# Kabellos ins Internet – WLAN macht`s möglich

Linux-Infotag Augsburg 2007

Karsten Nordsiek

Am Anfang war

Der Nettzwerg

Kleiner Tippfehler... Es muss natürlich das Netzwerk heißen

Das hatte einen kleinen aber entscheidenden Nachteil:


Den Kabelsalat, der dummerweise zudem auch ungenießbar ist

Und weil so ein Kabelsalat alles andere als Ordnung ins Chaos bringt haben sich einige kluge Köpfe Gedanken gemacht und:

| | |
|---|---|
| Das Trommeln erfunden? | Nein..... besser |
| Die Rauchzeichen erfunden? | Nein..... viel besser |

**Das WLAN erfunden**

WLAN ist die Abkürzung für **W**ireless **L**ocal **A**rea **N**etwork

Ins Deutsche übersetzt heißt dies sinngemäß kabelloses lokales Netzwerk

Die Übertragung erfolgt dabei via Funkwellen

Die hierfür reservierten Frequenzen befinden sich wie z. B. auch die Mikrowellen im Bereich von 2,4 Ghz bzw. 5 Ghz

Innerhalb von 2,4 Ghz sind in Deutschland 13 Kanäle freigegeben. Im Bereich 5 Ghz sind es sogar 19 nicht überlappende Kanäle

Zur Zeit gibt es drei gültige Standards:

IEEE 802.11a

- Frequenzbereich 5 Ghz

- Maximal 1000 mW / 30 dBm EIRP  in Deutschland unter besonderer Beachtung bestimmter Regeln möglich.

- Reichweite Bei freier Sicht mehrere Kilometer in Gebäuden meist nur 10 m. Dies ist von der Bauweise abhängig. Leichtbauwände lassen mehr Funkwellen durch als Stahlbetonwände

- Übertragungsgeschwindigkeit bis zu 54 Mbit/s

Vorteil: Nicht überlappende Frequnzbereiche. Damit verbunden weniger Störungen duch andere Funklans auf anderen Kanälen

Nachteil: Geringere Reichweite speziell bei Hindernissen

IEEE 802.11b

- Frequenzbereich 2,4 Ghz

- Maximal 100 mW / 20 dBm EIRP.

- Reichweite Bei freier Sicht mehrere Kilometer in Gebäuden meist nur 50 m. Dies ist von der Bauweise abhängig. Leichtbauwände lassen mehr Funkwellen durch als Stahlbetonwände

- Übertragungsgeschwindigkeit bis zu 11 Mbit/s

Vorteil: Größere Reichweite innerhalb von Räumen.

Nachteil: Geringere Datenrate mit nur 11 Mbit/s

IEEE 802.11g

- Frequenzbereich 2,4 Ghz

- Maximal 100 mW / 20 dBm EIRP

- Reichweite Bei freier Sicht mehrere Kilometer in Gebäuden meist nur 50 m. Dies ist von der Bauweise abhängig. Leichtbauwände lassen mehr Funkwellen durch als Stahlbetonwände

- Übertragungsgeschwindigkeit bis zu 54 Mbit/s

Vorteil: Höhere Datendurchsatzrate

Nachteil: Geringere Reichweite speziell bei Hindernissen

# Welche Hardware für was?

Der Accesspoint

*Foto Wikipedia.de*

Der Accesspoint dient in der Regel als Basisstation zwischen einzelnen Clients und verbindet diese meist mit einem weiteren Netz, z. B. dem Internet. In diesen Fällen ist der Accesspoint über ein Kabel mit dem Modem verbunden. Der Fachmann nennt dies

- Infrastrukturmodus

Eine weitere Möglichkeit, einen Accesspoint zu betreiben ist ihn zusammen mit anderen Accesspoints in einem großen Netz zu vereinen. Dadurch können größere Räume besser ausgeleuchtet werden. Die Zahl der Verbindungen ist jedoch auf 6 begrenzt. Dabei kann jeder Accesspoint aber immer nur mit seinen in Reichweite stehenden Nachbarn korrespondieren. Eine Weiterleitung der Pakete ist generell nicht vorgesehen. Als besondere Ausnahme ist hier das OLSR-Protokoll zu nennen, welches im Freifunknetz eingesetzt wird. Mit diesem ist  auch eine Weiterleitung der Pakete möglich. Der Modus nennt sich  auf Grund seiner unabhängig voneinander agierenden Accesspoints

- Ad-Hoc Modus

# Welche Hardware für was?

Die WLAN Karte Typ Cardbus/PCMCIA


*Foto Wikipedia.de*

Die WLAN Karte Typ Cardbus oder PCMCIA kommt zu überwiegendem Teil in mobilen Endgeräten wie z. B. Notebooks zum Einsatz. Sie wird jedoch heute immer mehr durch fest eingebaute WLAN Karten verdrängt.

Vorteile:

- Leicht einzubauen

- Nutzung in mehreren Geräten ohne Schraubarbeit möglich

Nachteile:

- Meist geringere Reichweite auf Grund schlechterer Antenne, manche Karten sind auch in der Ausgangsleistung begrenzt

Nutzung nur in Geräten mit Cardbus/PCMCIA Steckplatz möglich

# Welche Hardware für was?

Die WLAN Karte Typ PCI


*Foto Wikipedia.de*

Die PCI Karte ist für den Einsatz in stationären Rechnersystemen gedacht. Jeder Desktop PC als auch Server verfügt über PCI Steckplätze, sodass der Einbau in die verschiedenen Systeme keine Probleme bereiten sollte.

Vorteile:

Antenne meistens abnehmbar. Dadurch kann die Reichweite durch bessere Antennen erhöht werden.

Nachteile:

Muss in der Regel in den Rechner eingeschraubt werden

# Welche Hardware für was?

Der WLAN Stick Typ USB


*Foto Wikipedia.de*

Der WLAN USB Stick ist klein, handlich und schnell eingebaut. Er ist vor allem für den mobilen Einsatz gedacht. Kann aber auch an stationären Geräten angeschlossen werden.

Vorteile:

Schnell eingebaut

Mobil als auch Stationär nutzbar

Nachteile:

USB 2.0 für hohe Datenübertragungsraten erforderlich. Auf älterer Hardware u. U. nicht vorhanden

In der Regel keine Möglichkeit eine externe Antenne anzuschließen. Dadurch geringere Reichweite

**Wichtig:** Vor dem Kauf prüfen, ob der angestrebte WLAN Adapter auch unter Linux funktioniert!

Entscheidend:

Der eingebaute Chipsatz

Zu empfehlen:

Atheros, Orinoco, Prism und Ralink

Im Zweifelsfall:

Mit Knoppix ausprobieren.
Ein lspci gibt Auskunft ob der Chipsatz erkannt wurde

Auf gute Beratung im Geschäft achten, ggf. Mit Händler Kauf auf Probe vereinbaren. Sollte Händler zu keinen Zugeständnissen bereit sein: Laden verlassen, woanders kaufen

# Konfiguration des Accesspoints

- Modus Ad-Hoc oder Infrastruktur

- Die ESSID (**E**xtended **S**ervice **S**et **Id**entifier) Name des Netzwerks z. B. augsburg.freifunk.net

- Verschlüsselungstyp

  a) unverschlüsselt (sehr unsicher)

  b) Verschlüsselt WEP (unsicher) WEP = **W**ired **E**quivalent **P**rivacy

  c) Verschlüsselt WPA (sicher) WPA= **W**i-Fi **P**rotected **A**ccess

  d) Verschlüsselt WPA2 (sehr sicher) WPA2 = **W**i-Fi **P**rotected **A**ccess

- DHCP Server aktivieren wenn die Clients eine IP zugewiesen bekommen sollen (empfohlen)

## Konfiguration des WLAN Clients

- Auf der Kommandozeile bei unverschlüsseltem Netzwerk

  Mittels der Kommandos  iwconfig, ifconfig und dhclient

```
tux@erde:~$ su
(Root Rechte sind erforderlich!)
Pasword:

tux@erde# iwconfig ethX mode (Modus) essid (Name des
Netzwerks)

tux@erde# ifconfig ethX up

tux@erde# dhclient ethX
```

# Konfiguration des WLAN Clients

- Auf der Kommandozeile bei WEP verschlüsseltem Netzwerk

  Mittels der Kommandos  iwconfig, ifconfig und dhclient

```
tux@erde:~$ su
(Root Rechte sind erforderlich!)
Pasword:

tux@erde# iwconfig ethX mode (Modus) essid (Name des
Netzwerks) enc „WEP Schlüssel“ (Hexadezimale
Schreibweise)

tux@erde# ifconfig ethX up

tux@erde# dhclient ethX
```

## Konfiguration des WLAN Clients

- Auf der Kommandozeile bei WPA verschlüsseltem Netzwerk

  Mittels der Kommandos  iwconfig, ifconfig und dhclient zusätzlich ist das Tool wpa_supplicant erforderlich

Bevor man die WLAN Karte starten kann, sind einige Konfigurationsschritte notwendig. Dazu muss zunächst die Datei /etc/wpa_supplicant/wpa_supplicant.conf anpassen.

```
network={
        ssid="Netzwerkname"
        scan_ssid=1
        proto=WPA
        key_mgmt=WPA-PSK
        pairwise=TKIP (Temporal Key Integrity Protocol)
        group=TKIP
        psk="Hier den Schlüssel eintragen“ (Hexadezimal)"
}
```

# Konfiguration des WLAN Clients

Nachdem die Konfigurationsdatei ordnungsgemäß angelegt wurde kann Sie nun gestartet werden

```
tux@erde:~$ su
(Root Rechte sind erforderlich!)
Pasword:

tux@erde# sudo wpa_supplicant -i wlan0 -D wext -c
/etc/wpa_supplicant/wpa_supplicant.conf -d
```

Der Start mit den o. a. Optionen sorgt dafür, dass die Verbindung erst einmal nur getestet wird

```
tux@erde# iwconfig
```

Gibt dann Aufschluss darüber ob eine Verbindung zum Accesspoint aufgebaut werden konnte.

## Konfiguration des WLAN Clients

Konnte die Verbindung hergestellt werden, so kann nun mittels des folgenden Kommandos, dies dauerhaft für diese Sitzung übernommen werden.

```
tux@erde# sudo wpa_supplicant -i wlan0 -D wext -c
/etc/wpa_supplicant/wpa_supplicant.conf -B

tux@erde# dhclient ethX
```

Weitere Optionen zu wpa_supplicant finden sich in der Manpage von wpa_supplicant

## Konfiguration des WLAN Clients

- Auf der Kommandozeile bei WPA2 verschlüsseltem Netzwerk

Dazu muss zunächst die Datei /etc/wpa_supplicant/wpa_supplicant.conf anpassen.

```
network={
        ssid="Netzwerkname"
        scan_ssid=1
        proto=RSN
        key_mgmt=WPA-PSK
        pairwise=CCMP
        group=TKIP CCMP
        psk="Hier den Schlüssel eintragen (Hexadezimal)"
}
```

Ansonsten erfolgt die Konfiguration und Ausführung den Schritten im Abschnitt WPA Verschlüsselung.

## Konfiguration des WLAN Clients

Wer die Konfiguration dauerhaft beim Starten des Betriebssytems mitladen möchte, kann unter Debian basierenden Distributionen die Datei /etc/network/interfaces bearbeiten und um den Eintrag

```
iface wlan0 inet dhcp
        wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf
auto wlan0
```

erweitern. Dann wird auch bei jedem Start gleich der WPA Schlüssel mit geladen

## Und wenn alles geklappt hat.....