4 Wireless LAN IEEE 802.11

Mitte der neunziger Jahre fristete eine neue Technologie namens Wireless LAN noch ein Schattendasein. Dies änderte sich sehr schnell Anfang dieses Jahrzehnts, nachdem die benötigte Hardware deutlich billiger wurde. Wireless LAN wurde so schnell das optimale Medium, um Computer drahtlos untereinander und mit dem Internet zu verbinden. Kapitel 4 dieses Buches beschäftigt sich ausführlich mit diesem System, das vom IEEE (Institute of Electrical and Electronics Engineers) unter der Bezeichnung 802.11 standardisiert wurde. Der erste Teil des Kapitels beschreibt zunächst die technischen Grundlagen dieses Systems. Neben der Heimvernetzung und Hotspots kommen auch Themen wie Roaming und Wireless Bridging nicht zu kurz. Mit der Verbreitung dieses Systems wurde schnell entdeckt, dass Datensicherheit und Verschlüsselung einige gravierende Schwachstellen aufwiesen. Deshalb wird in diesem Kapitel auch gezeigt, wie diese beseitigt wurden und wie heute ein Wireless LAN sicher betrieben werden kann. Wireless LAN und UMTS werden oft miteinander verglichen, denn sie haben viele Gemeinsamkeiten. Da es aber auch viele Unterschiede gibt, stellt das Kapitel am Ende beide Systeme gegenüber und zeigt, für welche Anwendungen welches System am besten geeignet ist.

4.1 Wireless LAN Überblick

Wireless LAN (Local Area Network) trägt seinen Namen zu Recht, denn es basiert im Wesentlichen auf LAN Standards, die ursprünglich vom IEEE für die drahtgebundene Vernetzung von Computern in den 802.X Standards beschrieben sind. Diese LAN Standards werden im täglichen Sprachgebrauch auch oft als „Ethernet“ bezeichnet. Die drahtlose Variante, also das Wireless LAN (WLAN), wurde in den 802.11 Standards spezifiziert. Wie in Abbildung 4.1 zu sehen ist, dient WLAN heute hauptsächlich dazu, auf Schicht 3 des OSI Modells IP Pakete zu transportieren. Schicht 2, der Data Link Layer, wurde mit wenigen Änderungen aus der drahtgebundenen „Ethernetwelt“ übernommen. Um der drahtlosen Natur des Netzwerkes Rechnung zu tragen, wurden zusätzlich für Layer 2 einige Management Operationen definiert,

die in Kapitel 4.2 beschrieben werden. Lediglich Schicht 1, der Physical Layer, wurde komplett neu entwickelt, da bei WLAN kein Kabel, sondern Funkwellen für die Übertragung der Datenpakete verwendet werden.

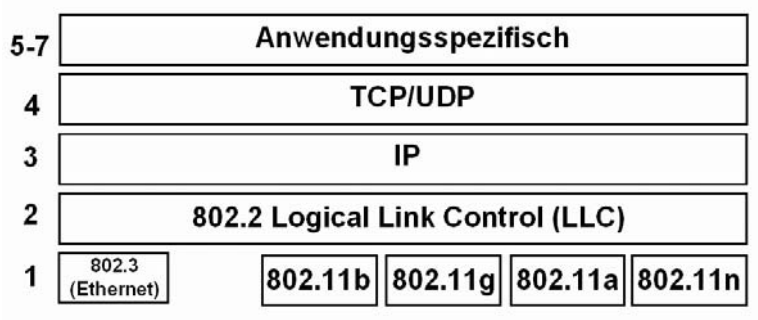

Abb. 4.1: WLAN Protokollstack

4.2 Geschwindigkeiten und Standards

Seit Bestehen der 802.11 Standards gab es zahlreiche Weiterentwicklungen bei der Funkübertragung. Aus diesem Grund gibt es mehrere Physical Layer, die in den Spezifikationen abgekürzt PHY genannt werden.

Standard	**Frequenzband (landesabhängig)**	**Geschwindigkeit**
802.11b	2.4 GHz, (2.401-2.483 GHz)	1-11 MBit/s
802.11g	2.4 GHz (2.401-2.483 GHz)	6-54 MBit/s
802.11a	5 GHz (5.150-5.350 GHz und 5.470-5725 GHz)	6-54 Mbit/s
802.11n	2.4 GHz (wie oben) 5 GHz (wie oben)	6-600 MBit/s

802.11b

Der große Durchbruch für WLAN erfolgte mit dem 802.11b Standard, mit dem Datenraten von 1-11 MBit/s möglich sind. Die Übertragungsrate richtet sich dabei hauptsächlich nach der Entfernung zwischen Sender und Empfänger, sowie nach der Anzahl der Hindernisse wie Wände oder Decken. 11 MBit/s sind dabei in Gebäuden nur über kurze Entfernungen in Größenordnungen von 10-20 Metern möglich. Die Redundanz in den Datenpaketen wird je nach Übertragungsqualität automatisch angepasst und reduziert so die Geschwindigkeit bei sehr schlechten Bedingungen auf bis zu 1 MBit/s. Die von vielen Herstellern angepriesene Reichweite von bis zu 300m wird bestenfalls bei 1 MBit/s nur im Freien erreicht, wenn keine Hindernisse zwischen Sender und Empfänger die Übertragung stören. Der 802.11b Standard sendet im 2.4 GHz ISM (Industrial, Scientific and Medical) Band, der in den meisten Ländern lizenzfrei verwendet werden darf. Wichtigste Bedingung für die Verwendung dieses Bandes ist die Beschränkung der maximalen Sendeleistung auf 100 mW. Das ISM Band ist ein öffentliches Frequenzband, neben WLAN senden hier auch noch andere Funksysteme wie z.B. Bluetooth.

802.11g

Im 802.11g Standard wurde ein im Vergleich zum 802.11b Standard weit komplexerer PHY spezifiziert, der Datenraten je nach Qualität des Übertragungsmediums von bis zu 54 MBit/s erlaubt. Auch dieser Standard sendet auf dem 2.4 GHz ISM Band und wurde so gestaltet, dass die Verfahren rückwärtskompatibel zu 802.11b sind. Somit ist sichergestellt, dass 802.11b Geräte auch mit 802.11g Geräten kommunizieren können. Mehr dazu in Kapitel 4.6 über die einzelnen PHYs.

802.11a

Zusätzlich zum 2.4 GHz ISM Band wurde auch im 5 GHz Frequenzbereich ein Band für WLAN freigegeben, für das zunächst der 802.11a Standard spezifiziert wurde. Wie beim 802.11g Standard sind auch hier Datenraten von 6-54 Mbit/s möglich. 802.11a Endgeräte wurden jedoch aufgrund der nötigen Rückwärtskompatibilität zu 802.11b/g nie besonders erfolgreich, da die Unterstützung von zwei Frequenzbereichen zusätzliche Kosten verursachte. In der Praxis standen dem bisher jedoch keine nennenswerten Vorteile gegenüber.

802.11n

Aufgrund der steigenden Datenraten bei lokalen Netzwerken und auch bei Internetzugängen per Kabel oder ADSL wurde bald klar, dass auch bei Wireless LANs weitere Geschwindigkeitssteigerungen notwendig waren. Nach einigen Jahren Standardisierungsarbeit einigten sich schließlich die beteiligten Firmen auf ein gemeinsames neues Verfahren, dass im IEEE 802.11n Stan-

dard definiert ist. Durch doppelte Kanalbreiten und zahlreichen weiteren Neuerungen, die im Laufe dieses Kapitels näher beschrieben werden, erreicht dieser Standard theoretische Spitzengeschwindigkeiten von bis zu 600 Mbit/s. Außerdem unterstützt der Standard sowohl das 2.4 GHz Band als auch das 5 GHz Band. Dies wurde notwendig, da das 2.4 GHz Band bereits sehr stark genutzt wird und in vielen Fällen nur im 5 GHz Band freie Kanäle zur Verfügung stehen. In vielen Fällen wird es in Zukunft nur dort möglich sein, hohe Datenraten zu erzielen, die für Anwendungen wie Video Streaming notwendig sind.

Proprietäre Systeme

Neben diesen Geschwindigkeitsstandards bieten manche Hersteller auch eigene, proprietäre oder in 802.11g als optional deklarierte Zusätze an, um so die Übertragungsgeschwindigkeit zu steigern. Der Geschwindigkeitsvorteil kann aber nur dann genutzt werden, wenn Sender und Empfänger vom gleichen Hersteller sind. Viele dieser proprietären Erweiterungen sind während der Standardisierung in 802.11n eingeflossen um in Zukunft ein Wildwuchs vermieden werden kann.

Weitere 802.11 Standards

Weitere 802.11 Standards, die in der nachfolgenden Tabelle aufgelistet sind, spezifizieren diverse zusätzliche optionale Wireless LAN Funktionalitäten:

Standard	Beschreibung
802.11e	Wichtigste neue Funktionalität des Standards sind Methoden, um für eine Übertragung eine bestimmte Quality of Service (QoS) zu gewährleisten. Damit ist es möglich, Bandbreite und schnellen Medienzugriff für Echtzeitanwendungen wie z.B. Voice over IP (VoIP) auch in stark ausgelasteten Netzen zu gewährleisten. Außerdem spezifiziert der Standard das Direct Link Protocol (DLP), mit dem zwei WLAN Endgeräte auch direkt unter Umgehung des Access Points Daten austauschen können. Dies steigert die Übertragungsgeschwindigkeit zwischen zwei drahtlosen Endgeräten wesentlich.
802.11f	Spezifikation für den Datenaustausch zwischen Access Points. Mehr dazu in Kapitel 4.3.1 über Extended Service Sets (ESS).

802.11h	Ergänzung für Standards im 5 GHz Bereich für Leistungsregelung und dynamische Frequenzwahl. In Europa sind ab einer gewissen Sendeleistung nur 802.11a Systeme zugelassen, die sich an diese Erweiterungen halten.
802.11i	Standardisiert erweiterte Authentifizierungs- und Verschlüsselungsalgorithmen für WLAN. Wichtiger Bestandteil von 802.11i ist 802.1x. Mehr hierzu in Kapitel 4.7 zum Thema WLAN Sicherheit.

4.3 WLAN Konfigurationen: Von Ad-hoc bis Wireless Bridging

Alle Stationen, die auf dem gleichen Übertragungskanal Daten austauschen, werden im 802.11 Standard unter dem Begriff Basic Service Set (BSS) zusammengefasst. Die Definition des BSS umfasst auch den geographischen Bereich, in dem sich die Teilnehmer des BSS aufhalten können. Ein BSS kann in folgenden unterschiedlichen Modi betrieben werden:

4.3.1 Ad-hoc, BSS, ESS und Wireless Bridging

Ad-hoc Mode (IBSS)

Im Ad-hoc Mode, auch Independent BSS (IBSS) genannt, kommunizieren zwei oder mehr WLAN Endgeräte direkt miteinander. Jede Station ist gleichberechtigt und Daten werden direkt von Endgerät zu Endgerät gesendet. Der Ad-hoc Mode entspricht also im Wesentlichen einem drahtgebundenen Ethernet, in dem ebenfalls alle Stationen gleichberechtigt sind und Datenpakete ebenfalls direkt zwischen zwei Teilnehmern ausgetauscht werden. Die gesendeten Daten werden zwar auch von allen anderen Teilnehmern des Netzwerks empfangen, von diesen aber ignoriert, weil die Zieladresse des Pakets nicht mit ihrer eigenen Adresse übereinstimmt. Alle Teilnehmer des Ad-hoc Netzes müssen sich zu Beginn auf die Werte für einige Parameter einigen und diese dann in ihren Endgeräten entsprechend konfigurieren. Wichtigster Parameter ist die Service Set ID (SSID), die als Namen für das Netzwerk dient. Weiterhin müssen alle Teilnehmer des Netzwerkes die gleiche Kanalnummer einstellen und auch der Verschlüsselungskey muss bei allen Teilnehmern gleich konfiguriert werden. Zwar kann das Ad-hoc Netzwerk auch ohne Verschlüsselung betrieben werden, aus Sicherheitsgründen ist hiervon jedoch abzuraten. Schließlich müssen sich die Teilnehmer noch auf die zu verwendenden IP Adressen einigen und auch diese

entsprechend in ihren Endgeräten eintragen. Die komplizierte Konfiguration ist einer der Gründe, warum der Ad-hoc Modus in der Praxis selten verwendet wird.

Infrastructure BSS

Eine der Hauptanwendungen eines WLAN Netzwerkes ist der Zugang zu einem Firmen- oder Heimnetzwerk, sowie dem Internet. Für diesen Zweck eignet sich der Infrastructure BSS Mode des WLAN Standards am besten. Im Unterschied zum Ad-hoc Mode gibt es hier einen so genannten Access Point, der eine zentrale Rolle übernimmt.

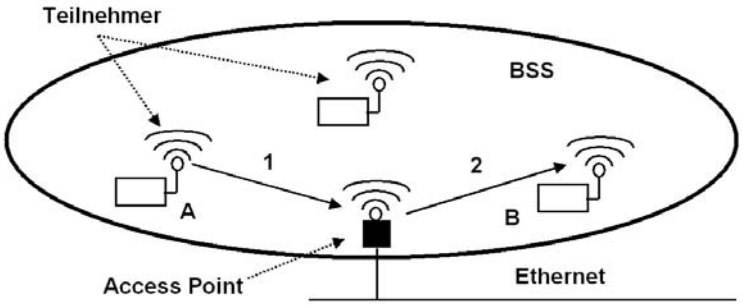

Abb. 4.2: Infrastructure BSS

Der Access Point bildet wie in Abbildung 4.2 gezeigt, den Übergang zwischen dem drahtlosen und drahtgebundenen Netzwerk für alle Endgeräte im BSS. Außerdem kommunizieren Endgeräte in einem Infrastructure BSS nicht direkt miteinander, sondern immer über den Access Point. Möchte Endgerät A an Endgerät B ein Datenpaket schicken, sendet es dies zunächst an den Access Point. Der Access Point analysiert die Zieladresse und stellt das Paket danach an Teilnehmer B zu. Auf diese Weise ist es möglich, Endgeräte im drahtlosen und im drahtgebundenen Netzwerk zu erreichen, ohne dass Teilnehmer wissen müssen, um welche Sorte Endgerät es sich handelt. Der zweite Vorteil dieses Verfahrens liegt darin, dass auch drahtlose Endgeräte über den Access Point miteinander kommunizieren können, die sich für eine direkte Kommunikation zu weit auseinander befinden. Dies kann z.B. der Fall sein, wenn sich wie in Abbildung 4.2 gezeigt, der Access Point zwischen Endgerät A und B befindet. Die Sendeleistung jedes Endgeräts reicht zwar aus, den Access Point zu erreichen, nicht jedoch das jeweils andere Gerät. Großer Nachteil dieses Verfahrens ist jedoch, das bei Kommunikation zwischen zwei drahtlosen Teilnehmern das Datenpaket zweimal über die Luftschnittstelle übertragen wird und somit die maximale Bandbreite des BSS halbiert wird. Aus diesem Grund wurde als Teil

des 802.11e Standards das optionale Direct Link Protocol (DLP) eingeführt, das eine direkte Kommunikation zwischen zwei Endgeräten erlaubt. In der Praxis implementieren jedoch heute erst wenige Endgeräte diese Erweiterung. Weitere Informationen hierzu in Kapitel 4.8.

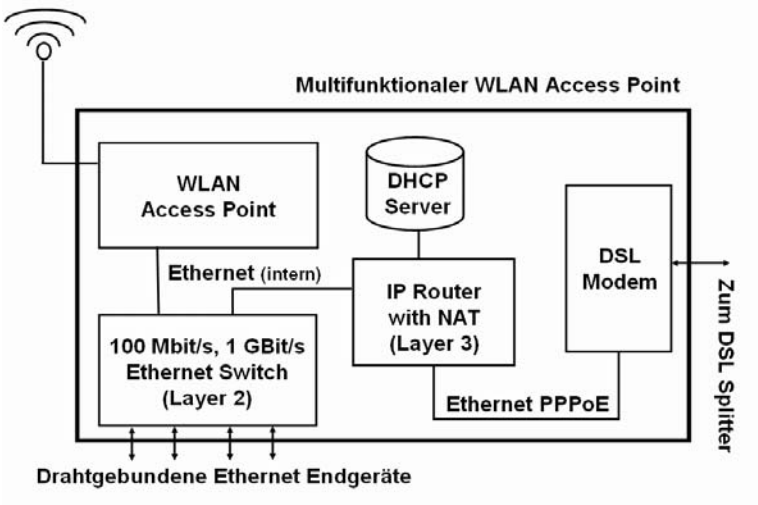

Abb. 4.3: Access Point, IP Router und DSL Modem in einem Gerät

Oft ist ein WLAN Access Point mit weiteren Funktionen ausgestattet:

- 100 MBit/s oder 1 GBit/s Anschlüsse für den Anschluss drahtgebundener Ethernet Endgeräte mit Layer 2 Switching Funktionalität.
- Oft dient ein WLAN Access Point im Heimbereich auch gleichzeitig als IP Router zum Internet und kann per Ethernet mit einem DSL oder Kabelmodem verbunden werden.
- Um Endgeräte automatisch für das Netzwerk zu konfigurieren, ist üblicherweise auch ein DHCP (Dynamic Host Configuration Protocol) Server in einem Access Point integriert. Dieser übergibt allen drahtlosen und drahtgebundenen Endgeräten die benötigen Netzwerkeinstellungen wie individuelle IP Adressen, sowie die Adresse des DNS Servers für die Namensauflösung und die IP Adresse des Internet Gateways.

- Schließlich kann auch das Kabelmodem oder das DSL Modem im Wireless LAN Access Point integriert sein. Dies ist sehr praktisch, da weniger Geräte verkabelt werden müssen und nur noch ein Netzteil für die Stromversorgung benötigt wird. Ein solcher voll integrierter Access Point ist in Abbildung 4.3 gezeigt.

Extended Service Set (ESS)

Da ein WLAN Access Point (AP) aufgrund seiner geringen Sendeleistung nur eine begrenzte Reichweite hat, sind in manchen Fällen mehrere APs notwenig, um ein bestimmtes Gebiet zu versorgen. Ändert ein mobiler Teilnehmer seinen Aufenthaltsort und kann dadurch von einem anderen AP besser versorgt werden, meldet sich die Netzwerkkarte automatisch beim neuen AP an. Eine solche Anordnung wird Extended Service Set (ESS) genannt und ist in Abbildung 4.4 dargestellt. Meldet sich ein Endgerät an einem anderen Access Point des ESS an, tauschen der neue und bisherige AP über die Ethernet Verbindung, die in den WLAN Standards auch Distribution System genannt wird, Teilnehmerinformationen aus. Zukünftig werden dann Pakete, die über das Distribution System für den Teilnehmer eingehen, über den neuen AP an den Teilnehmer zugestellt, der alte Access Point ignoriert fortan diese Pakete. Für höhere Schichten des Protokollstacks ist der Wechsel des Access Points in einem ESS nicht sichtbar, die IP Adresse kann deshalb beibehalten werden.

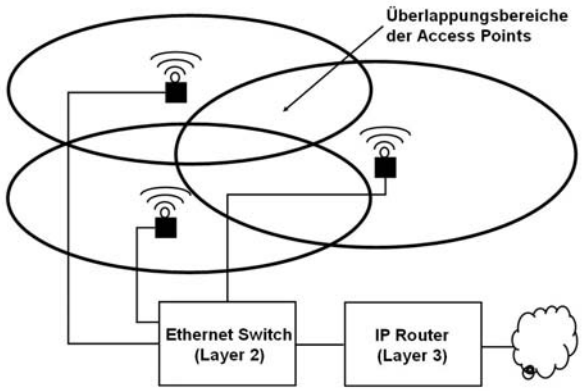

Abb. 4.4: Extended Service Set (ESS) mit 3 Access Points

Folgende Bedingungen müssen erfüllt sein, um den reibungslosen Übergang eines Teilnehmers zu einem anderen Access Point (AP) in einem ESS zu gewährleisten:

- Alle APs eines ESS müssen sich im gleichen IP Subnetz befinden, es dürfen also keine IP Router zwischen den APs liegen. Ethernetswitches, die auf OSI Layer 2 arbeiten, sind jedoch erlaubt. Dies limitiert das Ausbreitungsgebiet eines ESS beträchtlich, da IP Subnetze oft nicht sehr groß sind (z.B. ein Gebäude oder ein Stockwerk).
- Alle APs müssen die gleiche BSS Service ID, oft auch mit „SSID“ abgekürzt, besitzen. Mehr zur SSID in Kapitel 4.3.2.
- APs müssen auf unterschiedlichen Frequenzen senden und sich bei der Frequenzwahl an ein Muster halten, das in Abbildung 4.5 gezeigt wird.
- Viele APs verwenden für den Austausch der Teilnehmerinformationen bei einem AP Wechsel ein proprietäres Protokoll. Aus diesem Grund sollten alle APs eines ESS vom gleichen Hersteller stammen. Um ein ESS mit APs unterschiedlicher Hersteller zu ermöglichen, wurde vom IEEE Anfang 2003 der Standard 802.11f (Recommended Practice for Multi-Vendor Access Point Interoperability) verabschiedet, der aber nicht verpflichtend für Hersteller ist.
- Zwischen den Abdeckungsbereichen der einzelnen Access Points muss es eine Überlappung geben, damit Endgeräte auch in den Randgebieten die Netzabdeckung nicht verlieren. Da die APs mit unterschiedlichen Frequenzen senden, stellt diese Überlappung aber kein Problem dar.

Wireless Bridging

Eine weitere WLAN Variante ist das Wireless Bridging. In dieser Betriebsart wird das drahtgebundene Ethernet Distribution System zwischen zwei oder mehr APs eines ESS durch eine Funkstrecke ersetzt.

4.3.2 SSID und Frequenzwahl

Bei Inbetriebnahme eines Access Points gibt es zwei grundsätzliche Parameter, die individuell vergeben werden müssen:

SSID

Der erste Parameter ist die Basic Service Set ID, kurz SSID genannt. Die SSID wird vom Access Point über Beacon Frames, die in Kapitel 4.4 besprochen werden, in regelmäßigen Abständen über die Luftschnittstelle bekannt gegeben (Broadcast). Das Wort „Frame“ wird bei WLAN synonym zu „Paket“ verwendet. Die

SSID identifiziert einen Access Point eindeutig und ermöglicht es, mehrere unterschiedliche Access Points, die Zugriff auf unterschiedliche Netzwerke gewähren, am gleichen Ort zu betrieben. Eine Konfiguration von unabhängigen APs sollte nicht mit einem ESS verwechselt werden, das für alle APs die gleiche SSID verwendet. Üblicherweise wird für die SSID ein Textstring gewählt, da dieser bei der Konfiguration der Endgeräte später in einer Dialogbox dem User zur Auswahl des Access Points angeboten wird. Oft wird die SSID in Konfigurationsprogrammen auch als „Netzwerkname“ (Network Name) bezeichnet.

Kanäle im 2.4 GHz Bereich

Zweiter wichtiger Parameter, der bei Vorhandensein mehrerer APs sorgfältig gewählt werden sollte, ist die Sendefrequenz. Das ISM Band im 2.4 GHz Bereich von 2.410 MHz bis 2.483 MHz ist je nach Land in bis zu 13 Kanäle von jeweils 5 MHz Bandbreite unterteilt. Da ein WLAN Kanal eine Bandbreite von 25 MHz benötigt, sollten unterschiedliche WLAN Netze, die sich überlappen oder die gleiche Fläche abdecken, mindestens 5 ISM Kanäle Abstand zueinander halten. Wie in Abb. 4.5 dargestellt, können auf diese Weise 3 unabhängige BSS oder ein ESS mit sich überlappenden Grenzen von 3 Access Points betrieben werden. Bei 3 unabhängigen BSS ist diese Überlappung nicht unbedingt gewünscht, lässt sich in der Praxis jedoch oft nicht vermeiden. Bei 3 Access Points, die zusammen ein ESS bilden, ist diese Überlappung jedoch notwendig, um einen nahtlosen Wechsel von einem AP zum anderen zu ermöglichen. Um mindestens 5 Kanäle Abstand einzuhalten, müssen in den Access Points jeweils Kanal 1, 6 und 11 eingestellt werden.

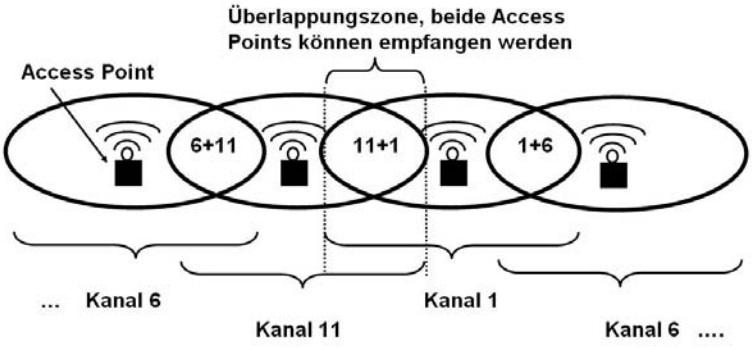

Abb. 4.5: Überlappende Abdeckung von Access Points

Kanäle 12 und 13 nur in Europa

Da die Kanäle 12 und 13 nur in Europa zugelassen sind, wird bei der Installation der meisten WLAN-Karten das Land abgefragt. Manche Produkte sparen sich jedoch diese Abfrage und blockieren Kanal 12 und 13 permanent. Steht deshalb beim Aufbau eines Access Points nicht fest, mit welchen Netzwerkkarten später auf das Netzwerk zugegriffen wird, sollten Kanal 12 und 13 nicht verwendet werden.

Kanäle im 5 GHz Bereich

802.11a und 802.11n Systeme senden im 5 GHz Bereich in Europa von 5.150 – 5.350 GHz und von 5.470 – 5.725 GHz. Zusammen sind dies 455 MHz, in denen 18 unabhängige WLAN Netzwerke Platz finden. Gegenüber den 3 unabhängigen Netzen im 2.4 GHz Band ist dies ein enormer Fortschritt. Da für diesen Frequenzbereich eine automatische Frequenzwahl vorgeschrieben ist, suchen sich Access Points automatisch einen freien Kanal.

Client Konfiguration von SSID und Frequenz

Auf Endgeräteseite ist die Grundkonfiguration des Wireless LANs für ein BSS und ESS einfacher. Das Endgerät sucht bei der Konfiguration alle Frequenzen nach vorhandenen Access Points ab und zeigt dann die gefundenen SSIDs an. Der Benutzer hat daraufhin die Möglichkeit, eine SSID auszuwählen. Dies ist in Abbildung 4.6 gezeigt. Der Sendekanal hingegen muss nicht ausgewählt werden, da das Endgerät beim Einschalten immer alle Kanäle nach einem Access Point mit der ausgewählten SSID durchsucht. Werden mehrere Access Points auf unterschiedlichen Frequenzen mit der gleichen SSID gefunden, handelt es sich um ein ESS. Das Endgerät wählt dann den Kanal, auf dem die Beacon Frames (vgl. nächster Abschnitt) am besten empfangen werden.

Die meisten WLAN Konfigurationsprogramme können heute unterschiedliche Konfigurationen zu speichern. Findet beim Systemstart die Software dann eine bekannte SSID, wird automatisch das dazugehörige Profil geladen. Somit ist es möglich, unterschiedliche Konfiguration für zuhause, für den Arbeitsplatz und für öffentliche Hotspots einmal anzulegen, die dann bei Bedarf automatisch aktiviert werden.

Sicherheit

Neben SSID und Sendekanal ist die Konfiguration der Verschlüsselung für Heim- und Firmennetzwerke ebenfalls sehr wichtig. Viele Produkte haben diese noch immer standardmäßig bei Auslieferung deaktiviert. Dies stellt ein großes Sicherheitsrisiko dar, da Funkwellen nicht an der Wohnungs- oder Bürotür halt machen. Mehr zu diesem wichtigen Thema in Kapitel 4.7.

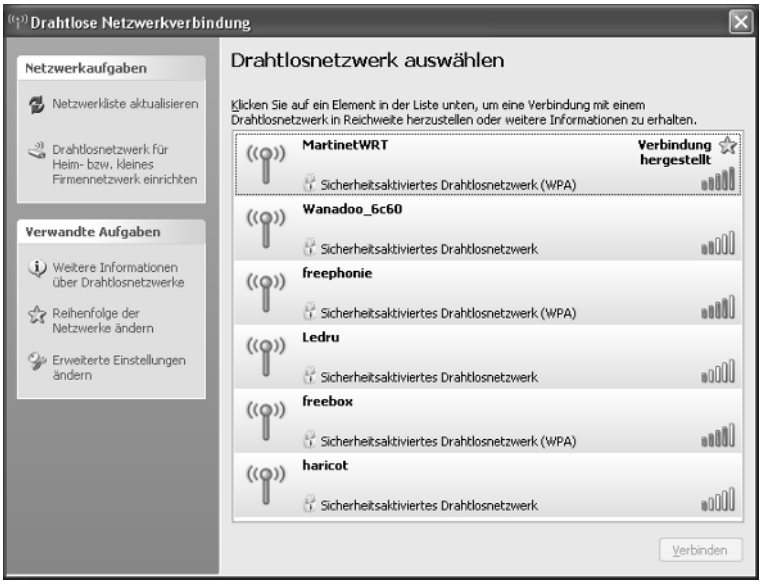

Abb. 4.6: Endgerätekonfiguration für ein BSS oder ESS.

4.4 Management Operationen

Im drahtgebundenen Ethernet genügt es, ein Endgerät mit einem Kabel am nächsten Hub oder Switch anzuschließen, um dem Endgerät Zugriff auf das Netzwerk zu gewähren. Ein solches physikalisches „Einstecken“ ist bei einem WLAN Endgerät nicht möglich. Zusätzlich verfügt ein WLAN Endgerät über Funktionen wie automatisches Roaming zu anderen Access Points eines ESS, oder die Verschlüsselung der Datenpakete auf Layer 2, die mit dem Netzwerk koordiniert werden müssen. Aus diesem Grund definiert der 802.11 Standard eine Reihe von Management Operationen und Nachrichten auf Layer 2, sowie zusätzliche Informationen im MAC Header von Datenpaketen, die im drahtgebundenen Ethernet nicht notwendig sind.

Scanning und Beacon Frames

In einem BSS nimmt der Access Point (AP) eine zentrale Rolle ein und stellt gleichzeitig den Übergang zum drahtgebundenen Ethernet her. Alle Datenpakete im WLAN werden immer an den AP geschickt, der dann die Weiterleitung an mobile und drahtgebundene Endgeräte übernimmt. Damit ein WLAN Endgerät beim Einschalten einen aktiven AP erkennen kann, sendet dieser in regelmäßigen Abständen (typisch sind 100 ms) Beacon Frames aus. Wie in Abbildung 4.7 auszugsweise gezeigt, enthalten Beacon Frames neben der SSID des Access Points noch eine Menge

weiterer Informationen, die einem Endgerät Aufschluss über Funktionen und Optionen des Access Points liefern. Jedes Bit des 2 Byte langen Capability Information Element (Capability IE) gibt Auskunft über eine bestimmte Eigenschaft. So ist zum Beispiel in Abbildung 4.7 zu sehen, dass der Access Point keine Verschlüsselung aktiviert hat (Privacy Disabled). Für umfangreichere Informationen wie z.B. die unterstützten Übertragungsraten, die mehr als ein Bit benötigen, werden eigene Information Elements (IE) im Beacon Frame verwendet. Jedes Information Element hat seine eigene ID wie z.B. 0 für das IE, das die SSID enthält, oder 1 für das IE „Supported (Data-) Rates“. Da IEs unter Umständen variable Längen haben (z.B. das SSID IE), folgt auf die ID eine Längenangabe. Somit ist es für das Endgerät möglich, optionale und evtl. unbekannte IEs, die Information für neuere Geräte enthalten, bei der Dekodierung der Nachricht zu überspringen.

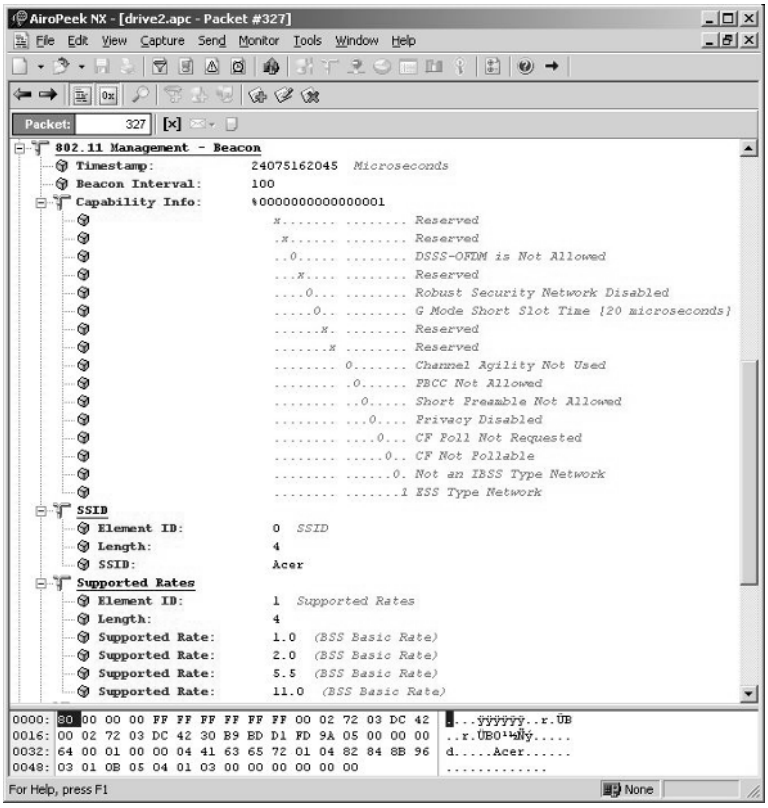

Abb. 4.7: Ausschnitt aus einem Beacon Frame

Ein Endgerät hat die Möglichkeit, bei der Netzsuche entweder nur passiv alle Kanäle nach Beacon Frames zu durchsuchen, oder aktiv mit Probe Request Frames einen Access Point zu suchen. In der Praxis verwenden die meisten Endgeräte beide Methoden. Empfängt ein Access Point einen Probe Request Frame, antwortet er mit einem Probe Response Frame, der die gleichen Informationen wie ein Beacon Frame enthält.

Nachdem ein Endgerät einen geeigneten Access Point gefunden hat, folgt im nächsten Schritt die Authentifizierung. Der Standard definiert dazu zwei Verfahren:

Open System Authentication

Die Open System Authentication trägt ihren Namen zu Unrecht, denn bei diesem Verfahren findet keine Authentifizierung statt. Das Endgerät sendet hier einen Authentication Frame mit einer Authentifizierungsanforderung an den Access Point (Authentication Request), der als Authentifizierungsalgorithmus Open System fordert. Weitere Authentifizierungsinformationen sind nicht nötig. Lässt der Access Point eine solche „Authentifizierung" zu, antwortet er mit einem positiven Statuscode und das Endgerät ist „authentifiziert".

Shared Key Authentication

Für die zweite Authentifizierungsart, der Shared Key Authentication, wird ein gemeinsamer Schlüssel benötigt, der dem Access Point und allen Endgeräten bekannt sein muss (shared). Bei einer solchen Authentifizierungsanforderung sendet der Access Point einen zufällig gewählten Text an das Endgerät zurück, der dann mit dem bekannten Key verschlüsselt wird (Challenge). Der so verschlüsselte Text wird dem Access Point zurückgeschickt (Response) und dort mit dem eigenen verschlüsselten Text verglichen. Stimmen beide Resultate überein, ist der Teilnehmer erfolgreich authentifiziert. Die Verwendung eines Schlüssels für alle Teilnehmer birgt jedoch Tücken und Sicherheitsrisiken. Weitere Informationen hierzu in Kapitel 4.7.

Association

Nach erfolgreicher Authentifizierung sendet ein Endgerät im nächsten Schritt einen Association Request (Zuordnungsanforderung) an den Access Point. Der Access Point antwortet daraufhin mit einer positiven Association Response Nachricht, in der die wichtigsten Systeminformationen wie das Capability Information Elemente noch einmal wiederholt werden. Außerdem wird dem Endgerät eine Association ID übergeben, die später für den Power Save Mode benötigt wird. Eine Trennung zwischen Authentication und Association wurde eingeführt, um einem Endgerät

den schnellen Wechsel zwischen Access Points des gleichen ESS zu ermöglichen.

Abbildung 4.8 zeigt die zwei für die Verbindungsaufnahme mit dem Netzwerk nötigen Prozeduren Authentication und Association. Acknowledgement Frames, die in Kapitel 4.5 eingeführt werden, wurden zur besseren Übersicht weggelassen.

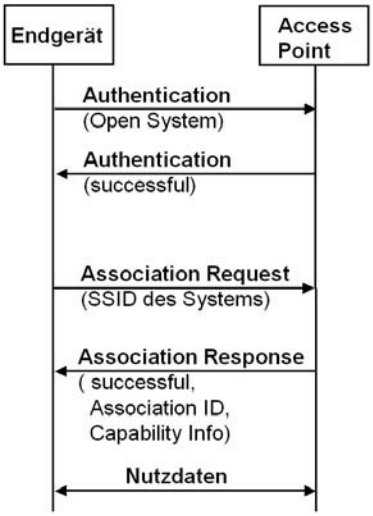

Abb. 4.8: Authentication und Association (ohne Acknowledgment Frames)

WEP Verschlüsselung der Datenpakete

Nach erfolgreicher Association des Endgeräts mit einem Access Point können bei offenen oder mit WEP geschützten Netzwerken sofort Nutzdatenpakete übertragen werden. Wurde im Access Point die WEP (Wired Equivalent Privacy) Datenverschlüsselung aktiviert, wird dies über das Capability Information Element bekannt gegeben. Alle Datenpakete werden dann vom Access Point und auch vom Endgerät vor der Übertragung mit dem gemeinsamen geheimen Schlüssel chiffriert. Da der ursprüngliche WEP Standard einige Sicherheitslücken aufweist, wurden mittlerweile weitere Verfahren wie WPA und WPA2 spezifiziert. Diese erfordern nach der Association Prozedur noch eine weitere Management Prozedur. Die Management Prozedur wird in Kapitel 4.7 näher beschrieben.

Verschlüsselung ohne Authentifizierung

Authentifizierung und Verschlüsselung sind unabhängig voneinander. So ist es heute bei den meisten Endgeräten und Access Points üblich, eine Open System „Authentication“ durchzuführen

und danach mit dem gemeinsamen geheimen Schlüssel den Datenverkehr per WEP, WPA oder WPA2 zu verschlüsseln. Endgeräte, die den geheimen Schlüssel nicht kennen oder einen falschen verwenden, können sich so zwar erfolgreich am Netzwerk anmelden, danach aber keine Daten korrekt senden oder empfangen. Manche Access Points bieten die Option, die Shared Authentication explizit einzuschalten. Dies bringt aber in der Praxis keine erhöhte Sicherheit. Darüber hinaus wird durch das Aktivieren der Shared Authentication die Konfiguration der Endgeräte erschwert, da neben der WEP Verschlüsselung noch zusätzlich manuell die Authentifizierung aktiviert werden muss.

Reassociation und Roaming

Befindet sich ein Endgerät in einem ESS mit mehreren Access Points (vgl. Abb. 4.4), kann es jederzeit zu einem anderen Access Point mit besserem Empfang für den aktuellen Aufenthaltsort wechseln. Die dazugehörende Prozedur wird Reassociation genannt und ist in Abbildung 4.9 dargestellt. Um dies zu ermöglichen, scannt ein Endgerät in Sende- und Empfangspausen alle Frequenzkanäle und kann so die Beacon Frames aller in der Nähe befindlichen APs empfangen. Anhand der SSID erkennt das Endgerät, welche APs zum aktuellen ESS gehören. Um zu einem neuen Access Point zu wechseln, ändert das Endgerät die Sende- und Empfangsfrequenz und sendet auf der neuen Frequenz einen Reassociation Request Frame. Dieser entspricht im Wesentlichen einem Association Request Frame mit der Ausnahme, dass zusätzlich noch die ID des vorherigen Access Points übergeben wird. Der neue Access Point sucht daraufhin über das drahtgebundene Ethernet (Distribution System) mit der übergebenen ID den bisherigen Access Point des Teilnehmers und informiert diesen über den Wechsel. Der bisherige Access Point sendet dem neuen Access Point dann eventuell zwischengepufferte Datenpakete des Endgeräts und löscht dessen Hardwareadresse und Association ID dann aus seiner Teilnehmerliste. Zukünftig eingehende Datenpakete über das drahtgebundene Distribution System, die immer von allen APs eines ESS empfangen werden, werden fortan nur vom neuen AP zum Teilnehmer übertragen und vom bisherigen AP ignoriert. Abgeschlossen wird die Reassociation Prozedur durch Senden einer positiven Reassociation Response Nachricht an das Endgerät.

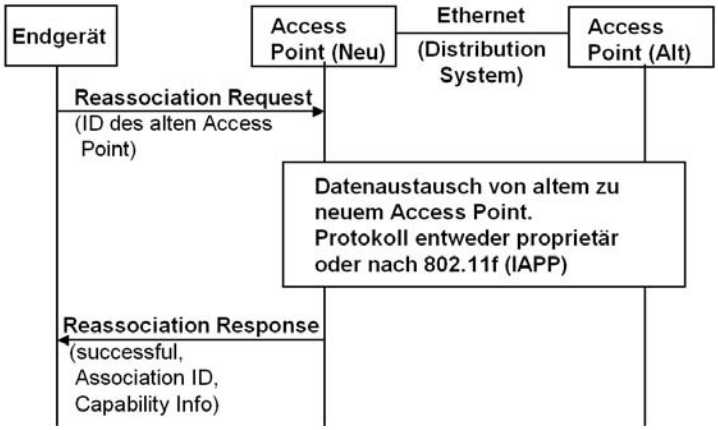

Abb. 4.9: Reassociation (ohne Acknowledgement Frames)

Nur die Signalisierung zwischen Endgerät und neuem Access Point der Reassociation Prozedur ist standardisiert. Für die drahtgebundene Kommunikation zwischen den Access Points gab es lange Zeit keinen Standard, so dass diese Prozedur von den Herstellern mit proprietären Protokollen gelöst wurde. Aus diesem Grund können in den meisten Fällen nur Access Points des gleichen Herstellers miteinander im gleichen ESS reibungslos eingesetzt werden. Mit Verabschiedung der 802.11f Empfehlung und des Inter Access Point Protocol (IAPP) könnte sich dies in Zukunft ändern.

Stromsparmodus (Power-Saving Mode)

Um die Laufzeit batteriebetriebener Geräte zu erhöhen, gibt es in den 802.11 Standards auch einen Stromsparmodus (Power-Saving Mode, PS). Dieser bremst die Datenübertragung in bestimmten Situationen etwas, reduziert aber die Leistungsaufnahme wesentlich.

Ist der Sendepuffer eines Endgeräts leer und wurden seit einiger Zeit auch keine Daten vom Access Point empfangen, kann ein Endgerät den PS Mode aktivieren. Dazu sendet das Endgerät einen leeren Frame an den Access Point, in dessen MAC-Header das PS Bit gesetzt ist. Der Access Point puffert danach alle für das Endgerät eingehenden Frames und das Endgerät kann somit die Stromzufuhr zu seinem Sender und Empfänger abschalten. Die Zeit zwischen letztem Datenpaket und dem Einschalten des PS Mode kann vom Endgerätehersteller selbst bestimmt werden. In der Praxis werden hier Werte z.B. von batteriebetriebenen Ge-

räten wie Mobiltelefonen mit Wifi Funktionalität von 0.5 Sekunden gewählt.

Möchte ein Endgerät wieder Daten senden, schaltet es seine Sende- und Empfangsstufe wieder ein und sendet einen leeren Frame mit deaktiviertem PS Bit. Danach können die neuen Frames mit Nutzdaten sofort gesendet werden.

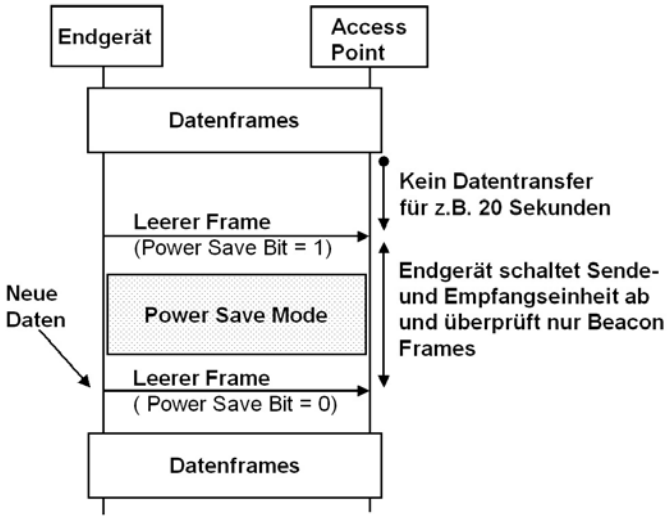

Abb. 4.10: Ein- und Ausschalten des Stromsparmodus (ohne Acknowledge Frames)

Traffic Indication Map (TIM)

Bei den meisten Anwendungen auf mobilen Endgeräten, wie z.B. dem webbrowsen, treffen nur in Ausnahmefällen nach dem Einschalten des PS Mode weitere Daten ein. Damit diese nicht verloren gehen, werden die Frames im Access Point zwischengespeichert. Aus diesem Grund muss das Endgerät auch im PS Modus periodisch seinen Empfänger aktivieren, um diese Pakete gegebenenfalls abholen zu können. Um ein Endgerät über gepufferte Frames zu informieren, gibt es in Beacon Frames das Traffic Indication Map (TIM) Information Element. Für jedes Endgerät ist in der TIM ein Bit vorhanden, das anzeigt, ob gepufferte Daten vorliegen. Das Endgerät identifiziert sein Bit in der TIM über seine Association ID (AID), die ihm bei der Association Prozedur übergeben wurde. Über die AID können bis zu 2007 Endgeräte angesprochen werden, die TIM ist also maximal 2007 Bits lang. Um die Beacon Frames möglichst klein zu halten, wird

mit Hilfe eines Offsets und einer Längenangabe nur ein Teil der TIM im Beacon Frame übertragen. Dies ist auch sinnvoll, da meist nur wenige Endgeräte an einem Access Point gleichzeitig betrieben werden.

Damit ein Endgerät nicht für jeden Beacon Frame seinen Empfänger einschalten muss, übergibt das Endgerät bei der Association Prozedur ein Listen Intervall an den Access Point, das vorgibt, in welchen Abständen die Beacon Frames überprüft werden. Akzeptiert der Access Point dieses Intervall, muss er eingehende Daten mindestens für diesen Zeitraum puffern. In der Praxis wird für das Listen Intervall zum Beispiel ein Wert von 3 verwendet. Dies bedeutet, dass das Endgerät nur jeden dritten Beacon Frame empfängt und somit seinen Empfänger für 300 ms abschalten kann. Ist das TIM Bit für das Endgerät nicht gesetzt, kann es nach Empfang des Beacon Frames seinen Empfänger wieder für die nächsten 300 Millisekunden deaktivieren.

Polling

Ist das TIM Bit für ein Endgerät gesetzt, aktiviert es neben seinem Empfänger auch seine Sendeeinheit und ruft die gepufferten Datenpakete über PS-Poll Frames beim Access Point ab. Als Antwort auf einen PS-Poll Frame erhält das Endgerät dann einen gepufferten Frame. Ist im MAC-Header des Frames das More Bit gesetzt, sind noch weitere Frames im Access Point gepuffert, die dann jeweils durch einen weiteren PS-Poll Frame angefordert werden müssen.

Gepufferte Broadcast und Multicast Frames nach DTIM

Auch Broadcast und Multicast Frames, die an mehrere oder alle Endgeräte gerichtet sind, müssen für Endgeräte im Power-Save Mode gepuffert werden. Statt jedoch diese Frames für jedes Endgerät einzeln zu puffern, gibt stattdessen das erste Bit in der TIM an (AID 0), ob Broadcastdaten gepuffert wurden. Diese Frames werden dann automatisch nach einem Beacon Frame gesendet, der statt einer TIM periodisch eine Delivery TIM (DTIM) enthält. In welchen Abständen statt der TIM eine DTIM gesendet wird, wird über eine Periode und einen Count Down Zähler in der TIM den Endgeräten mitgeteilt.

4.5 Die MAC Schicht

Das Medium Access Control Protocol (MAC, Layer 2) hat bei WLAN ähnlich wie im drahtgebundenen Ethernet unter anderem folgende Aufgaben:

- Es regelt den Zugriff der Endgeräte auf das Übertragungsmedium.

- Jedem Datenpaket wird ein MAC Header vorangestellt, der unter anderem die Adresse des Senders und Empfängers (MAC Adressen) enthält.

4.5.1 Zugriffssteuerung auf das Übertragungsmedium

Acknowledgement Frames

Aufgrund der höheren Fehleranfälligkeit der Datenübertragung über die Luftschnittstelle werden bei WLAN alle Datenpakete von der Gegenstelle nach korrektem Empfang durch ein Acknowledgement (ACK) Frame bestätigt. Dies ist ein großer Unterschied zum drahtgebundenen Ethernet, in dem Pakete nicht bestätigt werden. In allen bisherigen Abbildungen dieses Kapitels wurden diese Frames zur Übersichtlichkeit weggelassen. Abbildung 4.11 zeigt den Austausch von Frames zwischen Access Point und einem Endgerät zum ersten Mal mit ACK Frames. Jeder Frame, der entweder Nutzdaten oder Management Daten (Authentication, Association, etc.) enthält, muss von der Gegenseite durch ein ACK Frame bestätigt werden. Erst danach darf der nächste Nutzdatenframe vom gleichen oder einem anderen Endgerät gesendet werden. Bleibt der ACK Frame aus, muss das Datenpaket wiederholt werden.

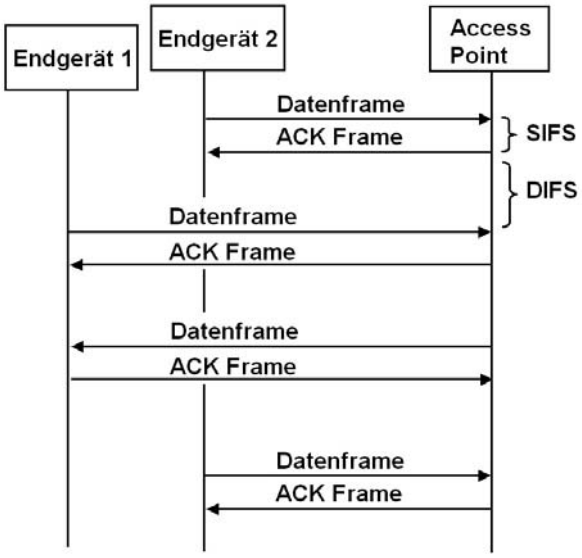

Abb. 4.11: Bestätigung (Acknowledgement) für jeden Frame

SIFS und DIFS

Durch einen sehr kurzen Sendeabstand zwischen Datenframe und ACK Frame, der Short Interframe Space (SIFS) genannt wird, ist sichergestellt, dass kein anderes Endgerät einen Frame dazwischen senden kann. Für normale Frames wird deshalb ein längerer Sendeabstand zum letzten Paket eingehalten, der DCF Interframe Space (Distributed Coordination Function Interframe Space, abgekürzt DIFS) genannt wird. Somit kann der ACK Frame auf jeden Fall gesendet werden, bevor eine andere Station den Kanal für einen normalen Frame verwenden darf. Mehr zum Thema DCF im nächsten Abschnitt.

Hidden Station RTS/CTS

Optional gibt es für ein Endgerät die Möglichkeit, die Luftschnittstelle für die Übertragung eines Frames im Vorhinein zu reservieren. Dies ist in Fällen sinnvoll, in denen Teilnehmer eines BSS zu weit voneinander entfernt sind, um die Datenpakete des jeweils anderen zu sehen. In diesen Fällen kann es passieren, dass beide Stationen gleichzeitig einen Frame an den Access Point senden und sich die Frames am Access Point gegenseitig stören. Dieses Szenario wird auch „Hidden Station“ Problem genannt. Um dieses Problem zu umgehen, sendet ein Endgerät wie in Abbildung 4.12 gezeigt vor dem Datenframe zuerst einen kurzen RTS (Ready to Send) Frame an den Access Point. Der Access Point antwortet daraufhin mit einem kurzen CTS (Clear to Send) Frame, und die Luftschnittstelle ist für den Teilnehmer reserviert. Während der RTS Frame vom zweiten Endgerät aufgrund des zu großen Abstands nicht gesehen wird, sieht es aber auf jeden Fall den CTS Frame, da dieser vom näheren Access Point gesendet wird. Damit das zweite Endgerät weis, wie lange es nicht senden darf, enthalten RTS und CTS Frames die Information, wie lange die Luftschnittstelle reserviert ist. Abgeschlossen wird die Übertragung des Frames wieder durch ein ACK Frame. Ob ein Endgerät ein Frame mit oder ohne RTS/CTS Sequenz überträgt, ist in den meisten Endgeräten in Abhängigkeit der Framegröße konfigurierbar. Dies ist sinnvoll, da der zusätzliche Zeitaufwand des RTS/CTS Mechanismus nur bei großen Paketen sinnvoll ist. Meist ist diese Option jedoch per Default deaktiviert und muss manuell konfiguriert werden.

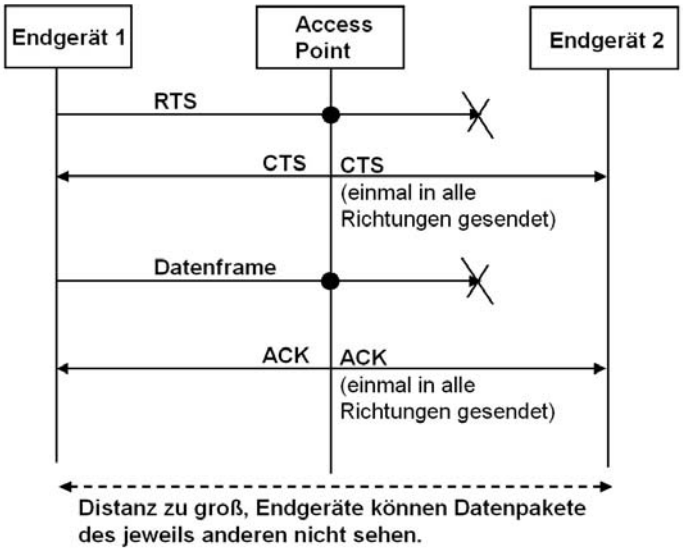

Abb. 4.12: Reservierung der Luftschnittstelle mit RTS/CTS

Distributed Coordination Function (DCF)

Bei Wireless LAN gibt es keine zentrale Steuerung, welcher Teilnehmer zu welchem Zeitpunkt auf das Übertragungsmedium (Luftschnittstelle) zugreifen darf. Jeder Teilnehmer trifft für sich die Entscheidung, wann ein anstehendes Datenpaket übertragen wird. Da aber möglichst keine Kollisionen mit anderen Teilnehmern auftreten sollen, koordinieren sich die Teilnehmer mit einem Verfahren, das Distributed Coordination Function (DCF) genannt wird. Dieser Ansatz unterscheidet sich grundlegend vom zentral gesteuerten Medienzugriff aller anderen Systeme, die in diesem Buch vorgestellt werden. Diese haben alle eine verwaltende Instanz, die genau vorgibt, welcher Teilnehmer zu welchem Zeitpunkt und für wie lange senden darf. Vorteil des DCF Verfahrens ist die einfache Implementierung in Endgeräten. Großer Nachteil des Verfahrens ist jedoch, dass keine Bandbreite reserviert oder garantiert werden kann. Besonders für Echtzeitanwendungen wie Sprach- oder Videotelefonie ist dies ein Problem, wenn das Medium von anderen Teilnehmern stark ausgelastet wird. Aus diesem Grund wurde im 802.11e Standard für Geräte und Anwendungen, die eine hohe Anforderung bezüglich konstanter Bandbreite und Medienzugriffszeit haben, eine DCF Erweiterung spezifiziert, die in Kapitel 4.8 beschrieben wird.

Wichtigster Teil der DCF ist das Medienzugriffsverfahren, das Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA) genannt wird. CSMA/CA ist CSMA/CD (CSMA/Collision Detect) sehr ähnlich, das im drahtgebundenen Ethernet verwendet wird, bietet aber einige zusätzliche Möglichkeiten, Kollisionen zu vermeiden.

Backoff

Möchte ein Endgerät ein Datenpaket versenden, und es wird keine Aktivität auf der Luftschnittstelle festgestellt, kann das Datenpaket ohne Verzögerung gesendet werden. Wird jedoch zu diesem Zeitpunkt gerade ein Datenpaket eines anderen Teilnehmers übertragen, muss das Endgerät zunächst warten, bis diese Übertragung abgeschlossen ist. Danach wartet das Endgerät noch das Ende der DIFS Periode ab. Um zu vermeiden, dass mehrere sendebereite Endgeräte danach gleichzeitig ihre Pakete absenden, wird zusätzlich noch eine per Zufallsgenerator in jedem Endgerät ermittelte Backoff-Zeit gewartet. Da mit großer Wahrscheinlichkeit jeder Teilnehmer eine andere Backoff-Zeit ermittelt hat, sendet somit nur ein Endgerät. Alle anderen sendebereiten Endgeräte sehen das Datenpaket, brechen ihre Backoff-Wartezeit ab und starten ihre Zugriffsprozedur erneut von vorn. Sollten trotz dieser Prozedur einmal zwei Endgeräte gleichzeitig senden, stören sich die Pakete gegenseitig und der Acknowledgement Frame bleibt aus. Beide Stationen müssen dann erneut versuchen, ihr Datenpaket zu senden. Bei einem Übertragungsfehler vergrößert sich jedoch die Zeitspanne für die mögliche Backoff-Zeit für das Endgerät. Somit wird erreicht, dass bei hoher Auslastung die Anzahl der Kollisionen gering bleibt.

Die Backoff-Zeit wird in Slots zu 20 Mikrosekunden eingeteilt. Beim ersten Sendeversuch gibt es bei 802.11b und g 31 Slots, von denen einer per Zufallsgenerator ausgewählt wird. Schlägt die Übertragung fehl, vergrößert sich das Fenster auf 63 Slots, danach auf 127 Slots usw., bis maximal 1023 Slots, was maximal 20 Millisekunden entspricht. Bei 802.11n wurde das erste Backoff Fenster auf 15 Slots verkleinert, was 0.3 Millisekunden entspricht.

Network Allocation Vector (NAV)

Zusätzlich zur Erkennung einer laufenden Datenübertragung und anschließender Backoff-Zeit enthält jedes Datenpaket auch eine Zeitspanne, wie lange die Übertragung des Datenpakets und anschließendem ACK Frame dauert. Diese Zeitspanne wird Network Allocation Vector (NAV) genannt. Diese zusätzliche Funktion ist vor allem dann sinnvoll, wenn wie in Abbildung 4.12 gezeigt, die Luftschnittstelle mit RTS und CTS Frames reserviert wird. Das RTS Frame enthält die Information, wie viel Zeit für

die Übertragung des CTS, des Datenpakets und das anschließende ACK Frame benötigt wird. Das anschließende CTS Paket der Gegenseite enthält dann einen etwas kleineren NAV, der nur noch die Zeitspanne für das anschließende Datenpaket und den ACK Frame enthält.

4.5.2 Der MAC Header

Wichtigste Aufgabe des MAC Headers auf Layer 2 ist die Adressierung der Endgeräte im lokalen Netzwerk. Zu diesem Zweck enthält der MAC Header eines WLAN Frames in gleicher Weise wie ein Frame im drahtgebundenen Ethernet die 48 Bit langen MAC Adressen von Sender (Source) und Empfänger (Destination). In einem Basic Service Set (BSS) wird ein Datenframe jedoch nicht direkt vom Sender zum Empfänger geschickt, sondern immer zuerst zum Access Point. Aus diesem Grund enthält der MAC Header eines Frames, wie in Abbildung 4.13 gezeigt, nicht zwei, sondern drei MAC Adressen. Die dritte MAC Adresse ist dabei die Adresse des Access Points. Dieser empfängt das Paket und überprüft, ob die MAC Adresse des Empfängers zu einem drahtlosen oder einem drahtgebundenen Endgerät gehört und leitet den Frame entsprechend weiter. Somit spielt es für das Endgerät keine Rolle, ob der Empfänger des Frames ein WLAN oder Ethernet Endgerät ist.

MAC Adressen

Frame Type

Weitere wichtige Elemente im MAC Header sind der Frame Type und Subtype. Das Frame Type Element gibt an, ob es sich beim aktuellen Frame um einen Nutzdatenframe, Management Frame (z.B. Association Request) oder Control Frames (z.B. ACK) handelt. Je nach Frame Type enthält das Subtype Element dann weitere Informationen. Bei Management Frames gibt das Subtype Feld an, um welche Management Operation es sich handelt (z.B. Authentication, Association, Beacon, etc.).

Control Flags

In den Frame Control Flags werden in jedem Frame zusätzliche Informationen zwischen zwei Teilnehmern ausgetauscht. Dort ist unter anderem angegeben, ob die Nutzdaten des Frames verschlüsselt sind (WEP enabled Bit), ob das Endgerät in den Stromsparmodus wechseln wird (Power Management Bit) und ob der Frame für einen Access Point bestimmt ist (To Distribution System Bit).

LLC Header

Bei Nutzdatenframes folgt auf den MAC Header, in gleicher Weise wie im drahtgebundenen Ethernet, der Logical Link Control Header (LLC Header, Layer 2). Dessen wichtigste Aufgabe ist es, das Layer 3 Protokoll zu identifizieren, das anschließend folgt.

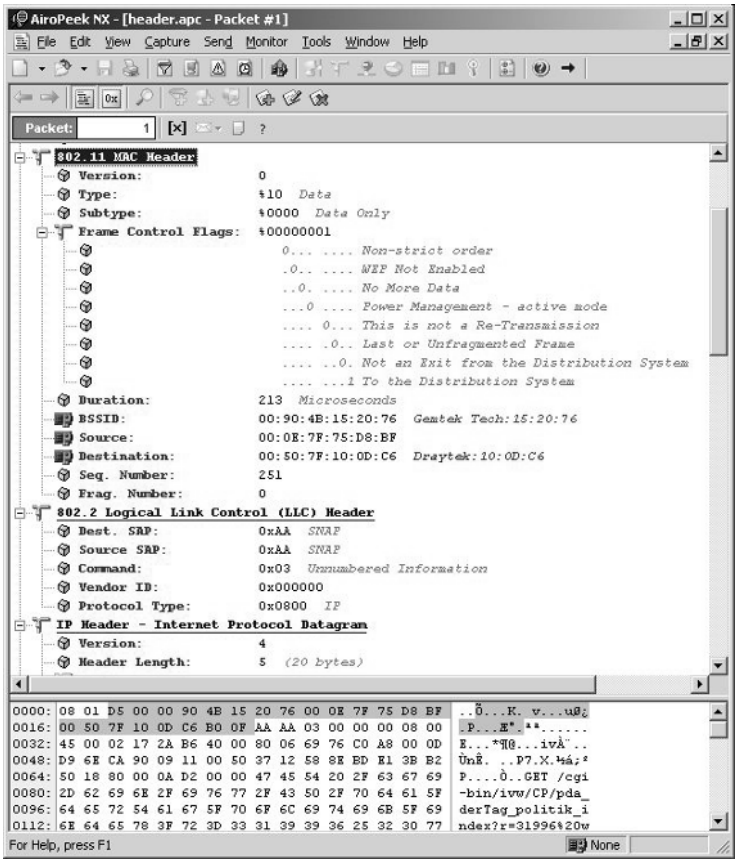

Abb. 4.13: MAC und LLC Header eines WLAN Frames

4.6 Physical Layer und MAC-Erweiterungen

Auf Layer 1, dem Physical Layer, gibt es wie in Kapitel 4.2 gezeigt, unterschiedliche Varianten mit unterschiedlichen Geschwindigkeiten, die in den Standards IEEE 802.11b, g, a und n beschrieben sind.

4.6.1 IEEE 802.11b mit bis zu 11 MBit/s

Mit einer maximalen Geschwindigkeit von bis zu 11 MBit/s erfolgte mit dem 802.11b Standard der Durchbruch von WLAN im Massenmarkt. Mit neueren Physical Layern wie 802.11g oder 802.11a sind mit der gleichen Bandbreitennutzung von etwa 22 MHz noch weit höhere Geschwindigkeiten möglich. Mehr dazu

im nächsten Abschnitt. Um ein Gefühl für ein 802.11 System im Vergleich zu anderen Technologien zu bekommen, sind folgende Daten hilfreich:

802.11b Eckdaten

- Maximale Leistung auf 0.1 Watt begrenzt.
- 22 MHz Bandbreite pro Kanal. Somit können im ISM Band drei Netze am gleichen Ort überlappend betrieben werden.
- Framegröße: 4-4095 Bytes, IP Frames sind jedoch meist nicht größer als etwa 1500 Bytes. Interessant ist hier der Vergleich zu anderen Technologien: In einem GPRS Paket, das wie in Kapitel 2.2.3 gezeigt, aus 4 Bursts zu je 114 Bits besteht, können nur 456 Bits übertragen werden. Bei Coding Scheme 2 bleiben hier nach Abzug der Fehlerkorrekturbits nur 240 Bits, also 30 Bytes. Während ein IP Paket über WLAN komplett in einem Paket übertragen wird, wird dieses in GPRS über mehrere Pakete aufgeteilt.
- Übertragungszeit eines großen Pakets: Dies ist zum einen von der Größe des Pakets und zum anderen von der Übertragungsrate abhängig. Wird ein großes Paket mit z.B. 1500 Bytes mit einer Übertragungsgeschwindigkeit von 1 MBit/s übertragen, dauert die Übertragung 12 Millisekunden. Bei gutem Empfang und einer Übertragungsgeschwindigkeit von 11 MBit/s dauert die Übertragung hingegen nur etwa 1.1 Millisekunden. Hinzu kommt noch die Übertragungszeit für den ACK Frame, sowie die Sendepause zwischen den Frames.
- Zeit zwischen Datenframe und ACK Frame (SIFS): 10 Mikrosekunden, oder 0.01 Millisekunden.
- Tritt ein Übertragungsfehler auf, wird das im letzten Absatz beschriebene Backoff-Verfahren angewandt. Ein Backoff Slot, von denen es bei der ersten Wiederholung 63 gibt, hat eine Länge von 20 Mikrosekunden oder 0.02 Millisekunden.
- Zu Beginn jedes Frames wird eine Präambel gesendet, die anderen Endgeräten die Übertragung ankündigt. Dies ist notwendig, damit sich alle anderen Endgeräte auf den Frame synchronisieren können. Die Präambel hat eine Länge von 144 Mikrosekunden, oder 0.144 Millisekunden.

PLCP Header und Übertragungsrate

Die Präambel ist Teil des Physical Layer Convergence Procedure (PLCP) Header, der vor jedem Frame gesendet wird. Der PLCP Header enthält auch die Information, mit welcher Übertragungsrate der nachfolgende MAC Frame gesendet wird. Bei 802.11 kann ein MAC Frame mit 1 MBit/s, 2, 5.5 und 11 MBit/s gesendet werden. Diese Flexibilität ist nötig, da Endgeräte mit schlechtem Empfang mit geringer Geschwindigkeit senden können, um somit die Redundanz zu erhöhen. Üblicherweise entscheidet das Endgerät automatisch anhand der Übertragungsbedingungen, mit welcher Geschwindigkeit ein Frame gesendet werden soll. Manche Endgeräte bieten aber auch die Möglichkeit, die maximale Datenrate fest einzustellen (z.B. auf 5.5 MBit/s). Dies hilft vor allem dann weiter, wenn die Automatik nur schlecht funktioniert. Bei manchen Access Points ist in der Praxis zu beobachten, dass Nutzdatenpakete zu einem Endgerät mit der zuletzt vom Endgerät gewählten Geschwindigkeit gesendet werden. Beacon Frames hingegen werden beispielsweise von manchen Access Points immer mit 1 oder 2 MBit/s übertragen. Auf diese Weise können auch weiter entfernte Geräte die Beacon Frames noch korrekt empfangen. Dies ist aber nicht vorgeschrieben und so senden manche Access Points die Beacon Frames mit 11 MBit/s. Dies erhöht zwar den Durchsatz des Netzwerkes geringfügig, weit entfernte Stationen werden aber Probleme haben, die Beacon Frames korrekt zu empfangen.

DSSS für 1 und 2 MBit/s

Für die Codierung der Daten eines Frames für die Übertragung mit 1 oder 2 MBit/s wird das Direct Sequence Spread Spectrum Verfahren (DSSS) verwendet. Ein Bit wird dabei nicht direkt übertragen, stattdessen werden 11 Chips übertragen. Für ein Bit mit dem Wert 1 wird die Chipsequenz „0,1,0,0,1,0,0,0,1,1,1“ übertragen, für ein Bit mit dem Wert 0 die Sequenz „1,0,1,1,0,1,1,1,0,0,0“. Diese Sequenzen werden auch Barker Code genannt. Da statt einem Wert nun 11 Werte pro Bit übertragen werden, erhöht sich die Redundanz ganz erheblich. Somit ist es möglich, auch bei einigen nicht korrekt empfangenen Chips das übertragene Bit dennoch korrekt zu erkennen.

Auch UMTS macht sich dieses Verfahrens, das „spreizen“ genannt wird, für die Erhöhung der Redundanz zunutze. Während bei WLAN jedoch nur ein Endgerät zu einer Zeit sendet (Time Division Multiple Access), ermöglicht das Spreizen bei UMTS zusätzlich die gleichzeitige Datenübertragung von mehrere Endgeräten (Code Division Multiple Access). Bei UMTS werden jedoch,

wie in Kapitel 3 gezeigt wurde, keine festen Sequenzen, sondern variable orthogonale Codes verwendet.

Modulation

Die Barker Chip Sequenz wird anschließend mit dem Differential Binary Phase Shift Keying (DBPSK) Verfahren mit einer Übertragungsgeschwindigkeit von 11 MChips/s übertragen. Dies ergibt somit eine Bitrate von 1 MBit/s. Beim DBPSK Verfahren ändert sich bei jeder Übertragung eines Chips mit dem Wert 1 die Phasenlage des Sinussignals um 180 Grad. Bei einem Chip mit dem Wert 0 hingegen ändert sich die Phasenlage nicht.

Für eine Übertragungsgeschwindigkeit von 2 MBit/s wird statt DBPSK das Differential Quadrature Phase Shift Keying (DQPSK) Verfahren angewandt. Statt einem Chip pro Übertragungsschritt werden hier 2 Chips übertragen. Die 4 (quadrature) möglichen unterschiedlichen Werte (00, 01, 10 oder 11) der 2 Chips werden in diesem Verfahren mit 90 Grad Phasenwechseln pro Übertragungsschritt kodiert.

HR/DSSS für 5.5 und 11 MBit/s mit CCK

Um bei gleicher Bandbreitennutzung noch schnellere Datenraten zu ermöglichen, wurde mit dem 802.11b Standard das Complementary Code Keying (CCK) Verfahren unter dem Namen High Rate DSSS (HR/DSSS) eingeführt. Statt ein Bit statisch in einer 11 Chip Barker Sequenz zu kodieren, werden die Bits beim CCK Verfahren wie folgt übertragen:

Um eine Datenrate von 11 MBit/s zu erhalten, werden die Bits eines Frames wie in Abbildung 4.14 gezeigt, zunächst in 8 Bit Blöcke eingeteilt. Die ersten zwei Bits werden wie beim vorhergehenden Verfahren auch per DQPSK in eine Änderung der Phasenlage in 90 Grad Schritten übertragen.

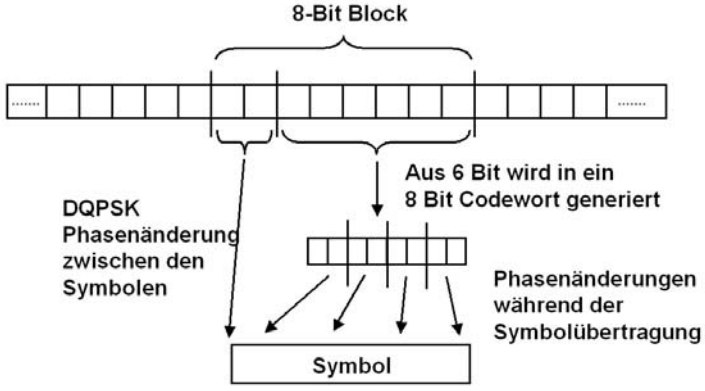

Abb. 4.14: Complementary Code Keying für 11 MBit/s

Aus den restlichen 6 Bits wird danach ein 8 Chip Codewort gebildet. Dieses 8 Chip Codewort wird auch Symbol genannt. Da 6 Bit in einem 8 Bit Symbol kodiert werden, ist auch hier noch eine gewisse Redundanz enthalten. Das so erhaltene Symbol wird wiederum in 4 Teile zu 2 Bits unterteilt und danach in Phasenänderungen kodiert übertragen.

Da die Taktgeschwindigkeit zum 1 bzw. 2 MBit/s Verfahren nicht geändert wurde, können auf diese Weise 11 MBit/s übertragen werden. Nachteil ist jedoch, dass in den übertragenen Informationen wesentlich weniger Redundanz vorhanden ist.

Header immer mit 1 MBit/s

Damit auch Endgeräte mit schlechten Empfangsbedingungen keine Kollisionen erzeugen, muss zumindest der Beginn eines Frames korrekt empfangen werden können. Um dies zu gewährleisten, wird der PLCP Header immer mit einer Geschwindigkeit von 1 MBit/s übertragen, auch wenn der anschließende MAC Frame mit 11 MBit/s übertragen wird. Da auch die Übertragungszeit für den anschließenden MAC Frame im PLCP Header enthalten ist, weis ein empfangendes Endgerät genau, wie lange das Medium besetzt ist, auch wenn die nachfolgenden „schnellen" Bits nicht korrekt empfangen werden können.

Geschwindigkeitsvergleich 802.11b und 10 MBit/s Ethernet

Vergleicht man die tatsächliche Geschwindigkeit eines 11 MBit/s Wireless LANs mit einem 10 MBit/s drahtgebundenen Ethernet, ist ein deutlicher Unterschied sichtbar. Ein 10 MBit/s Ethernet ermöglicht unter idealen Bedingungen einen maximalen Durchsatz von etwa 700-800 kByte/s. Bei WLAN beträgt die maximale Geschwindigkeit beim Datenaustausch zwischen zwei mobilen Endgeräten hingegen ‚nur' 300 kByte/s. Dies liegt an folgenden WLAN Eigenschaften, die in diesem Abschnitt beschrieben wurden:

- Der PLCP Header jedes WLAN Frames wird mit 1 MBit/s gesendet.
- Auf jeden Frame muss der Empfänger mit einem ACK Frame antworten. Auch dies kostet zusätzliche Zeit.
- Während bei Ethernet ein Frame direkt zum Empfänger geschickt wird, muss ein Frame in einem WLAN BSS zuerst an den Access Point geschickt werden. Dieser sendet das Paket dann an den Empfänger. Die Luftschnittstelle wird somit durch das Paket zweimal belegt. Die maximale Datenrate reduziert sich somit um die Hälfte.

4.6.2 IEEE 802.11g mit bis zu 54 MBit/s

Um die Übertragungsgeschwindigkeit weiter zu erhöhen, wurde für die 802.11g Standarderweiterung ein neues Modulationsverfahren mit der Bezeichnung Orthogonal Frequency Division Multiplexing (OFDM), gewählt. Mit dieser Modulation sind bei etwa gleicher Bandbreitennutzung wie bei 802.11b Geschwindigkeiten von bis zu 54 MBit/s möglich. Im Standard wird dieser Physical Layer als Extended-Rate (ERP) PHY bezeichnet.

OFDM

Das OFDM Modulationsverfahren unterscheidet sich grundlegend von den in 802.11b verwendeten Techniken. Wie Abbildung 4.15 vereinfacht zeigt, teilt OFDM den Übertragungskanal von etwa 20 MHz in 52 Unterkanäle (Sub-Channels) auf, über die unabhängig voneinander Daten übertragen werden können.

Die Unterkanäle werden als Orthogonal bezeichnet, weil die Amplituden der Nachbarkanäle an der Mittenfrequenz eines anderen Kanals genau Null sind. Somit haben sie keinen Einfluss auf die Amplitude eines anderen Kanals. Um Daten auf die Unterkanäle aufzumodulieren, wird beim OFDM Verfahren keine Phasenverschiebung wie in den bisherigen Verfahren verwendet, stattdessen werden die Informationen über die Höhe der Amplitude kodiert. Je nach Empfangsqualität des Signals wir die Amplitude in eine unterschiedliche Anzahl von Stufen aufgeteilt.

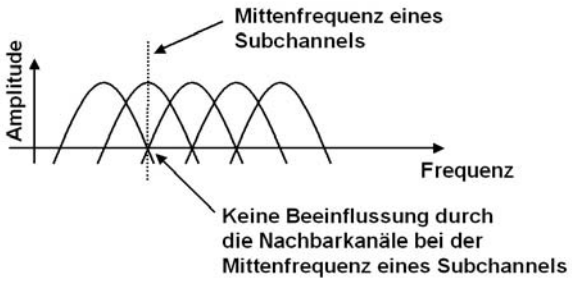

Abb. 4.15: Vereinfachte Darstellung des OFDM Modulationsverfahren

Um das Signal zu demodulieren, wird im Empfänger für jeden Übertragungsschritt eine FFT (Fast Fourier Transformation) Analyse durchgeführt. Mit diesem Verfahren ist es möglich, die Signalenergie (Amplitude) über das Frequenzband zu berechnen. Das Ergebnis einer FFT ist vereinfacht in Abbildung 4.15 gezeigt. Das Frequenzband ist dabei auf der der x-Achse aufgezeichnet

(statt wie bei anderen Verfahren die Zeit), die Amplitude auf der y-Achse.

Die folgende Tabelle zeigt die bei 802.11g möglichen Geschwindigkeiten:

Geschwindigkeit (MBit/s)	Modulation und Coding	Kodierte Bits pro Kanal	Kodierte Bits in 48 Kanälen	Datenbits pro Schritt
6	BPSK, R=1/2	1	48	24
9	BPSK, R=3/4	1	48	36
12	QPSK, R=1/2	2	96	48
18	QPSK, R=3/4	2	96	72
24	16-QAM, R=1/2	4	192	96
36	16-QAM, R=3/4	4	192	144
48	64-QAM, R=2/3	6	288	192
54	64-QAM, R=3/4	6	288	216

Bei günstigen Übertragungsbedingungen kann z.B. das 64 Quadrature Amplitude Modulation (64QAM) Verfahren verwendet werden. Zusammen mit einem ¾ Convolutional Coder (3 Datenbits pro 4 übertragenen Bits) und einer Schrittgeschwindigkeit (Symbol Speed) von 250.000 Symbolen/s wird dadurch eine Geschwindigkeit von 54 MBit/s erreicht (216 Bits pro Schritt * 250.000 Symbole/s = 54 MBit/s). Der Convolutional Coder, auch Faltungskodierer genannt, dient zur Erhöhung der Redundanz und wird auch bei GSM und UMTS verwendet (vgl. Kapitel 1.7.5 und Abb. 1.35).

802.11g ist kompatibel zu 802.11b

802.11g Endgeräte und Access Points sind abwärtskompatibel zu langsameren 802.11b Geräten. Das bedeutet, dass ein 802.11g Access Point auch 802.11b Endgeräte unterstützt, die mit maximal 11 MBit/s senden können. Im umgekehrten Fall können auch 802.11g Endgeräte mit 802.11b Access Points kommunizieren, wobei dann die Datenrate natürlich auf 11 MBit/s begrenzt ist.

Da langsame 802.11b Endgeräte die neue OFDM Modulationsart nicht erkennen können, müssen 802.11g Geräte Schutzmassnahmen ergreifen, sobald sich ein älteres 802.11b Gerät am Netzwerk anmeldet. Während mindestens ein solches Gerät am Access Point anmeldet ist, informiert dieser über einen Parameter in den Beacon Frames alle Teilnehmer des Netzwerkes. 802.11g Geräte senden dann vor dem eigentlichen Datenpaket ein Clear To Send (CTS) Paket. Dieses kann auch von 802.11b Endgeräten

dekodiert werden und enthält die Zeitdauer, die die Luftschnittstelle danach belegt ist. Somit ist sichergestellt, dass 802.11b Endgeräte nicht gleichzeitig mit 802.11g Geräten senden. Außerdem muss der PLCP Header jedes Frames mit 1 MBit/s gesendet werden, um von allen Geräten korrekt erkannt zu werden. Zusammen bringt dies in der Praxis jedoch aufgrund des zusätzlichen Overheads einen Geschwindigkeitsverlust von bis zu 40% mit sich. Aus diesem Grund kann in den meisten Access Points auch ein „G-Only“ Mode eingeschaltet werden, der diesen zusätzlichen Overhead vermeidet, ältere 802.11b Geräte jedoch ausschließt. Dieser Modus ist vor allem für private WLANs sinnvoll, in denen alle Endgeräte zu 802.11g kompatibel sind.

802.11g Geschwindigkeitsvergleich

Unter optimalen Übertragungsbedingungen sind in der Praxis Übertragungsgeschwindigkeiten von etwa 2.500 kByte pro Sekunde möglich. Kommunizieren zwei drahtlose Endgeräte miteinander, reduziert sich die maximale Geschwindigkeit auf etwa 1.200 kByte pro Sekunde, da alle Frames zuerst zum Access Point übertragen werden und erst von dort zum Empfänger weitergeschickt werden. Abhilfe wird hier der 802.11e Standard verschaffen, der am Anfang des Kapitels erwähnt wurde. Im Vergleich zu einem 802.11b Netz mit 600 bzw. 300 kByte/s zwischen zwei mobilen Endgeräten stellt der 802.11g Standard einen beachtlichen Fortschritt dar. Jedoch bleibt der Standard noch weit hinter einem 100 MBit/s drahtgebundenen Ethernet zurück, das mit einer Datenrate von etwa 7.000 kByte/s immer noch etwa um den Faktor 3 schneller ist.

4.6.3 IEEE 802.11a mit bis zu 54 MBit/s

Der 802.11a Standard ist im Wesentlichen mit dem zuvor beschriebenen 802.11g Standard identisch. Dieser Standard sendet jedoch im 5 GHz Bereich und ist somit nicht mit 802.11b Netzen kompatibel. Dies hat jedoch auch den Vorteil, dass die bei 802.11g verwendeten Verfahren für die Rückwärtskompatibilität hier nicht angewandt werden müssen und der PLCP Header statt mit 1 MBit/s mit 6 MBit/s gesendet werden kann. Reine 802.11a Netze sind somit deutlich schneller als gemischte 802.11b/g Netze und haben auch gegenüber reinen 802.11g Netzen einen kleinen Geschwindigkeitsvorteil durch den schnelleren PLCP Header.

4.6.4 IEEE 802.11n mit bis zu 600 MBit/s

Wie in Kapitel 4.6.2 gezeigt, sind mit dem 802.11g Standard Übertragungsgeschwindigkeiten unter günstigen Bedingungen von 20 – 25 MBit/s auf Applikationsebene zu erreichen. Für aktuelle ADSL oder Kabelanschlüsse ist diese Geschwindigkeit ausreichend. Zunehmend sind jedoch auch ADSL2+, VDSL und neue Kabelanschlüsse verfügbar, die höhere Geschwindigkeiten bieten und für die somit ein 802.11g Netzwerk nicht mehr ausreichend ist. Auch für die Anbindung von Endgeräten an zentrale Datei- oder Medienserver im Büro oder im Heimbereich, sowie für neue Anwendungen wie High Definition Video Streaming wird das Wireless LAN Netzwerk schnell zum Nadelöhr. Aus diesen Gründen entschlossen sich eine große Anzahl von Firmen in der 802.11n Arbeitsgruppe den Standard weiterzuentwickeln. Hauptziel für viele Firmen war die Erhöhung der Datenrate. Weitere Ziele waren die Erhöhung der Reichweite und die Einführung von Quality of Service (QoS) Mechanismen, um Applikationen wie Sprachtelefonie über IP (VoIP) oder Videostreaming auch in stark genutzten Drahtlosnetzwerken oder größeren Entfernungen mit guter Qualität zu ermöglichen. Aufgrund der großen Anzahl an Firmen, die sich an der Standardisierung beteiligten, wurde die 802.11n Erweiterung des Wireless LAN Standards sehr umfangreich und enthält zahlreiche optionale Funktionalitäten, die in der Praxis nur von höherwertigen Geräten genutzt werden. Im Folgenden werden deshalb zunächst jene neuen Funktionen des High Througput (HT) Physical Layers (PHY), sowie jene MAC Layer Erweiterungen beschrieben, die im Standard fest vorgeschrieben sind, sowie jene Optionen, die auch im Consumer Segment weite Verbreitung finden.

20 MHz und 40 MHz Kanäle

Einfachstes Mittel um die Geschwindigkeit zu steigern ist die Verbreiterung des Übertragungskanals. Zusätzlich zu 20 MHz Kanälen erlaubt der Standard nun auch die Verwendung von 40 MHz Kanälen. In der Praxis wurde dies schon von vielen Herstellen mit 802.11g proprietär implementiert, Endgeräte unterschiedlicher Hersteller waren jedoch nicht untereinander kompatibel.

Mehr Subkanäle

Für die Datenübertragung werden bei 802.11n statt 52 OFDM Subkanäle wie bei 802.11g nun 56 OFDM Subkanäle in einem 20 MHz Kanal verwendet. Die Bandbreite pro Subkanal ist bei beiden Varianten 312.5 kHz. Dies wurde erreicht, indem jeweils rechts und links im Frequenzband zwei weitere Subkanäle verwendet werden, die bei 802.11g noch nicht genutzt wurden. Die Anzahl der Pilotkanäle, die dem Empfänger das Ausmessen des

Kanals ermöglichen und keine Nutzdaten übertragen, bleibt in beiden Varianten bei vier. In einem 40 MHz Kanal werden insgesamt 114 Subkanäle verwendet, von denen 6 als Pilot verwendet werden.

	20 MHz non-HT (wie 802.11g)	**20 MHz HT**	**40 MHz HT**
Anzahl Carrier	48	52	108 (2* 54)
Anzahl Pilots	4	4	6
Gesamte Anzahl an Carriern	52	56	114 (2 * 57)
Nicht benutzte Carrier in der Mitte	1	1	3

Frame Aggregation

Der ursprüngliche Wireless LAN Standard verlangte nach jeder Übertragung eines Pakets eine Empfangsbestätigung der Gegenstelle durch ein Acknowledgement (ACK) Frame wie zuvor in Abbildung 4.11 gezeigt. Dies ist bei einem unzuverlässigen Übertragungsmedium wichtig, um Übertragungsfehler schnell korrigieren zu können, hat jedoch den Nachteil, dass die Luftschnittstelle nicht sehr effizient genutzt wird. Erst mit 802.11e wurden effizientere Verfahren standardisiert, die in Kapitel 4.8 und Abbildung 4.28 näher beschrieben werden. Um den Overhead weiter zu reduzieren, wurde im 802.11n Standard auf dem MAC Layer ein weiteres Verfahren eingeführt, um Pakete gebündelt übertragen zu können. Dieses Verfahren wird Frame Aggregation genannt. Statt jedes Paket einzeln zu übertragen und danach auf eine Bestätigung zu warten, kann der Sender jetzt Pakete auf dem MAC Layer bis zu einer Gesamtgröße von 65535 Byte bündeln und gemeinsam übertragen. Der Empfänger bestätigt dann das gesamte Bündel mit nur einem ACK Paket. Der Overhead wird dadurch vor allem dann stark minimiert, wenn ein Endgerät große Datenmengen überträgt und somit den Sendepuffer der Netzwerkkarte ständig gefüllt hält. Ein großer Nachteil ist jedoch,

dass bei einem Übertragungsfehler das komplette Paket erneut übertragen werden muss.

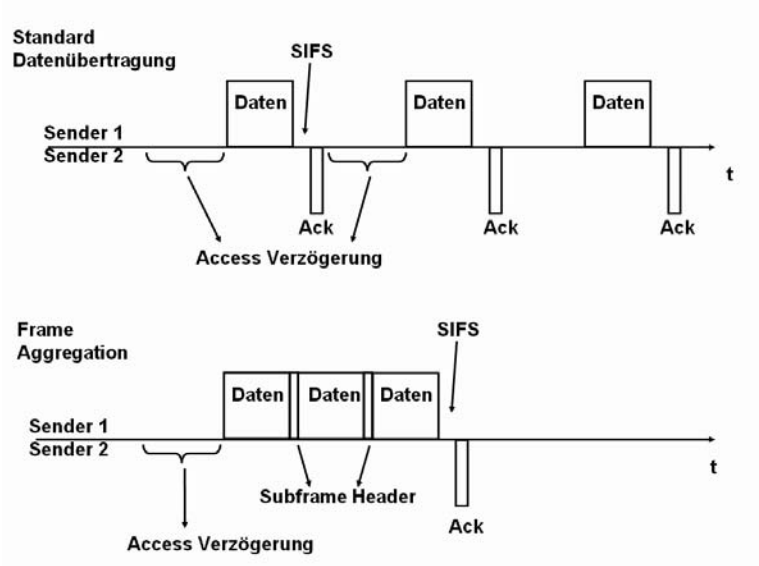

Abb. 4.16: Normale Datenübertragung im Vergleich mit Frame Aggregation

Verkürztes Guard Interval

Ein weiterer Parameter für die Optimierung der Luftschnittstelle ist das OFDM Guard Intervall. Dieses ist bei OFDM Übertragungen notwendig, um die Interferenz zwischen aufeinander folgenden Symbolen abklingen zu lassen. In der Praxis zeigte sich, dass für die meisten Umgebungen ein Guard Intervall von 400 ns pro Symbol statt bisher 800 ns ausreicht. Die Übertragungszeit eines OFDM Symbols verringert sich dadurch deutlich von 4 auf 3.6 Mikrosekunden, d.h. es können im gleichen Zeitraum mehr Symbole, also mehr Daten übertragen werden.

Weniger Fehlerkorrekturbits

Eine weitere Möglichkeit die Geschwindigkeit leicht zu steigern ist die Anzahl der Fehlerkorrekturbits weiter zu senken. Die niedrigste Codierrate in 802.11g Netzwerken ist 3/4, d.h. in 4 Bits sind drei Nutzdatenbits und ein Fehlerkorrekturbit enthalten. Bei 802.11n ist jetzt bei sehr guten Übertragungsbedingungen auch ein 5/6 Codierverfahren erlaubt, das für 5 Nutzdatenbits nur ein Fehlerkorrekturbit enthält.

Alle bisherigen Maßnahmen zusammen steigern die Geschwindigkeit um etwa das 2.5-fache verglichen mit 802.11g auf bis zu 150 MBit/s. Wie bei früheren Standards auch, bleibt auf Grund

der Acknowledgement Frames und anderen Eigenschaften der Luftschnittstelle für Applikationen in etwa die Hälfte dieser Geschwindigkeit übrig.

Verwenden des 2.4 GHz und 5 GHz Bands

Wie am Anfang des Kapitels in Abbildung 4.5 gezeigt, finden im 2.4 GHz ISM Band nur drei unabhängige Netzwerke mit einer Bandbreite von 20 MHz Platz. Besonders in Städten teilen sich jedoch weit mehr Netze das ISM Band. In einer solchen Situation schreibt der Standard vor, dass ein Access Point bei Empfang von Frames anderer Netzwerke in einem der zwei für den 40 MHz Doppelkanal verwendeten Bänder sofort in den 20 MHz Kanalmodus zurückschalten muss und erst 30 Minuten nach dem letzten Auffinden eines Frames eines anderen Netzwerkes den breiteren Kanal wieder aktivieren darf. In der Praxis kann somit der 40 MHz Kanalmodus im 2.4 GHz Band nur in den wenigsten Fällen verwendet werden. Zwar kann der Access Point in einem solchen Fall die Frequenz wechseln und dies den Endgeräten über Channel Switch Announcement Management Frames mitteilen, dies wird jedoch im überfüllten 2.4 GHz Band nur in den seltensten Fällen helfen. Der Standard erlaubt jedoch auch die Verwendung des 5 GHz Bandes, in dem bis zu neun 40 MHz oder achtzehn 20 MHz Netzwerke Platz finden. Da dieser Frequenzbereich bisher nur selten genutzt wird, ist es hier meist ohne Probleme möglich, einen breiteren Kanal zu betreiben. In der Praxis bieten jedoch erst wenige Access Point- und Endgerätehersteller 802.11n Geräte für den 5 GHz Bereich an. Apple ist mit manchen Notebookmodellen und dem Airport Express Access Point eine der wenigen Ausnahmen.

MIMO Spatial Multiplexing

Um die Geschwindigkeit und Reichweite weiter zu steigern, wurden im Standard sowohl für 20 MHz wie auch für 40 MHz Kanäle diverse Multiple Input – Multiple Output (MIMO) Verfahren spezifiziert. Die meisten Endgeräte werden zunächst MIMO Spatial Multiplexing bieten. Dieser MIMO Mode nutzt den Umstand, dass bei der Funkübertragung zwischen einem Sender und einem Empfänger ein Signal an Objekten reflektiert und der Empfänger somit nicht nur ein Signal, sondern mehrere identische sieht, die jedoch aus unterschiedlichen Richtungen kommen. Bei MIMO Spatial Multiplexing haben nun sowohl Sender wie auch Empfänger mehrere Antennen und auch mehrere Sende- bzw. Empfangsstufen. Der Sender sendet nun auf jeder Antenne auf der gleichen Frequenz einen anderen Datenstrom, die dann am Empfänger wieder von getrennten Empfangsstufen empfangen werden. Dies ist in Abbildung 4.17 gezeigt.

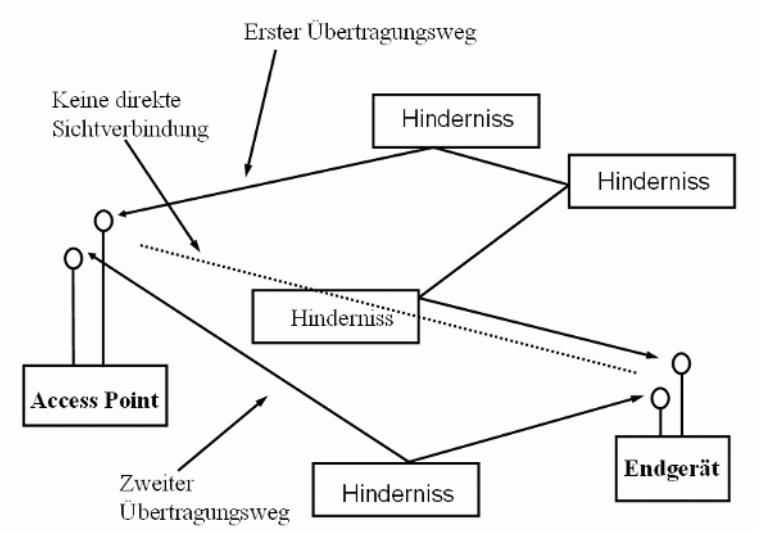

Abb. 4.17: 2x2 MIMO

Im Standard sind bis zu 4 MIMO Kanäle vorgesehen. Access Points müssen mindestens 2 MIMO Kanäle unterstützen, andere 802.11n Endgeräte, also Notebooks, USB Wifi Stecker und Einsteckkarten, sowie kleine Endgeräte wie PDA's, Mobiltelefone, etc., dürfen auch mit nur einen MIMO Pfad ausgestattet sein. Diese Regelung ist sinnvoll, da Access Points meistens nur wenige Restriktionen für Baugröße und Stromaufnahme haben. Kleine batteriebetriebene Geräte jedoch können mit nur einem MIMO Zweig kleiner und stromsparender sein. Zudem werden solche Endgeräte in der Praxis kaum die höheren Geschwindigkeiten benötigen. Da Endgeräte während der Association Prozedur dem Access Point ihre Fähigkeiten mitteilen könne, kann dieser dann z.B. einen 20 MHz Kanal ohne MIMO für ein VoIP Telefon verwenden und für das nächste Paket einen 40 MHz Kanal mit zwei MIMO Zweigen.

In der Praxis gibt es zur Zeit Geräte mit zwei Sende/Empfangseinheiten, was im günstigsten Fall die Datenrate gegenüber einem Single Input / Single Output (SISO) Endgerät verdoppelt. An dieser Stelle sei angemerkt, dass auch manche 802.11g Access Points über zwei Antennen verfügen. Diese haben jedoch nur eine Sende/Empfangseinheit und entscheiden auf Grund der Empfangslage, welche der beiden Antennen verwendet werden soll.

Insgesamt gibt es auf Grund der zahlreichen Variablen wie Anzahl der MIMO Kanäle, langer oder kurzer Guard Time, Modulation und Kodierung nun 77 mögliche Kombinationen, die zu unterschiedlichen Übertragungsgeschwindigkeiten führen. Die nachfolgende Tabelle zeigt exemplarisch einige Möglichkeiten.

	20 MHz, kein MIMO	20 MHz, 2 MIMO Streams	40 MHz 2 MIMO Streams
802.11b	1, 2, 5.5, 11 MBit/s		
802.11g	1, 2, 6, 9, 12, 18, 24, 36, 48, 54 MBit/s		
802.11n, GI 800ns	6.5, 13, 19.5, 26, 39, 52, 58.5, 65 MBit/s	13, 26, 39, 52, 78, 104, 117, 130 MBit/s	27, 54, 81, 108, 162, 216, 243, 270 MBit/s
802.11n, GI 400ns	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2 MBit/s	14.4, 28.9, 43.3, 57.8, 86.7, 115.6, 130, 144.4 MBit/s	30, 60, 90, 120, 180, 240, 270, 300 MBit/s

Die Tabelle zeigt auch anschaulich den Einfluss der Kanalbündelung und des kürzeren Guard Intervalls (GI). Durch die Kanalbündelung wird die Geschwindigkeit etwas mehr als verdoppelt, da zwischen den zwei Kanälen keine ungenutzten Subkanäle liegen und weniger Pilotkanäle verwendet werden. Der Einfluss des kürzeren Guard Intervalls zeigt sich vor allem bei einem 40 MHz Kanal mit zwei MIMO Streams. Durch das kürzere Guard Intervall kann die maximale Geschwindigkeit von 270 MBit/s auf 300 MBit/s gesteigert werden.

Geschwindigkeit in der Praxis

Zusammen mit den zuvor beschriebenen Verfahren, ergibt sich mit 2x2 MIMO (2 Senderantennen, 2 Empfängerantennen) eine maximale Geschwindigkeitssteigerung gegenüber 802.11g von Faktor 5 auf etwa 300 MBit/s auf der Luftschnittstelle. In einem 4x4 MIMO System, das 4 Antennen sowohl beim Sender als auch beim Empfänger benötigt, ist eine theoretische Maximalgeschwindigkeit von bis zu 600 MBit/s möglich.

In der Praxis erreichen derzeit erhältliche 2x2 MIMO Systeme auf dem Applikationslayer eine maximale Geschwindigkeit zwischen 80 und 110 MBit/s. Dies kann aber nur unter günstigen Bedin-

gungen, also auf kurzer Distanz von wenigen Metern, keine dicken Mauern zwischen den Geräten und im Greenfield Mode erreicht werden. Außerdem muss der Access Point unbedingt Gigabit Ethernet Ports unterstützen, um Datenraten über 100 MBit/s auch tatsächlich weiterleiten zu können. Unter weniger optimalen Bedingungen wählen die Endgeräte automatisch statt einer 64-QAM Modulation eine robustere Modulation (16-QAM, QPSK oder BPSK) und statt einer 5/6 Fehlerkorrektur Kodierung nur 3/4, 2/3 oder 1/2.

QoS

Eine weitere wichtige Eigenschaft von 802.11n zertifizierten Endgeräten ist die vorgeschriebene Implementierung der in 802.11e spezifizierten Quality of Service (QoS) Erweiterungen für die Luftschnittstelle. Mit dieser Erweiterung ist es möglich, dass Applikationen wie Voice over IP bevorzugt behandelt werden. Somit können Telefoniepakete oder Daten von anderen Applikationen, die eine konstante Bandbreite benötigen auch in Perioden mit hoher Netzwerklast (Streaming oder Übertragung von großen Dateien) deterministisch und zur richtigen Zeit übertragen werden. Da QoS in Zukunft eine wichtige Rolle spielen wird, geht Kapitel 4.8 näher auf dieses Thema ein.

HT Capabilities in Beacon und Management Frames

Beacon Frames von 802.11n Access Points enthalten eine Anzahl neuer Parameter. Der erste nennt sich „HT Capabilities“ (Element ID 45) und beschreibt, welche High Througput Funktionen der Access Point unterstützt. Die folgende Liste gibt einen Überblick über die wichtigsten Funktionen:

- Unterstützung des 40 MHz Modus (ja/nein).
- Anzahl der gleichzeitig unterstützten MIMO Streams und mögliche Modulations- und Kodiermodi (MCS).
- Unterstützung der auf 400ns verkürzten Guard Time .
- Ob der optionale MCS Feedback Modus unterstützt wird. Mit diesem kann der Empfänger dem Sender eine Rückmeldung über die zu verwendende Modulation geben und somit die Datenrate optimal an die Übertragungsbedingungen anpassen.
- STBC Diversity Support (siehe unten).
- Power Save Multipoll Support (PSMP), eine verbesserte Stromsparoption.
- Zahlreiche Parameter für das optionale MIMO Beamforming (siehe unten).

- Zahlreiche Parameter für die optionale Unterstützung diverser dynamischer Antennenauswahlverfahren. (siehe unten).

Der zweite neue Parameter in Beacon Frames ist der ‚HT Information' Parameter (Element ID 61). In diesem teilt der Access Point den Endgeräten mit, welche HT Funktionalitäten aktuell verwendet werden dürfen, und welche nicht. In der nachfolgenden Liste sind die wichtigsten Informationen zusammengefasst.

- Ob aktuell ein 40 MHz Kanal verwendet werden darf oder ob Übertragungen auf den 20 MHz Primärkanal limitiert sind.
- Operating Mode: Greenfield, HT-Mixed, Non-Member Protection Mode (Endgeräte, die mit anderen Access Points kommunizieren, senden im gleichen Band).
- Ob es Endgeräte im Netzwerk gibt, die nicht Greenfield Mode kompatibel sind.
- Overlapping BSS Protection: Entdeckt der Access Point Beacon Frames von anderen Access Points im gleichen Frequenzband, die nicht HT fähig sind oder im Mixed Mode arbeiten, kann mit diesem Bit Endgeräten signalisiert werden, ebenfalls den HT-mixed Mode zu aktivieren. Benachbarte Access Points, die dieses Bit sehen, selber jedoch keine nicht-HT Endgeräte beobachten können, müssen keine Sicherungsmaßnahmen treffen. Auf diese Weise wird erreicht, dass HT Netzwerke auf nicht kompatible Netzwerke in der Nähe Rücksicht nehmen, sich dies aber nicht über deren Grenzen hinaus fortsetzt.
- Secondary Beacon: Gibt an, ob dieses Beacon Paket im primären 20 MHz Kanal eines 40 MHz Kanals gesendet wurde, oder im zweiten 20 MHz Kanal.

Zusätzlich zu den Beacon Frames werden die HT Capability und HT Information Parameter von Access Points auch in Association-, Reassociation- und Probe Response Frames gesendet. Endgeräte erhalten somit auch während der Anmeldung und beim Wechsel des Access Points noch einmal zusätzlich alle unterstützten Parameter und die aktuelle Konfiguration.

Außer HT Parameter müssen 802.11n kompatible Access Points auch Informationen für das in der 802.11e Erweiterung spezifi-

zierte Quality of Service Handling in den Beacon Frames übertragen. Weitere Details hierzu in Kapitel 4.8.

Damit der Access Point auch über die Fähigkeiten jedes einzelnen Endgerätes im Netzwerk bescheid weiß, sendet auch ein Endgerät während der Association Prozedur seine „HT Information" an den Access Point. Somit ist es dann möglich, dass der Access Point für ein Endgerät Daten in einem 40 MHz Kanal mit kurzen Guard Intervall und zwei MIMO Streams überträgt, während Daten für ein Gerät mit weniger Fähigkeiten automatisch im 20 MHz Kanal, mit 800ns Guard Intervall und ohne MIMO geschickt werden.

Rückwärtskompatibilität zu 802.11b, g und a

Aufgrund der nötigen Rückwärtskompatibilität zu 802.11b, g und a, sowie den vielen Optionen der 802.11n Erweiterung muss ein Endgerät vor der Übertragung eines Datenpakets aus zahlreichen Optionen wählen. Wird ein Datenpaket an ein 802.11b Endgerät geschickt, kommt die HR/DSSS Modulation zum Einsatz. In Abhängigkeit des Übertragungskanals muss dann noch eine entsprechende Coderate gewählt werden. Für 802.11g Endgeräte wird für die Übertragung eine OFDM Modulation mit weniger Subkanälen (Non-HT Format) als für 802.11n Endgeräte verwendet, sowie ein 802.11g PLCP Header. Bei Übertragungen zwischen zwei 802.11n Geräten kommt ebenfalls die OFDM Modulation zum Einsatz, der PLCP Header ist jedoch kürzer und enthält HT spezifische Informationen (HT Greenfield Mode). Sind im Netzwerk 802.11n und 802.11g Geräte angemeldet (HT-Mixed Mode), wird, wie in Abbildung 4.18 gezeigt, ein entsprechend rückwärtskompatibler PLCP Header gesendet. Dieser kann auch von 802.11g Endgeräten dekodiert werden, umfasst jedoch einige Bytes mehr. Außerdem werden weniger OFDM Subkanäle verwendet. Falls auch 802.11b Endgeräte vorhanden sind, muss zudem noch ein CTS Paket in HR/DSSS Modulation der eigentlichen Übertragung vorangehen. Des Weiteren muss ein 802.11n Endgerät wissen, welche 802.11n Funktionalitäten die Gegenstelle unterstützt. Dies ist notwendig, um die OFDM Modulation entsprechend zu steuern (z.B. kurzes Guard Intervall), die Wahl zwischen einem 20 oder 40 MHz Kanal zu treffen, sowie die Anzahl der MIMO Kanäle und die Codierrate in Abhängigkeit der Kanalqualität zu bestimmen.

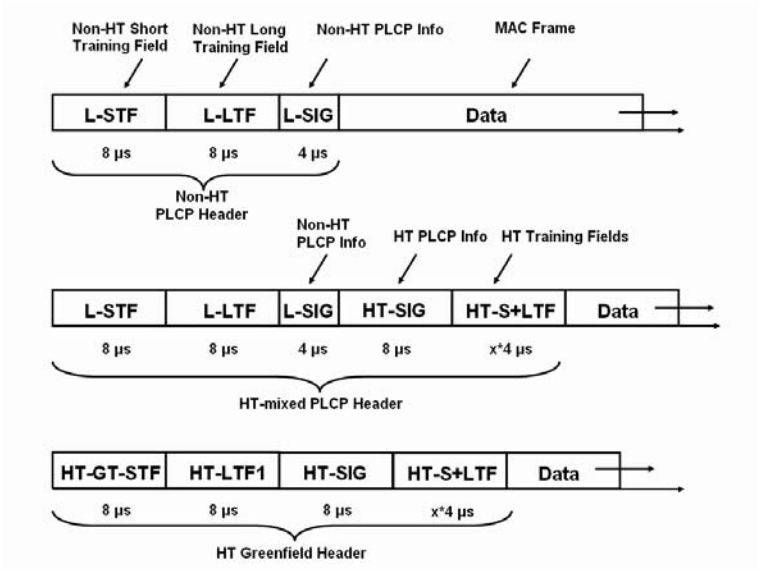

Abb. 4.18: PLCP Headervarianten

Selbst diese umfangreiche Liste berücksichtigt noch nicht zahlreiche weitere optionale 802.11n Funktionen, die nachfolgend beschrieben werden. Da diese Funktionen zum Teil recht komplex sind, ist davon auszugehen, dass die meisten davon anfangs nur in wenigen Endgeräten und Access Points implementiert sind.

Neuer Stromsparmodus: PSMP

Für batteriebetriebene Endgeräte ist es sehr wichtig, dass der Wireless LAN Chip in Zeiten, in denen keine Daten übertragen werden, nur minimale Energie benötigt. Für diesen Zweck gibt es den in Kapitel 4.4 vorgestellten Power Save (PS) Mode, der heute auch von vielen Endgeräten verwendet wird. Dieser Power Save Mode kann aber nicht aktiviert werden, wenn Multimedia Anwendungen wie Voice over IP z.B. alle 20 Millisekunden ein kleines Datenpaket von wenigen Mikrosekunden übertragen und dann für den Rest des Intervalls keine Daten übertragen. Auch wenn keine Daten übertragen werden, benötigt der WLAN Chip trotzdem Energie, da der Funkkanal weiterhin abgehört werden muss. Für solche Anwendungen wurde im 802.11n Standard optional ein zusätzlicher Stromsparmechanismus eingeführt, der Power Save Multi Poll (PSMP) genannt wird. Bei diesem Verfahren beantragt ein Endgerät beim Access Point periodisch Datenpakete einer bestimmten Größe senden und empfangen zu dür-

fen. Der Access Point setzt daraufhin ein PSMP Fenster auf und teilt dem Endgerät mit, zu welchen Zeiten dieses Fenster genutzt werden kann. Das Endgerät schaltet seinen Transciever dann nur während dieses Fensters ein und empfängt seine Datenpakete. Nach dem Downlink Fenster folgt automatisch ein Uplink Fenster, in dem ein Endgerät ohne vorherige Reservierung des Mediums seine Daten schicken kann. Während der restlichen Zeit kann das Endgerät dann seinen Transciever komplett abschalten und somit die Batterielaufzeit erhöhen.

Datenpakete in beide Richtungen enthalten im PSMP Modus nicht nur Nutzdaten, sondern auch Acknowledgement Informationen für die jeweils zuletzt empfangenen Datenpakete. Während eines PSMP Fensters kann ein Endgerät mehrere Datenpakete senden bzw. empfangen. Werden diese einzeln verschickt, muss zwischen den Datenpaketen eine SIFS Pause eingelegt werden oder optional eine kürzere Sendepause, die RIFS (Reduced Inter Frame Space) genannt wird. Datenpakete können auch mit dem weiter oben beschriebenen Frame Aggregation Verfahren in einem Physical Frame gebündelt werden.

Wie in Abbildung 4.19 gezeigt, kann ein PSMP Fenster auch von mehreren Endgeräten geteilt werden. Ein PSMP Frame am Anfang des Intervalls enthält Informationen für alle Endgeräte zu welchen Zeiten jedes einzelne Endgerät im PSMP Fenster Daten empfangen und senden darf. Der Standard gibt vor, dass PSMP Fenster alle 5 bis 40 Millisekunden eingelegt werden sollen, mit einer Granularität von 5 Millisekunden. Für Voice over IP ist z.B. ein Intervall von 20 Millisekunden interessant, da Sprachcodecs üblicherweise Sprachinformationen über diesen Zeitraum komprimieren und dann in einem kleinen Paket übertragen (vgl. Abbildung 1.34).

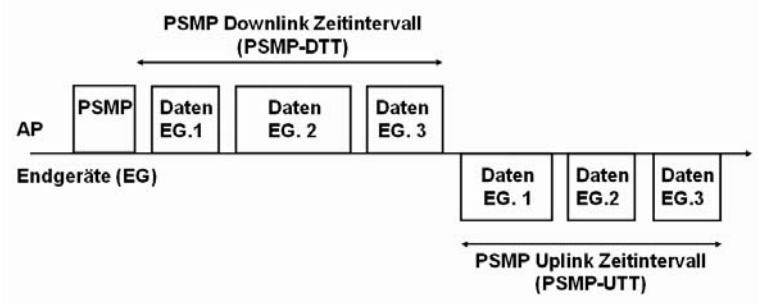

Abb. 4.19: Ein Power Save Multi Poll Fenster (PSMP), in dem mehrere Endgeräte senden und empfangen

Die PSMP Fenster und die für jedes Endgerät vorhandenen Übertragungszeiten sind für eine kontinuierliche und gleich bleibende Übertragung gedacht und so optimiert, dass bei konstanter Nutzung möglichst wenig Bandbreite ungenutzt bleibt. Nun kann es jedoch sein, dass ein Endgerät kurzzeitig mehr Bandbreite benötigt oder ein Paket aufgrund eines Übertragungsfehlers erneut übertragen werden muss. Dies kann dann nicht im normalen Zeitfenster geschehen, da für solche zusätzlichen Übertragungen kein Platz vorhanden ist. Für zusätzliche Uplink Kapazität kann das Endgerät deshalb dem Access Point über ein Flag im MAC Header mitteilen, dass zusätzliche Bandbreite benötigt wird. Dies ist ähnlich der Funktion des ‚Happy' Bit bei HSUPA (vgl. Kapitel 3.11.1). Der Access Point hat dann die Möglichkeit, an das nächste PSMP Fenster ein weiteres PSMP Fenster direkt anzuhängen und teilt dies im PSMP Frame, das jedem PSMP Fenster voransteht, den Endgeräten entsprechend mit. Tritt ein Übertragungsfehler in Uplink Richtung auf, signalisiert dies der Access Point dem Endgerät durch ein negatives Acknowledgement im nächsten PSMP Downlink Abschnitt und fügt ebenfalls ein PSMP Fenster an.

Weitere Funktionalitäten, die im Zusammenhang mit PSMP interessant sind, ist das Versenden eines Datenpakets ohne anschließendes Acknowledgement. Dies ist z.B. bei VoIP sinnvoll, da es evtl. besser ist ein Datenpaket zu verwerfen, anstatt einen großen Jitter Buffer vorzuhalten. Außerdem hat der Access Point die Möglichkeit, Endgeräten zu signalisieren, dass in diesem Netzwerk nur PSMP taugliche Geräte zugelassen sind. Damit können mehrere Access Points z.B. in einem Büro verteilt werden, von denen dann einer exklusiv spezielle Endgeräte wie z.B. VoIP Telefone bedient, während andere Access Points sich um Notebooks und andere Endgeräte kümmern.

MIMO Power Save Modi

Eine weitere Stromsparfunktion wurde im 802.11n Standard für MIMO Spatial Multiplexing (SM) fähige Endgeräte eingeführt. Auch wenn keine Daten übertragen werden, müssen diese im Standardmodus ständig mehrere Empfänger bereithalten, da der Access Point ihnen ja zu jeder Zeit ein Paket schicken kann. Um die Stromaufnahme für batteriebetriebene Geräte zu reduzieren, wurden zwei optionale MIMO SM Power Save Modi spezifiziert. Im statischen Modus signalisiert ein Endgerät einem Access Point über eine „SM Power Save Management Action Frame" Nachricht, wenn es den SM Power Save Modus an- oder abschaltet. Zusätz-

lich gibt es auch SM Power Save Bits im HT Capabilities Parameter, die ein Endgerät während der Association Prozedur verwenden kann, um dem Access Point mitzuteilen, dass es aktuell nur Single Stream Übertragungen zulässt. Des Weiteren gibt es auch einen dynamischen SM Power Save Modus. Hier schaltet das Endgerät alle zusätzlichen Empfänger ab und arbeitet im Single Stream Modus. Das Endgerät aktiviert seinen MIMO Modus wieder automatisch, sobald der Access Point das Endgerät mit einem Paket wie z.B. eine RTS/CTS Sequenz im Single Stream Modus adressiert. Alle nachfolgenden Frames schickt der Access Point ohne weitere Vereinbarung dann mit mehreren MIMO Streams.

MIMO Spatial Multiplexing steigert zwar die Datenrate, nicht jedoch die Reichweite eines Netzwerkes. Deshalb gibt es im Standard optional weitere Möglichkeiten, die zusätzlichen Sende- und Empfangseinheiten (Transciever) statt für erhöhten Durchsatz für eine bessere Reicherweite zu nutzen.

MIMO Beamforming

Eines dieser Verfahren ist das MIMO Beamforming. Hier wird über alle Transciever der gleiche Datenstrom gesendet. Durch geschickte Kombination der Sendeleistung und zeitlichen Versatz der Datenströme kann jedoch eine Richtwirkung erzeugt werden. Somit wird die gesamte Übertragungsleistung nicht gleichmäßig im Raum verteilt, sondern gezielt in der Umgebung des Empfängers konzentriert. Damit Beamforming funktioniert, benötigt der Sender Rückmeldungen vom Empfänger, um den Strahl (Beam) in die richtige Richtung zu dirigieren. Somit müssen sowohl der Sender als auch der Empfänger MIMO Beamforming unterstützten.

MIMO Diversity: Space Time Block Code (STBC)

Statt Beamforming kann die Reichweite eines Netzwerkes auch mit einem Verfahren gesteigert werden, das ein mathematisches Verfahren namens Space Time Block Code (STBC) nutzt. Unterstützen Sender und Empfänger diesen Modus, wird z.B. in einer 2x2 MIMO Konfiguration auch hier ein einzelner Datenstrom getrennt über zwei Pfade übertragen. STBC kodiert jedoch den Datenstrom für jeden Transmitter unterschiedlich und in einer Weise, dass diese zueinander orthogonal sind. Auf der Empfängerseite erhöht dies den Signal- zu Rauschabstand, was wiederum dabei hilft, die Signalstärke und damit den Durchsatz bei weiter entfernten Endgeräten zu steigern.

Antenna Selection und MRC

Unterstützt eine Gegenstelle keine der optionalen MIMO Funktionalitäten, gibt es für einen Empfänger noch andere optionale Möglichkeiten, die Signalqualität zu steigern. Hat das Endgerät mehrere Antennen, kann es untersuchen, mit welcher Antenne

Daten am besten empfangen werden und verwendet dann diese. In der Praxis kann dies durchaus eine deutliche Signalverbesserung für weiter entfernte Endgeräte bedeuten. Dies lässt sich anschaulich bei Endgeräten mit nur einer Antenne und schlechten Empfangsbedingungen nachvollziehen. Hier reicht bei schlechten Empfangsbedingungen oft schon das manuelle Versetzen der Antenne um wenige Zentimeter um den Empfang zu verbessern. Diese Funktionalität ist nicht 802.11n spezifisch sondern wird auch schon bei 802.11g Access Points eingesetzt, die mehrere Antennen haben. Ein etwas aufwändigeres Verfahren ist das Maximum Ratio Combining (MRC). Hier untersucht der Empfänger den eingehenden Datenstrom auf mehreren Receivern und kombiniert die zwei getrennt empfangenen Signale, um so den Signal zu Rauschabstand zu verbessern.

Welche MIMO Art für welchen Zweck

Für Endgeräte die sich näher am Access Point befinden, ist natürlich das zuerst beschriebene MIMO Spatial Multiplexing das Mittel der Wahl, um die Übertragungsgeschwindigkeit zu steigern. Die Transciever werden dann genutzt, um mehrere Datenströme parallel zu übertragen. Bei weniger günstigen Übertragungsbedingungen sind Beamforming und STBC das bessere Mittel, so sie denn von Sender und Empfänger unterstützt werden. Die damit erreichbaren Datenraten sind natürlich geringer als mit MIMO Spatial Multiplexing, da nur ein Datenstrom verwendet wird. Welches der Verfahren für eine Übertragung angewandt wird, muss der Sender selbständig anhand der Übertragungssituation entscheiden, sowie mit dem Wissen, welche MIMO Arten die Gegenstelle unterstützt. Bei mehreren Endgeräten im Netzwerk können alle Verfahren nebeneinander koexistieren. Ein Gerät mit guten Empfangsbedingungen wird dann vom Access Point mit Spatial Multiplexing bedient, während das nächste Paket an ein weiter entferntes Gerät mit STBC kodiert wird.

An dieser Stelle sei angemerkt, dass in Zukunft auch andere Technologien wie 802.16e WIMAX, HSPA+ und 3GPP LTE alle beschriebenen MIMO Arten unterstützen.

MCS Feedback

Eine weitere optionale Funktionalität, die in der 802.11n Arbeitsgruppe definiert wurde, ist das Modulation and Coding Scheme (MCS) Feedback. Ohne dieses Verfahren müssen Sender anhand der Signalstärke des zuletzt vom Empfänger erhaltenen Paketes oder dessen verwendeten MCS entscheiden, welche Modulation und Kodierung sie für die Übertragung des eigenen Paketes verwenden. Dies ist in der Praxis nicht optimal und führt dazu, dass unter Umständen ein MCS verwendet wird, der die Emp-

fangsbedingungen nicht optimal ausnutzt, sprich die Daten zu langsam überträgt. Mit MCS Feedback wurde eine Möglichkeit geschaffen, dass ein Sender von einem Empfänger Feedback über seine Empfangseigenschaften anfordern kann. Der Empfänger liefert dann Informationen im MAC Header in darauf folgenden Übertragungen implizit zurück.

Klassifizierung in der Praxis

In der Praxis wird es in Zukunft aufgrund der vielen möglichen Optionen schwierig werden, allein anhand der Bezeichnung ‚802.11n' die Leistungsfähigkeit und Effizienz eines Endgerätes zu beurteilen. Es bleibt deshalb abzuwarten, ob die Industrie darauf entsprechend reagiert und für Anwender klare Vergleichskategorien schaffen wird, um sich bei der Anschaffung gezielt für ein Gerät mit bestimmten Eigenschaften entscheiden zu können.

4.7 Wireless LAN Sicherheit

Sicherheit ist bei Wireless LAN vor allem deswegen ein sehr heftig diskutiertes Thema, da die normalen Sicherheitseinstellungen und Verfahren den Anwender nur ungenügend schützen. Im Auslieferungszustand ist die Verschlüsselung in so gut wie jedem Access Point deaktiviert. Wird die Verschlüsselung nicht explizit konfiguriert, kann jedes WLAN fähige Endgerät diesen Access Point ohne vorherige Erlaubnis des Besitzers verwenden. Diese Konfiguration eignet sich vor allem für öffentliche Hotspots, da hier stets wechselnde Teilnehmer einen Hotspot verwenden. Da die Daten aber unverschlüsselt übertragen werden, können diese sehr leicht von anderen abgehört werden. Noch bedenklicher ist diese Konfiguration für private Heimnetzwerke, die über den Access Point einen Zugang zum Internet herstellen. Wurde die Verschlüsselung nicht explizit konfiguriert, können Nachbarn ohne Wissen des Besitzers seine Internetverbindung nutzen. Außerdem ist es anderen möglich, den Datenverkehr abzuhören und so z.B. Passwörter etc. auszuspähen. Da auf alle Rechner des Netzwerks Zugriff besteht, können Angreifer auch direkt Schwachstellen der Betriebssysteme ausnutzen, um Daten auf den Rechnern ausspähen. Wie real diese Möglichkeit ist, zeigte eine Testfahrt. Von zwölf innerhalb von wenigen Minuten gefundenen Access Points wurden fünf ohne Verschlüsselung betrieben.

4.7.1 Wired Equivalent Privacy (WEP)

WEP Verschlüsselung und dessen Schwächen

Um WLAN Netzwerke vor unbefugter Nutzung und die Datenübertragung vor dem Abhören zu schützen, ist die Wired Equivalent Privacy (WEP) Verschlüsselung Teil des 802.11b, g und a Standards. Sie basiert ähnlich wie bei GSM und UMTS auf einem Stream Ciphering Algorithmus (vgl. Abb. 1.37), mit dem die Originaldaten mit einer Ciphersequenz verschlüsselt werden. Die Ciphersequenz wird für jedes Paket mit Hilfe eines Keys und eines Initial Vectors (IV) berechnet. Der Initial Vector ändert sich für jeden Frame und erzeugt somit wechselnde Ciphering Keys. WEP verwendet jedoch im Unterschied zu GSM oder UMTS nur einen Key für alle Anwender. Dies ist das erste große Problem vor allem bei der Verwendung von WLAN Netzwerken in Firmen. Da jeder Anwender den gleichen Schlüssel verwendet und diesen manuell in seinem Endgerät konfigurieren muss, kann dieser nicht geheim gehalten werden. Bei GSM oder UTMS hingegen ist ein individueller Schlüssel in der SIM Karte jedes Teilnehmers gespeichert und kann von dort nicht ausgelesen werden.

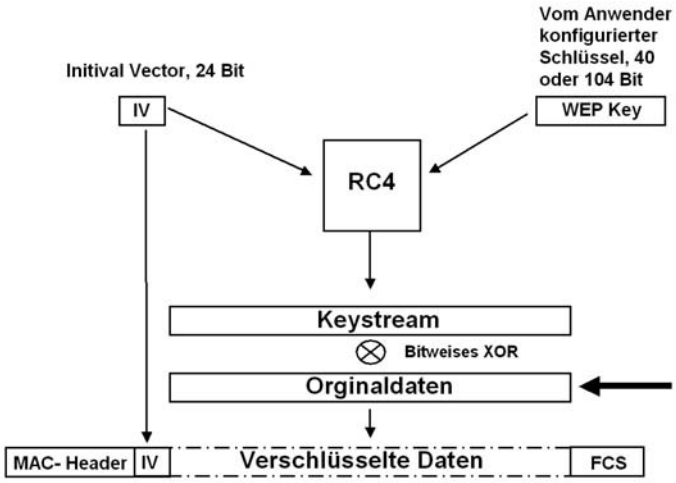

Abb. 4.20: WEP Verschlüsselung

Ein noch schwerwiegenderes Problem ist jedoch, dass der Beginn des verschlüsselten Frames immer die gleiche und somit bekannte Bytefolge des LLC Headers enthält. In Kombination mit bestimmten, im Klartext übertragenen IVs ist es für einen Angreifer möglich, den Schlüssel durch Analyse von etwa 5-6 Millionen

Datenpaketen zu berechnen. Die Länge des WEP Schlüssels spielt dabei nur eine untergeordnete Rolle. Tools, die dies automatisch erledigen, sind im Internet frei erhältlich, der Angreifer muss sich also lediglich in Reichweite des Netzwerkes aufhalten. Die Zahl der benötigten Pakete hört sich zunächst sehr groß an. Nimmt man für eine grobe Abschätzung jedoch an, dass jedes dieser 5 Millionen Datenpakete 300 Bytes an Nutzdaten enthält, so kann der Schlüssel durch Abhören von 5.000.000 Pakete * 0.3 kByte = 1.5 GByte an Daten ermittelt werden. Je nach Last des Netzwerkes lies sich somit der Schlüssel mit ersten Programmen in einem Zeitraum von mehreren Wochen bis hin zu wenigen Stunden errechnen. Im Laufe er Zeit wurden die automatisierten Tools zum Errechnen des Schlüssels immer ausgefeilter. Mittlerweile können diese in bestimmten Fällen durch erneutes Senden von Paketen, die zuvor abgehört wurden, Antwortpakete erzeugen. Somit sind diese Tools nicht mehr auf passives Abhören angewiesen, sondern erzeugen die Datenpakete unter Mithilfe des Netzwerkes für ihre Auswertung quasi selber. Somit ist es möglich, unabhängig von der Verkehrslast die Verschlüsselung in sehr kurzer Zeit zu überwinden.

Hide SSID und MAC-Adressen Filterung

Um die Sicherheit eines WLAN Netzwerkes zu erhöhen, bieten heute viele Access Points zwei weitere Sicherheitsmerkmale an: Durch Aktivieren der „Hide SSID“ Funktion sendet der Access Point Beacon Frames mit leerem SSID Feld. Dadurch ist der Access Point nur für Anwender sichtbar, die bei der manuellen Konfiguration ihres Endgeräts die korrekte SSID angeben. Per MAC-Adressen Filter lässt sich bei vielen Access Points außerdem festlegen, welche Endgeräte sich anmelden dürfen. Für Angreifer, die wie oben beschrieben, über das Wissen und die Möglichkeiten verfügen, den WEP Schlüssel zu errechnen, stellen diese Funktionalitäten aber keine großen Hürden da. Zwar wird die SSID durch die „Hide SSID“ Funktion aus den Beacon Frames entfernt, bei der Association Prozedur wird die SSID aber weiterhin unverschlüsselt übertragen. Auch die MAC-Adresse einer WLAN Karte kann von einem Angreifer ohne viel Mühe auf einen Wert geändert werden, die zuvor im Netzwerk beobachtet wurde.

4.7.2 WPA und WPA2 Personal Mode Authentifizierung

Aufgrund der oben beschriebenen Sicherheitsprobleme wurde von der IEEE 802.11i Arbeitsgruppe der 802.1x Standard erarbeitet. Dieser Standard bietet eine Lösung für sämtliche bisher be-

kannt gewordenen Sicherheitsprobleme. Da sich jedoch die Verabschiedung des Standards beträchtlich hinauszögerte, wurde die Industrie ihrerseits selbst aktiv und entwickelte in der Wifi Alliance die Wireless Protected Access (WPA) Spezifikation. WPA enthält alle wichtigen Funktionalitäten von 802.11i und wurde so spezifiziert, dass die neuen Funktionen auch mit Hardware funktionieren, die ursprünglich nur für WEP Verschlüsselung entwickelt wurde.

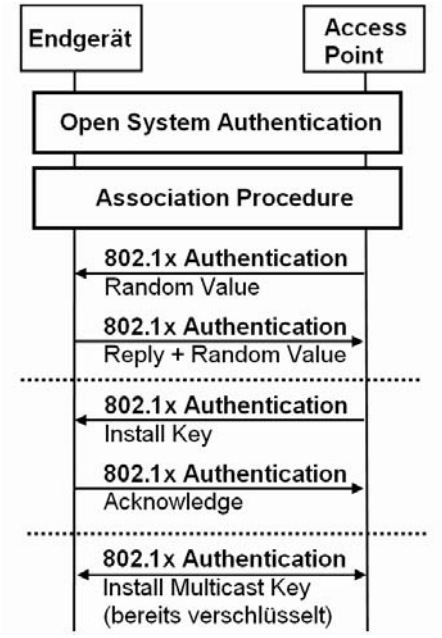

Abb. 4.21: WPA-PSK Authentifizierung und Schlüsselaustausch

Die Schwächen von WEP werden von WPA durch verbesserte Authentifizierung während der Verbindungsaufnahme und eine neue Verschlüsselung gelöst. Wie in Abbildung 4.8 gezeigt, meldet sich ein Teilnehmer bei einem Netzwerk durch eine Pseudo-Authentifizierung und eine Association Prozedur am Netzwerk an. Bei WPA folgt darauf eine weitere Authentifizierung und danach eine sichere Schlüsselübergabe für die Chiffrierung der Nutzdaten. Die erste Authentifizierung ist damit überflüssig, wurde aber dennoch aus Kompatibilitätsgründen beibehalten. Um Endgeräten mitzuteilen, dass ein Netzwerk WPA statt WEP unterstützt, enthalten Beacon Frames einen zusätzlichen WPA Parame-

ter. Dieser informiert Endgeräte, dass ein zusätzlicher Authentifizierungsschritt und Schlüsselaustauch nach der Association Prozedur notewendig ist. Der WPA Parameter enthält auch zusätzliche Informationen über den für die Authentifizierung und Verschlüsselung zu verwendenden Algorithmus. Erste WPA Endgeräte verwendeten zunächst nur TKIP (Temporal Key Integrity Protocol) für die Verschlüsselung. Neuere Endgeräte unterstützen auch AES (Advanced Encryption Standard), welcher bei WPA2 fest vorgeschrieben ist. Weitere Details dazu folgen im Laufe dieses Kapitels.

Abbildung 4.21 zeigt die vier neu hinzugekommenen Schritte für die WPA Pre-Shared Key (PSK) Methode um Endgeräte gegenüber dem Access Point zu authentifizieren und umgekehrt. Pre-Shared Key bedeutet in diesem Zusammenhang, dass im Access Point und im Endgerät das gleiche Passwort hinterlegt wurde. Außerdem einigen sich Endgeräte und Access Point während dieses Prozesses auf ein gemeinsames Schlüsselpaar für die Chiffrierung der Nutzdaten, die Session Keys. In der ersten Nachricht sendet der Access Point eine Zufallszahl an das Endgerät. Dieses verwendet dann die Zufallszahl und das gemeinsame Passwort (Pre-Shared Key), um eine Antwort zu generieren. Das Passwort hat eine Länge von 8 bis 64 Zeichen. Die Antwort wird dann zusammen mit einer weiteren Zufallszahl zurück an den Access Point geschickt. Der Access Point vergleicht im nächsten Schritt die Antwort mit der zuvor selber berechneten Antwort. Diese können nur identisch sein, wenn beide Seiten für die Berechnung der Antwort das gleiche Passwort verwendet haben. Stimmen die Antworten überein, ist das Endgerät authentifiziert. Im nächsten Schritt generiert der Access Point einen Sitzungsschlüssel (Session Key), welcher mit dem gemeinsamen Passwort verschlüsselt wird und zum Endgerät geschickt wird. Das Endgerät entschlüsselt den Sitzungsschlüssel mit dem gemeinsamen Passwort und bestätigt dem Access Point den korrekten Empfang der Nachricht. Diese Bestätigung aktiviert auch implizit die Verschlüsselung in beiden Richtungen. In einem letzten Schritt teilt dann der Access Point dem Endgerät noch den Schlüssel für die Dechiffrierung von Broadcast Frames mit. Diese Nachricht ist bereits verschlüsselt. Während der Sitzungsschlüssel für jedes einzelne Endgerät individuell ist, ist der Broadcast Schlüssel für alle Endgeräte gleich, da ein Broadcast Paket von allen Endgeräten gleichzeitig entschlüsselt werden muss.

Der Vorteil der Verwendung von individuell generierten Sitzungsschlüsseln gegenüber der direkten Verwendung des Pass-

worts für die Verschlüsselung ist, dass dieser während einer laufenden Verbindung geändert werden kann. Dies verhindert so genannte „Brute Force Attacken“, die versuchen, den Schlüssel durch ausprobieren zu erraten. Ein typischer Wert für das Austauschen des Sitzungsschlüssels ist eine Stunde.

4.7.3 WPA und WPA2 Enterprise Mode Authentifizierung

Zusätzlich zur WPA-PSK Authentifizierung, für die ein gemeinsamer Schlüssel (Pre-Shared Key) im Access Point und in den Endgeräten gespeichert werden muss, gibt es bei WPA und WPA2 auch einen Enterprise Mode für Firmen. Hier werden die Passwörter in einem zentralen Authentifizierungsserver, wie in Abbildung 4.22 gezeigt, gespeichert. Dies ermöglicht es Firmen, mehrere Access Points zu betreiben, ohne die Authentifizierungsinformationen in jedem einzelnen Access Point separat vorrätig zu halten. Außerdem ermöglicht diese Methode, Nutzer individuell zu authentifizieren. Somit kann für jeden Benutzer individuell eine Zugangsberechtigung erteilt und auch wieder entzogen werden. Die zwei wichtigsten Authentifizierungsserver sind RADIUS (Remote Authentical Dial In User Service), das normalerweise auf einem Unix Server läuft, oder der Microsoft Authentication Service auf einem Windows Server.

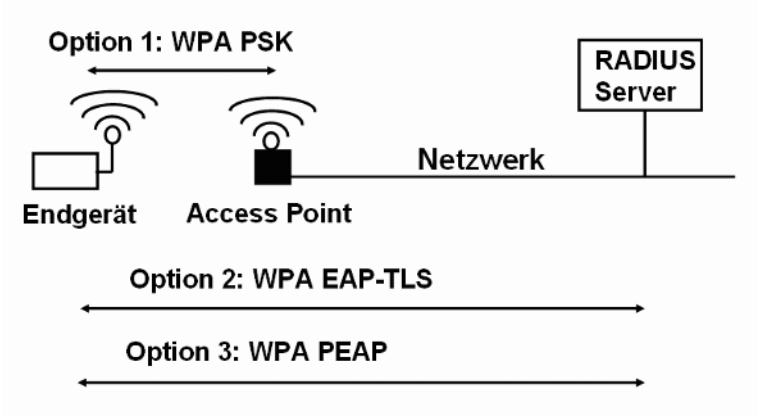

Abb. 4.22: Drei WPA Authentifizierungsmethoden

Aufgrund der verschiedenen Authentifizierungsserver kennt WPA mehrere Authentifizierungsprotokolle. Diese werden Extensible

Authentication Protocols (EAP) genannt. Ein sehr häufig genutztes EAP Protocol ist EAP Transport Layer Security (EAP-TLS) von Haverinen and Salovei, das in RFC 4186 beschrieben ist. Dieses Protokoll verwendet Zertifikate, die im Endgerät und Authentifizierungsserver gespeichert werden. Der wichtigste Teil des Zertifikats sind die öffentlichen Schlüssel (Public Keys) des Endgeräts und des Authentifizierungsservers. Diese Schlüssel werden verwendet, um die Sitzungsschlüssel (Session Keys) zu chiffrieren, die zwischen Endgerät und Netzwerk ausgetauscht werden. Wie zuvor beschrieben, werden dann die Sitzungsschlüssel verwendet, um die Nutzdaten zwischen Access Point und Endgerät zu verschlüsseln.

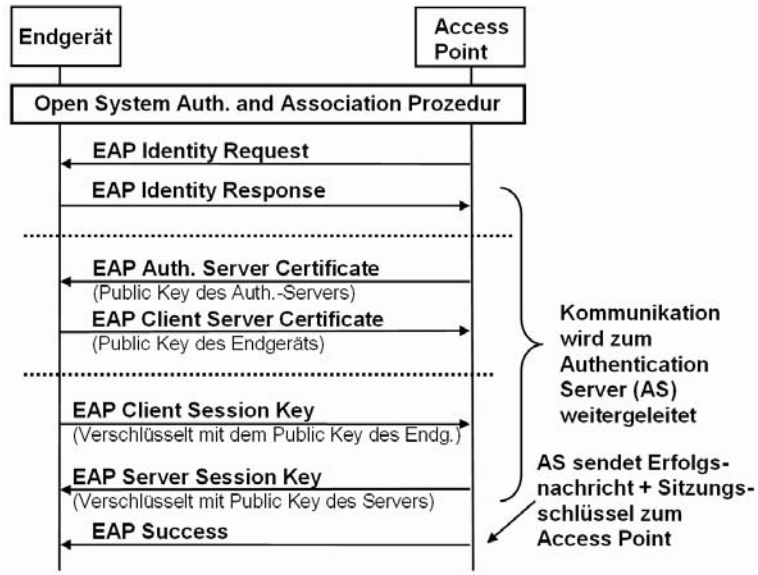

Abb. 4.23: EAP-TLS Authentifizierung

Nachdem der Sitzungsschlüssel mit dem öffentlichen Schlüssel chiffriert wurde, kann dieser nur mit dem privaten Schlüssel (Private Key) der Gegenstelle wieder dechiffriert werden. Dieser Vorgang wird in Abbildung 4.23 gezeigt. Da die privaten Schlüssel niemals zwischen Endgerät und Netzwerk ausgetauscht werden, kann durch Abhören der Verbindung der Session Key nicht kompromitiert werden. Somit kann auch die Übertragung der Nutzdaten später nicht von einem Angreifer dechiffriert werden. Einziger Nachteil der Nutzung von Zertifikaten ist der Umstand,

dass diese einmalig auf dem Endgerät installiert werden müssen. Dies ist etwas komplizierter als einfach ein Passwort zu vergeben, jedoch wesentlich sicherer, wenn die Zertifikate korrekt verteilt und installiert werden. Nicht gezeigt wird in Abbildung 4.23 die Übertragung des Sitzungsschlüssels für Broadcast Pakete, die unmittelbar nach der erfolgreichen Authentifizierung übertragen werden.

In Abbildung 4.23 ist außerdem zu sehen, dass der Access Point in der Authentifizierungsphase nur den Datenaustausch mit dem Authenticationserver zulässt. Erst nachdem die Authentifizierung erfolgreich abgeschlossen wurde, und nachdem der Server dem Access Point die Freigabe erteilt hat, erlaubt der Access Point dem Endgerät freien Zugriff auf das Netzwerk. Die Nutzdaten sind dann über die Luftschnittstelle schon verschlüsselt. Üblicherweise ist das erste Nutzdatenpaket eine DHCP (Dynamic Host Configuraiton Protocol) Anforderung, um eine IP Adresse zu erhalten.

Des Weiteren sei angemerkt, dass die EAP-TLS Authentifizierung große Ähnlichkeit zu TLS und SSL (Secure Socket Layer) hat. Diese Protokolle werden von HTTPS (Secure HTTP) für die Authentifizierung und Generierung von Sitzungsschlüsseln für eine sichere Verbindung zwischen einem Web Server und einem Webbrowser verwendet. Der Hauptunterschied zwischen EAP-TLS und der HTTP TLS Authentifizierungsprozedur ist, dass bei EAP-TLS eine gegenseitige Authentifizierung stattfindet, während sich bei HTTPS TLS nur der Web Server gegenüber dem Webbrowser authentifizieren muss. Aus diesem Grund benötigt der Webbrowser auch kein Zertifikat für den Aufbau einer verschlüsselten Verbindung.

Eine mögliche Alternative zu EAP-TLS ist Protected EAP (PEAP). Während dieses Protokoll seltener verwendet wird, hat PEAP jedoch den Vorteil dass auf der Nutzerseite ein Passwort statt eines Zertifikates verwendet werden kann.

4.7.4 Authentifizierung mit EAP-SIM

Eine wachsende Anzahl von GSM und UMTS Endgeräten haben heute auch ein integriertes Wifi Modul. Dieses Modul kann dann sowohl im heimischen Wifi Netzwerk, im Büro, oder auch über Hotspots für einen schnellen und kostengünstigen Zugang ins Internet sorgen. Mobilfunkbetreiber, die auch ein Wifi Hotspot Netzwerk betreiben, stehen nun vor dem Problem, wie sie ihre Kunden auch in ihrem Wifi Netzwerk authentifizieren können.

Zwar gibt es hier heute auf dem Markt schon einige Lösungen, die jedoch alle eine Interaktion mit dem Nutzer vorsehen. Da dies umständlich und für viele Applikationen hinderlich ist, wurde das EAP-SIM Protokoll in RFC 4186 spezifiziert. Bei dieser Art der Authentifizierung ist wie bei GSM oder UMTS keine Interaktion mit dem Nutzer nötig, da alle Informationen von der SIM Karte abgefragt werden.

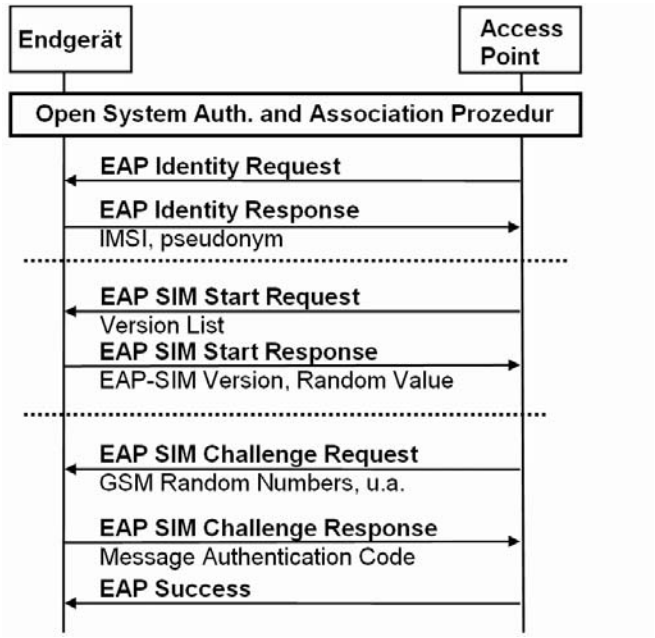

Abb. 4.24: EAP-SIM Authentifizierung

EAP-SIM verwendet die gleiche Authentifizierungsmethode wie bereits im Kapitel über WPA Personal und Enterprise Authentifizierung beschrieben. Abbildung 4.24 zeigt die Nachrichten, die während der Authentifizierung zwischen dem mobilen Endgerät und dem Authenifizierungsserver über einen EAP-SIM kompatiblen Access Point übertragen werden. Nach einer Wifi Open System Authentifizierung und der Association Prozedur startet das Netzwerk die EAP Prozedur durch Senden einer EAP Identiy Request Nachricht, auf die das mobile Endgerät mit einer EAP Identity Response Nachricht antworten muss. Die Identität die in dieser Nachricht zurückgegeben wird besteht aus einem Identity Type Identifier, der IMSI aus der SIM Karte und einem spezifi-

schen Postfix (Anhang) des Mobilfunkbetreibers. Alternativ kann das mobile Endgerät auch eine temporäre Identität (Pseudonym) an das Netzwerk schicken, das während einer früheren Authentifizierung ausgehandelt wurde. Das Pseudonym hat die gleiche Aufgabe wie die TMSI (Temporary Mobile Subscriber Identity) in GSM und UMTS Netzwerken, nämlich der Verschleierung der Identität gegenüber Abhörversuchen auf der Luftschnittstelle, hat jedoch ein anderes Format.

Im nächsten Schritt sendet dann das Netzwerk eine EAP-SIM Start Request Nachricht. Diese enthält Informationen über die unterstützten EAP-SIM Authentifizierungsalgorithmen. Das mobile Endgerät wählt dann einen dieser Algorithmen aus und antwortet mit einer EAP-SIM Start Response Nachricht. Diese enthält eine Zufallszahl, die später im Netzwerk zusammen mit dem geheimen GSM Schlüssel Kc für diverse Berechnungen verwendet wird. Da der geheime GSM Schlüssel Kc sowohl dem Netzwerk als auch der SIM Karte bekannt ist, kann sich auf diese Weise nicht nur das Endgerät gegenüber dem Netzwerk authentifizieren, sondern das Netzwerk auch gegenüber dem Endgerät.

An diesem Punkt verwendet der Authentifizierungsserver die IMSI des Teilnehmers, um vom Home Location Register (HLR) / Authentication Center (AuC) wie im Kapitel 1.6.4 beschrieben Authentication Triplets anzufordern. Das HLR/AuC antwortet auf diese Anfrage mit zwei oder drei Triplets, die jeweils eine Zufallszahl und Kc Chiffrierungsschlüssel enthalten. Diese werden dann verwendet, um die EAP-SIM Sitzungsschlüssel und andere Parameter für den Authentifizierungsprozess zu erzeugen. Diese werden dann in verschlüsselter Form zusammen mit den zwei oder drei GSM Zufallszahlen im Klartext zum mobilen Endgerät in der SIM Challenge Request Nachricht geschickt.

Das Endgerät schickt nach Empfang der Nachricht die GSM Zufallszahlen weiter zur SIM Karte. Die SIM Karte erzeugt mit diesen die GSM Signed Response (SRES) und die GSM Chiffrierschlüssel (Kc), die im folgenden verwendet werden, um die zuvor erhaltenen EAP-SIM Parameter zu entschlüsseln. Stimmt nach der Entschlüsselung die Signed Response vom Netzwerk mit der der SIM Karte überein, ist das Netzwerk authentifiziert und das Endgerät kann eine korrekte Antwort zurückschicken. Im Netzwerk wird diese Nachricht dann verifiziert und im Erfolgsfall eine EAP Success Nachricht an das Endgerät zurückgeschickt. Ab diesem Zeitpunkt hat das Endgerät dann Zugriff auf das Netzwerk.

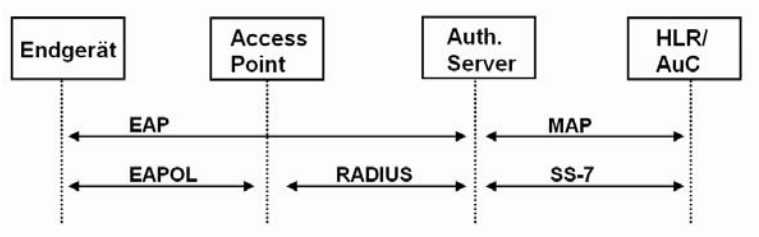

Abb. 4.25: An der EAP-SIM Authentifizierung beteiligte Komponenten

Abbildung 4.25 zeigt die bei der EAP-SIM Authentifizierung beteiligten Komponenten und Protokolle. Links ist das mobile Endgerät dargestellt, das seine EAP Nachrichten über das EAPOL Protokoll sendet. Für die Kommunikation zwischen Access Point und dem Authentifizierungsserver wird das RADIUS (Remote Authentication Dial In User Service) Protokoll verwendet. Der Authentifizierungsserver seinerseits kommuniziert mit dem HLR/AuC über das SS-7 Signalisierungsnetzwerk und dem MAP (Mobile Application Part) Protokoll.

4.7.5 Verschlüsselung mit WPA und WPA2

Um die Verschlüsselung gegenüber WEP zu verbessern, führt WPA das Temporal Key Integrity Protocol (TKIP) ein. Bei WEP wurde ein 24 Bit Initial Vector (IV), der WEP Schlüssel und der RC-4 Algorithmus verwendet, um eine Verschlüsselungssequenz für jedes Paket zu generieren (vgl. Abbildung 4.16). TKIP verwendet nun einen 48 Bit Initial Vector, einen Master Key und den RC-4 Algorithmus, um die Verschlüsselungssequenz für jedes Paket zu erzeugen. Dieses Verfahren ist wesentlich sicherer, da der Initial Vector verlängert wurde und der Master Key ständig (z.B. einmal pro Stunde) zwischen Endgerät und Access Point neu ausgehandelt wird.

Die von WPA verwendete Verschlüsselung entspricht nicht ganz den Anforderungen des 802.11i Standards, wird jedoch trotzdem als sicher angesehen. Vorteil des Verfahrens ist, dass TKIP mit Hardware kompatibel ist, die nur für den Einsatz mit WEP vorgesehen war.

Um Attacken zu verhindern, die eine Schwäche ausnützen, die beim Wiedereinspielen von zuvor abgehörten und leicht veränderten Paketen auftreten, wird der Initial Vector bei jedem Paket

um 1 erhört. WPA kompatible Gerät ignorieren Pakete mit schon verwendeten IV's und sind somit gegen diese Angriffsart immun.

In der Theorie können Access Points gleichzeitig WPA und WEP Endgeräte unterstützen. In der Praxis bieten dies jedoch nur wenige Access Points an. Dies ist auch sinnvoll, da dies die Sicherheit des Systems stark reduzieren würde.

Als zusätzliche Sicherheit führt TKIP auch einen Message Integrity Code (MIC) für jedes Datenpaket ein. Der Prozess für die Erzeugung des MIC wird manchmal auch als ‚Michael' bezeichnet. Im Unterschied zur CRC Prüfsumme, die weiterhin Teil jedes Datenpakets ist, ist wie folgt: Die CRC Prüfsumme wird aus dem Inhalt des Pakets mit einem öffentlich bekannten Algorithmus erzeugt. Der Empfänger kann somit prüfen, ob der Inhalt eines Pakets durch einen Übertragungsfehler geändert wurde. Da der Eingangsparameter und Algorithmus bekannt sind, ist die Prüfsumme jedoch nicht geeignet um zu überprüfen, ob das Paket gezielt durch einen Angreifer verändert wurde, da der Angreifer die Prüfsumme selber ändern könnte. Der MIC andererseits wird ebenfalls mit einem bekannten Algorithmus berechnet, hat jedoch als Eingangsparameter sowohl die Nutzdaten, als auch einen Message Integrity Key, der bei der TKIP Authentifizierung zusammen mit dem Sitzungsschlüssel erzeugt wurde. Einem Angreifer ist es somit nicht möglich, einen korrekten MIC zu berechnen und kann somit auch nicht den Inhalt des Pakets verändern. Bleibt anzumerken, dass sowohl der CRC als auch der MIC im verschlüsselten Teil des Datenpakets untergebracht sind. Um also die CRC Prüfsumme oder den MIC zu verändern, müsste ein Angreifer also zunächst einmal die RC-4 Verschlüsselung in Kombination mit den WPA Sicherheitsvorkehrungen überwinden.

Tritt während der Übertragung ein Fehler auf, sind beim Empfänger sowohl die MIC als auch die CRC Prüfsumme falsch. Der Empfänger eines Datenpaketes kann somit zwischen Übertragungsfehlern und Angriffen auf die Datenintegrität unterscheiden. WPA schreibt vor, dass Endgeräte die mehr als einen Frame pro Minute mit falschem MIC und korrektem CRC empfangen sich vom Netzwerk trennen müssen und danach eine Minute warten, bis sie sich wieder am Netzwerk anmelden. Auf diese Weise werden Attacken auf die Nutzdatenintegrität effektiv verhindert.

Nach der Verabschiedung des 802.11i Standards passte die Wifi Alliance den WPA Zertifizierungsprozess entsprechend an. WPA2

ist eine Implementierung des 802.11i Standards und ist Rückwärtskompatibel zu WPA. Das bedeutet, dass ein WPA2 zertifizierter Access Point auch ‚nur' WPA fähige Endgeräte unterstützt. WPA2 Access Points können auch ältere WEP Endgeräte unterstützen, wenn WPA/WPA2 deaktiviert wird. Zusätzlich zum TKIP Algorithmus, der mit WPA eingeführt wurde, unterstützt WPA2 nun auch die stärkere AES (Advanced Encryption Standard) Verschlüsselung. Wie bei WPA gibt es auch bei WPA2 in zwei Ausführungen: Ist ein Gerät für den „Personal Mode" zertifiziert, erlaubt es eine Authentifizierung mit einem Access Point per Pre-Shared Key (PSK) Verfahren. Für Firmen, in denen oftmals mehrere Access Points verwendet werden, sollte ein Access Point „WPA2 Enterprise Mode" zertifiziert sein. Zusätzlich zum PSK Verfahren unterstützen solche Access Points auch das 802.1x Authentifizierungsframework und können mit externen Authentifizierungsservern kommunizieren, wie dies weiter oben beschrieben wurde.

4.8 IEEE 802.11e und WMM – Quality of Service

Innerhalb von nur wenigen Jahren haben Wireless LANs die Kommunikation in Büros, Arbeits- und Wohnzimmer revolutioniert. Anfangs wurden Netzwerke hauptsächlich für Anwendungen wie Web Browsing und Zugriff auf Fileserver verwendet. Diese benötigen hohe Bandbreiten, stellen jedoch sonst nur geringe Anforderungen an das Übertragungsmedium in Punkto Verzögerungszeit und gleich bleibende Bandbreite. Mehr und mehr werden Wireless LANs heute jedoch auch von Anwendungen wie Voice over IP oder Videostreaming verwendet, die zusätzliche Anforderungen an ein Übertragungsmedium stellen. Videostreaming beispielsweise braucht neben einer hohen Bandbreite ebenso wie Voice over IP eine garantierte Mindestbandbreite und garantierte maximale Verzögerungszeiten beim Kanalzugriff, um Bild- und Tonaussetzer zu verhindern. Dies ist mit den bisher vorgestellten Wireless LAN Standards auch problemlos möglich, solange der Datenverkehr das Netzwerk nicht an seine Leistungsgrenzen bringt. Benötigt jedoch z.B. eine Multimediaübertragung schon einen Großteil der vorhandenen Bandbreite, können weitere Endgeräte, die gleichzeitig spontan Daten z.B. von einem Fileserver oder aus dem Internet abrufen, den Datenfluss der Multimedia Anwendung stören. Aus diesem Grund wurde mit IEEE 802.11e dem Wireless LAN Standard eine Quality of Service (QoS) Komponente hinzugefügt. Wie auch bei

anderen Erweiterungen gibt es Teile, die von einem Endgerät unterstützt werden müssen und andere, die nur optional sind.

WMM und 802.11e

Um die Markteinführung von 802.11e zu beschleunigen, wurde von der Wifi Alliance die Wifi Multi-Media (WMM) Spezifikation auf Basis von 802.11e entwickelt. Ist ein Access Point oder ein Endgerät WMM zertifiziert, enthält es alle von WMM vorgeschriebenen Funktionen und ist mit WMM zertifizierten Geräten anderer Hersteller kompatibel. Um sicherzustellen, dass QoS Erweiterungen in Zukunft in den meisten Geräten implementiert werden, schreibt sowohl der IEEE Standard als auch die 802.11n Zertifizierung der Wifi Alliance vor, dass die WMM QoS Erweiterungen bei 802.11n Endgeräten zum Funktionsumfang gehören müssen. Nachfolgend werden deshalb zunächst die von WMM verwendeten 802.11e Funktionalitäten beschrieben und danach optionale Komponenten, die zusätzlich unterstützt werden können.

DCF

Kern der Quality of Service Erweiterungen ist eine Erweiterung der Distributed Co-ordination Function (DCF), die den Zugriff von Endgeräten auf den Übertragungskanal regelt und in Kapitel 4.5.1 beschrieben ist. DCF schreibt vor, dass ein Endgerät vor der Übertragung eines Pakets eine variable Zeit warten muss, bevor es den Funkkanal belegt um somit Kollisionen von mehreren Endgeräten beim Kanalzugriff zu vermeiden. Die Wartezeit kann beim ersten Versuch bei 802.11b und g bis zu 31 Slots zu je 20 Mikrosekunden betragen. Ermittelt wird dieser Wert durch Erzeugen einer Zufallszahl zwischen 1 und 31. Sollte die Übertragung fehlschlagen, vergrößert sich sie Kanalzugriffswartezeit dann auf 63, 127, usw., bis maximal 1023 Slots, was 20 Millisekunden entspricht.

HCF

802.11e erweitert die DCF zur Hybrid Coordination Function (HCF). HCF umfasst zwei neue Kanalzugriffsverfahren, den Enhanced Distributed Channel Access (EDCA) und den HCF Controled Channel Access (HCCA). Außerdem ist HCF rückwärtskompatibel zu DCF, es können sich also gleichzeitig HCF und nicht HCF fähige Endgeräte im Netzwerk befinden. Im folgenden wird nun zunächst das EDCA Verfahren beschrieben, das Grundlage der WMM Spezifikation ist.

EDCA

Statt allen Endgeräten und allen Datenpaketen ein gleich langes Fenster für das Ermitteln der Zufallszahl zu geben, werden vier Quality of Service Klassen mit je einer Warteschlange eingeführt. Jeder QoS Warteschlange werden dann unterschiedliche Wartezeitfenster für Datenpakete beim Kanalzugriff zugeordnet. WMM

definiert je eine Warteschlange für Voice, Video, Background und Best Effort Daten. Jede Klasse hat folgende variablen Parameter:

- Anzahl der Slots die mindestens gewartet werden muss, bevor ein Datenpaket gesendet werden darf (Arbitration Interframe Space Number, AIFSN).
- Kleinstes Contention Window (CWMin), also die Anzahl der Slots, aus denen ein Zufallsgenerator eine Kanalzugriffswartezeit (Backoff) auswählen kann.
- Grösstes Contention Window (CWMax), die maximale Anzahl der Slots aus denen ein Zufallsgenerator eine Wartezeit nach fehlgeschlagenen Übertragungen auswählen kann.
- Transmit Opportunity (TXOP): Maximale Sendezeit. Granularität des Parameters ist 32 Mikrosekunden.
- Admission Control: Zeigt an, ob Endgeräte sich die Verwendung dieser Klasse genehmigen lassen müssen (siehe unten).

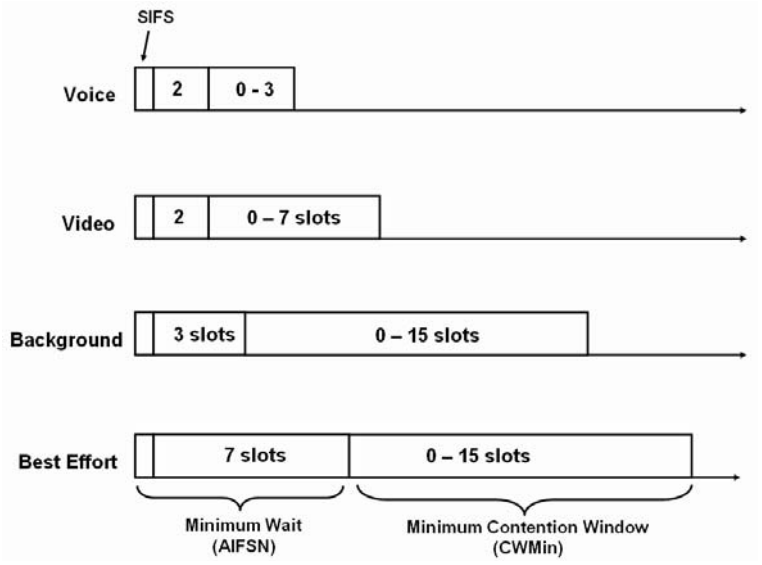

Abb. 4.26: WMM Prioritätsklassen mit beispielhaften Werten für CWMin, CWMax und TXOP

Abbildung 4.26 zeigt, wie diese Werte in der Praxis für die unterschiedlichen Prioritätsklassen gesetzt werden können. Sprachdaten haben sehr hohe Anforderungen an gleich bleibende Verzö-

gerungszeiten. Deshalb ist es in dieser QoS Kategorie wichtig, dass ein Datenpaket bei der Backoff Prozedur bevorzugt wird. Dies wird erreicht, in dem die kleinste Wartezeit (AIFSN) nur 2 Slots und das Contention Window nur maximal 3 Slots lang sind. Die maximale Wartezeit beträgt somit nur 5 Slots. Somit werden diese Datenpakete immer vor Best Effort Daten übertragen, da diese mindestens 7 Slots warten müssen, bevor das Contention Window überhaupt beginnt.

Da die Werte für CWMin, CWMax und TXOP variabel sind und in Access Points von diversen Herstellern auch manuell gesetzt werden können, werden diese über den WMM Parameter in Beacon Frames, sowie in Association- und Probe Response Frames den Endgeräten mitgeteilt.

Diffserv QoS auf Layer 3, QoS Control Field auf Layer 2

Wichtig bei Quality of Service Implementierungen ist auch, dass Applikationen ihre Daten möglichst einfach und von der Art der Netzwerkschnittstelle unabhängig einer QoS Klasse zuordnen können. Bei IP Datenpaketen geschieht dies beispielsweise über das Differentiated Services Feld (DSCP) im IP Header. Wenn von einer Applikation nicht speziell angefordert, ist dieses Feld auf „Default“ gesetzt. Abbildung 4.27 zeigt den IP Header eines Voice over IP Datenpakets, welches dieses Feld auf „Expedited Forwarding“ gesetzt hat. Der Netzwerktreiber der Wireless LAN Karte setzt dieses Feld dann entsprechend in den von 802.11e neu definierten QoS Parameter auf dem Wireless LAN MAC Layer um und stellt das Datenpaket in die Warteschlange für Voice Pakete.

Admission Control

Die Priorisierung von Datenpaketen auf der Luftschnittstelle wird in den meisten Netzwerkumgebungen die Quality of Service Anforderungen erfüllen. Befinden sich jedoch zu viele Anwendungen im Netzwerk die über EDCA eine höhere Priorität für ihre Datenpakete fordern, tritt erneut das schon von DCF bekannte Problem auf, dass die Anzahl der Paketkollisionen steigt. Somit steigt auch die Zugriffszeit auf das Netzwerk sprunghaft an und die Datenrate fällt. Dies kann nur verhindert werden, indem Endgeräte bzw. Anwendungen die Anforderungen eines neuen Datenstroms (z.B. erwartete Datenrate, Paketgröße, etc.) beim Access Point anmelden. Auf diese Weise kann der Access Point weiteren Teilnehmern den Zugang zu einer QoS Klasse verweigern, sobald die Netzwerklast dies nicht mehr zulässt. Diese Endgeräte oder Applikationen müssen dann eine schlechtere QoS Klasse verwenden. Im 802.11 Standard gibt es für diesen Zweck den optionalen Admission Control Mechanismus. In Bea-

con Frames wird dazu den Endgeräten mitgeteilt, ob für eine QoS Klasse eine Zugangskontrolle vom Access Point gefordert wird. Unterstützt ein Endgerät keine Admission Control, darf es eine QoS Klasse die der Access Point in Beacon Frames nur mit Admission Control zulässt, nicht verwenden.

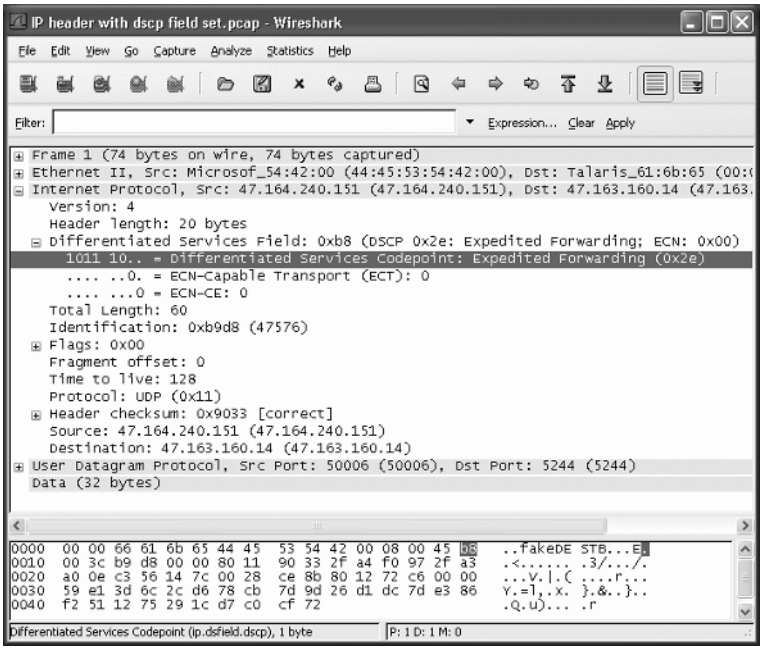

Abb. 4.27: QoS Markierung in einem IP Paket

Um einen neuen Datenstrom anzumelden, sendet ein Endgerät eine Traffic Specification (TSPEC) in einer ADDTS (Add Traffic Specification) Management Nachricht an den Access Point. Dieser überprüft daraufhin ob das Netzwerk den zusätzlichen Anforderungen gerecht werden kann und erteilt bzw. verweigert in einer Antwortnachricht eine Genehmigung. Wie der Access Point diese Prüfung durchführt ist vom Standard nicht definiert. In der Praxis fließen in eine solche Entscheidung viele zum Teil auch dynamische Parameter ein. Ein solch dynamischer Parameter ist z.B. die noch vorhandene Verkehrskapazität, die in einem Netzwerk momentan noch zur Verfügung steht. Dies hängt stark von den Empfangsbedingungen und Fähigkeiten der im Netzwerk befindlichen Endgeräte ab.

Packet Bursting und Block ACK

Neben Quality of Service Funktionalitäten führt die 802.11e Erweiterung auch eine Reihe von optionalen Funktionalitäten ein,

um die Kapazität der Luftschnittstelle besser zu nutzen. Wichtigste Funktionalität hierbei ist das Packet Bursting, das auch schon mit proprietären Erweiterungen des 802.11g Standards implementiert wurde und von 802.11e quasi legalisiert wird. Packet Bursting setzt voraus, dass im Sendepuffer eines Endgerätes mehrere Datenpakete auf die Übertragung warten. Statt nach dem Acknowledgement für ein Datenpaket den DCF Backoff Mechanismus zu verwenden, sendet das Endgerät nach einem Short Interfame Space (SIFS) sofort sein nächstes Datenpaket. Zusätzlich gibt es optional noch die Möglichkeit, zwischen Sender und Empfänger einen Block Acknowledgement Mode zu vereinbaren, falls beide Geräte dies unterstützen. Statt jedes Paket einzeln zu bestätigen, sendet der Empfänger wie in Abbildung 4.28 gezeigt, zuerst eine reihe Datenpakete und fordert dann ein Block Acknowledgement für alle Datenpakete an. Hat der Empfänger alle Datenpakete richtig empfangen, muss dieser nur eine einzige Bestätigung zurückschicken. Dies geschieht entweder sofort (Immediate Block ACK) oder erst etwas verzögert (Delayed Block ACK), um dem Empfänger mehr Zeit für die Analyse der empfangenen Daten zu geben.

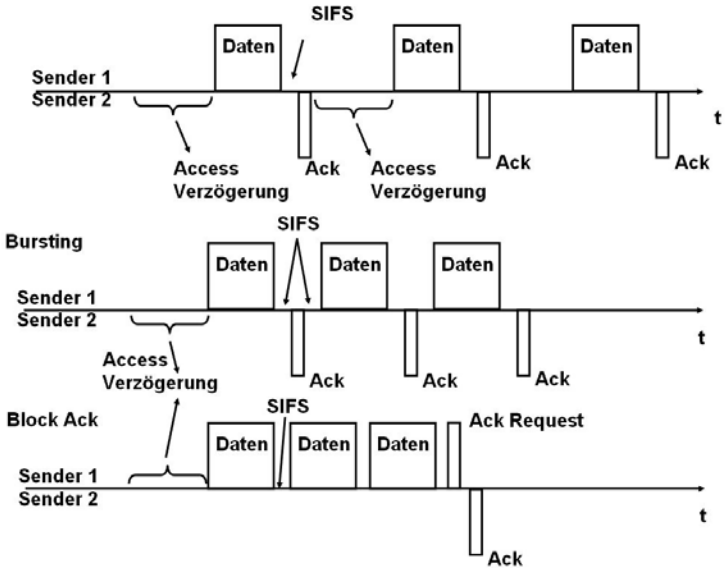

Abb. 4.28: Packet Bursing und Block Acknowledgements

Ob ein Access Point den Block ACK Mechanismus unterstützt, wird den Endgeräten über Beacon Frames im Capability Information Parameter mitgeteilt, während Endgeräte dem Access Point dies während der Association Prozedur mitteilen. Die in Abbildung 4.16 gezeigte Packet Aggregation, die mit 802.11n eingeführt wurde, kann zusätzlich zu Packet Bursting und Block ACK verwendet werden. Somit gibt es nun zahlreiche unterschiedliche Möglichkeiten, das Übertragungsmedium für die Übertragung von großen Datenmengen sehr effizient im Vergleich zum ursprünglichen Verfahren zu verwenden.

Automated Power-Save Delivery (APSD)

Zusätzlich zu dem in Kapitel 4.4 beschriebenen ursprünglichen Power Save (PS) Mode und dem in Kapitel 4.6.2 beschriebenen Power Save Multi Poll (PSMP) Mechanismus, der mit 802.11n spezifiziert wurde, führt der 802.11e Standard einen weiteren Power Save Mechanismums ein, das Automated Power-Save Delivery (APSD). Auch hier gibt es wieder mehrere Optionen. Beim Unscheduled-APSD (U-APSD), der von WMM optional unterstützt wird, vereinbaren Endgerät und Access Point, dass das Endgerät in den Schlafzustand überwechseln kann und dass in dieser Zeit eingehende Pakete im Access Point zwischengespeichert werden. Teil dieser Vereinbarung ist auch, Pakete welcher Prioritätsklasse mit diesem Algorithmus behandelt werden und welche Pakete weiterhin mit dem normalen PS Modus nach dem Aufwachen des Endgeräts zugestellt werden. Zusätzlich wird eine Service Periode (SP) vereinbart, in der das Endgerät nach dem Aufwachen aktiv ist, bevor es dann automatisch wieder in den Schlafzustand wechselt.

Bei U-APSD wird keine genaue Zeit vereinbart, nach der das Endgerät wieder aktiv sein muss. Stattdessen schickt das Endgerät einen Trigger Frame an den Access Point, sobald es wieder empfangsbereit ist. Datenpakete von QoS Klassen, für die U-APSD zuvor aktiviert wurde, werden dann automatisch innerhalb der Service Periode zugestellt. Am Ende der Service Periode wechselt das Endgerät wieder automatisch in den Schlafmodus. Pakete von QoS Klassen, für die kein U-APSD aktiviert wurden, müssen weiterhin mit den für das PS Verfahren nötigen Poll Frames einzeln angefordert werden. Ob ein Access Point U-APSD unterstützt, teilt dieser den Endgeräten im WMM Parameter in den Beacon Frames mit. Auf der Endgeräteseite wird der U-APSD Betrieb während der Association Prozedur über den QoS Capability Parameter vereinbart oder später während des Betriebs über eine Traffic Specification (TSPEC) Nachricht.

Zusätzlich spezifiziert der 802.11e Standard auch ein Scheduled-APSD (S-APSD) Betrieb, welcher allerdings bei WMM nicht vorgesehen ist. Statt eines Trigger Frames vereinbaren hier Endgerät und Access Point ein zyklisches Aktivitätsintervall.

Direct Link Specification (DLS), Direct Link Protocol

Während heute meist Endgeräte über den Access Point direkt mit dem Internet kommunizieren, gibt es mehr und mehr Anwendungen im Heimbereich, wie z.B. Video Streaming zwischen einem Notebook und einem Monitor oder Fernseher, die Daten zwischen zwei Endgeräten im gleichen Netzwerk übertragen. Daten können in einem solchen Fall bisher nicht direkt zwischen den Endgeräten ausgetauscht werden, sondern müssen zunächst zum Access Point geschickt werden und von dort dann weiter zum eigentlichen Empfänger. Da das Datenpaket in einem solchen Fall zweimal über die Luftschnittstelle übertragen werden muss, halbiert sich somit die maximal Bandbreite. Für solche Anwendungen wurde deshalb im 802.11e Standard das Direct Link Protokoll (DLP) spezifiziert. Möchten zwei Endgeräte direkt miteinander kommunizieren, richtet eines der beiden Endgeräte eine Anfrage an den Access Point. Dieser leitet die Anfrage an das andere Endgerät weiter. Befindet sich dieses in Reichweite des ersten Endgerätes und unterstützt ebenfalls das Direct Link Protocol, gibt es eine positive Antwort an den Access Point zurück, der diese wiederum an das anfragende Endgerät weiterleitet. Danach können die zwei Endgeräte dann direkt Verbindung aufnehmen und fortan unter Umgehung des Access Point Datenpakete austauschen.

HCCA

Der Vollständigkeit halber sei an dieser Stelle auch noch der optionale HCF Controlled Channel Access (HCCA) erwähnt. Dieser Scheduling Algorithmus kann statt EDCA verwendet werden, ist jedoch optional und nicht Teil der WMM Spezifikation. Somit ist es unwahrscheinlich, dass HCCA größere Verbreitung finden wird. HCCA ist im Unterschied zu EDCA ein zentraler Scheduling Algorithmus und ermöglicht dem Access Point den Kanalzugriff zu kontrollieren. Dazu sendet der Access Point Poll Frames an jedes Endgerät, dass danach die Möglichkeit hat, in einem vorgegebenen Zeitfenster seine Daten zu übertragen. Da der Access Point die Poll Frames schickt, bevor ein anderes Endgerät die Möglichkeit hat auf den Kanal zuzugreifen, wird auf diese Weise sichergestellt, dass nur Endgeräte die mit einer ADDTS Nachricht eine Traffic Specification TSPEC angefordert haben auch Daten übertragen können. HCCA unterstützt auch die zuvor erwähnten Quality of Service Klassen und kann somit wie EDCA, Paketen

mit bestimmten Quality of Service Anforderungen Priorität einräumen.

Wifi Analyse in der Praxis

Um ein Gefühl zu bekommen, welche der in diesem Kapitel vorgestellten Optionen in der Praxis verwendet werden, gibt es eine Anzahl von Netzwerkanalysetools, die sich für eigene Nachforschungen sehr gut eignen. Ein kostenloses und sehr leistungsfähiges Programm ist beispielsweise Wireshark, erhältlich unter http://www.wireshark.org. Unter Linux kann mit diesem Programm und diversen Wireless LAN Karten die Datenübertragung in einem Wifi Netzwerk aufgezeichnet und analysiert werden. Wireshark ist auch unter Windows erhältlich, für das Aufzeichnen von Wireless LAN Pakete ist jedoch ein spezieller Wireless LAN Adapter nötig. Außerdem bietet die Seite auch über das integrierte Wiki diverse Wifi Traces zum Download an, die ebenfalls einen guten Einblick in die Funktionsweise des Wireless LAN Standards bieten. Eine weitere interessante Alternative zum Aufzeichnen von Wifi Paketen ist die Anschaffung eines Linksys WRT54G Access Points, der sich mit einem freien Linux Betriebssystem namens OpenWRT und Kismet zu einem ausgezeichneten Paketmonitor und Aufzeichnungsgerät umfunktionieren lässt. Weitere Information hierzu finden sich im OpenWRT Wiki auf http://www.openwrt.org

4.9 Vergleich zwischen Wireless LAN und UMTS

Als vor einigen Jahren sowohl Wireless LAN als auch UMTS am Anfang ihrer Entwicklung standen, gab es zahlreiche Diskussion über einen Konkurrenzkampf der Systeme. Zwischenzeitlich sind beide Systeme herangewachsen und haben ihre Anwendungsgebiete gefunden.

Wireless LAN und 3.5G Netzwerke heute

Während Wireless LAN vor allem im Heim- und Bürobereich genutzt wird und in Form von Hotspots auch auf Flughäfen und in Hotels, hat sich UMTS insbesondere auch durch die Weiterentwicklungen wie HSDPA zum großflächigen Hotspot entwickelt, der fast überall verfügbar ist. Da HSDPA heute überall zusammen mit UMTS verfügbar ist, wird nachfolgend nur von UTMS gesprochen. Um vor allem die Konkurrenzsituation zwischen WLAN und UMTS zu untersuchen, widmet sich das letzte Unterkapitel dem Vergleich zwischen Wireless LAN und UMTS für Anwendungen außerhalb von Heim- und Büro.

Geschwindigkeit

Vergleicht man die maximal möglichen Geschwindigkeiten von WLAN und UMTS beim Einsatz außerhalb von Wohnung oder

Büro, ist zunächst ein großer Unterschied festzustellen. Während viele WLAN Hotspots heute noch den 802.11b Standard mit bis zu 11 MBit/s verwenden, werden im Zuge von Erweiterungen und durch Austausch alter Access Points auch 802.11g Geräte mit 54 MBit/s und in Zukunft auch 802.11n Access Points mit noch schnelleren Geschwindigkeiten und der WMM Quality of Service Erweiterung zum Einsatz kommen. Wie in diesem Kapitel gezeigt, können auf der Luftschnittstelle Datenraten von 5, 24 und 100 MBit/s erreicht werden. Demgegenüber stehen aktuelle 3.5G Datenraten von 3.6, 7.2 und 14.4 MBit/s, mit in der Praxis erreichbaren Datenrate von 2 bis 3 MBit/s. Zunächst scheinen deshalb WLAN Hotspots in punkto Geschwindigkeit einen Vorteil zu haben. Bei öffentlichen Hotspots ist jedoch nicht die Wireless LAN Geschwindigkeit der begrenzende Faktor, sondern die Geschwindigkeit der Anbindung des Access Points an das Internet. Vor allem bei kleinen Hotspots werden heute DSL Verbindungen mit einer Downlink Geschwindigkeit von wenigen MBit/s verwendet, die sich alle Anwender eines Hotspots teilen müssen. Die Kapazität des Wireless LANs kann also nicht vollständig ausgenutzt werden. Bei UMTS Netzwerken sind die genannten 2 – 3 MBit/s in der Praxis eine Geschwindigkeit, die sich ebenfalls die meisten Nutzer eines Sektors einer Basisstation teilen müssen. Eine UMTS Basisstation mit 3 Sektoren hat somit eine maximale Kapazität von etwa 9 MBit/s. Wird mehr Kapazität benötigt, können Netzwerkbetreiber auch von ihrem zweiten Frequenzband gebrauch machen und somit die Kapazität nochmals verdoppeln. Die Kapazität der Basisstation steigt somit auf 18 MBit/s an. Ein einzelner Teilnehmer ist jedoch weiterhin mit seiner Übertragungsrate auf einen Sektor und eine Frequenz begrenzt. Für heutige Anwendungen wie Web Browsing, Zugriff auf Unternehmensdaten und Dateiübertragungen reicht diese Bandbreite in den meisten Fällen aus und ermöglicht komfortables Arbeiten. Somit spürt ein Anwender in den meisten Fällen keinen großen Unterschied zwischen der Nutzung eines UMTS Netzwerks und eines WLAN Hotspots. Auch bei der Datenübertragung in Uplink Richtung, also vom Endgerät zu einem Server im Netzwerk liegen beide Netzwerktypen mit 200 kbit/s bis 1 MBit/s etwa gleich auf (ADSL Uplink Geschwindigkeit vs. HSUPA).

Es sollte aber nicht vergessen werden, dass eine Basisstation auch einen größeren geographischen Bereich als ein Wireless LAN Hotspot abdeckt. Zudem muss auch berücksichtigt werden, dass eine Basisstation auch für den Sprachverkehr in diesem Bereich verantwortlich ist und damit die Kapazität für den Daten-

verkehr verringert wird. Sollte deshalb ein Kapazitätsengpass in manchen Gebieten auftreten, können entweder weitere UMTS Basisstationen aufgestellt werden, oder kleine Gebiete mit so genannten Picozellen ausgeleuchtet werden. Diese sind in Größe und Form vergleichbar mit Wireless LAN Access Points.

Roaming und Verfügbarkeit

In den letzten Jahren war zu beobachten, dass Wireless LAN Access Points an vielen öffentlichen Plätzen wie z.B. Hotels, Flughäfen und Bahnhöfen installiert wurden. Auch in Zukunft ist zu erwarten, dass sich dieser Trend fortsetzt. Aufgrund der geringen Reichweite ist aber nicht gewährleistet, dass ein Hotspot immer am gewünschten Ort verfügbar ist. Dies ist z.B. in Hotels ärgerlich, wenn nur einzelne Etagen oder Bereiche mit Wireless LAN ausgestattet sind. Somit wird es weiterhin sorgfältiger Planung bedürfen oder einfach dem Zufall überlassen bleiben, ob am Zielort Wireless LAN zur Verfügung steht.

UMTS Netzwerke haben inzwischen eine große Flächendeckung in vielen Ländern erreicht. Selbst in ländlichen Gebieten ist bereits in vielen Fällen eine UMTS Abdeckung vorhanden, in jedem Fall sind jedoch zumindest GSM, GPRS und in vielen Fällen auch EDGE flächendeckend verfügbar. Durch Roaming Vereinbarungen ist außerdem sichergestellt, dass UMTS Netzwerke zusammen mit GSM in den meisten anderen Ländern der Welt verfügbar ist. Auch bei Wireless LAN Hotspot Betreibern ist zu beobachten, dass diese untereinander Roamingabkommen abschließen und sich z.B. ein französischer Kunde in Deutschland mit seinem Nutzeraccount aus Frankreich an vielen Hotspots anmelden kann. Ob dies jedoch an einem bestimmten Hotspot möglich ist, bleibt heute noch etwas dem Zufall überlassen.

Abrechnung

Da UMTS eine Weiterentwicklung von GSM und GPRS ist, bereitet auch die weltweite Abrechnung (Billing) keine Probleme. Diese Verfahren sind integraler Bestandteil des Netzwerkes. Manche Netzwerkbetreiber bieten seit einiger Zeit auch Tarife für Datenroaming an, so dass auch über UMTS Netzwerke im Ausland in vielen Fällen eine preisliche attraktive Internetnutzung möglich ist. Der Wireless LAN Standard hingegen beinhaltet keine standardisierte Abrechnung. Aufgrund eines fehlenden Standards und der vielen Anbieter gibt es heute zahlreiche Zahlungsmodelle. Diese reichen von Rubbelkarten, die z.B. an der Hotelrezeption gekauft werden können, über Kreditkartenzahlung, bis hin zur Abrechnung auf der GSM oder UMTS Mobilfunkrechnung eines Kunden. Letzteres ist nur möglich, wenn der WLAN Hotspot vom Mobilfunkbetreiber des Kunden betrieben

wird. In den meisten Fällen wird deshalb ein Kunde den Hotspot nicht sofort verwenden können, sondern muss sich erst um die Abrechnung kümmern.

Lawful Intercept

Bisher nicht vollständig geklärt ist die technische Umsetzung des Abhörens durch Behörden und Sicherheitsorganisationen (Lawful Intercept) von Nutzern eines Wireless LAN Hotspots. Für alle Telekommunikationsnetzwerke inklusive GSM, GPRS und UMTS gibt es in den meisten Ländern gesetzliche Bestimmungen und Verfahren, die das Abhören von Teilnehmern durch die Polizei und andere Organisationen regeln. Aufgrund des jungen Marktes ist dies bei Wireless LAN Hotspots bisher noch nicht der Fall und ist aufgrund der heutigen Architektur und Authentifizierung der Teilnehmer auch nicht so ohne weiteres möglich. Bei zunehmendem Erfolg von Wireless LAN ist jedoch anzunehmen, dass auch für Wireless LAN Regelungen eingeführt werden. Dies wird für viele Anbieter einen Umbau der Nutzeridentifizierung und Datenweiterleitung bedeuten.

Mobilität und Handover

Wireless LAN wurde für die Abdeckung von kleinen Flächen konzipiert. Diese kann durch Einsatz von mehreren Access Points, die zusammen ein Extended Service Set (ESS) bilden, begrenzt erweitert werden. Da sich alle Access Points im gleichen IP Subnet befinden müssen (vgl. Kapitel 4.4 und Abb. 4.9), ist somit die maximale Ausdehnung eines Netzes z.B. auf ein Gebäude begrenzt. Für die meisten Wireless LAN Anwendungen ist dies ausreichend, zumal auch ein automatischer Wechsel zwischen den einzelnen Access Points möglich ist. UMTS Netzwerke hingegen sind für die flächendeckende Versorgung konzipiert. Weiterhin legt der Standard, wie in Kapitel 3 gezeigt, besonderen Wert auf einen reibungslosen Handover, um Verbindungen auch über weite Distanzen, lange Zeiträume und hohen Geschwindigkeiten des Benutzers aufrechterhalten zu können. Nur so ist es möglich, mobil („on the move“) zu telefonieren oder mit einem PDA oder Notebook während einer Zugfahrt ständig Kontakt mit dem Internet oder einem Firmennetzwerk zu halten.

Zellgrößen

Auch bei der Zellgröße gibt es große Unterschiede zwischen Wireless LAN und UMTS. Wireless LAN ist aufgrund seiner maximalen Sendeleistung von 0.1 Watt auf eine Zellgröße von wenigen hundert Metern begrenzt. Innerhalb von Gebäuden sinkt die Rechweite aufgrund von Hindernissen wie z.B. Wänden auf wenige Zimmer. UMTS Zellen haben jedoch Reichweiten von mehreren Kilometern, können aber auch für die Versorgung von ein-

zelnen Gebäuden oder Stockwerken wie z.B. Einkaufszentren etc. verwendet werden (Picozellen).

Sicherheit

Wie in diesem Kapitel bereits diskutiert, wurde bei Wireless LAN an Sicherheit und Verschlüsselung erst nachträglich gedacht. Während es für Firmennetzwerke und private Hotspots heute mit WPA und WPA2 gute Sicherheitslösungen gibt, ist die Sicherheit bei öffentlichen Hotspots weiterhin ein Problem. Hier ist fraglich, ob sich WPA Verschlüsselung in Zukunft durchsetzten kann, da das Passwort für jeden Hotspot vom Nutzer manuell eingegeben werden müsste. Heutige Hotspots ohne WPA ermöglichen es Angreifern die sich ebenfalls im Hotspot befinden, mit einfachen Mitteln den Datenverkehr der Teilnehmer abzuhören und aufzuzeichnen. Da ohne zusätzliche Maßnahmen Datenpakete nicht verschlüsselt sind, können Passwörter und andere sensible Daten auf nicht verschlüsselten Webseiten oder Zugangsdaten bei nicht verschlüsselter Kommunikation mit einem eMail Server sehr einfach entwendet werden. Hotspotnutzer sollten deshalb drauf achten, dass sensible Daten nur auf geschützten Webseiten eingegeben werden (https) und für eMail nur verschlüsselte Verbindungen verwendet werden. Zusätzlich sollte grundsätzlich auch der gesamte Datenverkehr über einen verschlüsselten IPSec oder PPTP Tunnel geleitet werden. Dies erfordert jedoch einen nicht unerheblichen Aufwand und Know-How des Anwenders.

In UMTS Netzwerken ist Sicherheit Teil des Systemkonzepts. Nutzer müssen sich deshalb nicht selbst um die Verschlüsselung auf der Luftschnittstelle kümmern. Dies wird vom System automatisch ohne manuelle Eingabe eines Passworts ewährleistet, da der geheime Schlüssel auf der SIM Karte des Teilnehmers gespeichert ist.

Telefonie

Der leitungsvermittelnde Teil eines UMTS Netzwerkes ist speziell für Sprach- und Videotelefonie konzipiert. Diese Dienste sind zwei der wesentlichen Anwendungen von Mobilfunknetzwerken, die von Wireless LAN Hotspots heute nur unzureichend abgedeckt werden. Wie in diesem Kapitel gezeigt, geht der Trend auch bei Sprach- und Videoübertragung weg von der Leitungsvermittlung und hin zu Voice over IP. So ist es heute durchaus möglich, mit Notebooks und so genannten „Soft-Telefonie Clients“ über Wireless LAN zu telefonieren.

Darüber hinaus ist heute ein WLAN Chip schon in vielen Smartphones integriert und Voice over IP Programme ermöglichen das Telefonieren im Wireless LAN. Während dies zuhause oder im Büro meist keine Probleme mehr macht, gibt es in Wire-

less LAN Hotspots noch zwei Stolpersteine. Zum einen erfordern Hotspots normalerweise eine webbasierte Benutzerauthentifizierung. Vor dem Telefonieren muss ein Anwender deshalb zunächst mit dem integrierten Web Browser die Verbindung aktivieren. Ein zweites Problem tritt in Hotspots auf, die stark ausgelastet sind. Da die Distributed Coordination Function (vgl. Kapitel 4.5) nicht geeignet ist, die nötige Bandbreite und Verzögerungszeit für ein Telefongespräch zu garantieren, leidet die Qualität der Verbindung. Zwar sind hier schon Lösungsansätze wie z.B. der 802.11e Standard erkennbar, bis diese jedoch in der Mehrzahl der Wireless LAN Hotspots und Endgeräte verfügbar ist, werden sicher noch einige Jahre vergehen. Aber selbst dann wird Telefonie über Wireless LAN die Telefonie über UMTS oder GSM aufgrund der begrenzten Reichweite und fehlenden Handovers nur ergänzen, nicht jedoch ersetzten können.

Zusammenfassung der WLAN Eigenschaften

Zusammenfassend lässt sich feststellen, dass Wireless LAN eine Hotspottechnologie für Anwender ist, die in einem begrenzen Bereich für eine begrenzte Zeitdauer Zugriff auf das Internet benötigen. Aufgrund der im Vergleich zu UMTS einfachen Technologie sowie dem lizenzfreien Betrieb sind die Kosten für Installation und Betrieb weit geringer als für ein UMTS Netzwerk. Einen schnellen Zugang zum Internet vorausgesetzt, bieten WLAN Hotspots in diesem Umfeld mit seinen sehr schnellen Datenübertragungsraten viele Möglichkeiten. Endgeräte die in WLAN Hotspots verwendet werden sind hauptsächlich Notebooks, PDAs und zunehmend auch Smartphones, die UMTS und Wifi integrieren. An seine technischen Grenzen gelangt Wireless LAN bei mobilen Nutzern in Autos oder Zügen, sowie mit seinem maximalen Abdeckungsbereich in der Größenordnung eines Gebäudes. Im Zusammenhang mit Wireless LAN wird deshalb auch vom „**nomadischen Internet**“ gesprochen, da sich der mobile Nutzer während der Kommunikation in einem Hotspot aufhält und sich dort normalerweise nicht oder nur über kleine Distanzen bewegt.

Zusammenfassung der UMTS Eigenschaften

UMTS richtet sich an die Anforderungen mobiler Nutzer, die unterwegs kommunizieren möchten. Mit seinen schnellen Datentransferraten eignet sich UMTS ebenfalls gut für den Internetzugriff und viele Geschäftsreisende setzten heute auf UMTS Datenkarten um unabhängig vom nächsten WLAN Hotspot kommunizieren zu können. Die komplexe Technologie, die für die Mobilität des Teilnehmers und für Anwendungen wie Telefonie an jedem Ort unerlässlich ist, macht UMTS teurer als Wireless LAN. Dazu tragen auch die hohen Lizenzgebühren bei, die Mo-

bilfunkfirmen bereit waren, bei Frequenzversteigerungen in diversen Ländern zu bezahlen. Hauptanwendungsgebiete für UMTS sind somit neben mobiler Sprach- und Videotelefonie sowie einem Internetzugang für Notebooks auch typische Mobilfunkapplikationen für kleine Endgeräte wie WAP, MMS, eMail und Videostreaming, sowie Web 2.0 Anwendungen wie Podcasts, Einstellen von Bildern bei Diensten wie Flickr, Navigation mit online Kartenzugriff und nicht zu vergessen, Instant Messaging. Im Zusammenhang mit UMTS wird deshalb vom „**mobilen Internet**“ gesprochen, da Kommunikation immer und überall, selbst in Autos und Zügen möglich ist.

4.10 Fragen und Aufgaben

1. Welche Unterschiede gibt es zwischen der Ad-hoc und der BSS Betriebsart eines Wireless LAN?
2. Welche weiteren Funktionen werden oft zusätzlich in einem Wireless LAN Access Point eingebaut?
3. Was ist ein Extended Service Set (ESS)?
4. Welche Aufgabe hat die SSID und in welchen Frames wird diese verwendet?
5. Welche Stromsparmechanismen gibt es in den Wireless LAN Standards?
6. Warum werden in einem Wireless LAN Acknowledgement Frames verwendet?
7. Aus welchen zwei Gründen wird der RTS/CTS Mechanismus bei 802.11g verwendet?
8. Warum gibt es in einem BSS Szenario drei MAC-Adressen in einem Wireless LAN MAC Header?
9. Wie wird dem Empfänger die Datenrate des Nutzdatenpakets mitgeteilt?
10. Welche maximale Datenrate kann bei der Kommunikation zwischen zwei 802.11g Endgeräten in einem BSS erreicht werden?
11. Welche Nachteile hat das DCF Verfahren für Anwendungen wie Telefonie oder Video Streaming?

12. Welche Sicherheitslücken gibt es bei Wired Equivalent Privacy und wie werden diese durch WPA und WPA2 gelöst?
13. Mit welchen Verfahren steigert der 802.11n Standard die Übertragung im Vergleich zum bisherigen Standard?
14. Wie erreicht EDCA eine Priorisierung von Sprachdaten?

Lösungen sind auf der Website zum Buch unter http://www.cm-networks.de zu finden.