabel
802.3, Clause 24	100Base-T	1995	100 MBit/s	Twisted-Pair-Kabel (RJ-45), 100 m
802.3, Clause 26	100Base-Fx	1995	100 MBit/s	Glasfaserkabel
802.3, Clause 36	1000Base-T	1999	1 GBit/s	Twisted-Pair-Kabel (RJ-45), 100m
802.3, Clause 52	10GBase-SR	2002	10 GBit/s	Glasfaserkabel (SR = Short Range, „100m“)
802.3, Clause 55	10GBase-T	2006	10 GBit/s	Twisted-Pair-Kabel über 100m
IEEE 802.3ba-2010	40GbE 100GbE	2010	40 GBit/s 100 GBit/s	verschiedene physische Realisierungen

...

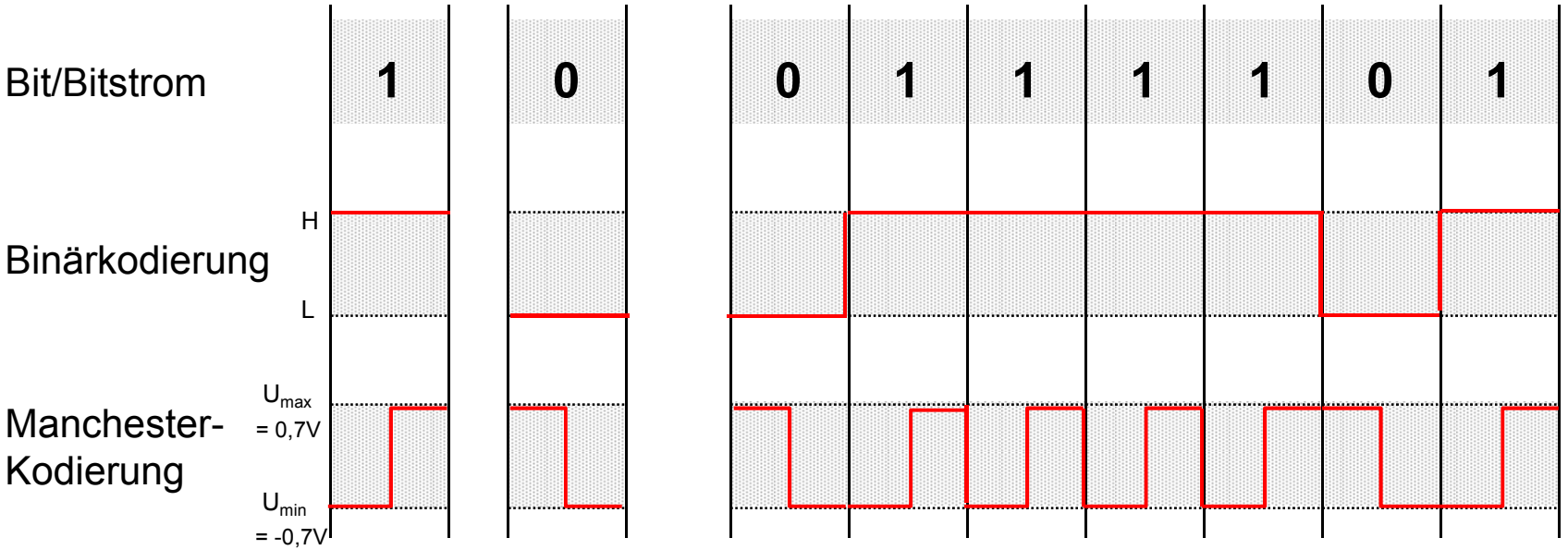
Beispiel-Architektur: LAN



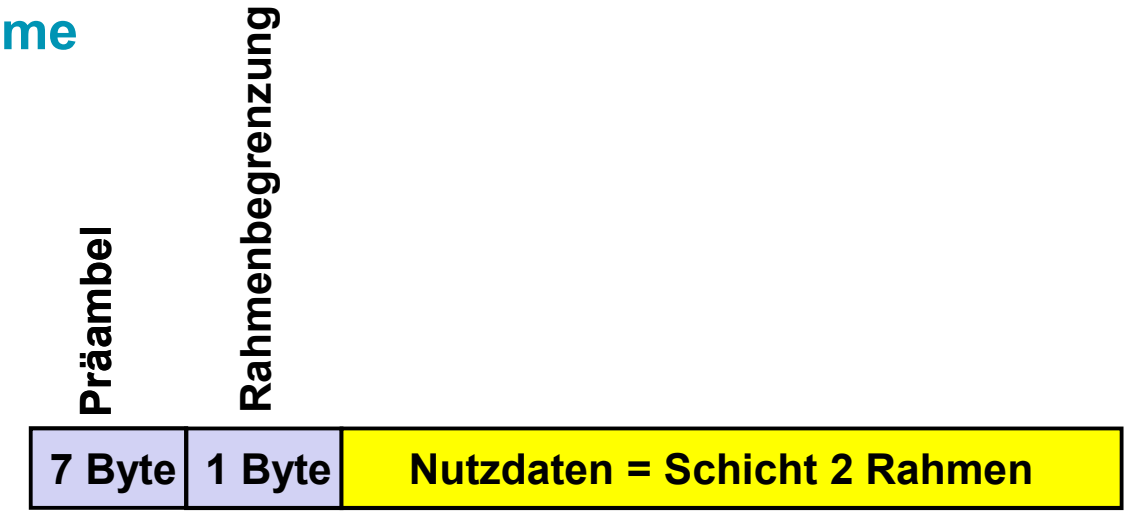
Quelle: http://www.microsens.com/de/produkte/kategorie/desktop-switches/gigabit-ethernet-switches/serie/Serie/show/gigabit-ethernet-5-port-office-switch-opt-managebar-526/

Beispiel: Bits als „übertragbare“ Signale

Manchester-Kodierung bei 10 Base T (= 10 Mbit/s Ethernet)



Ethernet Frame

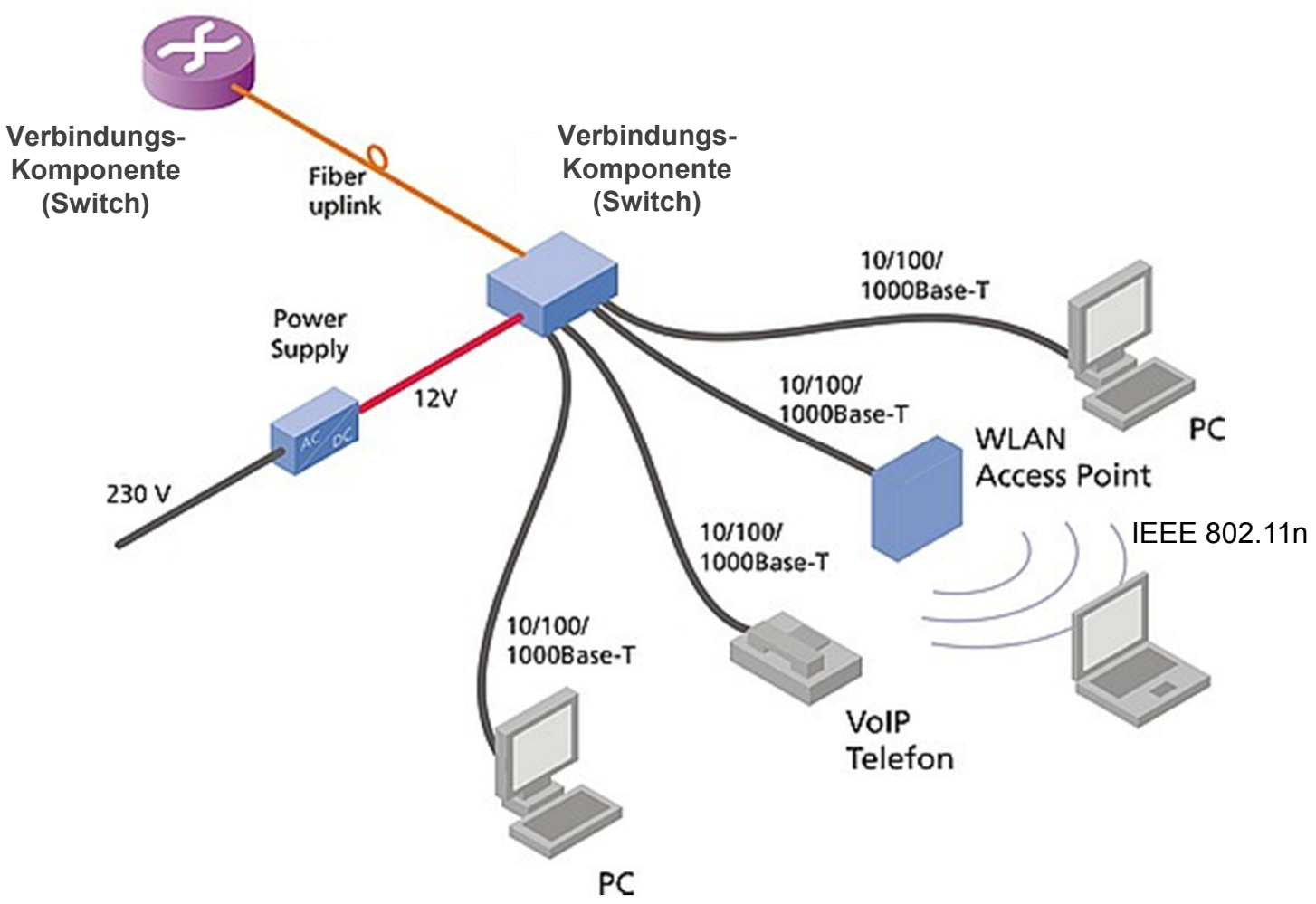


- **Präambel: Bitsequenz 10101010 1010 … (für Synchronisationszwecke)**
- **Rahmenbegrenzung (Start of Frame Delimiter): 10101011**

Überblick IEEE 802.11 WLAN-Standards

IEEE-Standard	Ursprüngliche Bezeichnung	MIMO	Datenrate	Frequenzbereich/ Bandbreite
802.11, Clause 16	IEEE 802.11	1x1	2 Mbit/s	2,4 GHz
802.11, Clause 17	IEEE 802.11b	1x1	11 Mbit/s	2,4 GHz
802.11, Clause 18	IEEE 802.11a	1x1	54 Mbit/s	5,0 GHz/ 20 MHz
802.11, Clause 19	IEEE 802.11g	1x1	54 Mbit/s	2,4 GHz/ 20 MHz
802.11, Clause 20, HT	IEEE 802.11n	1x1	65 Mbit/s 150 Mbit/s	2,4 oder 5,0 GHz/ 20 MHz 2,4 oder 5,0 GHz/ 40 MHz
802.11, Clause 20, HT	IEEE 802.11n	2x2	300 Mbit/s	2,4 oder 5,0 GHz/ 40 MHz
802.11, Clause 20, HT	IEEE 802.11n	3x3	450 Mbit/s	2,4 oder 5,0 GHz/ 40 MHz
802.11, Clause 20, HT	IEEE 802.11n	4x4	600 Mbit/s	2,4 oder 5,0 GHz/ 40 MHz
802.11, VHT	IEEE 802.11ac	1x1 - 8x8	86 Mbit/s - 6,9 Gbit/s	5,0 GHz/ 20 - 160 MHz
802.11, VHT	IEEE 802.11ad		6,7 Gbit/s	60 GHz

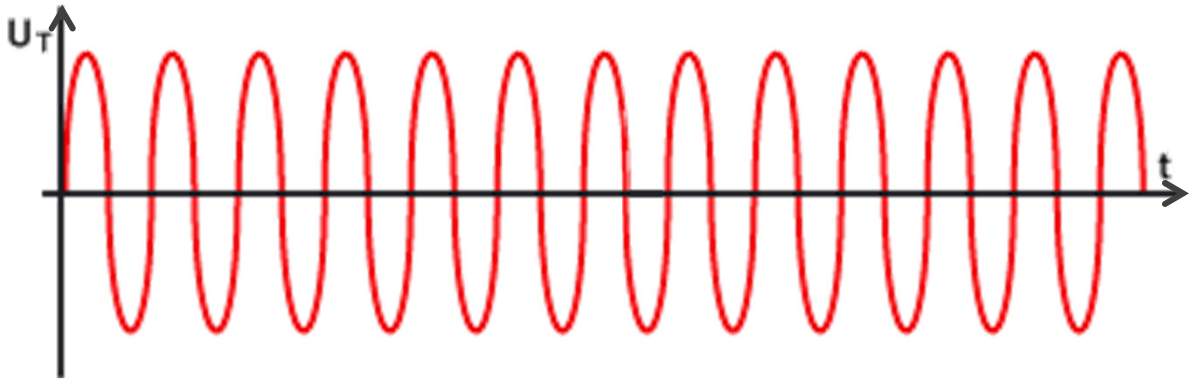
Beispiel-Architektur: LAN und WLAN



Quelle: http://www.microsens.com/de/produkte/kategorie/desktop-switches/gigabit-ethernet-switches/serie/Serie/show/gigabit-ethernet-5-port-office-switch-opt-managebar-526/

Bitübertragungsschicht in WLAN (1)

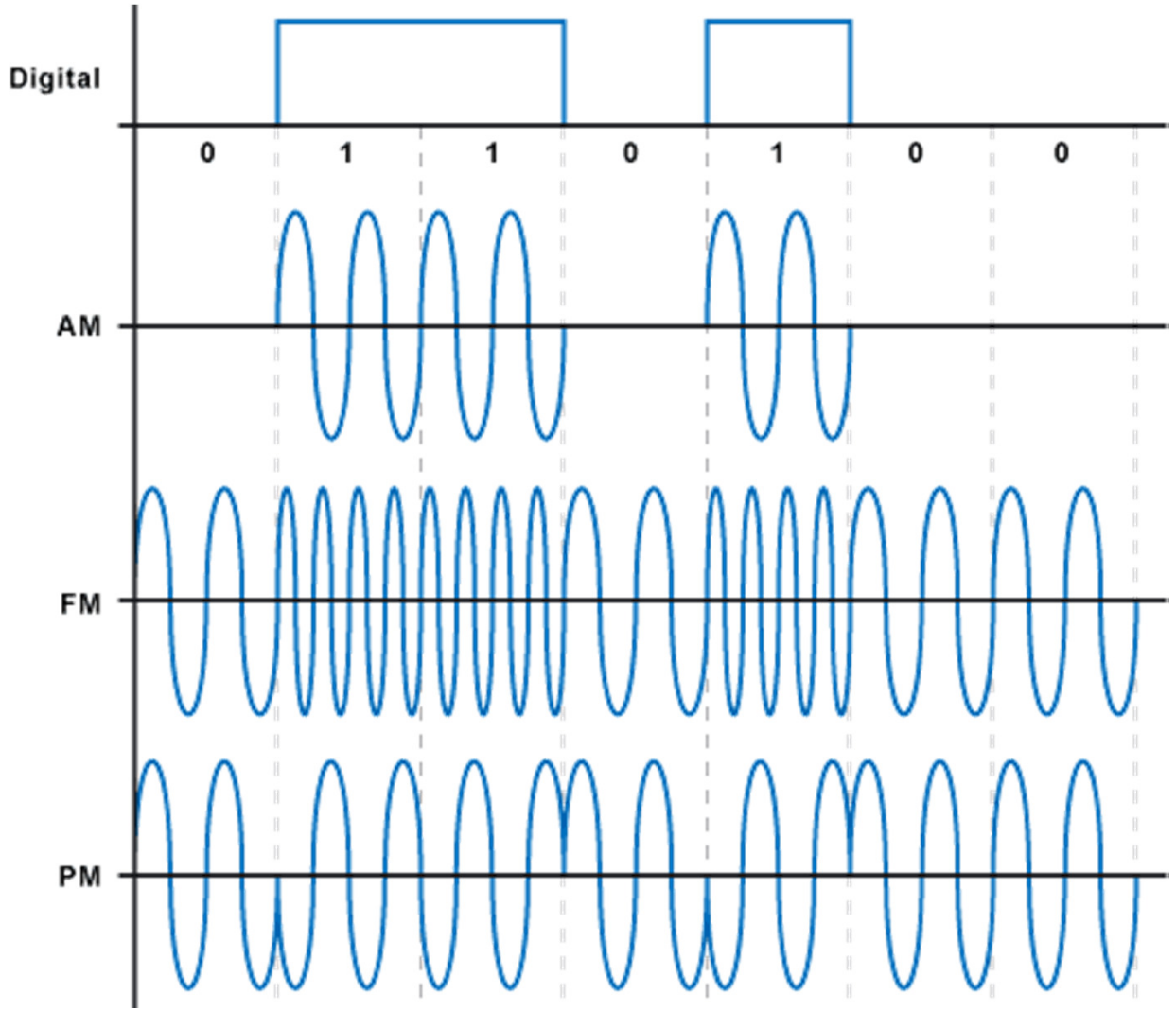
- Zur Übertragung der Daten wird ein Hilfs- oder auch „Trägersignal“ U_T verwendet, das im gewünschten Frequenzbereich/ Kanal liegt.



- Diesem Hilfssignal werden die Daten aufgeprägt, so dass sie z.B. im Bereich von 2,4 GHz übertragen werden können. Das wird „Modulation“ genannt.
- Dabei werden die Amplitude, die Frequenz- oder die Phase des ursprünglichen Trägersignals durch die Daten verändert.

Übersicht über verschiedene Modulationsverfahren

Prof. Dr. Kerstin Uhde
Hochleistungsnetze u. Mobilkommunikation



AM = Amplitudenmodulation

FM = Frequenzmodulation

PM = Phasenmodulation

0 => $f_T - \Delta f$

1 => $f_T + \Delta f$

0 => U_T , $\varphi_T = 0°$

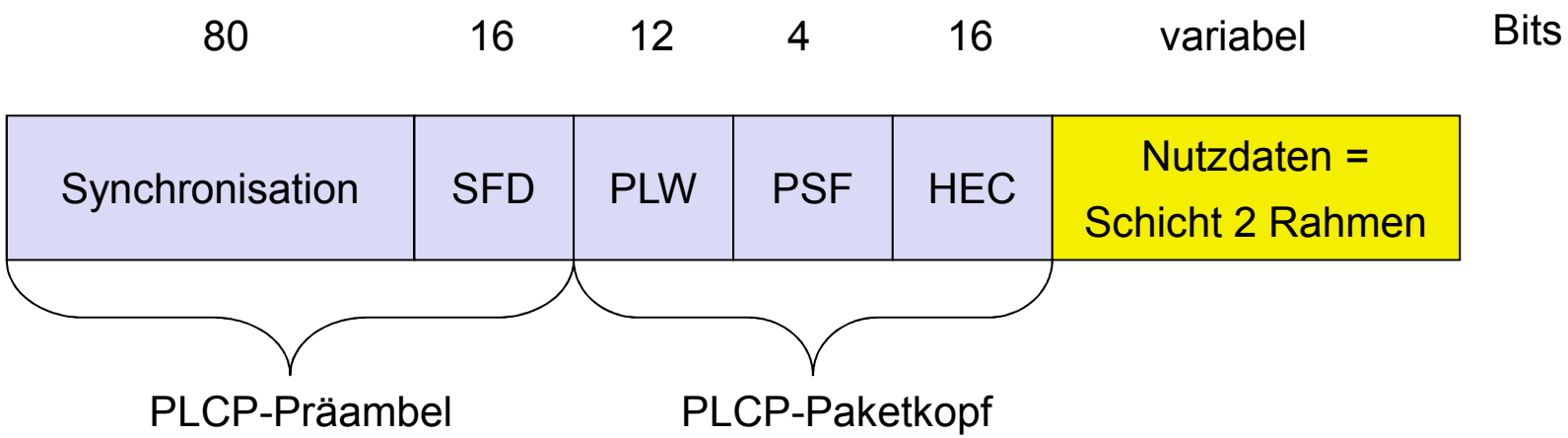
1 => - U_T , $\varphi_T = 180°$

Quelle:
http://www.elektronik-kompendium.de/sites/kom/0211195.htm

Bitübertragungsschicht in WLAN (2)

- **Höherwertige Modulationen:** Zur Erhöhung der maximalen Bitrate in einem festen Frequenzbereich können auch mehr als zwei „Träger-zustandswerte“ definiert werden. Das entspricht vom Prinzip her der Verwendung von mehreren Signalebenen zur Erhöhung der Kanalkapazität. Häufig ist eine Kombination aus Amplituden- und Phasenmodulation zu finden.
- Auch bei den WLAN Standards gibt es Protokollelemente der Schicht 1: Die Bitfolge beginnt mit einer Präambel gefolgt von einem besonderen Bitmuster, dem Start of Frame Delimiter (= SFD), der den Beginn der eigentlichen Daten anzeigt. Danach werden meistens die Länge der Nutzdaten und die Datenrate des Nutzdatenbereichs übertragen.

Beispiel: IEEE 802.11 PHY-Rahmen mit Datenrate 1 - 2 Mbit/s



PLCP = Physical Layer Convergence Protocol

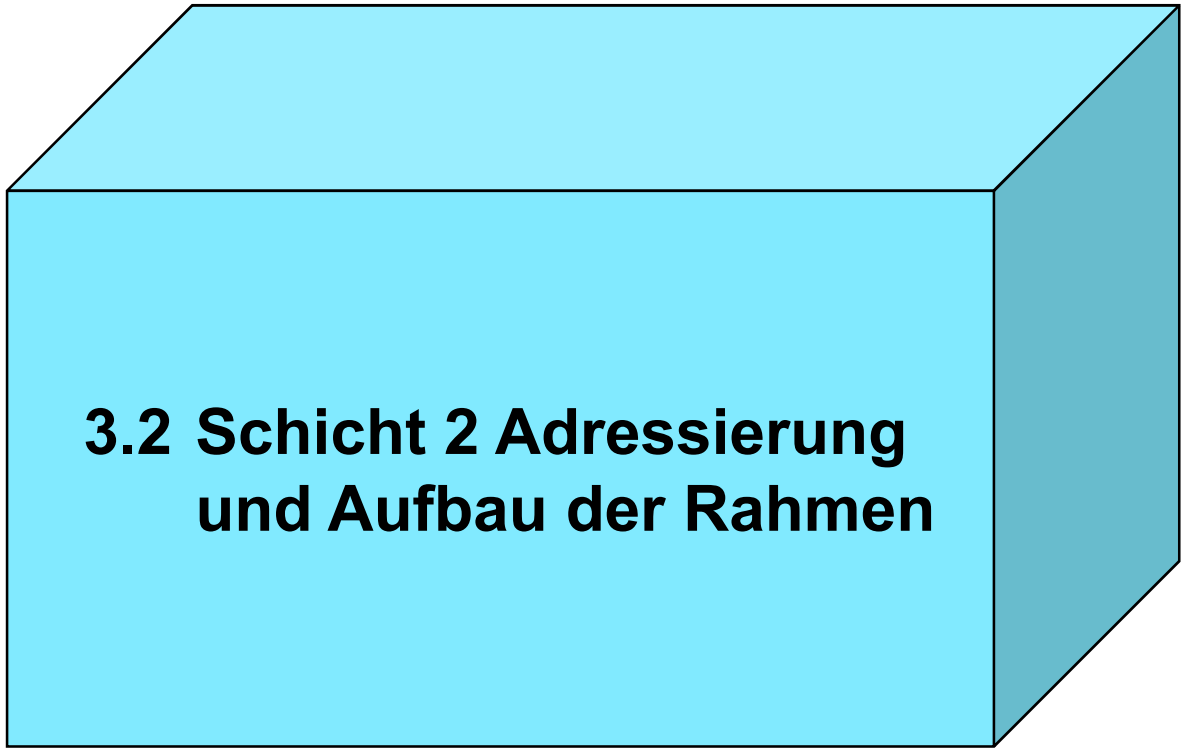
Synchronisation: festgelegte Bitfolge (010101 ...)

Startbegrenzer (SFD): 00001100 10111101

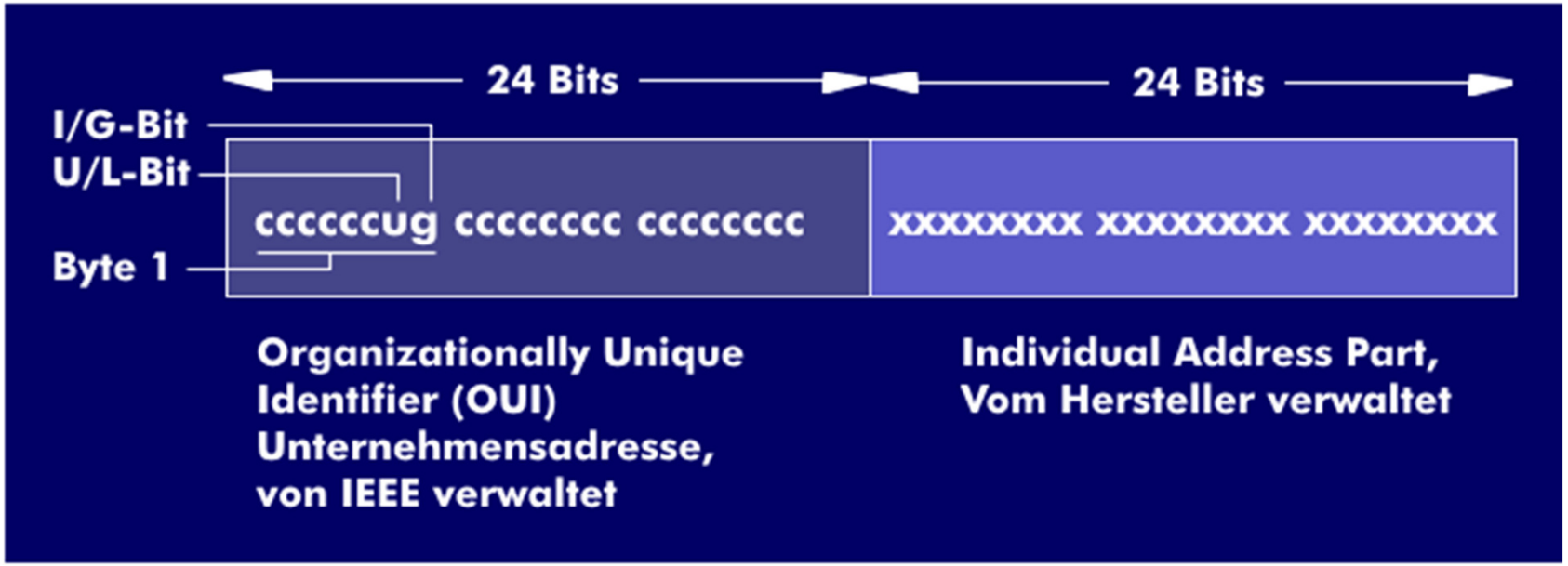
PLW: Länge der Nutzdaten (0 - 4095) (= PLCP-PDU Length Word)

PSF: Datenrate der Nutzlast (= PLCP Signalling Field)

HEC: Prüfsumme für Paketkopf (CRC mit $x^{16}+x^{12}+x^5+1$)


3.2 Schicht 2 Adressierung
und Aufbau der Rahmen

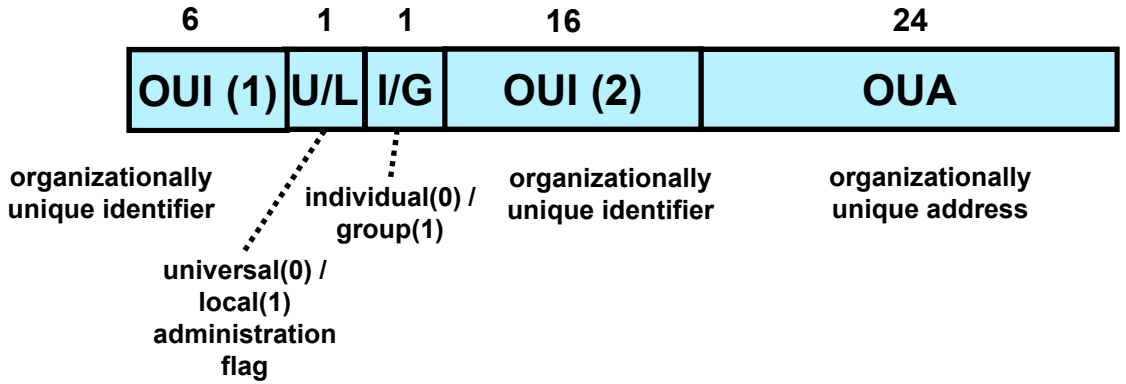
Adressierung MAC-Schicht (1): Aufbau der MAC-Adressen



Quelle: http://www.itwissen.info/definition/lexikon/MAC-Adresse-MAC-address.html

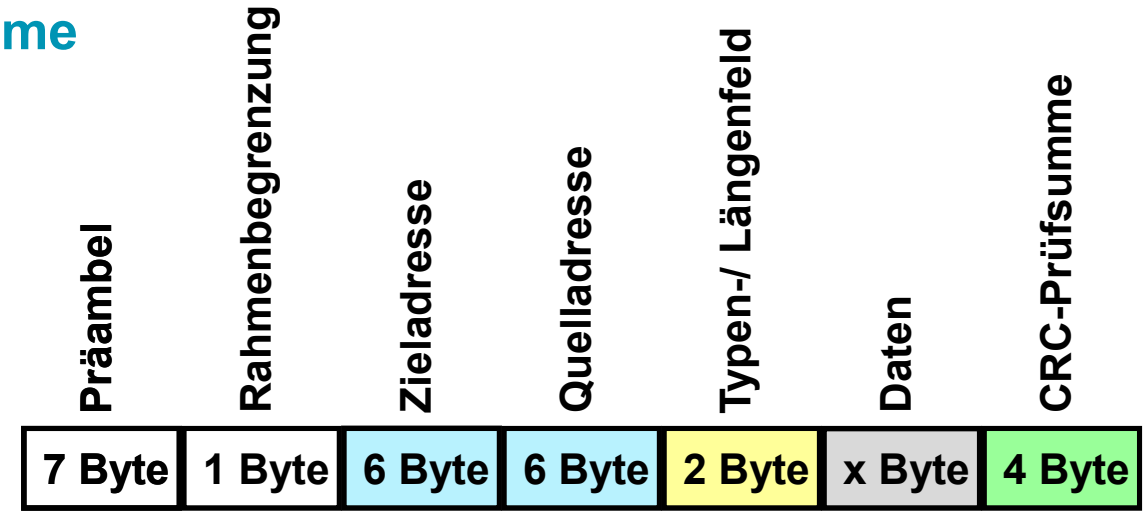
- **Länge der sogenannten „MAC“- oder Hardware Adresse = 6 Byte**

Adressierung MAC-Schicht (2): Aufbau der MAC-Adressen



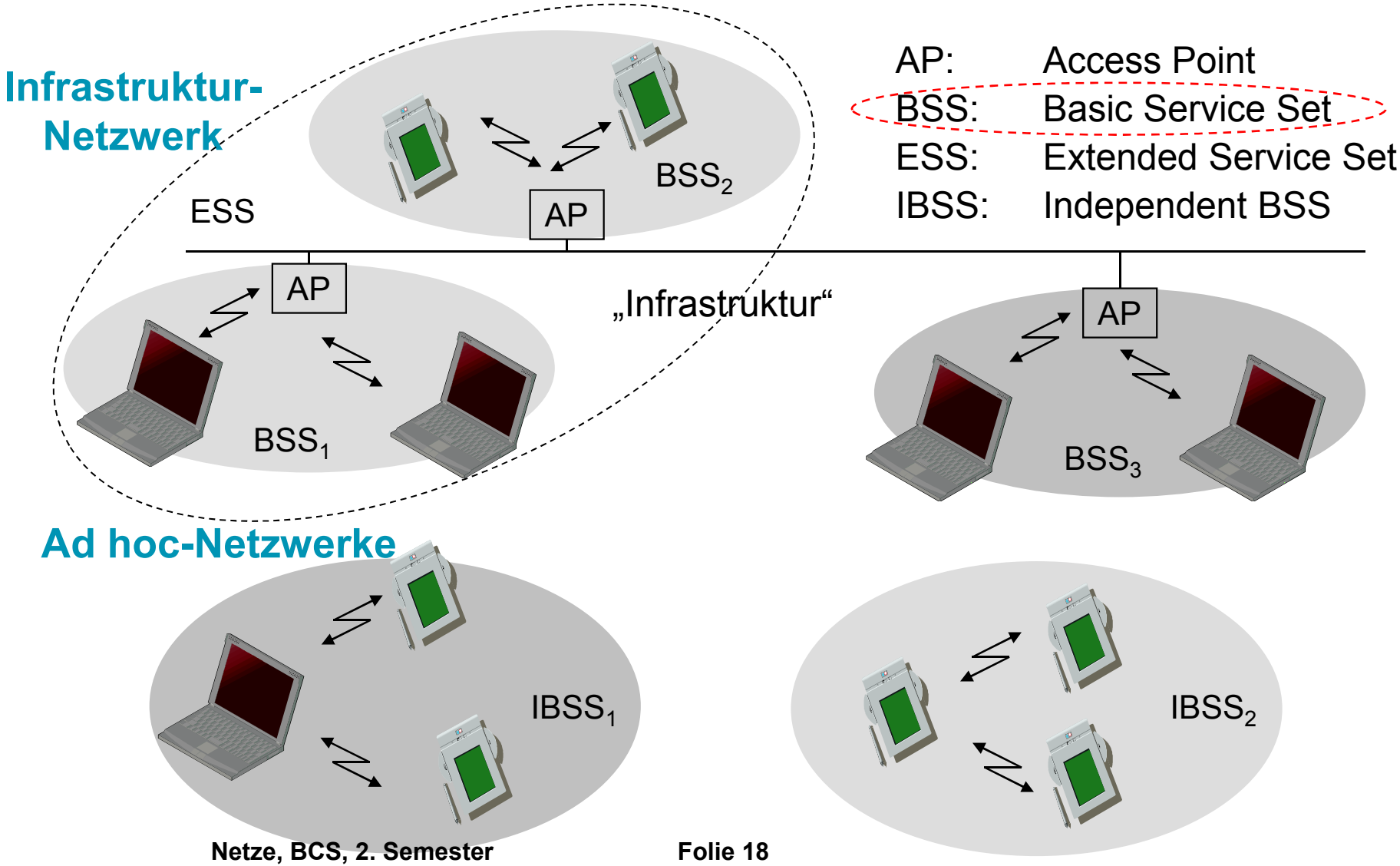
- U/L-Bit (Universal oder Local Bit)
  - 0 globale von IEEE verwaltete, weltweit eindeutige, fest eingebrannte Adresse
  - 1 lokale (von Software konfigurierte) Adresse
- I/G-Bit (Individual oder Group Bit)
  - 0 zur Adressierung einer einzelnen Station
  - 1 für eine Gruppen- oder Broadcast-Adresse
  - Broadcast-Adresse 0xFF-FF-FF-FF-FF-FF
- OUI: Hersteller-ID, dem Hersteller fest zugewiesen
- OUA: Stations-ID, vom Hersteller fest vergeben,

Ethernet Frame



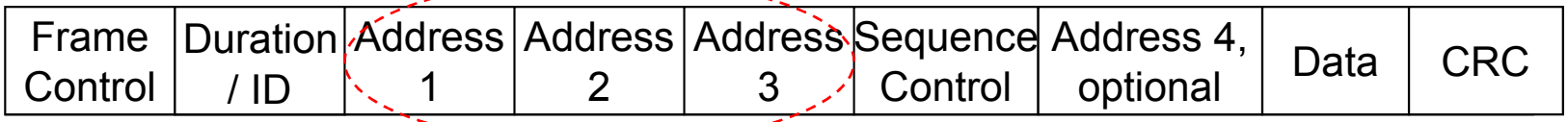
- Präambel: Bitsequenz 10101010 1010 … (für Synchronisationszwecke)
- Rahmenbegrenzung (Start of Frame Delimiter): 10101011
- **Ziel-/ Quelladresse: MAC Adresse des Empfängers bzw. des Senders**
- **Typen-/ (Längen-)feld: spezielle Rahmentypen (oder Längenangabe)**
- **Datenfeld: 46 bis 1500 Bytes**
- **CRC-Prüfsumme gemäß Cyclic-Redundancy-Check/ Polynomprüfverfahren**

Grundlegende Architektur von WLAN: Infrastruktur- und Ad hoc-Netzwerke



IEEE 802.11 Frame

- Datenrahmen (MAC-Datenrahmen)



Byte:	2	2	6	6	6	2	6	...	4

Frame Control: Protokollversion, Rahmentyp, Fragmentierung, 2 Bits für Bedeutung der Adressfelder

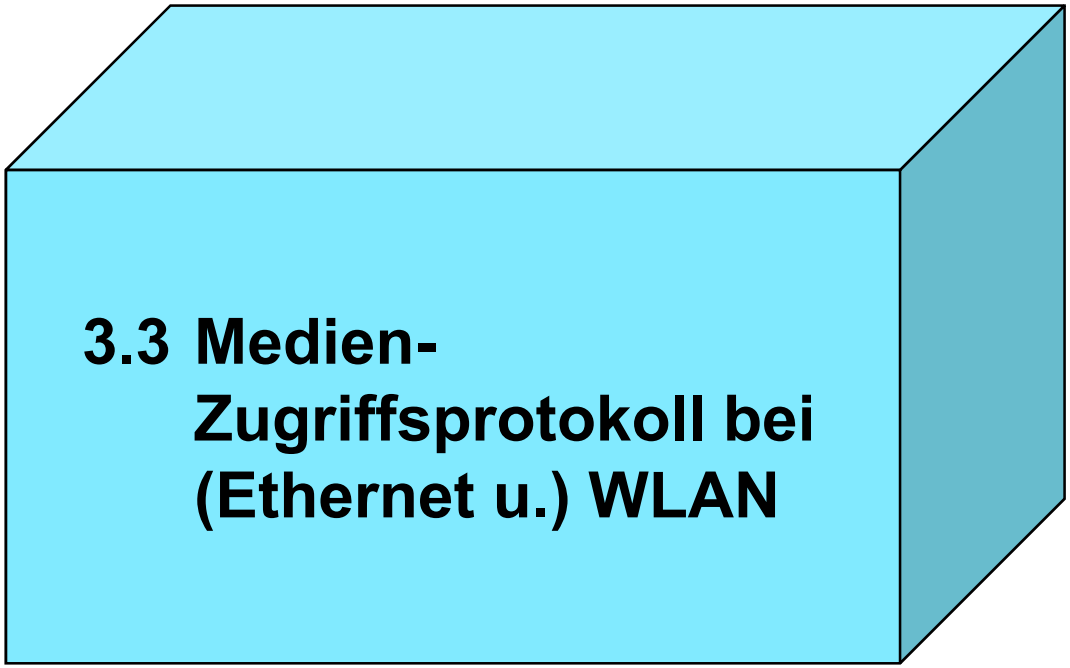
Duration/ID: Übertragungsdauer in µs (NAV = Network Allocation Vector) oder ID einer Station

Address 1 - 4: MAC-Adressen (Sender, Empfänger, BSS …)

Sequence Control: Folgenummern der Nutzdaten

Data: Nutzdaten (0 bis max. 2312 Byte)

CRC: Cyclic Redundancy Check, 32-Bit Prüfsumme über den Rahmen


3.3 Medien-
Zugriffsprotokoll bei
(Ethernet u.) WLAN

Problemstellung, Randbedingungen und Eigenschaften der MAC-Schicht

Grundproblem:

- **Datenübertragungen verschiedener Teilnehmer im gleichen „Kanal“ d.h. im gleichen Frequenzbereich**

Anforderungen:

- **faires Zugriffsverfahren, gleichberechtigte Stationen**
- **dezentral**
- **hohe Datenrate**

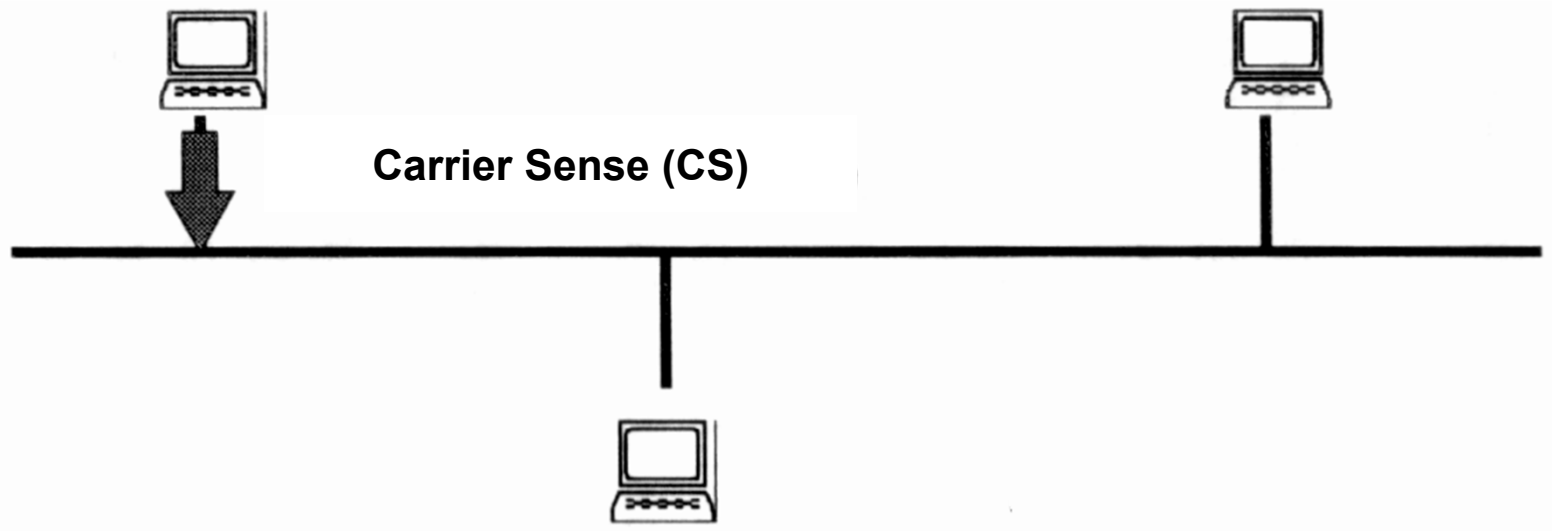
⇒ **CSMA/CA** (= Carrier Sense Multiple Access/ Collision Avoidance) **basiert auf dem gleichen Ansatz wie das Zugriffsverfahren CSMA/CD** (= Carrier Sense Multiple Access/ Collision Detection) **bei Ethernet, wurde aber an die Randbedingungen eines drahtlosen Mediums angepasst**

Eigenschaften:

- **nicht deterministisch**
- **keine garantierte Antwortzeit**

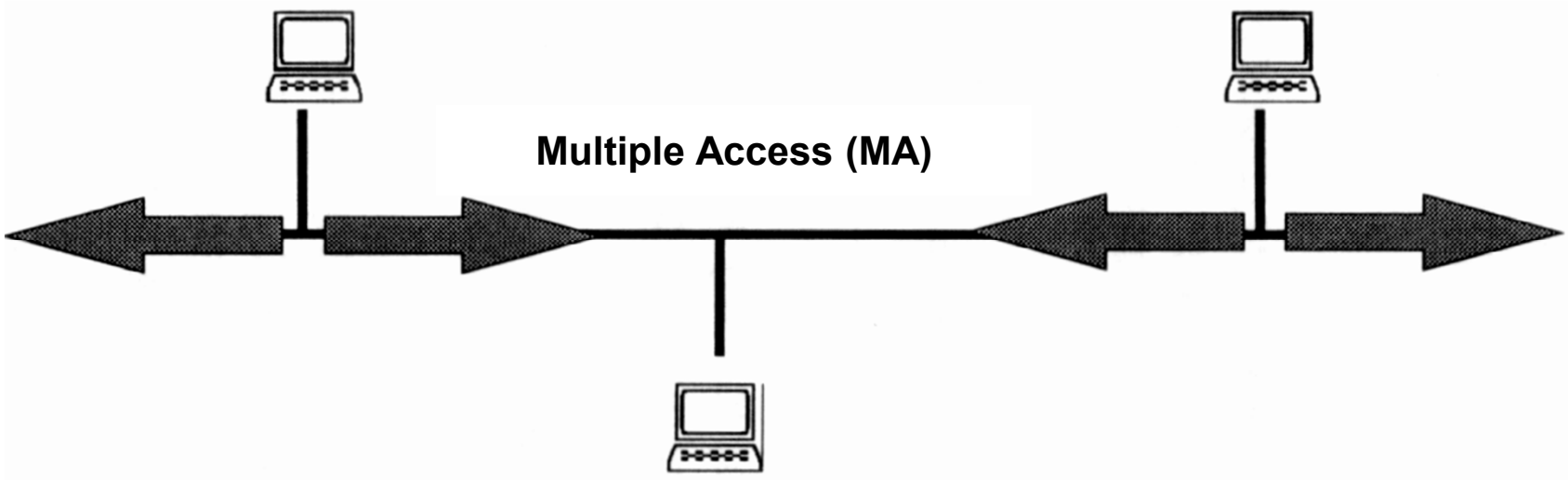
CSMA/ CD (1)

- Ethernet verwendet als Zugriffsverfahren CSMA/ CD (Carrrier Sense Multiple Access with Collision Detection)
- Jede Station überwacht das Medium (“carrier sensing, listen before talking”). Sicherheitsproblematik: “Jeder hört mit”.



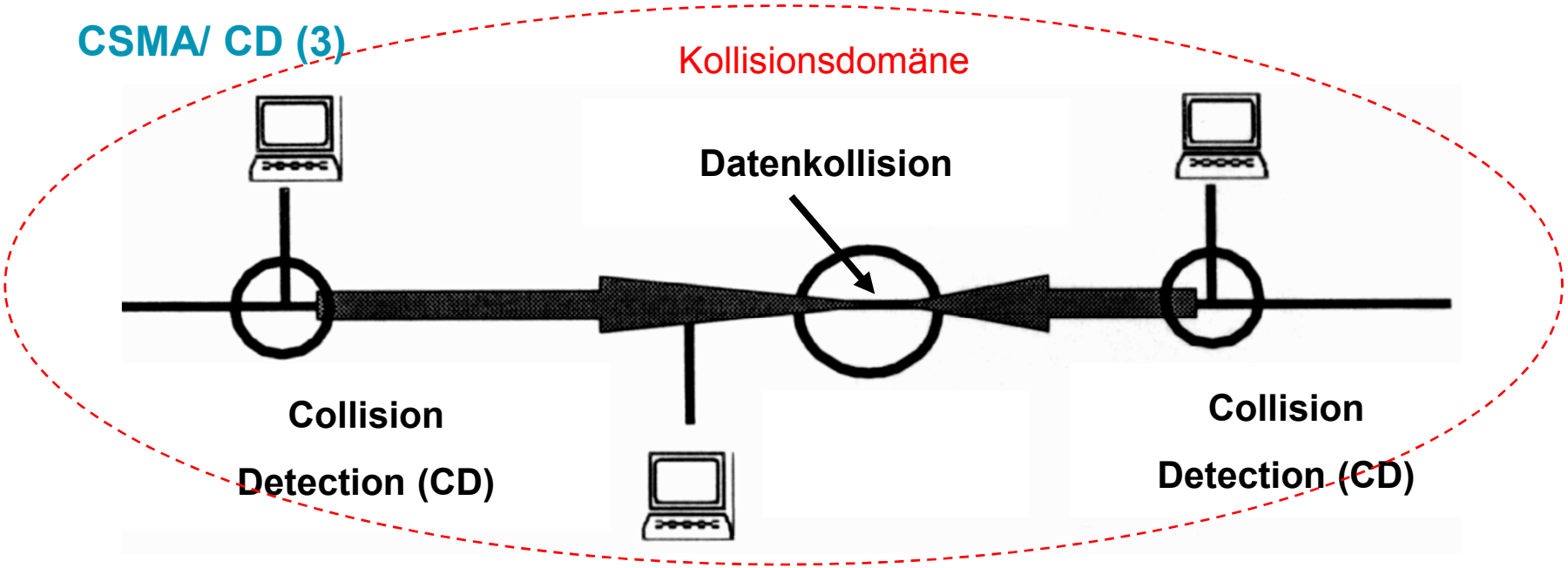
- Bei freiem Medium sendet eine Station nach einer (kurzen) Wartezeit.
- Falls das Medium belegt ist, wartet die Station bis das Medium wieder frei ist und beginnt nach einer zufälligen Zeit mit der Datenübertragung.

CSMA/ CD (2)



- Es kann passieren, dass mehrere Station gleichzeitig zu senden beginnen. Dann kommt es zu einer Kollision.
- Daher wird das Medium auch während der Sendung weiter abgehört.

CSMA/ CD (3)



- Ein Kollision wird vom Sender dadurch entdeckt, dass er beim Senden den Pegel des Ausgangssignals mit dem des Eingangssignals vergleicht (Feststellung einer Signalüberlagerung). Bei einer Kollision wird die Datenübertragung sofort abgebrochen und es wird ein spezielles Störsignal gesendet.
- Nach der Absendung des Störsignals wird eine zufallsbestimmte Zeit, die mit der Anzahl der Fehlversuche wächst, gewartet und die Übertragung bei Schritt 1 neu versucht (back-off-time).

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

- Eine normale Antenne kann entweder Daten senden **oder** Daten empfangen d.h. das Feststellen einer Kollision ist nicht direkt möglich!
- Daher wird in WLAN ein abgewandeltes Zugriffsverfahren verwendet: CSMA/ CA (Carrrier Sense Multiple Access with Collision Avoidance)
- Jede Datenübertragung wird bei CSMA/ CA vom Empfänger mit einem Acknowledge (ACK) bestätigt (Ausnahme: Broadcast Nachrichten).
- Damit es beim Senden des ACK **nicht** zu Kollisionen kommen kann, wird das ACK nach einer sehr kurzen Wartezeit gesendet, die kürzer ist die minimale Wartezeit, die bei einer Datenübertragung auftreten kann.
- Wartezeit vor einer normalen Daten Übertragung: DIFS: Data-Inter-Frame Spacing **plus** zufällige Wartezeit
- Wartezeit vor der Sendung von ACK (und einigen anderen Steuernachrichten) SIFS: Short Inter-Frame Spacing

  Es gilt: DIFS > SIFS

Der grundsätzliche Ablauf von CSMA/ CA (1)

- Die sendewillige Station hört das Medium ab.
- Ist das Medium frei, darf sie nach DIFS plus zufälliger Wartezeit mit der Sendung ihrer Daten beginnen.
- Ist das Medium nicht frei, wartet sie, bis das Medium frei wird und sendet dann nach DIFS plus einer zufälligen Wartezeit.
- Der Empfänger quittiert die Sendung mit einem ACK. Nach Erhalt des ACK ist die Datenübertragung abgeschlossen. (Das „Wettbewerbsfenster“ wird auf den minimalen Bereich gestellt.)
- Bei Ausbleiben des ACK erneutes Senden der Daten mit neuem (nicht bevorzugten!) Medienzugriff mit verdoppeltem Wettbewerbsfenster.
- Beginnt eine andere Station vorher zu senden, muss die sendewillige Station die Sendung ihrer Daten verschieben.
- Allerdings kann sie beim nächsten Sendeversuch ihre „Rest“-Wartezeit verwenden.

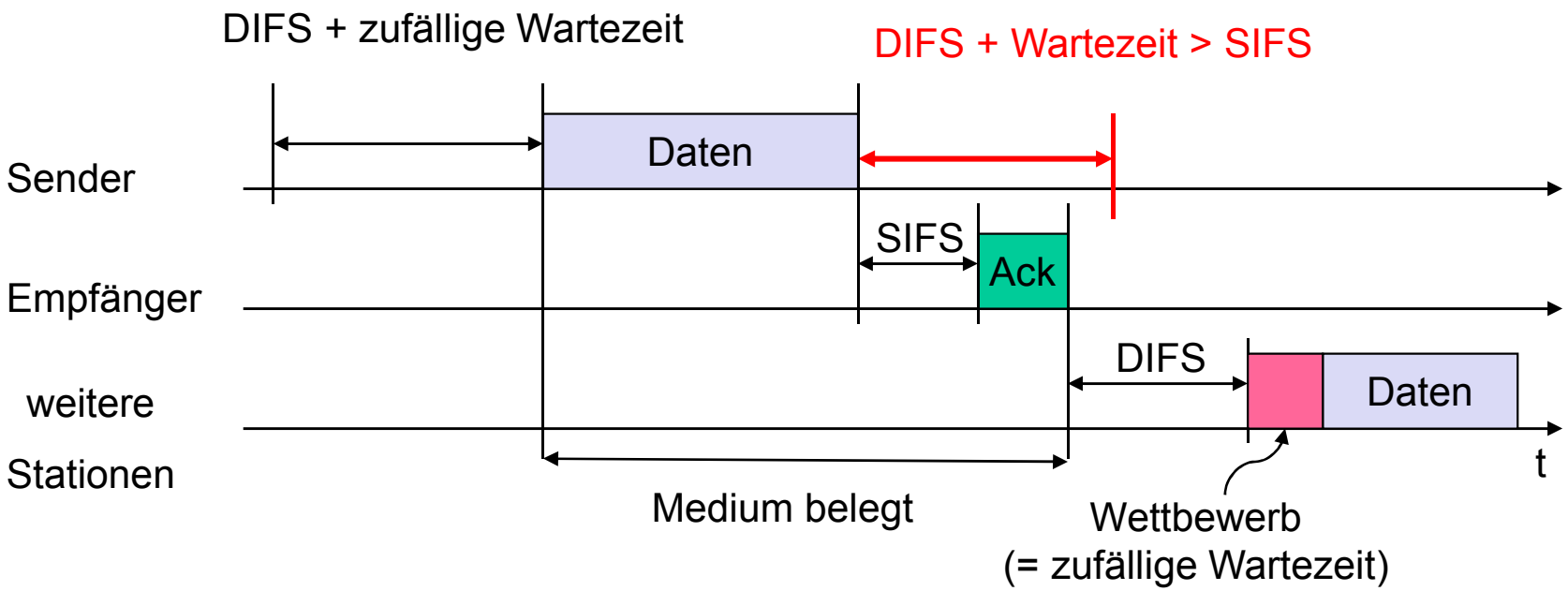
=> Verbesserung der Fairness!

Der grundsätzliche Ablauf von CSMA/ CA (2)

Wann treten Kollisionen auf?

- Wenn zwei Stationen (aus irgendeinem Grund) gleichzeitig zu senden beginnen d.h. wenn sie z.B. die gleichen zufälligen Wartezeiten erhalten ...
- Danach wird der Bereich aus dem die zufällige Zeit bestimmt wird verdoppelt, es läuft ein Backoff Mechanismus ab. Nach erfolgreicher Sendung wird wieder der minimale Bereich verwendet.

Ablauf einer Punkt-zu-Punkt Datenübertragung

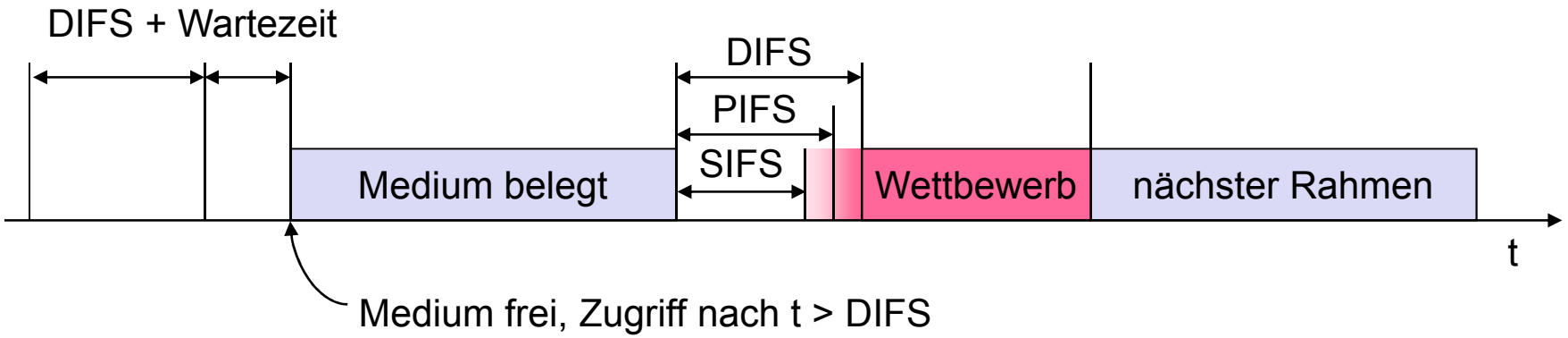


DIFS = **Data** Interframe Spacing > SIFS = **Short** Interframe Spacing

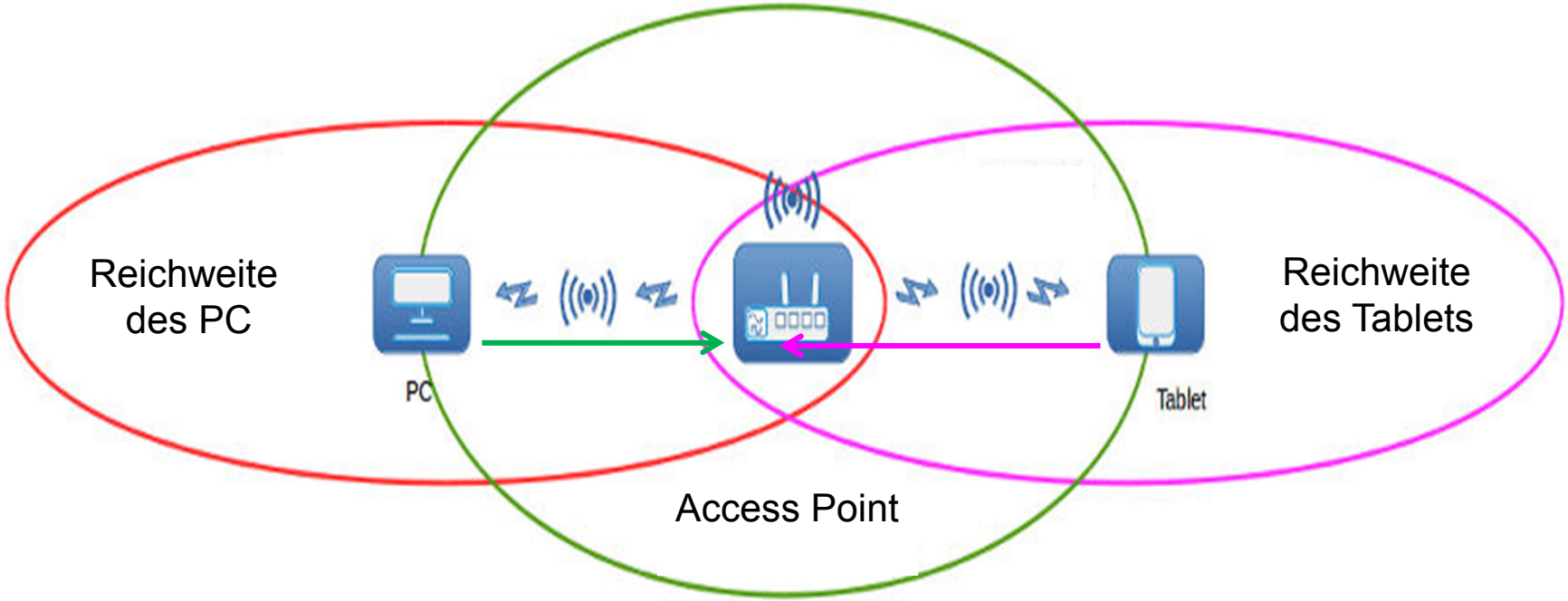
Medienzugriff wie beschrieben mit Bestätigung jeder Übertragung (nur bei Broadcast Nachrichten keine Bestätigung!), Feststellen einer Kollision durch Ausbleiben des ACK.

Konzept der unterschiedlichen Wartezeiten

- Prioritäten
  - werden durch Staffelung der Zugriffszeitpunkte geregelt
  - SIFS (Short Inter Frame Spacing) - 10µs
    - höchste Priorität, für ACK (und einige Steuernachrichten wie RTS, CTS …)
  - PIFS (PCF, Point Coordination Function IFS) - 30µs
    - mittlere Priorität, für zeitbegrenzte Dienste mittels PCF
  - DIFS (DCF, Distributed Coordination Function IFS) - 50µs
    - niedrigste Priorität, für Datendienste

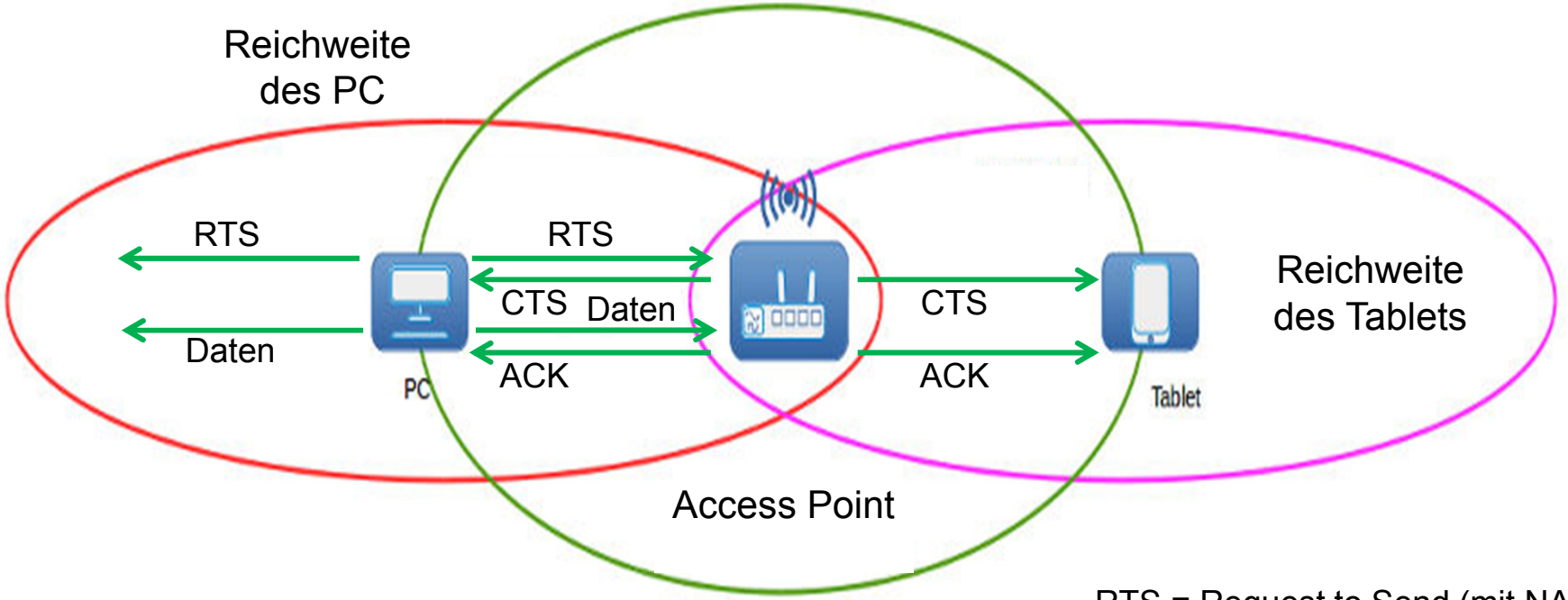


Problem der „Hidden Nodes“ in drahtlosen Netzen



Quelle: https://www.dasheimnetzwerk.de/Lexikon/Uebertragungsmedien/WLAN/Eintrag_WLAN_Einfuehrung.html

Problem der „Hidden Nodes“ in drahtlosen Netzen (2)

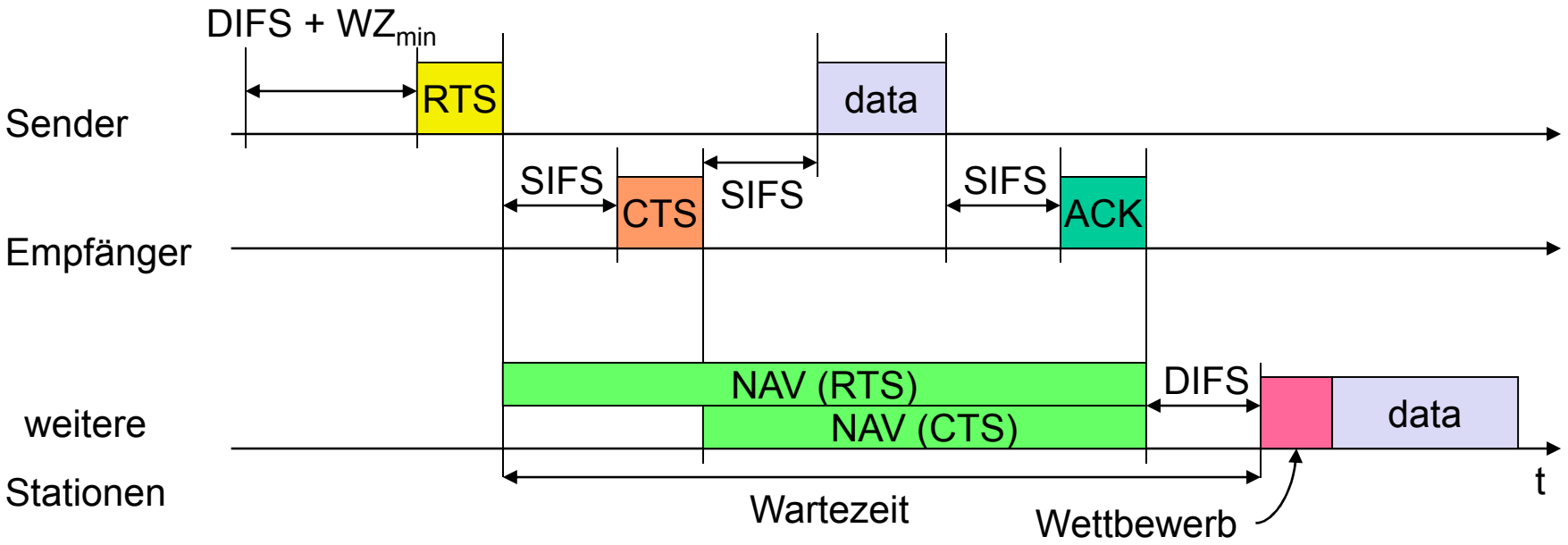


RTS = Request to Send (mit NAV)
CTS = Clear to Send (mit NAV)

Quelle: https://www.dasheimnetzwerk.de/Lexikon/Uebertragungsmedien/WLAN/Eintrag_WLAN_Einfuehrung.html

Zugriffsmechanismus bei IEEE 802.11 mit „Reservierung“ des Mediums

- Es gibt optional einen Zugriffsmechanismus, bei dem Sender und Empfänger vor der Übertragung der eigentlichen Daten ein Request to Send (RTS) und ein Clear to Send (CTS) austauschen. Sowohl in RTS als auch in CTS wird die Länge der Übertragung gesendet. Alle Stationen, die das RTS und/ oder das CTS empfangen, dürfen in dieser Zeit keine Daten senden.



NAV = Network Allocation Vector = „Reservierungszeit“, wird in RTS und CTS übertragen und wird von den anderen Stationen gespeichert

Weitere wichtige Aspekte in WLAN

- Wie können die Stationen feststellen, welche WLAN vorhanden sind und ob es möglich ist, sie zu nutzen?
- Wie wird sichergestellt, dass nur berechtigte Stationen das WLAN benutzen?
- Wie wird verhindert, dass andere Stationen die Daten mitlesen können?
- Welche Managementabläufe sind in einem WLAN notwendig?
  Was passiert beim Anschluss einer Station an ein WLAN?