***Experiment No -07***

***Aim:*** To setup and configure Wireless Access Point.

***Theory:***

In computer networking, a wireless access point (WAP) is a networking hardware device that allows a Wi-Fi compliant device to connect to a wired network. The WAP usually connects to a router (via a wired network) as a standalone device, but it can also be an integral component of the router itself. A WAP is differentiated from a hotspot, which is the physical location where Wi-Fi access to a WLAN is available.

Prior to wireless networks, setting up a computer network in a business, home or school often required running many cables through walls and ceilings in order to deliver network access to all of the network-enabled devices in the building. With the creation of the wireless access point, network users are now able to add devices that access the network with few or no cables. A WAP normally connects directly to a wired Ethernet connection and the WAP then provides wireless connections using radio frequency links for other devices to utilize that wired connection. Most WAPs support the connection of multiple wireless devices to one wired connection. Modern WAPs are built to support a standard for sending and receiving data using these radio frequencies. Those standards, and the frequencies they use are defined by the IEEE. Most APs use IEEE 802.11 standards.

***Configuration access:***

In order to configure the access point for your customer, 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 (for example, "http:/192.168.0.1" without the quotes). If the IP address in the laptop or PC is set within an acceptable range of the access point (the IP address would be 192.168.0.xxx, with the last three numbers something between 2 and 254), then the browser will render the configuration screens in a much improved format.

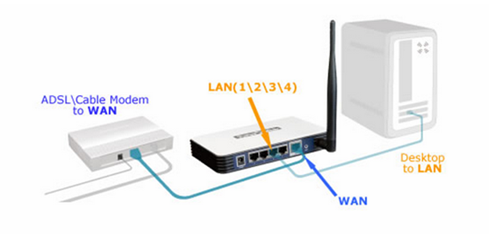
***Access point configuration options:***

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.

1. **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. In most cases, the use of static IP addresses in wireless access points is best, mainly to make operational support easier. Some wireless access points allow you to use dynamic host configuration protocol (DHCP) so that the wireless access point automatically obtains an IP address from a DHCP server. This may be beneficial for some home applications if the broadband service provider offers addresses via DHCP.
2. **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. Some wireless access points have a feature whereby the access point automatically sets its channel based on others already in use, making installation much easier (but keep in mind that this could cause dropped calls with voice applications).
3. **Transmit power.** In most cases, the transmit power should be set to the highest value (100 megawatts in the U.S.). 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 decrease overlap and potential interference. Lower power settings also limit the wireless signals from propagating outside the physically controlled area of the facility, which improves security.
4. **Service set identifier (SSID).** The SSID defines the name of a WLAN that users associate with. By default, the SSID is set to a common value, such as *tsunami* for Cisco products. 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. This keeps most client device operating systems (e.g., Windows Vista) from sniffing the SSID from access point beacons and automatically associating with the access point. Someone could, however, obtain the SSID using other sniffing tools that obtain the SSID from 802.11 frames when users first connect to the access point.
5. **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. As the link quality deteriorates, the access point will automatically throttle down to lower data rates in an attempt to maintain a connection. You can, however, exclude specific data rates. For example, you may want your customer's communications only at 11 Mbps or not at all. This could be necessary to support higher bandwidth applications.
6. **Beacon interval.** The beacon interval is the amount of time between access point beacon transmissions. The default value for this interval is generally 10 ms, 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. It's best to leave this setting alone. In some cases, though, you might want to experiment with setting the beacon interval to higher values to maximize 802.11 power management functions (if roaming doesn't suffer).
7. **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.
8. **Fragmentation.** Fragmentation 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.
9. **Encryption.** Most wireless access points allow the enabling of wired equivalent privacy (WEP), which encrypts the frame body (not headers) 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. When using 40-bit keys, you'll need to enter a key having 10 hexadecimal characters (0-9, a-f or A-F). 128-bit keys, which offer better security, are 26 hexadecimal characters long. For even better security, some wireless access points offer more advanced forms of encryption, such as Wi-Fi protected access (WPA) and 802.11i, which ensure that keys change automatically at a rate that hopefully thwarts a hacker from cracking the security.
10. **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. As a result, many wireless access points now include 802.1x mechanisms that authenticate users with an external authentication server. Certainly consider activating these more advanced authentication methods when configuring the access point. 802.11i and WPA include 802.1x mechanisms.
11. **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. Also, be certain to change the default administrative login username and password to ensure hackers don't have easy access to configuration settings.

***Steps to Configure Wireless Access Point***

1. Turn off your modem, router and computer.
2. Connect your modem to the WAN port of the TP-Link router via an Ethernet cable; connect a computer to TP-Link router’s LAN port via an Ethernet cable.
3. Power on your router and computer first and then modem.



*Step 1:*

Log into the router’s web-based management page.

*Step 2:*

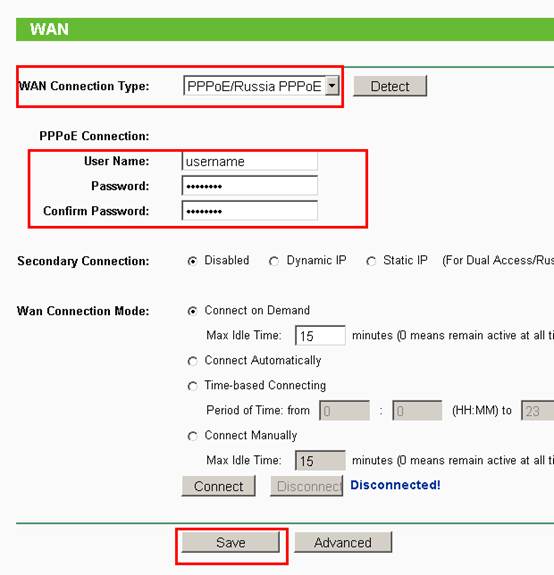
Configure WAN Connection Type:

On the router’s management page, click Network > WAN on the left of the web page:

Change the WAN Connection Type to PPPoE.

*Step 3:*

Enter your PPPoE username and password which are provided by your ISP.

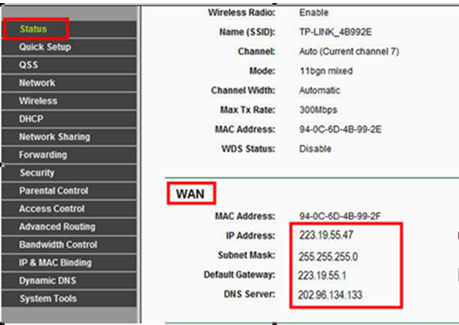


*Step 4:*

Click Save to save your settings, then the router will connect to Internet after a while.

*Step 5:*

Wait for a few minutes and check the WAN part on the Status page, if it shows any IP address (similar as below), that means th e connection between the Router and the Modem is established.



*Step 6:*

If there is not wan IP address and no internet access, please do a Power Cycle as the below:

1. Turn the DSL modem off first, then turn your router and computer off, and leave them off for about 2 minutes;
2. Turn the DSL modem on first, wait till the modem gets ready, then turn the router and your computer back on.

***Conclusion:*** Thus we have successfully setup and configured Wireless Access Point.