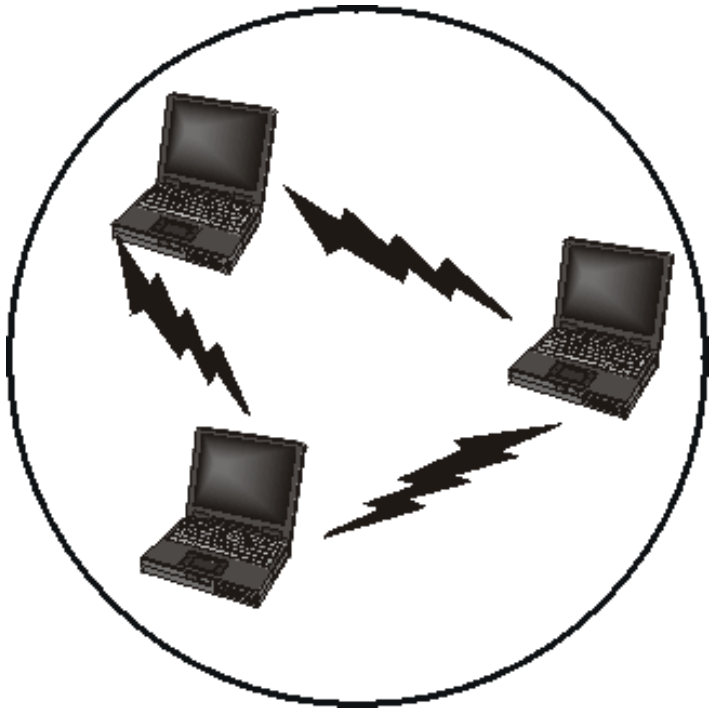
Sicherungsschicht

IEEE 802.11

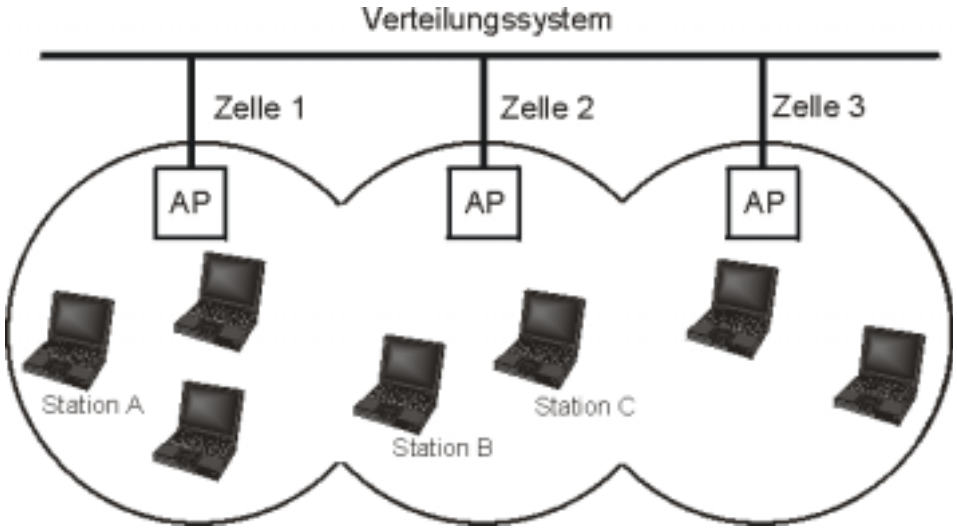
Ad-hoc Netzwerk

- **Ein Gruppe von Rechnern**
  - die untereinander kommunizieren können
    - „Zelle“
    - oder auch „Basic Service Set“
  - Mit einer eigenen Zell-Adresse (Namen)
  - Unabhängig von anderen Netzen
    - „Independent Basic Service Set“



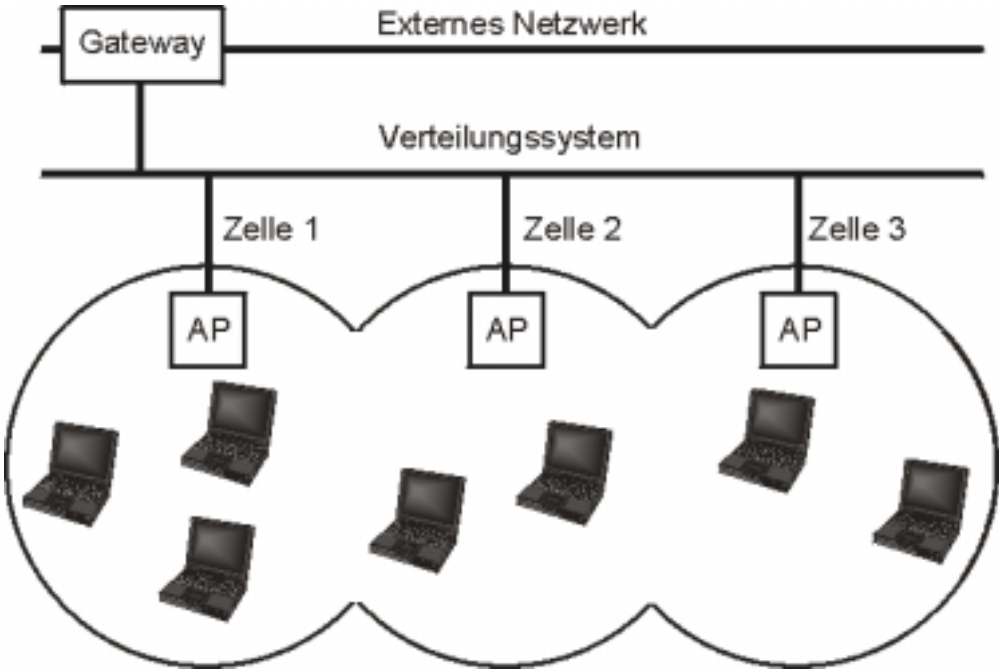
Infrastrukturnetzwerk

- **Zellen, die über ein Verteilungssystem miteinander verbunden sind**
  - Verteilungssystem nicht weiter def. (meist aber ein LAN)
  - „Extended Service Set“
- **Verbindung zwischen Verteilungssystem und Zelle ist ein Access Point (AP)**
  - Adresse der Zellen = Adresse des AP



Gateways

- **Ein Gateway („Portal“) verbindet das Verteilungssystem mit weiteren Netzen**
  - I.d.R. integrieren die APs die Portal-Funktion



Definitionen IEEE 802.11

IEEE 802.11 Begriff	Bedeutung
Station	Ein technisches System (Laptop, stationärer Rechner, Gerät, Maschine, ...), das nach dem IEEE 802.11 Standard drahtlos kommunizieren kann
Basic Service Set	Eine Zelle mehrerer Stationen, die räumlich so nahe beisammen sind, dass sie untereinander über das Funkmedium kommunizieren können
Ad-hoc-Netzwerk (auch *Independent Basic Service Set*)	Eine Zelle, die mit keinem weiteren Netzwerk verbunden ist
Infrastruktur-Netzwerk (auch *Extended Basic Service Set*)	Ein Netzwerk mit mehreren (drahtlosen) Zellen, die über ein weiteres Netzwerk miteinander verbunden sind
Verteilungssystem (Distribution System)	Das Netzwerk, das in einem Infrastruktur-Netzwerk die Zellen miteinander verbindet
AP	Die Station, die in einem Infrastruktur-Netzwerk eine Zelle mit dem Verteilungssystem verbindet
Portal	Ein Gateway zwischen dem Verteilungssystem eines Infrastruktur-Netzwerkes und anderen Netzwerken

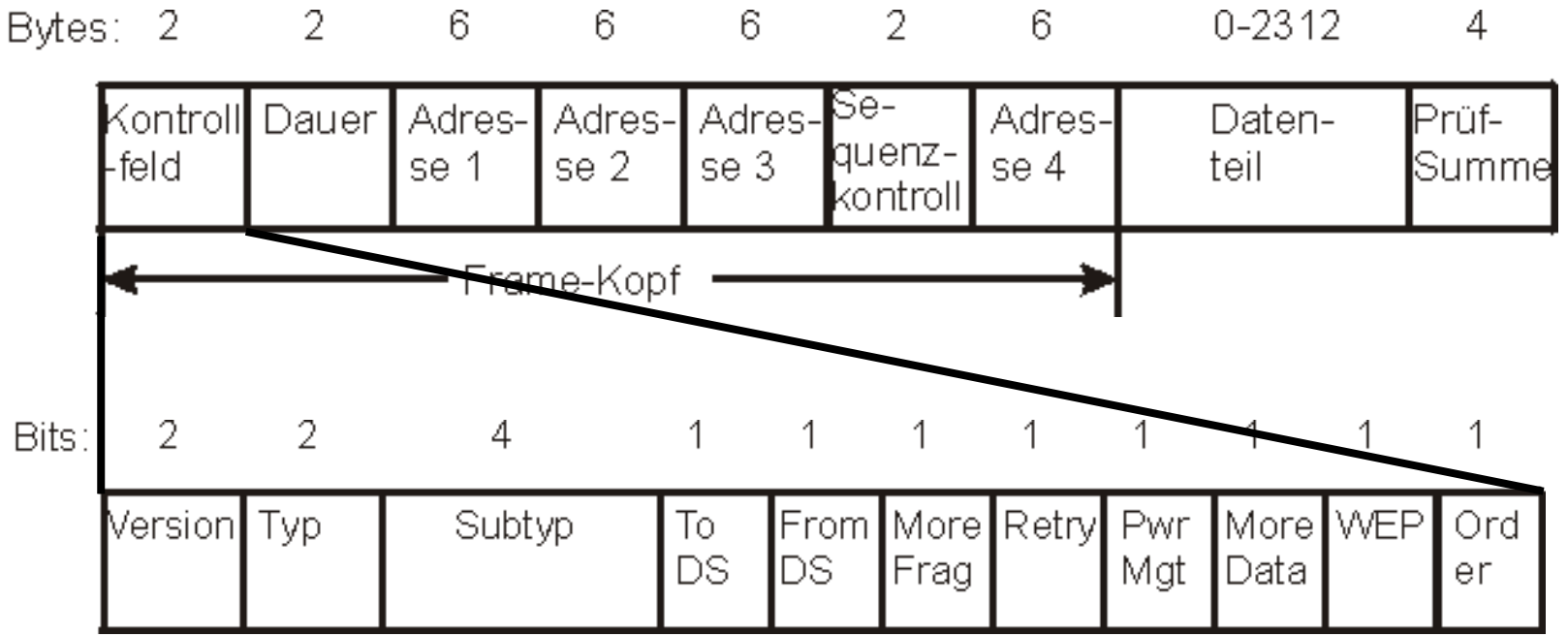
Adressen in IEEE 802.x

- **6 Byte (48 Bit)**
  - Auch genannt „MAC-Adressen“
  - Geschrieben: xx:xx:xx:xx:xx:xx
- **Identifiziert ein IEEE 802-Device**
- **z.B. eindeutig eine Netzwerkkarte**
  - I.d.R. in der Firmware „eingebrannt“
  - Präfix der Adresse identifiziert HW-Hersteller
  - Selten auch frei programmierbar
- **Sonderaddressen**
  - Broadcast-Adresse
    - FF: FF: FF: FF: FF: FF
  - Multicast-Adressen

```
00000C Cisco
00000F NeXT
000010 Sytek
00001D Cabletron
000020 DIAB
000022 Visual Technology
0000A2 Wellfleet
...
```

```
01-00-5E-00-00-00-  Internet Multicast (RFC-1112)
01-00-5E-7F-FF-FF
01-80-C2-00-00-00   Spanning tree (for bridges)
...
```

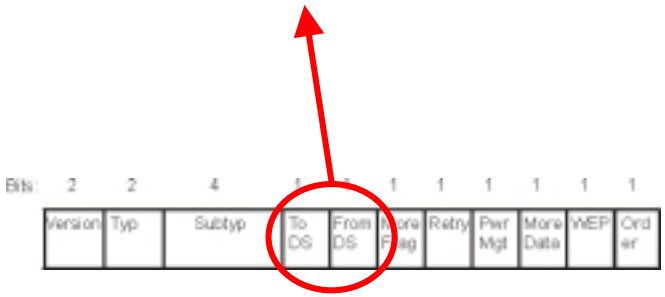
Aufbau eines Frames



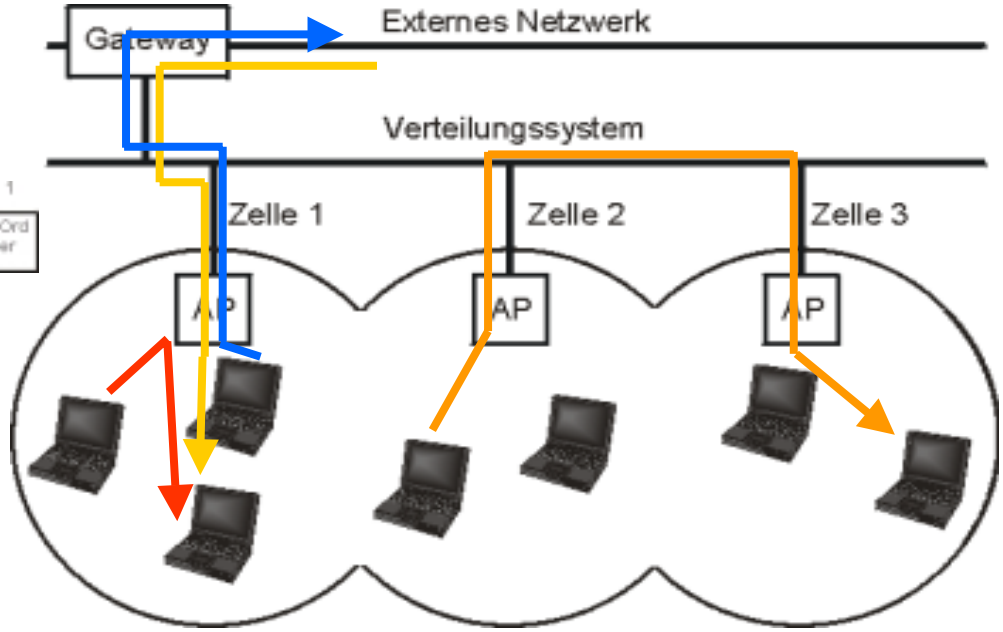
Bitfeld	Frame-Typ	Aufgabe
00	Management-Frame	Zellen-Verwaltung, z.B. Roaming
01	Kontroll-Frame	Zugriffskontrolle, z.B. Acknowledgements
10	Daten-Frame	Datenübertragung
11	Reserviert	

Adressen in IEEE 802.11 Frames

To DS	From DS	Adresse 1	Adresse 2	Adresse 3	Adresse 4
0	0	Empfänger	Sender	Zelle	-
0	1	Empfänger	Zelle	Sender	-
1	0	Zelle	Sender	Empfänger	-
1	1	Zelle	Zelle	Empfänger	Sender

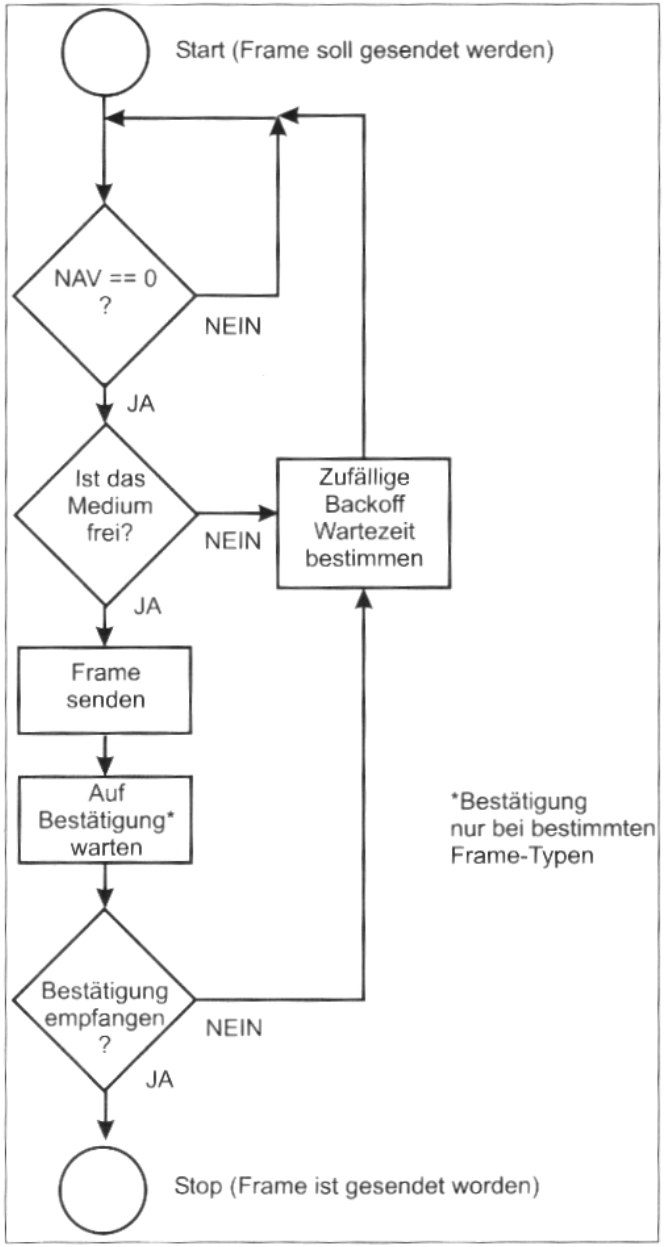


Kontrollfeld



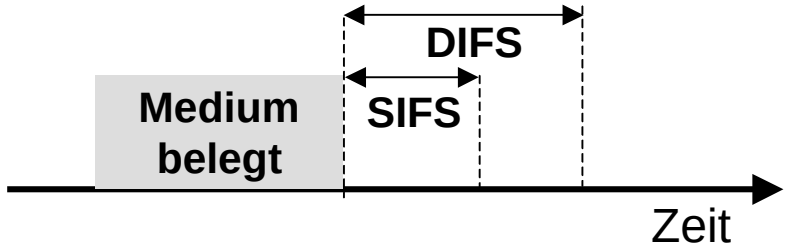
CSMA/CA

- **Standard-Zugriffsverfahren von IEEE 802.11**
- **Jede Station verwaltet einen Network Allocation Vector (NAV)**
  - Abgeleitet aus dem Feld „Dauer“ der Frames
  - Vemindert Wahrscheinlichkeit von Kollisionen
- **Kollisionen weiterhin möglich**
  - Erkennung durch ACKs
  - Teuer bei großen Frames



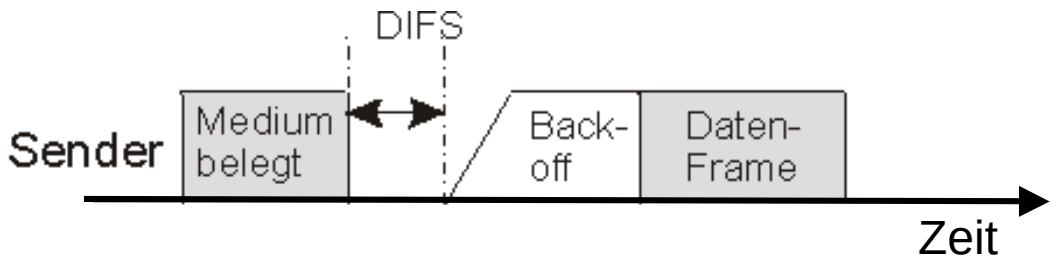
Interframespace (IFS)

- **Wie wird sichergestellt, dass ein ACK auch im Anschluss an ein Datenframe gesendet werden kann?**
  - Durch den NAV
  - Durch unterschiedliche Minimale Wartezeiten (IFS)
- **IFS-Typen**
  - Short IFS (SIFS) – ACKs und andere Kontrollframes
  - DCF IFS (DIFS) – Data- und Management-Frames
- **Länge der IFSs erzeugen Prioritäten!**

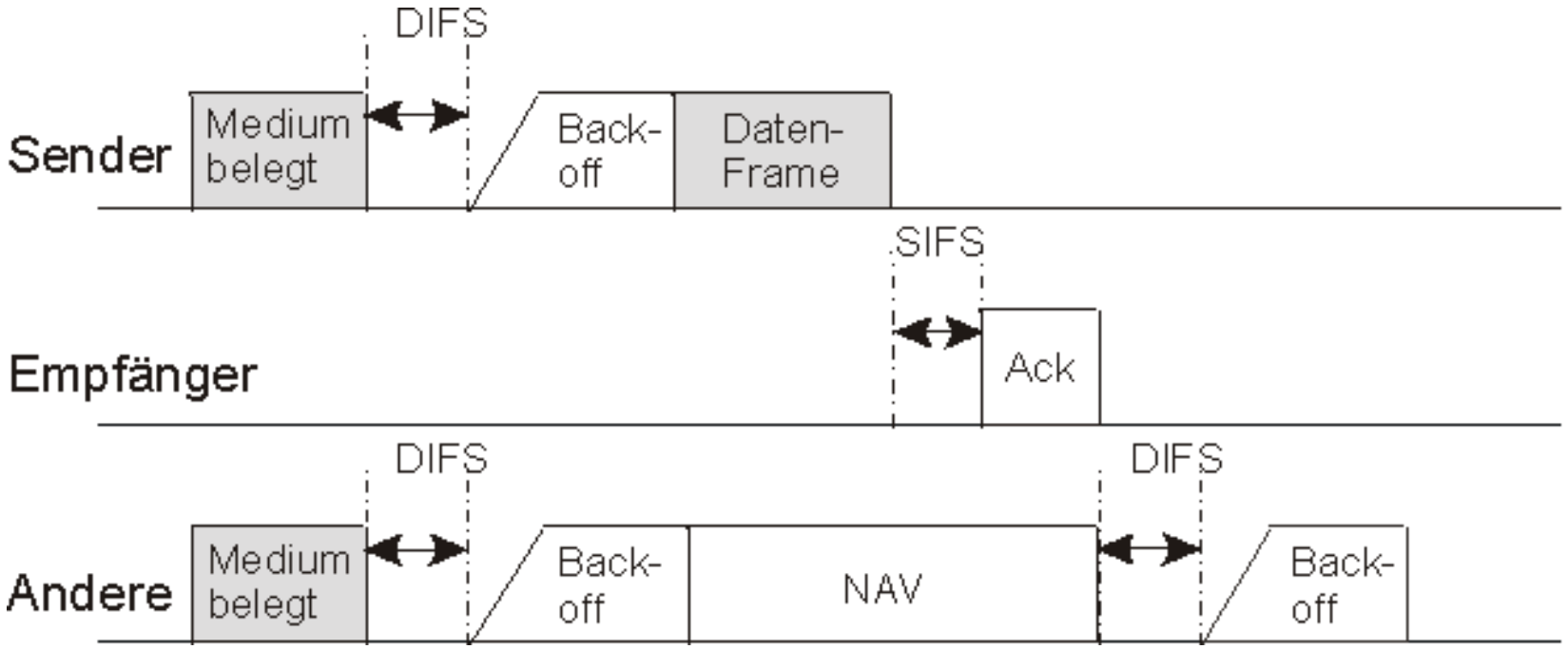


Sende-Backoff

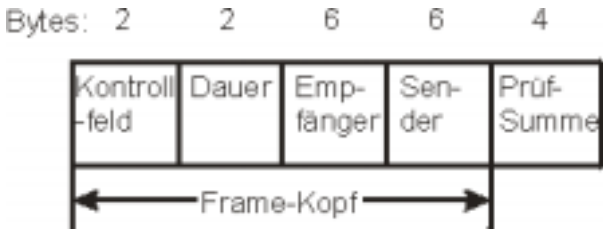
- **Wie wird sichergestellt, dass nach Ablauf des DIFS nicht alle sendewilligen Stationen senden (und kollidieren)?**
  - Durch einen weiteren zufälligen (aber kurzen) Backoff



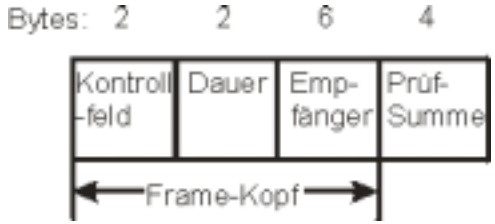
Ablauf beim Senden eines Frames



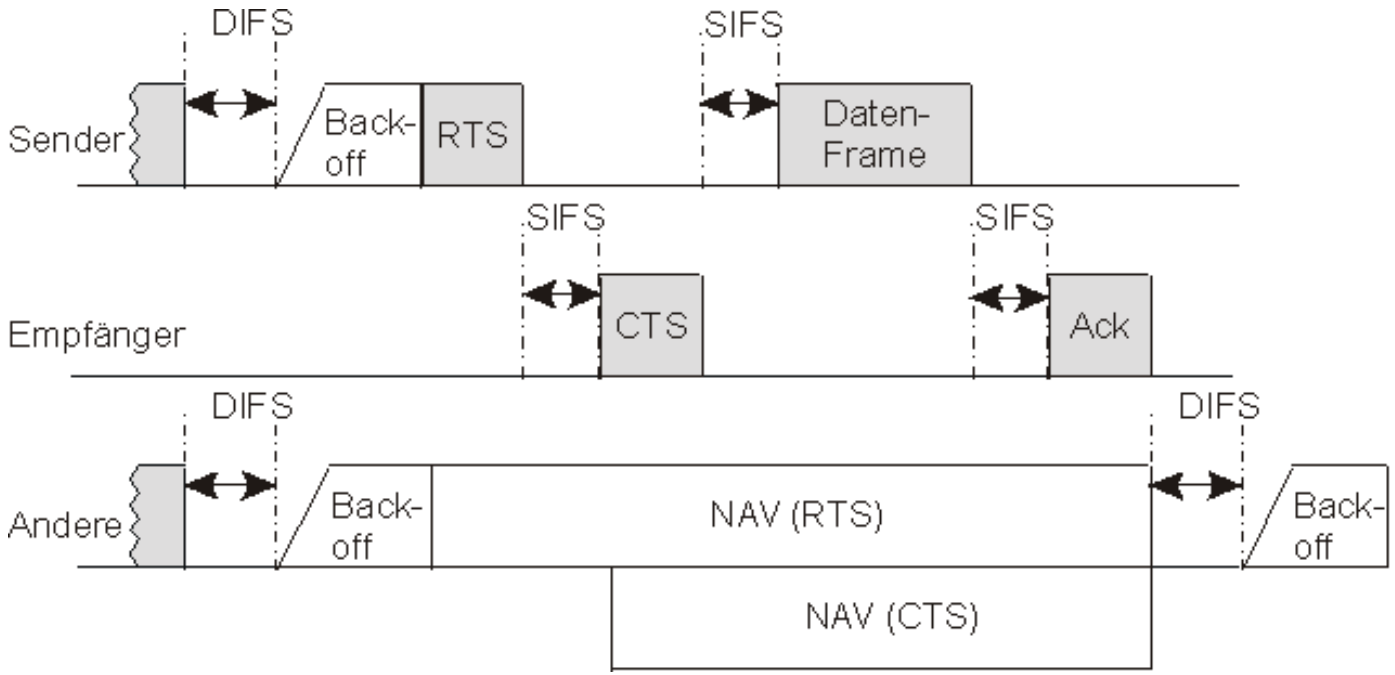
Ablauf mit RTS/CTS



RTS-Frame



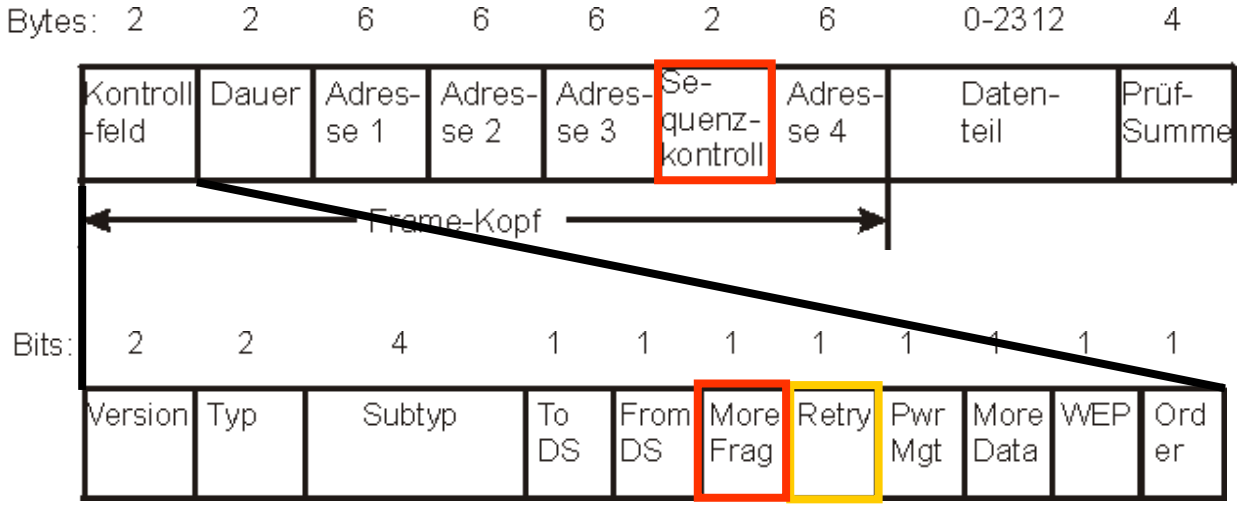
CTS-Frame

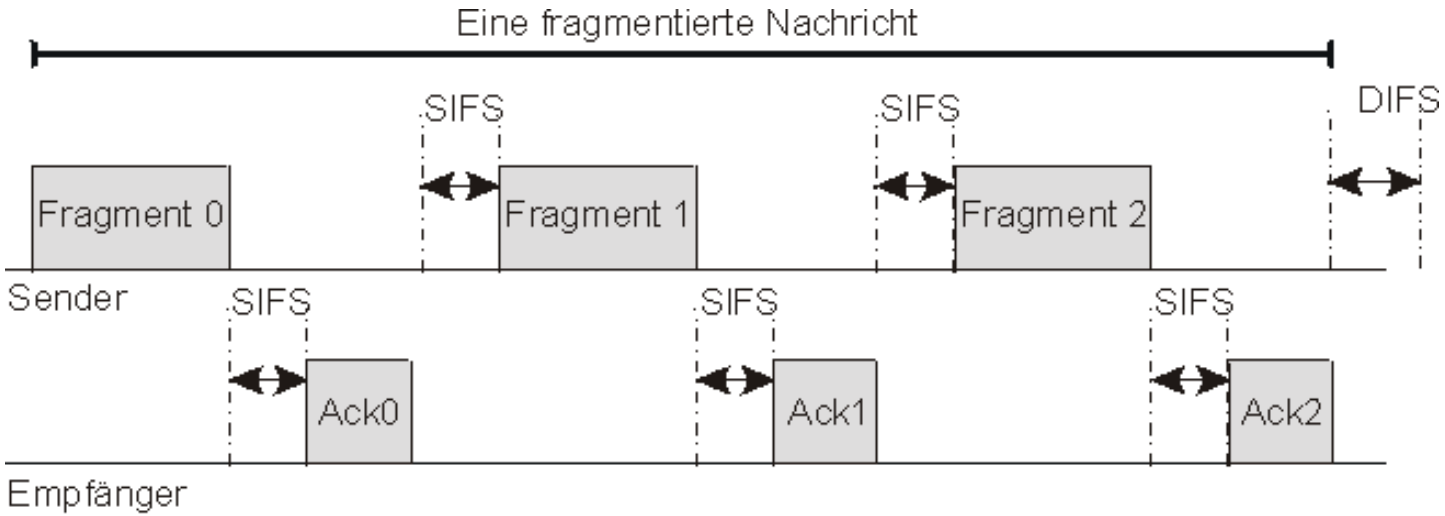


Trade-Offs bei RTS/CTS

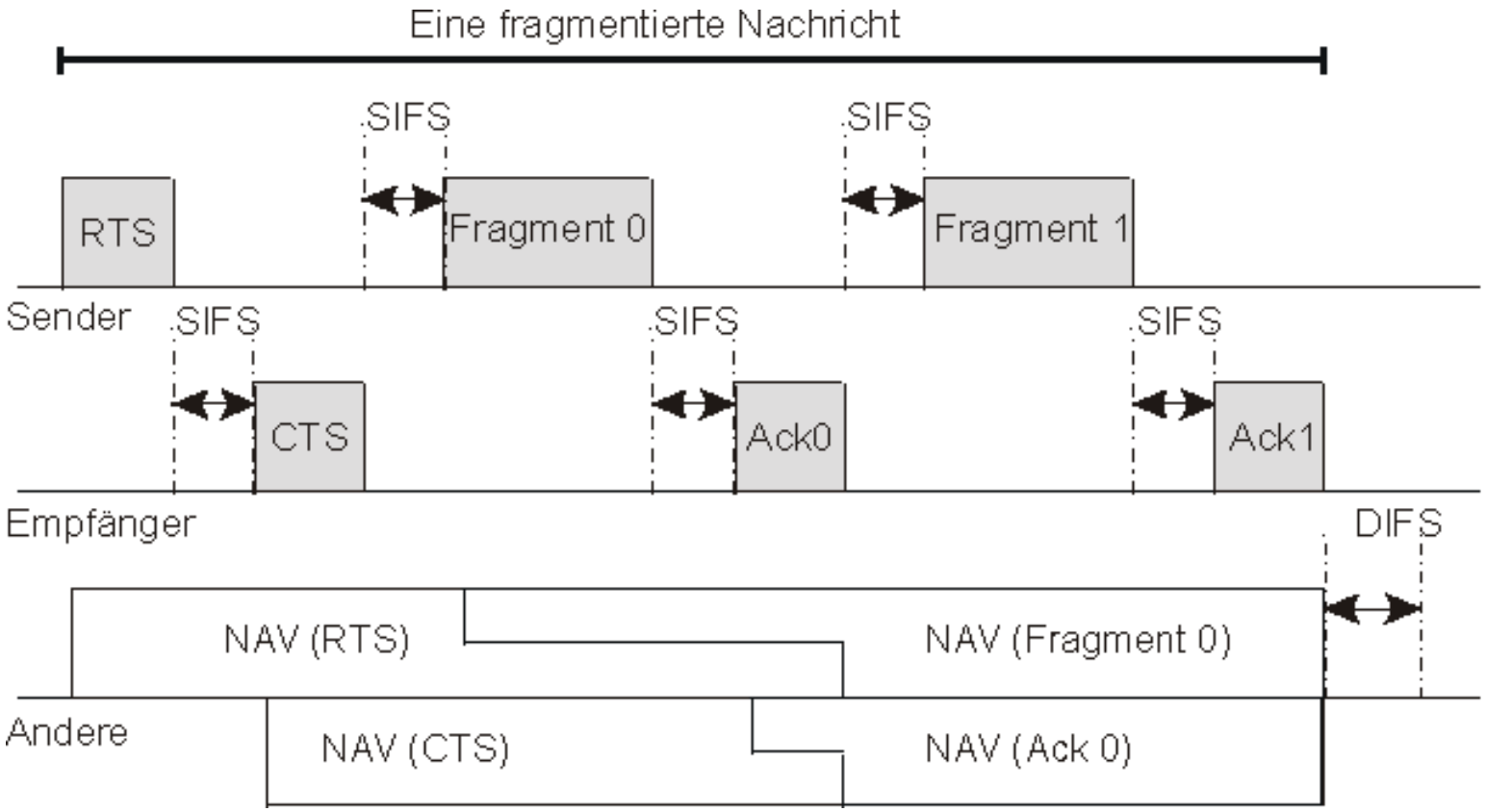
- **Vorteile:**
  - Vermeidet Kollisionen
  - Löst „Hidden-Station Problem“
- **Nachteile:**
  - Kostet Bandbreite / zusätzliche Latenzzeit
  - Weiterhin Kollisionen der RTS-Frames möglich
  - Nicht für Broad- und Multicasts
- **Anwendungsgebiet:**
  - Bei stark asymmetrischen Reichweiten
  - Bei großer Häufigkeit von langen Frames
  - Generell: bei Problemen mit Kollisionen

Fragmentierung





Fragmentierung mit RTS/CTS und NAV



Trade-Offs bei Fragmentierung

- **Vorteile:**
  - Zuverlässigere Übertragung
  - Kann Nachrichten größer als max. Frame-Länge übertragen
- **Nachteile:**
  - Kostet Bandbreite / zusätzliche Latenzzeit
  - Nicht für Broad- und Multicasts
- **Anwendungsgebiet:**
  - Bei hoher Frame-Verlustrate
  - In elektromagnetisch „verschmutzten“ Umgebungen

Der Beacon-Frame

- **Beacon = „Leuchtfeuer“**
- **Zur Erkennung der Zell-Informationen**
- **In Infrastruktur-Netzwerken**
  - Der AP sendet Beacon-Frames
- **In Ad-hoc-Netzwerken**
  - Jede Station kann senden
  - Wieder wird über zufälligen Timer entschieden

Zeit

Beacon-Frame - Format

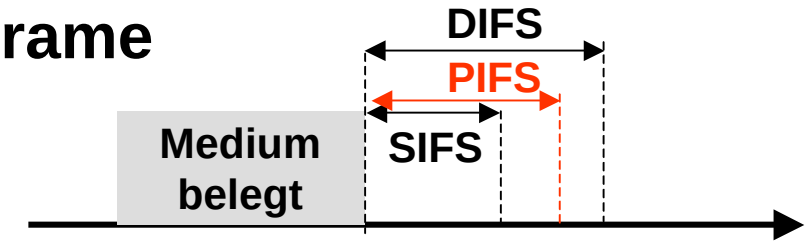
Information	Größe (Bytes)	Bedeutung
Timestamp	8	Die Uhrzeit des Senders (wird benutzt zur Uhrensynchronisation)
Beacon-Intervall	2	Die Zeitdauer zwischen zwei Beacon-Frames
Capability Information	8	Angaben zur Zelle: Ad-hoc oder Infrastruktur, CFP-unterstützt oder nicht, Verschlüsselung erforderlich oder nicht
Zellen-Adresse	6	Die Adresse der Zelle
Übertragungsraten	3-8	Angaben über die von der physikalischen Ebene in der Zelle eingesetzten Übertragungsraten
FH-Parameter	7	Falls die physikalische Ebene Frequency Hopping benutzt: Hopping-Sequenz , dwell-Zeit, ...
DS-Parameter	3	Falls die physikalische Ebene DSSS benutzt: Die aktuelle Kanalnummer
CF-Parameter	8	Falls der AP die CFP implementiert: Startzeit der nächsten CFP, maximale Dauer der CFP, Restdauer der laufenden CFP.
ATIM	4	Zum Stromsparen in Ad-hoc-Netzwerken
TIM		Zum Stromsparen in Infrastruktur-Netzwerken

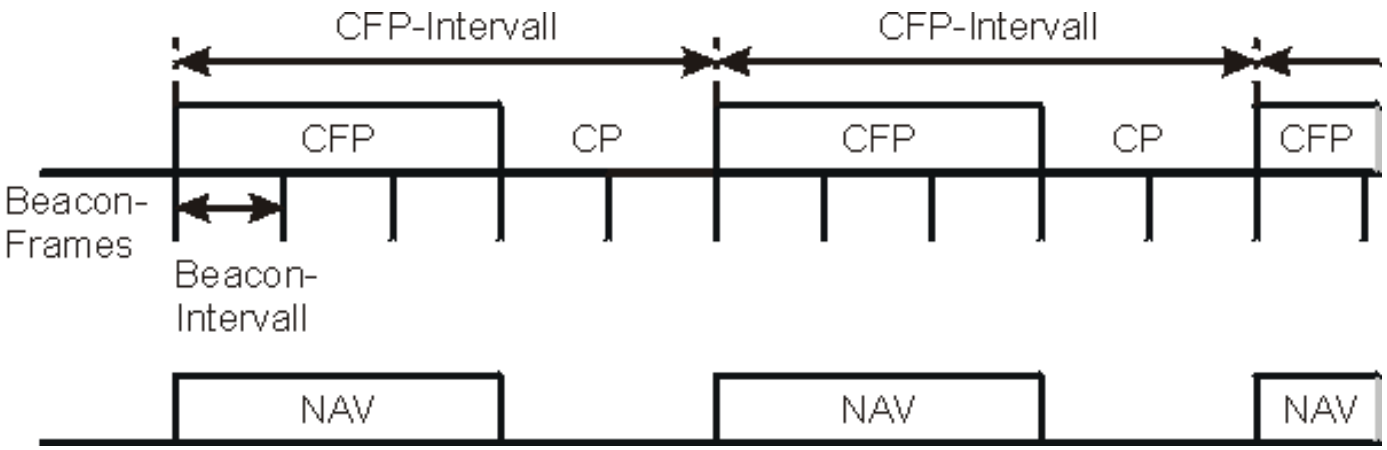
Zugriffsverfahren

- **Distributed Coordination Function (DCF)**
  - Wie bisher beschrieben
  - Verteilte Steuerung des Zugriffs
  - Mehrere Stationen können um den Zugriff konkurrieren: „Contention Period“ (CP)
  - Probabilistisches Verfahren
- **Point Coordination Function (PCF)**
  - Zentrale Steuerung des Zugriffs
  - Polling – AP ist der Koordinator
  - „Contention Free Period“ (CFP)
  - Deterministisches Verfahren
  - Optional

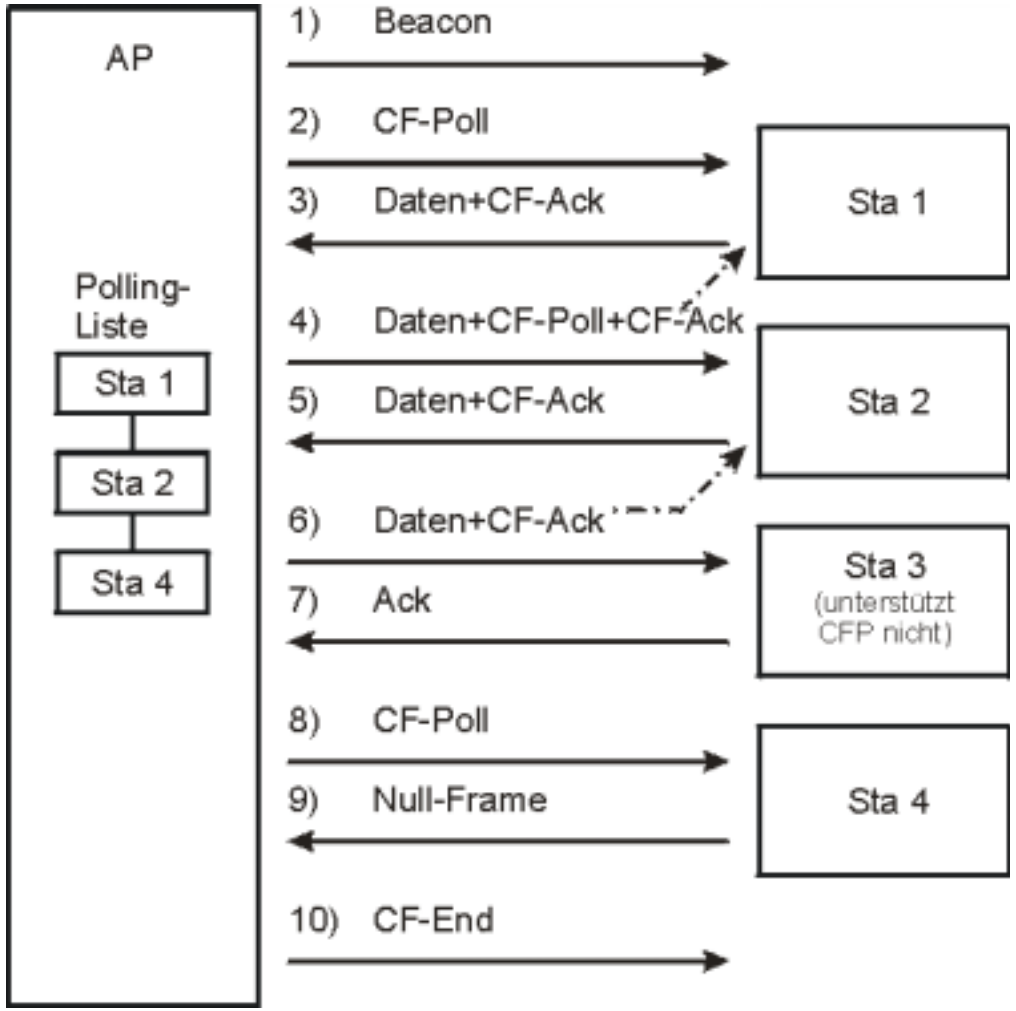
Wechsel CFP/CP

- **Länge CFP – Mehrere Beacon-Intervallen möglich**
- **Einleitung über Beacon-Frame**
  - Weiteres IFP
  - PCF IFS (PIFS)
  - Höhere Priorität als (standard) DCF IFS

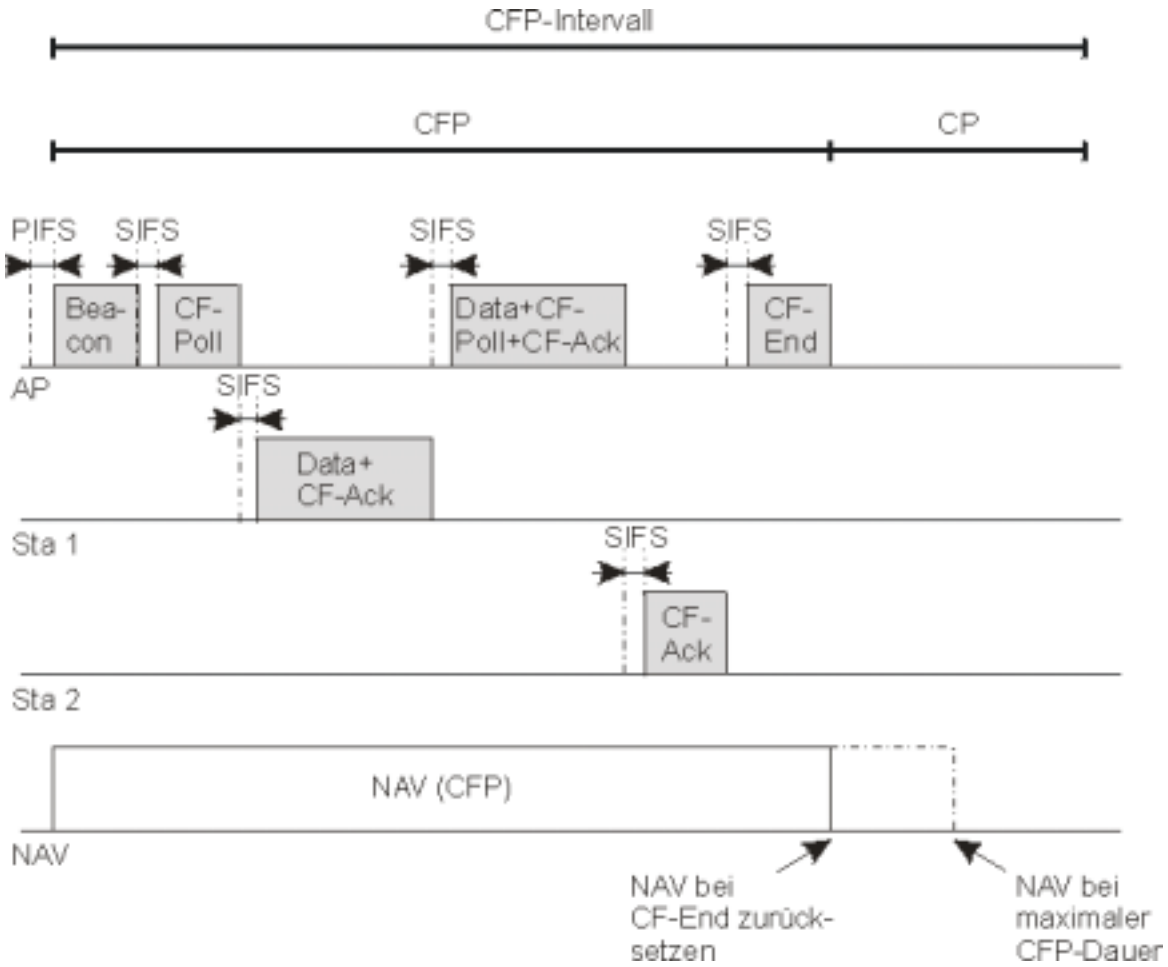




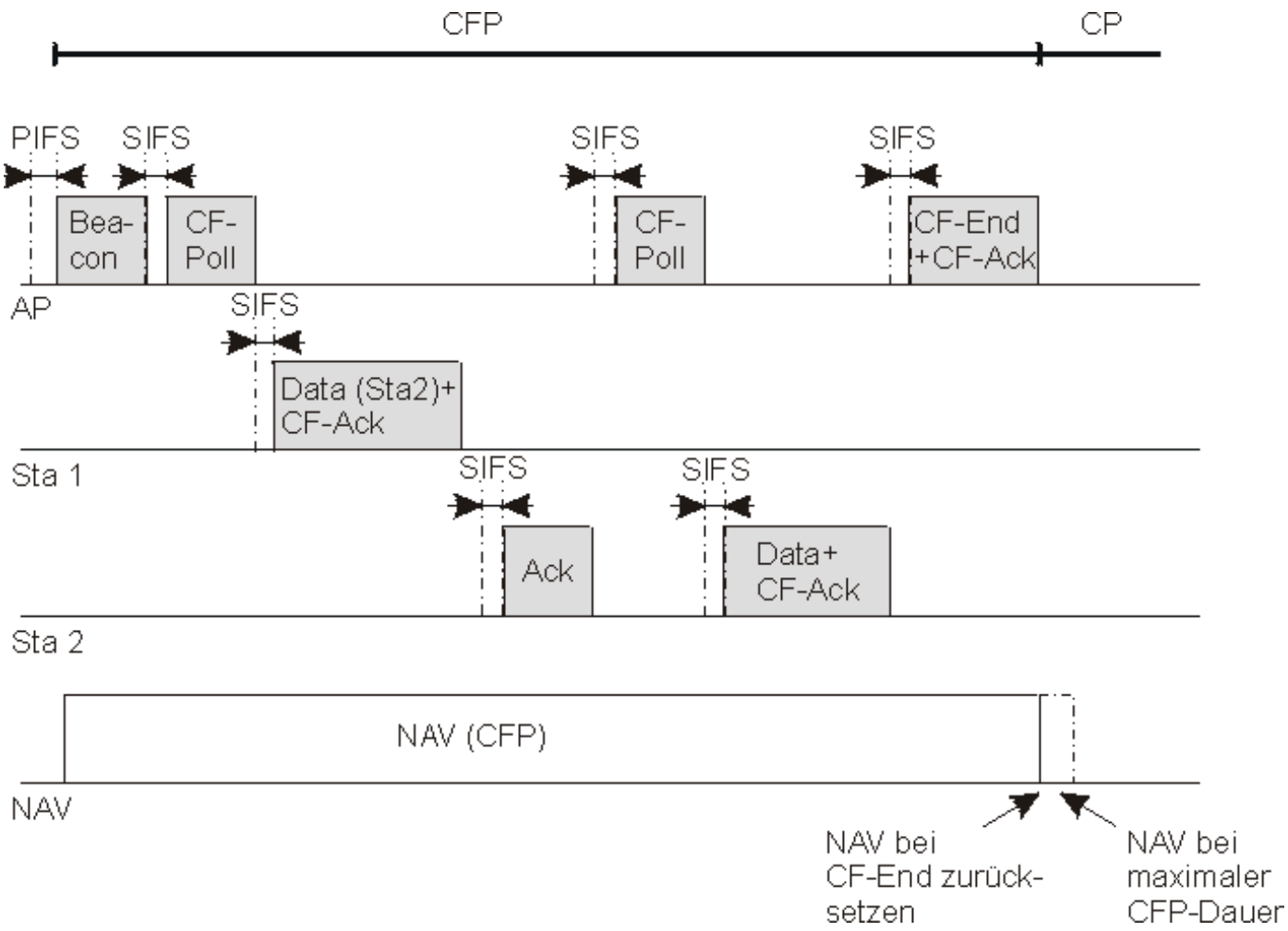
Beispiel: CFP - Framefolge



Ablauf in der CFP (über AP)



Ablauf in der CFP (direkt)



Scanning

- **„In welcher Zelle bin ich?“**
- **Passives Scanning**
  - Abhöhren aller Kanäle nach einem Beacon-Frame
- **Aktives Scanning**
  - Senden eine Management-Frames „Probe-Request“
  - Antwort Management-Frame „Probe-Response“
  - Enthält alle Daten, die auch im Beacon-Frame stehen
- **Entscheidung der scannenden Station, wo sie sich assoziieren will**
  - Anhand der Signalstärke oder
  - Anhand der Zell-Adresse

Sicherheit im WLAN

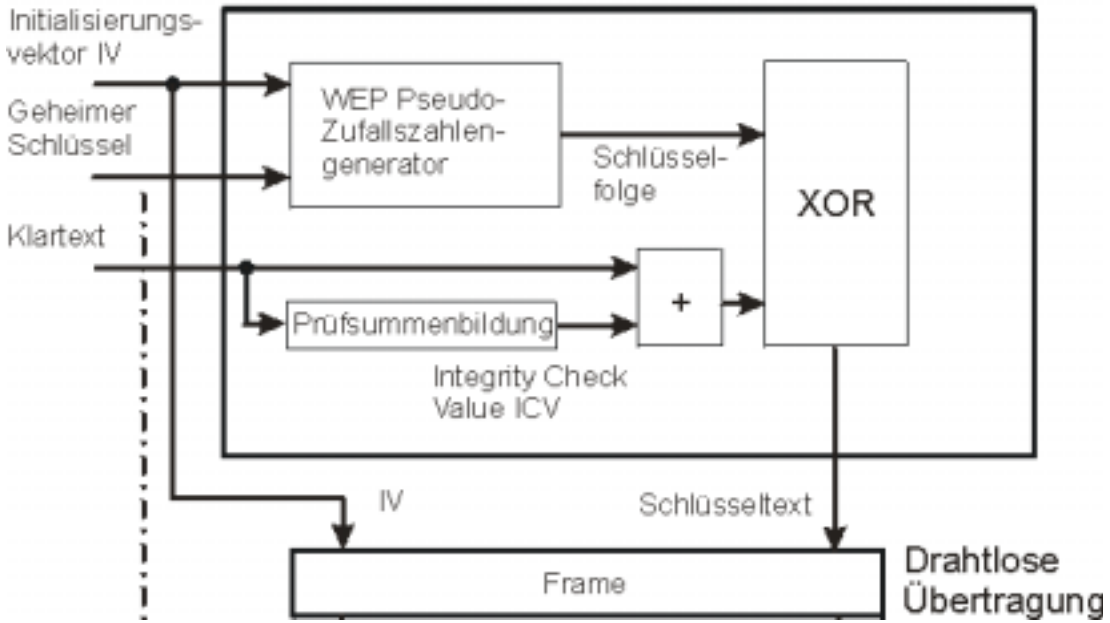
- **Mechanismen in der Sicherungsschicht**
  - Verschlüsselung (WEP)
    - symmetrisch
  - Authentifizierung
    - Beim AP
    - Aufsetzend auf Verschlüsselung
  - Zugangskontrolle
    - Über die MAC-Adressen

Verschlüsselung - WEP

- **Wired Equivalent Privacy (WEP)**
  - Ziel: Wie auf dem Kabel (aber auch nicht mehr)
- **Algorithmus**
  - Ron’s Code 4 Pseudo Random Number Generator (RC4)
  - Von RSA Security Inc.
- **Schlüssellängen**
  - 40 Bit (WEP 64)
  - 104 Bit (WEP 128)
- **Ziel**
  - Integrität, Vertraulichkeit, Authentizität (genauer: nur Zugangskontrolle)

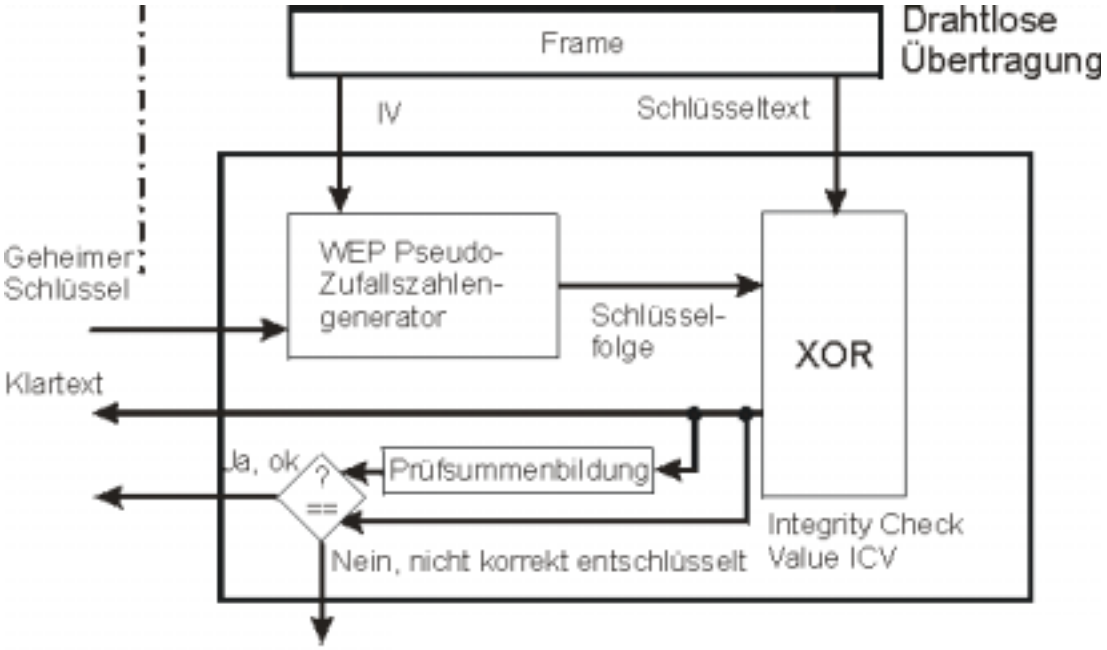
WEP (Verschlüsselung)

- **Daten (nicht der MAC-Header) werden mit Pseudozufallszahl des RC4 über XOR verknüpft**
- **Zusätzliche Prüfsumme (ICV)**
- **24 Bit Initialisierungsvektor im Klartext verschickt**



WEP (Entschlüsselung)

- **Verschlüsselte Daten wieder XOR mit der gleichen Pseudozufallszahl (= Identität)**
- **Prüfsumme muss übereinstimmen (Integrität)**

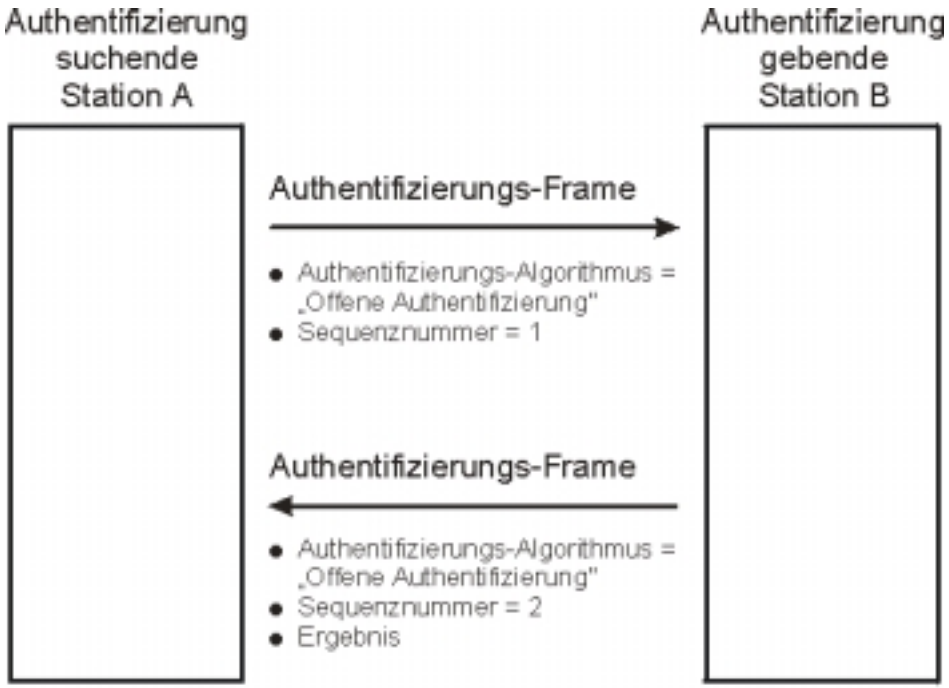


Trade-Offs des WEP-Verfahrens

- **Pros:**
  - Funktioniert für jedes Frame einzeln (wichtig bei Frame-Verlust)
  - Vergleichsweise einfach
  - Lizenzfrei (außerhalb der USA)
- **Cons:**
  - „Shared Key“-Verfahren alle Benutzen den gleichen Schlüssel (max. 4 verschiedene Schlüssel im AP sind Standard)
  - Kein Schlüsselmanagement vorgesehen
  - Es ist keine „starke Kryptographie“

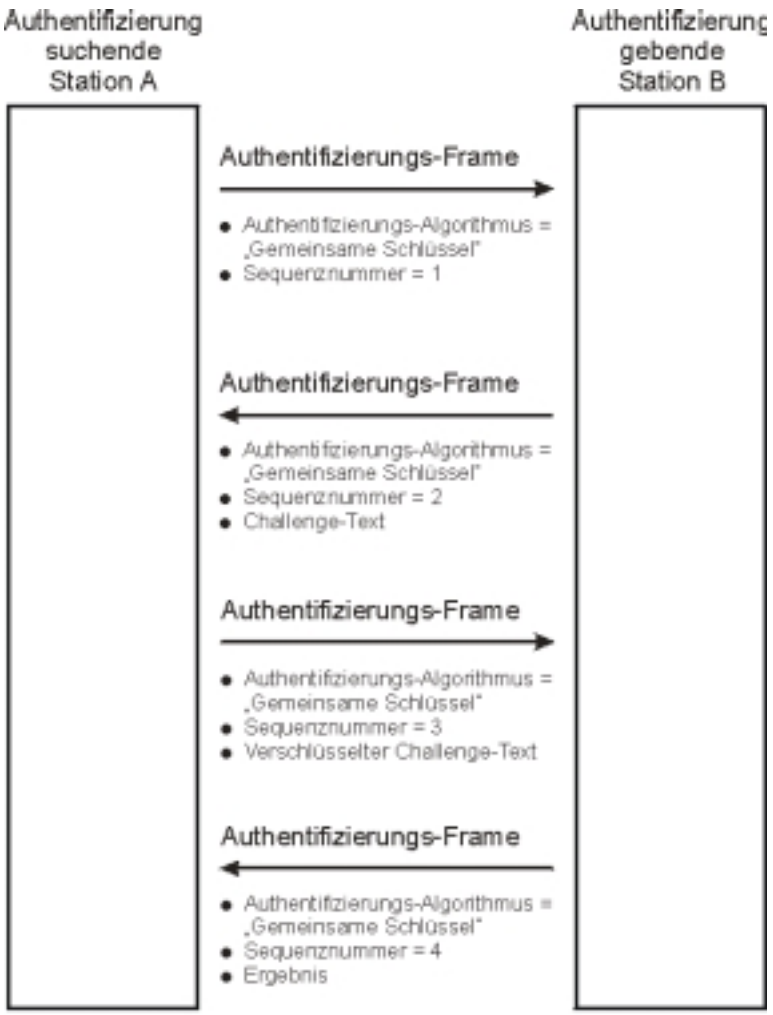
Authentifizierung (1)

- **Voraussetzung für Anmeldung**
- **„Wer ist der, der sich anmelden will?“**
- **Austausch von Management-Frames**
  - Mit Sequenznummern
- **Offene Authentifizierung**
  - Jeder darf
  - Nur für bekannte Service Set Identifiers (SSIDs)
  - „hidden“ SSIDs verschleiern Existenz von WLANs



Authentifizierung (2)

- **Durch gemeinsamen Schlüssel**
  - Benutzung des WEP-Verschlüsselungsverfahrens
  - Gemeinsames Geheimnis, z.B. Password

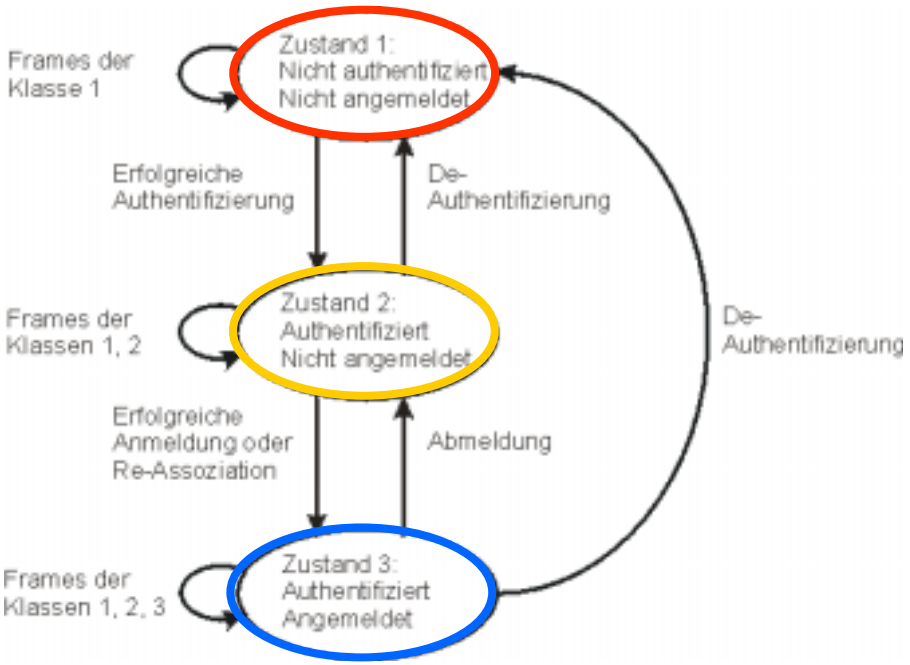


Zugangskontrolle

- **AP entscheidet anhand der MAC-Adresse, ob eine Station authentifiziert wird.**
- **Pros**
  - Einschränkungen möglich
- **Cons**
  - MAC-Adressen können gefälscht werden
    - Gefälschte Adressen werden bei „doppelter“ Anmeldung erkannt
  - Aufwendig zu managen
    - Zentraler Server (z.B. „RADIUS“) möglich
  - Passives Mithören immer möglich

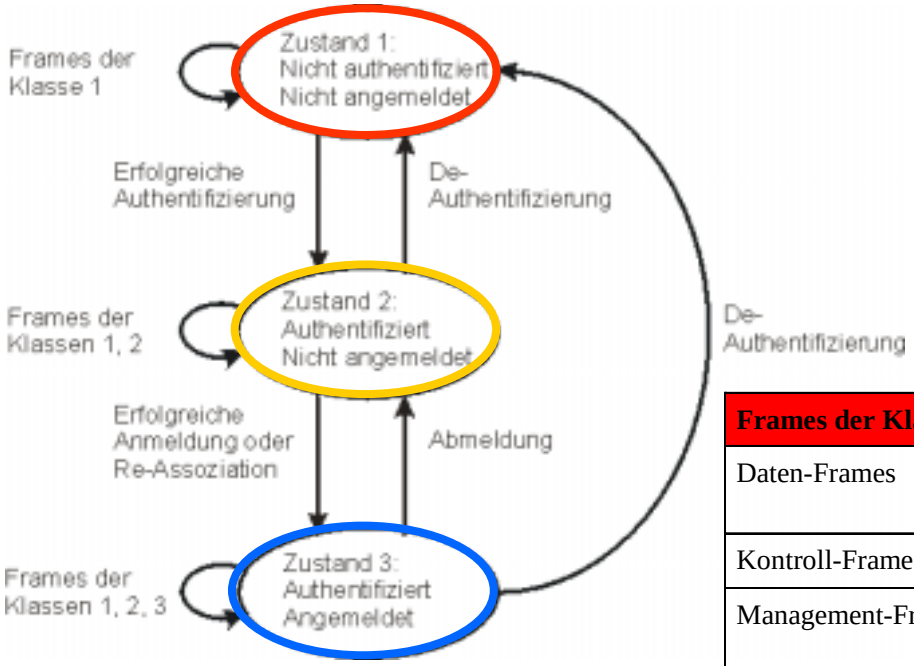
Assoziation

- **„Wer ist bei welchem AP angemeldet?“**
- **Association-Request**
  - Bitte um Aufnahme in die Zelle
- **Association-Response**
  - Entscheidung des AP
  - Datenrate und DCF Info
- **Disassociation-Request**
  - Abmeldung
- **Reassociation-Request**
  - Wie Association-Request
  - Mit Angabe der vorherigen Zelle



Zustandsübergänge

Zugelassene Frames



Frames der Klasse 1 (erlaubt in den Zuständen 1, 2 und 3)	
Daten-Frames	Alle, aber nur innerhalb der Zelle (Bits `To DS` und `From Ds` nicht gesetzt)
Kontroll-Frames	Alle außer `PS-Poll` (Strom sparen im Infrastruktur-Netzwerk)
Management-Frames	Alle außer `Association Request/Response`, `Reassociation Request/Response`, `Disassociation`
Frames der Klasse 2 (nur erlaubt in den Zuständen 2 und 3)	
Management-Frames	Alle übrigen, also `Association Request/Response`, `Reassociation Request/Response`, `Disassociation`
Frames der Klasse 3 (nur erlaubt im Zustand 3)	
Daten-Frames	Alle Daten-Frames, bei denen die Bits `To DS` oder `From Ds` gesetzt sind

Power-Management (1)

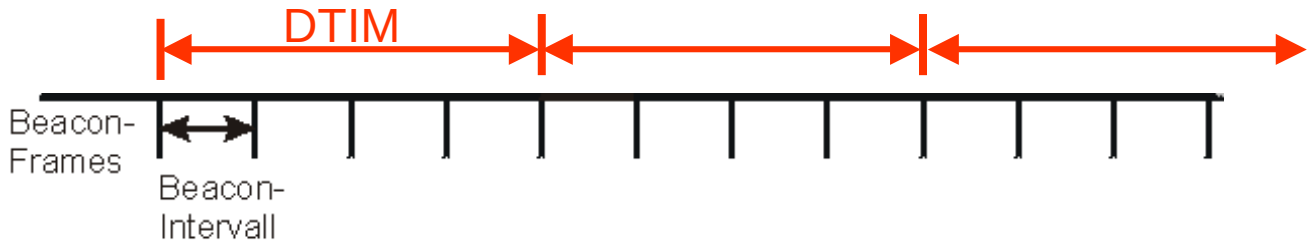
- **Wichtig für mobile Systeme**
- **Strom sparen heißt**
  - Nicht immer empfangsbereit (und sendebereit) sein zu müssen
  - Der Transceiver kann abgeschaltet werden
- **Annahme**
  - „Der AP ist immer wach“
- **Idee**
  - „Der AP speichert Frames für schlafende Stationen“

Power-Management (2)

- **Wie kommen Stationen an zwischengespeicherte Frames?**
- **Polling**
  - Station sendet *Power-Save-Poll* (PS-Poll) an den AP
  - AP antwortet mit Frame
    - Bit *More Data* gesetzt, wenn weitere Frames vorhanden
- **Woher weiß eine Station, dass Frames für sie vorliegen?**
- **AP sendet Traffic indication Map (TIM)**
  - Mit jedem Beacon Frame
  - Alle Stationen kennen die Beacon-Intervalle
  - Können zu bestimmten Vielfachen aktiv werden

Power-Management (3)

- **Was passiert mit Broad- und Multicasts?**
  - Werden auch gespeichert
  - Können nicht per PS-Poll abgerufen werden
  - Sondern werden in bestimmten Beacon-Intervallen an alle gesendet (Delivery TIM, DTIM)



- **Im Ad-hoc Netzwerk?**
  - Nach jeden Beacon bleiben alle Stationen eine Zeit aktiv
  - In dieser Zeit, kann jede Station, die etwas senden möchte, ein Ad-hoc TIM Management Frame senden
  - All Stationen, die als Empfänger genannt werden, müssen aktiv bleiben.