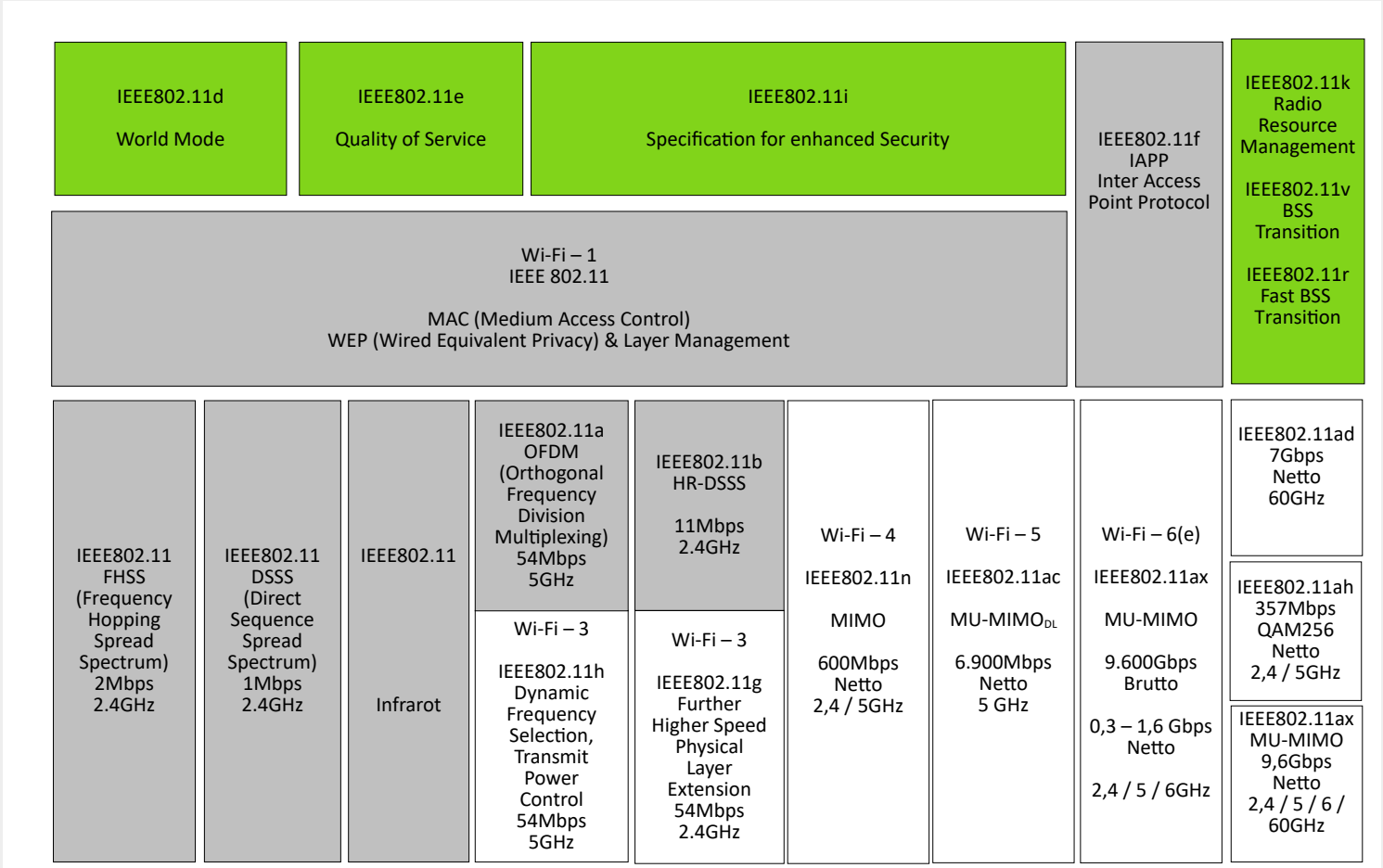
WLAN-Vorlesung
Teil-7

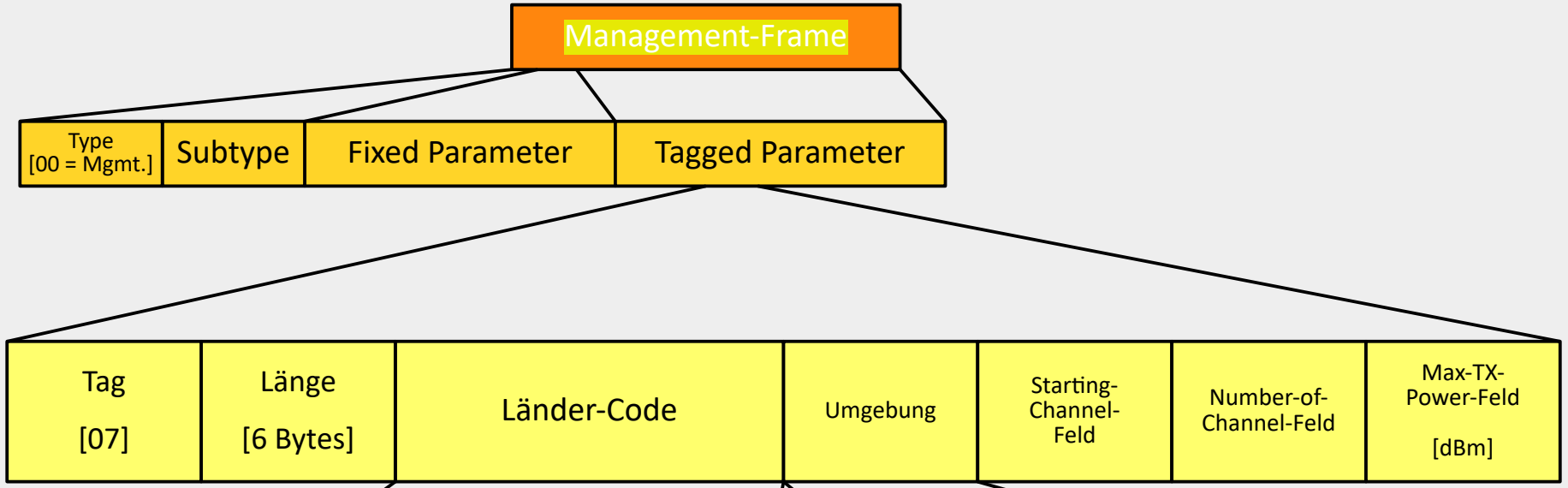
Inhalt

- Zusätzliche Standards im Zusammenhang mit IEEE802.11
  - Übersicht
  - World Mode
  - Quality of Service (QoS)
  - Handover
  - WPA
- Management Frames
- Anmeldungsverfahren
  - Scanning
  - Authentifizierung
  - Assoziierung

Übersicht


IEEE802.11d
World Mode
IEEE802.11e
Quality of Service
IEEE802.11i
Specification for enhanced Security
IEEE802.11f
IAPP
Inter Access
Point Protocol
IEEE802.11k
Radio
Resource
Management
IEEE802.11v
BSS
Transition
IEEE802.11r
Fast BSS
Transition
Wi-Fi – 1
IEEE 802.11
MAC (Medium Access Control)
WEP (Wired Equivalent Privacy) & Layer Management
IEEE802.11
FHSS
(Frequency
Hopping
Spread
Spectrum)
2Mbps
2.4GHz
IEEE802.11
DSSS
(Direct
Sequence
Spread
Spectrum)
1Mbps
2.4GHz
IEEE802.11
Infrarot
IEEE802.11a
OFDM
(Orthogonal
Frequency
Division
Multiplexing)
54Mbps
5GHz
Wi-Fi – 3
IEEE802.11h
Dynamic
Frequency
Selection,
Transmit
Power
Control
54Mbps
5GHz
IEEE802.11b
HR-DSSS
11Mbps
2.4GHz
Wi-Fi – 3
IEEE802.11g
Further
Higher Speed
Physical
Layer
Extension
54Mbps
2.4GHz
Wi-Fi – 4
IEEE802.11n
MIMO
600Mbps
Netto
2,4 / 5GHz
Wi-Fi – 5
IEEE802.11ac
MU-MIMO$_{DL}$
6.900Mbps
Netto
5 GHz
Wi-Fi – 6(e)
IEEE802.11ax
MU-MIMO
9.600Gbps
Brutto
0,3 – 1,6 Gbps
Netto
2,4 / 5 / 6GHz
IEEE802.11ad
7Gbps
Netto
60GHz
IEEE802.11ah
357Mbps
QAM256
Netto
2,4 / 5GHz
IEEE802.11ax
MU-MIMO
9,6Gbps
Netto
2,4 / 5 / 6 /
60GHz

World Mode



Länder-Code-Beispiel	Länderkennung	Land
44 45	DE	Deutschland
46 52	FR	Frankreich
49 54	IT	Italien
55 53	US	USA

Ländercode	Umgebung
20	offen und geschlossen
49	geschlossen
4F	offen

Quality of Service (QoS)

ACI	AC	Description
0	AC_BE	Best Effort
1	AC_BK	Background
2	AC_VI	Video
3	AC_VO	Voice

Stationen die QoS bearbeiten können, werden QoS Stations (QSTAs) genannt.
Access Points mit dieser Fähigkeit werden QoS APs (QAPs) genannt.
Die entsprechenden BSS werden QBSS genannt.

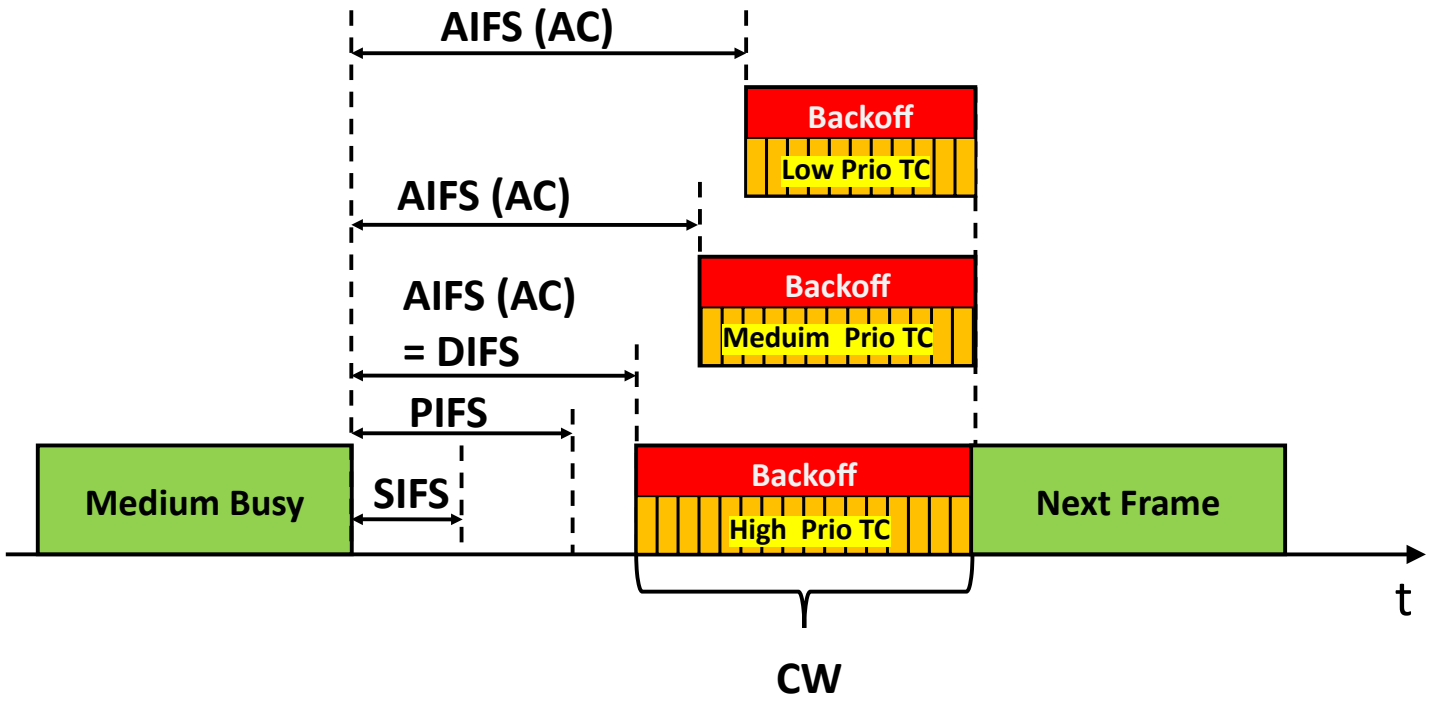
Es gibt 4 so genannte Access Kategorien (ACs)

- Best Effort
- Background
- Video
- Voice

Die ACs werden mit einem AC-Index (ACI) verwaltet.

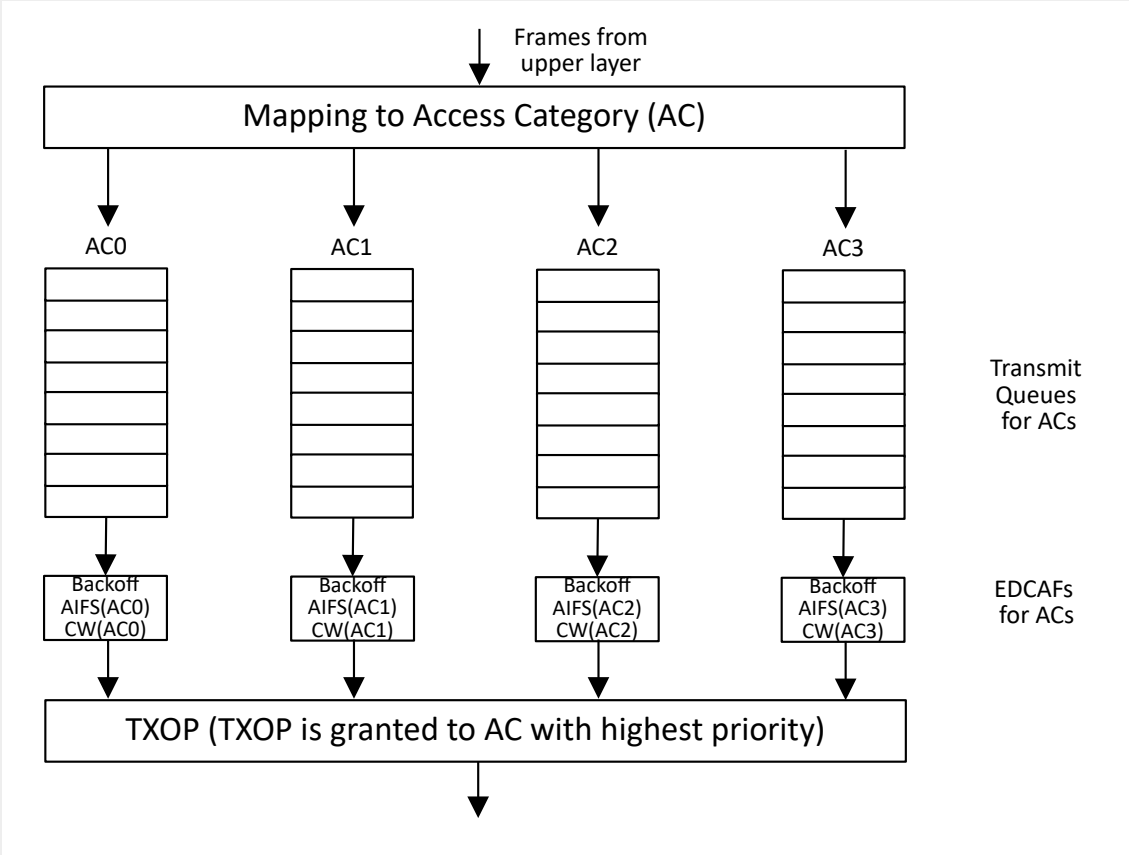
Der Zugriff auf das Medium ist neu zu organisieren.
Dazu dient der Enhanced Distributed Channel Access (EDCA)
Die Durchführung erfolgt in der EDCA-Function (EDCAF)

Abbildung der Prioritäten auf das Contention Window (CW)

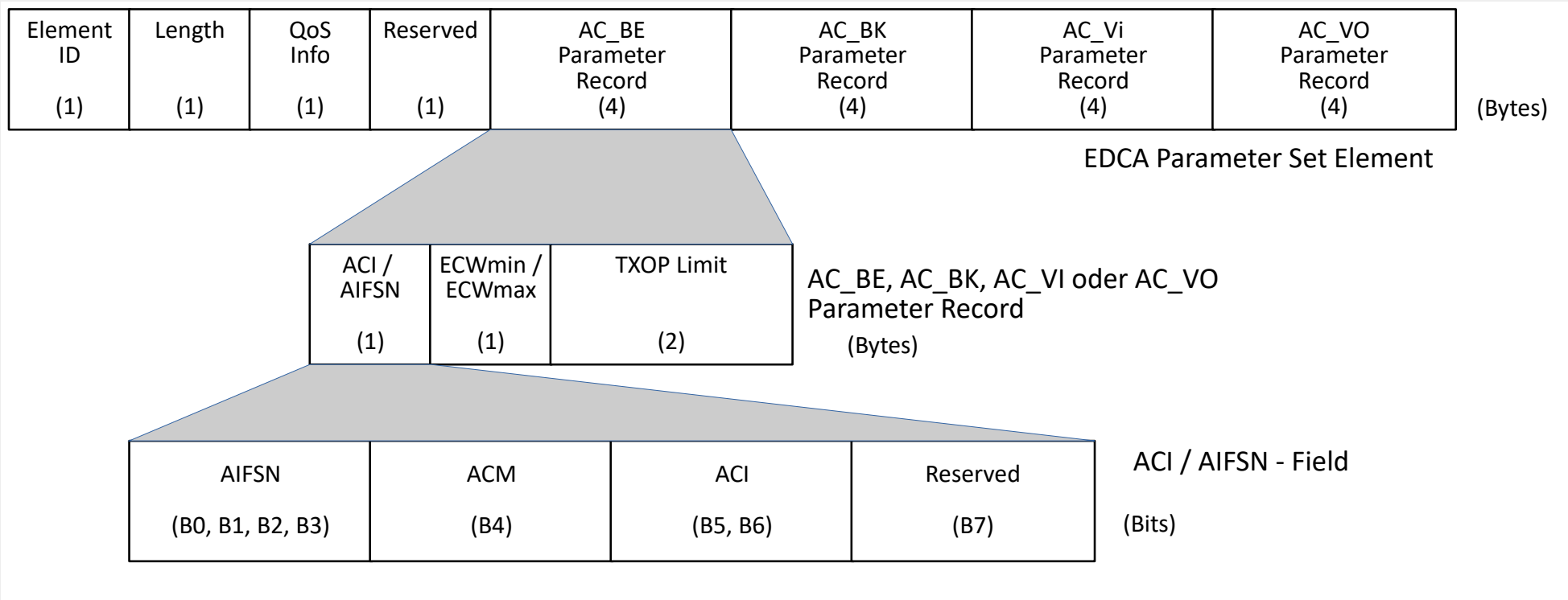


Prioritätenzuordnung

Priority	User Priority (UP)	Access Category (AC)	Designation
Lowest	1	AC_BK	Background
	2	AC_BK	Background
	0	AC_BE	Best Effort
	3	AC_BE	Best Effort
	4	AC_VI	Video
	5	AC_VI	Video
	6	AC_VO	Voice
Highest	7	SC_VO	voice



EDCA Parameter



Verbesserung des Handover

Erster Ansatz mit **IEEE802.11f** (Inter Access Point Protocol (IAPP)
(wurde 2003 verabschiedet und 2006 als Standard zurückgezogen)

Mit den Standards **IEEE802.11k,v,r** wird das so genannte Seamless Roaming ermöglicht.

IEEE802.11k ist dafür zuständig, dass die APs Bewegungen von Stationen mit dem Radio Ressource Management überwachen.

IEEE802.11v
Erkennt ein AP, dass eine Station dabei ist die Funkzelle zu verlassen, signalisiert sie das der Station. Daraufhin kann die Station eine Tabelle anfordern, in der die APs in der Umgebung mit Kanälen und Auslastung übermittelt wird. Damit kann die Station den optimalen nächsten AP auswählen.

IEEE802.11r (Fast-BSS-Transition = FT) wurde 2008 verabschiedet.
Übergang muss innerhalb von 50ms erfolgen um eine Sprachübertragung von VoIP zu ermöglichen

IEEE802.11i (WPA)

Da der Standard IEE802.11 mit der Wired Equivalent Privacy (WEP) nicht als sicher eingestuft wurde, musste an der Sicherheit nachgebessert werden.
Dazu wurde die Sicherheitsarchitektur Wi-Fi-Protected Access (WPA) entwickelt.

Umzusetzen waren die folgenden Forderungen:

- Die Pakete müssen sowohl verschlüsselt, als auch authentifiziert sein
- Ein Schlüssel wird nur für ein einziges Paket benutzt
- Die Pakete müssen eine unveränderbare Sequenznummer tragen
- Die Kommunikationspartner müssen sich gegenseitig authentifizieren

Das Verfahren muss mit der bisherigen Hardware bearbeitet werden können.

Dazu wurde das Temporal-Key-Integrity-Protocol (TKIP) entwickelt.

Zusätzlich konnte IEEE802.1x angewendet werden.

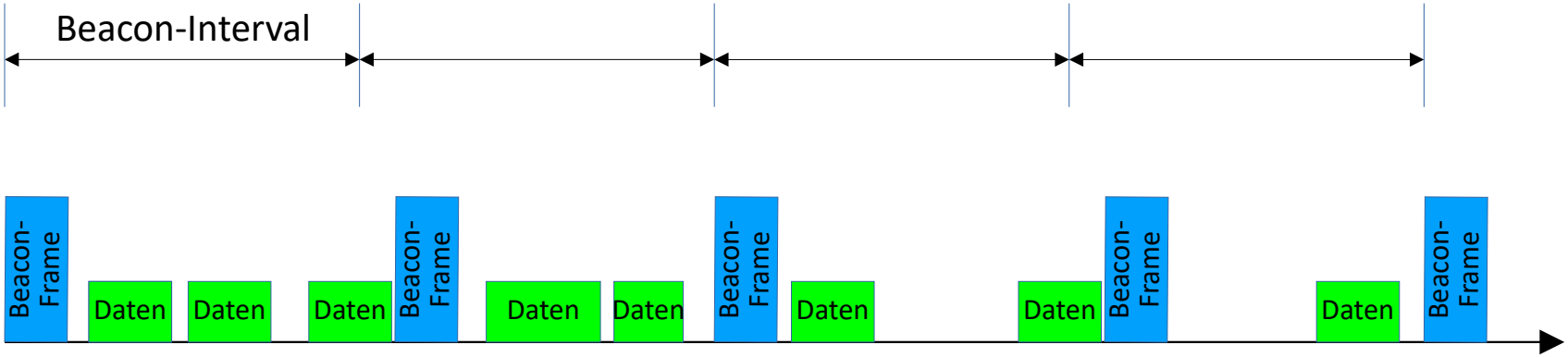
(Näheres Siehe im Kapitel Sicherheit)

Betrieb von IEEE802.11 im Detail (Management-Frames)

Die Steuerung der Verbindungen zu den Stationen erfolgt mit Management-Frames:

- Beacon-Frames
- Probe-Request-Frame
- Probe-Response-Frame
- Authentication-Frame
- Deauthentication-Frame
- Association-Request-Frame
- Association-Response-Frame
- Reassociation-Request-Frame
- Reassociation-Response-Frame
- Disassociation-Request-Frame
- Disassociation-Response-Frame
- Announcement-Traffic-Indication-Frame

Beacon-Frames



Verbindungsvorgang

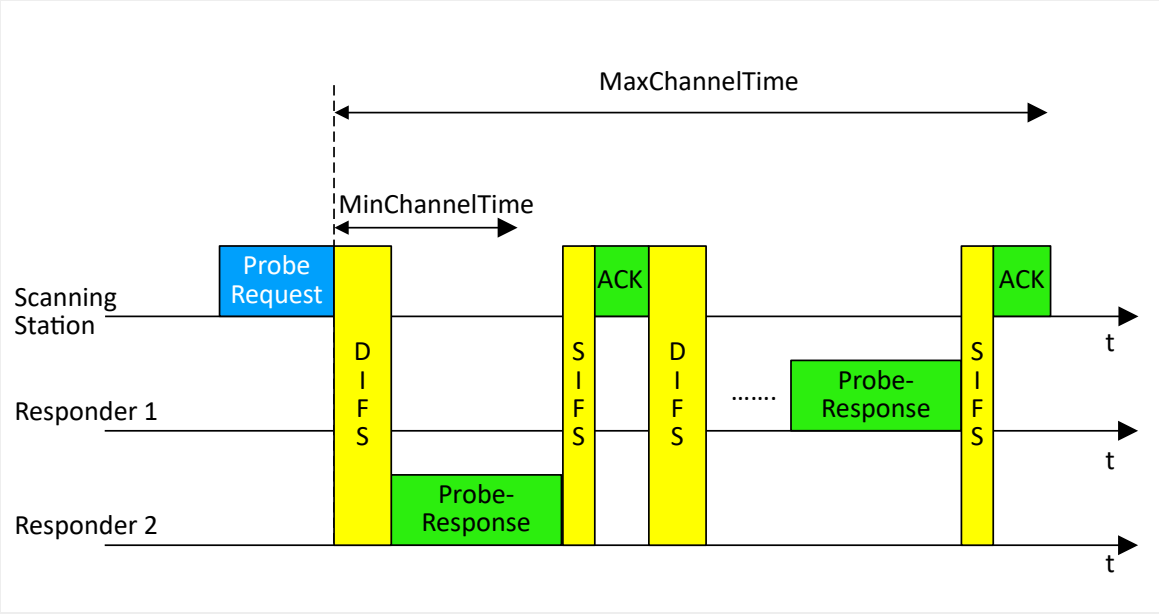
Um eine Verbindung mit einer anderen Station herzustellen sind grundsätzlich 3 Schritte durchzuführen

- Scanning
- Authentifizierung
- Assoziation

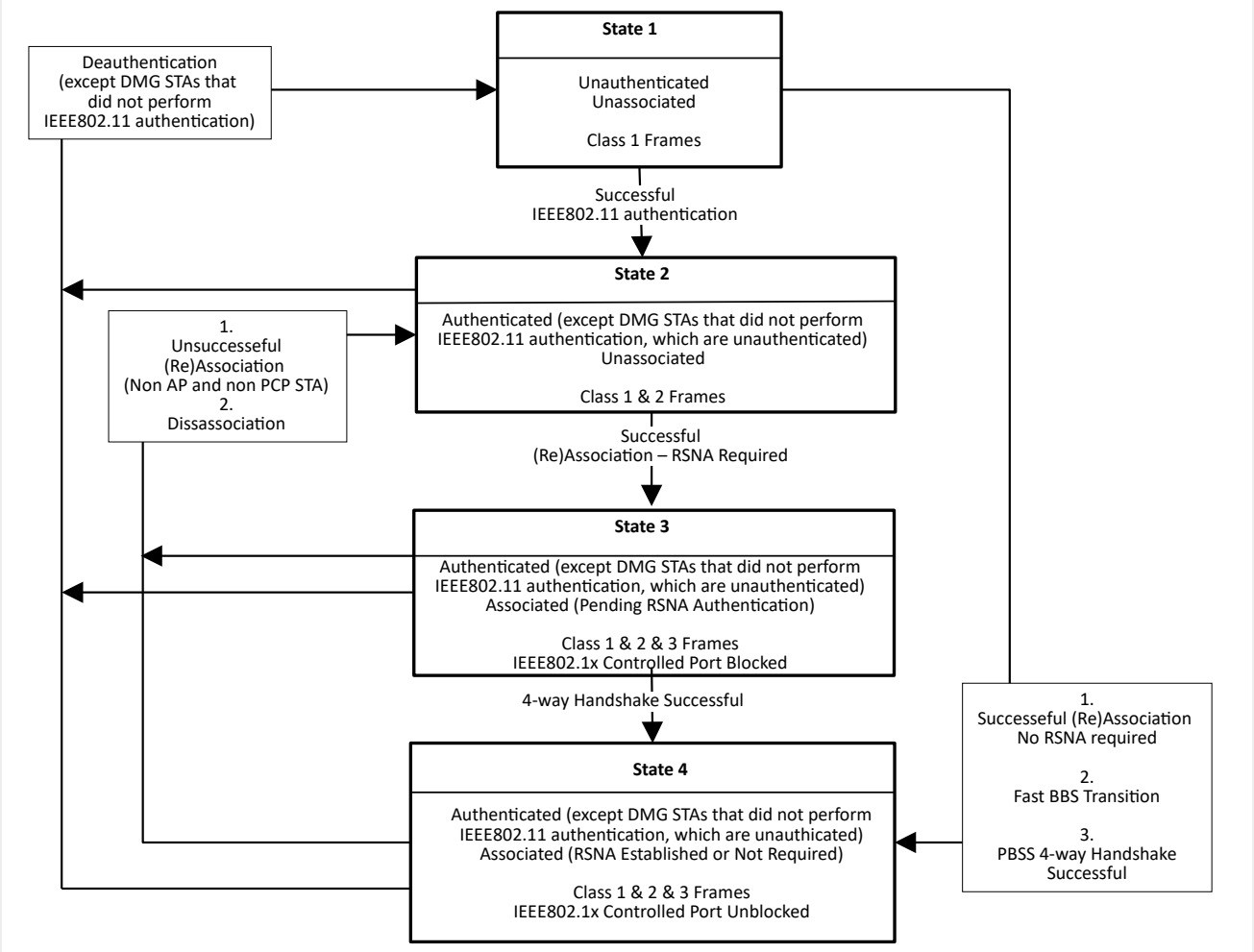
Scanning (active / passive)

Passive-Scanning:
Ein AP sendet periodisch Beacon-Frames in denen er die Eigenschaften der BSS mitteilt. Erkennt eine Station einen Beacon-Frame kann sie sich mit dem Sender verbinden.

Sucht eine Station eine andere Station, oder einen AP, kann das beim **Active-Scanning** mit einem Probe-Request durchgeführt werden.



Authentifizierung

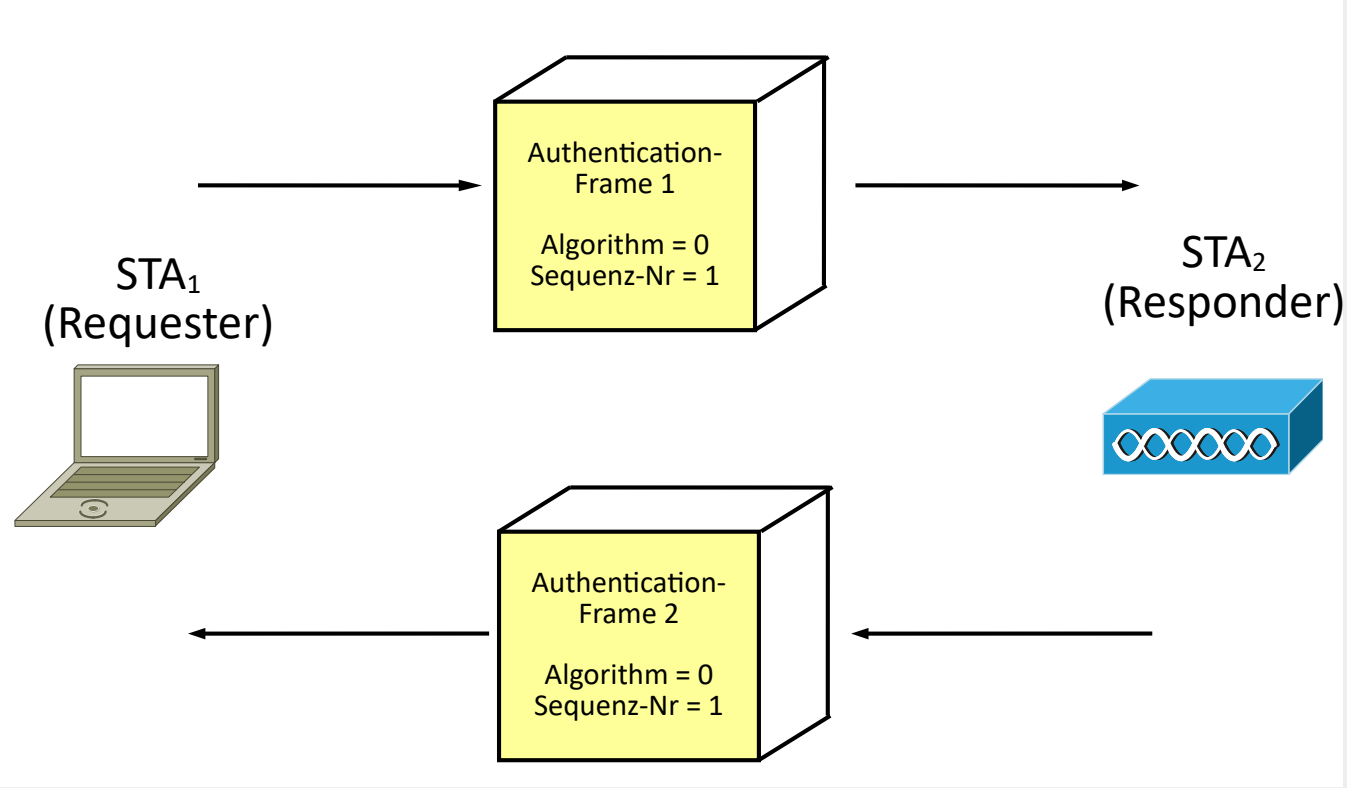


Autentifizierungsmöglichkeiten

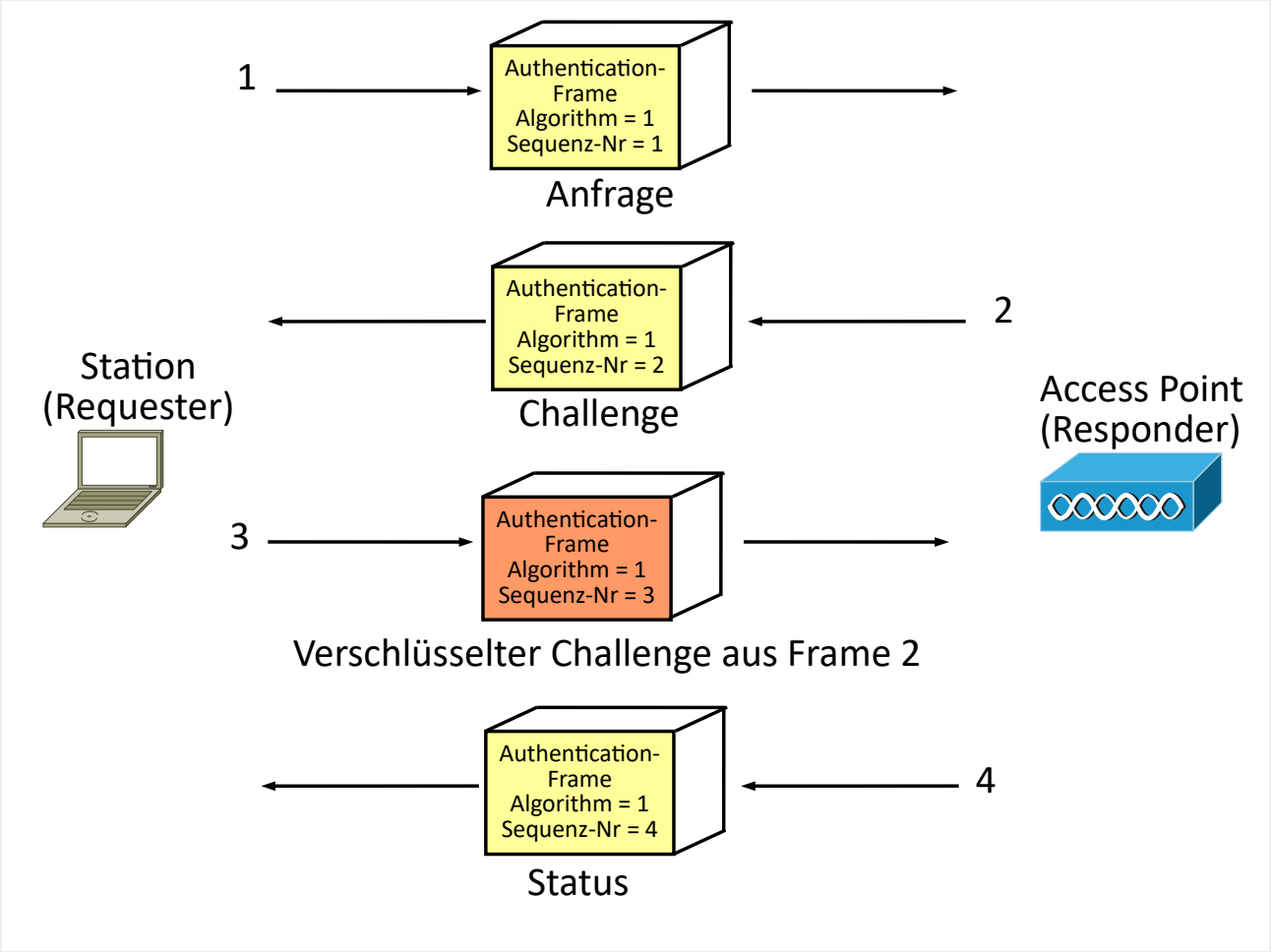
Die Authentifizierung erfolgt nach einer der beiden Vorgehensweisen:

- Open-System-Authentication
- Shared-Key-Authentication

Open-System-Authentication



Shared-Key-Authentication



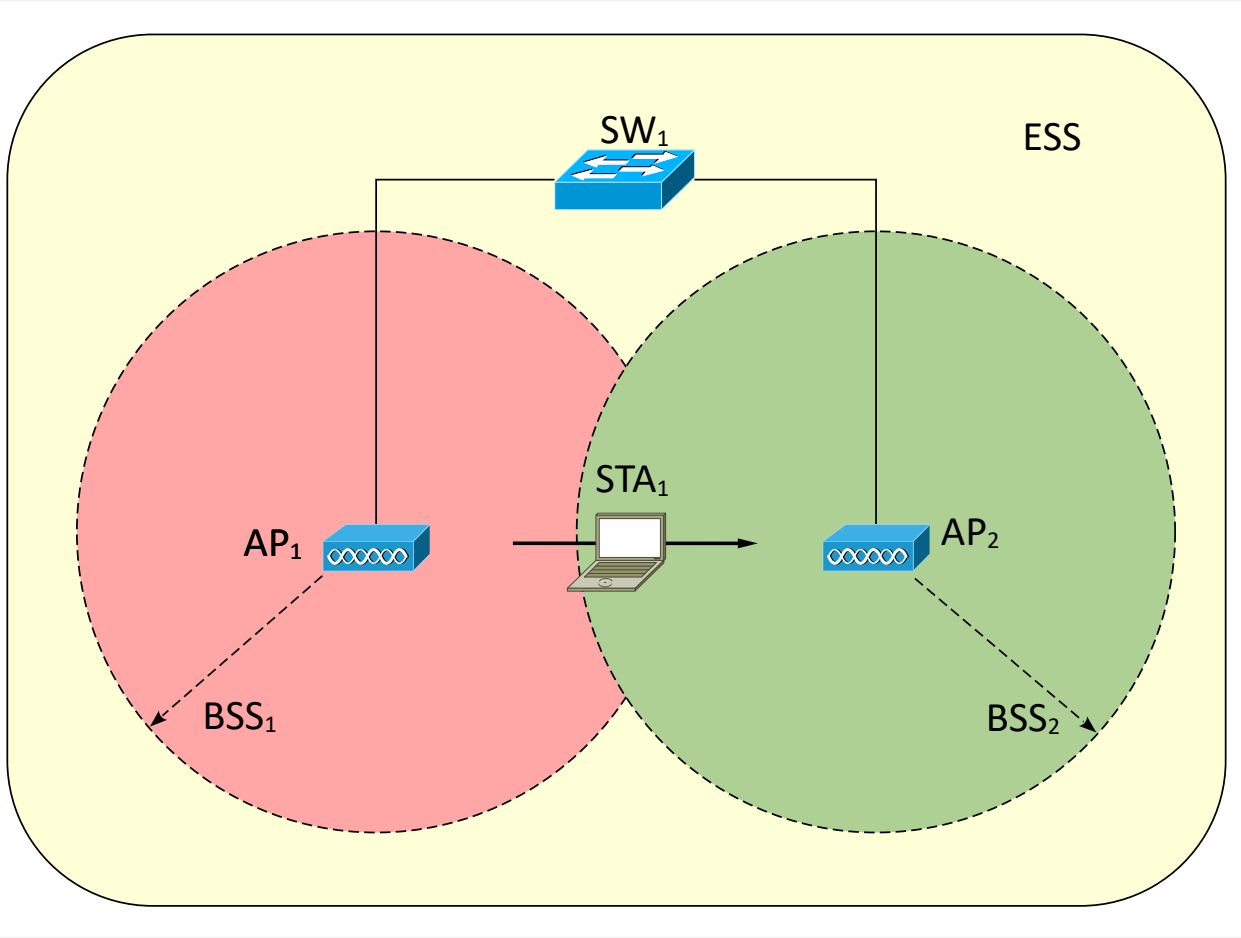
Assoziierung

Nach einer erfolgreichen Shared-Key- oder Open-System-Authentifizierung muss sich eine Station am Accesspoint assoziieren um eindeutig verwaltet werden zu können.

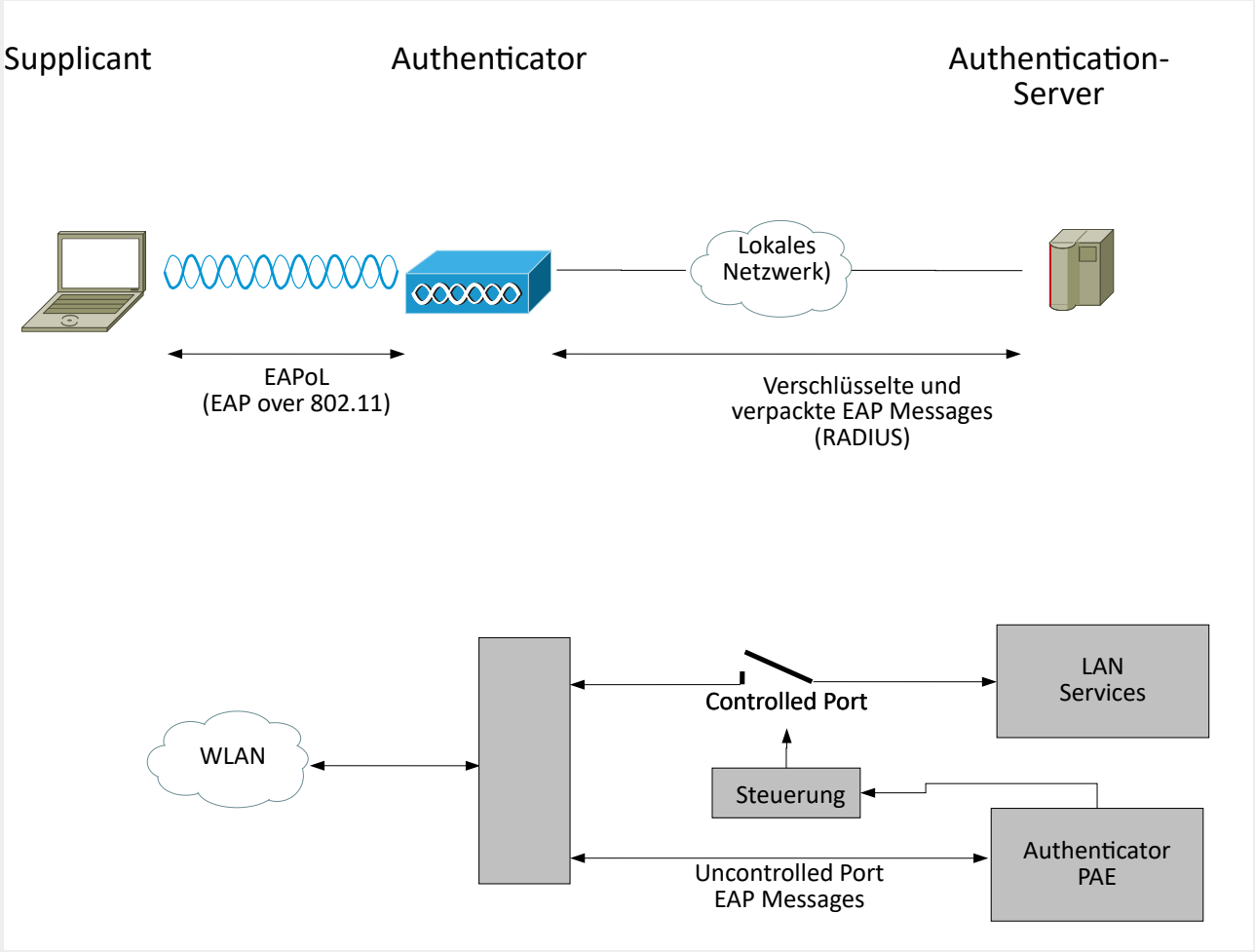
Ohne eine Assoziierung können keine Frames der Klasse 3 (also auch Daten) innerhalb einer Funkzelle ausgetauscht werden.

Bei der Assoziierung festgelegte Eigenschaften sind:
AID, Supported Rates, Extended Supported Rates, Power Capability, Supported Channels, Robust Security Network (RSN), Quality of Service (QoS) Capability, Radio Measurement (RM), Enabled Capabilities, Mobility Domain, Supported Operating Classes, High Throughput (HT) Capabilities 20/40 BSS Coexistence, Extended Capabilities, QoS Traffic Capability, TIM Broadcast Requests, Interworking, Multi-Band, DMG Capabilities, Multiple MAC-Sublayers, VHT Capabilities, Operating Mode Notification, Vendor Specific

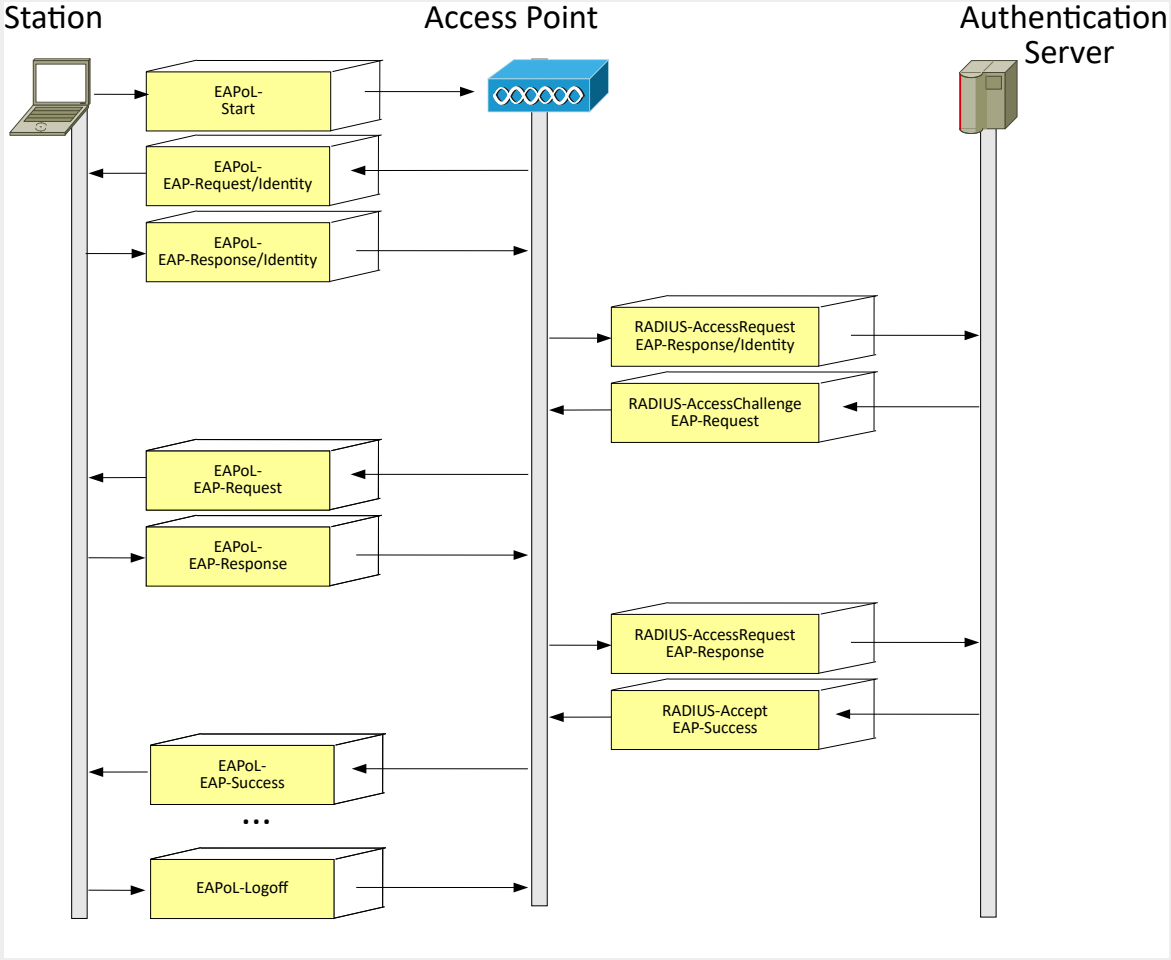
Reassoziierung



IEEE802.1x


Supplicant
Authenticator
Authentication-
Server
Lokales
Netzwerk)
EAPoL
(EAP over 802.11)
Verschlüsselte und
verpackte EAP Messages
(RADIUS)
WLAN
Controlled Port
LAN
Services
Steuerung
Authenticator
PAE
Uncontrolled Port
EAP Messages

WLAN Authentisierung nach IEEE 802.1x



Zusammenfassung

Zusätzliche Standards im Zusammenhang mit IEEE802.11

- Übersicht
- World Mode
- Quality of Service (QoS)
- Handover
- WPA

Management Frames

Anmeldungsverfahren

- Scanning
- Authentifizierung
- Assoziierung

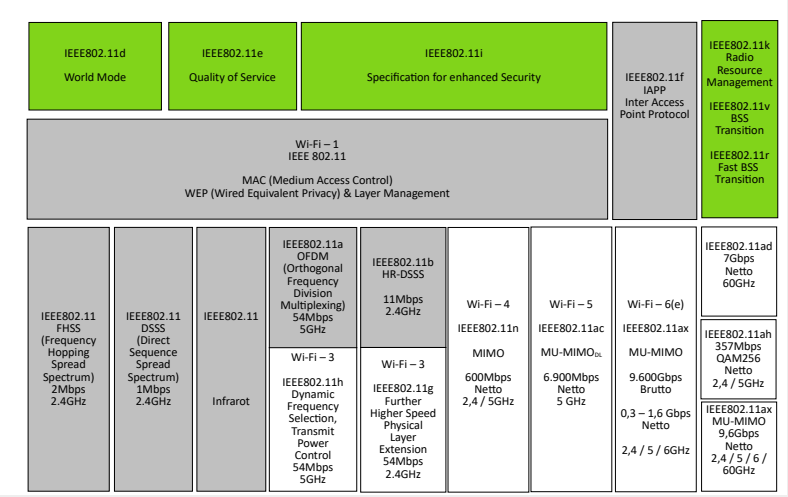
WLAN-Vorlesung
Teil-7

Inhalt

- Zusätzliche Standards im Zusammenhang mit IEEE802.11
  - Übersicht
  - World Mode
  - Quality of Service (QoS)
  - Handover
  - WPA
- Management Frames
- Anmeldungsverfahren
  - Scanning
  - Authentifizierung
  - Assoziierung

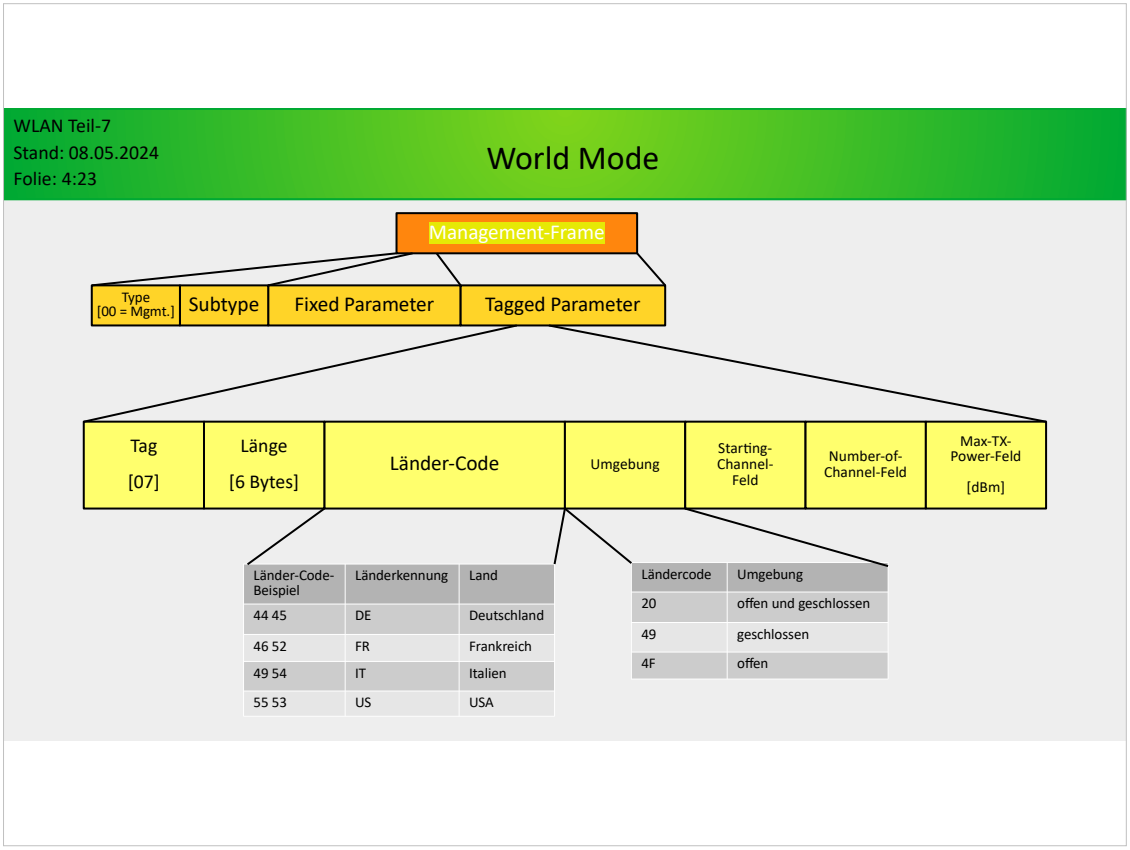
WLAN Teil-7
Stand: 08.05.2024
Folie: 3:23

Übersicht



Für das Funktionieren der Standards sind einige Erweiterungen erforderlich geworden. Hier die wichtigsten:

- IEEE 802.11d World Mode (Country Codes und daraus abgeleitete Parameter)
- IEEE 802.11e für Quality of Service (QoS)
- IEEE 802.11i für Security
- IEEE 802.11k,v,r für den Wechsel des BSS



Der World Mode ist ein Teil der Management-Frames (Type-Feld = 00)

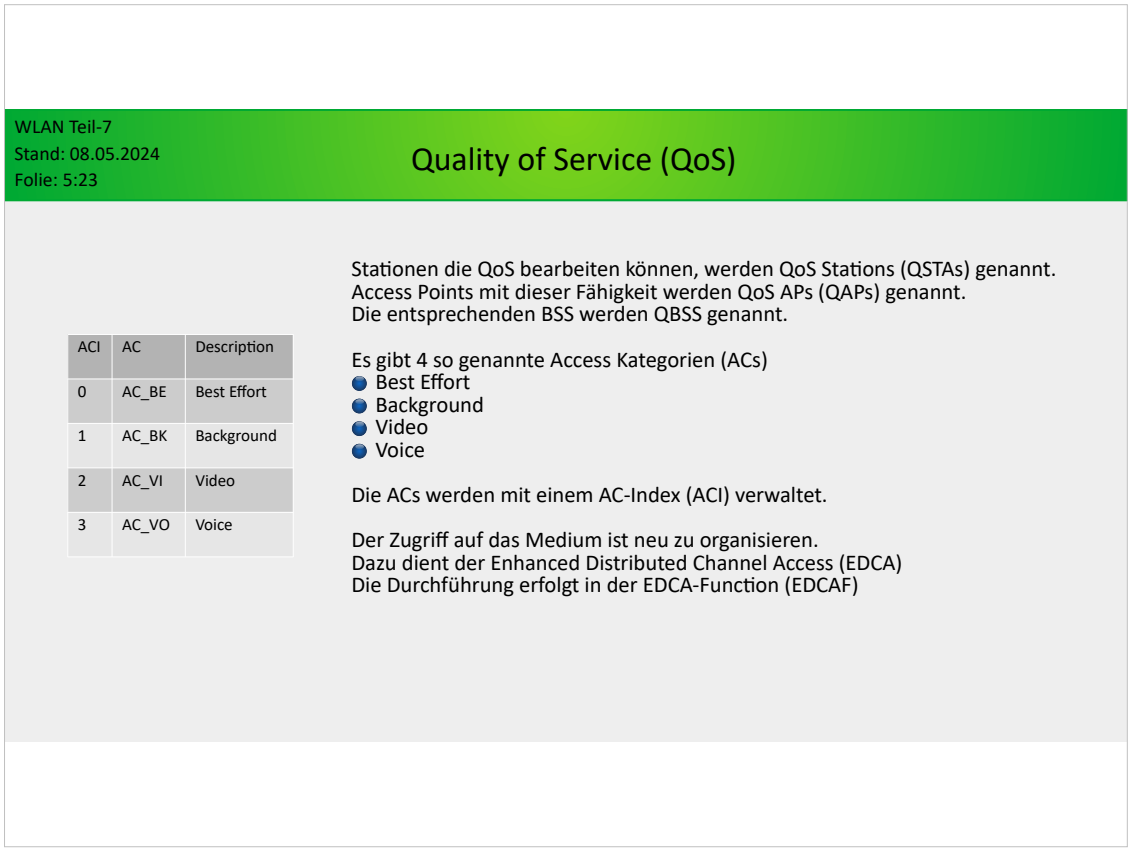
Bei den Tagged Parametern ist im Tag = 7 der Ländercode und weitere Parameter hinterlegt.
In der Folie sind beispielhaft die Codes für Deutschland (44 45), Frankreich (46 52) Italien (49 54) und die USA (55 53) dargestellt.

Danach folgt die Kennung für die Umgebung, in der die folgenden Parameter gelten.
(20 = offen und geschlossen (beliebig) / 49 geschlossen (innen) / 4F offen (draußen))

Über das folgende 1 Byte große Starting-Channel-Feld wird die erste zu nutzende Kanalnummer festgelegt.
(z. B. In Deutschland im 2,4GHz-Band die 1)

Danach folgt mit dem 1 Byte großen Number-of-Channel-Feld die Anzahl der zu nutzenden Kanäle.
(z. B. In Deutschland im 2,4GHz-Band 13)

Als letztes gibt das 1 Byte große Max-TX-Power-Feld die maximale zulässige Sendeleistung in dBm an.
(z. B. In Deutschland im 2,4GHz-Band 20 dBm))



Wenn die zur Verfügung stehende Bandbreite limitiert ist, wird gerne für kritische Applikationen die Forderung nach einer Bandbreitengarantie gestellt.
Da das in einem System mit einem Medienzugriffsverfahren wie CSMA nicht geht, ist man versucht mit einem Quality of Service (QoS) - Ansatz Bandbreite zu reservieren.

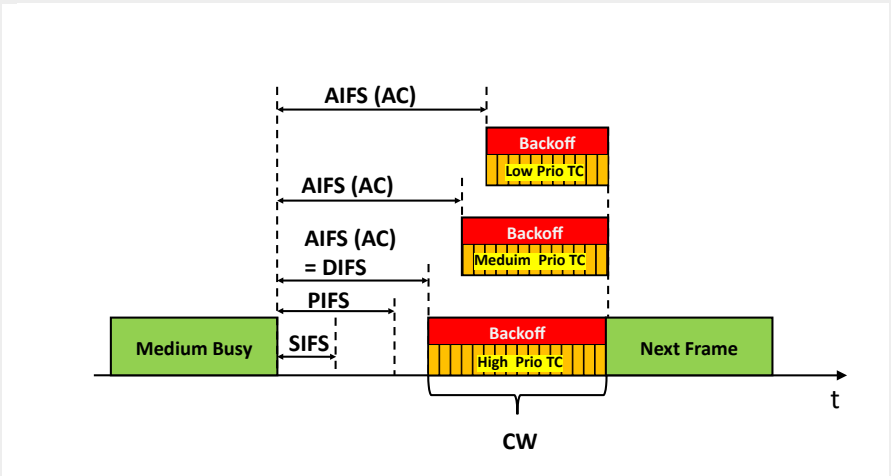
Dazu benötigt es die neue Medien-Zugriffs-Koordination namens Enhanced Distributed Channel Access (EDCA)

Damit werde die 4 Kategorien zur Verfügung gestellt:

- Best Efford
- Background
- Video
- Voice

WLAN Teil-7
Stand: 08.05.2024
Folie: 6:23

Abbildung der Prioritäten auf das Contention Window (CW)



Für jede Kategorie ist ein eigenes AIFS (Arbitration IFS)definiert. Innerhalb des AIFS haben wiederum alle Rahmen einer Kategorie dann das CW abzuhandeln.

Das AIFS mit mit der höchsten Priorität entspricht einem DIFS.

Am Ende des Tages gibt es jetzt eine Priorisierung nach Kategorien jedoch gibt es immer noch keine 100% Garantie, dass die Daten auch Ankommen.

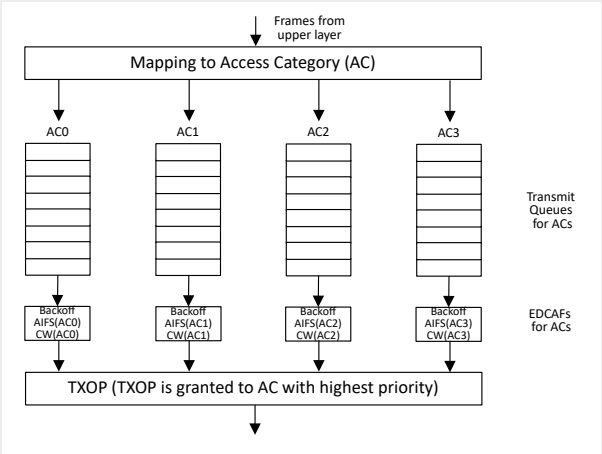
Die Werte für CWmin und CWmax wurden noch angepasst.

	bisher	neu
CW_{min}	10 - 15	0 - 255
CW_{max}	255	CW_{min} - 1024

WLAN Teil-7
Stand: 08.05.2024
Folie: 7:23

Prioritätenzuordnung

Priority	User Priority (UP)	Access Category (AC)	Designation
Lowest	1	AC_BK	Background
	2	AC_BK	Background
	0	AC_BE	Best Effort
	3	AC_BE	Best Effort
	4	AC_VI	Video
	5	AC_VI	Video
	6	AC_VO	Voice
Highest	7	SC_VO	voice



Beim Bearbeiten werden den Daten zuerst einer Kategorie zugeordnet und in die entsprechende Warteschlange einsortiert.

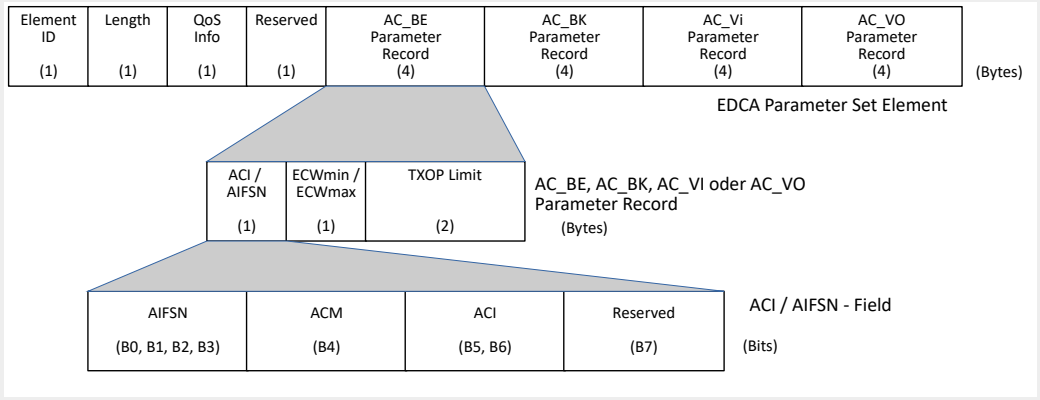
Für jede Warteschlange wird ein Medienzugriffsverfahren abgehandelt. Die höchsten Prioritäten werden zuerst abgehandelt. Damit gilt das Prinzip der Gleichberechtigung aller Geräte nicht mehr.

Damit werden quasi in einer Station 4 Stationen virtualisiert. Es entspricht einer Verlängerung der VLAN-Technologie.

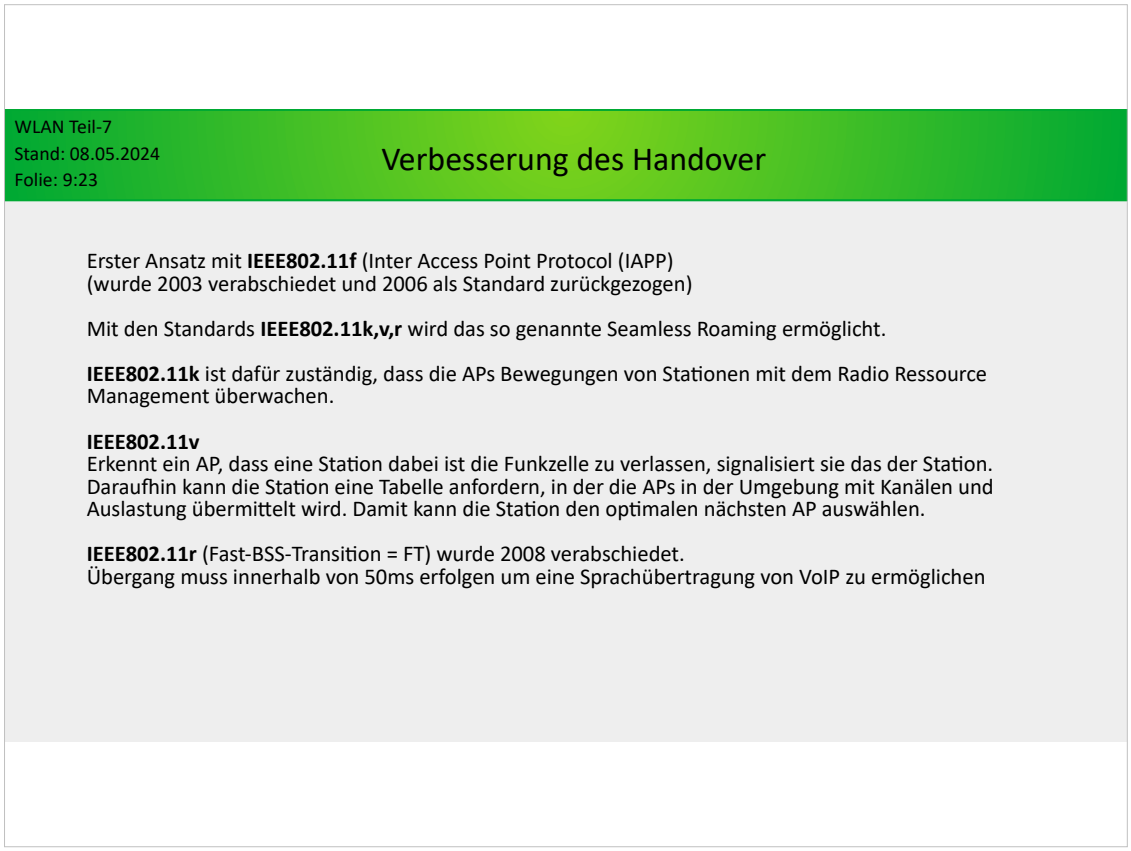
Zusätzlich wurden 8 User-Prioritäten eingeführt die den 4 Kategorien zugeordnet werden.

WLAN Teil-7
Stand: 08.05.2024
Folie: 8:23

EDCA Parameter



Für jede Kategorie wird im Header ein Parameter-Block reserviert



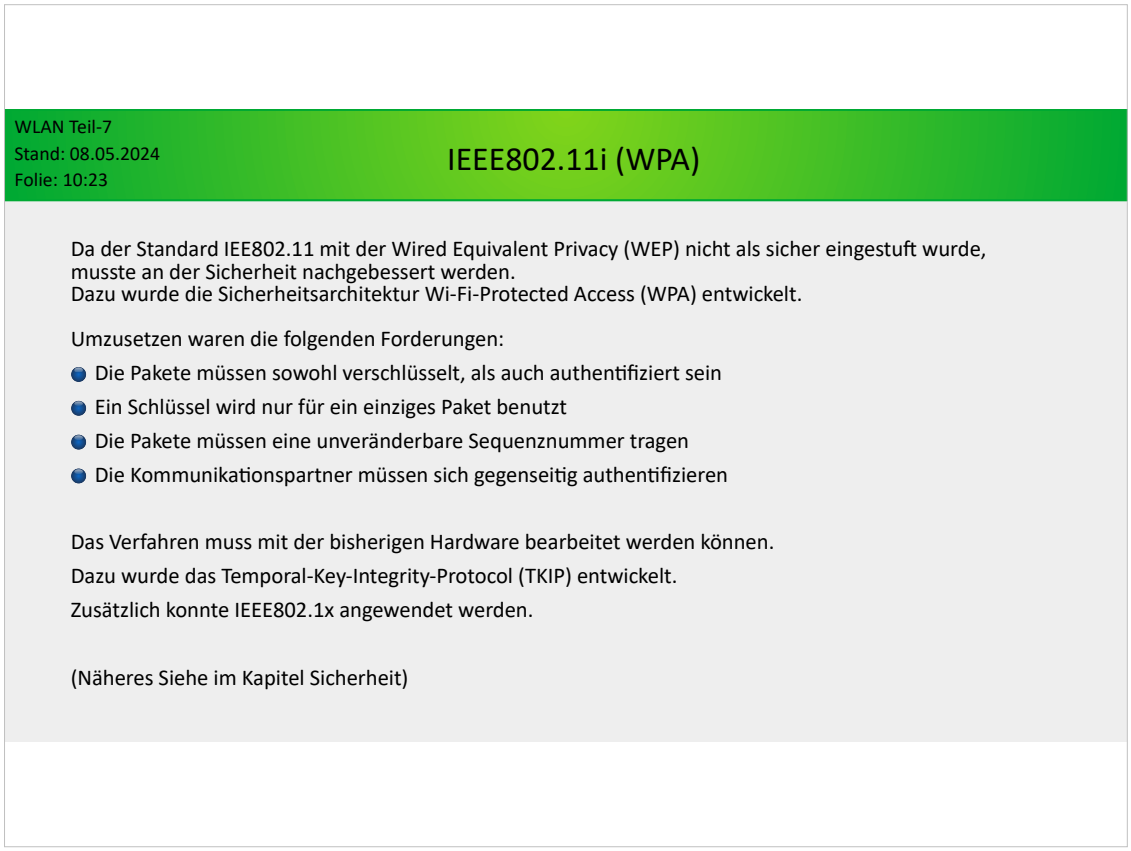
Für das Handover hat sich mittlerweile ein ganzes Standardbündel etabliert. IEEE802.11k,v,r.

IEEE-802.11k
Mit dem Radio Ressource Management wurde erreicht, dass ein AP die Verbindungen zu den Stationen überwacht. Dabei wird überprüft, ob das Signal einer Station sich verändert. Damit wird es einem AP ermöglicht eine Station zu verlanlassen, die BSS zu verlassen.

IE**EE-802.11v**
Mit diesem Standard wurden die folgenden Themen optimiert:

- BSS Transition-Verwaltung (Führung einer Liste mit APs in der Umgebung mit Kanal und Auslastungsinformation)
- Disassociation imminent (Signalisierung eines bevorstehenden BSS Wechsels vom AP an eine Station)
- Directes Multicast Service (DMS) (Optimierte Multicasts)
- BSS-Max-Idle-Service (Optimierung der Akkulaufzeit durch Festlegung wie lange eine Station schläft)

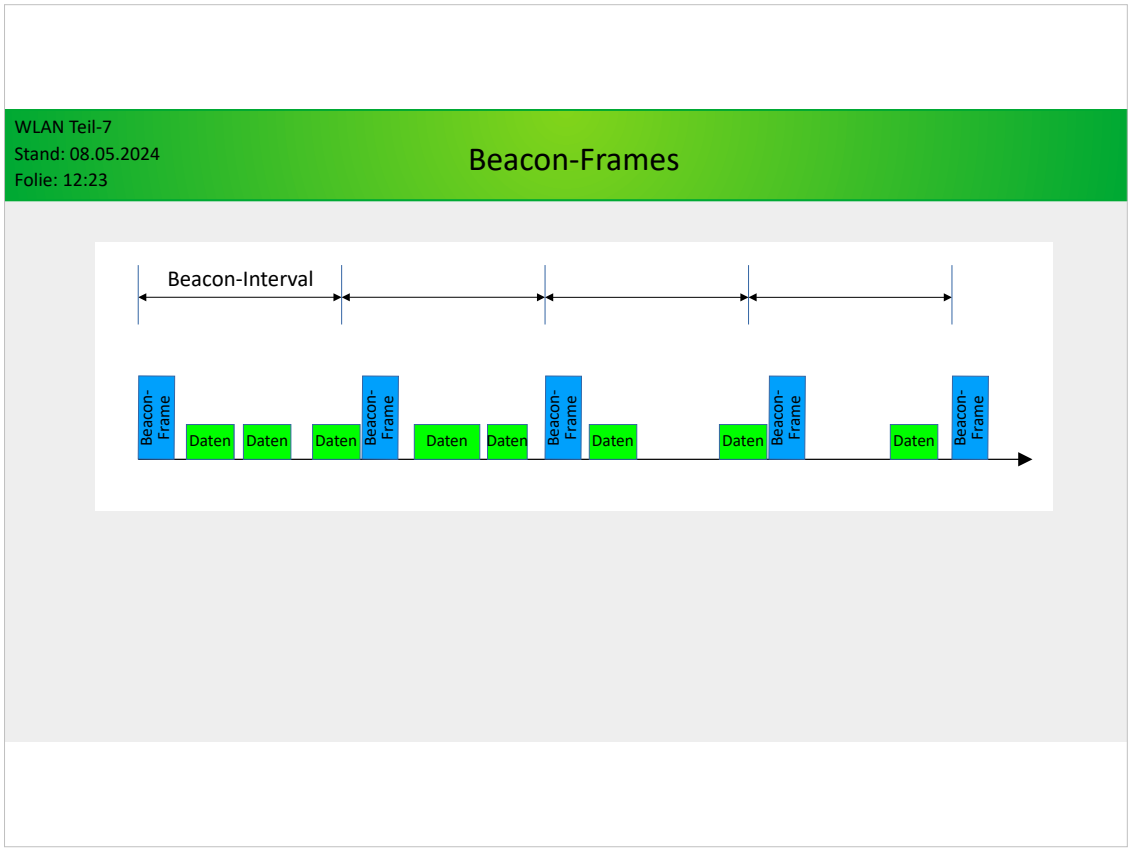
IEEE-802.11r
Fast-BSS-Transition (FT)



Da die Sicherheit in den ersten Standards schlecht war, musste mit unterschiedlichen Maßnahmen Abhilfe geschaffen werden.

IEEE802.11i war dann der erste Standard der die Sicherheitsmängel aufarbeitete und bei dem Teile der bisherigen Zwischenlösungen enthalten waren.

Management-Frames dienen der Organisation der Stationen und den Schritten beim Anmelden und beim Abmelden.

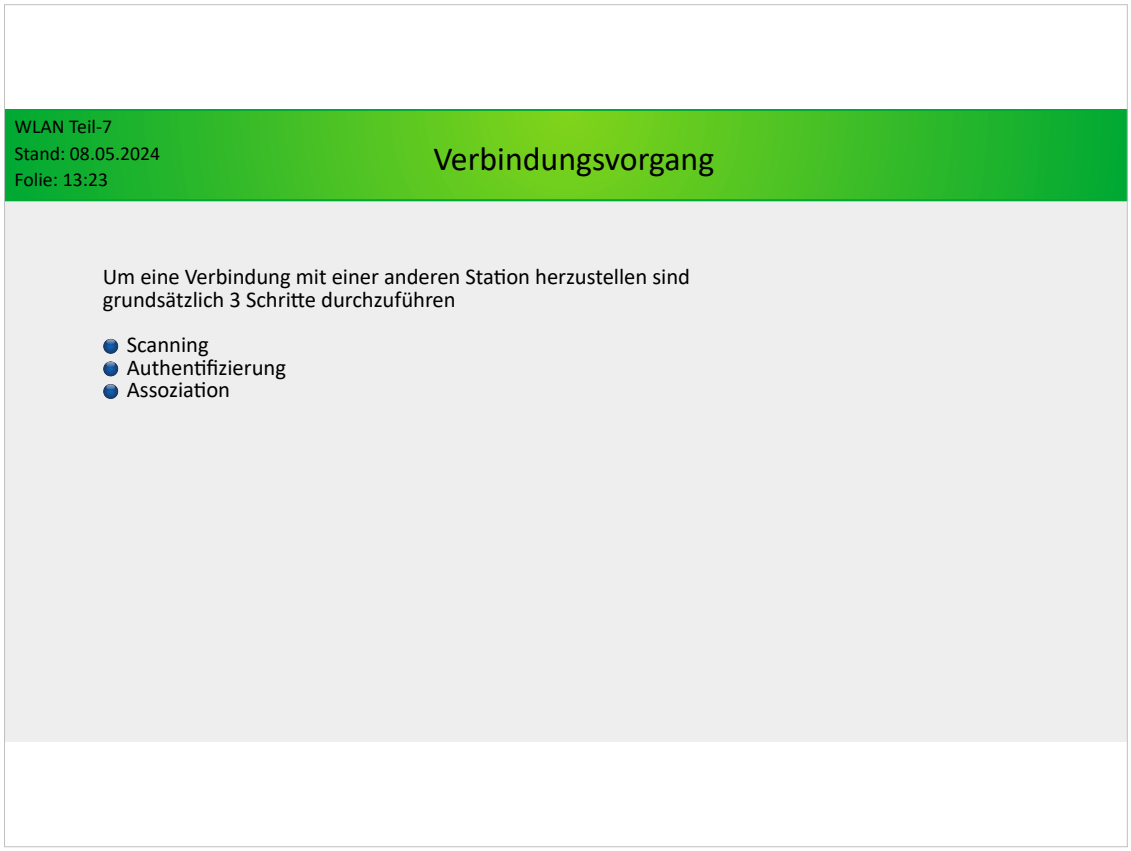


Beacon-Frames werden in einem Beacon-Intervall gesendet.

Der Startzeitpunkt eines Beacon-Intervalls wird als Target Beacon Transmission Time (TBTT) bezeichnet. Er wird von der TSF vom Timestamp-Feld abgeleitet. Innerhalb des Beacon-Intervalls ist das der Zeitpunkt 0. Von da an werden die Beacon-Frames im Abstand des Beacon-Intervalls gesendet. Auch diese Zeitpunkte werden TBTT genannt.

Ist der Kanal zum Beacon-Intervall belegt, muss gewartet werden und der Beacon-Frame wird zeitversetzt gesendet.

In der Fassung des IEEE802.11-Standards von 2016 kann ein Beacon Frame bis zu 68 Felder haben. Dabei gibt es feste Bestandteile und so genannte Informations-Elemente (IE). Je nach Konfiguration der WLAN Umgebung können die Informations-Elemente eines Parameter-Sets zum Beacon-Frame hinzu kommen. Die Informationselemente bestehen aus einer ein Byte langen Element-ID, eine ein Byte langen Längeninformation und aus einem bis zu 255 Byte langen variablen Informationsteil.



Die Verbindung zwischen zwei Stationen wird in 3 Schritten aufgebaut.

1. Scanning
Dabei werden die Kommunikationspartner gefunden

2. Authentifizierung
Dabei wird die Sicherheit zwischen den Stationen aufgebaut

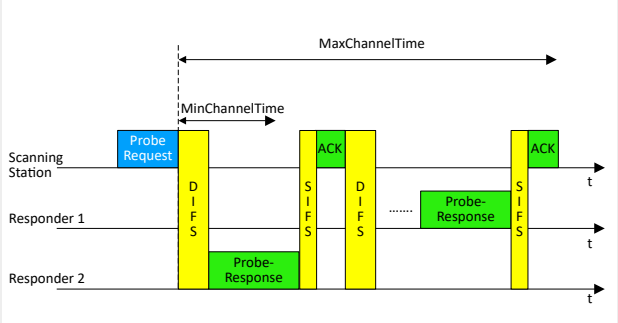
3. Assoziierung
Dabei wird die Verwaltung der Stationen abgehandelt (IDs usw.)

WLAN Teil-7
Stand: 08.05.2024
Folie: 14:23

Scanning (active / passive)

Passive-Scanning:
Ein AP sendet periodisch Beacon-Frames in denen er die Eigenschaften der BSS mitteilt. Erkennt eine Station einen Beacon-Frame kann sie sich mit dem Sender verbinden.

Sucht eine Station eine andere Station, oder einen AP, kann das beim **Active-Scanning** mit einem Probe-Request durchgeführt werden.



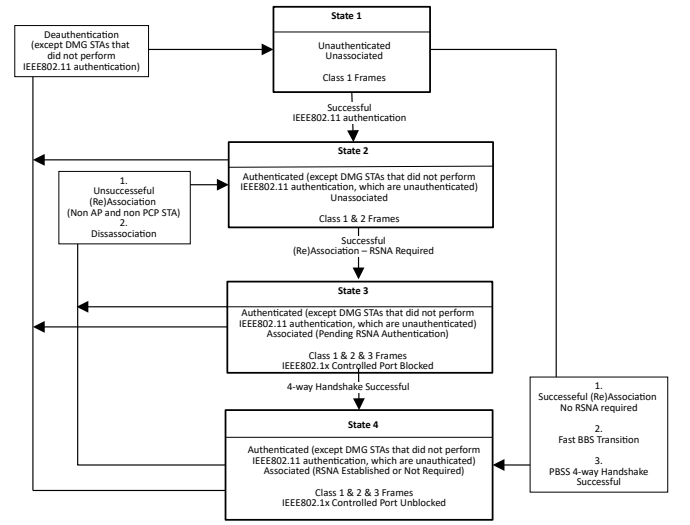
Beim passiven Scanning wird darauf gewartet, dass ein Beacon-Frame auf einem Kanal gesendet wird und dadurch eine andere Station erkannt wird.

Beim activen Scanning sendet eine Station einen Probe-Request aus um herauszufinden, ob auf dem Kanal ein potentieller Kommunikationspartner ist.

Dafür gibt es eine Mindest-Wartezeit und eine Maximal-Wartezeit.

WLAN Teil-7
Stand: 08.05.2024
Folie: 15:23

Authentifizierung



Der Gesamte Anmeldeprozess wird in 4 Stati durchlaufen:

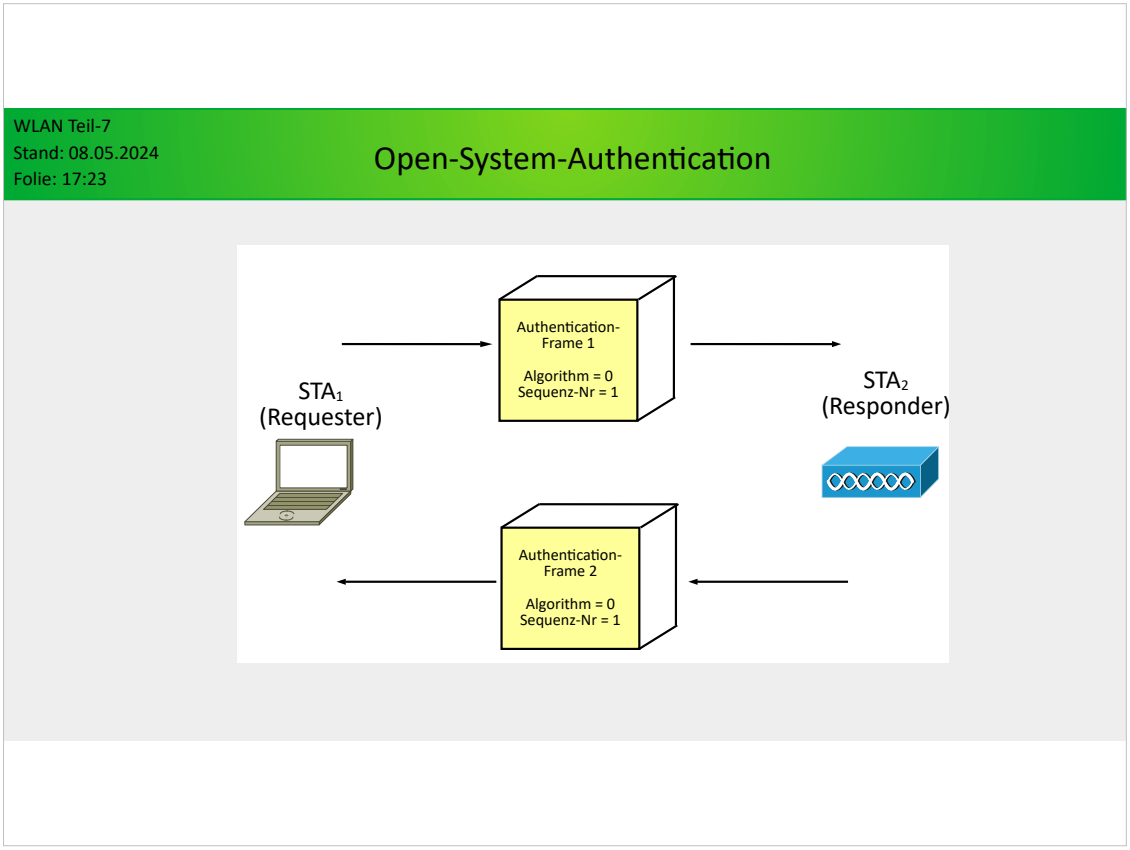
Status	Bedeutung
1	Nicht authentifiziert und nicht assoziiert
2	Authentifiziert und nicht assoziiert
3	Authentifiziert und Assoziierung ausstehend
4	Authentifiziert und Assoziiert

Je nachdem welcher Status erreicht ist, können entsprechende Frames gesendet werden.

Autentifizierungsmöglichkeiten

Die Authentifizierung erfolgt nach einer der beiden Vorgehensweisen:

- Open-System-Authentication
- Shared-Key-Authentication

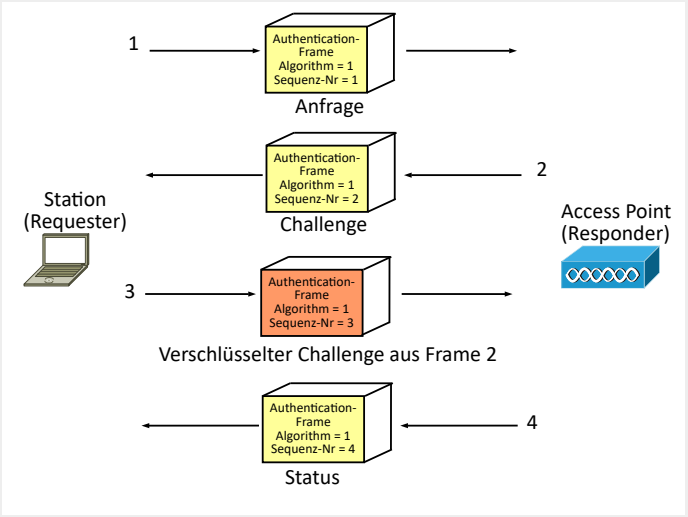


Die Open-System-Authentication ist eine Null-Authentifizierung.

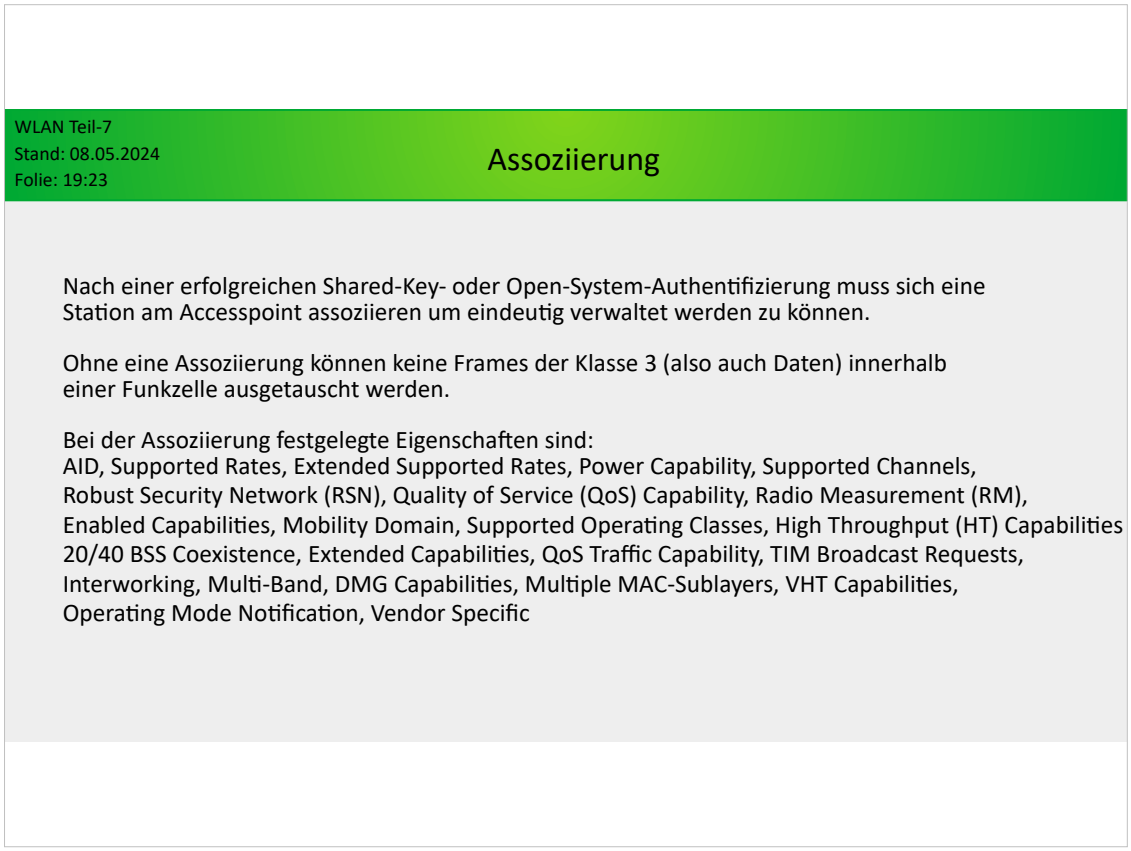
D. h. es wird immer positiv authentifiziert. Durch eine nachgeschaltete Authentifizierung kann dann immer noch ein Eindringling abgewehrt werden.

WLAN Teil-7
Stand: 08.05.2024
Folie: 18:23

Shared-Key-Authentication



Bei der Shared Key Authentication wird nach einer Anfrage ein Challenge Code vom AP zurückgesendet.
Die Station verschlüsselt den Challenge und sendet ihn zurück.
Kann der AP den verschlüsselten Code entschlüsseln ist die Authentifizierung erfolgreich und wird positiv quittiert.



Dazu sendet die Station einen Association-Request-Frame an den AP, in dem sie ihre Parameter / Fähigkeiten mitteilt.

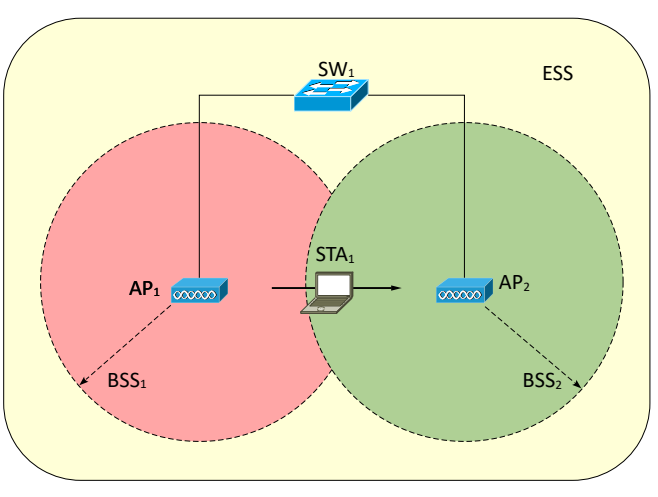
Als Antwort sendet der AP einen Association-Response-Frame an die Station zurück. Darin teilt sie ihrerseits ihre Fähigkeiten (also die obige Liste) und weitere Informationen mit:
Statuscode = 0 (SUCCESS) oder Grund
Association ID (AID)
...

War die Assoziierung erfolgreich, quittiert die Station den Empfang des Association-Response-Frames mit einem ACK-Frame.

Am Ende schaltet der AP auch die Verbindung zum Distribution System (DS) für die Station frei. Damit können vom AP Frames der Klasse 3 für die Station transportiert werden.

WLAN Teil-7
Stand: 08.05.2024
Folie: 20:23

Reassoziierung



Ist beim Verlassen einer BSS, die neue BSS mit der alten BSS über ein Distribution System (DS) verbunden, kann der Übergang mit einer Reassoziation erfolgen.

Dazu sendet die Station an den AP einen Reassociation-Request-Frame. Darin ist die MAC-Adresse des letzten APs enthalten.

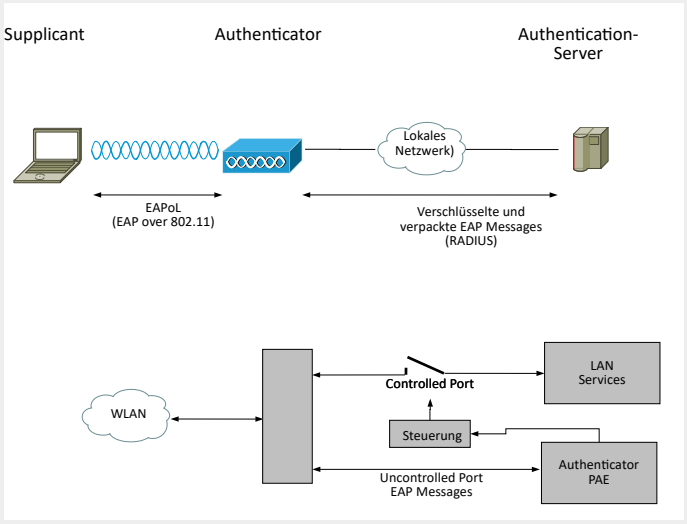
Der neue AP antwortet mit einem Reassociation-Response-Frame.
Falls der Status Code = „SUCCESS“ ist bekommt STA_1 ihre neue AID mitgeteilt unter der sie nun von AP_2 verwaltet wird.

Darauf hin sendet STA_1 einen ACK-Frame an den AP_2. AP2 sendet am Ende noch die Information über die erfolgreiche Reassoziation an das Distribution System um alle APs über den neuen Zustand informieren.

War STA1 nicht im Netzwerk authentifiziert beantwortet AP2 die den Reassociation-Request-Frame mit einem Deauthentication-Frame. Der Ablehnungsgrund ist aus dem Reason-Code ersichtlich.

WLAN Teil-7
Stand: 08.05.2024
Folie: 21:23

IEEE802.1x



Eine Station (Supplicant), die sich mit dem Accesspoint (Authenticator) verbinden möchte, kann zuerst nur über das Extensible Authentication Protocol over LAN (EAPoL) die Anmeldeinformation austauschen.

Die Anmeldeinformation kann z. B. aus einer MAC-Adresse oder einem Zertifikat bestehen.

Der Authenticator reicht die Anmeldeinformation verschlüsselt an den Authentication-Server weiter. Dieser prüft, ob dem Supplicant eine Verbindung in das lokale Netzwerk gestattet werden kann.

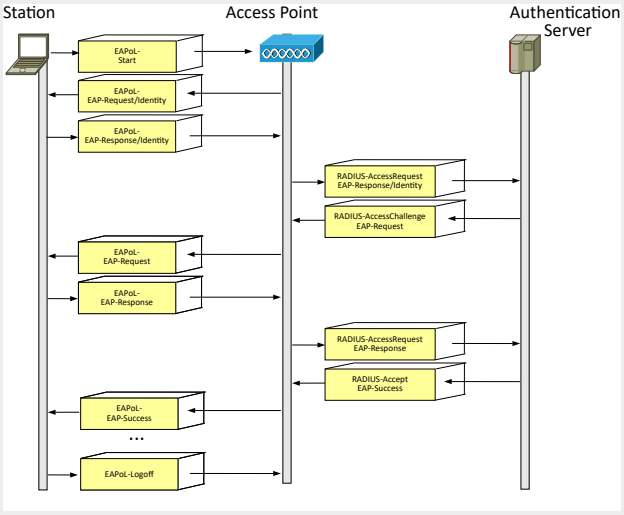
Ist dies der Fall schaltet der Authenticator den Weg für den Supplicant frei.

Der Zugriff auf die Dienste, die über das LAN zugänglich gemacht werden erfolgt über eine Steuerung auf dem Authenticator, die vom Authentication-Server getriggert wird.

Diese Vorgehensweise mit dem RADIUS-Protokoll abgehandelt.
Es eignet sich nicht nur für den Zugriff auf ein WLAN sonder auch von beliebigen Geräten per Kupferverbindung über einen Switch auf ein LAN.

WLAN Teil-7
Stand: 08.05.2024
Folie: 22:23

WLAN Authentisierung nach IEEE 802.1x



Bei der Abhandlung einer Authentifizierung startet der Supplicant mit einem Start-Paket die EAPol-Bearbeitung.

Darauf hin erfrägt der Authenticator die Anmeldeinformation.
Sobald der Supplicant die Anmeldeinformation mitgeteilt hat, kann sie vom Authenticator zum Authentication-Server per RADIUS-Protokoll weiter geleitet werden.

Mit dieser Information erzeugt der Authentication-Server einen Challenge der an den Supplicant weiter gereicht wird.

Aus dem Challenge erzeugt der Supplicant wiederum eine Antwort die an den Authentication-Server weiter gegeben wird. Entspricht die Antwort dem gewünschten Ergebnis, kann der Weg für den Supplicant freigeschaltet werden.

Zusammenfassung

Zusätzliche Standards im Zusammenhang mit IEEE802.11

- Übersicht
- World Mode
- Quality of Service (QoS)
- Handover
- WPA

Management Frames

Anmeldungsverfahren

- Scanning
- Authentifizierung
- Assoziierung