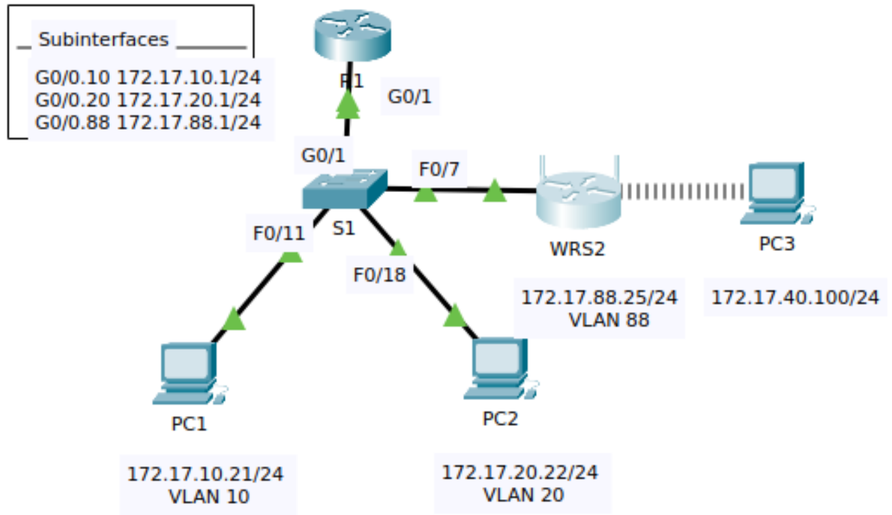
KEY PRACTICAL PRECAUTIONS FOR YOUR HOME WI-FI ROUTER

Yash N B002
Saakshi Jain B033
Anika Mayekar B040

WI-FI ROUTER

A Wi-Fi router is a networking device that connects to the internet and allows multiple devices, such as smartphones, computers, and smart home gadgets, to access and communicate over a wireless local network.

A Wi-Fi router links to the internet, permitting numerous devices like phones and computers to connect and communicate through a wireless local network



SECURING YOUR WI-FI ROUTER: PROTECTING AGAINST HACKERS AND DATA BREACHES

Weak Password and Default Passwords:

Open Networks: Leaving your Wi-Fi network open (without encryption) can allow anyone in the vicinity to connect. Always use WPA2 or WPA3 encryption for your network.

Guest Network Security: If you have a guest network, make sure it's isolated from your main network to prevent unauthorized access to your sensitive data.

Disabled Two-Factor Authentication (2FA): If your router supports 2FA, enable it for an extra layer of security.

ENHANCING WI-FI NETWORK SECURITY

Perimeter - Signal Strength:

Change your network's SSID to a unique name and set a strong, non-predictable password to enhance Wi-Fi security.

Password or Key-Based Security:
When securing a network or system, you have the option to use either passwords or key-based authentication.

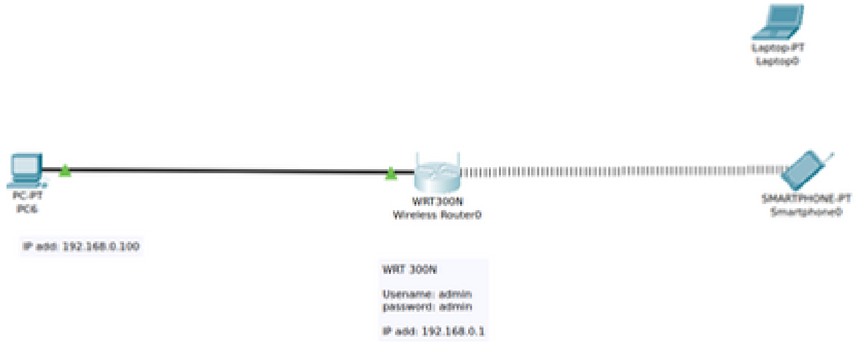
Encryption Key Strength:
The strength of an encryption key is crucial for data security

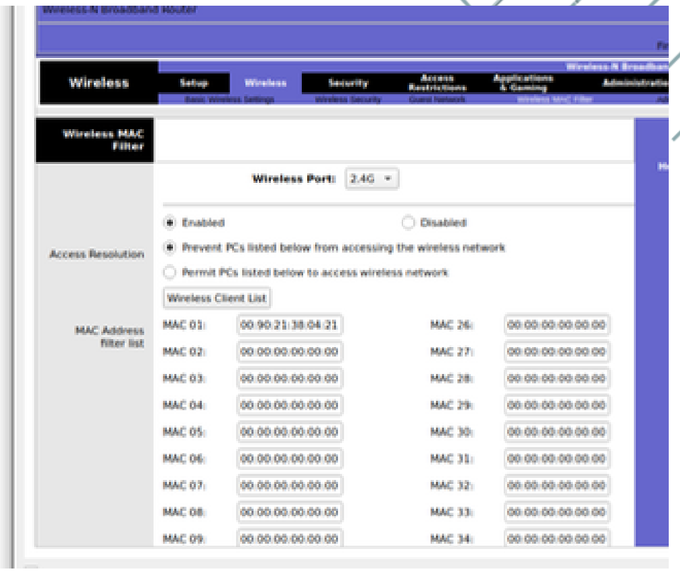
Encryption Key Strength:
The strength of an encryption key is crucial for data security

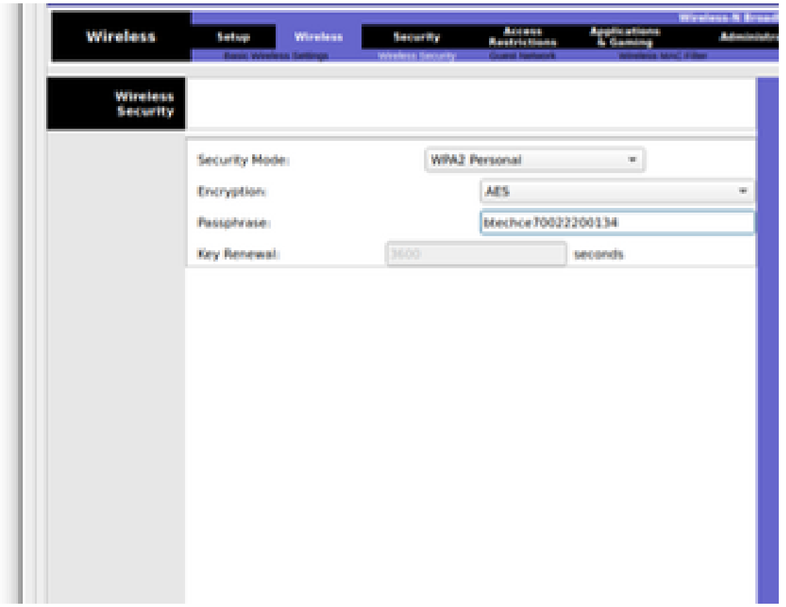
ENHANCING WI-FI NETWORK SECURITY

MAC Address Matching:

MAC addresses are unique identifiers assigned to network devices.

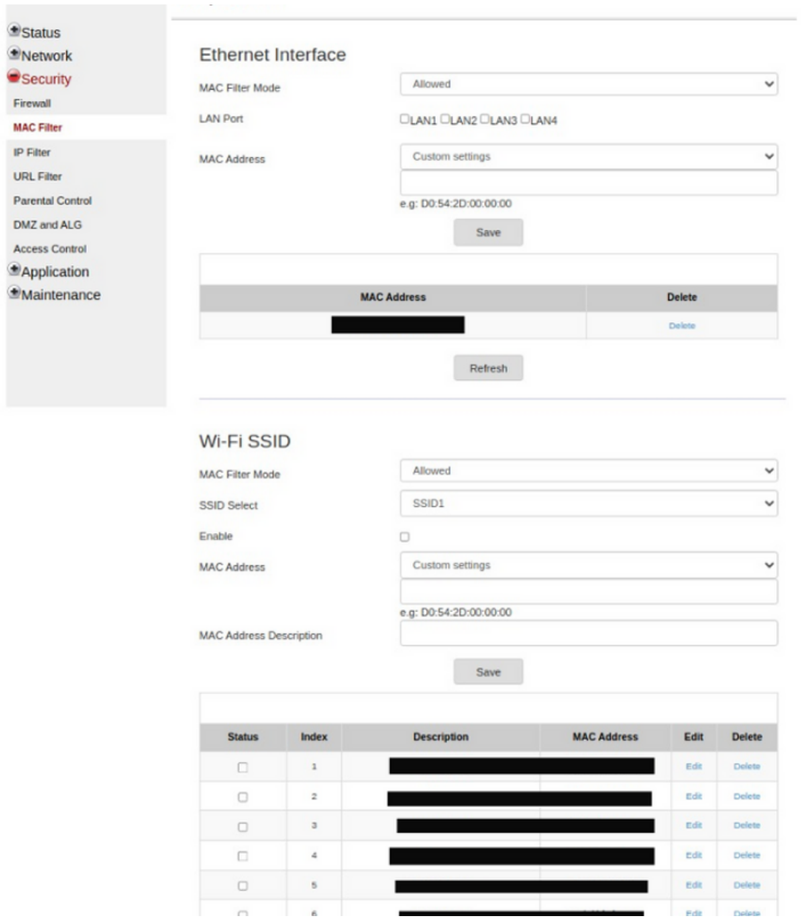


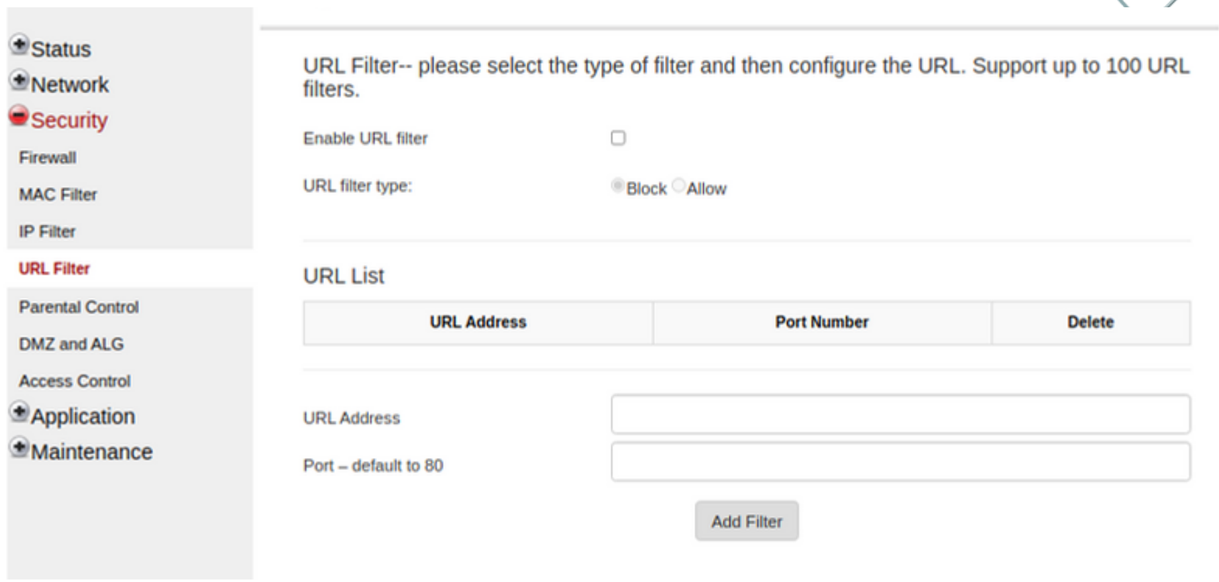


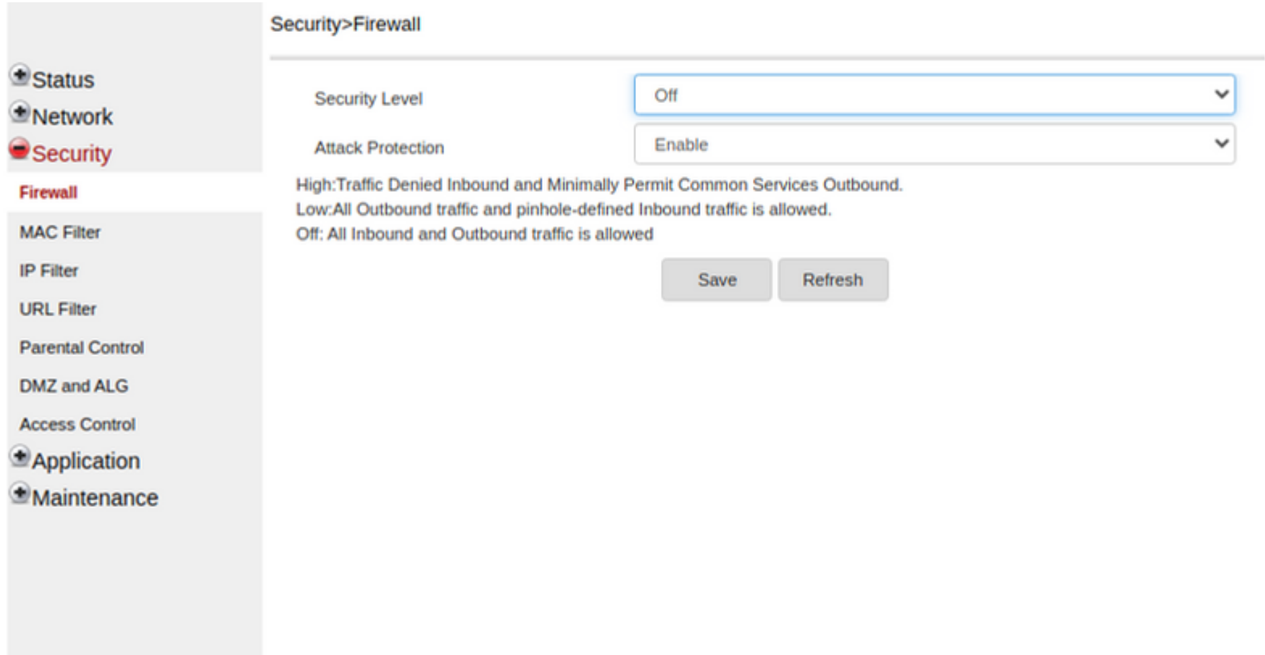


ENHANCING WI-FI NETWORK SECURITY

MAC Address Matching:

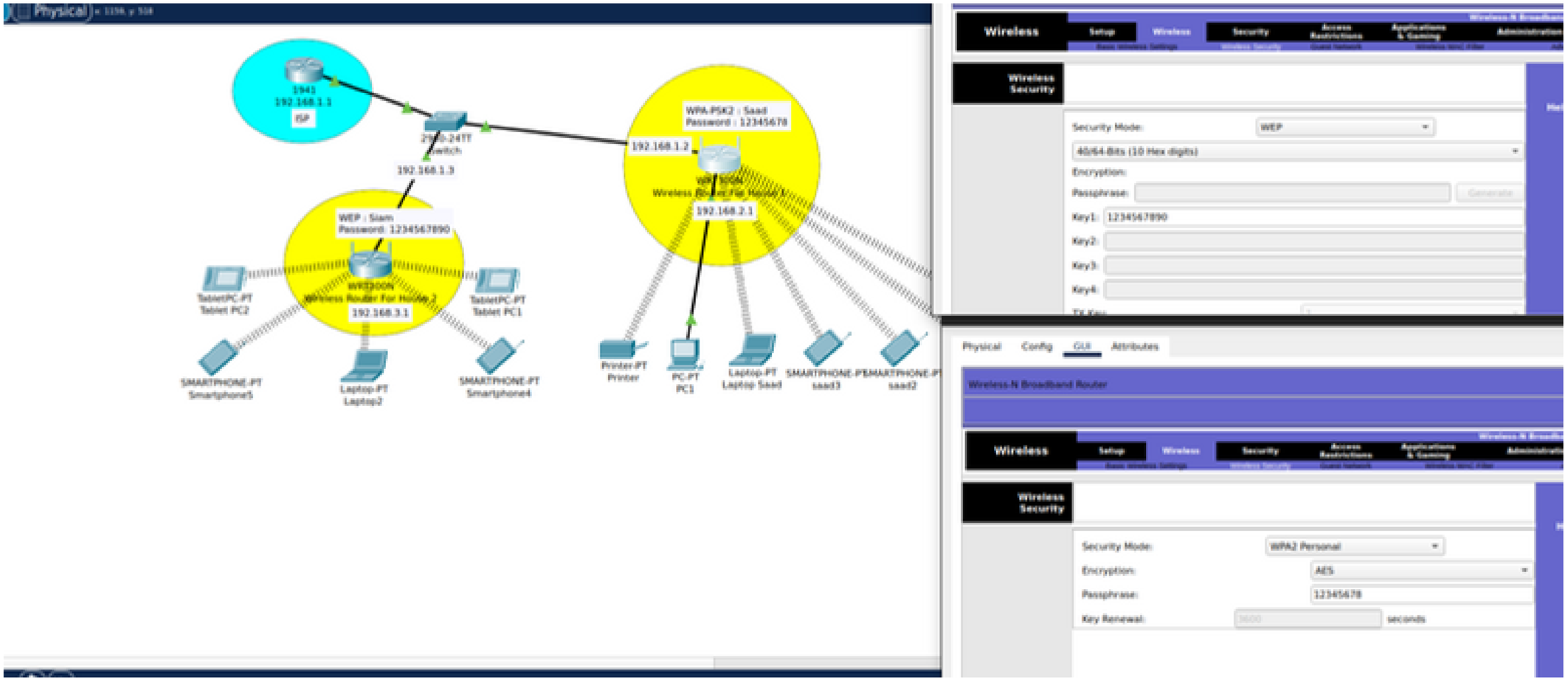






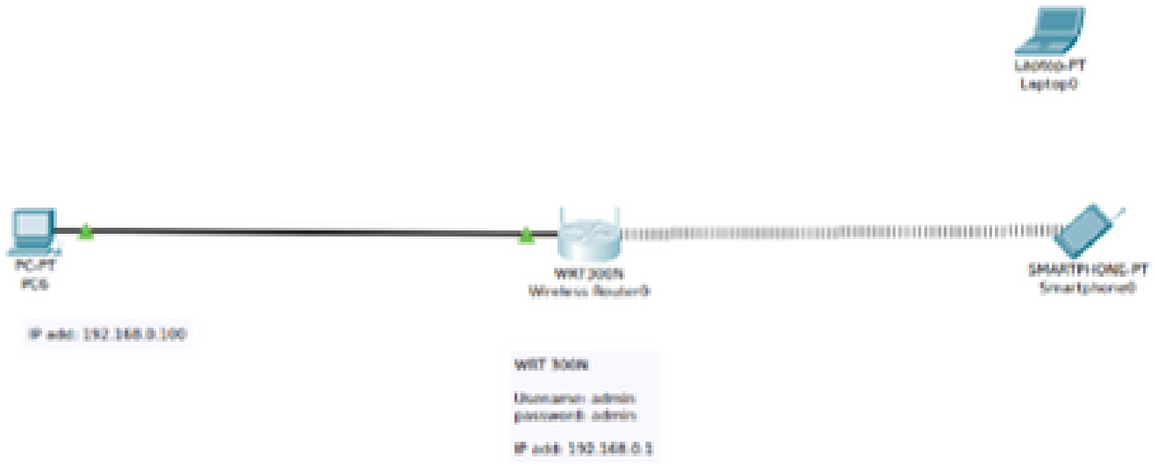
ENHANCING WI-FI NETWORK SECURITY

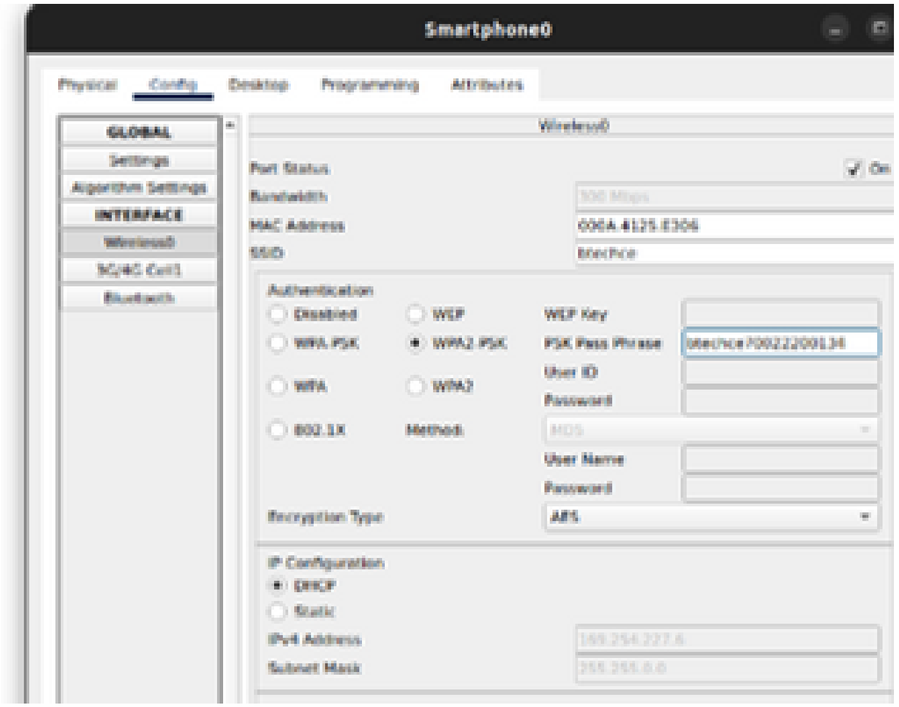
Enable WPA3 or WPA2 Encryption:



ENHANCING WI-FI NETWORK SECURITY

Enable WPA3 or WPA2 Encryption:





WIFI (WIRELESS) ENCRYPTION STANDARD

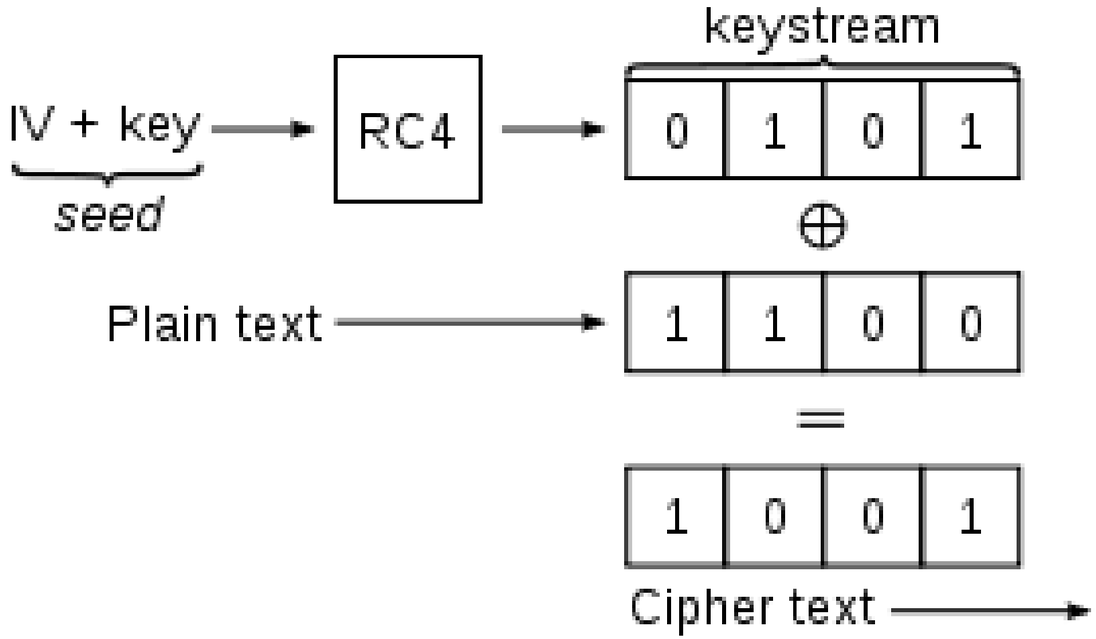
WIRED EQUIVALENT PRIVACY (WEP)

Developed in 1999.

Earliest wireless security protocol.

40 bit encryption key

Easily Hackable



Weak security
Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plaintext, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related-key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5,000 packets.

Standard 64-bit WEP uses a 40-bit key (also known as WEP-40), which is concatenated with a 24-bit initialization vector (IV) to form the RC4 key

stream cipher RC4

24-bit initialization vector (IV)

WIFI (WIRELESS) ENCRYPTION STANDARD

WI-FI PROTECTED ACCESS (WPA)

Developed in 2003. Stronger Encryption and Uses Temporal Key Integrity Protocol (TKIP)

TKIP employs a per-packet key

it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP

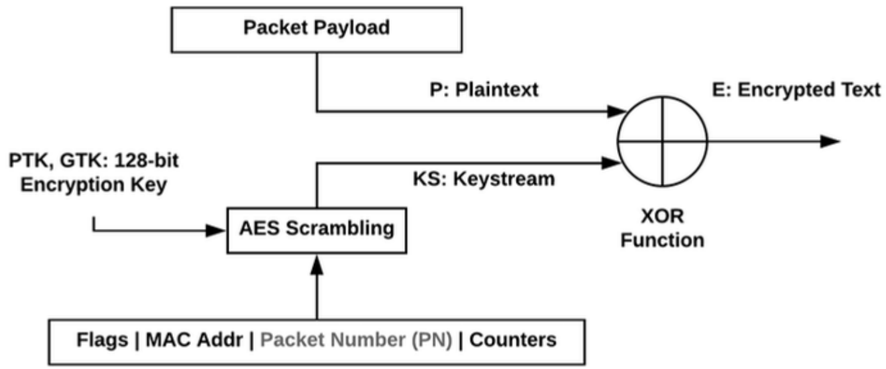
TKIP also includes a message integrity check (MIC) to ensure that the data has not been tampered with. TKIP is designed to be compatible with legacy hardware and software that does not support AES.

WIFI (WIRELESS) ENCRYPTION STANDARD

WI-FI PROTECTED ACCESS 2 (WPA2)

It introduced the Advanced Encryption System (AES) to replace the more vulnerable TKIP system used in the original WPA protocol. Used by the US government to protect classified data, AES provides strong encryption.

It ensures that data sent or received over your wireless network is encrypted, and only people with your network password have access to it.

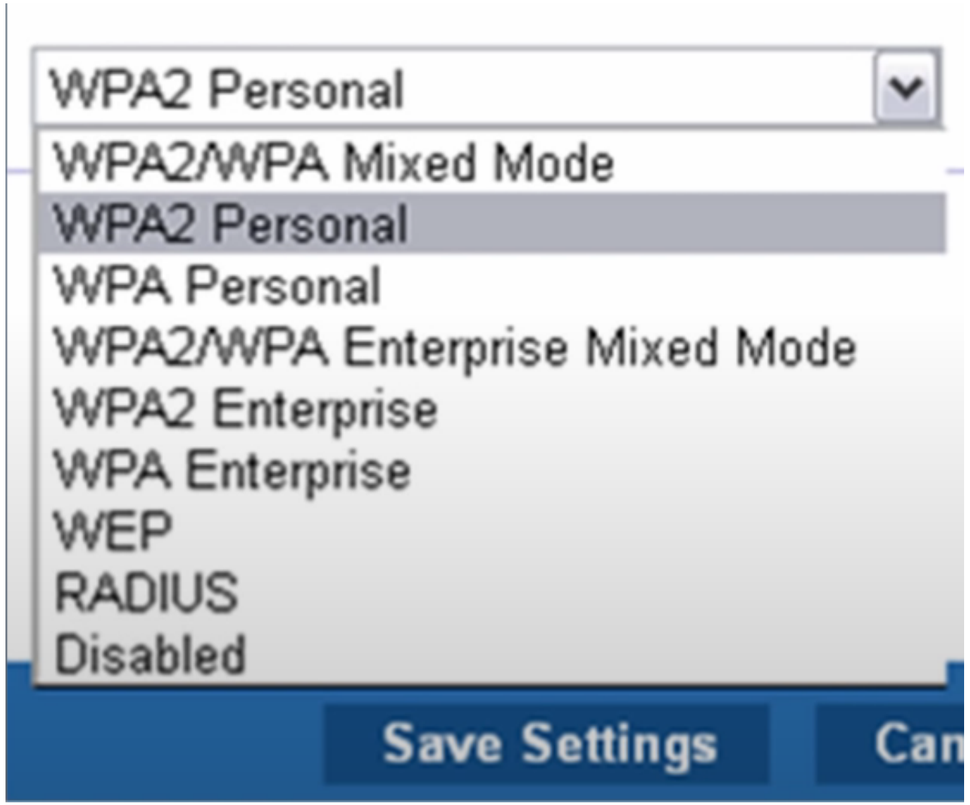


WIFI (WIRELESS) PASSWORD SECURITY

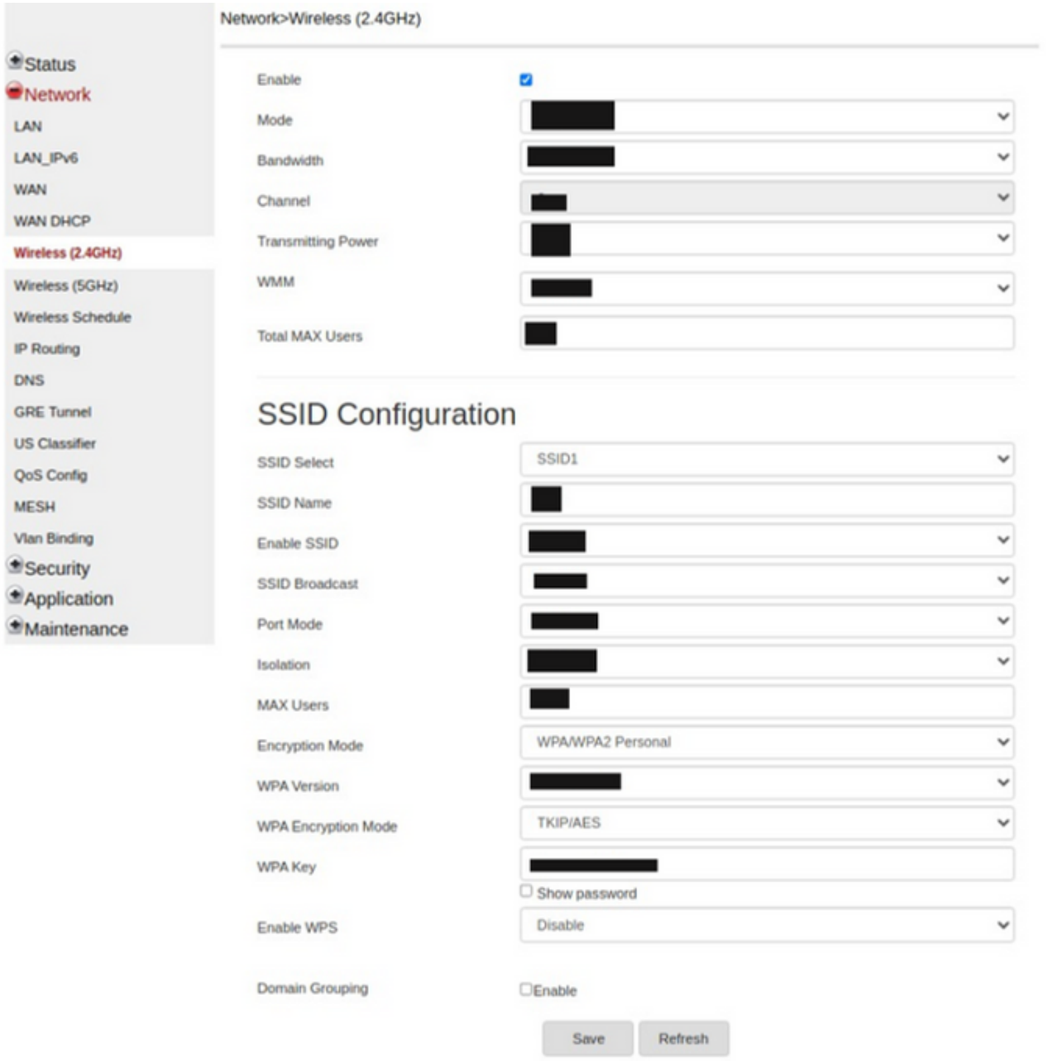
WI-FI PROTECTED ACCESS 2 (WPA2)

WPA2 offers two modes of operation:
WPA2-Personal uses a pre-shared key (PSK) for authentication, typically a passphrase known to authorized users. This mode is suitable for home networks and small businesses.

WPA2-Enterprise requires a RADIUS (Remote Authentication Dial-In User Service) server for authentication, making it suitable for larger organizations with more complex authentication needs.



WIFI (WIRELESS) PASSWORD SECURITY



SOME OTHER PRACTICAL MEASURES

Regular Password Updates: Change your Wi-Fi network password regularly, and consider using a password manager to generate and store complex passwords

Network Monitoring: Consider using network monitoring tools to keep an eye on network traffic and detect any unusual or unauthorized activity.

Strong, Unique Router Login: Your router's admin panel should have a strong, unique password that's separate from your Wi-Fi password.

Thank You!