

# Attacks on Wireless Networks

Nelson Murilo  
[<nelson@pangeia.com.br>](mailto:<nelson@pangeia.com.br>)



# Agenda

- Profile
- Types of wireless networks
- Wi-Fi network characteristics
- Today's standards
- Available protection methods
- Diagnostic tools
- Why attack wireless networks?
- Attacking low protection networks
- Attacking well-protected networks
- Conclusions

# Types of wireless networks

- Infrared
- Bluetooth
- Mobile telephone  
(GSM/GPRS/TDMA/CDMA/Edge/EVDO/etc.)
- **Wi-Fi**

# Wi-Fi network characteristics

- Wi-Fi uses **Industrial, Scientific&Medical (ISM)** bands

902	928 MHz
2.4	2.485 GHz (2.4 a 2.5 GHz in Brazil)
5.150	5.825 GHz

- WiMax (802.16/a) uses licensed bands (10-66/2-10Ghz)

# Wi-Fi network characteristics

- IEEE 802.11

Several standards already closed:

802.11b 22Mb 2.4Ghz

802.11a 54Mb 5.1GHz

802.11g 54Mb 2.4Ghz

802.11i - Security mechanisms

802.1x – Authentication mechanisms are used in cable and wireless networks

# Today's standards

**802.11b**

**WEP**

**802.11a/g**

**WEP/WPA (802.1x)**

**802.11i**

**WEP/WPA/RSN (AES,Ad-Hoc, etc)**

# Analysing tools



# Analysing tools

- Kismet
- Netstumbler
- Airsnort
- BSD Airtools
- WepCrack
- WepLab
- WepTools
- WepAttack
- Tcpdump
- Ngrep
- Ethereal

# Kismet

- Support to 802.11a/b/g
- Integration to GPS
- Produces traffic file in PCAP format
- Capable of generating maps (**gpsmap**)
- Detailed information:
  - Network name
  - Standard (a/b/g)
  - WEP use
  - Connected clients (mac, signal level,etc)
- **No break WEP**

# Kismet

Lat -15.763 Lon -47.881 Alt 3613.5f Spd 14.730m/h Hdg 0,000 Fix NONE D01:36:58

### Status JS

## Saving data files.

Found new network "Homenet54" bssid 00:07:40:4D:1A:5C WEP N Ch 3 @ 11.00 mbi

## Saving data files.

## Sorting by SSID

Battery: 76% 1h43m13s

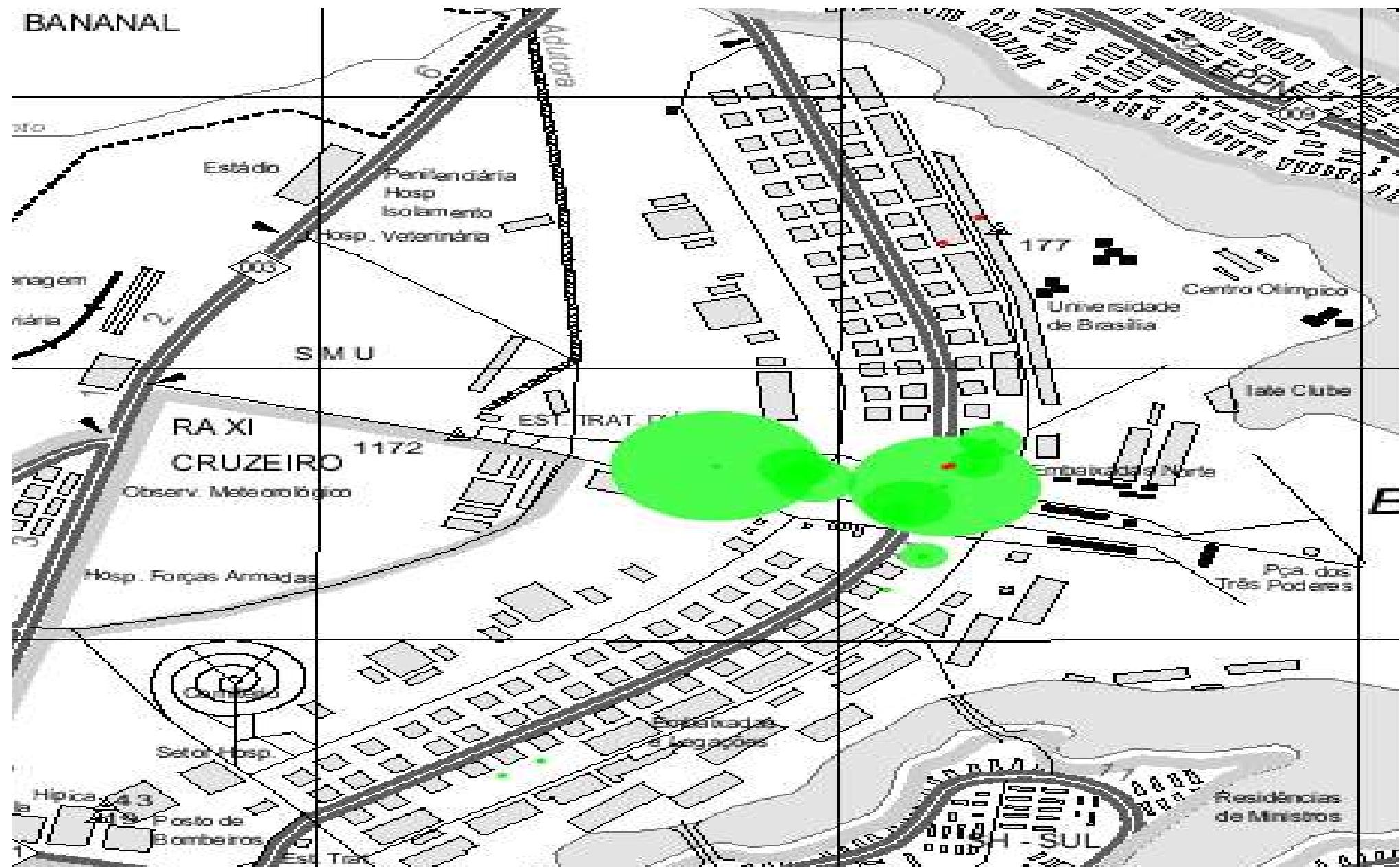
# Kismet

Network List—(SSID) Info  
Ntwrks

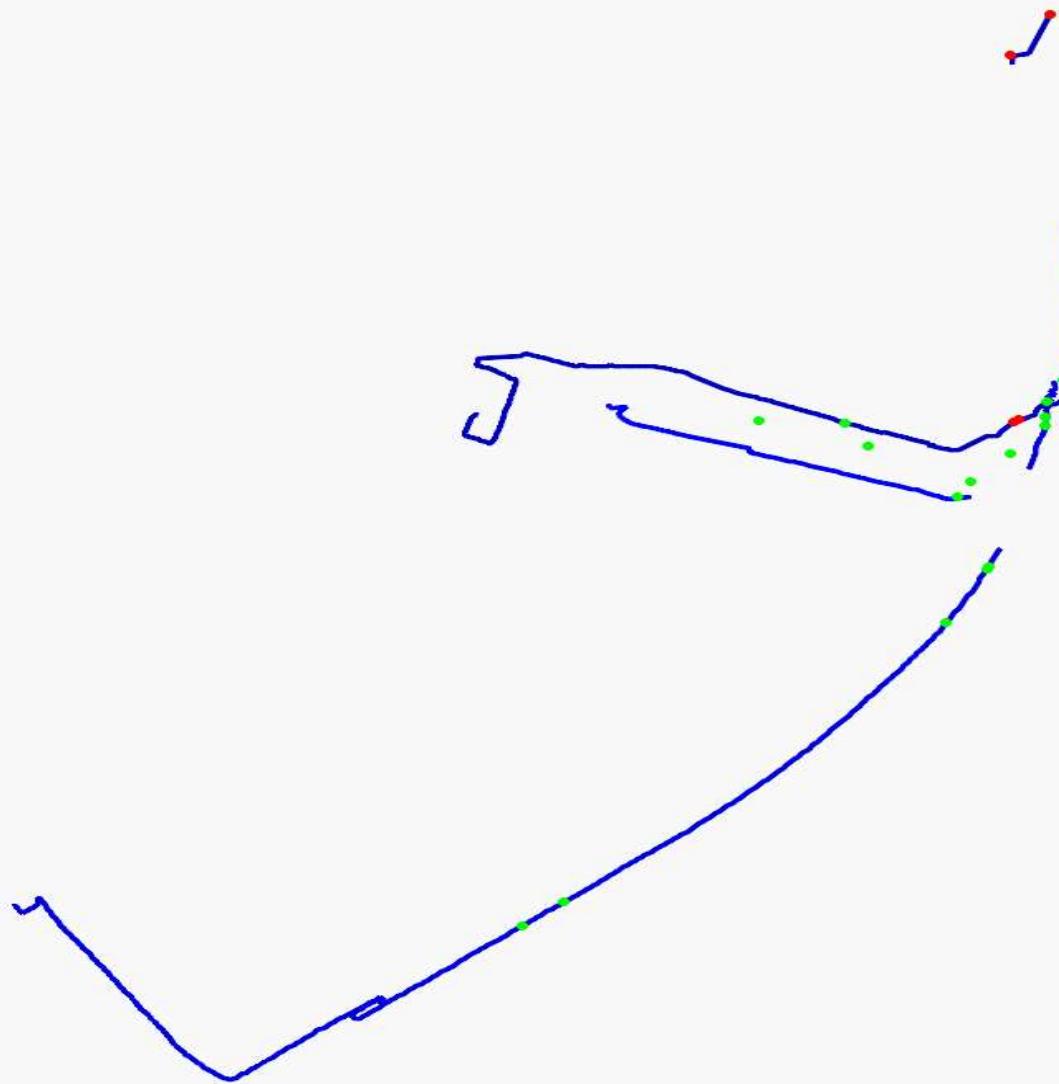
Name	T	W	Ch	Packts	Flags	IP Range
+ Data Strings Dump						All
icover						
zoneedit						
soacontact						
icover						
icover						
zoneedit						
soacontact						
icover						
icover						
zoneedit						
GET /RealMedia/ads/adstream_jx.ads/microsoftidg/homepage@Top3!Top3 HTTP/1.1						
Connection: Keep-Alive						
User-Agent: Mozilla/5.0 (compatible; Konqueror/2.2.2; QtEmbedded/640x480)						
Referer: http://idgnow.uol.com.br/AdPortalv5/Default.aspx						
Accept: application/x-javascript						
Accept-Encoding: x-gzip, gzip, identity						
Accept-Charset: iso-8859-1, utf-8, *, utf-8, *						
Accept-Language: en						
Host: www.icover.com.br						

Battery: 73% 1h35m25s

# Kismet



# Kismet



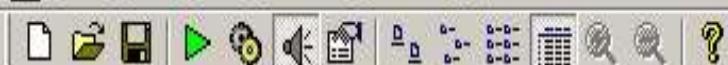
# Netstumbler

- Supports several plates 802.11a/b/g
  - GPS integration
  - Detailed information of signal level, WEP use and connected users (MAC)
- 
- Only for Windows
  - Doesn't capture traffic
  - No break WEP

# Netstumbler

Network Stumbler - [20040623181455.ns1]

File Edit View Device Window Help



MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR
0040F480B74E			1	11 Mbps		AP		
000C41A12534	linksys		6	11 Mbps	Linksys	AP		
02022D1D3D1A	montreal		10	11 Mbps	Proxim (Agere) ORINOCO	Peer	WEP	
02E027EDB080	UNINETVarig		1	11 Mbps	(User-defined)	Peer		
00022D512E88			1	11 Mbps	Proxim (Agere) ORINOCO	AP		
00601DF0FB60			3	11 Mbps	Proxim (Agere/WaveLAN)	AP		
00022D937760			9	11 Mbps	Proxim (Agere) ORINOCO	AP		
000278E33A12			11	2 Mbps	Samsung	AP		
00062524EA56			5	2 Mbps	Linksys	AP		
0006252579FD			9	11 Mbps	Linksys	AP		
00409655C84C	taz57kar		6	11 Mbps	Cisco	AP	WEP	
00032F1C0DB7	santa		6	22 Mbps	GST (Linksys)	AP		
000C41BD527F	linksys		1	11 Mbps	Linksys	AP		

# Airsnort

- Graphic interface
- File generation in PCAP format
- Permits file loading in PCAP format
- Support WEP key break (~100Mb-1Gb)
- GPS integration
- WEP use information
- Low number of plates (chipsets) supported
- No details with connected clients and signal levels

# Airsnort

**AirSnort**

**File Edit Settings Help**

		Network device <b>eth0</b>		Refresh		40 bit crack breadth: <b>20</b>					
		Driver type <b>wlan-ng</b>				128 bit crack breadth: <b>2</b>					
<b>Load crack file</b>											
<b>Save crack file</b>											
<b>Log to file</b>											
<b>Load pcap file</b>											
<b>Exit</b>		Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	PW: Hex	PW: ASCII
FF:FF:FF:FF:FF:FF				Tue Jun 29 13:37:45 2004	00:00:00	11	134	0	0		
00:02:2D:1E:3A:51				Tue Jun 29 14:18:11 2004	00:00:00		431	0	0		
00:40:F4:80:B7:4E				Tue Jun 29 13:42:03 2004	00:00:00		244	0	0		
00:0C:41:42:49:E4	Y			Tue Jun 29 13:41:18 2004	00:00:00	1	19	0	0		
00:0D:88:A6:CE:FB				Tue Jun 29 13:41:27 2004	00:00:00	6	2	0	0		
00:00:00:00:00:00	Y			Tue Jun 29 13:42:32 2004	00:00:00		1	0	0		
00:90:4B:0B:9C:F2 wireless				Tue Jun 29 13:54:01 2004	AA:AA:03		42	26	0		
00:0C:41:18:6D:BF	Y			Tue Jun 29 13:44:37 2004	00:00:00	6	3	0	0		
00:01:F4:75:24:2B	Y			Tue Jun 29 13:45:40 2004	00:00:00	11	2	0	0		
00:02:2D:93:77:60 APIS402				Tue Jun 29 13:46:14 2004	97:68:F0		1	1	0		
00:02:2D:51:2E:88 UNINetVarigSul	Y			Tue Jun 29 14:02:08 2004	00:00:00	9	52	0	0		
00:02:6F:05:44:05	Y			Tue Jun 29 14:18:10 2004	AA:AA:03	1	1136	1093	0		
00:60:1D:F0:FB:60 APISSouth				Tue Jun 29 13:49:48 2004	24:4B:01		58	57	0		
00:60:1D:F0:FC:9D				Tue Jun 29 14:04:25 2004	00:00:00	3	26	0	0		
00:02:78:F4:6A:A8 CPAP				Tue Jun 29 14:01:47 2004	00:00:00	11	37	0	0		
90:38:12:7C:3C:AB	Y			Tue Jun 29 13:48:51 2004	00:00:00	6	2	0	0		
00:06:25:24:9E:00				Tue Jun 29 13:51:37 2004	18:B8:68		1	1	0		
76:00:BA:00:93:01 MB06	Y			Tue Jun 29 14:01:48 2004	00:00:00	3	15	0	0		
02:E0:27:ED:B0:80 UNINetVarig				Tue Jun 29 13:52:39 2004	00:00:00	6	2	0	0		
00:06:F4:04:D1:9B				Tue Jun 29 14:02:02 2004	00:00:00	1	23	0	0		
00:0C:41:18:38:CB LookVg1				Tue Jun 29 13:53:11 2004	00:00:00		3	0	0		
58:65:DF:D3:98:52				Tue Jun 29 13:54:46 2004	00:00:00	6	1	0	0		
00:E0:98:BE:A1:7A MetroY				Tue Jun 29 13:58:17 2004	00:00:00		1	0	0		
				Tue Jun 29 14:18:10 2004	00:00:00	1	15	0	0		

**Start**    **Stop**    **Clear**

# WepAttack

- Attacks based in:
  - Brute force
  - Dictionary
- Reads files in PCAP format
- Permits integration with traditional password breakers, like **John The Ripper**

# WepLab

- Attacks based in :
  - Brute force
  - Dictionary
  - Vector initialization fragilness
- Reads files in PCAP format
- Breaks faster than other tools since there is no correct traffic standard

# Ethereal

- Graphic tool (Unix/Windows)
- Reads and records in PCAP format
- Permit traffic filtering
- Permits several types of statistical generation
- Permits reassembling of traffic
- Doesn't have resources for search patterns

# Ethereal

(Untitled) - Ethereal

File Edit View Capture Analyze Statistics Help

Display Match Prepare

Follow TCP stream

Stream Content

GET / HTTP/1.1  
Host: www.h2hc.com.br  
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.7) Gecko/20040624 Debian/1.7-2  
Accept: text/xml,application/xml,application/xhtml+xml+xml;text/html;q=0.9;text/plain;q=0.8,image/png,\*/\*;q=0.7  
Accept-Encoding: gzip,deflate  
Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7  
Keep-Alive: 300  
Connection: keep-alive  
If-Modified-Since: Mon, 14 Jun 2004 19:29:59 GMT  
If-None-Match: "1f40ea-16c8-40cdfcb7"

HTTP/1.1 304 Not Modified  
Date: Wed, 07 Jul 2004 05:27:53 GMT  
Server: Apache  
Connection: close  
ETag: "1f40ea-16c8-40cdfcb7"

Frame 164 (76 bytes on wire, 76 bytes captured)  
Linux cooked capture  
Internet Protocol, Src Addr: 192.168.11.3 (192.168.11.3), Dst Addr: 200.206.136.1 (200.206.136.1)  
Transmission Control Protocol, Src Port: 48991 (48991), Dst Port: 80 (80)

00 00 04 00 01 00 06 00 e0 00 87  
10 45 00 00 3c eb f7 40 00 40 06 :  
20 c8 ce 88 54 80 78 00 50 d2 f2 5  
30 a0 02 16 d0 b3 ee 00 00 02 04

Filter: (ip.addr eq 192.168.11.3 and port 80)

Gravar Como Imprimir Entire conversation (579 bytes) ASCII E

Filter out this stream X Fechar

# ATTACK!

A GAME OF WORLD CONQUEST

AND EXPANSION



the road to VICTORY!



EAGLE GAMES

AGES 10  
AND UP

# Available protection methods

- Disabling ESSID broadcast
- Filtro de MAC
- Disabling ESSID broadcast
- Individual client traffic isolation
- WEP
- 802.1x
- WPA
- WPA2/RSN
- Monitoring

# Disabling ESSID broadcast

AirSnort

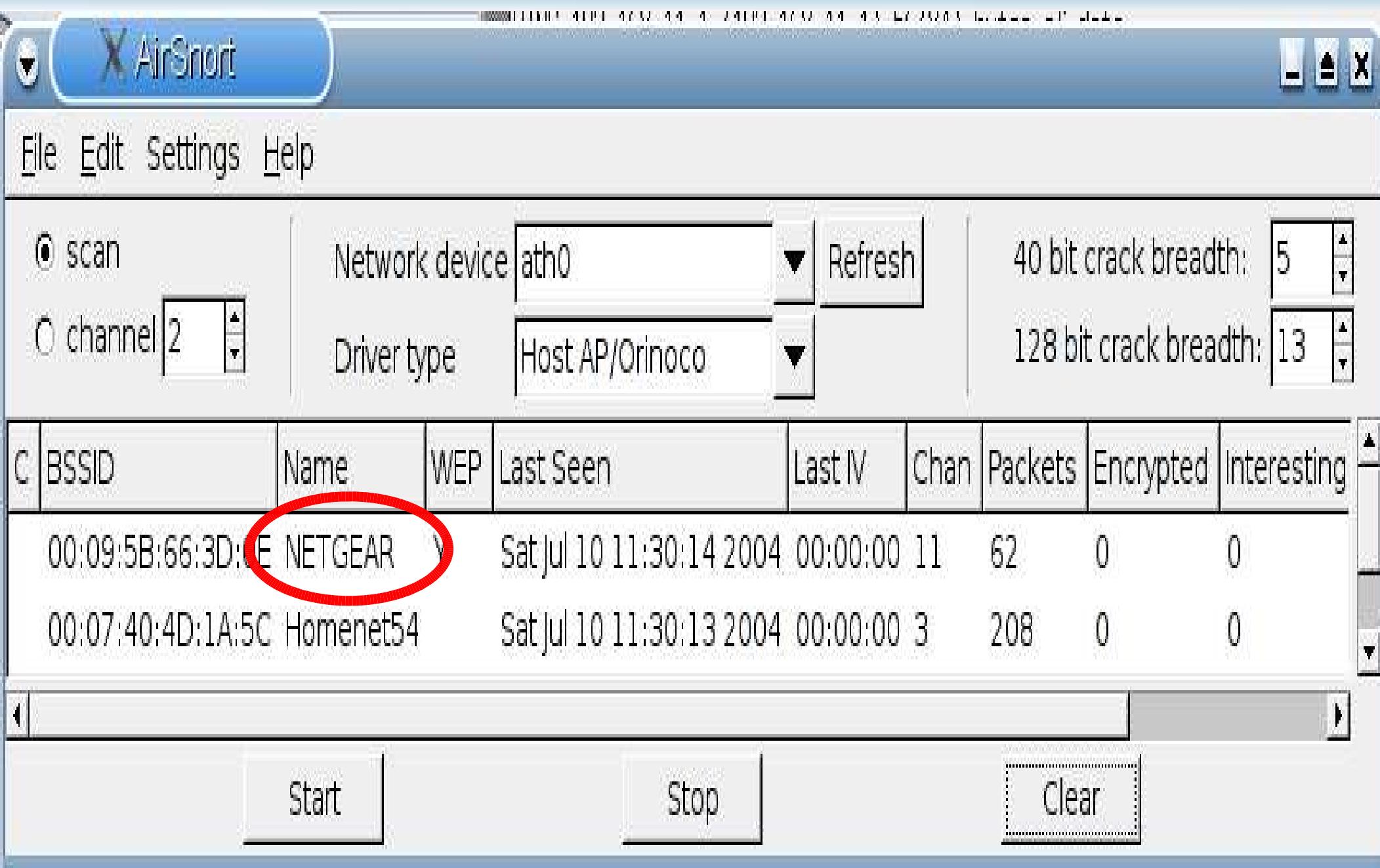
File Edit Settings Help

scan      Network device: ath0      Refresh  
 channel [2]      Driver type: Host AP/Orinoco

40 bit crack breadth: 5      128 bit crack breadth: 13

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting
	00:09:5B:66:3D:E	NETGEAR		Sat Jul 10 11:30:14 2004	00:00:00	11	62	0	0
	00:07:40:4D:1A:5C	Homenet54		Sat Jul 10 11:30:13 2004	00:00:00	3	208	0	0

Start      Stop      Clear



# Disabling ESSID broadcast

## Options

Channel / Frequency:

11 / 2.462GHz ▾

Data Rate:

best ▾

Transmit Power:

full ▾

Beacon Interval:  
(20 - 1000)

100 ms

DTIM (1 - 255):

1

WEP/WPA Status

Enabled

[Configure WEP/WPA](#)

## Access Point Connections

Allow access by:

All Wireless stations

Trusted PCs only

[Trusted PCs List](#)

**Enable bridging to wired LAN**

**Enable ESSID broadcast**

# Disabling ESSID broadcast

AirSnort

File Edit Settings Help

scan      Network device: ath0      Refresh      40 bit crack breadth: 5  
 channel 6      Driver type: Host AP/Orinoco      128 bit crack breadth: 13

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interest
	00:09:5B:66:3D:0E		Y	Fri Jul 9 22:43:50 2004	00:00:00	11	8	0	0
	00:07:40:4D:1A:5C	Homenet54		Fri Jul 9 22:43:50 2004	00:00:00	3	11	0	0

Start Stop Clear

# Disabling ESSID broadcast

Kismet-Jul-09-2004-1.dump - Ethereal

File Edit View Capture Analyze Statistics Help

No. Time Source Destination Protocol Info

196	47.625055	Melco_4d:1a:5c	Broadcast	IEEE 802 Beacon frame
197	47.627722	Netgear_66:3d:0e	Broadcast	IEEE 802 Beacon frame
198	47.729449	Netgear_66:3d:0e	Broadcast	IEEE 802 Beacon frame
199	48.851042	Netgear_66:1e:3d	Broadcast	IEEE 802 Beacon frame
200	48.953120	Netgear_66:1e:3d	Broadcast	IEEE 802 Beacon frame
201	50.391745	Netgear_66:3d:0e	Broadcast	IEEE 802 Beacon frame
202	50.494164	Netgear_66:3d:0e	Broadcast	IEEE 802 Beacon frame
203	51.121786	Melco_4d:1a:5c	Broadcast	IEEE 802 Beacon frame
204	51.224310	Melco_4d:1a:5c	Broadcast	IEEE 802 Beacon frame

Frame 202 (81 bytes on wire, 81 bytes captured) ....

    > IEEE 802.11

    > IEEE 802.11 wireless LAN management frame

        > Fixed parameters (12 bytes)

        > Tagged parameters (45 bytes)

            Tag Number: 0 (SSID parameter set)

            Tag length: 7

            Tag interpretation: .....

0000 80 00 00 00 ff ff ff ff ff ff 00 09 5b 66 3d 0e .....[f=..

0010 00 09 5b 66 3d 0e b0 12 37 b0 94 1a 00 00 00 00 ..[f=... 7.....

0020 64 00 31 04 00 07 00 00 00 00 00 00 00 01 08 82 d.1.....

0030 84 8b 96 0c 18 30 48 03 01 0b 05 04 00 01 00 00 .....0H.....

0040 07 06 55 53 20 01 0b 1b 2a 01 00 32 04 12 24 60 ..US ... \*..2..\$`

0050 6c | .....

Filter: Expression... Limpar Aplicar File: Kisme P: 379 D: 379

# Disabling ESSID broadcast

Kismet-Jul-09-2004-1.dump - Ethereal

File Edit View Capture Analyze Statistics Help

No. Time Source Destination Protocol Info

195	46.514662	Melco_4d:1a:5c	Broadcast	IEEE 802 Beacon frame
196	47.025839	Melco_4d:1a:5c	Broadcast	IEEE 802 Beacon frame
197	47.627722	Netgear_66:3d:0e	Broadcast	IEEE 802 Beacon frame
198	47.729449	Netgear_66:3d:0e	Broadcast	IEEE 802 Beacon frame
199	48.851042	Netgear_66:1e:3d	Broadcast	IEEE 802 Beacon frame
200	48.953120	Netgear_66:1e:3d	Broadcast	IEEE 802 Beacon frame
201	50.391745	Netgear_66:3d:0e	Broadcast	IEEE 802 Beacon frame
202	50.494164	Netgear_66:3d:0e	Broadcast	IEEE 802 Beacon frame
203	51.121786	Melco_4d:1a:5c	Broadcast	IEEE 802 Beacon frame
204	51.224310	Melco_4d:1a:5c	Broadcast	IEEE 802 Beacon frame
205	51.326591	Melco_4d:1a:5c	Broadcast	IEEE 802 Beacon frame
206	51.634823	Melco_4d:1a:5c	Broadcast	IEEE 802 Beacon frame
207	51.808480	Aqere_2b:e3:1d	Broadcast	IEEE 802 Probe Request

Tag interpretation: Homenet54

0000 80 00 00 00 ff ff ff ff ff ff 00 07 40 4d 1a 5c .....@M.\  
0010 00 07 40 4d 1a 5c 20 c1 90 01 92 13 8c 00 00 00 ..@M.\ .....  
0020 64 00 01 00 00 09 48 6f 6d 65 6e 65 74 35 34 01 d....Homenet54.  
0030 04 82 84 8b 96 03 01 03 05 04 00 01 00 00 2a 01 .....\*.  
0040 07 2f 01 07 32 08 0c 12 18 24 30 48 60 6c dd 05 ./2...\$0H`I..  
0050 00 10 18 01 01 .....

Filter: Expression... Limpar Aplicar Interpretation P: 379 D: 379

# Disabling ESSID broadcast

Kismet-Jul-09-2004-1.dump - Ethereal

No. Time Source Destination Protocol Info

204	51.224310	Melco_4d:1a:5c	Broadcast	IEEE 802 Beacon frame
205	51.326591	Melco_4d:1a:5c	Broadcast	IEEE 802 Beacon frame
206	51.634823	Melco_4d:1a:5c	Broadcast	IEEE 802 Beacon frame
207	51.808480	Agere_2b:e3:1d	Broadcast	IEEE 802 Probe Request
208	51.837298	Agere_2b:e3:1d	Broadcast	IEEE 802 Probe Request
209	51.879227	Agere_2b:e3:1d	Broadcast	IEEE 802 Probe Request
210	51.892972	Agere_2b:e3:1d	Netgear_66:3d:0e	IEEE 802 Association Request
211	51.894428	Netgear_66:3d:0e	Agere_2b:e3:1d	IEEE 802 Association Response

Frame 207 (39 bytes on wire, 39 bytes captured) ....

IEEE 802.11

IEEE 802.11 wireless LAN management frame

Tagged parameters (15 bytes)

Tag Number: 0 (SSID parameter set)

Tag length: 7

Tag Interpretation: NETGEAR

Tag Number: 1 (Supported Rates)

0000 40 00 00 00 ff ff ff ff ff 00 02 2d 2b e3 1a @..... ....-+..  
0010 ff ff ff ff ff 50 13 00 07 4e 45 54 47 3 41 .....P...NETGEA  
0020 52 01 04 02 04 0b 16 R.....

Filter: Expression... Limpar Aplicar Interpretation P: 379 D: 379

# Disabling ESSID broadcast

```
23:05:16.386193 Beacon () [1.0 2.0 5.5 11.0 6.0 12.0 24.0 36.0 Mbit]
ESS CH: 11
23:05:16.488612 Beacon () [1.0 2.0 5.5 11.0 6.0 12.0 24.0 36.0 Mbit]
ESS CH: 11
23:05:17.321039 Beacon (Homenet54) [1.0 2.0 5.5 11.0 Mbit] ESS
CH: 3
23:05:17.629271 Beacon (Homenet54) [1.0 2.0 5.5 11.0 Mbit] ESS
CH: 3
23:05:17.802928 Probe Request (NETGEAR) [1.0 2.0 5.5 11.0 Mbit]
23:05:17.831746 Probe Request (NETGEAR) [1.0 2.0 5.5 11.0 Mbit]
23:05:17.873675 Probe Request (NETGEAR) [1.0 2.0 5.5 11.0 Mbit]
23:05:17.887420 Assoc Request (NETGEAR) [1.0 2.0 5.5 11.0 Mbit]
```

# Disabling ESSID broadcast

There are still other moments where ESSID has traffic:

- Search for active concentrator
- Answer to concentrator search
- Concentrator reassociation

# Available protection methods

- ~~Disable ESSID broadcast~~
- MAC filter
- Individual client traffic isolation
- WEP
- 802.1x
- WPA
- WPA2/RSN
- Monitoring

# MAC filter

**NETGEAR ProSafe Dual-Band Wireless Firewall FWAG114**

**settings**

SWITCHES / ROUTERS / MODEMS / SECURITY / SUPPORT / HOME / BUSINESS / SERVICES

Setup Wizard

**Setup**

- Basic Settings
- Wireless 11a
- Wireless 11b/g

**Security**

- Logs
- Block Sites
- Rules
- Services
- Schedule
- E-mail

**VPN**

- IKE Policies
- VPN Policies
- CAs
- Certificates
- CRL
- VPN Status

**Wireless 11b/g Trusted PCs**

Trusted PCs List

Wireless Adapter MAC address

Add

Delete

Back

**Wireless 11b/g Trusted PCs Help**

**Trusted PCs List**

This lists any PCs you have entered. If you have not entered any PCs, this list will be empty.

To delete an existing entry, select it and then click the "Delete" button.

**Add new Trusted PC**

Use this to add PCs to the *Trusted PCs* list.

**Wireless Adapter MAC address**

Enter the MAC address of the Wireless Adapter. This is also called the *Physical Address*, *Hardware Address* or *MAC address*. It consists of 12 Hex digits. (A hex digit has a value of 0 to 9 or A to F). The software provided with your Wireless card can be used to determine the address of the Wireless adapter.

Click the "Add" button to add your entry to the Trusted PC list.

# MAC filter

Wireless LAN Access Point  
**AirStation**  
**WBR-G54**

[▲Return to TOP](#)

[▼LAN settings](#)

[Wireless](#)

[Wireless security](#)

[LAN port](#)

[DHCP server](#)

[Wireless LAN](#)

[Computer  
Limitation](#)

[Wireless  
bridge\(WDS\)](#)

[►WAN settings](#)

[►Network  
settings](#)

[►Management](#)

[►Logout](#)

## Access Limit

Do not  
limit

Registration for the connecting PC's MAC address

Only registered PC's can communicate with the AirStation after the Limit button has been Set.

MAC address to be registered  Register Number(0/64)

MAC Address

List of all PCs that are allowed to communicate

MAC Address

00:E0:00:87:62:0D  Enable connection

# Filtro de MAC

## Linux

```
# ifconfig ath0 hw ether 00:00:00:00:00:01
```

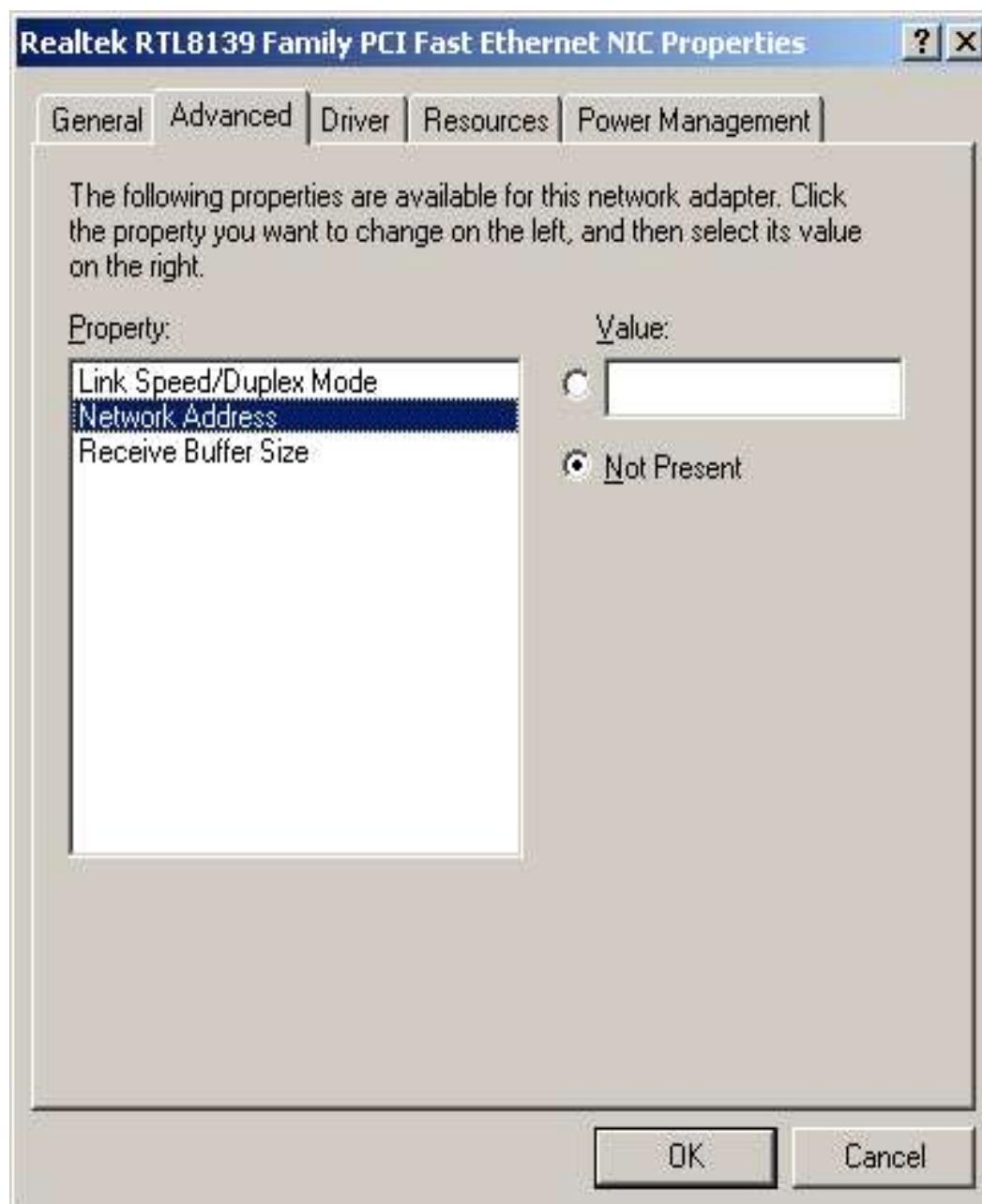
## FreeBSD

```
# ifconfig xl3 ether 00:00:00:00:00:01
```

## OpenBSD/NetBSD

```
# wiconfig wi0 -m 00:00:00:00:00:01
```

# MAC filter

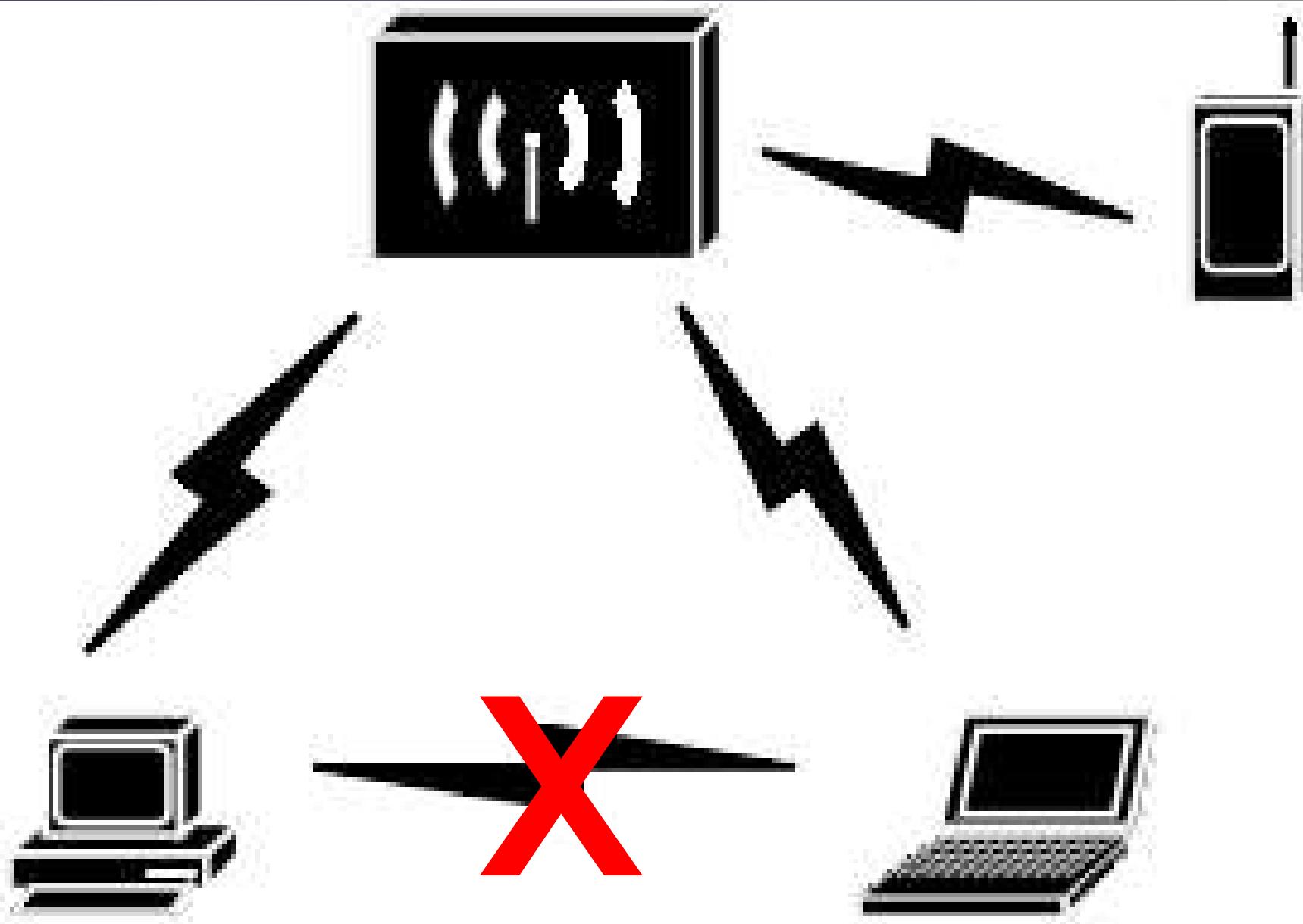


# Available protection methods

- ~~Disable ESSID broadcast~~
- ~~MAC filter~~
- Individual client traffic isolation
- WEP
- 802.1x
- WPA
- WPA2/RSN
- Monitoring

# Client traffic isolation

PSPF( Publicly Secure Packet Forwarding) ou Privacy Separator



# Client traffic isolation

```
ping -c 3 192.168.11.2
PING 192.168.11.2 (192.168.11.2) 56(84) bytes of data.
From 192.168.11.4 icmp_seq=1 Destination Host Unreachable
From 192.168.11.4 icmp_seq=2 Destination Host Unreachable
From 192.168.11.4 icmp_seq=3 Destination Host Unreachable
--- 192.168.11.2 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time
2017ms
```

**However, traffic continues to be possibly captured**

```
22:44:37.605465 192.168.11.2.33010 > oscommerce.pulver.com.www: . ack
27075 win 59684 <nop,nop,timestamp 907215 341459491> (DF)
22:44:37.609406 oscommerce.pulver.com.www > 192.168.11.2.33010: P
27075:27120(45) ack 542 win 6492 <nop,nop,timestamp 341459495 907176>
(DF)
22:44:37.613282 192.168.11.2.33010 > oscommerce.pulver.com.www: . ack
27120 win 59684 <nop,nop,timestamp 907216 341459495> (DF)
22:44:38.260568 192.168.11.2.33010 > oscommerce.pulver.com.www: P
542:996(454) ack 27120 win 59684 <nop,nop,timestamp 907280 341459495>
(DF)
```

# Available protection methods

- Disable ESSID broadcast
- MAC filter
- Every client traffic isolation
- WEP
- 802.1x
- WPA
- WPA2/RSN
- Monitoring

# Airsnort

AirSnort

File Edit Settings Help

Load crack file Network device eth0 Refresh 40 bit crack breadth: 20  
Save crack file Driver type wlan-ng 128 bit crack breadth: 2  
Log to file  
Load pcap file

	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	PW: Hex	PW: ASCII
Exit	A:5C Homenet54 FF:FF:FF:FF:FF:FF		Tue Jun 29 13:37:45 2004 00:00:00	11	134	0	0			
	00:02:2D:1E:3A:51		Tue Jun 29 14:18:11 2004 00:00:00		431	0	0			
	00:40:F4:80:B7:4E		Tue Jun 29 13:42:03 2004 00:00:00		244	0	0			
	00:0C:41:42:49:E4	Y	Tue Jun 29 13:41:18 2004 00:00:00	1	19	0	0			
	00:0D:88:A6:CE:FB		Tue Jun 29 13:42:32 2004 00:00:00		1	0	0			
	00:00:00:00:00:00	Y	Tue Jun 29 13:54:01 2004 AA:AA:03		42	26	0			
	00:90:4B:0B:9C:F2 wireless		Tue Jun 29 13:44:37 2004 00:00:00	6	3	0	0			
	00:0C:41:18:6D:BF	Y	Tue Jun 29 13:45:40 2004 00:00:00	11	2	0	0			
	00:01:F4:75:24:2B	Y	Tue Jun 29 13:46:14 2004 97:68:F0		1	1	0			
	00:02:2D:93:77:60 APIS402		Tue Jun 29 14:02:08 2004 00:00:00	9	52	0	0			
	00:02:2D:51:2E:88 UNINetVarigSul	Y	Tue Jun 29 14:18:10 2004 AA:AA:03	1	1136	1093	0			
	00:02:6F:05:44:05	Y	Tue Jun 29 13:49:48 2004 24:4B:01		58	57	0			
	00:60:1D:F0:FB:60 APISSouth		Tue Jun 29 14:04:25 2004 00:00:00	3	26	0	0			
	00:60:1D:F0:FC:9D		Tue Jun 29 14:01:47 2004 00:00:00	11	37	0	0			
	00:02:78:F4:6A:A8 CPAP		Tue Jun 29 13:48:51 2004 00:00:00	6	2	0	0			
	90:38:12:7C:3C:AB	Y	Tue Jun 29 13:51:37 2004 18:B8:68		1	1	0			
	00:06:25:24:9E:00		Tue Jun 29 14:01:48 2004 00:00:00	3	15	0	0			
	76:00:BA:00:93:01 MB06	Y	Tue Jun 29 13:52:39 2004 00:00:00	6	2	0	0			
	02:E0:27:ED:B0:80 UNINetVarig		Tue Jun 29 14:02:02 2004 00:00:00	1	23	0	0			
	00:06:F4:04:D1:9B		Tue Jun 29 13:53:11 2004 00:00:00		3	0	0			
	00:0C:41:18:38:CB LookVg1		Tue Jun 29 13:54:46 2004 00:00:00	6	1	0	0			
	58:65:DF:D3:98:52		Tue Jun 29 13:58:17 2004 00:00:00		1	0	0			
	00:E0:98:BE:A1:7A MetroY		Tue Jun 29 14:18:10 2004 00:00:00	1	15	0	0			

Start Stop Clear

# WepAttack

```
# wepattack -w /usr/share/dic/dic1.txt -f Kismit-Jun-29-1.dump
```

```
# bzcat wordlist.bz2 | wepattack -f Kismet-Jun-29-2004-1.dump
```

```
# john --incremental --stdout:13 | wepattack -f Kismet-Jun-29-2004-1.dump
```

# WepLab

```
weplab -r Kismet-Jun-25-2004-1.dump Kismet-Jun-25-2004-1.dump
```

```
weplab - Wep Key Cracker Wep Key Cracker (v0.0.7-beta).
```

```
Jose Ignacio Sanchez Martin - Topo[LB] <topolb@users.sourceforge.net>
```

```
Total valid packets read: 286
```

```
Total packets read: 1335
```

```
10 packets selected.
```

```
Packet 0 --> 78 total lenght, 50 data lenght (just encrypted data)
```

```
Packet 1 --> 78 total lenght, 50 data lenght (just encrypted data)
```

```
Packet 2 --> 78 total lenght, 50 data lenght (just encrypted data)
```

```
Packet 3 --> 78 total lenght, 50 data lenght (just encrypted data)
```

```
Packet 4 --> 78 total lenght, 50 data lenght (just encrypted data)
```

```
Packet 5 --> 78 total lenght, 50 data lenght (just encrypted data)
```

```
Packet 6 --> 78 total lenght, 50 data lenght (just encrypted data)
```

```
Packet 7 --> 78 total lenght, 50 data lenght (just encrypted data)
```

```
Packet 8 --> 78 total lenght, 50 data lenght (just encrypted data)
```

```
Packet 9 --> 92 total lenght, 64 data lenght (just encrypted data)
```

```
Opening packet file for loading all the IV
```

```
Total valid packets read: 256
```

```
Total packets read: 1335
```

```
Total unique IV read: 25
```

```
25 Weak packets gathered:
```

```
Compressing IV table...
```

# Deciphering captured traffic

## Decrypt (included in airsnort package)

```
# decrypt (-p <pw> | -f <dictfile>) [-b] [-o <offset>] -m <bssid> -e  
<infile> -d <outfile>
```

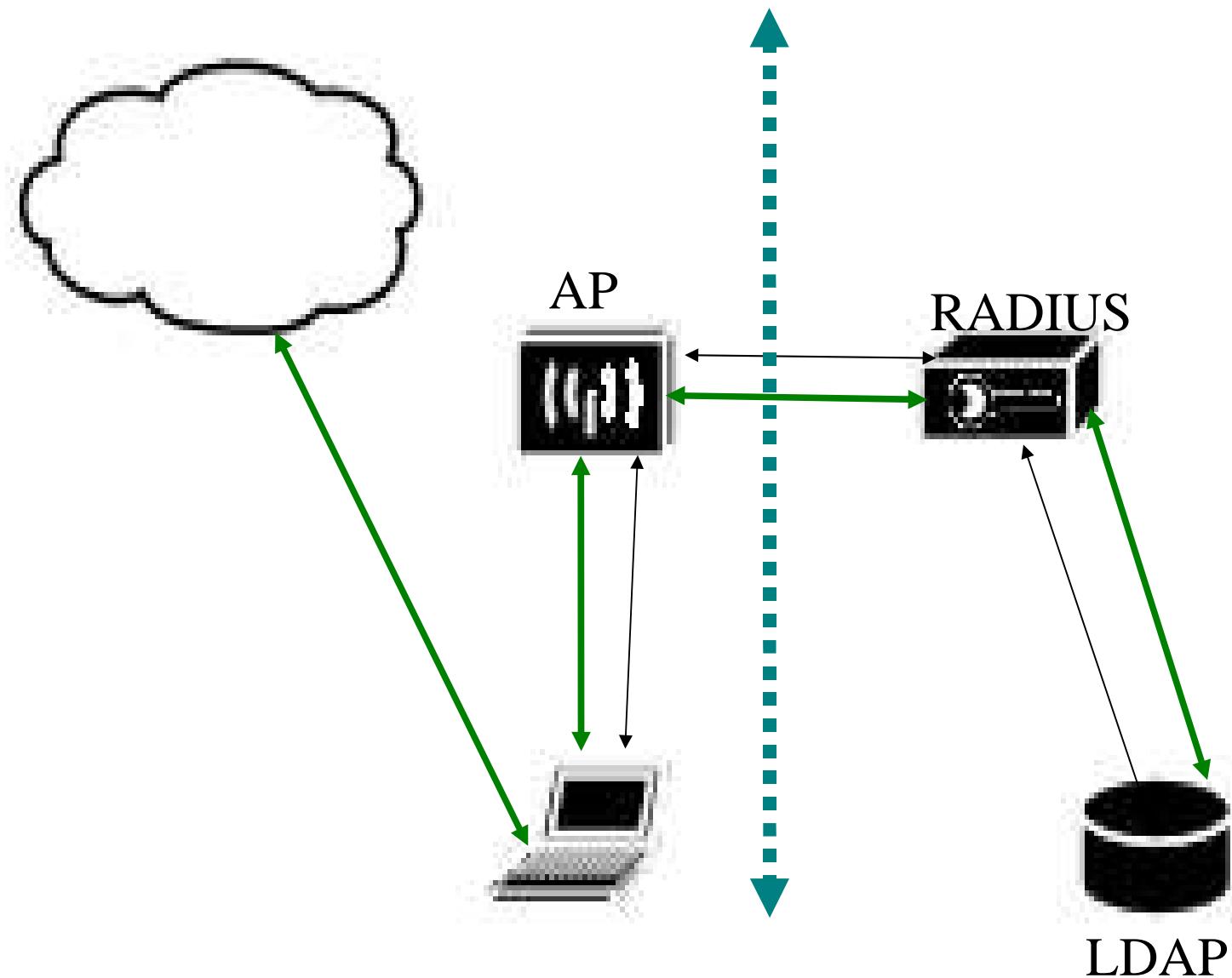
Examples:

```
# decrypt -p SMART -m AF:E8:E9:6C:11:81 -e wep.pcap -d  
nowep.pcap
```

# Available protection methods

- Disable ESSID broadcast
- MAC filter
- Individual client traffic isolation
- WEP
- 802.1x
- WPA
- WPA2/RSN
- Monitoring

# 802.1x



# 802.1x + WEP

Enabled

WEP

WEP key 

WEP key 

1: ASCII   
2: ASCII   
3: ASCII   
4: ASCII

TKIP  WPA-PSK  
(Pre-Shared Key) 

(8 to 63 characters ASCII / 64 digits hexadecimal)  
\* If IEEE802.1x/EAP authentication is used, keep this field blank.

AES 

WPA Group Rekey Interval  0 Sec

Do not authorize  Authorize

RADIUS Authentication

RADIUS Server

RADIUS Port

RADIUS Key

# XSupplicant

---

Supported methods:

- EAP-AKA
- EAP-GTC
- EAP-MD5
- EAP-MSCHAPv2
- EAP-OTP
- EAP-SIM
- LEAP
- PEAP (MSCHAPv2)
- EAP-TLS
- EAP-TTLS (CHAP, MSCHAP, MSCHAPv2, PAP)

# XSupplicant

[ALL] Got EAP-Request-Authentication.

[STATE] Processing AUTHENTICATING state.

[STATE] Sending EAPOL-Response-Authentication

[AUTH TYPE] --- SSL : SSLv3 read server hello A

[AUTH TYPE] --- SSL : SSLv3 read server certificate A

[ALL] Sending TLS ACK!

[...]

[ALL] Got EAP-Success!

Authenticated!

[ALL] Processing command : dhclient -q %i

[ALL] Returning command : dhclient -q ath0

[ALL] Actual command being called is dhclient

[ALL] Generating key block!

[ALL] Using session key const of : client EAP encryption

[STATE] (global) -> **AUTHENTICATED**

# XSupplicant

```
eap_tls {  
    user_cert = /etc/ssl/certs/cert-clt.pem  
    user_key  = /etc/ssl/certs/cert-clt.pem  
    user_key_pass = <BEGIN_PASS>verysecret<END_PASS>  
    root_cert = /etc/ssl/certs/root.pem  
    root_dir = /etc/ssl/certs  
    chunk_size = 1398  
    random_file = /dev/urandom  
}
```

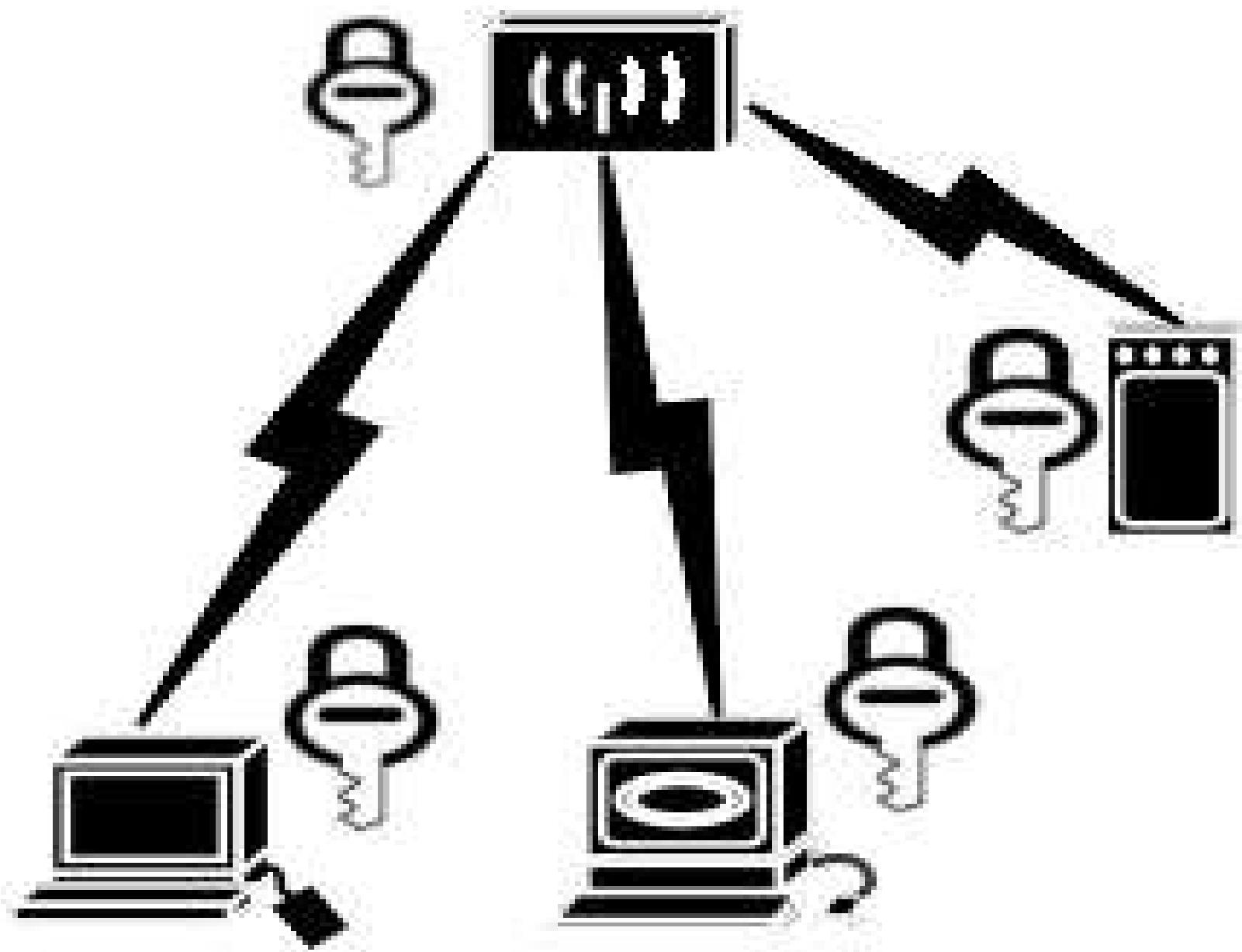
# Available protection methods

- Desabilitar broadcast do ESSID
- Filtro de MAC
- Individual client traffic isolation
- WEP
- 802.1x
- WPA
- WPA2/RSN
- Monitoring

# Attacks on WPA

- WPA – PSK ( Pre-shared Key)
- WPA Enterprise
- Attacks on concentrator
- Attacks on clients

# WPA - PSK



# WPA - PSK

```
# wpa_supplicant -w -i ath0 -c /etc/wpa_supplicant.conf -d 1
RX EAPOL from 00:09:5b:66:3d:0e
IEEE 802.1X RX: version=1 type=3 length=127
EAPOL-Key type=254
WPA: RX message 1 of Group Key Handshake from 00:09:5b:66:3d:0e
(ver=1)
WPA: Group Key - hexdump(len=32): a6 44 18 ea 08 88 f5 bc 1a 85 1a
db ab a6 3b 61 aa b6 02 78 29 57 42 7e 1d a0 69 3a f6 25 40 08
WPA: Installing GTK to the driver (keyidx=2 tx=0).
WPA: RSC - hexdump(len=6): 00 00 00 00 00 00
wpa_driver_madwifi_set_key: alg=TKIP key_idx=2 set_tx=0 seq_len=6
key_len=32
WPA: Sending EAPOL-Key 2/2
WPA: Key negotiation completed with 00:09:5b:66:3d:0e
```

# Attacks on WPA-PSK

```
static int wpa_config_parse_psk(struct wpa_ssid *ssid, int line, const char *value)
{
    if (*value == "") {
        char *pos;
        int len;
        value++;
        pos = strrchr(value, '');
        if (pos)
            *pos = '\0';
        len = strlen(value);
        if (len < 8 || len > 63) {
            wpa_printf(MSG_ERROR, "Line %d: Invalid passphrase "
                       "length %d (expected: 8..63) '%s'.",
                       line, len, value);
            return -1;
        }
        wpa_hexdump_ascii(MSG_MSGDUMP, "PSK (ASCII passphrase)",
                          value, len);
    }
    ssid->passphrase = strdup(value);
    return ssid->passphrase == NULL ? -1 : 0;
}
[...]
```

# Attacks on concentrator

## Manufacturer's configurations

<u>Manufacturer</u>	<u>Product Revision</u>	<u>Protocol</u>	<u>User</u>	<u>Password</u>	<u>Access</u>	<u>Validated</u>	
D-Link	Cable/DSL Routers/Switches	Multi	(none)	admin	Admin	No	
D-Link	DI-614+	HTTP	user	(none)	User	No	
D-Link	DI-614+	HTTP	admin	(none)	Admin	No	
D-Link	DI-701	unknown	Multi	admin	year2000	Admin	No
D-link	DI-714P+	Multi	admin	_____BLANK_____	192.168.0.1	No	
D-Link	DI-804 v2.03	Multi	admin	(none)	Admin	No	
D-Link	DWL 900AP	Multi	admin	public	Admin	Yes	

# Attacks on concentrator

Sensitive information in clear text

## Wireless 11b/g WEP/WPA Settings

Network Authentication:

Open ▾

Data Encryption:

WEP ▾

Passphrase :

64 bits ▾

Generate

Encryption Key (Hex 0-9 A-F)

Key 1:  

Key Size

64 bits ▾

Key 2:

64 bits ▾

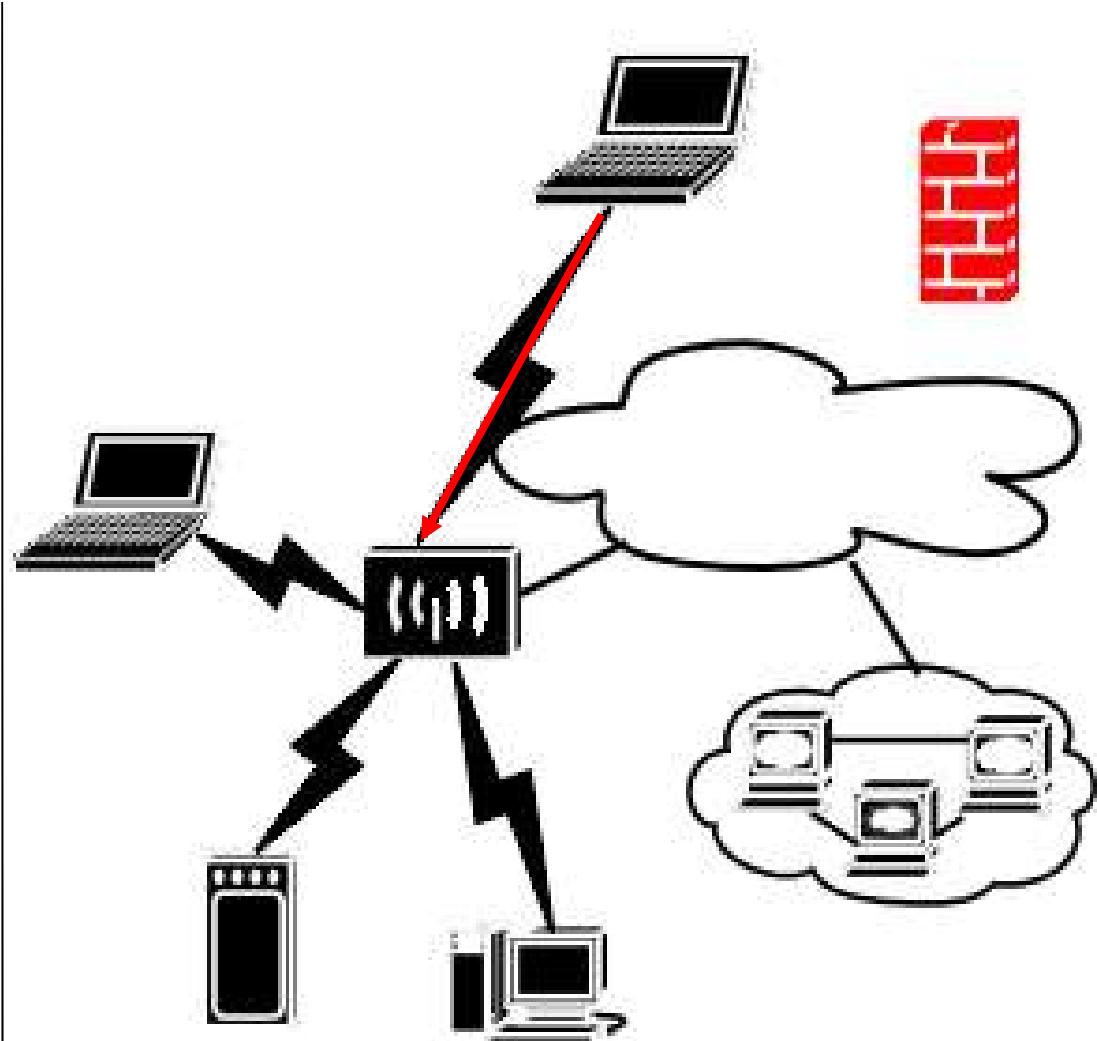
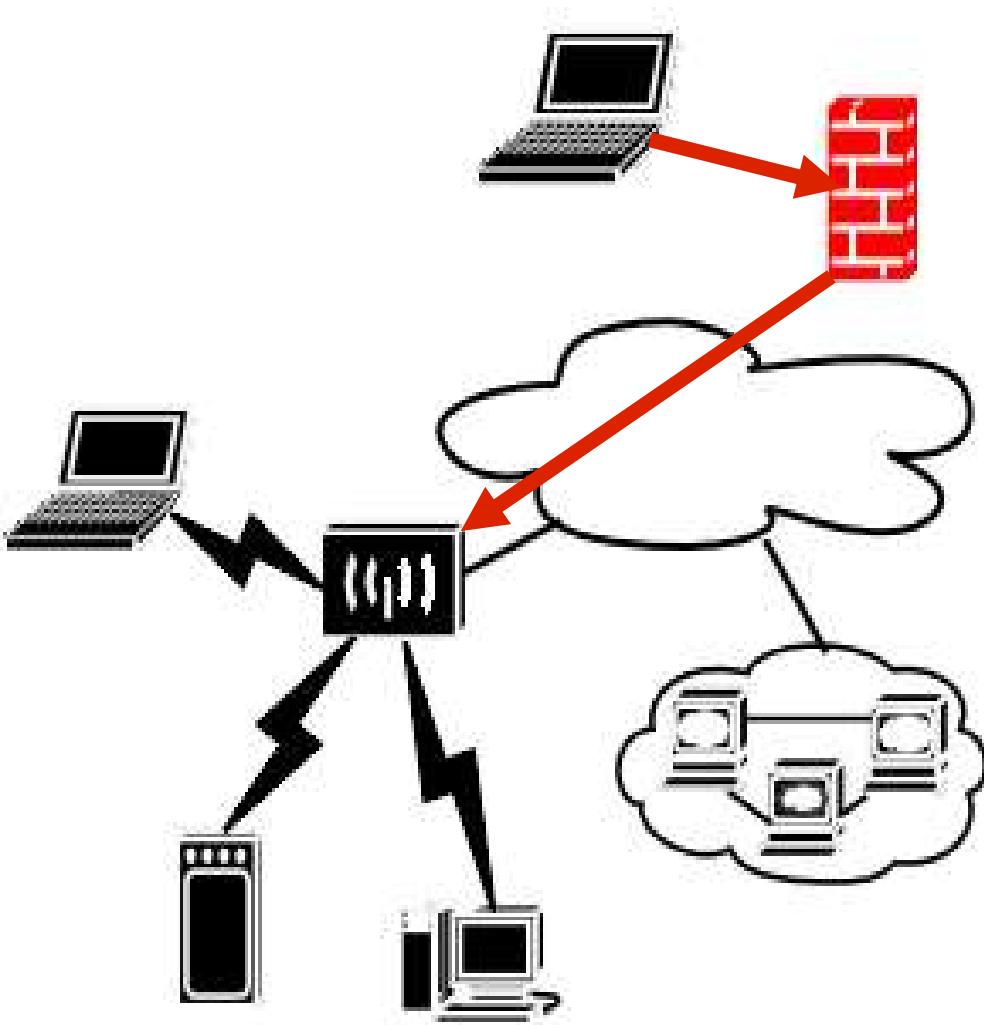
Key 3:

64 bits ▾

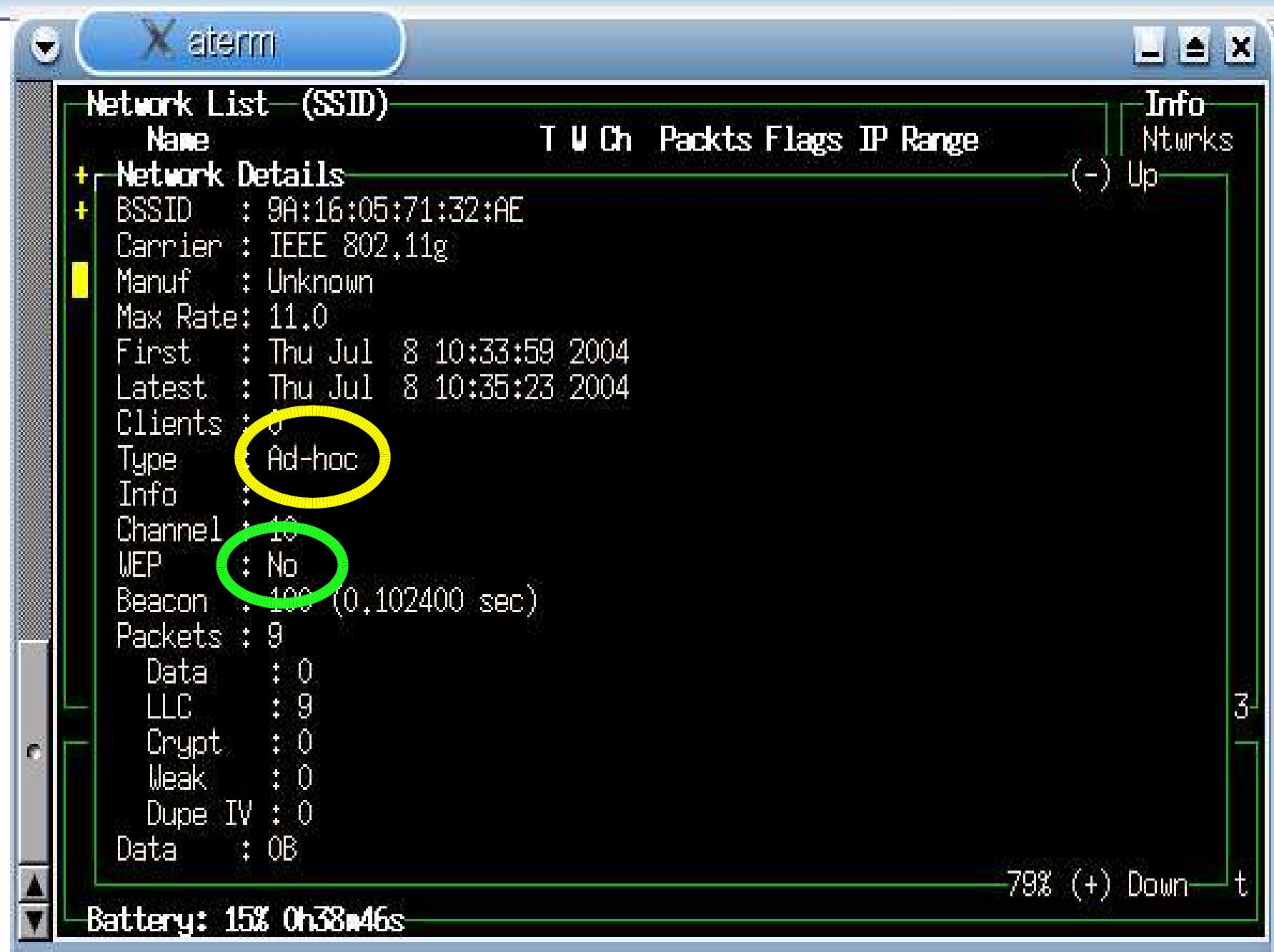
Key 4:

64 bits ▾

# Attacks on concentrator



# Attacks on clients



# Attacks on clients

```
# iwconfig wlan0 essid hotel
```

```
# iwconfig wlan0 mode Ad-Hoc
```

```
# echo "[...] hardware ethernet 9A:16:05:71:32:AE
```

```
[...]" > /etc/dhcpd.conf
```

```
# dhcpcd wlan0
```

# Attacks on clients

Network 7: "santa marta" BSSID: "00:06:25:03:21:51"

Type : probe

Carrier : 802.11g

Info : "None"

Channel : 00

WEP : "No"

Maxrate : 11.0

---

```
# airsnarf
```

# Attacks on clients

```
# iwconfig ath0
ath0    IEEE 802.11  ESSID:"NETGEAR"
        Mode:Managed  Frequency:2.462GHz
        Access Point: 00:09:5B:66:3D:0E
        Bit Rate:54Mb/s  Tx-Power:off  Sensitivity=0 / 3
        Retry:off  RTS thr:off  Fragment thr:off
Encryption key:4141-4141-41  Security mode:open
        Power Management:off
        Link Quality:46/94  Signal level:-49 dBm
        Noise level:-95 dBm
        Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
        Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

# WPA\_Supplicant

## Supported WPA/IEEE 802.11i resources:

WPA-PSK ("Personal-WPA")

WPA with EAP (p.e, com servidor RADIUS) ("WPA-Infrastructure")

Key management by CCMP, TKIP, WEP104, WEP40

WPA and full IEEE 802.11i/RSN/WPA2

RSN: PMKSA cache, pre-authentication

## EAP supported methods (IEEE 802.1X Supplicant):

EAP-TLS

EAP-PEAP/MSCHAPv2 ( PEAPv0 e PEAPv1)

EAP-PSK

EAP-PEAP/TLS (PEAPv0 e PEAPv1)

EAP-PEAP/GTC (PEAPv0 e PEAPv1)

EAP-PEAP/OTP (PEAPv0 e PEAPv1)

EAP-PEAP/MD5-Challenge (PEAPv0 e PEAPv1)

EAP-TTLS/EAP-MD5-Challenge

EAP-TTLS/EAP-GTC

EAP-TTLS/EAP-OTP

EAP-TTLS/EAP-MSCHAPv2

EAP-TTLS/EAP-TLS

EAP-TTLS/MSCHAPv2

EAP-TTLS/MSCHAP

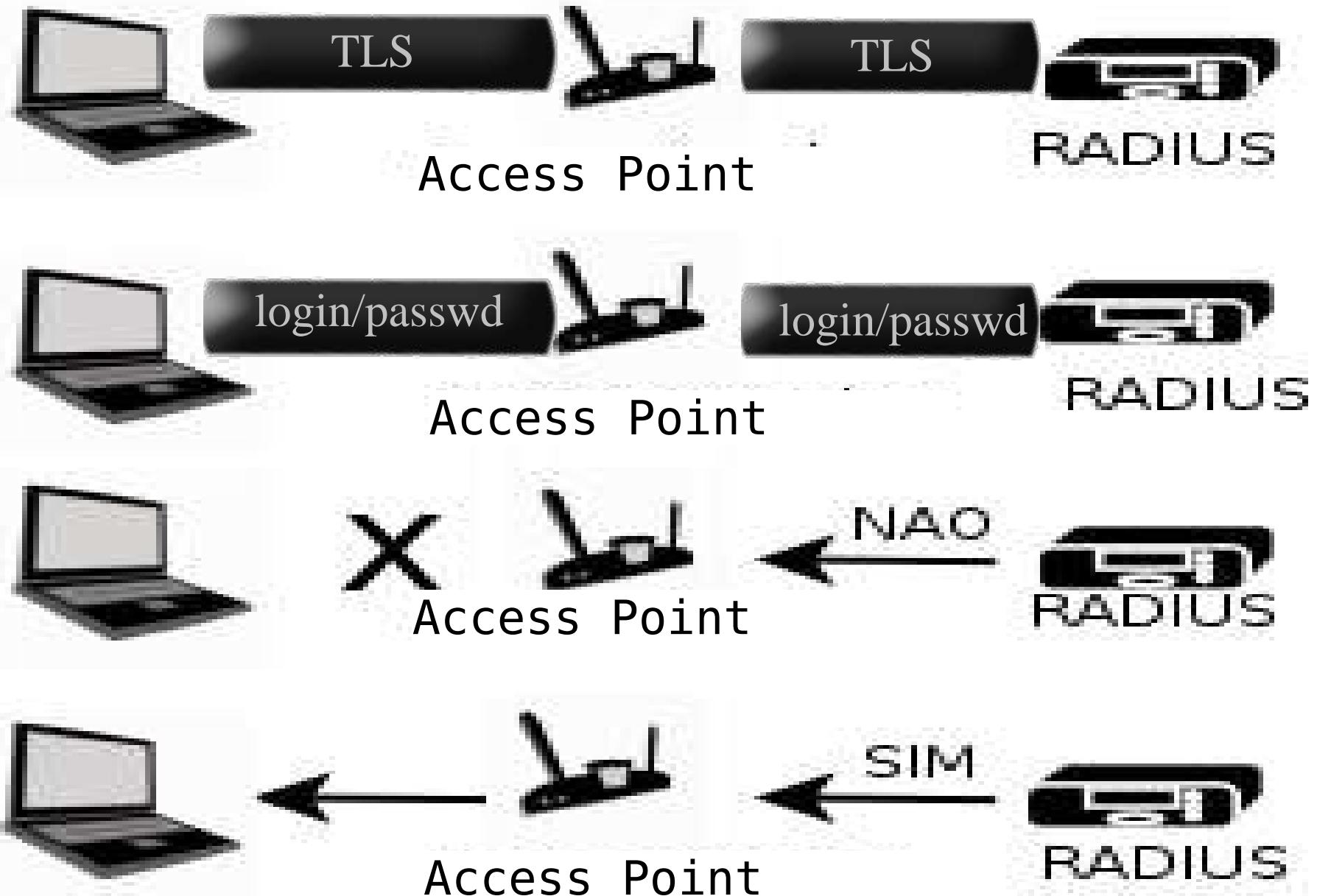
EAP-TTLS/PAP

EAP-TTLS/CHAP

EAP-SIM

EAP-AKA

# WPA EAP\_TTLS



# WPA EAP\_TTLS

[...]

EAP-TTLS: received Phase 2: code=1 identifier=6 length=22

EAP-TTLS: Phase 2 EAP Request: type=4

EAP-TTLS: Phase 2 EAP packet

EAP-MD5: generating Challenge Response

EAP-TTLS: AVP encapsulate EAP Response - hexdump(len=22): 02 06 00 16  
04 10 fa 9b b5 84 1e 18 ff 0e 3e 49 9f c4 de ee ac 0a

EAP-TTLS: Encrypting Phase 2 data - hexdump(len=32): 00 00 00 4f 40 00 00  
1e 02 06 00 16 04 10 fa 9b b5 84 1e 18 ff 0e 3e 49 9f c4 de ee ac 0a 00 00  
wpa\_driver\_madwifi\_set\_key: alg=TKIP key\_idx=1 set\_tx=0 seq\_len=6 key  
\_len=32

WPA: Sending EAPOL-Key 2/2

WPA: Key negotiation completed with 00:09:5b:66:1e:3d

Cancelling authentication timeout

EAPOL: External notification - portValid=1

EAPOL: SUPP\_PAE entering state **AUTHENTICATED**

# WPA EAP\_TTLS

```
$ cat /etc/wpa_supplicant.conf
```

```
network={  
    ssid="MARINET"  
    scan_ssid=1  
    key_mgmt=WPA-EAP  
    eap=TTLS  
    anonymous_identity="anonimo"  
    ca_cert="/etc/ssl/certs/root.pem"  
    identity="nelson"  
    password="OblesqBlom"  
}
```

```
$ cat /usr/local/etc/raddb/users
```

```
[...]  
“nelson” Auth-Type :=EAP,  
User-Password == ” OblesqBlom”
```

# WPA - EAP\_TLS

```
$ wpa_supplicant -c /etc/wpa_supplicant.conf -i ath0 -d 1
```

```
[...]
```

```
WPA: RX message 1 of Group Key Handshake from 00:09:5b:66:1e:3d (ver=1)
```

```
WPA: Group Key - hexdump(len=32): 7e 12 d0 4e ca c9 b2 c3 45 9f 43 13 c3 23 5e  
bc 97 8c 66 6f 08 8f 61 52 e1 28 eb 00 da 53 d1 52
```

```
WPA: Installing GTK to the driver (keyidx=2 tx=0).
```

```
WPA: RSC - hexdump(len=6): 00 00 00 00 00 00
```

```
wpa_driver_madwifi_set_key: alg=TKIP key_idx=2 set_tx=0 seq_len=6 key_len=32
```

```
WPA: Sending EAPOL-Key 2/2
```

```
WPA: Key negotiation completed with 00:09:5b:66:1e:3d
```

```
Cancelling authentication timeout
```

```
EAPOL: External notification - portValid=1
```

```
EAPOL: SUPP_PAE entering state AUTHENTICATED
```

# WPA EAP\_TLS

```
$ cat /etc/wpa_supplicant
```

```
network={  
    ssid="MARINET"  
    scan_ssids=1  
    proto=WPA  
    pairwise=CCMP TKIP  
    group=CCMP TKIP  
    key_mgmt=WPA-EAP  
    eap=TLS  
    identity="nelson"  
    #ca_cert="/etc/ssl/certs/demoCA/cacert.pem"  
    ca_cert="/etc/ssl/certs/root.pem"  
    client_cert="/etc/ssl/certs/cert-clt.pem"  
    private_key="/etc/ssl/certs/cert-clt.pem"  
    priority=1  
private_key_passwd='5upers3crEt'  
}
```



# Available protection methods

- Desabilitar broadcast do ESSID
- Filtros de MAC
- Isolamento do tráfego de cada cliente
- WEP
- 802.1x
- WPA
- WPA2/PSK
- Monitoring

# Monitoring

---

**“The optimist does not know what awaits him.”**

**-- Millor Fernandes, Brazilian writer**

# Monitoring

## Generic Monitoring

- Logs, snort, prelude, etc

## Specific Monitoring

- Access pointer resources. kismet, snortwireless, etc

## Best of both worlds

- kismet + snort

# Monitoring

## Access Pointer

### Attached Devices

#### DHCP Addresses

#	IP Address	Device Name	MAC Address
1	192.168.0.3	--	00:0c:41:0a:25:20
2	192.168.0.2	--	00:e0:98:74:c0:ba

Refresh

# Monitoring - Kismet

- Netstumbler, Wellenreiter, Airjack,
- SSID same name switching channels
- Associate and continue probe
- Disassociation requests in broadcast

# Monitoring - Kismet

Network List (SSID)

Name	T	U	Ch	Packts	Flags	IP Range	Size
* ! Howenet54	A	N	003	250	T4	200.215.182.20	0B
* MARINET	A	Y	052	29		0.0.0.0	0B
NETGEAR	A	N	011	158		0.0.0.0	0B

Info

Ntrwrks	3
Pckts	503
Cryptd	0
Weak	0
Noise	4
Discrd	61
Pkts/s	0
athero	
Ch:	2
Elapsd	00:08:26

Status

ALERT: Suspicious client 00:02:2D:2B:E3:1D - probing networks but never participating.  
ALERT: Suspicious client 00:02:2D:2B:E3:1D - probing networks but never participating.  
ALERT: Suspicious client 00:02:2D:2B:E3:1D - probing networks but never participating.  
ALERT: Suspicious client 00:02:2D:2B:E3:1D - probing networks but never participating.

Battery: AC charging 60% until 47s

# Kismet + Snort

```
$ grep fifo /etc/kismet.conf
```

```
fifo=/var/log/kismet fifo
```

For combined monitoring, in real time:

```
snort -r /var/log/kismet fifo
```

# Advanced mapping

The screenshot shows the Network Stumbler application interface. The title bar reads "Network Stumbler - [20040624095015]". The menu bar includes File, Edit, View, Device, Window, and Help. The toolbar contains icons for Channels, SSIDs, Scan, and Help. The left sidebar lists network nodes under "SSIDs": "linksys", "montreal", "santa", "taz57kar", and "UNINetVarig". A "Filters" section is also present. The main pane displays a table of scanned networks:

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+	Noise-	SNR+	IP Addr
00409655C84C	taz57kar		6	11 Mbps	Cisco	AP	WEP	-93	-100	-100	7	

Status indicators at the bottom include "Ready", "Not scanning", and "GPS: Disa".

Network 6: "taz57kar" BSSID: "00:40:96:55:C8:4C"

Type : infrastructure

Carrier : 802.11b

Info : "AP350-ORGAO PUBLI^F"

Channel : 06

WEP : "Yes"

# References

## Useful Links

<http://www.google.com>

<http://www.yahoo.com>

<http://www.dmoz.org>

<http://www.ask.com>

# Bluetooth

- Frequency 2.4GHz
- Point to point or network use (piconets 1+7)
- Range up to 250 meters
- Bluetooth access point for connection with IP networks (routing)

# Bluetooth

```
# hcitool scan  
scanning ...
```

```
00:10:60:A2:09:2C
```

**Bluetooth Access Point Router**



# Bluetooth

**Bluetooth Access Point Router**

File Edit View Favorites Tools Help

Back  Search Favorites   

Address  http://192.168.2.1/status.htm Go

**Bluetooth Access Point Router**

[Index](#)

> General Information

( Click on the Host icon to delete that PAN user )

**Getway Information**

Global IP(WAN)	10	61	5	117
System IP(LAN)	192	168	2	1
Gateway(LAN)	192	168	2	1
Netmask(LAN)	255	255	255	0
DNS	168	95	1	1

**Op Mode** Routing Mode

**BT Name** Bluetooth Access Point Router

**BT Address** 00:10:60:A2:09:2C

**WAN Type** DHCP

**Connectability** Enable

**Security Mode** No Security

**Host List**

 00:10:60:AA:67:89 LEWIS252
 00:02:5B:00:A5:A5 HP-XT395
 00:09:C5:03:0A:6D GRONK

 Done  Internet

# Bluetooth - Monitoring

```
# hcidump -a -r
HCIDump - HCI packet analyzer ver 1.10
HCI Event: Connect Request (0x04) plen 10
HCI Command: Accept Connection Request (0x01|0x0009) plen 7
HCI Event: Command Status (0x0f) plen 4
HCI Event: Connect Complete (0x03) plen 11
[...]
HCI Event: Remote Name Req Complete (0x07) plen 255
. ) . W ` . N o k i a   6 6 0 0 ...
ACL data: handle 0x0029 flags 0x02 dlen 82
L2CAP(d): cid 0x0041 len 78 [psm 3]
RFCOMM(d): UIH: cr 1 dlc 6 pf 1 ilen 73 fcs 0x93 credits 1
...I...!.I.m.a.g.e.(.0
.2.9.)...j.p.g.....r
.B..i m a g e / j p e g . D .. 2 0
0 4 0 3 0 6 T 1 5 4 0 4 2
ACL data: handle 0x0029 flags 0x01 dlen 164
L2CAP(d): cid 0x0041 len 672 [psm 3]
RFCOMM(d): UIH: cr 1 dlc 6 pf 1 ilen 666 fcs 0x93 credits 1
...H.....J F I F ....
.....(....0 6 / 0 3 / 2
0 0 4 . 1 4 : 4 0 : 4 0 . M o d e = 1 .
```

# Attacks on Wireless Networks

Nelson Murilo  
[<nelson@pangeia.com.br>](mailto:<nelson@pangeia.com.br>)

