LAB EXPERIMENT – 1

Q. Make an experiment to implement WEP/WPA 2 PSK, 802.1x EAP Security Protocol.

Sol.

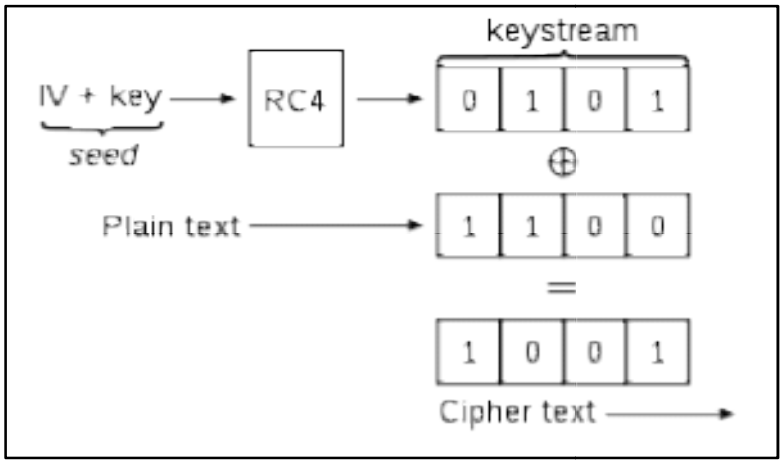
- **WEP :** Wired Equivalent Privacy is an alogrithm designed for wireless networks. Its intention was to provide data confidentiality with compared to the wired networks.

  It uses 10 or 26 hex digit key which was widely use when it was introduced.

  WEP uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity. It was deprecated in 2004 and is documented in the current standard.

  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. At the time that the original WEP standard was drafted, the U.S. Government's export restrictions on cryptographic technology limited the key size. Once the restrictions were lifted, manufacturers of access points implemented an extended 128-bit WEP protocol using a 104-bit key size (WEP-104).

WORKING OF WEP



- **WPA :** Wifi Protected Access (WPA), Wifi Protected Access II (WPA2), Wifi Protected Access III (WPA3) are the three security and srecurity certification programs added by the Wifi Alliance to secure wireless computer networks. These were added because of the major weaknesses found in the WEP system.

  It became available in 2003 and later on, in 2004 WPA2 was introduced with more security and recently in 2018, the WPA3 was introduced with several security inprovements over the previous version.

  Working of WPA :

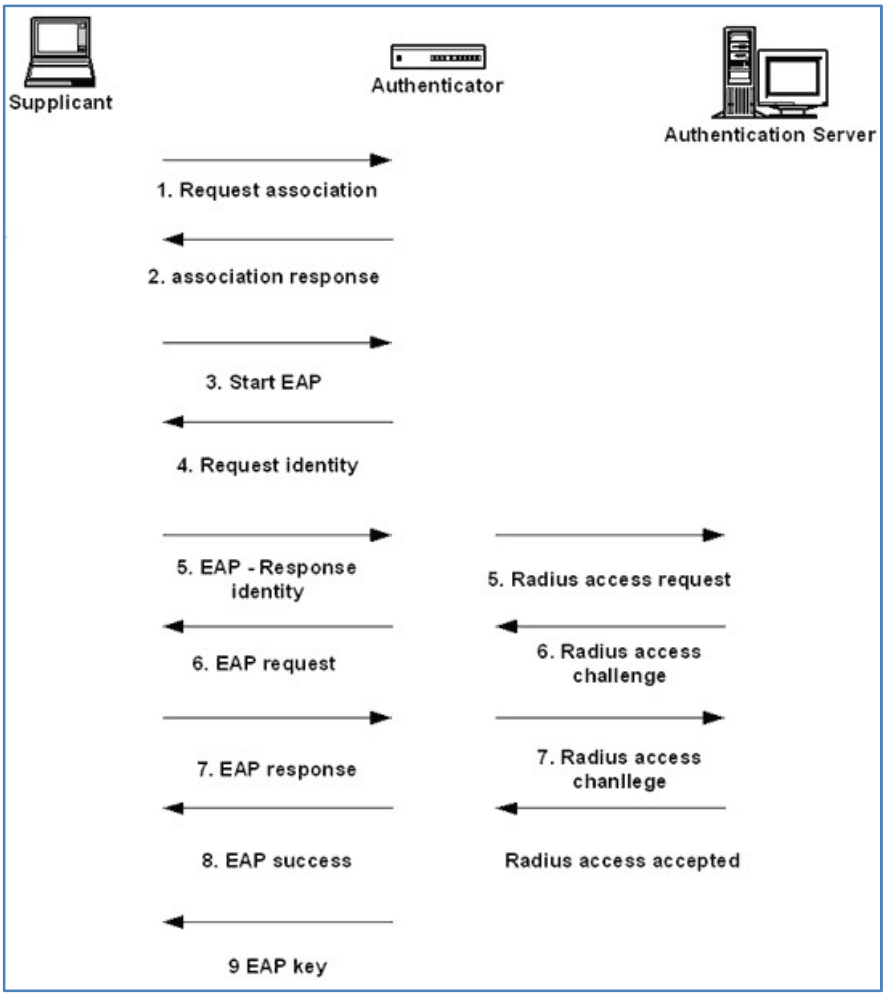
  This is designed for home and small office networks and doesn't require an authentication server. Each wireless network device encrypts the network traffic by deriving its 128-bit encryption key from a 256-bit shared key. This key may be entered either as a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 printable ASCII characters. If ASCII characters are used, the 256-bit key is calculated by applying the PBKDF2 key derivation function to the passphrase, using the SSID as the salt and 4096 iterations of HMAC-SHA1. WPA-Personal mode is available with both WPA and WPA2.

- **802.1x EAP :** The main parts of 802.1x Authentication are:

  1. A supplicant, a client end user, which wants to be authenticated.

  2. An authenticator (an access point or a switch), which is a "go between", acting as proxy for the end user, and restricting the end user's communication with the authentication server.

  3. An authentication server (usually a RADIUS server), which decides whether to accept the end user's request for full network access.



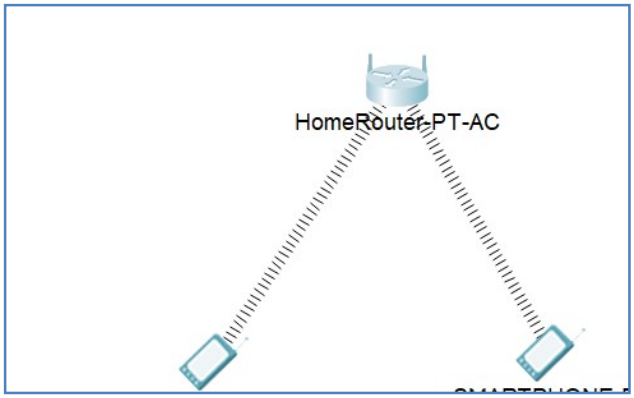
WORKING OF 802.1x EAP

Practical :

- **Implementing WEP / WPA 2 PSK in Packet Tracer**

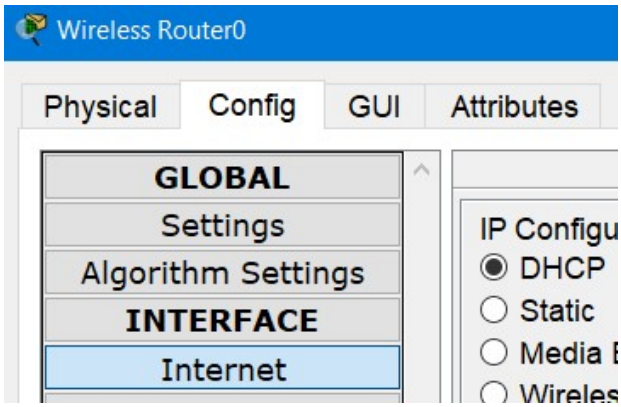
Step 1: Open and setup Packet tracer.

Step 2 : Select 1 Home router and 2 end devices from the bottom menu.

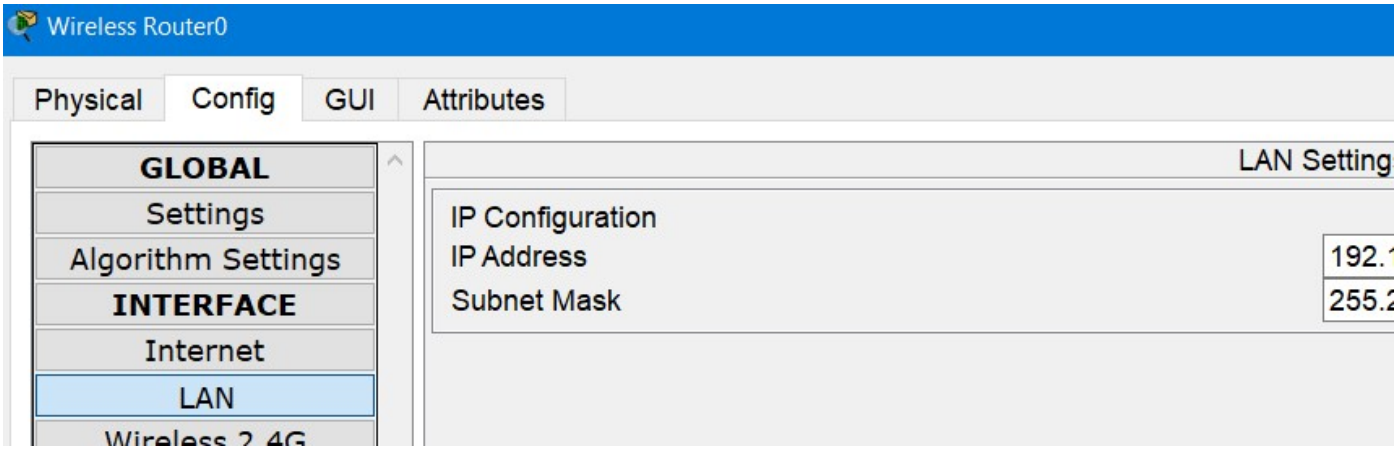


Step 3 : Double click on the home router and go to config section.

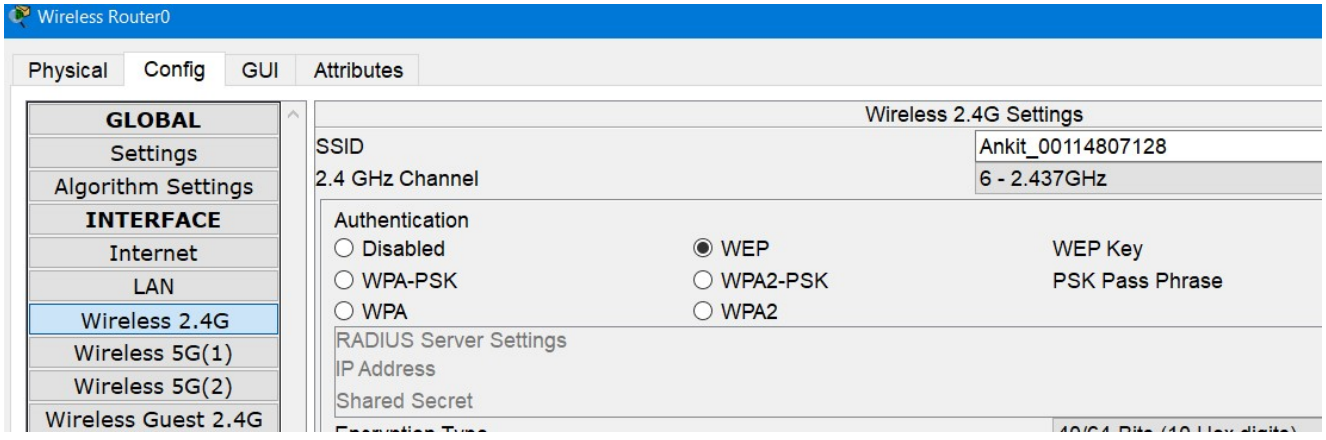
Step 4 : In config, Goto interfaces >> Internet and select DHCP.



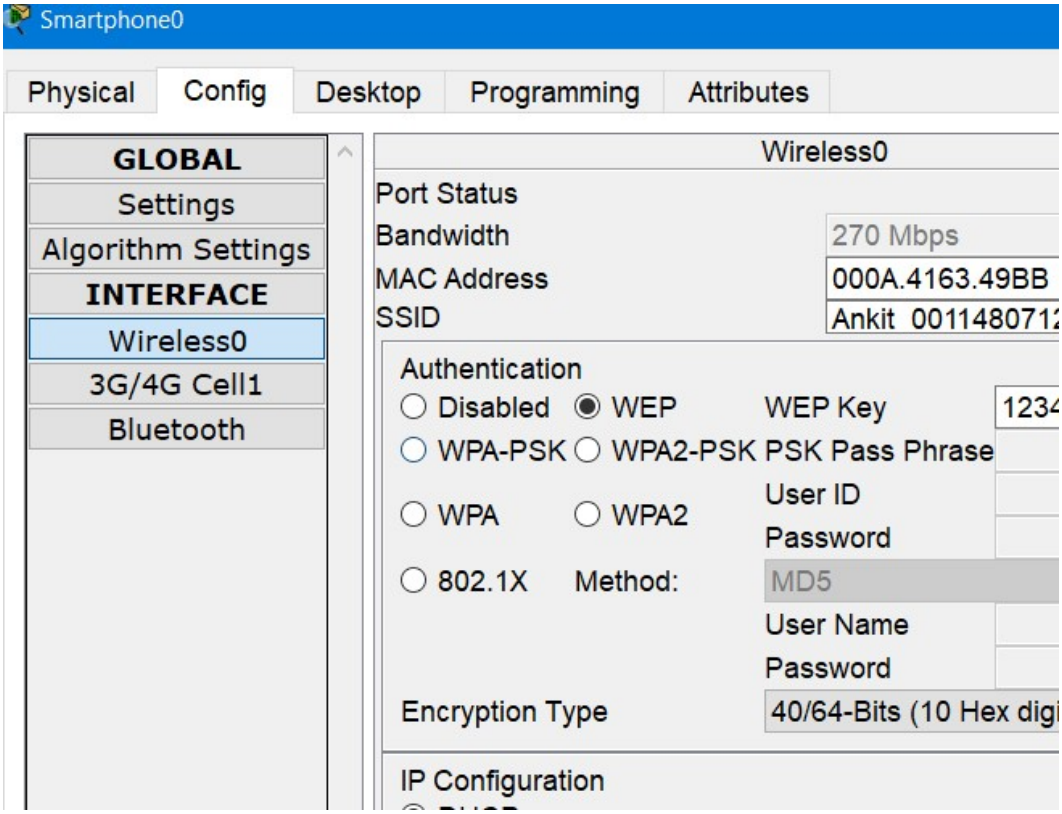
Step 5 : Then Goto LAN, and put the IP address : 192.168.0.1 and subnet mask as 255.255.255.0



Step 6 : Then goto Wireless 2.4G and select any from WEP/WPA-PSK/WPA2-PSK and enter the passkey and the SSID above them.



Step 7 : Now close the window and goto each connected device >> config >> wireless0 and enter the same ssid and passkey, which were entered in the home router.



Now after a while, the devices will be shown connected wirelessly.

- **Various wireless attacks :**

  1) <u>Packet Sniffing :</u>

  Networks are designed to facilitate and accelerate the traffic of information. In order to achieve this goal, the information is sent in packets across both wired and wireless networks. Due to the nature of wireless networks, these packets are sent through the air. As a result, it is very easy to capture them.

  A great deal of traffic is sent through wireless networks, such as RTP, SNMP or HTTP. The common feature of these is the fact that they are in plain text. Which means, one can easily read them with the

help of free access tools like Wireshark. As a result, someone with malicious intentions can simply steal your passwords and similar sensitive information.

2) Rouge Access Point :

Rouge access point refers to any unauthorized access point (AP) on a network. It can be created by an attacker or even a misinformed employee. Moreover, rouge APs make the entire network vulnerable to DoS attacks, packet captures, ARP poisoning and more.

3) Jamming :

Jamming (also known as network interference) aims to disrupt the network. Due to the wireless features, interference is almost unavoidable. A pair of Bluetooth headphones or even a microwave oven can cause mild interference. Most of the time, ill intended intruders combine jamming techniques with other methods like evil twinning. If you want to protect your organization, you should invest in a spectrum analyser, boosting the power of existing access points or using different frequencies.

4) Eavesdropping :

An eavesdropping attack, also known as a sniffing or snooping attack, is a theft of information as it is transmitted over a network by a computer, smartphone, or another connected device. The attack takes advantage of unsecured network communications to access data as it is being sent or received by its user.