Ein Verlagsbeihefter der Heise Zeitschriften Verlag GmbH & Co. KG

extra

Networking

Schwerpunkt: Wireless LANs

Veranstaltungen

Februar 2008, Zürich/Düsseldorf/München
Kerberos – LDAP – Active Directory
www.ix-konferenz.de

28. – 29. Januar 2008, Augsburg
8. Konferenz Mobile Commerce
www.wi-mobile.de/18.0.html

19. – 21. Februar 2008, Düsseldorf
EMV 2008
www.mesago.de/de/EMV/main.htm

4. – 9. März, Hannover
Cebit 2008
www.cebit.de

7. – 10. April 2008, Orlando, Florida
Storage Networking World USA Spring 2008
www.snwusa.com

Herbst 2008, Ort steht noch nicht fest
10. Wireless Technologies Kongress 2008
www.mesago.de/de/WT/main.htm

iX extra Networking zum Nachschlagen: www.heise.de/ix/extra/netzwerke.shtml

Vom Kabel befreit

Endgeräte mit WLAN-Schnittstelle

Nur wenige Neuerungen der Informationstechnik haben sich so schnell durchgesetzt wie Wireless LANs. Nach relativ kurzer Zeit am Markt sind sie heute allgegenwärtig. Und die Entwicklung geht rasant weiter – mit schnellerer Datenübertragung, komfortablerer Benutzung und hin zu neuen Anwendungsfeldern.

Bezeichnend für die rasante Entwicklung der WLANs ist, dass praktisch alle Pioniere – wie Aironet, Lucent, Proxim, Symbol – nicht mehr als selbstständige Firma existieren. Wohl aber deren Technik und weiterentwickelte Produkte. Denn mehrheitlich wurden sie von Schwergewichten der Branche übernommen: Symbol von Motorola, Aironet von Cisco, Lucent fusionierte mit Alcatel, und Proxim gehört heute zu Terabeam. Da alle Netzwerkhersteller WLAN-Komponenten im Programm haben und fertige Chipsets den einfachen Einbau in Endgeräte ermöglichen, haben es Spezialhersteller zunehmend schwer und fungieren entweder als OEM-Zulieferer (wie Trapeze Networks für Nortel oder Aruba Networks für Alcatel-Lucent) oder spezialisieren sich auf zusätzliche Software oder Services.

Obwohl Wireless Local Area Network als Oberbegriff für alle drahtlosen lokalen Datennetze stehen kann, wird er umgangssprachlich nur noch auf Funknetze nach IEEE 802.11 angewendet – in seinen verschiedenen Ausprägungen inzwischen der Standard in diesem Bereich. Vom Institute of Electrical and Electronics Engineers (IEEE) verabschiedet, gibt es inzwischen etwa zwei Dutzend Unterstandards, von denen vor allem drei von Bedeutung sind: 802.11b mit 11 MBit/s im Frequenzband von 2,4 GHz, 802.11g mit 54 MBit/s im gleichen Band und 802.11a mit 54 MBit/s im 5-GHz-Band. Da das 2,4-GHz-Band weltweit frei und ohne Lizenzen nutzbar ist, können WLANs ohne Auflagen überall aufgebaut werden. Allerdings nutzen auch andere Funktechniken diesen Bereich – von schnurlosen Telefonen über Bluetooth bis zum Mikrowellenherd. Deshalb soll die Freigabe des 5-GHz-Bandes in vielen Ländern Entlastung bringen.

Synonym für WLAN ist häufig der Begriff WiFi zu lesen, was für Wireless Fidelity steht und ein Markenname der Wireless Ethernet Compatibility Alliance (WECA) ist, einer Herstellervereinigung, die Tests und Zertifizierungen vornimmt und mit dem WiFi-Label die Einhaltung des Standards 802.11 bestätigt.

Technisch eng mit dem Ethernet (IEEE 802.3) verwandt, ist Wireless LAN nach 802.11 eine ideale Ergänzung zu drahtgebundenem Ethernet, und beides lässt sich einfach kombinieren oder auch austauschen. Den offensichtlichen

Vorteilen (Mobilität, einfache Nutzung) stehen Beschränkungen bei Geschwindigkeit und Verfügbarkeit sowie die Notwendigkeit des Einsatzes von Verschlüsselungstechniken gegenüber.

Kombigeräte beliebt

Im WLAN werden Endgeräte und Access Points (AP) unterschieden. Erstere waren bisher hauptsächlich PCs und PDAs. Ein Ad-hoc-Modus (auch Peer to Peer) sieht vor, dass zwei WLAN-Clients direkt und ohne Access Point kommunizieren. In der Praxis spielt das aber kaum eine Rolle; in der Regel erfolgt der Betrieb im sogenannten Infrastrukturmodus, also über einen Access Point. Dieser arbeitet als klassische Bridge auf OSI-Layer 2 und verbindet WLANs zumeist mit drahtgebundenem Ethernet. Gleichzeitig sorgt er als Repeater dafür, dass Clients im direkten Umfeld miteinander kommunizieren können.

Während Access Points in Unternehmensnetzen und öffentlichen WLANs in großer Zahl im Einsatz sind, wurden sie im Heimnetz zunehmend von Kombigeräten mit integriertem DSL-Router verdrängt. Nur wenn die Reichweite nicht ausreicht, kommen zusätzliche APs zum Einsatz. WLANs lassen sich zwar auch als Funkbrücke zwischen zwei Ethernet-Segmenten nutzen, doch in der Praxis besteht ihre Aufgabe fast ausschließlich in der drahtlosen Anbindung von Endgeräten, vor allem von Notebooks. Ist die Reichweite des Access Point oder Wireless Routers nicht ausreichend, sollte man als Erstes über eine leistungsstärkere Antenne nachdenken. Bleiben die Probleme, können sogenannte Range Extender die Lösung sein, die das Signal verstärkt weitersenden. Zu bedenken ist aber, dass die volle Performance nur mit zwei Sende- und Empfangseinheiten erreicht wird; bei günstigen Geräten, die über nur eine Antenne verfügen, halbiert sich der Durchsatz.

In der Regel dienen zur räumlichen Erweiterung zusätzliche Access Points, entweder per Ethernet angebunden oder drahtlos. Dazu beherrschen die meisten Geräte die Funktion WDS (Wireless Distribution System), mit der man die Netzabdeckung auf einfache Art und Weise drahtlos erweitern kann. Weitere Access Points arbeiten dabei transparent als Bridge, sodass keine Konfigurationsänderungen an den Clients nötig sind. Auch viele Router lassen sich zur Bereichserweiterung zweckentfremden, wozu sie entweder als Repeater oder als Wireless Bridge eingesetzt werden. Das ergibt beispielsweise dann Sinn, wenn Altgeräte vorhanden sind.

Das Überall-LAN

Im Wesentlichen lassen sich drei Einsatzgebiete von Wireless LANs unterscheiden: Unternehmensnetze, Heimvernetzung und öffentliche Funknetze (Hotspots). Der Aufbau von öffentlichen WLANs ist weniger von technischen Finessen als vielmehr von der Suche nach geeigneten Geschäftsmodellen geprägt.

Auf Diät: Thin APs

Service-Provider und große Firmeninstallationen mit Hunderten oder Tausenden Access Points stellen besondere Anforderungen an die WLAN-Hardware und -Software. Im Vordergrund stehen hier die Möglichkeit der Automatisierung des Betriebes und des Managements, also Hardware- und Software-Monitoring, sowie zentrale Konfiguration und Software-Updates.

Während im Heimbereich der Trend zu immer mehr Funktionen im WLAN-Router oder Access Point geht, entwickeln sich Geräte für den Firmeneinsatz gerade in die entgegengesetzte Richtung. Der Grund liegt auf der Hand: Wird im Heimnetz ein Access Point eingesetzt, so ergibt es Sinn, zusätzliche Funktionen gleich mit einzubauen; beim Einsatz von mehreren Hundert Geräten kann es aber vorteilhaft sein, diese einfach zu halten und wenn möglich die Funktionen in zentrale Komponenten zu verlagern. Von einigen Herstellern wurde dafür einmal der Begriff Thin Access Points geprägt; man findet ihn zwar nur noch selten – die Umsetzung aber schon.

Einmal nämlich wegen des Kostenaspektes, aber auch wegen des erleichterten Managements, und nicht zuletzt sind neue Funktionen möglich: das erwähnte WLAN-Roaming etwa, wofür im Access Point übergreifende Funktionen vorhanden sein müssen. Diese werden in sogenannten WLAN-Switches realisiert, an die die Access Points angeschlossen sind und die zunächst einmal grundsätzliches Layer-2-Switching erbringen – darüber hinaus aber auch eine Reihe von komplexeren Funktionen für die Konfiguration und Steuerung der Access Points, etwa Load Balancing, Quality of Service, Nutzerauthentifizierung oder Sicherheitsfunktionen.

Allein schon durch die Tatsache, dass die Access Points ihre Konfiguration bei jedem Booten vom zentralen Switch holen, erhöht die Sicherheit, denn ein abgeschraubter Access Point gibt so keine Daten preis. Alternativ zu WLAN-Switches kann zum zentralen Management von Access Points auch ein WLAN-Controller an nur einer Stelle im Netzwerk zum Einsatz kommen.

Das Konzept der Thin Clients bietet auch eine hohe Flexibilität beim Ausbau oder Upgrade von WLANs, zum Beispiel bei einem Umstieg auf neue Access Points nach 802.11n. Hier ist nicht viel mehr zu tun, als neue Access Points an die Wand zu schrauben, da alle Informationen über Konfiguration, Sicherheitseinstellungen et cetera im WLAN-Switch stecken. Je nach Hersteller findet man diese einfachen Access Points dann unter Namen wie Radio Ports, Access Ports, Air Hubs oder Mobility Points. Wie die Arbeitsteilung zwischen Acces Point und WLAN-Switches genau umgesetzt ist, variiert von Hersteller zu Hersteller. Deshalb ist Interoperabilität eher unwahrscheinlich und im Einzelfall zu prüfen.

Eine klare Einteilung in „Thin“ oder „Fat“ Access Points ist schwierig, da immer mehr sinnvolle Mischformen existieren. Waren Thin Access Points zunächst eine Entwicklung kleinerer Spezialanbieter (Airespace, Aruba, Chantry, Trapeze usw.), sind sie inzwischen durch Übernahmen und OEM-Verträge Bestandteil des Produktportfolios aller großen Netzwerkhersteller.

Da WLANs gerade dort installiert werden, wo eine weitere Verkabelung schwierig oder unmöglich ist, gilt Gleiches häufig für den Stromanschluss. Deshalb werden Access Points für den Einsatz in Unternehmen zunehmend mit Power-over-Ethernet ausgerüstet (siehe iX extra 01/2005), sodass die Stromspeisung über das angeschlossene Ethernet-Kabel erfolgt und kein separater Stromanschluss notwendig ist.

Der Begriff Hotspot fällt häufig im Zusammenhang mit öffentlichen (public) Wireless LANs, er kann sich aber auch auf jeglichen WLAN-Zugang beziehen. Das kommt daher, dass öffentliche WLANs an stark frequentierten Punkten eingerichtet werden: Flughäfen, Hotels, Gaststätten oder Tankstellen. Allerdings bedeutet das nicht unbedingt WLAN-Access im gesamten Gebäude: Auf Flughäfen reduziert sich der Empfang häufig auf die Lounges und bestimmte Bereiche; in manchen Hotels gibt es nur in der Lobby oder einer speziellen WLAN-Zone Empfang.

Da die physische Infrastruktur in der Regel nur einmal aufgebaut wird, entwickelte sich in den letzten Jahren ein regelrechter Run auf die besten Standorte – betrieben vor allem von den großen Service-Providern. Gleichzeitig stellte sich die Frage, ob eine Eigenrealisierung der Hotel- oder Gaststättenbetreiber oder ein Betreibermodell eines Service-Providers besser funktioniert. Beide Varianten sind gleichermaßen vorzufinden, aber inzwischen ist der Markt öffentlicher Hotspots schon in der Konsolidierungsphase. Bis auf wenige große Ketten arbeiten fast alle mit Provider-Lösungen. Der Hauptgrund liegt im Aufwand für den Betrieb und die Sicherheit – besonders aber für die Abrechnung. Die Service-Provider bringen hier die Möglichkeit der Abrechnung direkt über bestehende Mobilfunk- oder Internet-Accounts mit.

Auch die Provider-Landschaft hat sich inzwischen konsolidiert: Außer der Deutschen Telekom sind kaum noch andere im Hotspot-Geschäft vertreten. Vodafone als zweitgrößter Anbieter hat seine installierte Basis an den britischen Hotspot-Spezialisten The Cloud abgegeben und wickelt nur noch die Zahlungen

Futuristisch mutet die neue MIMO-Antennentechnik an – hier am WZR-G300N von Buffalo (Abb. 1).

Outdoor-Vernetzung durch Mesh-Technik

Während man WLAN-Access-Points anfangs als reinen Drahtersatz im lokalen Netz einsetzte, zeigten sich schnell die Vorteile beim Einsatz außerhalb von Gebäuden, etwa auf dem Campus, dem Werksgelände oder in einer Fußgängerzone. Speziell dafür ausgelegte sogenannte Outdoor-Geräte müssen nicht nur robust und wetterbeständig sein, sondern auch vor Diebstahl geschützt werden – und dies nicht nur mechanisch, sondern auch softwareseitig, damit ein demontierter Access Point nicht innerhalb eines Firmennetzes als Trojanisches Pferd eingesetzt werden kann. Soll ein Gebiet flächendeckend mit WLAN erschlossen werden, stellt sich meist heraus, dass nicht an allen notwendigen Stellen drahtgebundene Schnittstellen zum Anschluss der Access Points zur Verfügung stehen. Im Normalfall ist jeder Access Point direkt an das drahtgebundene LAN oder WAN angeschlossen – innerhalb von Unternehmen zumeist an einen Ethernet-Port, außerhalb an DSL, in Deutschland seltener auch an einen Kabelanschluss. Steht dies nicht zur Verfügung, liegt der Gedanke nahe, mehrere Access Points über weitere Funkfrequenzen zu verbinden. Diese Technik einer Funk-Vermaschung bezeichnet man als Meshed Networks oder kurz als Mesh. Damit lassen sich auch auf einfache Weise Ad-hoc-Netze einrichten oder die Reichweite eines bestehenden WLAN erhöhen.

Sind WLAN-Access-Points normalerweise an einen drahtgebundenen Backbone angeschlossen, so bilden sie hier selbst den Backbone. Damit halbiert sich der Durchsatz, da sich benachbarte Access Points einen Funkkanal teilen und nur halbduplex arbeiten können. Deshalb werden entsprechende Geräte in der Regel mit drei Funkteilen und Antennen ausgerüstet: eines für die Kommunikation innerhalb der Funkzelle, eines zur Verbindung zur nächsten Funkzelle und eines aus Gründen der Redundanz und Performance. Da eine gezielte Wegsuche zwischen den Knoten stattfinden muss, mutieren die einfachen Access Points zu Routern, wobei sich die klassischen Routing-Protokolle als wenig effizient erweisen.

Zudem trifft man eine Reihe von Problemen wieder, die mit dem Umstieg auf geswitchte Netze gerade gelöst schienen – etwa die Behandlung von Kollisionen und Performancegrenzen in einem Shared Medium.

Die Lösung genau dieser Probleme soll der neue Standard IEEE 802.11s bringen, mit dessen Verabschiedung 2008 gerechnet wird und der die bisher proprietären Ansätze der Hersteller – SEE-Mesh (Simple Efficient Extensible) von Intel und Cisco sowie Wi-Mesh von Philips und Nortel – zusammenführen soll. Eine der wichtigsten technischen Neuerungen ist ein neuer Routingmechanismus, der statt auf IP- auf MAC-Level arbeitet und damit die spezifischen Eigenschaften der Funkverbindung berücksichtigen kann. Daneben wird ein deterministisches Zugriffsverfahren eingesetzt, das Zeitschlitze nutzt (Mesh Deterministic Access – MDA) anstelle des konkurrierenden Zugriffs auf das Shared Medium.

Mithilfe der Mesh-Technik ist es möglich, große Gebiete flächendeckend mit einem Internetzugang zu versorgen, etwa ein Werksgelände oder einen Campus. Es gibt bereits Pläne, ganze Städte drahtlos zu vernetzen, etwa New York durch den Einbau von Access Points in die Straßenlaternen oder San Francisco als Pilotprojekt von Google und Earthlink. Technisch ist dies heute kein Problem, allerdings ist zu hinterfragen, mit welchem Geschäftsmodell das Geld verdient werden kann, das die Investitionen rechtfertigt.

Das Londoner Projekt eines 22 km langen WLAN-Bandes entlang der Themse arbeitet deshalb mit der Einblendung von Werbung, und in Paris wird das freie WLAN von der Stadtverwaltung getragen. Der Aufbau des WLAN-Netzes in San Francisco verzögert sich bereits zum wiederholten Mal, weil das ursprüngliche Geschäftsmodell überarbeitet werden soll. In Deutschland ist Empelde, ein 11 000-Seelen-Ort am Stadtrand Hannovers, seit Anfang November flächendeckend mit WLAN versehen. Der Zugang wird durch ortsansässige Supermärkte und Fachhändler finanziert und von HotSpot betrieben (www.free-hotspot.com).

ab. Hinter den geplanten 10 000 Hotspots liegt man weit zurück und setzt nur noch auf hochfrequentierte Standorte. So ist die Deutsche Telekom mit circa 9000 Hotspots in Deutschland der dominierende Anbieter – teils unter eigenen Marken (T-Mobile, T-Home, T-Online), teils aber auch als Betreiber für Hotels und Gaststätten unter deren Logo. Das Netz wird ständig erweitert; gleichzeitig gibt es einen Rückbau unprofitabler Standorte.

Das Dilemma für die Service-Provider ist, dass mit den Hotspots allein an den Entgelten für den Netzzugang verdient wird und nicht – wie ursprünglich angestrebt – mit darauf aufbauenden Diensten und Inhalten. Reiner Internetzugang unterliegt einem starken Preisverfall, auch wenn man das angesichts der Preise vieler Hotspots nicht glauben will. Während in den USA etwa die Mehrzahl der Hotspots in Hotels und Motels frei ist und oft damit geworben wird, ist dies in Deutschland eher selten.

Public WLAN hat eine so große Verbreitung erlangt, dass man auf Flughäfen und in Hotels sicher sein kann, einen Hotspot zu finden; hinzu kommen viele Restaurant- und Tankstellenketten, etwa Starbucks, McDonalds oder Tank & Rast. Möchte man wissen, wo ein drahtloser Internetzugang zur Verfügung steht, kann man sich auf den Internetseiten der Anbieter darüber informieren (etwa www.t-home.de/hotspot/standortsuche für die Hotspots der Deutschen Telekom). Noch einfacher geht es mit Portalen, die anbieterübergreifend informieren, zum Beispiel www.mobileaccess.de und www.hotspot-locations.de für internationale Standorte. Auch Intel stellt entsprechende Informationen zur Verfügung.

Ergänzung, nicht Konkurrenz

Wireless LAN ergänzt andere Funkverfahren und steht weniger, wie häufig angenommen, im Wettbewerb mit ihnen. So sorgen kombinierte Adapterkarten mit WLAN-, UMTS- und GPRS-Funktionen für nahezu lückenlosen Datenempfang. Wo verfügbar, wird der größere Durchsatz von WLAN genutzt, sonst die Flächenabdeckung von zunächst UMTS, dann GPRS. Im Bereich Voice over IP dürften nur Kombigeräte mit WLAN und GSM überleben, wobei WLAN hier nicht wegen der Bandbreite, sondern aufgrund der günstigeren Kostenstruktur den Vorrang erhält.

Ähnlich wird es sich in Zukunft wohl mit dem Funkstandard IEEE 802.16 (Wimax – Worldwide Interoperability for Microwave Access) verhalten, den Teile der Industrie als den nächsten großen Trend im Bereich der Funknetze und auch als Nachfolger für WLANs sehen – unter anderem, weil Intel das Thema ähnlich fördert wie seinerzeit WLAN mit der Integration in den Centrino-Chipsatz. Zwar lassen sich mit Wimax wesentlich größere Distanzen überbrücken (bis zu 50 km), aber das geht bei zunehmender Nutzerzahl zu Lasten der übertragenen Datenmenge. Außerdem ist Wimax wenig robust beim Durchdringen von Wänden, sodass gegenwärtig noch eine Außenantenne notwendig ist. In Anbetracht weiterer Durchsatzsteigerungen bei WLAN und DSL wird Wimax wohl weder WLAN ablösen noch in großem Umfang als Zugangstechnik dienen, sondern eher eine sinnvolle Ergänzung beispielsweise in dünn besiedelten Gebieten sein.

Noch nicht fertig

Renner in Produkttests und Herstellerwerbung sind gegenwärtig sogenannte Draft-N-Geräte. Dahinter verbergen sich Router und Access Points, die WLAN nach der noch in Entwicklung befindlichen Norm 802.11n anbieten. Da diese vom IEEE noch nicht verabschiedet

Freie WLANs: Mein LAN, dein LAN

In Anbetracht von Millionen von DSL-Anschlüssen mit einer Flatrate liegt der Gedanke nahe, diese Kapazität mit anderen zu teilen. Die bekannteste Initiative dazu startete das britisch-spanische Unternehmen Fon (www.fon.com/de), das einen eigenen WLAN-Router (La Fonera) anbietet und die Nutzer dazu anhält, den heimischen Hotspot für andere Benutzer zu öffnen. Als Fon-Mitglied kann man an allen anderen Fon-Hotspots kostenlos surfen; Nicht-Mitgliedern werden Tickets angeboten, woran wiederum der Hotspot-Besitzer mitverdienen kann. Zwar findet sich auf der Fon-Website inzwischen eine beachtliche Zahl von teilnehmenden WLANs, aber die Zugänge befinden sich im Vergleich zu kommerziellen Hotspots häufig an ungünstigen Standorten.

Zurückhaltung gegenüber dem Angebot dürfte, neben mangelnder Solidarität, auch in rechtlichen Aspekten zu suchen sein, denn hier greifen fremde Nutzer auf den privaten Internetanschluss zu, für den der Besitzer die Verantwortung trägt. Auch wenn Fon den wirklichen Nutzer identifizieren kann, bleibt das Verfahren zumindest in Deutschland bedenklich, weil im Zweifelsfall die Beweislast allein beim Anschlussbesitzer liegt.

Auch wenn über Fon kostenfreier Internetzugriff möglich ist, so deuten die Investoren (u. a. Google, Ebay und Sequoia Capital, der größte Kapitalgeber im Silicon Valley) eher auf ein kommerzielles Unternehmen hin als auf eine gemeinnützige Organisation. Für den anfangs verschenkten La-Fonera-Router werden in der kleinsten Ausführung jetzt 35 Euro fällig, und die Ticketeinnahmen behält Fon zur Hälfte. Als einer der ersten Anbieter hat Fon die Bedeutung von Hotspots für das Telefonieren erkannt: Über Anteilseigner Skype kann man kostenlos telefonieren, und in den Niederlanden gibt es ein Paket mit einem kostenlosen Voice-over-IP-Anschluss und Nokia-Handy von debitel.

Ein Gegenstück zu Fon bildet die deutsche Initiative Freifunk (www.freifunk.de). Während Fon eigene Hardware liefert, stellt Freifunk eine Linux-basierte Firmware zur Verfügung, die auf einer großen Anzahl handelsüblicher Router läuft. Auch gibt es keine kommerzielle Komponente wie bei Fon; Freifunk folgt einer Vision der Verbreitung freier Netzwerke, der Demokratisierung der Kommunikationsmedien und der Förderung lokaler Sozialstrukturen. Ein ähnliches nichtkommerzielles Konzept liegt auch Maxspot zugrunde (www.maxspot.de), während Sofanet (www.sofanet.de) wiederum das Ziel verfolgt, den heimischen DSL-Anschluss über WLAN mit Nachbarn zu teilen. Sofanet liefert hierfür eine zweite DSL-Kennung, Verschlüsselung und Nutzeridentifikation, was gerade die rechtlichen Probleme in Deutschland lösen soll.

ist, sondern nur als Entwurf (Draft) vorliegt, wurde obiger Name geprägt, der elegant verbirgt, dass es sich nicht um standardkonforme Geräte handelt. Deshalb sind derzeit vor allem Heimrouter im Angebot, da bei nur einem eingesetzten Gerät kaum mit Kompatibilitätsproblemen zu rechnen ist – volle Abwärtskompatibilität zu 802.11a, b und g vorausgesetzt. Mit der Draft-Version 2.0 ist die Standardisierung zudem so weit fortgeschritten, dass die Risiken von Kompatibilitätsproblemen als gering eingeschätzt und durch die Vorteile (Geschwindigkeit und Reichweite) aufgewogen werden, sodass die Netzwerkhersteller erste Produkte für den Firmeneinsatz präsentieren (etwa Cisco Aironet 1250).

Außerdem versprechen einige Hersteller eine Anpassung an den endgültigen Standard durch ein Software-Update. Ein Versprechen mit Risiken, denn es sind durchaus noch Änderungen möglich, die Hardwareanpassungen erfordern. Um ein gewisses Maß an Interoperabilität zu gewährleisten und die Zeit bis zum Erscheinen des endgültigen Standards zu überbrücken, hat die WiFi-Organisation aber angekündigt, auf Grundlage der Version 2.0 Tests und Zertifizierungen vorzunehmen.

Inzwischen hat die zuständige IEEE Task Group die 500 noch offenen Punkte diskutiert und den Entwurf für Version 3.0 erstellt. Obwohl bereits seit mehreren Jahren daran gearbeitet wird, ist mit einer Veröffentlichung des endgültigen Standards 802.11n erst in der zweiten Jahreshälfte 2008 zu rechnen. Vielleicht gerade wegen der langen Vorlaufzeit gehen die Entwickler davon aus, dass sich der neue Standard auch in den Firmennetzen ebenso schnell durchsetzen wird wie sein Vorgänger – verbessert er doch wiederum die wesentlichen Leistungsparameter, die WLAN gegenüber drahtgebundenem Ethernet benachteiligen: Datendurchsatz und Reichweite.

So sieht der Standard einen maximalen Datendurchsatz von 300 MBit/s vor, was immerhin fünfmal so viel ist wie bisher möglich; verfügbare Geräte bleiben aber – zumindest mit Verschlüsselung – noch weit darunter. Auch die Reichweiten können sich erhöhen und werden mit maximal 300 m angegeben. 802.11n nutzt bekanntlich die gleichen Frequenzbänder wie bisherige Standards (2,4 GHz und 5 GHz), neu ist aber, dass diese wahlweise und auch zusammen genutzt werden können. Obwohl bisher in Deutschland fast ausschließlich im 2,4-GHz-Band gefunkt wird, erwartet man, dass in Zukunft vermehrt Produkte auf den Markt kommen, die als sogenannte Dual-Band-Geräte die Vorteile beider Frequenzen ausnutzen. Theoretisch sollten damit bis zu 600 MBit/s möglich sein – allerdings mit reduzierter Reichweite durch die kurzwelligeren Signale im 5-GHz-Band. Auch abseits von 802.11n gibt es bereits Kombigeräte für beide Frequenzbänder, etwa den Zyxel Wireless Access Point NWA-3500, der 802.11g und 802.11a kombiniert und damit standardkonform bleibt.

Proprietäres integriert

Einige der verwendeten Techniken sind eigentlich nicht neu, sondern bereits als proprietäre Herstellererweiterungen bekannt, etwa als Super G oder Super AG von Chiphersteller Atheros, die damit bedeutungslos werden.

Um dem neuen Standard größtmögliche Flexibilität zu verleihen, werden Funktionen unterschieden, deren Implementierung Pflicht ist, und optionale. Damit ist es möglich,

WLAN-EQUIPMENT FÜR PRIVATANWENDER, FIRMEN UND SERVICE PROVIDER

3Com	www.3com.de
Alcatel-Lucent	www.alcatel-lucent.de
Allnet	www.allnet.de
Alvarion	www.alvarion.com
Aruba Networks	www.arubanetworks.com
Asus	www.asus.com
AVM	www.avm.de
Belkin	www.belkin.de
Bluesocket	www.bluesocket.com
Buffalo	www.buffalo-technology.de
Cisco Systems	www.cisco.de
Colubris Networks	www.colubris.com
Devolo	www.devolo.de
D-Link	www.dlink.de
Edimax	www.edimax.com
Extreme Networks	www.extremenetworks.com
Funkwerk	www.funkwerk-ec.de
Hewlett Packard	www.hewlett-packard.de
Lancom	www.lancom-systems.de
Linksys	www.linksys.de
Motorola	www.motorola.de
Netgear	www.netgear.de
Nortel Networks	www.nortel-networks.de
Proxim	www.proxim.de
RadioLAN	www.radiolan.de
Siemens	www.gigaset.siemens.com
Sitecom	www.sitecom.com
SMC Networks	www.smc.de
SpectraLink	www.spectralink.com
Strix Systems	www.strixsystems.com
Trapeze Networks	www.trapezenetworks.com
Trendnet	www.trendnet.com/ge
U.S.Robotics	www.usr-emea.com
Vierling	www.vierling.de
Xirrus	www.xirrus.com
ZyXEL	www.zyxel.de

Spröder Industriecharme: Bei Outdoor Access Points kommt es vor allem auf Robustheit an – als Beispiel der Mesh Wireless Router MWR6300 von Motorola (Abb. 2).

sowohl Power-Hardware mit hohem Durchsatz und großer Reichweite zu konstruieren als auch abwärtskompatible, kleine, Strom sparende und günstige Endgeräte, die von bestimmten Draft-N-Features profitieren, aber zum Beispiel nur Daten langsamer übertragen. Als erster Chiphersteller hat Broadcom eine 802.11n-Lösung auf einem einzigen Chip realisiert, der in Kürze in großen Stückzahlen verfügbar sein soll. Als Zielmärkte sieht der Hersteller bislang wenig vernetzte Geräte wie Kameras, Set-Top-Boxen und Fernseher, da der in 65-Nanometer-CMOS-Technik gefertigte Chip Strom sparende, günstige und kompakte Designs erlaubt.

Das höhere Tempo der 802.11n-Geräte beruht im Wesentlichen auf der Nutzung mehrerer Antennen (MIMO), Packet Aggregation und Kanalbündelung. Wie das im Detail funktioniert, beschreibt der Kasten „Alles neu: Was 802.11n-Geräte schnell macht".

WEP ist tot

Dass Fortschritt aber auch im Weglassen bestehen kann, zeigt sich bei der Verschlüsselung: Die (unsichere) WEP-Verschlüsselung ist in 802.11n nicht mehr vorgesehen. Stattdessen wird das neue WPA2-PSK (Pre Shared Key) eingeführt, das allerdings erhöhte Anforderungen an die Hardware stellt, da hier mit AES (Advanced Encryption Standard) ein neuer Verschlüsselungsalgorithmus anstelle von RC4 zum Einsatz kommt.

Die bereits auf dem Markt befindlichen Geräte lassen auch erste Aussagen zu, mit welchem Datendurchsatz in der Praxis zu rechnen ist. So erzielen die besten Geräte mehr als 100 MBit/s (im 2,4-GHz-Band). Das ist zwar nicht einmal die Hälfte der theoretischen Übertragungskapazität, aber das kennt man ja schon von den bisherigen Standards: 802.11g-Geräte beispielsweise schaffen 20 bis 25 MBit/s netto bei nominal 54 MBit/s. Bei allen Angaben ist Vorsicht geboten: Die Werte werden nur bei geringen Entfernungen (unter 10 m) erreicht. Bei größeren Abständen und massiven Hindernissen bricht der Durchsatz ein. Außerdem werden Spitzenwerte häufig nur unverschlüsselt oder mit einer schwachen Verschlüsselung erreicht, da die AES-Verschlüsselung extrem viel Rechenleistung beansprucht – allerdings kann man für die Zukunft schnellere Hardware erwarten.

Zu bedenken ist auch, dass sich die Bandbreite aufteilt, wenn mehrere Clients im Einsatz sind. Damit beeinflusst ein Endgerät mit laufendem Backup oder Video-Streaming die Performance der anderen Clients. Zur Entlastung insbesondere bei der Videoübertragung arbeitet man bereits am neuen Standard 802.11z, der den Datenaustausch zwischen zwei Endgeräten direkt ohne Umweg über die Basisstation erlauben soll (Direct Link Setup). Das spart etwa bei der Übertragung zwischen Fernseher und Videorekorder die Hälfte der Bandbreite.

MAR: Internet in Bewegung

Obwohl Wireless LAN bereits Mobilität assoziiert, besteht der Wunsch, auch im Auto oder Zug Internet nutzen zu können. Zu diesem Zweck kommen sogenannte Wireless Mobile Access Router (MAR) ins Spiel. Da hier in der Regel eine Integration in bestehende Systeme bereits auf Modulebene erfolgen muss, liefern die Hersteller keine kompletten Geräte, sondern nur Platinen und Entwicklungssysteme. So hat die Deutsche Telekom begonnen, ihre neuen Telefonsäulen mit einem WLAN-Modul auszustatten; die Deutsche Bahn installiert WLAN-Access-Points in ihren ICE-Zügen. Zunächst sind nur wenige Strecken damit ausgerüstet (von Frankfurt nach Hamburg, Köln und München), und die Implementierungsphase wird sich noch etwas hinziehen, da man sowohl in den Zügen als auch an den Strecken entsprechende Hardware benötigt. In Zusammenarbeit mit T-Mobile wird vor allem in den Tunneln neue Sendetechnik installiert, für die Anbindung der Züge kommt UMTS zum Einsatz. Steht UMTS nicht flächendeckend zur Verfügung, greift man auf andere Funktechniken zurück, wie im Thalys in Frankreich (Satellitenverbindung in Zusammenarbeit mit 21Net) oder im Southern Express in Großbritannien (Wimax) getestet.

FlyNet wieder eingestellt

Bis vor rund einem Jahr war sogar in einigen Flugzeugen der drahtlose Internetzugang via WLAN möglich, etwa auf den Langstrecken der Lufthansa (FlyNet). Dieser von Boeing unter dem Namen Connexion angebotene Service nutzte acht geostationäre Satelliten zur Datenübertragung. Ende 2006 wurde der Dienst dann von Boeing eingestellt, da man mit der Einnahmesituation nicht zufrieden war. Lufthansa hat aber bereits angekündigt, einen neuen WLAN-Dienst mit einem anderen Partner aufzubauen. Die selbstverständliche Nutzung von WLAN an Bord könnte die Frage aufwerfen, warum Mobilfunkgeräte strikt verboten sind, WLAN aber erlaubt werden kann. Grund ist die um den Faktor 10 bis 20 geringere Strahlung von Wireless LANs gegenüber Handys, die sich für die Flugzeugelektronik als unbedenklich herausgestellt hat.

In Bewegung

Eine zunehmend wichtigere Funktion im Wireless LAN ist das vom Mobilfunk bekannte Roaming, also die Übergabe offener Verbindungen (sogenannter Sessions) von einem Access Point zum anderen (auch Handover genannt). Wie der Name Hotspot bereits andeutet, handelt es sich bei WLAN nicht um eine flächendeckende Infrastruktur. Deshalb spielten Roaming-Funktionen bei der ursprünglichen Entwicklung der Standards keine Rolle. Insbesondere der Einsatz von WLAN-Telefonen, aber auch anderer mobiler Endgeräte wie PDAs und Mobiler Access Router erfordert nun die Möglichkeit, bei Bewegung der Endgeräte die Verbindung nicht abreißen zu lassen. Dafür wurde das Inter Access Point Protocol (IAPP) entwickelt und inzwischen in den IEEE 802.11f-Standard aufgenommen. Es definiert herstellerübergreifendes Roaming in WLAN-Netzen.

Da das Handover mittels IAPP von einem Access Point zum anderen mehrere 100 ms in Anspruch nehmen kann, ist es aber für unterbrechungsfreies Telefonieren in Bewegung nur bedingt geeignet – schließlich toleriert der Mensch nur Unterbrechungen unter 50 ms. Deshalb wird auch am 802.11r-Standard gearbeitet, der speziell den Roaming-Anforderungen von Voice over WLAN Rechnung tragen soll. Mit der Verabschiedung durch IEEE wird im April 2008 gerechnet.

Wireless LAN steht auch als Beispiel dafür, dass sich vorteilhafte Technik nicht im Selbstlauf am Markt durchsetzt. Sie wurde von Intel massiv gefördert, indem man WLAN-Funktionen in alle Notebook-Chipsätze integrierte und die Gerätehersteller verpflichtete, WLAN zu implementieren, wenn sie mit dem Centrino-Logo werben wollten. Dies sollte für zwei Innovationen stehen: Stromsparen und Mobilität durch Wireless LAN. Auch die vierte Generation von Centrino-Chipsätzen schreibt WLAN vor. Hersteller, die mit dem Centrino-Pro-Logo werben wollen, müssen zudem einen WLAN-Chip der neuesten Generation verwenden, wovon der neue Intel WiFi Link 4965AGN bereits den erwarteten 802.11n-Standard unterstützt.

So dürften in Kürze also Millionen entsprechender Notebooks produziert werden, und man darf gespannt sein, ob mit Verabschiedung des endgültigen Standards deren volle Kompatibilität wirklich gewährleistet ist.

Mittelfristig soll WLAN auch bestehende DECT-Installationen in den Firmen ablösen, da sich hiermit sowohl Sprache als auch Daten übertragen lassen. Selbst Siemens als maßgeblicher DECT-Entwickler schätzt Wireless LAN als eine Technik ein, mit der man ähnlich große Installationen realisieren kann, und hat mit dem kanadischen Unternehmen Chantry entsprechendes Know-how eingekauft. Gegenwärtig steht dem breiten Einsatz nur noch der Energiehunger der WLAN-Telefone entgegen.

DIE WICHTIGSTEN WLAN-STANDARDS IM ÜBERBLICK

Standard	Frequenz	Datendurchsatz	proprietäre Herstellererweiterungen
802.11a (40 MHz)	5 GHz	54 MBit/s	108 MBit/s durch Nutzung doppelter Bandbreite
802.11b (802.11b+) (40 MHz)	2,4 GHz	11 MBit/s	22 MBit/s durch Nutzung doppelter Bandbreite
802.11g	2,4 GHz	54 MBit/s	108 MBit/s (Super G)
802.11n (Draft 2.0)	2,4 GHz und/oder 5 GHz	300 MBit/s in einem Frequenzband	

Aber sicher

Ein zentrales Thema bei der Implementierung von Wireless LAN – egal ob im Privathaushalt oder Firmennetz – ist die Sicherheit. Während im drahtgebundenen Netz die erste Sicherheitsstufe bereits im physischen Zugang zu den Firmenräumen oder in die Wohnung besteht, kann ein Einbruch in das Funknetz bequem von der Straße aus erfolgen und hinterlässt auch keine Spuren. Deshalb sind Verschlüsselungsmechanismen

Alles neu: Was 802.11n-Geräte schnell macht

Neben der Flexibilität bei den Frequenzen sind es besonders drei neue technische Lösungen, die 802.11n ausmachen: MIMO (Multiple Input Multiple Output), Kanalbündelung und Packet Aggregation.

Die Unterstützung der MIMO-Technologie sieht man den Geräten auf den ersten Blick an: Sie verfügen über mehrere Antennen, und wie der Name sagt, mehrere parallele Sende- und Empfangsteile; der Standard sieht zwei bis vier vor. Dies vervielfacht die Übertragungskapazität. Ein zweiter Vorteil ist, dass mehrere Antennen die Reichweite erhöhen, indem die Sendeenergie nicht mehr in alle Richtungen verteilt wird, sondern gezielt in Richtung des Empfängers. An der Signalstärke je Antenne ist erkennbar, aus welcher Richtung die Gegenstelle sendet, und man kann so die größte Sendeleistung in diese Richtung schicken. Aus der unterschiedlichen Ansteuerung der Antennen entsteht dann eine keulenförmige Ausrichtung der Strahlung, auch als Beamforming bezeichnet.

Empfangsseitig garantieren mehrere Antennen ein stärkeres Signal. Diese Funktion – auch Smart Antennas genannt – ist nicht auf Draft-N-Endgeräte beschränkt; von der erhöhten Reichweite können auch ältere Endgeräte profitieren, wenn der MIMO-Router im 802.11g- oder 802.11b-Kompatibilitätsmodus läuft. Und: Nicht nur die Reichweite erhöht sich, auch Störungen machen sich weniger bemerkbar, womit es seltener zur Verlangsamung der Übertragung kommt als bisher. Insbesondere wenn ohne Sichtverbindung Reflexionen auftreten, spielt MIMO seine Stärke aus. Denn mehrere Antennen ermöglichen, aus den unterschiedlichen Signallaufzeiten auf die Reflexionen zu schließen. Besonders robust ist die Übertragung natürlich, wenn beide Seiten mehrere Antennen einsetzen.

Mehrere parallele Datenströme erfordern allerdings auch mehrere Sende- und Empfangseinheiten, sodass Draft-N-Geräte nicht nur teurer sind, sondern auch mehr Energie verbrauchen und mehr Wärme abstrahlen. Für den Einsatz im Notebook bedeutet dies eine geringere Akkulaufzeit.

Nicht immer ist die neue Antennentechnik aber auf den ersten Blick zu erkennen. So besitzen die meisten Notebooks bereits zwei um 90 Grad versetzte Antennen – allerdings versteckt im Display-Gehäuse und nur, um das jeweils stärkere Signal der besser ausgerichteten Antenne zu nutzen.

Der zweite Geschwindigkeitsschub neben MIMO resultiert aus der Kanalbündelung. So lassen sich jetzt zwei der 20 Kanäle parallel nutzen – standardkonform aber nur nach vorheriger Prüfung, ob diese auch frei sind. Offen ist noch, ob es diese Funktion auch im 2,4-GHz-Band geben wird, wo nur drei Kanäle zur Verfügung stehen und in vielen Netzen bereits erhebliche Enge herrscht.

Im Verhältnis zu den bisher beschriebenen Techniken steuert Packet Aggregation mit rund 10 Prozent wenig zur Beschleunigung bei. Sie fasst mehrere Datenpakete zusammen und übermittelt die zugehörigen Verwaltungsfunktionen nur einmal. Außerdem werden die Sendepausen zwischen den Paketen weiter verkürzt.

im WLAN unverzichtbar. Nicht nur, dass eigene Daten ohne sie zugänglich sein können – es besteht auch die Gefahr der Haftung für illegale Aktionen Fremder über den eigenen Internetanschluss. Dennoch haben Tests gezeigt, dass etwa jeder sechste AP in Deutschland ungesichert ist.

Spezielle WLAN-Scanner (Sniffer) helfen, WLAN-Hotspots zu finden – entweder als Monitoring-Software für Windows, Linux und für PDAs oder aber als spezielle kompakte Geräte, die einzig für diesen Zweck eingesetzt werden und in einfachen Varianten bereits für wenige 10 Euro zu haben sind. Letztere zumeist ohne Display und nur mit ein paar LEDs, die WLANs anzeigen. Unterschieden werden aktive Softwaresniffer wie Netstumble, die eine Kommunikation zum Hotspot aufnehmen, und passive Scanner wie Kismet, die nur die übertragenen Datenpakete aufzeichnen.

Als eine einfache Methode gegen das Anmelden Fremder im eigenen Hotspot galt lange das Abschalten der SSID-Broadcasts, um Hackern das Auffinden des WLAN zu erschweren. Es wird heute aber eher dazu geraten, hier seine E-Mail-Adresse oder den Namen einzutragen, um Nachbarn bei Überlappungen und Störungen die Möglichkeit zu geben, Kontakt aufzunehmen.

Viele Router erlauben, eine Liste der MAC-Adressen (Ethernet-Hardware-Adressen) anzulegen, die bedient werden – jede andere Hardware ist dann ausgeschlossen. Dies ist ein wirksamer – wenn auch kein vollständiger – Schutz, unerwünschte Endgeräte aus dem WLAN auszuschließen. Allerdings entsteht bei wechselnder Hardware und wechselnden Nutzern etwas Aufwand. Um die Positivliste der MAC-Adressen nicht von Hand eintragen zu müssen, bietet eine Reihe von Heimroutern (etwa AVMs Fritzbox) die Funktion, alle gerade angemeldeten Endgeräte automatisch in die MAC-Adressliste aufzunehmen.

Absolutes Muss in jedem privaten und Firmen-WLAN und die einzige Möglichkeit, ein Wireless LAN wirklich sicher zu machen, ist aber die Verschlüsselung der Daten. Das zu Beginn der WLAN-Entwicklung genutzte WEP-Verfahren (Wired Equivalent Privacy) bietet keinen ausreichenden Schutz und ist auch ohne tiefe Kenntnisse mithilfe entsprechender Tools schnell zu knacken. Es gewährleistet somit kaum noch Sicherheit, und wenn viele Hersteller es in ihren Geräten anbieten, so schadet das eigentlich mehr als es nützt, weil es Sicherheit vorgaukelt, die nicht vorhanden ist und dem Nutzer eine Wahl lässt, die keine ist. Stand der Dinge ist inzwischen WPA (WiFi Protected Access), was praktisch alle neueren Geräten anbieten. Vorsicht ist aber bei Spezialequipment angebracht, etwa WLAN-Webcams, weil sich hier immer noch Geräte finden, die kein WPA beherrschen.

WPA gilt bei richtigem Einsatz als sicher; als Weiterentwicklung bieten viele Geräte bereits WPA2, das auch Bestandteil des 802.11n-Standards sein wird. Statt der auch von WEP verwendeten RC4-Kodierung kommt hier das neue AES-Verfahren zum Einsatz, was die Sicherheit weiter erhöht. Die Erfahrungen mit bereits auf dem Markt befindlichen Geräten zeigen aber, dass es große Ansprüche an die Rechenleistung stellt und der Durchsatz bei den meisten Geräten dadurch sinkt.

In Firmennetzen kann zusätzliche Sicherheit durch eine logische Trennung des WLANs vom restlichen Netz und eine weitere Firewall sowie durch den Einsatz von Intrusion-Detection-Systemen im WLAN erreicht werden.

Für den Zugriff auf Firmennetze über das öffentliche Internet sind VPNs der Standard und unabdingbar, da sie zum einen die Daten verschlüsseln, zum anderen vor den Gefahren des Internet (etwa Viren) schützen. Deshalb sollte auch beim Zugriff auf öffentliche Server vom Firmennotebook aus immer ein VPN aufgebaut werden, da dann die Sicherheitsmechanismen der Firma (etwa Firewall) greifen. Bei der Nutzung öffentlicher Hotspots hat dies den positiven Nebeneffekt, dass stets eine verschlüsselte Kommunikation stattfindet. Für den Privatgebrauch sind VPNs schwieriger zu nutzen. Wer nicht selbst einen VPN-Server betreiben will, findet in Deutschland kaum Anbieter, die Privatnutzern einen entsprechenden Service zur Verfügung stellen. Obwohl dies gerade für Wireless LAN ein sinnvoller Dienst wäre, bietet ihn keiner der großen deutschen Service-Provider an, sondern nur wenige Spezialanbieter wie etwa Hotsplots (www.hotsplots.de) oder Sofa Networks (www.sofanet.de). (JS/hw)

Uwe Schulze
ist Fachautor in Berlin.

In iX extra 2/2008

Mobility – Notebooks als Desktop-Ersatz

Eigentlich gilt für Notebooks die Devise: Je leichter, desto besser. Doch bei einer Kategorie der tragbaren Rechner ist das Gewicht nur ein Maßstab unter anderen: bei den sogenannten Desktop-Replacement-Geräten. Die sollen vor allem ein genügend großes Display haben und eine ergonomische Tastatur. Nur in puncto Lautstärke werden sie ähnlich beurteilt wie ihre kleinen Brüder: Leiser ist besser.

Sonderthema – Mobile Device Management

Sowohl Firmen als auch Mobilfunkanbieter müssen eine immer größere Anzahl mobiler Endgeräte vom Mobiltelefon über den PDA bis zum Notebook verwalten. Hierbei geht es nicht nur um die Konfiguration und das Durchsetzen von Sicherheitsrichtlinien, sondern auch um das Installieren, Updaten und Warten der Software auf den Geräten. Durch Mobile Device Management lassen sich diese Verwaltungsaufgaben zentral erledigen.

Erscheinungstermin:
17. Januar 2008

DIE WEITEREN IX EXTRAS

Ausgabe		Thema	Erscheinungstermin
03/08	Security	Malware-Trends – Trojaner, Bot-Netze et cetera	21.2.2008
04/08	Storage	Energieeffiziente Server- und Storage-Systeme	20.3.2008
05/08	Networking	Loadbalancing	17.4.2008