Descriu les tècniques d'encriptació de les xarxes sense fils i els seus punts vulnerables

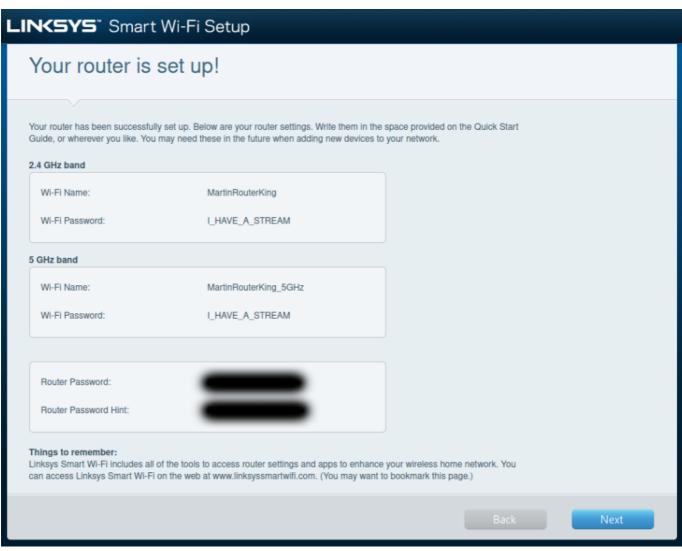
Índex

- Configuració Router
- Executa una instrucció i envia el resultat d'aquesta a una altre instrucció.
- Configura el router per tal que faci servir un passsword tipus WEP.
- Configura el router per tal que faci servir un password tipus WPA.
- Configura el router per tal que faci servir un password tipus WPA2.
- Configura la targeta wifi per tal que estigui en mode monitor.

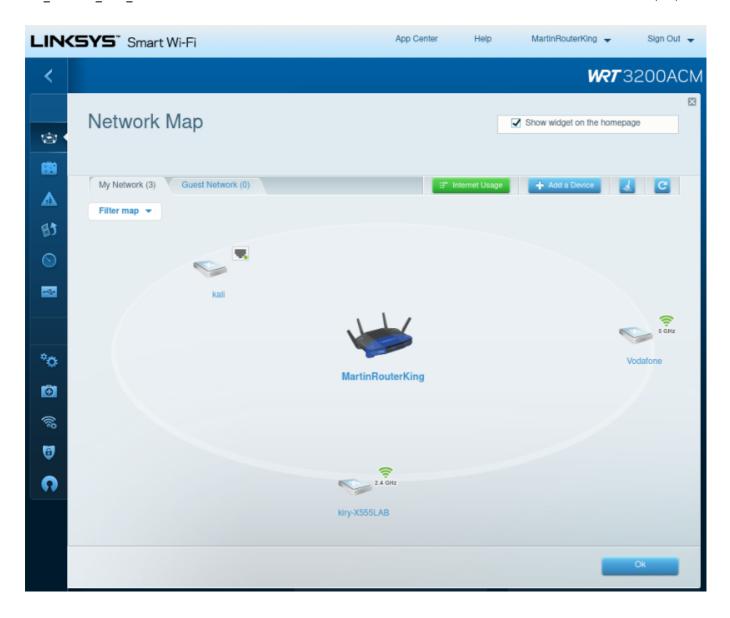
Configuració Router



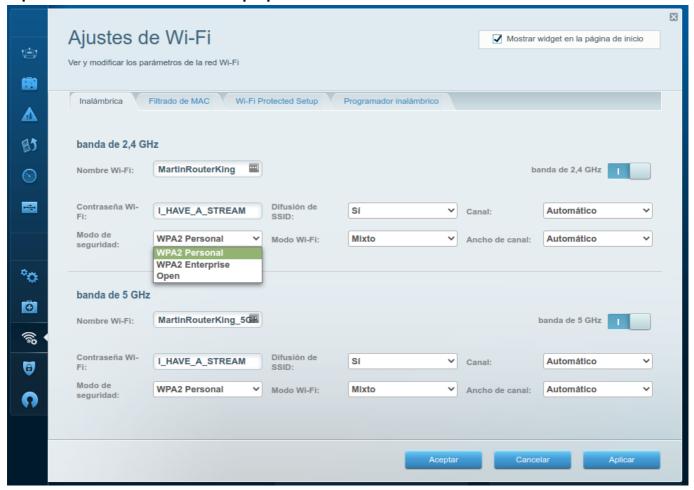








Aquests són els sistemes de xifrat que permet utilitzar el router



Segons la pàgina del fabricant sobre aquest model:

WPA2 Personal, WPA2 Enterprise

Tecnología Wi-Fi:

Gigabit de doble banda MU-MIMO AC1900, 600 + +2600 Mbps

Funciones destacadas:

- 802.11b
- 0 802.11
- o 802.11g
- o 802.11n
- o 802.11ac

Velocidad Wi-Fi:

AC3200 (N600 + AC2600)

Bandas Wi-Fi:

2,4 y 5 GHz (doble banda simultánea)

Alcance Wi-Fi:

Casas muy grandes

Número de puertos Ethernet:

- o 1 puerto WAN Gigabit
- o 4 puertos LAN Gigabit

Otros puertos:

- o Un (1) puerto USB 3.0
- o Un (1) puerto combinado eSATA/USB 2.0
- Encendido

Antenas:

4 antenas de doble banda externas y extraíbles

Procesador:

1,8 GHz de doble núcleo

Indicadores LED:

Alimentación Internet, 2.4 GHz, 5 GHz, eSATA, USB1 (USB 2.0), USB2 (USB 3.0), LAN 1-4 (actividad/10/100 Mbps), LAN 1-4 (1

Gbps), WPS

Encriptación inalámbrica:

WPA2 Personal, WPA2 Enterprise

Compatibilidad con redes VPN:

- o PPTP
- o IPSec pass-through

Sistemas operativos certificados:

MacOS (10.X o superior), Windows 7, Windows 8.1 (funciona con

Windows 10)

Requisitos mínimos del sistema:

- Internet Explorer® 8
- o Safari® 5 (para Mac®)
- Firefox® 8
- Google Chrome™

Dimensiones (L x A x A):

245,87 x 193,80 x 51,82 mm sin antenas

Peso:

798,32 g

Temperatura de funcionamiento:

Entre 0 v 40 °C

Temperatura de almacenamiento:

Entre -20 y 60 °C

Humedad de funcionamiento:

Entre 10 y 80 % sin condensación

Funciones de seguridad:

- WPA/WPA2
- Encriptación del vínculo mediante AES de 128 bits

Conformidad con las normativas:

FCC clase B

Otras certificaciones:

Certificación DFS de FCC

Información adicional:

Compatible con software de código abierto para OpenWRT y DD-

WRT

Fuente de alimentación:

Entrada de corriente: 100-240 V ~ 50-60 Hz; Salida de corriente: 12

V/3,0 A

https://www.linksys.com/es/wireless-routers/wrt-wireless-routers/linksys-wrt3200acm-ac3200-mu-mimogigabit-wifi-router/p/p-wrt3200acm/

Executa una instrucció i envia el resultat d'aquesta a una altre instrucció.

Llistar els fitxers i directoris i els ordenem aleatòriament.

```
ls -1 | sort -R
```

Per l'anterior pràctica també vam fer alguns exemples com el següent, que llista les interfícies de xarxa i es filtra la sortida amb *awk*:

```
ip -o link show | awk -F': ' '{print $2}'
```

Configura el router per tal que faci servir un passsword tipus WEP.

El sistema de xifrat WEP (Wired Equivalent Privacy) ja està obsolet perquè és fàcil de desxifrar. Per tant, aquest router no es pot configurar per fer servir aquest tipus d'encriptació. Dels xifrats que es demanen en aquesta pràctica, és el més dèbil.

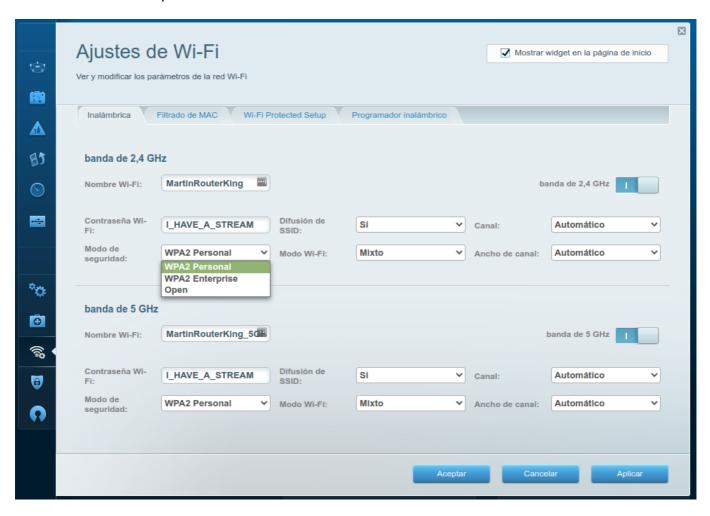
En resum, no és segur fer-ho servir.

Configura el router per tal que faci servir un password tipus WPA.

Igual que passa amb el WEP, aquest router tampoc ens permet configurar un password amb WPA, ja que es considera dèbil i ja es pot desxifrar sense gaire dificultat. Tot i que és més segur que el WEP, no és suficient.

Configura el router per tal que faci servir un password tipus WPA2.

Per defecte ja tenim configurat el password amb WPA2, perquè només ens permet configurar una WPA2 Personal o WPA2 Enterprise.



Segons https://www.tp-link.com/es/support/faq/500/:

WPA-Personal (WPA-PSK): Aquest mode és adequat per a les xarxes domèstiques. Els usuaris que es connecten a la xarax ho fan a partir d'una contrasenya o punt d'accés (AP).

WPA-Enterprise (WPA-802.1x, RADIUS): Aquest mode està més pensat per a les xarxes sense fil en entorns no domèstics. Ofereix un control individual pels usuaris que es connecten. Quan els usuaris intenten connectar-se a la xarxa, ho han de fer amb unes credencials de sessió.

Configura la targeta wifi per tal que estigui en mode monitor.

Per l'anterior pràctica ja vaig configurar la targeta per treballar en mode monitor.

Fem una prova amb aircrak-ng per monitorar:

sudo airmon-ng start wlp14s0

```
.ssh sudo airmon-ng start wlp14s0
Found 4 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode
     PID Name
     806 avahi-daemon
     812 NetworkManager
     850 wpa supplicant
     872 avahi-daemon
PHY
           Interface
                                 Driver
                                                       Chipset
phy0
           wlp14s0
                                 ath9k
                                                       Qualcomm Atheros AR9462 Wireless Network Adapter (rev 01)
                      (mac80211 monitor mode vif enabled for [phy0]wlp14s0 on [phy0]wlp14s0mon)
                      (mac80211 station mode vif disabled for [phy0]wlp14s0)
```

sudo airmon-ng check kill
sudo airodump-ng wlp14s0mon

CH 11][Elapsed: 18 s][2021-11-11 19:57										
BSSID	PWR	Beacons	#Data,	#/s	СН	МВ	ENC (CIPHER	AUTH	ESSID
00:0C:E6:10:13:05	-1	Θ	0	Θ	11	-1				<length: 0=""></length:>
1C:28:AF:C3:21:E0	-54	39	0	0	1	130	WPA2	CCMP	MGT	eduroam
00:0C:E6:10:01:03	-43	14	0	0	11	54e.	WPA	TKIP	PSK	alumnesBAT
E8:9F:80:1C:3A:19	-41	48	10	0	11	540	WPA2	CCMP	PSK	Linksys02848
00:0C:E6:10:01:00	-48	13	6	0	11	54e.	WPA2	CCMP	PSK	educat1x1
00:0C:E6:10:01:05	-51	13	9	0	11	54e.	WPA	TKIP	PSK	alumnesCF
00:0C:E6:10:03:03	-39	14	0	0	11	54e.	WPA	TKIP	PSK	alumnesBAT
1C:28:AF:C1:D3:04	-48	13	0	0	1	130	OPN			gencat_ENS_EDU_PORTAL
00:0C:E6:10:03:00	-42	14	0	0	11	54e.	WPA2	CCMP	PSK	educat1x1
00:0C:E6:10:03:01	-53	15	0	0	11	54e.	WPA	TKIP	PSK	docent
1C:28:AF:C1:D3:02	-47	14	0	0	1	130	WPA2	CCMP	MGT	gencat_ENS_EDU
1C:28:AF:C3:21:E1	-50	13	0	0	1	130	WPA2	CCMP	MGT	<length: 0=""></length:>
1C:28:AF:C1:D3:01	-49	14	0	0	1	130	WPA2	CCMP	MGT	<length: 0=""></length:>
1C:28:AF:C3:21:E4	-51	13	0	0	1	130	OPN			gencat_ENS_EDU_PORTAL
00:0C:E6:10:01:01	-42	12	0	0	11	54e.	WPA	TKIP	PSK	docent
1C:28:AF:C3:21:E2	-51	13	0	0	1	130	WPA2	CCMP	MGT	gencat_ENS_EDU
E8:9F:80:1C:35:61	-52	56	19	0	6	540	WPA2	CCMP	PSK	MosEisley
00:0C:E6:10:07:05	-63	13	19	0	11	54e.	WPA	TKIP	PSK	alumnesCF
00:0C:E6:10:07:00	-56	14	0	0	11	54e.	WPA2	CCMP	PSK	educat1x1
00:0C:E6:10:03:05	-44	14	0	0	11	54e.	WPA	TKIP	PSK	alumnesCF