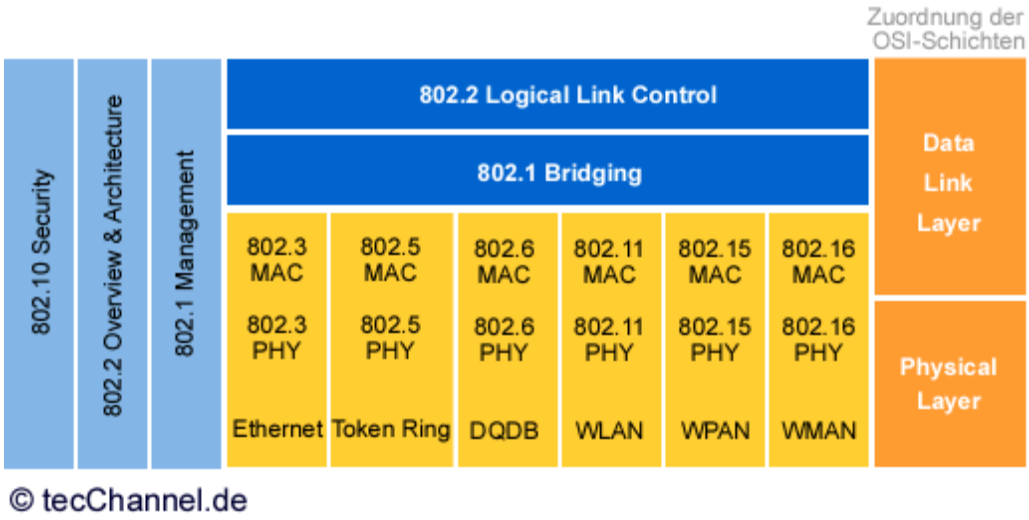
802.11: Standard für drahtlose Netze

Wireless LANs mausern sich von der Nischenlösung zur echten Netzalternative. Als Motor der Entwicklung fungiert der Standard 802.11. Er macht das herstellerübergreifende Zusammenspiel der Komponenten möglich
VON AXEL SIKORA

Die Standards des LAN/WAN Standards Committee (auch IEEE802) des US-amerikanischen Ingenieurverbands IEEE (sprich: I-triple-E) bilden die allgegenwärtige Basis für die Vernetzung von Rechnern.

Das wohl bekannteste Teilstück des IEEE-Regelwerks sind die Ethernet-Standards der Arbeitsgruppe 802.3 (IEEE 802.3 CSMA/CD). Sie umfassen Geschwindigkeitsklassen von 10 MBit/s bis zu den gegenwärtig in der Spezifikation befindlichen 10 GBit/s



IEEE802-Familie: Die wichtigsten Standards und ihre wechselseitigen Beziehungen im Überblick.

Um in dem immensen Wachstumsmarkt der drahtlosen Übertragungsprotokolle im Geschäft zu bleiben, hat IEEE 1997 mit 802.11 den ersten herstellerunabhängigen Standard für Wireless LANs (WLANs) verabschiedet.

Wireless-LAN-Gremien

Im Umfeld von IEEE802.11 agieren auch zwei Industriegremien. Die Wireless LAN Association (WLANA) soll die Verbreitung des Standards durch Marketing und Öffentlichkeitsarbeit unterstützen. Die Wireless Ethernet Compatibility Alliance (WECA) zertifiziert unter dem Schlagwort Wi-Fi (Wireless Fidelity) die Interoperabilität 802.11-kompatibler Geräte.

Neben 802.11 arbeitet IEEE noch an zwei weiteren Standards zur drahtlosen Signalübertragung. Der IEEE802.15 soll die Netze niedriger Bandbreite und Reichweite (bis 10 m) abdecken, also Personal Area Networks (PANs). Der wichtigste Standard in diesem Bereich ist bislang Bluetooth.

IEEE802.16 beschreibt breitbandige Netze im mittleren Entfernungsbereich bis etwa 50 km. Als primärer Kandidat für solche Metropolitan Area Networks (MANs) fungiert derzeit HiperLAN/2 des europäischen Standardisierungsgremiums ETSI (European Telecommunications Standards Institute).

Verfahren und Frequenzen

Der Standard IEEE802.11 wurde nach sieben Jahren Entwicklung 1997 erstmals festgelegt. Er spezifiziert Bandbreiten von 1 und 2 MBit/s. Die Spezifikation umfasst die Beschreibung eines MAC-Protokolls und dreier alternativer PHY-Technologien. Neben zwei Frequenz-Spreizverfahren (Spread Spectrum Technologies - SST) für Funkwellen im 2,4-GHz-Band zählt dazu auch ein Infrarot-Verfahren.

Gerade die Übertragung im lizenzierungsfreien ISM-Band macht WLANs besonders interessant. Dieser Frequenzbereich lässt sich weltweit für industrielle, wissenschaftliche und medizinische Zwecke (Industrial, Scientific, Medical) nutzen. Daher arbeiten etliche drahtlose Kommunikationsverfahren - auch Bluetooth - auf der entsprechenden Frequenz. Allerdings operieren hier zahlreiche potenzielle Störquellen, nicht zuletzt Mikrowellenherde. Genau deswegen wurde das ISM-Band ursprünglich freigegeben: Für viele lizenz- und kostenpflichtige Übertragungsverfahren weist es ein zu hohes Aufkommen an Störern auf.

Nicht alle Nationen erlauben die vollständige Verwendung des Frequenzbereichs, einige beschränken die Anzahl verfügbarer Kanäle. Davon sind insbesondere Japan, Frankreich und Spanien betroffen. Auch die weitere Spezifikation, vor allem die erlaubte Sendeleistung und die Modulationsverfahren, unterscheiden sich zum Teil deutlich.

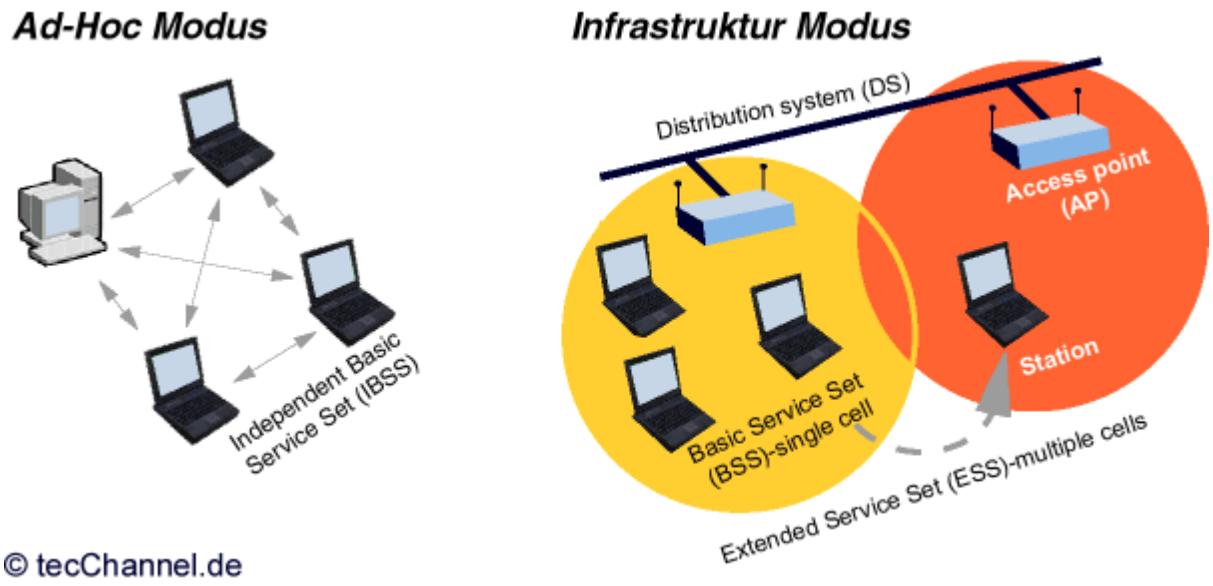
Schnelle 801.11-Varianten

Schon bei der Zertifizierung des ursprünglichen 802.11-Standards war abzusehen, dass eine Datenrate von maximal 2 MBit/s für einen Markterfolg nicht ausreichen würde. Aus diesem Grund hatten zu diesem Zeitpunkt bereits mehrere Anbieter proprietäre Lösungen entwickelt. Um eine Aufsplitterung des Markts zu vermeiden, wurden dem Standard 1999 mit 802.11a und 802.11b zwei weitere Bestandteile hinzugefügt. Beide verfolgen das Ziel, höhere Bandbreiten zu erreichen. Allerdings beschreiten sie dabei völlig verschiedene Wege.

802.11a löst sich vom ursprünglich verwendeten ISM-Band und weicht auf das 5-GHz-Band aus, in dem sich per se größere Bandbreiten erzielen lassen. 802.11b dagegen stellt eine rückwärtskompatible Erweiterung des originären 802.11-Standards dar. In seiner momentanen Definition erreicht 802.11b eine Brutto-Datenrate von 11 MBit/s bei einem Nutzdatenanteil bis zu 7 MBit/s. Damit entspricht die b-Variante etwa dem drahtgebundenen 10-MBit/s-Ethernet nach IEEE802.3, wie es noch in vielen Installationen zu finden ist.

Topologie im Funknetz

IEEE802.11 unterscheidet zwei grundsätzliche Betriebsarten: den Ad-hoc- und den Infrastruktur-Modus. Im Ad-hoc-Modus kommunizieren Endgeräte in einem Peer-to-Peer-Netzwerk unmittelbar miteinander. Solche Independent Basic Service Sets (IBSS) erlauben den schnellen, einfachen und kostengünstigen Aufbau von Netzwerken über kurze Entfernungen und mit begrenzter Teilnehmerzahl. Im Infrastruktur-Modus erfolgt die Kommunikation über einen Zugangspunkt (Access Point - AP), der als Relaisstation die Reichweite der Funkzelle verdoppelt. Zudem fungiert der AP quasi als Funk-Hub und stellt typischerweise auch die Verbindung zum drahtgebundenen Netz her.



In der einfachsten Version besteht ein Infrastruktur-Funknetz aus einem AP und einer Gruppe von drahtlosen Stationen. Ein solches Netzwerk wird als Basic Service Set (BSS) bezeichnet. Koppelt man mehrere BSS über ein LAN, so spricht man von einem Extended Service Set (ESS). In diesem Modus spielt die korrekte Zuordnung der Stationen zu einem BSS sowie der Wechsel zwischen den einzelnen BSS-Sets (Roaming) eine entscheidende Rolle.

Daher müssen sich im Infrastruktur-Modus alle Stationen bei einem Access Point anmelden. Sie übertragen dann auf dem Kanal, der vom jeweiligen AP verwendet wird. Ein Wechsel der Zuordnung kann durch eine Veränderung der Kanaleigenschaften erfolgen (speziell beim Ortswechsel von mobilen Stationen) oder auch vom Administrator im Sinne eines Load Balancing vorgegeben werden.

802.11: Der MAC-Layer

Die Kanalzugriffsschicht (MAC -Layer) von 802.11 weist eine enge Verwandtschaft mit der kabelgebundenen Variante 802.3 auf. Allerdings muss der drahtlose Standard auf die Besonderheiten der Übertragungsstrecke Rücksicht nehmen. Insbesondere entfällt hier die Möglichkeit zum Überwachen von Kollisionen. Daher greift 802.11 auf eine Zugangskontrolle (Access Control) nach dem CSMA/CA-Algorithmus zurück.

Das Akronym steht für Carrier Sense Multiple Access with Collision Avoidance. Multiple Access deutet an, dass mehrere Kommunikationsteilnehmer einen gemeinsamen Übertragungskanal nutzen (Shared Medium). Carrier Sense zeigt an, dass jeder Kommunikationsteilnehmer den gemeinsamen Kanal überwacht und seine eigene Tätigkeit an dessen Zustand anpasst. Collision Avoidance beschreibt einen Mechanismus, der dabei Kollisionen zu vermeiden versucht.

Eine zentrale Rolle bei der Funktionsweise des Zugriffsmechanismus spielt die Zeit zwischen zwei Datenpaketen, der sogenannte Interframe Space (IFS). Um die Belegung des Mediums zu ermitteln, hört eine sendewillige Station für die IFS-Zeit das Medium ab. Tritt während dieser Zeitspanne keine Kommunikation auf, ist das Medium mit hoher Wahrscheinlichkeit frei. Der 802.11- Standard definiert vier verschiedene IFS-Zeiten, die drei unterschiedliche Prioritätsstufen für den Zugriff widerspiegeln. Dabei gilt: Je kürzer der IFS, desto höher die Priorität

Distributed Coordination Function

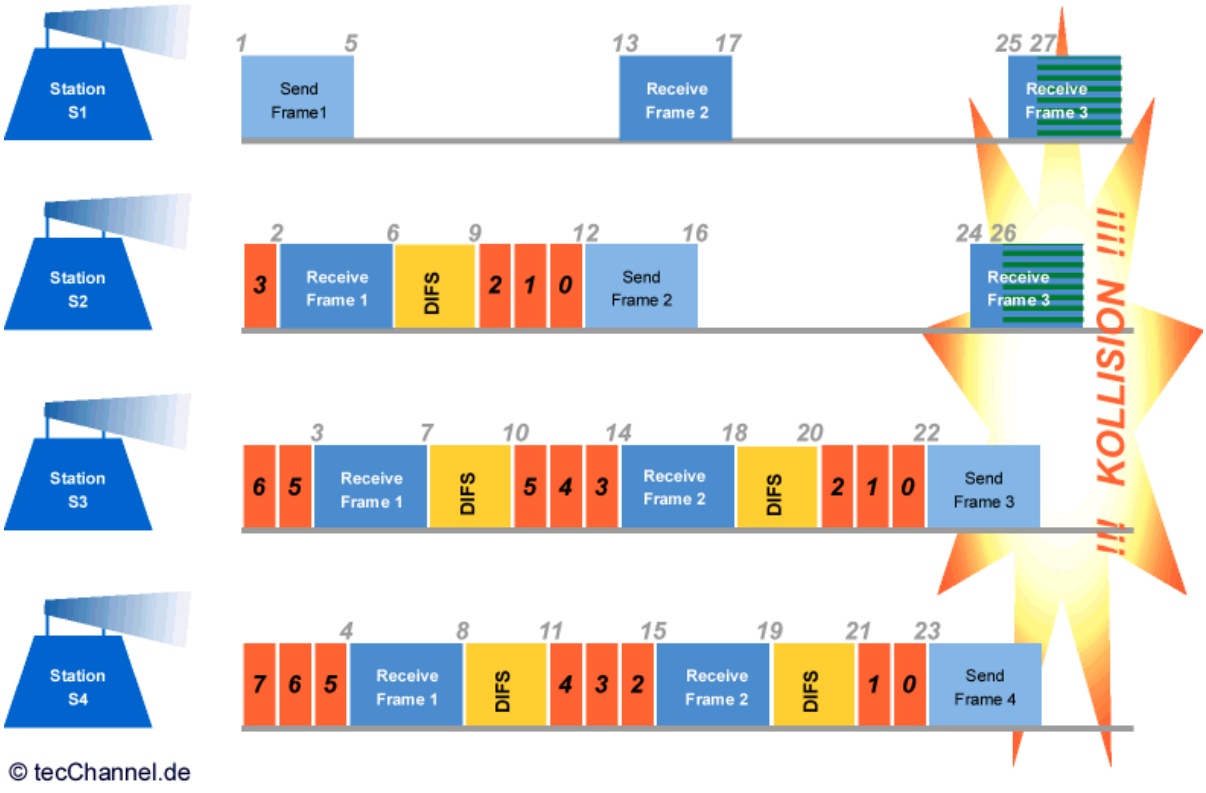
Die grundlegende IFS-Zeit ist die Distributed IFS (DIFS). Die auf ihr basierende Distributed Coordination Function (DCF) nutzt alle Stationen, um Zugang zum Übertragungsmedium zu bekommen. Der sendewillige Teilnehmer hört zunächst das Medium ab (Listen Before Talk - LBT).

Bleibt das Medium mindestens für die DIFS-Zeit frei, kann die Übertragung starten. Wird das Medium dagegen als belegt erkannt, stellt die Station die Übertragung für eine bestimmte Wartezeit zurück. Die Bestimmung dieser Zeitspanne erfolgt innerhalb des so genannten Backoff-Prozesses. Das recht aufwendige Backoff-Verfahren dient dazu, die Wahrscheinlichkeit von Kollisionen so weit wie möglich zu verringern.

Zunächst generiert die Station eine zwischen Null und einem Maximum liegende Pseudo-Zufallszahl. Das gewählte Maximum bezeichnet man als Contention Window (Englisch "contention" für Streit, Zank, Streitpunkt). Die Zufallszahl, multipliziert mit einer Zeitschlitzdauer, dient als Backoff-Counter. Solange die Station das Medium als belegt erkennt, bleibt dieser Zähler konstant. Wird das Medium frei, wartet die Station zunächst die DIFS-Zeit ab. Anschließend zählt sie den Backoff-Counter bis Null zurück. Ist nun das Medium noch immer frei, steht dem Senden nichts mehr im Weg

Collision Avoidance

Auch die DCF kann jedoch das Auftreten von Kollisionen nur minimieren, jedoch nicht gänzlich vermeiden, wie das folgende Beispiel zeigt:



1: Station S1 beginnt die Übertragung eines Rahmens Frame 1. Alle anderen Stationen befinden sich in verschiedenen Stadien des Backoff. Sie dekrementieren also den Backoff-Zeitgeber in jedem Zeitschlitz, in dem das Medium als frei erkannt wird.

2: Nach einer (von der räumlichen Entfernung der beiden Stationen abhängigen) Verzögerungszeit empfängt S2 den Rahmen. Da das Medium als belegt erkannt wird, stoppt das Herunterzählen des Backoff-Zählers.

3, 4: Nach entsprechenden Verzögerungszeiten empfangen auch S3 und S4 den Rahmen von S1 und halten ihre Backoff-Zähler an.

5: S1 beendet die Übertragung des Rahmens.

6, 7, 8: S2, S3 und S4 erkennen das Medium wieder als frei und warten eine DIFS-Zeit ab.

9, 10, 11: Nach Ablauf der DIFS-Zeit beginnen die Stationen erneut, ihre Backoff-Zähler zu dekrementieren.

12: Der Backoff-Zähler von S2 läuft ab. Daher beginnt S2 unmittelbar mit der Übertragung des Rahmens Frame 2.

13: Nach einer Verzögerungszeit empfängt S1 den Rahmen. Da sich S1 nicht im Backoff befindet, hat dies für diese Station keine Auswirkungen.

14, 15: Sobald S3 und S4 den Rahmen empfangen, erkennen sie das Medium als belegt und stoppen das Herunterzählen des Backoff-Counters.

16: S2 beendet die Übertragung.

17: S1 erkennt das Medium wieder als frei. Da keine Informationen zur Übertragung anstehen, hat dies aber keine weiteren Auswirkungen.

18, 19: S3 und S4 erkennen das Medium wieder als frei und warten eine DIFS-Zeit ab.

20, 21: Nach Ablauf der DIFS-Zeit beginnen beide Stationen, ihren Backoff-Zähler zu dekrementieren.

22: Der Backoff-Zähler von S3 läuft ab, die Station beginnt unmittelbar mit der Übertragung des Rahmens Frame 3.

23: Gleichzeitig läuft der Backoff-Zähler von S4 ab. Auch diese Station beginnt unmittelbar mit der Übertragung eines Rahmens (Frame 4). Eine Kollision bahnt sich an.

24, 25: S2 und S1 empfangen Frame 3 zunächst störungsfrei.

26, 27: Station S2 empfängt die Überlagerung der übertragenen Rahmen Frame 3 und Frame 4.

Bestätigungsmechanismen

Bei der drahtlosen Datenübertragung können durchaus Kollisionen auftreten und die Datenpakete von verschiedenen sendenden Kommunikationsteilnehmern zerstören.

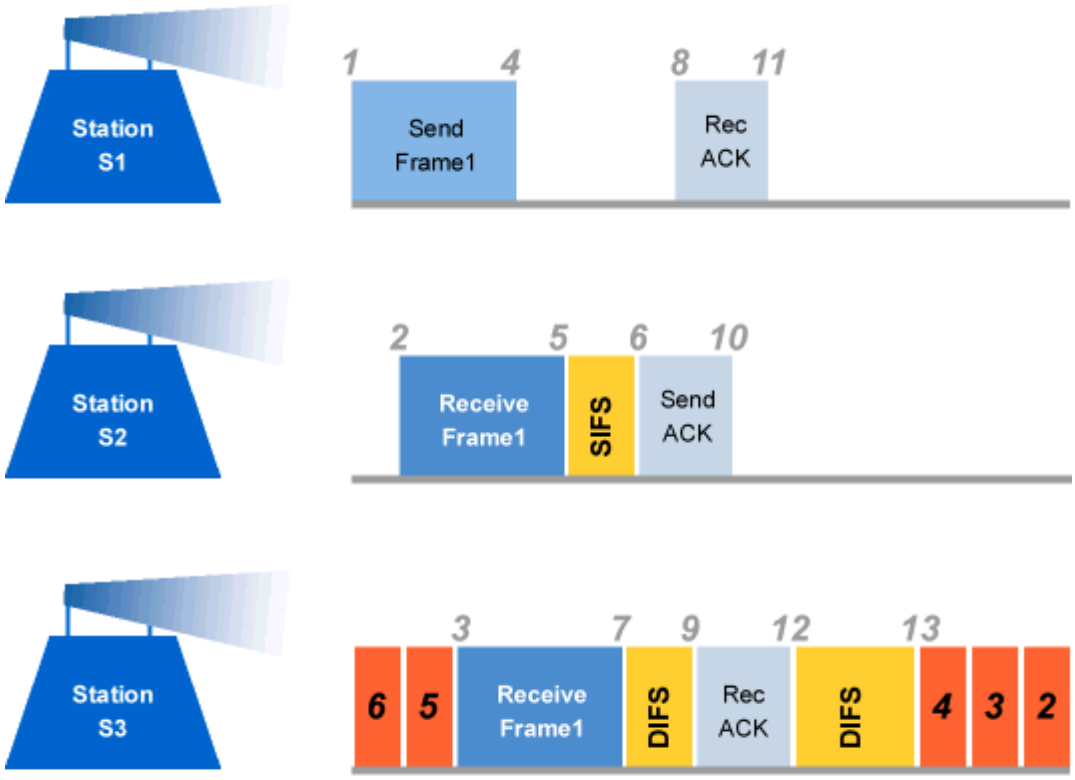
Hierin unterscheidet sich der CSMA/CA-Algorithmus nach 802.11 grundsätzlich von dem CSMA/CA-Verfahren, wie es bei seriellen Bussen eingesetzt wird. Dort können zwar auch Kollisionen auftreten. Durch die Festlegung von zwei Prioritätsebenen für die möglichen Signalpegel "0" und "1" setzt sich dort jedoch die "wichtigere" Nachricht störungsfrei durch.

Zudem besteht in drahtlosen Systemen keine realistische Möglichkeit, Kollisionen zu erkennen. Ein CSMA/CD-Algorithmus wie beim Ethernet nach 802.3 ist daher nicht möglich.

Deswegen muss bei der drahtlosen Übertragung nach 802.11 der ordnungsgemäße Empfang eines Rahmens quittiert werden. Die Versendung der Quittung (Acknowledgement - ACK) erfolgt nach einer Wartezeit, die man als Short Interframe Space (SIFS) bezeichnet. Dieser SIFS ist kürzer als der DIFS, so dass die Bestätigung nicht die Wartezeiten der normalen Datenübermittlung einhalten muss. Durch die kürzere Wartezeit erhalten die Quittungsrahmen eine höhere Priorität als die normalen Datenpakete.

SIFS und DIFS

Wie das Zusammenspiel zwischen Quittungs- und Datenrahmen funktioniert, sehen wir uns wieder an einem konkreten Beispiel an:



© tecChannel.de

Quittung zuerst: Der kürzere SIFS gibt ACKs gegenüber normalen Datenpaketen den Vorrang.

1: Station S1 beginnt die Übertragung eines Rahmens Frame 1 an S2. Zu diesem Zeitpunkt befindet sich S3 im Backoff-Prozess.

2: S2 beginnt mit dem ordnungsgemäßen Empfang von Frame 1.

3: Auch S3 empfängt den Rahmen. Das Medium wird als belegt erkannt, der Backoff-Zähler stoppt.

4: S1 beendet die Übertragung des Rahmens.

5: S2 erkennt das Medium wieder als frei. Da die Übertragung ordnungsgemäß abgeschlossen wurde, beginnt die Station ein SIFS-Warte-Intervall, um anschließend eine Quittung zu versenden.

6: Nach Ablauf von SIFS versendet S2 den ACK-Rahmen.

7: S3 erkennt das Medium wieder als frei und beginnt ein DIFS-Warte-Intervall.

8: S1 empfängt den ACK-Rahmen.

9: S3 empfängt den ACK-Rahmen und stellt fest, dass das Medium belegt ist. Daher bricht sie das noch nicht beendete DIFS-Warte-Intervall ab.

10: S2 beendet die Übertragung des ACK-Rahmens.

11: S1 beendet den Empfang des ACK-Rahmens.

12: S1 beendet den Empfang des ACK-Rahmens und beginnt ein neues DIFS-Warte-Intervall.

13: Nach dessen vollständigem Ablauf kann der Backoff-Zähler von S1 weiter dekrementiert werden.

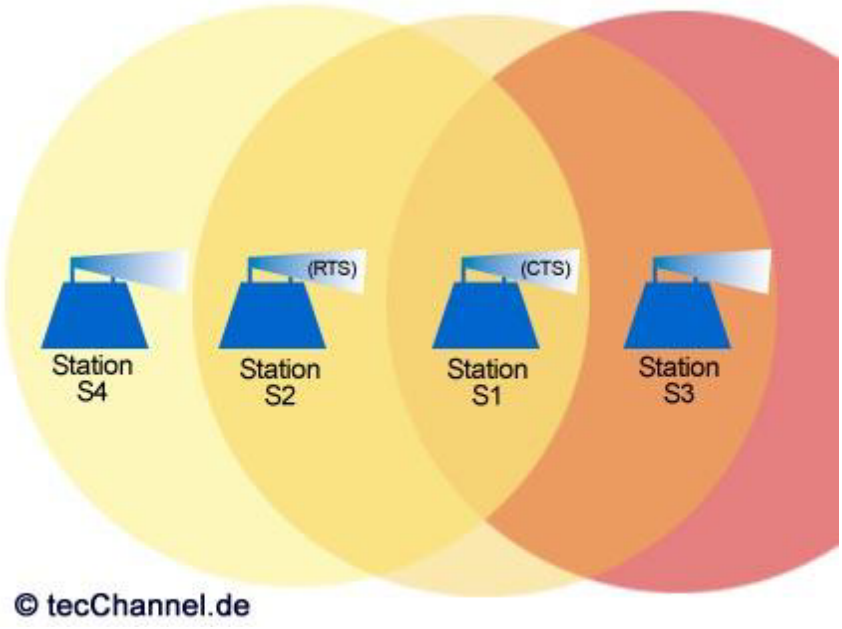
Verhalten bei Kollisionen

Während des Quittierungsverlaufs kann es vorkommen, dass eine Station S1 das Acknowledgement für das gesendete Paket nicht innerhalb des festgelegten Zeitintervalls empfängt. Dies kann (mindestens) zwei Ursachen haben: Zum einen könnte eine Kollision von zwei Datenpaketen aufgetreten sein. Zum anderen ist es nicht ausgeschlossen, dass der ACK-Rahmen selbst durch eine Kollision zerstört wurde. Letzteres tritt vor allem in ausgedehnten Funknetzen auf, wenn die Summe aus SIFS und der maximalen Ausbreitungszeit in Hin- und Rückrichtung größer ist als die DIFS einer sendebereiten Station.

Bleibt die Empfangsbestätigung aus, bereitet die sendende Station eine Retransmission vor. Dazu begibt sie sich in den Backoff-Zustand. Um die Wahrscheinlichkeit einer erneuten Kollision zu verringern, verdoppelt sie dazu nach jeder erfolglosen Übertragung den Wert des Contention Window, bis ein vorgegebenes Maximum CWmax erreicht ist. Nach einem erfolgreichen Sendevorgang setzt sie CW wieder auf den Ausgangswert CWmin zurück und hält so die Wartezeiten im System möglichst kurz.

Versteckte Stationen

Alle beschriebenen Verfahren funktionieren zuverlässig, solange sämtliche Stationen miteinander in Funkkontakt stehen. Ansonsten kann eine der Stationen das Medium als frei erkennen, obwohl dies für die andere Station nicht zutrifft. Ein mögliches Szenario zeigt die unten stehende Abbildung.



Hidden-Station-Problem: Nicht immer liegen alle Stationen innerhalb der gegenseitigen Reichweite.

Station S1 kann hier von zwei weiteren Stationen (S2, S3) Daten empfangen. Ein unmittelbarer Funkkontakt zwischen S2 und S3 ist dagegen nicht möglich. Sendet nun S3 eine Nachricht an S2, erscheint das Medium dennoch für S2 als frei. Überträgt gleichzeitig S1 ein Datenpaket an S2, kann S2 es nicht fehlerfrei empfangen. Anders als bei drahtgebundenen Medien lässt sich bei Funknetzen nur auf Empfängerseite prüfen, ob eine Kollision vorliegt.

Um solche Situationen zu vermeiden, beinhaltet das 802.11-Protokoll den so genannten RTS-CTS-Mechanismus. Ein Request-To-Send-Rahmen (RTS) wird von der sendewilligen Station an den

Empfänger geschickt und von diesem mit einem Clear-To-Send-Rahmen (CTS) beantwortet. Klappt dieser Austausch problemlos, beginnt der Sender nach Ablauf der SIFS-Zeit die Datenübertragung.

RTS, CTS und NAV

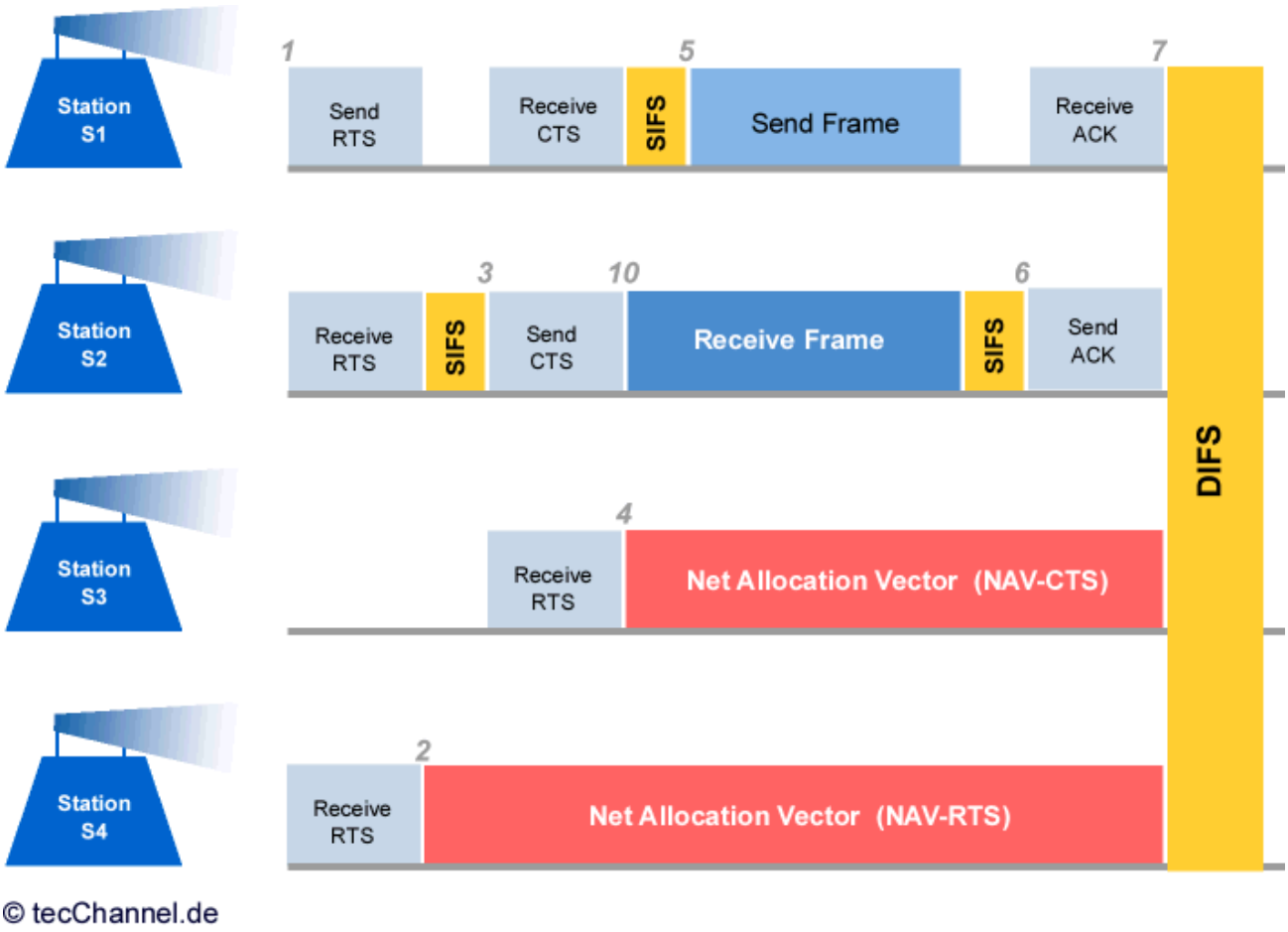
Falls der CTS-Rahmen nicht innerhalb einer festgelegten Zeitdauer empfangen wird, beginnt der RTS-CTS-Austausch nach Ablauf eines normalen Backoff-Zyklus erneut. Durch die Verwendung von SIFS erhalten CTS-Antworten dabei eine höhere Priorität als der normale Datenverkehr.

Zwei Sachverhalte gilt es im Zusammenhang mit dem RTS-CTS-Mechanismus allerdings im Hinterkopf zu behalten. Zum einen schreibt 802.11 die Implementierung der RTS-Seite nicht zwingend vor. Es muss lediglich jedes Gerät in der Lage sein, einen RTS-Frame innerhalb der geforderten Zeit mit dem zugehörigen CTS-Rahmen zu beantworten.

Zum anderen enthalten die RTS- und CTS-Frames ein Feld, das die Dauer für die Übertragung des Datenrahmens angibt. Diese Information werten alle Stationen aus, die RTS/CTS-Signale empfangen. Sie aktivieren in diesem Fall einen Zeitgeber (Net Allocation Vector - NAV), der im Gegensatz zum Backoff-Zähler unabhängig vom Zustand des Übertragungsmediums dekrementiert wird. Während der resultierenden NAV-Zeit beginnen die jeweiligen Stationen nicht mit Übertragungsvorgängen, was die Wahrscheinlichkeit von Kollisionen drastisch verringert.

Ablauf des RTS-CTS-Mechanismus

Auch hier verdeutlichen wir uns die Funktionsweise anhand eines praktischen Beispiels. In der unten stehenden Abbildung sehen Sie das zugehörige Zeitdiagramm (ohne Berücksichtigung der Signallaufzeiten auf dem Medium).



Kollisionsvermeidung: Per RTS und CTS reservieren sich kommunikationswillige Stationen das Netz.

1: S1 beginnt die Übertragung eines RTS-Rahmens an S2. Auch S2 und S4 empfangen diesen Frame.

2: Nach dem Empfang des RTS-Rahmens setzt S4 den NAV-Zeitgeber und verhält sich ruhig. Der NAV von S4 enthält die benötigte Zeit für CTS-, Daten- und ACK-Rahmen zuzüglich der jeweiligen SIFS-Intervalle.

3: Ein SIFS-Zeitintervall später sendet S2 den CTS-Rahmen. Er kann auch von S1 und S3 empfangen werden.

4: S3 setzt seinen NAV-Zeitgeber auf die für die Übertragung des Daten- und des ACK-Rahmens benötigte Zeit zuzüglich der dazwischen liegenden SIFS-Zeit und verhält sich ruhig.

5. S1 überträgt nach dem Empfang des CTS-Rahmens und einem SIFS-Intervall den Datenrahmen.

6. S2 bestätigt den Empfang nach einem SIFS-Intervall mit einem ACK-Rahmen.

7: Die Datenübertragung ist erfolgreich abgeschlossen, die NAV-Zeitgeber der beiden an der Kommunikation nicht beteiligten Stationen sind abgelaufen. Nach Verstreichen einer DIFS-Zeit kann eine neue Datenübertragung beginnen.

Der RTS-CTS-Mechanismus schützt zwar offensichtlich vor Kollisionen, verursacht aber zusätzlichen Protokollverkehr. Um den Overhead bei kurzen Datenpaketen zu minimieren, wird der RTS-CTS-Austausch erst ab einer gewissen Paketgröße (RTS threshold) aktiviert. Daneben bewährt sich der RTS-CTS-Mechanismus auch beim Betrieb überlappender BSS und IBSS

Point Coordination Function

Die Point Coordination Function dient der Unterstützung zeitkritischer Dienste. Sie erlaubt dem jeweiligen Point Coordinator (PC) den priorisierten Zugriff auf das Übertragungsmedium. So agiert üblicherweise ein Access Point mit Festnetz-Zugang als PC. Zwar definiert 802.11 PCF als optional. Dennoch müssen alle Stationen in der Lage sein, den entsprechenden Medien-Zugriffsregeln Folge zu leisten. Stationen, die auf Anfragen des PC auch antworten können, werden CF-Pollable genannt. Neben dem AP können nur solche Stationen Daten entsprechend der PCF übertragen.

Die PCF steuert die Übertragung der Rahmen während einer wettbewerbsfreien Zeit (Contention Free Period - CFP), die sich mit der durch die DCF gesteuerten Wettbewerbs-Periode abwechselt. Die CFP wird in regelmäßigen Zeitabständen mit der CFP-Rate wiederholt und startet mit der Übertragung eines Beacons (Englisch Leuchtfeuer, Signalfeuer), der die maximale Dauer der CFP enthält. Alle Stationen im BSS außer dem PC setzen ihren NAV auf diesen Wert.

Ist das Übertragungsmedium frei, übernimmt nach Ablauf der PCF-IFS (PIFS) zu Beginn der CFP der PC die Steuerung. Die PIFS ist länger als die SIFS, aber kürzer als die DIFS. Die PCF weist also eine höhere Priorität auf als die normale Übertragung, muss jedoch Quittierungen abwarten. Während der gesamten CFP bleibt der PC steuernd tätig. Er führt eine so genannte Polling List und fragt in der CFP alle Stationen auf dieser Liste der Reihe nach ab, ob sie eine Übertragung wünschen. Dabei identifiziert er die Stationen über einen Association Identifier (AID).

802.11: Der PHY-Layer

Auf der Bitübertragungsschicht ergeben sich naturgemäß die größten Unterschiede zur drahtgebundenen Kommunikation. Bei der Spezifikation des physischen Protokolls sind die Eigenschaften der Übertragung über die Luftschnittstelle zu berücksichtigen. Das gilt besonders für die möglichen Störungen, für die im Wesentlichen drei Ursachen in Frage kommen:

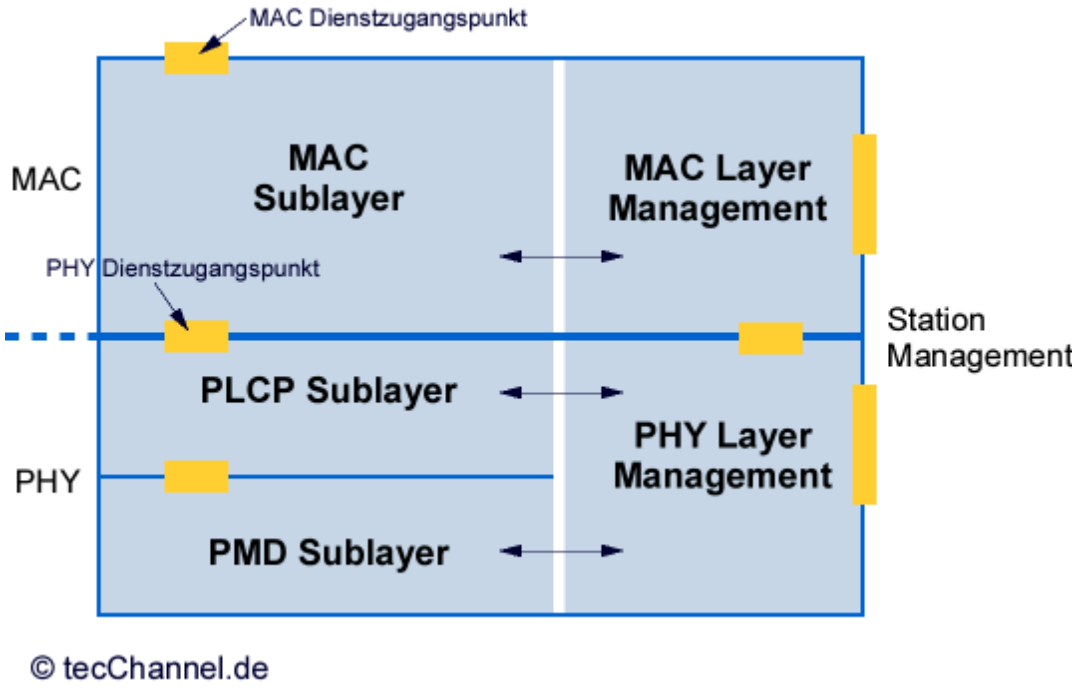
- Rauschen und Interferenzen im Übertragungskanal
- Signale anderer Stationen, die nach dem 802.11-Standard arbeiten. Selbst wenn deren Signalpegel für einen Datenaustausch nicht mehr ausreicht, können sie unter Umständen die

Übertragungsverfahren noch beeinflussen.
- Signale anderer Stationen, die nicht dem 802.11-Standard entsprechen, aber den gleichen Frequenzbereich nutzen.

Alle für das 2,4-GHz Band genutzten Protokolle greifen dazu auf Frequenz-Spreizverfahren zurück. IEEE802.11 sieht dazu zwei verschiedene Techniken vor: Frequency Hopping Spread Spectrum (FHSS) und Direct Sequence Spread Spectrum (DSSS). Als zusätzliches Bitübertragungsprotokoll sieht der Standard eine physische Infrarot-Schnittstelle im Wellenlängenbereich von 850 bis 950 nm vor, die jedoch keine praktische Relevanz erlangt hat.

Aufbau des PHY-Layer

Auf Grund der Tatsache, dass die Charakteristika der drei möglichen Übertragungsverfahren speziell in ihrem Zeitverhalten sehr unterschiedlich sein können, sieht 802.11 eine weitere Aufteilung der Protokolle in den einzelnen Schichten vor. Neben der auch in anderen Protokollen üblichen Aufteilung einer Schicht in einen Sublayer und einen Management-Layer ist hier die weitere Aufteilung der Bitübertragungsschicht besonders interessant.

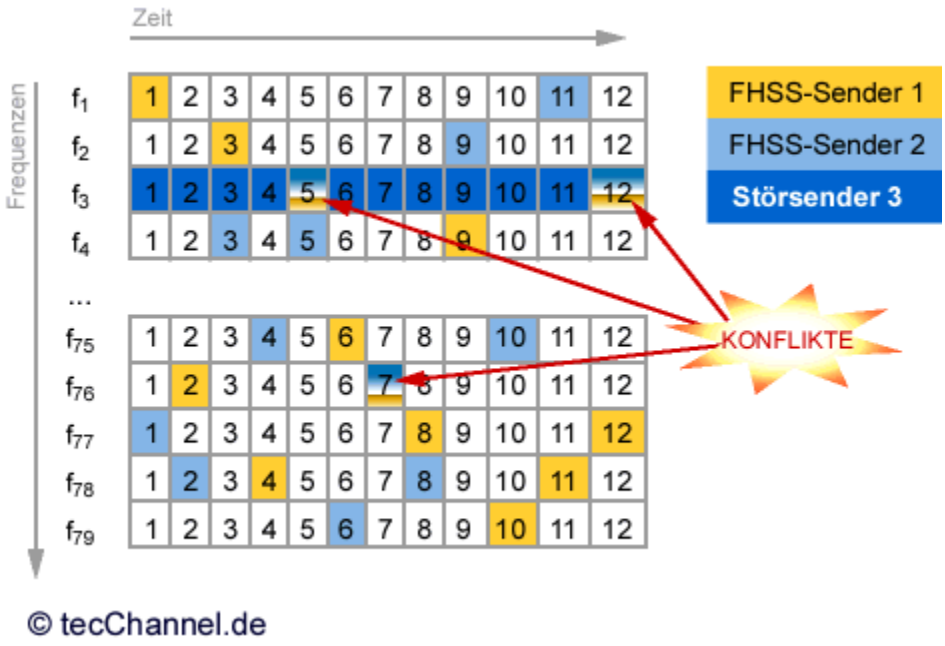


802.11-PHY: Der PLCP Sublayer stellt den höheren Protokollschichten ein medienunabhängiges Interface zur Verfügung.

In dieser Konfiguration übernimmt das Physical Medium Dependant Sublayer (PMD) die Modulation und Kodierung, während das Physical Layer Convergence Protocol (PLCP) unabhängig vom Medium eine übliche PHY-Schnittstelle zur Verfügung stellt. Insbesondere liefert das PLCP auch das Clear Channel Assignment Signal (CCA), das den aktuellen Zustand des Mediums anzeigt.

FHSS: Funktionsprinzip

Das FHSS -Verfahren erlaubt auf einer einfachen Basis den gleichzeitigen Betrieb mehrerer Systeme im selben Frequenzbereich. Dabei sorgt es für eine faire Verteilung des Übertragungsmediums. Das Prinzip des Frequency Hopping besteht darin, dass sowohl Sender als auch Empfänger die Trägerfrequenz nach einer festgelegten Abfolge wechseln



Störresistent: Durch den steten Wechsel der Sendefrequenz minimiert FHSS den Einfluss potenzieller Störquellen.

Wie das funktioniert, verdeutlicht die oben stehende Abbildung. Der Sender 1 hat beispielsweise mit seiner Gegenstelle die Frequenzfolge f1, f76, f2, f78, f3, f75, f76, f77, f4, f79, f78, f77 ausgehandelt. Der laufende Wechsel begrenzt Störungen durch frequenzfeste Stationen, etwa einen Mikrowellenherd (Station 3), oder durch andere FHSS-Sender (Station 2) auf sehr kurze Zeitabschnitte.

FHSS: Frequenznutzung

Für das FHSS-Verfahren sieht IEEE802.11 bis zu 79 nicht überlappende Frequenzbereiche mit einer Bandbreite von je 1 MHz vor. Dabei fasst es drei Gruppen mit je 26 Mustern zusammen. Die Abfolge der Frequenzen wird aus einer Basisfolge berechnet, die einer Pseudo-Zufallskette im Intervall von 0 bis 78 entspricht. Die minimale Sprungdistanz beträgt dabei 6 Kanäle.

Die Basisfolge wird beispielsweise vorgegeben als:

b(i) = 0, 54, 70, 45

Die Übertragungsfrequenz der Basisfolge ergibt sich dann als:

f0(i) = 2402 + b(i) [GHz]

Die Übertragungsfrequenz des k-ten aus dieser Basisfolge abgeleiteten Musters berechnet sich zu:

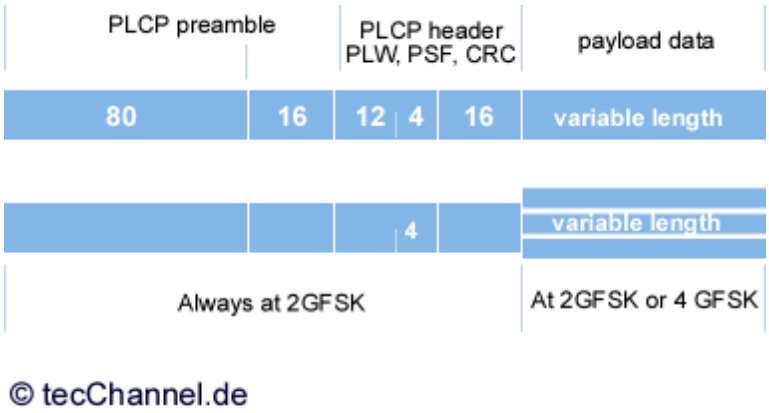
fk(i) = 2402 + (b(i) + k) mod 79 [GHz]

In den Regionen mit einer eingeschränkten Breite des ISM-Bands (Japan, Frankreich, Spanien) reduziert sich mit der Anzahl der nutzbaren Frequenzbereiche auch die mögliche Gerätedichte

FHSS: Nutzbare Sprungsequenzen			
Region	**Frequenzband (GHz)**	**Sprungfrequenzen (GHz)**	**Nutzbare Sequenzen**
Europa, USA	2,4000- 2,4835	2,402- 2,483	79
Japan	2,4710- 2,4970	2,473- 2,495	23
Frankreich	2,4465- 2,4835	2,447- 2,473	27
Spanien	2,4450- 2,4750	2,448- 2,482	35

FHSS: Rahmenformat

Das Rahmenformat auf der FHSS -Übertragungsstrecke verdeutlicht die unten stehende Abbildung. Grundsätzlich zerfallen die Frames in eine Präambel, den Header sowie die eigentlichen Nutzdaten. Die Präambel besteht aus festgelegten Bitfolgen. Die ersten 80 Bit dienen vor allem der Signalerkennung, es folgt ein 16 Bit langer Frame Delimiter zur Synchronisierung. Der Header beginnt mit einem 12 Bit langen Length Word (PLW), das die Länge des Datenpakets in Bytes angibt. Daran schließt sich ein 4 Bit langes Signaling Field (PSF) an, das die gewünschte Übertragungsgeschwindigkeit anzeigt. Es folgt ein 16 Bit langer, per CRC errechneter Header Error Check.

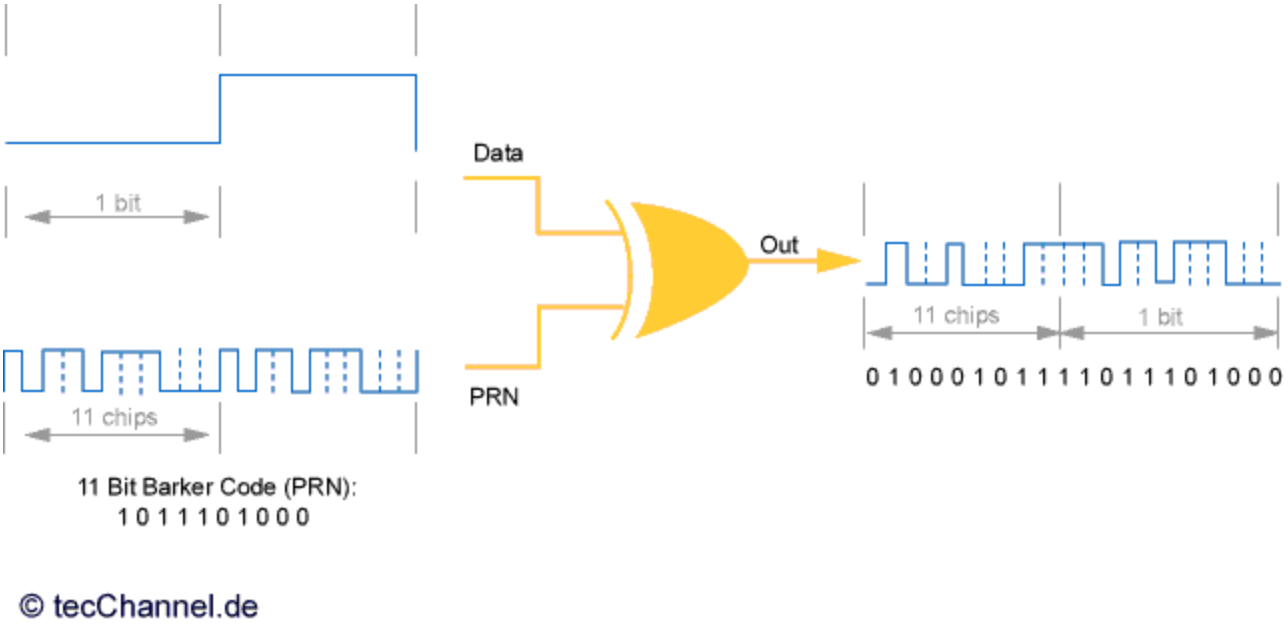


FHSS-Paketformat: Die PLCP-Präambel dient vornehmlich der Synchronisation, der Header übermittelt Längen- und Korrekturinformationen.

Präambel und Header werden grundsätzlich mit einer Datenrate von 1 MBit/s übertragen, während sich die Datenpakete mit 1 oder 2 MBit/s senden lassen. Dabei ist die Betriebsart mit 1 MBit/s im ursprünglichen 802.11-Standard von 1997 für alle Geräte vorgeschrieben. Erst später wurde dem Standard eine optionale Übertragungsrate von 2 MBit/s hinzugefügt. Die Erhöhung der Bandbreite resultiert dabei aus einer Multilevel-Modifikation der ursprünglichen GFSK-Modulation (Gaussian Phase Shift Keying). Sie verdoppelt die Signalrate auf zwei Bits pro Symbol.

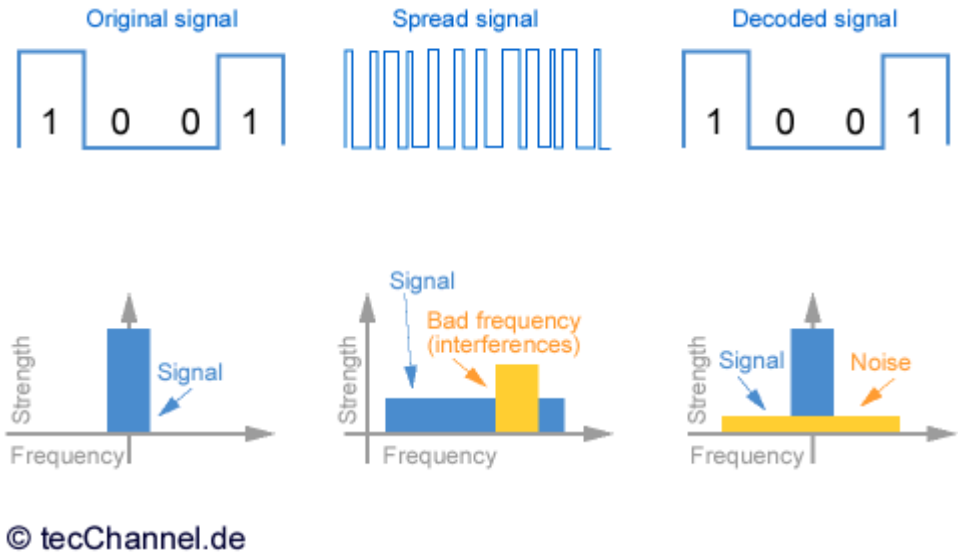
DSSS: Funktionsprinzip

Direct Sequence Spread Spectrum realisiert die Frequenzspreizung durch eine XOR-Verknüpfung der Daten mit einer Zufallsdatenfolge. Die verwendete Pseudo-Random Numerical Sequence (PN) weist eine höhere Bitrate auf als der Nutzdatenstrom. Die einzelnen Signale innerhalb der PN-Sequenz bezeichnet man dabei als Chips. Dieser Datenstrom mit höherer Bitrate wird nun noch moduliert (Phase Shift Keying - PSK). Die Verknüpfung mit der PN-Folge spreizt das Leistungsspektrum des Signals über den verfügbaren Frequenzbereich, lässt die Signalleistung jedoch unverändert.



Direct Sequence: Auf der Sendeseite verknüpft DSSS die Daten mit einer zufallsgenerierten Bitfolge

Bei der Spreizung mit einem elfstelligen Barker-Code, der besonders gute Autokorrelations-Eigenschaften aufweist, ergibt sich eine Bandbreite von 22 MHz pro Sequenz. Die Länge des Barker-Codes entspricht dabei der in den Freigaberichtlinien der Aufsichtsbehörden festgelegten Mindestlänge für einen Spreizcode.

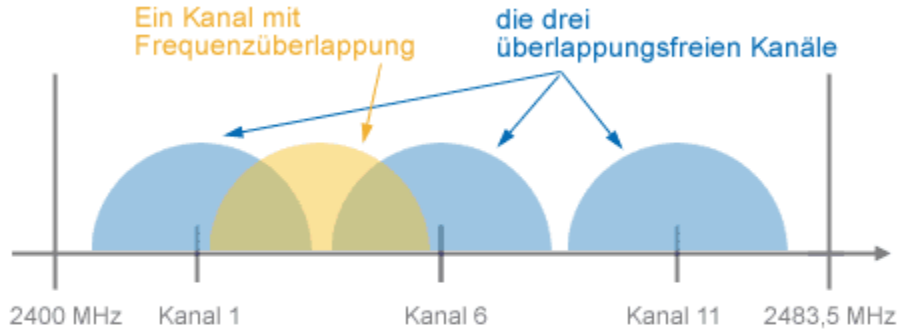


Wenig anfällig: Die Aufspreizung des Signals minimiert die Auswirkungen schmalbandiger Störungen.

Auf der Empfängerseite dient ein so genannter angepasster Korrelator zum Ausfiltern der Nutzdaten aus der überlagerten PN-Folge. Verschiedene Filter setzen dazu jeweils unterschiedliche PN-Folgen an. Der Filter mit dem besten Output transformiert anschließend das Leistungsspektrum des gespreizten Signals zurück. Dabei wandelt er automatisch schmalbandige Störungen hoher Intensität in ein breitbandiges Rauschen niedriger Intensität um.

DSSS: Frequenznutzung

Aus der Kanalbandbreite von 22 MHz folgt, dass sich im ISM-Band lediglich drei DSSS-Kanäle nebeneinander anordnen lassen. Der massive Vorteil des Verfahrens besteht jedoch darin, dass sich die gespreizten Frequenzbänder auch überlappen dürfen. Im 802.11-Standard sind dazu insgesamt 14 Sequenzfolgen festgelegt. Auch hier ergeben sich, wie schon bei FHSS, lokale Unterschiede



Überlappung möglich: IEEE802.11 sieht für das ISM-Frequenzband bis zu 14 mögliche Kanäle vor.

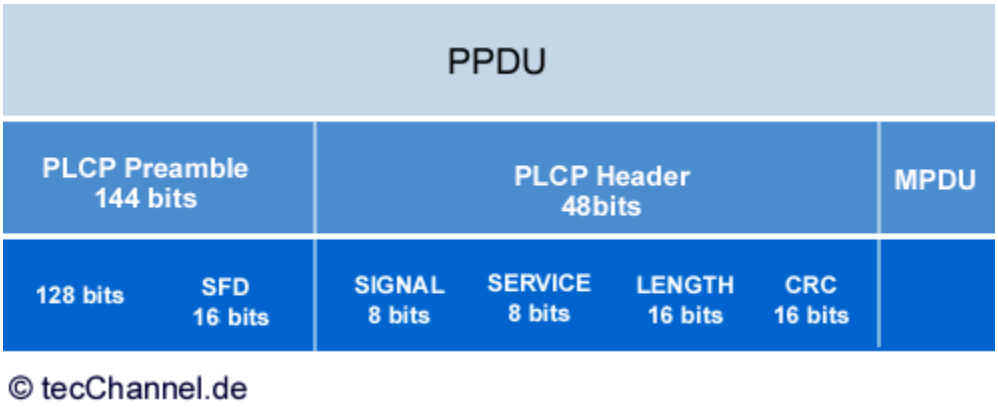
Das Direct-Sequence-Prinzip kommt übrigens auch in CDMA-Mobilfunknetzen zum Einsatz. Dort erhalten aber meist alle Kanäle die gleiche Basisfrequenz und unterscheiden sich nur durch die unterschiedlichen PN-Sequenzen.

DSSS: Verfügbare Kanäle

Region	Frequenzband (GHz)	DSSS- Nutzung (GHz)	Kanäle	Sendeleistung
USA	2,4000 - 2,4835	2,412 - 2,462	11	1000 mW
Europa	2,4000 - 2,4835	2,412 - 2,472	13	100 mW (EIRP)
Japan	2,4710 - 2,4970	2,484	1	10 mW/MHz
Frankreich	2,4465 - 2,4835	2,457 - 2,462	2	100 mW (EIRP)
Spanien	2,4450 - 2,4750	2,457 - 2,472	4	100 mW (EIRP)

DSSS: Rahmenformat

Das Rahmenformat auf der DSSS-Übertragungsstrecke verdeutlicht die unten stehende Abbildung. Grundsätzlich zerfallen die Frames in eine Präambel, den Header sowie die eigentlichen Nutzdaten. Wie bei FHSS besteht die Präambel aus festgelegten Bitfolgen. Die ersten 128 Bit dienen vor allem der Signalerkennung, es folgt ein 16 Bit langer Frame Delimiter zur Synchronisierung. Der Header beginnt mit einem Signal Field in Byte-Länge, das die gewünschte Übertragungsgeschwindigkeit anzeigt. Daran schließt sich ein 8 Bit langes Service-Kennzeichen an, das für die künftige Benennung von Diensten reserviert ist. Es folgen ein Length Word, das die Länge des Datenpakets in Bytes angibt, sowie ein CRC-basierter Header Error Check.



DSSS-Frame-Format: Präambel und Header fallen deutlich umfangreicher aus als bei FHSS

Die Übertragung von Präambel und Header erfolgt grundsätzlich mit einer Datenrate von 1 MBit/s, für Datenpakete lässt sich die Bandbreite wie bei FHSS optional verdoppeln. Damit sich Bündelfehler besser ausgleichen lassen, werden die Daten via Scrambler in eine neue Abfolge gebracht. Im Gegensatz zu Systemen der Sprachübertragung dient diese Verwürfelung nicht der höheren Fehlertoleranz bei Büschelfehlern, sondern einem Ausgleich des Frequenzspektrums (Whitening)

802.11-Zusatzfeatures

Neben den für MAC- und PHY-Layer beschriebenen Eigenschaften kennt IEEE802.11 weitere Gerätemerkmale. Dazu zählen beispielsweise Synchronisation und ein Energiesparmodus.

Die Timing Synchronisation Function (TSF) dient zum Abgleichen der Systemzeit aller Stationen. Sie wird durch regelmäßiges Versenden des TSF-Zeitgebers zu den durch Target Beacon Transmission Times (TBTT) festgelegten Zeiten in einem so genannten Beacon gewährleistet. In Infrastrukturnetzen zeichnet der Access Point für dessen Aussendung verantwortlich, in Ad-hoc-Netzen teilen sich alle Stationen diese Aufgabe. Dazu strahlen die Stationen den Beacon mit verschiedenen, zufällig ausgewählten Verzögerungszeiten aus.

Da viele der drahtlosen Geräte mobil und somit batteriebetrieben arbeiten, sieht der Standard auch einen Energiesparmodus vor. Dessen Einsatz muss allerdings mit den anderen Stationen im Netz "abgesprochen" werden. Auch im so genannten Doze-Modus bleiben die Stationen weiter ansprechbar. Dafür sorgen spezielle Monitoring-Algorithmen, die sich im Infrastruktur- und Ad-hoc-Modus unterscheiden.

Sicherheit im Funknetz

Drahtlose Netzwerke stellen ein gewisses Sicherheitsrisiko dar. Die Ausbreitung der Funkwellen beschränkt sich ja nicht auf das Netzwerk im engeren Sinn, die Konversation kann von jedem innerhalb der Funkreichweite befindlichen IEEE802.11-Empfänger abgehört werden. Daher sieht der Standard die Implementierung einer Reihe von Sicherheitsmerkmalen vor.

Auf der niedrigsten Ebene erfolgt die Zulassung der Teilnehmer über einen als Electronic System ID (SSID, ESSID) bezeichneten Schlüssel. Die für alle Systeme im Netz identische SSID legt der Administrator bei der Konfiguration der Clients und Access Points fest.

Daraus resultieren zwei gravierende Einschränkungen. So zeigt die SSID zwar das allgemeine Zugangsrecht des Teilnehmers an, eine eindeutige Identifikation erlaubt sie aber nicht. Zudem ist es häufig kein Problem, die SSID eines WLANs herauszufinden. Dazu trägt nicht zuletzt bei, dass die meisten Hersteller erlauben, in den Konfigurationsdateien für die SSID die Option "any" anzugeben: Dies authentisiert den Einsatz in allen Funknetzwerken.

Authentifizierung auf Link- und Benutzerebene

In Infrastruktur-Netzen lässt sich der Zugang zum Netz auf zugelassene Stationen beschränken. Die Identität der Endgeräte wird bei der im Rahmen des 802.11 möglichen Link Level Authentification zwischen den beteiligten Stationen ausgetauscht. Dazu muss der Administrator die MAC-Adressen der Geräte in die Zugangslisten der Access Points eintragen.

Hier bleibt jedoch ebenfalls ein gewisses Sicherheitsrisiko bestehen. Bei den meisten auf dem Markt verfügbaren Produkten lässt sich die MAC-Adresse des Rechners verändern, so dass auch hier ein missbräuchlicher Einsatz möglich erscheint. Zudem ergibt sich - zumindest in größeren Netzen - ein Problem praktischer Natur: Bislang bieten nur wenige Hersteller komfortable Werkzeuge zum Verwalten ausgedehnter WLANs an. Daher kommt in Netzen mit vielen Teilnehmern und Access Points ein erheblicher Administrationsaufwand auf den Systemverwalter zu, wenn er den Benutzern ein komfortables Roaming ermöglichen will.

Um die Authentifizierung nicht nur auf Geräteebene, sondern auch benutzerbezogen zu unterstützen, implementieren daher fast alle Hersteller inzwischen den Remote Authentification Dial-In User Service (RADIUS). Er ermöglicht die zentrale Verwaltung von Benutzeridentifikationen und Passwörtern.

Verschlüsselung mit WEP

Der Inhalt von Funknachrichten kann im Rahmen der Wired Equivalent Privacy (WEP) nach einem 40-Bit-RC4-Algorithmus verschlüsselt werden. Dabei handelt es sich allerdings um einen optionalen Bestandteil des Standards, der nicht in jeder Implementierung vorhanden sein muss. Zudem setzen die Hersteller proprietäre Werkzeuge zur Schlüsselverwaltung ein, worunter die Interoperabilität zwischen WLAN-Komponenten unterschiedlicher Herkunft leidet.

Sowohl die Tatsache, dass es sich hier um ein relativ gut angreifbares Stromchiffrier-Verfahren handelt, als auch die geringe Schlüsseltiefe haben in der letzten Zeit für einige Diskussionen rund um WEP gesorgt. So kommt etwa eine an der University of California in Berkeley (UCB) zusammengestellte Untersuchung zu dem Schluss, dass WEP sowohl gegen aktive wie passive Kryptoanalysen verwundbar sei.

Über die 40-Bitkodierung hinaus bieten mittlerweile die meisten Hersteller eine Kodierung mit 128 Bit Verschlüsselungstiefe an. Hierbei handelt es sich allerdings um proprietäre Entwicklungen, die nicht herstellerübergreifend zusammenarbeiten. Zudem legen die Ergebnisse der UCB-Untersuchung nahe, dass die Verwundbarkeit von WEP eher mit dem Systemdesign als der Schlüsseltiefe zusammenhängt.

Daher sollte man beim Einsatz von WLANs zusätzliche Schutzmechanismen in Erwägung ziehen. So lassen sich auf Grund der Einbettung in die IEEE802-Standards auch bei WLANs alle Sicherheitsmechanismen der höheren Protokollebenen, wie etwa IPSec, problemlos einsetzen.

Antennentechnik

Die Übertragung mit Hilfe elektromagnetischer Wellen setzt den Einsatz von Sende- und Empfangsantennen voraus. Hier existieren verschiedene Bauformen, die zwar nicht im Standard beschrieben werden, jedoch die Leistungsfähigkeit stark beeinflussen können. Dabei bestimmt die Richtcharakteristik der Antenne wesentlich die Reichweite und die Qualität der Funkübertragung und damit die erzielbare Geschwindigkeit.

So lässt sich beispielsweise mit Richtantennen die verfügbare Sendeleistung auf einen geringen Raumwinkel bündeln. Auf diesem Weg können auch in Europa, wo die maximale Sendeleistung auf 100 mW beschränkt ist, fest installierte Systeme bei Sichtverbindung Reichweiten von 1 bis 2 km erzielen. Damit eignen sich 802.11b-Systeme auch für die Kopplung räumlich entfernter LANs.

Beim mobilen Einsatz dagegen stört eine Richtcharakteristik eher. Hier ist eine möglichst gleichmäßige Ausstrahlung in alle Richtungen anzustreben. Zwar erreichen die mit den meisten Systemen ausgelieferten Antennen diese Richtungsunabhängigkeit problemlos. Jedoch kann die Abstrahlung durch unmittelbar in der Nähe der Antenne befindliche Gegenstände abgeschattet werden. Deswegen ist der Standort der Antennen von zentraler Bedeutung.

Bauformen von Antennen

Die Baugröße von WLAN-Antennen hält sich auf Grund der verwendeten Wellenlänge in komfortablen, handhabbaren Grenzen. So misst eine Antenne mit der Länge einer Wellenlänge im 2,4-GHz Band etwa 12,5 cm. Entsprechend lässt sich eine (/4-Antenne auf etwas mehr als 3 cm unterbringen. Wegen der geringen Antennenmaße existiert eine Vielzahl von Bauarten. Integrierte Antennen passen problemlos an die WLAN-PC-Card oder in den Deckel von Notebooks.

Für stationäre Geräte eignen sich dagegen eher externe Antennen. Zwar fügt diese Anschlussform dem Kabelgewirr unter dem Schreibtisch eine weitere lästige Leitung hinzu. Andererseits können im stationären Einsatz bereits wenige Dutzend Zentimeter Standortdifferenz über Wohl oder Wehe der drahtlosen Verbindung entscheiden. Eine Verschiebung der Antenne lässt sich im Zweifelsfall wesentlich leichter vornehmen als ein Standortwechsel des Rechners.

Herstellerspezifische Merkmale

Die Hersteller von 802.11-Geräten haben nur wenige Möglichkeiten, sich von den Mitbewerbern zu differenzieren. Bei Systemen, die nach einem festen Standard arbeiten, lässt sich das über die eigentliche Funktionalität des Geräts kaum erreichen. Die Differenzierung kann lediglich über Zusatzdienste erfolgen, die über die im Standard beschriebenen Funktionen hinausgehen.

Dabei ergeben sich einige typische Ansatzpunkte. Dazu zählt nicht zuletzt die Sicherheit: Die Implementierung des optionalen WEP und die Kodierung mit 128 Bit haben wir bereits angesprochen. Auch bei der Administration gehen die Hersteller eigene Wege. Bieten sie eine zentrale Geräte- oder Benutzerverwaltung, bezieht diese meist nur die eigenen Systeme in die Erkennung ein und kann Geräte anderer Hersteller nicht oder nur eingeschränkt administrieren.

Die genannten und verschiedene weitere "kleingedruckte" Aspekte beeinträchtigen in der Praxis die Interoperabilität der Systeme wesentlich. Deshalb empfehlen praktisch alle verfügbaren Testergebnisse, trotz des zu Grunde liegenden einheitlichen Standards, beim Aufbau von WLANs möglichst nur Systeme eines Herstellers zu verwenden.

802.11a: Standard mit Schwierigkeiten

Während der 802.11-Standard im 2,4 GHz- ISM-Band operiert, nutzt die Variante 802.11a eine Übertragung im 5-GHz-UNII-Bereich. IEEE hat hier Datenraten von 6 bis 54 MBit/s geplant, Standards für 6, 12 und 24 MBit/s wurden bereits festgelegt. Die ersten 802.11a-konformen Geräte sollen Ende 2001 erscheinen.

IEEE802.11a greift auf ein Orthogonal Frequency Division Multiplexing (OFDM) zurück. Dieses Verfahren soll insbesondere den mit der Varianz der Signallaufzeiten (Delay Spread) über unterschiedliche Ausbreitungspfade (Multipath) verbundenen Schwierigkeiten begegnen. Der hier gewählte Ansatz besteht darin, die Symboldauer recht lang zu wählen und eine Modulationsart mit einem großen Verhältnis von Bits zu Symbolen zu wählen. Dabei benutzt OFDM eine Reihe von Unterfrequenzen (Subcarrier Frequencies), die zueinander orthogonal sind. Jede Unterfrequenz lässt sich getrennt auf die Besonderheiten des Übertragungskanals anpassen.

Allerdings bringt 802.11a bislang einige wesentliche Nachteile mit sich. So bestehen im 5-GHz Band deutliche Probleme durch Rauschen, Abschattungen und andere parasitäre Effekte. Die entsprechenden technischen Gegenmaßnahmen verteuern die Endgeräte deutlich. Zudem ist der UNII-Bereich bis dato lediglich in den USA zur Benutzung freigegeben. In Europa hat ETSI Teile dieses Frequenzbands bereits für konkurrierende drahtlose Übertragungssysteme wie HiperLAN und

HiperLAN2 reserviert. Und nicht zuletzt verbaut der Wechsel in einen ganz anderen Frequenzbereich eine kostengünstige Migration bereits installierter WLAN-Systeme.

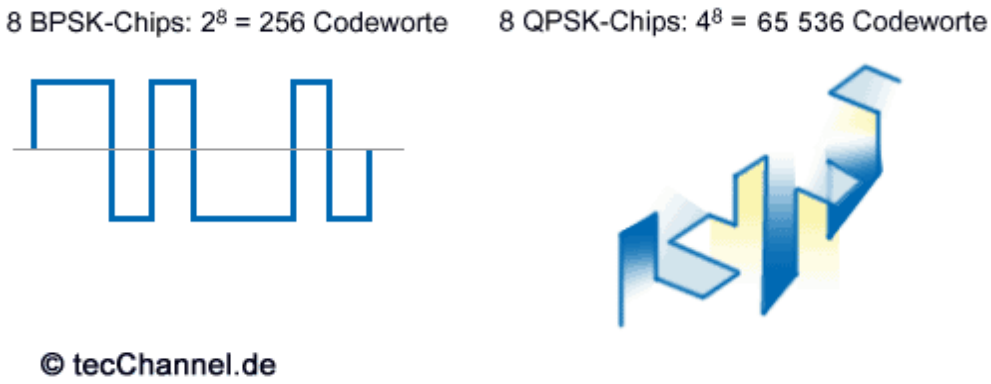
802.11b: Die schnelle Variante

Die genannten Nachteile von 802.11a haben dazu geführt, dass stattdessen die Variante 802.11b sehr beliebt geworden ist. Der im September 1999 ratifizierte Standard (in älteren Quellen auch als 802.11HR bezeichnet) spezifiziert Systeme mit einer Bandbreite von 5,5 oder 11 Mbps im 2,4-GHz-Band. Als Bandspreizverfahren kommt einheitlich DSSS in einer zu 802.11/1997-DSSS-kompatiblen Form zum Einsatz. Der gemeinsame PHY-Standard soll die Interoperabilität aller standardisierten 802.11b -Geräte gewährleisten.

Wegen der höheren Datenrate benötigt 802.11b einen verbesserten Signal-Rausch-Abstand (Signal-to-Noise-Ratio - SNR). Das macht sich sowohl in einer höheren Störempfindlichkeit als auch in geringeren Reichweiten bemerkbar. Als Adaptionsmaßnahme passt 802.11b die Datenrate dynamisch und für die höheren Protokollschichten transparent an die Gegebenheiten des Übertragungskanals an. Das kann dazu führen, dass auch Systeme nach 802.11b nur mit 1 oder 2 MBit/s übertragen.

Verbesserte Modulationsverfahren

Die Erhöhung der Datenrate basiert im Wesentlichen auf einem Modulationsverfahren mit verbesserter Nutzung des Frequenzspektrums. Das hier zum Zuge kommende Quadrature Phase Shift Keying (QPSK) überträgt mehr Bits pro Symbol als das bei 802.11 eingesetzte Binary Phase Shift Keying (BPSK). Darüber hinaus werden andere PN-Folgen eingesetzt, die man als Complimentary Code Keying (CCK) bezeichnet (siehe Abbildungen).



Modulation: CCK erweitert das ursprünglich vorgeschlagene MBOK zu komplexen Strukturen.

Im Sinne des Investitionsschutzes hatten vor allen Dingen die Hersteller Lucent und Harris (Prism) versucht, mit der Entwicklung proprietärer Systeme den Standardisierungsprozess im 2,4-GHz-Bereich für ihre Produkte zu entscheiden. Aber das Standardisierungsgremium wählte weder die Pulse Position Modulation (PPM) von Lucent für Datenraten von 5 und 10 MBit/s noch das MBOK (M-ary Bi-Orthogonal Keying) von Harris mit Datenraten von 5,5 und 11 MBit/s.

802.11b: Datenraten und Modulation

Datenrate	Codelänge	Modulation	Symbolrate	Bits/Symbol
1 MBit/s	11 (Barker)	BPSK	1 MS/s	1
2 MBit/s	11 (Barker)	QPSK	1 MS/s	2
5,5 MBit/s	8 (CCK)	QPSK	1,375 MS/s	4
11 MBit/s	8 (CCK)	QPSK	1,375 MS/s	8

MS/s = Megasymbole pro Sekunde

Weitere IEEE802.11-Standards

Neben den bereits erwähnten Standards 802.11a und 802.11b umfasst IEEE811 noch eine Reihe weiterer Substandards. Ein Großteil davon durchläuft derzeit noch den Normierungsprozess.

Zu den interessantesten Projekten zählt die Arbeit der Task Group 802.11g. Seit Mai 2000 bereitet sie eine Spezifikation für eine schnellere 802.11- MAC im 2,4-GHz-Band vor. Als Ziel peilt die verantwortliche Higher Rate IEEE802.11b Study Group (HRbSG) die Erhöhung der Datenrate auf mindestens 20 MBit/s an.

IEEE802.11-Arbeitsgruppen	
Task Group	**Arbeitsgebiet**
802.11b-cor	Korrekturen der 802.11-MIB
802.11d	Aktualisierung der Regulatory Domains
802.11e	MAC-Erweiterungen
802.11f	IAPP (Inter Access Point Protocol)
802.11g	Erweiterung von 802.11b für höhere Datenraten
802.11h	Frequenzspektrum von 802.11a

Weiter führende Informationen

Während Fachliteratur zum Thema IEEE802.11 bislang nur spärlich vorliegt, finden sich im Internet bereits zahlreiche weiter führende und ergänzende Informationen zu WLANs jeder Art. Wir haben für Sie eine Auswahl der interessantesten Angebote aus beiden Bereichen zusammengestellt. (jlu)

802.11 im Internet

ComNets

Der Lehrstuhl für Kommunikationsnetze an der RWTH Aachen offeriert zahlreiche Artikel rund um drahtlose Netzwerktechnologie von DECT bis HiperLAN.

IEEE 802.11

Die Arbeitsgruppe 802.11 des IEEE definiert nicht nur WLANs, sondern bietet auch entsprechende technische Hintergrund-Dokumente an.

Wireless Nets

Der US-Consulting-Anbieter Wireless Nets hat auf seiner Website zahlreiche Artikel rund um alle Aspekte des WLAN-Betriebs gesammelt.

WECA

In der "Learing Zone" der Wireless Ethernet Compatibility Alliance finden sich Whitepapers und Tutorials rund um den 802.11-Standard.

WLANA

Die Wireless LAN Association bietet Grundlagen- und Anwendungsberichte zum Thema drahtlose Netzwerke an.

Literatur zu 802.11-Netzen

Nett, B., Mock, M., Gergeleit, M.: **Das drahtlose Ethernet**; Addison-Wesley, München 2001; ISBN 3-8273-1741-X

Das Buch bietet eine aktuelle und umfassende Beschreibung der technischen Grundlagen und Einsatzmöglichkeiten 802.11-basierter Wireless LANs.

Walke, B.: **Mobilfunknetze und ihre Protokolle, Band 2**; Teubner 2000; ISBN 3-519-16431-0

Der Band liefert einen recht vollständigen Überblick, ist aber weder auf dem neuesten Stand, noch konsistent bearbeitet. Die Seiten 404 bis 427 beschreiben das Thema 802.11.

Santamaria, A., Lopez-Hernandez, F.J.: **Wireless LAN Systems**; Artech House, Boston, London 1994, ISBN 0-89006-609-4.

Das Buch bietet trotz des Alters einen guten Überblick über die grundsätzlichen Verfahren und Zusammenhänge in drahtlosen Netzen.