

COMPUTER SYSTEMS SERVICING

Information Sheet: 1.1

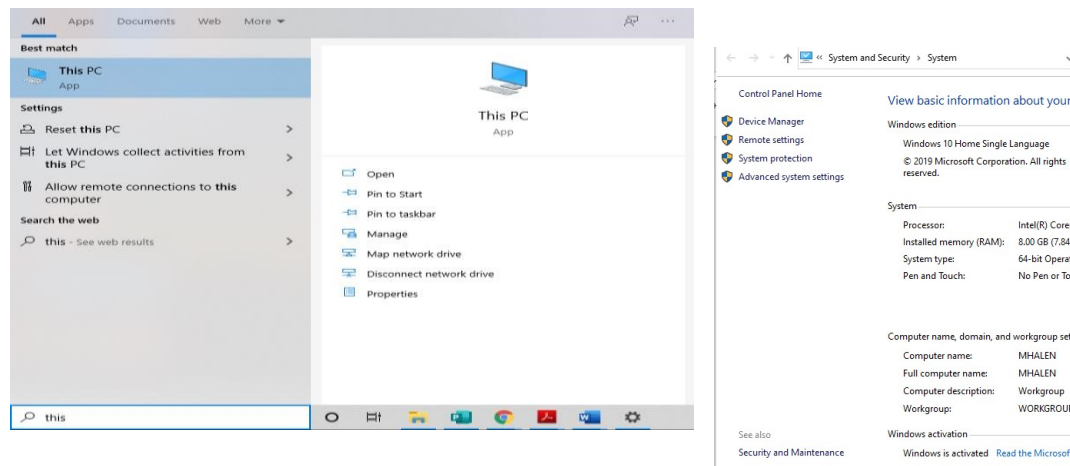
Configure Client Device Setting

1. Setting up Time and Date

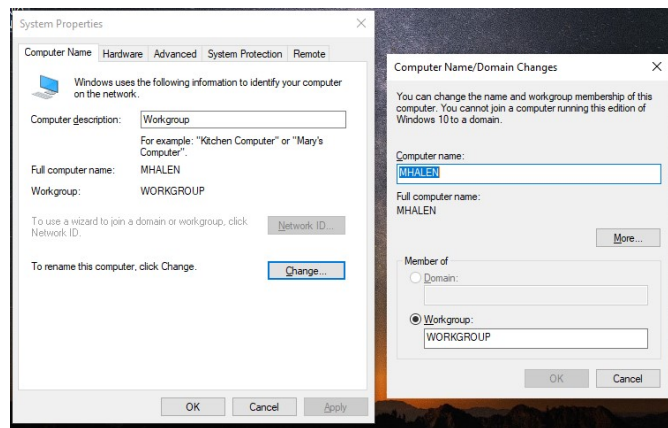
- a. On Windows 10 OS, to set up the Time and Date go to the right bottom of your taskbar see figure below:



- b. Right click on the area of time and date then choose “Adjust date/time”. Then the date/time settings will appear
 - c. If you wish to set your date/time automatically just click “ON” at “Set Time Automatically”. If not, you can turn it off and be the one to set date/time.
 - d. You could also set “Time Zone” it is located below change date and time. You could choose Beijing, Kuala Lumpur or Taipei, Philippines is none on the choices just choose a Time Zone that much on our Time “UTC+8”.
- #### 2. Set up Computer Name
- a. In setting up your Computer Name, Go to Start Menu and search for “My PC”, and other Windows OS version you can find it on Desktop a Computer Icon with a name of “My Computer”. For Win10, please see figure below:
 - b. Then “Control Panel” will appear. Click on “Change Settings” button that is shown below:



c. After clicking “Change Settings”, another Set Up will appear. You can now change the “Computer Description” and “Computer Name.” As shown on figure below:



- **Note:** Setting up your Computer Name is important. This will serve as the Identity of your computer. It will be useful when it comes on setting up your Computer Network. The Server/Hardware Network will identify what PC is being connected or configured.

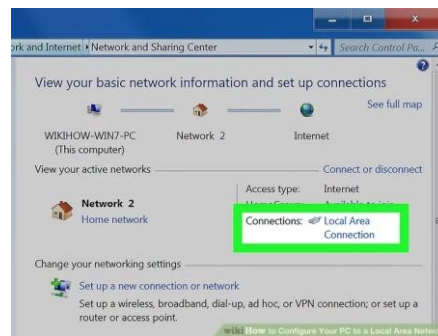
3. Install and Configure Network Driver

- a. In every personal computer, it is necessary to install a network driver so that your computer will have an access on every network connection it may need. The first step to do is to select a Compatible driver’s pack for your PC. Depends on your OS. Below is an example:

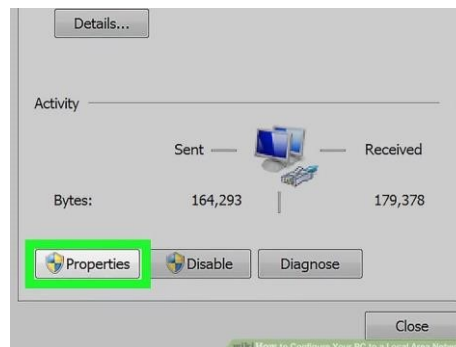
There are different versions of DriverPack Solution: 15, 14, 13, 12, 11, 10 & 8. You should be careful on choosing a driver pack; it should be compatible with your PC specification.

After the installation of your network driver, you are ready to configure your network. To configure the network of your PC, Right-click on your network connection. You'll see this in your System Tray. If you are connecting your computers through a switch with no router, you'll need to assign each computer on the network its own individual IP address. This process is handled automatically if you're using a router. Think of an IP address as a mailing address. Each computer on the network needs a unique IP address so that information sent across the network reaches the correct destination.

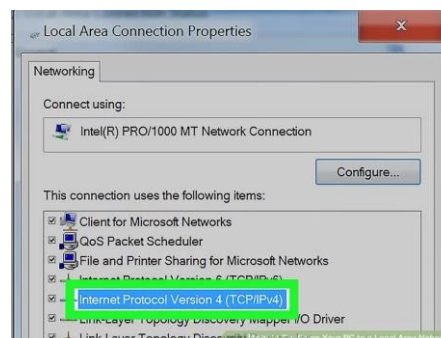
- A. Right-click on your network connection.
- B. Click Open Network and Sharing Center.
- C. Click the Ethernet link at the top of the window. You'll see this next to "Connections."



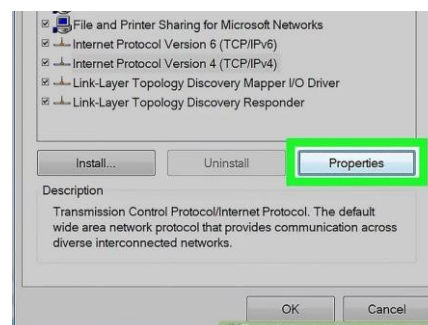
- D. Click Properties.



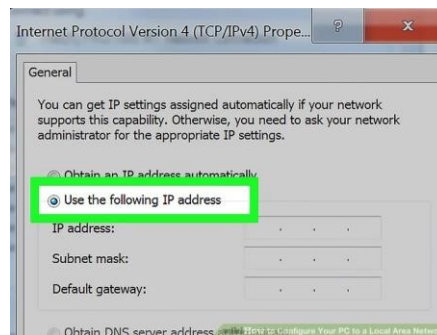
- E. Click Internet Protocol Version 4 (TCP/IPv4). Make sure you don't uncheck it, just highlight it.



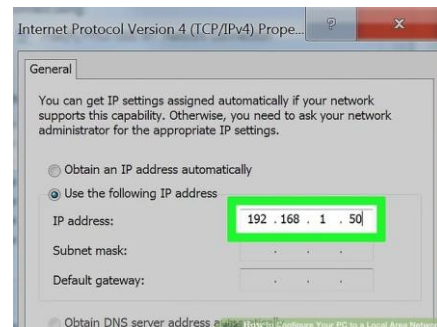
- F. Click Properties.



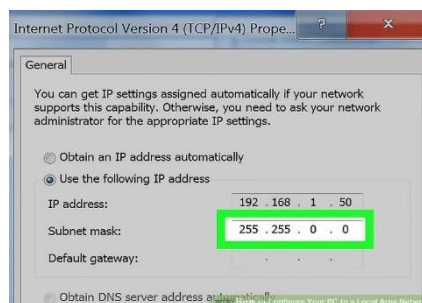
- G. Click the Use the following IP Address radio button.



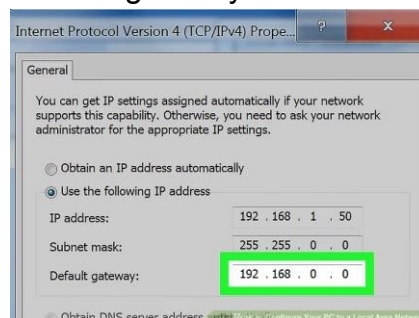
H. Type 192.168.1.50 into the IP address field.



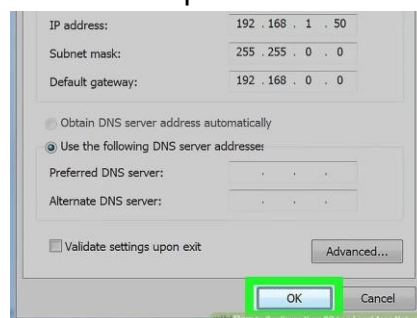
I. Type 255.255.0.0 into the Subnet mask field.



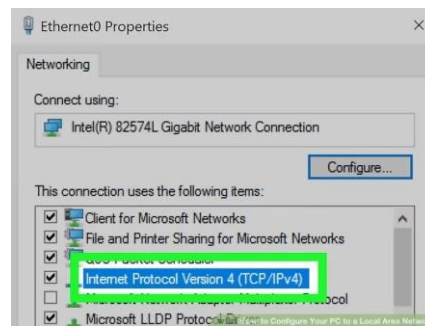
J. Type 192.168.0.0 into the Default gateway field.



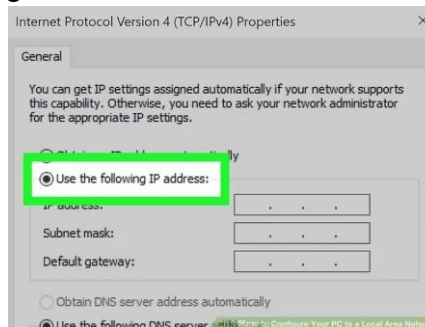
K. Click OK. This will save the settings for that computer. This computer is now configured on your network with a unique IP address.



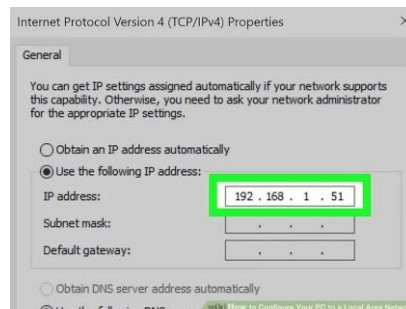
L. Open the Internet Protocol Version 4 properties on the next computer. Follow the steps above on the second computer to open the Internet Protocol Version 4 (TCP/IPv4) Properties window.



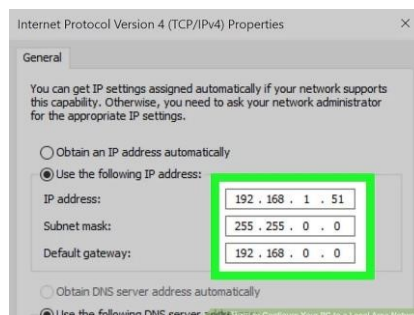
M. Click the Use the following IP Address radio button.



N. Type 192.168.1.51 into the IP address field. Notice that the final group of numbers has incremented by 1.



O. Enter the same values for Subnet Mask and Default Gateway. These values should be the same as they were on the first computer (255.255.0.0 and 192.168.0.0 respectively)



4. Install necessary software application e.i MS Office and Anti virus

a. You may install necessary software applications for your PC like MS Office and an Antivirus. See figures below for references:



Information Sheet :1.2

Configuring Local Area Network

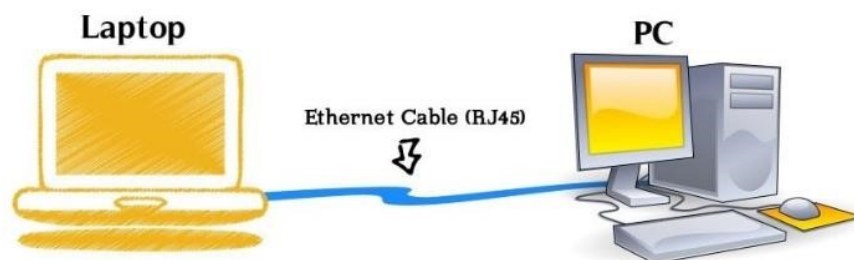
A Local Area Network (LAN) is a group of computers and associated devices that share a common communications line or wireless link to a server. Typically, a LAN encompasses computers and peripherals connected to a server within a distinct

geographic area such as an office or a commercial establishment. Computers and other mobile devices use a LAN connection to share resources such as a printer or network storage.

Equipment and Peripherals Needed for Configuring LAN

Equipment/ Peripherals Name	Description	Image
Personal Computer (PC)	a multipurpose electronic computer whose size, capabilities, and price make it feasible for individual use. PCs are intended to be operated directly by an end user, rather than by a computer expert or technician.	
Ethernet cables	Networking hardware used to connect one network device to other network devices or to connect two or more computers to share printers, scanners etc. Different types of network cables, such as coaxial cable, optical fiber cable, and twisted pair cables, are used depending on the network's physical layer, topology, and size.	

Be sure to connect first the cross-over ethernet cable to the PCs that you will use.

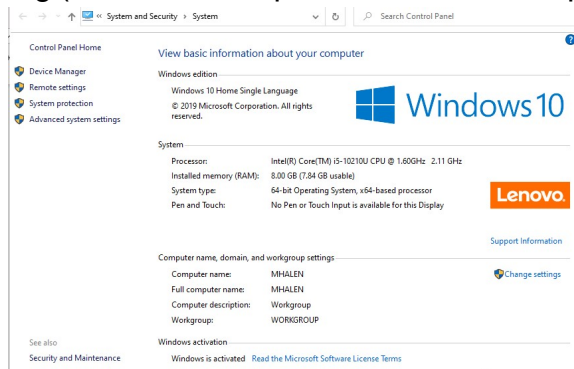


When Equipments and Peripherals are all ready, we will now proceed on Installing and configuring Local Area Network. Below are steps in configuring Local Area Network.

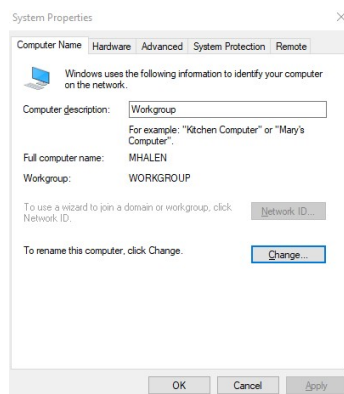
1. On Desktop ==> Select My Computer ==> Right Click ==> Select properties.



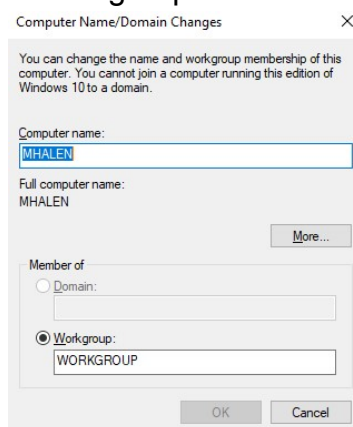
2. Select Change Setting (administrative permission will be required in this procedure).



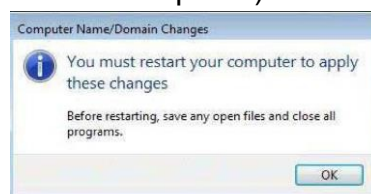
3. Click or select Change.



4. Change computer name and workgroup name. Then, click OK.



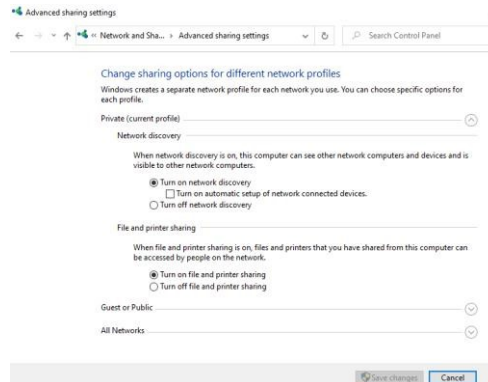
5. Save the change (A Reboot will be required).



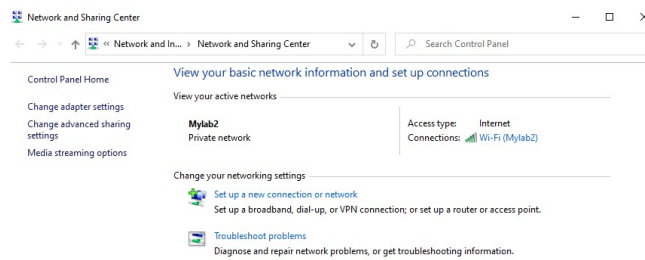
6. After Reboot ==> Right Click on My Network Place ==> Properties.



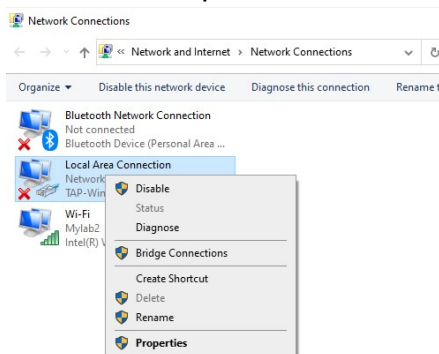
7. Turn on Network discovery, File sharing, Printer Sharing.



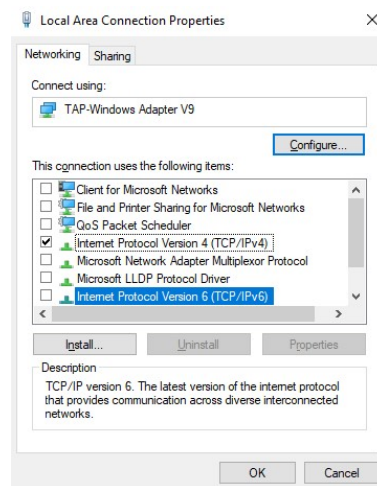
8. Click on Set Up network connections.



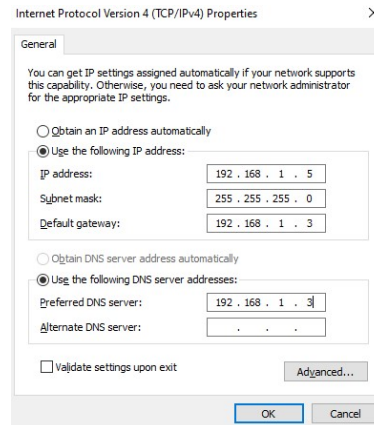
9. Select Local Area Connection ==> Properties



10. Select Internet Protocol version 4 (TCP/IPv4) ==> properties.



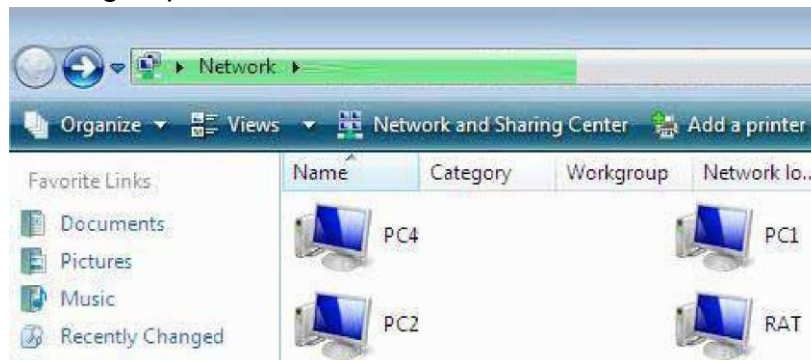
11. Now enter the assigned IP address and then click OK.



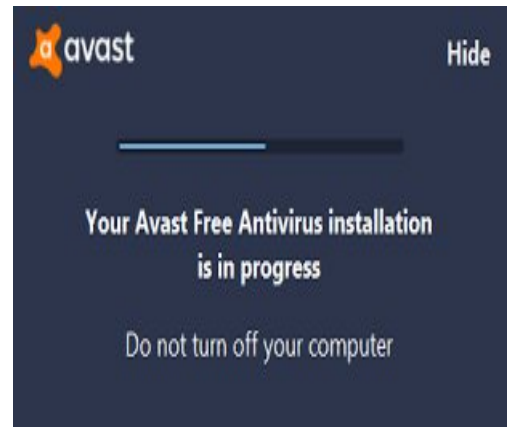
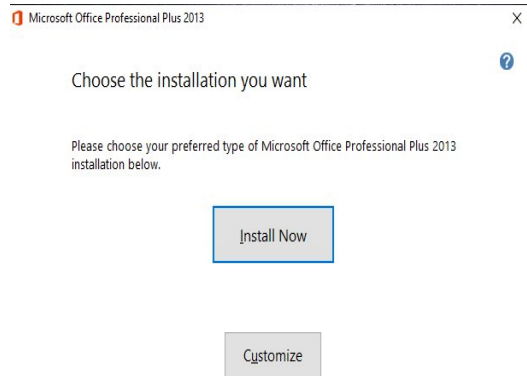
12. Now open My network place ==> Click to change then Select Turn on network discovery and file sharing.



13. If you could see all computers in My Network place, you have successfully configured a workgroup.



13.

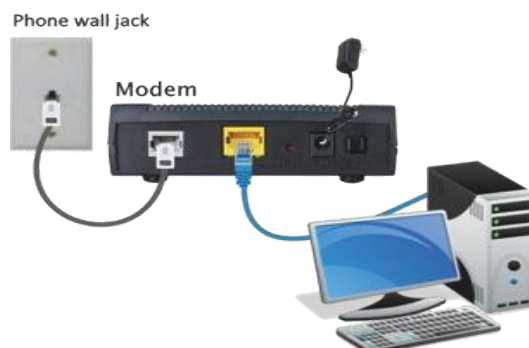


Information Sheet 1.3

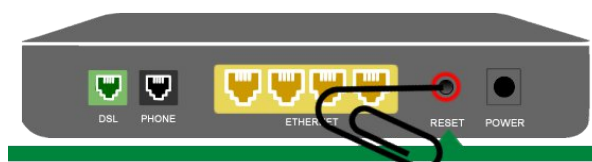
Configuring Wide Area Network

As we gather all the peripherals and equipment needed, we will proceed on Configuring Wide Area Network. Same process with Router but this time we will use Modem or the Access Point. See steps listed below:

1. Gather your Modem, Ethernet Cable and Personal Computer. Connect each peripheral using the Ethernet Cable. Directly connect Modem to your Personal Computer using the Ethernet Cable. This will just be use for the setting up processes.

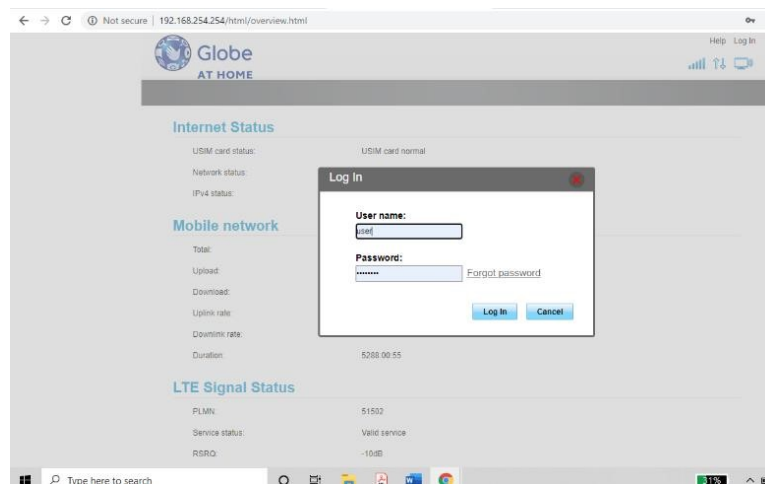


2. Reset the Modem.

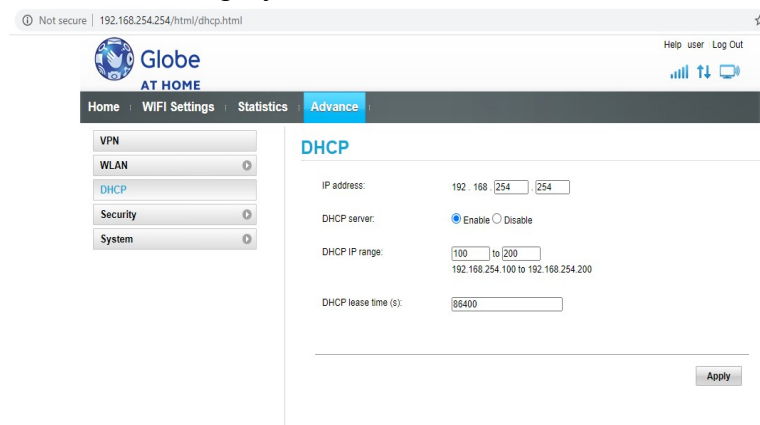


Follow these steps to perform a modem reset:

- a. Press the reset button in and hold it for 15 seconds. You should feel a slight click when you press it. When done correctly, the power light on the modem will start flickering orange/red.
 - b. Wait 3 to 5 minutes. The power light will turn amber and you will need to run through the modem activation process as if setting it up for the first time. You may be asked for account login information to configure your modem.
 - c. When the internet light turns green, you should be able to access the internet.
 - d. Your previously connected devices may not be able to connect until you reenter the network security key (WiFi password) in the wireless settings on each device.
3. Go to browser either "Google Chrome" or "I explorer". And type in the default IP Address of your Modem. It depends on the manufacturer. For this learning material, we will use 192.168.254.254. And a Dialog box will pop up and you will need to enter the default username and password.



4. Repeat the step shown on Configuring your Router.
- a. Go to Network Tab. Change your IP address. Click Save then it will reboot.



b. Go to DHCP tab and click Disable Button.

The screenshot shows the DHCP configuration page. On the left, a sidebar contains links for VPN, WLAN, DHCP (selected), Security, and System. The main content area is titled 'DHCP' and includes the following settings:

- IP address: 192.168.254.254
- DHCP server: ☐ Enable ☒ Disable
- DHCP IP range: 100 to 200 (with a note: 192.168.254.100 to 192.168.254.200)
- DHCP lease time (s): 86400

An 'Apply' button is located at the bottom right of the settings area.

c. Unlike on Router we need to set up Wireless Tab on Modem. Click Wireless Tab. Click on WPA/WPA2 – Personal (Recommended) then enter your desired PSK Password. It must consist of alphanumeric characters. The browser will reboot.

The screenshot shows the 'WLAN Basic Settings' page. The left sidebar has links for VPN, WLAN (selected), WLAN Basic Settings (selected), WLAN Advanced Settings, WLAN MAC Filter, WPS Settings, DHCP, Security, and System. The main content area is titled 'WLAN Basic Settings' and includes the following settings:

- WLAN module: ☒ Enable ☐ Disable
- SSID: Mylab2
- Security mode: WPA/WPA2-PSK
- WLAN key: [password field]
- Show password: ☐
- SSID broadcast: ☒ Enable ☐ Disable

A note at the bottom states: 'Note: If SSID broadcast is disabled, you must enter a valid SSID to connect to a Wi-Fi network. For details, see the [help](#).' 'Apply' and 'Cancel' buttons are at the bottom right.

SSID	Security mode	Status	Options
Mylab2	WPA/WPA2-PSK	On	Edit
HUAWEI-B315-302D-1	WPA/WPA2-PSK	Off	Edit
HUAWEI-B315-302D-2	WPA/WPA2-PSK	Off	Edit
HUAWEI-B315-302D-3	WPA/WPA2-PSK	Off	Edit

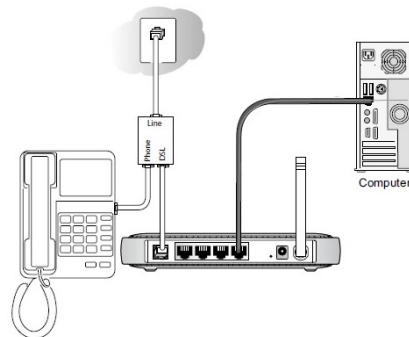
Configure Wireless Setting

After configuring the Router and Modem we will now proceed on setting up the wireless network.

1. First, we need to check whether you have a wireless adapter.
 - a. Select the Start button, type Device Manager in the search box, and then select Device Manager.
 - b. Expand Network adapters.
 - c. Look for a network adapter that might have wireless in the name.

2. Setting up the modem and Internet connection

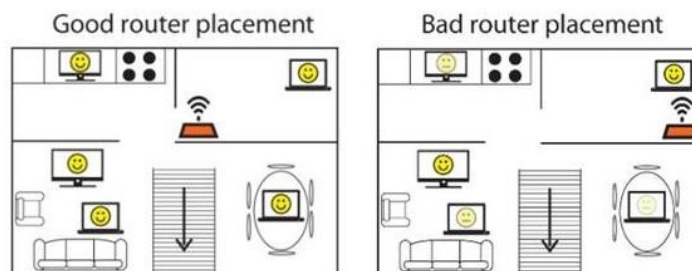
After you have all the equipment, you'll need to set up your modem and Internet connection. If your modem wasn't set up for you by your Internet service provider (ISP), follow the instructions that came with your modem to connect it to your PC and the Internet. If you're using Digital Subscriber Line (DSL), connect your modem to a phone jack. If you're using cable, connect your modem to a cable jack.



3. Positioning the wireless router

Put your wireless router somewhere where it will receive the strongest signal with the least amount of interference. For better results, follow these tips:

- a. Place your wireless router in a central location. Place the router as close to the center of your home as possible to increase the strength of the wireless signal throughout your home.



- b. Position the wireless router off the floor and away from walls and metal objects, such as metal file cabinets. The fewer physical obstructions between your PC and the router's signal, the more likely that you'll be using the router's full signal strength.

- c. Place your wireless device's antennas. Do not to place all the antennas straight upward but at an angle against the horizontal line.



Stay away from high-powered appliances. When the router transmitting signals, the high-power electrical appliances and iron products may cause interference to Wi-Fi, so try to avoid microwave oven, weak current box, TV and other electrical appliances.

- d. It is better to place the wireless router on a table or shelf and keep it at a certain height so that the omnidirectional antenna's transmitting ability can be utilized.

Securing Your Wireless Network

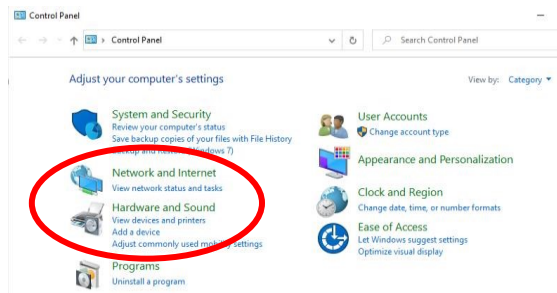
Security is always important; with a wireless network, it's even more important because your network's signal could be broadcast outside your home. If you don't help secure your network, people with PCs nearby could access info stored on your network PCs and use your Internet connection.

To help make your network more secure:

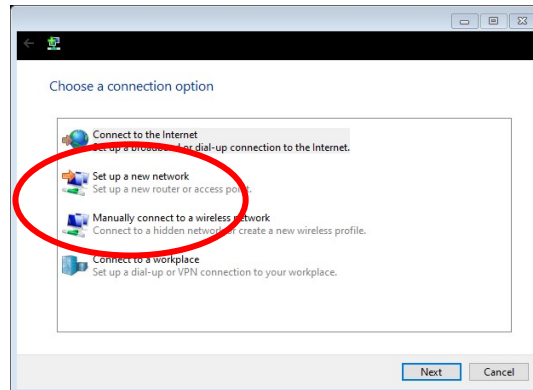
- Change the default user name and password. This helps protect your router. Most router manufacturers have a default user name and password on the router and a default network name (also known as the SSID). Someone could use this info to access your router without you knowing it. To help avoid that, change the default user name and password for your router.
- Set up a security key (password) for your network. Wireless networks have a network security key to help protect them from unauthorized access. We recommend using Wi-Fi Protected Access 2 (WPA2) security if your router supports it.

Some routers support Wi-Fi Protected Setup (WPS). If your router supports WPS and its connected to the network, follow these steps to set up a network security key:

1. Select the **Start** button, look for Control Panel and click **Network and Internet**. Then look for Network and Sharing Center.



2. Select Set up a new connection or network.



3. Select **Set up a new network**, and then choose **Next**.

The wizard will walk you through creating a network name and a security key. If your router supports it, the wizard will default to Wi-Fi Protected Access (WPA or WPA2) security. We recommend that you use WPA2, because it offers better security than WPA or Wired Equivalent Privacy (WEP) security. With WPA2 or WPA you can also use a passphrase, so you don't have to remember a cryptic sequence of letters and numbers.

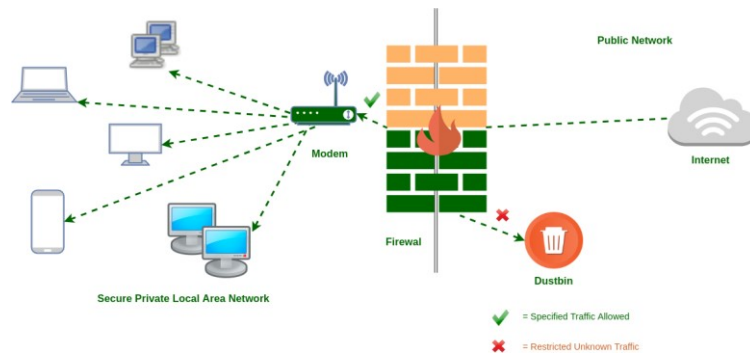
Connect a PC to your wireless network

1. Select the **Network** or icon in the notification area.
2. In the list of networks, choose the network that you want to connect to, and then select **Connect**.
3. Type the security key (often called the password).
4. Follow additional instructions if there are any.

Information Sheet:1.5

Setting Up Firewall with Advanced Setting

A firewall is hardware or software that can help protect your PC from unauthorized users or malicious software (malware). Running a firewall on each PC on your network can help control the spread of malicious software on your network, and help protect your PCs when you're accessing the Internet.



Port Protection

Every communication using TCP/IP is associated with a port number. HTTPS, for instance, by default uses port 443. A firewall is a way of protecting a computer from intrusion through the ports.

With port protection, the user can control the type of data sent to a computer by selecting which ports will be open and which will be secured. Data being transported on a network is called traffic.

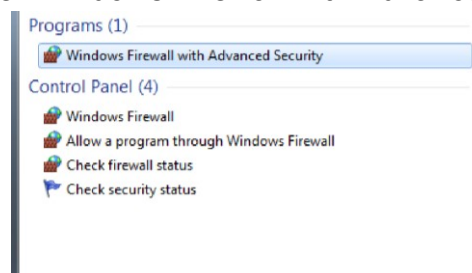
Setting Up Firewall with Advanced Security

You have several alternatives to opening the Windows Firewall with Advanced Security:

1. One is to open the standard Windows Firewall window, by going to "Control Panel > System and Security -> Windows Firewall". Then, click or tap Advanced settings.

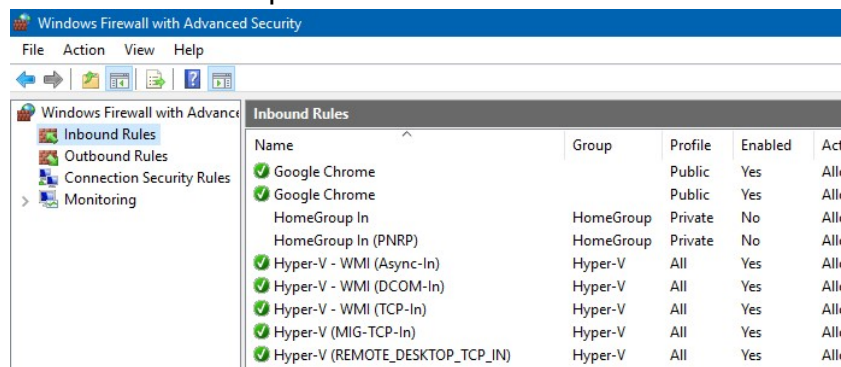


2. In Windows 7, another method is to search for the word firewall in the Start Menu search box and click the "Windows Firewall with Advanced Security" result.

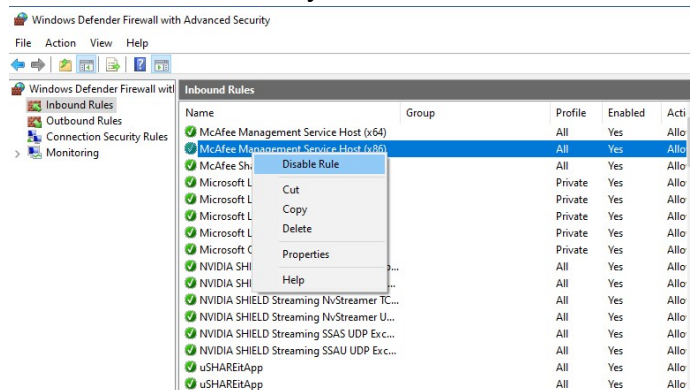


3. In Windows 8.1, Windows Firewall with Advanced Security is not returned in search results and you need to use the first method shared above for opening it.
4. In Windows 10, you can use either of the 2 methods.
5. What Are The Inbound & Outbound Rules?

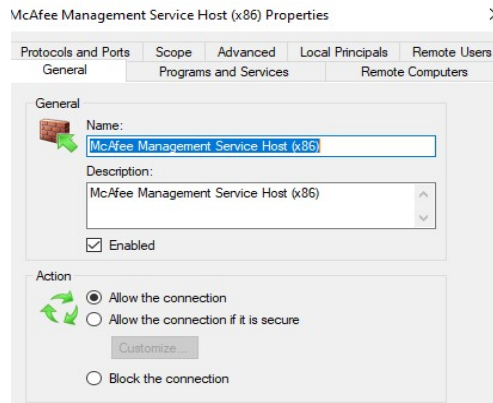
- a. In order to provide the security you need, the Windows Firewall has a standard set of inbound and outbound rules, which are enabled depending on the location of the network you are connected to.
- b. Inbound rules are applied to the traffic that is coming from the network and the Internet to your computer or device. Outbound rules apply to the traffic from your computer to the network or the Internet.
- c. These rules can be configured so that they are specific to: computers, users, programs, services, ports or protocols. You can also specify to which type of network adapter (e.g. wireless, cable, virtual private network) or user profile it is applied to.
- d. In the Windows Firewall with Advanced Security, you can access all rules and edit their properties. All you have to do is click or tap the appropriate section in the left-side panel.



6. The rules used by the Windows Firewall can be enabled or disabled. The ones which are enabled or active are marked with a green check-box in the Name column. The ones that are disabled are marked with a gray check-box.
7. If you want to know more about a specific rule and learn its properties, right click on it and select Properties or select it and press Properties in the column on right, which lists the actions that are available for your selection.



8. In the Properties window, you will find complete information about the selected rule, what it does and in when it is applied. You will also be able to edit its properties and change any of the available parameters.



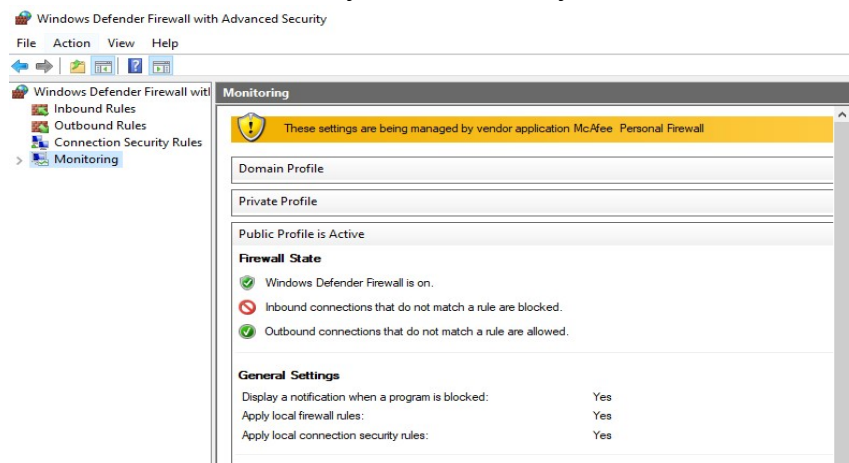
9. What Are The Connection Security Rules?

- Connection security rules are used to secure traffic between two computers while it crosses the network. One example would be a rule which defines that connections between two specific computers must be encrypted.
- Unlike the inbound or outbound rules, which are applied only to one computer, connection security rules require that both computers have the same rules defined and enabled.
- If you want to see if there are any such rules on your computer, click or tap "Connection Security Rules" on the panel on the left. By default, there are no such rules defined on Windows computers and devices. They are generally used in business environments and such rules are set by the network administrator.



10. What Does the Windows Firewall with Advanced Security Monitor?

The Windows Firewall with Advanced Security includes some monitoring features as well. In the Monitoring section you can find the following information: the firewall rules that are active (both inbound and outbound), the connection security rules that are active and whether there are any active security associations.



- You should note that the Monitoring section shows only the active rules for the current network location. If there are rules which get enabled for other network locations, you will not see them in this section.