HANSER

Leseprobe

zu

„Computernetzwerke“

von Rüdiger Schreiner

Print-ISBN: 978-3-446-46005-8
E-Book-ISBN: 978-3-446-46010-2

Weitere Informationen und Bestellungen unter
http://www.hanser-fachbuch.de/978-3-446-46005-8
sowie im Buchhandel

Inhalt

Vorwort

Noch ein Buch über Netzwerke? In jeder Buchhandlung gibt es sie bereits meterweise. Aber dieses Buch unterscheidet sich von den anderen und hat eine besondere Geschichte. Der beste Aspekt daran ist, dass es nicht geplant war. Beruflich arbeite ich sehr viel mit Computerbetreuern zusammen, in allen Schattierungen der Ausbildung und des Wissensstandes, von Hilfsassistenten ohne Computererfahrung bis hin zu professionell ausgebildeten Fachkräften.

Wenn diese Probleme haben, die sie nicht lösen können oder Beratung brauchen, wenden sie sich an mich. Und dies in einer völlig inhomogenen Umgebung, mit Windows, Linux, MacIntosh, Sun, etc. Die Fluktuation ist sehr groß, in großen Teilen der Umgebung muss das Rad ständig neu erfunden werden.

Im Laufe der Jahre fiel mir auf, dass immer wieder dieselben Fragen, immer wieder Verständnisprobleme an denselben Stellen auftreten. Weshalb? Netzwerke sind heute eine unglaublich komplexe Angelegenheit. Aber wie der Computer selbst, finden sie immer mehr Einzug auch in Privathaushalte. Längst ist die Zeit vorbei, in der es zu Hause nur wenige Rechner gab. Längst sind wir so weit, dass viele Haushalte mehrere Computer besitzen und untereinander Daten austauschen und ans Internet wollen. Viele Spiele sind netzwerkfähig geworden, Drucker, Faxgeräte und Scanner werden gemeinsam genutzt. Oft ist es kein Problem, ein paar Rechner zusammenzuhängen und ein kleines Netzwerk zum Laufen zu bekommen. Aber wenn es Probleme gibt, sind die meisten verloren.

Ebenso ist in kleineren und mittleren Unternehmen (oft durch die Aufgabentrennung in grossen Unternehmen ebenso) das IT-Personal meist auf die Betreuung der Rechner und Server ausgerichtet. Das Netzwerk wird meist eingekauft und als Black-Box betrieben. Netzwerke sind oft ein „Buch mit sieben Siegeln“ und eine Infrastruktur, die wie das Telephon behandelt wird. Jeder verlässt sich darauf, aber wenn es nicht funktioniert, ist die Katastrophe da. Oft wird „gebastelt“, bis es irgendwie funktioniert, ohne darüber nachzudenken, dass es noch viel besser sein könnte, performanter und stabiler und nicht nur einfach funktionieren kann.

Im Bereich Netzwerk gibt es eine unheimliche Grauzone des Halbwissens. Ähnliches sieht man bei den Betriebssystemen. CD rein, Setup angeklickt, 15 mal „OK“ gedrückt und der Rechner läuft – solange, bis es Probleme gibt.

Viele sind sehr interessiert am Thema Netzwerk. Der Einstieg aber ist schwer, das Thema ist keine Wochenendsache und meist fehlen die Ansprechpartner. Beklagt wird von den

meisten, dass es auf dem Markt entweder Bücher gibt, die nur sehr oberflächlich sind, oder aber sofort auf einen Level gehen, in dem der Einsteiger verloren ist. Weiter sind sehr viele Bücher zu einem hochspeziellen Thema geschrieben worden und erlauben so nur den Einstieg in kleine Teilbereiche. Oft ist die Sicht der Lehrbücher herstellerbezogen. Linux-Netzwerke, Windows-Netzwerke, meist Nebenkapitel in Büchern über die Betriebssysteme selbst. Oder es sind Bücher von Herstellern der Netzwerkgeräte, die detailliert das Featureset und die Konfiguration beschreiben.

Sicher sind diese Bücher sehr gut – aber nicht für einen Einstieg geeignet. Sie behandeln speziell die Konfigurationen und Möglichkeiten ihrer Geräte und Umgebungen – und nicht der Standards. Auch sind sie nicht für einen Heimanwender geeignet, der mehr verstehen will, und ebenso nicht für eine Firmenleitung oder IT-Abteilung kleiner und mittlerer Umgebungen, die strategisch entscheiden müssen, welchen Weg sie im Bereich Netz gehen wollen.

Dieselbe Erfahrung musste ich selbst machen, als ich erstmalig mit dem Thema Netzwerke konfrontiert wurde. Es gibt viele gute Kurse und Ausbildungen, meist von den Herstellern der Geräte. Eine Privatperson oder kleine Firma kann aber nicht tausende Euro bezahlen, aus einfachem Interesse. Immer wieder erkläre ich dasselbe neu. Und oft hörte ich: „Kannst Du mir nicht ein Buch empfehlen, das wirklich einen Einstieg erlaubt? Das soviel Grundwissen vermittelt, dass man versteht, wie das alles funktioniert, aber auf einer für jedermann verständlichen Basis? Ohne aber nur oberflächlich zu sein? Das ein breites Spektrum des „Wie“ bietet, verstehen lässt und den „Aha-Effekt“ auslöst?“

Ein Bekannter, der gutes Computer-, aber kein Netzwerk-Know-How hatte, bat mich, ihn ins Thema Netzwerke einzuweisen. Wir trafen uns eine Weile regelmäßig und ich überlegte mir, wie ich ihn an das Thema heranbringen kann. Aus diesen Notizen, „Schmierzetteln“ und Zeichnungen stellte ich eine kleine Fibel zusammen. Weiter fand ich Interesse in einem Computer-Verein, baute die Unterlagen aus und hielt den ersten „Netzwerkkurs“. Die Resonanz war enorm. Nie hätte ich gedacht, dass so viele Interesse haben. Vom Schüler, der seine PCs zum Spielen vernetzen will, über den KMU-Besitzer, der Entscheidungsgrundlagen sucht, bis zum IT-Spezialist, der über den Tellerrand schauen wollte, war alles vertreten.

Die Teilnehmer brachten mich auf die Idee, aus den Unterlagen ein Buch zu machen. Dies ist die Geschichte dieses Buches. Das Ziel ist, dem Leser zu ermöglichen, Netzwerke wirklich zu verstehen, egal ob in großen Umgebungen oder zu Hause. Das Ziel ist, soviel Know-How zu erarbeiten, dass der Interessierte versteht, wie es funktioniert und aufbauen kann, und der Einsteiger, der in Richtung Netz gehen will, das Handwerkszeug bekommt, um tiefer einzusteigen und sich an die „dicken Wälzer“ zu wagen. Gezeigt wird, wie es wirklich funktioniert, wie es strukturiert ist und welche großen Stolperfallen es gibt. Genauso soll der Leser in der Terminologie firm werden.

Ein interessierter Einsteiger will nicht 200 Seiten Kommandozeile eines Routers lesen, sondern verstehen, was ein Router wirklich ist. Ist es sein Job oder Interesse, soll er dann nach der Lektüre dieses Buches in der Lage sein, die Erklärungen dieser Kommandozeile sofort zu verstehen. Das Hauptziel dieses Buches sind die Grundlagen und ihr Verständnis. Wer die Grundlagen verstanden hat, dem fügt sich alles wie ein Puzzle zusammen. Leider wird darauf in der Literatur zu wenig eingegangen. Diese Lücke will das Buch schließen. Ein gutes Fundament, Verständnis und „wirklich verstehen“ ist der Leitfaden. Am Ende soll der

Leser qualitativ, aber nicht oberflächlich, alle Informationen und Zusammenhänge kennen, wird arbeitsfähig sein, in der Terminologie firm und bereit für den nächsten Schritt. Die Grundlagen werden mit Absicht ziemlich tief behandelt, denn ein Verstehen der Basis ist immer Voraussetzung für ein fundiertes Wissen. Dies ist in jedem komplexen Thema so. Daher gibt es einige Exkurse in die Physik und Mathematik. Das hört sich abschreckend an, sie sind aber, so hoffe ich, für jeden verständlich gehalten.

Das Buch wurde bewusst als ein Buch zum Lesen geschrieben. Trockene Theorie, die manchen bekannt ist, manchen nicht, habe ich als Exkurse an das Ende des Buches ausgelagert, um den Fluss nicht zu stören. Wer diese Grundlagen nicht hat, ist gebeten, sich die Mühe zu machen, diese Exkurse zur richtigen Zeit zu lesen; es wird im Text jeweils darauf verwiesen. Ich rate dazu, das Buch nicht einfach wie einen Roman zu lesen, sondern sehr bewusst und kapitelweise. Es stecken viele Informationen in sehr kompakter Form darin. Man ist leicht versucht, es in einem Zug zu lesen, doch wird dabei eine Menge untergehen. Ein Repetitorium und Fallbeispiele geben am Ende die Möglichkeit, mit dem Erlernten umzugehen.

Zum Schluss möchte ich nicht versäumen, einigen Personen zu danken, die einen großen Anteil am Entstehen der Unterlagen beziehungsweise des Buches hatten: Herrn Prof. Dr. F. Rösel für die Chancen und die Möglichkeit der Weiterbildungen; Herrn Dr. H. Schwedes für die Korrekturlesung und die wertvollen Anregungen; der Linux Usergroup Lörrach e. V. für das tolle Feedback; Herrn H. Volz für die akribische fachliche Korrekturlesung und seine Anmerkungen; Herrn Dr. P. Zimak für die stets offene Türe und die vielen beantworteten Fragen in den letzten Jahren; und nicht zuletzt ganz besonders meiner Familie für die gestohlene Zeit.

Das Buch ist aus den Erfahrungen in Jahren der Praxis entstanden – es ist ein Buch der Praxis und ein dynamisches Buch, das aus ständigem Feedback gewachsen ist. In diesem Sinne wünsche ich Ihnen möglichst großen Gewinn und viel Spaß bei seiner Lektüre. Eines haben mir die bislang abgehaltenen Netzwerkkurse und Diskussionen gezeigt: Ein so trockenes Thema wie Netzwerke kann auch Spaß machen! Interessant ist es allemal.

Lörrach, im Oktober 2005
Rüdiger Schreiner

Vorwort zur siebten Auflage

Eben habe ich das Vorwort gelesen, das ich zur ersten Auflage geschrieben habe. Danach das Vorwort zur sechsten Auflage. Als ich die erste Auflage veröffentlicht habe, ist mein Sohn kurz vor der Einschulung gewesen, letztes Jahr hat er Abitur gemacht und dieses Jahr beginnt er zu studieren. Das hat nichts mit Computernetzwerken zu tun, aber es macht mir immer wieder klar, wieviel Zeit seit der ersten Auflage des Buches vergangen ist. Im Vorwort zur sechsten Auflage schrieb ich, dass ich es fast ein wenig unheimlich finde, wie sich dieses Buch auf dem Markt hält. Eigentlich haben Sach- und Fachbücher in einer schnell-

lebigen Umgebung wie der IT eine kurze Lebensdauer. Dieses Buch hingegen verkauft sich seit 14 Jahren stetig, die Rezensionen sind sehr gut und das Feedback, das ich bekomme, ausgezeichnet. Ein häufiges Feedback meiner Leser ist, dass das Buch eine Lücke schließt. Es füllt die Lücke zwischen den sehr guten und detaillierten Fach-„Wälzern“, die Einsteiger überfordern und den zu oberflächlichen Nebenkapiteln zum Thema Netzwerke in IT-Lehrbüchern. Das didaktische Konzept, Grundlagen zu erarbeiten und bis zur Anwendung zu beschreiben, mit der direkten Verbindung zur Praxis, wird sehr gut bewertet.

Das Buch ist speziell für Einsteiger in dieses Thema konzipiert und bringt sie auf ein fundiertes und arbeitsfähiges Level. Es bietet die Chance, anzufangen und die Grundlagen kennen zu lernen und zu verstehen, aber es berücksichtigt auch die Anforderungen im Berufsalltag. Es freut mich sehr, dass das Buch breit in der Lehre eingesetzt wird. Noch mehr freut mich, dass ich – auch nach 14 Jahren – immer noch Feedback von eben diesen Lehrenden und meinen Lesern bekomme, mit dem Wunsch, das Buch weiter zu pflegen.

Ich habe das Buch nie grundlegend verändert, aber stetig erweitert. Ich bleibe beim Konzept: von den Grundlagen zur Funktion und Anwendung. Das Verständnis der Grundlagen ist die Basis für den Einstieg und die Weiterentwicklung des Themas. Wer die Grundlagen nicht verstanden hat, dem wird es schwerer fallen fortgeschrittene Probleme zu lösen. Ich kann dies häufig in meinem Arbeitsumfeld beobachten. So scheitert z. B. ein anspruchsvolles Debugging, wenn die grundlegenden Zusammenhänge nicht klar sind.

Ich habe das Buch zur siebten Auflage geringfügig erweitert und es modernisiert. 2005 habe ich manchmal von „im Test“ geschrieben, oder „wird bald kommen“. Vieles davon ist heute Wirklichkeit geworden. Ich habe auch kleine Fehler korrigiert, die mir von aufmerksamen Lesern gemeldet wurden. Dafür an diese vielen Dank!

Ich bedanke mich bei meinem Kollegen H. Volz für die Korrekturlesung der neuen Seiten. Und Ihnen, liebe Leser, danke ich für Ihr andauerndes Interesse.

Und zum siebten Mal wünsche ich Ihnen viel Kurzweil und Gewinn bei der Lektüre.

Schopfheim, im März 2019

Rüdiger Schreiner

8 Wireless LAN, Funknetze, Voice

Der Netzwerkanschluss ohne „Kabelsalat“ und physikalische Konzentratoren setzt sich explosionsartig durch. Während noch vor ein paar Jahren die Zahl der Computer viel geringer war und auch nur wenige Haushalte Computer besaßen, ist der Computer heute ein normales Gerät geworden.

Immer mehr setzt es sich durch, dass mehrere Computer pro Haushalt vorhanden sind und alle einen Internetanschluss wünschen. Somit hat das Thema Netzwerk auf einmal Einzug in die Privathaushalte gehalten.

Da die meisten keine strukturierte Netzwerkverkabelung zu Hause haben und auch nicht verlegen lassen möchten, ist das Funknetzwerk eine günstige und einfache Alternative. Inzwischen setzt sich immer mehr durch, öffentliche Gebäude, Bahnhöfe, Schulen, Universitäten etc. mit sogenannten Hotspots (öffentlich zugängliche Funknetzzugänge) auszurüsten, um jedermann, der mit dem Laptop oder Smartphone unterwegs ist, die Möglichkeit zu verschaffen, sich mit dem Internet zu verbinden.

Ein riesiger Nachteil ist die Sicherheit. Hier sorgt fehlendes Know-how der Heimanwender für große Risiken. Meist ist der durchschnittliche Heimanwender kein Computerexperte. Wenige bedenken, dass ein Netzwerk eine Kommunikation in beiden Richtungen erlaubt. Wer sein Funknetz völlig ungeschützt betreibt, riskiert, dass sich jeder auf der Straße vor dem Haus einklinken kann und Vollzugriff auf sämtliche Netzwerkressourcen hat. Sehr viele Rechner zu Hause sind in der Regel nicht einmal durch ein Passwort geschützt, ebenso die Access-Router, Netzwerkdrucker etc.

Im gewerblichen Umfeld, bei Praxen, Kanzleien, Firmen etc., kann dies sogar erhebliche juristische Konsequenzen haben. Hier muss auf jeden Fall vermieden werden, dass zum Beispiel Kunden- oder Patientendaten auf einmal offen für die Welt liegen.

Das sogenannte War-Driving („kriegsmäßiges Herumfahren“) ist weit verbreitet. Hier fahren Hacker mit einem Laptop auf den Knien herum und suchen offene Funknetze, die sie benutzen, um ihr illegales Hobby über den Anschluss anderer auszuüben. Sie sind dabei in der Regel sicher. Es wird selten gelingen, sie zu erwischen.

Meist ist dies mit dem sogenannten War-Chalking („kriegsmäßiges Kreidezeichnen“) verbunden. Diese Hacker benutzen die gefundenen, offenen Anschlüsse nicht nur für sich selbst, sondern hinterlassen Kreidezeichnungen, die anderen Hackern Hinweise über Verschlüsselungen, Zugang etc. geben, um ihren Kollegen den Zugang zu erleichtern.

In den Wohngebieten mancher Großstädte hat man in Testmessungen bereits Stadtviertel gefunden, die eine bis zu 25% ungeschützte Netzabdeckung geboten haben. Daher sollte man seinen Internetanschluss, sofern man ihn über ein Funknetz in der gesamten Wohnung/Haus propagiert, auf jeden Fall vor unbefugter Nutzung schützen. In der Regel lesen wir in der Presse von Viren und Trojanern und Schadsoftware, sogenannter Malware, die große Schäden anrichten. Dies ist aber nur die Spitze des Eisberges und nur ein kleiner Teil der negativen Seiten der Netzwerke.

HINWEIS: Ein Hacker möchte in der Regel nichts kaputt machen, sondern unerkannt bleiben und fremde Ressourcen nutzen.

Sei es, dass er (oder immer im Hintergrund natürlich auch sie) die Prozessorleistung nutzen will, die er nicht hat, oder aber einfach Speicherplatz. Illegale Daten lagern sich am besten dort, wo sie nicht verfolgbar sind. Sind illegale Daten, Spionage, Pornografie etc. aufzubewahren, dann am besten dort, wo nicht verfolgt werden kann, wer sie dort gelagert hat. Der Besitzer des Rechners ist dann erheblich gefordert zu beweisen, dass er nicht der ist, der sie besorgt und gespeichert hat. Im Internet existieren ganze Verzeichnisse, wo wer ungeschützt ist, und viele Illegale tauschen sich, völlig unbemerkt von den Besitzern der Ressourcen, dort aus. Oben haben wir erfahren, dass PAT und Firewalls uns davor schützen, dass von außen zugegriffen wird. Dies kann ausgehebelt werden. Das Problem sind vor allem Trojaner und Backdoor-Programme, die mit E-Mail und vielen anderen Mechanismen verteilt werden. Sie werden im Hintergrund unbemerkt installiert und öffnen eine Verbindung von innen nach außen, auf die sich die Autoren dieser Programme aufsatteln. Damit ist jede Firewall und jedes PAT umgehbar. Erhebliche Pools von solchen meist unbemerkten Schadprogrammen sind Shareware und Peer-to-Peer-Applikationen zum Austausch von Software, Filmen und Musik.

Das hier Gesagte gilt natürlich für alle Netzwerkzugänge. Mit Wireless wird aber in der Regel sehr unachtsam umgegangen, daher sei es hier erwähnt. Zum Glück haben auch die Provider reagiert. Funkrouter werden heute standardmäßig mit eingeschalteter Verschlüsselung ausgeliefert.

Der Datenaustausch über Funk ist längst ein Klassiker. Die Telefonie ist hier schon seit Langem etabliert. Fast jeder hat ein Handy, zu Hause wird schon lange schnurlos telefoniert. Die Verfahren sind unterschiedlich, aber sie wachsen zusammen. Bald wird es keinen Unterschied mehr geben. Schon jetzt gibt es Handys, die sich des Handynetzes bedienen, wenn man unterwegs ist, sich aber zu Hause in die Feststation einbuchen, sobald sie erreichbar ist. Sprich, ab dann wird über das Festnetz telefoniert.

Immer mehr wird Voice over IP ein Thema und damit das Internet/Intranet immer mehr zum Transportmedium für Sprache. Der Dienst löst sich vom Draht. Das Handy als Zugangsmedium zum Internet ist ebenfalls etabliert. E-Mail, Browsing, Modemfunktion etc. sind heute etabliert. Daher werde ich Voice over IP hier in diesem Kapitel mit behandeln, die Verschmelzung ist im Gange und bereits nahe Zukunft.

8.1 Access-Points und Antennen, Anschlüsse

Wie bei jedem Dienst über Funk muss es einen Sender und einen Empfänger geben. Wie beim Funktelefon auch, geht die Datenübertragung in beide Richtungen. Das heißt, der Funknetzwerkadapter des PC oder Notebooks ist genauso Sender und Empfänger wie der „Sender“, der sogenannte Access-Point, das Gerät, das die Verbindung zum physikalischen Netzwerk herstellt.

Es gibt auf dem Markt die verschiedensten Antennentypen mit den verschiedensten Abstrahlungscharakteristiken. Welche geeignet sind, muss aus der Topologie der Umgebung mit Sachverstand entschieden werden.

So gibt es beispielsweise Richtantennen, die in einer definierten Richtung strahlen, weiter Antennen mit kugelförmiger Abstrahlung und solche mit birnenförmiger Charakteristik.

Für ein normales WLAN zu Hause reicht meist die mitgelieferte Standardantenne. Wird professionell verfunkt, müssen die Räume funktechnisch vermessen werden, um später Zonen zu vermeiden, die ohne Empfang sind. Clientseitig gibt es viele Lösungen, es gibt PCI-Netzwerkadapter, USB-Adapter, PCMCIA-Karten und Mini-PCI-Adapter. In den meisten Notebooks und Smartphones ist heute WLAN fest eingebaut.

8.2 Störungen

Störmöglichkeiten gibt es viele. Wir können hier nur die wichtigsten Effekte betrachten. Meist handelt es sich um Störstrahlungen oder Hindernisse, wenn ein Funknetz nicht funktioniert.

Sind andere Funknetze derselben Frequenz in der Nähe, stören sich ihre Signale gegenseitig. Dies ist durch Wahl einer anderen Frequenz zu beheben (siehe unten).

Neben der Signaldämpfung durch die Entfernung haben Hindernisse natürlich einen Störeffekt. Ein Funknetzwerk verläuft nur bei Sichtverbindung perfekt. Hierbei ist auch das Material entscheidend. Betonwände mit ihrer Stahlmatteneinlage wirken wie ein Faradaykäfig. Dies sieht man deutlich, wenn Handys in Betongebäuden oft kein Netz finden. Daher ist die vertikale Anbindung über Stockwerke meist kritischer als horizontal über mehrere Räume hinweg, da in den Decken meist mehr Metall verarbeitet ist als in den Wänden. Ebenso können thermisch isolierende Fenster Funkkiller sein, sie sind oft mit einer unsichtbaren Metallschicht bedampft.

Die Störungsquellen im Funkbereich sind immens, ein Effekt, der immer mehr zunimmt. Nicht nur andere Funknetze, auch Wetterphänomene, elektrische Schaltungen, Entladungen aller Art, Mikrowellenherde, Leuchtstoffröhren, Bluetooth und vieles mehr können ein Funksignal stören.

8.2.1 Interferenzen, Multipath-Effekt

An Hindernissen, Wänden, Decken und Böden kann es nicht nur zu einer Dämpfung des Signals kommen, sondern auch zu Reflexionen und dadurch zu Interferenzen. Es kann passieren, dass in einem Raum ein Funk-Interferenzmuster entsteht, das dafür sorgt, dass im Zentimeterbereich Zonen entstehen, die guten Empfang haben, abgewechselt mit Zonen ganz ohne Empfang. Hier kann ein kleines Ausrichten des Empfängers oder der Antennen des Access-Points oft große Qualitätsunterschiede im Empfang bewirken. Sind sehr viele Hindernisse zu überwinden, muss vermessen oder probiert werden, wo der günstigste Ort für den Access-Point ist und wie die Antennen auszurichten sind. Durch Reflexionen sieht eine Empfänger-Antenne dasselbe Signal mehrfach, wie ein Echo, zeitverzögert. Dies nennt man den Multipath-Effekt. Die primären und die reflektierten Signale stören sich.

Abhilfe schafft hier, die Reflexionsbedingungen zu ändern, was nicht leicht ist, da dies Decken-, Boden- und Wandbeläge, also bauliche Gegebenheiten, betrifft.

Weiter kann man, wenn die Entfernungen kurz sind und ein Signal guter Qualität vorliegt, die Sendeleistung des Access-Points drosseln. An nahezu allen Geräten ist dies möglich. Dadurch werden die Reichweite der Reflexionen und die Häufigkeit der Echos zurückgedrängt.

Eine dritte Möglichkeit ist der Einsatz von Access-Points mit sogenannter Antennen-Diversity. Dies ist ein Verfahren, bei dem der Access-Point mit zwei Antennen arbeitet und die Signalqualität pro verbundenem Client misst. Er sendet dann nur über die Antenne, welche die bessere Verbindung hat. Sind die Antennen leicht gerichtet, können so Multi-Path-Effekte vermindert werden, da die meisten Reflexionen in der Regel aus verschiedenen Richtungen kommen.

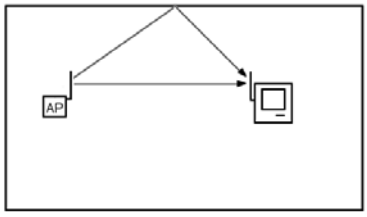

BILD 8.1 Der Multi-Path-Effekt. Eine ungerichtete Antenne strahlt in alle Richtungen aus. Wird ein Signal zum Beispiel an einer Wand reflektiert, erreicht es den Empfänger mehrfach. Der zurückgelegte Weg und damit die Laufzeit unterscheiden sich. Die Signale stören sich. Ein Interferenzmuster entsteht. Ist die Phasenverschiebung so groß, dass sich die Signale auslöschen, empfängt der Empfänger nichts mehr.

8.2.2 Hidden-Node-Problem

WLAN funktioniert als Shared Medium, ähnlich dem Verkehr über Thin-Wire. WLAN ist immer halbduplex. Eine Antenne kann nur senden oder empfangen.

Das Zugriffsverfahren ist hier CSMA/CA (siehe oben). Der Client „horcht“ also vor der Sendung, ob die Frequenz frei ist. Stehen zwei Clients nun so weit auseinander, dass sie zwar den Access-Point erreichen, sich aber gegenseitig nicht empfangen können, senden sie, und

Kollisionen treten ein. Hier kann nur eines helfen: Der Access-Point selbst muss als Vermittler über das Verfahren RTS/CTS (Ready to Send/Clear to Send, siehe oben) oder andere die Sendungen der Clients koordinieren. Er muss auf Anfrage publizieren, ob das Medium zur Verfügung steht oder nicht.

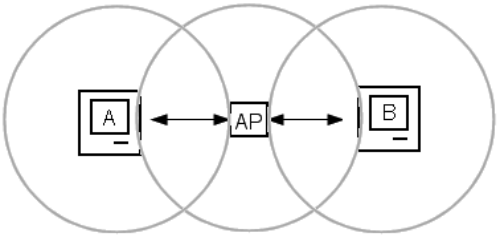

BILD 8.2 Das Hidden-Node-Problem. Jeder Sender hat eine definierte Reichweite (graue Bereiche). Beide Rechner, A und B, können den Access-Point erreichen, sie „sehen" einander aber nicht. Daher können sie auch nicht wissen, wann der andere sendet. Hier muss der Access-Point vermitteln.

8.2.3 Generelles

Die Möglichkeiten der Störungen sind vielfältig. Als Regel gilt, zu Hause und im Privatbereich reicht es, die Mittel zu benutzen, die mit den Access-Points und Adaptern geliefert werden. Fast alle haben Monitore (meist Software) zur Messung der Signalqualität, die mehr oder weniger genau sind.

Wird aber professionell im gewerblichen Bereich verfunkt, muss vorher funktechnisch ausgemessen werden, insbesondere auch nach baulichen Veränderungen im Nachhinein. Hier müssen professionelle Messmethoden eingesetzt werden, da die Störungen oft sehr schwer zu identifizieren sind.

Besonders gilt dies, wenn Roaming (die Übergabe eines Clients von einem Access-Point zum anderen beim örtlichen Wechsel des Clients) eingesetzt werden soll. Hier dürfen sich die Funkbereiche der Access-Points nicht zu dicht überlappen.

Ebenso muss genau vermessen werden, wenn eine häufige Überlappung von Funkzellen zu erwarten ist, die verschiedenen Netzen angehören. Die Anzahl der möglichen Frequenzen ist gering, und sie müssen sinnvoll so abgewechselt werden, dass keine Störungen auftreten. Hier muss ein sogenannter Flächenwabenplan in der Planung erstellt werden.

8.3 Die Funkzelle und die Kanäle

Jeder Access-Point hat eine gewisse Reichweite. Den Raum um den Access-Point, in dem mit ihm verbunden werden kann, sprich die Reichweite seines Senders, nennt man seine Funkzelle. Werden mehrere verschiedene Funknetze auf engem Raum betrieben, zum Beispiel in Mehrfamilienhäusern, können sich die Funkzellen überschneiden, und es kann durch diese Störungen zu einer drastischen Reduktion der Verbindungsgeschwindigkeit kommen. Für

diese Fälle kann man die Access-Points auf verschiedene, festgelegte Funkkanäle (Frequenzen) einstellen. Alle Teilnehmer eines Funknetzes müssen denselben Kanal benutzen.

Sollten mehrere Kanäle in der Umgebung unbelegt sein, ist es das Beste, den weitest entfernten zu benutzen, um die Störeinflüsse zu minimieren.

Die Access-Points und Empfänger schalten sich bei niederem Signalpegel automatisch in der Geschwindigkeit zurück, bevor der Empfang zum Erliegen kommt. Daher ist es kein Hardware- oder Konfigurationsfehler, wenn die Geschwindigkeit, die angezeigt wird, nicht die maximal mögliche des Access-Points ist. Hier muss gleichzeitig auf die Qualität der Verbindung geachtet werden.

8.4 Betriebsmodi

Funknetze lassen sich in zwei verschiedenen Modi betreiben: einerseits im Ad-hoc-, andererseits im Infrastrukturmodus.

Im Ad-hoc-Modus ist das Funknetz ein Peer-to-Peer-Verbund von Wireless-Adaptern. Einen Access-Point gibt es nicht. Alle sind gleichberechtigt. Dies ist zum Beispiel eine schnelle Methode, um Notebooks kurzerhand zu verbinden, um schnell und einfach Daten auszutauschen, Konferenzen abzuhalten oder PDAs zu synchronisieren. Das Ad-hoc-Netz ist in der Regel isoliert, sprich nicht mit anderen Netzen verbunden.

Im Infrastrukturmodus wird über Access-Points kommuniziert. Der Access-Point ist in der Regel die Verbindung zum physikalischen Netzwerk, daher wird ein Internet-Zugang über WLAN in der Regel immer im Infrastrukturmodus sein. Im Infrastrukturmodus kommunizieren alle mit und über den Access-Point. Im Standard 802.11a (Standards s. u.) gibt es nur den Infrastrukturmodus, bei 802.11 b und g beide. Die Access-Points stellen hier die zentralen Verteiler dar.

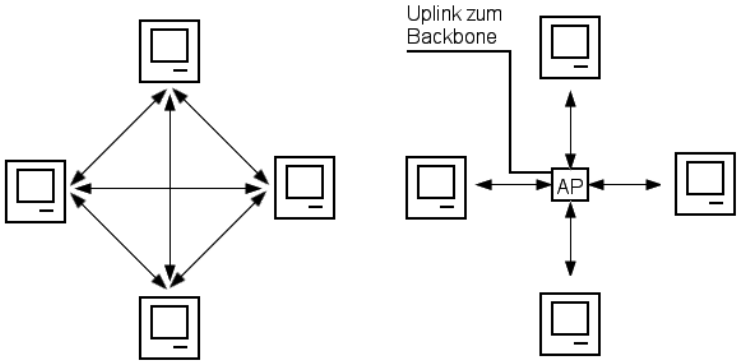

BILD 8.3 Im Ad-hoc-Modus (links) gibt es keinen Access-Point. Alle Funknetzadapter sind gleichberechtigt, und jeder kommuniziert mit jedem (Bild links). Im Infrastruktur-Modus verläuft die gesamte Kommunikation über den (oder mehrere) Access-Points (Bild rechts). Während Netze im Ad-hoc-Modus isoliert sind, kann im Infrastrukturmodus durch einen Uplink vom Access-Point aus die Verbindung zu einem kabelgebundenen Netzwerk hergestellt werden.

8.5 Namen, das Beacon

Jedes Funknetz hat einen Namen, die sogenannte SSID (Service Set IDentifier), der es identifiziert.

Jeder Access-Point sendet in der Regel von sich aus in regelmäßigen Abständen ein kleines Datenpaket aus, das die Parameter des Netzes wie die SSID, den Verschlüsselungsmodus etc. enthält. Dieses Paket nennt man Beacon. Damit kann jeder, der eine Funknetzwerkkarte hat, das WLAN „sehen“.

Will man sein Netz besser absichern, kann man die Aussendung der SSID unterdrücken (SSID-Broadcast abschalten). Nun sieht man die Kennung nicht mehr und muss den Namen explizit kennen, um sich verbinden zu können. Das ist aber ein schwacher Schutz, auf den Sie sich nicht verlassen sollten.

8.6 Verschlüsselung

Als Verschlüsselung wird standardmäßig im WLAN-Bereich WEP (Wired Equivalent Privacy) angeboten. Dies ist ein symmetrisches Verschlüsselungsverfahren. Es wird mit Schlüsseln von 64 oder 128 Bit gearbeitet. Dieses Verfahren gilt heute als nicht mehr sicher. Selbst der 128-Bit-Schlüssel lässt sich mit einem schnellen Rechner in kürzester Zeit berechnen, wenn der Datenverkehr mitgelesen werden kann – bei WLAN ist dies fast nie sicher zu verhindern.

Um die Sicherheit zu erhöhen, hat die Wi-Fi-Alliance (siehe unten) ein neues Verfahren entwickelt, das WPA-Verfahren (Wi-Fi Protected Access). Es funktioniert genauso wie WEP, ändert aber regelmäßig automatisch die Schlüssel im Hintergrund und erschwert damit die Berechnung bis zur Unmöglichkeit.

Hierbei wird das TKIP-Protokoll (Temporary Key Integrity Protocol) verwendet, das die Schlüssel verwaltet. Die Alterung eines Schlüssels kann nach der übertragenen Datenmenge oder der Zeit eingestellt werden.

Wenn möglich, sollte WPA2 eingesetzt werden und nicht das unsichere WEP. Wer es absolut sicher will, verzichtet auf beide und verbindet den Client mit dem Access-Point über VPN.

Dies ist besonders im Firmenumfeld zu empfehlen. Hierbei kann der Access-Point selbst der Terminator für den VPN-Tunnel sein. Einige Geräte bieten diese Funktion an. Ansonsten kann der Tunnel irgendwo im Backbone an einem Router oder VPN-Server enden.

8.7 Aufbau eines Infrastruktur-WLAN

Im Infrastrukturmodus verläuft die Kommunikation über den Access-Point. Dieser stellt die Verbindung zum physikalischen Netz dar. Es gibt auf dem Markt eine derartige Fülle von Geräten unterschiedlichster Implementierungen und Bauarten, dass hier keine Standardbeschreibung abgegeben werden kann. Sie alle zu diskutieren ist nicht möglich.

Die Access-Points können in allen möglichen Bauarten gekauft werden. Sie gibt es mit Funktionen von der reinen Bridge ins Netzwerk bis hin zum vollwertigen Router oder einer Firewall. Manche lassen sich je nach ihrer Funktion konfigurieren.

Während im Heimumfeld meist der Wireless-Router, mit integriertem Switch für den Anschluss von Ethernet-Kabeln für Desktop-PCs, manchmal sogar mit DSL-Modem zum Kombi-Gerät integriert, vorherrscht, wird im gewerblichen Umfeld bei der Verfunkung mehr die Variation als transparente Bridge als Access-Point eingesetzt. Hier übernimmt der Access-Point fast nur noch eine Antennenfunktion ohne eigene Intelligenz. Services wie das Roaming (Weiterreichen eines Clients von Access-Point zu Access-Point bei Bewegung), Routing, Switching, VLANs, Access-Control und DHCP-Services werden im Hintergrund von zentralen, leistungsfähigen Geräten übernommen. Die Umgebung wird dadurch auch wesentlich leichter zentral zu managen, da die Konfigurationen nicht an vielen Acess-Points verteilt vorgenommen werden müssen, sondern lediglich einmal an den zentralen Geräten. Ebenso können die Zugangsberechtigung, Verschlüsselungen und vieles andere mehr zentral eingerichtet und terminiert werden.

In der Regel übernehmen dies Appliances, sogenannte Wireless-LAN-Controller. Wer viele Sender in verschiedenen Gebäuden betreibt, wird ohne sie nicht auskommen, die Funkumgebung ist sonst nicht mehr zu managen. Die modernen Appliances regeln auch automatisch die Funkkanäle, die Sendestärke etc. Sie wechseln automatisch die Frequenzen, wenn Störungen auftauchen. In der Regel sind diese Lösungen proprietär. Das heißt, man muss sich auf einen Hersteller festlegen. Die Vorteile sind in großen Umgebungen aber immens. Wer möchte ein Software-Update an 200 Geräten in acht Gebäuden Stück für Stück durchführen?

Inwieweit diese Trennung oder Integration der Services und Geräte infrage kommt, muss von Fall zu Fall entschieden werden. Ein solches Funksystem ist in das Security-Konzept einer Firma zu integrieren.

Zu Hause sollte man dafür sorgen, dass die eigene Umgebung geschützt ist, aber so einfach strukturiert als möglich bleibt. Hier ist dafür zu sorgen, dass die eigenen Daten nicht zugänglich sind, keine illegalen Daten heimlich „gelagert“ werden können, zum Beispiel durch geeignete Passwörter und Verschlüsselung. Ebenso sollte kein Missbrauch mit dem Internet-Anschluss ermöglicht werden.

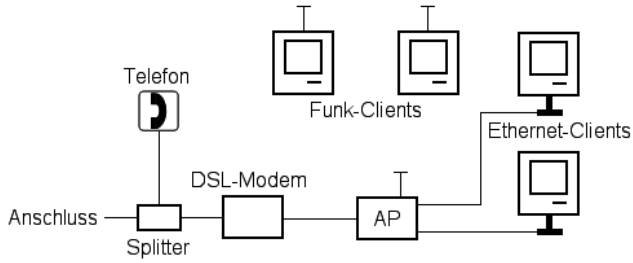

BILD 8.4 Der mögliche Aufbau eines Netzwerkes zu Hause oder in kleinen Umgebungen. Am Telefonanschluss werden per Splitter das DSL- und das Telefonsignal getrennt. Das DSL-Modem decodiert das Signal und stellt Ethernet zur Verfügung. Der Access-Point (AP) ist hier ein integriertes Kombi-Gerät. Er ist NAT-Router, Firewall und DHCP-Server in einem Gerät, hat mehrere geswitchte Ports für PCs, die über Kabel angeschlossen werden, und ist gleichzeitig Wireless-Access-Point. Alle Netzwerkfunktionen sind hier in einem einzigen Kombi-Gerät zusammengefasst.

Es ist zwar „nett“, anderen seinen Internetzugang frei zur Verfügung zu stellen. Die juristischen Konsequenzen aber sollten mit bedacht werden. Wenn von einer IP-Adresse aus juristisch relevante Vorgänge oder sogar Straftaten verübt werden, ist der Besitzer der Adresse im Erklärungszwang. Die Transaktionen im Internet werden von den Providern geloggt. Bei einem Vergehen kann der Provider sagen, wer wann welche Adresse hatte, aber es ist in der Regel durch PAT etc. nicht möglich, das Endgerät genau zu identifizieren. Die Vorsicht im privaten Umfeld muss nicht übertrieben werden, der mögliche Schaden sollte aber ebenfalls nicht unterschätzt werden.

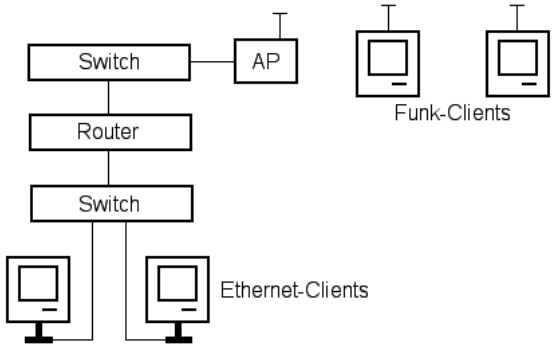

BILD 8.5 Der mögliche Aufbau einer größeren, professionellen Umgebung. Die Access-Points (AP) sind hier einfache Bridges ohne große Funktionalität und Intelligenz. Die Services wie DHCP, Firewall, Routing, Switching etc. werden von den sehr viel leistungsfähigeren Core-Switches und Routern übernommen. Aus Sicherheitsgründen werden die Funk-Clients in einem gesonderten Subnetz geführt, nicht zusammen mit den fest angeschlossenen Rechnern. Somit kann auf dem Router (oder einer Firewall) gezielt für Security gesorgt werden. Für die Funk-Clients können so leicht höhere Sicherheitskriterien angewandt werden. In gewerblichen Umgebungen sollte auf jeden Fall VPN eingesetzt werden. Der Router stellt die Verbindung zum Backbone oder Internet her (nicht eingezeichnet). In großen Umgebungen regelt ein weiteres Gerät, der WLAN-Controller, die Access-Points.

8.8 Stromversorgung der Sender

Ein Access-Point braucht, selbstverständlich, eine Stromversorgung. Theoretisch muss also ein Stromkabel mit dem Netzwerkkabel, das den Access-Point erschließt, verlegt werden. Um dies zu vermeiden, gibt es Power over Ethernet, auch Power-Injection genannt. Hier wird die Versorgungsspannung über das Ethernet-Kabel in den Access-Point geführt.

Power-Injection gibt es in verschiedenen Varianten. Einmal wird ein Koppler zwischengeschaltet (Power-Injector), der Strom bezieht und einspeist, im anderen Fall liefert bereits der Switch, an dem gepatcht wird, von sich aus den Strom über die Anschlussports (PoE, Power over Ethernet). PoE wird auch angewandt, um IP-Telefone mit Strom zu versorgen.

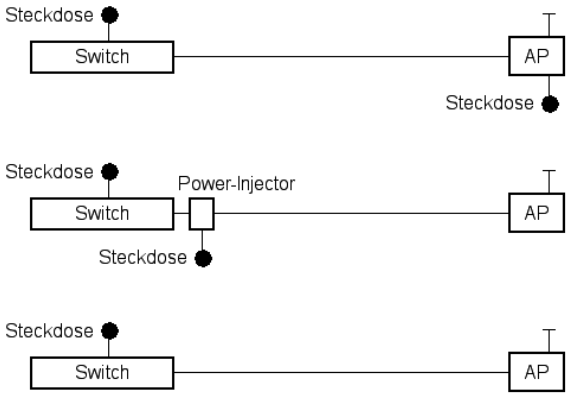

BILD 8.6 Es gibt mehrere Möglichkeiten, einen Access-Point (AP) mit Strom zu versorgen. Herkömmlich muss eine Stromversorgung bis an den AP geführt werden, er steckt schlichtweg in der Steckdose (oben). Mit dem Verfahren Power over Ethernet wird der Strom über das Netzwerkkabel geleitet. Dies kann einmal dadurch geschehen, dass man einen Power-Injector dazwischen patcht, der Strom aus der Steckdose bezieht und ins Netzwerkkabel einspeist (Mitte), oder der Switch, an dem der AP angeschlossen ist, speist den Strom direkt aus seiner eigenen Stromversorgung ein.

Bei PoE ist noch Vorsicht geboten. Bei den ersten Implementationen wurde der Strom für die Sender über die ungenutzten Adern des Netzwerkkabels geleitet. Wir erinnern uns, bei Fast Ethernet benötigten wir vier Adern, ein Netzwerkkabel hat acht. Dies war aber nicht immer möglich. Um Geld zu sparen, hat man früher oft zwei Netzwerkdosen mit einem Kabel erschlossen, mit Doppeldosen. Hier sind alle acht Adern in Nutzung. Mit der Entwicklung des N-Standards mussten sich die Hersteller jedoch etwas einfallen lassen. Ein Access-Point nach N-Standard bietet eine Brutto-Datenrate von bis zu 600 MBit/s. Daher müssen diese Access-Points mit Gigabit-Ethernet erschlossen werden. Hier sind sowieso alle acht Adern im Betrieb. Dies wurde gelöst, Strom und Signal werden in die Kabel eingekoppelt und am Ziel wieder elektronisch abgekoppelt. Diese Verfahren funktionieren auch über Doppeldosen. In der Übergangsphase aber sollte man sicherstellen, welchen Standard eine Stromquelle liefert, um Schäden zu vermeiden. PoE arbeitet mit 48 Volt, hier riskiert man eventuell große Schäden, wenn man alte und neue Standards mischt.

8.9 Mesh

Eine Besonderheit bei der Verfunkung ist das Meshing. Dies wird vor allem im Freien eingesetzt. Hier wird nicht jeder Access-Point an das kabelgebundene Netz angeschlossen, sondern nur einer oder einige. Die anderen werden per Funk angeschlossen. Praktisch ist dies zum Beispiel auf großen Plätzen, es müssen keine Netzwerkkabel verlegt werden. Die Stromversorgung der Access-Points kann zum Beispiel über Straßenlaternen erfolgen, damit müssen gar keine Kabel verlegt werden. In der Regel wird ein Funkbackbone in 802.11a (siehe unten) zwischen den Access-Points aufgebaut und per 802.11g (siehe unten) mit den Endgeräten kommuniziert.

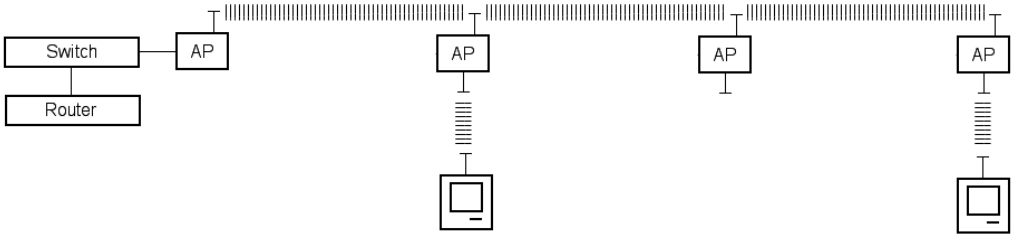

BILD 8.7 Ein Mesh-Verbund. Ein AP ist an das Netzwerk per Kabel angeschlossen. Über Funk sind die anderen erschlossen. In der Regel wird der Mesh mit 802.11a (siehe unten) als Backbone aufgebaut. Die Kommunikation mit den Endgeräten verläuft über 802.11g (siehe unten).

8.10 Wi-Fi und Proprietäres

Viele Hersteller waren mit dem Standard nicht zufrieden und wollten höhere Übertragungsraten und Extrafunktionen. Dies ist mit proprietären Methoden wie einer Kanalbündelung oder mit Kompressionsverfahren möglich. Wie bei allem hat dies neben den Vorteilen aber auch Nachteile. Es können bei proprietären Verfahren nur Access-Points und Adapter dieser Firmen und Verfahren miteinander eingesetzt werden. Eine Kompatibilität gibt es hier nicht. Meist wird angeboten, dass sich die Adapter bei einem Fehlen der erweiterten Implementierungen automatisch auf den Standard zurückschalten.

Daher hat sich eine Gruppe von Firmen zusammengeschlossen und die WECA-Vereinigung (Wireless Ethernet Compatibility Alliance) gebildet. Diese vergibt das Wi-Fi-Logo (Wireless Fidelity). Wer es verwenden will, muss seine Geräte und Adapter einem Test unterziehen lassen. Sind diese absolut kompatibel, werden sie zertifiziert.

Das Wi-Fi-Logo besagt also, dass zum Beispiel die Adapter eines Herstellers garantiert an den Access-Points anderer anbinden können, wenn alle zertifiziert sind.

Dieses Zertifikat ist jedoch freiwillig. Trägt es ein Gerät nicht, bedeutet dies nicht, dass es nicht kompatibel ist. Auch gibt es viele Geräte, welche die Erweiterungen ihrer Hersteller haben und unter sich mit höherer Geschwindigkeit kommunizieren können, dies mit anderen Wi-Fi-Geräten aber nur nach Standard tun.

Auch hier gilt wiederum dasselbe wie bei der festen Infrastruktur. In gewerblichen Umgebungen sollte man auf eine gewisse Homogenität achten, entweder mit zertifizierten Standards oder mit einer Festlegung auf einen Hersteller.

Wer viel unterwegs ist und in vielen verschiedenen Umgebungen andocken will, sollte sich an die Standards halten.

8.11 Voice over IP

Über ein Netzwerk lassen sich bekanntlich nicht nur statische Daten im Sinne eines reinen Informationsaustausches übertragen, sondern mit der ständig größer werdenden Bandbreite, die zur Verfügung steht, auch dynamische Echtzeitdaten wie Video und Sprache. Versendet man eine Datei, ist nichts zu bemerken, wenn die Qualität der Verbindung schlecht ist; es wird nur wahrgenommen, dass „es langsamer“ ist. Verworfene und defekte Pakete werden neu versendet. Die Übertragungsprotokolle sind sehr effizient in der Fehlerkorrektur. Videoströme und Sprache aber sind äußerst empfindlich. Bilder ruckeln und bekommen Farbfehler/Pixelfehler, wenn Pakete verloren gehen oder es Verzögerungen in der Übertragung gibt. Sprachdaten werden sehr schnell unverständlich. Es treten unerwünschte Echos auf, Störgeräusche und vieles mehr. Da die Bandbreite von WLAN in den letzten Jahren stark erhöht wurde, ist auch Voice over Wireless im Kommen. Daher habe ich VOIP hier integriert.

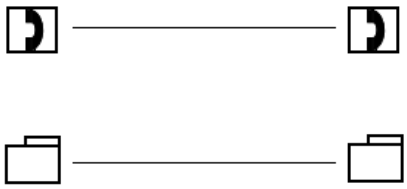

BILD 8.8 Werden Dateien übertragen (unten), spielt es oft keine Rolle, wenn vereinzelt Fehler auftreten. Bei Echtzeitdaten aber, wie Sprache, muss der Datenstrom in beiden Richtungen eine gewisse Qualität besitzen.

8.11.1 VoIP im Privatbereich

Voice over IP (VoIP) wird zusehends immer attraktiver und immer mehr genutzt. War dies mit einem Modem als Internetanschluss früher aufgrund der Geschwindigkeit nicht vernünftig möglich, ist es heute mit den schnellen DSL-Anschlüssen meist problemlos machbar. Mit zunehmender Bandbreite etabliert sich die Telefonie über das Internet. Wer einen Anschluss mit Flatrate besitzt, telefoniert in der Regel kostenlos, egal wohin. Schematisch funktioniert das nach einem Anmeldesystem.

Die Teilnehmer verbinden sich mit einem Voice-Server-Verbund im Internet, sie melden sich an. Will nun jemand einen anderen erreichen, prüft der Voice-Server, ob dieser Teilnehmer angemeldet ist. Ist dies der Fall, schickt der Server dem Anrufenden ein Signal, dass er dabei ist, die Verbindung zu starten. Dieser hört das Freizeichen. Dem zu erreichenden Teilnehmer schickt der Server ein Anrufsignal, sein Telefon läutet. Kommt die Verbindung zustande, zieht sich der Server zurück. Die Verbindung läuft nun direkt von einem Teilnehmer zum anderen. Wird das Gespräch beendet, melden sich beide als wieder frei an.

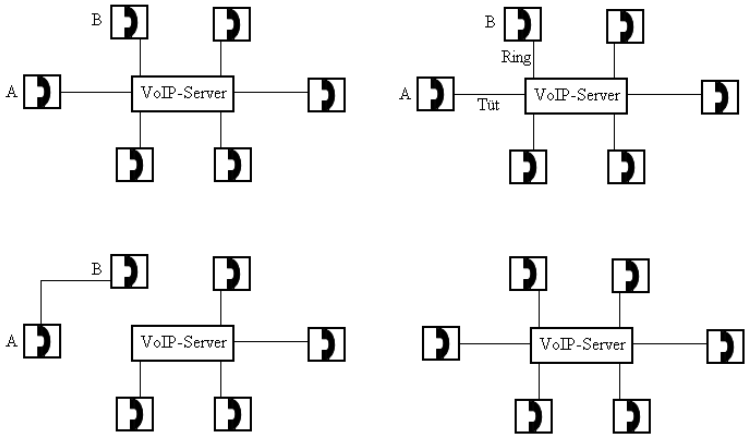

BILD 8.9 Die Kunden melden sich bei den Servern als parat an (links oben). Möchte nun A B erreichen, schickt er dem Server einen Request. Dieser prüft, ob B angemeldet ist. Wenn ja, schickt der Server A ein O. K., A hört das Anrufzeichen. Bei B klingelt das Telefon (rechts oben). Ist die Verbindung etabliert, werden die Codecs, Parameter etc. ausgehandelt und der Server zieht sich aus der Kommunikation zurück, sie ist nun end-to-end (links unten). Wird die Verbindung beendet, melden sie sich als wieder frei zurück (rechts unten).

Es gibt auch kostenpflichtige Gateways, die ermöglichen, dass ein Internet-Telefon ins Festnetz (oder Mobilfunknetz) telefonieren kann und umgekehrt.

Als Endgeräte fungieren in der Regel ein PC mit Headset und der nötigen Software (auch Soft-Phone genannt), ein IP-Phone oder ein Mobiltelefon (WLAN).

Ein IP-Phone hat den Vorteil, dass nicht immer ein PC laufen muss, um erreichbar zu sein. Da die IP-Adressen in der Regel dynamisch sind, kann von den meisten Anbietern eine sogenannte SIP-Adresse bezogen werden. Somit ist man am Dienst namentlich präsent, egal wo man ist und welche Adresse man hat. SIP selbst bietet noch keine Möglichkeit zu telefonieren. SIP ist das Session Initiation Protocol. Die Daten der Sprache müssen digitalisiert und codiert werden, meist wird auch noch eine gewisse Kompression angewandt, bevor man sie über das Internet auf die Reise schicken kann. Das SIP-Protokoll handelt die Verbindung aus, überträgt die nötigen Informationen über die verwandten Codecs, mit denen codiert wurde, etc. Die Datenübertragung regelt dann meist das Real-Time Transport Protocol RTP, das die Daten über UDP überträgt.

Es gibt noch viele andere Verfahren. Skype ist zum Beispiel ein solcher Dienst, der weit verbreitet ist. Dies ist aber closed source. Der große Vorteil von SIP-Anbietern und SIP-Adressen ist, dass man weltweit unter derselben Nummer erreichbar ist.

8.11.2 VoIP im Firmenbereich

VoIP als Ersatz der klassischen Telefonie setzt sich auch im professionellen Umfeld immer mehr durch. Meist wird migriert, wenn die Telefonanlagen ersetzungsbedürftig werden. VoIP als Ersatz der klassischen Telefonanlagen ist initial meist eine sehr große Investition. Im Gegensatz zum Privatumfeld können hier Qualitätsschwankungen oder schlecht ver-

ständliche Sprache nicht geduldet werden. Daher müssen meist spezielle Router eingesetzt werden, die den Transport garantieren können (Quality of Service, QoS). Durch die stark erhöhten Bandbreiten in den letzten Jahren werden die Netze (besonders im Backbone) aber immer schneller. Daher kann auch ohne QoS gearbeitet werden, wenn einfach genug Bandbreite zur Verfügung steht.

Weiter braucht es Server, die die Telefonate verwalten und abwickeln, und natürlich die dazu ausgebildeten Techniker. Der große Vorteil ist, dass nun Netzwerk und Telefonie über ein und dasselbe Medium übertragen werden können. Die meisten Hersteller von IP-Phones bieten bereits WLAN-Telefone an. Hier kann auch das Wireless-LAN als Medium benutzt werden.

Im professionellen Umfeld werden auch Netzwerkgeräte verwendet, die eine priorisierte Abhandlung von Voice-Paketen sicherstellen können. Die Stromversorgung der Telefone muss geregelt werden. Wer nicht für jedes Telefon eine Steckdose verbrauchen will, muss diese über das Netzwerk speisen, dies erfordert spezielle Switches oder Geräte (siehe PoE, Power over Ethernet). Dies ist auch meist der Grund für die hohe Anfangsinvestition.

8.12 Powerline – eine Alternative

Wer keinen Kabelsalat haben will, aber auch das Funknetz scheut, kann sich durch eine weitere einfache Methode behelfen, durch die Stromleitung. Powerline ist ein Standard, der entwickelt wurde, um Daten über normale Stromleitungen zu übertragen.

Das Signal wird dabei aufmoduliert und am Empfängerort wieder ausgefiltert. Nötig sind für eine Kommunikation also mindestens zwei Powerline-Bridges.

Die Übertragungsrate liegt bei ca. 80 MBit/s (zum Teil schon bei 200 MBit/s, auch diese Technologie wird ständig weiterentwickelt).

Wie beim Funknetz kann jeder „mithören“, der Zugriff zur selben Stromleitung hat. Daher empfiehlt es sich, die Datenübertragung zu verschlüsseln.

Probleme kann es mit diesem Verfahren geben, wenn der Sender und der Empfänger (sprich zwei Geräte oder Netzwerke, Datenübertragung im Netzwerk ist eigentlich immer bidirektional, beide sind Sender und Empfänger) an verschiedenen Linien (Phasen) der Stromversorgung angeschlossen sind. Oft kann das Signal die Phasentrennung nicht überspringen. Hilfe bietet da ein guter Elektriker. Mit sogenannten Phasenkopplern kann der Signalübergang erreicht werden.

Ebenso sollte kein aktiver Stromzähler zwischen Sender und Empfänger sitzen. Viele von ihnen sind als Rückstreufilter gebaut, um den Stromunternehmern eine störungsfreie Fernwartung ihrer Knotenpunkte über das eigene Netz zu ermöglichen. Daher werden von den Versorgungsunternehmen an den Übergängen zu den Endverbrauchern meist alle Frequenzen herausgefiltert, die nicht vom Stromlieferanten herrühren.

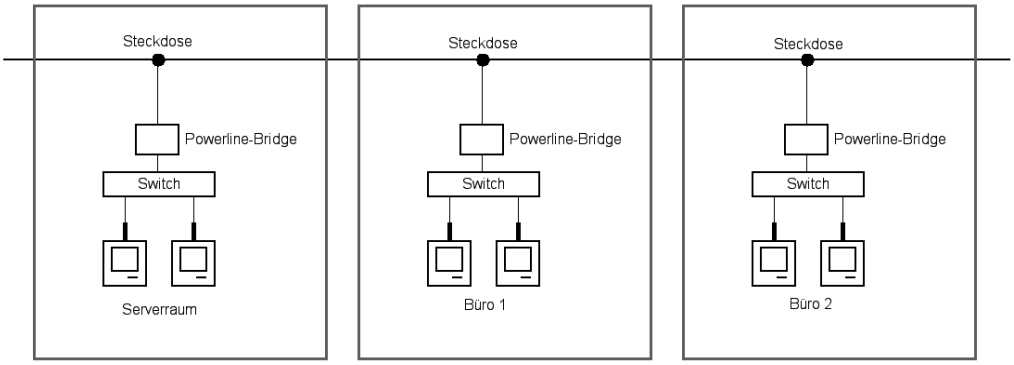

BILD 8.10 Vernetzung über Powerline-Bridges. Der Datentransport erfolgt über die herkömmliche Steckdose. Die verbundenen Räume müssen an einer Phase hängen, oder es muss mit Phasenkopplern gearbeitet werden. Wer keine abgeschlossene Umgebung hat, sollte die Daten verschlüsselt übertragen. Wie bei jedem Shared Medium kann jeder, der Zugang zu einer Steckdose hat, den Verkehr mithören.

8.13 Zukunft

Das Internet wird immer mehr zur Übertragung aller möglichen Informationen genutzt. Ob Daten, Voice, Fax oder Media-Streaming, ob wireless oder drahtgebunden – es ist zu erwarten, dass in einigen Jahren alle diese Dienste zusammenwachsen oder zumindest verschmelzen. Schon heute gibt es Anbieter, die Telefon, Fernsehen und Internet über einen Anschluss anbieten. Moderne DSL-Router verfügen bereits heute über Anschlüsse für die Internet-Telefonie. Über die Satellitenschüssel werden schon heute IP-Daten versendet. Die Dienste wachsen immer mehr zusammen.

Mit Verfahren wie WiMAX, DVB-T, DVB-S, WLAN, LTE etc. trennt sich die Verbindung auch zusehends von den Drähten. Ich vermute, dass es in naher Zukunft irgendwann nur noch ein Multifunktionsgerät geben wird, einen Anschluss, wahrscheinlich wireless, der alles in einem leisten wird, Telefon, Radio, Fernsehen, Internet etc. Schon heute ist das Tethering weit verbreitet. Hier wird z. B. über UMTS eine Verbindung vom Smartphone zum Internet hergestellt. Das Smartphone „spielt“ dann Access-Point. Der Besitzer kann sich nun mit einem oder mehreren Geräten mit WLAN verbinden und diese Verbindung nutzen (wer das ungeschützt macht, erlaubt natürlich jedem anderen auch zu verbinden).

Die Entwicklung, die die Technologien zusammenwachsen lässt, ist bereits deutlich erkennbar.

8.14 Standards und Parameter

Inzwischen gibt es viele verschiedene Standards im Bereich WLAN, und viele sind in der Entwicklung. Ständig wird an höheren Geschwindigkeiten und besseren Verbindungen gearbeitet. Es gibt hier auch einige proprietäre Verfahren, die zum Beispiel über Verfahren wie die Kanalbündelung etc. höhere Geschwindigkeiten erlauben – meist auf Kosten der Kompatibilität.

Wireless-LAN ist nicht „Ethernet over Funk“, sondern eine eigene Implementation in der 802-Familie. Mit 802.11 wurde 1997 von der IEEE ein Standard für Funknetzverbindungen im 2,4-GHz-Band mit Geschwindigkeiten von 1 MBit/s und 2 MBit/s beschrieben. Dazu gab es noch eine physikalische Schnittstelle für Infrarot, die nie richtig entwickelt wurde. Die sehr geringe Reichweite und die Tatsache, dass direkte Sichtverbindung notwendig ist, machte diese Schnittstelle unbrauchbar.

Heute sind wesentlich höhere Verbindungsgeschwindigkeiten möglich beziehungsweise im Test. Ein ganz großes Problem bei der Entwicklung von Funkstandards war die Unverfälschtheit der übertragenen Informationen. Während im Anfang des Radios Rauschen und Störungen alltäglich waren (und in manchen analogen Bändern heute noch sind), kann bei der Datenübertragung nicht akzeptiert werden, dass Bits verfälscht werden. Natürlich ist es schöner, Mozart ohne Rauschen zu hören, aber Sprache und Musik sind im Verständnis auch bei einer relativ hohen Fehlerrate brauchbar.

Daher musste schon in den Kinderschuhen der Wireless-Datenübertragung dafür gesorgt werden, dass Störungen gefiltert und korrigiert werden können. Es gibt heute sehr viele Standards im Bereich 802.11. Viele sind für den Endkunden transparent, die Buchstaben gehen schon bis 802.11z. Ich möchte hier nur die beschreiben, die tagtäglich im Einsatz sind.

8.14.1 802.11

802.11 wurde im ISM-Frequenzband (Industrial, Scientific, Medicine) angesiedelt, das lizenzfrei von allen benutzt werden kann. Daher ist es dort „eng“ geworden. In diesem Frequenzbereich tummeln sich aufgrund der kostenlosen Nutzung Bluetooth, Heim-Audio- und Videosysteme, Garagentorsteuerungen, Bewegungs- und Feuermelder, Alarmanlagen etc.

Der verfügbare Frequenzbereich erstreckt sich über 14 Kanäle mit einem Abstand von 5 MHz mit den Mittelfrequenzen von 2412 MHz bis 2472 MHz. Hier gibt es regionale Unterschiede, Kanal 14 ist zum Beispiel nur in Japan zugelassen, 12 und 13 in Europa, in Amerika sind nur die Kanäle 1–11 erlaubt.

TABELLE 8.1 Kanäle im ISM-Band

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Amerika												X	X	X
Europa														X
Japan														

Die Mittelfrequenzen sind: 2412, 2417, 2422, 2427, 2432, 2437, 2442, 2447, 2452, 2457, 2462, 2467, 2472 und 2477 MHz.

Aufgrund der oben beschriebenen Forderung, unverfälscht und fehlerfrei zu übertragen, können die Kanäle nicht eng genutzt werden. Für die Übertragung benötigen wir eine „Kanalbandbreite“ von ca. 20 MHz um die Mittelfrequenzen herum, im Standard 802.11 werden 30 MHz gefordert. Ab dann kann sichergestellt werden, dass sich die Kanäle nicht überlappen, also gegenseitig stören. Warum so breite Kanäle um eine Mittelfrequenz herum? Dafür müssen wir in die Technik der Funkübertragung hineinschauen.

8.14.2 Bandspreizung

Um Datensignale per Funk übertragen zu können, müssen sie „vorbereitet“ werden. Die Unverfälschtheit muss gewährleistet sein, sei es durch Prüfmechanismen oder andere Kontrollen, zerstörte oder gestörte Daten müssen erneut angefordert werden. Sinnvoll ist, schon im Vorfeld die größten Störmöglichkeiten zu minimieren. Man wählte dazu das Verfahren der Bandspreizung, das in der Militärfunktechnik schon lange bekannt war. Zur Minimierung der Störungen wird das Signal zuerst gespreizt, dann auf die Trägerfrequenzen aufmoduliert und übertragen.

Was bedeutet nun gespreizt? 802.11 beschreibt zwei Verfahren, von denen eines in Betrieb gegangen ist (DSSS).

8.14.2.1 DSSS, Direct Sequence Spread Spectrum

Bei DSSS wird eine Datensequenz mit einem bestimmten Bitcode bearbeitet, in der Funktechnik sagt man, gescrambelt. Das bedeutet, Bit für Bit wird die Information vor der Sendung mit XOR-Operationen gegen einen festgelegten Bitcode codiert. Und zwar mit einer höheren Bitrate als die eigentliche Sendung. Das eigentliche Signal wird also über die Frequenzen „verschmiert“. Die Intensität des Signals sinkt dabei. Dies nennt man Chipping und die Coderate die Chipping-Frequenz.

Die XOR-Funktion ist eine logische Funktion wie AND oder OR. Hat man eine Schaltung mit zwei Eingängen und einem Ausgang, bekommt bei AND der Ausgang den Wert eins, wenn beide Eingänge den Wert eins haben. Bei OR bekommt der Ausgang den Wert eins, wenn einer der beiden Eingänge oder beide den Wert eins haben. Bei XOR (exclusive-or) bekommt der Ausgang nur dann den Wert eins, wenn die Eingänge unterschiedliche Zustände haben.

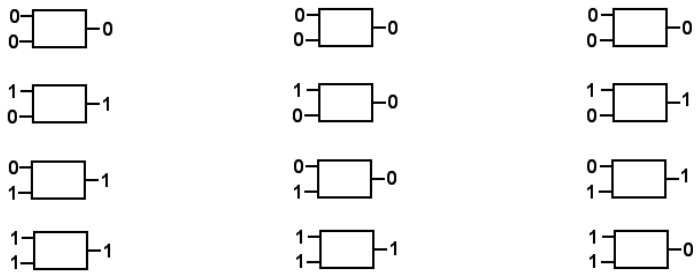

BILD 8.11 Drei neuronale Zellen mit den Funktionen OR (links), AND (Mitte) und XOR (rechts). Bei XOR wird der Ausgang nur eins, wenn die Eingänge unterschiedliche Werte haben.

Chippt man nun ein Signal aus zwei Bit mit einer 8-Bit-Chipping-Sequenz, könnte dies zum Beispiel so aussehen: Wir wollen die Zustände 0 und 1 übertragen, die Chipping-Sequenz sei 00110011:

Zu sendende Bits:	0 1
8-Bit-Spreizung:	0000000011111111
Chipping-Sequenz:	0011001100110011
Ergebnis XOR:	0011001111001100

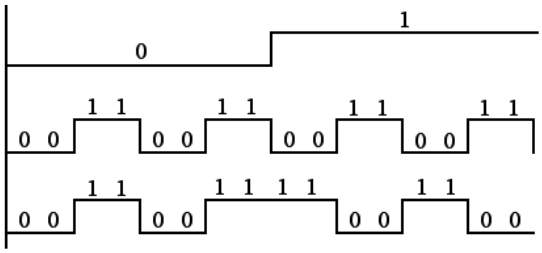

BILD 8.12 Das Chipping. Die ursprünglich zu sendende Bitfolge 0 1 (oben) wird mit dem Bitcode 00110011 (Mitte) gescrambelt. Das Ergebnis ist der Bitcode, der zur Sendung aufmoduliert wird (unten).

Am Empfänger kommt nun „der Trick“: Wie man mathematisch beweisen kann (was wir aber hier nicht tun werden), erhält man bei XOR-Operationen den ursprünglichen Bitcode zurück, wenn man dieselbe XOR-Operation mit derselben Chipping-Sequenz erneut durchführt. Das gespreizte Signal wird also entspreizt.

Gescrambelte Folge:	0011001111001100
Chipping-Sequenz:	0011001100110011
Ergebnis (XOR):	0000000011111111
Integrative Entspreizung:	0 1

Die ursprüngliche Bitrate des Ursignales (also unserer 0 und 1) nennt man die Sampling-Periode. Das Ergebnis der XOR-Operation wird in Stücke der Sampling-Periode zerlegt und integrativ ausgewertet. Also: $8 \times 0/8 = 0$ und $8 \times 1/8 = 1$.

Was macht das für einen Sinn? Hier passieren zwei Dinge von größter Bedeutung. Zum einen gibt es hier eine Möglichkeit einer Fehlererkennung und -korrektur. Wäre unser entspreiztes Signal nun in der ersten Sampling-Periode 00000100, wüssten wir, dass das nicht sein kann. Innerhalb einer Periode müssen alle Bits gleich sein, denn wir haben dasselbe Bit acht Mal gechippt. Daher können wir sicher davon ausgehen, dass hier eine Störung passiert ist und das Ergebnis 00000000 sein muss. Ist die Störung zu groß, sodass nicht mehr eindeutig entschieden werden kann, muss die Übertragung nochmals angefordert werden. Ansonsten kann der Fehler korrigiert werden.

Zum anderen haben wir noch einen weitreichenden Effekt in der Funktechnik. Durch das Chipping wird das Signal auf verschiedene Frequenzen verteilt und damit in der Intensität geringer. Es kann sogar im Rauschen untergehen. Im Militärfunk erhoffte man sich damit, Funksendungen verstecken zu können. Nur wer den Chipcode und die Sampling-Rate kennt, kann das Signal wiederherstellen.

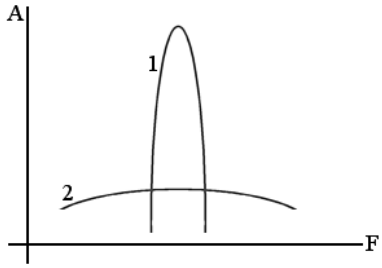

BILD 8.13 Das ursprüngliche Signal (1) wird durch das Chipping auf mehrere Frequenzen verteilt (2). Die Intensität sinkt dabei stark ab. Hier schematisch, die Fläche unter beiden Signalen sollte dieselbe sein. Das Signal ist als solches kaum noch zu sehen.

Ein Störsignal ist meist engbandig. Der Sender codiert störungsfrei. Der Empfänger erhält das Signal mit einer Störung. Durch das erneute Chipping wird das ursprüngliche Signal wiederhergestellt, die Störung aber wird nur einmal vom Empfänger gechippt, sprich „verschmiert", und sinkt in der Intensität weit ab, wird bedeutungslos oder kann gefiltert werden. Dadurch werden Störungen eliminiert.

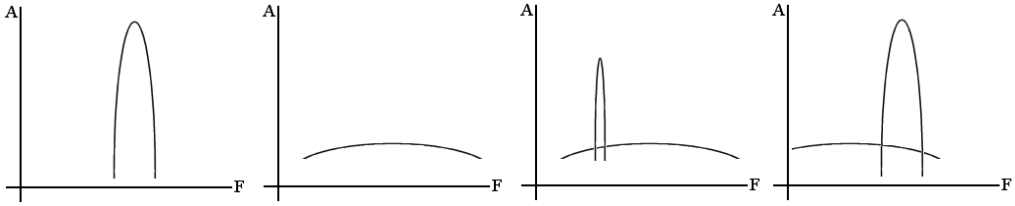

BILD 8.14 Bild links: das ursprüngliche Signal. Mitte links: das gespreizte Signal. Mitte rechts: eine Störung wird eingestreut. Rechts: Durch das Chipping wird das eigentliche Signal wiederhergestellt, die Störung aber unterdrückt.

Die Signale werden also zweifach bearbeitet, einmal gespreizt und dann auf die Trägerfrequenzen aufmoduliert. Zur Modulation kommen noch Fehlerkorrekturmechanismen. Die einzelnen Modulationsverfahren werde ich nicht ausführlich beschreiben. Sie arbeiten mit Phasen- und Amplitudenmodulation. Das ist extrem komplex, führt tief in die Mathematik und Physik, das ist genug Stoff für ein eigenes Buch, das überlasse ich Büchern zur Funktechnik.

Die Kombination aus Codierungs-, Modulationsverfahren und Fehlerkorrekturmechanismen bestimmt die einzelnen Geschwindigkeitsraten, die in einem Standard möglich sind. Automatisch werden diese an die bestehenden Verhältnisse angepasst. Sind Verbindungen schlecht oder das Signal schwach, werden Modulationen verwendet, die eine geringere Datenrate bieten, aber robuster sind; ist die Verbindung gut, werden Verfahren gewählt, die eine höhere Informationsdichte pro Zeiteinheit übertragen.

Jetzt verstehen wir, warum es zum Beispiel heißt bei 802.11a und g gibt es folgende feste Übertragungsraten, auf die sich die Geräte selbst einstellen, je nach Signalgüte:

MBit/s	Modulation	Korrektur
6	BPSK	1/2
9	BPSK	3/4
12	QPSK	1/2
18	QPSK	3/4
24	16-QAM	1/2
36	16-QAM	3/4
48	64-QAM	2/3
54	64-QAM	3/4

(Für Interessierte: BPSK: Binary Phase Shift Keying, QPSK: Quadrature Phase Shift Keying, QAM: Quadrature Amplitude Modulation)

Die Kanäle sind also in 5-MHz-Abständen definiert, wir brauchen aber für eine Übertragung 30 MHz Abstand. Das bedeutet, wir haben in diesem Frequenzband (ISM) nur drei überlappungsfreie Kanäle, nämlich 1, 7 und 13. In der Literatur wird oft von 1, 6 und 11 gesprochen. Das liegt daran, dass es viele Übersetzungen aus der amerikanischen Literatur sind, dort sind die Kanäle 12 und 13 nicht zugelassen.

HINWEIS: Einige Geräte, die für den amerikanischen Markt gebaut sind, können die Kanäle 12 und 13 technisch gar nicht nutzen. In Europa stehen daher für sie bei Standardumgebungen (1, 7, 13) lediglich zwei Kanäle zur Verfügung.

8.14.2.2 FHSS

Der Standard 802.11 beschreibt ein weiteres Verfahren der Bandspreizung, FHSS, Frequency Hopping Spread Spectrum. Hier wird nach einem festgelegten Muster die Trägerfrequenz gewechselt. Genauso muss der Empfänger nach demselben Muster auf diesen Frequenzen empfangen. Tritt nun eine Störung auf einer Frequenz auf, geht nur ein kleiner Teil der gesendeten Information verloren und muss nachgefordert werden. Treten Störungen in einer Frequenz häufig oder dauernd auf, kann diese vom Hopping ausgeschlossen werden. Für Interessierte: Bluetooth arbeitet nach FHSS.

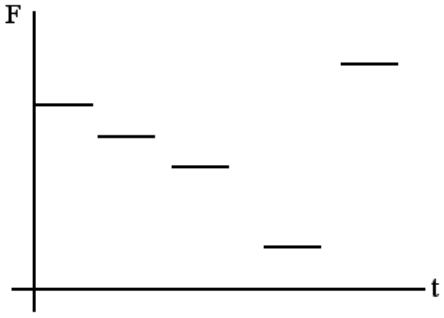

BILD 8.15 FHSS. Der Sender springt nach einem festen Muster auf verschiedenen Trägerfrequenzen. Der Empfänger muss dieses Muster kennen und genauso auf den verschiedenen Frequenzen empfangen. Frequenzen, die mit Störungen behaftet sind, können durch einen Wechsel des Musters ausgeklammert werden.

8.14.3 802.11b

1999 wurde mit 802.11b die Spreiztechnik DSSS zu HR-DSSS (High-Rate Direct Sequence Spread Spectrum) erweitert, was nun Geschwindigkeiten von 5.5 und 11 MBit/s erlaubte.

8.14.4 802.11a

1999 wurde parallel mit 802.11a ein neues Fenster im-5 GHz-Band erschlossen. Man wollte der Überfüllung des 2,4-GHz-Bereiches ausweichen. Durch eine völlig andere Technik der Codierung, OFDM (Orthogonal Frequency Division Multiplexing) statt DSSS, waren nun Raten bis 54 MBit/s möglich. Das neue Frequenzband hatte nicht die Last der vielfältigen Nutzung durch andere Funktechniken, aber „Geburtsschwierigkeiten“ unter anderem technischer Art. Es dauerte relativ lange, bis die Hersteller der Sender und Endgeräte 802.11a großflächig unterstützten. Die Frequenz ist höher, die Wellenlänge damit kürzer. Damit ist auch die Materialdurchdringung geringer.

Im 5-GHz-Band gibt es nationale Unterschiede. Nicht überall sind alle Bereiche freigegeben. In Europa sind es die Bereiche 5,15 GHz bis 5,35 GHz und 5,47 GHz bis 5,725 GHz. In den USA stehen zwölf jeweils 20 MHz breite Kanäle zur Verfügung, in Europa insgesamt 19.

Amerika, Europa:

5180, 5200, 5220, 5240, 5260, 5280, 5300, 5,320 (MHz).

Europa:

5500, 5520, 5540, 5560, 5580, 5600, 5620, 5600, 5660, 5680, 5700 (MHz).

Amerika:

5735, 5755, 5775, 5835 (MHz).

8.14.4.1 OFDM

Mit 802.11a kam eine neue Spreiztechnik zum Einsatz, OFDM, Orthogonal Frequency Division Multiplex. Hier wird nicht mit einem Bitcode gescrambelt; hier wird ein Kanal mit 20 MHz Kanalbandbreite in 64 Subkanäle aufgeteilt, die sehr engbandig sind. 48 werden parallel zur Übertragung verwendet, vier zur Synchronisation. Am oberen und unteren Rand bleiben je sechs Subkanäle unbenutzt, sodass zwischen den Kanälen zwölf Subkanäle zur Trennung verbleiben. Jede Frequenz wird für sich moduliert. Die einzelnen Kanäle sind orthogonal zueinander, das heißt, der Frequenzmittelpunkt (Scheitel) eines Subkanals liegt genau im Nulldurchgang der benachbarten. So stören sich die Signale am wenigsten und die überlagerten Signale können am Empfänger durch Fourier-Transformation wieder leicht separiert werden. Gibt es dauernde Störungen in einem Subkanal, kann dieser gemieden werden. Intelligente Fehlerkorrekturmechanismen machen die Methode fehlertolerant. Sollte trotzdem etwas verloren gehen, muss nur ein Bruchteil nachgesendet werden.

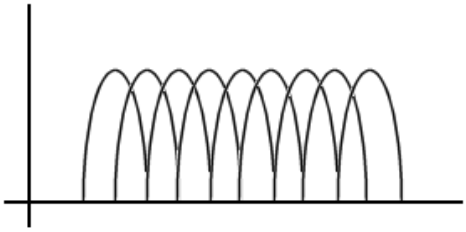

BILD 8.16 OFDM. Ein Kanal wird in Subkanäle unterteilt. Die Frequenzen werden so gewählt, dass der Scheitel eines Signales genau am Nullpunkt der benachbarten liegt. So lassen sich die überlagerten Signale beim Empfänger durch Fourier-Transformation wieder gut trennen.

8.14.5 802.11h

802.11a wurde für Amerika definiert. Um auch in Europa zugelassen zu werden, wurden Erweiterungen eingeführt. 802.11h integriert zwei Verfahren: Transmit Power Control (TPC) und Dynamic Frequency Selection (DFS).

TPC sorgt dafür, dass Sender und Empfänger den Kanal mit der besten Verfügbarkeit aussuchen und die Sendeleistung auf das benötigte Minimum drosseln.

DFS sorgt dafür, dass WLAN-Geräte sofort den Kanal wechseln, wenn Verkehr von Nicht-WLAN-Geräten detektiert wird. Dies ist der Schutz anderer Nutzer dieser Frequenzen, die Vorrang haben, sogenannte Primärnutzer. Das sind vor allem Radaranlagen. Dies war die Voraussetzung zur Freigabe der Frequenzen in Europa.

8.14.6 802.11g

2003 wurde das Codierungsverfahren OFDM in das 2,4-GHz-Band übernommen. Seither kann auch in diesem Band mit Raten von bis zu 54 MBit/s gesendet werden.

8.14.7 802.11n

Noch schneller. Ein ehrgeiziges Ziel war es, das Wired LAN in der Geschwindigkeit zu erreichen. Fast Ethernet, also 100 MBit/s, war das Ziel. 2009 wurde der Standard 802.11n veröffentlicht.

Innerhalb der gegebenen Grenzen wurden Verfahren eingeführt, die bereits aus der Militär- und Radartechnik bekannt waren. Neben der seriellen Codierung der Signale wurden räumliche Codierungen eingeführt. Bei 802.11n wird mit mehreren Antennen gearbeitet. Mit mehreren Antennen lassen sich deutliche Gewinne erzielen. Systeme mit mehreren Antennen für Sendung und Empfang sind in der Lage, auf denselben Frequenzen mehrere Datenströme zu versenden und zu empfangen, parallel. 802.11n arbeitet in beiden Bereichen, im 2,4- und im 5-GHz-Bereich, wenn möglich gleichzeitig. Die Kanalbandbreite wurde auf optional 40 MHz erweitert. Damit waren völlig neue Codierungen möglich. Aufgrund der „Enge“

im 2,4-GHz-Bereich ist es selten möglich, die 40-MHz-Breiten zu nutzen. Im 5-GHz-Bereich aber ist dies möglich.

HINWEIS: Es gibt Adapter, meist im Billig-Segment, die zwar 802.11n unterstützen, aber nur im 2,4-GHz-Bereich. Diese bringen keine Performance.

802.11n-Geräte kennen drei Modi des Betriebes: Legacy (802.11a/b/g), Mixed-Mode (802.11n und 802.11a/b/g) und Greenfield (nur 802.11n)

Greenfield schaltet alle Kompatibilitäten ab. Die Performance ist maximal. Dieser Modus sollte nur in abgeschlossenen Umgebungen eingesetzt werden. 802.11a-Geräte erkennen diese Datenströme im 5-GHz-Bereich nicht mehr als WLAN, sondern als fremden, sprich Primärnutzer, und geben die Frequenzen frei (DFS), werden also gestört.

Eine Lösung ist, Access-Points, die diese Möglichkeit bieten, im 2,4-GHz-Band auf Legacy und im 5-GHz-Band auf n einzustellen. Somit sind die nötigen Features für alle möglich.

8.14.7.1 Antenna-Diversity

Schon mit zwei Antennen kann Antenna-Diversity genutzt werden. Durch Laufzeitunterschiede in Mehrwegeausbreitungen können Interferenzen entstehen, die das Signal unbrauchbar machen oder schwächen. Hat man zwei Antennen im richtigen Abstand, bilden sich alternierende Interferenzmuster. Sendet der Sender in der Kommunikation mit dem Client nur mit einer, kann diese Störung umgangen werden.

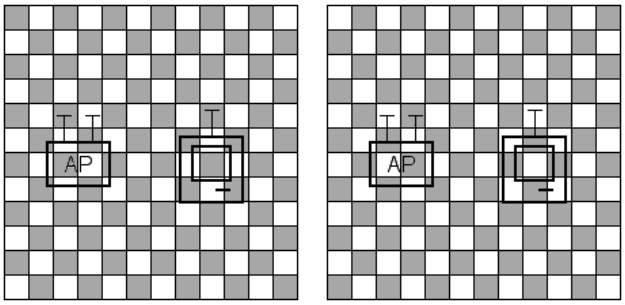

BILD 8.17 Zwei Antennen im richtigen Abstand (1/2 Wellenlänge) erzeugen alternierende Interferenzmuster. (Hier sehr symbolisch abgebildet.) Kommuniziert der Sender nur mit einer Antenne mit dem Client, ist dieser außerhalb der destruktiven Interferenz.

8.14.7.2 Gruppengewinn

Mit mehreren Antennen kann auch mehr Leistung entnommen werden. In der Funktechnik nennt man dies Gruppengewinn.

8.14.7.3 MIMO, Multiple Input Multiple Output

Der größte Vorteil mehrerer Antennen aber ist ein anderer. Hat man mehrere Antennen an Sender und Empfänger, können diese verschiedenen Datenströme gleichzeitig auf einer Frequenz versenden, je Antennenpaar einen Datenstrom. Diese Ströme nennt man Spatial

Streams. Technisch ist das möglich, da mehrere Antennen ermöglichen, räumliche Informationen zu ermitteln, eine weitere Dimension kommt hinzu.

Technisch sind zurzeit vier Streams mit vier Antennen möglich. Bei Raten von 150 MBit/s pro Stream sind Bruttoraten von 600 MBit/s für 802.11n beschrieben. Diese Adapter sind aber sehr teuer und zurzeit noch experimentell. Zwei Streams sind im Moment üblich. Hier entstehen auch Kosten im Installationsbereich. Wer auf 802.11n aufrüstet, muss eines bedenken: Um die Datenrate bieten zu können, muss der Anschluss der Access-Points angepasst werden. Sind sie mit Fast Ethernet erschlossen, also 100 MBit/s, reicht dies für die volle Performance nicht mehr aus.

MIMO kann einerseits verwendet werden, um bei einer Verbindung von zwei Geräten die Datenrate zu verdoppeln oder um mit zwei Stationen mit der vollen Bandbreite zu kommunizieren.

MIMO nutzt die Tatsache aus, dass mehrere, voneinander definiert entfernte Antennen dasselbe Signal senden. Durch die Laufzeitunterschiede, die Wege sind ja verschieden groß, kommen die Signale leicht phasenverschoben an. Aus den Laufzeitunterschieden ergibt sich eine lineare Matrix, die von ASICs gelöst werden kann. Bei MIMO müssen laufend Tuning- und Testsignale versendet werden, da sich zum Beispiel Personen im Raum bewegen oder sich der Client bewegt. Mehrwegeausbreitungen werden verwendet, um die Raumgeometrie zu erkennen.

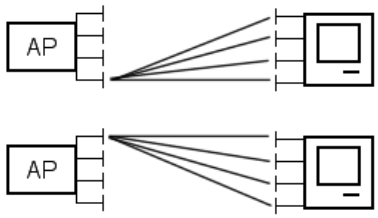

BILD 8.18 MIMO. Wird mit mehreren Antennen gesendet, trifft das Signal aufgrund der Laufzeitunterschiede leicht phasenverschoben ein. Hier im Bild sehen Sie zwei Möglichkeiten von acht. Aus diesen Informationen entsteht eine lineare Matrix, über die sich die Streams zuordnen lassen.

8.14.7.4 Beamforming

Der Einsatz mehrerer Antennen erlaubt auch, dass die Abstrahlung des Signals in Richtung des Empfängers optimiert werden kann, dies nennt man Transmit-Beamforming. Der Empfänger erhält eine höhere Eingangsleistung. Damit kann zu „gehaltvolleren“ Codierungen gewechselt werden, die Übertragungsrate wird erhöht.

(Das Beamforming ist schon lange bekannt, vor allem in der Militärfunktechnik, hier heißt es „Phase-Shift-Array“ und wird auch für Richtungsbestimmungen eingesetzt.) Wird ein Signal über mehrere Antennen versendet, können diese Sendungen bewusst zeitverzögert zwischen den Antennen erfolgen. Dadurch wird die Ausbreitung der Wellenfront gerichtet.

Sowohl für Beamforming als auch für MIMO muss dem Sender und Empfänger der Raum „bekannt“ sein.

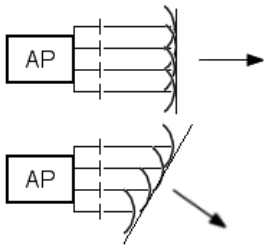

BILD 8.19 Beamforming. Wird ein Signal zeitversetzt von mehreren Antennen ausgesendet, kann die Richtung der Ausbreitung der Wellenfront gesteuert werden.

8.14.7.5 Packet-Aggregation

Bei Packet-Aggregation wird das WLAN-Frame so vergrößert, dass mehrere Datenpakete hineinpassen. Der Overhead von Headern wird reduziert. Bei häufigen Störungen entfällt der Vorteil, da nun größere Pakete mehrfach gesendet werden müssen.

8.15 Kompatibilität und Effizienz

Allen Verfahren ist eines gemeinsam. Sie konzentrieren sich auf Techniken, die eine Kanalbandbreite von ca. 20 MHz benötigen. Das bedeutet nicht, dass sie kompatibel sind, sondern dass sie in den zur Verfügung stehenden Frequenzen koexistieren können. Die Mittelfrequenzen mit ihrem Kanalband sind nahezu gleich. In Mischumgebungen wird nur häufig der Fall auftreten, dass die 40 KHz Kanalbandbreite nicht zur Verfügung stehen. 802.11n arbeitet dann nicht mit der vollen Performance. Wi-Fi-Adapter handeln aus, mit welchem Standard sie kommunizieren.

Wie oben beschrieben gibt es in allen Standards feste Übertragungsraten, die sich aus der Kombination der Codierungs- und Modulationsverfahren ergeben. Hier wird technisch immer der Weg gegangen, zwischen Geschwindigkeit und Stabilität abzuwägen. Ist ein Signal robust und klar, werden die Verfahren auf Bandbreite optimiert, ist das Signal schwach oder mit Störungen behaftet, wird die Geschwindigkeit zurückgeschaltet und mehr Wert auf Stabilität gelegt. Funknetzverfahren sind hoch komplexe, dynamische und anpassungsfähige Konstrukte. Viele dieser Techniken sind in anderen Funkverfahren ebenfalls im Einsatz, sei es GPS, UMTS oder GPRS. Die angegebenen Übertragungsraten sind immer Bruttoraten unter optimalen Bedingungen. In der Realität kann als Faustwert die Hälfte der Bruttorate bei guten Bedingungen erreicht werden.

Geräte, die nach 802.11b arbeiten, sind inzwischen Störquellen. Sie können die Codierungen von 802.11 a, g und n nicht verstehen. In Mischumgebungen muss daher allen bekannt gemacht werden, dass b-Geräte im Einsatz sind, was alle anderen stark abbremst. Schon ein b-Client kann die Performance in einem Raum zerstören. Wer High-Speed-WLAN sicher benötigt, der muss 802.11b abschalten und dafür sorgen, dass keine Geräte mehr diese Adapter benutzen.

802.11g und 802.11n benötigen eine Kanalbandbreite von 20 MHz. Daher wäre es eigentlich möglich, im 2,4-GHz-Band vier überlappungsfreie Kanäle zu nutzen, 1, 5, 9 und 13. Aber 1, 7 und 13 werden in der Regel immer noch benutzt, zur Kompatibilität mit Geräten nach 802.11b, ein Kanal also „verschenkt“.

8.16 Super-High-Speed, die Zukunft

Parallel werden zurzeit zwei neue Standards bearbeitet, die eine noch größere Steigerung der Übertragungsraten ermöglichen sollen, bis hin zu 7 GBit/s. Sie werden nicht in Konkurrenz entwickelt, sondern sollen sich ergänzen.

8.16.1 802.11ac

Dies ist eine Weiterentwicklung von 802.11n im 5-GHz-Band. Die wesentlich höhere Verbindungsrate soll durch dieselben, weiterentwickelten Techniken erzielt werden. Die Kanäle werden auf 160 GHz verbreitert, es wird mit 8x MIMO gearbeitet und das Beamforming soll perfektioniert werden. Die verbreiterten Kanäle erlauben Codierungsverfahren mit wesentlich höherer Übertragungskapazität.

Es ist jedoch fraglich, ob diese Technik, außer bei hochgetunten Punkt-zu-Punkt-Verbindungen ohne Störeinflüsse, einsetzbar ist. Eine Kanalbandbreite von 160 MHz mit der ständigen „Bedrohung“ von DFS scheint nicht realistisch.

Auch ist fraglich, ob bei mobilen Endgeräten ein 8x MIMO technisch und preislich machbar ist.

8.16.2 802.11ad

Hier werden völlig neue Wege beschritten, eine Kompatibilität zu anderen Standards ist nicht mehr vorgesehen. Der Standard arbeitet im 60-GHz-Band. Dort ist noch genug Platz für mehrere Kanäle mit einer Kanalbandbreite von bis zu 2 GHz.

Dieses Funkband ist ungenutzt und ebenfalls frei. Hier gibt es aber eine große Einschränkung. Bei 2,4 GHz liegt die Wellenlänge bei ca. 15 cm. Bei 5 GHz liegt sie bei ca. 7 cm. Bei 60 GHz haben wir Wellenlängen von ca. 5 mm. Eine Materialdurchdringung findet so gut wie nicht mehr statt. Vorteil: WLANs in benachbarten Räumen stören sich nicht, Nachteil: Ein Access-Point pro Raum wird nötig.

Index

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z