

INFOSAT

Europas Nr. 1 zum Thema Sat & Digital

www.infosat.info

Digitaloffensive im Kabel

Die Pläne der großen
Netzbetreiber

Hinter den Kulissen

Wer verkauft was
bei Samsung?

Geeignet für PREMIERE

Wechsel des
Crypt-Systems

Digitale Terrestrik

Wie geht's weiter
mit DVB-T?

Sat-Programme pur

Fremdsprachen auf
Hot Bird 13° Ost

IFA-Nachlese 2003

Technik und Trends,
Zahlen und Fakten

Kabelinitiative von Eutelsat

Interview
mit Volker Steiner

Neue DAB-Programme

Einkaufen über
das Radio

Ihr Recht auf Sat-Empfang

INFOSAT hilft Ihnen weiter

Installation der Sat-Schüssel: So einfach geht's

WORKSHOP
WAN für Internet
via Satellit



ISSN 0933-6907 Y 9271

INFOSAT

SATELLIT ♦ KABEL ♦ INTERNET

INFOSAT

Workshop: Wireless-LAN einrichten für Internet via Satellit

Haben Sie schon einmal darüber nachgedacht, Internet via Satellit zu nutzen und Ihre Computer dabei drahtlos miteinander zu vernetzen? In unserem Wireless-LAN-Special zeigen wir Ihnen in wenigen Schritten, wie es geht, und was Sie auf keinen Fall vergessen sollten. Ein Beitrag von Sandra Leyh und Dieter Kneffel von mobileaccess.de.

Hotspots in Deutschland

Die Zahl der verfügbaren Hotspots steigt stetig. Doch wo befindet sich der nächstgelegene öffentliche WLAN-Zugang? Unter <http://mobileaccess.de> sind Hotspots in ganz Deutschland, Österreich und Schweiz gelistet. Im Detail wird erklärt, wie der Zugang konfiguriert werden muss. Neben den Nutzern können Betreiber Hotspots verzeichnen lassen und so ihre Angebot öffentlich machen.



Checkliste: Bevor es losgeht

- WLAN Grundlagen
- richtige Ausrüstung
- Reichweite des Hotspots festlegen
- Netzwerkeinstellungen
- WLAN Einstellungen
- Optimierung und Sicherung des Netzes

WLAN – Grundlagen

Momentan gibt es drei miteinander konkurrierende Standards für drahtlose Netzwerke. Wi-Fi (802.11b) wird vor allem in größeren Unternehmen eingesetzt und bietet eine recht große Reichweite.

802.11a bietet eine größere Bandbreite und weniger Interferenzprobleme, dafür aber auch eine geringere Reichweite. Bluetooth eignet sich für temporäre Netzwerke mit kleinen Reichweiten. Wi-Fi ist die momentan beliebteste und preiswerteste Spezifikation für drahtlose LANs. Wi-Fi arbeitet im 2,4-GHz-Frequenzbereich und überträgt Daten innerhalb seiner Reichweite von 300 Metern mit Geschwindigkeiten von bis zu 11 Mbit/s. Ein ausgeglichenes Verhältnis aus Kostengünstigkeit, Bandbreite und vor allem der Reichweite haben Wi-Fi zum dominanten Standard im Unternehmens- wie auch im Privatbereich gemacht.

Neue Produkte nach dem Standard 802.11g bieten mittlerweile bis zu 108 Mbit/s und sind kompatibel zu Wi-Fi/802.11b. Eine Besonderheit sind Produkte mit 22 Mbit/s beziehungsweise 44 Mbit/s nach dem Standard 802.11b+. Diese sind ebenfalls kompatibel zu 802.11b mit 11 Mbit/s, werden aber wohl auf kurz oder lang vom Markt verschwinden, da sich zunehmend Produkte mit 802.11g als Standard etablieren.

Der Betrieb eines WLANs ist in Deutschland anmelde- und gebührenfrei. Bei Verwendung von zusätzlichen Antennen ist darauf zu achten, dass die maximal erlaubte Sendeleistung von 20dBm (100mW) ERP nicht überschritten wird.

Die richtige Ausrüstung

Jedes Endgerät, das mit Ihrem Netz verbunden werden soll, benötigt ein „Funkgerät“ um drahtlos kommunizieren zu können. Besitzt man ein älteres Notebook, kann man es leicht um einen drahtlosen PC-Card-Adapter ergänzen, neuere Notebooks



Bild: Intel

sind heute bereits standardmäßig mit diesen Funktionen ausgestattet. Kleinere CompactFlash-Karten sind gut für Handhelds geeignet, allerdings auch teuer und

Überblick Ausrüstung

- WLAN Access-Point
- Netzwerkkarte und Patchkabel
- WLAN Adapter, wahlweise PCI, PCMCIA oder USB
- Windows 98 Second Edition/2000/ME/XP als Betriebssystem

haben nur eine beschränkte Reichweite. Für PCs sollte man USB- oder PCI-Adapter in Betracht ziehen. Durch ein entsprechendes Kabel erlauben USB-Adapter zudem eine optimalere Positionierung und damit

WEITERE INFORMATIONEN

WLAN Hardware-Hersteller

www.agere.com
www.cisco.com
www.d-link.de
www.intel.com
www.intersil.com
www.lancom.de
www.linksys.de
www.netgear.de
www.orinocowireless.com
www.smc-europe.com
www.usr-emea.com

unter Umständen eine Verbesserung des Empfangs. Sind alle Geräte bereit für den drahtlosen Netzzugang, benötigen Sie einen zentralen Access-Point (AP/Basisstation), mit dem sie kommunizieren können. Der AP dient als Switch/Hub und erlaubt mehreren Computern die gemeinsame Nutzung einer Breitbandverbindung. Achten Sie beim Kauf auch auf den Antennenanschluss: Nicht alle Access-Points und WLAN-Adapter bieten Anschlussmöglichkeiten für externe Antennen zur Verbesserung der Reichweite.

Der richtige Ort

Zunächst sollte man den Einsatzort zu Hause oder im Büro genau unter die Lupe nehmen. Dazu begeht man das Gebiet, das vom Netz abgedeckt werden soll, um den besten Ort für den AP (Access-Point) zu finden. Jede Wand und jede Zimmerdecke stellt für Funksignale jeder Art ein potenzielles Hindernis dar. Gipswände sind am leichtesten zu durchdringen, Stahl oder Stein ist das für drahtlose Netze am schlechtesten geeignete Wandmaterial. Unter idealen Bedingungen, das heißt bei freier Sicht, sind Reichweiten bis zu 300 Metern möglich. Bei Verwendung externer (Richt-)Antennen sogar noch deutlich mehr. Hier einige allgemeine Tipps für die optimale Platzierung:

- ▶ Störquellen ausschließen: Zwischen Access Point und Client sollten möglichst wenige Hindernisse sein.
- ▶ Ideal: Funkstrecke mit Sichtverbindung zwischen Access Point und Client. So erzielen Sie auch über weite Strecken gute Datenraten.
- ▶ Externe Antennen: Verwenden Sie am AP stärkere Antennen, oder rüsten Sie die PC-Card mit einer externen Antenne auf, wenn sie über einen entsprechenden Anschluss verfügt.
- ▶ Um die nötigen Kabel so kurz wie möglich zu halten, sollte der Access-Point so nah wie möglich bei der externen Antenne platziert werden.

Netzwerkeinstellungen

Um SkyDSL mit mehr als nur einem Arbeitsplatz per WLAN nutzen zu können, sind einige Einstellungen auf den Rechnern notwendig. Der PC mit angeschlossenem

+++ WLAN+++PRODUKTNEWS+++WLAN+++PRODUKTNEWS+++WLAN+++

+++ Die Firma Tiptel AG aus Ratingen bietet mit den Telekommunikationsanlagen tiptel 3011 office und tiptel 3022 office zwei Produkte an, die neben den klassischen Telefonie-Funktionen auch Netzwerkanchluss für ein DSL-Modem sowie WLAN zur Vernetzung von Laptops und Notebooks bieten. Die beiden Anlagen können auf einem Steckplatz mit den optional lieferbaren WLAN-Modulen aufgerüstet werden und so Daten mit bis zu 22 Mbit/s übertragen. (www.tiptel.de) +++ WLAN aus der Steckdose gibt es von der Aachener Firma devolo AG. Der HomePlug-Adapter MicroLink dLAN Wireless kombiniert die Vernetzung beliebig vieler PC's über die Stromleitungen im Haus mit der Flexibilität der Drahtlos-Technologie nach dem Standard IEEE-802.11b. Damit wird jede Steckdose zum WLAN-Anschluss und das haus-eigene Stromnetz zum Netzwerk-Hub. (www.devolo.de)+++

Receiver und Zugangssoftware – nennen wir ihn im folgenden ‚Server‘ – übernimmt dann die Funktion eines Routers/Gateways. Weitere PCs werden dann zum Beispiel per LAN oder eben WLAN mit diesem Router verbunden.

Installation der WLAN-Hardware

Sofern Sie bereits ein kleines Heimnetzwerk mit einem Hub/Switch besitzen, wird der Access-Point mittels Netzkabel an den Hub gesteckt. Alternativ ist es ausreichend, wenn Sie Ihren WLAN Access-Point direkt (gegebenenfalls per Cross-Kabel, gekreuztes Patchkabel für PC-PC Koppelung) mit der Netzwerkkarte in Ihrem Server verbinden. Die Konfiguration des Access-Points erfolgt meist über den Browser. Konfigurieren Sie den Access-Point wie im Handbuch des jeweiligen Herstellers beschrieben und geben Sie dem drahtlosen Netzwerk einen Namen – die sogenannte SSID. Installieren Sie dann

den WLAN-Adapter in Ihrem PC/Notebook und tragen dort ebenfalls die gleiche SSID ein – damit weiß Ihr Notebook, an welchem Access-Point es sich einbuchen muß. Testen Sie nun, ob der Access-Point von dem PC mit WLAN-Adapter gefunden wird – die meisten WLAN-Adapter bieten Ihnen in der mitgelieferten Software/Treiber die Möglichkeit nach verfügbaren drahtlosen Netzwerken zu suchen. Zum Ausprobieren ist es sinnvoll, wenn Sie die Verbindung zwischen Access-Point und Notebook mit WLAN-Adapter im gleichen Raum testen, um so Störquellen auszuschließen. Wird der Access-Point gefunden, funktioniert soweit alles und Sie können mit der Vergabe von IP-

WEITERE INFORMATIONEN

Tools zur Analyse von WLANs
www.stumbler.net
www.wildpackets.com
www.kismetwireless.net
<http://kismac.binaervarianz.de>

Der IEEE 802.11 Standard im Überblick

Seit seiner Verabschiedung im Jahre 1997 ist der WLAN Standard IEEE 802.11 um zahlreiche Zusätze erweitert worden. Hier finden Sie eine aktuelle Übersicht. Auskunft über den aktuellen Status der neuen Erweiterungen finden Sie direkt auf den Webseiten der IEEE, unter <http://grouper.ieee.org/groups/802/11/>

Standard Beschreibung

802.11	Protokoll und Übertragungsverfahren für drahtlose Netze, 1997 zunächst nur für 2 Mbit/s bei 2,4 GHz definiert
802.11a	WLAN mit bis zu 54 Mbit/s im 5 GHz Bereich, zwölf nicht-überlappende Kanäle, Modulation: Orthogonal Frequency Division Multiplexing (OFDM)
802.11b	WLAN mit bis zu 11 Mbit/s im 2,4 GHz Bereich, drei nicht-überlappende Kanäle
802.11b+	WLAN mit bis zu 22 Mbit/s im 2,4 GHz Bereich, Modulation: PBCC, Hardware basiert meist auf TI-ACX100 Chipset
802.11g	54-Mbit/s-WLAN im 2,4 GHz-Band, Modulation OFDM
802.11h	Ergänzungen zum 802.11a für Europa: DFS (Dynamic Frequency Selection) und TPC (Transmit Power Control)
802.11i	Verbesserung der Verschlüsselung: AES, 802.1x (RADIUS) (Ergänzend/Aufbauend auf WEP und WPA)
802.11n	geplante Erweiterung für ein zukünftiges, schnelleres WLAN mit 108 Mbit/s - 320 Mbit/s

G L O S S A R

A Access Point, AP

Zentraler Funkknoten, der für ein bestimmtes Gebiet die Versorgung der Clients mit der drahtlosen Netzanbindung übernimmt.

C Client

Ein Rechner, der über einen Access-Point die Verbindung zum lokalen Netz herstellt.

D DHCP

Dynamic Host Configuration Protocol - Protokoll in IP-basierten Netzen, über das den Clients automatisch eine IP-Adresse zugewiesen wird.

I IEEE

Institute of Electrical and Electronics Engineers, Vereinigung der Elektro- und Elektronikingenieure, die weltweite Standards für elektronische und elektrische Übertragungen definiert.

M MAC, Media Access Code

Bezeichnet die sechsstellige, eindeutige Hardware-Adresse, die jeder Hersteller seinen Netzwerkgeräten zuteilt.

S Secret Key, WEP Key

Der vom Anwender eingestellte Schlüssel für das WEP-Verfahren, der auf Access Point und WLAN-Client identisch sein muss.

S SSID, ESSID

[Extended] Service Set Identification - Alphanumerischer Name des Funknetzes, zu dem ein Access-Point oder ein WLAN-Client gehören.

W Wardriving

Begriff aus der Hackerszene, der das Ausspähen zugänglicher WLANs aus einem fahrenden Auto heraus bezeichnet.

W WECA

Wireless Ethernet Compatibility Alliance - Freiwilliger Zusammenschluss der meisten Anbieter von WLAN-Produkten, der die Zusammenarbeit der Geräte unterschiedlicher Hersteller miteinander prüft und zertifiziert (siehe auch WiFi).

W WEP

Wired Equivalent Privacy, von der IEEE definiertes Verschlüsselungsverfahren für drahtlose Netze nach dem Standard 802.11

Adressen an Ihre Geräte beginnen. Achten Sie beim Eintragen der Adressen darauf, dass sich alle Rechner im gleichen IP-Subnetz befinden und keine Adresse mehr als einmal vergeben wird.

Beispielkonfiguration

Weisen Sie Ihrem Server eine feste IP-Adresse zu, etwa 192.168.0.1, Netzmaske 255.255.255.0. Analog dazu stellen Sie Ihren WLAN Access-Point auf die IP-Adresse 192.168.0.50, Netzmaske 255.255.255.0 und tragen Sie als Gateway die Adresse Ihres Servers ein - in unserem Fall also die 192.168.0.1. Aktivieren Sie auf dem Access-Point den DHCP-Server damit dieser automatisch die passenden Adressen an Ihre anderen Rechner vergeben kann. PCs mit WLAN-Adapter belassen Sie am einfachsten mit der Einstellung „IP-Adresse automatisch beziehen“.

Funktionsweise

In unserer Beschreibung beziehen wir uns auf einen Computer mit installierter Zugangssoftware der Telekom, die Einstellungen sollten bei den meisten anderen Anbietern jedoch analog funktionieren. Im wesentlichen besteht die Zugangssoftware für T-DSL via Satellit aus einem so genannten Proxy-Client. Dieser ist notwendig, da der Datenfluß aufgesplittet werden muß: Ankommende Daten (download) kommen mit hoher Geschwindigkeit per Satellit, abgehende Daten (upload) werden zum Beispiel über Telefonmodem oder ISDN ins Internet geschickt. Während der normalen Installation übernimmt die Software die Einstellung der erforderlichen „Umleitungen“ des Datenstromes.

Per default werden folgende Ports für den Proxy verwendet:

HTTP	9202
Secure (HTTPS)	9202
FTP	9202
SOCKS	9203

Um nun von anderen PCs aus ins Internet zu kommen, müssen die Browser und anderen Internetprogramme wie FTP ebenfalls so konfiguriert werden, dass sie den Proxy verwenden.

So nehmen Sie die notwendigen Einstellungen im Internet Explorer 5 vor: Wählen Sie aus der Menüleiste „Extras/Internet-

Geräte-Übersicht (Auswahl) für das private WLAN**Access Points**

- NETGEAR WG602, 802.11b/g, 54 Mbit/s
- DLink DWL-2000AP, 802.11b/g, 54 Mbit/s
- Lancom Systems 3550, 802.11a/b/g, 54 Mbit/s

WLAN-Adapter PCMCIA

- DLink DWL-660, 802.11b, 11 Mbit/s, Antennenanschluss
- NETGEAR WAG511, 802.11a/b/g, 54 Mbit/s
- PROXIM/Orinoco Combo Card, 802.11a/b/g, 11/54 Mbit/s

WLAN-Adapter USB

- NETGEAR MA111 USB Adapter Stick, 802.11b, 11 Mbit/s
- SIEMENS Gigaset USB Adapter, 802.11b, 11 Mbit/s

optionen/Verbindungen“. Klicken Sie unten bei „LAN-Einstellungen“ auf „Einstellungen...“ und machen Sie einen Haken bei „Proxyserver für LAN verwenden“. Wenn Sie nun auf „Erweitert...“ klicken, können Sie in dem folgenden Fenster die IP-Adresse Ihres Servers sowie die oben genannten Ports eintragen.

Optimierung und Sicherung des Netzes

WLANs sind einfach einzurichten, dieser Komfort geht aber auf Kosten der Sicherheit. Dabei ist es mit wenig Aufwand möglich, ein WLAN abzusichern. Für private Funknetze, die mit wenigen Clients und einer Basisstation betrieben werden, reichen meist wenige Schritte:

G L O S S A R

W WiFi

Wireless Fidelity: Mit diesem Zertifikat werden WLAN-Produkte versehen, die ihre reibungslose Zusammenarbeit mit Geräten unterschiedlicher Hersteller während einer Prüfung durch die WECA unter Beweis gestellt haben.

W WPA

WiFi Protected Access - Zusätzliche Sicherheitsmerkmale, basierend auf WEP. Unter anderem erlaubt WPA die Benutzung eines zentralen Servers zur Benutzerverwaltung mittels 802.1x



Beispielkonfiguration

1. SSID/ESSID

Jedes WLAN trägt einen Namen, die so genannte (E)SSID (Extended Service Set Identifier). So soll gewährleistet werden, dass Sie sich im richtigen Netz anbinden. Seien Sie kreativ und wählen einen ungewöhnlichen Namen für Ihr Netz, also am besten nicht nur einfach „WLAN“. Jeder, der sich in Ihrer Reichweite befindet, kann das Netz auf diese Weise entdecken.

Als Sicherheitsmaßnahme empfiehlt es sich, den „Broadcast“ der ESSID abzuschalten. Dies bedeutet: Nur wem der Netzwerkname explizit mitgeteilt wird, weiß von der Existenz des Netzes.

2. Access-Point absichern

Die meisten Access-Points werden über einen Web-Browser administriert. Das ist komfortabel und vor allem plattformunabhängig. Der Zugang zur Admin-Webseite ist durch ein Passwort geschützt.

Tipp: Deaktivieren Sie die Optionen „Remote-Zugriff“ und „Remote-Firmware-Update“ und konfigurieren Sie das WLAN lokal.

Vergessen Sie nicht, nach erfolgreicher Installation auch dem Access-Point ein neues Passwort zu geben.

3. Verschlüsselung und Authentifizierung

WEP (Wired Equivalent Privacy) ist ein Verfahren zur Datenverschlüsselung und Authentifizierung. Es gilt zu verhindern, dass übertragene Inhalte von Unbefugten gelesen, fremden Stationen Zugang zum Netz gewährt oder aber Übertragungen manipuliert werden. Dazu bedient es sich eines

Hotspots in Deutschland

Wäre es nicht schön, wenn Sie einfach mit Ihrem Notebook oder PDA aus dem Café oder Stadtpark auf Ihren PC zuhause zugreifen könnten? Oder vielleicht Angebote der Geschäfte abrufen, an denen Sie gerade vorbeilaufen? Oder mal kurz einen Abstecher ins Internet machen? Natürlich wäre es schön, doch würde das eine ganze Stange kosten: teures Handy, monatliche Grundgebühr, von den Verbindungspreisen ganz zu schweigen. Nun, tatsächlich ist sowas nicht umsonst zu

64(40) oder 128(104) Bit langen Schlüssels (Key), der sowohl dem Access Point wie auch dem WLAN-Client bekannt sein muss. Neue Geräte bieten sogar Verschlüsselung bis 256 Bit an. Dieser Basisschlüssel lässt sich meist über die Management-Software des Access-Point oder die Eigenschaften der WLAN-Karte einstellen. Tipp: Ändern Sie Ihren Schlüssel in unregelmäßigen Abständen.

4. MAC-Filter

Sichern Sie Ihr WLAN über so genannte Access Control Lists (ACL) ab, indem Sie nur bestimmten MAC-Adressen Zugang zu Ihrem Funknetz geben. Windows gibt nach Eingabe des Befehls „ipconfig /all“ die MAC-Adressen in Ihrem Rechner Preis. Diese finden sie hinter dem Eintrag „Physikalische Adresse“. Linux- und MacOS X Nutzer erreichen die Adressen über den Befehl „ifconfig“. Jetzt müssen Sie nur noch die gültigen MAC-Adressen in die Konfiguration der Basisstation eintragen. Bei kleinen WLANs ist dies kein Problem, wenn aber mehrere Access-Points mit vielen Benutzern verwaltet werden müssen, kann es schnell in Arbeit ausarten. Für die Verwaltung in großen WLANs gibt es so genannte Radius-Server (Remote Dial-In User Authentication Service), die zentral die ACLs gespeichert haben und sich mit den Access Points synchronisieren. Neuere Access-Points sind bereits mit dieser Option ausgestattet, meist zu finden unter der Bezeichnung 802.1x

Nicht vergessen – Windows sichern

In einem Netzwerk sollten Sie generell darauf achten, dass Sie Sicherheitslücken in Windows abschalten: Fast alle fernsteuerbaren Windows-Dienste laufen über den so genannten Server-Dienst. Die meisten

haben, doch mit etwas Eigeninitiative wird es Sie bei weitem nicht soviel kosten, wie heutige kommerzielle Anbieter von Ihnen verlangen. Mit etwas Geld für die nötige Hardware, einen Teil Ihrer Zeit und vielleicht noch etwas Strom sind auch Sie dabei. Mehr dazu in den FAQs von <http://mobileaccess.de>. Dort finden Sie eine umfassende Plattform zur Planung und Realisierung Ihres persönlichen 4G Netzwerks und Ansprechpartner für den Aufbau Ihres eigenen WLAN Netzwerkes oder Hotspots.

WLAN-Nutzer werden keine Server-Dienste zur Verfügung stellen und können diesen Dienst einfach abschalten.

Wer dennoch ein offenes Netzwerk betreiben möchte, sollte zumindest keine Dateien auf den Computern im Netzwerk freigeben (Dateifreigabe) und unbedingt eine Firewall aktivieren. ■

IR 1003/2616