Drahtlose Netze

Michael Dienert

15. Oktober 2012

Inhaltsverzeichnis

Zusammenfassung

abstract fehlt noch

1 Wer ist verantwortlich für welche Normierung

1.1 ITU

Die ist die **Internationale Fernmeldeunion** (*International Telecommunication Union*) und kümmert sich darum, dass **alle Telekommunikationssysteme international kompatibel** sind.

Innerhalb der ITU gibt es Unterteilungen. Die beiden wichtigsten:

ITU-T das **T** steht für *Telekommunication*. Die ITU-T ist verantwortlich für Telefonsysteme.

ITU-R das **R** steht für *Radioncommunication*. Die ITU-R regelt die Vergabe von Funkfrequenzen und Standards in der drahtlosen Kommunikation.

Die ITU-R regelt, welche Funkfrequenzbereiche für WLANs vorgesehen sind

1.2 IEEE

IEEE ist die Abkürzung von *Institute of Electrical and Electronics Engineers*, einem weltweit tätigen Verein, der Standards für die Nachrichten-, Energie und Informationstechnik verabschiedet.

Im Februar 1980, wurde innerhalb des IEEE ein Projekt mit der Nummer 802 [1] gestartet, das sich um Standards der meisten Netzwerktechnologien der ISO-Schichten 1 und 2 kümmert.

Für einzelne Netztechnologien wurden wiederum Arbeitsgruppen gebildet, die durchnummeriert wurden. Beispiele:

802.3 Ethernet, CSMA/CD

802.5 TokenRing

802.11 Wireless Lokal Area Networks

802.15 Bluetooth

IEEE 802.11 regelt, wie die Funkfrequenzsignale mit den Daten moduliert werden.

[1] Jahr: 80, Monat: 2

1.3 WiFi-Alliance

WiFi steht für *Wireless Fidelity* (drahtloses Vertrauen) und ist eine *Herstellervereinigung*.

> Das WiFi-Label soll dem Kunden zusichern, dass damit ausgestattete Geräte untereinander kompatibel sind.

2 Ethernet und WLAN

Drahtlose Netze nach 802.11 haben viele Gemeinsamkeiten mit dem klassischen Ethernet (802.3).

Gemeinsamkeiten

Shared Medium Klassisches Ethernet auf Koax-Leitungen und WLAN arbeiten beide mit einem einzigen Übertragungsmedium:

- **Ethernet** Koax-Leitung mit vielen Teilnehmern
- **WLAN** Funkkanäle, also Frequenzbereiche, in denen ein zulassungsfreier Betrieb gestattet ist (ISM-Bänder)

wahlfreier Zugriff die Teilnehmer sind gleichberechtigt, jeder kann auf das Medium (Kabel/Funkkanal) zugreifen, wenn dieses frei ist.

Kollisionen es kann passieren, dass Teilnehmer gleichzeitig zu senden anfangen. Dadurch entstehen Kollisionen. Die Behandlung von Kollisionen ist bei Ethernet und WLAN leicht unterschiedlich.

Unterschiede und Nachteile gegenüber modernen, kollisonsfreien Netzen

Störungen Funkkanäle werden leicht durch elektromagnetische Wellen von aussen gestört. Eine Übertragung wird dadurch u.U. unmöglich.

Beispiel: Störung von WLANs mit 2.4GHz durch Mikrowellengeräte.

WLANs, die in unmittelbarer Nachbarschaft betrieben werden, stören sich gegenseitig. Da die Anzahl an WLANs an einem Standort bei den 2.4GHz-WLANs auf maximal 4 begrenzt ist, kann das einen Betrieb ebenfalls unmöglich machen.

Ethernet-Kupfer-Leitungen sind wesentlich störunempfindlicher und LWL-Leitungen sind gegen elektromagnetische Störungen völlig imun.

Sicherheit WLANs lassen sich sehr leicht abhöhren. Es genügt ein Notebook mit entsprechender Hardware (heutzutage absoluter Standard).

Kupferleitungen lassen sich nur mit speziellen Geräten abhören (die Kupferleitung wirkt wie eine Antenne und strahlt -wenn auch sehr schwach- Signale ab).

Natürlich können Ethernet-Leitungen angezapft werden, dafür ist dann aber schon mehr Aufwand und kriminelle Energie notwendig.

Anzahl Teilnehmer Der allergrösste Nachteil von WLANs: das WLAN verhält sich wie ein Hub. Es ist also nur Halbduplex-Betrieb möglich.

Aufwand WLANs sind im privaten Bereich ungeheuer populär, da keinerlei Verkabelungsarbeiten notwendig sind. Bei kommerziellen Anlagen sollte immer eine Verkabelung vorgenommen werden.

3 ISM-Bänder

ISM steht für *Industrial, Scientific and Medical*. Damit sind eine Reihe von Funkfrequenzbereichen gemeint, die zum Teil einen genehmigungsfreien Betrieb von Hochfrequenzanlagen unter Auflagen (z.B. geringe Sendeleistung) erlauben.

Die ISM-Bänder werden -wie kann es anders sein- von der ITU-R (Kap. 1.1) vergeben.

Beispiele für Anwendungen:

- Babyphone
- Modellfernsteuerungen
- Funkgeräte kleiner Reichweite (PMR 446)
- Zentralverriegelung, Garagentoröffner
- Mikrowellenherde
- WLANs

Die WLAN-Standards 802.11b, 802.11g und 802.11n arbeiten auf dem 2.4 GHz-ISM Band. Dadurch können sie u. U. stark von ISM-Geräten gestört werden. Z.B. strahlen Mikrowellenherde bei 2.455 GHz und stören damit diese WLAN-Geräte stark.

In Europa liegt der Frequenzbereich des Standards 802.11a und 802.11n im 5GHz-Modus (802.11n hat noch einen zweiten Frequenzbereich von 5GHz) ausserhalb der ISM-Bänder. Damit sind diese WLAN-Netze nicht so störanfällig.

3.1 2.4 GHz ISM-Band

Das ISM-Band bei 2.4 GHz reicht von 2.4 bis 2.5 GHz, ist also 100MHz breit. Allerdings wurde für WLAN-Anwendungen nicht der gesamte 100MHz breite Bereich freigegeben: Nur die Kanäle unterhalb von 2.484 MHz sind erlaubt.

Welche Betriebsart welche Kanäle belegt, zeigt Abb. 1.

Die neuere Modulationsart OFDM benötigt bei gleicher Datenrate nur ein 20MHz breites Band. Damit lassen sich 4 Funknetze an einem Ort gleichzeitig betreiben (Kanäle 1, 5, 9 und 13).

Bei der alten Modulationsart DSSS ist der Bandbreitenbedarf 22MHz, deshalb passen da nur 3 Funknetze auf den Kanälen 1, 6 und 11 parallel ins ISM-Band.

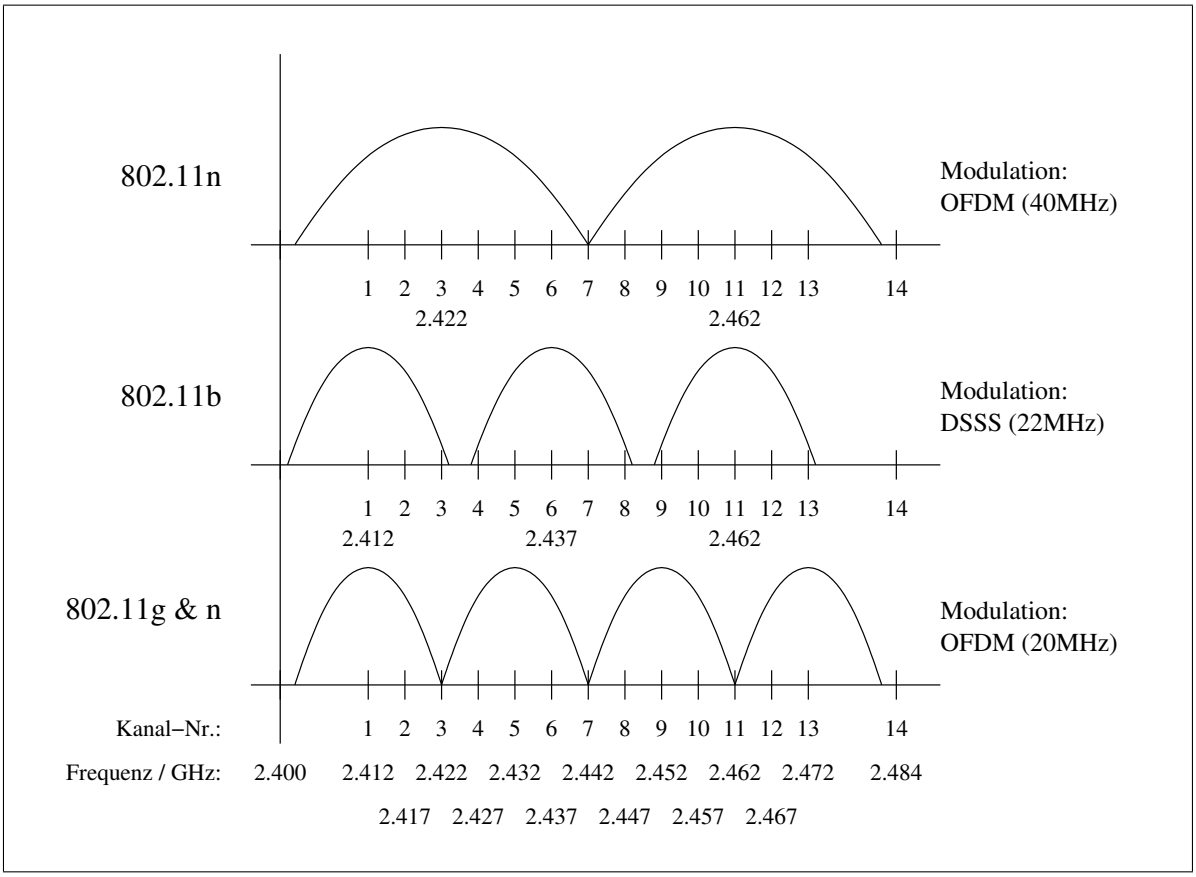

Abbildung 1: Der Bandbreitenbedarf der verschiedenen 802.11-Technologien bei 2.4 GHz

4 Strahlungsleistung

Die Strahlungsleistung einer Sendeantenne wird mit **EIRP** angegeben. Dabei steht EIRP für *equivalent isotropically radiated power.*

Erklärung: eine Antenne strahlt Funkwellen ab. Das tut sie aber nicht gleichmässig in alle Richtungen, sondern die Strahlungsleistung konzentriert sich in manchen Richtungen wie z.B. das Licht unter einem Lampenschirm.

Spezielle *Richtantennen* konzentrieren die Funkwellen sogar wie der Reflektor eines Autoscheinwerfers.

Dieses Konzentrieren der Funkwellen wird *Antennengewinn* genannt.

Damit Funkgeräte nicht andere Geräte stören, wird deshalb nicht die Leistung am Antenneneingang begrenzt, sondern es wird reguliert, wie "hell" sozusagen der "Lichtkegel" bei einer bündelnden Antenne sein darf, damit er andere nicht blendet.

Die EIRP ist die Leistung am Antenneneingang multipliziert mit dem Antennengewinn.

Vorstellen kann man sich das etwa so: wenn man mit einer Taschenlampe in einem Zimmer die Wand anleuchtet, ist die EIRP im Leuchtfleck die Leistung, die ich einer nackten Glühlampe zuführen muss, damit es an der Stelle der Wand genauso hell wird. Da die nackte Glühlampe den ganzen Raum ausleuchtet und die Taschenlampe nur einen kleinen Fleck, ist die EIRP viel höher, als die Leistung der Taschenlampenbirne.

4.1 Antennengewinn

Der Antennengewinn ist der Faktor, um den bei einer bündelnden Antenne im Strahlungsbündel mehr Leistung vorhanden ist, als bei einer Antenne, die in alle Richtungen gleichmässig abstrahlt (Isotropenstrahler).

Dieser Faktor wird in Dezibel angegeben:

Antennengewinn $g = 10 \cdot log \frac{P_{Antenne}}{P_{Isotropenstrahler}}$

Der Gewinn einer Antenne wirkt sich nicht nur beim Senden, sondern auch beim Empfang aus.

Die Antennengewinne (in Dezibel) von Sende- und Empfangsantenne dürfen addiert werden.

4.2 Berechnung der Strahlungsleistung (EIRP)

Strahlungsleistung $EIRP = 10^{g/10} \cdot P_{WLAN}$

Beispiel: An einen Access-Point wird eine Antenne angeschlossen, die 6dB Gewinn hat. Der Sendeteil des Access-Points hat eine Ausgangsleistung von 100mW. Dann ist die EIRP:

$EIRP = 10^{6/10} \cdot 100mW = 400mW$

4.3 Anpassung der Ausgangsleistung

In Deutschland ist die Strahlungsleistung (EIRP) von WLAN-Sendern reglementiert:

Frequenz	EIRP
2.4 GHz	100mW
5 GHz	500mW

Wird nun eine Antenne mit höherem Gewinn verwendet als die mitgelieferte, ist die Sendeleistung entsprechend zu senken, damit die EIRP nicht überschritten wird.

Inzwischen ist auch Richtfunk im 5GHz-Band mit bis zu 4W EIRP möglich, das erfordert aber eine Anmeldung bei der Netzagentur.

4.4 Strahlungsleistung und Reichweite

Möchte man die Reichweite eines Funksystems verdoppeln, muss man die Strahlungsleistung vervierfachen. In Dezibel ausgedrückt: pro 6db mehr Strahlungsleistung verdoppelt sich die Reichweite.

5 Übersicht WLAN-Standards

5.1 Modulation

Die einzelnen WLAN-Standards arbeiten mit z.T. unterschiedlichen Modulationsverfahren. Modulieren heisst, die digitalen Informationen mit Änderungen der Funkfrequenz (Frequenzmodulation FM) oder zeitlichen Verschiebungen im Funksignal (Phasenmodulation PSK) zu übertragen.

Folgende Verfahren sind gebräuchlich:

DSSS Direct Sequence Spread Spectrum; wird bei 802.11 und 802.11b vewendet. DSSS ist nicht so leistungsfähig wie die nachfolgend aufgeführten Modulationsarten.

OFDM Orthogonal Frequency Division Multiplex; OFDM ist der Standard bei 802.11a und 802.11g. Es kann bei gleichem Bandbreitenverbrauch mehr Daten übertragen als DSSS.

MIMO Multiple Input Multiple Output : mehrere Sender, Empfänger und Antennen (bis zu 4 Antennen pro Seite) können gleichzeitig betrieben werden. MIMO wird bei 802.11n verwendet und erreicht Datenraten bis zu 600MBit/s.

5.2 Trägerfrequenz

In Europa sind die beiden Trägerfrequenzen 2.4 GHz (eine ISM-Frequenz) und 5 GHz gebräuchlich. Siehe auch Kap. 3.

Vor- und Nachteile:

Reichweite Signale kleinerer Frequenz haben eine höhere Reichweite. D.h. mit 2.4 GHz kann man grössere Distanzen überbrücken als mit 5 GHz. Das wird aber wieder ausgeglichen, da die EIRP bei 5GHz 500mW betragen darf. Bei 2.4 GHz sind es nur 100mW.

Abschattung Je höher die Frequenz, desto eher verhalten sich die Funkwellen wie Licht. D.h. werden von Gegenständen blockiert (es gibt dann einen Funkschatten).

Belegung Da 2.4 GHz auch von vielen ISM-Geräten benutzt wird und es inzwischen zu viele 2.4 GHz WLANs gibt, gibt es hier viele Störungen. 5 GHz Geräte sind noch lange nicht so verbreitet und damit sind 5GHz-WLANs störungsfrei (noch).

Protokoll	veröffentlicht	Frequenz	Durchsatz (netto)	Datenrate (brutto)	Multiplex-verfahren	Reichweite (im Haus, abhängig von Wänden)	Reichweite (Radius im Freien, inkl. einer Wand)
802.11	1997	2.4 GHz	0.9 Mbit/s	2 Mbit/s	DSSS	ca. 20m	ca. 100m
802.11a	1999	5 GHz	23 Mbit/s	54 Mbit/s	OFDM	ca. 35m	ca. 120m
802.11b	1999	2.4 GHz	4.3 Mbit/s	11 Mbit/s	DSSS	ca. 38m	ca. 140m
802.11g	2003	2.4 GHz	19 Mbit/s	54 Mbit/s	OFDM	ca. 38m	ca. 140m
802.11n	2009-10	2.4 GHz 5 GHz	74 Mbit/s	248 Mbit/s (600 Mbit/s)	MIMO	ca. 70m	ca. 250m
802.11y	2008-09	3.7 GHz	23 Mbit/s	54 Mbit/s		ca. 50m	ca. 5000m

6 Access Points

AccessPoints sind WLAN-Geräte, die ausser der Hardware für die Funkübertragung eine Schnittstelle zum kabelgebundenen Ethernet haben.

Der AP konvertiert also EthernetII(802.3)-Frames in das 802.11-WLAN-Rahmenformat. Die Nutzlast der Rahmen (TCP/IP) bleibt unangetastet.

Die WLAN-Teilnehmer buchen sich mit einem bestimmten Verfahren beim AP ein, etwa so, wie Ethernet-Geräte an einen Hub angeschlossen werden. Der AP bildet somit einen *drahtlosen Hub*.

7 CSMA/CA

CSMA/CA funktioniert sehr ähnlich wie CSMA/CD von Ethernet. Nur wird statt *Collision Detection (CD) Collison Avoidance (CA)* verwendet, weil es technisch sehr schwierig wäre, eine Kollisionserkennung zu bauen (Grund: Funkgeräte können nicht gleichzeitig senden und empfangen).

Stattdessen sendet der Empfänger nach erfolgreichem Empfang eine Bestätigung an den Sender. Mit dieser Bestätigung weiss der Sender dass keine Kollision stattgefunden hat.

8 Hidden Nodes Problem

Beim Carrier-Sense-Verfahren hören die Stationen das Medium ab. Ist nichts zu hören, kann gesendet werden.

Nun kann es passieren, dass z.B. 3 Stationen A, B, C so auf einer Linie liegen, dass jeweils A und B bzw. B und C sich sehen, aber nicht A und C, weil sie zu weit auseinander sind und das Funksignal zu schwach wird. Damit würde das Carrier-Sense-Verfahren nicht mehr funktionieren und es käme zu Kollisionen.

8.1 RTS/CTS

Abhilfe schafft das RTS/CTS-Verfahren (RTS = Request to Send, CTS = Clear to Send).

Wird RTS/CTS eingeschaltet, übernimmt der Access-Point die Rolle des Chefs: wer senden möchte, beantragt (Antrag = RTS) eine Sendeerlaubnis (CTS). Wer die Sendeerlaubnis nicht hat, muss still sein.

Mit RTS/CTS wird der Access-Point also zum Busmaster, der die Zugriffe auf das Medium koordiniert.

9 Begriffe

9.1 Basic Service Set

Bilden WLAN-Geräte ein sog. Ad-Hoc-Netz, spricht man von einem *Independent Basic Service Set* . Bei einem Ad-Hoc-Netz gibt es *keinen Access-Point*.

Mehrere WLAN-Geräte, die sich bei einem Access-Point eingebucht haben bilden ein sog. *Basic Service Set*.

9.2 Extended Service Set

Bei Extended Service Sets werden mehrere Access-Points verwendet, um die Reichweite zu erhöhen. Meistens verwenden die einzelnen APs eine einheitliche Kennung (SSID, siehe Unten), damit die Clients leicht von einem AP zum nächsten wechseln können (Roaming).

9.3 SSID

SSID = Service Set Identifier. Die SSID ist ein frei wählbarer Name (32 ASCII-Zeichen) für ein Service Set.

9.4 BSSID

Die BSSID ist die MAC-Adresse des Access-Points, der das Service-Set bedient.

10 Netzbeitritt (Association)

Möchte eine Station einem Funknetz beitreten, läuft Folgendes ab:

Beacon Beacon bedeutet wörtlich übersetzt *Funkfeuer*. Das sind kurze Funksignale (10 mal pro Sekunde), die der Access-Point abgibt, damit die Clients ihn überhaupt finden können.

Man kann sich den Beacon also wie einen Leuchtturm der vor sich hinblinkt, vorstellen.

Im Beacon enthalten ist die SSID. Dies lässt sich abschalten, was aber nicht dem WLAN-Standard entspricht!

Probe Hat ein Client einen Beacon empfangen, sendet er seinerseits:

- SSID
- Unterstützte Datenraten

Und der AP antwortet mit:

- SSID
- Unterstützte Datenraten
- Verschlüsselungsverfahren

Authentication Es gibt zwei Authentifizierungsarten:

Open bedeutet *keine Authentifizierung*

Shared Key Eine Authentifizierung, die auf einem zwischen AP und Client ausgetauschten Schlüssel basiert. Dieser Authentifizierungsmechanismus heisst **WEP** (Wired Equivalent Privacy). WEP ist absolut unsicher und wird bei modernen WLAN-Geräten durch bessere Techniken *ergänzt*.

Association ist die Authentifizierung mit WEP erfolgreich, tauschen AP und Client einige Daten aus:

- Client MAC-Address
- Access-Point-MAC-Address (BSSID) vlg. 9.4
- eine Association-ID: *AID*

Association: da der AP einen drahtlosen Hub darstellt, wird bei der Association ein virtueller Port am Hub für den jeweiligen Client bereitgestellt. D.h. der Client "stöpselt" sich virtuell am AP ein

11 Sicherheit

Der ursprüngliche Standard WEP ist heutzutage absolut untauglich, um ein WLAN abzusichern. Verwendung findet er nur noch bei Netzbeitritt (Association, s.o.).

Ist der Netzbeitritt erfolgt, können AP und Client 802.1-Datenpakete austauschen und mit dem *Extensible Authentication Protocol* (EAP) die eigentliche Authentifizierung aushandeln.

11.1 WPA und WPA2

Aktueller Standard ist **WPA2** (WiFi Protected Access, Vers. 2).

- WPA2 implementiert den Standard 802.11i
- WPA2 verwendet AES als Verschlüsselungsalgorithmus
- WPA2 ist der Nachfolger von WPA. WPA wurde von der WiFi-Alliance als Verbesserung von WEP entwickelt, war aber kein IEEE-Standard (sondern eben ein Pseudeostandard).
- WPA verwendet TKIP als Verschlüsselung

11.2 Pre-Shared-Key

Zur Authentifizierung kann WPA2 zwei Verfahren benutzen:

Pre-Shared-Key ein PSK ist ein geheimer, **vorher** ausgetauschter Schlüssel. Schlüssellänge bei WPA2: 63 Zeichen.

> Die Authentifizierung mit PSK wird auch als *Personal Mode* bezeichnet, da sie vor allem für Privatanwendungen verwendet wird.

Radius Neben dem *Personal Mode* mit PSK, gibt es den *Enterprise Mode*, bei dem die Authentifizierung über einen *RADIUS Server* erfolgt.

Ein RADIUS Server ist ein Dienst, der Benutzername und Kennwort bei der Anmeldung überprüft. Er arbeitet mit Datenbanken oder Verzeichnisdiensten (LDAP).