SWISS AMATEUR TELEPRINTER GROUP

HAMNET: WLAN Introduction

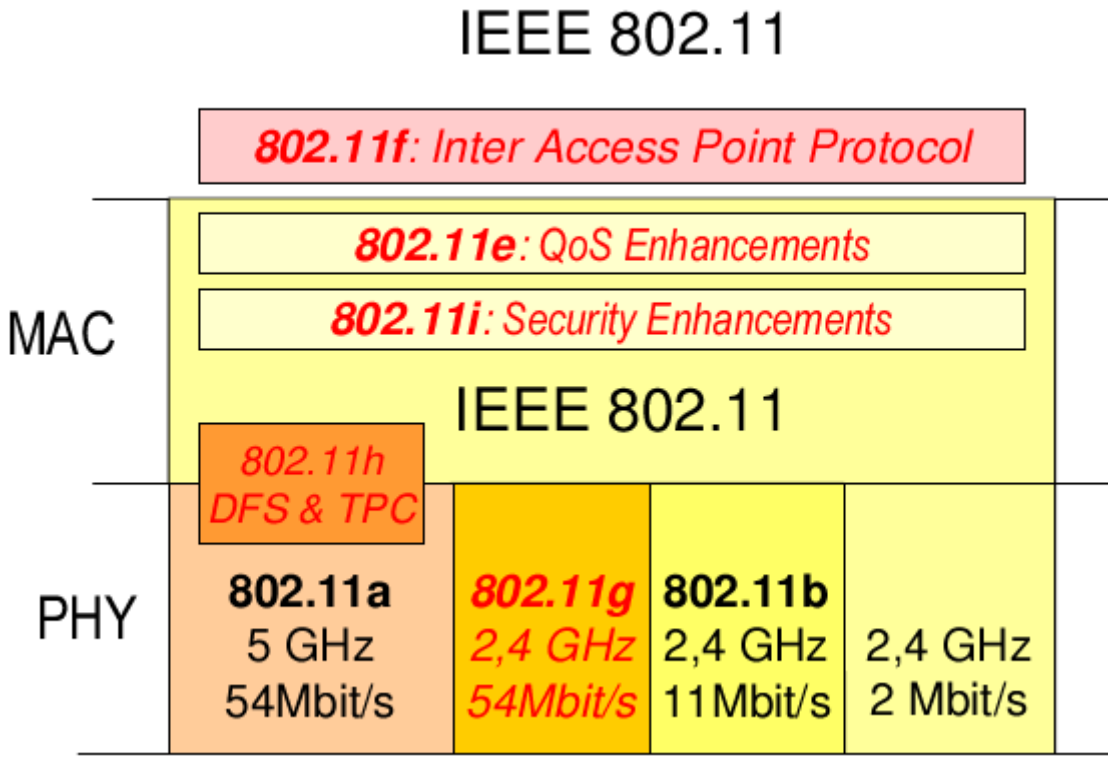
Dominik Bugmann
hb9czf@swiss-artg.ch

7. November 2009

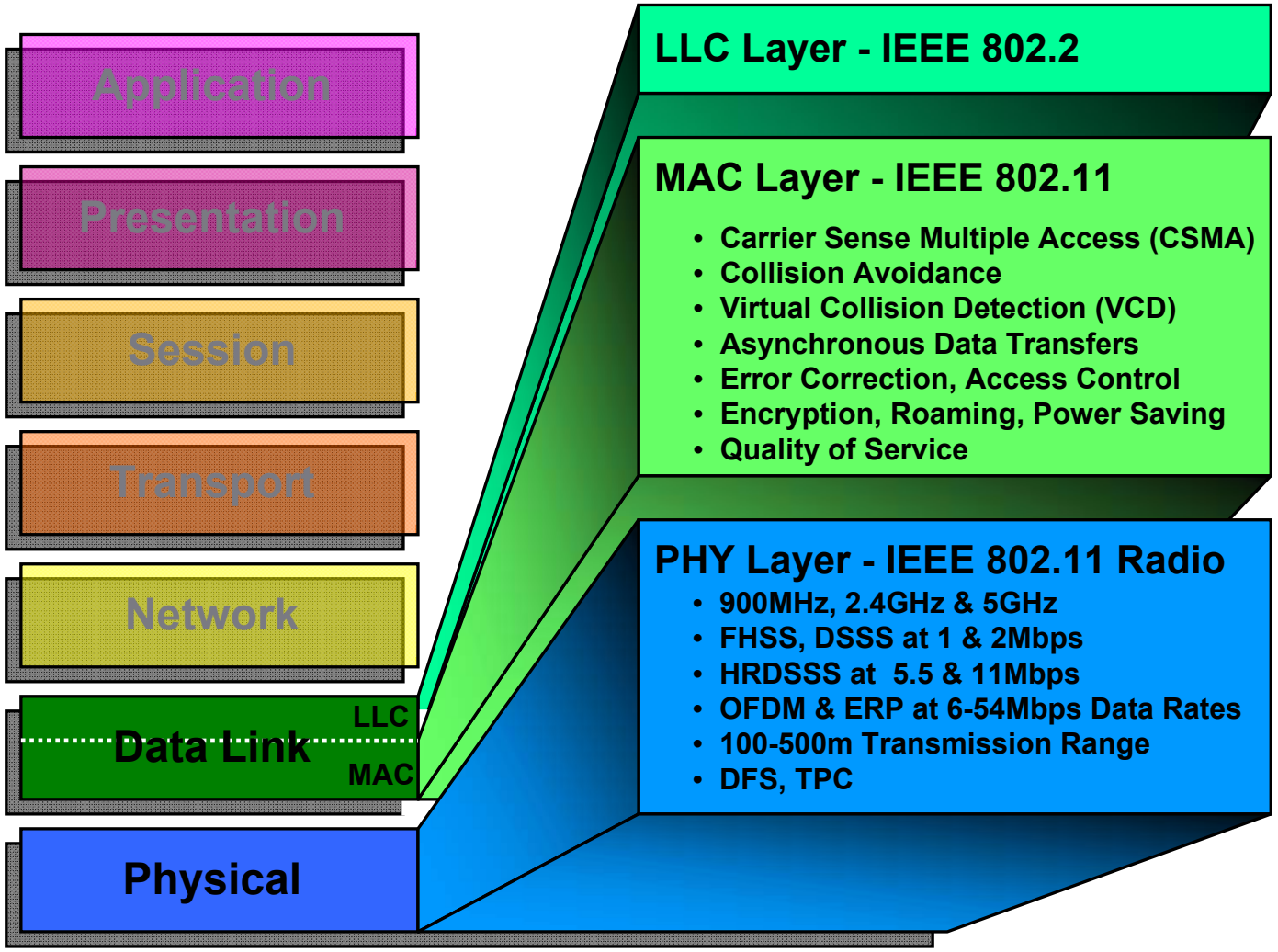
Thomas Ries
hb9xar@uska.ch

Übersicht

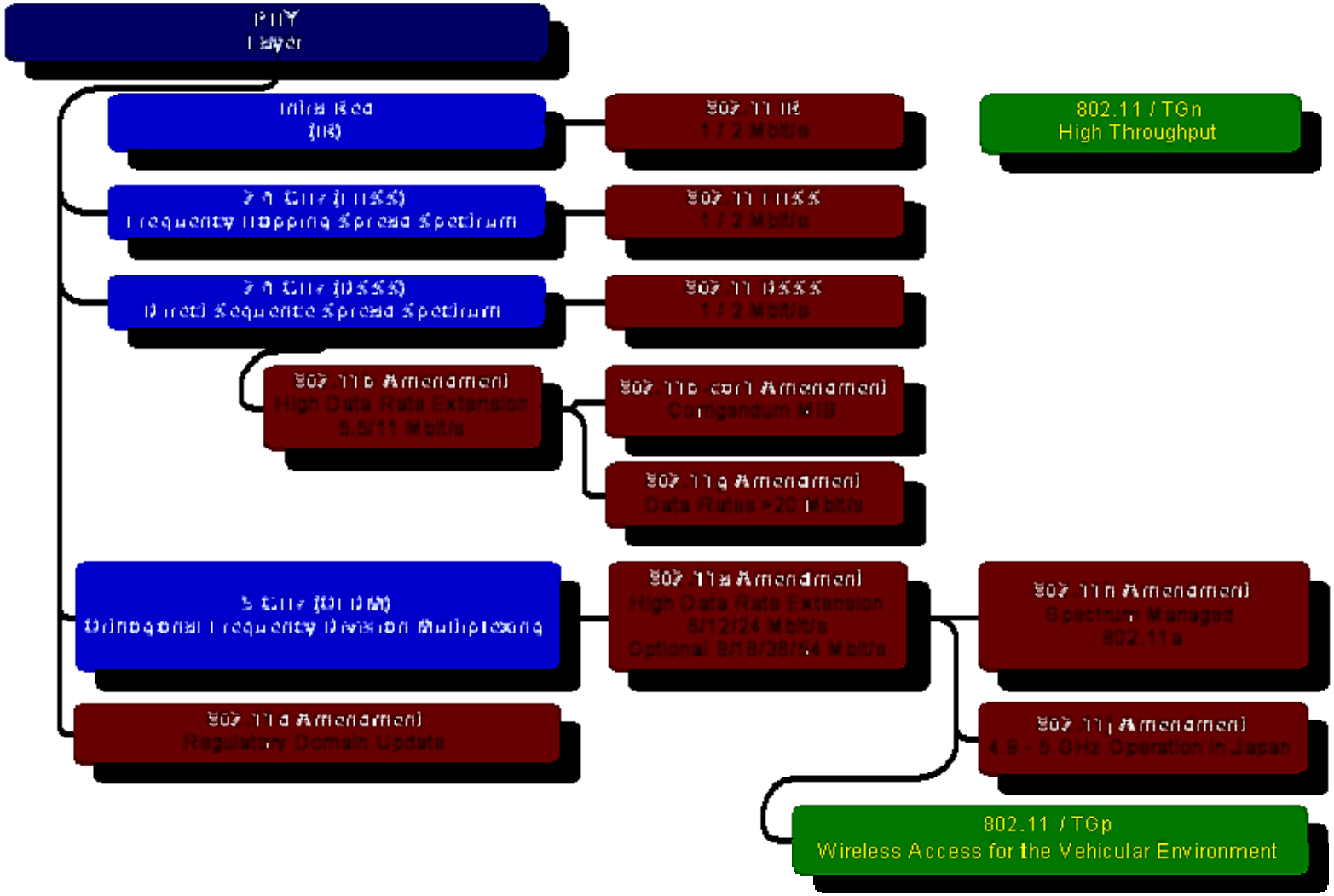
- **Der 802.11 WLAN Standard**
- **802.11 PHY Layer (OSI Layer 1 – Physical)**
- **802.11 MAC Layer (OSI Layer 2 – Data Link)**



Der IEEE 802.11 WLAN Standard



802.11 PHY Layer

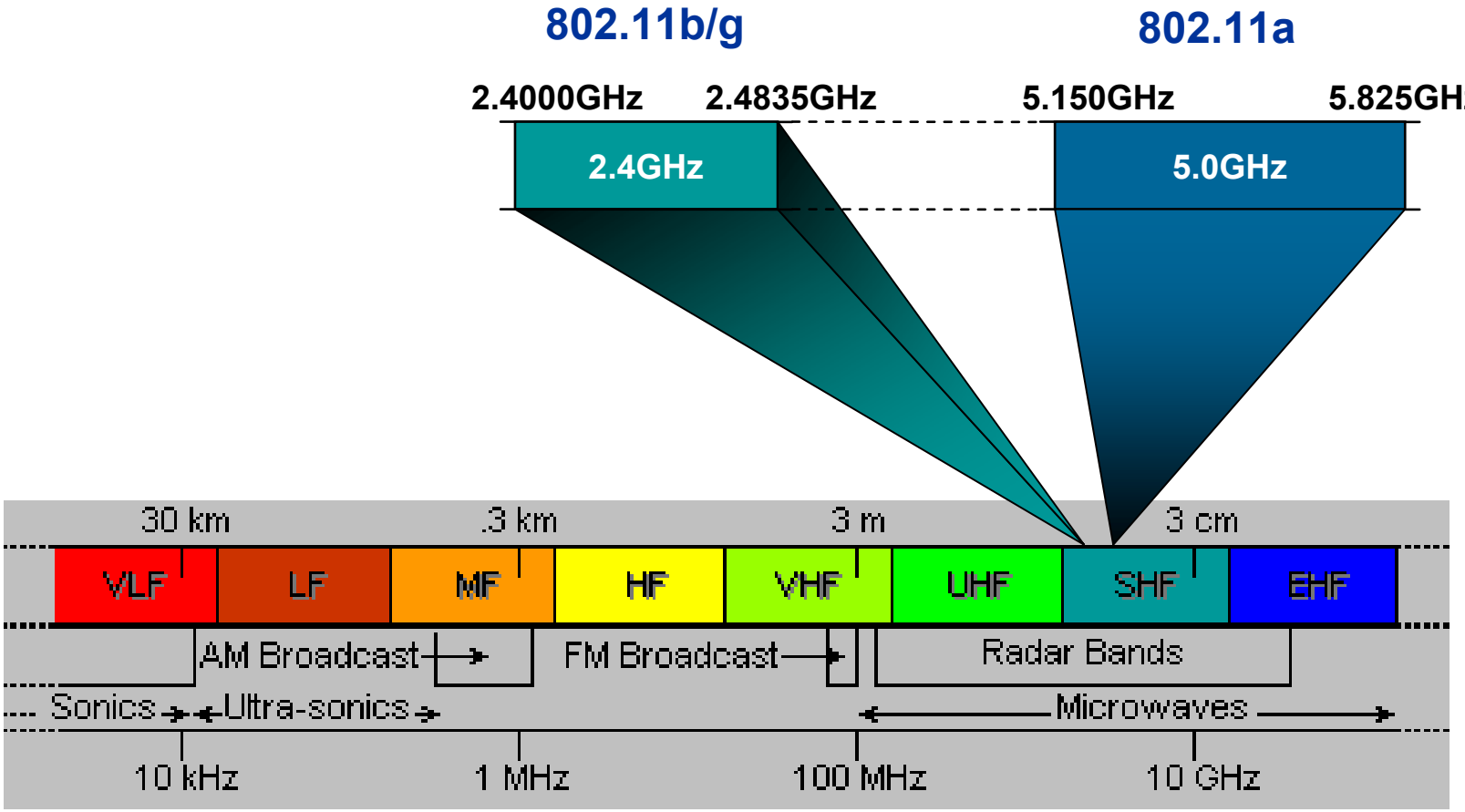


802.11 PHY Layer: Physical

Der Physical Layer definiert:

- **Frequenzbereich/Medium**
  - Infrarot
  - Radio (2.4 GHz, 5 GHz)
- **Kanalraster & Zuweisung**
- **Spread Spectrum Technik**
  - Frequency Hopping (FH)
  - Direct Sequence (DS)
  - Orthogonal Frequency Division Multiplexing (OFDM)
- **Modulation der Daten**
  - BPSK
  - QPSK
  - QAM

802.11 PHY: Das HF Spektrum



802.11 PHY: Spread Spectrum Techniken

- **Was ist “Spread Spectrum”**
  - Es wird nicht mit einem festen Träger gearbeitet. Die HF Energie wird über ein weites Frequenzband verteilt.
  - Das erhöht die Immunität gegenüber Interferenzen und kann das Abhören erschwehren.
- **Frequency Hopping (FH)**
  - Ein schmalbandiges Signal “hüpft” über mehrere Kanäle in einer pseudo-zufälligen Reihenfolge.
- **Direct Sequence (DS)**
  - Das eigentlich Signal wird mit einem weiteren digitalen Signal moduliert um es über eine grössere Bandbreite zu spreizen.
- **Orthogonal Frequency Division Multiplexing (OFDM)**
  - Verteilt ein Signal auf mehrere orthogonale Sub-Carriers

802.11 PHY: 802.11

- **Ursprünglicher Wireless Standard (von 1997)**
- **Inzwischen veraltet und nicht mehr verwendet**
- **Datenraten 1Mbps & 2Mbps**
- **Medium**
  - Infrarot
  - 2.4 GHz FH (Frequency Hopping) Spread Spectrum
  - 2.4 GHz DS (Direct Sequence) Spread Spectrum

802.11 PHY: 802.11a

- **Erweiterung des 802.11 Wireless Standard (1999)**
  - Datenraten bis zu 54Mbps
  - Operiert im 5GHz Frequenzband
  - Bis zu 24 nicht überlappende Kanäle
- **Weniger Störungen als 802.11b/g**
  - Nicht so stark verbreitet 802.11b/g
  - Weniger/keine Störungen durch andere Geräte (Microwellen-öfen, Wireless Telefone, Bluetooth Geräte)
- **Typische Reichweite**
  - Innen: 15m
  - Aussen: 30m

802.11 PHY: 802.11a

- **Datenraten: 6, 9, 12, 18, 24, 36, 48 & 54Mbps**
- **Modulation: OFDM**
- **Modulation der Sub-Kanäle**
  - Binary Phase Shift Keying (BPSK) (6 & 9Mbps)
  - Quadrature Phase Shift Keying (QPSK) (12 & 18Mbps)
  - 16 Quadrature Amplitude Modulation (QAM) (24 & 36Mbps)
  - 64 Quadrature Amplitude Modulation (QAM) (48 & 54Mbps)
- **Forward Error Correction (FEC)**
- **Bis zu 24 Kanäle verfügbar**
  - Abhängig von regionalen regulatorischen Bestimmungen
- **Regionale Bestimmungen für…**
  - Transmit Power
  - Indoor/Outdoor usage
- **DFS & TPC (802.11h)**
  - Erkennung und Vermeidung von Störungen bei Radar Anlagen

802.11 PHY: 802.11b

- **Erweiterung des 802.11 Wireless Standard (1999)**
  - Datenraten bis zu 11Mbps
  - Operiert im selben 2.4GHz Frequenzband wie 802.11
- **14 Kanäle (überlappend) im 2.4GHz ISM Band**
- **Typische Reichweite**
  - Innen: 30m bei 11Mbps, 90m bei 1Mbps
  - Aussen: 90m, bis 8km bei Antennen mit hohem Gewinn

802.11 PHY: 802.11b

- **Datenraten von 5.5 und 11Mbps**
- **Modulation**
  - Complementary Code Keying (CCK) (DS Spread Spectrum)
  - Verwendet ein Set von 64 8-chip code words for encoding data
  - A chipping rate of 11MHz is maintained so spreading is as for 802.11 DSSS
- **Gleiche Kanalstruktur wie 802.11 DSSS**

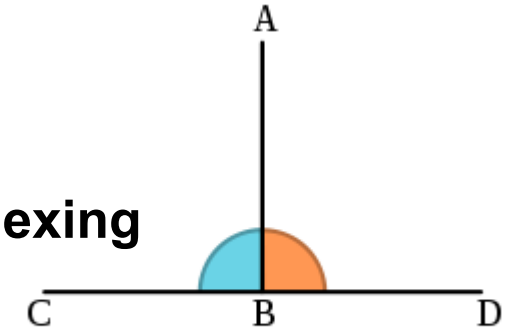
802.11 PHY: 802.11g

- **Erweiterung des 802.11 Wireless Standard (2003)**
  - Datenraten bis zu 54Mbps
  - Operiert im selben 2.4GHz Frequenzband wie 802.11 / 802.11b
- **802.11g ist “state of the art” und die heutzutage meist verwendete WLAN Technologie.**
- **Typische Reichweite**
  - Innen: 45m
  - Aussen: 90m

802.11 PHY: 802.11g

- **OFDM im 2.4GHz Band mit Rückwärtskompatibilität zu 802.11b (CCK/DSSS)**
- **Datenraten von 6, 9, 12, 18, 24, 36, 48 & 54Mbps**
- **Modulation der Daten**
  - Gleich wie bei 802.11b und 802.11a
- **Forward Error Correction (FEC)**
- **4 nicht überlappende Kanäle (14 überlappende)**
- **802.11b Schutzmechanismen (Kompatibilität) reduzieren den effektive Durchsatz in b/g gemischten Umgebungen**
  - CTS-to-self: Broadcast für Kanalreservation
  - RTS/CTS: Handshaking für Kanalreservation

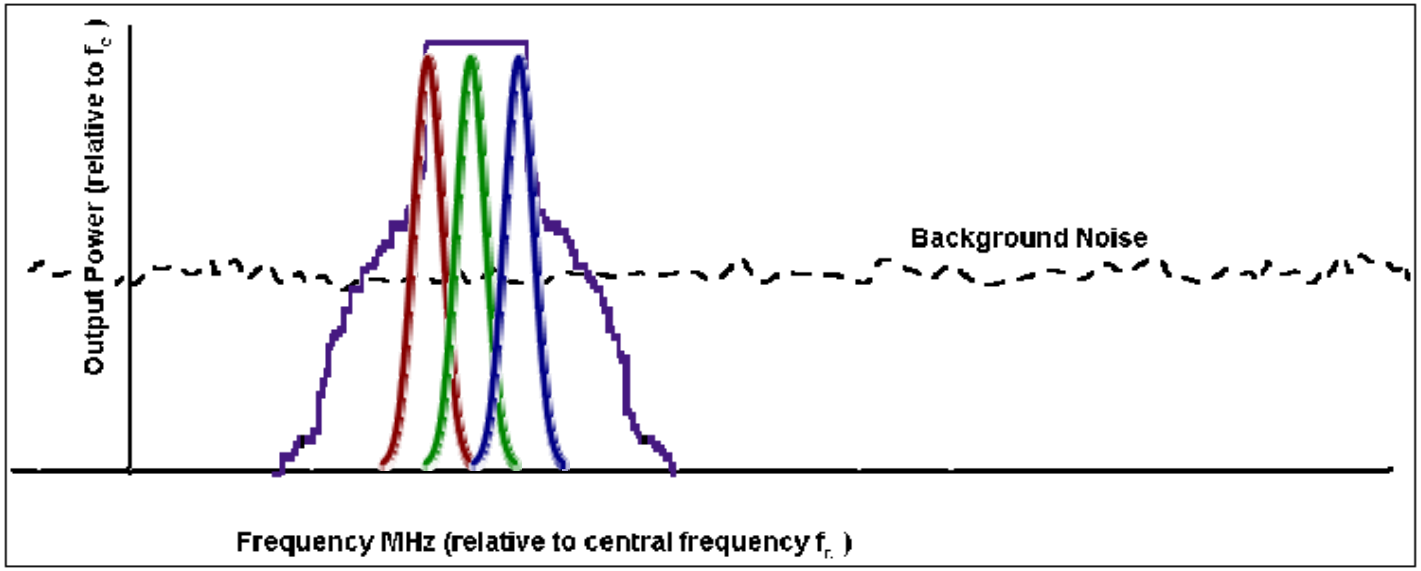
OFDM – etwas mehr im Detail



- **Orthogonal Frequency Division Multiplexing**
- **Orthogonal?**
  - “In communications, multiple-access schemes are orthogonal when an ideal receiver can completely reject arbitrarily strong unwanted signals using different basis functions than the desired signal.”
  - “One such scheme is TDMA, where the orthogonal basis functions are non-overlapping rectangular pulses ("time slots").“
  - “Another scheme is orthogonal frequency-division multiplexing (OFDM), which refers to the use, by a single transmitter, of a set of frequency multiplexed signals with the exact minimum frequency spacing needed to make them orthogonal so that they do not interfere with each other.”

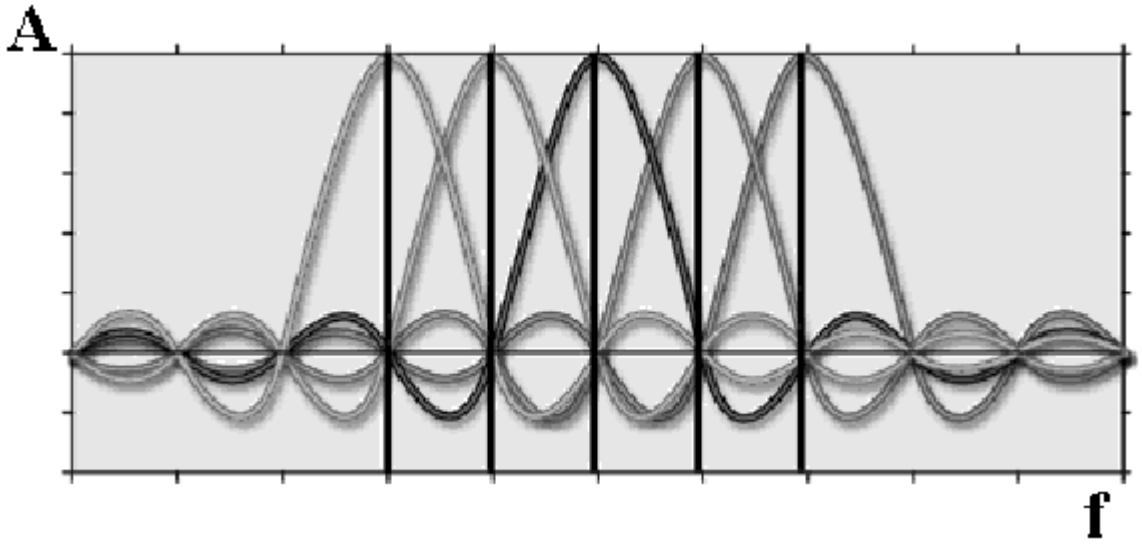
OFDM – Signal

- **Daten werden auf mehreren Sub-Kanälen verteilt gesendet**
  - Abstand der Sub-Kanäle ist genau ½ Lambda (0.3125 MHz)
  - 52 Sub-Kanäle pro OFDM Kanal (48 Daten, 4 Pilot)
  - Modulation der Daten mittels BPSK, QPSK, QAM mit FEC



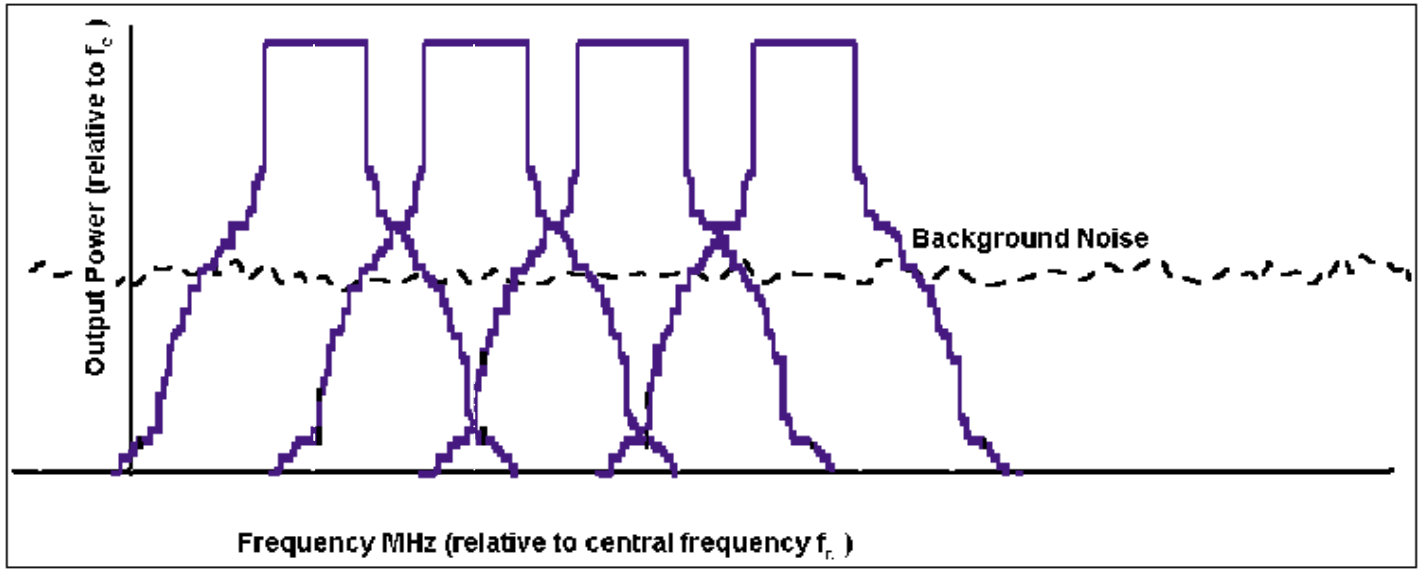
OFDM – Signal

- Die Spektren der Sub-Kanäle überlappen sich zwar, die Sub-Träger stehen jedoch *orthogonal* zueinander. D.h. die Sub-Träger beeinflussen sich nicht gebenseitig (ein Sub-Träger hat keinen Amplitudenanteil bei den Frequenzen der anderen Sub-Träger)



OFDM – Channels

- **OFDM Kanäle**
  - Ein einzelner OFDM Kanal belegt ein ca. 20MHz breites Segment im Spektrum
  - Das ergibt bis zu 24 nicht überlappende Kanäle (im 5GHz Spektrum)



OFDM – Mathematik

$$\nu(t) = \sum_{k=0}^{N-1} X_k e^{j2\pi kt/T}, \quad 0 \le t < T,$$

$$\frac{1}{T}\int_0^T \left(e^{j2\pi k_1 t/T}\right)^* \left(e^{j2\pi k_2 t/T}\right) dt$$

$$= \frac{1}{T}\int_0^T e^{j2\pi(k_2-k_1)t/T}\, dt = \delta_{k_1 k_2}$$

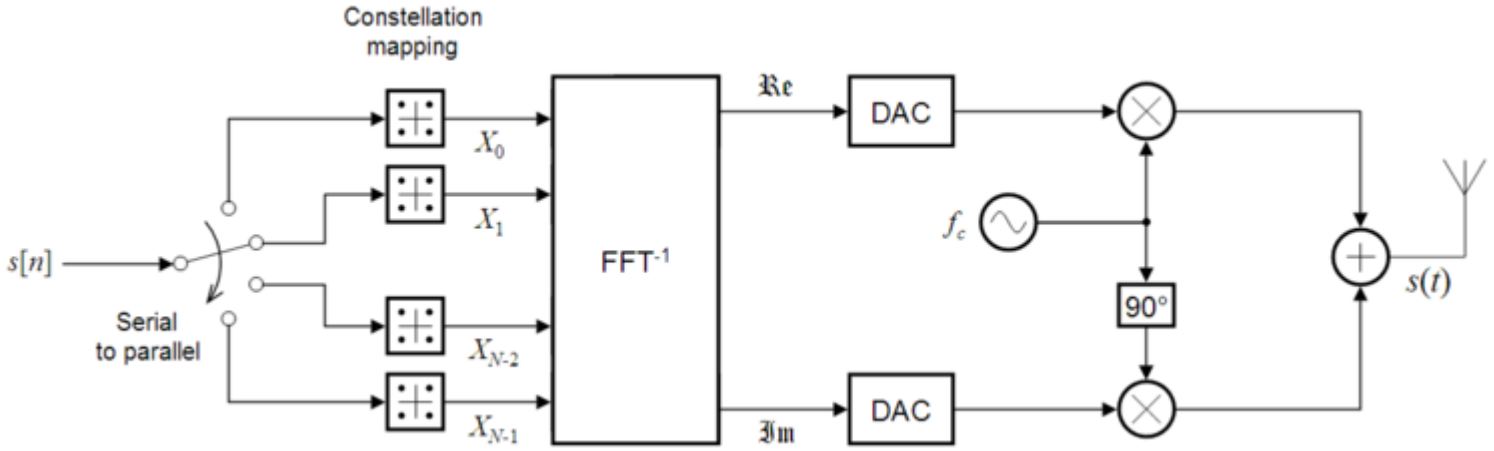
$$\nu(t) = \sum_{k=0}^{N-1} X_k e^{j2\pi kt/T}, \quad -T_{\mathrm{g}} \le t < T$$

$$s(t) = \Re\left\{\nu(t) e^{j2\pi f_c t}\right\}$$

$$= \sum_{k=0}^{N-1} |X_k| \cos\left(2\pi[f_c + k/T]t + \arg[X_k]\right)$$

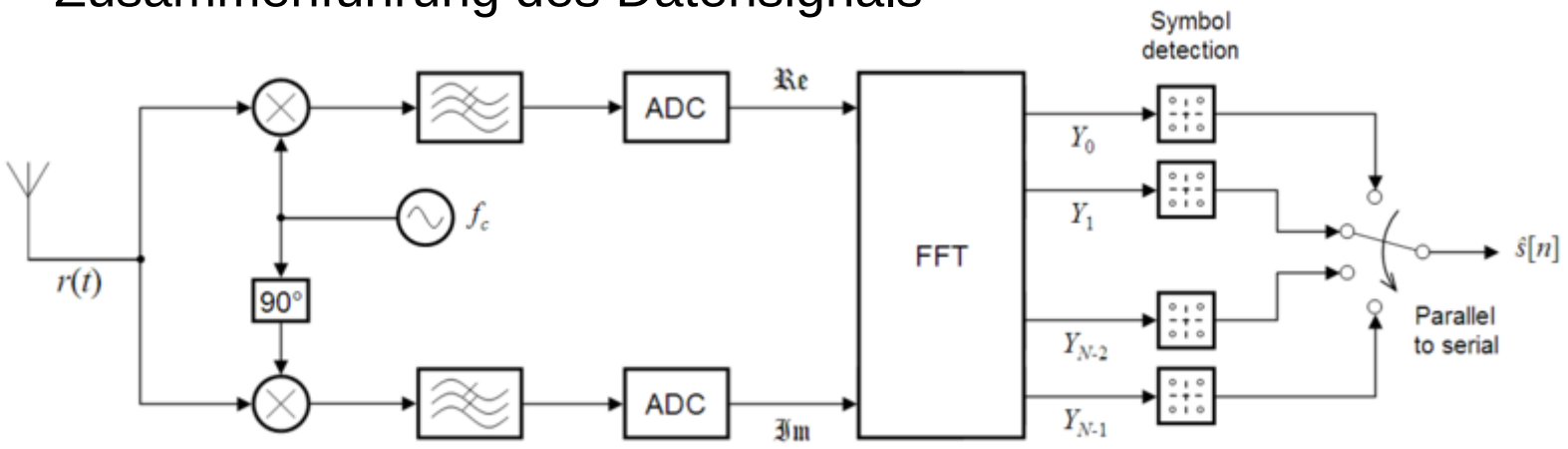
OFDM – Modulation

- **Frequenz Domain**
  - Das Datensignal wird auf *N* Sub-Carrier (Sub-Kanäle) verteilt
- **Inverse Fourier Transformation**
  - Frequenz Spektrum -> I und Q Signale in der Zeit Domain
- **Zeit Domain**
  - I und Q werden zusammengeführt (bekannt von SDR)

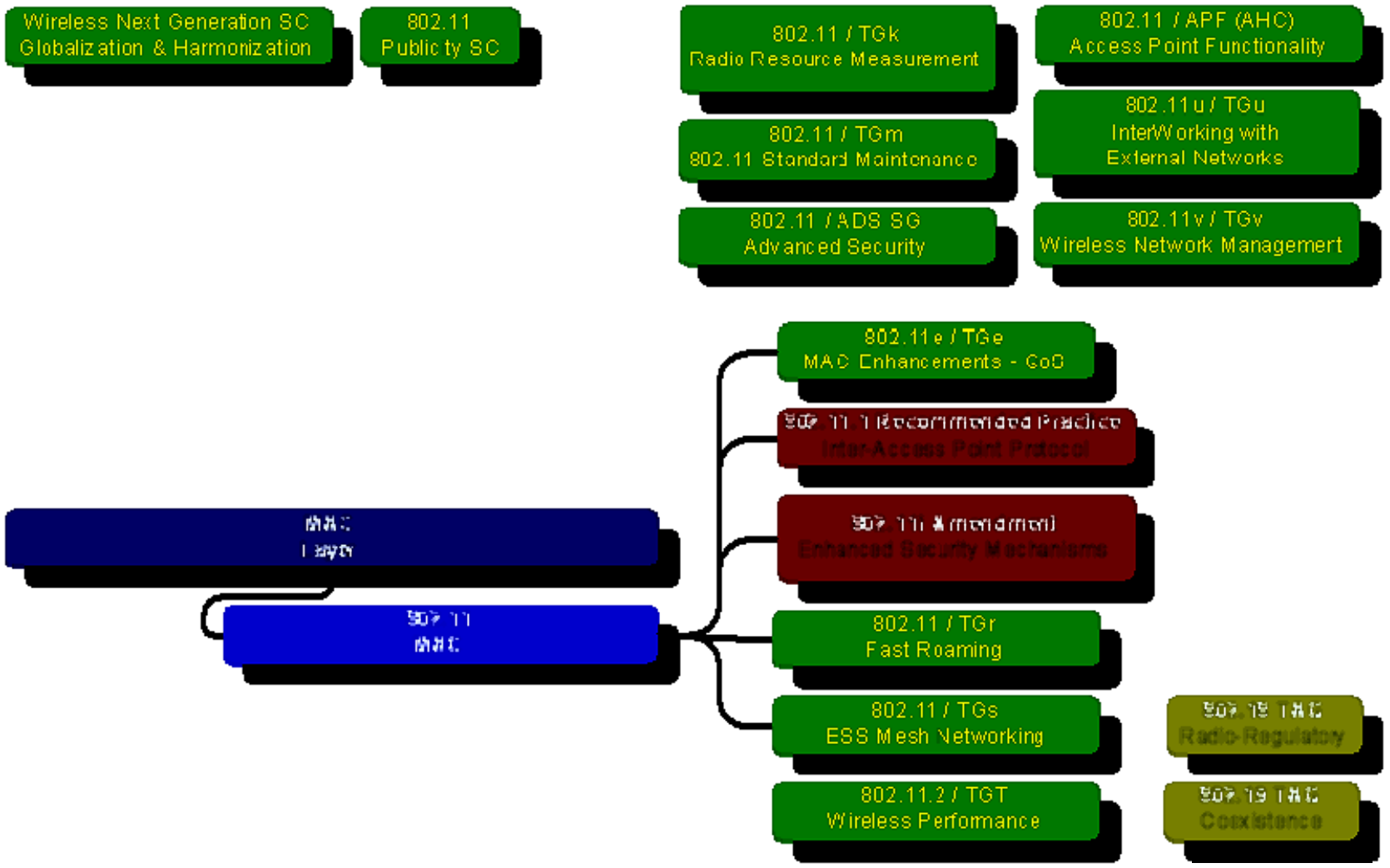


OFDM – Demodulation

- **Zeit Domain**
  - Zerlegung des Signals in I/Q, dann A/D Wandlung
- **Fourier Transformation**
  - Zeitdarstellung -> Frequenzdarstellung (*N* Sub-Carriers)
- **Frequenz Domain**
  - Auswertung der einzelnen Sub-Carrier
  - Zusammenführung des Datensignals



802.11 MAC Layer

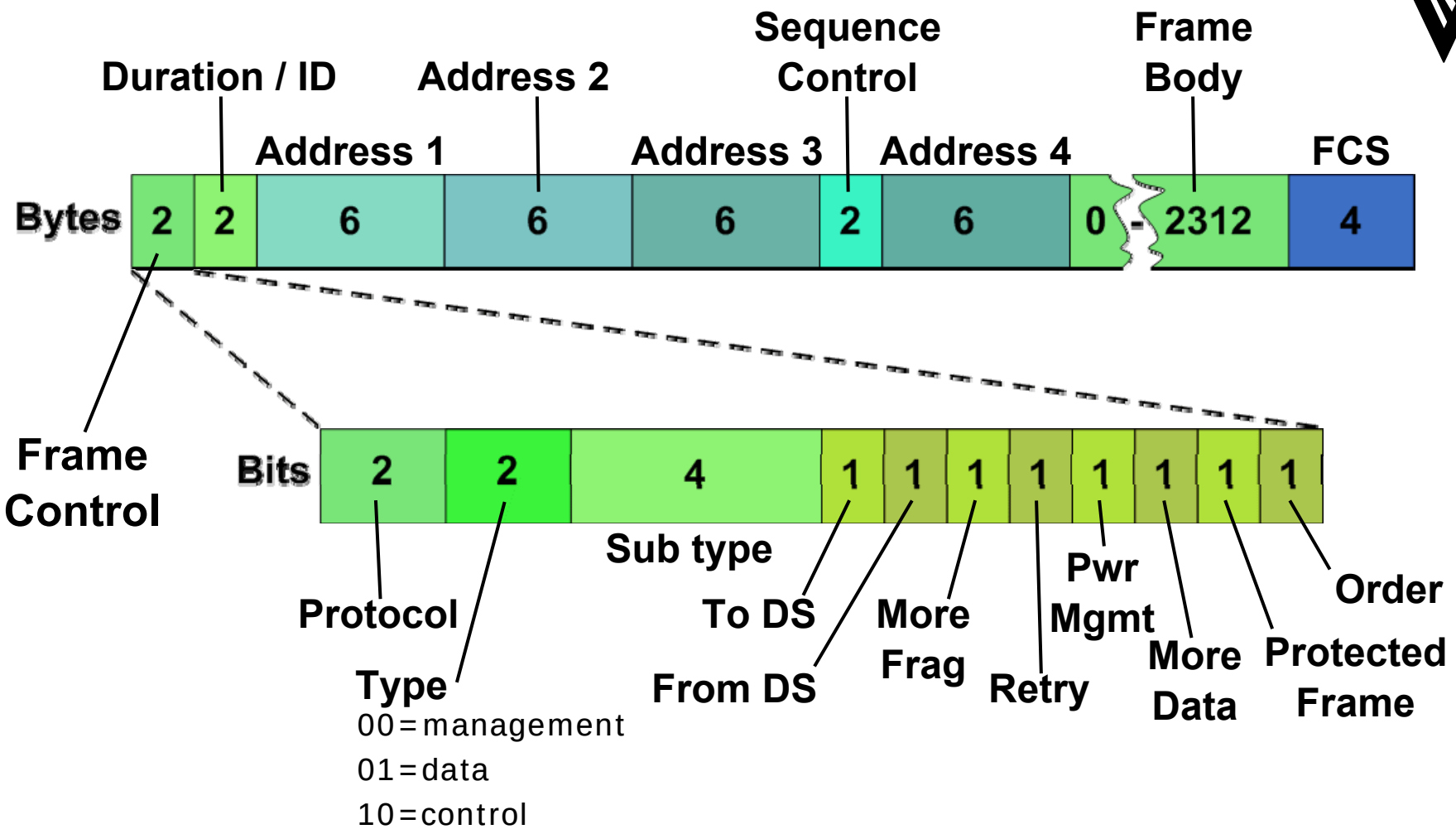


802.11 MAC Layer: Media Access Control

Der Media Access Control Layer definiert:

- **Framing**
  - Generic Frame Format
  - Common Data & Control Frames
  - Common Management Frames
  - Frame Timing
- **Media Access (Zugriff auf den Kanal)**
  - Das “Hidden Node Problem“
  - CSMA/CA in Operation
  - CSMA/CA mit VCD (virtual carrier detection) in Operation
- **Reliable Delivery**
  - Positive ACKs und Retransmissionen
- **Station Association (Anmelden von Stationen)**
- **QoS (Quality of Service)**

802.11 MAC: Generic Frame Format



802.11 MAC: Common Data & Control Frames

- **Daten Frames**
  - Normale Datenpakete
  - Null frame
    - MAC Header mit Power Management Bit gesetzt, ohne Nutzdaten – damit sagt ein Client dem AP, dass er schlafen geht (Power Save Modus).
  - CF-Ack, CF-Poll & CF-Ack+CF-Poll
- **Control Frames**
  - Request to send (RTS) - Anfrage für eine Kanalreservation
  - Clear to send (CTS) - Erlaubnis für den Kanalzugriff
  - Acknowledgement (Ack) - Empfangsbestätigung eines Frames
  - Power Save Poll - Anfrage eines Client im Power Save Modus ob Daten beim AP abzu-holen sind

802.11 MAC: Common Management Frames

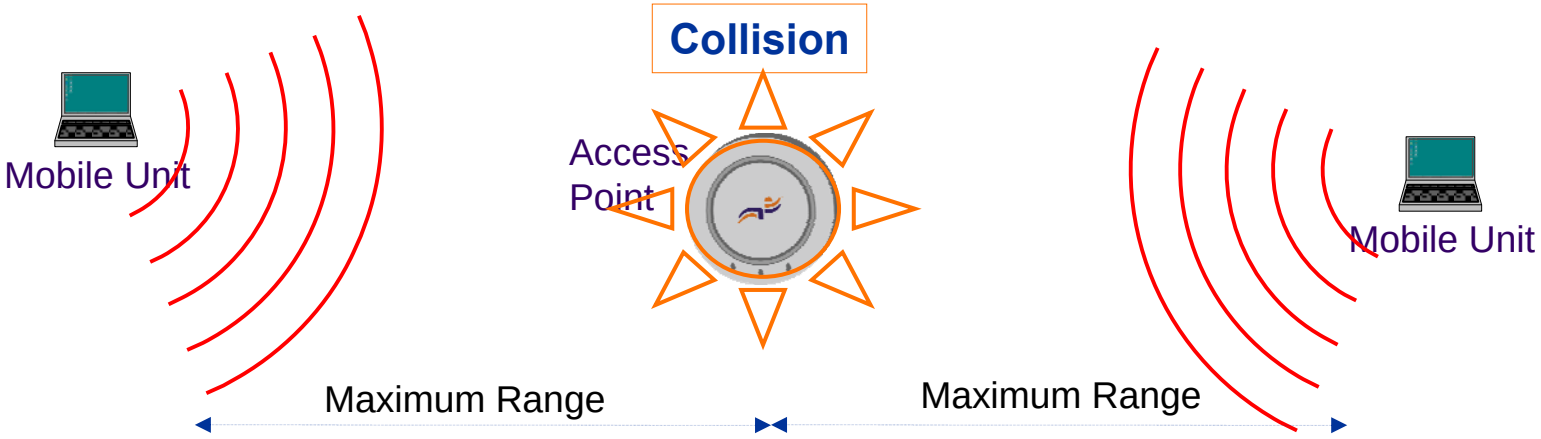
- **Beacon**
  - Broadcast in regelmässigen Intervallen durch den AP (Access Point)
- **Probe / Probe Response**
  - Probes werden von einem Client gesendet um einen spezifischen AP zu finden
  - Der spezifische AP antwortet mit einer Probe Response (“Beacon auf Anfrage”)
- **Association Request / Response**
  - Request eines Clients an einen AP um einem WLAN beizutreten
- **Authentication**
  - Authentifizierung von Clients in einem WLAN

802.11 MAC: Common Management Frames

- **Re-association Request / Response**
  - Verwendet um zwischen verschiedenen AP's im selben WLAN zu Roamen
- **Disassociation / De-authentication**
  - Wird von einem Client gesendet um die Verbindung zum WLAN zu lösen (beenden)

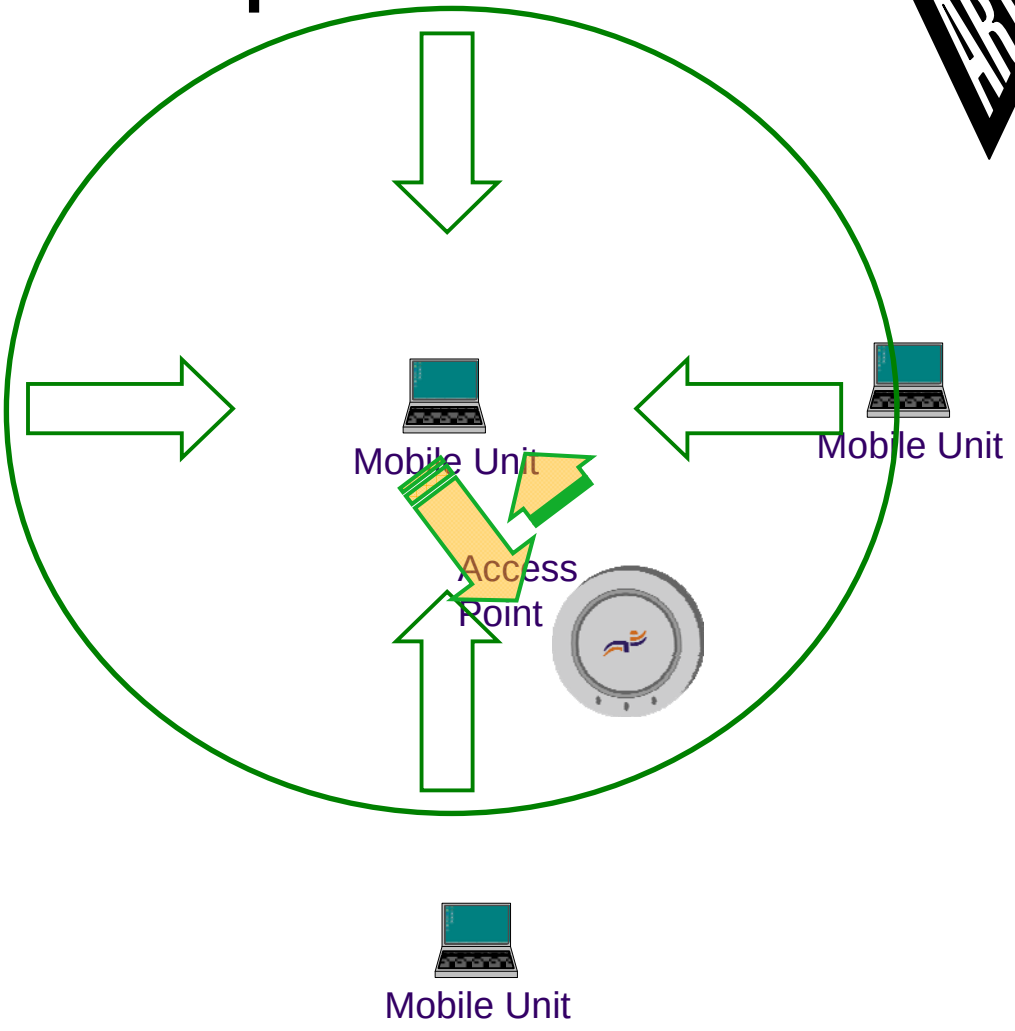
802.11 MAC: Das “Hidden Node Problem”

- **Das “Hidden Node” Problem beschreibt die Situation bei der zwei Clients – die sich nicht gegenseitig sehen können – mit demselben AP verbunden sind.**
  - In einer sehr aktiver WLAN Umgebung kann dies bis zu 40% Datenverlust durch Kollisionen und Retransmissionen verursachen.
  - VCD (RTS/CTS) verhindert diese Probleme.



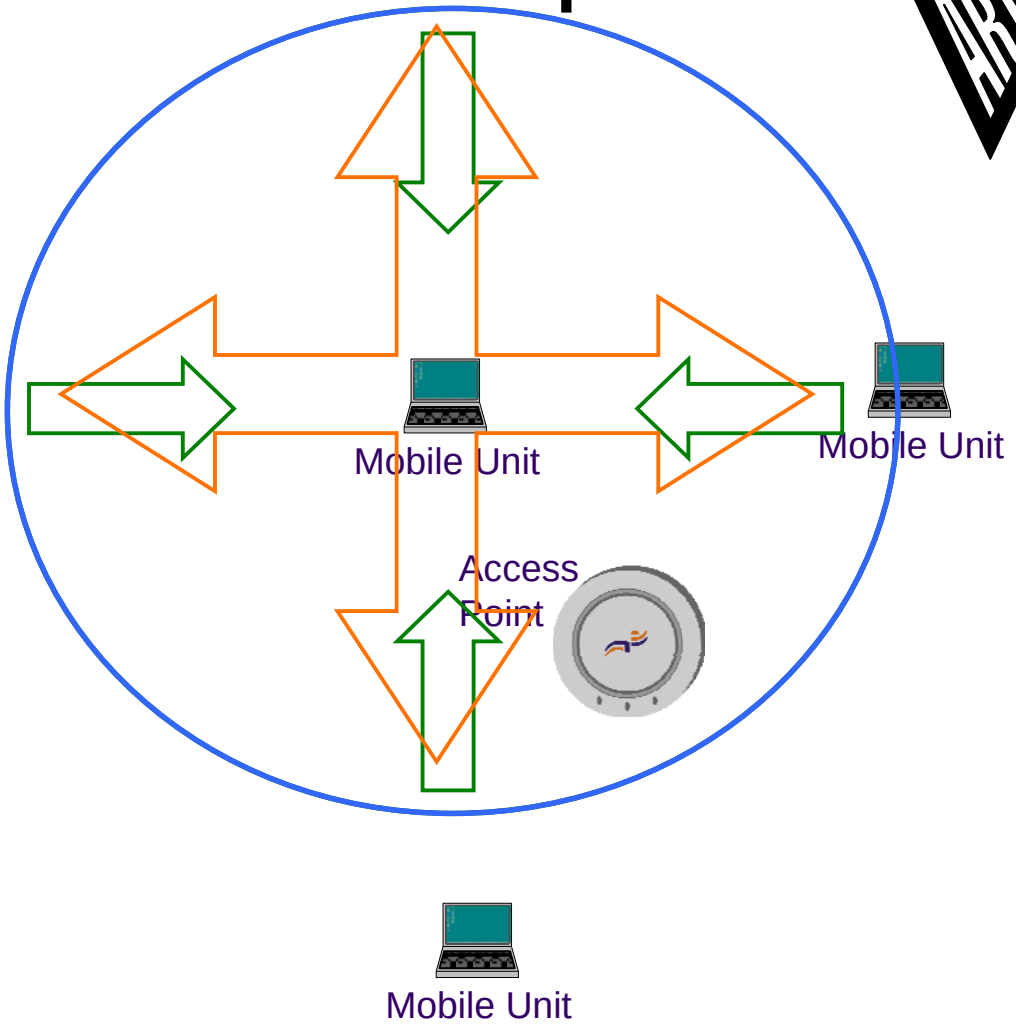
802.11 MAC: CSMA/CA in Operation

1. Clear Channel Assessment
2. Clear Channel ascertained
3. Client sends queued data
4. AP sends Ack



802.11 MAC: CSMA/CA mit VCD in Operation

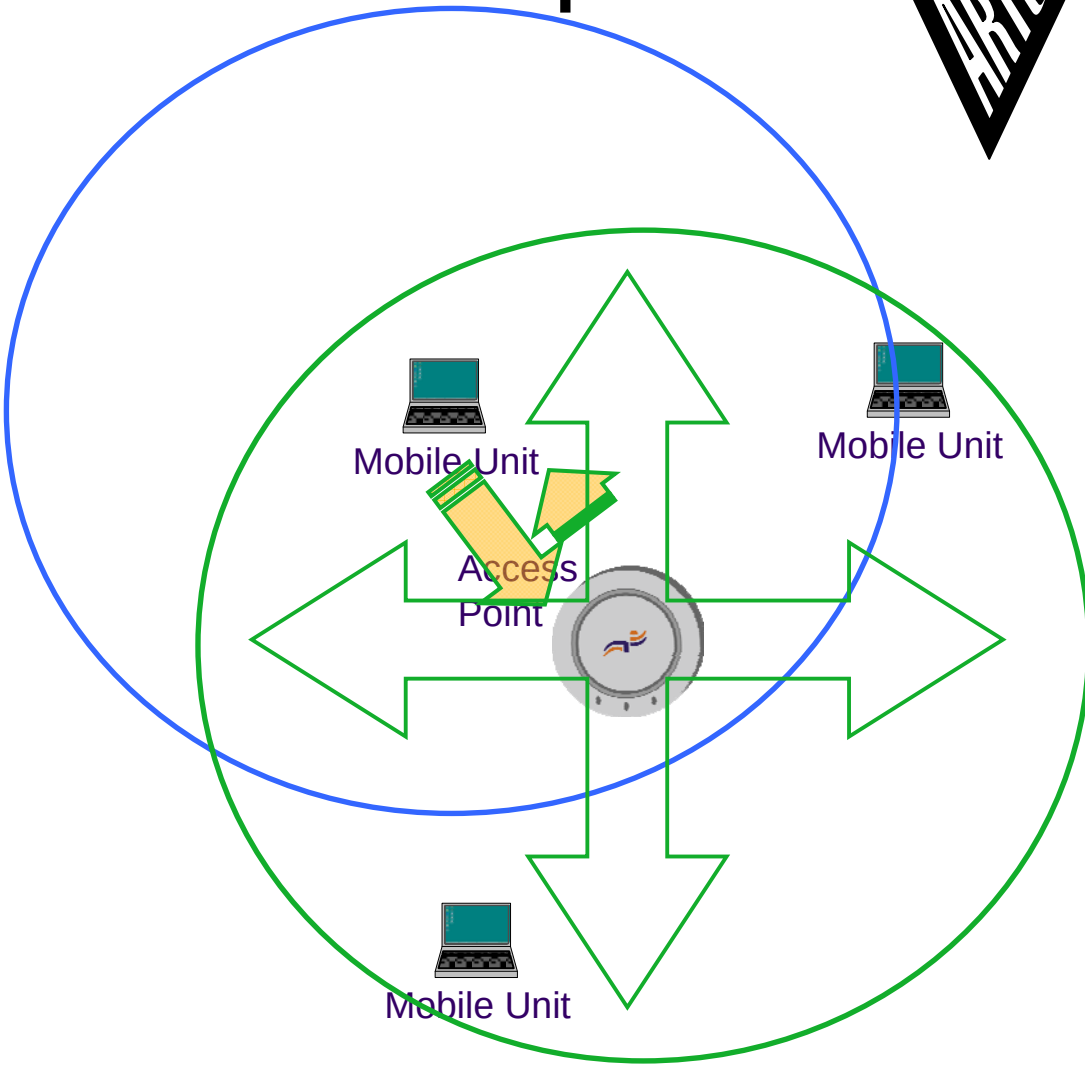
1. Clear Channel Assessment
2. Clear Channel ascertained
3. Request to Send (RTS)



Secure zone of silence centered on the MU

802.11 MAC: CSMA/CA mit VCD in Operation

1. Clear Channel Assessment
2. Clear Channel ascertained
3. Request to Send (RTS)
4. Clear to Send (CTS)
5. Client sends queued data
6. AP sends Ack



Secure zone of silence centered on the AP

802.11 MAC: Reliable Delivery

- **Positive Acknowledgements und Re-Transmissions**
  - Alle Frames werden vom Empfänger bestätigt.
  - Falls ein Frame nicht mit ACK bestätigt wird, wird das Frame wiederholt.
  - RTS threshold: Definiert die Framegrösse ab der RTS/CTS verwendet werden muss.
  - Retry counters
    - Short: für Frames kleiner als der RTS threshold
    - Long: für Frames grösser als der RTS threshold
  - Fragment Lifetime: Fragmente werden nur eine begrenzte Zeit aufbewahrt, danach werden sie verworfen.
  - Protokolle auf höheren Ebenen (Layer 3, z.B. TCP) verwenden ihre eigenen Mechanismen um eine zuverlässige Übertragung sicherzustellen.

802.11 MAC: Reliable Delivery

- **Fragmentierung**
  - Grosse L3 Pakete müssen unter Umständen fragmentiert werden.
  - Fragmentierung kann die Zuverlässigkeit einer Übertragung erhöhen - kleine Pakete haben eine höhere Chance ohne Fehler übertragen zu werden.

IEEE 802.11 WLAN Zusammenfassung

- **Multi-Vendor Interoperability**
- **PHY Layers**
  - **Legacy 802.11:** 1 & 2Mbps im 2.4GHz ISM Band
  - **802.11a:** 6–54Mbps im 5GHz UNII & ISM Band
  - **802.11b:** 5.5 & 11Mbps im 2.4GHz ISM Band
  - **802.11g:** 1–54Mbps im 2.4GHz ISM Band
- **Der MAC Layer**
  - Das Framing und Timing ist optimiert für drahtlose Übertragung.
  - Bietet eine zuverlässige Übertragung durch ACK und Retransmissionen.
- **802.11g und 802.11b Geräte können miteinander kommunizieren**
- **802.11a ist nicht kompatibel mit 802.11b/g**

802.11 Terminologie

- BSS: **Basic Service Set, an 802.11 wireless network with 2 or more stations**
- ESS: **Extended Service Set, a group of 802.11 APs using the same SSID**
- SSID: **Service Set Identifier, a logical wireless network name**
- BSSID: **Basic Service Set Identifier, typically the MAC address of an AP's radio**
- ESSID: **Extended Service Set Identifier, a logical wireless network name**
- IBSS: **Independent BSS, 802.11 stations operating in Ad-hoc mode (i.e. no APs)**
- DCF: **Distributed Coordination Function, contention-based 802.11 channel access**
- PCF: **Point Coordination Function, contention free channel access using polling**
- HCF: **Hybrid Coordination Function, mixed contention and contention free channel access to support 802.11e QoS**

Glossar

Ack : **an acknowledgement frame**
AIFS : **Arbitration Inter Frame Space, used for 802.11e QoS**
BPSK: **Binary Phase Shift Keying, a generic data modulation method**
BSS : **Basic Service Set, an 802.11 wireless network with 2 or more stations**
BSSID : **Basic Service Set Identifier, typically the MAC address of an AP's radio**
CA : **Collision Avoidance**
CCK : **Complementary Code Keying, a data modulation method specified by 802.11b**
CF : **Contention Free, a deterministic media access method**
CSMA : **Carrier Sense Multiple Access, a contention-based (stochastic) media access method**
DBPSK : **Differential BPSK, a data modulation method specified for legacy 802.11 DS systems**
dBr : **Decibel relative to a reference level**
DCF : **Distributed Coordination Function, contention-based 802.11 channel access**
DHCP : **Dynamic Host Configuration Protocol**
DIFS : **Distributed Inter Frame Space, an 802.11 timing value for contention control**
DQPSK : **Differential QPSK , a data modulation method specified for legacy 802.11 DS systems**
DS : **Distribution System, the wired backbone and services interconnecting APs**
DTIM : **Delivery TIM, a beacon element indicating buffered broadcast/multicast traffic**
ESS : **Extended Service Set, a group of 802.11 APs using the same SSID**
ESSID : **Extended Service Set Identifier, a logical wireless network name**
FCS : **Frame Check Sequence**
FEC : **Forward Error Correction**
GFSK : **Gaussian Frequency Shift Keying, a data modulation method specified for legacy 802.11 FH systems**

Glossar

HCF : **Hybrid Coordination Function, mixed contention and contention free channel access to support 802.11e QoS**

IBSS : **Independent BSS, 802.11 stations operating in Ad-hoc mode**

Mbps : **Mega bits per second**

MHz : **Mega Hertz**

MIMO : **Multi Input Multi Output**

MU : **Mobile Unit**

NAV : **Network Allocation Vector, a timer set by the duration field in a received frame that indicates when the channel will next be free for a new transmission**

NIC : **Network Interface Card**

OFDM : **Orthogonal Frequency Division Multiplexing, an RF coding scheme used by 802.11a and 802.11g**

PCF : **Point Coordination Function, contention free channel access using polling**

PIFS : **PCF Inter Frame Space , an 802.11 timing value for contention free operation**

QAM : **Quadrature Amplitude Modulation, a data modulation method specified for 802.11a and 802.11g systems**

QPSK : **Quadrature Phase Shift Keying, a generic data modulation method**

SIFS : **Short Inter Frame Space , an 802.11 timing value allowing priority access for control frames**

SSID : **Service Set Identifier, a logical wireless network name**

TGn Sync : **An industry Alliance with a proposal for 802.11n MIMO**

TIM : **Traffic Indicator Map, a beacon element indicating buffered unicast traffic**

TSPEC : **Traffic Specification, connection characteristics requested by a client station**

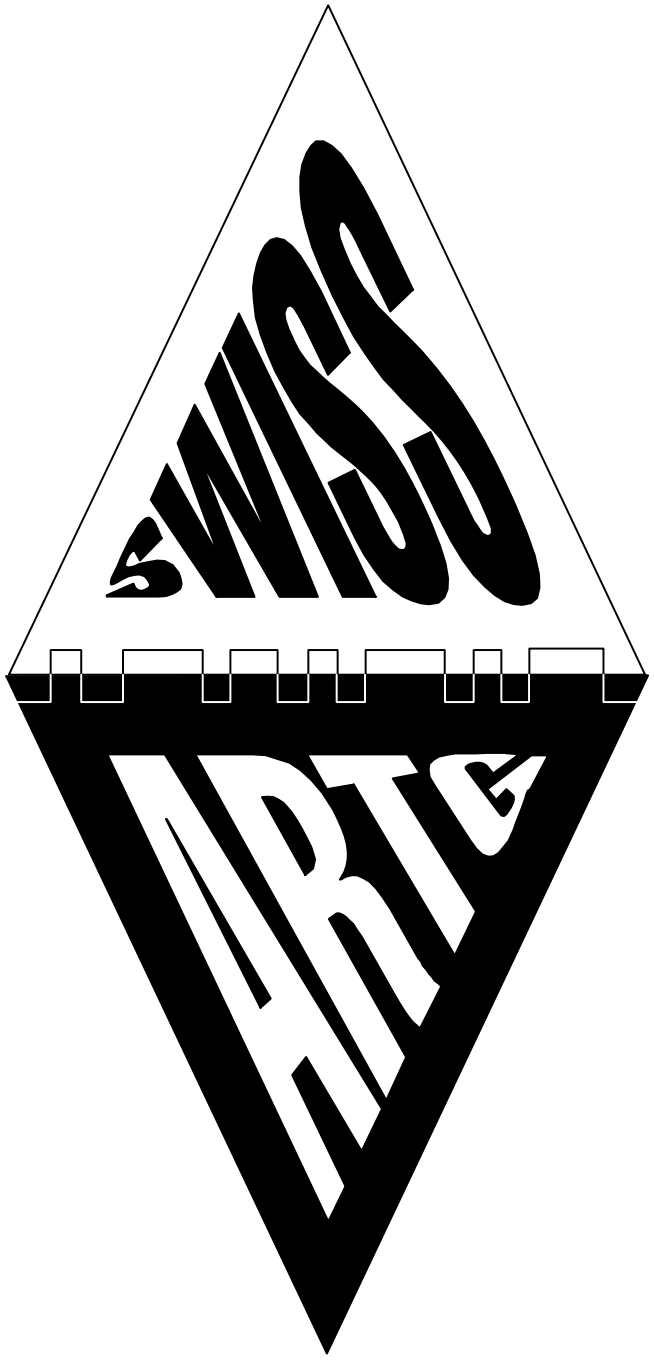
TU : **Timing Unit, equal to 1024µs**

UWB : **Ultra Wide Band**

WWiSe : **An industry Alliance with a proposal for 802.11n MIMO**

SWISS AMATEUR TELEPRINTER GROUP

Fragen ?


SWISS
ABTG