7.3.1.1 Technische Grundlagen

Einer der ersten verfügbaren Wireless Standards war IEEE 802.11, der bereits 1997 verabschiedet wurde. 802.11 erlaubte drahtlose Netzwerke mit einer Übertragungsrate von bis zu 2MBit/sec. Höhere Übertragungsraten wurden erst mit dem 1999 verabschiedeten Standard 802.11b verfügbar, mit dem bis zu 11MBit/sec übertragen werden können. Beide Standards arbeiten in dem sogenannten ISM (Industrial, Scientific und Medical)-Band im Frequenzbereich von 2.45 GHz. Die Funkübertragung erfolgt dabei auf einzelnen Kanälen, wobei jeder Kanal für eine leicht unterschiedliche Frequenz steht. Auf diese Weise können mehrere Sende-/Empfangseinheiten nebeneinander arbeiten, ohne sich gegenseitig zu stören. In Europa sind insgesamt 13 Kanäle verfügbar, in anderen Ländern, insbesondere in den USA sind nur 11 Kanäle erlaubt. Daher werden auch die Geräte oftmals als European- oder World-Edition vermarktet, die dann entweder über 13 oder nur 11 Sende-/Empfangskanäle verfügen.

Eine weitere Steigerung der Übertragungsrate auf bis zu 54MBit/sec verspricht der ebenfalls 1999 verabschiedete Standard 802.11a. Allerdings werden Geräte, die entsprechend 802.11a arbeiten, nicht mehr mit Geräten kompatibel sein, die mit 802.11b arbeiten, da die 54MBit-Technologie ein anderes Frequenzband im Frequenzbereich von 5 GHz verwendet. Um dennoch kompatibel zu den inzwischen sehr weit verbreiteten Geräten zu bleiben, die im 2.45-GHz-Band arbeiten, können die neuen Geräte mit zwei Sendern/Empfängern ausgestattet werden, so daß sie in beiden Frequenzbändern arbeiten können. Eine Alternative verspricht der noch in Entwicklung befindliche Standard 802.11g, mit dessen Hilfe Geräte im 2.45-GHz-Band Datenübertragungsraten von bis zu 54Mbit/sec erreichen, ohne die Kompatibilität zu den 802.11b-Geräte aufgeben zu müssen. Erreicht wird diese Leistungssteigerung durch verbesserte Modulationstechniken.

Zur Zeit werden fast ausschließlich Geräte verkauft, die nach 802.11b arbeiten, also eine maximale Datenübertragungsrate von 11MBit/sec erreichen. 802.11b erlaubt neben der Übertragungsrate von 11Mbit weitere Level mit 5.5 und 2 und 1 MBit/sec. Die Geräte wählen je nach Signalstärke die beste Übetragungsrate selbständig aus, falls keine festen Konfigurationsvorgaben existieren.

Um sicherzustellen, daß Geräte unterschiedlicher Hersteller nicht nur auf dem Papier miteinander kompatibel sind, sondern auch in der Praxis zusammen arbeiten, wurde eine Testsuite für 802.11b-Geräte von der Wireless Ethernet Compatibility Alliance (WECA) entwickelt, einem Zusammenschluß verschiedener Hersteller von Wireless-Produkten. Jedes Produkt, das diese Tests besteht, erhält ein WIFI (Wireless Fidelity)-Emblem. Die WIFI-Auszeichnung von Produkten soll dem Anwender die Sicherheit geben, daß alle so ausgezeichneten Geräte herstellerübergreifend untereinander kompatibel sind.

Ein wichtiger Punkt für den Aufbau und Betrieb eines Funknetzes ist natürlich die Reichweite der Funksignale. Die Reichweite hängt sowohl von der Sende-

leistung der beteiligten Geräte als auch von der örtlichen Gegebenheiten ab. Typische Wireless-Geräte arbeiten mit einer Sendeleistung von 35mW (*m*illi *W*att), einer im Vergleich z. B. zu Handys, die mit bis zu 2000 mW senden können, eher geringen Leistung. Sehr wichtig sind die örtlichen Gegebenheiten. So kann im Freien eine Reichweite von bis zu ca. 500 m erzielt werden, wo hingegen in massiv gebauten Gebäuden evtl. nur 30 m überbrückt werden können. Je massiver die Baustruktur ist, wobei Metallbeschichtungen, wie z. B. Aluminium-Folie zur Wärmeisolation, besonders abschirmend wirken, desto geringer ist die Reichweite der Wireless-Geräte.

7.3.1.2 Wireless und Linux

Linux unterstützt schon seit einiger Zeit Wireless-Hardware. In einem aktuellen Kernel sollten alle benötigten Treiber bereits als Module mitübersetzt sein. Linux bietet sowohl für einige Wireless PCI-Karten als auch für sehr viele PCMCIA-Karten die notwendige Treiberunterstützung. Wireless PCI-Karten können verwendet werden, um einen Desktop-PC drahtlos mit anderen Rechner zu vernetzen, während →*PCMCIA*-Karten speziell für Laptops und andere mobile Geräte gedacht sind. Eine weitere Gruppe stellen die USB-basierten Karten dar, deren Bedeutung immer mehr zunimmt.. Für Linux gibt es bisher nur für wenige solcher Karten Unterstützung, was sich aber sicherlich im Laufe der Zeit ändern wird.

Die Inbetriebnahme einer Wireless-Karte unter Linux gestaltet sich grundsätzlich sehr einfach und besteht nur aus wenigen Schritten. Zum einen muß der entsprechende Kernel-Treiber für die jeweilige Karte geladen werden. Speziell für PCMCIA-Karten wird diese Aufgabe i. d. R. schon durch die Konfiguration des Linux-PCMCIA-Systems übernommen. In den meisten Fällen muß hier lediglich die PCMCIA-Karte eingesteckt werden, und der korrekte Treiber wird geladen. Bei PCI- und USB-basierten Karten sollte zuerst versucht werden, die Karte mit dem Konfigurationswerkzeug der Distribution (bei SuSE: YaST) zu konfigurieren. Gelingt dies nicht, muß die Auswahl des Treibers manuell, z. B. aufgrund des Kartentyps und Herstellers, erfolgen. Nötigenfalls können einfach verschiedene Treiber ausprobiert werden. An Treibern stehen grundsätzlich drei verschiedene Quellen zur Verfügung: Die Treiber des PCMCIA-Systems, die Kernel-basierten PCMCIA-Treiber sowie Treiber des WLAN-NG-Projekts. Weitere Informationen hierzu finden sich in Abschnitt 7.3.3.2 auf Seite 655.

Neben dem Laden der Treiber sind verschiedene Einstellungen für ein WLAN möglich, die für das Funktionieren sehr wichtig sind. Diese Einstellungen können unter Linux mit Hilfe des Programms `iwconfig` vorgenommen werden, das Teil der sogenannten Wireless Tools ist. Die Wireless Tools sind eine Sammlung von Linux-Programmen und Bibliotheken, die bei SuSE Linux in dem Paket `wireless-tools` enthalten sind. Das Wesentliche an den Wireless-Tools ist

die Tatsache, daß die möglichen Einstellungen mit *einem* Werkzeug für alle Kartentypen gemacht werden. Hierzu wurden im Kernel die sogenannten Wireless Extensions implementiert, letztlich eine Programmierschnittstelle (API), die es dem Benutzer erlaubt, unterschiedliche Treiber für Wireless-Hardware in einheitlicher Weise, z. B. mit `iwconfig`, zu konfigurieren. Die Wireless Extensions wurden als Erweiterung der Netzwerkschnittstellen implementiert, daher stammt auch die Namensanalogie des Werkzeugs zur Konfiguration von Netzwerkkarten `ifconfig` und dem Werkzeug zur Konfiguration von Wireless-Netzwerkkarten `iwconfig`.

Die wichtigsten Parameter, die eingestellt werden müssen, um ein neues Gerät in ein Wireless LAN einzubinden, sind die sogenannte →*SSID* und Einstellungen zur verschlüsselten Datenübertragung mit Hilfe von →*WEP*. Die SSID (Service Set Identifier), manchmal auch als Netzwerk-Name bezeichnet, dient der logischen Trennung von verschiedenen Funknetzwerken. Da Funknetzwerke keine klare räumliche Abgrenzung ermöglichen und sich somit überlappen können, wird eine Zeichenkette als Schlüssel verwendet, um Zugang zu *einem bestimmten* Funknetz zu erhalten. Alle Geräte eines Funknetzes teilen sich diesen gemeinsamen Schlüssel. Die Konfiguration des Access-Points (die Sende/Empfangs-Station, über die eine Anbindung an ein Festnetz durchgeführt wird, s. u.) entscheidet darüber, welche SSID von den mobilen Client-Rechnern verwendet werden muß[2]. Dabei kann ein Access-Point so konfiguriert werden, daß er die SSID ständig mit aussendet, so daß jeder Client sie hören kann. In diesem Fall darf auf dem Client einfach die Zeichenekette `any` als SSID verwendet werden. Strahlt der Access-Point die SSID jedoch nicht aus, so kann die verwendete SSID nur vom Administrator des Access-Points erfahren werden und muß beim Client entsprechend konfiguriert werden. In diesem Fall wird die →*SSID* also als ein erstes Mittel dazu verwendet, den Zugriff auf ein Funknetz einzuschränken, so daß nicht jeder, der mit einem Laptop in der Hand an dem vernetzten Bereich vorbeikommt, das Netz automatisch sieht und direkten Zugriff darauf erhält.

Der zweite für die Inbetriebnahme wichtige Parameter betrifft die Sicherheitseinstellungen für die Funkübertragung. In der Default-Konfiguration werden alle Daten unverschlüsselt übertragen, d. h. jeder, der sich im Bereich des Funknetztes aufhält, kann alle Daten problemlos abhören. Ein Verfahren zur verschlüsselten Datenübertragung, das von allen Geräten unterstützt wird, ist WEP, eine Verschlüsselungsverfahren, das als minimaler Schutz vor Abhörversuchen Dritter gewertet werden kann. WEP basiert auf einem gemeinsamen geheimen Schlüssel, der von allen Geräten geteilt wird. Wer seinen Rechner in ein bestehendes WLAN integriert, muß sich erkundigen, ob WEP verwendet wird. Darüber hinaus muß er noch den WEP-Schlüssel kennen (sozusagen das Passwort). Wer sein

[2] Wie später noch dargestellt wird, kann ein Funknetz auch auch ganz ohne Access-Point im sogenannten Ad-Hoc-Modus betrieben werden. In diesem Fall sind lediglich die SSID-Einstellungen der an dem Netz beteiligten WLAN-Karten von Interesse.

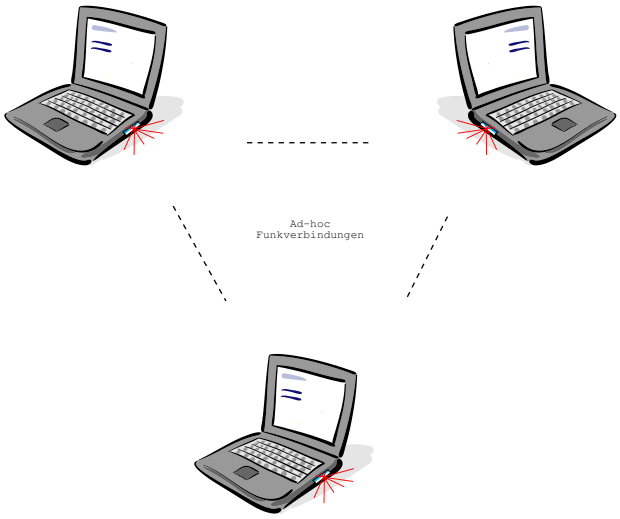

Abbildung 7.4: Der Ad-hoc-Betriebsmodus eines WLANs

eigenes WLAN aufbaut, sollte zunächst für erste Tests ganz auf die Verschlüsselung verzichten und diese erst dann aktivieren, wenn das WLAN grundsätzlich funktioniert. Auch WEP bietet leider keine 100% Sicherheit. Mehr zu diesem Thema wird in Abschnitt 7.3.4.3 auf Seite 678 gesagt.

7.3.2 Struktur eines WLANs

Bevor ganz konkret auf die Konfiguration eines WLANs eingegangen wird, soll zunächst dargestellt werden, welche Varianten es beim Aufbau von WLAN Netzwerken gibt. Ein 802.11 Wireless LAN kann grundsätzlich in zwei verschiedenen Modi aufgebaut bzw. betrieben werden, die als Ad-hoc- und Infrastructure-Mode bezeichnet werden.

Ad-hoc Im Ad-hoc-Modus besteht ein Wireless Netzwerk einfach aus den beteiligten Client-Rechnern, die mit Hilfe einer WLAN-Karte direkt miteinander kommunizieren können. Diese Art der Vernetzung ist in Abbildung 7.4 dargestellt. Zur Vernetzung wird in diesem Fall außer den beteiligten Rechnern und den WLAN-Karten für diese Rechner keine weitere Hardware, wie z. B. eine zentrale Komponente, benötigt. Jeder Rechner, der über eine WLAN-Karte verfügt, kann direkt mit anderen Rechnern des gleichen WLANs, die sich in Reichweite befinden, kommunizieren. Der Ad-hoc-Modus wird in einigen Fällen auch als peer-to-peer-Modus oder als IBSS (Independent Basic Service) bezeichnet. Obwohl IBSS die im Standard offiziell eingeführte

Bezeichnung für diesen Modus darstellt, wird sie relativ selten verwendet. Daher wird im folgenden nur vom Ad-hoc-Modus gesprochen.

Infrastructure Ein Wireless LAN, das im Infrastructure-Modus (offiziell auch als BSS oder ESS[3] bezeichnet) betrieben wird, verfügt im Gegensatz zum Ad-hoc-WLAN über eine oder mehrere, zentrale Komponenten, über die aller Funkverkehr abgewickelt und der Zugriff auf das Medium unter den Anwendern geregelt wird. Eine solche Komponente wird *Access Point* genannt. Ein Access Point ist eine eigenständige Sende/Empfangseinheit, die zusätzlich über eine Anbindung an das Festnetz verfügt. Rechner, wie z. B. Laptops mit WLAN-Karten, die Daten untereinander austauschen wollen, müssen dies im Infrastructure-Modus *immer* über den Access-Point tun, sie kommunizieren also *nicht* direkt untereinander. Eine solche Konfiguration ist in Abbildung 7.5 auf der nächsten Seite dargestellt. Neben der reinen Sende- /Empfangsfunktion sowie der Anbindung von Wireless vernetzten Rechnern an ein Festnetz bieten Access Points den Client-Systemen auch die Möglichkeit zu Roamen, was insbesondere für größere Organisationen wichtig ist. Soll z. B. ein ganzer Campus einer Universität drahtlos vernetzt sein, so ist die Ausdehnung des Gebiets, das drahtlos vernetzt werden muß, i. d. R. größer als die Reichweite, die mit zwei Funknetzwerkkarten überwunden werden kann. In diesem Fall können einfach ein oder mehrere Access Points auf dem Gelände aufgestellt werden, so daß überall ein ausreichend guter Funkkontakt von einem Access-Point zu einer WLAN-Karte, z. B. in einem Laptop, möglich ist. Ein Client-Rechner, z. B. der eines Studenten, der mit seinem Laptop über den Campus geht, muß daher je nach seinem Standort von unterschiedlichen Access Points „bedient“ werden. Mit Roaming wird die Möglichkeit, z. B. eines Laptops, beschrieben im Fall einer Standortveränderung unterbrechungsfrei die Verbindung von einem Access Point an einen anderen zu übergeben. Für den Benutzer des Laptops ist dieses Umschalten transparent und ermöglicht auf diese Weise eine fast beliebige Ausdehnung eines Funknetzes, durch das sich der Anwender frei und ohne Unterbrechung der Netzverbindung bewegen kann. Das Roaming selbst erfolgt automatisch durch die beteiligten Access Points ohne zutun des Anwenders.

Neben den genannten Funktionen statten Hersteller Access Points häufig zusätzlich mit speziellen Funktionen aus, z. B. als Router für einen DSL-Anschluß als auch mit zusätzlicher Firewall-Funktionalität. Als Hardware für Wireless-Funktionalität kommt übrigens im Inneren des Access Points nicht selten eine Wireless PCMCIA-Karte des gleichen Herstellers zur Verwendung.

[3] Der Begriff BSS (Basic Service Set) bezeichnet einen Access-Point mit Anbindung an ein Festnetz, der Wireless Clients bedient. Der Befriff ESS (Extended Service Set) meint ein oder mehrere BSS, die ein gemeinsames Subnetz bilden.

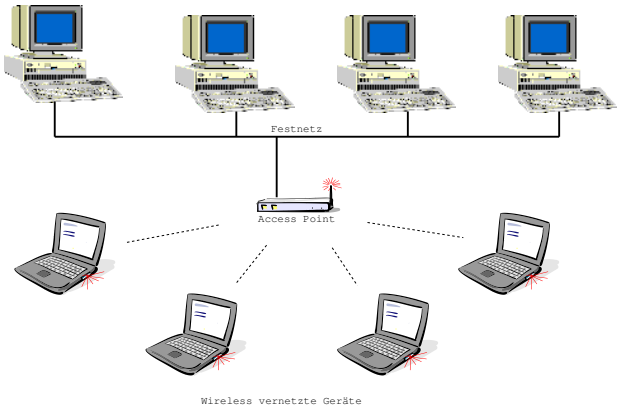

Abbildung 7.5: Der Infrastructure-Betriebsmodus eines WLANs

Aus dem Gesagten ergeben sich ganz klar die Anwendungsszenarien für beide Modi. Sollen nur zwei oder drei Rechner miteinander vernetzt werden, kann die preiswertere Variante der Ad-hoc Vernetzung verwendet werden. Wer zusätzlich eine Anbindung an ein Festnetz benötigt und auch Roaming-Funktionalität benötigt, sollte in einen Access Point investieren und sein Funknetz im Infrastructure Modus betreiben.

Im folgenden wird, falls nichts anderes gesagt wird, davon ausgegangen, daß ein Funknetz im Infrastructure-Modus mit einem Access Point betrieben wird. Daher wird in den folgenden Abschnitten zunächst auf die Konfiguration des Access Points eingegangen und erst dann auf die Konfiguration der Client-WLAN-Karten. Hinweise für die Konfiguration, um ein WLAN im Ad-hoc-Modus zu betreiben, werden in Abschnitt 7.3.3.4 auf Seite 672 gegeben.

7.3.2.1 Hinweise zur Standortwahl eine Access Points

Wer ein Funk-LAN neu aufbaut und dabei einen Access Point verwendet, sollte sich ein paar Gedanken über die Plazierung dieses Geräts machen. Da die Vernetzung über Funkwellen im 2 bzw. 5 GHz-Bereich erfolgt, kann der Standort entscheidend darüber sein, welcher Bereich mit einem Access Point abgedeckt werden kann. Funkwellen in diesem Frequenzbereich werden durch alle festen Substanzen abgeschwächt. Insbesondere Metalle oder metallische Beschichtungen, z. B. auf Folien zur Wärmeisolierungen etc., können die Funksignale fast ganz abschirmen.

Ein Access Point sollte nun einfach so positioniert werden, daß sich möglichst wenig der oben genannten Hindernisse auf dem Weg zu den Client-Rechnern befinden. Auf der anderen Seite muß auch das Festnetz oder der DSL-Anschluß noch