Student Name	**Ayush Nigade**
SRN No	**202201820**
Roll No	**33**
Program	**Computer Engg**
Year	**Third Year**
Division	**E**
Subject	**Computer Network Laboratory (BTECCE22506)**
Assignment No	**7**

Assignment Number - 07

Title : Configuration of Wireless Access Point

Problem Statement : Configuration of Wireless access point/Router with static IP addressing and DHCP with MAC security and filters.

Theory :

Wireless access point

A Wireless Access Point (WAP) is a networking device that allows connecting the devices with the wired network. A Wireless Access Point (WAP) is used to create the WLAN (Wireless Local Area Network), it is commonly used in large offices and buildings which have expanded businesses.

It is easier and simpler to understand and implant the device. It can be fixed, mobile or hybrid proliferated in the 21st century. The availability, confidentiality, and integrity of the communication and network are a responsibility and to be ensured about that.

A wireless AP connects the wired networks to the wireless client. It eases access to the network for mobile users which increases productivity and reduces the infrastructure cost.

How an end user client with a WLAN NIC accesses a LAN

- To allow clients to find the AP easily, the AP periodically broadcasts beacons, announcing its (SSID) Service Set Identifier, data rates, and other WLAN information.
- SSID is a naming scheme for WLANs to allow an administrator to group WLAN devices together.
- To discover APs, clients will scan all channels and listen for the beacons from the AP(s). By default, the client will associate itself with the AP that has the strongest signal.
- When the client associates itself with the AP, it sends the SSID, its MAC address, and any other security information that the AP might require based on the authentication method configured on the two devices.
- Once connected, the client periodically monitors the signal strength of the AP to which it is connected.

- If the signal strength becomes too low, the client will repeat the scanning process to discover an AP with a stronger signal. This process is commonly called roaming.

SSID and MAC Address Filtering

When implementing SSIDs, the AP and client must use the same SSID value to authenticate. By default, the access point broadcasts the SSID value, advertising its presence, basically allowing anyone access to the AP. Originally, to prevent rogue devices from accessing the AP, the administrator would turn off the SSID broadcast function on the AP, commonly called SSID cloaking. To allow a client to learn the SSID value of the AP, the client would send a null string value in the SSID field of the 802.11 frame and the AP would respond; of course, this defeats the security measure since through this query process, a rogue device could repeat the same process and learn the SSID value.

Therefore, the APs were commonly configured to filter traffic based on MAC addresses. The administrator would configure a list of MAC addresses in a security table on the AP, listing those devices allowed access; however, the problem with this solution is that MAC addresses can be seen in clear-text in the airwaves. A rogue device can easily sniff the airwaves, see the valid MAC addresses, and change its MAC address to match one of the valid ones. This is called MAC address spoofing.

Wireless Network Security

WEP

WEP (Wired Equivalent Privacy) was first security solutions for WLANs that employed encryption. WEP uses a static 64-bit key, where the key is 40 bits long, and a 24-bit initialization vector (IV) is used. IV is sent in clear-text. Because WEP uses RC4 as an encryption algorithm and the IV is sent in clear-text, WEP can be broken. To alleviate this problem, the key was extended to 104 bits with the IV value. However, either variation can easily be broken in minutes on laptops and computers produced today.

WPA

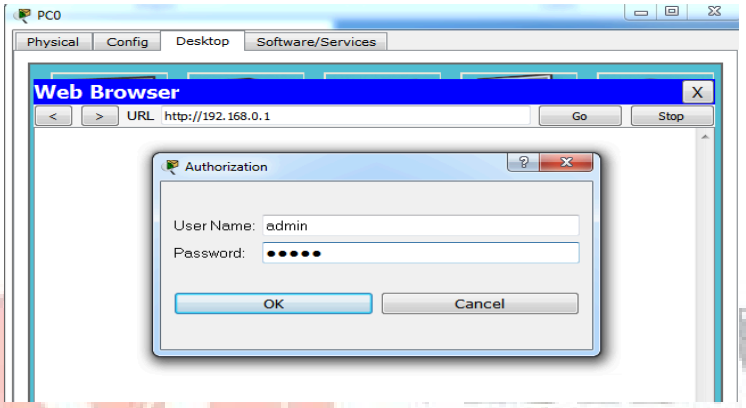
Wi-Fi Protected Access (WPA) was designed by the Wi-Fi Alliance as a temporary security solution to provide for the use of 802.1x and enhancements in the use of WEP until the 802.11i standard would be ratified. WPA can operate in two modes: personal and enterprise mode. Personal mode was designed for home or SOHO usage. A pre-shared key is used for authentication, requiring you to configure the same key on the clients and the AP. With this mode, no authentication server is necessary as it is in the official

802.1 x standards. Enterprise mode is meant for large companies, where an authentication server will centralize the authentication credentials of the clients.

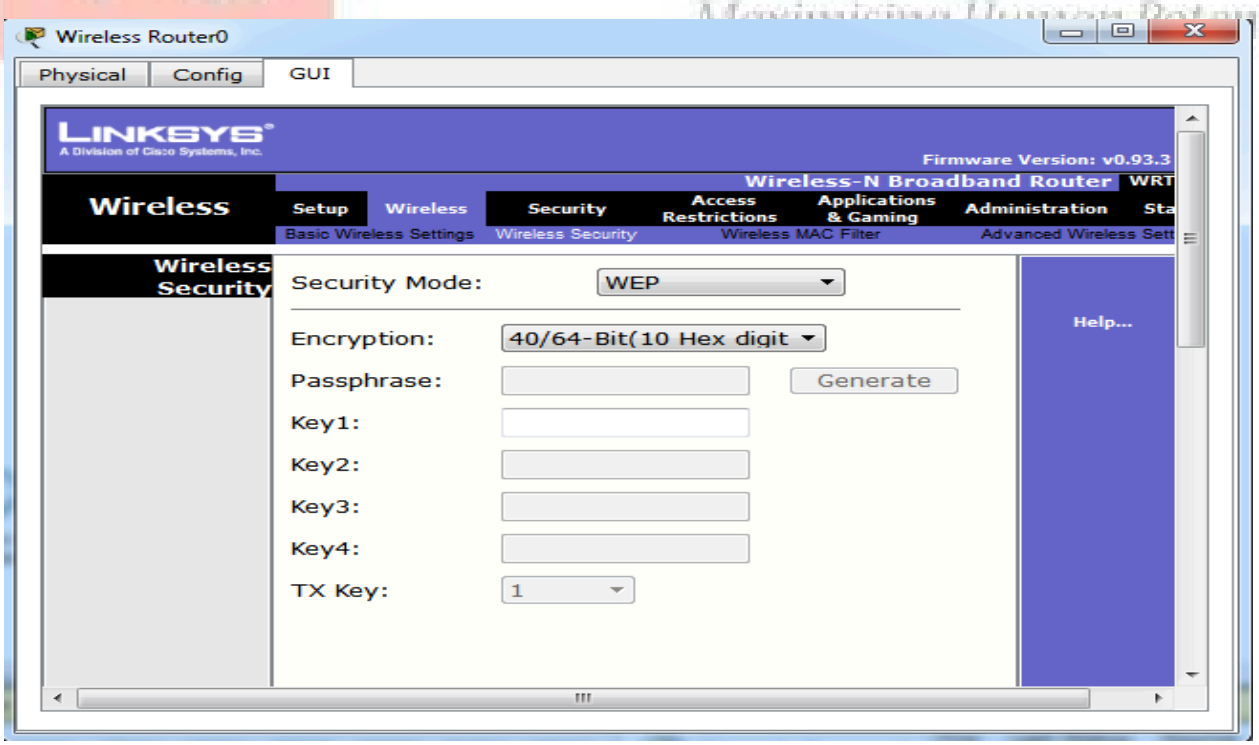
WPA2

WPA2 is the IEEE 802.11i implementation from the Wi-Fi Alliance. Instead of using WEP, which uses the weak RC4 encryption algorithm, the much more secure Advanced Encryption Standard (AES)–counter mode CBC-MAC Protocol (CCMP) algorithm is used.

WLAN with static IP addressing and DHCP with MAC security and filters

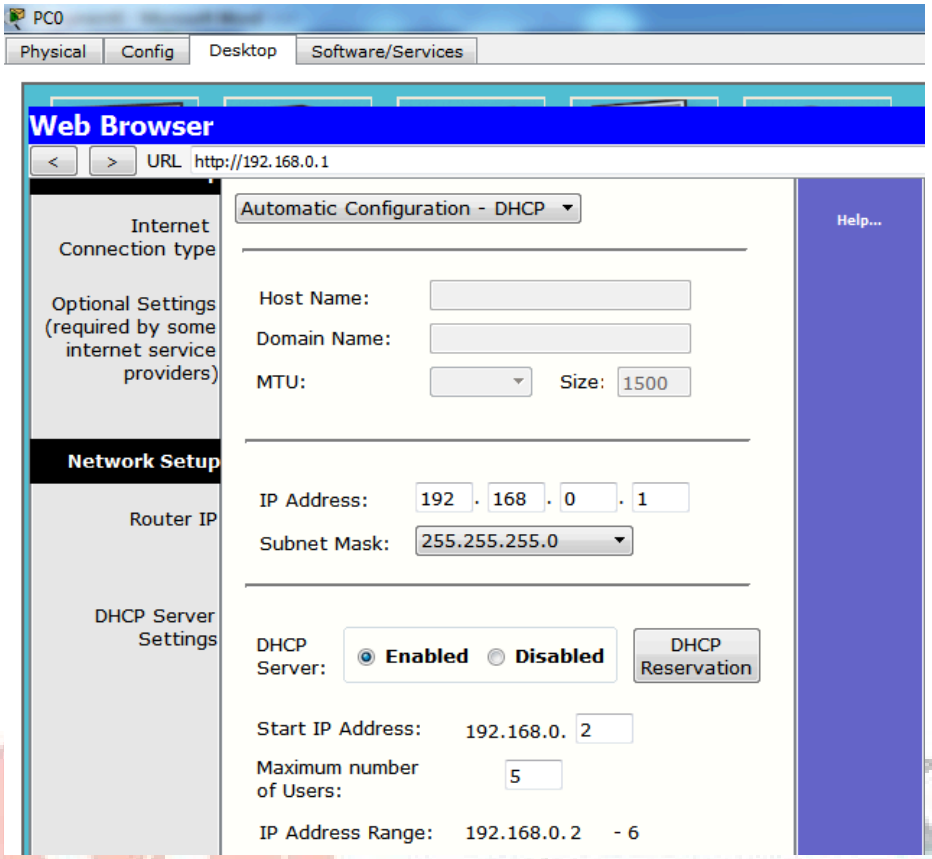


Wireless Security

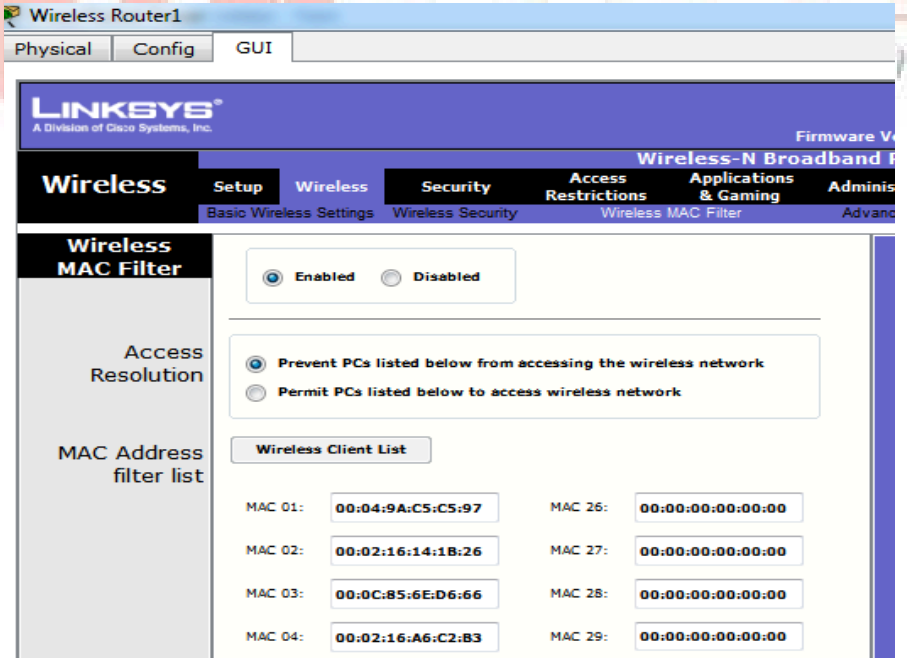


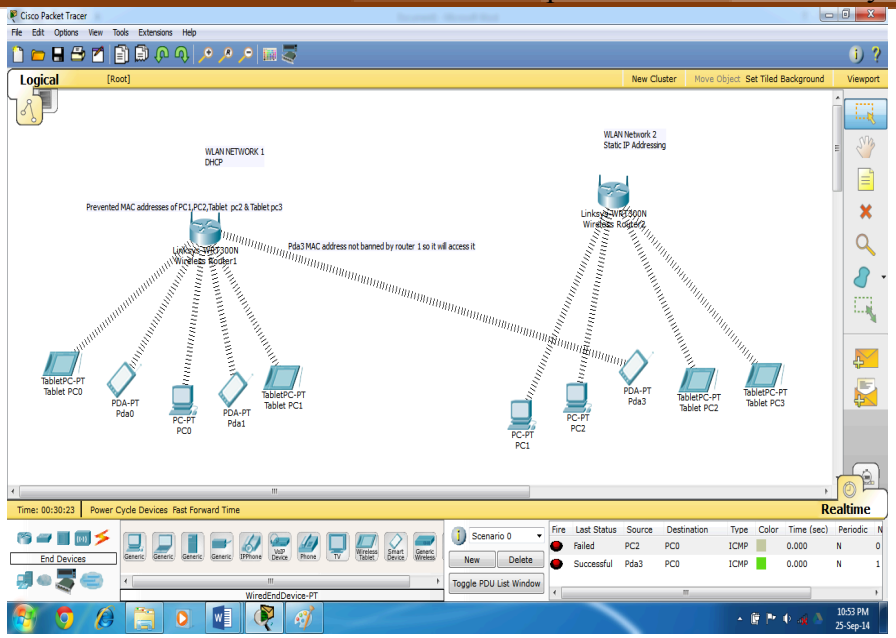
Configuring Wireless router by using PC.

Through web browser of PC0 configure Wireless router



MAC Filtering





Conclusion :

In conclusion, understanding the configuration of a wireless access point (WAP) is crucial for establishing a secure, efficient, and reliable network. By learning how to configure a WAP, I gained valuable insights into the importance of setting up network parameters, such as SSID naming, security protocols (WPA2 or WPA3), and managing user access through MAC address filtering. Additionally, I understood how proper channel selection and signal optimization contribute to reducing interference and ensuring better connectivity.