Themenabend Wireless LAN

Was nicht auf der Verpackung steht

Axel Wachtler <axel.wachtler@gmx.de>

Frank Becker <fb@alien8.de>

Sven Klemm <sven@elektro-klemm.de>

Chaostreff Dresden http://www.c3d2.de

2004-03-12

Agenda

- Protokoll
- WEP-Attacke mit Airsnort
- im Netz des Nachbarn (Wardriving)
- Risiko WLAN Home-Router
- VPN in 10 min
- Freie Netze: Mobile Mesh

Das Protokoll

(Präsentation von Axel)

WEP-Knacken

WEP-Attacke mit Airsnort

- http://airsnort.shmoo.com/
- AirSnort benötigt ca. 5-10 Millionen verschlüsselte Pakete. 1 Mio. Pakete rund 1GB (variabel)
- Ca. 16 Mio Schlüssel möglich für WEP (128 bit Key), ca. 3000...9000 davon sind haben schwachen Schlüssel („interesting“).
- Dann braucht AirSnort weniger als 1s.
- Für einen 128 Bit Schlüssel, ca. 1500...4500 „interesting“ Pakete benötigt. Für andere Schlüssellängen, ca. 115 Pakete pro Byte Schlüssellänge (optimistisch).
- http://www.heise.de/security/artikel/38099/0

WEP-knacken: wepattack

- http://wepattack.sf.net
- Brute Force Wörterbuchattacke
- kann mit john genutzt werden

  http://www.openwall.com/john
- 1 Packet necessary

Aufspüren von W-LANs (Wardriving)

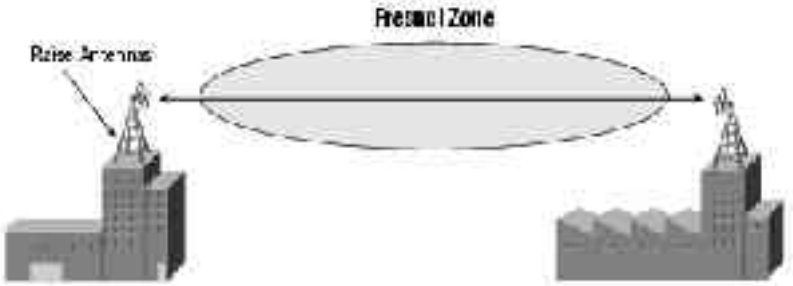
Wardriving Hardware

- Ausrüstung:
  - Laptop mit Prism2/Orinoco/Cisco WLAN-Karte (Karte muss sich in Monitor Mode schalten lassen)
  - optional: externe Antenne
  - optional: GPS-Maus
  - viel elektrische Energie ;)

Antennen

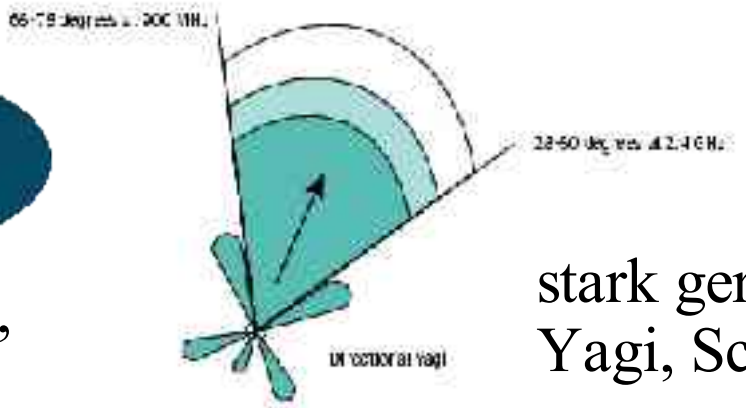
http://www.cisco.com/en/US/products/hw/wireless/ps469/products_data_sheet09186a008008883b.html

- Funkwellen im 2.4 - 2.4835 GHz Band
- Sichtkontakt (Taschenlampe)



Omidirektional
Rundstrahler

leicht gerichtet,
Patchantenne

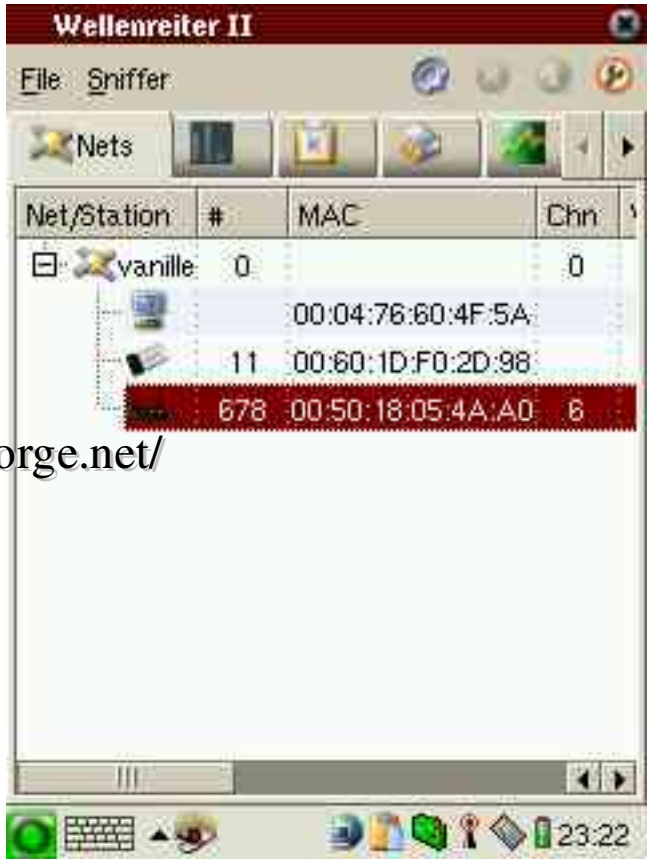


stark gerichtet
Yagi, Schüssel

Antennen

Wardriving: Software

- Kismet http://www.kismetwireless.net
- Wellenreiter http://www.wellenreiter.net/
- Prismstumbler http://prismstumbler.sourceforge.net/
- Airsnort http://airsnort.shmoo.com/
- wavemon
- Netzwerkanalysetools (nmap, hping2, nc, p0f, nbtscan, amap, dsniff, ip, nemesis, ifconfig, arpspoof, arping, tcpdump, ethereal, ethercap, vim,...)



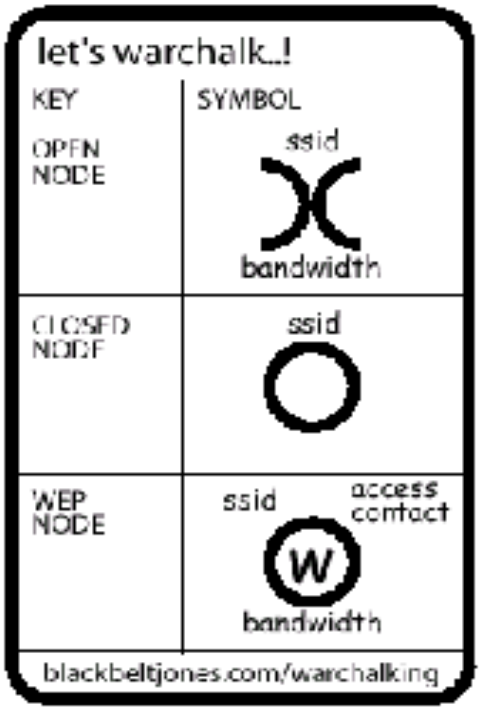
Wardriving: Vorgehen

- NIC MAC Adresse variieren

```
ifconfig eth1 hw ether 01:02:03:04:05:06
```

- Antenne in die Luft

<u>Standard SSIDs</u>
·3Com: 101
·Addtron: WLAN
·Cisco: tsunami
·Compaq: Compaq
·Intel: intel
·Linksys: linksys
·Netgear: NETGEAR



Wardriving: Netzscan

- passives Scannen (auf allen Kanälen lauschen)
  - warten auf beacon Frames (beinhalten SSID, Übertragungsraten, Zeitstempel, ...)
- aktives Scannen (wenn SSID versteckt ist
  - warten auf *Probe Request* (Broadcast) von Client, sendet SSID mit
  - Server antwortet mit *Probe Response*
  - einige APs antworten auf *Probe Request* mit SSID ANY oder „“ mit der SSID
  - *Association Request* enthält auch SSID

Wardriving: Kismet

- das Kismet -
  im Islam das dem Menschen von Allah zugeteilte, unabänderliche Schicksal

Wardriving: Kismet Beispiel

```
Network 3: "www.fbn-dd.de (KAM)" BSSID: "00:02:2D:40:9A:E0"
    Type      : infrastructure
    Carrier   : 802.11b
    Info      : "None"
    Channel   : 01
    WEP       : "No"
    Maxrate   : 11.0
    LLC       : 5
    Data      : 0
    Crypt     : 0
    Weak      : 0
    Total     : 5
    First     : "Wed Mar 10 23:07:57 2004"
    Last      : "Wed Mar 10 23:08:58 2004"
    Min Loc: Lat 51.069492 Lon 13.756177 Alt 414.809998 Spd 0.000000
    Max Loc: Lat 51.069492 Lon 13.756177 Alt 414.809998 Spd 0.000000
```

Wardriving: Bsp. Hotelnetz

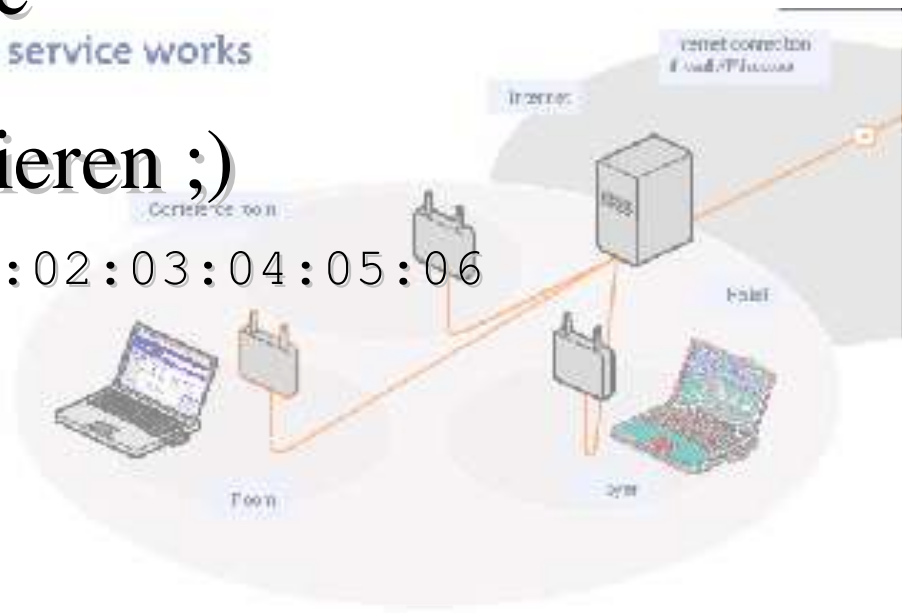
Swisscom Eurospot Retailpricing (including VAT) (in € if not specified)

Voucher Type	Germany	United Kingdom, Ireland	France	Benelux	Spain, Portugal	Italy	Pan Europe**
VAT included	16,0%	17,5%	19,6%	Bel: 21% Ned: 19% Lux: 15%	Spain: 16% Portugal: 17%	20,0%	Country of Purchase
1/2 h*	4,50	£ 3,00	4,50	4,50	4,50	4,90	5,20
2 h*	9,50	£ 5,00	9,50	9,00	7,50	9,90	10,90
24 h*	24,50	£ 17,00	29,00	29,00	15,00	19,90	27,90
7 days*	69,00	£ 46,00	69,00	65,00	69,00	59,90	77,90
30 days*	129,00	£ 86,00	129,00	115,00	129,00	99,90	145,90
1 year*	949,00	£ 633,00	1020,00	949,00	949,00	799,90	1079,00

WD: MAC-Zugangskontrolle

- MAC-Adresse der WLAN-Karte auf Access Point freigeschaltet
- unverschlüsselter Traffic
- NIC MAC Adresse variieren ;)

```
ifconfig eth1 hw ether 01:02:03:04:05:06
```

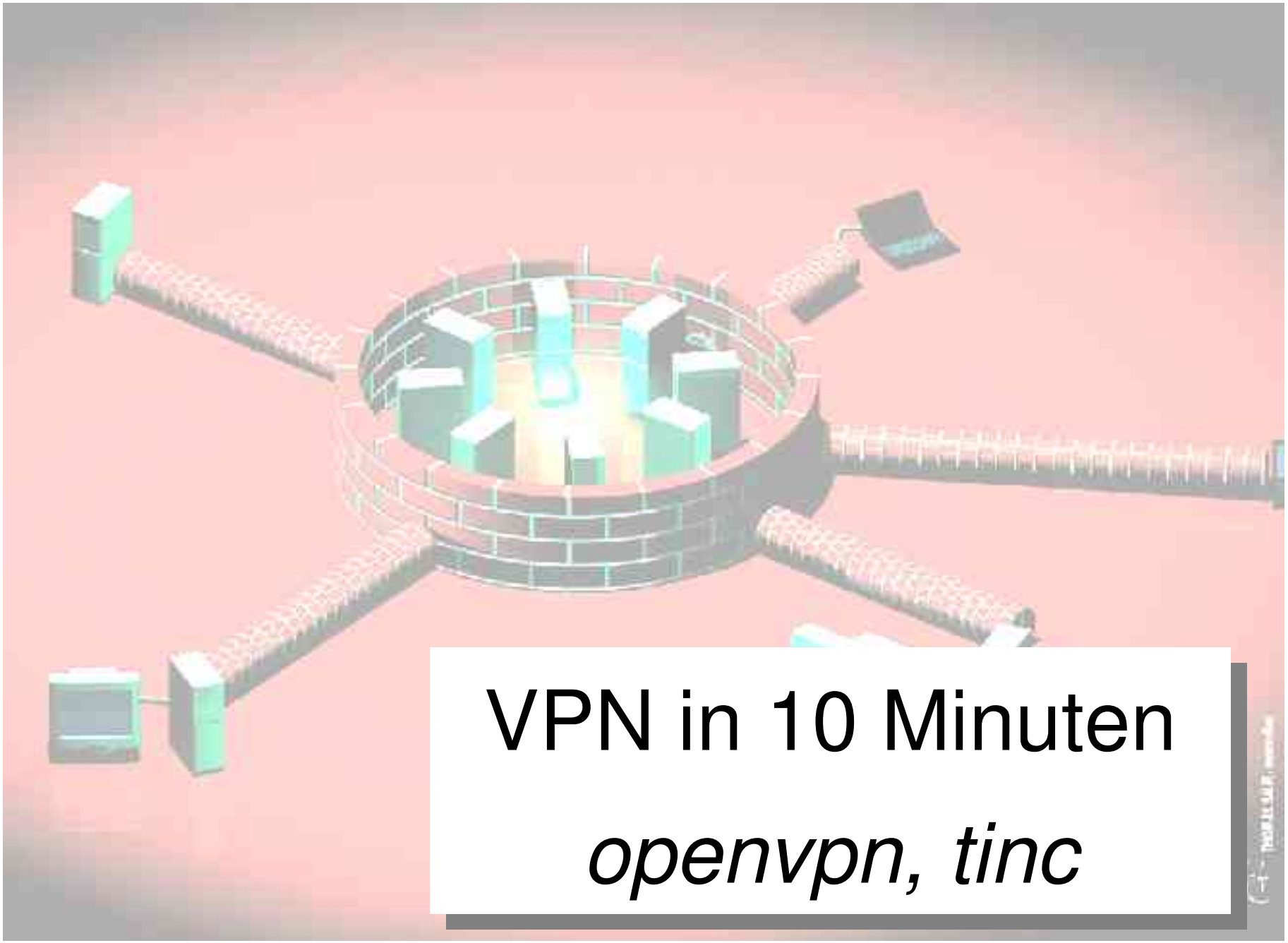


W-LAN SOHO Router

(Demonstration von Sven)

W-LAN Soho-Router

- Absicherung:
  - Anleitung lesen
  - Defaulteinstellungen ändern
  - nach Firmware-Upgrades suchen/fragen
  - zusätzliche Schutzmechanismen (z. B. Firewall) nutzen

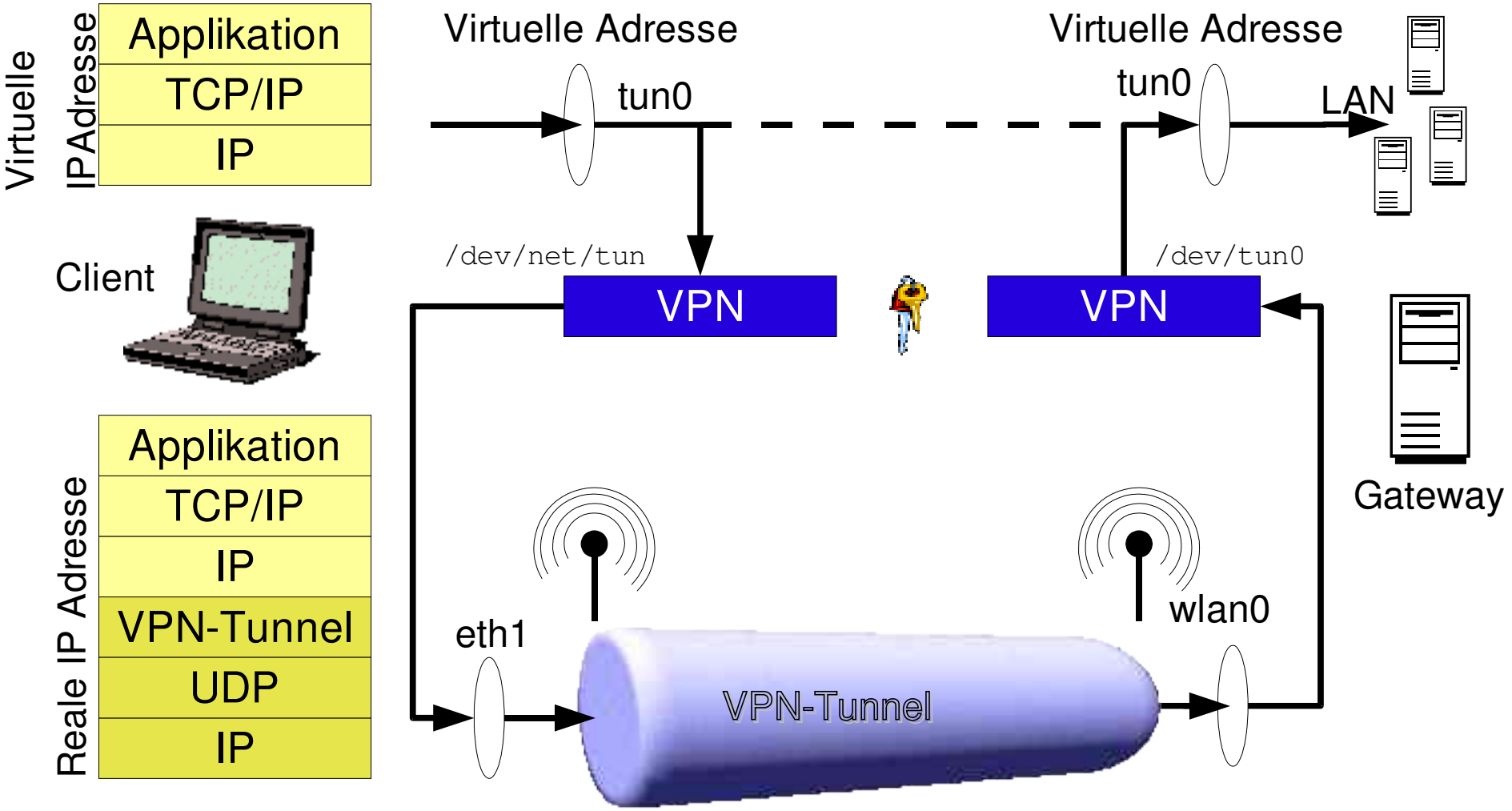


VPN in 10 Minuten

openvpn, tinc

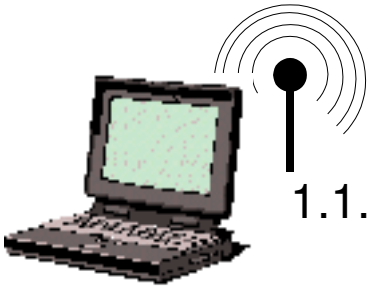
VPN: Tunnel Prinzip

nach „Offener Tunnel“ Linux-Magazin 01/2003



VPN: OpenVPN Quick Setup

http://openvpn.sourceforge.net




```
modprobe tun

openvpn --remote 2.2.2.2 --dev tun0 \
    --ifconfig 10.0.0.2 10.0.0.1
```

mit Verschlüsselung

```
openvpn --remote 2.2.2.2 --dev tun0 \
    --ifconfig 10.0.0.1 10.0.0.2 \
    --secret key
```

```
modprobe tun
echo 1 > /proc/sys/net/ipv4/ip_forward
openvpn --remote 1.1.1.1 --dev tun0 \
--ifconfig 10.0.0.1 10.0.0.2
```

mit Verschlüsselung

```
openvpn --genkey --secret key
scp key root@1.1.1.1:

openvpn --remote 2.2.2.2 --dev tun0 \
    --ifconfig 10.0.0.1 10.0.0.2 \
    --secret key
```

Firewall anpassen! Achtung, UDP 5000 auf WLAN I/Fs erlauben

http://slackerbit.ch/archives/2002/12/11/**securing_wifi_with_openvpn**.html

VPN: OpenVPN mit Config-Files


```
kruitzer:~# less /etc/openvpn/gw.conf
#!/bin/bash
# Fire up openvpn shared secret vpn
# Frank Becker <fb@alien8.de>
#
dev tun0
dev-node /dev/misc/net/tun
remote 192.168.8.254
ifconfig 192.168.4.228 192.168.4.1
secret /etc/openvpn/openvpn.key
```

```
gw:~# less /etc/openvpn/gw.conf
#!/bin/bash
# Fire up openvpn shared secret vpn
# Frank Becker <fb@alien8.de>
#
dev tun0
remote 192.168.8.228
#float
ifconfig 192.168.4.1 192.168.4.228
secret /etc/openvpn/openvpn.key
# OpenVPN uses UDP port 5000 by default.
# Each OpenVPN tunnel must use
# a different port number.
port 5000
#daemon
```

VPN: OpenVPN Features

- Tunnelt IP über single-port UDP oder TCP
- cross-platform: Linux, Solaris, OpenBSD, FreeBSD, NetBSD, Mac OS X, and Windows 2000/XP (auch dazwischen)
- alle Kypto-, Zertifizierungs- u. Authentifizierungsfeatures von OpenSSL
- alle Cipher, Schlüssellängen, HMAC von OpenSSL
- statischer Key oder Zertifikatsbasierte Public Key Verschlüsselung
- real-time adaptive Kompression und Traffic Shaping
- dynamische Endpunkte (DHCP, dynamische IP-Adressen)
- Tunnel über NAT
- Tunnel über Bridges mit virtual tap device

VPN: Tinc Features

http://tinc.nl.linux.org

- Verschlüsselung, Authentifizierung (OpenSSL) und Kompression (zlib)
- automatisches Full Mesh Routing
- Einfach erweiterbares VPN (neues Config-File, fertig)
- Bridges möglich
- IPv6 Unterstützung
- O/S: Linux, FreeBSD, OpenBSD, NetBSD, Mac OS/X, Solaris, Windows 2000/XP

VPN: Tinc Quick Setup 1(2)

http://www.vanheusden.com/Linux/tinc_mini_howto.html


```
mkdir -p /etc/tinc/hosts

cat /etc/tinc/tinc.conf
ConnectTo=gw-wlan
Device=/dev/net/tun
Name=cl1-wlan
PrivateKeyFile=/etc/tinc/rsa_key.priv

tincd -K

cat << EOF >> /etc/tinc/hosts/cl1-wlan
Subnet=192.168.1.0/24
Address=1.1.1.1
EOF
scp /etc/tinc/hosts/cl1-wlan \
    2.2.2.2:/etc/tinc/wlan/hosts/
```

```
mkdir -p /etc/tinc/hosts

cat /etc/tinc/tinc.conf

Device=/dev/net/tun
Name=gw-wlan
PrivateKeyFile=/etc/tinc/rsa_key.priv

tincd -n wlan -K

cat << EOF >> /etc/tinc/hosts/gw-wlan
Subnet=192.168.2.0/24
Address=2.2.2.2
EOF
scp /etc/tinc/hosts/gw-wlan \
    1.1.1.1:/etc/tinc/wlan/hosts/
```

VPN: Tinc Quick Setup 2(2)

http://www.vanheusden.com/Linux/tinc_mini_howto.html


```
cat /etc/tinc/tinc-up
ifconfig $INTERFACE 192.168.1.1 \
    netmask 255.255.0.0 up
#ip address add 192.168.1.1/16 brd + \
    dev $INTERFACE label $INTERFACE
```

```
cat /etc/tinc/tinc-up
ifconfig $INTERFACE 192.168.2.1 \
    netmask 255.255.0.0 up
#ip address add 192.168.2.1/16 brd + \
    dev $INTERFACE label $INTERFACE
```

- ip-Doku: http://linux-ip.net/html/index.html
- tinc -n wlan: /etc/tinc/wlan ... für mehrere Configs
- -up,-down Skripte auch für Hosts
- FireWall: tcp 665 / udp 665
- FreeX 02/2004

Linux-Magazin 10/2003 http://www.linux-magazin.de/Artikel/ausgabe/2003/10/tinc/tinc.html

Intressant bzgl. Sicherheitsschwachstellen: IV, Seq.-Nummer

Freie Netze

Freie Netze: Definition

- nicht-kommerzieller W-LAN-Verbund
- Netzwerkinfrastruktur:
  - steht allen offen
  - kann von allen genutzt werden
  - jeder trägt seinen Teil bei
- Entspricht dem PicoPeering Agreement

Freie Netze: Warum?

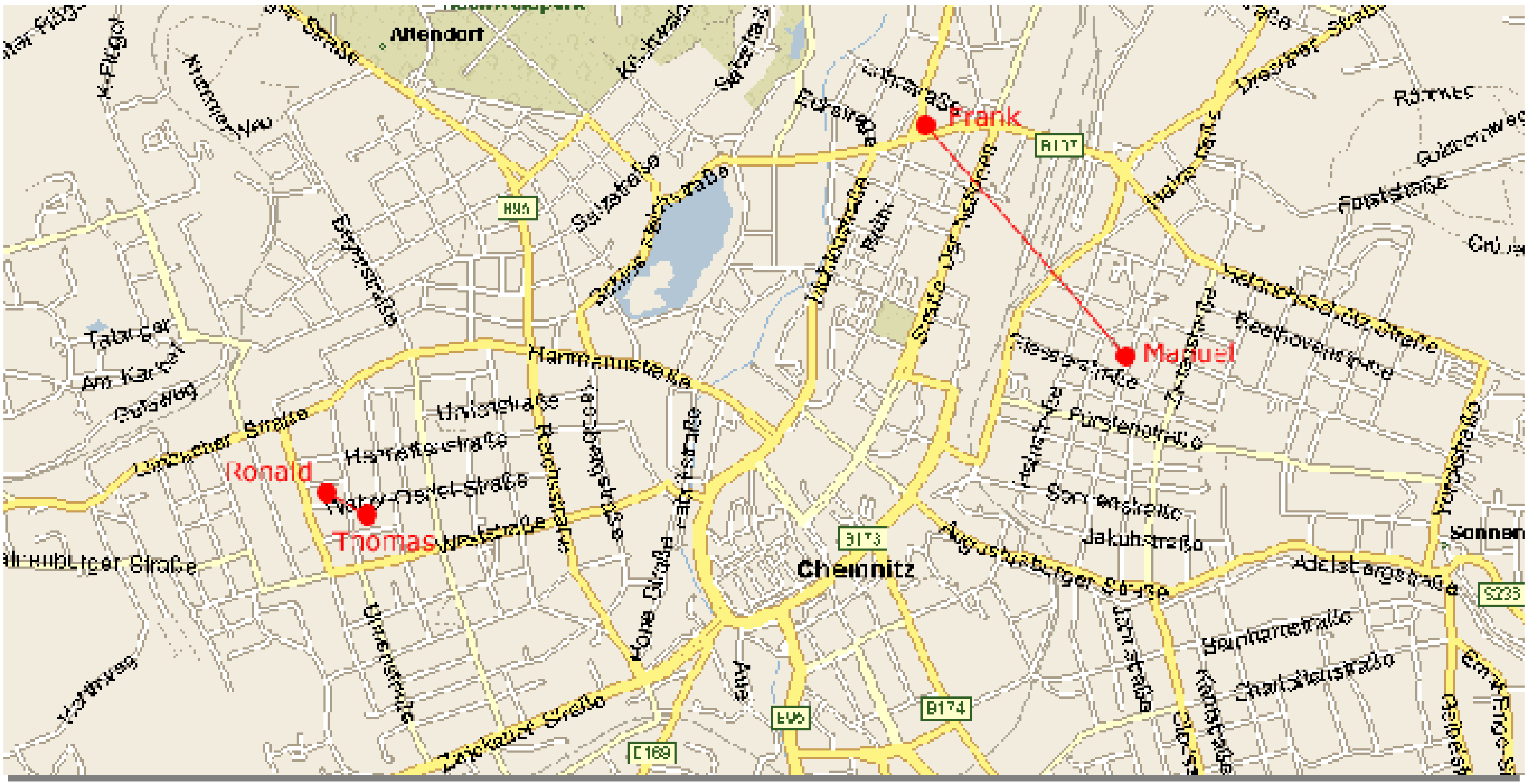
- Dient dem Austausch von Informationen, Kommunikation
- Open Source Idee
- Warum funken Amateurfunker?
- spart Geld (oder auch nicht ;)

Freie Netze: Zensur

- keine Zensur für die gewaltlose Ausübung der Meinungsfreiheit
- Wau Holland: "*Wir müssen die Rechte der Andersdenkenden selbst dann beachten, wenn sie Idioten oder schädlich sind. Wir müssen aufpassen. Wachsamkeit ist der Preis der Freiheit --- Keine Zensur!*".
- Gesellschaftl. Probleme lassen sich nicht technisch lösen.

Freie Netze: Chemnitz

- Chemnitz: http://wlan.in-chemnitz.de/



Freie Netze: Dresden

Current nodes

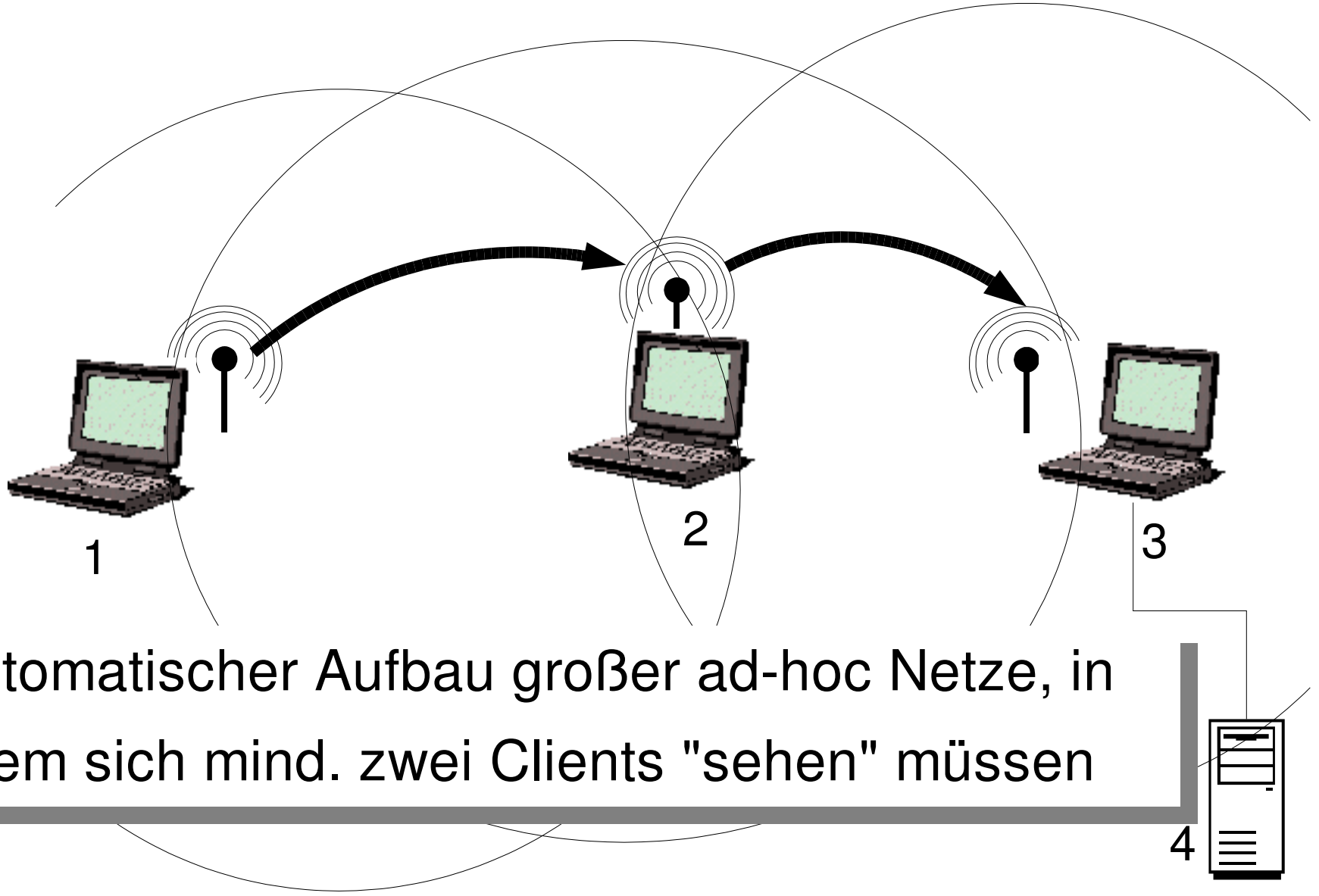
ID	Name	Suburb	Map	Ifs	Status	Age
1	Wasserfuhr.com	Pieschen			fullup	2d
2	mirdbroker.de				waiting	22d
3	intellinaut.de	Dresden			waiting	47d
4	klitzner				rootap	22d
5	Kalisti				fullup	2d
6	deffastathlon				fullup	22d
9	TUD-Zellescher-Weg				fullup	47d
10	TUD-Bergstrasse	Dresden			fullup	47d
12	Albrechter				waiting	22d

Topographic view

Network connectivity view


Mobile
Mesh

Mobile Mesh: Was ist das?



automatischer Aufbau großer ad-hoc Netze, in dem sich mind. zwei Clients "sehen" müssen

Mobile Mesh: Protokolle

- Link Discovery (MMLDP)
  - Hello message mit eignen I/F-Adressen und I/F-Adressen von der letzten Hello message
- Routing (MMRP)
  - basiert auf „link state approach“ und verwendet „least cost paths“ zw. jeder Quelle und jedem Ziel.
  - zusätzl. LSP Liste von "externen Route Advertisements"
- Border Discovery(MMBDP)
  - Tunnel zw. zwei oder mehr Knoten über Festnetz

Mobile Mesh: Software

- `mmdiscover` - Link discovery
- `mmrp` - Mobile Mesh Routing Protocol und bestimmt „least cost“ Routen
- `mmborder` – Aufspüren von „Border Routen“ und automatisch Tunnel aufsetzten

Aufruf: Freies WLAN mit MM

- Interessenten bitte E-Mail an

  fb@alien8.de

- Bald (Juni) Mailingliste, Web-Seite
- Freiwillige vor!

Und jetzt?

Auf in's Troll!