1 WLAN Standards

1.1 802.11 Standards

IEEE 802.11 ist der Hauptstandard, unter dem alle WLAN-Standards zusammengefasst sind. Die folgende Tabelle zeigt die unterschiedlichen Unterstandards und deren Besonderheiten:

Standard	Jahr	Übertragungs-rate	Reichweite*	Parallel nutzbare Kanäle	Besonderheiten
802.11	1997	1 – 2 Mbit/s	100m (20m)		Erster WLAN-Standard
802.11 a	1999	bis 54 Mbit/s	120m (35m)	19	- 5 GHz-Band; wird von Militär und Flugsicherung genutzt, daher nur Nutzung innerhalb von Gebäuden mit verringerter Sendeleistung erlaubt. - Nutzung von OFDM[1]
802.11 b	1999	bis 11 Mbit/s	140m (38m)	3	- 2,4 GHz-ISM[2]-Band - Erweiterung von 802.11
802.11 g	2003	54 Mbit/s	140m (38m)	3	- 2,4 GHz-Band mit OFDM - Abwärtskompatibel zu 802.11 b
802.11 n	*2006* 2009	bis 600 Mbit/s	250m (70m)	3 bzw. 1 oder 19 bzw. 9[3]	- MCS[4]-Modulation Berücksichtigung von Interferenzen, Bewegung von Sender bzw. Abschwächung des Signals zur Optimierung der Übertragungsrate - Einsatz von MIMO[5]-Antennentechnik (2-4 Antennen) zur Übertragungsraten- und Reichweitensteigerung
802.11 ac	2013	bis 1 Gbit/s	50m	28 + 40	- Höhere Übertragungsrate im 5 GHz-Band
802.11 ad	2012	Bis 7 Gbit/s	10m		- 60 Ghz mit Beamforming-Antennen - dachte für Videosysteme

*Tabelle 1: 802.11 Hauptstandards; *: Werte in Klammern innerhalb von Gebäuden. Kann sehr stark variieren*

Standard	Erweitert	Besonderheit
802.11d	a, b, g, h	länderspezifisches WLAN; Regelt technische Unterschiede in Ländern
802.11e	a, g, h	Bietet QoS für Echtzeitanwendungen
802.11f	a, g, h	Roaming zwischen Access Points im Netz; wurde 2006 zurückgezogen;
802.11h	a	Kanalwahl; Harmonisierung von 802.11 a durch DFS[6] und TPC[7]
802.11i	a, b, g, h	TKIP[8], PSK[9] und EAP[10] sowie AES[11] zwischen a und b Einführung von WPA[12] bzw. WPA2 lösen das unsichere WEP[13] ab.
802.11j	a, h	HiperLAN; Erweiterung für japanischen Markt

Tabelle 2: 802.11 Erweiterungsstandards

1 OFDM: **O**rthogonal **F**requency **D**ivision **M**ultiplex
2 ISM: **I**ndustrial, **S**cientific, **M**edical
3 abhängig von verwendeter Kanalbreite 20/40MHz
4 MCS: **M**odulation **C**oding **S**cheme
5 MIMO: **M**ultiple **I**nput, **M**ultiple **O**utput
6 DFS: **D**ynamic **F**requency **S**election
7 TPS: **T**ransmission **P**ower **C**ontrol
8 TKIP: **T**emporal **K**ey **I**ntegrity **P**rotocol
9 PSK: **P**re-**S**hared-**K**ey
10 EAP: **E**xtensible **A**uthentication **P**rotocol
11 AES: **A**dvanced **E**ncryption **S**tandard
12 WPA: **W**iFi **P**rotected **A**ccess
13 WEP: **W**ired **E**quivalent **P**rivacy

1.2 Übertragungsrate in Abhängigkeit der Entfernung

Je weiter Sender und Empfänger voneinander entfernt sind, umso mehr müssen die beiden Endpunkte ihre Datenrate drosseln, um die Verbindung aufrechterhalten zu können. Das folgende Diagramm verdeutlicht diese Abhängigkeit für 802.11g.

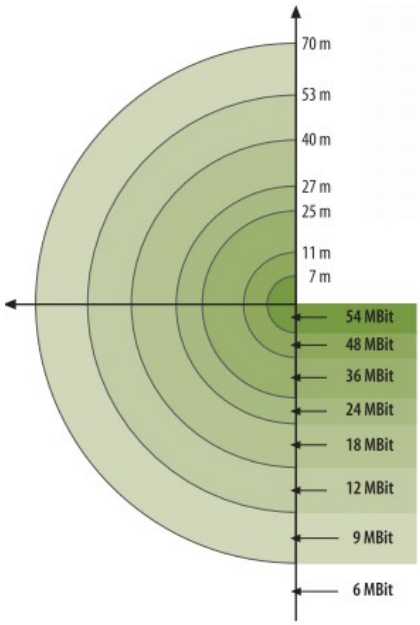


Abbildung 1: Übertragungsrate in Abhängigkeit der Entfernung; Quelle: c't 13/09 S.88

Im nachfolgenden Diagramm sind die unterschiedlichen Varianten Empfangs- und Sendevarianten aufgezeigt.

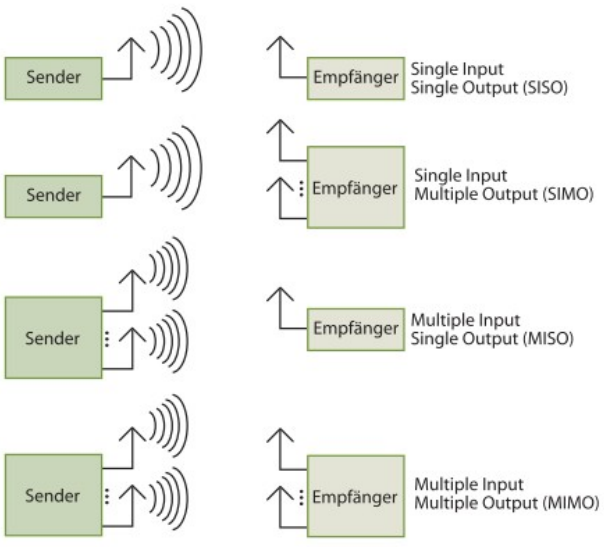


Abbildung 2: Unterschiedliche Sende-/Empfangsvarianten; Quelle: c't 13/09 S.88

Die Logik hinter den Bezeichnungen **SISO**, **SIMO**, **MISO** und **MIMO** bezieht sich jeweils auf eine **Funkverbindung (radio link)**. Dabei wird der Sender als **INPUT** interpretiert, also als in die Funkverbindung **hinein**sendend. Und der **Empfänger** als **OUTPUT** interpretiert, also aus der Funkverbindung **heraus**empfangend.

Geschieht dies mit **mehr als einer Antenne**, so handelt es sich um **multiple** (mehrfaches) **INPUT**/**OUTPUT**.

Bei den **Multiple-Input-Verfahren** werden die gleichen Daten über mehrere Antennen versendet. Der Empfänger kann aus den empfangenen Signalen das optimale Signal extrahieren. Der Vorteil bei diesem Vorgehen liegt darin, dass nur der Sender über mehrere Antennen verfügen muss und der Empfänger ggf. sogar mit einer Antenne auskommt, wodurch Platz gespart werden kann (vgl. Mobilfunktelefone).

1.3 Frequenzspektren

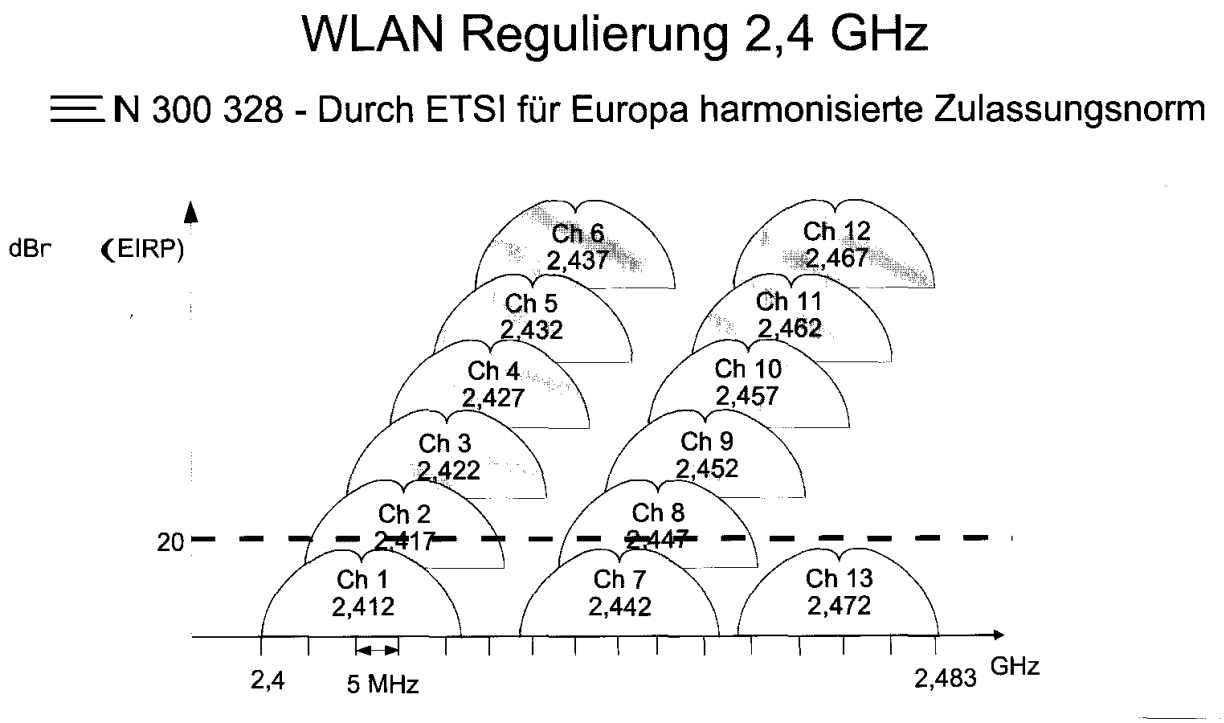


Abbildung 3: Kanalraster für Europa im 2,4GHz-Band

Die obige Abbildung zeigt das Kanalraster für das 2,4 GHz-Band. Wichtig ist dabei zu beachten, dass zwar die Überlagerung unmittelbar am AP gering, aber an anderen Stellen innerhalb der Funkzelle trotzdem sehr hoch sein kann. Der AP erfasst in seinen Statusdialogen eben nur die Strahlung, die er direkt an seiner Antenne messen kann. Daher ist es sinnvoll das gesamte Gebiet, in dem das WLAN genutzt werden, soll mit einem Messgerät abzuschreiten, um sicherzustellen, dass möglichst keine zu großen Beeinflussungen von anderen APs ausgehen.

2 Zugriffsverfahren im WLAN

2.1 CSMA/CA[14]

Das bei WLAN verwendete Zugriffsverfahren ist eine Abwandlung des bereits vom Ethernet bekannten CSMA. Hier allerdings nicht mit **Kollisionserkennung (CD)** sondern mit **Kollisionsvermeidung (CA)**. Aufgrund der relativ hohen Sendeleistung ist der Sender kaum in der Lage eine Kollision zu erkennen. Bei der Vermeidung werden die folgenden Fälle unterschieden:

1. Jeder darf senden, wenn das Medium hinreichend lange frei war und zuvor keine Übertragung stattgefunden hat.
2. Wurde gerade gesendet, so müssen die Stationen warten und in die sogenannte „Contention[15] Phase" (vgl. Kollisionsauflösung bei CSMA/CD) wechseln.

Innerhalb der **Contention Phase** wird die Zeit nach Beendigung der aktuellen Übertragung in Zeitschlitze (time slots) aufgeteilt. Per Zufall wird von den Stationen einer dieser **time slots** ausgewählt und mit dem Senden begonnen. Dies kann aber dennoch eben dann zu Kollisionen führen, wenn sich zwei Teilnehmer denselben time slot aussuchen.

Ein Weiteres Problem sind die sogenannten der **„unsichtbaren Stationen"**. Es kann vorkommen, dass zwei Stationen so weit voneinander entfernt sind, dass sie gerade außerhalb ihrer Empfangsbereiche sind. Hierdurch sind sie nicht in der Lage zu erkennen, dass sie sich gegenseitig stören.

14 CSMA/CA: **c**arrier **s**ense **m**ultiple **a**ccess/**c**ollision **a**voidance; Kollisionsvermeidung
15 Contention: eng. Wettstreit, Streitigkeit, Auseinandersetzung

Dieses Problem lässt sich mittels **RTS**[16] und **CTS**[17] lösen. Hier sendet eine sendewillige Station statt ihrer Daten in ihrem time slot zunächst ein RTS. Hiermit kündigt sie durch ein kurzes Paket an, dass sie senden will und wie lange sie vorhat zu senden. Die benachbarte Station, die ein freies Medium detektiert, antwortet daraufhin mit CTS, sodass alle anderen Stationen wissen, dass das Medium ab jetzt belegt sein wird und für wie lange. Da alle Stationen, die nichts mit der Übertragung zu tun haben, somit über die Belegung des Mediums informiert sind, ohne das Medium unmittelbar daraufhin abzuhören, nennt man dieses Verfahren auch „virtual carrier sense". Die RTS Pakete sind besonders kurz, sodass selbst bei Kollision dieser Pakete nur kurze Kollisionen entstehen.

Ein weiterer Mechanismus steuert die Wartezeiten zwischen den einzelnen Sendephasen. Mittels des **SIFS**[18] wird den Stationen Zeit gegeben, zwischen Empfangs- und Sendemodus zu wechseln. Eine weitere Zeit ist als **DIFS**[19] definiert und dient dazu die unterschiedlichen Laufzeiten der Signale auszugleichen.

Die folgende Abbildung verdeutlicht die Zusammenhänge:

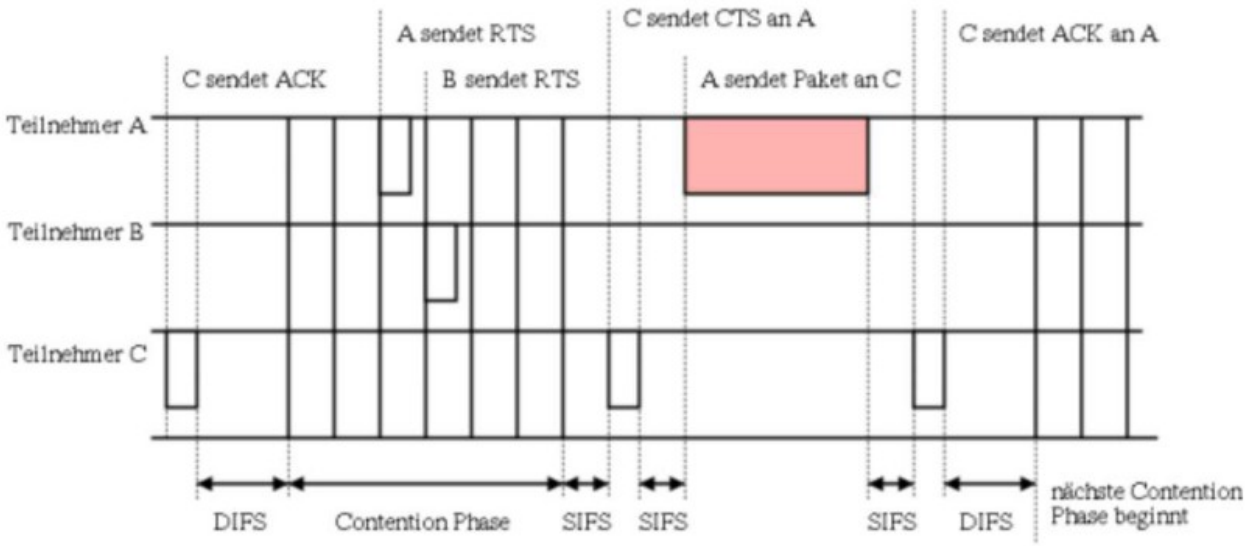


Abbildung 4: CSMA/CA mit RTS/CTS Handshake; Quelle. Uni-Oldenburg, Medium Access Control

Gut geeignet ist dieses Verfahren vor allem in sogenannten Ad-Hoc Netzen, da es ohne zentrale Steuerung auskommt. Allerdings zum Preis schlechter Ausnutzung der Bruttoübertragsrate.

2.2 Polling

Abweichend vom dezentralen CSMA wird der Zugriff auf das Medium beim Polling von der Basisstation gesteuert. Polling kann demnach bei Ad-Hoc-Netzen nicht eingesetzt werden.

Die Basisstation fragt in der ersten Phase die Teilnehmerstationen an, ob sie Bedarf für eine Sendung haben. Dies geschieht ähnlich wie bei CSMA. Die hier vorkommenden Kollisionen werden durch zufälliges Senden reduziert.

Nach dieser Phase „pollt" die Basisstation die sendewilligen Teilnehmer ab, so dass es zu einem kontrollierten Sendeverhalten kommt. Durch diese Kontrolle ist es auch möglich, ein QoS für einzelne Stationen zu realisieren. Bei CSMA/CA wäre dies nicht realsierbar.

16 RTS: **r**equest **t**o **s**end
17 CTS: **c**lear **t**o **s**end
18 SIFS: **s**hort **i**nter**f**rame **s**pacing
19 DIFS: **D**CF **i**nter**f**rame **s**pacing; DCF: **d**iscret **c**osine **f**ourier transformation

3 WLAN Verbindungstypen

3.1 Ad-Hoc (ohne APs)

Unter einer **Ad-Hoc**[20]-Verbindung versteht man eine spontane Verknüpfung von zwei oder mehr WLAN-fähigen Endgeräten. Dabei kommt kein AP zum Einsatz, sondern die Geräte verbinden sich unmittelbar miteinander. Diese Art der Zusammenschaltung sollte nur für temporäre Verbindungen und wenige Clients genutzt werden, da jedes Endgerät eine eigene Routing-Tabelle pflegen muss. Ein dauerhafter

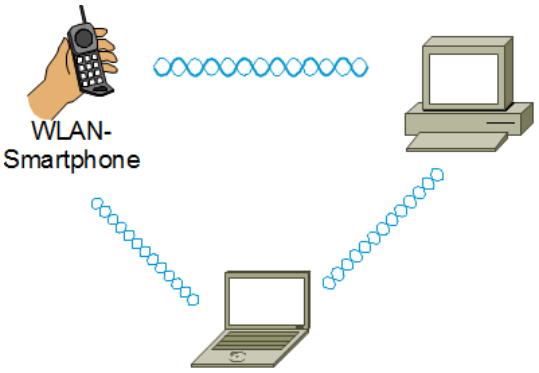
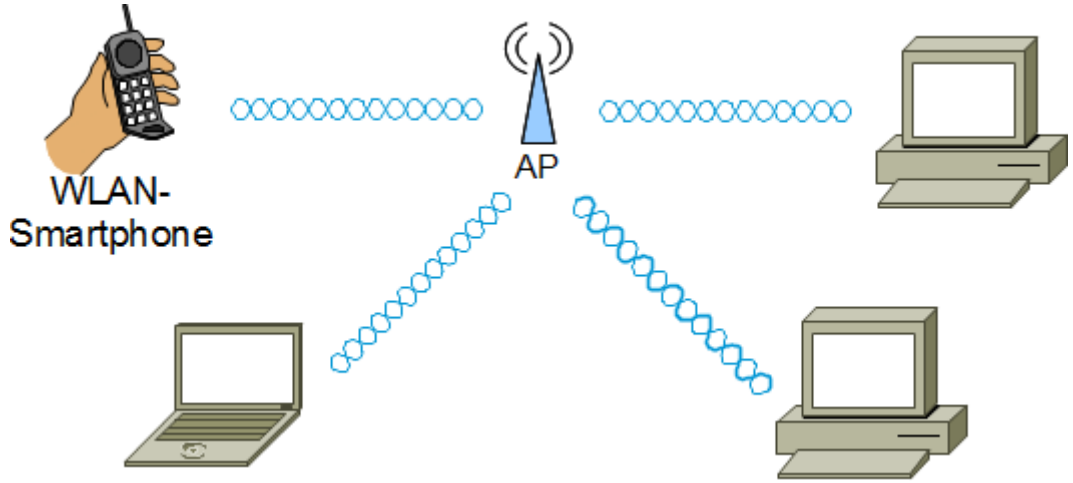


Abbildung 5: Ad-Hoc Netz

Betrieb ist sinnvoller mit der Infrastruktur-Variante (s. 3.2) umzusetzen.

3.2 Infrastruktur (mit APs)

Bei der **Infrastruktur**-Variante werden APs zur Bildung von Inseln eingesetzt. Die Endgeräte werden in der sogenannten AP-Betriebsart betrieben. Der AP bildet hierbei die „WLAN-Zentrale", über die alle Nachrichten laufen.



Zur Absicherung des Zugriffs werden Verschlüsselungsverfahren wie WEP, WPA bzw. WPA 2 eingesetzt. WEP gilt als unsicher, da hier in regelmäßigen Abständen der Schlüssel (40 bzw. 64-bit) übertragen wird und dieser mit moderner Hardware binnen kurzer Zeit entschlüsselt werden könnte. WEP sollte demnach ausschließlich aus Kompatibilitätsgründen eingesetzt werden, wenn ältere Hardware, die keine WPA-Variante unterstützt betrieben werden muss.

Zur Vereinfachung der WLAN-Konfiguration kann WPS[21] verwendet werden. Es werden vier Varianten bei WPS unterschieden:

- PIN Zahlencode; persönlicher Code
- PBC Push Button Configuration; Per Taster (Hard- oder Software) wird WPS aktiviert
- UFD USB Flash Drive; Austausch per USB-Stick
- NFC Near Field Communication; Geräte werden sehr nah zueinander positioniert

20 Ad hoc: lateinisch „zu diesem" im Sinne von „zu diesem Augenblick" oder „aus dem Stehgreif"
21 WPS: **W**iFi-**P**rotected **S**etup; Automatisiertes Verfahren zur Konfiguration von Clients

3.3 WLAN-Roaming

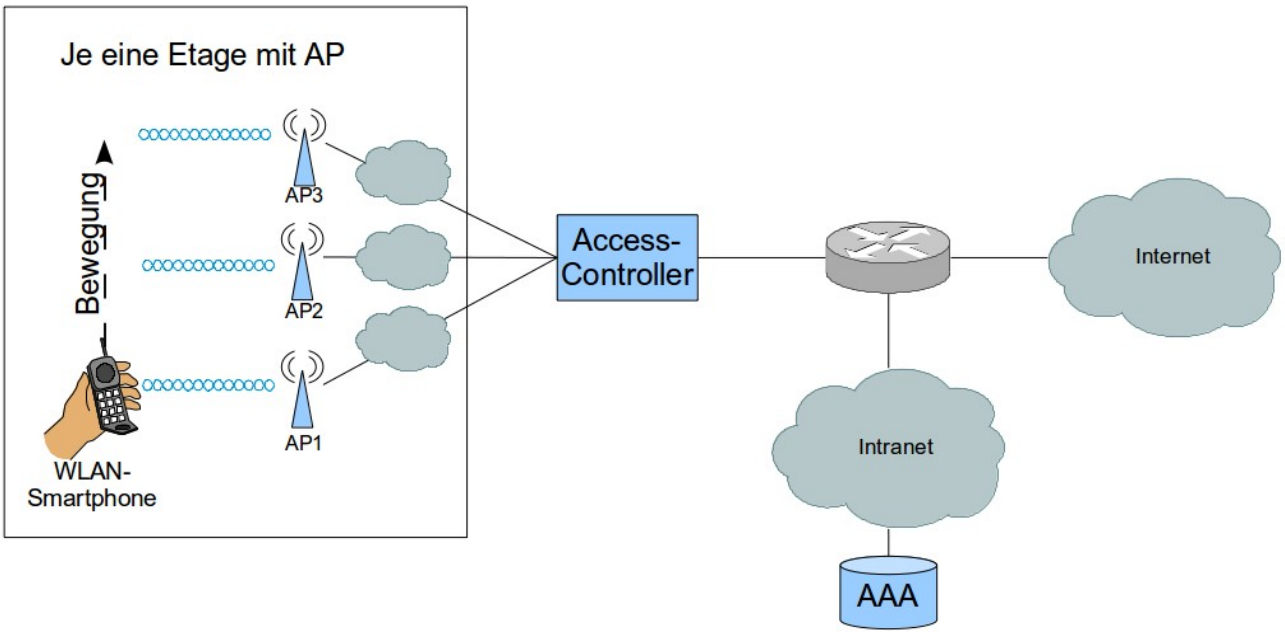


Abbildung 6: Beispiel für WLAN-Roaming in einem Hotel

Beim **WLAN-Roaming** werden die beiden folgenden Fälle unterschieden:

1. Layer 2 Roaming
2. Layer 3 Roaming

Im ersten Fall müssen sich die beiden AP im selben Subnetz befinden und benachbarte Funkzellen müssen sich in Randgebieten überlagern. Der Client kann daraufhin bei einem Wechsel in eine neue Funkzelle dort bereits eine neue Verbindung aufbauen, bevor er in der alten Zelle die Verbindung löst.

Hier kommt das 802.11 f (IAPP[22]) zu Einsatz im zweiten Fall kommt MIP[23] zum Einsatz. Hier müssen sich die beiden APs nicht im selben Subnetz befinden. Dem Client wird wie bei einem postalischen Nachsendeantrag von sogenannten Mobility Agents das IP-Paket aus dem ursprünglichen Subnetz (Heimatnetz) in sein aktuelles Subnetz (Fremdnetz) nachgesendet. Hierzu gibt es je einen:

- Heimatagent (HA, Home Agent) und
- Fremdagent (FA, Foreign Agent).

Wobei sich der HA um die Zustellung/Nachsendung der IP-Pakete in das neue Fremdnetz kümmert. Anhand einer sogenannten CoA[24], die ihm vom FA mitgeteilt wird und die als Nachsendeadresse für den Client dient, kann der HA die Daten an den neuen FA senden. Der FA kennt den Client und stellt die Pakete sowie mögliche Rückantworten zu.

22 IAPP: **In**ter **A**ccess **P**oint **P**rotocol
23 MIP: **M**obile **IP**
24 CoA: **C**are-**o**f-**A**ddress