

# **Wireless LAN Evaluierung**

## **Arbeitsweise, Varianten, Schwachstellen, Planung, Installation**

**von**

**Dipl.-Math. Cornelius Höchel-Winter**

mit Einzelbeiträgen von

Mark Groten  
Dr. Simon Hoff  
Dipl.-Inform. Gaby van Laak  
Dr. Joachim Wetzlar

#### 5.4 Übertragungstechnik (PHY-Layer)

Der **Physical Layer (PHY)** des IEEE 802.11 ist in zwei Sublayer aufgeteilt. In der ersten Schicht „**Physical Medium Dependent**“ sind die schnittstellenspezifischen Funktionen der verschiedenen physikalischen Schnittstellen und die zugehörigen Übertragungstechniken festgelegt. In der zweiten Schicht stellt das **PLCP (Physical Layer Convergence Protocol)** dem übergeordneten, gemeinsamen MAC-Layer einheitliche, technologiespezifische Schnittstellen zur Verfügung.

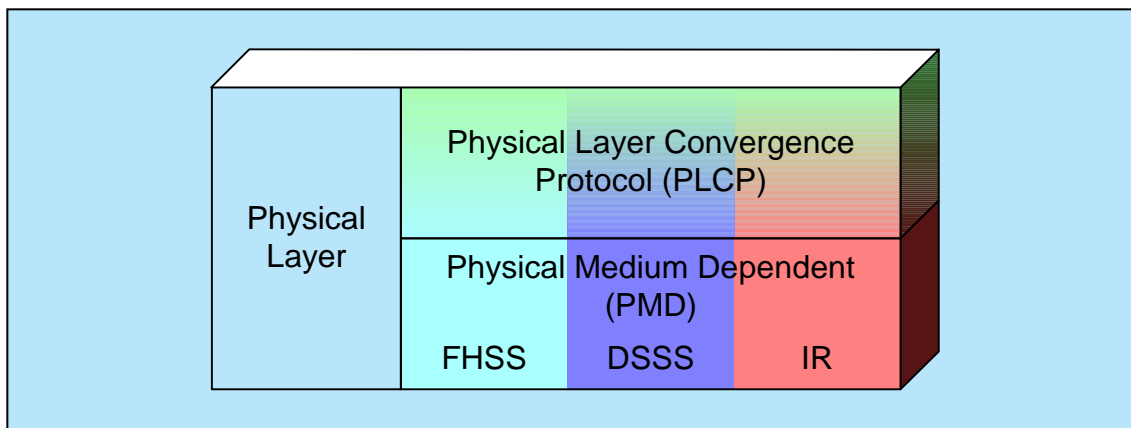


Abbildung 5.15: Physical Layer

Im ursprünglichen Standard 802.11 von 1997 sind drei physikalische Schnittstellen definiert:

- DSSS im 2,4-GHz-Band,
- FHSS im 2,4-GHz-Band und
- eine Infrarot-Schnittstelle.

Daneben definiert der Standard 802.11a eine vierte Schnittstelle im 5-GHz-Band mit Übertragungsraten bis 54 Mbit/s.

Nach 1999 wurde dann in mehreren Schritten das DSSS-Interface im 2,4-GHz-Band erweitert. Zunächst wurden im Standard IEEE 802.11b die Übertragungsraten auf 11 Mbit/s erweitert. Hierzu sind mit CCK und PBCC zwei erweiterte Modulationsverfahren definiert, die aber weiterhin mit derselben Taktrate arbeiten wie das DSSS-Interface. Darüber hinaus sieht der Standard für beide Modulationen ein optionales, kürzeres Headerformat vor.

Dieser Standard wurde 2003 nochmals durch den Standard 802.11g erweitert. Hierbei wird die gesamte OFDM-Technologie des 802.11a mit allen Formaten in das 2,4-GHz-Band übernommen. Damit werden auch hier Übertragungsraten bis 54 Mbit/s zur Verfügung gestellt. Zusätzlich können alle Systeme nach 802.11g kompatibel zu 802.11b betrieben werden und unterstützen daher beide Header-Formate des 11b. Zwei weitere Modulationsverfahren ergänzen das

Portfolio: eine Erweiterung der PBCC-Modulation unterstützt Übertragungsraten bis 33 Mbit/s und eine Mischform aus 11b-Header und OFDM-Datenteil mit den OFDM-Raten bis zu 54 Mbit/s. Beide optionalen Formate werden mit beiden 11b-Headerformaten unterstützt.

Die folgende Tabelle fasst die zurzeit definierten Schnittstellen zusammen.

<b>IEEE 802.11:</b>		
I.	DSSS	
II.	FHSS	
III.	Infrarot	
<b>IEEE 802.11b:</b>		
IV.	DSSS/CCK	umfasst I.
V.	DSSS/CCK/short	optional, umfasst IV.
VI.	DSSS/PBCC	optional, umfasst IV.
VII.	DSSS/PBCC/short	optional, umfasst VI.
<b>IEEE 802.11g:</b>		
VIII.	OFDM	umfasst V.
IX.	DSSS/PBCC	optional, umfasst VII. und VIII.
X.	CCK-OFDM	optional, umfasst VIII.
<b>IEEE 802.11a:</b>		
XI.	OFDM	

**Tabelle 5.2: Physikalische Schnittstellen des 802.11**

### 5.4.3 Extended High Rates nach 802.11g

Mit der zweiten Erweiterung von 2003 wurden weitere Modulationsverfahren für das Interface festgelegt. Verpflichtend für alle Systeme nach 802.11g wird das OFDM-Verfahren aus dem Standard IEEE 802.11a aus dem 5-GHz-Band in das 2,4-GHz-Band übernommen. Dieses Verfahren stellt acht weitere Übertragungsraten mit 6, 9, 12, 18, 24, 36, 48 und 54 Mbit/s zur Verfügung, wobei lediglich 6, 12 und 24 Mbit/s verpflichtend für alle Systeme vorgeschrieben sind.

**OFDM (Orthogonal Frequency Division Multiplexing)** verwendet eine gänzlich andere Modulationstechnologie als die bisher beschriebenen Verfahren (siehe auch Kapitel 3.4.2.1). OFDM unterteilt prinzipiell den verfügbaren Frequenzbereich in mehrere Unterkanäle (Carrier). Das Datensignal wird meist über geeignete fehlertolerante Kodierungen abgesichert und dann auf den Unterkanälen parallel übertragen.

Der Standard 802.11a legt pro Kanal 52 Unterkanäle fest, von denen jedoch vier zur Synchronisation genutzt werden und nur 48 zur Datenübertragung zur Verfügung stehen. Der Datenstrom wird über Vorwärtsfehlerkorrektur-Codes im Verhältnis 1:2, 2:3 oder 3:4 gesichert, auf die Unterkanäle verteilt und dort mit vier möglichen Modulationsverfahren übertragen. Die vom Standard unterstützten Modulationen und die daraus resultierenden Übertragungsraten sind in der folgenden Tabelle 5.3 aufgelistet.

Kodier-Verhältnis	Modulation	Kodierte Chips pro Carrier	Bits pro Symbol	Datenrate
1 : 2	BPSK	1	24	6 Mbit/s
3 : 4	BPSK	1	36	9 Mbit/s
1 : 2	QPSK	2	48	12 Mbit/s
3 : 4	QPSK	2	72	18 Mbit/s
1 : 2	16-QAM	4	96	24 Mbit/s
3 : 4	16-QAM	4	144	36 Mbit/s
2 : 3	64-QAM	6	192	48 Mbit/s
3 : 4	64-QAM	6	216	54 Mbit/s

**Tabelle 5.3: Modulationsverfahren und Datenraten nach IEEE 802.11a**

Zusätzlich zu den OFDM-Verfahren fordert der 802.11g-Standard, dass alle Systeme auch die DSSS/CCK-Modulation nach 802.11b unterstützen, und zwar sowohl in der Long-Header-Version als auch mit Short Headers. Damit muss

bei 11g-Produkten das Short-Header-Format verpflichtend von allen Systemen unterstützt werden.

#### 5.4.3.1 Optionale Modulationen im 802.11g

Wie im 802.11b-Standard führt auch der 802.11g-Standard die optionalen **PBCC**-Modulationsverfahren weiter. Nach den 5,5- und 11-Mbit/s-Varianten nach 802.11b definiert der neue Standard zwei weitere Varianten mit 22 Mbit/s und 33 Mbit/s. Für beide Verfahren wird die 1/2-Kodierung durch eine 2/3-Kodierung ersetzt. Das hiermit aus je zwei Datenbits entstehende Triple wird jeweils einem Symbol zugeordnet und über eine 8-wertige PSK übertragen.

Bleibt man also bei der bekannten Taktrate von 11 MChip/s erhält man eine Datenübertragungsrate von 22 Mbit/s. Um die Datenrate von 33 Mbit/s zu erreichen, muss die bis dahin unveränderte Taktrate auf 16,5 MChip/s angehoben werden.

Insgesamt werden im 802.11g also drei verschiedene PHY-Headerformate unterstützt:

1. das Long-Header-Format nach 802.11,
2. das Short-Header-Format nach 802.11b und
3. OFDM-Header.

Das Long-Header-Format ist interoperabel mit den DSSS-Formaten mit 1 und 2 Mbit/s, mit den 802.11b-Formaten mit 5,5 und 11 Mbit/s und mit den PBCC-Formaten mit 5,5 bis 33 Mbit/s. Das Short-Header-Format wird wie im 802.11b mit Datenraten von 2 Mbit/s bis 11 Mbit/s und den PBCC-Formaten unterstützt.

Um auch die hohen Übertragungsraten der OFDM-Modulationen mit einem kompatiblen Header ausrüsten zu können, wurde ein drittes, ebenfalls optionales Verfahren definiert, welches die DSSS-Header mit einem OFDM-Datenteil kombiniert. Dieses **CCK-OFDM**-Verfahren hat die Besonderheit, dass unmittelbar nach dem Header von einer Single-Carrier-Transmission auf eine Multi-Carrier-Transmission umgeschaltet werden muss, um den OFDM-Datenteil zu senden.

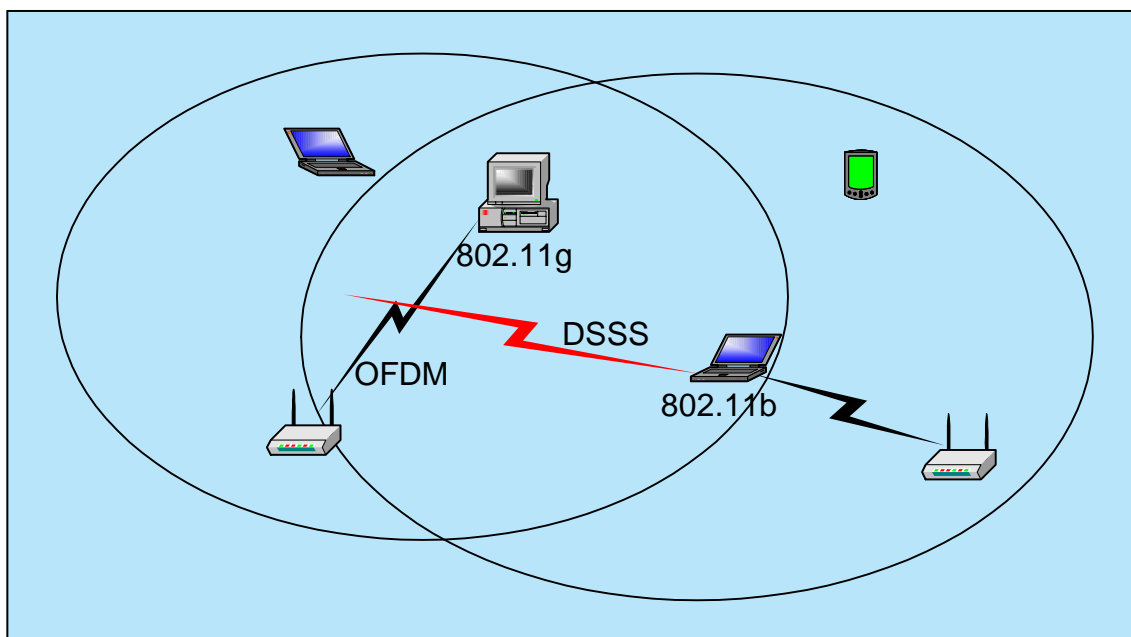
#### 5.4.4 Interoperabilität zwischen 802.11b und 802.11g

Zusammenfassend kann man feststellen, dass der Standard 802.11g im Wesentlichen die Technologien aus 802.11a und 802.11b in einem Gerät und einem Frequenzband zusammenführt. Leider sind diese Technologien jedoch nicht kompatibel und daher müssen zusätzliche Vorkehrungen getroffen werden, damit sich die technologische Kompatibilität der Geräte, die im Standard ja gefordert ist, auch praktisch durch einen gleichzeitigen Betrieb im selben WLAN auszahlen kann. Was nützt ansonsten ein Access Point, der zwar beide Übertragungsformate beherrscht, wenn in einem WLAN nicht auch beide Formate tatsächlich eingesetzt werden können.

Wie am Ende des vorigen Kapitels bemerkt, sind zunächst einmal die Header der beiden verpflichtend vorgeschriebenen Modulationen OFDM und DSSS/CCK nicht interoperabel. Der Standard fordert zwar, dass 11g-Geräte sowohl OFDM- als auch DSSS-Sendungen erkennen können und damit genau wissen, wann andere Systeme senden und wann das Medium frei ist. Das können aber 11b-Geräte nicht! Zwar gibt es mit CCK-OFDM ein Verfahren, das diesen Konflikt lösen kann, da es einen kompatiblen 11b-Header benutzt, aber leider ist dieses Verfahren nur optional. Das heißt, man kann sich nicht darauf verlassen, dass alle Produkte dieses Verfahren unterstützen werden. Die Erfahrung lehrt im Gegenteil, dass die Unterstützung optionaler Verfahren eher die exotische Ausnahme bleibt. Die Intension der IEEE an diesem Punkt ist klar: Weg mit den Altlasten, hin zu OFDM, und zwar in Reinkultur.

Damit sind aber in einem gemischten WLAN mit 11g- und 11b-Geräten die OFDM-Frames hochgradig gefährdet von den 11b-Geräten abgeschossen zu werden, da diese die OFDM-Frames nicht sehen können. Der Standard empfiehlt (!) an dieser Stelle, dass die Access Points alle 11g-Systeme dynamisch in einen Kompatibilitätsmodus schalten. In diesem Modus werden alle OFDM-Frames durch einen vorangehenden RTS-CTS-Handshake im (langsamen!) 11b-Format geschützt. Diese RTS- und CTS-Frames informieren das WLAN darüber wie lange das Medium belegt sein wird und werden von den 11b-Systemen verstanden. Der zu erwartende Overhead dieses Kompatibilitätsmodus wird enorm sein (siehe auch Kapitel 5.5.6.1).

Ungünstigerweise überlässt es der Standard auch noch den Herstellern Entscheidungskriterien zu implementieren, ob und wann dieser Modus eingeschaltet wird, oder ob es günstiger ist, das Risiko einzugehen und die OFDM-Frames nicht zu schützen. Wichtig bei diesen Überlegungen ist in jedem Fall, dass dieser Mechanismus auch Funkzellen übergreifend funktionieren muss. Es nützt nämlich nichts, wenn in einem reinen 11g-Netzwerk auf den RTS-CTS-Schutz der OFDM-Frames verzichtet wird, solange ein überlappendes Netz mit 11b-Geräten für massive Interferenzen sorgt.



**Abbildung 5.20: Interferenzen durch 802.11b im 802.11g-Netz**

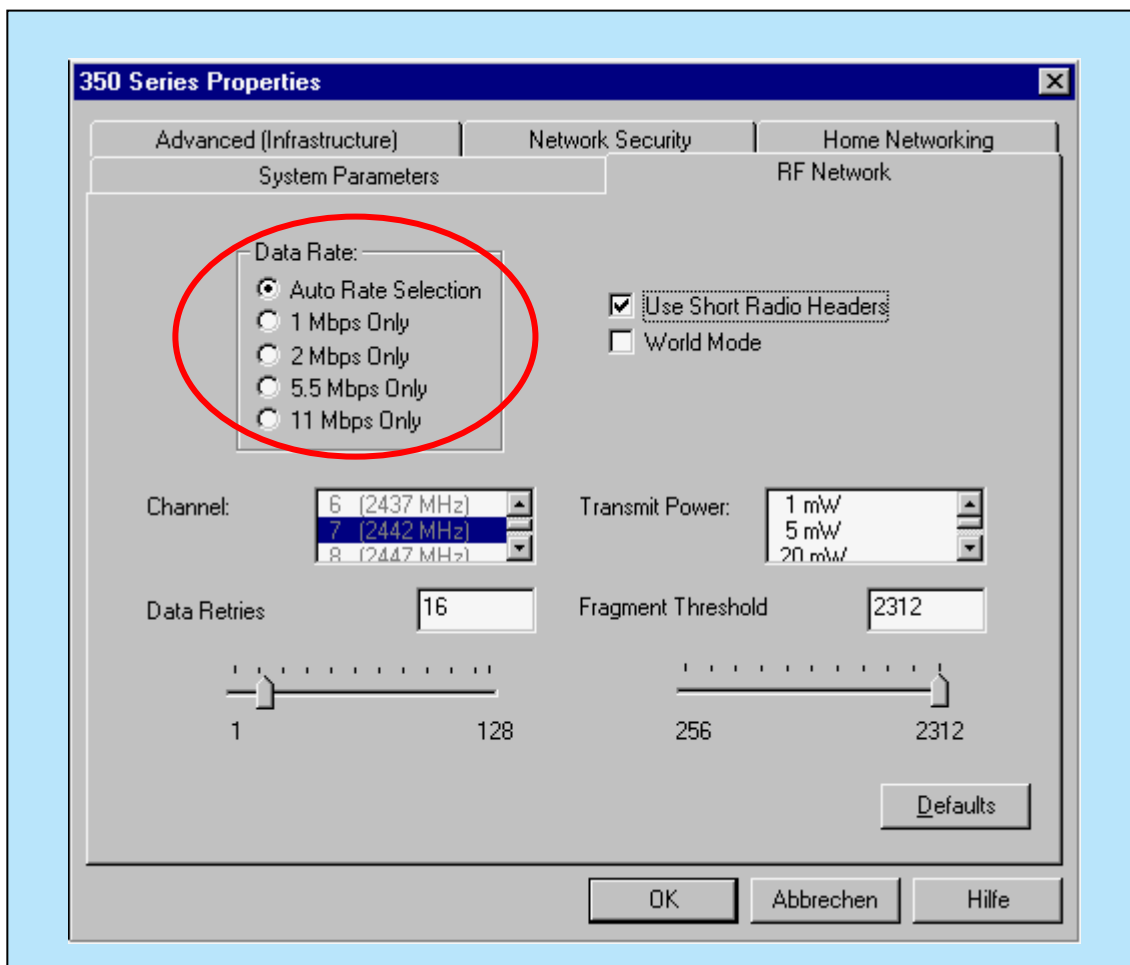
Die Zusammenführung von 802.11a und 802.11b führt jedoch noch zu einem weiteren Problem. Das bei Wireless LANs verwendete Medienzugangsverfahren CSMA/CA setzt auf verschiedenen Timern auf (für Details zum Verfahren siehe Kapitel 5.5.2), einer davon ist die so genannte *Slot Time*. Anhand dieser Slot Time berechnet jede Station die Zeit, die sie warten muss bis sie endlich senden darf, nachdem das Medium von einer anderen Station belegt war. Im 802.11 und unverändert auch im 802.11b wird die Slot Time für das DSSS-Interface auf  $20\ \mu\text{s}$  festgelegt, im 802.11a dagegen für die OFDM-Verfahren auf  $9\ \mu\text{s}$ . Es ist nun aber offensichtlich, dass in einem Netzwerk alle aktiven Systeme die gleiche Slot Time verwenden müssen. Ansonsten werden nämlich die Systeme, die die höhere Slot Time verwenden, im Mittel länger warten und damit deutlich benachteiligt.

Im Mischbetrieb müssen also alle Stationen in einer Funkzelle auf  $20\ \mu\text{s}$  zurückschalten, sobald sich eine einzige 11b-Station anmeldet. Dieses Zurückschalten sollte standardgemäß dynamisch während des aktiven Netzwerkbetriebs möglich sein, allerdings gibt es Produkte (bzw. Firmwareversionen), die im gemischten Modus von Anfang an quasi mit gezogener Handbremse fahren.

Auch dieser Punkt muss zellenübergreifend funktionieren, da sonst die Zelle mit den höheren Timern ins Hintertreffen gerät.

Konfigurationsparameter wie „11g-only“ oder „Mixed Mode“ scheinen die angesprochenen Probleme zu adressieren, wobei die genaue Bedeutung dieser Einstellungen in den meisten Fällen nicht klar wird. Zumindest im „11g-only-Modus“ lassen die getesteten Access Points keine 11b-Clients mehr zu und setzen dann vermutlich die kürzere Slot Time von  $9\ \mu\text{s}$  ein.

## 5.4.5 Rate Selection

**Abbildung 5.21: Konfiguration der Datenrate**

Alle WLAN-Systeme, angefangen von den ersten Produkten nach 802.11 über 802.11a und 11b bis zu den neusten nach 802.11g und 11h haben die Eigenschaft, mehrere verschiedene Übertragungsraten zu unterstützen. Dies ist sinnvoll, da die höheren Übertragungsraten durch empfindlichere Modulationen und durch weniger fehlertolerante Kodierungen erkauft wurden. So sind die CCK-Verfahren aus 802.11b wie die im Kapitel 3.4.1 vorgestellten CDMA-Verfahren entfernungs- und geschwindigkeitsempfindlich. D.h. die Qualität des empfangenen Signals nimmt mit wachsender Entfernung vom Sender stärker ab als bei den niedrigeren Übertragungsraten. Bei den OFDM-Verfahren wird bei gleicher Modulation eine 1/2-Kodierung durch eine 3/4-Kodierung ersetzt. Mit wachsender Entfernung sinkt aber einerseits die Signalstärke und andererseits nehmen Reflexionen und Dämpfung zu. Das Signal wird also immer ungenauer und versinkt gleichzeitig im allgemeinen Rauschen. Eine robustere Kodierung und Modulation kann da weiter helfen.

Die Systeme haben daher die Möglichkeit, die Übertragungsrate für jeden einzelnen Frame je nach aktueller Verbindungsqualität neu anzupassen. Der genaue Algorithmus dieser **dynamischen Geschwindigkeitsanpassungen** ist dabei den jeweiligen herstellerspezifischen Implementationen überlassen. Bei den meisten untersuchten Produkten konnte dieser Automatismus im Konfigurationsmenü abgeschaltet und eine Datenrate fest voreingestellt werden.

Von den Herstellern wird gerne eine streng hierarchische Anpassung der Datenraten in mehreren Stufen postuliert, beispielsweise bei 802.11b von 11 Mbit/s in einem inneren Bereich um den Sender über 5,5 Mbit/s und 2 Mbit/s in entfernten Bereichen bis zu 1 Mbit/s im Bereich maximaler Reichweite.

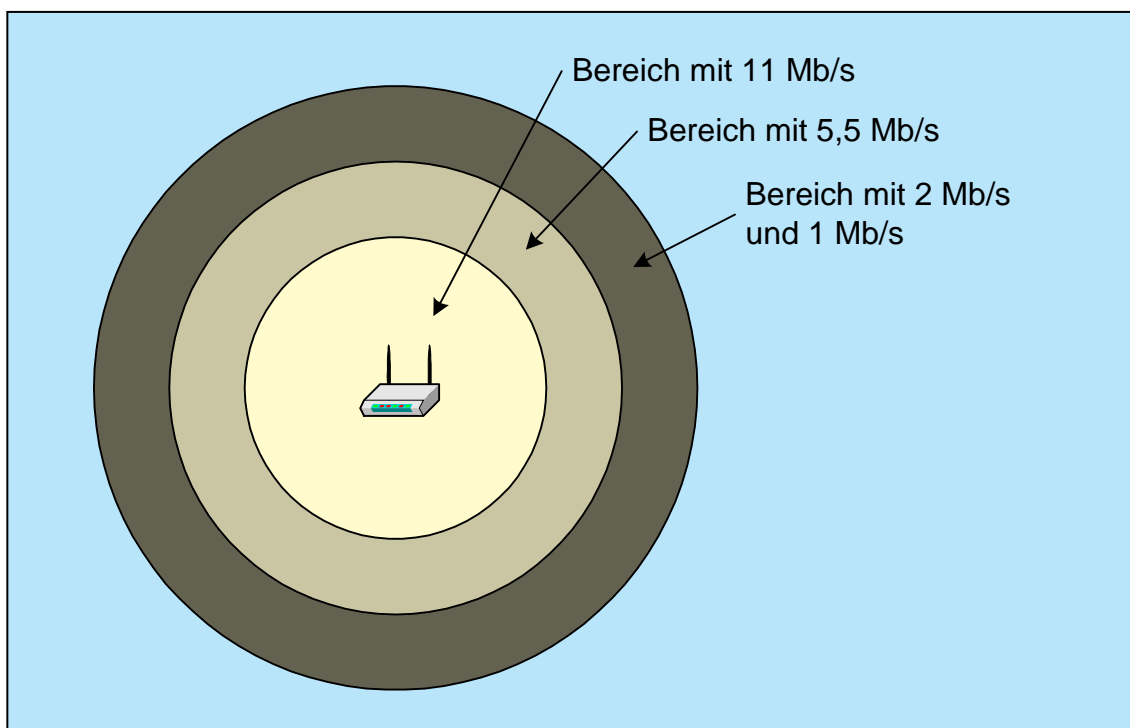


Abbildung 5.22: Prospektdarstellung zur Ratenanpassung

Diese Darstellung konnte in den Praxistests in dieser symmetrischen Form nicht bestätigt werden. Im Gegenteil: gerade mit 11b-Produkten wurde in den meisten Umgebungen auch der maximale Abdeckungsbereich noch mit nominalen Datenraten von 11 Mbit/s versorgt. Hinter diesem Bereich waren dann nach wenigen Metern in der Regel keine stabilen Netzwerkverbindungen mehr möglich (vgl. auch Kapitel 7.4). Allerdings stellt man bei detaillierteren Untersuchungen fest, dass praktisch an jedem Punkt ein bunter Mix aus den verfügbaren Übertragungsraten besteht. Mit wachsender Entfernung verschiebt sich dabei die prozentuale Verteilung der Datenraten hin zu den niedrigeren Raten.

**Statistics** Refresh

**For Rate 1.0Mb/s (basic):**

Received Packets	4	Received Bytes	146
Xmit Packets OK	0	Xmit Bytes OK	0
Max Retry Packets	0	Max Retry Bytes	0
Total RTS Retries	0	Total Data Retries	0
Xmit Life Excd. Pkts.	0	Xmit Life Excd. Bytes	0
Xmit Cancelled Pkts.	0	Xmit Cancelled Bytes	0

**For Rate 2.0Mb/s (basic):**

Received Packets	2	Received Bytes	73
Xmit Packets OK	1	Xmit Bytes OK	54
Max Retry Packets	0	Max Retry Bytes	0
Total RTS Retries	3	Total Data Retries	4
Xmit Life Excd. Pkts.	0	Xmit Life Excd. Bytes	0
Xmit Cancelled Pkts.	0	Xmit Cancelled Bytes	0

**For Rate 5.5Mb/s (basic):**

Received Packets	0	Received Bytes	0
Xmit Packets OK	18	Xmit Bytes OK	14237
Max Retry Packets	1	Max Retry Bytes	26
Total RTS Retries	35	Total Data Retries	26
Xmit Life Excd. Pkts.	0	Xmit Life Excd. Bytes	0
Xmit Cancelled Pkts.	0	Xmit Cancelled Bytes	0

**For Rate 11.0Mb/s (basic):**

Received Packets	51	Received Bytes	6040
Xmit Packets OK	69	Xmit Bytes OK	20053
Max Retry Packets	0	Max Retry Bytes	0
Total RTS Retries	1	Total Data Retries	26
Xmit Life Excd. Pkts.	0	Xmit Life Excd. Bytes	0
Xmit Cancelled Pkts.	3	Xmit Cancelled Bytes	102

Abbildung 5.23: Verteilung der Datenraten

Bei den OFDM-Modulationen scheinen dagegen die hohen Datenraten so empfindlich zu sein, dass tatsächlich bevorzugt beim Durchgang durch Wände deutliche Ratenumschaltungen zu beobachten sind (siehe zum Beispiel Abbildung 7.10 und folgende).

#### 5.4.5.1 Basic Rates

Nun werden in einem WLAN wie im LAN nicht nur Unicasts sondern auch Multicasts und Broadcasts versendet. Da im Infrastructure-Netzwerk jedoch alle Frames von Clients zunächst an den Access Point geschickt werden, ist hier der Access Point die einzige Station, die Multicast und Broadcasts verschickt.

Solange nur Unicasts ausgetauscht werden, passiert dies im Wireless LAN auf der Basis einer Punkt-zu-Punkt-Verbindung. Da sich der Client vor der Aufnahme einer Datenverbindung bei seinem Access Point anmelden muss und im