Wireless LAN

von Andreas Spiegel

Allgemein

-Alle momentan in Europa und Deutschland zugelassenen FunkLAN Systeme benutzen das europaweit vom Normungsgremium ETSI festgelegte Frequenzband zwischen 2,4 und 2,5 GHz für das keine Lizenzgebühren anfallen.

-WLANs gemäß der Spezifikation IEEE 802.11b haben eine Bruttoübertragungsrate von 11 MBit/s.

-Ein Funknetz lässt sich wahlweise im so genannten Ad-hoc-Modus oder einem ‘Infrastructure Mode’ betreiben

-FunkLANs sichern den Datenverkehr mittels einem Verfahren zur Bandspreizung

-Zugelassene Geräte dürfen in Deutschland genehmigungs- und gebührenfrei betrieben werden

Architektur

Wireless LANs als Brücke zum Internet

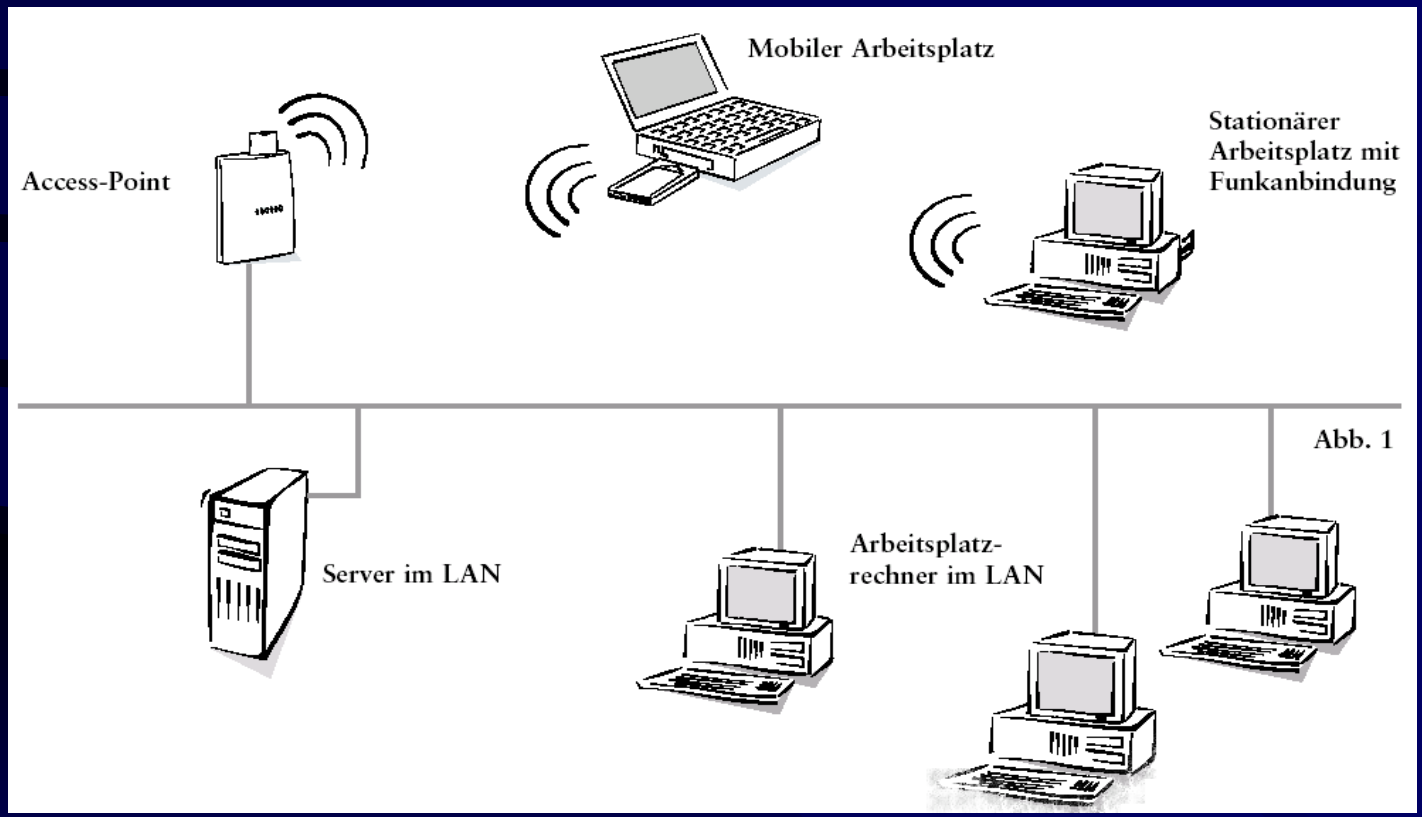
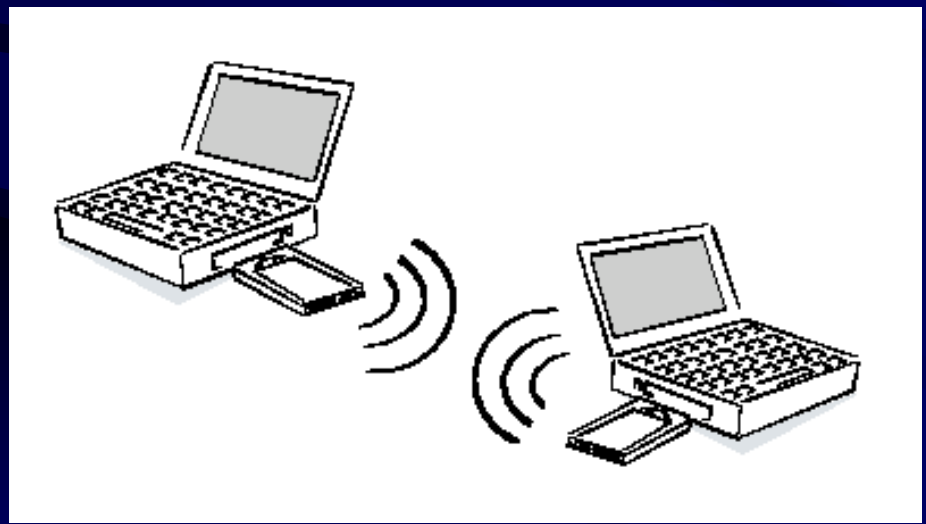


Abb. 1

Ad-hoc Modus

Ad-hoc-Modus

- Hierbei kommunizieren die Stationen in einem begrenzten Sendebereich direkt miteinander.
- Im Grunde genommen handelt es sich um Punkt-zu-Punkt-Verbindungen, da aber jeder Rechner mehrere dieser Verbindungen unterhalten kann, spielt das praktisch keine Rolle.
- Zur Inbetriebnahme muss man auf allen Clients einen einheitlichen Namen für das Funknetz einstellen
- Einsatzgebiet: z.B. Besprechung im Konferenzraum



Infrastructure Modus

- Im Infrastructure Mode hingegen vermittelt eine spezielle Basisstation, Access Point genannt, zwischen den Clients. Er dient zum einen als Bridge zum drahtgebundenen Netz, vermittelt also Pakete zwischen den Netzen hin und her. Zum anderen arbeitet ein Access Point als Repeater, das heißt er empfängt die Pakete der Stationen und leitet sie an andere weiter. Dabei sorgt er für eine gerechte Verteilung der Übertragungskapazität.

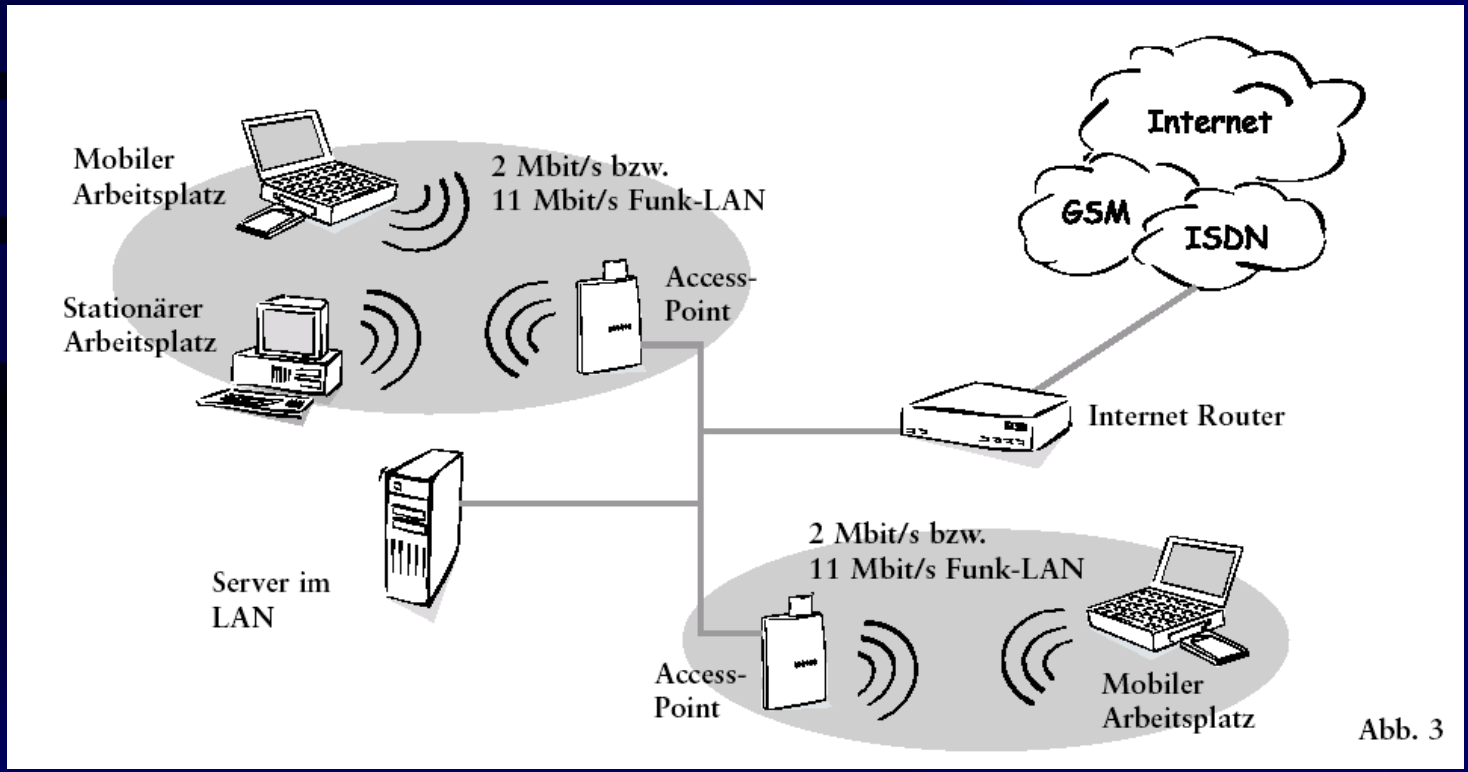


Abb. 3

Roaming

Netzwerk mit Verbindung zu mehreren Funk-LAN-Zellen

Durch entsprechende Konfiguration der Access-Points können mehrere Funk-LAN-Zellen zu einer aktiven Zelle vereinigt werden. Durch diese Maßnahme wird ein unterbrechungsfreier Wechsel zwischen den einzelnen Zellen möglich. Um eine möglichst große Reichweite zu erhalten, sollten die Access-Points an strategisch günstigen Punkten im Gebäude aufgestellt werden.

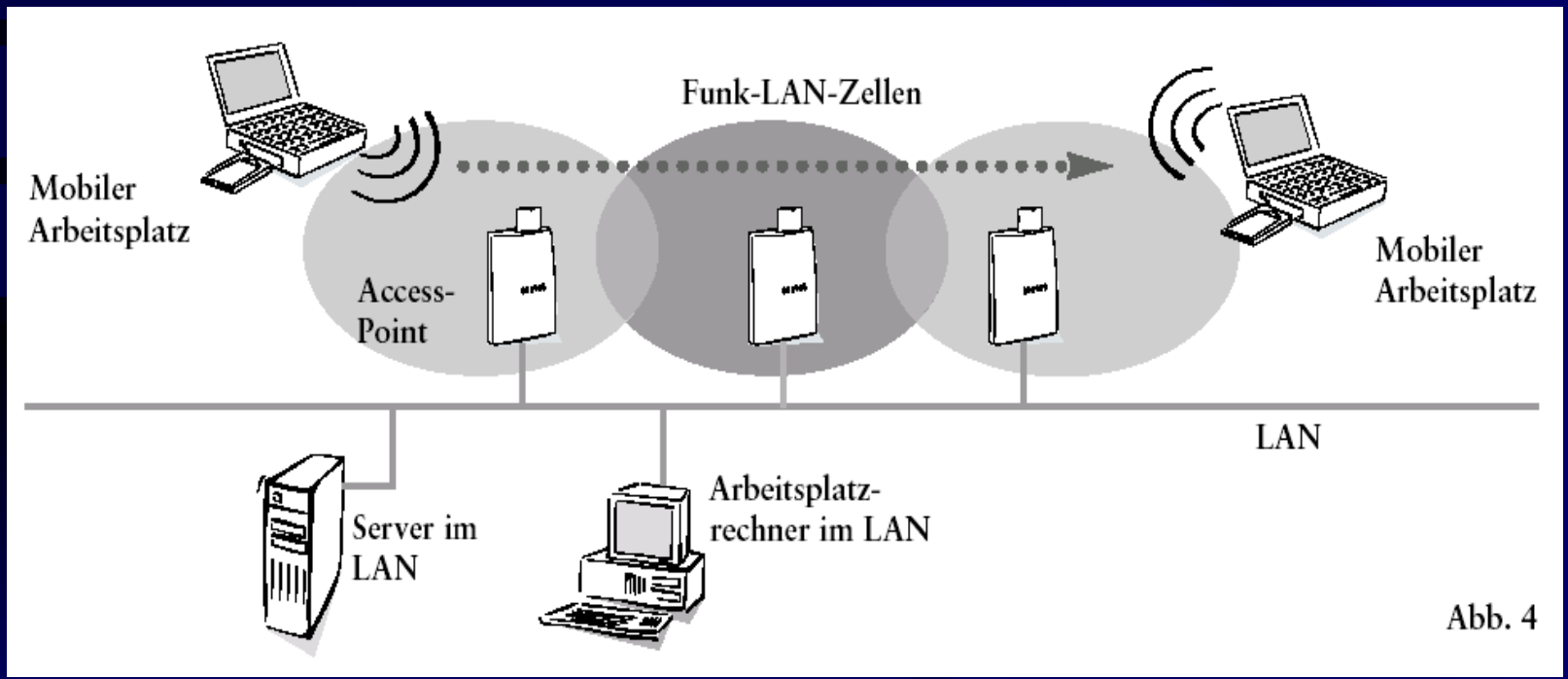


Abb. 4

Access Point

-Der Access Point (AP) stellt für die Funk-LAN-Teilnehmer die Verbindung zur übrigen verkabelten Netz-Welt über ganz normale Ethernet-Schnittstellen her und bildet um seinen Standort eine sogenannte "Funkwolke" oder "Zelle".

-Access Points gibt es inzwischen in verschiedenen Ausprägungen: in der klassischen Form mit einem Ethernet-Anschluss oder als so genanntes ‘Home Residential Gateway’, also mit Anschluss an ISDN oder DSL, manche sogar mit integriertem Hub, um auch kabelgebundene Rechner anzubinden.

-Im Vergleich zu einer Funkkarte kostet ein Access Point allerdings viele Euro mehr und stellt in kleinen drahtgebundenen Netzen, in denen ohnehin eine Maschine als Gateway zum Internet dient oder schon ein Router für den gemeinsamen Internet-Zugriff existiert, eine durchaus vermeidbare Investition dar.

von Andreas Spiegel

Client Adapter

Wie eine herkömmliche Netzwerkkarte ermöglicht der CA den Anschluss ans Netzwerk. Da wir uns hier in einer Funkumgebung befinden, enthält jeder CA anstatt eines Kabelanschlusses eine Antenne. CA sind als PCI-Karte, PCMCIA-Slot Karte und USB Version erhältlich. Besonders empfehlenswert sind direkt in Notebooks integrierte WLAN-Adapter. Diese bieten gegenüber den anderen Versionen einerseits eine bessere Antenne, wodurch sich die Reichweite erheblich verbessert; andererseits ist durch die Integration die Beschädigungsgefahr viel kleiner.

von Andreas Spiegel

Reichweite

- Die Reichweiten betragen - abhängig von der Art von Wänden, Mobiliar etc. - typisch ca. 50 bis 500 m rund um den Access Point, wobei Zusatzantennen die Reichweite noch weiter verbessern können.

- Mit wachsender Entfernung bricht die Verbindung dabei auch nicht etwa plötzlich ab, sondern es wird - abhängig von der Empfangs-Feldstärke - automatisch auf niedrigere Übertragungsraten mit entsprechend höherer Reichweite umgeschaltet: Von 11 Mbps z.B. auf 5,5 Mbps, 2 und schließlich 1 Mbps. In umgekehrter Richtung funktioniert der Prozeß in gleicher Weise, d.h. mit Annäherung verbessert sich der Datendurchsatz wieder.

- Große Areale wie z.B. ausgedehte Gebäude, ausgedehnte Fabriken oder Firmengelände können zu einem logisch zusammenhängenden Mehrzellen-Funk-Netz ausgebaut werden, in dem sich der einzelne Teilnemer völlig frei bewegen kann, ohne die Verbindung zum Netzhintergrund zu verlieren. Diese automatische Überleitung des Funk-LAN-Teilnehmers von einer der jeweils durch Accss-Points gebildeten Zellen zur nächsten wird "Roaming" genannt. Es funktioniert so ähnlich, wie Sie das auch vom Mobiltelefon her kennen.

Sicherheitsprobleme

	SSID	WEP	MAC-Filterung	Authentifizierung	VPN mit Verschlüsselung
Externes Abhören möglich	JA	JA	JA	JA	NEIN
Mitbenutzung durch Externe	NEIN	JA	JA	NEIN	NEIN
Abhören durch Interne	JA	JA	JA	JA	NEIN
Vorteile	einfache Installation	Im 802.11 Standard und somit bei allen entsprechenden Produkten integriert.	Schutz vor Mitbenutzung durch unautorisierte Clients	an Benutzer gebunden	an Benutzer gebunden, sehr sicher
Nachteile	SSID sind leicht herauszufinden und daher für die Sicherheit nicht zu gebrauchen. Änderungen müssen bei allen CA nachgeführt werden	WEP-Verschlüsselung lässt sich durch Abhören von einigen Stunden WLAN-Daten knacken.	Gebunden an physische Karte, nicht an den Benutzer. Grosser Aufwand für die Nachführung der MAC-Adressliste. Unsicher.	Da die Übertragung unverschlüsselt erfolgt, werden Benutzername und Passwort im Klartext übertragen! Deshalb Einsatz von Verschlüsselungstechnologien (SSH, SSL) notwendig !	grosser Installationsaufwand und kaum verfügbare Unterstützung der Hersteller
Bemerkungen	Nur für die Segmentierung (Zugriffsunterteilung) von APs gedacht			Ist nur über die Verwendung von RADIUS Servern per SSH zu empfehlen	

Datensicherheit 1

- FunkLAN´s sichern den Datenverkehr mittels einem Verfahren zur Bandspreizung (Spread-Spectrum, SS) gegen Abhören und Störungen, dieses Verfahren entspricht einer komplexen Kodierung, die ein Abhören schon durch die eingesetzten technischen Prinzipien sehr schwer macht. Alle z.Zt. bekannten zugelassenen FunkLAN Systeme setzen zwei verschiedene Techniken ein, das sogenannte Direct Sequence SS (DSSS) und das Frequency Hopping SS (FHSS) Prinzip.

- Beim Frequence Hopping vereinbaren Sender und Empfänger während des Verbindungsaufbaus eine Folge, nach der einige Male pro Sekunde die Sendefrequenz umgeschaltet wird. Ein nicht autorisierter Zuhörer kann diesen Sprüngen nicht folgen, die Synchronisation zwischen Sender und Empfänger bedeutet jedoch zusätzlichen Ballast (Overhead) in der Datenübertragung.

- Direct Sequence verschlüsselt jedes Bit in eine Bitfolge, den Chip, und sendet diesen auf das Frequenzband aufgespreizt. Für unbefugte Lauscher verschwindet das Signal dadurch im Hintergrundrauschen, erst der autorisierte Empfänger kann es wieder ausfiltern.

- Alle Funk-LANs setzen zusätzlich Verfahren wie Daten-Verschlüsselung, Benutzer-Authentifizierung, MAC-Adressfilterung, Benutzergruppen-Kodierung oder ähnliches ein.

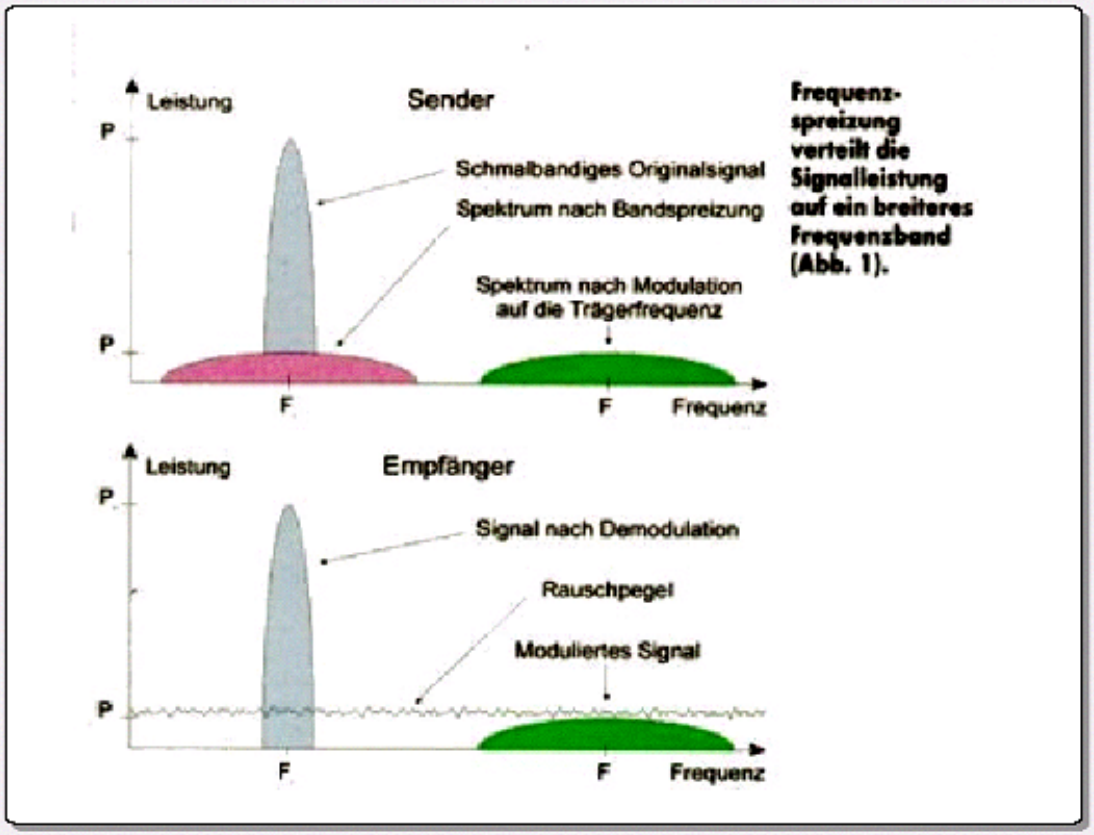
Datensicherheit 2

Das DSSS System ist unempfindlicher gegen Störungen und hat sich als Lösung mit den meisten installierten Geräten in diesem Markt durchgesetzt.

DSSS

Direct Sequence Spread Spectrum

(Frequenz spreizung)



Rechtliche Grundlage

- Rechtliche Hindernisse für den Einsatz eines FunkLAN´s bestehen nicht, drahtlose Netze gelten als nichtöffentliche Funkanwendungen. Für Einrichtung und Betrieb solcher Netze auf eigenem Grundstück sind keine Anmelde- oder Genehmigungsverfahren notwendig und es fallen auch keinerlei Gebühren an.

- Der Hersteller ist dafür zuständig, das die Geräte selbst eine sogenannte Allgemeingenehmigung erhalten und der Anwender darf diese dann ohne Einschränkung auf seinem Gelände einsetzen.

- Durch den "erweiterten Grundstücksbegriff" ist es sogar möglich Gelände des selben Besitzers über "Hindernisse, die leicht zu überwinden sind und die Rechte Dritter nicht verletzen" hinweg mittels FunkLAN zu koppeln.
  Dies gilt z.B. bei Geländen die durch eine öffentliche Straße, einen Fluß oder eine Eisenbahnlinie getrennt sind.

- Erst beim Überqueren von z.B. fremden Grundstücken ist seit Mitte 1997 eine sehr einfache formlose Anmeldung beim BAPT (Bundesamt für Post und Telekommunikation) notwendig, die keine Gebühr kostet.

Gesundheitliche Aspekte

- Das System FunkLAN wurde hinsichtlich seiner ausgesendeten elektrischen und der daraus abgeleiteten magnetischen Feldstärken und hinsichtlich seiner Leistungsflußdichte bei einer Speiseleistung von 100 mW mit einer sinusförmigen Frequenz von 2,46 GHz vermessen.

- Sämtliche Meßwerte liegen weit unterhalb der von der DIN VDE 0848, Teil 2, E/10/91 Expositionsbereich 1 und der 26. Verordnung zum Bundes Immissionsschutzgesetz vorgegebenen Grenzwerte bei Einhaltung des Mindestabstandes zwischen Antenne und Person von 50 cm.

- Im Vergleich zu Mobilfunktelefonen ist die Sendeleistung der LAN-Adapter mit max. 100mW rund 20- bis 30-mal niedriger und ist somit sehr gering.

- Die geringe Sendeleistung wird nach modernsten Modulationstechniken auch noch auf einen breiten Frequenzbereich aufgeteilt, wobei die Nutzinformation - fast schon im normalen Funk-Rauschen - redundant übertragen wird. Funk-LAN Karten stören daher andere Funkdienste nicht und werden im Gegenzug auch von anderen Funkdiensten nicht wirksam gestört.

- Diese Übertragungs-Technolgie entstammt ursprünglich militärischen Verwendungszwecken und bringt so auch hoch entwickelte Sicherheiten gegen "Abhören" mit sich.

Installation einer PC-Card 1

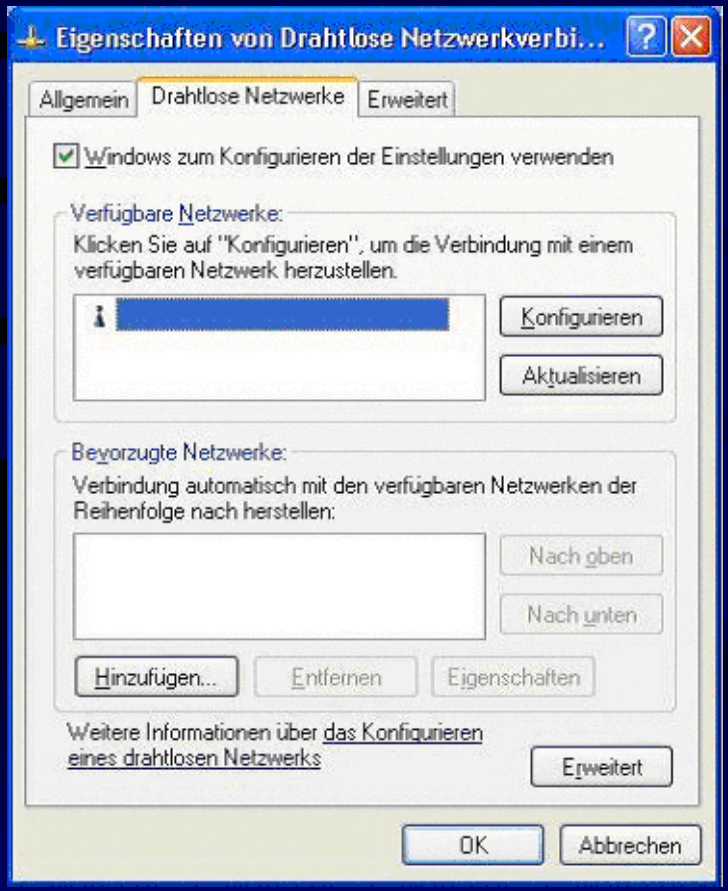
Installation der Orinoco PC Card unter Windows XP

- Hier gibt es einige Unterschiede gegenüber den älteren Windowssystemen, da die Funk-Unterstützung in XP integriert ist. Es empfielt sich, als erstes die aktuellsten Treiber des Herstellers der Funkkarte herunterzuladen und zu installieren. Nach Beendigung des Setups sind noch folgende Schritte durchzuführen:

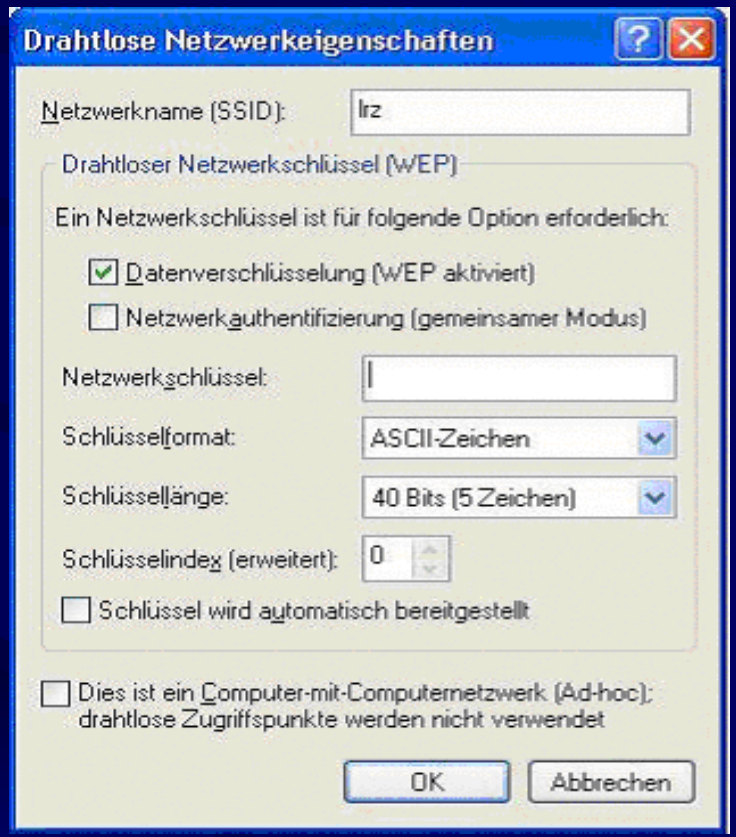
Durch Start->Alle Programme->ORINOCO->Client Manager sollte sich nun der Client Manager starten lassen.
Unter **Actions** ist dann **Add/Edit Configuration Profile** aufzurufen.

Installation einer PC-Card 2

Im folgenden Fenster klickt man dann auf **Hinzufügen**.



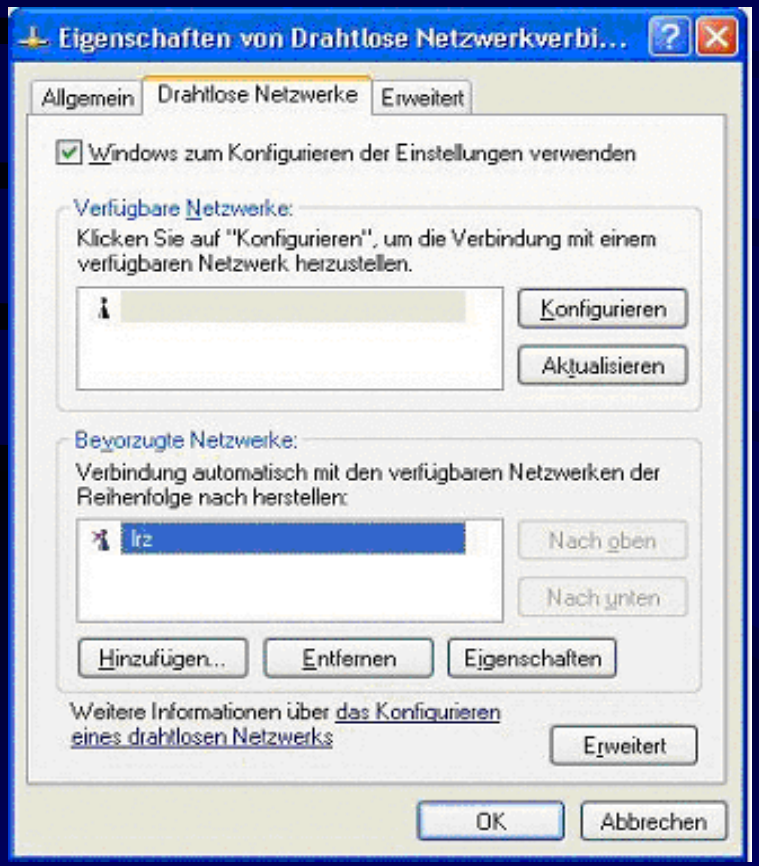
Bei Netzwerkname ist der im jeweiligen Areal gültige Name einzugeben. Das Kästchen **Datenverschlüsselung** muss aktiviert, **Netzwerkauthentifizierung** und **Schlüssel wird automatisch bereitgestellt** müssen deaktiviert sein. Das Feld **Schlüssellänge** ist auf **40 Bits (5 Zeichen)** einzustellen. Bei Netzwerkschlüssel trägt man den ersten der 4 Schlüssel ein.



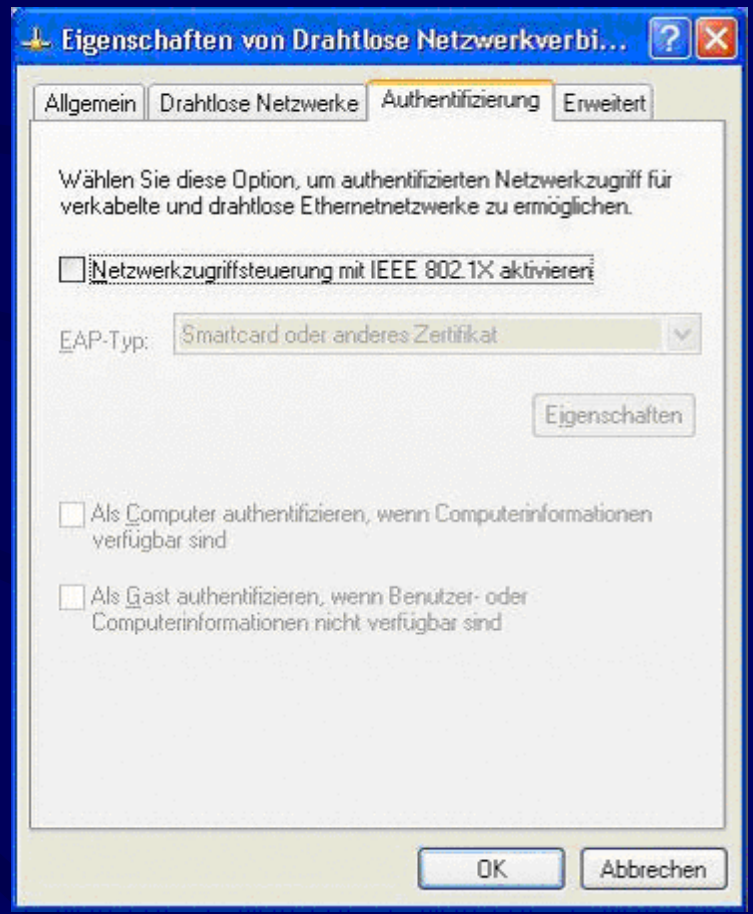
von Andreas Spiegel

Installation einer PC-Card 3

Nach **OK** ist der letzte Schritt für die Schlüssel 2-4 zu wiederholen: Bei markiertem Netzwerk **Irz** klickt man auf **Eigenschaften** und stellt den **Schlüsselindex** nacheinander auf 1,2 und 3 und trägt dazu jeweils den Schlüssel (Key) 2,3 und 4 ein, dazwischen immer auf **OK** klicken.



Schließlich ist noch sicherzustellen, dass unter **Authentifizierung** die **Netzwerkzugriffsteuerung mit IEEE 802.1x** nicht aktiviert ist.



von Andreas Spiegel

Installation einer PC-Card 4

Jetzt sollte die Signalanzeige nach Grün wechseln, wenn sich der PC im Empfangsbereich des Access Points befindet.

Es muss nun eine IP-Verbindung zum VPN-Server möglich sein, dies kann in einem Eingabeaufforderungs-Fenster durch **ping *xxxxx.xx*** getestet werden. Zur Nutzung muss jetzt noch eine VPN-Verbindung konfiguriert werden.

Einrichten einer VPN 1

- Bei einem VPN wird über eine bestehende Verbindung eine zweite Verbindung (Tunnel-Verbindung) aufgebaut, welche den gesamten Datenverkehr über einen dedizierten Rechner, den VPN-Server leitet.

- Der Sinn der Sache ist die Sicherung gegen unbefugten Zugang. Voraussetzung zum erfolgreichen Anmelden beim VPN-Server ist eine gültige Benutzerkennung (Login-Name) und Passwort. Es sind genau dieselben Kennungen/Passwörter wie beim Modem/ISDN-Zugang zu verwenden (falls vorhanden).

Einrichten einer VPN 2

Einrichten einer VPN unter Windows XP

- Erstellen Sie eine neue Verbindung durch **Start->Verbinden mit -> Alle Verbindungen anzeigen**, dann unter Netzwerkaufgaben **Neue Verbindung erstellen**.

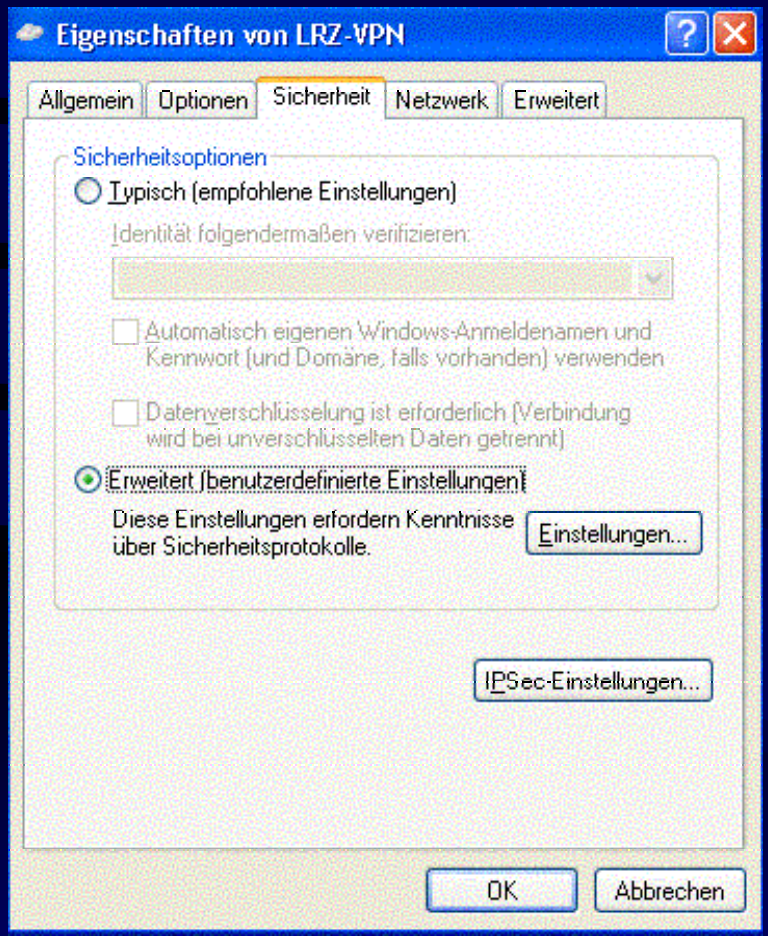
- Wählen Sie im nächsten Fenster Weiter, bei Netzwerkverbindungstyp dann **Verbindung mit dem Netzwerk am Arbeitsplatz herstellen**.

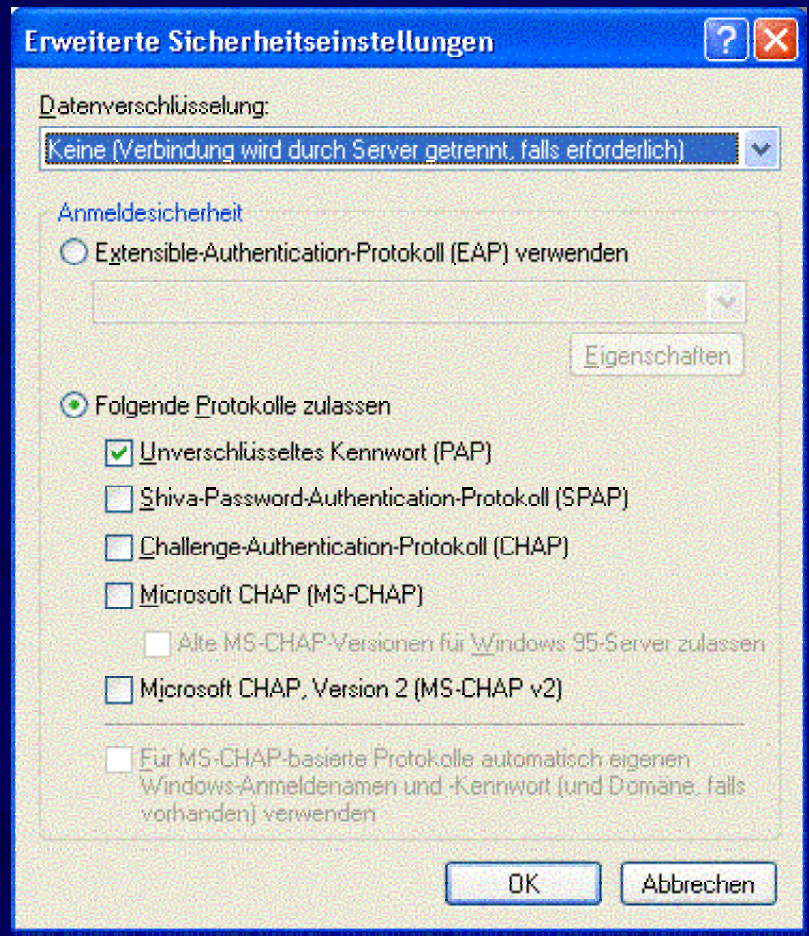
- Im nächsten Schritt markieren Sie **VPN-Verbindung**. Geben Sie ihr einen Namen, z.B. **LRZ-VPN**. Als nächstes kann je nach Belieben **Keine Anfangsverbindung, automatisch wählen** oder **Automatisch diese Anfangsverbindung wählen** markiert werden.

- Bei VPN-Serverauswahl ist **der Servername** einzutragen.

Einrichten einer VPN 3

Wichtig: Nach dem Fertigstellen muss Authentifizierung mit unverschlüsseltem Kennwort eingestellt werden. Dazu klickt man mit der rechten Maustaste auf das Verbindungssymbol (LRZ-VPN) und wählt **Eigenschaften -> Sicherheit -> Erweitert -> Einstellungen**. Im erscheinenden Fenster muss **Unverschlüsseltes Kennwort (PAP)** angekreuzt werden, alle anderen Häkchen sind zu entfernen.





von Andreas Spiegel

Vorteile von Funk-LANs

- Höhere Flexibilität als kabelgebundene Netzwerke
- Größere Mobilität, dadurch höhere Produktivität und schnellere Verfügbarkeit
- In der Regel preiswerter (teure strukturierte Verkabelung wird gespart)
- Ein Funk-LAN kann bei Wechsel der Räumlichkeiten mitumgezogen werden
- Netzwerk-baisierende Computeranwendungen sind jetzt auch da kürzestfristig anbietbar, wo Löcher nicht gebohrt und Kabel z.B. nicht verlegt werden dürfen, wie beispielsweise bei historischen Gebäuden, Museen usw.
- Manchmal lohnt sich auch eine aufwendige Verkabelung nicht, was für Messestände, Schulungsveranstaltungen u.ä. gelten kann.
- Oder aber, die Mobilität ist eine zwingende Forderung. So können sich z.B. Kran- oder Container-Fahrzeuge oder Gabelstabler völlig frei im Hafen oder auf dem Werksgelände bewegen und sind dennoch allzeit integraler Bestandteil des Unternehmens-Netzes.

Nachteile von Funk-LANs

- In der Regel langsamer als kabelgebundene Netze
- Größerer Aufwand in der Planungsphase (Platzierung von Funkzellen...)
- Mehr Sicherheitsüberlegungen notwendig
- Datendurchsatz nimmt mit zunehmender Enfernung von der Funkzelle ab
- Ungünstige bauliche Gegebenheiten (dicke, feuchte Wände usw.) reduzieren Reichweite
- Trotz Standard immer noch gewisse Inkompatibilität zwischen versch. Herstellern feststellbar

Vergleich aktueller LANs

	Kupfer-Kabel LAN (802.3) Fast Ethernet	Wireless LAN IEEE 802.11b	Wireless LAN 802.11a / Hyperlan2 (ca. 2002)
Verkabelungskosten	Hoch	gering	gering
Hardwarekosten	niedrig	hoch	hoch
Sicherheit	rel. hoch (switched)	gering	gering
Reichweite	150 m	25-100 m	25-100 m
Nominalbandbreite	100 Mbit/s	11 Mbit/s	22-55 Mbit/s
Durchsatz	~90 Mbit/s	~5 Mbit/s	10-25 Mbit/s
Verzögerung	sehr niedrig	mittel	mittel
Zuverlässigkeit	Hoch	rel. gering	rel. gering
Strahlung	Praktisch keine	gering	gering

Weitere Entwicklung 1

- Doch auch im Bereich der drahtlosen Netze dreht sich die Geschwindigkeitsspirale nun scheinbar immer rascher nach oben. Bei allen Ansätzen ist man sich soweit einig, dass das 2,4-GHz-Band nunmehr ausgereizt ist und man nun auf das 5-GHz-Band gehen muss. Dies trifft für den bereits spezifizierten 802.11a-Standard (Übertragungsraten prinzipiell von 6 bis 54 MBit/s

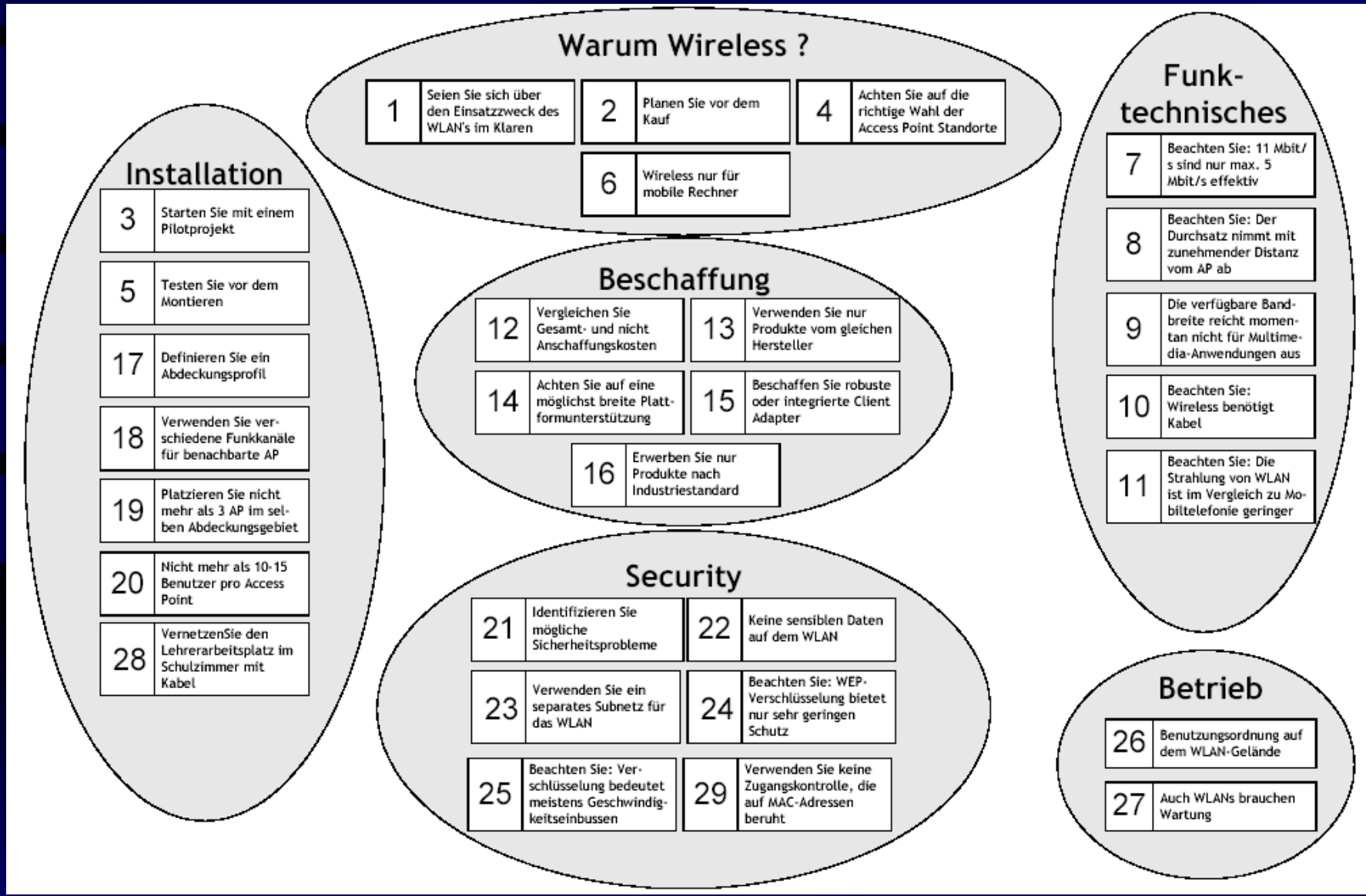
- Obwohl Hiperlan Type 1 schon seit mehreren Jahren als Standard vorliegt und neben der hohen Übertragungsrate von bis zu 24 MBit/s auch Quality of Service- (QoS-) Parameter und die Abwicklung isochronen Datenverkehrs bietet wurde zur Komplettierung des Hiperlan/1-Standards ein neues Projekt gestartet, um die drahtlose Version von ATM zu definieren.

- Dieses drahtlose ATM-Projekt ist unter der Bezeichnung Hiperlan Type 2 (Hiperlan/2) bekannt, und scheint in der Industrie auf deutlich höheres Interesse zu stoßen, als Typ 1. Die drahtlose ATM-Variante unterstützt natürlich die gleichen QoS-Parameter wie die drahtgebundene Version. Außerdem verfügt Hiperlan/2 über zahlreiche Sicherheits-Services und das so genannte Handover - wenn eine Bewegung zwischen lokalen Bereichen und Weitbereichen oder von firmeninternen nach öffentlichen Umgebungen stattfindet. Hiperlan/2 hat eine sehr hohe Übertragungsrate, die auf dem physikalischen Layer bis zu 54 MBit/s und auf Layer 3 bis zu 25 MBit/s beträgt. Um diese zu bewerkstelligen, macht Hiperlan/2 von einer Modularisierungsmethode Gebrauch, die sich Orthogonal-Frequency-Digital-Multiplexing (OFMD) nennt.

Weitere Entwicklung 2

- Der designierte Nachfolgestandard 802.11a (ja -- bei der IEEE kommt manchmal "a" nach "b") definiert zwar eine Übertragungsrate 54 MBit/s, erkauft dies aber durch Inkompatibilität zum Vorgänger.
- Als Alternative wollen Cisco und Intersil deshalb den IEEE-Standard 802.11g durch ein Referenzmodell vorantreiben. 802.11g spezifiziert ebenfalls 54 MBit/s, soll dabei aber die Abwärtskompatibilität wahren.
- Welcher Standard sich also für zukünftige Funknetze durchsetzen wird, bleibt weiterhin offen

Empfehlungen



von Andreas Spiegel