15/09/2020 **Mohd. Aftab Alam**
02013302717

EXPERIMENT 4

Aim :

Configure Access Point with Point to Point.

Theory :

In order to configure the access point, you can connect a laptop or PC to the wireless access point's console port via a serial cable. Through the use of terminal software, you can view access point configuration screens and change specific settings, such as radio channel and transmit power. The problem is that this method of accessing the configuration screens is often character-based and not user-friendly. Plus, a serial cable limits how far you can move from the wireless access point when performing the configurations.

If your laptop or PC is equipped with a radio card, then you can access the configuration screens through the use of a web browser by typing the Internet Protocol (IP) address of the access point as the URL for the web page. If the IP address in the laptop or PC is set within an acceptable range of the access point, then the browser will render the configuration screens in a much improved format.

Access Point Configuration Options :

Wireless access points include a wide variety of configuration settings, and the following represents the more common items you can change with tips on how to configure them.

***IP Address* –** Every wireless access point indeed, every client and server as well must have a unique IP address to enable proper operation on the network. The wireless access point will come with a pre-assigned IP address, but you'll probably need to change it to match the address plan of your customer's corporate network.

***Radio Channel* –** Set the radio channels in wireless access points within range of each other to different channels. This will prevent them from interfering with each other. With 802.11b and 802.11g networks, use channels 1, 6 and 11 to ensure enough frequency separation to avoid conflicts. 802.11a channels, however, don't overlap, so just be sure the adjacent 802.11a wireless access points are set to different channels.

***Transmit Power* –** In most cases, the transmit power should be set to the highest value. This maximizes range, which reduces the number of wireless access points and cost of the system for your customer. If you're trying to increase the capacity of your customer's network by placing wireless access points closer together, set the power to a lower value to decease overlap and potential interference.

***Service Set Identifier (SSID)* –** It defines the name of a WLAN that users associate with. By default, the SSID is set to a common value. In order to improve security, you should change the SSID to a non-default value to minimize unauthorized users from associating with the access point. For even better security, some wireless access points let you disable SSID broadcasting.

***Data Rate* –** Most wireless access points allow you to identify acceptable data rates. By default, 802.11b wireless access points operate at 1, 2, 5.5 and 11 Mbps data rates, and 802.11g access points operate at data rates of 6 to 54 Mbps, depending on the quality of the link between the client device and the access point.

***Beacon Interval* –** It is the amount of time between access point beacon transmissions. The default value for this interval is generally 10ms, that is, 10 beacons sent every second. This is sufficient to support the mobility speed of users within an office environment. You can increase the beacon interval and have lower overhead on the network, but then roaming will likely suffer.

***Request-To-Send/Clear-To-Send (RTS/CTS)* –** The RTS/CTS function alleviates collisions due to hidden nodes, which occurs when multiple stations are within range of a common wireless access point but out of range of each other. In most cases it's best to disable RTS/CTS.

***Fragmentation* –** This can help reduce the amount of data needing retransmission when collisions or radio frequency (RF) interference occur. This can improve performance in some cases by enabling the clients and access points to retransmit smaller packets when errors are found.

***Encryption* –** Most wireless access points allow the enabling of wired equivalent privacy (WEP), which encrypts the frame body of each data frame. Use WEP as a minimum level of protection. WEP is somewhat static and requires you to configure each access point and client device with the same encryption key.

***Authentication* –** As part of the 802.11 standard medium access control (MAC) functions, wireless access points implement the default 802.11 open system authentication and sometimes shared key authentication. Neither one of these forms of authentication provides very good security.

***Administrative Interfaces* –** In order to improve security for your customer, be sure to disable the console port of the access point to avoid the possibility of an unauthorized person reconfiguring an access point and removing encryption and authentication functions.

Configuration – It has two parts :

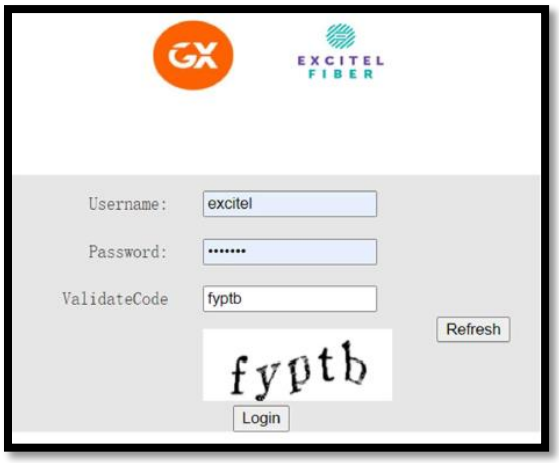
- Configuring the Internet Part, where we tell the Router how to connect to the internet.
- Configuring the Wi-Fi Part, where we decide the name and password with which we connect to the Router.

Password Creation have been explained, few high end routers have two bands to work on – 2.4 GHz and 5 GHz

- 2 GHz band provides higher range, but lesser speed.
- 5 GHz band provides lower range, but higher speed.

Step 1 : Login into your account using your username and password –

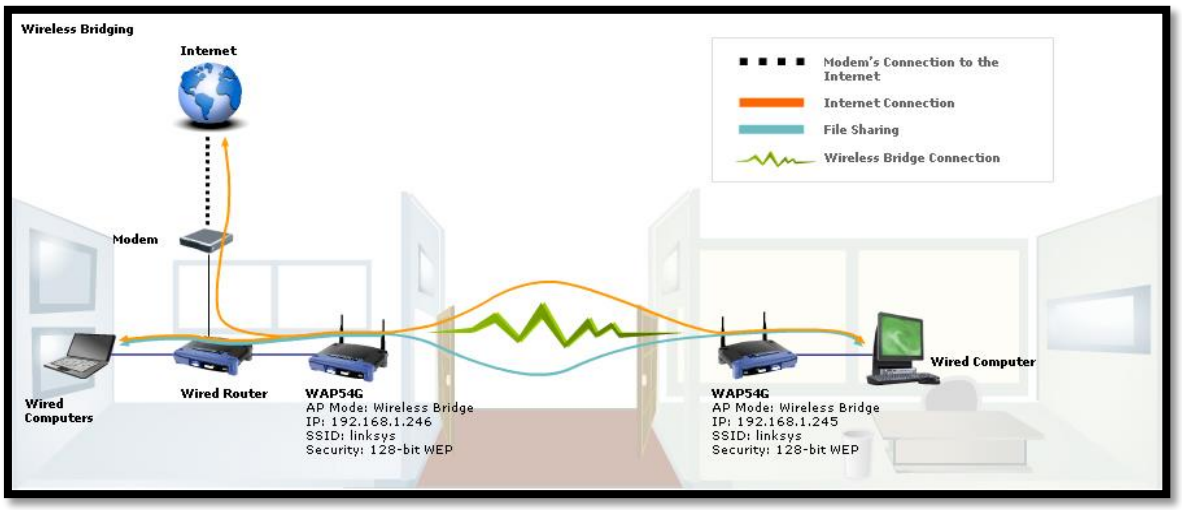
Router Brand	Common Default IP Addresses
Asus	192.168.1.1, 192.168.2.1
Benatone	192.168.1.1
Belkin	192.168.1.1, 192.168.2.1
Cisco	192.168.1.1, 192.168.0.30, 192.168.0.50
Dell	192.168.1.1
D-Link	192.168.1.1, 192.168.0.1
Gigabyte	192.168.1.254
Google	192.168.86.1, 192.168.0.1
GX	192.168.1.1
Huawei	192.168.1.1, 192.168.0.1, 192.168.3.1, 192.168.8.1
Microsoft	192.168.2.1
Netgear	192.168.0.1 , 192.168.0.227

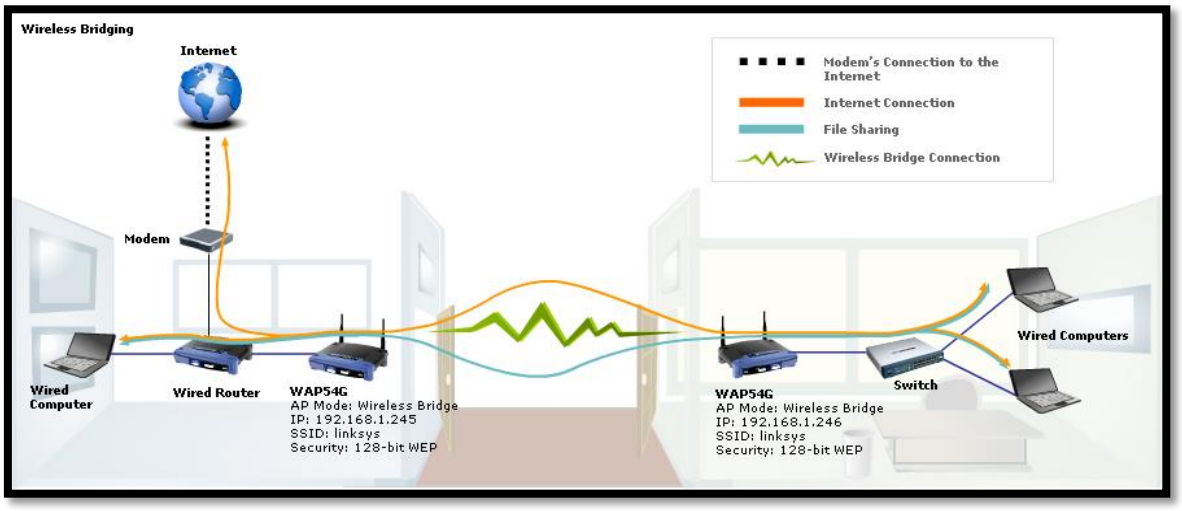


Configuring Access Point with Point to Point :

GX Wireless-G Access Points can be configured as an Access Point, Access Point Client, Wireless Repeater, and Wireless Bridge. The Wireless Bridge mode will turn the access point into a wireless bridge. Wireless clients will not be able to connect to the access point in this mode.

NOTE **-** When an access point is configured as a wireless bridge, it will link a wireless network to a wired network allowing you to bridge two networks with different infrastructure.





To configure an access point as a wireless bridge, you need to perform three steps :

1. Checking the Wireless MAC Address of an Access Point
2. Setting-Up Wireless Bridge Mode on the WAP54G
3. Changing the LAN IP Address of the Wireless Bridge

Checking the Wireless MAC Address of an Access Point :

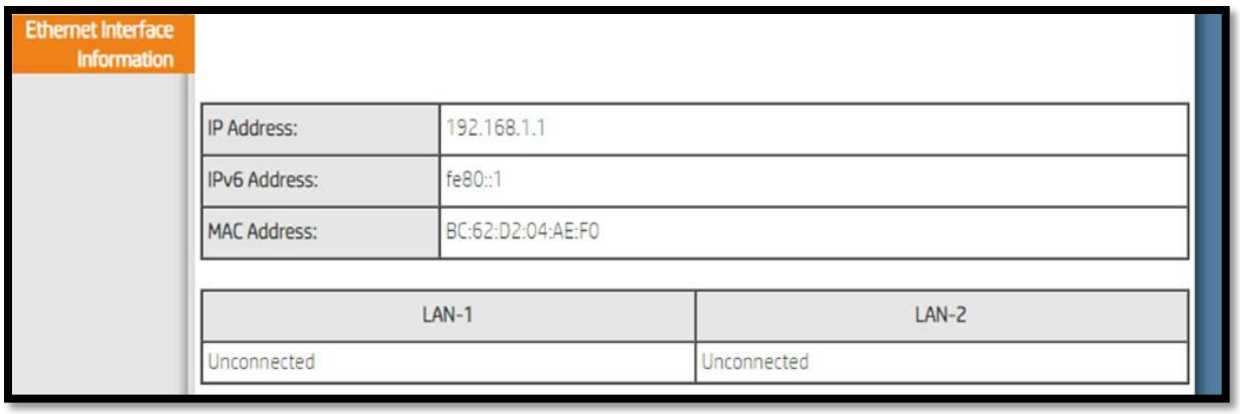
The following steps will be performed on the main access point using a wired computer –

Step 1 – Connect a computer to the access point.

Step 2 – Assign a static IP Address on the computer.

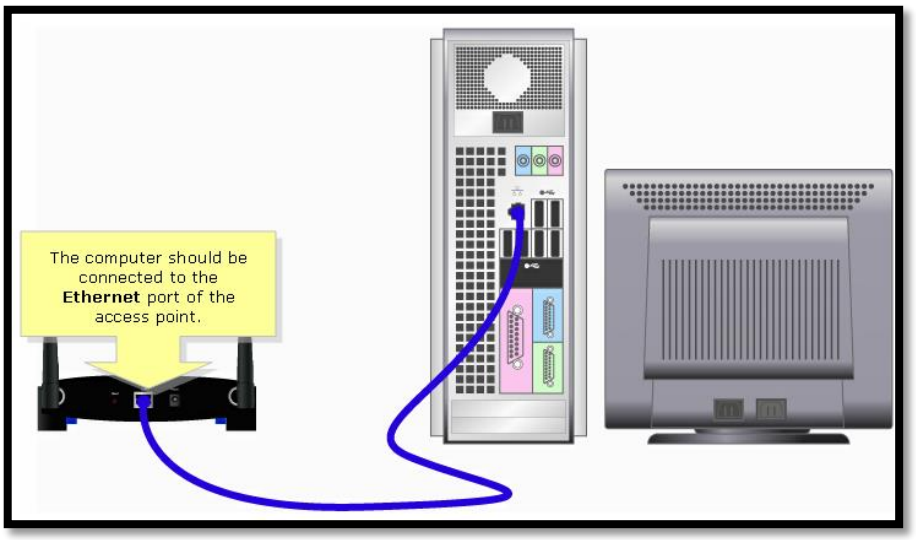
Step 3 – Open the access point's web-based setup page.

Step 4 – When the access point's web-based setup page opens, take note of the Wireless MAC Address.



Setting-Up Wireless Bridge Mode on the WAP54G :

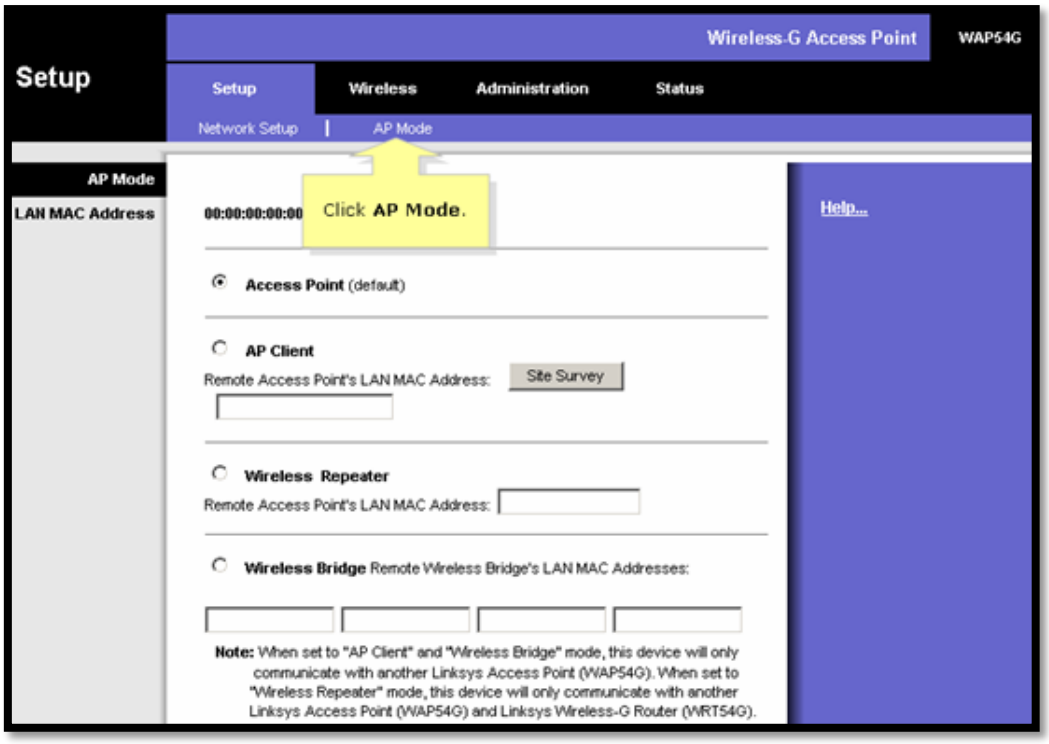
Step 1 – Connect a computer to the access point you want to configure as a wireless bridge.



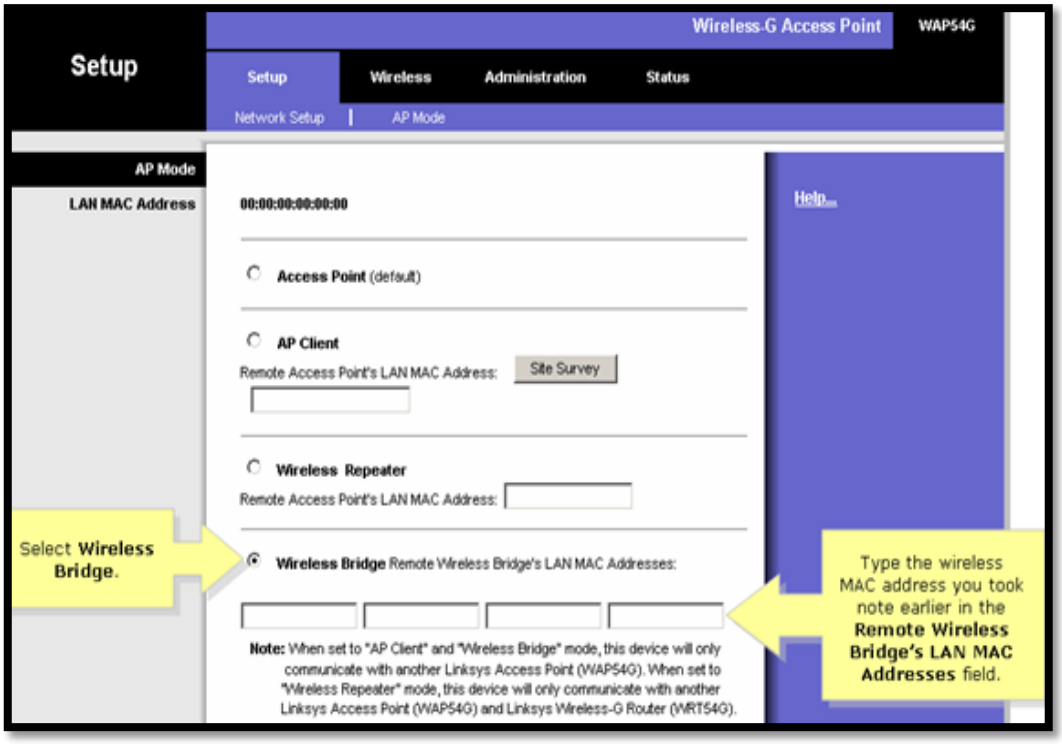
Step 2 – Assign a static IP Address on the computer.

Step 3 – Open the access point's web-based setup page.

Step 4: Then the access point's web-based setup page opens, click AP Mode. The access point's web-based setup page may differ depending on the access point's version number.



Step 5 – Select Wireless Bridge and type the remote access point's MAC Address that you took note of earlier. Remove the colons (:) when typing the MAC Address on the Remote Access Point's LAN MAC Address field.



Step 6 – Click on the button