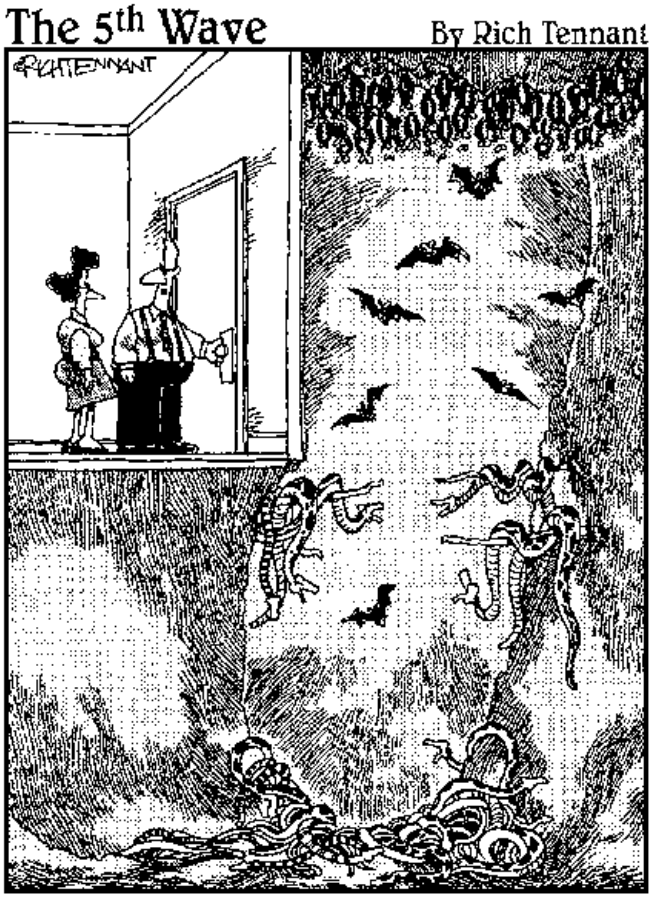
Teil I

Ihr Netzwerk planen und einkaufen



»Dieser Teil des Tests wird uns sagen, ob Sie persönlich dem Job des Netzwerkadministrators gewachsen sind.«

In diesem Teil ...

Dieser Teil bietet Ihnen die Grundlagen, die Sie benötigen, um tief in die Welt der Wireless-Netzwerke eintauchen zu können. Sie werden die Elemente entdecken, die Sie als wissender Nutzer von Wireless-Netzwerken kennen müssen, und Sie werden sehen, wie und warum die Planung des Einsatzes dieser Technologie eine sehr kritische Komponente ist. Bei Ihrer Planung werden Sie feststellen, wie wichtig Standorterhebungen für Ihre Implementation sind. Schließlich werden wir Ihnen zeigen, wie Sie das richtige Equipment Ihren Anforderungen und Bedürfnissen entsprechend auswählen. Sie werden außerdem die verschiedenen Wireless-Modi und -Frequenzen kennen lernen, was Ihnen dabei helfen wird, Equipment zu kaufen, das Ihrem Plan entspricht.

Die Ketten entfernen: Willkommen in der Wireless-Welt

1

In diesem Kapitel

- Die Risiken und die Vorteile des Wireless-Networkings
- Wireless-Netzwerk-Typen und -Akronyme
- Ihr Wireless-Netzwerk planen und installieren
- Administration und Troubleshooting

Wir kommen zu einer interessanten Zeit für alle Netzwerkadministratoren und Benutzer, denn wir befreien uns von den Ketten unserer verkabelten Welt und überschreiten die Grenze zum Wireless-Networking. Dieses Buch zeigt Ihnen die notwendigen Schritte, um diesen Übergang so nahtlos und zuverlässig wie möglich zu vollziehen, während Ihre Unternehmenswerte natürlich vor unautorisierten Zugriffen geschützt bleiben.

In vielen Büroumgebungen sind die Schreibtische und die Desktop-Computer darauf feste Einrichtungsgegenstände. Jeden Tag kommen Sie ins Büro, setzen sich an den Schreibtisch und schalten den Computer ein – bereit dazu, den Tag zu beginnen. Sie haben auch kaum eine andere Wahl, denn Ihr Computer benötigt ein Kabel bis zum Netzwerk, damit Ihre Applikationen und das Internet Sie bei der Arbeit unterstützen können. Schon jahrelang sind Sie verkabelt.

Vielleicht haben Sie aber schon gesehen, wie Wireless-Networking Ihrem Geschäft eine Möglichkeit bietet, die Kosten für Drähte und Kabel hinter sich zu lassen, und die Welt der Radio- oder Funkwellen zu betreten. Können Sie sich vorstellen, darauf warten zu müssen, dass jemand ins Büro oder nach Hause zurückkehrt, nur um ihn per POTS erreichen zu können?

Ähm..., was ist POTS? *Plain Old Telephone Service*, zu gut Deutsch: altes Telefon, Kabel, Einschränkungen. Falls Sie heute ein Teenager sind, haben Sie die Tatsache, dass Sie niemanden erreichen konnten, der nicht in der Nähe seines Heim-Telefons war, nie gekannt. Sie kannten immer schon Mobiltelefone und besitzen wahrscheinlich selbst eins oder zwei. Nun können Sie Ihren Computer in dieselbe drahtlose Welt überführen und sich von denselben Einschränkungen, eine feste, physische Verbindung haben zu müssen, befreien. Sie können auf der Terrasse sitzen und den Sonnenschein genießen, während Ihr Laptop drahtlos mit Ihrem lokalen Netzwerk und dem Internet verbunden ist. Nur ein paar Jahre früher war dies nicht möglich.

Die Risiken und die Vorteile des Wireless-Networkings

Wireless zu gehen bietet wunderbare Vorteile, aber die Wireless-Freiheit bringt auch ein paar Probleme mit sich. Sie müssen diese Vorteile und Probleme kennen, wenn Sie diese faszinierende neue Welt betreten wollen. Wie Oprah Winfrey einst sagte: »Ich glaube, dass eines der größten Risiken des Lebens ist, niemals ein Risiko einzugehen.« Was wir tun müssen, ist, kalkulierte Risiken eingehen – mit Voraussicht und intelligenter Analyse.

Was Sie riskieren

Welchen Arten von Risiken sind Sie durch Wireless-Networking ausgesetzt? Sind es mehr oder weniger Risiken als bei verkabelten Netzwerken? Kapitel 9 gibt Einblick in diese Risiken, während spätere Kapitel Lösungen bieten. Kurz gesagt, die Risiken beim Einsatz von Wireless-Netzwerken unterscheiden sich von denen bei verkabelten Netzwerken. Bei verkabelten Netzwerken hilft uns die physische Sicherheit, uns vor den Schwachstellen unserer lokalen Netzwerke zu schützen – das ist wie mit Türschlössern und Überwachungskameras. Angreifer müssen sich physisch mit dem Netzwerk verbinden, um es angreifen zu können. Nun höre ich viele von Ihnen sagen, dass dies so nicht stimmt, denn Wählverbindungen oder Remote-Access-Points bieten genügend Angriffspunkte, die sich nutzen lassen. Das stimmt, aber dies ist lediglich ein Aspekt dabei, Zugriff auf ein Netzwerk zu erlangen. Und wenn Sie Modems oder externen Zugriff verbieten, bleibt der physische Zugriff als einziger Punkt übrig. Dies ist bei Wireless nicht der Fall.

Viele von Ihnen werden sich bestimmt noch daran erinnern, wie Sie vor ein paar Jahren Fernsehantennen nutzten, um TV-Sender zu empfangen. Einige von Ihnen nutzen vermutlich immer noch Antennen. Dies ist ein Wireless-Modell. Greifen Sie zu einer Antenne, schließen Sie sie an Ihr TV-Gerät an, und los geht's! Nun können Sie dies auch mit einem Computer tun. Fügen Sie ein Wireless-Modem und eine Antenne (die Teil des Modems oder im Computer integriert sein kann) hinzu, und halten Sie Ausschau nach Wireless-Signalen, mit denen Sie sich verbinden und die Sie nutzen können. Free Wireless! Na gut, nicht wirklich. Ja, Sie können es so machen, wie wir beschrieben haben. An vielen Orten ist es allerdings illegal, Netzwerke zu benutzen, die jemand anderem gehören.

In einem Wireless-Netzwerk geben Sie Ihr Netzwerk der Welt bekannt. »Hallo? Hier bin ich. Komm und krieg mich.« Wireless-Netzwerke bitten darum, benutzt (oder missbraucht) zu werden. Und an dieser Stelle unterscheiden sie sich von Netzwerken, die auf Kabel basieren. In späteren Kapiteln werden wir beschreiben, wie Leute inhaftiert wurden, weil sie unter Verwendung von Access-Points, die ungesichert und für jedermann zugriffsbereit in der Nachbarschaft verfügbar waren, auf Pornographie zugegriffen haben. Sie wollen ganz bestimmt nicht, dass eines Tages die Polizei an Ihre Tür klopft und nach illegalem Netzwerkverkehr fragt, oder? Nun, dies ist eines der Risiken von Wireless.

Die illegale Nutzung Ihres Netzwerks ist Ihr schlimmster Alptraum. Dabei könnte es sich um die gerade eben beschriebene Situation handeln oder um einen Hacker, der in Ihr Netzwerk

eindringt, um kommerzielle Geheimnisse zu stehlen. Beides ist nicht gut. Die meisten dieser Risiken sind zurückzuführen auf ein schwaches Design und die ungenügende Nutzung der im Wireless-Netzwerk verfügbaren Sicherheitskomponenten. Teil C zeigt Ihnen, wie Sie Ihr Wireless-Netzwerk vernünftig vor Eindringlingen schützen.

Die Vorteile

Die Vorteile eines Wireless-Netzwerks können fast unermesslich sein. Wie wir vorher erwähnt haben: Können Sie sich eine Welt ohne Mobiltelefone vorstellen? Sie unterstellen fast automatisch, dass Sie Menschen jederzeit erreichen können, indem Sie sie auf ihren Mobiltelefonen anrufen. Stellen Sie sich nun vor, nicht an Ihren Schreibtisch gefesselt zu sein, um Ihre Arbeit zu erledigen. Mit den aktuellsten Tablet-PCs können Sie sich frei im Büro bewegen (Roaming), von Meeting zu Meeting, den Tablet-PC in Ihrer Hand, immer verbunden, immer verfügbar. Sie können auch in der Kantine sitzen, Ihren Kaffee trinken und dabei an einem großen Geschäftsbericht arbeiten. Oder Sie genießen ein paar Tage Sonne, die Sie vermissen würden, wenn Sie in Ihrem Büro sitzen müssten.

Stellen Sie sich vor, wie nützlich Wireless-Verbindungen in Flughäfen sein können, während Sie auf Ihren niemals pünktlichen Flug warten. Nun können Sie immerhin ein wenig Arbeit erledigen, im Internet browsen oder sich mit anderen Passagieren verbinden, um die Zeit bis zum Flug gut zu nutzen.

Die nächsten paar Jahre werden eine Revolution im Networking bringen, sowohl persönlich als auch auf den Job bezogen, denn Wireless-Networking wird *unerlässlich* werden.

Einsatzgebiete von Wireless-Netzwerken

Wo werden Sie dieses fantastische Wireless-Networking nutzen? Wir diskutieren den Einsatz in Flughäfen und im Büro – Haupteinsatzgebiete für jeden Geschäftsmann auf Reisen. Die Menge Arbeit, die zusätzlich erledigt werden kann, ist immens, was für Sie hoffentlich zu mehr Verantwortung und höherem Einkommen führt. Auf jeden Fall sollte Wireless-Networking Ihnen mehr Zeit mit der Familie einbringen. Wie bitte? Wie das? Ganz einfach: Betrachten Sie einmal die Arbeit, die Sie jeden Tag erledigen müssen, und die Deadlines, die Sie einzuhalten haben. Nun können Sie sich bereits im Zug, der Sie zum Arbeitsplatz oder nach Hause bringt, Ihrer Arbeit widmen. Oder denken Sie an all die Stunden, die Sie frustriert wartend auf Flughäfen verbringen – diese Zeit können Sie nun für Ihre Arbeit nutzen, so dass Sie mehr Zeit mit Ihrer Familie verbringen können, wenn Sie schließlich zu Hause eintreffen. Alles klar?

Der Nutzen von Wireless-Netzwerken endet hier aber noch nicht. Falls sich Bill Gates tatsächlich durchsetzen kann, werden wir die Wireless-Welt in unseren Kühlschränken, Herden, Kaffeekannen und Haus-Alarmanlagen wiederfinden. Halt! Einiges davon gibt es ja bereits.

Hier sind einige weitere Verwendungszwecke:

- ✔ **Heim- oder Bürosicherheit:** Wireless-Kameras können Sie mit Ihrer Web-Site verbinden, um das Büro visuell zu überprüfen, falls Sie nicht da sind. Wir hoffen natürlich, dass Sie diese Funktion nur nutzen, um nach Büroschluss die Räumlichkeiten zu untersuchen, um dabei beispielsweise festzustellen, ob alle Türen verschlossen sind und niemand eingebrochen ist. Natürlich kann Sie niemand daran hindern (Gesetze ausgenommen) zu überprüfen, ob Ihre Mitarbeiter tatsächlich arbeiten und keine Party veranstalten.
- ✔ **Medizin:** Stellen Sie sich einen Ort vor, an dem Ärzte einen kleinen Tablet-PC mit sich herumtragen und jederzeit und sofort Ihre medizinische Historie abrufen können. Und wenn der Arzt schon dabei ist, kann er auch gleich ein Rezept zur Apotheke senden und Ihnen damit ersparen, diese Hieroglyphen, die er *Handschrift* nennt, selbst dorthin zu tragen. Die Krankenschwestern könnten Ihre vitalen Kennzeichen in ein Wireless-Gerät eingeben, um Ärzten sofortigen Zugriff zu erlauben. Vielleicht wird der Arzt Resultate ins Labor senden, andere Ärzte um Rat fragen und Sie ganz einfach besser versorgen, weil er voll verbunden ist.
- ✔ **Live-Daten-Updates:** Daten können sofort aktualisiert werden, ohne dass darauf gewartet werden muss, dass Mitarbeiter ins Büro zurückkehren und Berichte über Inspektionen oder Verkäufe schreiben. Diese Mitarbeiter geben die Daten einfach in ihr kleines Wireless-Gerät ein und senden sie für die weitere Verarbeitung direkt zum Haupt-Computer. Das beschleunigt natürlich den Verkaufszyklus oder die Sammlung von Daten, die die Geschäftsdatenbank jeden Monat benötigt.
- ✔ **Geschäftsapplikationen:** Auf der Seite der Geschäftsapplikationen bauen Unternehmen wie Microsoft, Peoplesoft und SAP Wireless direkt in ihre Produkte ein, um die Benutzer besser zu bedienen und die Datennutzung effektiver zu gestalten. Einige Immobilienmakler nutzen Wireless, um ihren Brokern Zugriff auf die Liste der Immobilien zu geben, was einen dramatischen Einfluss auf den Erfolg der Broker haben kann. Stellen Sie sich beispielsweise einmal vor, dass ein Kunde einen Besichtigungstermin für einen bestimmten Haustyp vereinbart, beispielsweise Bungalows, und der Broker nun mit einer Liste von Immobilien erscheint, die diesem Typ genau entsprechen. Nehmen Sie nun an, dass der Kunde nach einem Blick auf die verfügbaren Häuser seine Meinung ändert und doch lieber ein Zweifamilienhaus haben möchte. Der Broker kann nun sofort in seinem Wireless-Gerät eine neue Suche starten, statt einen neuen Termin mit dem Kunden vereinbaren zu müssen. Zack, Sofortverkauf.

Die Nutzung von Wireless-Netzwerken wird in den nächsten paar Jahren wie eine Rakete abgehen. Mehr und mehr Hersteller werden das Konzept in ihre Angebote integrieren, uns von unseren Schreibtischen oder den manuellen Methoden der Eingabe neuer Daten in unsere Systeme zu befreien.

Die Netze sortieren: Brauche ich ein WPAN, WLAN oder WMAN?

Akronyme sind die Kennzeichen aller Profis. Sei es eine Krankenschwester oder ein Doktor, die oder der nach einem EKG fragt, oder ein Buchhalter, der über ROI diskutiert, Sie müssen schon die Fachsprache kennen, um mitreden zu können. So ist es auch mit Wireless-Netzwerken.

Es gibt eine Reihe unterschiedlicher Typen von Netzwerken, deren Klassifizierungen sich primär nach den jeweils überbrückbaren Distanzen richten. Tabelle 1.1 zeigt, in welcher Beziehung sie zur verdrahteten Welt und untereinander stehen.

Netzwerktyp	Verdrahtet	Wireless
LAN	IEEE 802.3 (Ethernet)	IEEE 802.11x
WAN	IEEE 1394 USB	IEEE 802.15.1 IEEE 802.15.3 IEEE 802.15.4
MAN	Breitband (DSL, Kabel)	IEEE 802.16

Tabelle 1.1: Verschiedene Netzwerktypen

Das IEEE (Institute of Electrical and Electronics Engineers) bietet Standards, denen jeder folgen sollte. Dies beinhaltet Standards für verdrahtete und Wireless-Netzwerke. Die durch IEEE vergebenen Nummern werden schnell unter den Industriebenutzern bekannt. Die 802-Serie schreibt vor, wie jedes Format arbeiten muss. Auf zahlreichen Web-Sites finden Sie interessante Informationen über diese Standards und deren Nutzung. Eine dieser Web-Sites ist `www.dailywireless.org/index.php`. Diese Site informiert aktuell darüber, was in der Wireless-Welt los ist.

Beeindrucken Sie Ihre Freunde dadurch, dass Sie den 802.11-Standard erwähnen, den Ihr Wireless-Netzwerk nutzt. Dabei handelt es sich entweder um a, b oder g. 802.11b ist gegenwärtig der populärste Standard, aber 802.11g holt schnell auf.

Werden wir persönlich: WPAN

Das *Wireless Personal Area Network (WPAN)* besteht aus Wireless-Aktivitäten geringer Reichweite, beispielsweise Bluetooth und FireWire. Wireless mit dieser Reichweite basiert auf dem Standard IEEE 802.15. Die Übertragungen in diesen Netzwerken erreichen etwa 10 Meter. Es handelt sich also um Ihre unmittelbare, persönliche Umgebung. Das Netzwerk verbraucht sehr wenig Strom und ist ein Ad-hoc-Netzwerk. Falls Sie sich innerhalb der Reichweite befinden und ein anderes Gerät existiert, können Sie die Hand ausstrecken und es berühren.

Dieses Spektrum ist für interpersonelle Verbindungen entworfen, beispielsweise für die Verbindung zweier PDAs oder den Anschluss einer Wireless-Tastatur, -Maus oder eines Wireless-Dru-

ckers an Ihren Computer. Das ist nützlich und hilft Ihnen, sich von all den Kabeln zu befreien, die typischerweise zur Durchführung dieser Aufgaben benötigt werden. Datenübertragungen erfolgen mit rund 1 MBit/s im Bluetooth-Protokoll.

Viele von Ihnen schwelgen bereits in der Wireless-Personal-Area-Network-Welt, beispielsweise mit Ihren mit Infrarot ausgestatteten PDAs, die Sie dazu benutzen, um Informationen zu anderen PDA-Nutzern zu beamen. Andere laufen auf Flughäfen mit Bluetooth-Headsets für ihre Mobiltelefone herum. Das gefällt uns. Das schlägt dieses dumme Kabel, das blöd um den Hals hängt, um Längen. Wir sind allerdings nicht sicher, ob Sie bemerken, wie viele Leute glauben, dass Sie mit ihnen reden, statt zu telefonieren.

Ein anderes nettes Einsatzgebiet dieses Spektrums ist die Verbindung Ihres PDAs mit Ihrer Arbeitsstation oder Ihrem Laptop zum Zwecke der Datensynchronisierung. Oder der Anschluss eines Bluetooth-fähigen Modems. Warum ein Bluetooth-Modem? Nun, wenn Sie reisen, können Sie sich in Ihrem Hotel mit einer Wählleitung verbinden. Viele Hotels wechseln zur Wireless-Connectivity, aber ebenso viele sind noch nicht dort angekommen. Die Verwendung eines Bluetooth-Modems bietet Ihnen also einen Grad dieser Wireless-Connectivity, während Sie durch Ihr Hotelzimmer wandern oder sogar auf den Balkon treten – Sie bleiben die ganze Zeit lang verbunden.

Ein weiteres Einsatzgebiet dieses Spektrums ist die Verbindung mit anderen Laptop-Benutzern, um schnell und einfach und ohne Netzwerkkarten und -kabel Daten auszutauschen. Sie können dies zwar auch mit WLAN-Technologie tun, aber der Einsatz von Infrarot erlaubt Ihnen einen schnellen Dateiaustausch mit anderen Benutzer mit geringem Aufwand und ohne Trouble.

Ein schneller Hinweis zur Klarstellung: Bei Personal Area Networks (PAN) geht es tatsächlich um die Nutzung eines nahen elektrischen Feldes zum Senden von Daten über unterschiedliche Geräte mit dem Körper als Medium. Die Bezeichnung war wirklich so gemeint, wie sie in Wireless Personal Area Networks benutzt wird. Trotzdem ist es heute eine akzeptierte und wechselhaft gebrauchte Bezeichnung. Wenn Sie einen Artikel lesen wollen, der die ursprüngliche Nutzung beschreibt, dann besuchen Sie `www.wirelessdevnet.com/channels/bluetooth/features/pans.html`, die Web-Site eines Wireless-Entwicklers.

Der heilige Gral des Wireless-Networkings: WLAN

WLAN ist für den größten Teil der Geschäftswelt der heilige Gral des Wireless-Networkings. Unter Verwendung des Standards IEEE 802.11 ist das WLAN der Hauptbetrachtungsgegenstand dieses Buchs. Wireless Local Area Networking (WLAN) verbindet Ihren Laptop oder Tablet-PC mit Ihrem Büro und erlaubt Ihnen die freie Bewegung (Roaming) bei der Arbeit, während Sie verbunden bleiben. Bald werden Sie in der Lage sein, Ihrem Boss zu sagen, dass Sie arbeiten, während Sie tatsächlich beim Cola-Automaten stehen und mit der netten Kollegin (oder dem Kollegen) oder Freunden plaudern. Guck, Boss, ich lade gerade den neuen Verkaufsbericht runter und diskutiere ihn mit Silvia, während ich meinen Durst stille.

Hierher stammt der Begriff Wi-Fi, der manchmal stellvertretend für den Standard IEEE 802.11 gebraucht wird. Die Wireless-Connectivity dehnt sich über Ihren Schreibtisch hinweg weiter aus. Distanzen bis zu etwas mehr als 150 m lassen sich ohne störende Interferenzen erreichen. Mit Repeatern und zusätzlichen Access-Points sind sogar noch größere Distanzen möglich. Wir werden Ihnen mit diesem Buch helfen, die Protokolle zu verstehen, Sicherheit zu implementierten und vieles mehr.

Vermutlich interessiert Sie das WLAN am meisten. Wir konzentrieren uns in diesem Buch also darauf. Ein Wireless Local Area Network entspricht dem verdrahteten Local Area Network, das Sie jeden Tag in Ihrem Büro oder vielleicht sogar zu Hause benutzen. Es ist im Wesentlichen eine Verbindung von Geräten, die es erlaubt, Ressourcen gemeinsam zu benutzen. WLANs sind nützlich, weil Sie bei der Installation von Kabelproblemen befreit werden. Außerdem müssen Sie keine Löcher mehr bohren, um Kabel durch Wände zu verlegen.

Besonders für kleine und mittlere Unternehmen kann dies vorteilhaft sein, weil solche Unternehmen möglicherweise ihre Geschäftsräume nur gemietet haben. In solchen Fällen ist es sicher keine einfache Entscheidung, zahlreiche Löcher zu bohren oder den Fußboden aufzureißen, um Kabel zu verlegen. Ein richtig konfiguriertes und geschütztes WLAN bietet unvergleichbaren Zugriff, ohne dass Sie sich um solche Probleme kümmern müssen. Sie können ein WLAN nutzen, um Ihr Netzwerk über die Wände und Decken Ihres Gebäudes hinweg auszudehnen, vielleicht bis zu einem angrenzenden Konferenzraum oder zur Kantine. So können Ihre Mitarbeiter selbst dann noch zugreifen, wenn sie ihr Mittagessen zu sich nehmen.

Natürlich muss man sich über einige Dinge Gedanken machen, und die Sicherheit ist enorm wichtig. Richtig konfiguriert befreit Sie ein WLAN allerdings. Sie können Gebiete der Connectivity entdecken, an die Sie noch niemals zuvor gedacht haben.

Wo das Gummi die Straße berührt: WMAN

Das *Wireless Metropolitan Area Network*, kurz *WMAN*, wird manchmal auch als *Wi-Max* oder *WirelessMan* bezeichnet. Hier sind die erreichbaren Distanzen sehr viel größer als bei den zuvor erwähnten Standards. Basierend auf dem Standard IEEE 802.16 bietet das WMAN große Distanzen und hohe Zugriffsgeschwindigkeiten. Dieser Standard konzentriert sich auf die effiziente Nutzung der Bandbreite im 10- bis 66-GHz-Bereich. Eine Erweiterung des Standards, 802.16a, erlaubt den Zugriff auch im 2- bis 11-GHz-Bereich.

Das WMAN bietet Wireless-Zugriff auf Gebäude durch Nutzung externer Antennen, die auf zentrale Basisstationen zugreifen. Das WLAN ist großartig für ein Gebäude oder ein paar Etagen, aber falls Ihre Organisation groß ist und sich über mehrere geografisch voneinander getrennte Gebäude erstreckt, benötigen Sie vielleicht die zusätzliche Distanz, die WMAN bietet. Ein Vorteil dieses Protokolls ist, dass es Quality-of-Service (QoS) erlaubt, um den Nutzen im Geschäft weiter zu erhöhen. Dies erlaubt einem Verkäufer, einen bestimmten Grad von Service zu garantieren. Natürlich können Sie von einem der Anbieter, die WMANs installiert haben, einfach nur Platz in einem solchen Netzwerk kaufen. Das Unternehmen VeriLAN (`www.verilan.com`) stellte einen solchen Service beispielsweise erstmals 2004 zur Verfügung.

Ein neuerer Standard ist 802.20. Dieser Standard bietet Connectivity-Geschwindigkeiten von bis zu 1 MBit/s für Kraftfahrzeugverkehr, der mit einer Geschwindigkeit von bis zu 250 km/h unterwegs ist. Das ist cool: Nun können Sie nicht nur mit überhöhter Geschwindigkeit über die Autobahn fliegen, Sie können dabei auch noch mit einem Wireless-Netzwerk verbunden sein. Wir vermuten, dass die Polizei an diesem spezifischen Band besonders interessiert ist.

Wireless-Netzwerke nutzen

Ein Wireless-Netzwerk zu nutzen erfordert eine Anzahl Komponenten und kritisches Denken, bevor dem ersten Benutzer erlaubt wird, sich zu verbinden. In den nächsten paar Abschnitten werden wir diese Komponenten besprechen.

Auf Netzwerke zugreifen

Für den Zugriff auf ein Wireless-Netzwerk brauchen Sie Werkzeuge. Sie müssen außerdem die gewünschten Distanzen und Übertragungsgeschwindigkeiten berücksichtigen, um die richtige Technik auszuwählen. Um es kurz zusammenzufassen: Es gilt, an einige miteinander konkurrierende Standards zu denken. Tabelle 1.2 zeigt die populärsten Standards.

Standard	Was er bedeutet
802.11a	54 MBit/s Geschwindigkeit im 5-GHz-Band
802.11b	11 MBit/s Geschwindigkeit im 2,4-GHz-Band
802.11g	54 MBit/s, rückwärtskompatibel zu 802.11b
802.15	Personal-Area-Network-Standard. Bluetooth ist der typische Name

Tabelle 1.2: Populäre Wireless-Standards

Es existieren noch viele weitere Standards. Sie finden eine Liste aller Standards im Anhang B, aber die in Tabelle 1.2 gezeigten sind die populärsten. Um sie zu nutzen, muss Ihre Netzwerkkarte den Standard unterstützen – natürlich gemeinsam mit Ihrem Wireless-Access-Point. Sobald Sie Ihrer Maschine oder Ihrem PDA eine Wireless-Netzwerkkarte hinzugefügt haben, können Sie loslegen und Mobilität genießen, während Sie mit dem Netzwerk verbunden bleiben.

Abhängig davon, welchen Wireless-Standard Sie nutzen, kann sich Ihr Roaming über die Büroetage oder das gesamte Gebäude einschließlich Parkplatz ausdehnen. In einem der folgenden Kapitel werden wir einiges zu den Nachteilen sagen.

Das Netzwerk erweitern

Nun, da Sie verbunden sind, könnte Ihnen in den Sinn kommen, dass Sie diesen Grad an Zugriff gerne auch an anderen Standorten hätten. Diese Freiheit ist ansteckend. Um dies in die Tat

umzusetzen, müssen Sie entweder das Netzwerk erweitern oder Ihre Fähigkeit, das aktuelle Netzwerk zu erreichen.

Eine einfache Methode zur Ausdehnung Ihrer Reichweite ist, Ihre Antenne zu verbessern. Ihre Netzwerkkarte nutzt normalerweise eine kleine Antenne, die entweder gleich auf der Karte untergebracht ist oder sich irgendwo im Computer befindet. Letzteres ist bei einem Centrino- oder AirPort-Chipset der Fall. Das funktioniert großartig für die in Ihrem Wireless-Netzwerk typischen Distanzen, ist bei größeren Distanzen aber problematisch. Durch Hinzufügen einer High-gain-Antenne zu Ihrem Computer oder PDA verbessern Sie signifikant Ihre Fähigkeit, das Netzwerk aus wesentlich größeren Entfernungen zu erreichen.

Die alternative Methode ist, Ihr Netzwerk unter Verwendung von Repeatern und zusätzlichen Access-Points zu erweitern. An dieser Stelle ist Planung effektiv, um zu gewährleisten, dass Sie Ihre Anforderungen schon vor dem Start kennen, um dann die zur Erfüllung dieser Anforderungen notwendige Technik implementieren zu können.

Gebäude miteinander verbinden

Vielleicht möchten Sie, dass alle Gebäude Ihres Unternehmens über ein nahtloses Netzwerk unter Verwendung von Wireless-Frequenzen miteinander verbunden sind. Sie können dies mit mehreren Methoden tun, einige davon sind richtig fortschrittliche Methoden, die sich empfehlen, wenn Ihre Gebäude sehr weit voneinander entfernt liegen.

Die Verbindung von Netzwerken, die sich in unterschiedlichen Gebäuden befinden, führt zu wichtigen Vorteilen. Beispielsweise braucht ein Benutzer, der auf Daten zugreifen muss, die sich in einer zentralen Ressource im anderen Gebäude befinden, nicht mehr quer über den Parkplatz zu diesem Gebäude zu laufen.

Zwei übliche Methoden zum Überbrücken dieser Lücke sind Point-to-Point- und Point-to-Multipoint-LAN-Brücken. Mit diesen Techniken kann sich Ihr Wireless-Netzwerk von einem Raum über ein Gebäude, über mehrere Gebäude oder gar über die ganze Stadt hinweg ausdehnen. Dies ist allerdings eine komplexe Implementation, und vermutlich etwas, was die Leute, für die dieses Buch geschrieben ist, kaum nutzen werden. Abbildung 1.1 zeigt, wie jede Brücke funktioniert.

Mobil werden

Wie es in dem Song heißt: »We're on the road again.« Wir reisen ganz schön viel, und Zugriff auf unsere E-Mails und unser Büro zu erhalten, ist sehr wichtig. Meistens erhalten wir Zugriff über einen lokalen Anruf bei unserem Netzwerk-Service-Provider. Diesen Zugriff nutzen wir dann für den Brückenschlag zu unserem Büro, und schließlich sind wir verbunden.

Aus Sicherheitsgründen nutzt Peter einen verschlüsselten Tunnel für den Zugriff auf sein Heimbüro. Nachdem er verbunden ist, kann er leicht auf alle seine Maschinen zugreifen und alle gewünschten Dateien laden. Auf diesem Weg bleibt alles, was er tut, fremden Augen verborgen.

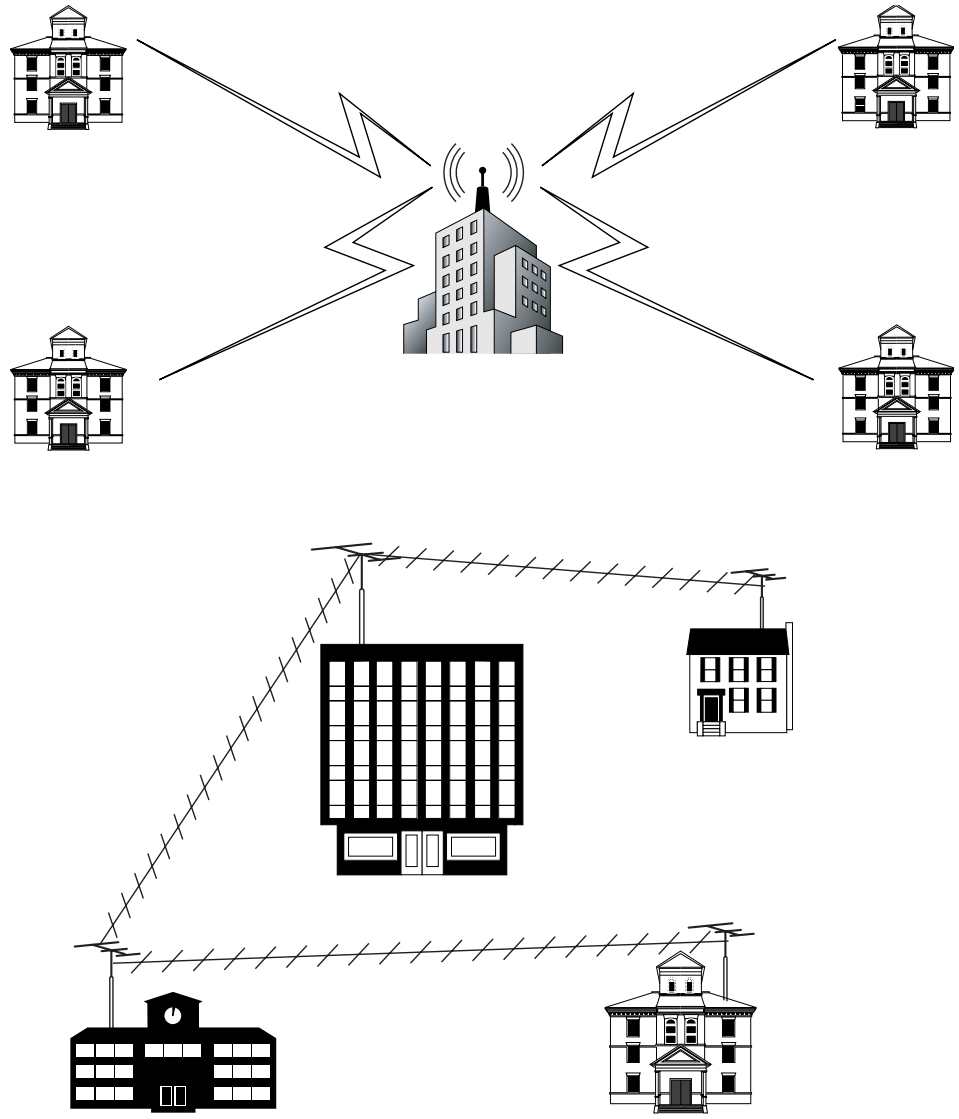


Abbildung 1.1: Point-to-Point-Netzwerk-Brücke (oben) und Point-to-Multipoint-Netzwerk-Brücke (unten)

Eine Sache, die sich ändert, ist der reduzierte Bedarf an festnetzbasierten Telefonleitungen beziehungsweise deren Anbieter (z. B. Telecom). Da zunehmend mehr Hotels, Flughäfen und Cafés Wireless-Access-Hotspots installieren, wird es leichter und leichter, uns zu verbinden. »Kannst du mich hören?« Die Antwort lautet immer häufiger »Ja!«.

Es gibt zahlreiche Utilities wie Boingo, die Wireless-Zugriff weltweit in Cafés, Restaurants und Hotels bieten. Sich zu verbinden, wenn man mobil ist, ist oft sehr einfach. Boingo bietet kostenlose Software, die Wireless-Netzwerk-Hotspots findet und die Verbindung für Sie herstellt. Sie zahlen Boingo eine Gebühr für den Zugriff auf deren *Hotspots* irgendwo in der Welt.

Die Post auf den Weg bringen

Ein offensichtliches Bedürfnis mobiler Reisender ist der Zugriff auf ihre E-Mail. Wo wären wir ohne E-Mail? Auch dies wird immer einfacher. Vor Jahren schleppte Monika Krokodilklemmen und ein langes, an einem Ende abisoliertes Telefonkabel mit sich herum. Damit konnte sich Monika in fremden Ländern, in denen Datenzugriff eingeschränkt oder nicht existent war, mit dem Telefonsystem verbinden. Obwohl sich dies natürlich inzwischen geändert hat und fast jedes Hotel-Telefonsystem Modemzugriff gestattet, beginnt Wireless, sich durchzusetzen und zur Norm zu werden. Das ist sicherlich einfacher, als Kabel aus der Wand zu reißen, um sich zu verbinden!

Sobald Sie über einen Wireless-Access-Point Zugriff auf das Internet haben, ist der Abruf Ihrer E-Mail ein Kinderspiel. Ideal ist noch immer, ein Virtual-Private-Network (VPN) zu nutzen, damit Ihre E-Mail und Ihre Passworte nicht im Klartext das Netzwerk passieren, sondern durch einen verschlüsselten Tunnel. In der Wireless-Welt ist das sogar noch wichtiger, denn diese Netzwerke sind viel anfälliger dafür, dass jemand im selben Netzwerk den Verkehr durchschnüffelt und sieht, was Sie gerade so machen.

Eine andere Methode ist die Verwendung eines PDAs, beispielsweise des neuen Treo 600 oder Blackberry, für den Zugriff auf Ihre E-Mail. Daten, die durch das GPRS-Netzwerk des Mobiltelefons reisen, sind etwas weniger verletzbar als solche, die über eine Wi-Fi-Verbindung wandern. Außerdem ist die Sache sehr bequem: Sie schalten einfach nur Ihr Gerät ein, verbinden sich mit dem lokalen Service-Provider, und Zack! Sie haben Post!

Lust aufs Netzwerk bekommen

Okay, Sie sind gefesselt von den Möglichkeiten und wollen Ihr eigenes Wireless-Netzwerk haben. Als Besitzer einer kleinen Firma können Sie es sich nicht leisten, jemanden mit der Installation und Pflege dieses Netzwerks zu beauftragen. Sie müssen also verstehen, wie Sie diese Sache selbst bewerkstelligen können.

Es ist eine Sache, sich etwas zu wünschen, aber eine völlig andere, es auf nützliche und sichere Art zu erhalten. Sie müssen bestimmte Schritte ausführen, um Ihr Geschäft und Ihre Wireless-Investition zu schützen. *Planung*, diese von vielen als unangenehm empfundene Beschäftigung, ist absolut notwendig.

Ihr Wireless-Netzwerk planen

Im Kapitel 2 finden Sie alles, was Sie für die Erstellung eines Plans für Ihr neues Wireless-Netzwerk brauchen. Wir können es nicht häufig genug wiederholen: *Überspringen Sie dieses Kapitel nicht*. Eine Wireless-Lösung zu implementieren kann so einfach sein, wie einen Access-Point in Ihrem Netzwerk zu installieren und Ihre Mitarbeiter sofort darauf zugreifen zu lassen.

Aber selbst bei diesem einfachen Ansatz gibt es ein paar Probleme. Wo werden Sie den Access-Point hinstellen? Viel zu viele Organisationen platzieren ihn innerhalb des Netzwerks – was die falsche Stelle für eine Wireless-Verbindung ist. Ihr Netzwerk muss vor jedem potenziellen Wireless-Angriff geschützt werden, und darum muss der Zugriff auf der Außenseite Ihrer Firewall stattfinden, was die Benutzer dazu zwingt, ihre Identitäten zu authentifizieren, bevor sie Zugriff auf das interne Netzwerk erlangen.

Wo wird der Wireless-Zugriff gebraucht? Es ergibt wenig Sinn, ihn im Hauptbüro zu platzieren, wenn die Gebäudestruktur verhindert, dass das Signal das gewünschte Publikum erreicht. Schließlich müssen Sie den erforderlichen Grad an Sicherheit konfigurieren, der gewährleistet, dass nur autorisierte Benutzer zugreifen können.

Ihr Wireless-Netzwerk installieren

Abhängig von der Größe Ihres Wireless-Netzwerks kann die Installation desselben so einfach sein, wie einen Access-Point auf den Tisch zu stellen oder an die Wand zu schrauben und ihn mit der Stromquelle zu verbinden. Allerdings kann es ebenso gut notwendig sein, ein komplexeres System zu installieren, das Repeater, Router und externe Antennen verwendet. Vorsichtige Platzierung und Installation sind erforderlich, um zu gewährleisten, dass alle Ihre Anforderungen erfüllt werden und Sie fehlerfreie Connectivity erhalten.

Wenn Sie die Planung der Installation abgeschlossen haben, werden Sie mit der Installation beginnen müssen. Wenn Sie dies tun, werden Sie einer gewissen Struktur folgen wollen, um die Implementation reibungslos durchzuführen. Schauen Sie sich zunächst noch einmal Ihren Plan an, um zu sehen, ob er vollständig ist. Packen Sie dann das Equipment aus, das Sie installieren wollen, und überprüfen Sie, ob alle Teile da sind und nichts beschädigt ist. Verbinden Sie dann alle Teile. Für einen Access-Point bedeutet dies im Normalfall, dass Sie die externe Antenne, die mit dem Gerät geliefert wurde, hinzufügen. Vielleicht installieren Sie aber externe High-gain-Antennen, die sich auf dem Dach befinden müssen. Was kommt zuerst? Das Huhn oder das Ei? Installieren Sie die Antenne und die Verkabelung und schließen Sie sie dann an den Access-Point an.

Installieren Sie weitere Access-Points und Repeater, so, wie es Ihr Plan vorsieht. Installieren Sie dann Wireless-Netzwerkkarten in ein paar Laptops, damit Sie den Zugriff testen können, nachdem Sie das Netzwerk konfiguriert und geschützt haben. Nachdem sämtliche Hardware an ihrem Platz ist, müssen Sie das Netzwerk konfigurieren.

Ein Wireless-Netzwerk konfigurieren

Nachdem alle Access-Points installiert sind, müssen Sie das Netzwerk konfigurieren. Durch die Konfiguration des Netzwerks richten Sie die Software und alle ihre Komponenten so ein, dass ein Wireless-Signal klar übertragen wird und Ihre Netzwerkkarten darauf zugreifen können.

Die Konfiguration umfasst eine Reihe von Aktivitäten. Dazu gehört die Einstellung der Grundparameter, die dem Access-Point und den Netzwerkkarten die Kommunikation erlauben, womit gewissermaßen Ihr Einstieg in die Wireless-Welt beginnt. Andere Punkte sehen Sie in Tabelle 1.3.

Parameter	Beschreibung
Stellen Sie Ihre IP-Adresse ein	Sie müssen die IP-Adresse Ihrer Netzwerkkarte einstellen, damit sie den Access-Point erkennt.
Testen Sie die Verbindung mit dem Befehl `ping`.	Verwenden Sie diesen Befehl, um zu überprüfen, dass Sie den Access-Point erreichen können.
Öffnen Sie die Administrationsmenüs	Um Geräteparameter einzustellen, müssen Sie das Hauptmenü des Geräts öffnen. Geben Sie die vom Hersteller vorgegebene Benutzername/Passwort-Kombination ein, um dies durchzuführen.
Stellen Sie die Optionen ein	Sie müssen die Uhrzeit einstellen, den Remote-Zugriff ausschalten, entscheiden, ob Sie DHCP nutzen wollen oder nicht, und überprüfen, ob die IP-Adressierung Ihren Anforderungen entspricht.
Aktualisieren Sie auf die aktuellste Firmware	Dies ist wichtig. Folgen Sie den Anleitungen und besuchen Sie die Web-Site des Herstellers, um die aktuellste Firmware herunterzuladen. Damit gewährleisten Sie, dass Ihr Gerät up-to-date ist und alle Hersteller-Patches implementiert sind.

Tabelle 1.3: Konfigurieren des Wireless-Netzwerks

Die Konfiguration erlaubt Ihren Geräten, sich miteinander und, falls erforderlich, mit Ihrem lokalen Netzwerk zu verbinden. Sobald dies erledigt ist, müssen Sie noch sicherstellen, dass Ihre Verbindungen sicher sind.

In der Wireless-Welt sicher bleiben

Ihr Netzwerk zu schützen oder zu sichern ist der wichtigste Teil Ihres Wireless-Ausflugs. Überspringen Sie diesen Punkt trotz all Ihrer Freude, mit dem Wireless-Netzwerk verbunden zu sein, bloß nicht. Es gibt in diesem neuen wilden Wilden Westen viele Risiken für Ihr Netzwerk, Ihre Benutzer und Ihre Daten. Die Risiken haben mitunter seltsame Namen, beispielsweise War Driving und War Flying. Sie hatten keine Ahnung, dass Sie eine besonders geheimnisvolle Welt der Kriegsführung betreten, oder?

War Driving und *War Flying* sind Übungen, bei denen jemand, der mit spezieller Software, einem Laptop mit Wireless-Netzwerkkarte und einer externen Antenne ausgerüstet ist, herumfährt oder sogar herumfliegt. Mit Hilfe dieses Equipments wird er oder sie Ihr Wireless-Netzwerk finden und ausprobieren, ob Sie Sicherheit verwenden. Sie bieten eine offene Tür, wenn Sie diese Schritte überspringen und keine Sicherheit einrichten.

Andere Risiken sind Diebstahl und Datenverlust. Unter Verwendung dieses ungeschützten Wireless-Access-Points stehlen Eindringlinge Kreditkarten-Nummern, Adressen und sogar Pass-Codes, falls Sie diese auf einem Computer irgendwo in Ihrem Netzwerk speichern. Diese Leute werden vielleicht sogar Ihr spezielles Rezept für frittiertes Hühnchen stehlen, mit dem Sie eigentlich Kentucky Fried Chicken Konkurrenz machen wollten.

Glücklicherweise gibt es einige Dinge, die Sie tun können, um Sicherheitsverletzungen zu verhindern oder den Einbruch in Ihr Netzwerk wenigstens zu erschweren. Es beginnt mit dem Einschalten von Verschlüsselung und dem Nutzen von Techniken wie Extended-Authentication-Protocols (EAP), um zu gewährleisten, dass sich nur autorisierte Benutzer mit Ihrem Netzwerk verbinden. Die Zugriffssicherheit können Sie schließlich wirklich verbessern, wenn Sie eine Virtual-Private-Networking (VPN) genannte Technik einsetzen. Wir werden Sie mit Schritt-für-Schritt-Prozeduren und detaillierten Diskussionen in späteren Kapiteln durch alle diese Dinge führen.

Ein Wireless-Netzwerk administrieren und pflegen

Nachdem Ihr Wireless-Netzwerk sicher eingerichtet ist, werden Sie es jederzeit benutzen wollen. Warum auch nicht? Dies ist ein guter Grund für die Implementation eines Wireless-Netzwerks. Befreien Sie sich selbst und bewegen Sie sich mit Ihrer Maschine, während Sie mit dem Netzwerk verbunden bleiben, sei es im Konferenzraum oder im Park.

All dies hat natürlich seinen Preis, denn nichts ist permanent, und alles verlangt einen gewissen Grad Administration und Pflege. Abhängig von der Größe Ihrer Client-Basis kann sich eine MAC-Filterung genannte Technik als sehr zeitraubend erweisen. Sie müssen Listen aller verwendeten MAC-Adressen und der korrespondierenden Netzwerkkarten pflegen, um deren Nutzung nachverfolgen zu können. Und Änderungen sind notwendig, wenn die Netzwerkkarte eines Benutzers ausfällt oder Laptops ihre Besitzer wechseln und nicht länger Zugriff benötigen.

Das Troubleshooting, also die Fehlersuche in jeder Art Netzwerk, erfordert konstante Beobachtung und Analysen. In der Wireless-Welt gibt es Probleme wie die sich ändernden *Fresnel-Zonen*, wo Objekte Ihr Signal blockieren. Ein anderer Punkt, der permanenter Pflege bedarf, könnte der Free-Space-Loss sein, bei dem das sich ändernde Wetter Signalverluste zur Folge hat. Außerdem müssen Sie natürlich die typischen und abnormalen Verkehrslasten kennen. Benutzer, die plötzlich riesige Dateien herunterladen (Ihre Benutzer würden doch niemals Musik herunterladen, oder?), können das Netzwerk enorm verlangsamen. Jemand muss aufpassen und Maßnahmen ergreifen, die solche Performance-Einbrüche verhindern, damit jeder fröhlich bleibt.

In diesem Buch werden wir Ihnen viele Werkzeuge und einige Techniken zum Management eines laufenden Wireless-Netzwerks vorstellen. Sie müssen Ihre Benutzer glücklich halten, so glücklich, wie sie waren, als sie sich das erste Mal mit dem Wireless-Netzwerk verbunden und die Freiheit entdeckt haben.

Konvergenz der Wireless-Technologien – Was wird die Zukunft bringen?

Wo werden wir in den nächsten paar Jahren sein? Das weiß niemand so richtig. Wir können aber qualifizierte Vermutungen äußern. Bereits heute sehen wir eine große Zunahme der Verwendung von Wireless-Technologien. Wo wir noch vor wenigen Jahren im Hotel einchecken, das Telefon suchten und unser Modem anschlossen, schauen wir uns nun zuerst nach einer Wireless-Verbindung um. Klaus nutzt seinen Treo-600, um E-Mail zu senden und zu empfangen, zu Hause anzurufen und im Web zu surfen.

Dies ist ein Gebiet, in dem Wireless-Konvergenz in Zukunft abgehen wird wie eine Rakete. Wir erwarten, dass alle großen Hotelketten innerhalb der nächsten drei bis vier Jahre komplett wireless sein werden. Laut einer durch Ipsos-Insight durchgeführten Studie von Internet-Trend wuchs die Wireless-Internet-Nutzung in 2003 um 145 Prozent mit 79 Millionen eindeutigen Besuchern. Die Studie sagt, dass knapp 40 Prozent der Menschen mit verkabeltem Internet-Anschluss Wireless-Netzwerke ausprobiert haben. Wir gehen davon aus, dass diese Zahlen in den kommenden Jahren noch übertroffen werden.

In Flughäfen werden Ihre Verbindungen über das Wireless-Netzwerk bekannt gegeben werden. Sie werden Informationen über Verspätungen oder Ankünfte in Echtzeit erhalten. Nicht länger werden Sie sich fragen müssen, was eigentlich los ist, wenn sich Ihr Flug verspätet.

Wireless-Connectivity wird weiter wachsen und immer tiefer in unsere Leben eindringen. Schauen Sie nach Wireless-Sicherheitssystemen für zu Hause und im Büro – gemeinsam mit Instant-Messaging und Web-Seiten-Fotos werden diese Systeme mehr Sicherheit bieten und Einbrüche schneller erkennen. Damit brauchen Sie vielleicht nicht mehr mitten in der Nacht aufzustehen, um auf einen Alarm im Büro zu reagieren. In den nächsten paar Jahren werden Sie sich vielleicht einfach anmelden und einen möglichen Einbruch über Remote-Kameras verifizieren, bevor Sie sich anziehen und ins Büro fahren. Ein Freund von uns hat kürzlich eine Web-Kamera in seinem Wochenendhaus installiert. Nun kann er sich mit dem Internet verbinden, seine Home-Page aufrufen und online nachsehen, ob es geschneit hat oder ob jemand eingebrochen ist. Das ist super, denn das Wochenendhaus ist zwei Stunden Fahrtzeit entfernt.