



KEY PRACTICAL PRECAUTIONS FOR YOUR HOME WI-FI ROUTER

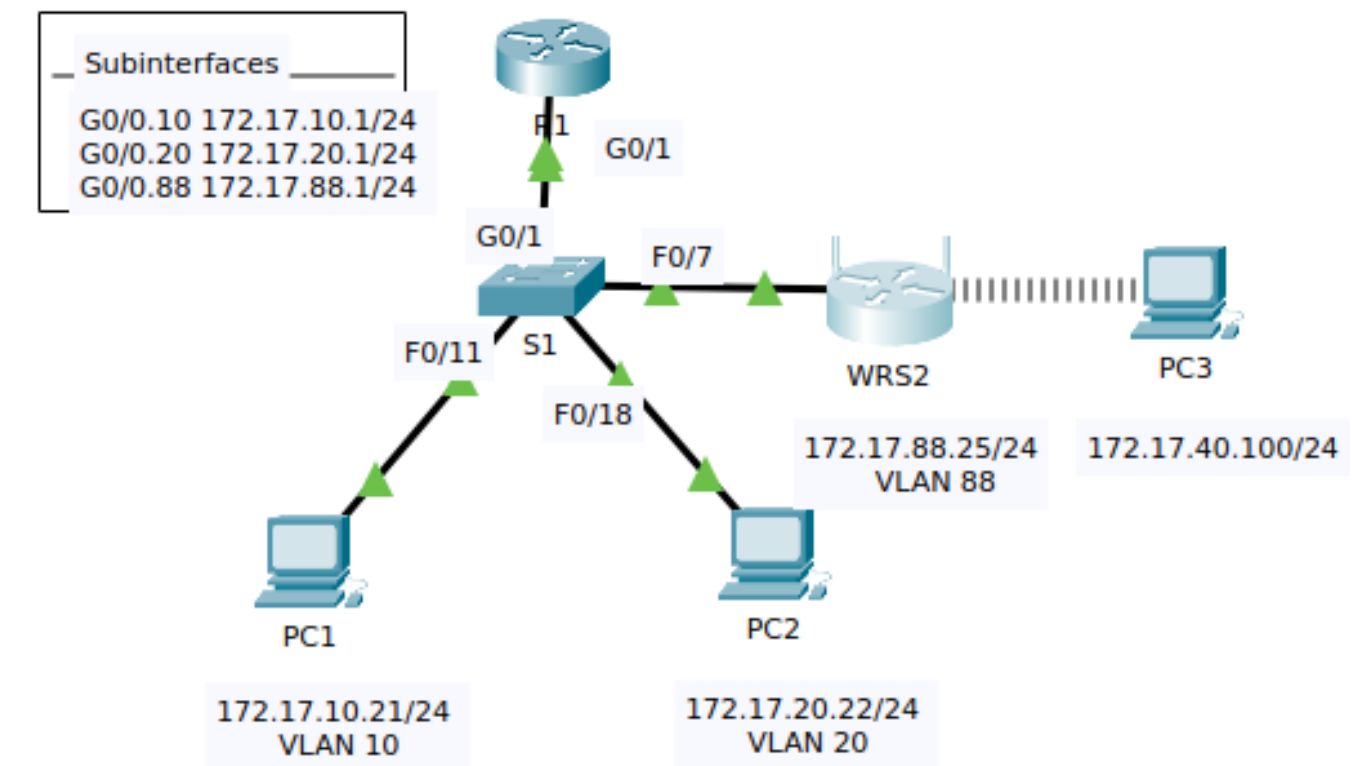
Yash N B002
Saakshi Jain B033
Anika Mayekar B040



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

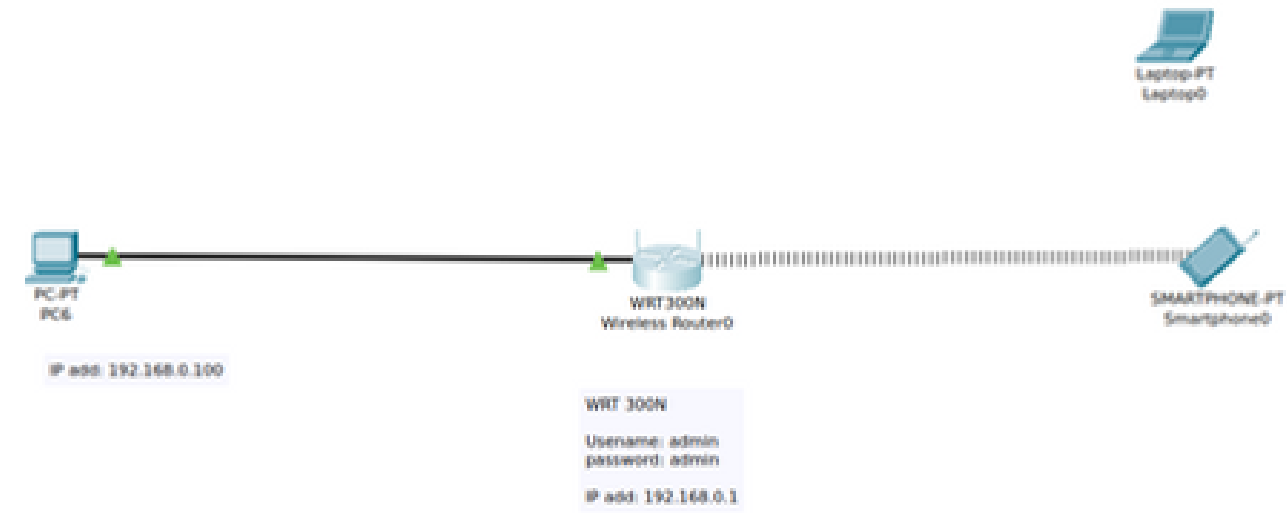
Encryption Key Strength:

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.



Wireless N Broadband Router

Wireless

Setup Wireless Security Access Restrictions Applications & Gaming Administration

Basic Wireless Settings Wireless Security Guest Network Wireless MAC Filter

Wireless MAC Filter

Wireless Port: 2.4G

☒ Enabled ☐ Disabled

☒ Prevent PCs listed below from accessing the wireless network ☐ Permit PCs listed below to access wireless network

Wireless Client List

MAC 01:	00:90:21:38:04:21	MAC 26:	00:00:00:00:00:00
MAC 02:	00:00:00:00:00:00	MAC 27:	00:00:00:00:00:00
MAC 03:	00:00:00:00:00:00	MAC 28:	00:00:00:00:00:00
MAC 04:	00:00:00:00:00:00	MAC 29:	00:00:00:00:00:00
MAC 05:	00:00:00:00:00:00	MAC 30:	00:00:00:00:00:00
MAC 06:	00:00:00:00:00:00	MAC 31:	00:00:00:00:00:00
MAC 07:	00:00:00:00:00:00	MAC 32:	00:00:00:00:00:00
MAC 08:	00:00:00:00:00:00	MAC 33:	00:00:00:00:00:00
MAC 09:	00:00:00:00:00:00	MAC 34:	00:00:00:00:00:00



Wireless

Setup Wireless Security Access Restrictions Applications & Gaming Administration

Basic Wireless Settings Wireless Security Guest Network Wireless MAC Filter

Wireless Security

Security Mode: WPA2 Personal

Encryption: AES

Passphrase: Mechoe70022200134

Key Renewal: 3600 seconds

ENHANCING WI-FI NETWORK SECURITY

MAC Address Matching:

Status

Network

Security

Firewall

MAC Filter

IP Filter

URL Filter

Parental Control

DMZ and ALG

Access Control

Application

Maintenance

Ethernet Interface

MAC Filter Mode

Allowed

LAN Port

☐ LAN1 ☐ LAN2 ☐ LAN3 ☐ LAN4

MAC Address

Custom settings

e.g: D0:54:2D:00:00:00

Save

MAC Address	Delete
	Delete

Refresh

Wi-Fi SSID

MAC Filter Mode

Allowed

SSID Select

SSID1

Enable

☐

MAC Address

Custom settings

e.g: D0:54:2D:00:00:00

Save

Status	Index	Description	MAC Address	Edit	Delete
<input type="checkbox"/>	1			Edit	Delete
<input type="checkbox"/>	2			Edit	Delete
<input type="checkbox"/>	3			Edit	Delete
<input type="checkbox"/>	4			Edit	Delete
<input type="checkbox"/>	5			Edit	Delete
<input type="checkbox"/>	6			Edit	Delete

Status

Network

Security

Firewall

MAC Filter

IP Filter

URL Filter

Parental Control

DMZ and ALG

Access Control

Application

Maintenance

URL Filter-- please select the type of filter and then configure the URL. Support up to 100 URL filters.

Enable URL filter

☐

URL filter type:

☒ Block ☐ Allow

URL List

URL Address	Port Number	Delete
URL Address		
Port – default to 80		

Add Filter

Status

Network

Security

Firewall

MAC Filter

IP Filter

URL Filter

Parental Control

DMZ and ALG

Access Control

Application

Maintenance

Security>Firewall

Security Level

Off

Attack Protection

Enable

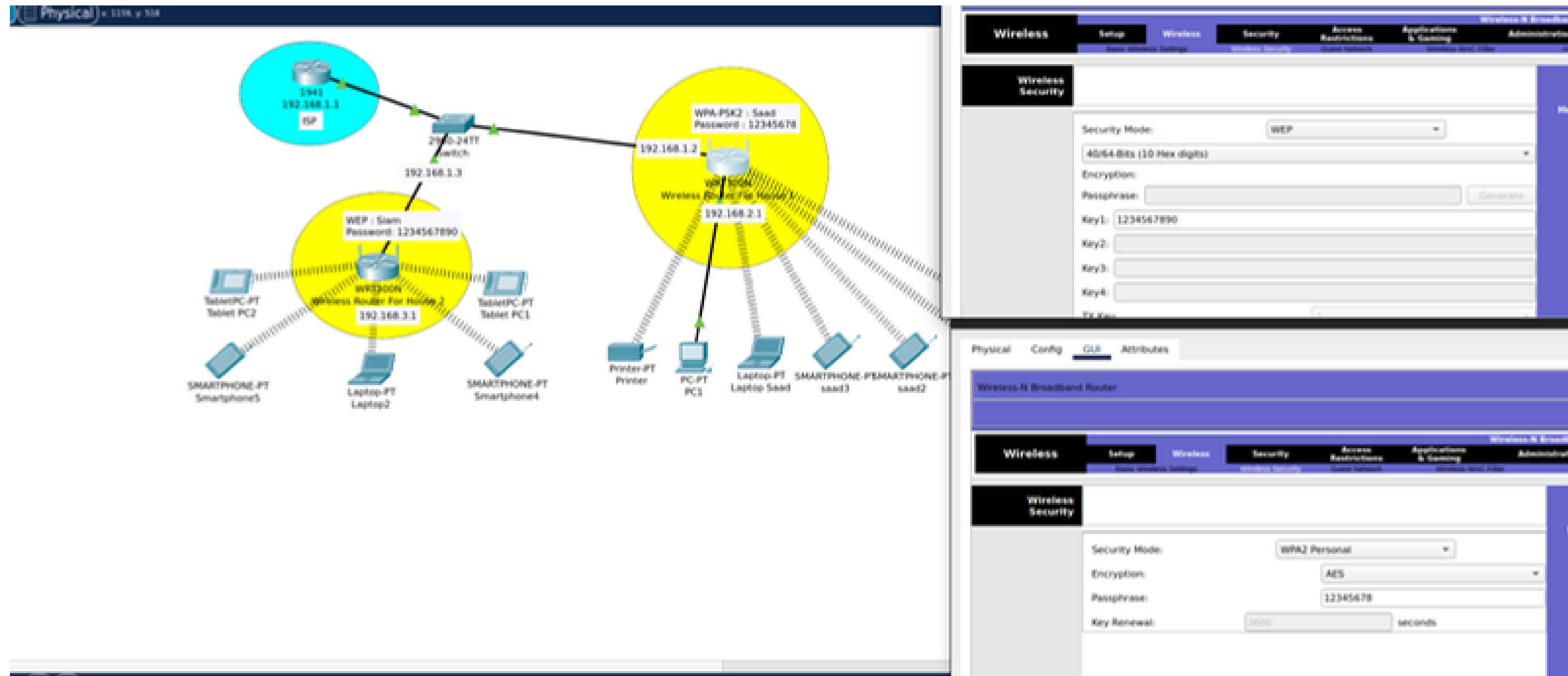
High:Traffic Denied Inbound and Minimally Permit Common Services Outbound.
Low:All Outbound traffic and pinhole-defined Inbound traffic is allowed.
Off: All Inbound and Outbound traffic is allowed

Save

Refresh

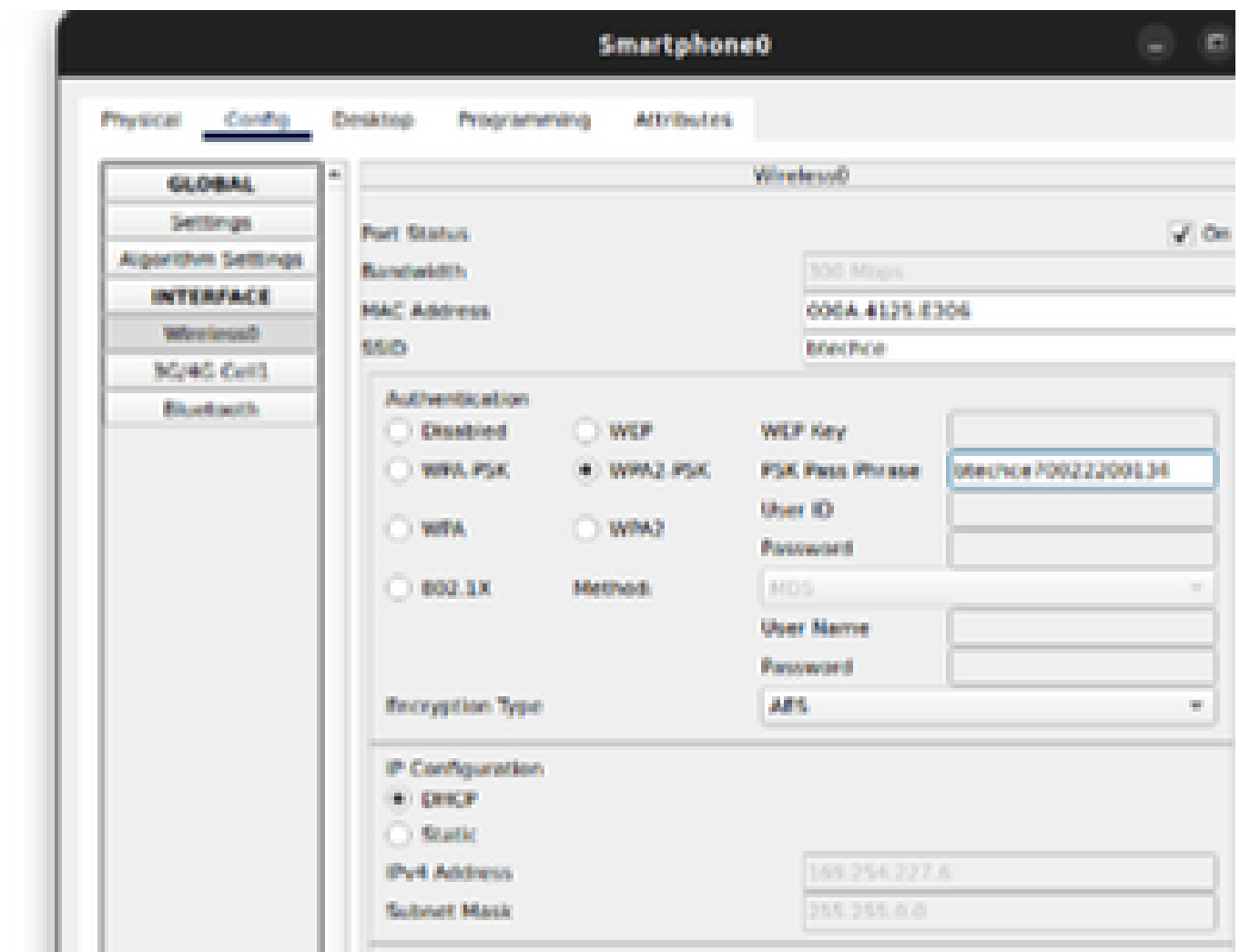
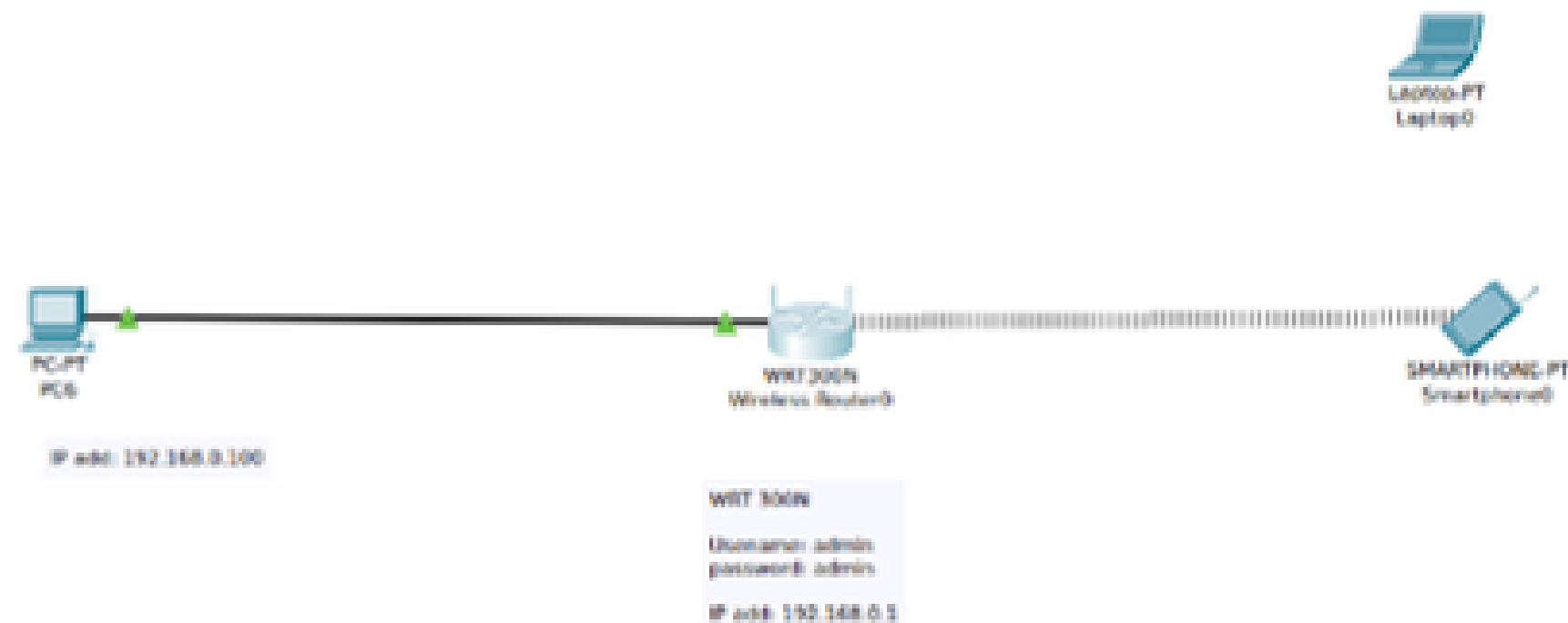
ENHANCING WI-FI NETWORK SECURITY

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.

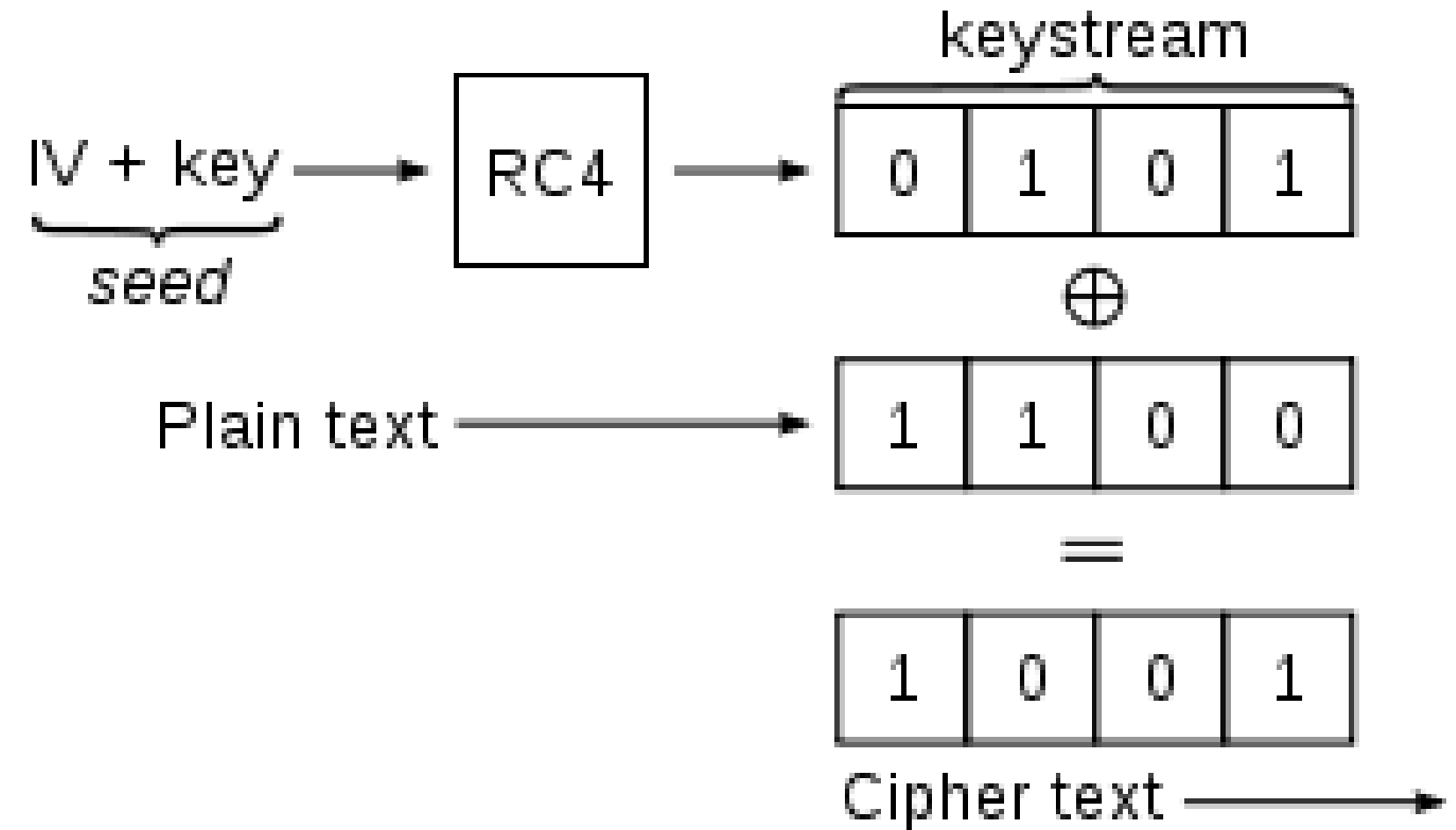
Earliest wireless security protocol.

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

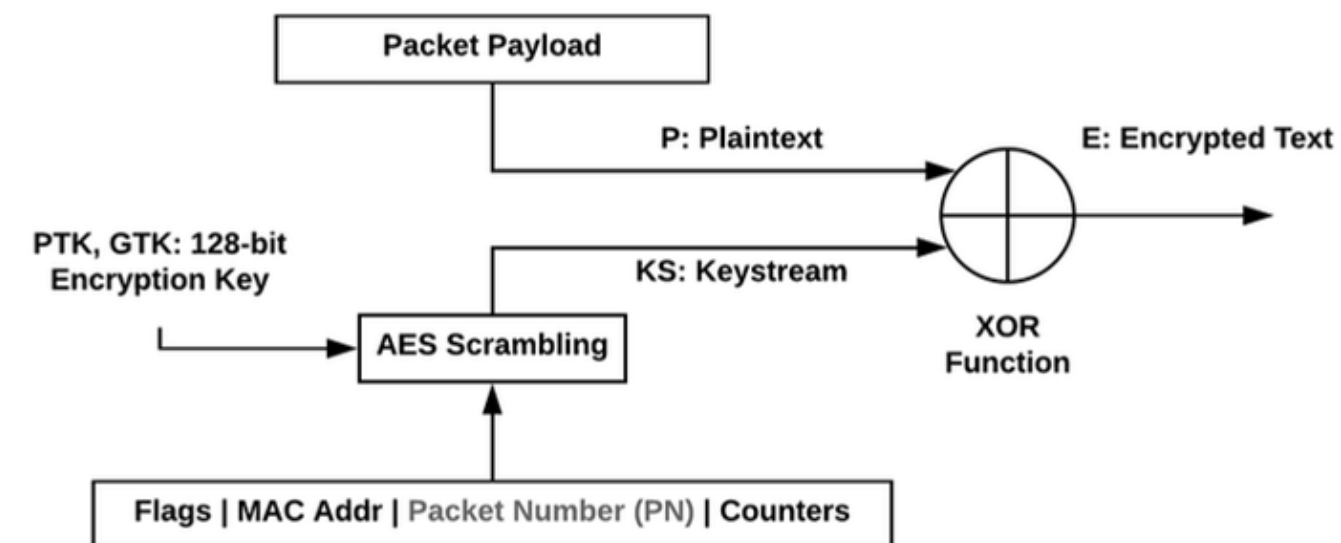
TKIP also includes a message integrity check (MIC) to ensure that the data has not been tampered with. TKIP is designed to be compatible with legacy hardware and software that does not support AES.

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.



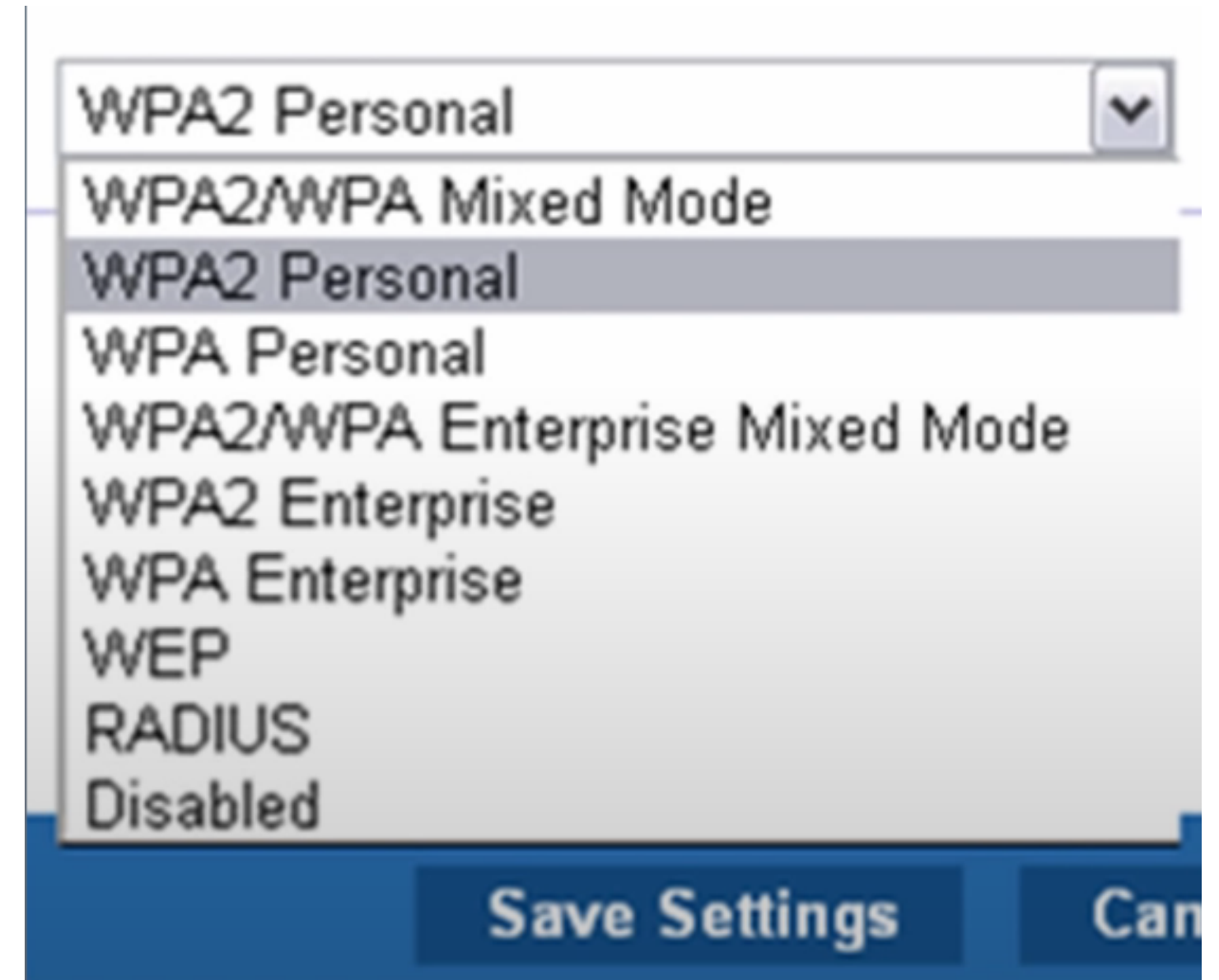
WIFI (WIRELESS) PASSWORD SECURITY

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

Status

Network

LAN

LAN IPv6

WAN

WAN DHCP

Wireless (2.4GHz)

Wireless (5GHz)

Wireless Schedule

IP Routing

DNS

GRE Tunnel

US Classifier

QoS Config

MESH

Vlan Binding

Security

Application

Maintenance

Network>Wireless (2.4GHz)

Enable☒

Mode

Bandwidth

Channel

Transmitting Power

WMM

Total MAX Users

SSID Configuration

SSID Select

SSID1

SSID Name

Enable SSID

SSID Broadcast

Port Mode

Isolation

MAX Users

Encryption Mode

WPA/WPA2 Personal

WPA Version

WPA Encryption Mode

TKIP/AES

WPA Key

☐ Show password

Enable WPS

Disable

Domain Grouping

☐ Enable

Save

Refresh

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!

