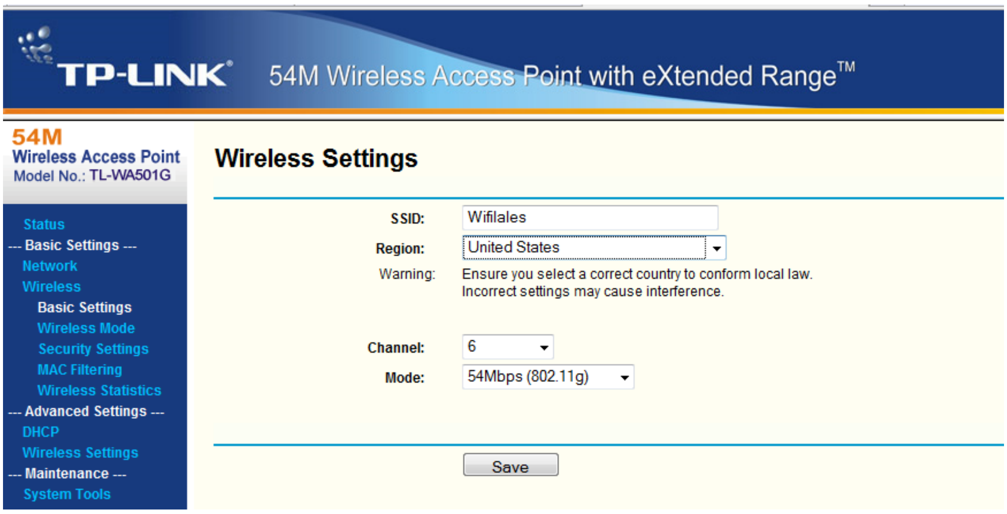
ACTIVIDAD 9 – SEGURIDAD EN LAS COMUNICACIONES INALÁMBRICAS – TEMA 2

a) Configuración de un punto de acceso inalámbrico seguro. http://www.tp-link.com/simulator/TL-WA501G/userRpm/index.htm

Nos vamos a la página arriba indicada y vamos a ir a Wireless Settings y vamos a cambiar el SSID y vamos a ponerle Wifilales



Wireless Settings

SSID: Wifilales

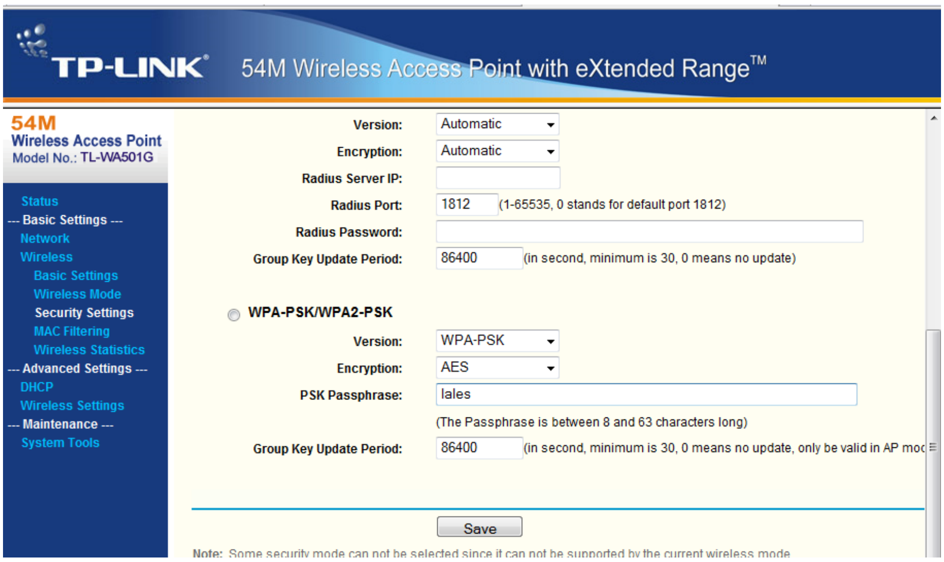
Region: United States

Warning: Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

Channel: 6

Mode: 54Mbps (802.11g)

Ahora vamos a poner en Security Settings que encripte con WPA-PSK/WPA2-PSK y vamos a elegir la versión WPA-PSK y en Encryption vamos a elegir AES y la contraseña será lales



Version: Automatic

Encryption: Automatic

Radius Server IP:

Radius Port: 1812 (1-65535, 0 stands for default port 1812)

Radius Password:

Group Key Update Period: 86400 (in second, minimum is 30, 0 means no update)

○ WPA-PSK/WPA2-PSK

Version: WPA-PSK

Encryption: AES

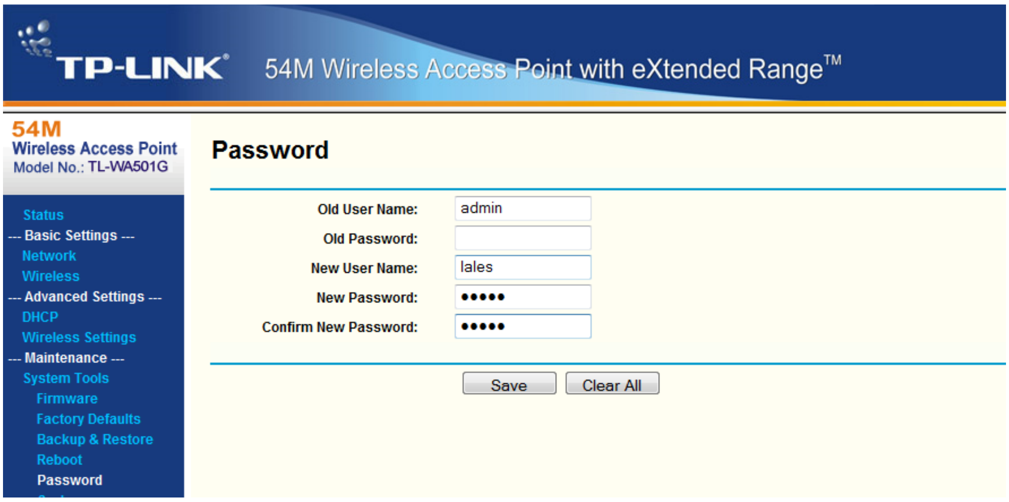
PSK Passphrase: lales

(The Passphrase is between 8 and 63 characters long)

Group Key Update Period: 86400 (in second, minimum is 30, 0 means no update, only be valid in AP moc

Note: Some security mode can not be selected since it can not be supported by the current wireless mode

Y en la contraseña del administrador vamos a poner en Maintenance y Password un nuevo usuario y una contraseña

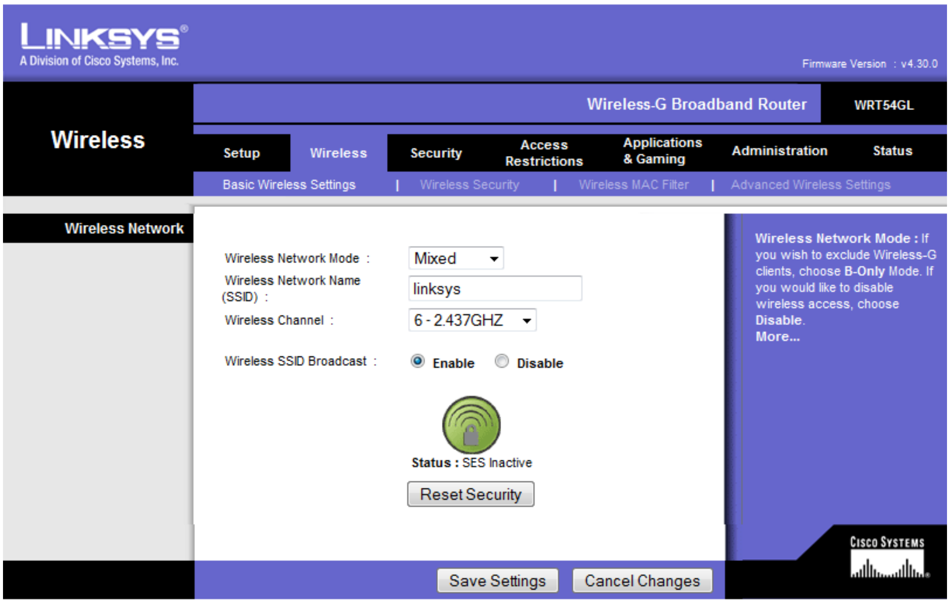


Password

Old User Name:	admin
Old Password:	
New User Name:	lales
New Password:	●●●●●
Confirm New Password:	●●●●●

b) Configuración de un router de acceso inalámbrico CISCO LINKSYS WRT54GL, utilizando un simulador. http://ui.linksys.com/files/WRT54GL/4.30.0/Setup.htm

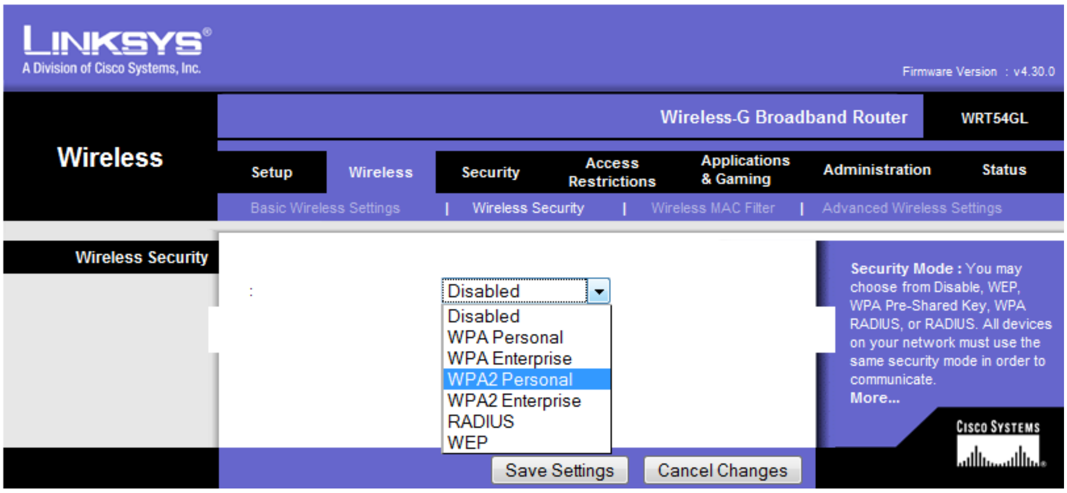
Entramos en el simulador, por medio del navegador y ponemos la dirección arriba indicada, en Wireless podemos cambiar el SSID



Wireless Network Mode :	Mixed
Wireless Network Name (SSID) :	linksys
Wireless Channel :	6 - 2.437GHZ
Wireless SSID Broadcast :	● Enable ○ Disable

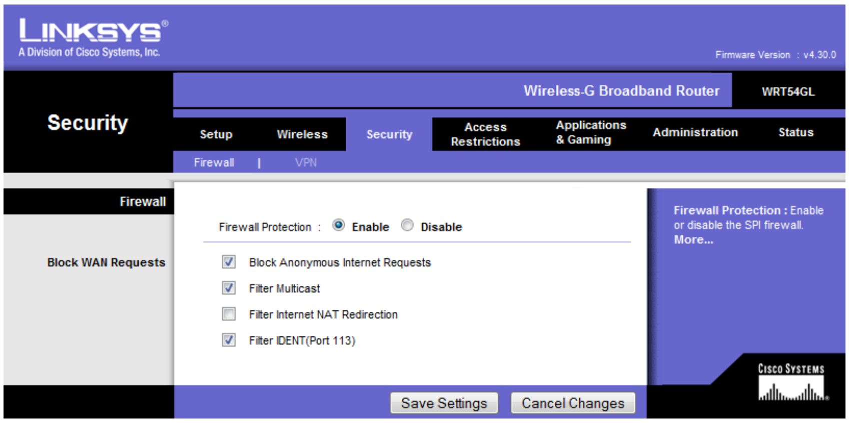
Wireless Network Mode : If you wish to exclude Wireless-G clients, choose **B-Only** Mode. If you would like to disable wireless access, choose **Disable**.
More...

A continuación vamos a elegir Wireless Security y vamos a poner WPA2 Personal para que encripte de esta manera



Security Mode : You may choose from Disable, WEP, WPA Pre-Shared Key, WPA RADIUS, or RADIUS. All devices on your network must use the same security mode in order to communicate.
More...

Después en Security Firewall lo activamos con Enable

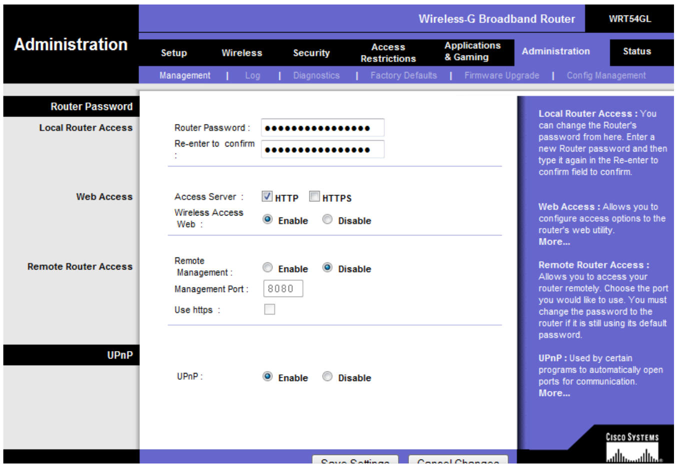


Firewall Protection : ● Enable ○ Disable

☑ Block Anonymous Internet Requests
☑ Filter Multicast
☐ Filter Internet NAT Redirection
☑ Filter IDENT(Port 113)

Firewall Protection : Enable or disable the SPI firewall.
More...

Y a continuación en Administration Management podemos cambiar la contraseña y la encriptar del modo elegido anteriormente



Router Password : ●●●●●●●●●●●●●●●●
Re-enter to confirm : ●●●●●●●●●●●●●●●●

Access Server : ☑ HTTP ☐ HTTPS
Wireless Access Web : ● Enable ○ Disable

Remote Management : ○ Enable ● Disable
Management Port : 8080
Use https : ☐

UPnP : ● Enable ○ Disable

Local Router Access : You can change the Router's password from here. Enter a new Router password and then type it again in the Re-enter to confirm field to confirm.

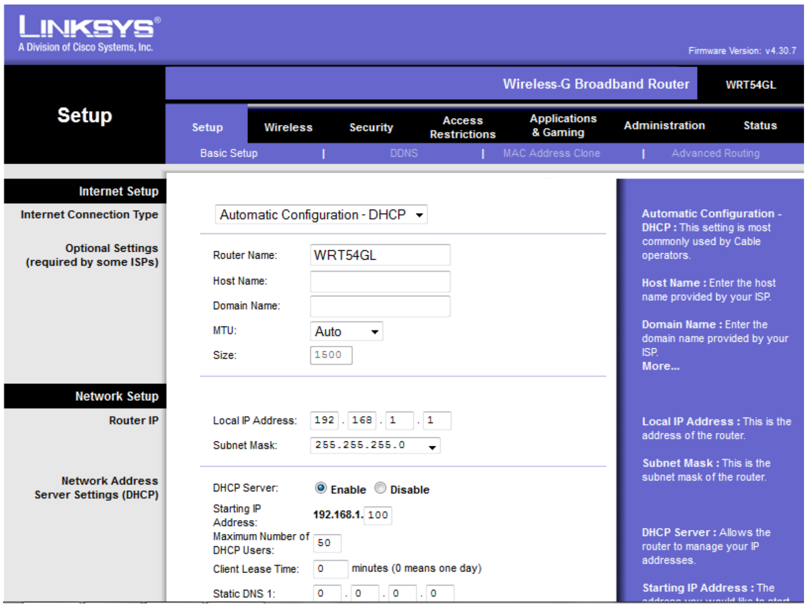
Web Access : Allows you to configure access options to the router's web utility.
More...

Remote Router Access : Allows you to access your router remotely. Choose the port you would like to use. You must change the password to the router if it is still using its default password.

UPnP : Used by certain programs to automatically open ports for communication.
More...

c) Configuración de un router de acceso inalámbrico CISCO Linksys seguro y un cliente de acceso inalámbrico en Windows y GNU/Linux.
- Filtro MAC, WPA, Control parental.

Conectamos el Router al pc y empezamos la configuración
Accedemos desde el navegador poniendo la dirección por defecto 192.168.1.1 y el usuario y contraseña por defecto admin



Internet Setup

Internet Connection Type: Automatic Configuration - DHCP

Optional Settings (required by some ISPs)

Router Name: WRT54GL
Host Name:
Domain Name:
MTU: Auto
Size: 1500

Network Setup

Router IP
Local IP Address: 192 . 168 . 1 . 1
Subnet Mask: 255.255.255.0

Network Address Server Settings (DHCP)
DHCP Server: ● Enable ○ Disable
Starting IP Address: 192.168.1. 100
Maximum Number of DHCP Users: 50
Client Lease Time: 0 minutes (0 means one day)
Static DNS 1: 0 . 0 . 0 . 0

Automatic Configuration - DHCP : This setting is most commonly used by Cable operators.

Host Name : Enter the host name provided by your ISP.

Domain Name : Enter the domain name provided by your ISP.
More...

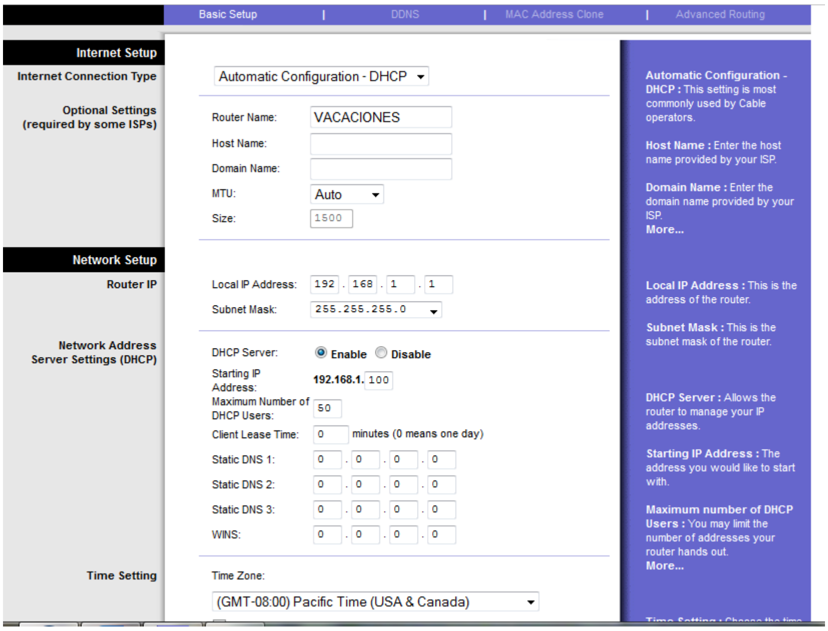
Local IP Address : This is the address of the router.

Subnet Mask : This is the subnet mask of the router.

DHCP Server : Allows the router to manage your IP addresses.

Starting IP Address : The

Cambiamos el nombre del Router por el de vacaciones



Internet Setup

Internet Connection Type: Automatic Configuration - DHCP

Optional Settings (required by some ISPs)

Router Name: VACACIONES
Host Name:
Domain Name:
MTU: Auto
Size: 1500

Network Setup

Router IP
Local IP Address: 192 . 168 . 1 . 1
Subnet Mask: 255.255.255.0

Network Address Server Settings (DHCP)
DHCP Server: ● Enable ○ Disable
Starting IP Address: 192.168.1. 100
Maximum Number of DHCP Users: 50
Client Lease Time: 0 minutes (0 means one day)
Static DNS 1: 0 . 0 . 0 . 0
Static DNS 2: 0 . 0 . 0 . 0
Static DNS 3: 0 . 0 . 0 . 0
WINS: 0 . 0 . 0 . 0

Time Setting
Time Zone: (GMT-08:00) Pacific Time (USA & Canada)

Automatic Configuration - DHCP : This setting is most commonly used by Cable operators.

Host Name : Enter the host name provided by your ISP.

Domain Name : Enter the domain name provided by your ISP.
More...

Local IP Address : This is the address of the router.

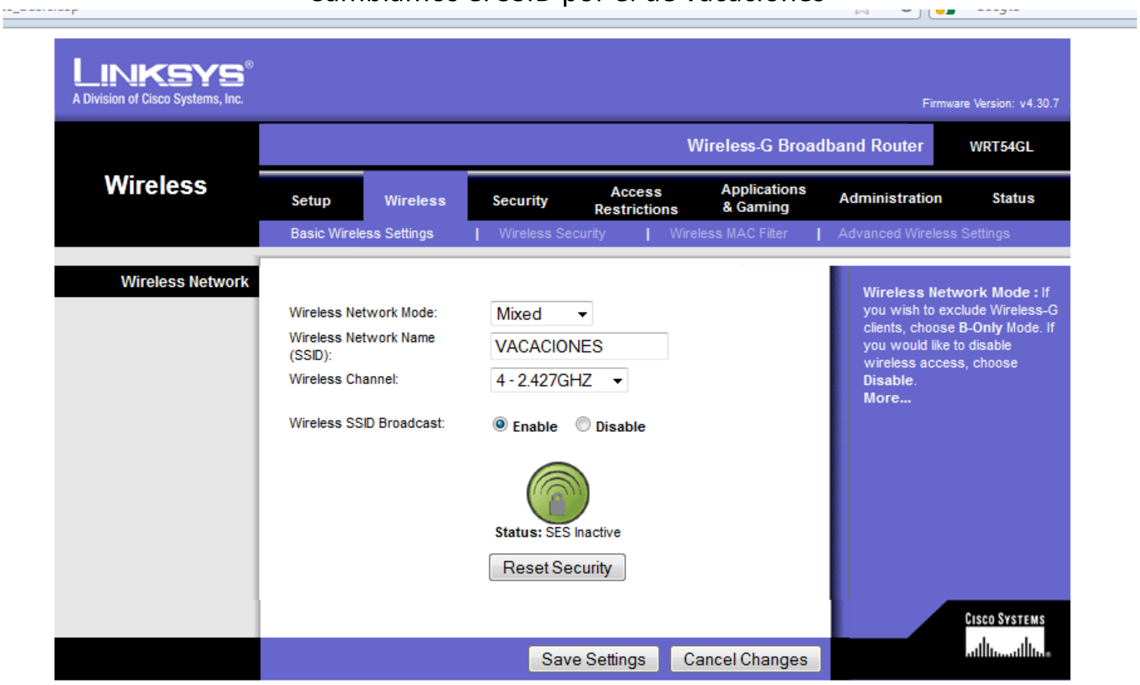
Subnet Mask : This is the subnet mask of the router.

DHCP Server : Allows the router to manage your IP addresses.

Starting IP Address : The address you would like to start with.

Maximum number of DHCP Users : You may limit the number of addresses your router hands out.
More...

Cambiamos el SSID por el de vacaciones


LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: v4.30.7
Wireless-G Broadband Router
WRT54GL
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings
Wireless Network

Wireless Network Mode: Mixed

Wireless Network Name (SSID): VACACIONES

Wireless Channel: 4 - 2.427GHZ

Wireless SSID Broadcast: ● Enable ○ Disable

Status: SES Inactive

Wireless Network Mode : If you wish to exclude Wireless-G clients, choose **B-Only** Mode. If you would like to disable wireless access, choose **Disable**.
More...

Cisco Systems
Save Settings
Cancel Changes

Generamos una clave WEP de la palabra vacaciones

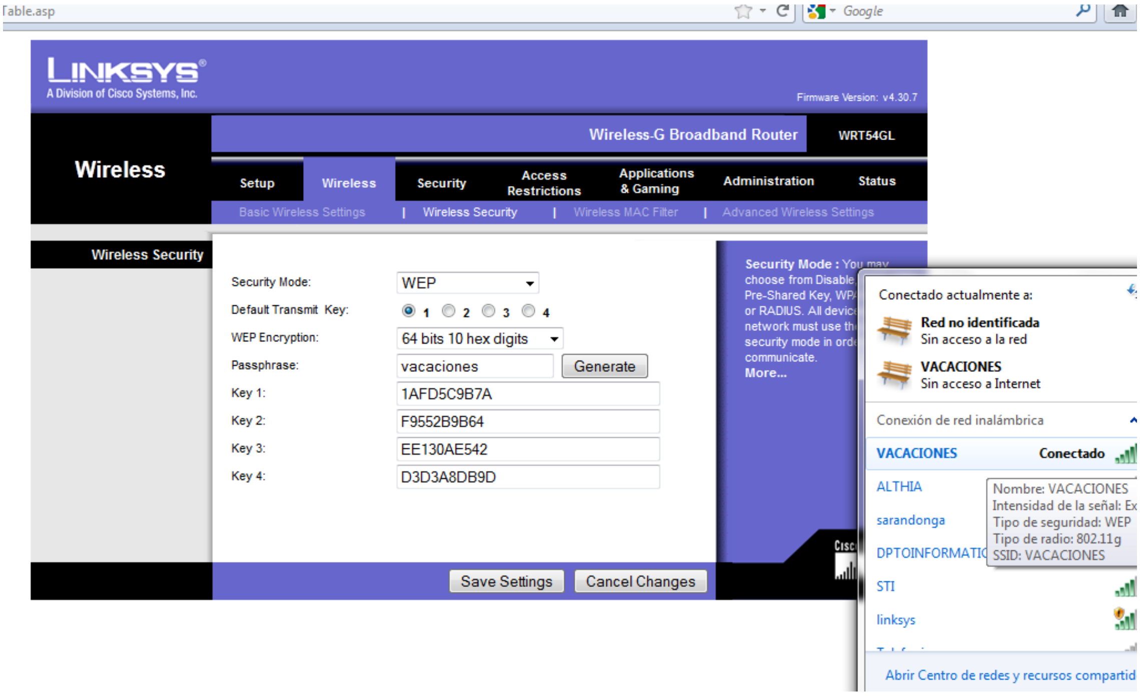


Table.asp
Google
LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: v4.30.7
Wireless-G Broadband Router
WRT54GL
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings
Wireless Security

Security Mode: WEP

Default Transmit Key: ● 1 ○ 2 ○ 3 ○ 4

WEP Encryption: 64 bits 10 hex digits

Passphrase: vacaciones

Key 1: 1AFD5C9B7A

Key 2: F9552B9B64

Key 3: EE130AE542

Key 4: D3D3A8DB9D

Save Settings
Cancel Changes

Security Mode : You may choose from Disable, Pre-Shared Key, WP or RADIUS. All devic network must use th security mode in ord communicate.
More...

Conectado actualmente a:

Red no identificada
Sin acceso a la red

VACACIONES
Sin acceso a Internet

Conexión de red inalámbrica

VACACIONES **Conectado**

ALTHIA

sarandonga

DPTOINFORMATIC

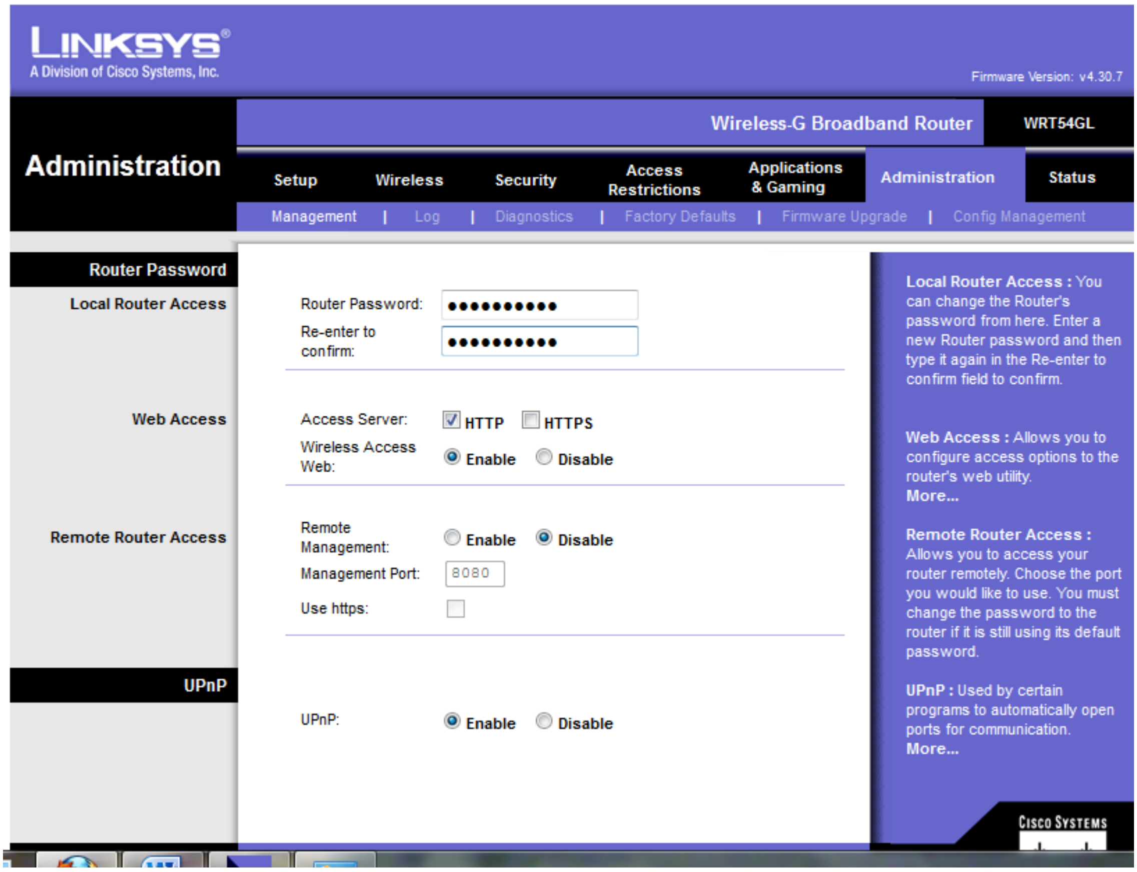
STI

linksys

Nombre: VACACIONES
Intensidad de la señal: Ex
Tipo de seguridad: WEP
Tipo de radio: 802.11g
SSID: VACACIONES

Abrir Centro de redes y recursos compartid

Cambiamos la contraseña


LINKSYS® A Division of Cisco Systems, Inc.

Firmware Version: v4.30.7

Wireless-G Broadband Router WRT54GL

Administration

Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status

Management | Log | Diagnostics | Factory Defaults | Firmware Upgrade | Config Management

Router Password

Local Router Access

Router Password: ••••••••••

Re-enter to confirm: ••••••••••

Web Access

Access Server: ☑ HTTP □ HTTPS

Wireless Access Web: ● Enable ○ Disable

Remote Router Access

Remote Management: ○ Enable ● Disable

Management Port: 8080

Use https: □

UPnP

UPnP: ● Enable ○ Disable

Local Router Access : You can change the Router's password from here. Enter a new Router password and then type it again in the Re-enter to confirm field to confirm.

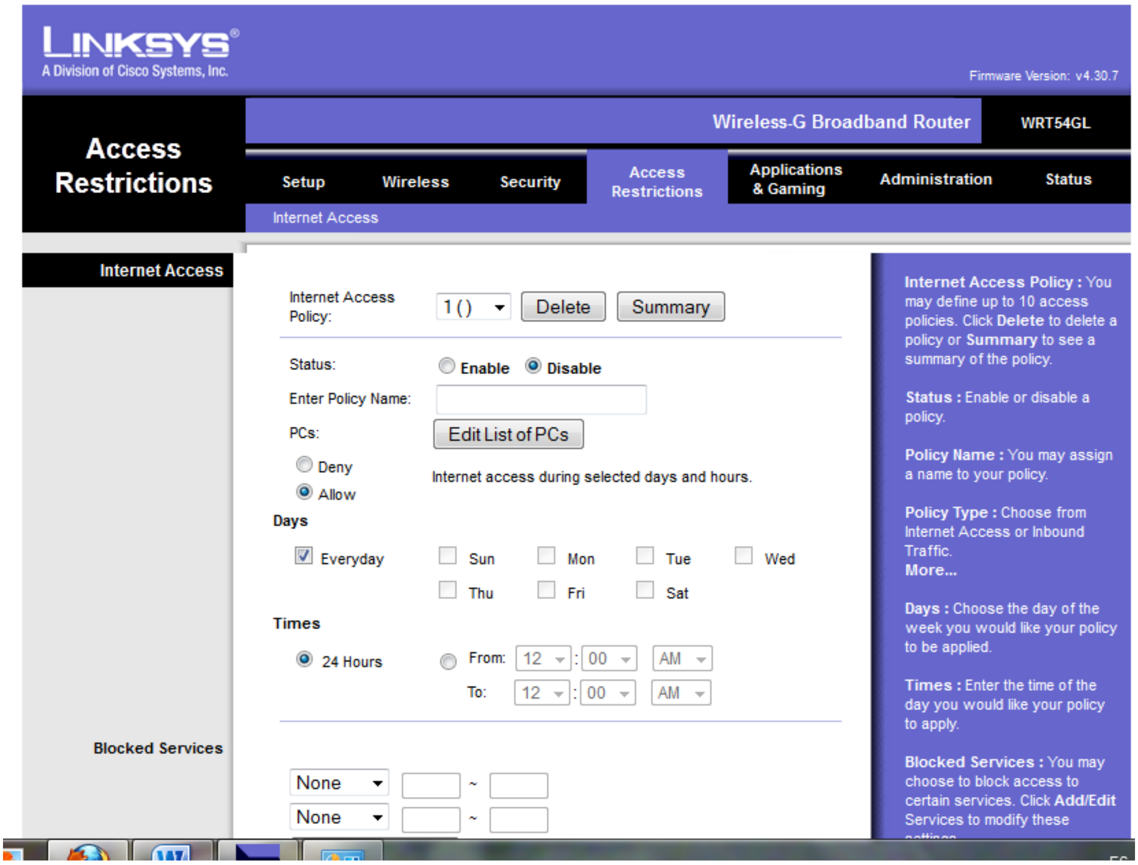
Web Access : Allows you to configure access options to the router's web utility.
More...

Remote Router Access : Allows you to access your router remotely. Choose the port you would like to use. You must change the password to the router if it is still using its default password.

UPnP : Used by certain programs to automatically open ports for communication.
More...

CISCO SYSTEMS

Y ahora creamos el control parental con las restricciones que queremos


LINKSYS® A Division of Cisco Systems, Inc.

Firmware Version: v4.30.7

Wireless-G Broadband Router WRT54GL

Access Restrictions

Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status

Internet Access

Internet Access

Internet Access Policy: 1 () [Delete] [Summary]

Status: ○ Enable ● Disable

Enter Policy Name:

PCs: [Edit List of PCs]

○ Deny
● Allow
Internet access during selected days and hours.

Days

☑ Everyday □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Times

● 24 Hours ○ From: 12 : 00 AM To: 12 : 00 AM

Blocked Services

None ~
None ~

Internet Access Policy : You may define up to 10 access policies. Click **Delete** to delete a policy or **Summary** to see a summary of the policy.

Status : Enable or disable a policy.

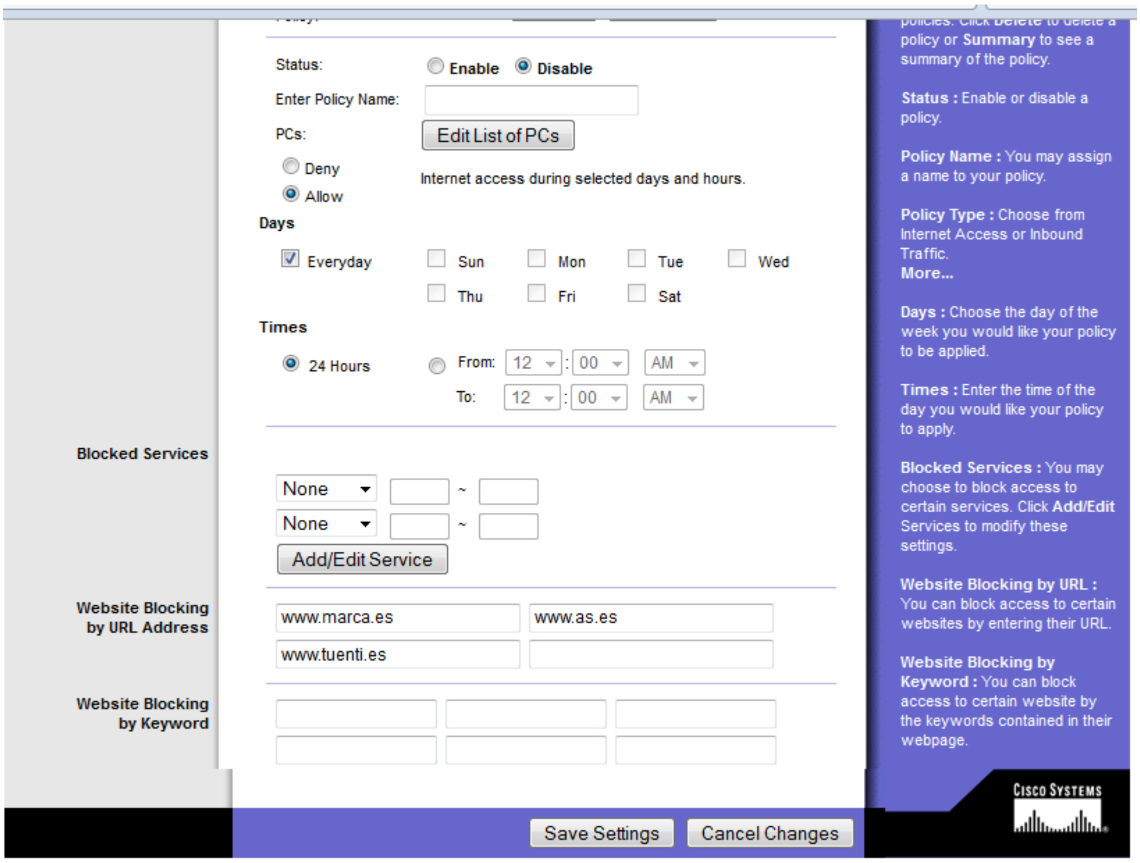
Policy Name : You may assign a name to your policy.

Policy Type : Choose from Internet Access or Inbound Traffic.
More...

Days : Choose the day of the week you would like your policy to be applied.

Times : Enter the time of the day you would like your policy to apply.

Blocked Services : You may choose to block access to certain services. Click **Add/Edit** Services to modify these



Status: ○ Enable ● Disable

Enter Policy Name:

PCs: Edit List of PCs

○ Deny
● Allow
Internet access during selected days and hours.

Days

☑ Everyday □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Times

● 24 Hours ○ From: 12 : 00 AM To: 12 : 00 AM

Blocked Services: None ~ / None ~

Website Blocking by URL Address: www.marca.es, www.as.es, www.tuenti.es

Website Blocking by Keyword:

policies. Click **Delete** to delete a policy or **Summary** to see a summary of the policy.

Status : Enable or disable a policy.

Policy Name : You may assign a name to your policy.

Policy Type : Choose from Internet Access or Inbound Traffic.
More...

Days : Choose the day of the week you would like your policy to be applied.

Times : Enter the time of the day you would like your policy to apply.

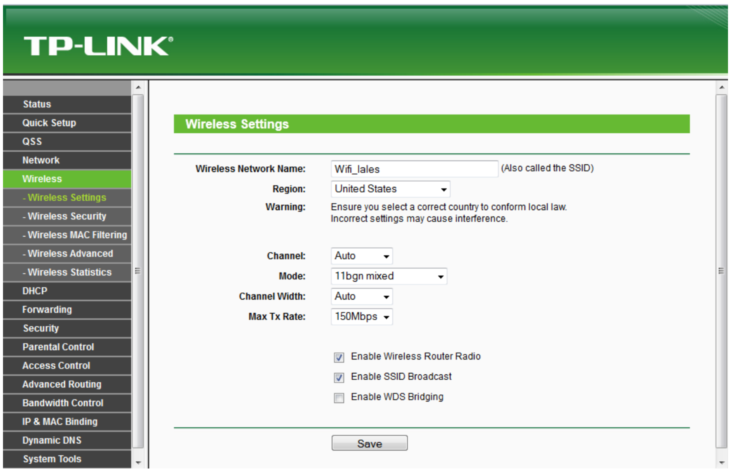
Blocked Services : You may choose to block access to certain services. Click **Add/Edit** Services to modify these settings.

Website Blocking by URL : You can block access to certain websites by entering their URL.

Website Blocking by Keyword : You can block access to certain website by the keywords contained in their webpage.

d) Configuración de un router de acceso inalámbrico TP-LINK, utilizando un simulador. http://www.tp-link.com/en/support/emulators/

Nos vamos a la página arriba indicada y vamos a configurar el Router inalámbrico de forma simulada, para ello vamos primero a Wireless Settings y cambiamos el SSID y ponemos Wifi_lales



Wireless Settings

Wireless Network Name: Wifi_lales (Also called the SSID)

Region: United States

Warning: Ensure you select a correct country to conform local law.
Incorrect settings may cause interference.

Channel: Auto

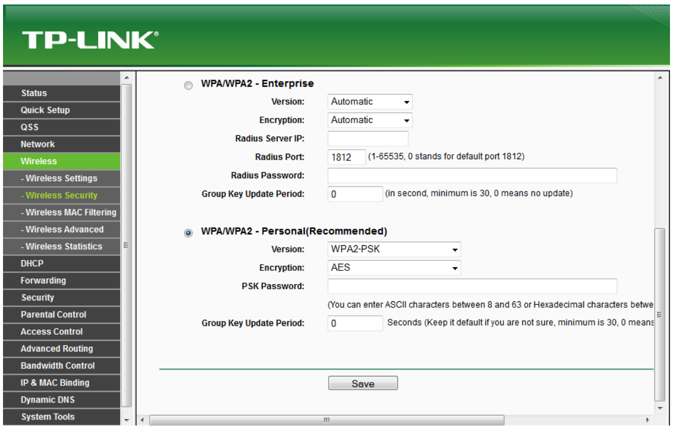
Mode: 11bgn mixed

Channel Width: Auto

Max Tx Rate: 150Mbps

☑ Enable Wireless Router Radio
☑ Enable SSID Broadcast
□ Enable WDS Bridging

A continuación vamos a Wireless Security y vamos a cambiar la forma de cifrado y elegimos Versión WPA2-PSK y en Encryption AES



○ WPA/WPA2 - Enterprise

Version: Automatic

Encryption: Automatic

Radius Server IP:

Radius Port: 1812 (1-65535, 0 stands for default port 1812)

Radius Password:

Group Key Update Period: 0 (in second, minimum is 30, 0 means no update)

● WPA/WPA2 - Personal(Recommended)

Version: WPA2-PSK

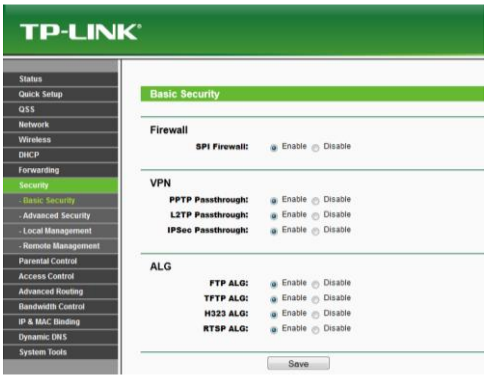
Encryption: AES

PSK Password:

(You can enter ASCII characters between 8 and 63 or Hexadecimal characters betwe

Group Key Update Period: 0 Seconds (Keep it default if you are not sure, minimum is 30, 0 means

En Security, Basic Security vamos a poner Firewall en Enable



Basic Security

Firewall

SPI Firewall: ● Enable ○ Disable

VPN

PPTP Passthrough: ● Enable ○ Disable

L2TP Passthrough: ● Enable ○ Disable

IPSec Passthrough: ● Enable ○ Disable

ALG

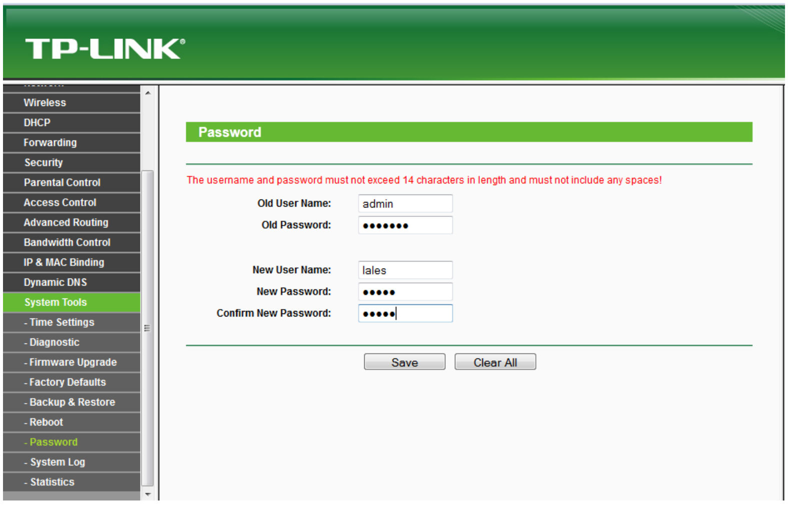
FTP ALG: ● Enable ○ Disable

TFTP ALG: ● Enable ○ Disable

H323 ALG: ● Enable ○ Disable

RTSP ALG: ● Enable ○ Disable

Y ahora en System Tools cambiamos la contraseña y el usuario



Password

The username and password must not exceed 14 characters in length and must not include any spaces!

Old User Name: admin

Old Password: •••••••

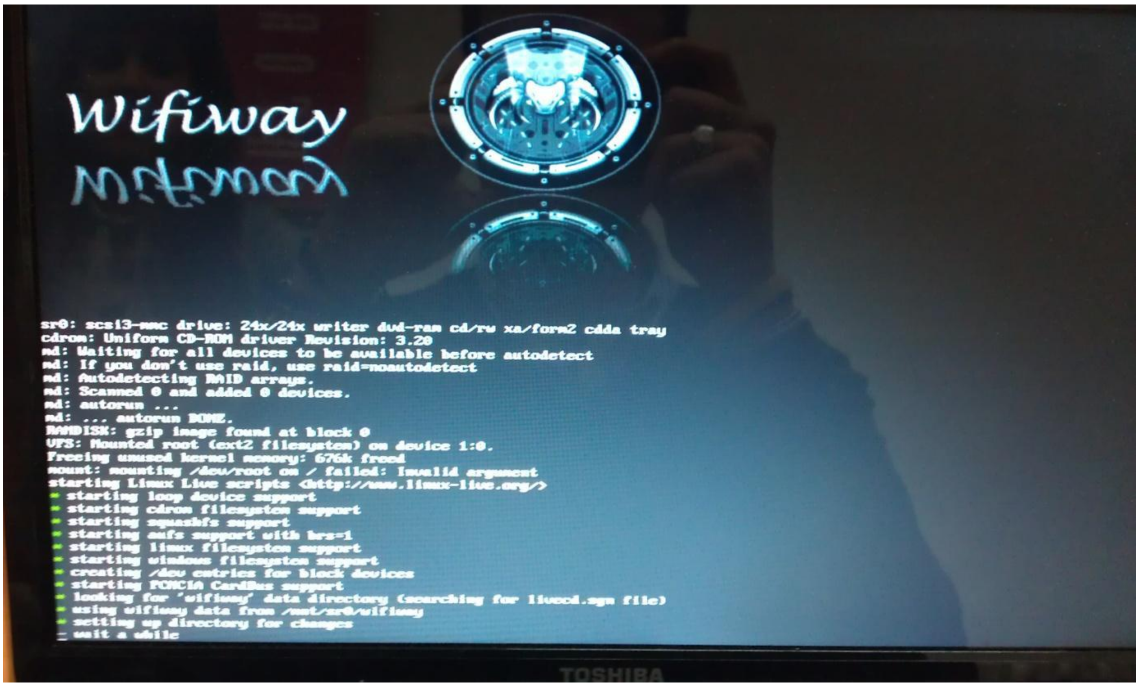
New User Name: lales

New Password: •••••

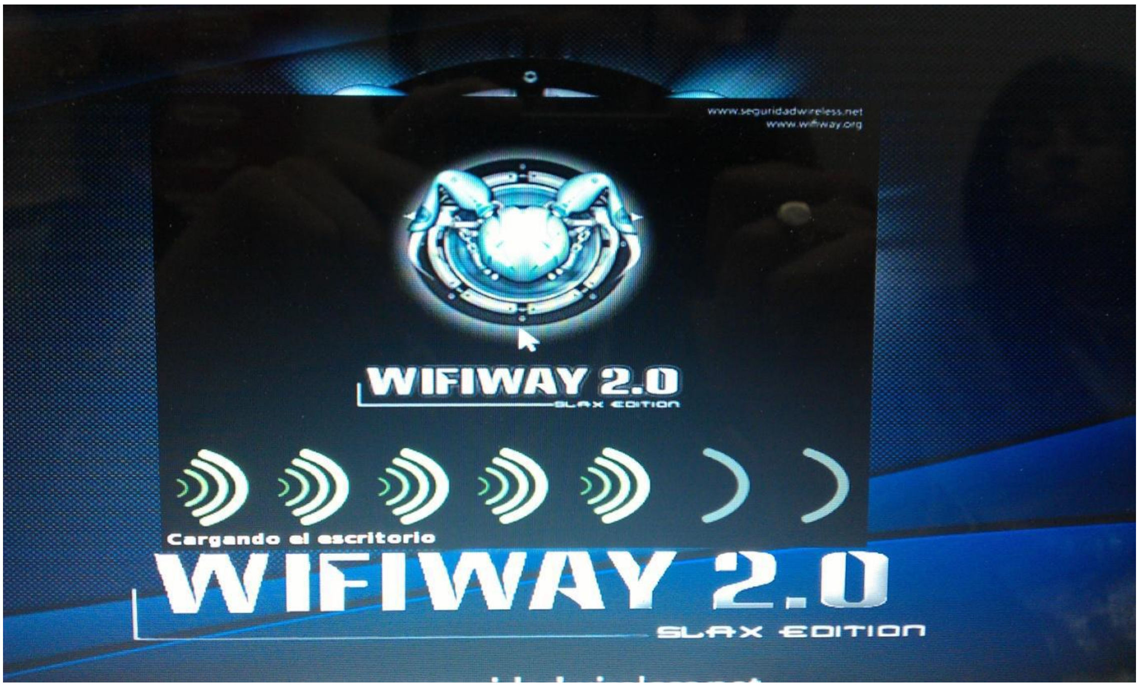
Confirm New Password: •••••

e) Realiza una auditoria Wireless para medir el nivel de seguridad de una red inalámbrica, utilizando una distribución Live (Backtrack, Wifiway, Wifislax, etc) para monitorizar y recuperar contraseñas inalámbricas WEP.

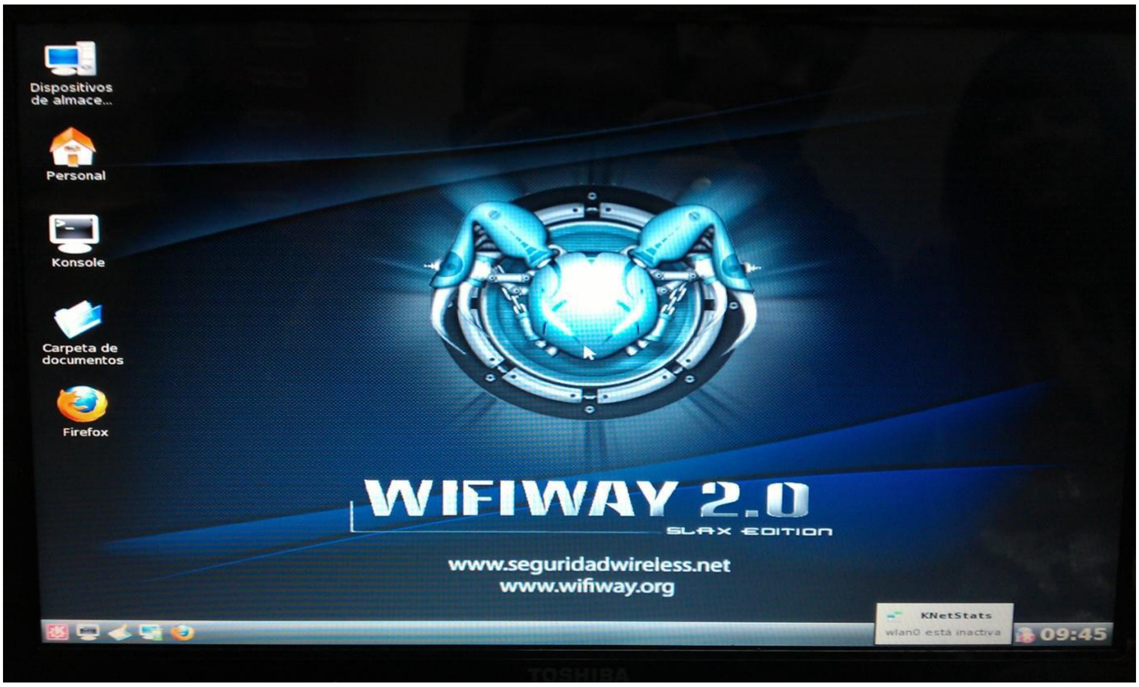
Introducimos el CD para que el ordenador arranque desde él

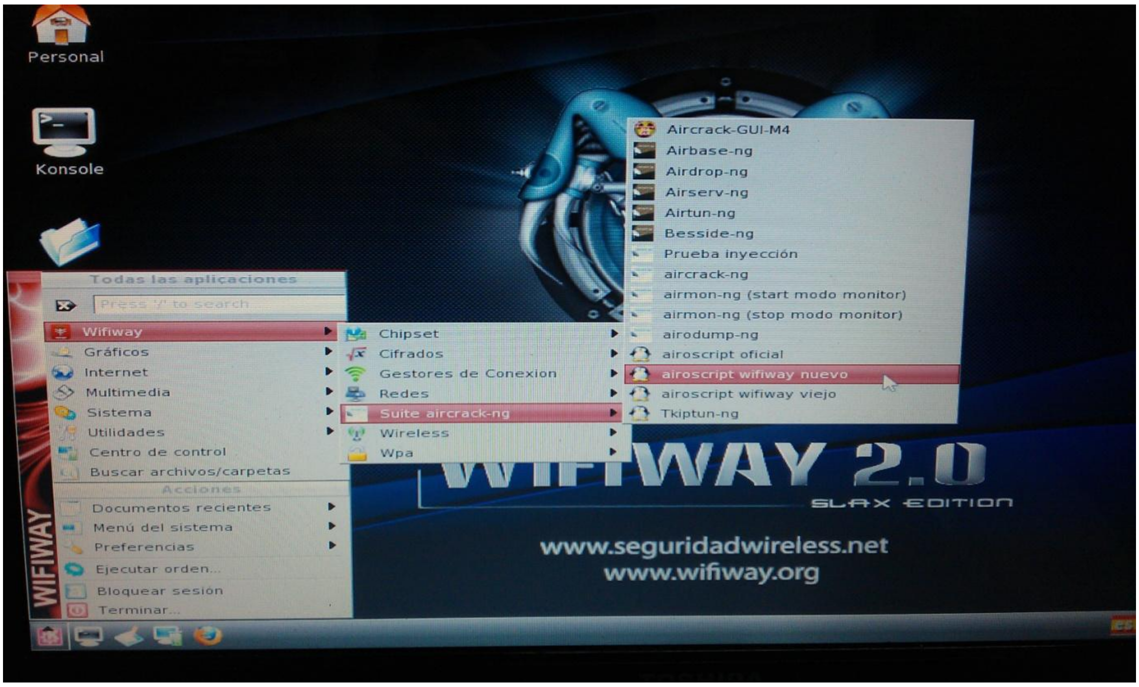


```
sr0: scsi3-mmc drive: 24x/24x writer dvd-ram cd/rw xa/form2 cdda tray
cdrom: Uniform CD-ROM driver Revision: 3.20
md: Waiting for all devices to be available before autodetect
md: If you don't use raid, use raid=noautodetect
md: Autodetecting RAID arrays.
md: Scanned 0 and added 0 devices.
md: autorun ...
md: ... autorun DONE.
RAMDISK: gzip image found at block 0
VFS: Mounted root (ext2 filesystem) on device 1:0.
Freeing unused kernel memory: 676k freed
mount: mounting /dev/root on / failed: Invalid argument
starting Linux Live scripts <http://www.linux-live.org/>
 * starting loop device support
 * starting cdrom filesystem support
 * starting squashfs support
 * starting aufs support with brs=1
 * starting linux filesystem support
 * starting windows filesystem support
 * creating /dev entries for block devices
 * starting PCMCIA CardBus support
 * looking for 'wifiway' data directory (searching for livecd.sgn file)
 * using wifiway data from /mnt/sr0/wifiway
 * setting up directory for changes
 - wait a while
```

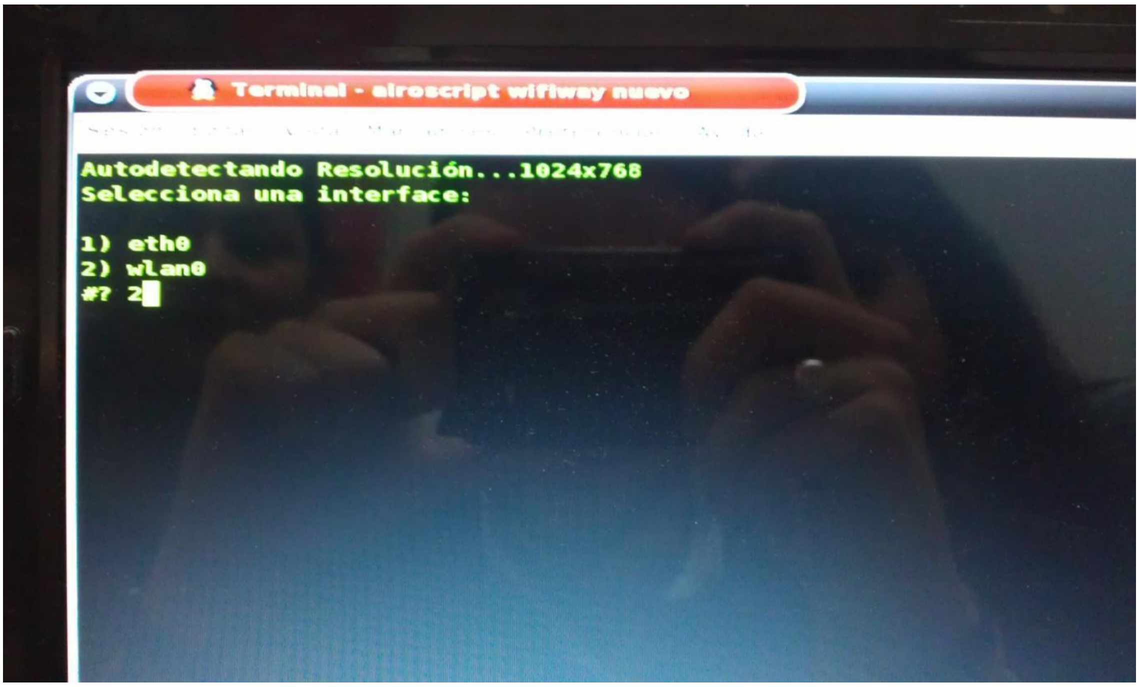


Una vez en la pantalla principal nos vamos al menú de inicio



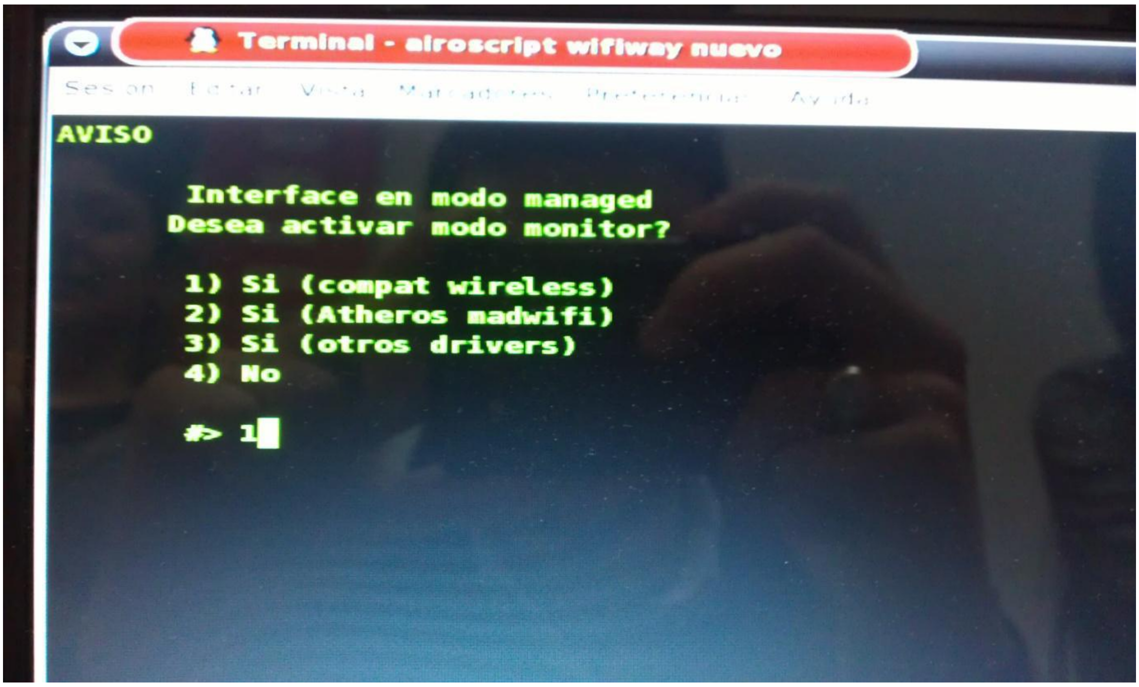


Elegimos la opción wlan0



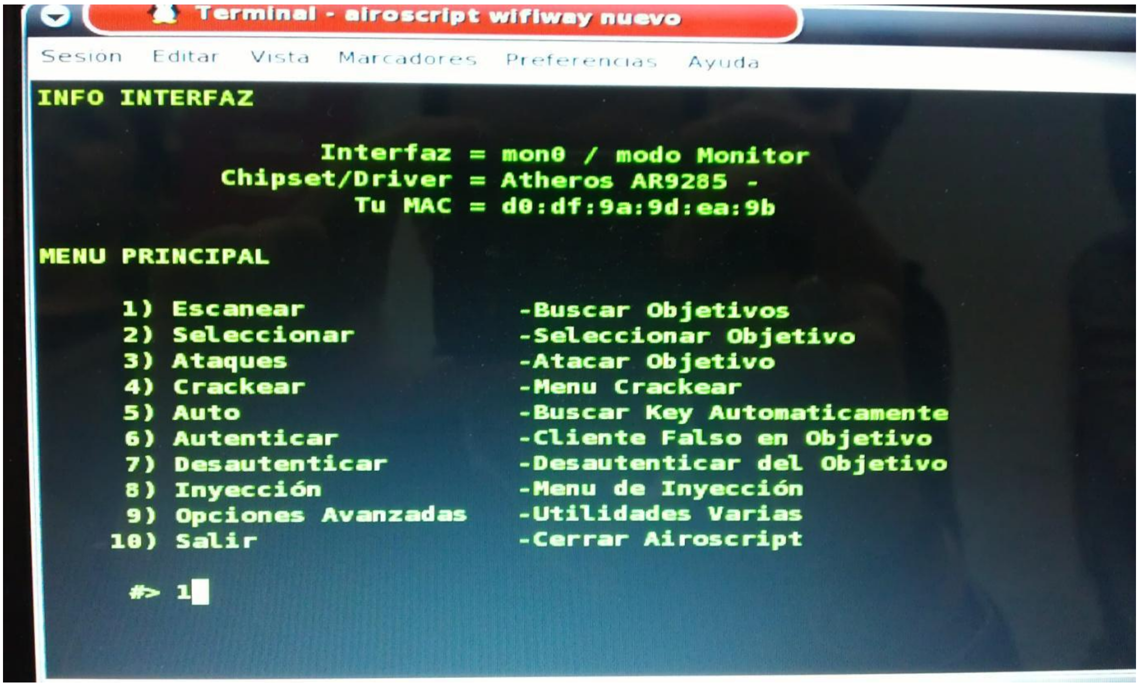
```
Autodetectando Resolución...1024x768
Selecciona una interface:

1) eth0
2) wlan0
#? 2
```

A continuación la opción 1, activar modo monitor



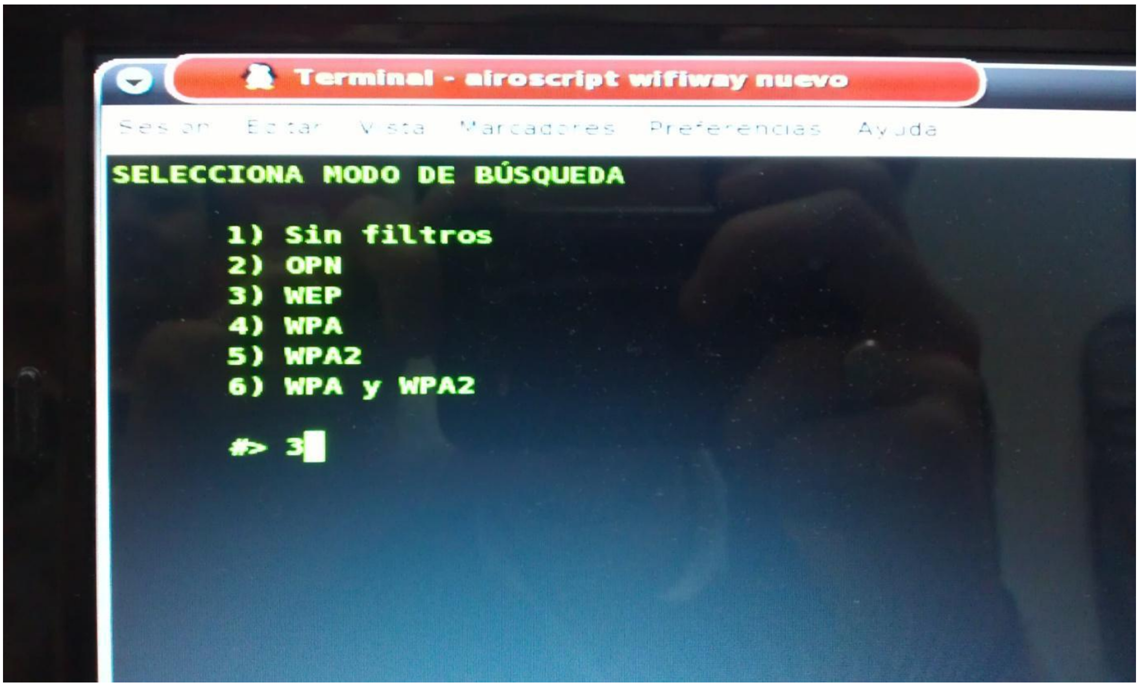
```
AVISO

        Interface en modo managed
       Desea activar modo monitor?

        1) Si (compat wireless)
        2) Si (Atheros madwifi)
        3) Si (otros drivers)
        4) No

        #> 1
```

Ahora la opción Escanear, 1



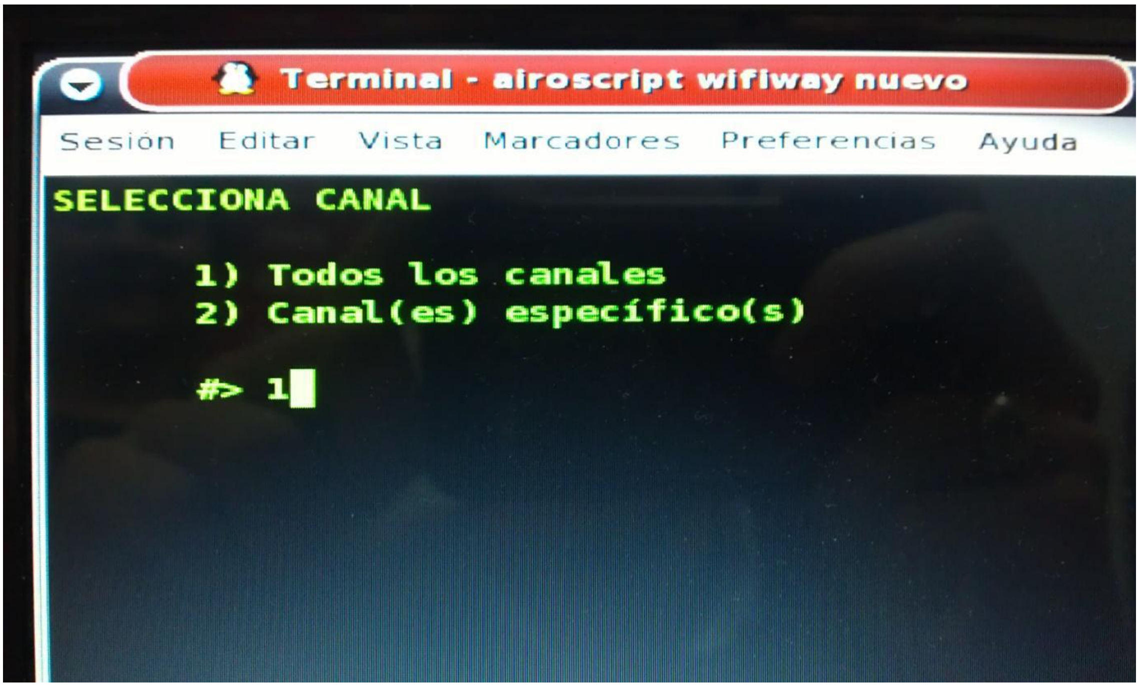
```
INFO INTERFAZ

             Interfaz = mon0 / modo Monitor
       Chipset/Driver = Atheros AR9285 -
               Tu MAC = d0:df:9a:9d:ea:9b

MENU PRINCIPAL

     1) Escanear                -Buscar Objetivos
     2) Seleccionar             -Seleccionar Objetivo
     3) Ataques                 -Atacar Objetivo
     4) Crackear                -Menu Crackear
     5) Auto                    -Buscar Key Automaticamente
     6) Autenticar              -Cliente Falso en Objetivo
     7) Desautenticar           -Desautenticar del Objetivo
     8) Inyección               -Menu de Inyección
     9) Opciones Avanzadas      -Utilidades Varias
    10) Salir                   -Cerrar Airoscript

      #> 1
```

Modo de Búsqueda de encriptación elegimos WEP, 3



```
SELECCIONA MODO DE BÚSQUEDA

      1) Sin filtros
      2) OPN
      3) WEP
      4) WPA
      5) WPA2
      6) WPA y WPA2

      #> 3
```

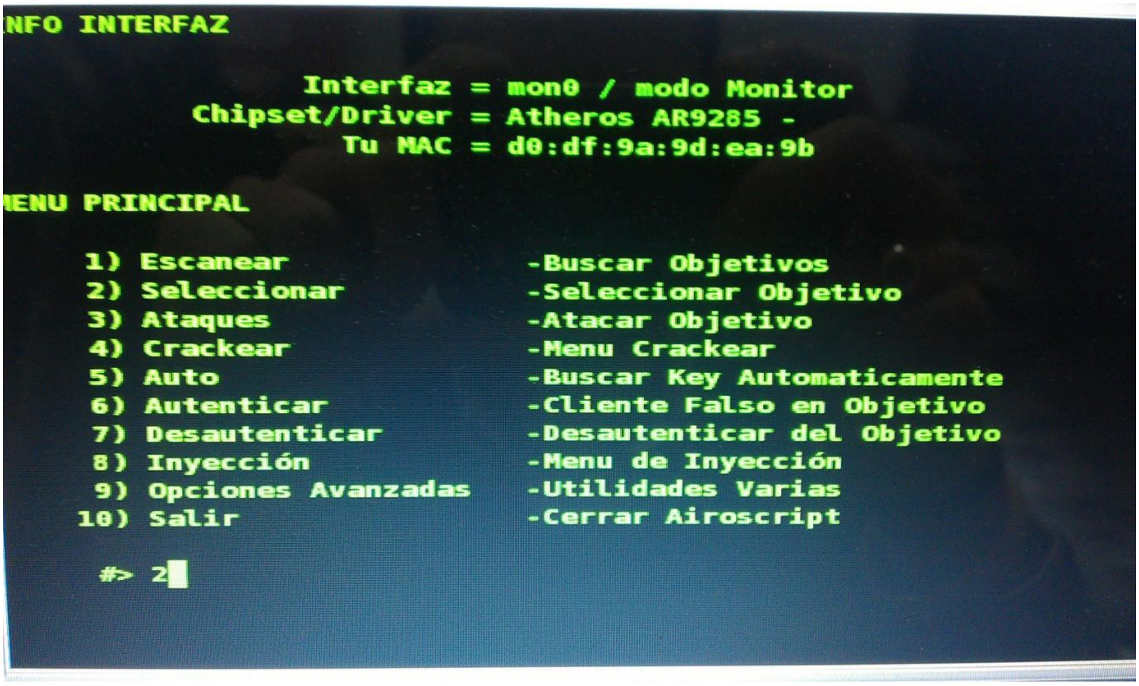
Que busque en todos los canales



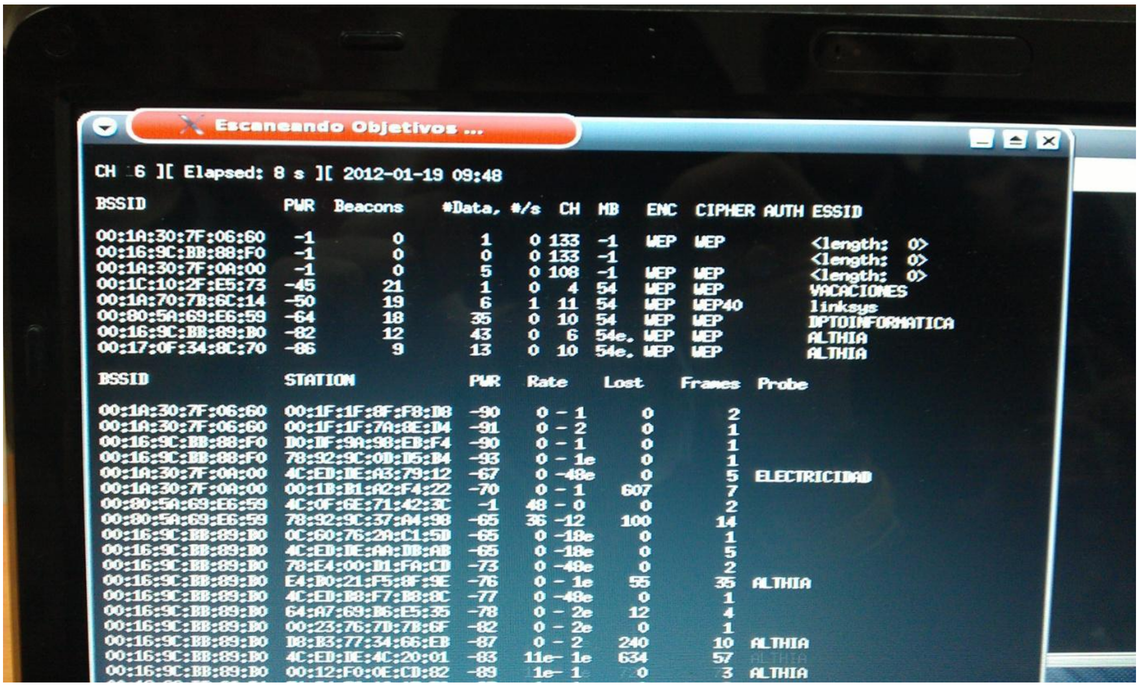
Terminal - airoscript wifiway nuevo
Sesión Editar Vista Marcadores Preferencias Ayuda

```
SELECCIONA CANAL

        1) Todos los canales
        2) Canal(es) específico(s)

        #> 1
```

Ahora vamos a seleccionar objetivo

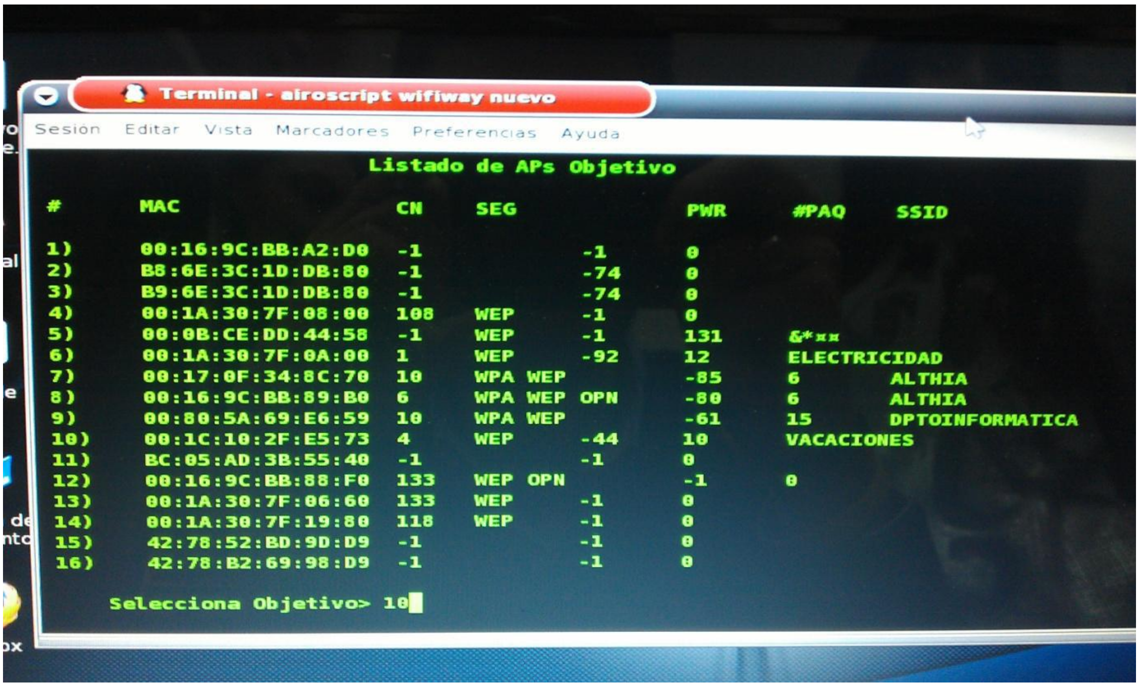


```
NFO INTERFAZ

                Interfaz = mon0 / modo Monitor
          Chipset/Driver = Atheros AR9285 -
                  Tu MAC = d0:df:9a:9d:ea:9b

IENU PRINCIPAL

     1) Escanear                 -Buscar Objetivos
     2) Seleccionar              -Seleccionar Objetivo
     3) Ataques                  -Atacar Objetivo
     4) Crackear                 -Menu Crackear
     5) Auto                     -Buscar Key Automaticamente
     6) Autenticar               -Cliente Falso en Objetivo
     7) Desautenticar            -Desautenticar del Objetivo
     8) Inyección                -Menu de Inyección
     9) Opciones Avanzadas       -Utilidades Varias
    10) Salir                    -Cerrar Airoscript

     #> 2
```



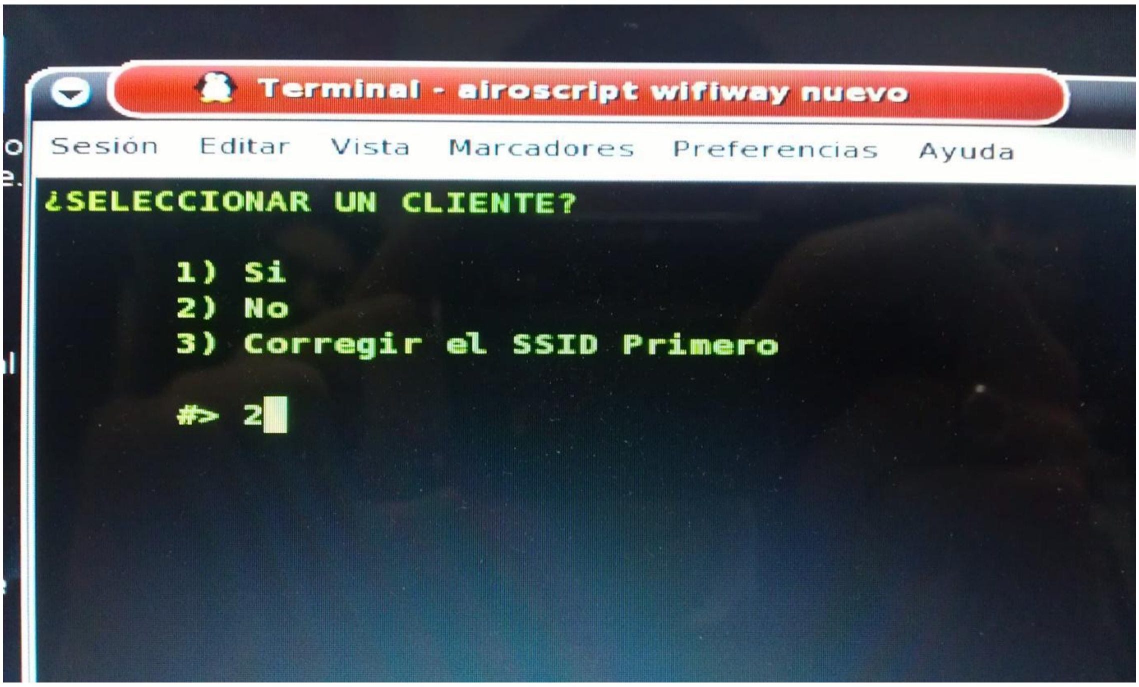
```
CH  6 ][ Elapsed: 8 s ][ 2012-01-19 09:48

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

00:1A:30:7F:06:60   -1        0        1    0 133  -1   WEP  WEP         <length:  0>
00:16:9C:BB:88:F0   -1        0        0    0 133  -1                    <length:  0>
00:1A:30:7F:0A:00   -1        0        5    0 108  -1   WEP  WEP         <length:  0>
00:1C:10:2F:E5:73  -45       21        1    0   4  54   WEP  WEP         VACACIONES
00:1A:70:7B:6C:14  -50       19        6    1  11  54   WEP  WEP40       linksys
00:80:5A:69:E6:59  -64       18       35    0  10  54   WEP  WEP         DPTOINFORMATICA
00:16:9C:BB:89:B0  -82       12       43    0   6  54e. WEP  WEP         ALTHIA
00:17:0F:34:8C:70  -86        9       13    0  10  54e. WEP  WEP         ALTHIA

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:1A:30:7F:06:60  00:1F:1F:8F:F8:D8  -90    0 - 1      0        2
00:1A:30:7F:06:60  00:1F:1F:7A:8E:D4  -91    0 - 2      0        1
00:16:9C:BB:88:F0  D0:DF:9A:98:EB:F4  -90    0 - 1      0        1
00:16:9C:BB:88:F0  78:92:9C:0D:D5:B4  -93    0 - 1e     0        1
00:1A:30:7F:0A:00  4C:ED:DE:A3:79:12  -67    0 -48e     0        5  ELECTRICIDAD
00:1A:30:7F:0A:00  00:1B:B1:A2:F4:22  -70    0 - 1    607        7
00:80:5A:69:E6:59  4C:0F:6E:71:42:3C   -1   48 - 0      0        2
00:80:5A:69:E6:59  78:92:9C:37:A4:98  -65   36 -12    100       14
00:16:9C:BB:89:B0  0C:60:76:2A:C1:5D  -65    0 -18e     0        1
00:16:9C:BB:89:B0  4C:ED:DE:AA:DB:AB  -65    0 -18e     0        5
00:16:9C:BB:89:B0  78:E4:00:D1:FA:CD  -73    0 -48e     0        2
00:16:9C:BB:89:B0  E4:B0:21:F5:8F:9E  -76    0 - 1e    55       35  ALTHIA
00:16:9C:BB:89:B0  4C:ED:B8:F7:B8:8C  -77    0 -48e     0        1
00:16:9C:BB:89:B0  64:A7:69:B6:E5:35  -78    0 - 2e    12        4
00:16:9C:BB:89:B0  00:23:76:7D:7B:6F  -82    0 - 2e     0        1
00:16:9C:BB:89:B0  D8:B3:77:34:66:EB  -87    0 - 2    240       10  ALTHIA
00:16:9C:BB:89:B0  4C:ED:DE:4C:20:01  -83  11e- 1e    634       57  ALTHIA
00:16:9C:BB:89:B0  00:12:F0:0E:CD:82  -89   1e- 1     720        3  ALTHIA
```

Ya ha encontrado vacaciones, y elegimos la 10



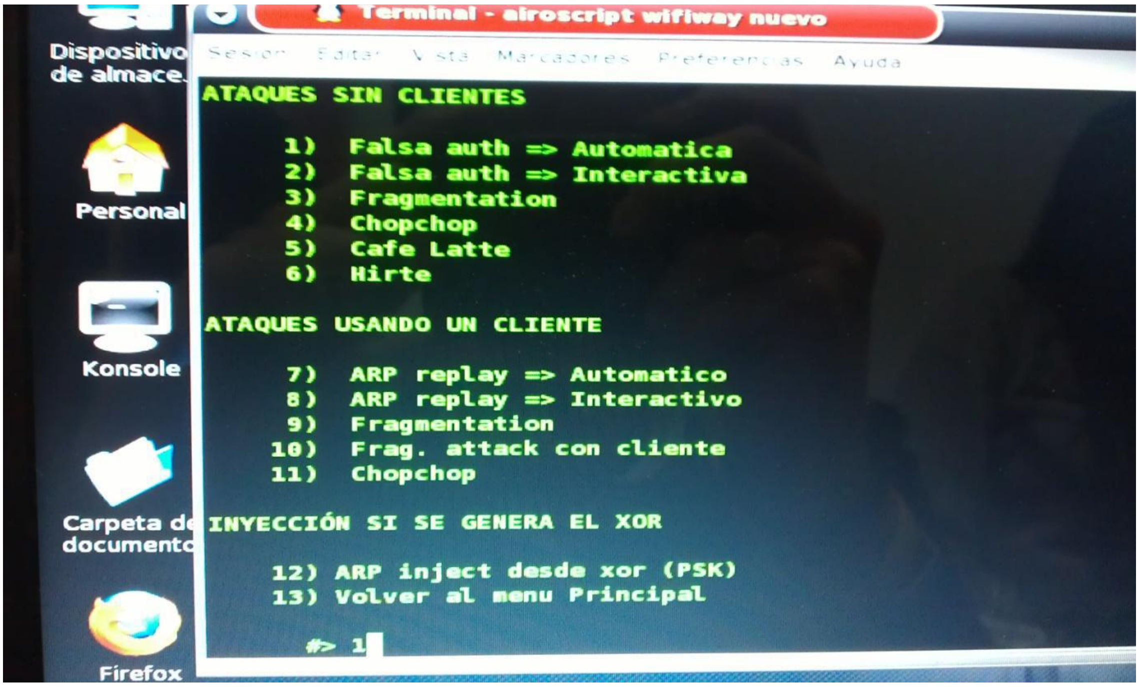
```
                        Listado de APs Objetivo

 #       MAC                 CN    SEG                PWR     #PAQ      SSID

 1)      00:16:9C:BB:A2:D0   -1               -1      0
 2)      B8:6E:3C:1D:DB:80   -1               -74     0
 3)      B9:6E:3C:1D:DB:80   -1               -74     0
 4)      00:1A:30:7F:08:00   108   WEP        -1      0
 5)      00:0B:CE:DD:44:58   -1    WEP        -1      131     &*¤¤
 6)      00:1A:30:7F:0A:00   1     WEP        -92     12      ELECTRICIDAD
 7)      00:17:0F:34:8C:70   10    WPA WEP            -85     6         ALTHIA
 8)      00:16:9C:BB:89:B0   6     WPA WEP OPN        -80     6         ALTHIA
 9)      00:80:5A:69:E6:59   10    WPA WEP            -61     15        DPTOINFORMATICA
10)      00:1C:10:2F:E5:73   4     WEP        -44     10      VACACIONES
11)      BC:05:AD:3B:55:40   -1               -1      0
12)      00:16:9C:BB:88:F0   133   WEP OPN            -1      0
13)      00:1A:30:7F:06:60   133   WEP        -1      0
14)      00:1A:30:7F:19:80   118   WEP        -1      0
15)      42:78:52:BD:9D:D9   -1               -1      0
16)      42:78:B2:69:98:D9   -1               -1      0

     Selecciona Objetivo> 10
```

Ahora seleccionar un cliente, le decimos opción 2, no


Terminal - airoscript wifiway nuevo
Sesión Editar Vista Marcadores Preferencias Ayuda

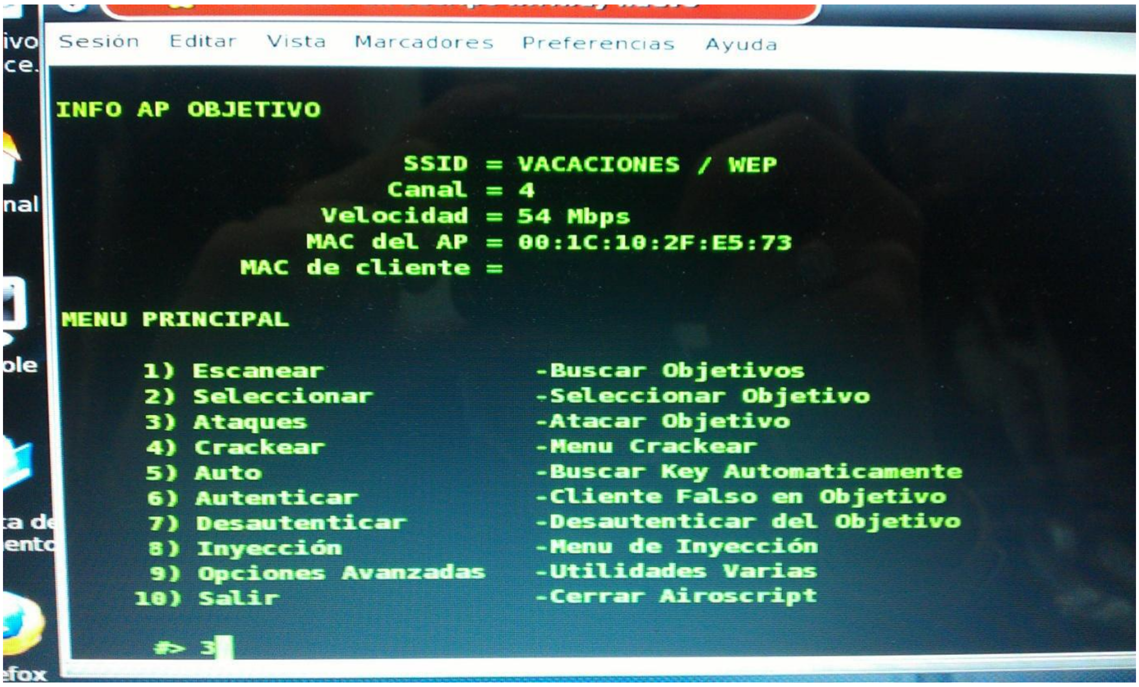
```
¿SELECCIONAR UN CLIENTE?

        1) Si
        2) No
        3) Corregir el SSID Primero

        #> 2
```

Ahora ponemos opción automática, 1

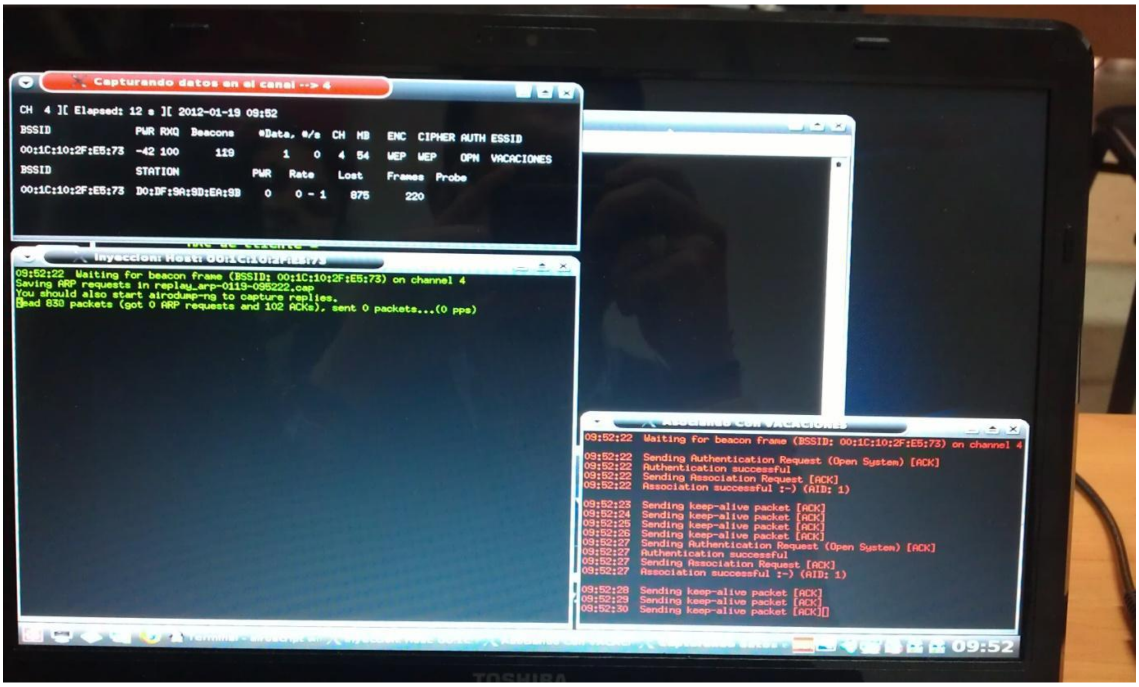

Terminal - airoscript wifiway nuevo
Sesion Editar Vista Marcadores Preferencias Ayuda
Dispositivo de almace
Personal
Konsole
Carpeta de documento
Firefox

```
ATAQUES SIN CLIENTES

        1)  Falsa auth => Automatica
        2)  Falsa auth => Interactiva
        3)  Fragmentation
        4)  Chopchop
        5)  Cafe Latte
        6)  Hirte

ATAQUES USANDO UN CLIENTE

        7)  ARP replay => Automatico
        8)  ARP replay => Interactivo
        9)  Fragmentation
       10)  Frag. attack con cliente
       11)  Chopchop

INYECCIÓN SI SE GENERA EL XOR

       12) ARP inject desde xor (PSK)
       13) Volver al menu Principal

          #> 1
```

Ahora elegimos opción 3, Ataques



```
INFO AP OBJETIVO

                     SSID = VACACIONES / WEP
                    Canal = 4
                Velocidad = 54 Mbps
               MAC del AP = 00:1C:10:2F:E5:73
           MAC de cliente =

MENU PRINCIPAL

     1) Escanear                -Buscar Objetivos
     2) Seleccionar             -Seleccionar Objetivo
     3) Ataques                 -Atacar Objetivo
     4) Crackear                -Menu Crackear
     5) Auto                    -Buscar Key Automaticamente
     6) Autenticar              -Cliente Falso en Objetivo
     7) Desautenticar           -Desautenticar del Objetivo
     8) Inyección               -Menu de Inyección
     9) Opciones Avanzadas      -Utilidades Varias
    10) Salir                   -Cerrar Airoscript

       #> 3
```

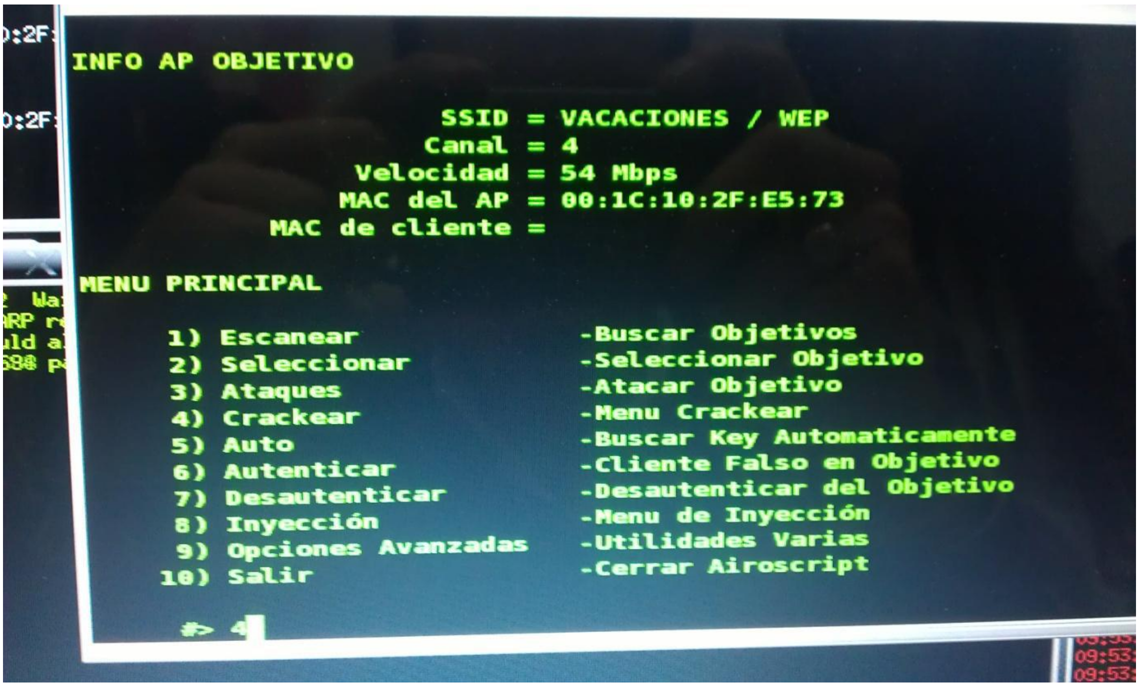

Capturando datos en el canal --> 4
Inyeccion: Host: 00:1C:10:2F:E5:73
Asociando con VACACIONES
09:52

```
CH  4 ][ Elapsed: 12 s ][ 2012-01-19 09:52

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

00:1C:10:2F:E5:73  -42 100      119        1    0   4  54   WEP  WEP    OPN  VACACIONES

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:1C:10:2F:E5:73  D0:DF:9A:9D:EA:9B    0    0 - 1    875      220
```

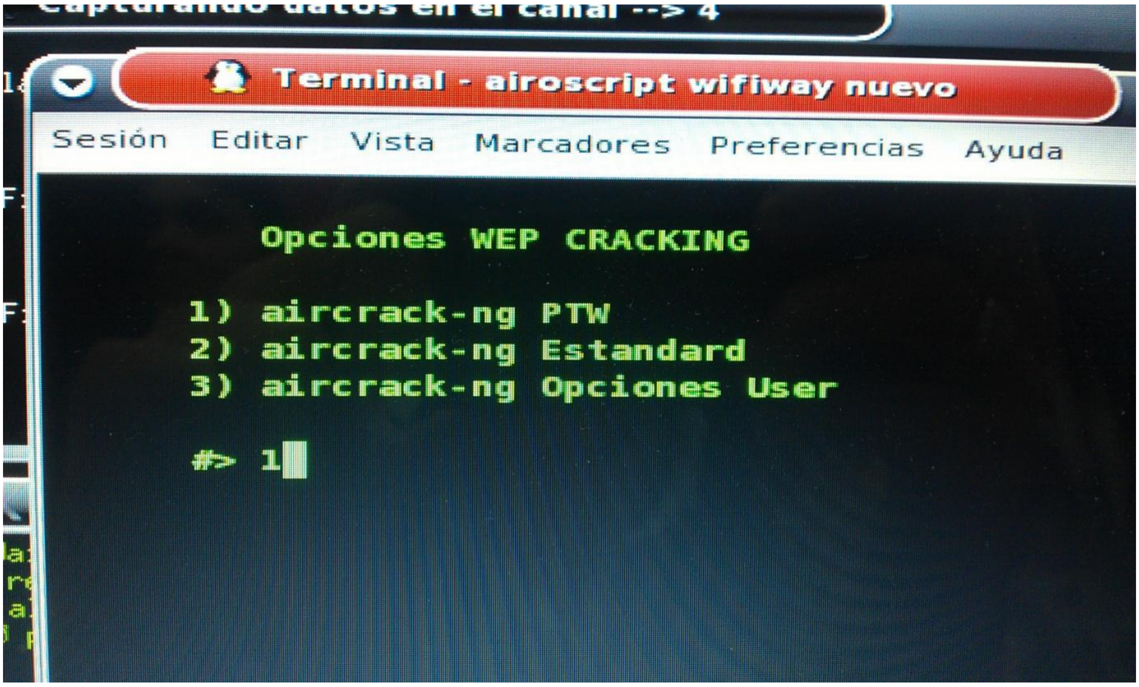
```
09:52:22  Waiting for beacon frame (BSSID: 00:1C:10:2F:E5:73) on channel 4
Saving ARP requests in replay_arp-0119-095222.cap
You should also start airodump-ng to capture replies.
Read 830 packets (got 0 ARP requests and 102 ACKs), sent 0 packets...(0 pps)
```

```
09:52:22  Waiting for beacon frame (BSSID: 00:1C:10:2F:E5:73) on channel 4

09:52:22  Sending Authentication Request (Open System) [ACK]
09:52:22  Authentication successful
09:52:22  Sending Association Request [ACK]
09:52:22  Association successful :-) (AID: 1)

09:52:23  Sending keep-alive packet [ACK]
09:52:24  Sending keep-alive packet [ACK]
09:52:25  Sending keep-alive packet [ACK]
09:52:26  Sending keep-alive packet [ACK]
09:52:27  Sending Authentication Request (Open System) [ACK]
09:52:27  Authentication successful
09:52:27  Sending Association Request [ACK]
09:52:27  Association successful :-) (AID: 1)

09:52:28  Sending keep-alive packet [ACK]
09:52:29  Sending keep-alive packet [ACK]
09:52:30  Sending keep-alive packet [ACK]
```

Ahora le damos a opción 4, Crackear



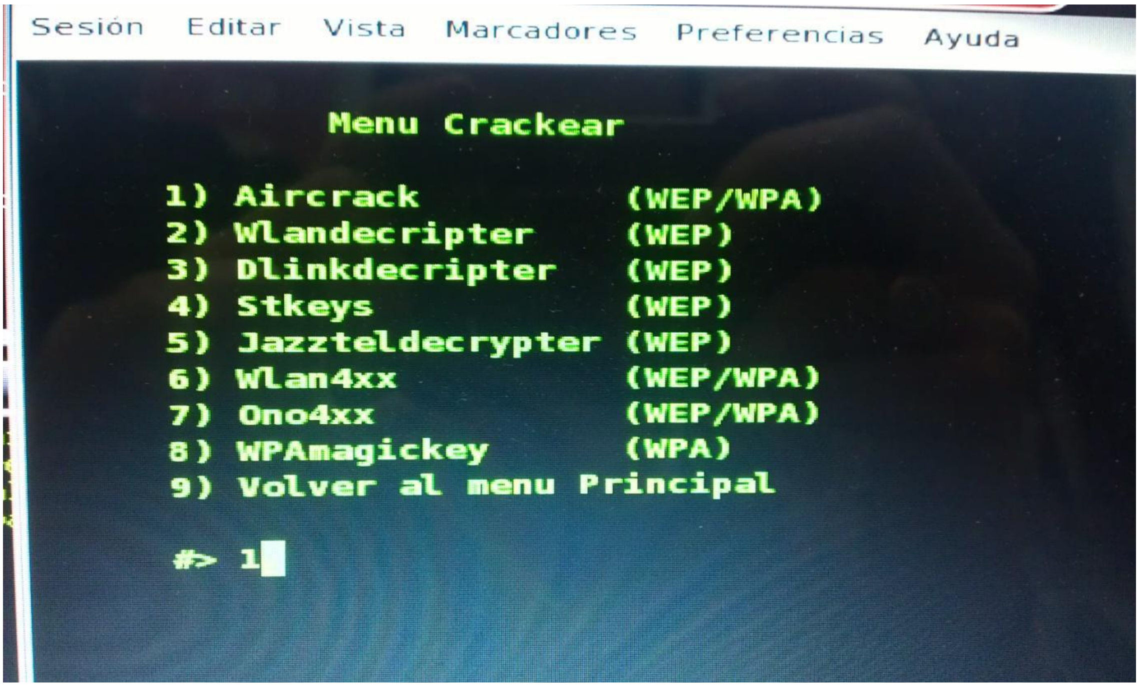
```
INFO AP OBJETIVO

                    SSID = VACACIONES / WEP
                   Canal = 4
               Velocidad = 54 Mbps
              MAC del AP = 00:1C:10:2F:E5:73
          MAC de cliente =

MENU PRINCIPAL

     1) Escanear                 -Buscar Objetivos
     2) Seleccionar              -Seleccionar Objetivo
     3) Ataques                  -Atacar Objetivo
     4) Crackear                 -Menu Crackear
     5) Auto                     -Buscar Key Automaticamente
     6) Autenticar               -Cliente Falso en Objetivo
     7) Desautenticar            -Desautenticar del Objetivo
     8) Inyección                -Menu de Inyección
     9) Opciones Avanzadas       -Utilidades Varias
    10) Salir                    -Cerrar Airoscript

      #> 4
```



Terminal - airoscript wifiway nuevo

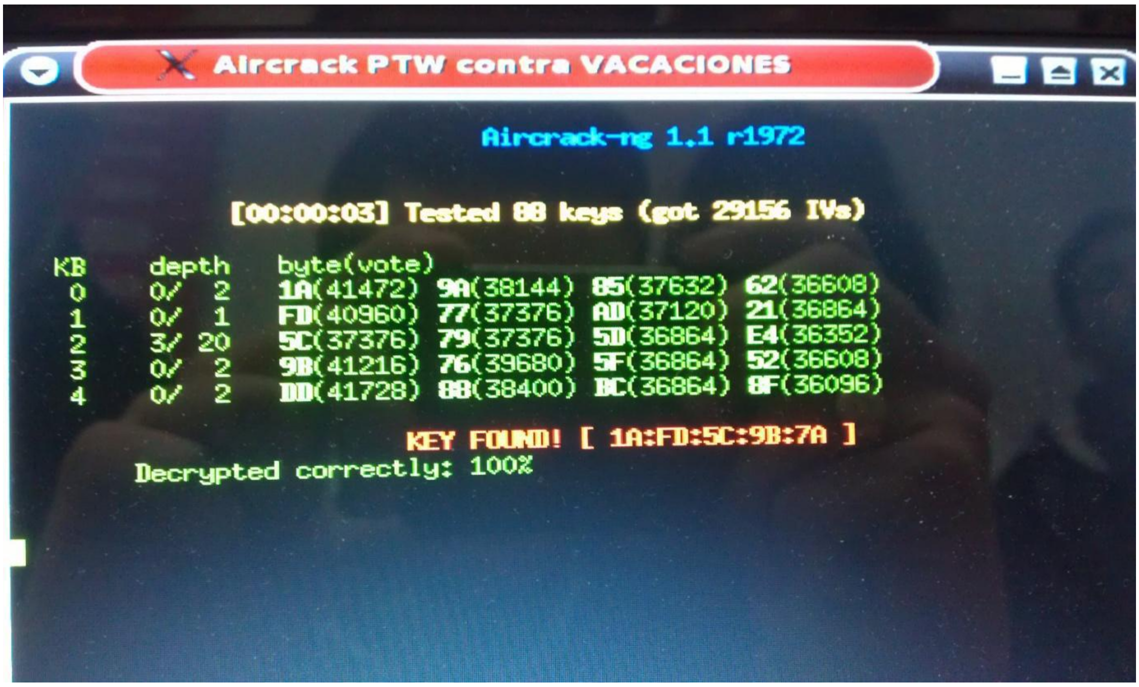
```
     Opciones WEP CRACKING

  1) aircrack-ng PTW
  2) aircrack-ng Estandard
  3) aircrack-ng Opciones User

  #> 1
```

Ahora opción 1, para que elija Aircrack



```
              Menu Crackear

      1) Aircrack           (WEP/WPA)
      2) Wlandecripter      (WEP)
      3) Dlinkdecripter     (WEP)
      4) Stkeys             (WEP)
      5) Jazzteldecrypter   (WEP)
      6) Wlan4xx            (WEP/WPA)
      7) Ono4xx             (WEP/WPA)
      8) WPAmagickey        (WPA)
      9) Volver al menu Principal

      #> 1
```

Y ya nos ha encontrado la contraseña



```
                              Aircrack-ng 1.1 r1972


                 [00:00:03] Tested 88 keys (got 29156 IVs)

KB    depth   byte(vote)
 0    0/  2   1A(41472) 9A(38144) 85(37632) 62(36608)
 1    0/  1   FD(40960) 77(37376) AD(37120) 21(36864)
 2    3/ 20   5C(37376) 79(37376) 5D(36864) E4(36352)
 3    0/  2   9B(41216) 76(39680) 5F(36864) 52(36608)
 4    0/  2   DD(41728) 88(38400) BC(36864) 8F(36096)

                         KEY FOUND! [ 1A:FD:5C:9B:7A ]
     Decrypted correctly: 100%
```