

IEEE802.11 Wireless LAN

Stefan May, Christian Rieck

7. November 2003

Inhaltsverzeichnis

1	Einführung	2
2	Netzwerkformen und Komponenten	3
2.1	Ad-Hoc Netzwerk	3
2.2	Infrastruktur	3
2.3	Komponenten	4
3	Physical Layer	4
3.1	Frequency Hopping Spread Spectrum (FHSS)	4
3.2	Direct Sequence Spread Spectrum (DSSS)	6
4	Medium Access Control	7
4.1	CSMA/CA	7
4.2	Acknowledgement Frame	7
4.3	Interframe Spaces	7
4.4	Backoff	8
4.5	Hidden Station Problem	9
4.6	Fragmentierung	10
5	Sicherheit	11
5.1	Wired-Equivalent-Privacy-Algorithmus (WEP)	11
5.2	Authentifizierung	12
6	WLAN Produkte	14
6.1	Netzwerkkarten	14
6.2	Geräte für Infrastruktur	14
6.3	Antennen	14
7	Literatur	15
8	Abkürzungen	16

1 Einführung

Es gibt den WLAN IEEE Standard 802.11, 802.11b, 802.11a, 802.11g, 802.11h. WLAN ist kein Ethernet bei dem man das Kabel einfach weggelassen hat. WLAN stellt einen eigenen Standard dar. Sie dienen aber zur Erweiterung von Ethernet-Netzwerken. Es gibt momentan 5 Standards die nach IEEE spezifiziert sind.

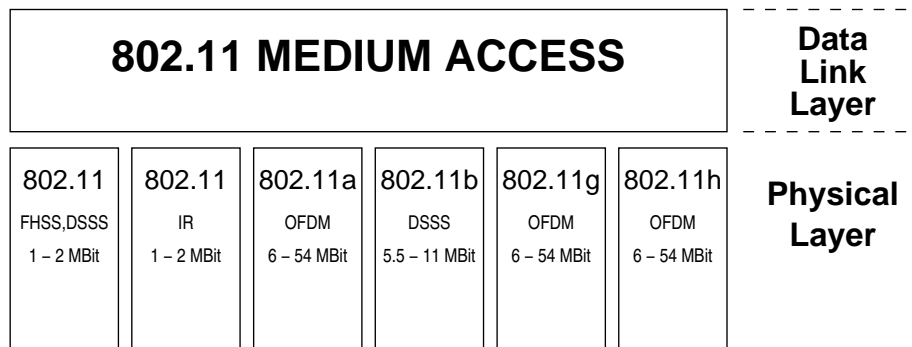


Abbildung 1: Übersicht über IEEE802.11

IEEE 802.11 wurde 1997 verabschiedet und legt eine Datenübertragung mit 1 oder 2 Mbit/s im 2,4 GHz Frequenzband fest. Wie jeder andere 802.x Standard beschreibt auch der 802.11 Standard den MAC-Layer (Media Access Control Layer) und Physical-Layer im OSI-Schichtenmodell. Unter 802.11 ist ein einziger MAC definiert, der jeweils mit einem der fünf spezifizierten unterschiedlichen Physical Layer zusammen arbeiten kann.

Die Physical-Layer arbeiten entweder nach dem Frequency Hopping Spread Spectrum (FHSS) oder nach dem Direct Sequence Spread Spectrum (DSSS) im 2,4 GHz-Band oder mit dem Infrarot Physical Layer. Dem IR-Layer wird aber keine Aufmerksamkeit gewidmet, da es auf dem Markt keine WLAN Produkte gibt, die mit Infrarottechnologie arbeiten.

IEEE 802.11b wurde 1999 verabschiedet, er definiert eine Datenrate von 5,5 und 11 Mbit/s im 2,4 GHz Band. 802.11b arbeitet nur im DSSS-Verfahren.

IEEE 802.11a wurde ebenfalls 1999 verabschiedet und erreicht eine Datenrate bis 54 Mbit/s im 5 GHz Band. Allerdings ist 802.11a in Europa noch nicht zugelassen.

Das Frequenzband für die Datenübertragung nach dem Standard IEEE 802.11g ist das gleiche wie bei IEEE 802.11b, nämlich 2,4 bis 2,4835 GHz. Hier soll die nächste Evolutionsstufe durch das Modulationsverfahren OFDM (Orthogonal Frequency Division Multiplexing) die fast fünffache Datenrate im Vergleich zu den heute verfügbaren 11 Mbit/s erreichen. Weiterhin ist in diesem Standard eine Abwärtskompatibilität zu heutigen Systemen vorgesehen. Ein langsame Migration mit Mischbetrieb soll dadurch gesichert werden. Aufgrund des gleichen Frequenzbandes sind auch die gleichen Antennen einsetzbar, allerdings liegen Aussagen zu Reichweiten noch nicht vor.

Das bislang für die Anwendung Wireless LAN noch unbenutzte Frequenzband bei 5 GHz steht in Deutschland kurz vor der Freigabe durch die Reg TP (Regulierungsbehörde für Telekommunikation und Post). Hier wird ebenfalls ei-

ne hohe Datenrate mit dem Modulationsverfahren OFDM ermöglicht. Der Standard für diese Technologie hat die Bezeichnung IEEE 802.11a/h, wobei 802.11a die Variante für die USA ist. Diese Variante soll mit Limitierungen bezüglich des nutzbaren Frequenzbandes und der Sendeleistung als Sonderfall in Europa und damit in Deutschland zugelassen werden. Eine Ausnutzung der gesamten in Europa zur Verfügung stehenden Möglichkeiten und auch die Beachtung von zusätzlichen Forderungen bei 5 GHz soll mit dem Standard 802.11h erfolgen. Es sollen hier ein größeres Frequenzband mit mehr Gesamtkapazität benutzbar und teilweise höhere Sendeleistungen erlaubt sein. Daran sind allerdings zwei Bedingungen geknüpft, die automatische Wahl des Frequenzkanals und die dynamische Anpassung der Sendeleistung. Diese Auflagen sind notwendig, da in Europa Satelliten- und Radarsysteme in diesem Frequenzband nicht gestört werden dürfen. Auf der anderen Seite könnten sie in der Praxis aber auch einen stabilen Funkbetrieb der neuen Wireless LANs gewährleisten.

Da für beide angekündigten neuen Technologien derzeit Standards bzw. Freigaben noch nicht endgültig vorliegen, und auch Erfahrungswerte im praktischen Einsatz fehlen, ist für Betreiber von Wireless LANs noch nicht vorhersehbar, welche Technologie sich durchsetzen wird. Auch stellt sich vielfach noch die Frage, welche Technologie unter verschiedenen Einsatzszenarien Vor- oder Nachteile bringt.

Als Ausblick für einen Zeithorizont von etwa 2 Jahren und als Lösung der Technologiefrage bei Wireless LANs ist mit Combo-Modulen zu rechnen. Sie sollen einen vollständig abwärtskompatiblen Standard IEEE 802.11g im 2,4 GHz-Band und gleichzeitig die Standards IEEE 802.11a und 802.11h im noch wenig genutzten 5 GHz-Band unterstützen, so wie man es von Dual-Band-Handys kennt.

2 Netzwerkformen und Komponenten

Der Standard IEEE802.11 definiert zwei grundsätzliche Netzwerkformen, das Ad-Hoc Netzwerk und das Infrastrukturnetzwerk.

2.1 Ad-Hoc Netzwerk

Die einfachste Form ist das Ad-Hoc Netzwerk. Es besteht aus mehreren Stationen, die gemeinsam eine Funkzelle bilden. Die Funkzelle ist der Ausleuchtungsbereich aller Stationen. Jede Station muß sich in der Reichweite aller anderen Stationen befinden.

Die Kommunikation erfolgt direkt zwischen den einzelnen Stationen.

2.2 Infrastruktur

Das Infrastrukturnetzwerk definiert eine neue Komponente, den Access Point. Dieser bildet ein zentrales Element in einem Infrastrukturnetzwerk. Die Funkzelle wird hier durch den Ausleuchtungsbereich des Access Point definiert. Die Kommunikation erfolgt nicht direkt zwischen den Stationen. Jedes Paket wird über den zentralen Access Point verschickt.

Infrastrukturnetzwerke erreichen aus diesem Grund eine höhere Reichweite. Die Stationen müssen sich untereinander nicht mehr erreichen. Dies führt

allerdings zu Problemen, die später noch besprochen werden.

2.3 Komponenten

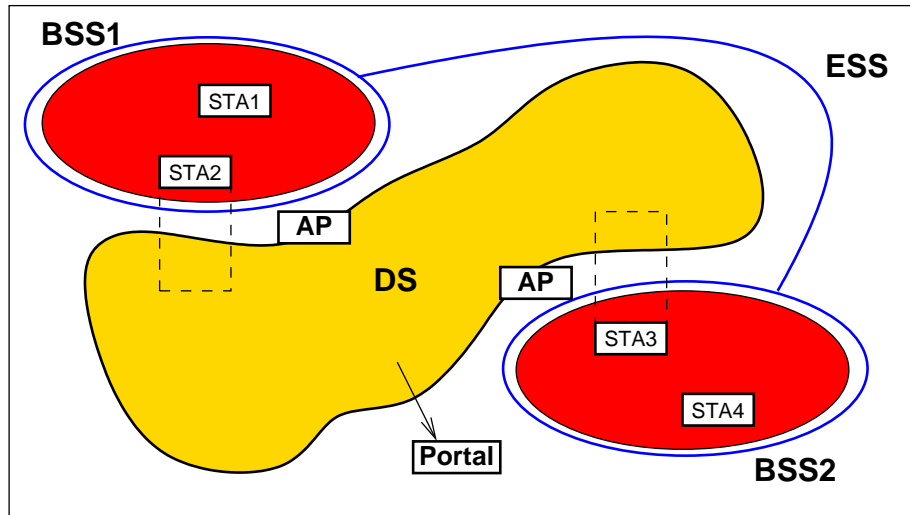


Abbildung 2: Komponenten von IEEE802.11

Die einfachste Form, die durch IEEE802.11 definiert wird, ist das Ad-Hoc Netzwerk. Es wird durch den Ausleuchtungsbereich aller Stationen festgelegt. Diese Funkzelle wird Basic Service Set (BSS) genannt. Steht dieser BSS allein ohne weitere Infrastruktur, wird dieser BSS als Independent Basic Service Set (IBSS) bezeichnet.

BSS

Ein Distribution System (DS) sorgt für die Verbindung von BSS, die sich nicht gegenseitig erreichen. Ein DS ist ein logisches Konstrukt, das in einem Access Point (AP) implementiert wird. Das DS sorgt für die Weiterleitung von Paketen zwischen BSS und für die Kommunikation zwischen den Stationen.

DS, AP und Portal

Eine weitere Komponente ist das Portal. Ein Portal sorgt für den Zugang zu drahtgebundenen Netzwerken. Im Allgemeinen ist das Portal im Access Point integriert.

Ein Extended Service Set (ESS) bildet einen Zusammenschluss von mehreren BSS. Zentraler Bestandteil ist das DS, welches das Rückgrat des ESS bildet. Ein ESS ist die Zusammenfassung eines unabhängigen WLAN.

ESS

Ein komplexes Beispiel zeigt Abbildung 3. Es zeigt ein Wireless LAN im Zusammenspiel mit einem drahtgebundenen Netzwerk.

3 Physical Layer

3.1 Frequency Hopping Spread Spectrum (FHSS)

Bei der FHSS-Technologie wird die vorhandene Bandbreite (2,4-2,4835 GHz) in 79 Frequenzunterbänder mit je 1 MHz unterteilt. Jedes der 79 Frequenzunterbänder stellt einen Kanal bereit, die im Wechsel zwischen den Systemen verwendet werden. Über eine sogenannte Hopping-Sequenz springen Sender und

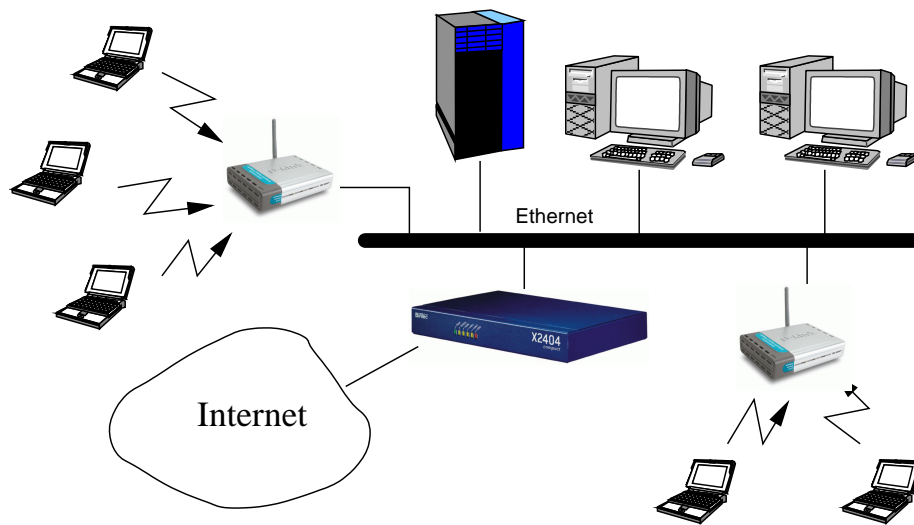


Abbildung 3: Beispiel für ein Infrastrukturnetzwerk

Empfänger während der Übertragung gleichzeitig zwischen den Kanälen. Ein Kanal darf maximal 400 ms belegt werden und der Abstand der nacheinander verwendeten Kanäle muß mindestens 6 MHz betragen. Dies entspricht 2,5 Kanalwechsel pro Sekunde. Die Belegung der 79 Kanäle wird über eine 79-stellige Hopping-Sequenz festgelegt, die ein Hüpfmuster darstellt und die die Reihenfolge der Kanalbelegung festlegt. Systeme die Daten austauschen, verwenden dieselbe Hopping-Sequenz. Es ist aber möglich das zufällig zwei Sender zur gleichen Zeit den gleichen Kanal belegen und eine Kollision auftritt. Die dabei auftretenden Fehler werden durch ein wiederholtes Senden der Daten korrigiert. Eine Kollision kann maximal 400 ms auftreten, und nach dem Kanalwechsel durch das unterschiedliche Wechselverhalten ist die Kollision wieder aufgehoben.

Die erzielbare Datenrate ist jedoch bei FHSS-Systemen auf 2Mbit/s begrenzt. Laut IEEE 802.11 sind nur 1 Mbit/s und 2 Mbit/s im Physical-Layer definiert. Wollte man die Datenrate erhöhen, müßte man die Bandbreite der Frequenzunterbänder erhöhen. Dies würde aber die Anzahl der Kanäle reduzieren und dies wiederum die Anzahl der Kollisionen erhöhen.

Für das Aussenden der Daten übernimmt der PLCP des Physical-Layer, die Daten des MAC-Layer und packt diese Daten für die Übertragung in ein bestimmtes Frameformat, dessen Header 5 Felder beinhaltet und eine Länge von 128 Bit hat. Auf der Seite des Empfängers werden die Informationen des PLCP-Headers zur Steuerung des Empfängers auf der PHY-Ebene genutzt und der Header wieder entfernt.

SYNC 80 bit	SFD 16 bit	PLW 12 bit	PSF 4 bit	Error Header Check 16 bit	PSDU
PLCP Preamble		PLCP Header			Daten

Abbildung 4: FHSS Frame Format

SYNC kennzeichnet den Frameanfang und Sender und Empfänger synchronisieren sich über diesen,

SFP (Start Frame Delimiter) zeigt das Ende von SYNC ab und kennzeichnet den eigentlichen Frameanfang.

PLW (PSDU-Length-Word) gibt die Länge des Datenteils in Byte an, die vom MAC-Layer übergeben werden. maximal 4095 Byte

PSF (PLCP-Signaling Field) gibt die Datenrate an, mit der der Inhalt der PSDU übertragen wird. FHSS jedoch nur 1 oder 2 Mbit/s

Header Error Check Field ist die Fehlerprüfung des PLCP-Headers.

PSDU beinhaltet die Daten des MAC-Layer, die als MPDU bezeichnet werden. Maximale Länge 4095 Bytes.

3.2 Direct Sequence Spread Spectrum (DSSS)

Bei der DSSS-Technologie, laut IEEE 802.11b wird die vorhandene Bandbreite (2,4 - 2,4835 GHz) in 13 Frequenzunterbänder mit einer Bandbreite von jeweils 22 MHz und 30 MHz Abstand zwischen den Frequenzbändern aufgeteilt. Jedes der Frequenzbänder stellt einen Kanal bereit. Anders als bei der FHSS-Technologie, sendet ein Sender immer auf demselben Kanal und es findet während der Aussendung der Daten kein Kanalwechsel statt.

Für die Datenübertragung über DSSS werden die Daten beim Senden gespreizt. Die Spreizung führt dazu, daß im Gegensatz zum schmalbandigen Senden (FHSS), über einen größeren Frequenzbereich gearbeitet wird. Dadurch ist bei einem evtl. schmalbandigen Störeinfluß nur ein Teil der Information gestört, während bei schmalbandiger Datenübertragung das komplette Signal verloren ginge. Die Intensität des breitbandigen Signals wird letztendlich unter die Rauschgrenze gebracht, wodurch benachbarte Systeme weniger gestört werden und die Dichte unterschiedlicher Systeme, bezogen auf eine bestimmte Fläche erhöht werden kann.

Die vom MAC-Layer übergebenen Daten werden für die Übertragung bei DSSS-Systemen in ein Frameformat verpackt, dessen PLCP-Header 6 Felder beinhaltet und eine Länge von 192 Bits hat. DSSS Frameformat

SYNC 128 bit	SFD 16 bit	Signal 8 bit	Service 8 bit	Length 16 bit	CRC 16 bit	MPDU
PLCP Preamble		PLCP Header				Daten

Abbildung 5: DSSS Frame Format

SYNC darüber synchronisieren sich Sender und Empfänger

SFD (Start Frame Delimiter) zeigt den Anfang der Physical-Layer Parameter an

Signal zeigt die Datenrate der zu übertragenden Daten an

Service zeigt bestimmte Eigenschaften für die Datenraten an, z.B. Sendefrequenz, Modulationsverfahren, Wep

Length zeigt die Zeit an, die für die Übertragung der PSDU-Daten benötigt wird.

CRC (Cyclic Redundancy Check) über die Fehlerfreiheit des PLCP-Header.

4 Medium Access Control

Das Funkmedium ist ein Shared-Medium. Bei gleichzeitigem Zugriff kann es zu Kollisionen kommen. Deshalb kommt dem MAC-Layer eine besondere Bedeutung zu. Zu seinen Aufgaben gehört deshalb der geordnete Zugriff auf das Medium und die Erkennung und Beseitigung von Kollisionen. Zusätzlich zu diesen Aufgaben definiert IEEE802.11 eine Reihe weiterer Funktionen, wie Fragmentierung, Frame-Wiederholung im Fehlerfall sowie Empfangsbestätigung bei fehlerfrei empfangenen Frames.

4.1 CSMA/CA

Das Zugriffsverfahren für IEEE802.11 wird CSMA/CA genannt. Die Abkürzung steht für Carrier Sense Multiple Access/ Collision Avoidance. Ziel dieses Verfahrens ist die Vermeidung von Kollisionen.

Dies wird zunächst durch CSMA erreicht. Bei diesem Verfahren horcht eine sendewillige Station zunächst auf dem Medium, ob keine Datenübertragung stattfindet. Empfängt die Station kein Signal, geht sie von einem freien Medium aus. Starten allerdings mehrere Stationen gleichzeitig die Aussendung, so kommt es zu einer Kollision.

Diese Kollisionen sollen durch das Verfahren CA vermieden werden. In IEEE802.11 ist dies durch den Network Allocation Vector (NAV) realisiert. Dieser NAV wird durch das Feld Duration/ID im MAC-Frame definiert und bestimmt die Zeitdauer, die dieses Frame auf dem Medium für die Übertragung benötigt. Erst nachdem der NAV abgelaufen ist, ist das Medium wieder als frei deklariert. Kollisionen werden also vermieden.

4.2 Acknowledgement Frame

Kollisionen sind durch das Verfahren CSMA/CA aber immer noch nicht ausgeschlossen. Wie können also Kollisionen auf dem Medium erkannt werden?

Das Acknowledgement Frame wird bei erfolgreichem Empfang versendet. Bei Ausbleiben dieses Frames liegt offenbar eine Störung oder Kollision vor. Kollisionen können also durch das Bestätigen des Empfangs erkannt werden.

Wenn ein gesendetes Paket nicht innerhalb einer bestimmten Zeit bestätigt wird, werden die Daten noch einmal versendet.

4.3 Interframe Spaces

Ein Problem ist aber folgendes Szenario: Es gibt mehrere sendewillige Stationen. Station A hat das Paket ausgesendet und wartet nun auf Bestätigung. Nachdem

der NAV von Station B abgelaufen ist, beginnt sie sofort mit der Aussendung ihres Frames. Wie kann sichergestellt werden, daß das Frame von Station A innerhalb kurzer Zeitspanne bestätigt werden kann?

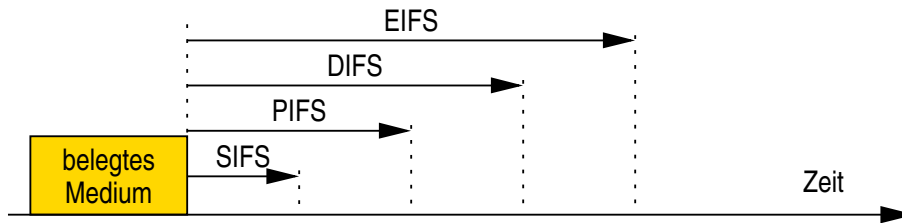


Abbildung 6: Interframe Spaces

Dieses Problem wird durch die Interframe Spaces gelöst. Interframe Spaces geben Mindestabstände nach der Belegung des Mediums an. Es gibt insgesamt vier Interframespaces:

SIFS Short Interframe Space

PIFS PCF Interframe Space

DIFS DCF Interframe Space

EIFS Extendes Interframe Space

Durch die Interframe Spaces können nun Pakete priorisiert behandelt werden. Nach dem SIFS dürfen Acknowledgement Frames versendet werden. Normale Datenframes erst nach dem DIFS.

4.4 Backoff

Nach dem DIFS kann es wieder zu einer Konkurrenz zwischen verschiedenen sendewilligen Stationen kommen. Dies wird durch eine zufällige Backoff Zeit vermieden, die vor Aussendung des Datenframe gewartet wird. Backoff

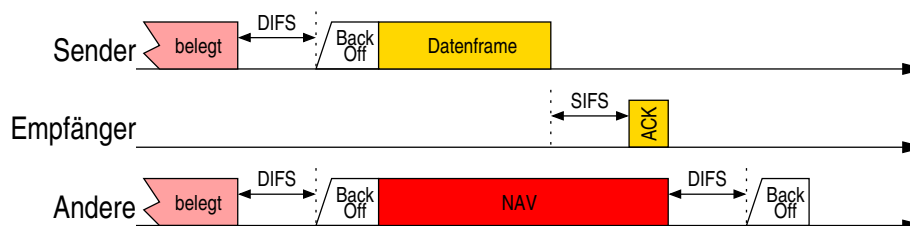


Abbildung 7: Datenübertragung ohne Kollision

Eine Übertragung eines Paketes ohne Kollision ist in Abbildung 7 zu sehen. Nach Belegung des Mediums wird nach dem DIFS eine zufällige Backoff Zeit gewartet und dann bei einem freien Medium mit der Aussendung des Datenframes begonnen. Alle anderen Stationen setzen ihren NAV nach dem Feld Duration/ID im MAC Header. Für andere Stationen ist das Medium ab diesem Zeitpunkt gesperrt.

Nach dem Empfang des Frames wird das Datenframe durch Aussendung eines Acknowledgement Frame bestätigt. Dieses Frame wird nach Ablauf des SIFS gesendet. Für alle anderen Stationen ist nach Ablauf des DIFS und des NAV das Medium wieder frei.

4.5 Hidden Station Problem

Ein weiteres Problem ist das Hidden Station Problem.

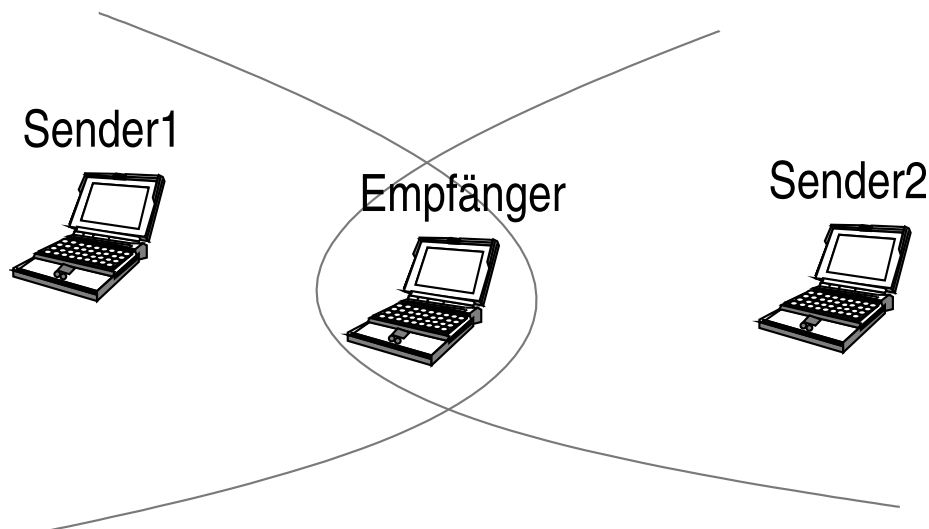


Abbildung 8: Hidden Station Problem

Das Verfahren CSMA kann hier nicht angewendet werden, da Sender 1 und Sender 2 sich nicht innerhalb ihrer Reichweite befinden. Bei gleichzeitiger Aussendung kann es deshalb sehr häufig zu Kollisionen kommen.

Dieses Problem kann durch ein Handshaking Verfahren gelöst werden. Bei diesem Verfahren wird das Medium explizit durch den Empfänger freigegeben. RTS/CTS

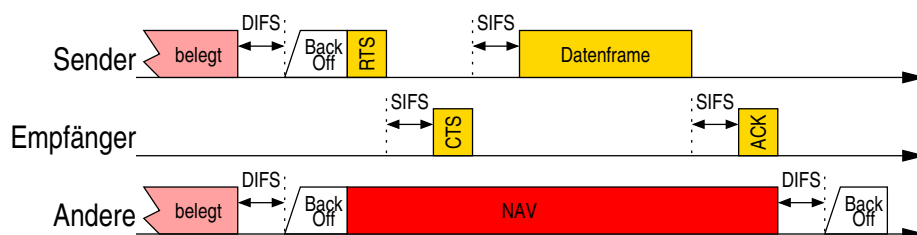


Abbildung 9: Handshake Verfahren bei IEEE802.11

Vor Aussendung eines Datenframe wird zunächst ein Ready To Send (RTS) Frame gesendet. Dieses Frame wird durch den Empfänger mit einem Clear To Send (CTS) Frame bestätigt. Beide Frames haben eine hohe Priorität und werden nach Ablauf des SIFS gesendet. Nach Empfang des CTS Frame ist das Medium für den Sender explizit freigegeben. Alle anderen Stationen sind durch den NAV blockiert, bis zur Bestätigung des Frames durch den Empfänger.

Vorteil dieses Verfahrens ist die Vermeidung von Kollisionen beim Hidden Station Problem. Nachteilig wirkt sich die höhere Latenz und verringerte Bandbreite aus. RTS Frames können immer noch kollidieren, allerdings ist das Medium auch nicht so lang belegt, wie bei Aussendung eines Datenframes. Kollisionen werden also bei diesem Verfahren früher erkannt, sind aber nicht vollkommen ausgeschlossen.

Verwendung wird dieses Verfahren bei stark asymmetrischen Ausbreitungsbedingungen und bei Netzwerken mit großen Frames und vielen Kollisionen. Beispiele sind Büros mit vielen Wänden und einer hohen Anzahl an Stationen.

4.6 Fragmentierung

Eine weitere Aufgabe des MAC Layers ist die Fragmentierung. Diese gehört eigentlich nicht in diese Schicht, kann aber in bestimmten Umgebungen große Vorteile bieten.

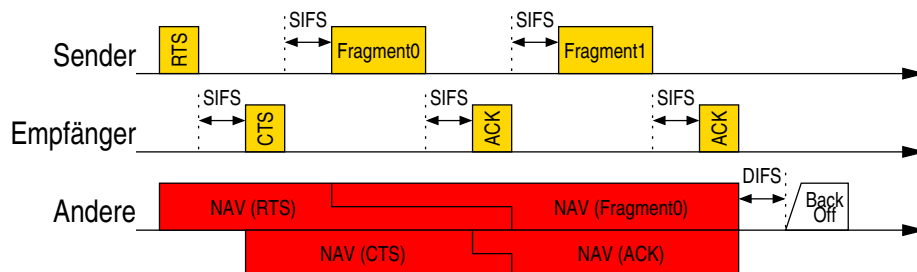


Abbildung 10: Übertragung von fragmentierten Frames

Im MAC Header ist bei fragmentierten Paketen das Bit More Frag im Frame Control Feld gesetzt. Es zeigt der empfangenden Station an, daß weitere Fragmente folgen. Im letzten Fragment ist dieses Bit 0. Die Aussendung der Datenfragmente erfolgt in diesem Fall nach dem SIFS und nicht erst nach einem DIFS, wie es bei normalen Datenframes üblich ist. Abbildung 10 zeigt den zeitlichen Verlauf einer Übertragung mit fragmentierten Frames und Handshaking.

Seine Vorteile kann dieses Verfahren bei der Übertragung von großen Frames in stark gestörten Umgebungen ausspielen. Die Übertragungszeit wird reduziert und damit auch die Wahrscheinlichkeit von Störungen innerhalb eines Fragments. Bei Störungen muss dann nur ein kurzes Fragment, statt eines großen Datenframe, neu übertragen werden. Nachteilig wirkt sich wie beim Handshaking die höhere Latenz und die geringere Bandbreite aus.

Die Fragmentierung kann nicht nur bei zu großen Paketen erfolgen, sondern auch bei Paketen ab einer gewissen Größe. So kann durch Wahl einer bestimmten maximalen Größe eines Fragments die Störungsanfälligkeit verringert werden.

5 Sicherheit

5.1 Wired-Equivalent-Privacy-Algorithmus (WEP)

Drahtgebundene Lokale Netzwerke sind gegen einen unbefugten Zugriff recht gut abgesichert. Um Zugriff zu erhalten, müßte sich ein Unbefugter direkt in das Netzwerk einklinken. Anders sieht es bei drahtlosen Netzen aus. Die Daten werden über Funk übertragen und jeder, der sich in der Reichweite eines drahtlosen Netzwerks aufhält, kann theoretisch mitlauschen.

Das Verschlüsselungsverfahren WEP soll Lauscher außen vorhalten und dem WLAN eine vergleichbare Sicherheit bieten. Dazu wird der Datenteil der Frames verschlüsselt übertragen. Ein Unbefugter sieht so abgehörte Daten nur als Schlüsseltext, dem ohne Schlüssel keine Informationen entnommen werden können. Außerdem können Unbefugte keine verschlüsselten Daten versenden. Nur Teilnehmer eines Netzwerks, die im Besitz des Schlüssels sind, können Informationen sinnvoll entschlüsseln und Daten austauschen.

WEP stellt die Grundlage aller kryptografischen Sicherheitsmechanismen in WLAN's dar. Der Wep-Algorithmus basiert auf einem gemeinsamen geheimen WEP-Schlüssel, der 40Bit (WEP40) oder 104 Bit (WEP128) umfaßt und der zur Verschlüsselung des Datenteils der Frames und zur Authentifizierung dient.

WEP40 ist im IEEE 802.11 Standard implementiert. WEP128 wurde von den Herstellern eingeführt und ist mittlerweile in allen WLAN-Produkten vorhanden.

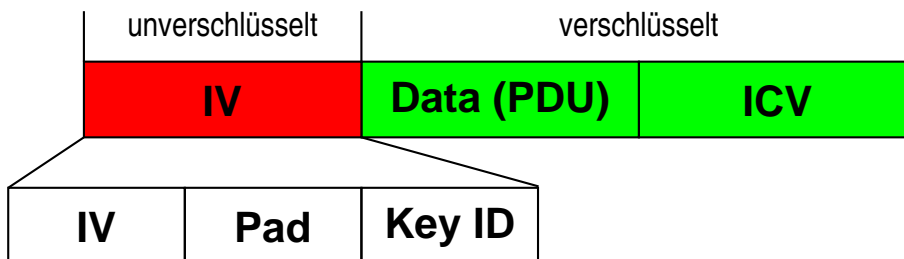


Abbildung 11: 32 bit langes IV Feld

Das WEP-Feld im Frame Control Feld ist auf 1 gesetzt und signalisiert dem Empfänger, daß der Datenteil verschlüsselt ist. An jedes verschlüsselte Datenteil wird eine 32-Bit Prüfsumme, die über die unverschlüsselten Daten gebildet wird, angehängt. Die Prüfsumme wird als ICV (Integrity Check Value) bezeichnet. Vor die Daten wird ein 32 Bit langes IV-Feld gesetzt, Abbildung 11. Das IV-Feld setzt sich aus einem 24 Bit langen Initialisierungsvektor (IV), 6 Bit langen PAD Feld und 2 Bit langem Key-ID Feld zusammen.

Über KEY-ID wird einer von 4 möglichen Schlüsseln gewählt, der vom Empfänger für die Entschlüsselung genutzt werden muss. PAD ist immer auf 0 gesetzt. Der IV ergänzt lediglich den geheimen WEP-Schlüssel zum Gesamtschlüssel der zur Initialisierung des Pseudo-Random-Number-Generator verwendet wird. Der PRNG erzeugt schließlich den Schlüsselstrom für den zur Authentifizierung und Datenverschlüsselung eingesetzten Chiffrierer. (RC4 von RSA Data Security) Der IV wird unverschlüsselt übertragen, damit der Empfänger weiß welchen der 4 Schlüssel er zur Entschlüsselung verwenden muss.

Die ICV (Prüfsumme) wird vom Empfänger benutzt, um zu überprüfen, ob

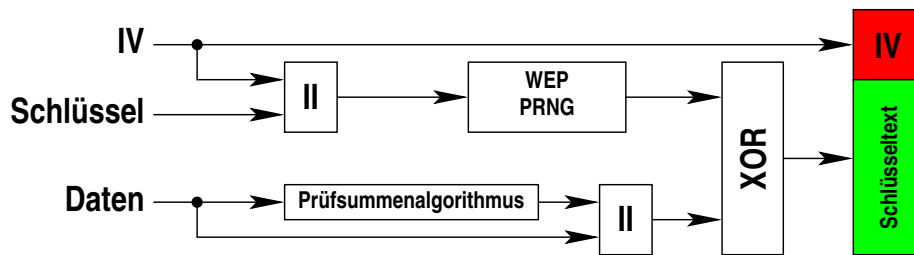


Abbildung 12: WEP Verschlüsselungsalgorithmus

er den Datenteil des Frames richtig entschlüsselt hat. Die ICV wird sendeseitig über die unverschlüsselten Daten gebildet und zum senden mitverschlüsselt. Der Empfänger entschlüsselt die ICV und vergleicht diese mit einer selbst ermittelten Prüfsumme, die er über die entschlüsselten Daten bildet. Sind ICV und die selbstgebildete Prüfsumme gleich, so geht der Empfänger von einer erfolgreichen Entschlüsselung aus.

Bleibt nur noch die Frage wie die WEP-Schlüssel vergeben werden??? Der WEP-Schlüssel ist entweder 40 Bit oder 104 Bit lang. In der Regel steht WLAN Komponenten eine Menüseite zur Verfügung, auf der bis zu 4 WEP-Schlüssel vergeben werden können. Die WEP-Schlüssel werden dort als Kennwort vergeben, wobei die eine Länge von 5 Zeichen (WEP40) oder 13 Zeichen (WEP128) haben müssen.

5.2 Authentifizierung

Wenn ein Client auf das Netzwerk zugreifen will, muss er sich zuerst authentifizieren, also beim Netz, vertreten durch den Access Point, anmelden. Hierzu stellt WEP nicht nur Funktionen zur Datenverschlüsselung, sondern auch zur Authentifizierung und Integritätssicherung, zur Verfügung. Die WLAN-Authentifizierung beruht nun auf zwei möglichen Verfahren. Entweder die Open System Authentication (laut IEEE 802.11). Hier findet keine Authentifizierung statt, d.h. das Netz ist für alle frei, die diese Methode akzeptieren. Oder man nutzt die sichere Variante, Shared Key Authentication. Diese verwendet ein Challenge-Response-Verfahren mit einem geheimen Schlüssel zur Authentifizierung.

Es beruht auf dem Austausch von 4 Managementframes. Das erste Managementframe des Station A teilt mit, dass er eine Shared Key Authentifizierung durchführen möchte. Station B antwortet mit einem 128 Byte langen Challenge-Text. Dieser Challenge Text wird mit einem PRNG erzeugt und mit WEP chiffriert. Station A kopiert den erhaltenen Challenge Text in dem Managementframe, verschlüsselt diesen wieder mit WEP und schickt diesen zurück an B. Station B entschlüsselt diesen wieder, prüft ICV auf Übereinstimmung. Stimmt ICV überein, wird die Authentifizierung von A akzeptiert. Das Ergebnis schickt B nun zu A, die Identität von A ist sichergestellt und der Zugriff auf das Netzwerk freigegeben.

Allerdings ist das WEP als Sicherheitsverfahren schon sehr oft in Kritik geraten. Der Schlüssel im RC4-Verfahren arbeitet statisch und der IV ziemlich kurz ist (24-Bit) gibt es nur eine geringe Anzahl von Variationsmöglichkeiten.

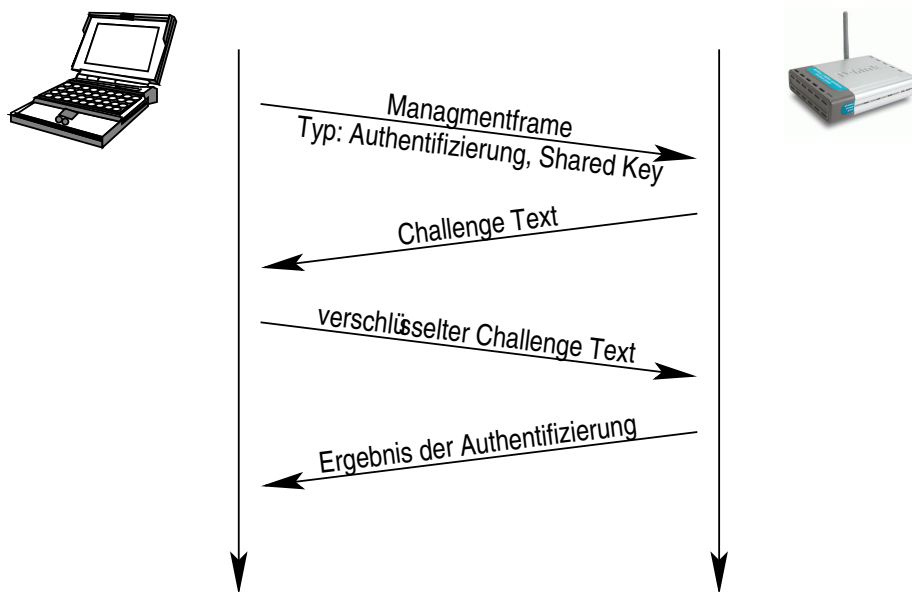


Abbildung 13: Authentifizierung bei IEEE802.11

Auf diese Weise wird es Lauschern ermöglicht, in relativ kurzer Zeit genug Informationen zu sammeln, um den eigentlich geheimen Schlüssel zu überwinden. Bis heute sind von den Herstellern von WLAN-Produkten zwei weitere Verfahren zur Authentifizierung eingeführt worden. Zum einen lässt sich die Anmeldung auf bestimmte MAC-Adressen beschränken, und zum anderen kann man den SSID (Service Set Identifier) dazu nutzen, einen zusätzlichen Schlüssel zu generieren, der für den Zugriff auf das Netzwerk bekannt sein muss.

Die Einschränkung bezüglich der MAC-Adressen wird über Listen geregelt, die auf den Access Points verwaltet werden. In einer Access Control List (ACL) werden die MAC-Adressen aufgelistet, von den Stationen, die sich anmelden dürfen. Verläuft die Prüfung positiv, dürfen sich die Stationen anmelden. Andernfalls werden sie abgewiesen. Die Verwaltung ist aber problematisch, denn die MAC-Adressen aller zugelassenen Stationen müssen manuell eingetragen werden und ständig aktualisiert werden.

Bei der Sicherheitssteigerung über die SSID macht man sich die Tatsache zu nutze, dass die Stationen sich mit der richtigen SSID beim Access Point anmelden müssen. Die Access Points versenden die SSID normalerweise in regelmäßigen Abständen als Broadcast. Schränkt man aber diese Bekanntgabe ein und die richtige SSID manuell an den Stationen ein, so können sich die Stationen mit der richtigen SSID am Access Point anmelden. So schafft man eine einfache Beschränkung durch ein einfaches Passwort. Man darf natürlich jetzt vom Access Point nicht mehr die SSID als Broadcast versenden. Dies lässt sich aber bei den WLAN-Produkten über die Option SSID-Broadcast ausschalten.

Beide Verfahren (ACL und SSID) werden heute von den meisten Herstellern implementiert, um die Sicherheit der Netzwerke zu gewährleisten. Nachteilig ist aber an beiden Verfahren, dass die MAC-Adressen und die SSID generell unverschlüsselt übertragen werden. Demnach können mit Hilfe von Protokol-

Analysatoren diese mitgeschnitten und dargestellt werden. Er empfiehlt sich WEP zu verwenden und zusätzlich die Filterung von MAC-Adressen und die zusätzliche Zugangskontrolle von SSID.

Aber sehr sicher ist es noch nicht.

6 WLAN Produkte

Auf dem Markt gibt es heute eine Reihe von interessanten Produkten. Dazu zählen verschiedene Bauformen von Netzwerkkarten, Infrastrukturprodukte, wie Access Points oder Router, sowie Antennen zur Vergrößerung der Reichweite von WLANs.

6.1 Netzwerkkarten

Bei den Netzwerkkarten gibt es heute verschiedene Bauformen, wie PCMCIA für Notebooks, Compact Flash Adapter für PDAs oder PCI und USB für Desktop PCs. Alle diese Netzwerkkarten unterscheiden sich fast ausschließlich im verwendeten Unterstandard (z.B. 802.11a oder 802.11b) und damit in ihrer verfügbaren Bandbreite. Es sind meist Antennen integriert, die normale Reichweiten zwischen 30m in Gebäuden und 300m außerhalb erreichen.

6.2 Geräte für Infrastruktur

Für Infrastrukturnetzwerke bietet der Markt eine ganze Fülle von Produkten. Dies sind zum einen reine Access Points für die Vergrößerung der Reichweite, die gleichzeitig den Zugriff auf drahtgebundene Netzwerke erlauben. Es gibt jedoch ausschließlich Access Points, die den Zugriff auf Ethernet 802.3 Netzwerke erlauben. Andere Zugänge zu drahtgebundenen Netzwerken gibt es nicht. Ein weiteres Infrastrukturprodukt sind Router, bei denen der Access Point integriert ist. Diese Router ermöglichen den Zugang auch über Breitband oder ISDN auf das Internet oder Firmennetzwerke. Auch hier gibt es fast ausschließlich Produkte für DSL und ISDN. Zusätzlich existieren auf dem Consumer-Markt Bauformen mit integrierten Hubs oder Switches, die den Aufbau eines kleinen drahtgebundenen Netzwerkes ermöglichen. In allen Produkten sind Antennen meist integriert oder es sind kleine Dipol-Antennen außen am Gerät befestigt. Teilweise können aber auch externe Antennen angeschlossen werden.

6.3 Antennen

Antennen sind sehr wichtig für eine sichere und stabile Übertragung. Sie dienen der Signalbündelung und der Verbesserung des Signal Rausch Abstandes (SNR Signal to Noise Ratio). Die Verbesserung des SNR wird als Antennengewinn bezeichnet. Dieser wird in der relativen Einheit dBi angegeben. Bezugspunkt ist ein isotroper Strahler¹ mit einem Gewinn von 1dBi. Ein Gewinn von 6dBi bedeutet dabei eine Verdoppelung des Gewinn in Bezug zum isotropen Strahler.

Es gibt eine sehr große Zahl von Antennenformen, die für die Übertragung im Frequenzbereich von 2,4 GHz in Frage kommen. Eine Auflistung gibt die verschiedenen Vor- und Nachteile der jeweiligen Bauform wieder.

¹Strahler mit kugelförmiger Ausbreitungscharakteristik

Dipol Rundstrahler mit einem Gewinn von 1,5dbi. Er wird sehr oft als einfache Antenne integriert.

Vertical Collinear ebenfalls ein Rundstrahler, dessen Ausbreitung in der Ebene erfolgt. Der Gewinn beträgt 5-11dbi. Gut geeignet für APs in Gebäuden

Yagi Antenne mit starker Richtwirkung und hohem Gewinn von 11-35dbi. Dient der Überbrückung von großen Reichweiten bei Punkt zu Punkt Verbindungen.

Waveguide ebenfalls starke Richtwirkung mit Gewinn 10-15dbi.

Quad Gewinn 10dbi mit kugelförmiger Ausbreitungscharakteristik, deshalb gut geeignet als Feed für Parabolantennen

Helix starke Richtwirkung mit hohem Gewinn 10-21dbi. Als Besonderheit drehende Polarisation, deshalb keine Mischung von Antennen möglich.

Die Übersicht gibt nur einen kleinen Teil der möglichen Bauformen wieder. Weitere Antennenformen werden auf vielen Internetseiten oder im ARRL Antenna Handbook von R. Dean Straw vorgestellt.

Es sei bemerkt, daß der Selbstbau und die Inbetriebnahme von Antennen bestimmten Restriktionen unterliegt. Die Inbetriebnahme ist nur dem zertifizierten Funkamateurl gestattet. Antennen, die im Fachhandel erhältlich sind, werden durch ein Zertifikat der RegTP genehmigt und sind frei verwendbar.

7 Literatur

Jörg Rech Ethernet Technologien und Protokolle für die Computervernetzung, Heise Verlag, 1. Auflage 2002

R. Dean Straw ARRL Antenna Book, 20th Bk&Cr

<http://www.myteron.de/wavehan/> (29.10.2003)

<http://standards.ieee.org/getieee802/> (20.10.2003)

8 Abkürzungen²

BSS	Basic Service Set	DQPSK	differential quadrature phase shift keying
ACK	acknowledgment	DS	distribution system
AID	association identifier	DSAP	destination service access point
AP	access point	DSM	distribution system medium
ATIM	announcement traffic indication message	DSS	distribution system service
BSA	basic service area	DSSS	direct sequence spread spectrum
BSS	basic service set	DTIM	delivery traffic indication message
BSSID	basic service set identification	ED	energy detection
CCA	clear channel assessment	EIFS	extended interframe space
CF	contention free	EIRP	equivalent isotropically radiated power
CFP	contention-free period	ERS	extended rate set
CID	connection identifier	ESA	extended service area
CP	contention period	ESS	extended service set
CRC	cyclic redundancy code	FC	frame control
CS	carrier sense	FCS	frame check sequence
CTS	clear to send	FER	frame error ratio
CW	contention window	FH	frequency hopping
DA	destination address	FHSS	frequency-hopping spread spectrum
DBPSK	differential binary phase shift keying	FIFO	first in first out
DCE	data communication equipment	GFSK	Gaussian frequency shift keying
DCF	distributed coordination function	IBSS	independent basic service set
DCLA	direct current level adjustment	ICV	integrity check value
DIFS	distributed (coordination function) interframe space	IDU	interface data unit
DLL	data link layer	IFS	interframe space
Dp	desensitization	Imp	intermodulation protection
		IR	infrared

²Quelle: ANSI/IEEE Std 802.11, 1999 Edition

ISM industrial, scientific, and medical	PMD-SAP physical medium dependent service access point
IV initialization vector	PN pseudo-noise (code sequence)
LAN local area network	PPDU PLCP protocol data unit
LLC logical link control	ppm parts per million
LME layer management entity	PPM pulse position modulation
LRC long retry count	PRNG pseudo-random number generator
lsb least significant bit	PS power save (mode)
MAC medium access control	PSDU PLCP SDU
MDF management-defined field	RA receiver address
MIB management information base	RF radio frequency
MLME MAC sublayer management entity	RSSI received signal strength indication
MMPDU MAC management protocol data unit	RTS request to send
MPDU MAC protocol data unit	RX receive or receiver
msb most significant bit	SA source address
MSDU MAC service data unit	SAP service access point
N/A not applicable	SDU service data unit
NAV network allocation vector	SFD start frame delimiter
PC point coordinator	SIFS short interframe space
PCF point coordination function	SLRC station long retry count
PDU protocol data unit	SME station management entity
PHY physical (layer)	SMT station management
PHY-SAP physical layer service access point	SQ signal quality (PN code correlation strength)
PIFS point (coordination function) interframe space	SRC short retry count
PLCP physical layer convergence protocol	SS station service
PLME physical layer management entity	SSAP source service access point
PMD physical medium dependent	SSID service set identifier
	SSRC station short retry count
	STA station

TA transmitter address

TBTT target beacon transmission time

TIM traffic indication map

TSF timing synchronization function

TU time unit

TX transmit or transmitter

TXE transmit enable

UCT unconditional transition

WAN wide area network

WDM wireless distribution media

WDS wireless distribution system

WEP wired equivalent privacy

WM wireless medium