IEEE 802.11 WLAN

Netzwerkgrundlagen

Markus Zeilinger[1]

[1]FH Oberösterreich
Department Sichere Informationssysteme

Sommersemester 2023

FH OBERÖSTERREICH
UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA

Wichtiger Hinweis

Alle Materialien, die im Rahmen dieser LVA durch den LVA-Leiter zur Verfügung gestellt werden, wie zum Beispiel Foliensätze, Audio-Aufnahmen, Übungszettel, Musterlösungen, ... dürfen ohne explizite Genehmigung durch den LVA-Leiter NICHT weitergegeben werden!

Überblick Funktechnologien (unvollständig!)

Distanz	Ausdehnung	Benennung	Technologien
0 m	"Am Körper"	Wireless Body Area Networks (WBAN)	ZigBee, Bluetooth/BLE, Z-Wave, Thread & Matter, EnOcean, RFID/NFC, KNX-RF, IEEE 802.15.4, 6LoWPAN, HomeMatic/BidCoS, DECT ULE, IEEE 802.11 WLAN
1 m	"In Griffweite"	Wireless Personal Area Networks (WPAN)	
10 m 100 m 1 km	Raum Gebäude Campus	Wireless Local Area Network (WLAN)	
10 km	Stadt, Ort	Wireless Metropolitan Area Network (WMAN)	WiMAX
100 km 1000 km	Land/Staat Kontinent	Wireless Wide Area Network (WWAN)	LoRaWAN, SigFox, 3G/4G/5G, NarrowBand-IoT, LTE-M
10000 km	Planet Erde	Internet	

Funktechnologien, Interest Groups, Standards & Links

Technologie	Hersteller/Treiber	Link
Zigbee	Connectivity Standards Alliance (CSA)	https://csa-iot.org/all-solutions/zigbee/
Bluetooth	Bluetooth SIG	https://www.bluetooth.com/
Z-Wave	Z-Wave Alliance	https://z-wavealliance.org/
Thread	The Thread Group	https://www.threadgroup.org/
Matter	Connectivity Standards Alliance (CSA)	https://csa-iot.org/all-solutions/matter/
EnOcean	EnOcean Alliance	https://www.enocean-alliance.org/de/
RFID/NFC	NFC Forum	https://nfc-forum.org/
KNX-RF	KNX Association	https://www.knx.org/
6LoWPAN	6lowpan WG IETF (beendet)	https://datatracker.ietf.org/wg/6lowpan/about/
HomeMatic/BidCoS	eQ-3	https://www.eq-3.de/
DECT ULE	ULE Alliance	https://www.ulealliance.org/
IEEE 802.11 WLAN	Wi-Fi Alliance	https://www.wi-fi.org/
~~WiMAX~~	~~WiMAX Forum~~	~~https://wimaxforum.org/~~
LoRaWAN	LoRa Alliance	https://lora-alliance.org/
SigFox	SigFox	https://www.sigfox.com/
3G/4G/5G, NB-IoT, LTE-M	3GPP	https://www.3gpp.org/

Medium Funk

- Viele Funktechnologien arbeiten auf lizenz- und meist auch genehmigungsfrei nutzbaren Frequenzbändern.
- ISM (Industrial, Scientific and Medical) Band, z. B.
  - 433.05 - 434.79 MHz (Autoschlüssel, Rauchmelder, Babyfon, Thermometer)
  - 2.4 - 2.5 GHz (WLAN, ZigBee, Bluetooth)
  - 5,725 GHz - 5,875 GHz (WLAN)
  - 5,925 Ghz - 7,125 GHz (WLAN, Wi-Fi 6) (!! NEW !!)
- SRD (Short Range Device) Band, z. B.
  - 863 - 870 MHz (Thermometer, Alarmanalagen, ZigBee, IEEE 802.15.4)
- Das Medium Funk ist störungsanfälliger als verdrahtete Kommunikation!
- Am Medium Funk sind Maßnahmen zur Realisierung der Schutzziele der Informationssicherheit Pflicht (Abhörbarkeit)!

IEEE 802.11 Wireless LAN (WLAN)

- IEEE 802.11 ist eine Standard-Familie für drahtlose Kommunikation im LAN-Bereich.
- Der IEEE 802.11 Standard spezifiziert die Bitübertragungsschicht (PHY) und die Media Access Control (MAC) Teilschicht ($\widehat{=}$ Schicht 2).
- Die erste Standardversion wurde 1997 veröffentlicht (aktuell IEEE 802.11-2020).
- Wi-Fi Alliance: Vereinigung von rund 900 Herstellern von Equipment im WLAN-Bereich.
  - Ziel: Sicherstellung der Kompatibilität von WLAN-Produkten verschiedener Hersteller.
- IEEE 802.11 WG: `http://grouper.ieee.org/groups/802/11/`
- WG Status: `http://www.ieee802.org/11/Reports/802.11_Timelines.htm`

IEEE 802.11 Standard - Historie

Jahr	Standard	Frequenz	Datenrate	Bemerkung
1997	IEEE 802.11	2.4 GHz	2 Mbps	Wired Equivalent Privacy (WEP)
1999	IEEE 802.11b	2.4 GHz	11 Mbps	
	IEEE 802.11a	5 GHz	54 Mbps	Wegen Interferenzen mit z. B. Radarsystemen in Europa kaum Verbreitung
2001	WEP broken!	Seit 2001 gilt WEP (bzw. der verwendete Stream Cipher RC4 [1]) als gebrochen!		
2003	IEEE 802.11g	2.4 GHz	54 Mbps	
	WPA	Wi-fi Protected Access (WPA)		
2004	IEEE 802.11i	MAC Security Enhancements (aka Wi-fi Protected Access 2 [WPA2])		
2009	IEEE 802.11n	2.4 & 5 GHz	600 Mbps	MIMO
2011	WPS broken!	Mehrere Schwachstellen in Wi-fi Protected Setup (WPS)		
2013	IEEE 802.11ac	5 GHz	6.93 Gbps	
2017	KRACK	KRACK (Key Reinstallation AttaCK) [2]		
2018	WPA3	Wi-fi Protected Access 3 (WPA3)		
2021	IEEE 802.11-2020	Letzte kummulierte Standard-Version (= IEEE 802.11-2016 + alle Erweiterungen seit 2016)		
2021	IEEE 802.11ax	2.4, 5 & 6 GHz	9.60 Gbps	High Efficiency WLAN (höhere Datenraten, geringer Latenz)
2021	IEEE 802.11ay	60 GHz	20-40 Gbps	Nachfolger IEEE 802.11ad

Quelle: http://www.ieee802.org/11/Reports/802.11_Timelines.htm

IEEE 802.11 Standard - Upcoming

Jahr	Standard	Frequenz	Datenrate	Bemerkung
2025?	IEEE 802.11be	2.4, 5 & 6 GHz	30 Gbps	Extremely High Throughput (EHT) (IEEE 802.11ax Nachfolger)
2026?	IEEE 802.11bi			Enhanced Data Privacy
2024?	IEEE 802.11bh			Randomized and Changing MAC Addresses

Quelle: http://www.ieee802.org/11/Reports/802.11_Timelines.htm

Aktuelle Zertifizierungsprogramme der Wi-fi Alliance

- Im Oktober 2018 veröffentlicht die Wi-fi Alliance ein neues Benennungsschema für WLAN-Generationen[1]:
  - Wi-Fi 1-3: Legacy IEEE 802.11b-g
  - Wi-Fi 4: IEEE 802.11n
  - Wi-Fi 5: IEEE 802.11ac (State-of-the-Art)
  - Wi-Fi 6: IEEE 802.11ax (State-of-the-Art)
  - Wi-Fi 6E[2]: IEEE 802.11ax im 6 GHz Bereich
  - Wi-Fi 7[3]: IEEE 802.11be (angekündigt)

[1] https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-6

[2] https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-brings-wi-fi-6-into-6-ghz

[3] https://www.wi-fi.org/who-we-are/current-work-areas#Wi-Fi%207

WLAN Equipment

- NICs für Endgeräte (Station, STA)
  - Via (Mini-)PCI(e), USB, früher: PCMCIA und Cardbus
- Access Points (AP)
  - Erlauben Kommunikation zw. den STAs im WLAN und zw. den STAs und dem verdrahteten Netz.
- WLAN Router, WLAN Repeater, Mesh Router
  - Equipment mit WLAN-Schnittstelle und erweiterten Funktionen (z. B. DSL/Kabel Modem, Switch, Firewall, Mesh Funktionalität, ...)
- Antennen
  - Rundstrahlantennen zur Abdeckung von Flächen (Räume, Stockwerke, Areale).
  - Richtfunkantennen (für Punkt-zu-Punkt-Verbindungen, z. B. zwischen Gebäuden).
  - Multi Input Multi Output (MIMO) Technik.

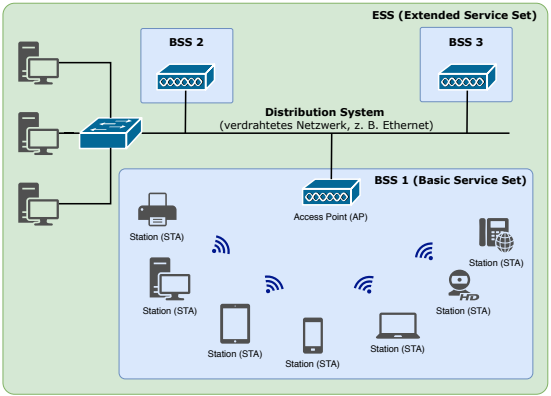


Abbildung 1: Infrastructure Mode: Der AP stellt die Kommunikation zwischen den STAs und vom/ins verdrahtete Netzwerk (Distribution System) sicher.

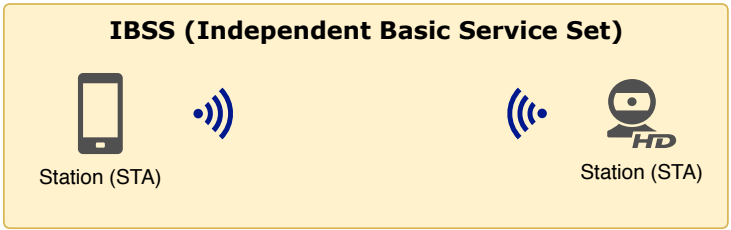


Abbildung 2: Ad-hoc Mode: Direkte STA zu STA Kommunikation ohne Infrastruktur.

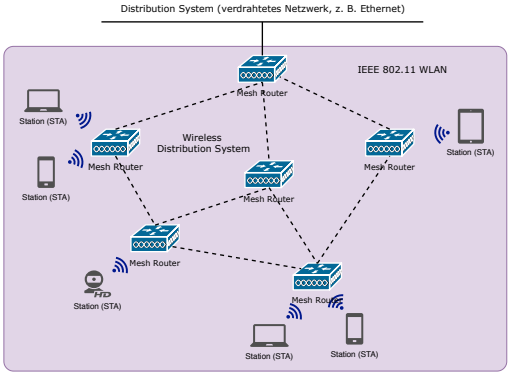
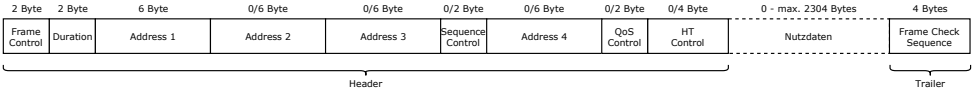


Abbildung 3: Mesh Mode (IEEE 802.11s): Das Distribution System kann (auch) drahtlos sein, d. h. Mesh Router können Daten über die drahtlose Schnittstelle an andere Mesh Router weitergeben.

- Basic Service Set (BSS) = ein Access Point (AP) und die damit assoziierten Stations (STA).
- Independent Basic Service Set (IBSS) = die STAs eines Ad-hoc-Netzwerks.
- Extended Service Set (ESS) = mehrere BSS und Systeme im verdrahteten Netz verbunden über ein Distribution System (DS) (z. B. Campus WLAN).
- BSSID, IBSSID = MAC-Adresse des APs am WLAN Interface im BSS o. zufällig generiert im IBSS.
- ESSID, SSID = logischer Name des ESS (z. B. fhhgb, eduroam).

Frame Format nach IEEE 802.11



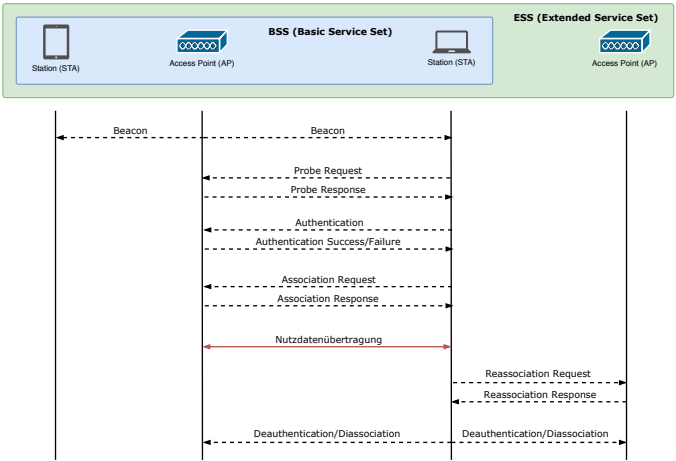
- IEEE 802.11 WLAN kennt drei verschiedene Frame-Typen (definiert in Frame Control [FC]):
  - Management Frames: Steuerung der Services eines IEEE 802.11 WLANs, v. a. Ausgleich der fehlenden Link-Charakteristik.
  - Control Frames: Medienzugriffssteuerung, Acknowledgements
  - Data Frames: Nutzdaten
- Die vier Adressfelder werden je nach Quelle und Ziel des Frames (STA $\rightarrow$ STA, STA $\rightarrow$ Ethernet, Ethernet $\rightarrow$ STA, ...) genutzt.
- Für IEEE 802.11/802.11a/b/g/n/ac ist die max. Framegröße 2304 Bytes, für IEEE 802.11ad 7920 Bytes (Maximum Transmission Unit, MTU) (s. [3, S. 768]).

Management Frames I

- Steuerung der Services eines IEEE 802.11 Netzwerks (z. B. Auffinden von APs, An-/Abmelden vom Netzwerk, ...).
- Ausgleichen der fehlenden Link-Charakteristik.

Subtype	Bezeichnung	Beschreibung
0000	Association Request	Erstellen und Übertragen von AP-STA-Beziehungen (= Associations).
0001	Association Response	
0010	Reassociation Request	
0011	Reassociation Request	
0100	Probe Request	Auffinden von APs/Netzen (allgemein oder bestimmt).
0101	Probe Response	
1000	Beacon	Signalisierung seiner Dienste durch einen AP.
1010	Diassociation	Löschen einer Association.
1011	Authentication	De-/Authentifizierung einer STA an einem AP.
1100	Deauthentication	
...	...	...

Management Frames II



Medienzugriffssteuerung (CSMA/CA) I

- IEEE 802.11 definiert eine s. g. Distributed Coordination Function (DCF) als Verfahren zur Medienzugriffssteuerung (dezentral, CSMA/CA)
- CSMA/CA = Carrier Sense Multiple Access with Collision Avoidance (vs. Detection bei CSMA/CD im Ethernet!)
  - Im Medium Funk sind Kollisionen wesentlich häufiger als auf einem Kabel.
  - Funkeinheit arbeitet Half-Duplex, d. h. gleichzeitiges Senden und Empfangen (Horchen auf Kollisionen während des Sendens) ist nicht möglich.
  - $\rightarrow$ Kollisionen verhindern, NICHT erkennen (Collision Avoidance)!

Medienzugriffssteuerung (CSMA/CA) II

1. Physikalische Carrier-Sense-Funktion, d. h. Horchen, ob das Medium frei ist.
2. Virtuelle Carrier-Sense-Funktion
   - Steuerung über einen Timer, s. g. Network Allocation Vector (NAV).
   - Dieser Timer wird durch Duration/ID-Werte aus empfangenen Frames gesetzt/aktualisiert.
   - Die im NAV gespeicherte Zeit wird gewartet, um laufende Übertragungen nicht zu unterbrechen.
3. Nach Ablauf des NAV + Medium ist frei + nach einer zufälligen Backoff-Zeit, erfolgt das Senden des Datenframes.
4. Empfänger sendet nach Empfang des Frames eine Bestätigung (ACK).
5. Nur wenn der Sender das ACK innerhalb einer definierten Zeitspanne empfängt, gilt das Frame als korrekt übertragen (ansonsten Retransmission).

Medienzugriffssteuerung (CSMA/CA) III

- Hidden-Station-Problem
  - Drei STAs A, B und C, B sieht/kennt A und C, A und C sehen/kennen einandern nicht (Funkreichweite).
  - Beide STAs A und C beginnen gleichzeitig, an B zu senden $\rightarrow$ Kollision.
  - Lösung: Request-to-Send (RTS) & Clear-to-Send (CTS) Mechanismus.

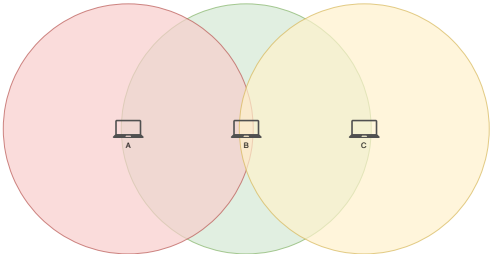


Abbildung 4: Hidden-Station-Problem: STA B ist in Funkreichweite von STA A und STA C, die beiden aber nicht in der des jeweils anderen. Beginnnen STA A und STA C gleichzeitig an B zu senden, kommt es zu einer Kollision.

Medienzugriffssteuerung (CSMA/CA) IV

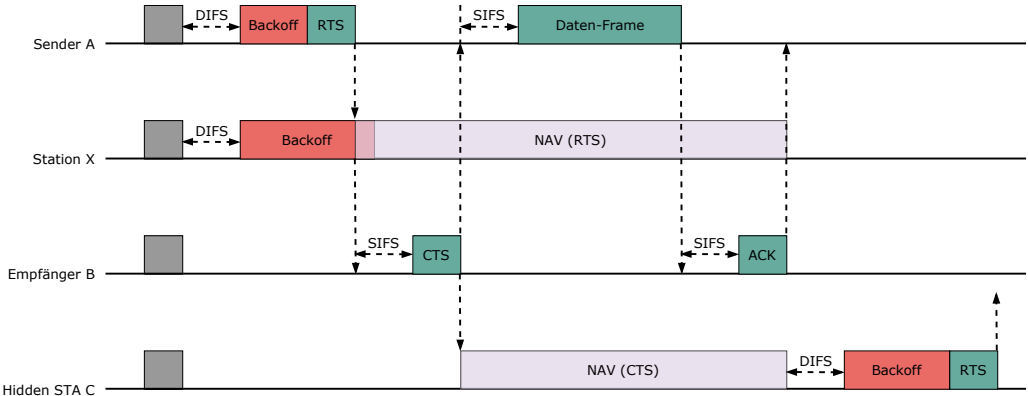
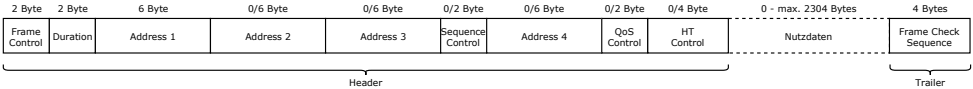


Abbildung 5: CSMA/CA mit RTS/CTS-Mechanismus zur Behebung des Hidden-Station-Problems (DIFS = DCF Interframe Space, SIFS = Short Interframe Space).

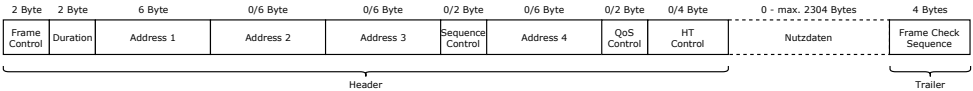
Add-Ons (Zusatzmaterial)

Allgemeines Frame Format nach IEEE 802.11



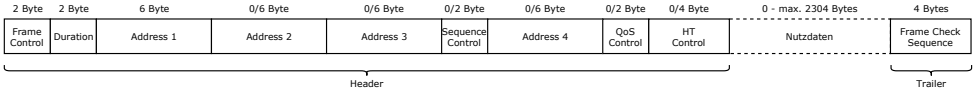
- Frame Control (FC): Bitmap, u. a. zur Spezifikation des Frame Types, des Frame Subtypes und der verwendeten Adressfelder.
- Duration/ID: I. A. die Übertragungsdauer des Frames für die Medienzugriffssteuerung (virtuelle Carrier-Sense-Funktion) (Details s. [3, S. 766]).

Allgemeines Frame Format nach IEEE 802.11 II



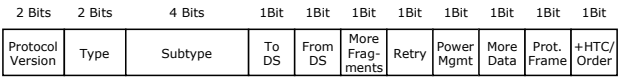
- Address 1-4: Je nach Quelle und Ziel und deren Position im drahtlosen oder verdrahteten Netz werden ein bis alle der vier Adressfelder genutzt.
  - Destination Address (DA): Ziel des Frames.
  - Source Address (SA): Quelle des Frames.
  - Receiver Address (RA): Empfänger des Frames (z. B. Access Point).
  - Transmitter Address (TA): Sender des Frames (z. B. Access Point).
- IEEE 802.11 Adressen sind 48-Bit MAC Adressen.

Allgemeines Frame Format nach IEEE 802.11 III



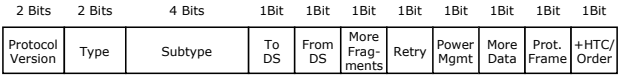
- Frame Body: Für IEEE 802.11/802.11a/b/g/n/ac ist die max. Framegröße 2304 Bytes, für IEEE 802.11ad 7920 Bytes (Maximum Transmission Unit, MTU) (s. [3, S. 768]).
- Frame Check Sequence (FCS): Prüfsumme für die Fehlererkennung, CRC (Cyclic Redundancy Check Verfahren), s. Ethernet.

Frame Control (FC) I



- Type: Typ des IEEE 802.11 Frames
  - Management Frame (00): Steuerung der Services eines IEEE 802.11 WLANs, Ausgleich der fehlenden Link-Charakteristik
  - Control Frame (01): Medienzugriffsteuerung, Acknowledgements, ...
  - Data Frame (10): Nutzdaten
- Subtype: Untertyp, spezifiziert den Typ genauer, z. B. Type = 00 (Management Frame) + Subtype = 1000 (Beacon Frame).

Frame Control (FC) II



- ToDS & FromDS: Gibt an, ob Ziel oder Quelle im Distribution System (DS) liegen und gibt damit die Nutzung und Interpretation der vier Adressfelder vor.

#	ToDS	FromDS	Address 1	Address 2	Address 3	Address 4
1	0	0	RA = DA	TA = SA	BSSID	n/a
2	0	1	RA = DA	TA = BSSID	SA	n/a
3	1	0	RA = BSSID	TA = SA	DA	n/a
4	1	1	RA	TA	DA	SA

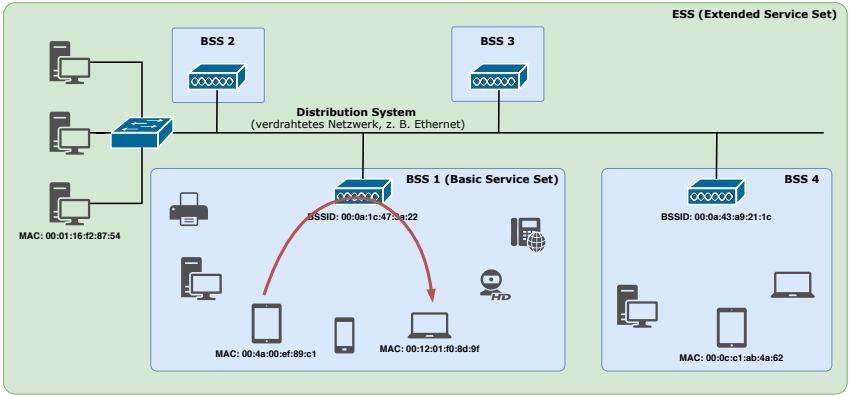
- In den meisten Management und in allen Control Frames sind ToDS und FromDS auf 0 gesetzt!

Frame Control (FC) III

2 Bits	2 Bits	4 Bits	1Bit	1Bit	1Bit	1Bit	1Bit	1Bit	1Bit	1Bit
Protocol Version	Type	Subtype	To DS	From DS	More Frag-ments	Retry	Power Mgmt	More Data	Prot. Frame	+HTC/ Order

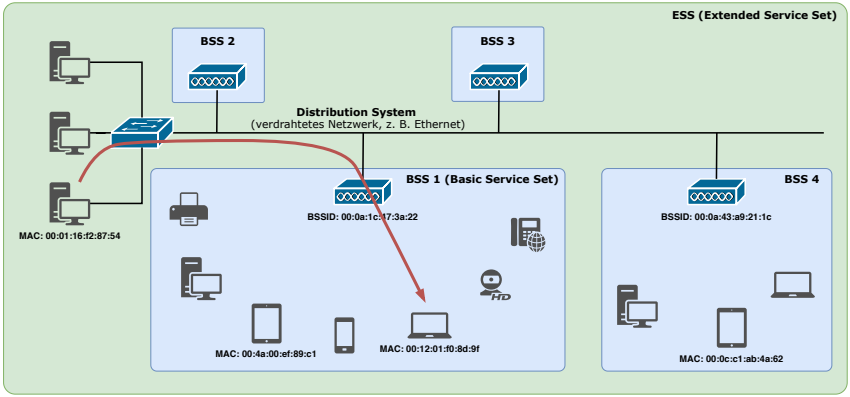
- Protected Frame: Gibt an, ob der Frame Body kryptographisch geschützt ist (egal ob WEP, WPA, WPA2 oder WPA3).

Intra-BSS Datenverkehr



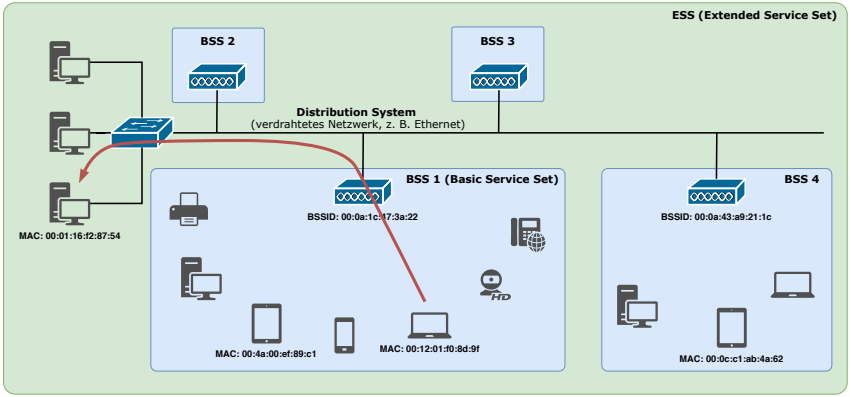
#	ToDS	FromDS	Address 1	Address 2	Address 3	Address 4
1	0	0	00:12:01:f0:8d:9f	00:4a:00:ef:89:c1	00:0a:1c:47:3a:22	n/a

Frame aus dem DS



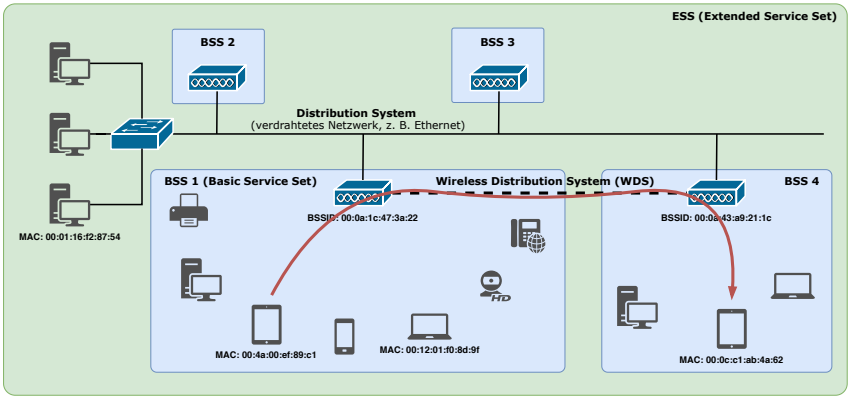
#	ToDS	FromDS	Address 1	Address 2	Address 3	Address 4
2	0	1	00:12:01:f0:8d:9f	00:0a:1c:47:3a:22	00:01:16:f2:87:54	n/a

Frame in das DS



#	ToDS	FromDS	Address 1	Address 2	Address 3	Address 4
3	1	0	00:0a:1c:47:3a:22	00:12:01:f0:8d:9f	00:01:16:f2:87:54	n/a

Inter-BSS Datenverkehr über ein Wireless Distribution System (WDS)



#	ToDS	FromDS	Address 1	Address 2	Address 3	Address 4
4	1	1	00:0a:43:a9:21:1c	00:0a:1c:47:3a:22	00:0c:c1:ab:4a:62	00:4a:00:ef:89:c1

Referenzen I

[1] S. Fluhrer, I. Mantin und A. Shamir, Weaknesses in the key scheduling algorithm of RC4, 2001. DOI: 10.1007/3-540-45537-x_1.

[2] M. Vanhoef und F. Piessens, „Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2,“, 2017, ISBN: 9781450349468. DOI: 10.1145/3133956.3134027.

[3] „IEEE Standard for Information Technology–Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks–Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,“ Techn. Ber., 2021, S. 1–4379. DOI: 10.1109/IEEESTD.2021.9363693.

UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA
OBERÖSTERREICH