Ataques à redes sem fio

Nelson Murilo
<nelson@pangeia.com.br>

Agenda

- Tipos de rede sem fio
- Características de redes Wi-Fi
- Padrões atuais
- Métodos de proteção disponíveis
- Ferramentas de diagnóstico
- Problemas com listas de itens de segurança
- Outros problemas de segurança relacionados
- Soluções robustas (atuais e futuras)

Tipos de redes sem fio

(GSM/GPRS/TDMA/CDMA/Edge/EVDO/etc)

Características de redes Wi-Fi

Wi-Fi usa ISM (Industrial, Scientific and Medical)

902 - 928 MHz

2.4 - 2.485 GHz (2.4 a 2.5 GHz no Brasil)

5.150 - 5.825 GHz

WiMax usa faixas licenciadas

802.16: 10-66GHz

802.16a: 2-10GHz

Características de redes Wi-Fi

- IEEE 802.11

Vários padrões já fechados:

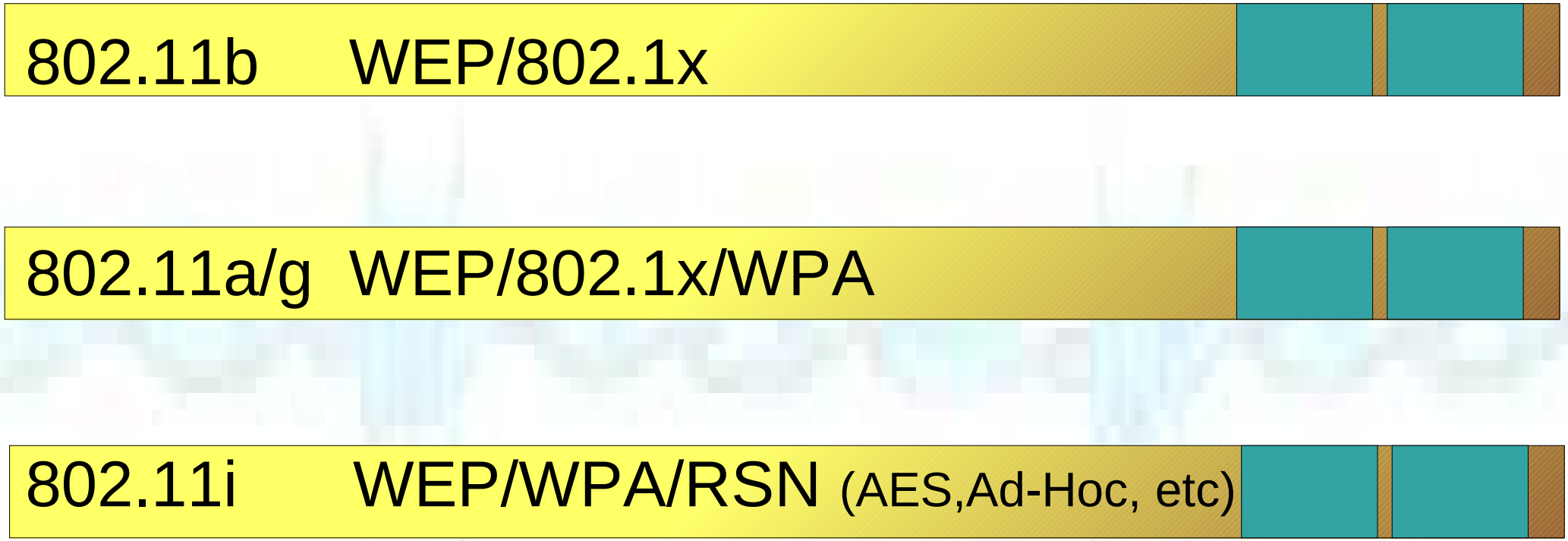
802.11b 22Mb 2.4Ghz

802.11a 54Mb 5.1GHz

802.11g 54Mb 2.4Ghz

802.11i - Mecanismos de segurança

Padrões de segurança atuais

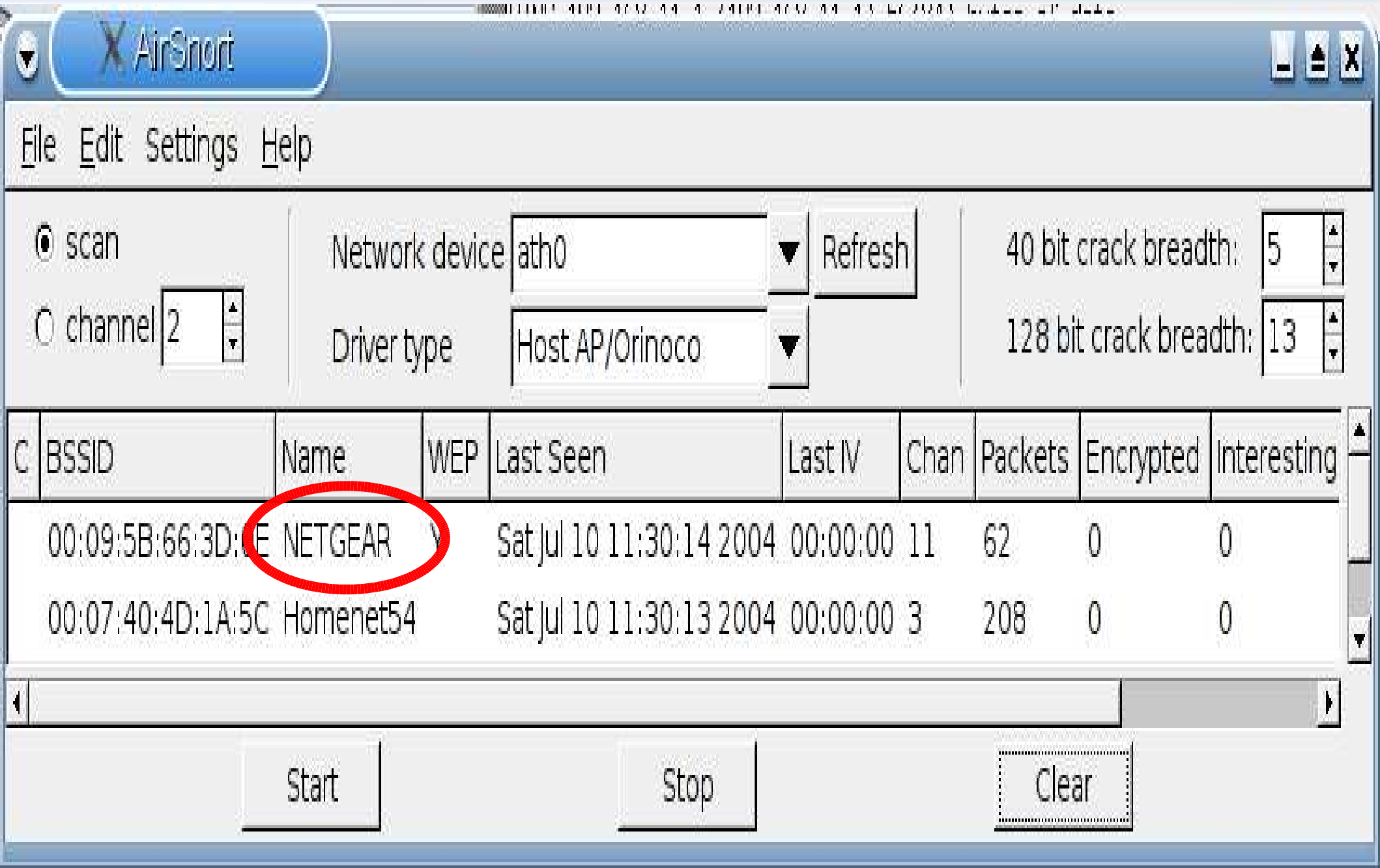



ATTACK!
A GAME OF WORLD CONQUEST
EAGLE GAMES
EXPANSION
the road to VICTORY!
AGES 10
AND UP

Métodos de proteção disponíveis

- Desabilitar broadcast de ESSID
- Filtro de MAC
- Isolamento do tráfego de cada cliente
- WEP
- 802.1x
- WPA
- WPA2/RSN
- Monitoramento

Desabilitar broadcast de ESSID



Desabilitar broadcast de ESSID

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

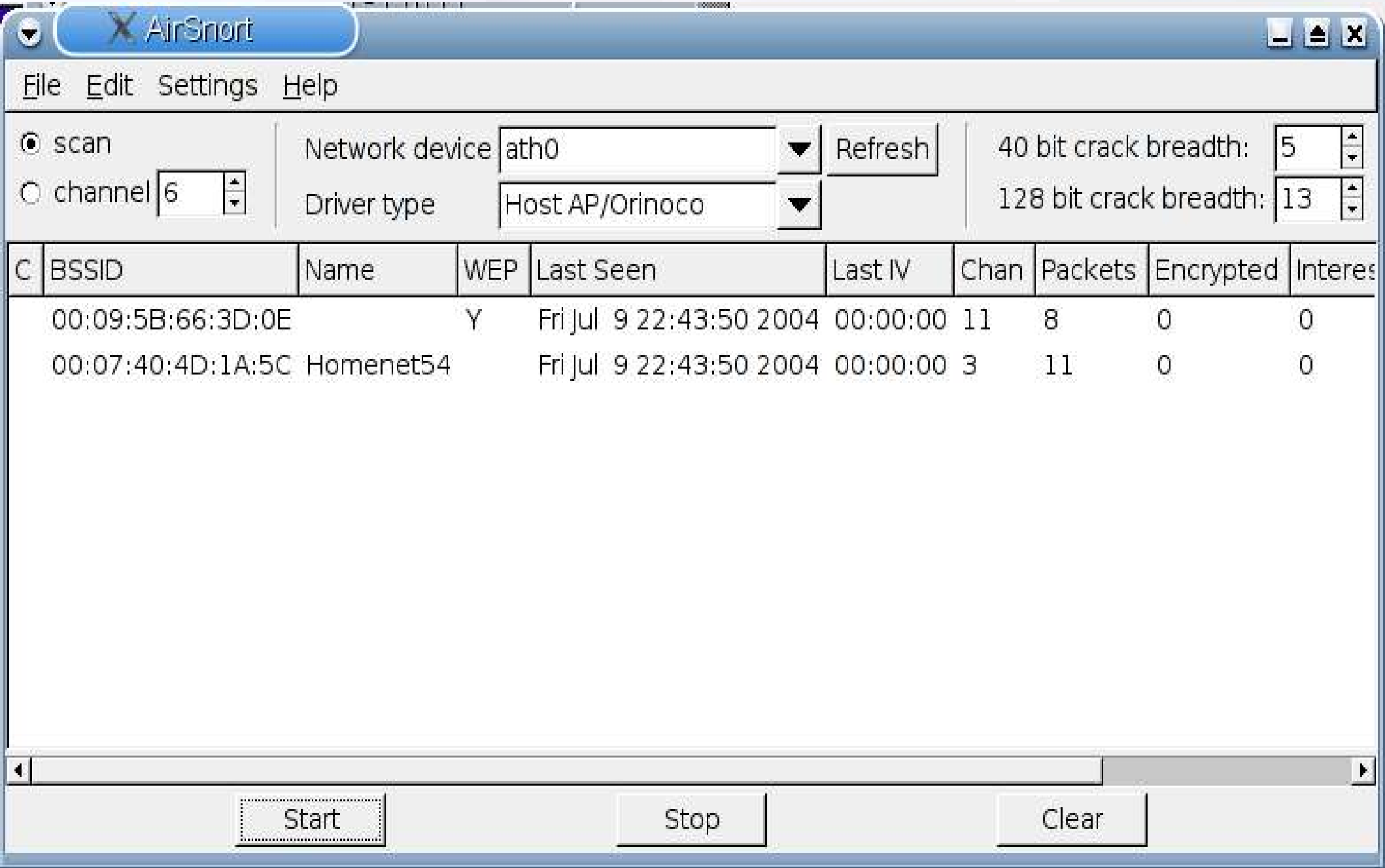
Allow access by:

- All Wireless stations
- Trusted PCs only

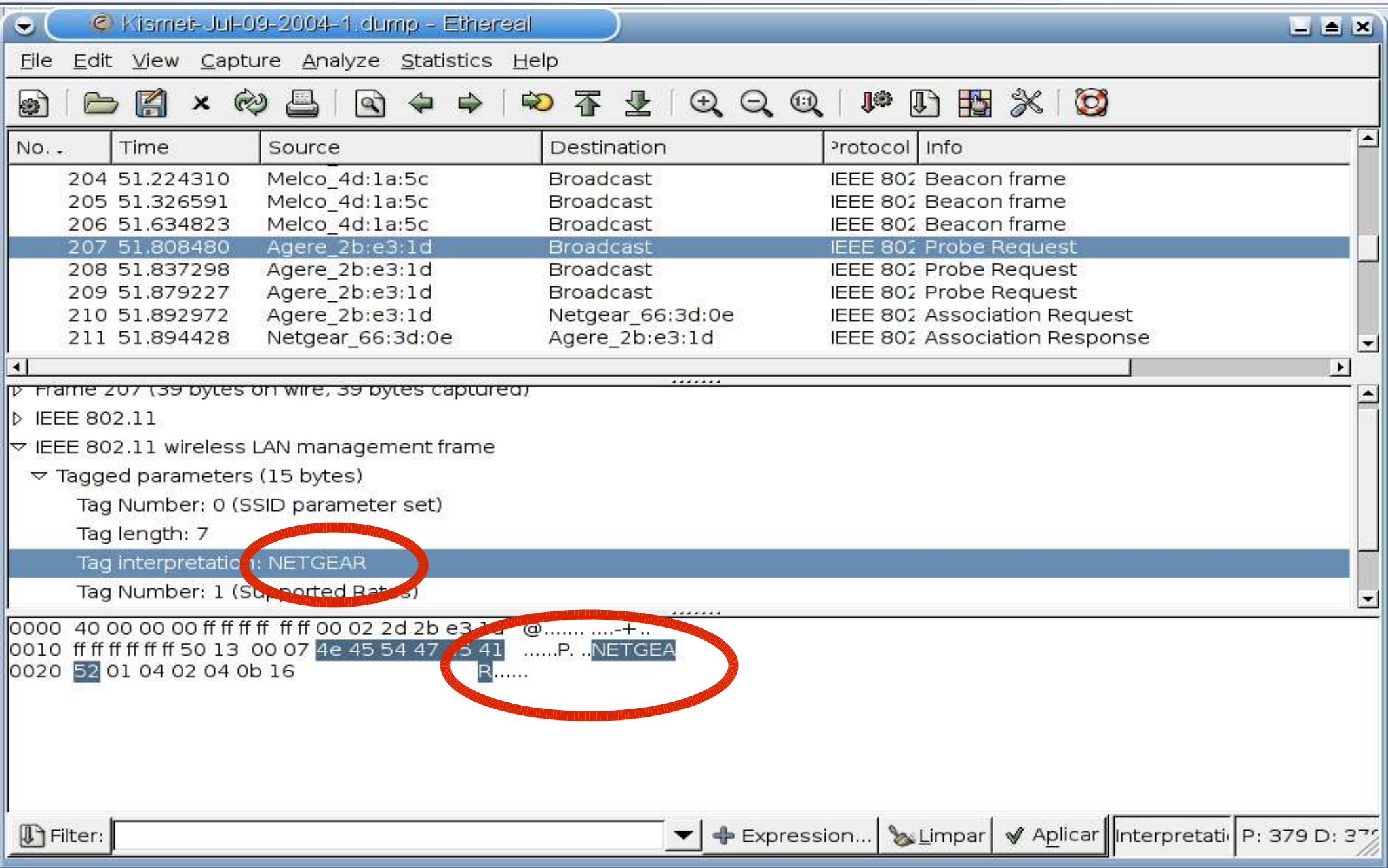
Trusted PCs List

- [x] **Enable bridging to wired LAN**
- [ ] **Enable SSID broadcast**

Desabilitar broadcast de ESSID



Desabilitar broadcast de ESSID



Desabilitar broadcast de ESSID

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]

Desabilitar broadcast de ESSID

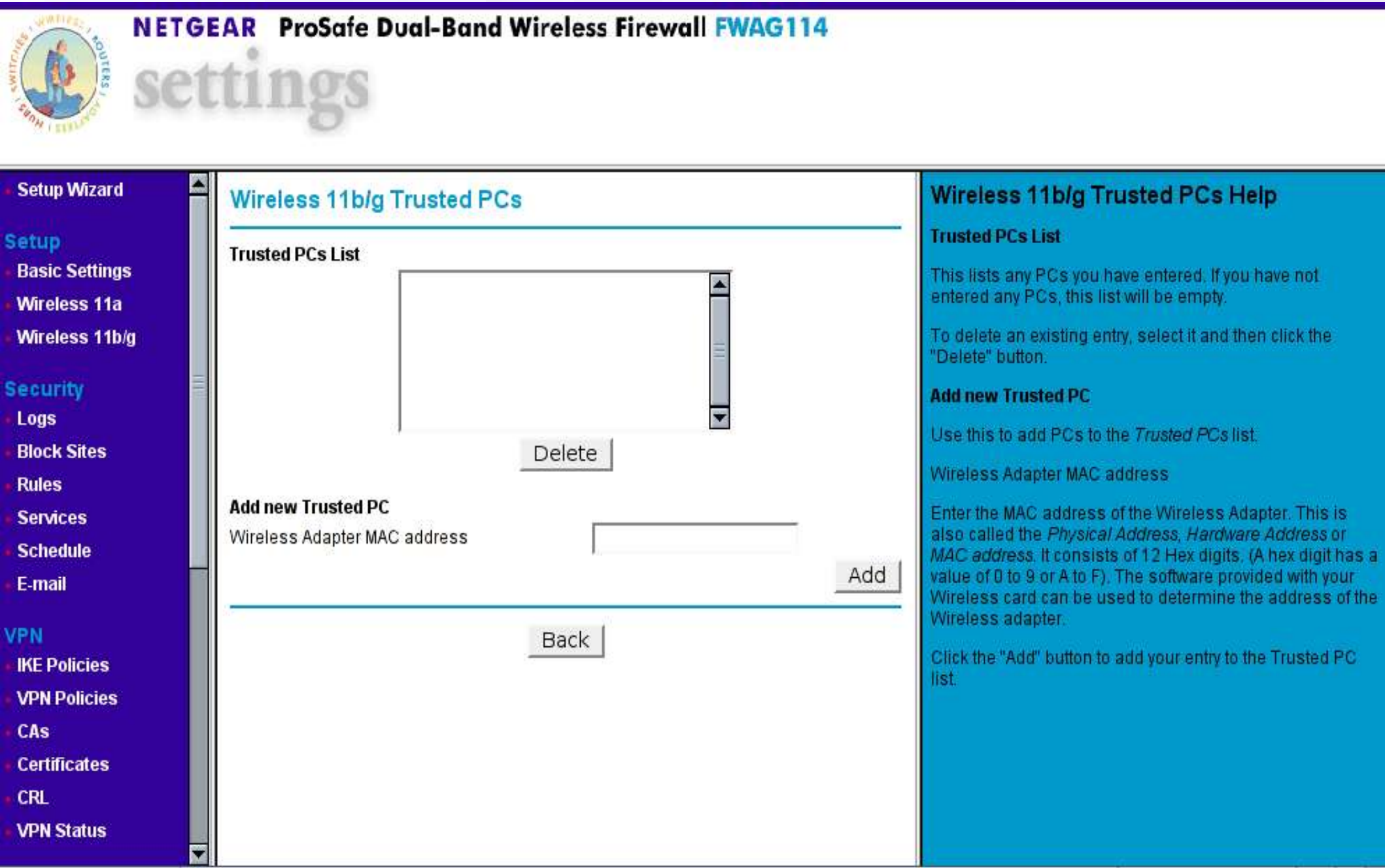
Existem ainda outros momentos onde o ESSID trafega:

- Busca por concentrador ativo
- Resposta à busca por concentrador
- Reassociação com concentrador

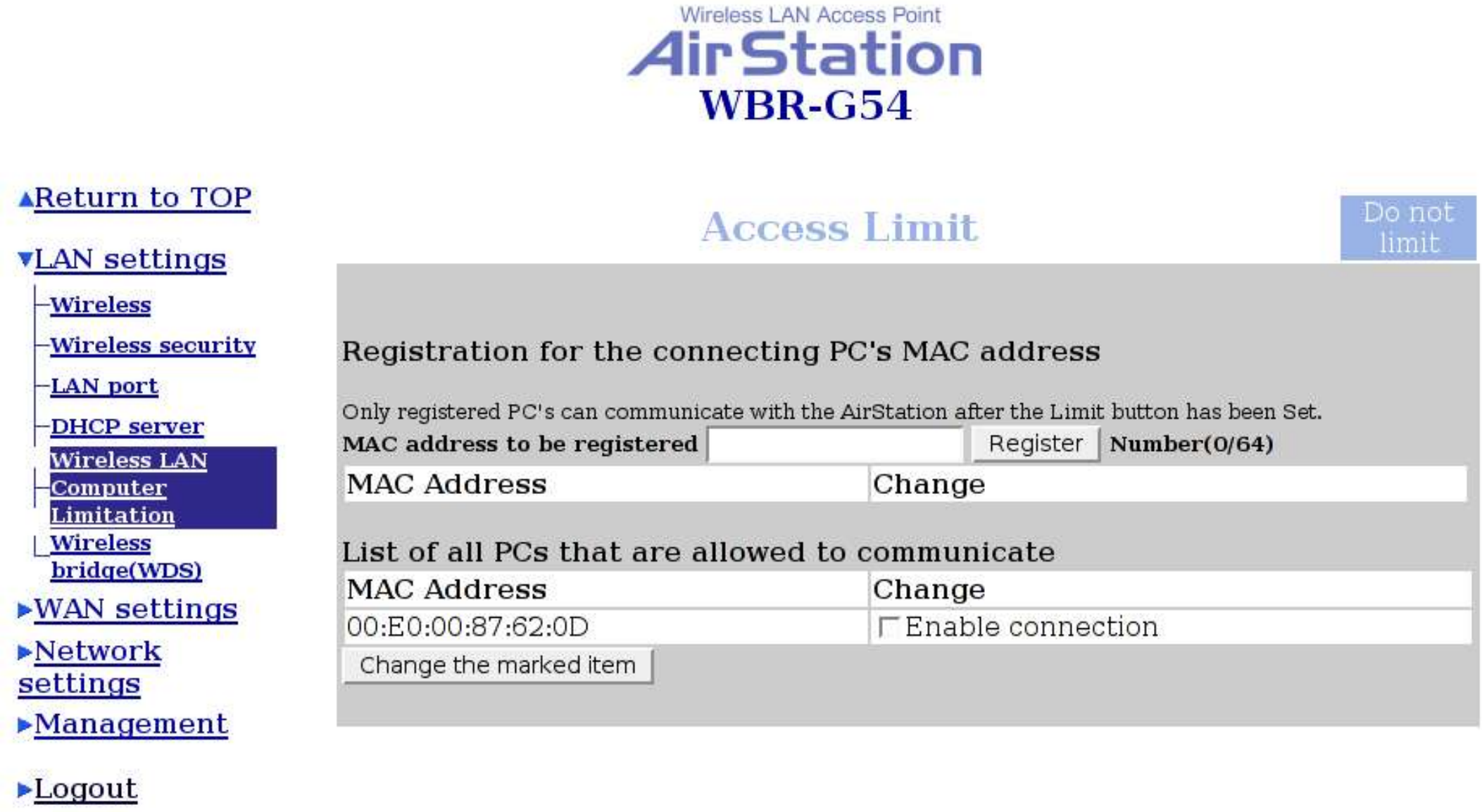
Métodos de proteção disponíveis

- [redacted]
- Filtro de MAC
- Isolamento do tráfego de cada cliente
- WEP
- 802.1x
- WPA
- WPA2/RSN
- Monitoramento

Filtro de MAC



Filtro de MAC



Filtro de MAC

Linux

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

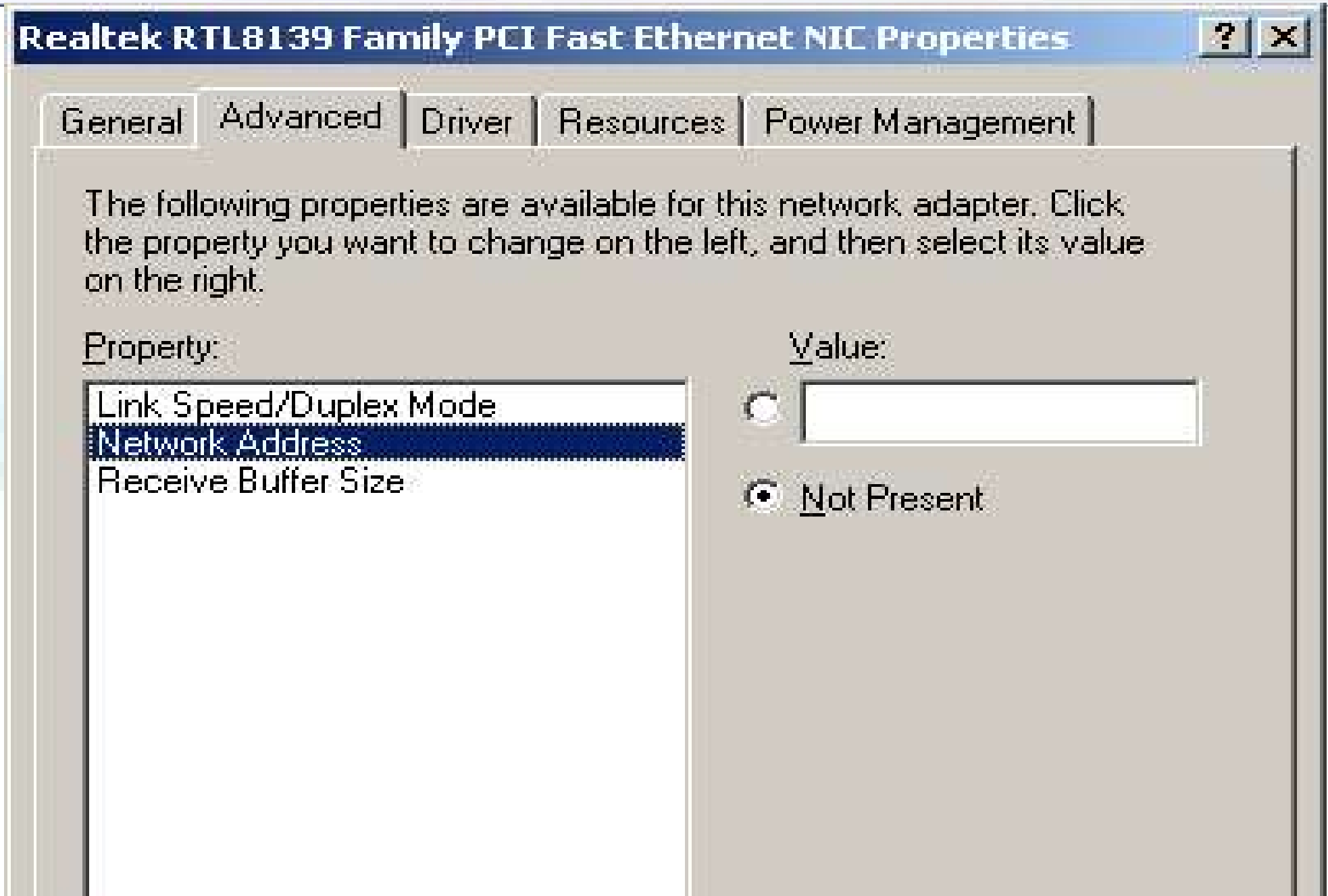
FreeBSD

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

OpenBSD/NetBSD

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

Filtro de MAC

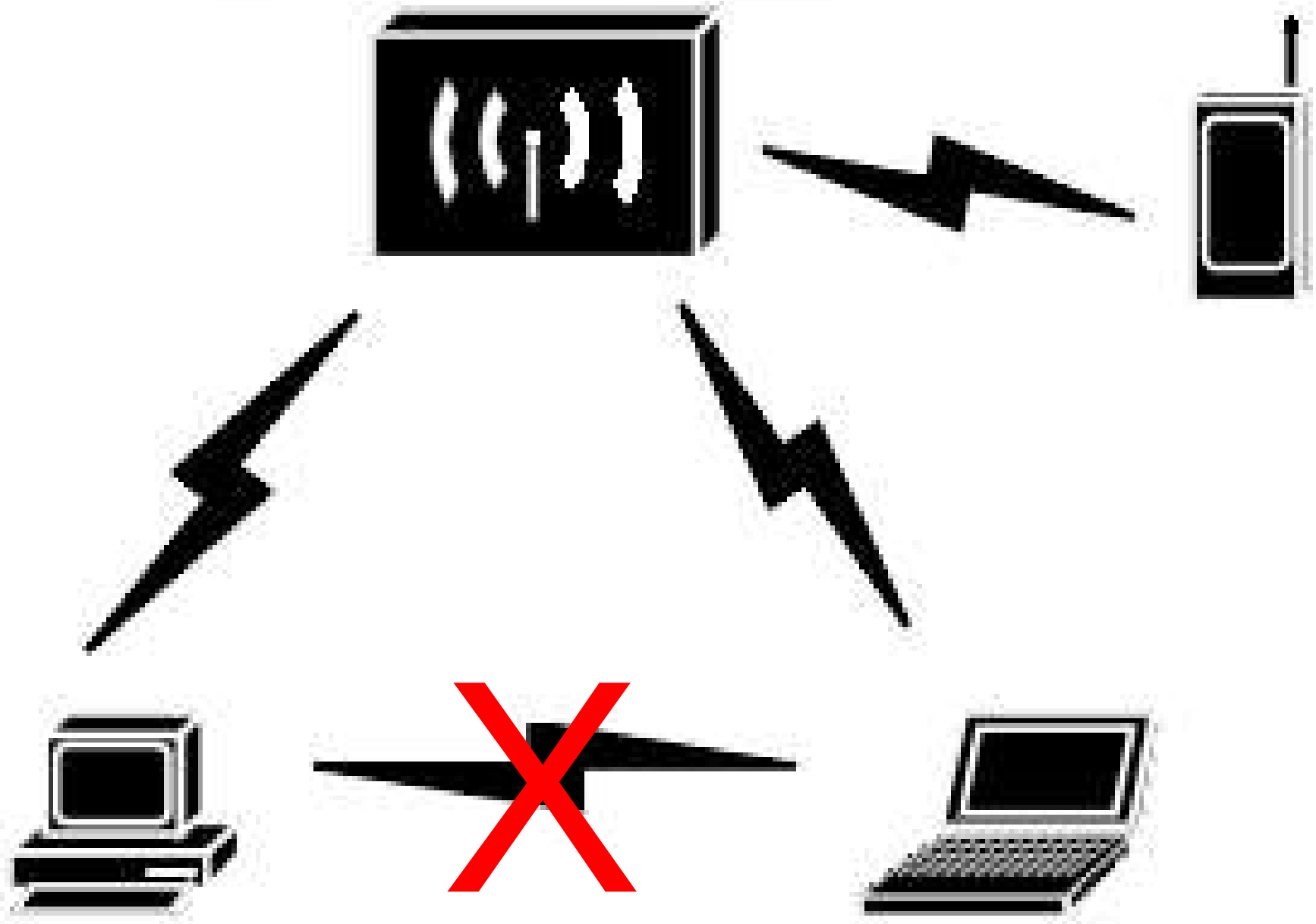


Métodos de proteção disponíveis

- [redacted]
- [redacted]
- Isolamento do tráfego de cada cliente
- WEP
- 802.1x
- WPA
- WPA2/RSN
- Monitoramento

Isolamento de tráfego por cliente

PSPF(Publicly Secure Packet Forwarding) ou Privacy Separator



Isolamento de tráfego por cliente

```
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
```

Porém o tráfego continua passível de ser capturado

```
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)
```

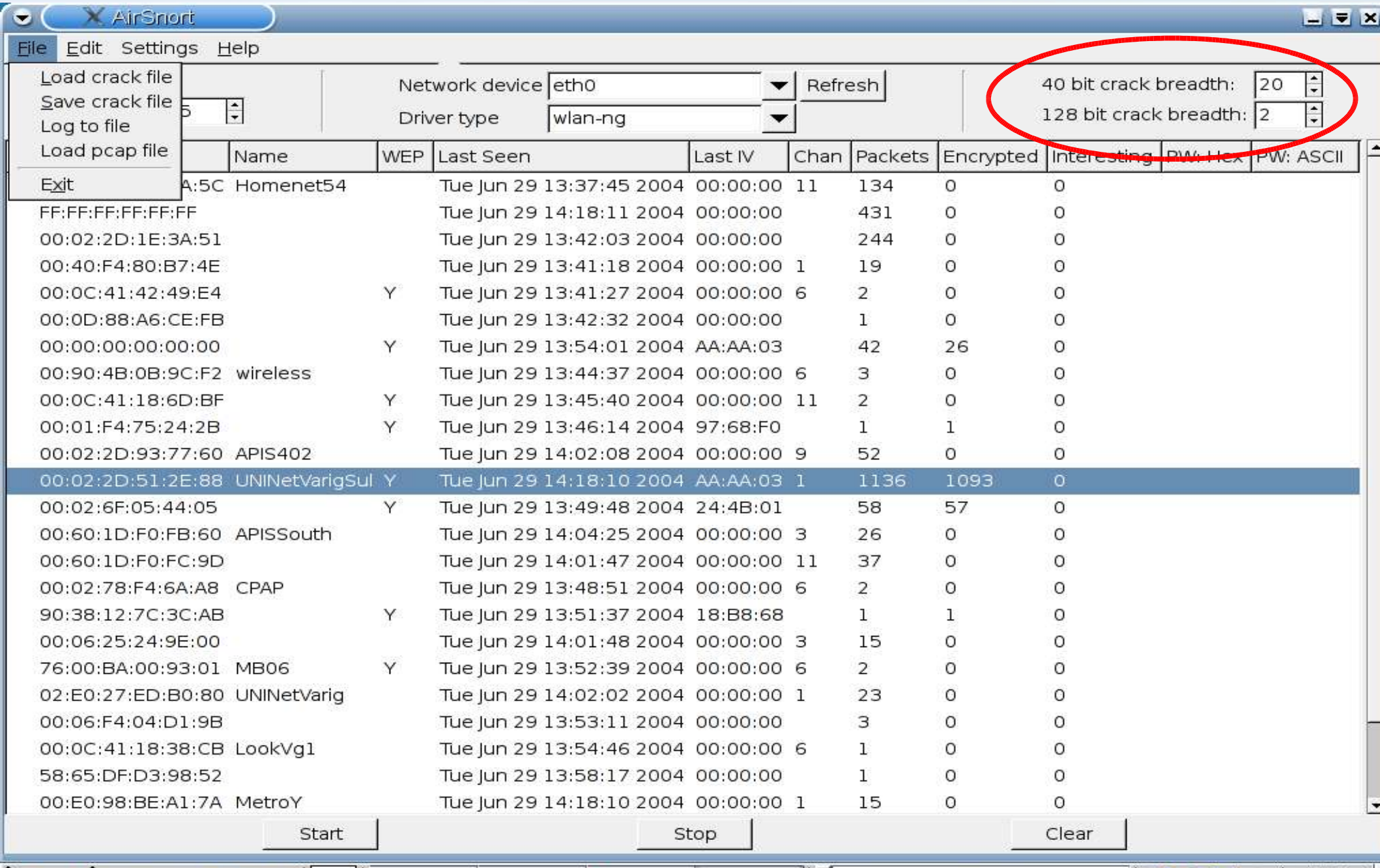
Métodos de proteção disponíveis

- [redacted]
- [redacted]
- [redacted]ente
- WEP
- 802.1x
- WPA
- WPA2/RSN
- Monitoramento

Airsnort

- Interface gráfica
- Geração e carga de arquivo no formato PCAP
- Suporte a quebra de chaves WEP (~100Mb-1Gb)
- Integração com GPS
- Informações de uso de WEP
- Baixo número de placas (chipsets) suportadas
- Sem detalhes como clientes conectados e nível de sinal

Airsnort


AirSnort
File Edit Settings Help
Load crack file
Save crack file
Log to file
Load pcap file
Exit
Network device eth0 Refresh
Driver type wlan-ng
40 bit crack breadth: 20
128 bit crack breadth: 2
Name WEP Last Seen Last IV Chan Packets Encrypted Interesting PW: Hex PW: ASCII
A:5C Homenet54 Tue Jun 29 13:37:45 2004 00:00:00 11 134 0 0
FF:FF:FF:FF:FF:FF Tue Jun 29 14:18:11 2004 00:00:00 431 0 0
00:02:2D:1E:3A:51 Tue Jun 29 13:42:03 2004 00:00:00 244 0 0
00:40:F4:80:B7:4E Tue Jun 29 13:41:18 2004 00:00:00 1 19 0 0
00:0C:41:42:49:E4 Y Tue Jun 29 13:41:27 2004 00:00:00 6 2 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

- Ataques baseados em :
  - Força bruta
  - Dicionário
- Lê arquivos no formato PCAP
- Permite integração com quebradores de senha tradicionais, como o **John The Ripper**

WepAttack

```
# wepattack -w /usr/share/dic/dic1.txt -f Kismet-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

Ataques baseados em :

- Força bruta
- Dicionário
- Fragilidades do vetor de incialização

- Lê arquivos no formato PCAP
- Quebra mais rápido que outra ferramentas, desde que exista padrão de tráfego correto

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...
```

Decifrar tráfego capturado

Decrypt (integrante do pacote airsnort)

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

Exemplos:

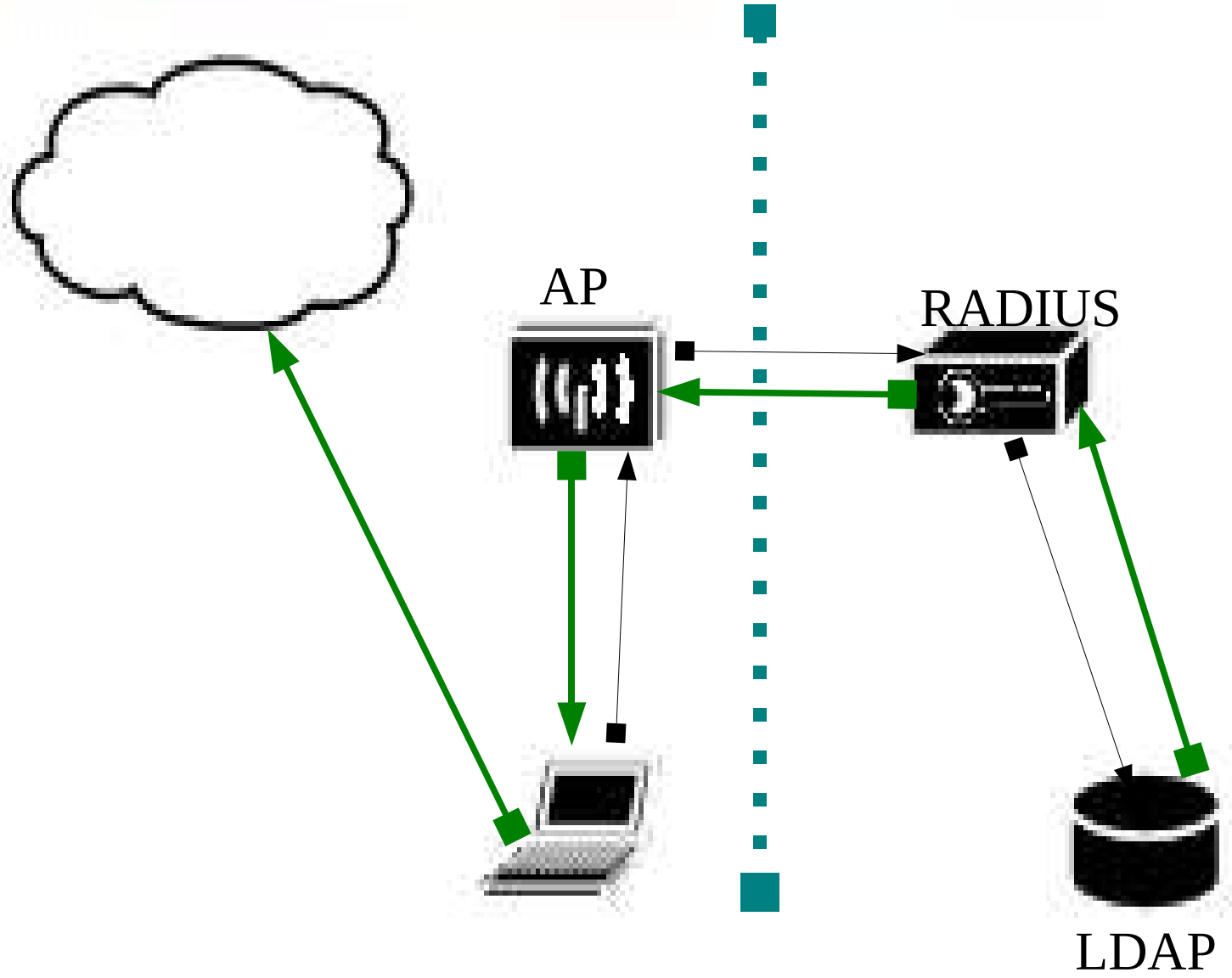
decrypt -p SMART -m AF:E8:E9:6C:11:81 -e wep.pcap -d nowep.pcap

decrypt -p 53:4D:41:52:54 -m AF:E8:E9:6C:11:81 -e wep.pcap -d nowep.pcap

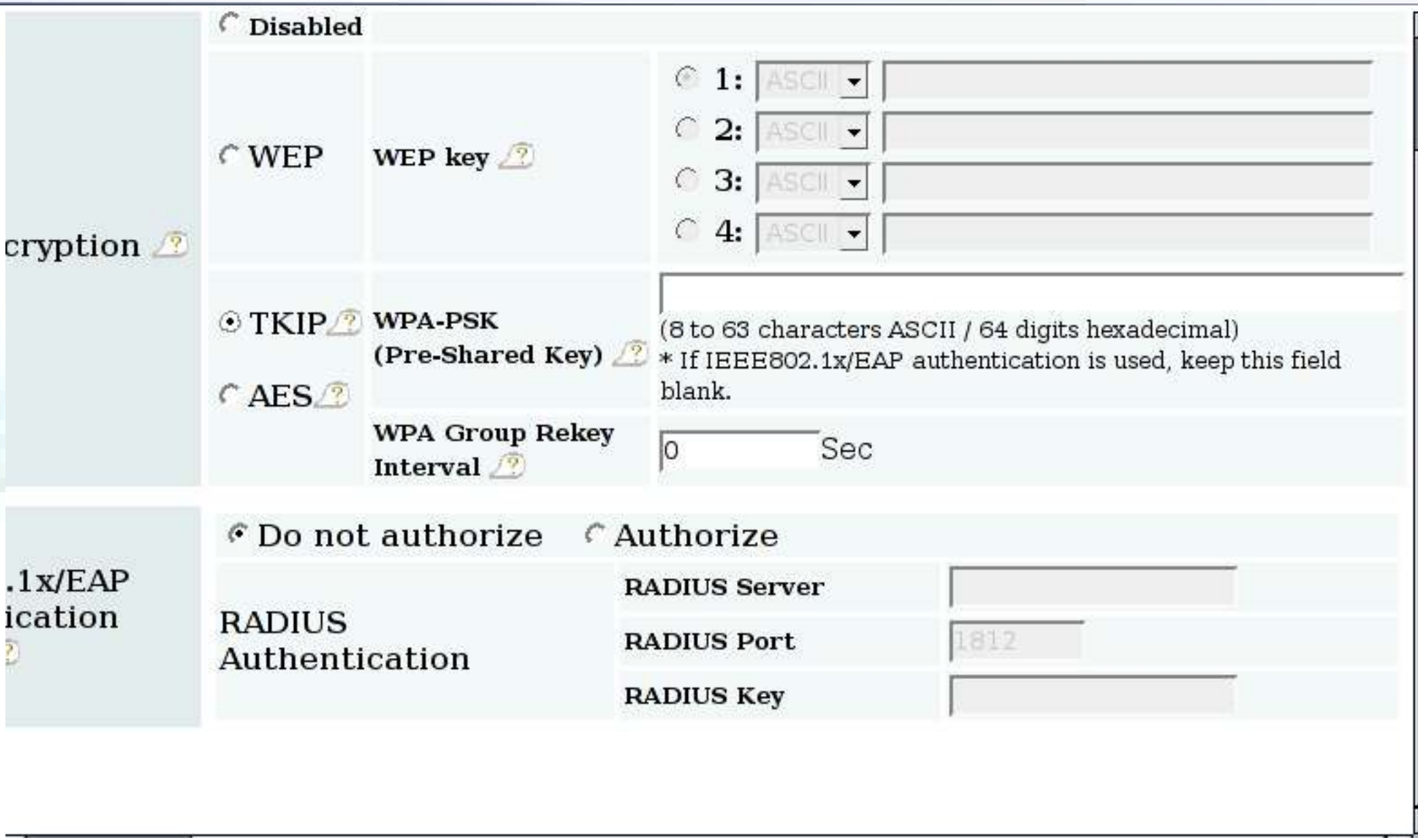
Métodos de proteção disponíveis

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- 802.1x
- WPA
- WPA2/RSN
- Monitoramento

802.1x



802.1x + WEP


Disabled
WEP
WEP key
1:
2:
3:
4:
ASCII
cryption
TKIP
AES
WPA-PSK
(Pre-Shared Key)
(8 to 63 characters ASCII / 64 digits hexadecimal)
* If IEEE802.1x/EAP authentication is used, keep this field blank.
WPA Group Rekey Interval
0
Sec
Do not authorize
Authorize
.1x/EAP
ication
RADIUS Authentication
RADIUS Server
RADIUS Port
1812
RADIUS Key

XSupplicant

Métodos suportados:

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

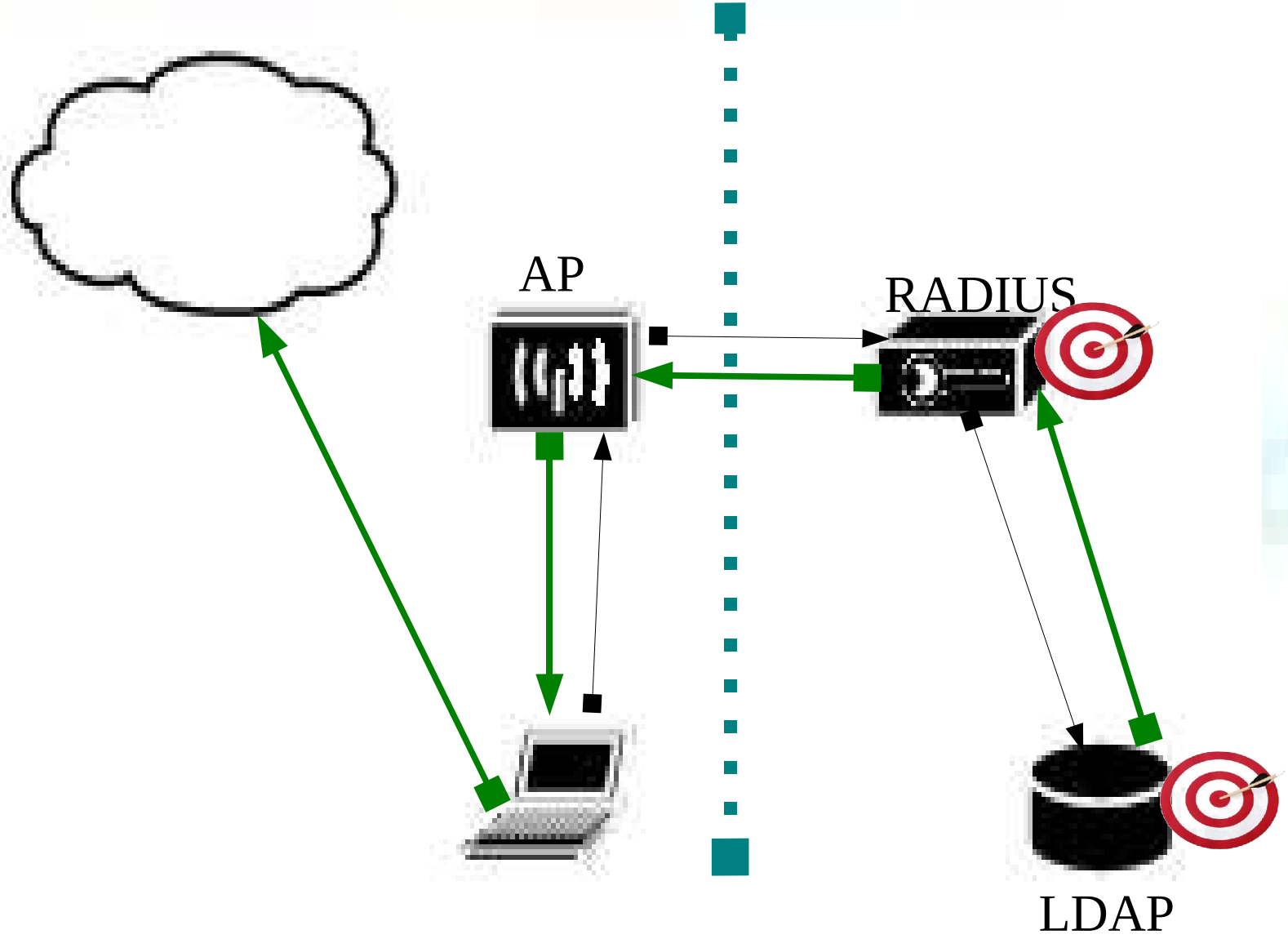
XSupplicant

[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>muitosecreta<END_PASS>
    root_cert = /etc/ssl/certs/root.pem
    root_dir = /etc/ssl/certs
     chunk_size = 1398
    random_file = /dev/urandom
}
```

802.1x



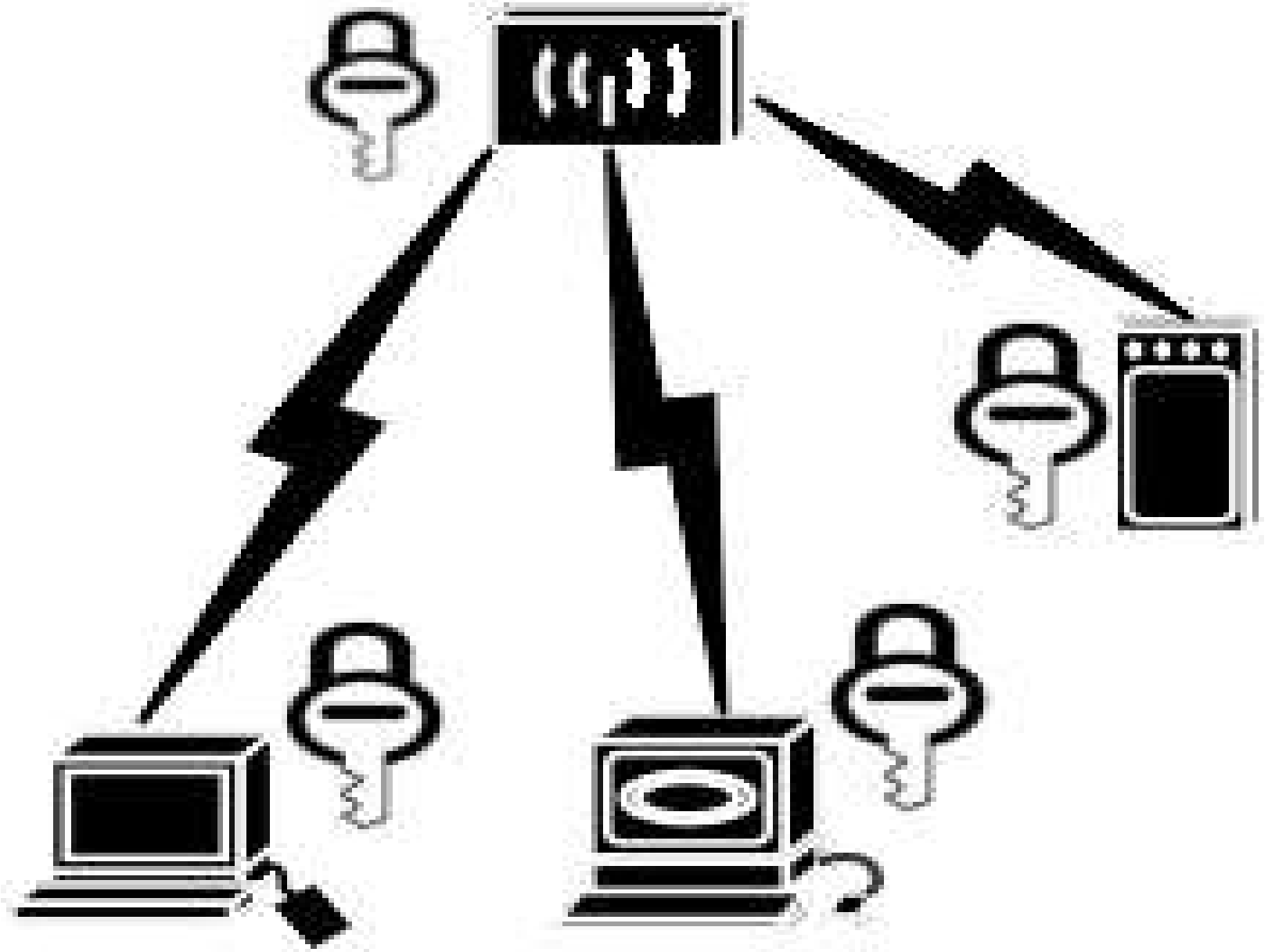
Métodos de proteção disponíveis

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- WPA
- WPA2/RSN
- Monitoramento

Ataques ao WPA

- WPA – PSK (Pre-shared Key)
- WPA Interprise
- Ataques ao concentrador
- Ataques aos clientes

WPA - PSK



WPA - PSK

 # wpa_supplicant -w -i ath0 -c /etc/wpa_supplicant -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

Ataques ao 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;
        }
[...]
```

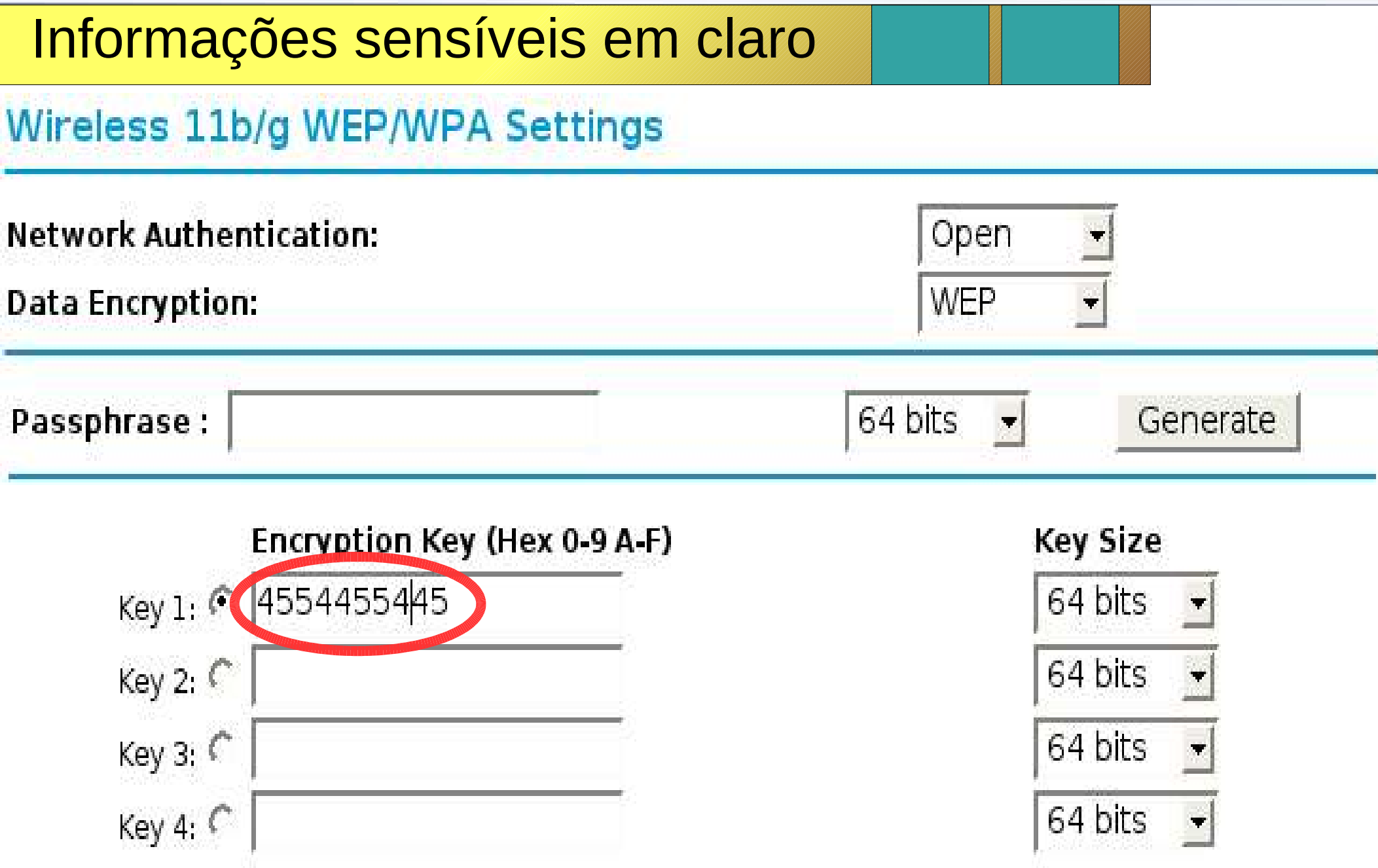
Ataques ao concentrador

Configurações de fábrica

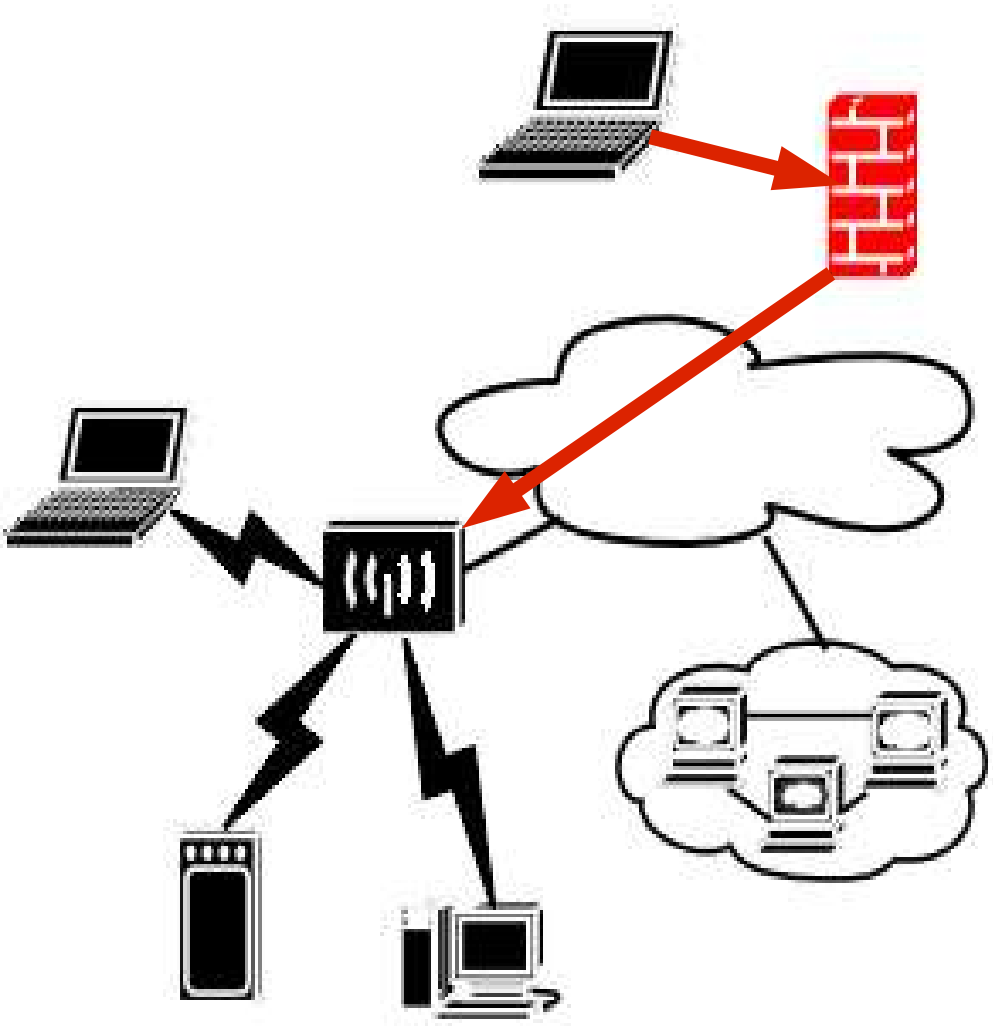
Manufactor	Product	Revision	Protocol	User	Password	Access	Validated
D-Link	Cable/DSL Routers/Switches	Multi	(none)	admin		Admin	No
D-Link	DI-614+		HTTP	user	(none)	User	No
D-Link	DI-614+		HTTP	admin	(none)	Admin	No
D-Link	DI-701	unknown	Multi	admin	year2000	Admin	No
D-link	DI-714P+		Multi	admin	____BLANK___	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

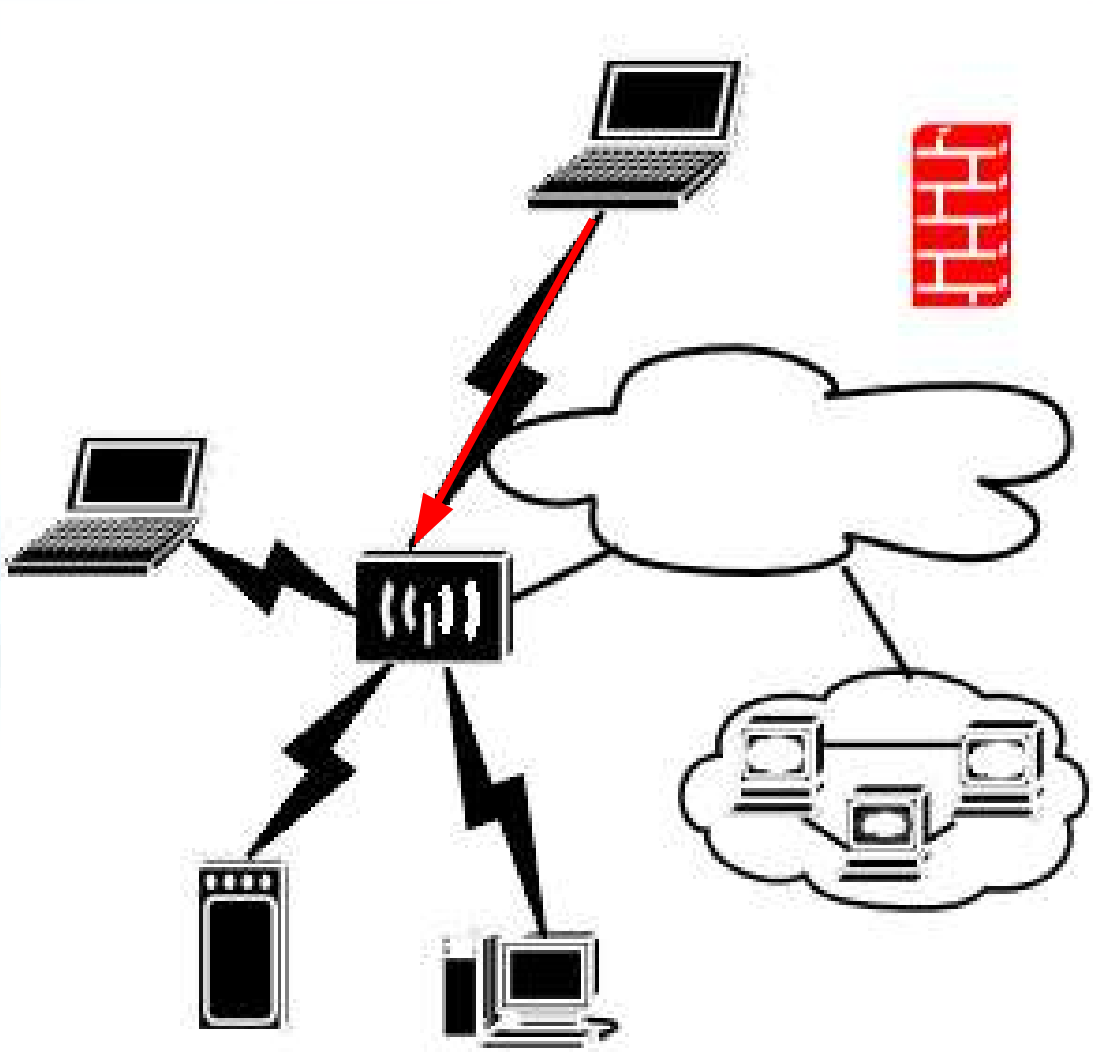
Ataques ao concentrador

Informações sensíveis em claro

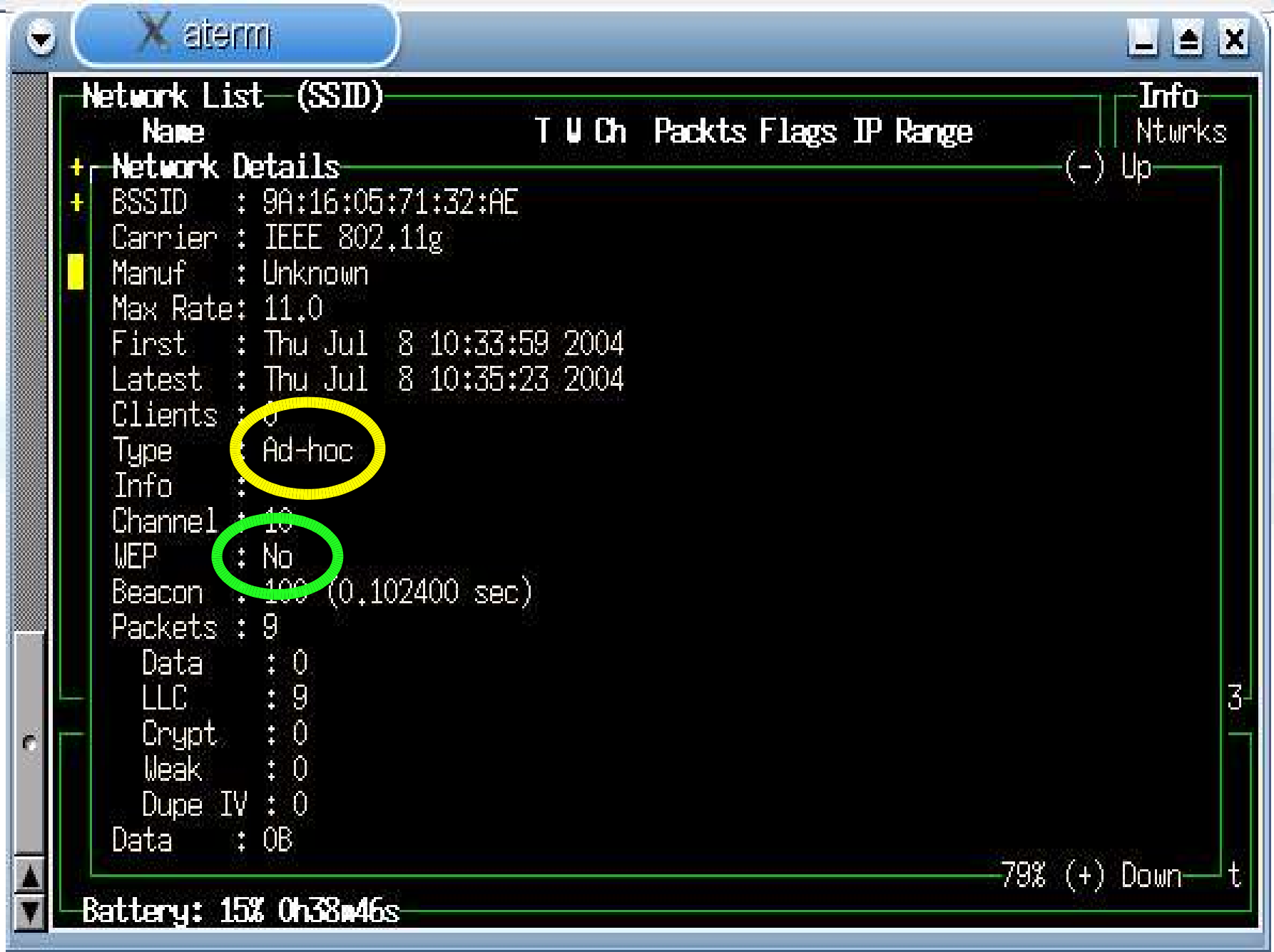


Ataques ao concentrador





Ataques à clientes



Ataques à clientes

iwconfig wlan0 essid **hotel**

iwconfig wlan0 mode Ad-Hoc

echo “[...] hardware ethernet 9A:16:05:71:32:AE

[...]” > /etc/dhcpd.conf

dhcpd wlan0

Ataques à clientes

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

Ataques à clientes

```
# 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

Recursos WPA/IEEE 802.11i suportados:

WPA-PSK ("WPA-Pessoal")

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

Gerenciamento de chaves para CCMP, TKIP, WEP104, WEP40

WPA and full IEEE 802.11i/RSN/WPA2

RSN: PMKSA cache, pré-autenticação

Métodos EAP (IEEE 802.1X Supplicant) suportados:

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

[...]
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

```
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

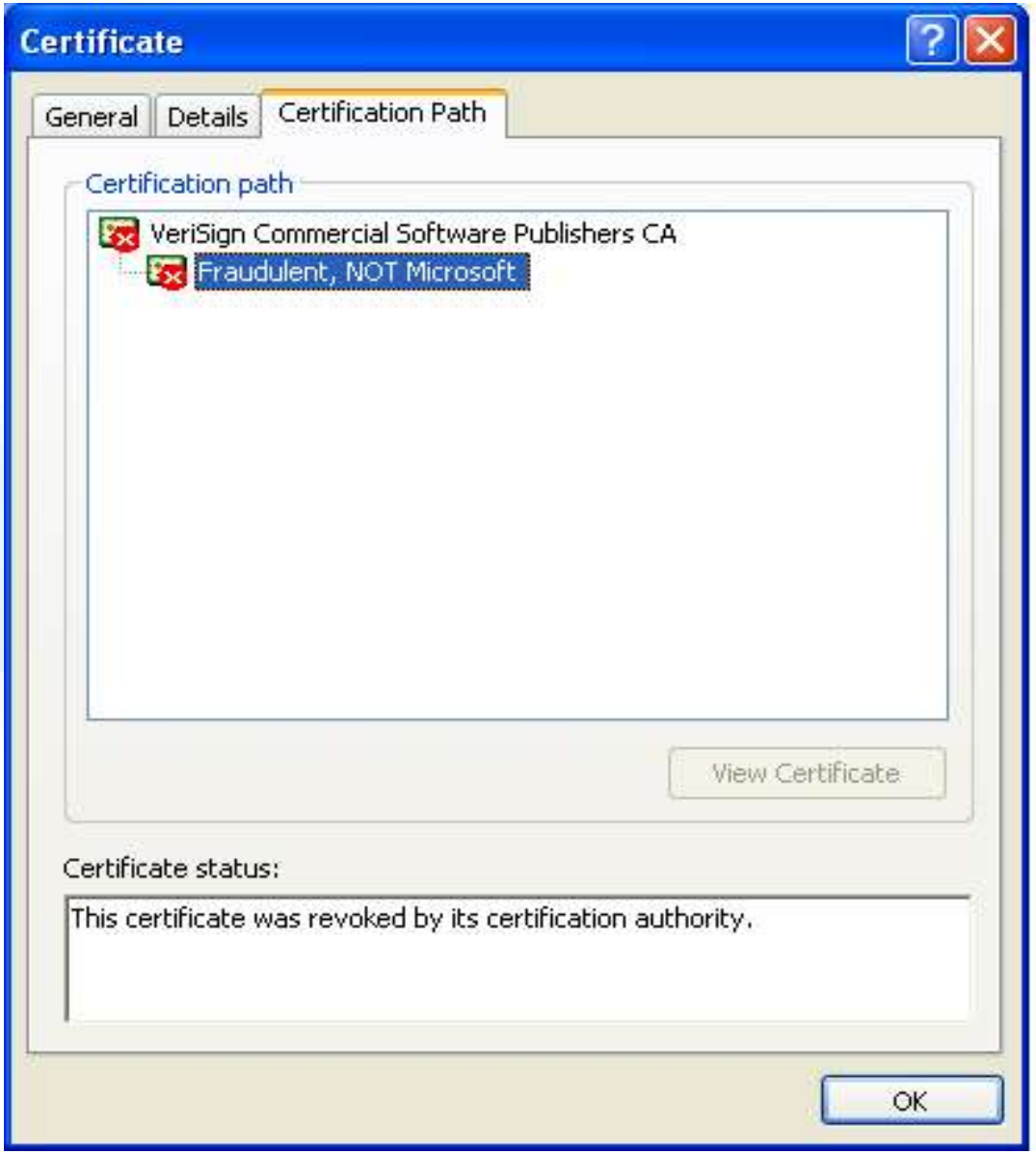
EAPOL: External notification - portValid=1

EAPOL: SUPP_PAE entering state **AUTHENTICATED**

WPA EAP_TLS

$ cat /etc/wpa_supplicant

```
network={
    ssid="MARINET"
    scan_ssid=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="5upers3crEt4"
}
```


Certificate
General
Details
Certification Path
Certification path
VeriSign Commercial Software Publishers CA
Fraudulent, NOT Microsoft
View Certificate
Certificate status:
This certificate was revoked by its certification authority.
OK

Métodos de proteção disponíveis

- Desabilitar broadcast do ESSID
- Filtro de MAC
- Isolamento de tráfego de cada cliente
- WEP
- 802.1x
- WPA
- WPA2/RSN
- **Monitoramento**

Monitoramento

“O otimista não sabe o que o espera”

-- Millor

Monitoramento

Monitoramento genérico

Logs, snort, prelude, etc

Monitoramento específico

- Recursos do concentrador. kismet, snortwireless, etc

Melhor dos mundos

- kismet + snort

Monitoramento

Concentrador

Attached Devices

DHCP Addresses

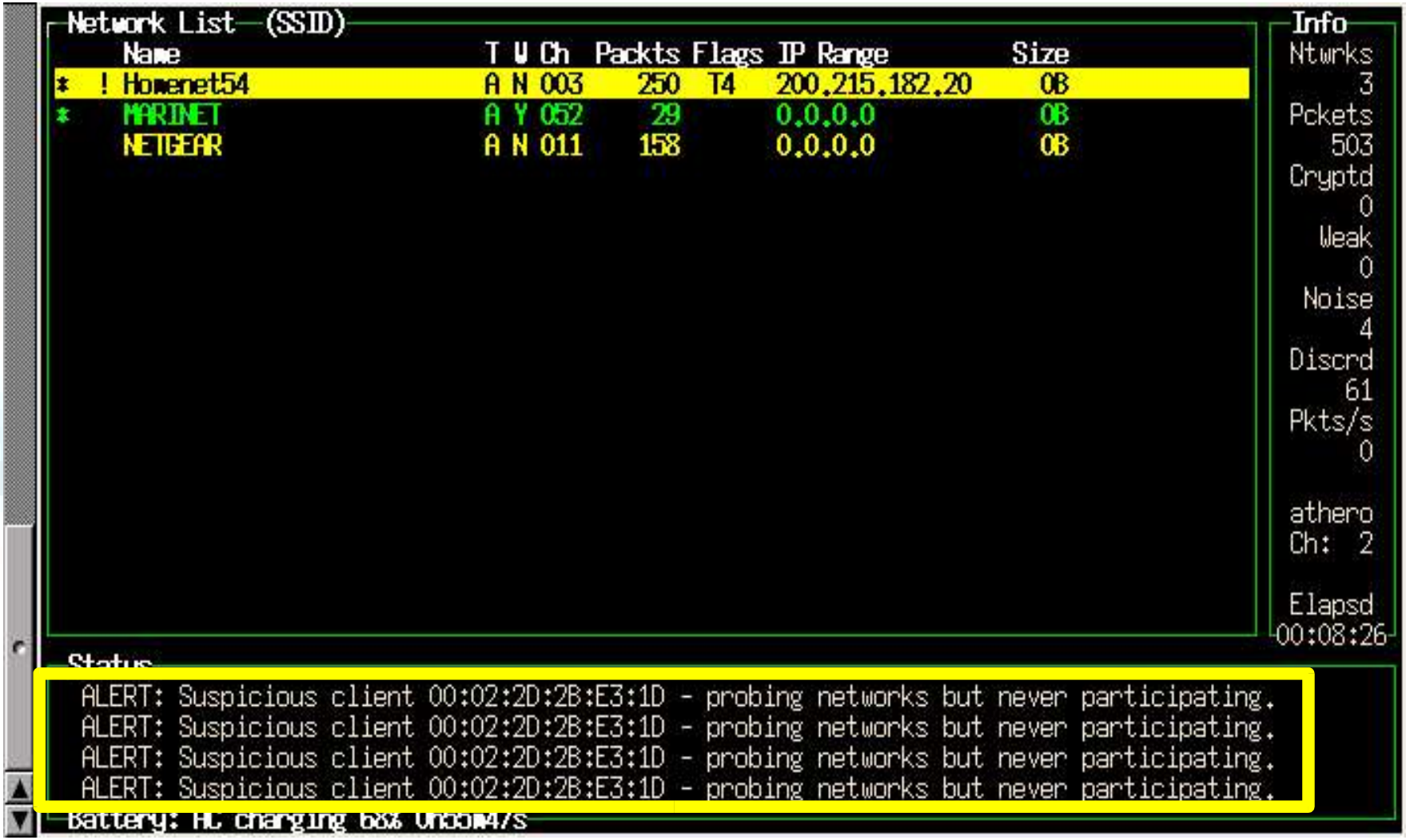
#	IP Address	Device Name	MAC Address
1	192.168.0.3	--	00:0c:41:0a:25:20
2	192.168.0.2	--	00:e0:98:74:c0:ba

Refresh

Monitoramento - Kismet

- Netstumbler, Wellenreiter, Airjack,
- SSID de mesmo nome trocando de canal
- Associa e continua o probe
- Pedidos de disassociação em broadcast

Monitoramento - Kismet



Kismet + Snort

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

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

Para um monitoramento combinado, em tempo real:

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

Referências

Links úteis

http://www.google.com

http://www.yahoo.com

http://www.dmoz.org

http://www.ask.com

Bluetooth

- **Freqüência 2.4GHz**
- **Uso ponto a ponto ou rede (piconets 1+7)**
- **Alcance de até 250 metros**
- **Concentradores bluetooh para conexão com redes IP (roteamento)**

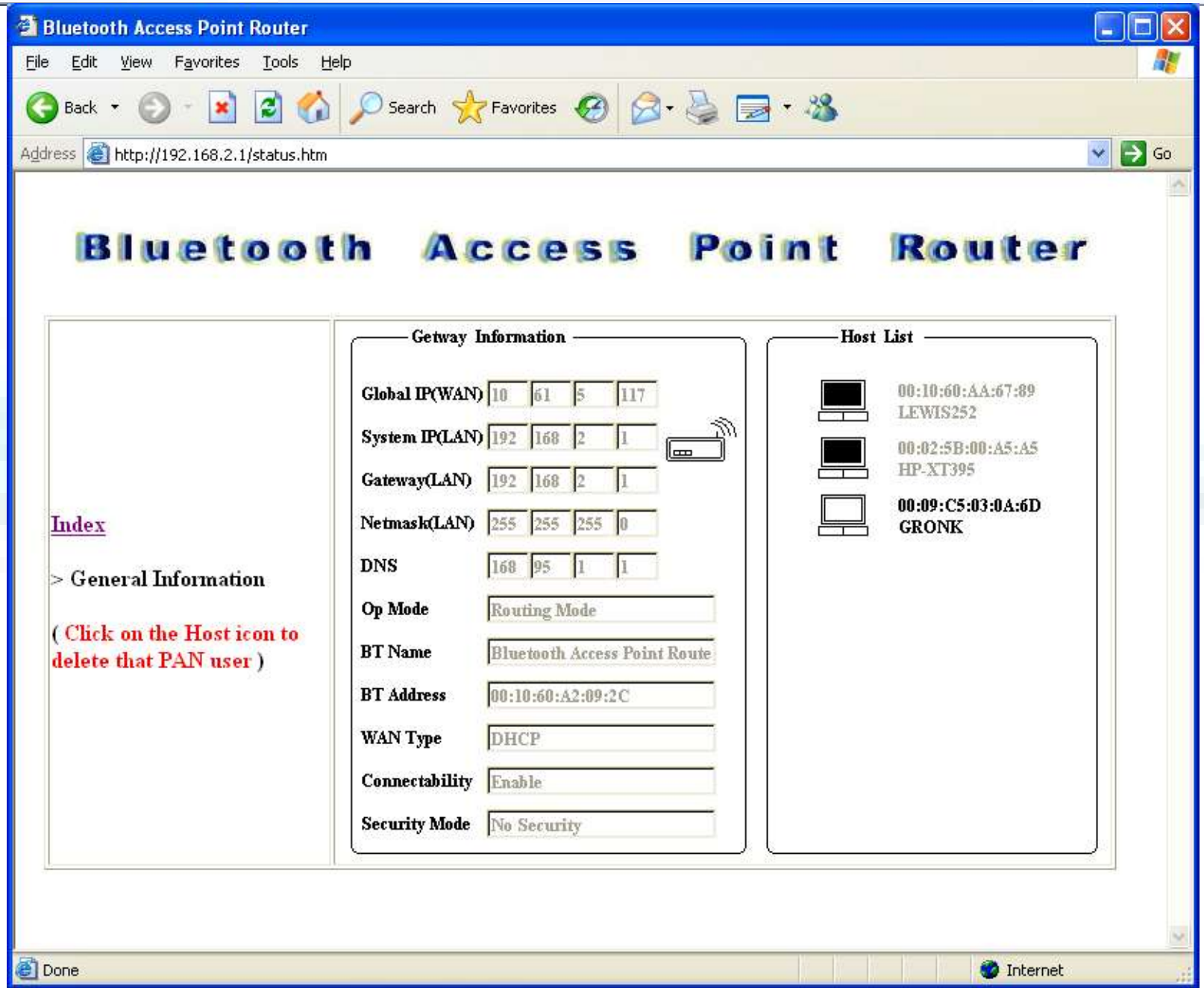
Bluetooth

 # 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 Route
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 - Monitoramento

 # 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 dlci 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 dlci 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 .

Referências