Wireless LANs

IEEE 802.11

F. Hodel

Wireless LAN‘s sind stark im Aufkommen. Leider lassen Viele dabei die Sicherheit ausser Acht. Das muss nicht so sein.

Wireless Standards

- **802.11b**
  - etablierter Standard, CCK Modulation
  - 1, 2, 5.5, oder 11 Mbps, duplex: "22 Mbps"
  - 2.4 GHz (nur drei freie Kanäle)
- **802.11g**
  - kompatibel mit 802.11b, Standard seit Juli 2003
  - ODFM Modulation, max. 54 Mbps
  - 2.4 GHz (nur drei freie Kanäle, beeinträchtigt von 802.11b)
- **802.11a**
  - 6, 12, 24 (pflicht), 18, 36, 48 und 54 Mbps (optional)
  - ODFM Modulation
  - 5 GHz (ev. reduzierte Reichweite im Gebäude, aber 19 freie Kanäle)
- **802.11n**
  - 2.4 GHz, Kanalbreite auf 20-40 MHz vergrössert, höherer Durchsatz
- **Bluetooth**
  - nur für kürzeste Distanzen (im gleichen Raum)

• 802.11b ist momentan am meisten verbreitet. Er eignet sich für ca. 10 Stationen (theoretisch bis 64) an einem Access Point. Die Geschwindigkeit müssen sich alle Stationen teilen!

• 802.g hat eine etwa 5-fache Übertragungsleistung. Da es auf den gleichen Frequenzen arbeitet, kann es kompatibel zum 802.11b betrieben werden (dann aber gebremst auf 11 Mbps).

• 802.11a hat auch die höhere Übertragungsleistung, benützt den 5GHz Bereich und ist daher nicht kompatibel zu 802.11b. Allerdings gibt es dort mehr freie, nicht überlappende Kanäle.

•802.11n benutzt breitere Kanäle dank MIMO (Multiple Input Multiple Output) mit mehreren Antennen. Dies ergibt eine höhere Übertragungsrate oder eine bessere Reichweite, verschlimmert aber das Kanalproblem (benutzt zwei benachbarte Kanäle von je 20 MHz!).

•802.11n-lite verwendet nur einen Kanal und erlaubt eine Bruttorate von 150 Mbps

• Bluetooth ist für den Personal-Bereich gedacht: Umkreis ein paar Meter im gleichen Raum, also kaum geeignet für ein „LAN“. Ausserdem eignet es sich gut für Geräte mit sehr geringem Stromverbrauch (z.B. Natel).

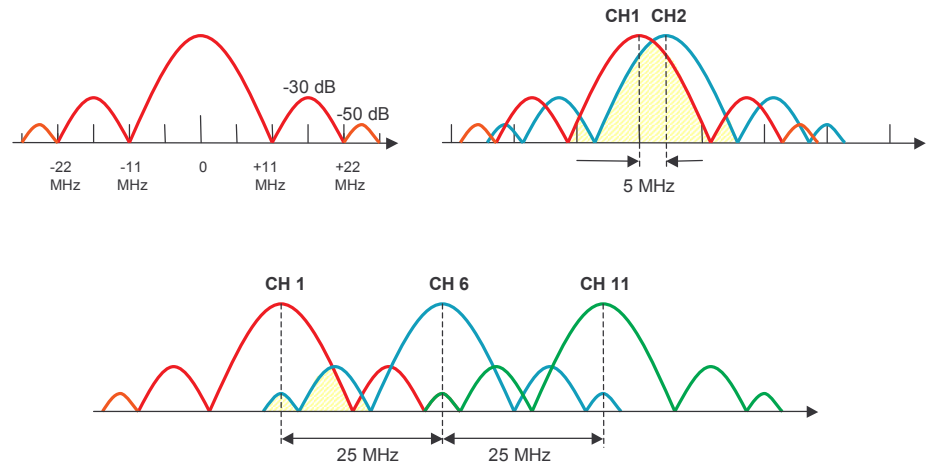
Wireless Daten

Protokoll	Jahr	Frequenz	Durchsatz (netto)	Durchsatz (brutto)	Multiplex-Verfahren	Reichweite im Hause	Reichweite im Freien
802.11b	1999	2.4 GHz	4.4 Mbps	11 Mbps	DSSS	38m	140m
802.11a	1999	5 GHz	23 Mbps	54 Mbps	OFDM	35m	120m
802.11g	2003	2.4 GHz	19 Mbps	54 Mbps	OFDM	38m	140m
802.11n	2009	2.4 GHz 5 GHz	74 Mbps	248 Mbps	MIMO	70m	250m
802.11y	2008	3.7 GHz	23 Mbps	54 Mbps		50m	5000m

Die obige Tabelle bietet eine Übersicht der verschiedenen WLAN Varianten. Beachten Sie, dass der angegebene Schätzwert für den Durchsatz (netto) nur bei optimalem Signal erreicht wird. Bei Störungen oder wenn das Signal schwach ist, sind die erreichbaren Werte wesentlich kleiner! Insbesondere wenn die Distanz über etwa einem Drittel der maximal möglichen liegt, sind nur noch kleinere Übertragungsraten möglich. Man kann also die Geschwindigkeit ausreizen **oder** die Distanz, aber nie beides gleichzeitig!

Die Varianten im 2.4 GHZ Bereich stören sich gegenseitig, insbesondere frisst 802.11n fast die ganze Bandbreite weg. Genügend freie Kanäle gibt es im 5 GHz Bereich des 802.11a. Die Kanäle liegen hier 20 MHz (statt 5 MHz) auseinander und überlappen daher nicht.

Kanäle



Die Kanäle sind etwa 22 MHz breit, aber im Abstand von 5 MHz definiert. Deshalb ergibt sich eine grosse Überlappung benachbarter Kanäle.

Man sollte einen Plan mit allen Access Points machen (eigene und die der Nachbarn!). Gut getrennt (>30dB) sind:

- Kanäle 1, 6 und 11. Wenn das nicht geht, kann man auch die
- Kanäle 1, 4, 8 und 11 nehmen.

802.11a verfügt im Gegensatz dazu über 19 Kanäle in einem Abstand von 20 MHz.

802.11b Standard

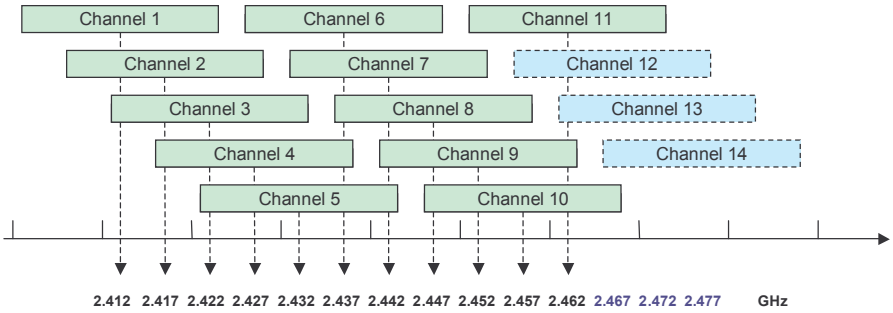
- 1, 2, 5.5, oder 11 Mbps, auch adaptiv
  - ca. 50 mW Sendeleistung (Handy: bis 2 Watt!)
  - CSMA/CA Carrier Sense Multiple Access / Collision Avoidance
  - Frequenzbereich: 2.4 -2.483 GHz (Mikrowellen)
- **WiFi**: erlaubt Interoberabilität der Geräte verschiedener Hersteller (Wireless Fidelity)
- **WEP** Wired Equivalent Privacy: Verschlüsselung mit 40/64 oder 104/128 Bit (24 Bit Initialisierungsvektor)
  - von Haus aus bei allen Produkten deaktiviert (=Plug & Play!)
- DSSS Direct (Sequence Spread Spectrum) oder (FHSS Frequency Hopping Spread Spectrum) mildern den Einfluss von Störsendern

Die Übertragungsrate kann dynamisch gewählt werden. Mit anderen Modulationsarten kann so bei niedrigeren Geschwindigkeiten eine grössere Distanz erreicht werden.

• WiFi ist eine Vereinigung, die Tests zur Interoperabilität macht. Geräte mit diesem Zertifikat arbeiten gut zusammen. Auf proprietäre Spezialitäten muss man dann allerdings verzichten.

• WEP ist ein in allen Geräten eingebaute Verschlüsselung. Möglich ist eine 40/64 (mit/ohne Initialisierungsvektor) und die einzig sinnvolle 104/128 Verschlüsselung. WEP ist (leider) fehlerhaft definiert und deshalb knackbar. Allerdings sollte man dies trotzdem nutzen, denn es braucht doch einige Zeit, den Schlüssel zu analysieren.

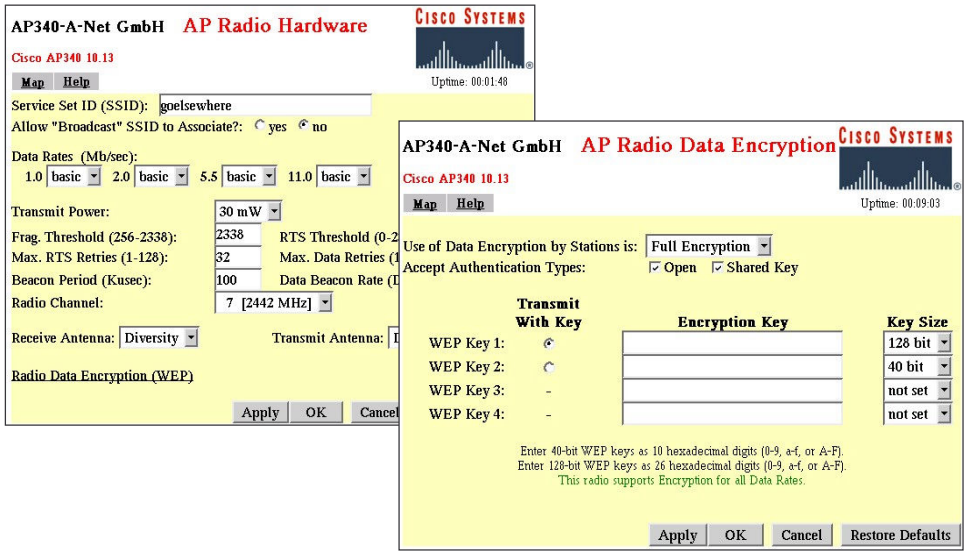
Kanäle



Hier ist die genaue Lage der Kanäle dargestellt. Die Kanäle 12 bis 14 sind nur in gewissen Ländern freigegeben und werden nicht von allen Adaptern unterstützt.

In der Schweiz sind meist die Kanäle 1 bis 13 verfügbar.

Beispiel: AccessPoint



Hier zwei Konfigurationsbilder von einem Access Point Cisco Aironet 340.

Linkes Bild:

Man sieht die automatisch wählbaren Übertragungsraten. Hier sind alle Varianten offen: 1, 2, 5.5 und 11 Mbps.

Die Sendeleistung ist auf 30 mW eingestellt, das Maximum für dieses Modell. Falls nicht notwendig, kann sie weiter reduziert werden.

Als Kanal ist der Kanal 7 voreingestellt. Damit übernehmen die Client Adapter die 4.442 GHz.

Rechtes Bild:

Hier wird die WEP-Verschlüsselung eingestellt. Möglich sind Schlüssel von 40 Bit und 104 Bit. Neben diesen frei wählbaren Bits kommt der 24 Bit Initialisierungsvektor hinzu. Es können 4 Schlüssel definiert werden, aber nur einer ist aktiv.

Leider gibt es im WiFi-Standard kein Verfahren, den Schlüssel automatisch zu wechseln.

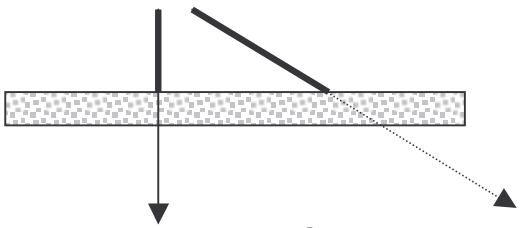
Störsender

- WLANs arbeiten im Industrial, Scientific & Medical Bereich (lizenzfrei bei geringer Leistung)
- mögliche Störquellen
  - Mikrowellenofen (vor allem undichte)
  - Bluetooth
  - DECT Telefone (Home Handy)
  - Möbel aus Metall
  - Liftschächte
  - Eisenbeton (je mehr Eisen ...)
  - WLAN der Nachbarfirma (nur 3 nicht überlappende Kanäle)

Die Wireless LANs arbeiten im 2.4 GHz Bereich, der lizenzfrei ist, aber auch von wissenschaftlichen und medizinischen Geräten benutzt wird.

Als besonders lästige **Störsender** erweisen sich DECT-Handys, Mikrowellengeräte und benachbarte Wireless LANs. Man sollte hier *nicht* die Sendeleistung erhöhen (das führt zu einem Wettrüsten), sondern durch geeignete Kanalwahl und mit Richtantennen eine richtige Lösung anstreben.

Auf der gleichen Etage können Wände durchdrungen werden, weniger günstig sind Betonwände (wegen den Armierungseisen) und Gibswände (viel Wasser). Böden lassen sich meist nur *senkrecht* durchdringen (sind fast immer aus Beton mit viel Eisen), schräg wird gleichermassen der Boden dicker und es geht kaum noch. Deshalb: mindestens einen Access Point pro Etage vorsehen.



Liftschächte stören auch (viel Metall). Schliesslich will man kaum ein WLAN, das immer beim Halt des Liftes auf der eigenen Etage ausfällt. :-)

Möglichkeiten

- Ad hoc Modus
  - mehrere PCs (typischerweise Notebooks) bilden in einem Meetingraum ein Peer-Netz
  - erster PC bestimmt den Namen des Netzwerks
- Infrastructure Modus
  - in einem Gebäude sind ein oder mehrere Access Points installiert
  - normalerweise besteht eine Verbindung zum übrigen LAN
- Wireless Bridge
  - zwei oder mehr Bridges verbinden LAN-Segmente
  - transparenter LAN-Betrieb für alle LAN-Stationen
- Mischformen
  - z.B. WAN-Router oder Firewall mit Access Point

Der **Ad hoc** Modus eignet sich für ein Konferenz-Zimmer *ohne* Access Point. Der **erste PC** bestimmt den Namen des Netzwerks, die anderen übernehmen ihn. Es sollten *nicht* zwei PCs den Namen festlegen, dann gibt es zwei Netzwerke mit dem gleichen Namen! Die Leistung ist meist relativ gering (100 - 300 kbps mit 802.11b).

Der **Infrastructure Modus** ist die häufigste Art, ein Wireless LAN zu bilden. Die Leistung ist hier deutlich höher und erreicht etwa 5 Mbps. Kanal und Name des Netzwerks werden vom **Access Point** festgelegt. Die meisten Access Points haben auch einen Ethernet Anschluss, damit gelangt man ist normale Firmen-LAN.

Mit einem Paar von **Wireless Bridges** können zwei LAN-Segmente verbunden werden. Die LAN-Stationen merken davon nichts (eben eine Bridge) und können mit den Stationen im anderen LAN arbeiten. Die Leistung erreicht auch etwa 5 Mbps (802.11b). Die Distanzen hängen stark von den eingesetzten **Antennen** ab, können aber einige 10 km erreichen. Teilweise können auch drei, vier Bridges kombiniert werden. Allerdings geht der Durchsatz dann zurück.

Besonders für den Home-Bereich gibt es viele Mischformen, etwa *ADSL-Router* mit *Access Point* oder Firewall mit Access-Point. Damit fährt man günstiger, als mit Einzelgeräten, allerdings hat man bei einem allfälligen Ausfall dann gar nichts mehr.

Ad Hoc Modus

- Ad hoc (lateinisch: sofort)
- keine Infrastruktur notwendig
- minimal zwei Notebooks mit WLAN Adapter genügen
- Datenaustausch: normale Shares (Freigaben), FTP etc.
- Vorsicht: Berechtigung der Freigaben korrekt gesetzt?
- SSID: Name des Netzwerks (ist *kein* Passwort!)

Im Ad hoc Modus ist *kein* Access Point notwendig. Zwei Notebooks können direkt eine Verbindung aufbauen. Dazu können alle LAN-Protokolle eingesetzt werden:

• Datei und Druckerfreigabe (NetBios oder NetBios over IP)

• FTP mit einem FTP-Server

• Telnet etc.

Aufpassen muss man, dass die Freigaben mit guten Passwörtern gesichert sind, sonst hört der Nachbar hinter der Wand mit ...

Um mit einem Windows XP SP2 System ein **Ad-hoc Netzwerk aufzubauen,** gehen Sie wie folgt vor:

--Start → Verbinden mit → Drahtlose Netzwerkverbindung

-- Dann links: Erweiterte Einstellungen ändern → Reiter [Drahtlosnetzwerke] → [Hinzufügen]

-- Netzwerkname: ad-hoc-test

-- Netzwerkauthentifizierung: Offen

-- Datenverschlüsselung: WEP

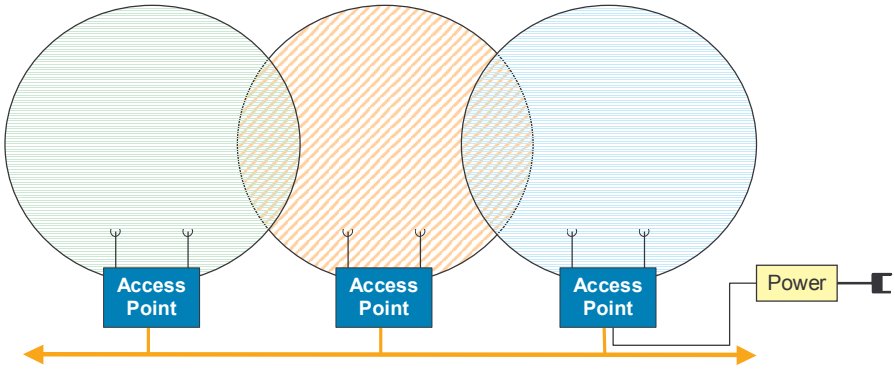
-- Netzwerkschlüssel: aabbccddee (nicht wirklich sicher!)

-- [x] **Dies ist ein Computer-zu-Computer Netzwerk** (Ad-hoc)

-- [OK]

Infrastructure Modus

- Access Point im Hause installiert
- verbunden mit dem Firmen-LAN
- Name des Netzwerks: SSID Service Set IDentifier
- Roaming: von einem Access Point zum nächsten ohne Unterbruch

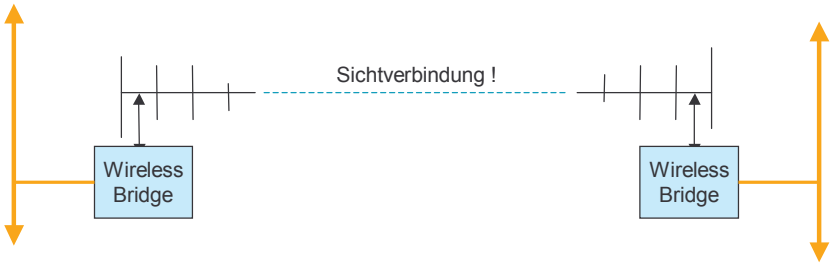


Beim Infrastructure Modus werden oft ganze Gebäude flächendeckend mit einem Wireless LAN erschlossen. Dann sind mehrere Access Points auf einer Etage notwendig. Das benötigt einen guten Kanal-Plan. Bei geeigneter Konfiguration und Access Points vom gleichen Hersteller kann ein Roaming erreicht werden, das heisst ein Notebook kann vom Bereich eines Access Points zum nächsten wandern, ohne die Verbindung zu verlieren.

Solche Access Points werden oft mit Power over Ethernet angeschlossen. Damit wird er nur mit einem RJ45 Kabel erschlossen und kommt so ins Ethernet und erhält auch gleich den Strom über dieses Kabel.

Wireless Bridge

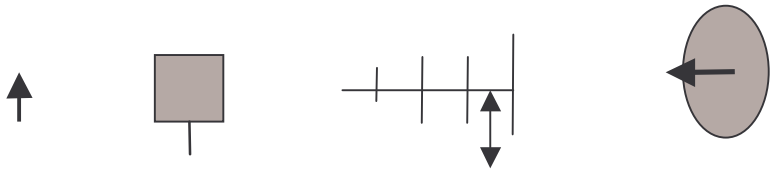
- ein Paar Bridges verbindet zwei LAN-Segmente
  - transparent für alle Protokolle (TCP/IP, NetBios, SNA etc)
  - keine Trennung des IP-Subnetzes
- mit Yagi Antennen ein paar Kilometer
- mit Dish-Antennen bis max. 40 km (!) bei 1 Mbps



Mit Wireless Bridges werden zwei Ethernet Segmente verbunden. Als Bridge gehen alle Protokolle durch. Die Übertragung sollte mit WEP gesichert werden.

Als Antennen kommen die normalen Rundstrahler, flächige Strahler, Yagi und Dish-Antennen in Frage.

In den Katalogen der Hersteller finden sich Diagramme, welche die Richtwirkung einer Antenne aufzeigen.



Vorteile Wireless LAN

- kein teures Verlegen von Kabeln (ca. Fr. 600.- pro Dose)
- leicht transportierbar (z.B. Umzug in anderes Gebäude, Ausstellung)
- rasch aufgebaut (Ausstellungen, Meeting)
- Flexibilität am Arbeitsplatz
- Bridge: Wegfall von Mietleitungen
- Reichweiten:
  - 15-20m im Gebäude
  - 100-200m im freien Gelände (Sichtverbindung)
  - einige Kilometer mit Yagi/Dish-Antennen (Sichtverbindung)

Die Kosten für das Verlegen von Kabelanschlüssen werden meistens unterschätzt. Teuer ist primär das Verlegen und nicht das Material.

Das Wireless LAN kann diese Kosten vermeiden, vor allem wenn es sich um temporäre Installationen (Provisorium, Ausstellungen) handelt.

Im Gegensatz zu Kabeln ist ein WLAN auch leicht zu transportieren.

Echt mobile Arbeitsplätze (etwa Inventaraufnahme mit Notebook im Lager) können trotzdem dauernd mit dem LAN verbunden bleiben.

Bridges können bei Sichtverbindung eine kostspielige Mietleitung ersetzten (z.B. „Leitung“ auf die andere Strassenseite).

Gefahren von WLANs

- Standardmässig sind alle Verschlüsselungen ausgeschaltet
  - jeder kann mitmischen, auch vom Velo/Auto aus („Wardriving“), Cabriolets bevorzugt, da kein Metalldach :-)
- WEP Verschlüsselung (Wired Equivalent Privacy)
  - WEP64 (Key 10 Stellen hex = 40 Bit)
  - WEP128 (Key 26 Stellen hex = 104 Bit)
  - Vorsicht: Key steht teilweise im Klartext in der Konfiguration
- WPA, WPA-PSK und WPA2, WPA2-PSK
  - WPA = WiFi Protected Access nach 802.11i
  - Benutzer muss sich am WLAN anmelden
  - Pro Session wird eine neuer Schlüssel generiert

WLANs sind auch dem „Plug n Play“ Wahn verfallen. So schalten alle Hersteller jegliche WEP-Verschlüsselung aus und viele (vor allem private) Nutzer lassen das so. Das führt zu Schlagzeilen wie „Wireless LAN in 5 Sekunden geknackt“.

So unsicher sind die WLANs aber *nicht*, aber man muss auf jeden Fall die **WEP Verschlüsselung einschalten** und zwar mit 104/128 Bit. Das ist zwar nicht völlig sicher, aber ein Hacker muss doch einigen Aufwand betreiben und sich im Empfangsbereich des WLAN‘s befinden. Allerdings werden die Tools zum Knacken immer raffinierter. War früher WEP 128 nur innert Tagen zu entschlüsseln, geht dies heute innerhalb einer halben Stunde.

Eine Lösung sind WEP 156 Verschlüsselungen. Diese sind jedoch nicht standardisiert und nicht alle Geräte können dies. Besser ist ein Verfahren mit WPA und WPA2 Verfahren. Hier muss sich der Benutzer am WLAN anmelden mit einem Passwort. Bei jedem Verbindungsaufbau wird dann ein neuer Schlüssel generiert. Bei WPA-PSK und WPA2-PSK benutzen alle Teilnehmer am WLAN das gleiche Passwort (PSK=PreShared Key). Bei WPA und WPA2 verfügt jeder Benutzer über ein eigenes Passwort, das in einem RADIUS-Server hinterlegt sein muss.

Sicherheit: WEP

- ohne Verschlüsselung: fahrlässig!!!
  - SSID dient nur der Identifikation des WLANs, ist ***kein*** Passwort
  - SSID steht im Klartext in einzelnen Paketen!
  - SSID von Standard ändern, Name ohne Bezug auf Firma
  - Mac-Adressen-Filter: wertlos, innert Sekunden geknackt!
- WEP64: zu schwach
- WEP128 knapp brauchbar, wenn:
  - der Key regelmässig geändert wird (=manuell auf allen Stationen)
  - das WLAN nur eingeschaltet ist, wenn es benutzt wird (z.B. in einem Sitzungszimmer nur aktiv, wenn eine Sitzung stattfindet)
- WEP 156: beherrschen viele Geräte nicht
  - Scheint knackbar wie WEP 128, es dauert nur länger

Ein WLAN sollte **nie ohne** Verschlüsselung betrieben werden (ausser Sie wollen einen Hot Spot betreiben). Die SSID ist *kein* Passwort, sie dient nur der Identifikation des WLANs, je nach SSID ist ein PC quasi im Hub eines bestimmten LANs eingesteckt. Die SSID sollte auch nicht versteckt werden, da sie auch dann trotzdem in gewissen Paketen im Klartext steht und der Hacker somit die verschlüsselte *und* unverschlüsselte Version der SSID erhält – ein Nachteil.

Viele Access Points erlauben das Einschalten von Mac-Address Filtern. Diese sind *ohne Mühe* zu knacken, der Hauptaufwand ist das Booten des entsprechenden Tools.

WEP 64 verschlüsselt mit 40 Bit nach dem RC4 Verfahren – für die heutigen Rechner viel zu wenig. Wertlos.

WEP 128 (auch RC4) mit 104 Bit gibt einen knapp brauchbaren Schutz. Allerdings muss der Schlüssel regelmässig gewechselt werden und das WLAN nur eingeschaltet sein, wenn es wirklich benötigt wird (z.B. in einem Sitzungszimmer nur während Sitzungen). Mit den aktuellen Tools läst sich WEP 128 in einem 54 Mbps WLAN 802.11g in etwa 30 Minuten knacken, wenn viel Traffic herrscht. Spezialisten (Erik Tews, Andrei Pychkine, Ralf-Philipp Weinmann) von der Uni Darmstadt schaffen ein 802.11g Netz in 20 Sekunden, ein 802.11b Netz in 80 Sekunden.

Der Vorteil von WEP 128 ist, dass es praktisch alle (auch ältere) Geräte können (z.B. Nintendo, Playstation).

Bei WEP 156 dauert das Knacken des längeren Schlüssels etwas länger. Es ist aber auf den meisten Geräten nicht verfügbar.

Gute Sicherheit: WPA

- WPA und WPA2: gute Sicherheit
  - Beim WiFi Protected Access muss sich jeder Benutzer beim WLAN anmelden (Passwort 8 bis 63 Byte lang).
  - Für jede Verbindung wird ein 128 Bit Schlüssel generiert
  - Schlüssel wird nach Ablauf erneuert
  - Benutzerdatenbank in einem externen **RADIUS** Server
- WPA: gute Sicherheit:
  - TKIP (Temporal Key Integrity Protocol)
  - Heute auf den meisten Geräten verfügbar (Win XP mit SP2)
- WPA2: sehr gute Sicherheit
  - AES-Schlüsselung
  - Nicht überall verfügbar (Win XP SP2 nur mit KB917921)

WPA und WPA2 sind der aktuelle Stand der Technik und bieten einen guten Schutz. Beide benutzen eine Benutzerdatenbank von einem Radius Server (Remote Access and Dial-In Server). Dieser kann extern (Linux, Windows) betrieben werden oder (selten) auf einem Access Point realisiert sein. Da bei jeder Verbindung der Schlüssel geändert wird, gelten beide mit den heutigen PCs als nicht knackbar.

Verlässt eine Mitarbeiter die Firma, wird sein Konto auf dem Radius Server gelöscht und die übrigen Benutzer müssen nichts tun.

Richtig gesichert ist ein WLAN mit einer zusätzlichen VPN IPsec Verschlüsselung. Dazu ist auf den Notebooks ein **VPN-Client** notwendig und hinter dem Access Point steht ein Firewall als VPN-Gateway zum Firmennetz.

Eine zusätzliche Massnahme ist das Eingrenzen des **Empfangsbereichs**. Sorgen Sie durch Wahl der Antenne und des Standortes, dass das WLAN nur in den erforderlichen Räumen empfangen werden kann. Also nie die Antenne bei einem Fenster aufstellen.

Gute Sicherheit: WPA-PSK

- WPA-PSK und WPA2-PSK: gute Sicherheit
  - PSK = Pre-Shared Key (für alle gleich)
  - Analog WPA und WPA2: Jeder Benutzer muss sich beim WLAN anmelden
  - Es ist aber *kein* RADIUS Server notwendig:
    Alle Benutzer verwenden das gleiche Passwort
  - Heute zu empfehlende Methode für Private und kleine WLANs

WPA-PSK und WPA2-PSK bieten die gleiche Sicherheit wie WPA und WPA2. Aber es ist *kein* Radius Server notwendig, da Alle mit dem gleichen Passwort arbeiten, dem Pre-Shared Key. Dies eignet sich für kleinere Installationen. Ein Nachteil ist, dass beim Wegzug eines Mitarbeiters der Key geändert werden muss und dies ist notwendig auf den Access Points und auf allen PCs.

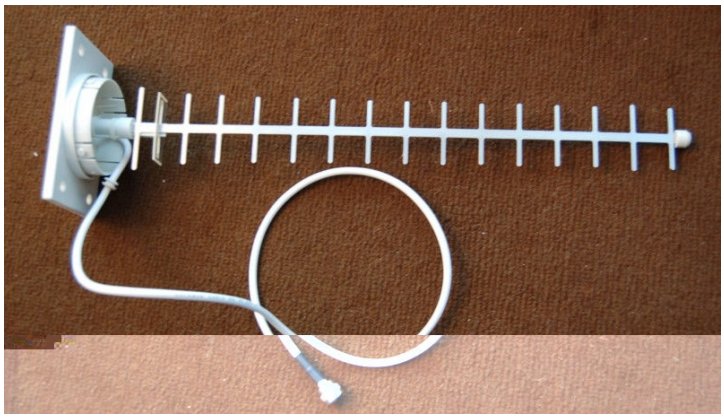
Natürlich lässt sich auch hier die Sicherheit weiter erhöhen, wenn zusätzlich ein VPN mit IPsec eingerichtet wird.

Antennen

- externe Antennen einsetzbar bei Bridges und Access Points
- selten auch bei Adaptern
- Gain (=Verstärkung) wird in dBi angegeben: +3dBi = Verdoppelung
  - keine (passive) Antenne verstärkt wirklich, sie kann lediglich bündeln
  - 0 dBi = idealer Kugelstrahler, der die Energie in alle Richtungen gleich abstrahlt
  - 2.5 dBi = normale, reale Antenne, die eine apfelförmige Abstrahlung hat
  - 6-8 dBi: etwa Verdoppelung der Reichweite in 90-Grad Kegel
  - Dish-Antenne: z.B. 21 dBi für etwa 128-fache Distanz
- Benutzen der Antennen zum Abgrenzen/Erweitern sinnvoll

Antennen sind ein gutes Mittel, um die Reichweite von WLANs zu erweitern und das Signal von unerwünschten Orten (Büros der Nachbarfirma) fernzuhalten. Also Access Point nie am Fenster aufstellen, sondern im Mittelgang. Mit Rundstrahl-Antennen kann das Signal horizontal in der Etage konzentriert werden. Ein Empfang in den Etagen darunter und darüber ist damit erschwert. Ausserdem können Trennwände und Böden mit metallischer Farbe undurchlässig gemacht werden. Auch Fenster mit aufgedampfter Metall- Beschichtung verhindern ein Austreten des Signals in den Garten..

Beispiel: Yagi-Antenne



Antenne:

- Gain: ca 20 dBi
- Zweck: Fernverbindung bis ca. 10 km

Mit stark bündelnden Antennen (Yagi- oder Dish-Antennen) sind bei Sichtverbindung Distanzen bis zu 40 km möglich, bei gleicher Sendeleistung.