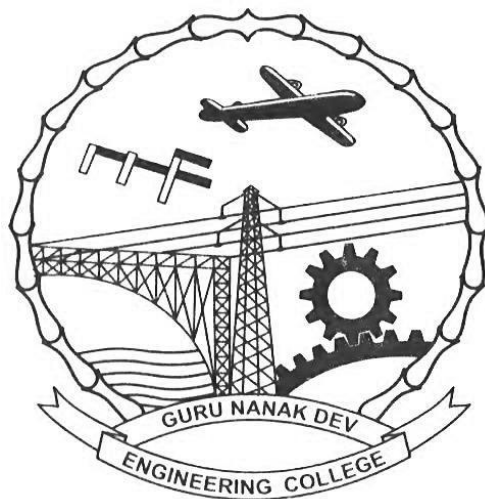


# **INSTRUCTION MANUAL**

## **Computer Networks-II LAB (BTCS-507)**



**Prepared by**

**Er. Mandeep Kaur**  
**Assistant Professor (CSE)**

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**

**GURU NANAK DEV ENGINEERING COLLEGE**

**LUDHIANA – 141006**

## **DECLARATION**

This Manual of Computer Networks-II Lab (BTCS-507) has been prepared by me as per syllabus of Computer Networks-II Lab (BTCS-507).

**Signature**

# Syllabus

1. To configure the IP address for a computer connected to LAN and to configure network parameters of a web browser for the same computer.
2. To plan IPv6 address scheme for a local area network comprising of 'n' terminals.
3. To develop programs for implementing / simulating routing algorithms for Adhoc networks.
4. To install any one open source packet capture software like Wireshark etc.
5. To configure Wireless Local Loop.
6. To plan Personal Area Network.
7. To configure WLAN.
8. To configure Adhoc networks.
9. To install and configure wireless access points.

# INDEX

<b>S.No</b>	<b>PRACTICAL Name</b>	<b>Page.No.</b>
<b>1</b>	To configure the IP address for a computer connected to LAN	1
	To configure network parameters of a web browser.	7
<b>3</b>	To Configuring a Wireless Access Point	11
<b>4</b>	To configure Personal Area Network	13
<b>5</b>	To plan IPv6 address scheme for a local area network comprising of 'n' terminals.	17
<b>6</b>	To install any one open source packet capture software like Wireshark	21
<b>7</b>	To configure Wireless Local Loop	33
<b>8</b>	To Configure Ad Hoc Wireless Network.	39
<b>9</b>	To Configure WLAN.	47

## **PRACTICAL 1: To configure the IP address for a computer connected to LAN**

It is very important to setup a static ip address, if you are going to use port forwarding. When you have port forwarding setup, your router forwards ports to an ip address that you specify. This will probably work when you initially set it up, but after restarting your computer it may get a different ip address. When this happens the ports will no longer be forwarded to your computer's ip address. So the port forwarding configuration will not work.

### **What is an ip address?**

IP addresses are four sets of numbers separated by periods that allow computers to identify each other. Every computer has at least one ip address, and two computers should never have the same ip address. If they do, neither of them will be able to connect to the internet.

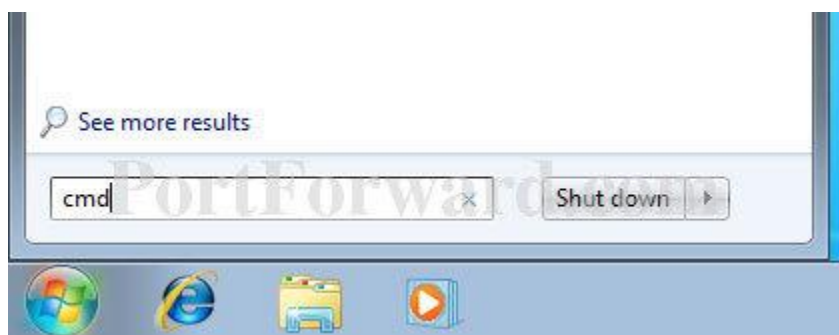
**Dynamic vs Static IPs** Most routers assign dynamic IP addresses by default. They do this because dynamic ip address networks require no configuration. The end user can simply plug their computer in, and their network will work. When ip addresses are assigned dynamically, the router is the one that assigns them. Every time a computer reboots it asks the router for an ip address. The router then hands it an ip address that has not already been handed out to another computer. This is important to note. When you set your computer to a static ip address, the router does not know that a computer is using that ip address. So the very same ip address may be handed to another computer later, and that will prevent both computers from connecting to the internet. So when you assign a static IP addresses, it's important to assign an IP address that will not be handed out to other computers by the dynamic IP address server. The dynamic IP address server is generally referred to as the dhcp server.

### **Setting up a static IP for Windows**

If you have a printer, before you begin print out this page!

Step 1:

Open up the start menu, and look for the *Search programs and files* box. You should now see the following window.



Step 2:

Type **cmd** in the *Search programs and files* box, and press **Enter** on your keyboard. This will bring up a black command prompt window.

```
C:\ C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\user>cd\..
C:\>ipconfig/all_
```

Step 3:

The command prompt may look different on your screen, but it doesn't really matter. Type **ipconfig /all** in that window, and then press the **enter** key. This will display a lot of information. If it scrolls off the top you may need to enlarge the window.

```
C:\ C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\user>cd\..
C:\>ipconfig/all
Windows IP Configuration
    Host Name . . . . . : bbsbec_183
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Broadcast
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . : CSE NETWORKS
    Description . . . . . : Broadcom NetXtreme 57xx Gigabit Controller
    Physical Address. . . . . : 00-1D-09-08-41-69
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 172.16.1.191
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 172.16.0.1
    DHCP Server . . . . . : 172.16.13.1
    Lease Obtained. . . . . : Wednesday, July 24, 2013 12:21:28 PM
    Lease Expires . . . . . : Wednesday, July 24, 2013 1:21:28 PM

C:\>
```

#### Step 4:

Select a unique IP for the PC of 192.168.1.# where # is in the range 2-99 or 150-254 (this avoids any conflict with the default DHCP address range of 100-149). Example: 192.168.1.5

I want you to write down some of the information in this window. Take down the IP address, Subnet Mask, Default Gateway, and Name Servers. Make sure to note which is which. We are going to use this information a little bit later. We are only concerned with IPv4 entries, you can ignore the IPv6 stuff.

The name server entries are a bit complicated. Name Server is just another name for DNS(domain name server) server. Some router's act as a proxy between the actual name servers and your computer. You will know when this is the case, because the Default Gateway will list the same ip address as the Name Servers entry. We need to have the correct Name Server IP addresses. If we do not, you will not be able to browse the web. There are a couple ways to get these. The first way is to log into your router's web interface, and look at your router's status page. On that page you should see an entry for DNS Servers, or Name Servers. Write down the ipaddresses of your Name Servers. Another way to get the correct Name Servers to use, is to give your ISP a call. They should know the ip addresses of your Name Servers right off. If they ask you why you need them, you can tell them you are trying to setup a static IP address on your computer. If they try to sell you a static external ip address, don't buy it. That's an entirely different thing that what you are trying to setup.

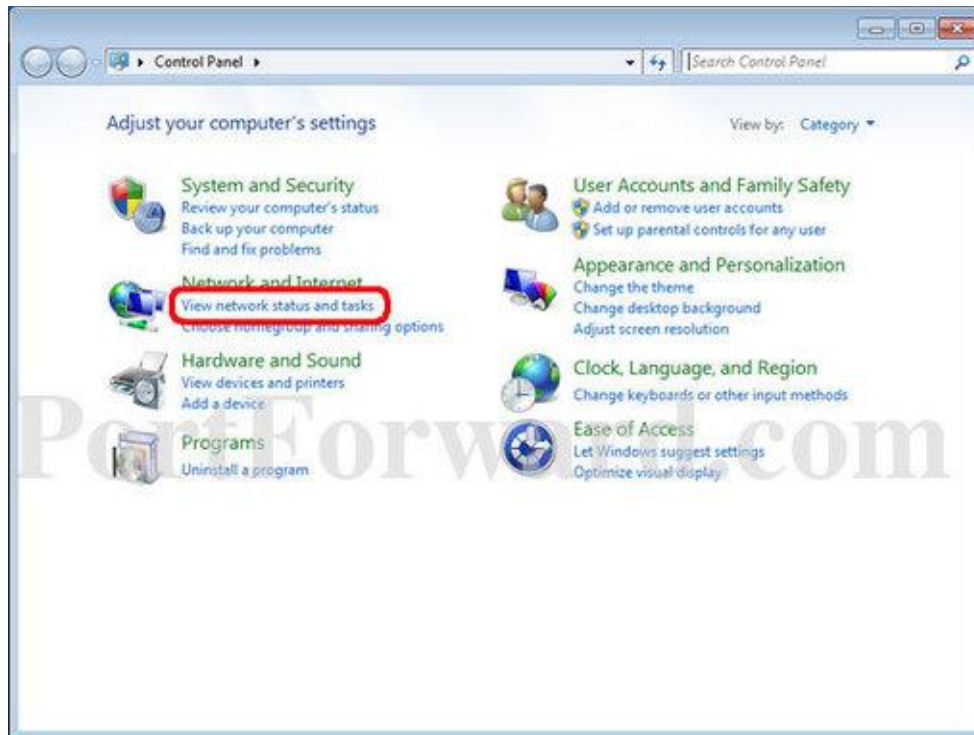
Type **exit** in this window, then press the **enter** key to close it.

#### Step5:

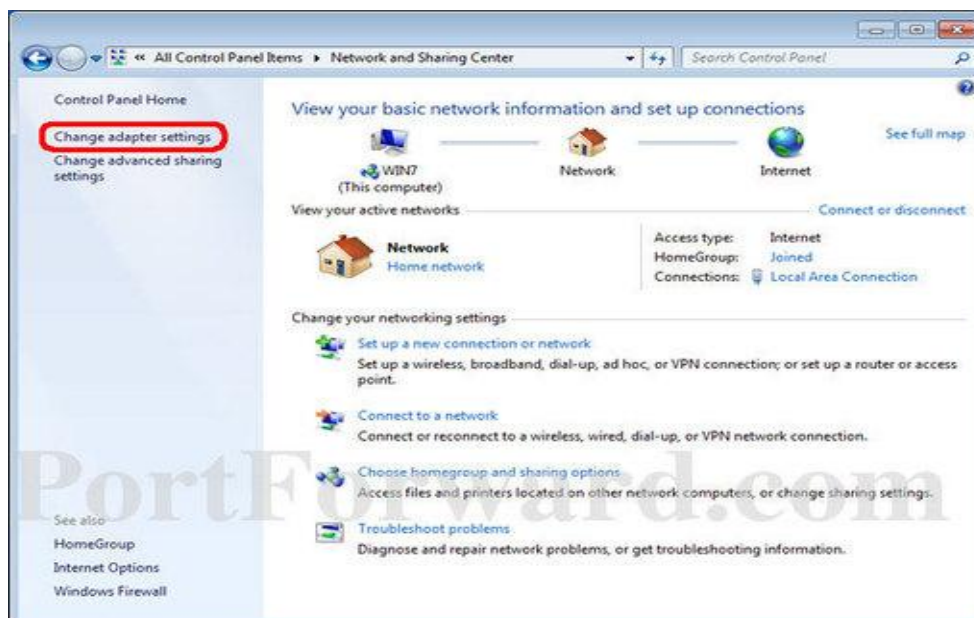
Once again open the start menu. This time click **Control Panel**.



Step 6:  
Click on **View Network Status and Tasks**.



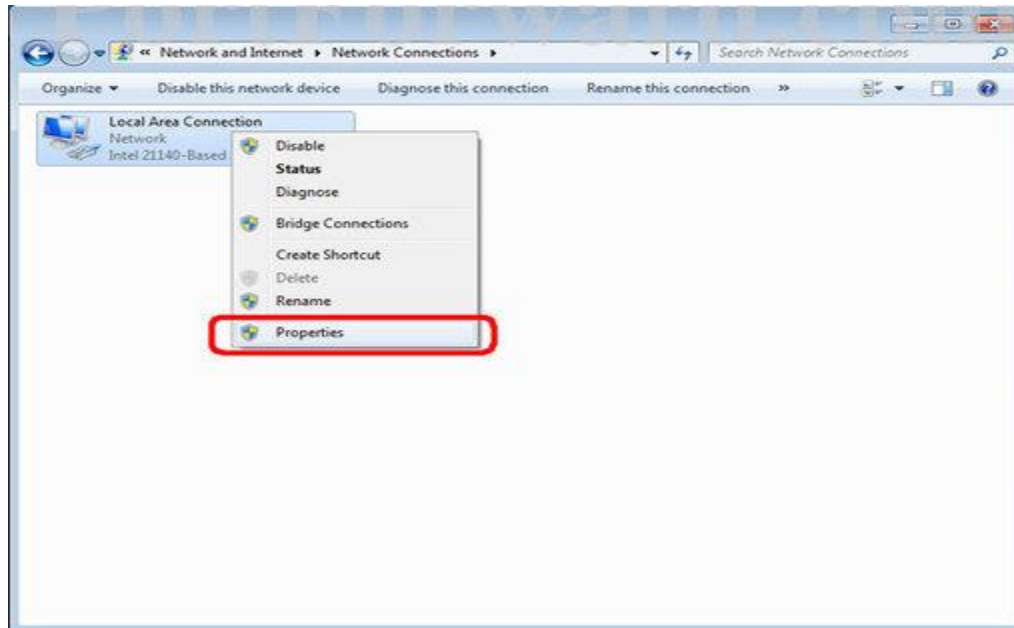
Step 7:  
Single click **Change adapter settings** on the left side of your screen.





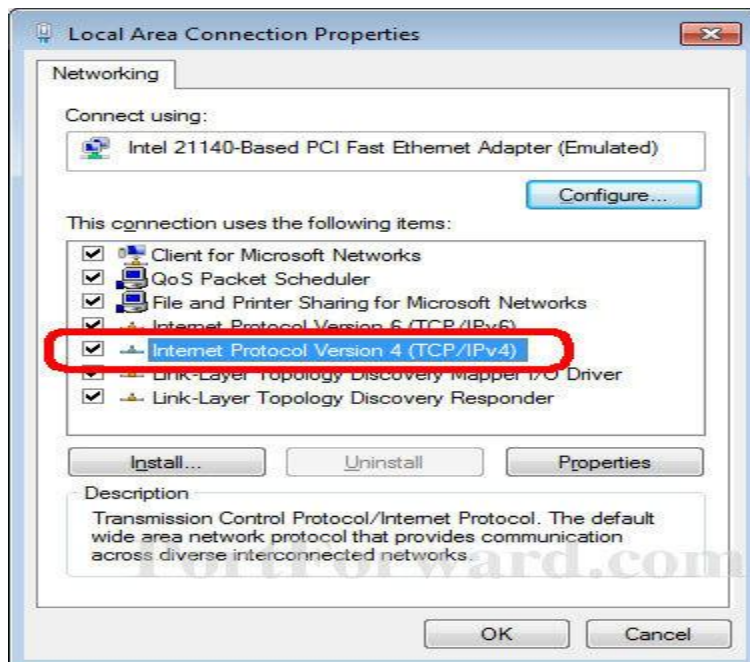
Step8:

You might have more than one Internet connection listed here. You will need to determine which adapter is your connection to the Internet if this is the case. Right click on your network adapter and choose **properties** to open up the properties window of this internet connection.

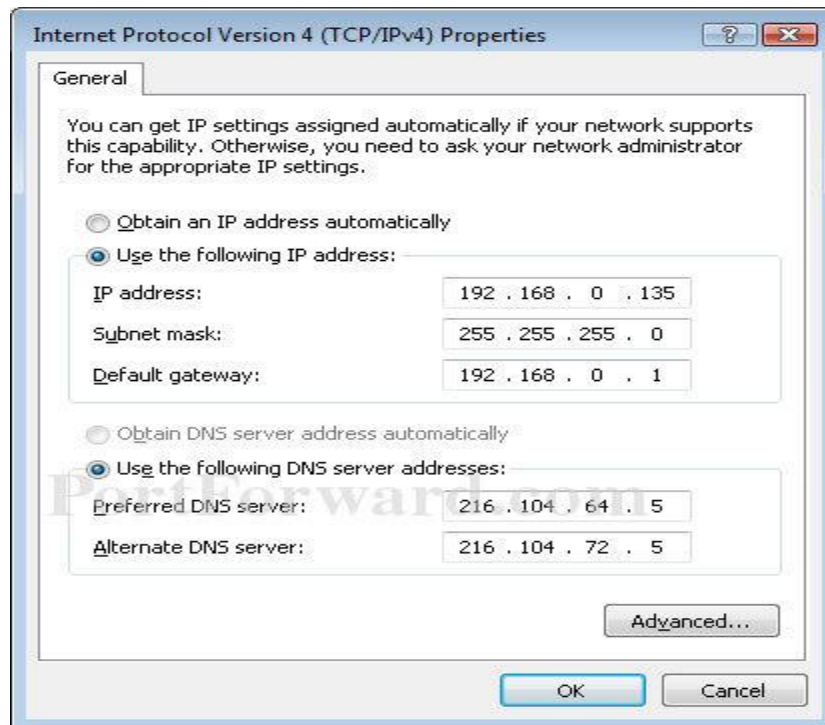


Step 9:

Click **Internet Protocol Version 4(TCP/IPv4)** and then the **Properties** button.



You will see the following screen:



#### Step10:

Before you make any changes, write down the settings that you see on this page. If something goes wrong you can always change the settings back to what they were! You should see a dot in the **Obtain an IP address automatically** box. If you do not, your connection is already setup for a static ip. Just close all these windows and you are done.

Put the subnet mask we previously found in the **subnet mask** section. The default gateway should go into the **Default gateway** box. Enter the dns servers we prevoiusly found into the two **DNS Server** boxes. Click okay all the way out of this menu.

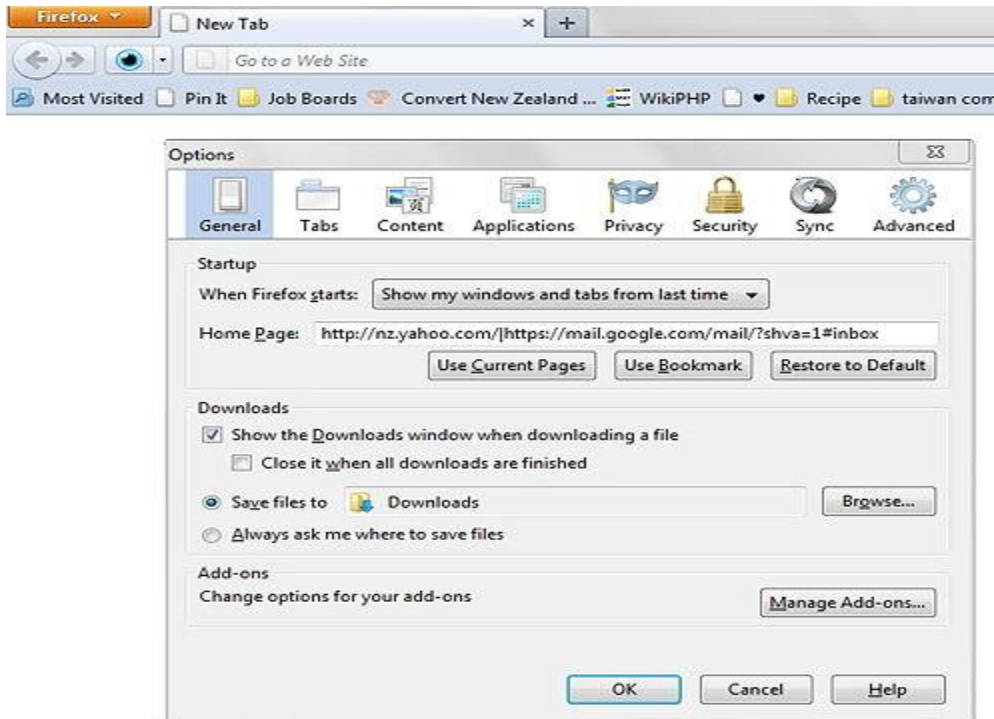
If you find that you can not pull up webpages, the problem is most likely the dns numbers you entered. Give your ISP a call, and they will be able to tell you which dns servers to use. This is a question they answer all of the time. They will be able to tell you what you should use right away.

That's it you should be done! If you can't connect to the internet go back and change your configuration back to what it originally was.

## PRACTICAL 2: To configure network parameters of a web browser

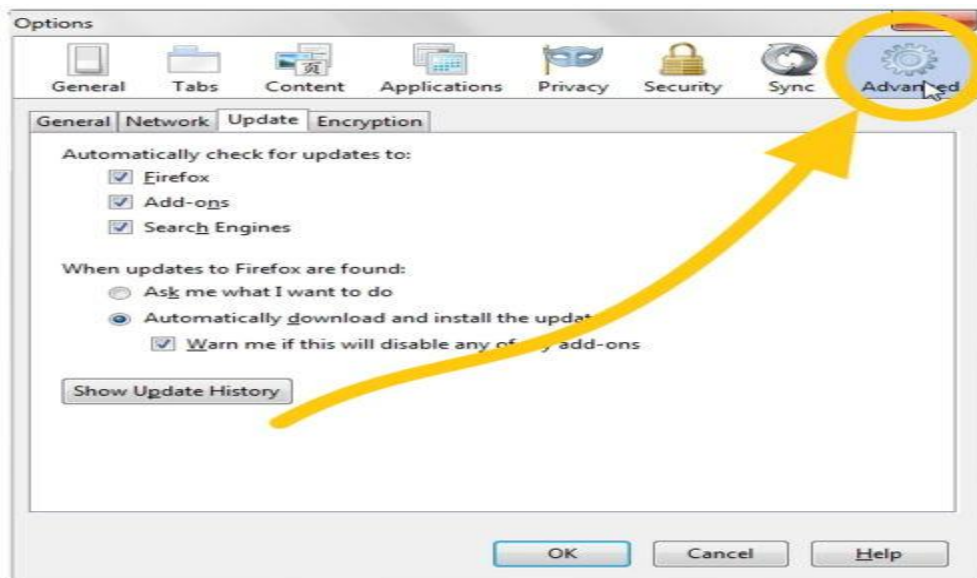
- 1

Open the browser and select Mozilla Firefox Options under the tools tab.

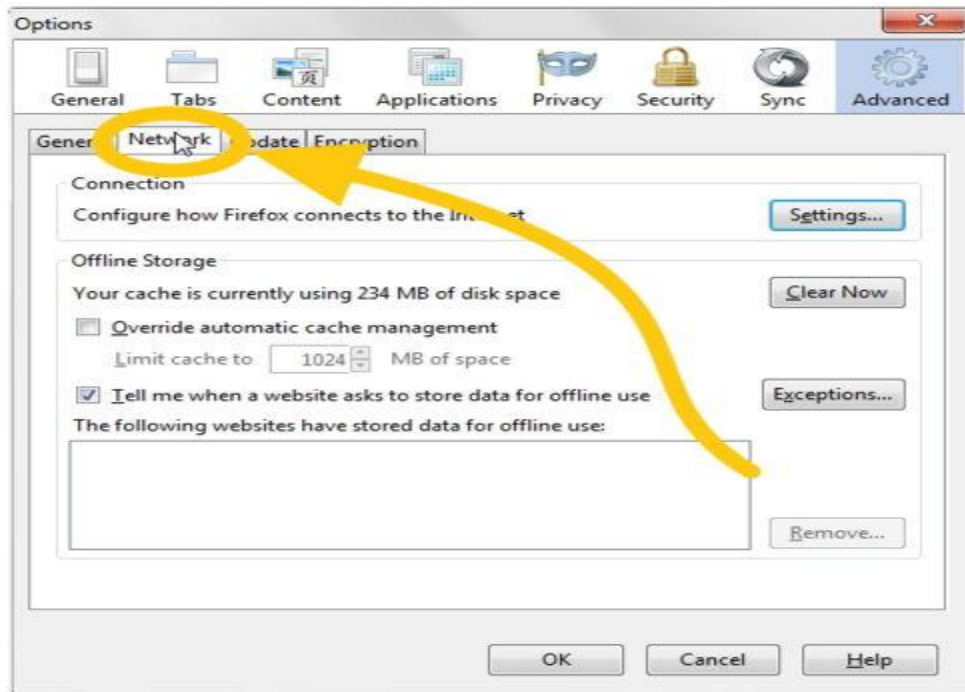


- 2

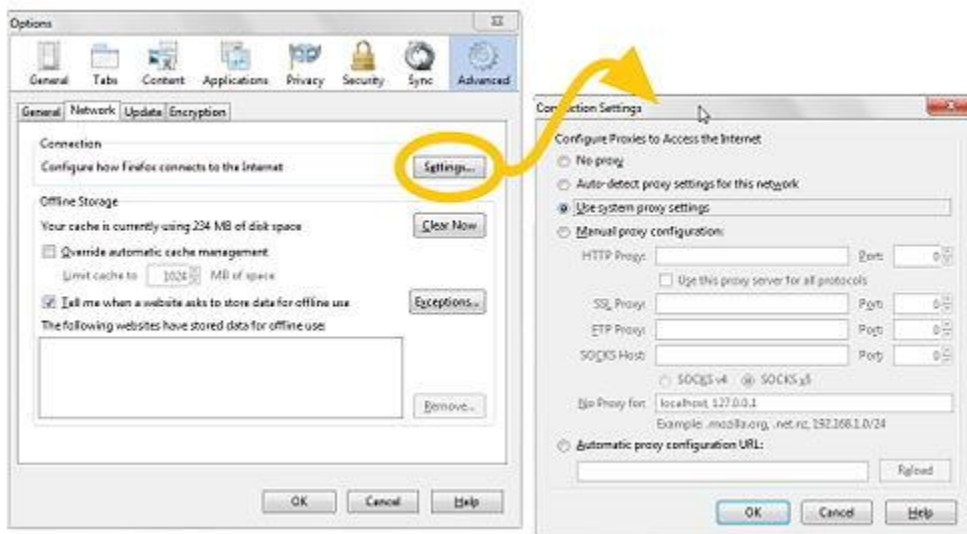
Click on the Advanced category.



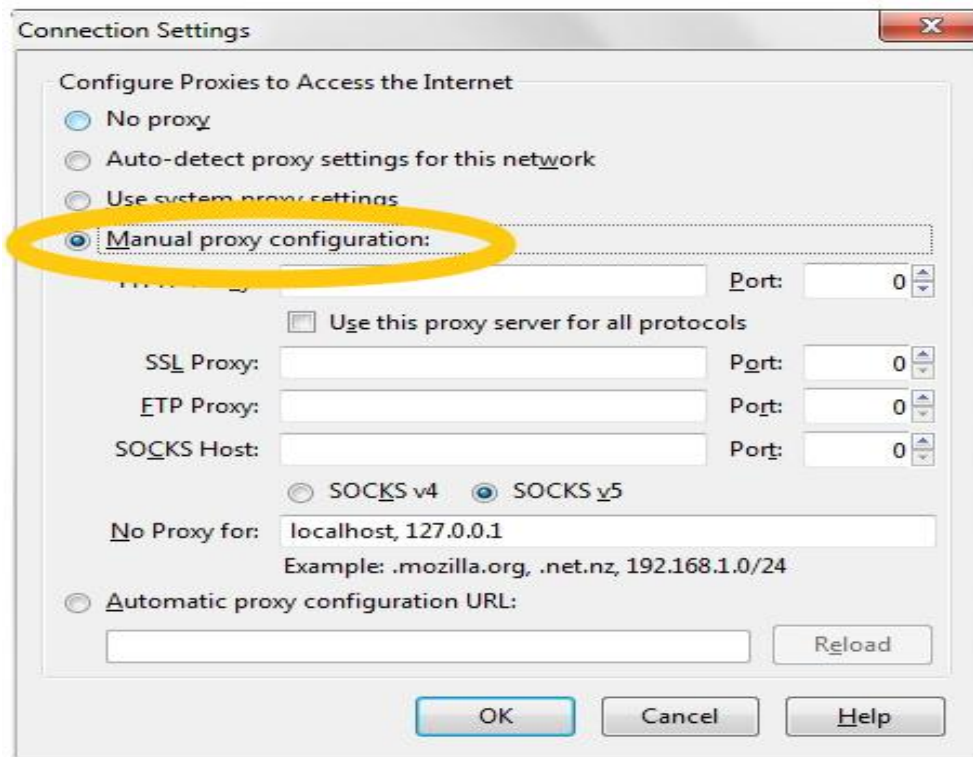
- 3 Click on Network tab.



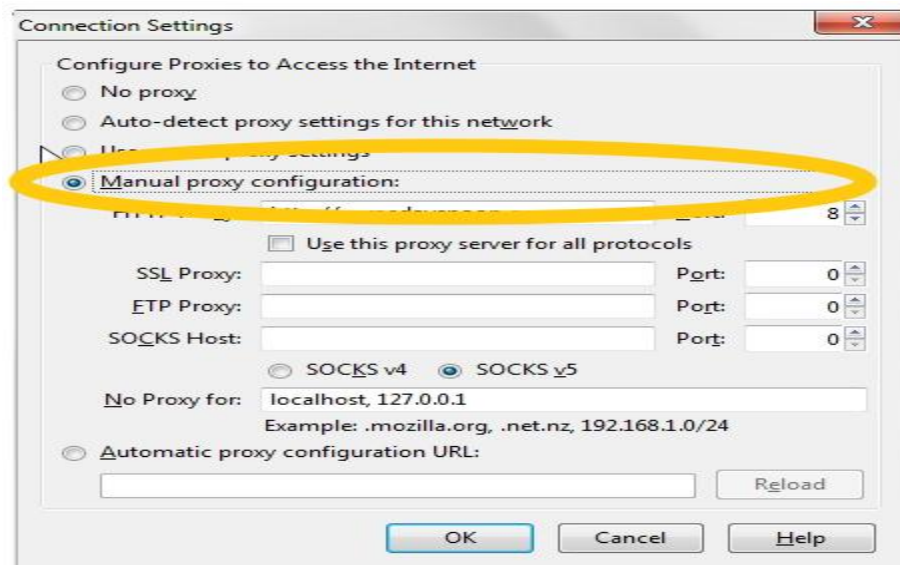
- 4 Click Settings under Connection.



- 5  
**Check Manual proxy configuration.**

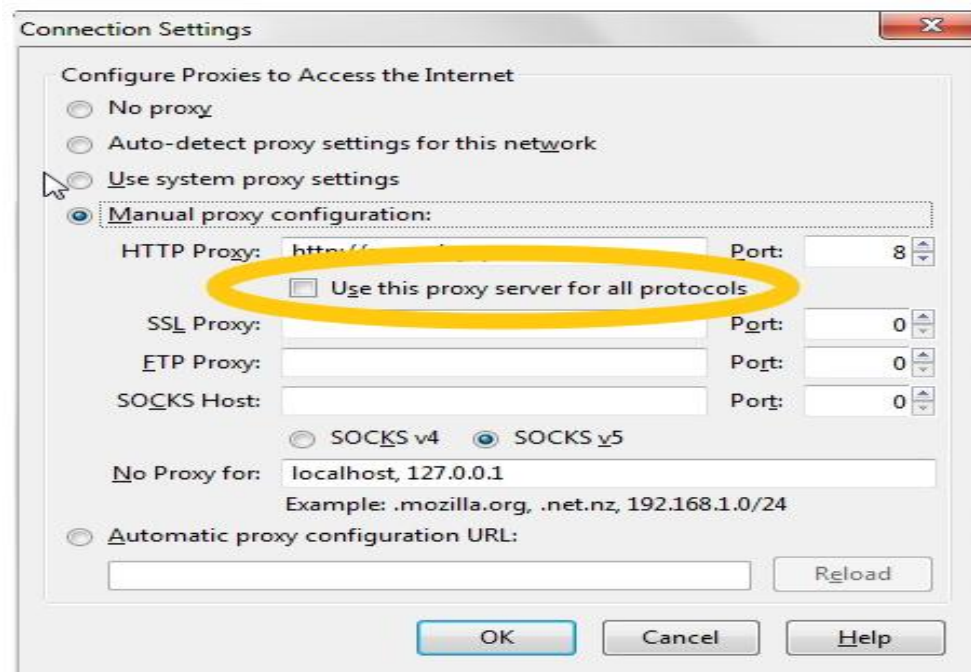


- 6  
**Enter proxy server IP address and port number.**



- 7

If you want, check the box that says Use this proxy server for all protocols.



## PRACTICAL 3: To Configuring a Wireless Access Point

The physical setup for a wireless access point is pretty simple: You take it out of the box, put it on a shelf or on top of a bookcase near a network jack and a power outlet, plug in the power cable, and plug in the network cable.

The software configuration for an access point is a little more involved, but still not very complicated. It's usually done via a Web interface. To get to the configuration page for the access point, you need to know the access point's IP address. Then, you just type that address into the address bar of a browser from any computer on the network.

Multifunction access points usually provide DHCP and NAT services for the networks and double as the network's gateway router. As a result, they typically have a private IP address that's at the beginning of one of the Internet's private IP address ranges, such as 192.168.0.1 or 10.0.0.1. Consult the documentation that came with the access point to find out more.

### Basic configuration options:

When you access the configuration page of your wireless access point on the Internet, you have the following configuration options that are related to the wireless access point functions of the device. Although these options are specific to this particular device, most access points have similar configuration options.

- **Enable/Disable:** Enables or disables the device's wireless access point functions.
- **SSID:** The Service Set Identifier used to identify the network. Most access points have well-known defaults. You can talk yourself into thinking that your network is more secure by changing the SSID from the default to something more obscure, but in reality, that only protects you from first-grade hackers. By the time most hackers get into the second grade, they learn that even the most obscure SSID is easy to get around. So leave the SSID at the default and apply better security measures.
- **Allow broadcast SSID to associate?** Disables the access point's periodic broadcast of the SSID. Normally, the access point regularly broadcasts its SSID so that wireless devices that come within range can detect the network and join in. For a more secure network, you can disable this function. Then, a wireless client must already know the network's SSID in order to join the network.
- **Channel:** Lets you select one of 11 channels on which to broadcast. All the access points and computers in the wireless network should use the same channel. If you find that your network is frequently losing connections, try switching to another channel. You may be experiencing interference from a cordless phone or other wireless device operating on the same channel.
- **WEP — Mandatory or Disable:** Lets you use a security protocol called *wired equivalent privacy*.



## DHCP configuration

You can configure most multifunction access points to operate as a DHCP server. For small networks, it's common for the access point to also be the DHCP server for the entire network. In that case, you need to configure the access point's DHCP server. To enable DHCP, you select the Enable option and then specify the other configuration options to use for the DHCP server.

Larger networks that have more demanding DHCP requirements are likely to have a separate DHCP server running on another computer. In that case, you can defer to the existing server by disabling the DHCP server in the access point.

## Set Up a Wireless Router as an Access Point on a Network

These instructions explain how to set up a NETGEAR wireless router as an access point on a network with another router (the main router).

### To set up the second router as an access point:

**STEP 1.** Connect a computer to one of the LAN (not WAN) Ethernet ports at the back of the router.

**STEP 2.** Access the router menu by opening a browser and typing in the address bar [www.routerlogin.com](http://www.routerlogin.com) or [www.routerlogin.net](http://www.routerlogin.net).

**STEP 3.** Type in the user name *admin* and the password (the default is *password* in lower-case letters).

**STEP 4.** Click the Advanced tab and then select **Setup > LAN**.

**STEP 5.** In the IP Address field, change the LAN IP address of the router to 192.168.1.100 (same IP segment of the main router, 192.168.1.1) and clear the **DHCP server** check box. Then click **Apply**.

**STEP 6.** Select Wireless Setup, and specify the wireless settings that you require (SSID, Channel, Security).

**STEP 7.** Connect the router that you just set up as an access point to one of the available *Ethernet* ports of the other router in the network (the main router). Power cycle both of the routers. The second router now is set up and connected to function as an access point.



## PRACTICAL 4: To configure Personal Area Network

A private network is one which either does not connect to the internet, or is connected indirectly using NAT (Network Address Translation) so its addresses do not appear on the public network. However, a private network allows you to connect to other computers that are on the same physical network. This is desirable when you wish to communicate with a group of other computers or share data and internet connectivity is not necessary.

**1 Plan your network.** This is probably the hardest part of setting up a network.

Draw any routers you may be using to separate major portions of your network first. Smaller private networks do not require routers, but may still use them for administrative reasons. Routers are only required if you are planning to a) Divide your network into multiple smaller networks, or b) Allow indirect internet access using NAT. Next, add any switches and hubs. For small networks, only one switch or hub may be necessary.

Draw boxes to represent the computers and lines connecting the devices together. This drawing will serve as your network diagram.

Although diagrams intended only for your own use may use any symbols you desire, use of industry standard symbols make this task simpler and eliminates confusion for others. Typical industry standard symbols are:

- Routers: Circle with four arrows arranged in a cross. Or just a cross if drawing a quick draft.
- Switches: Square or rectangle, with four staggered arrows, two in each direction. Represents the concept of signals being "switched" - relayed only out the port which leads to the intended user based on address.
- Hubs: Same as switch, with a single double-headed arrow. Represents the concept of all signals being blindly repeated out all ports without concern for which port leads to the intended recipient.
- Lines and squares can be used to represent connections leading to computers.
- 2

### Create an address plan

- IPv4 (IP ver. 4) addresses are written like this: xxx.xxx.xxx.xxx (four numbers separated by three dots), in all RFC-1166 compliant countries. Each number ranges from 0 to 255. This is known as "Dotted Decimal Notation" or "Dot Notation" for short. The address is divided into two portions: the network portion and the host portion.

For "Classful" networks, the network and host portions are as follows:  
("n" represents the network portion, "x" represents the host portion)

When the first number is 0 to 126 - **nnn**.xxx.xxx.xxx (ex. 10.xxx.xxx.xxx)  
These are known as "Class A" networks.

When the first number is 128 to 191 - **nnn.nnn**.xxx.xxx (ex. 172.16.xxx.xxx)

These are known as "Class B" networks.

When the first number is 192 to 223 - **nnn.nnn.nnn.xxx** (ex. 192.168.1.xxx)

These are known as "Class C" networks.

When the first number is 224 to 239 - The address is used for multi-casting.

When the first number is 240 to 255 - The address is "experimental".

Multicast & Experimental addresses are beyond the scope of this article. However, do note that because IPv4 does not treat them the same way as other addresses they should not be used.

For simplicity "non-classful networks", sub-netting, and CIDR will not be discussed in this article.

The network portion specifies a network; the host portion specifies an individual device on a network.

For any given network:

- The range of all possible host portion numbers gives the Address Range.  
(ex. 172.16.xxx.xxx the range is 172.16.0.0 to 172.16.255.255)
- The lowest possible address is the Network Address.  
(ex. 172.16.xxx.xxx the network address is 172.16.0.0)  
This address is used by devices to specify the network itself, and **cannot be assigned to any device.**
- The highest possible address is the Broadcast Address.  
(ex. 172.16.xxx.xxx the broadcast address is 172.16.255.255)  
This address is used when a packet is meant for **all** devices on a specific network, and **cannot be assigned to any device.**
- The remaining numbers in the range are the Host Range.  
(ex. 172.16.xxx.xxx the host range is 172.16.0.1 to 172.16.255.254)  
These are the numbers you can assign to computers, printers, and other devices.  
**Host Addresses** are individual addresses within this range.
- Assign network(s). A network, for this purpose, is any group of connections separated by a router.

Your network may not have routers or, if accessing the Internet with NAT, have only one router between your private network and the public internet. If this is your only router, or if you have no routers, your entire private network is considered one network.

Choose a network with a host range large enough to provide an address to each device. Class C networks (ex. 192.168.0.x) allow for 254 host addresses (192.168.0.1 to 192.168.0.254), which is fine if you have no more than 254 devices. But if you have 255 or more devices, you will either need to use a Class B network (ex. 172.16.x.x) or divide your private network into smaller networks with routers.

If additional routers are used, they become "internal routers", the private network becomes a "private intranet", and each group of connections is a separate network requiring its own network address and range. This includes connections between routers, and connections directly from a router to a single device.

For simplicity, the remainder of these steps will assume you have only one network, of 254 or less devices, and uses 192.168.2.x as an example. We will also assume you are not using DHCP (Dynamic Host Control Protocol) to assign host addresses automatically.

- 3  
**Write "192.168.2.x"** in the corner somewhere. If you have more than one network it's best to write each address near the network it belongs to.

- 4  
**Assign host addresses within the range of 1 to 254 to each computer.** Write the host addresses next to the devices they belong to on the diagram. At first you may wish to write the entire address (ex. 192.168.2.5) next to each device. However, as you become more proficient simply writing the host portion (ex. .5) may help save time.

Switches will not require addresses for the purpose discussed here. Routers will require addresses as described in the "Important Notes" section.

- 5  
**Write down the subnet mask near the network address.** For 192.168.2.x, which is a Class C, the mask is: 255.255.255.0 The computer needs it to tell which part of the IP address is the network and which is the host.

IPv4 originally used the first number (ex. 192) to determine this based on the address class, as described above. However, the advent of subnetting and nonclassful networking made it necessary to provide a mask because other ways of dividing the address into network and host portions are now possible. For Class A addresses the mask is 255.0.0.0, for Class B it's 255.255.0.0 (More information in the Important Notes section.)

- 6  
**Connect your network.** Gather all needed materials including cables, computers, ethernet switches, and (if used) routers. Locate the Ethernet ports on the computers and other devices. Look for the 8-pin modular connector. (RJ-45 style) It looks like a standard telephone jack except it's a bit larger because it has more conductors.

Connect the cables between each device, just as in your map. If an unforeseen circumstance causes you to vary from the diagram, make notes to show any changes.

- 7  
**Boot all the computers connected to the network.** Power on all other connected devices. (Some devices have no "power switch" and will power up simply by plugging them in.)

- 8  
**Configure the computers for networking.** Go to internet options (this varies depending on the Operating System), and go to the dialog box that lets you change the TCP/IP protocol. Change the radio buttons from "Obtain from DHCP server automatically" to "Use the following IP address:". Type in your IP address for that computer, and the appropriate subnet mask

(255.255.255.0).

If you have no routers, leave the "Default Gateway" and "DNS server" fields blank.

If connecting to the internet using NAT, use the **Host Address** assigned to the router between your private network and the internet as both the DNS server and the Default Gateway. **Do not use the Network Address (192.168.2.0)**

If using more than one router see the Important Notes section.

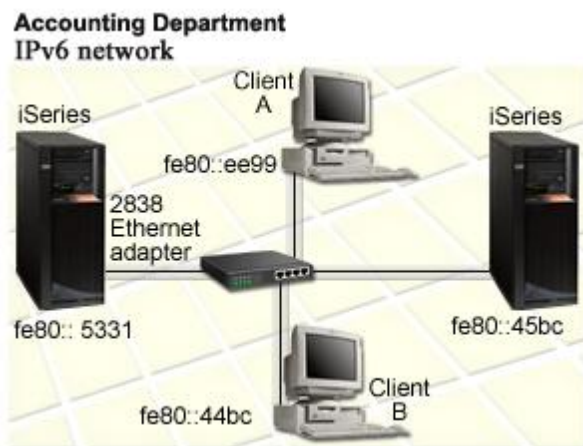
If configuring a home network with a relatively new router, This section can be ignored as long as the network is connected correctly, The router will assign network addresses to everything on the network going into your network, until it hits another router.

- 9

**Verify connectivity.** The simplest way to do this is with Ping. Bring up MS-DOS or the equivalent on other OS's, (In Windows open the command prompt which is located in the Start Menu - Accessories - Command Prompt) and type in: ping 192.168.2.[insert host number here]. Do this on one host and ping to all other hosts. Remember, your router is considered a host. If you cannot reach one, read over the steps again or contact a professional.

## **PRACTICAL 5: To plan IPv6 address scheme for a local area network comprising of 'n' terminals.**

One of the main benefits of Internet Protocol version 6 (IPv6) over previously used Internet Protocol version 4 (IPv4) is the large address-space that contains (addressing) information to route packets for the next generation Internet. IPv6 supports 128-bit address space and can potentially support 2<sup>128</sup> or 3.4W1038 unique IP addresses (as opposed to 32-bit address space of IPv4). With this large address-space scheme, IPv6 has the capability to provide unique addresses to each and every device or node attached to the Internet



To configure an Ethernet line description for IPv6, you must use the IPv6 Configuration wizard in iSeries Navigator. IPv6 may only be configured from iSeries Navigator, and may not be configured from the character-based interface.

The wizard requires the name of the hardware communications resource on the server on which you will configure IPv6; for example, CMN01. This must be either a 2838 or 2849 Ethernet adapter that is not currently configured for IPv4.

To use the IPv6 Configuration wizard, follow these steps:

1. In iSeries Navigator, select your server —> Network —> TCP/IP Configuration.
2. Right-click IPv6, select IPv6 Configuration, and follow the wizard's instructions to configure an Ethernet line for IPv6.

### **Configure ipv6 in windows 7 steps**

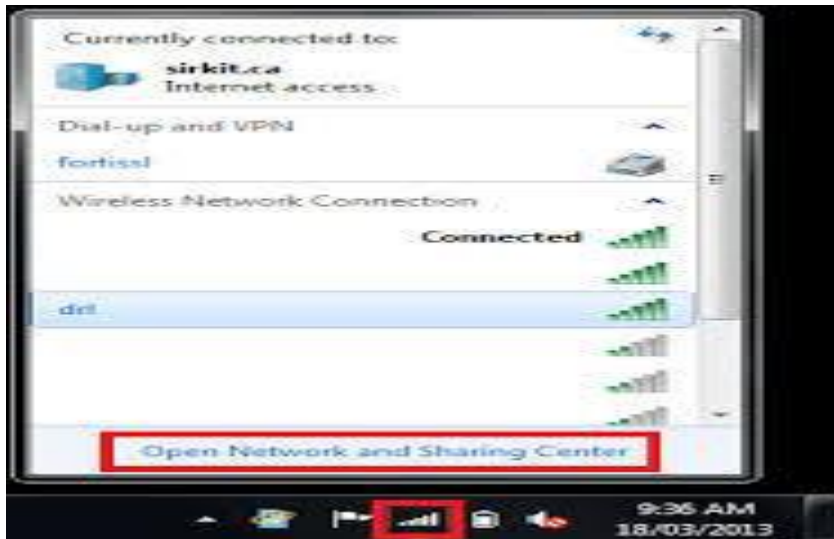
Windows 7 enables IPv6 by default. Should your IPv6 connection not automatically work, try:

1. Right-click the Wi-Fi icon in the system tray and open Network and Sharing Center.
2. Click on the adapter you are using to get a Status window.
3. Click on Properties.
4. Select Internet Protocol Version 6 (TCP/IP) and choose Properties.
5. Choose "Obtain an IPv6 address automatically."
6. Press OK and then close out of the Properties and Network and Sharing Center.

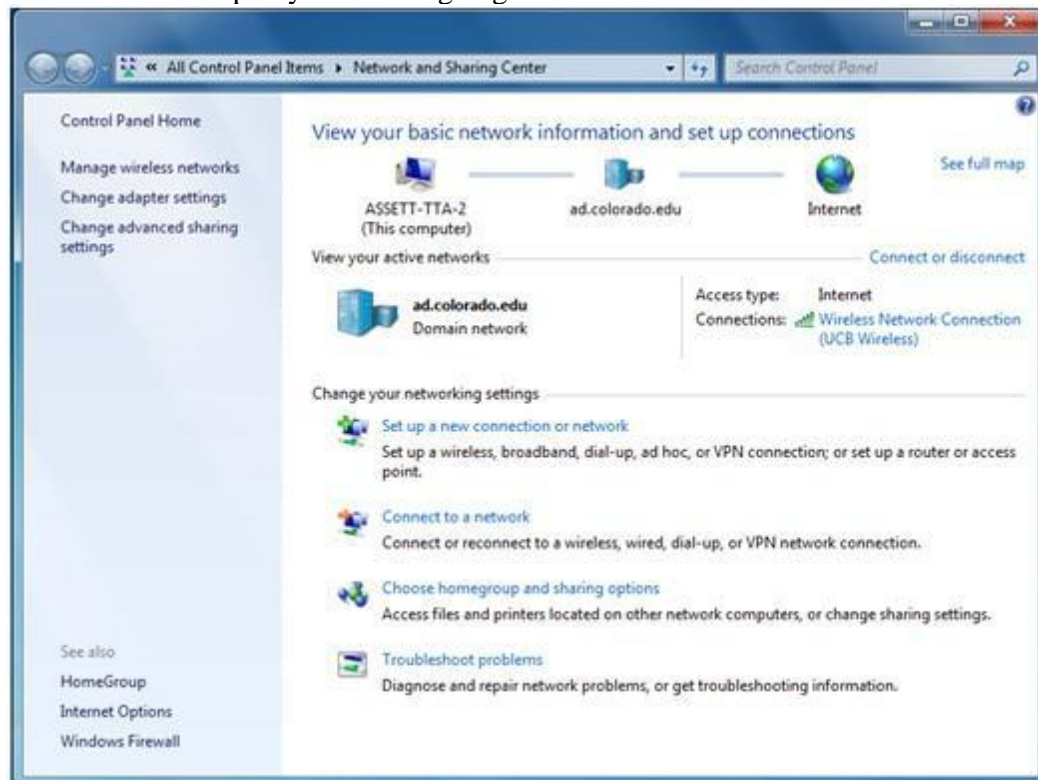
## Microsoft Windows 7

Windows 7 enables IPv6 by default. Should your IPv6 connection not automatically work, try:

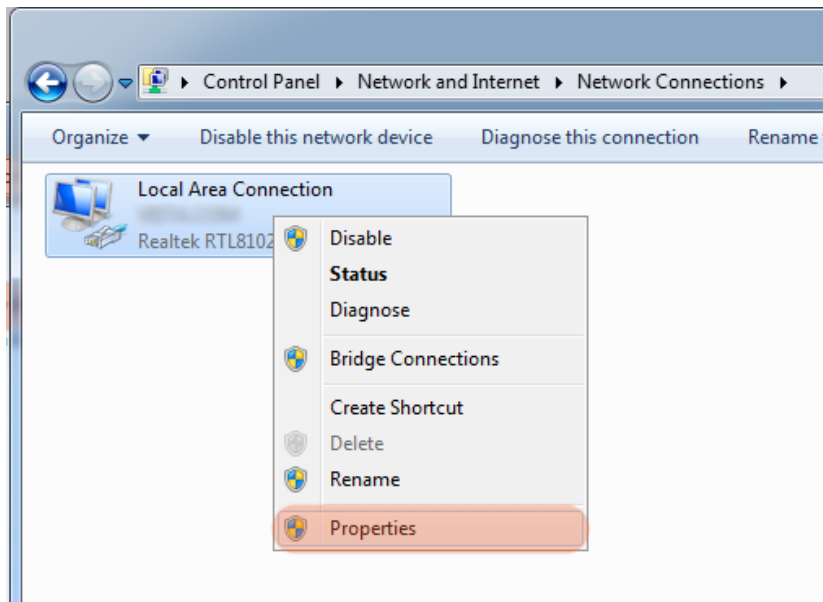
1. Right-click the Wi-Fi icon in the system tray and open *Network and Sharing Center*.



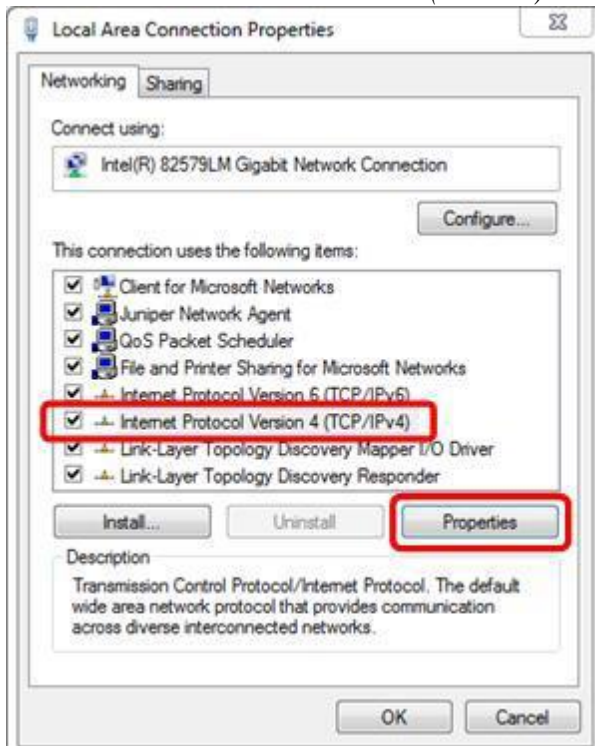
2. Click on the adapter you are using to get a Status window.



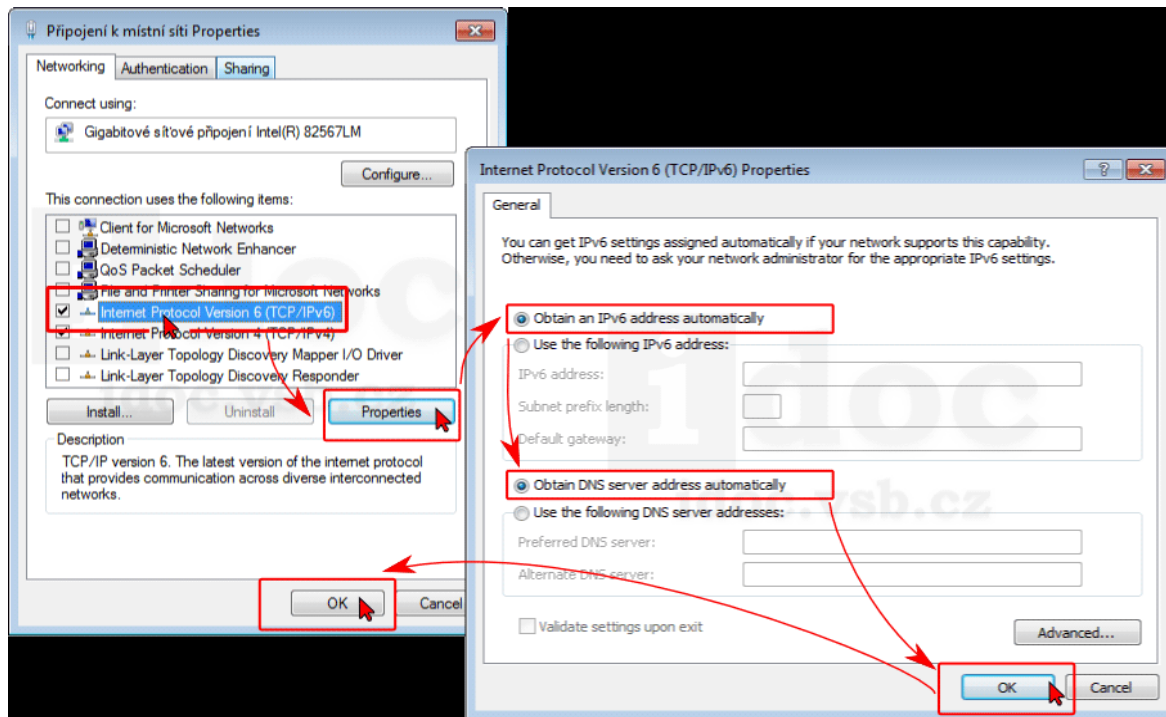
3. Click on Properties.



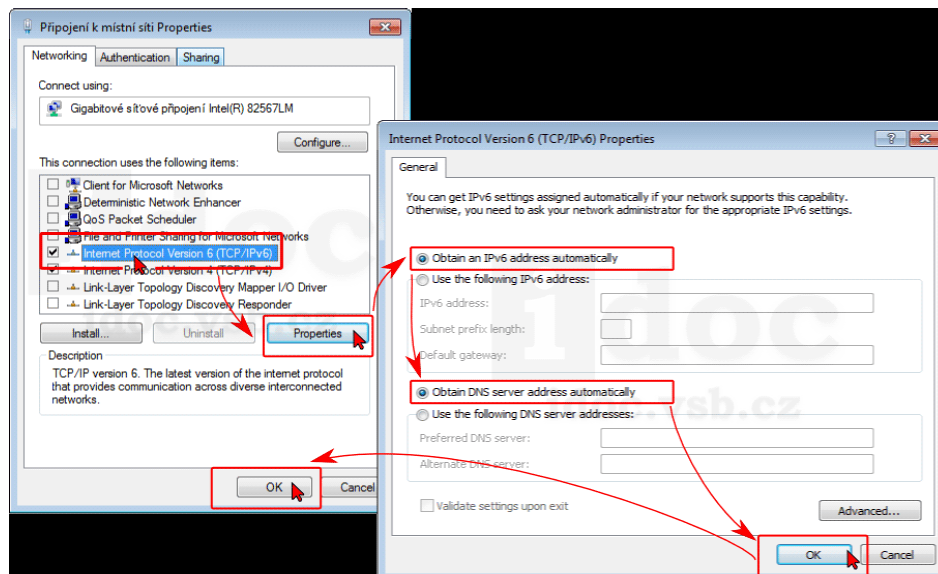
4. Select *Internet Protocol Version 6 (TCP/IP)* and choose *Properties*.



5. Choose "*Obtain an IPv6 address automatically.*"



6. Press *OK* and then close out of the *Properties* and *Network and Sharing*





## PRACTICAL 6- To install any one open source packet capture software like Wireshark

### Step 1 – Download Wireshark

Run as Administrator

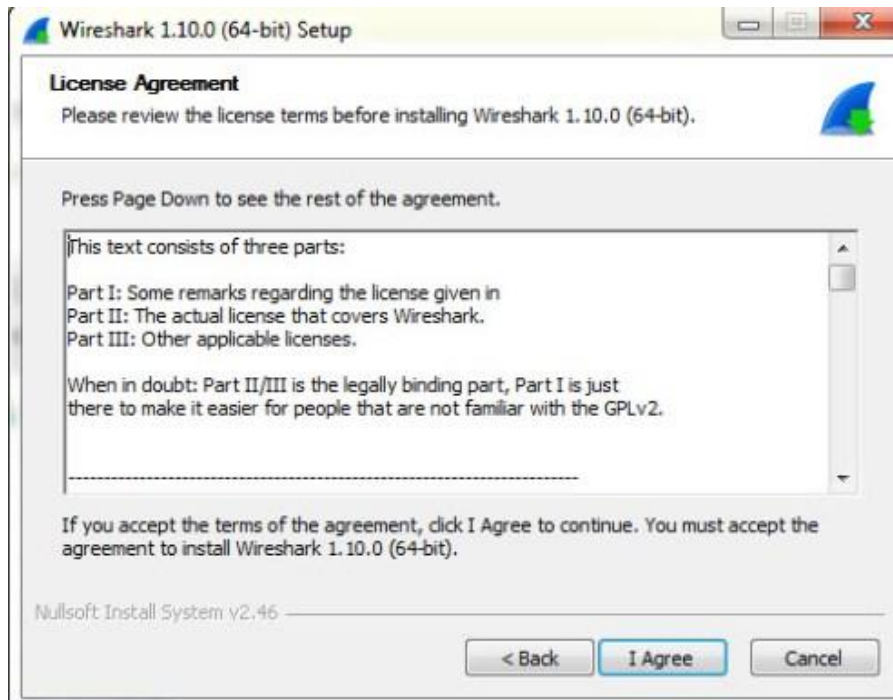


### Step 2 – Install

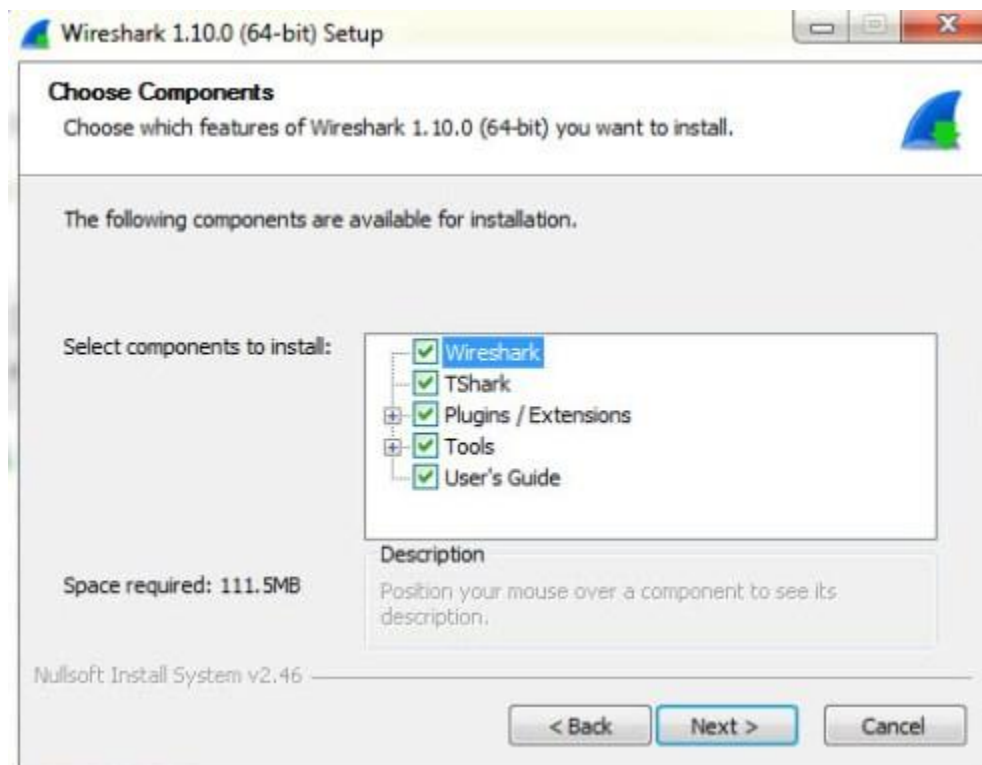
Next



I Agree

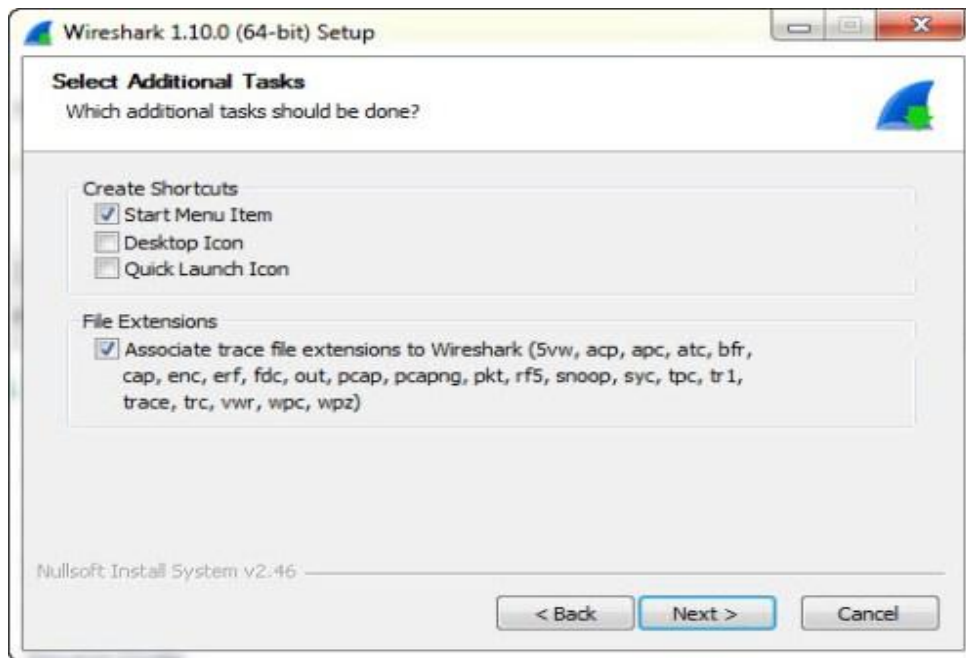


Next Disk space needed is 112 mb



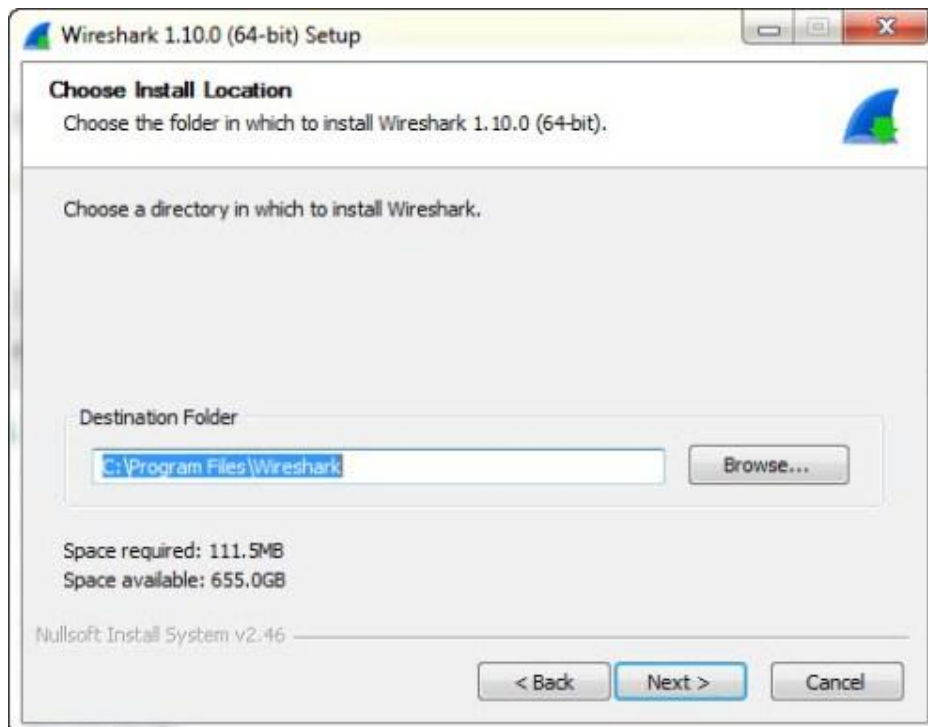
Next

Choose if Start Menu or Desktop Icon is preferred



Next

By default it installs into the directory c:\ Program Files\ Wireshark

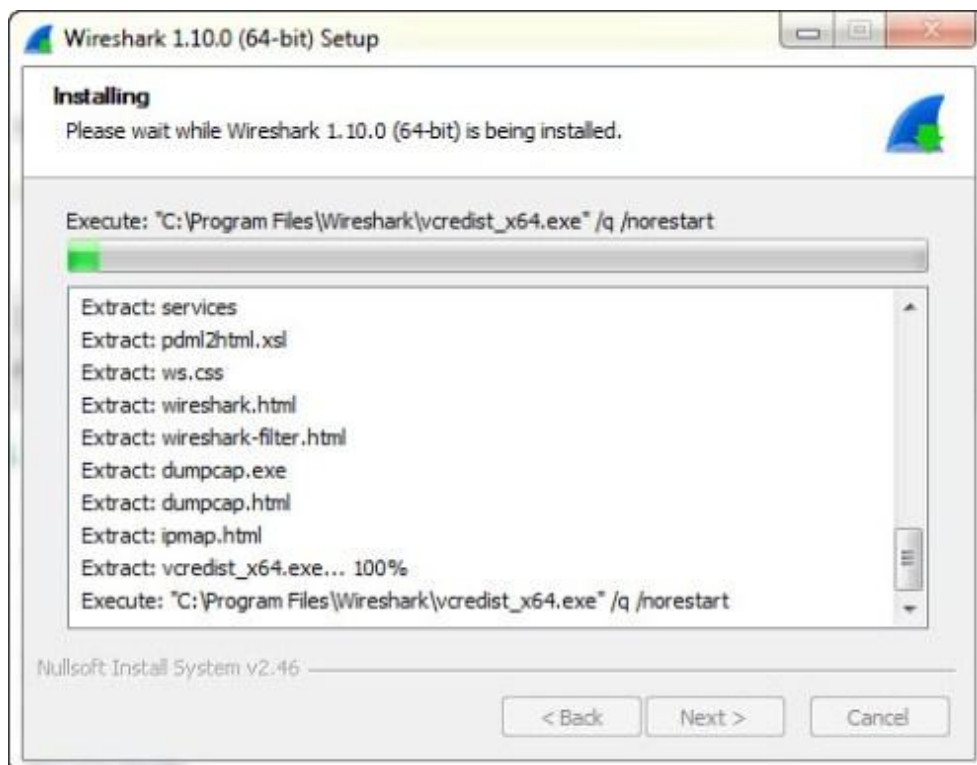


# Install WinPcap – as Wireshark won't work otherwise

Install



Wait for the files to extract....



## Step 2 – Install WinPcap

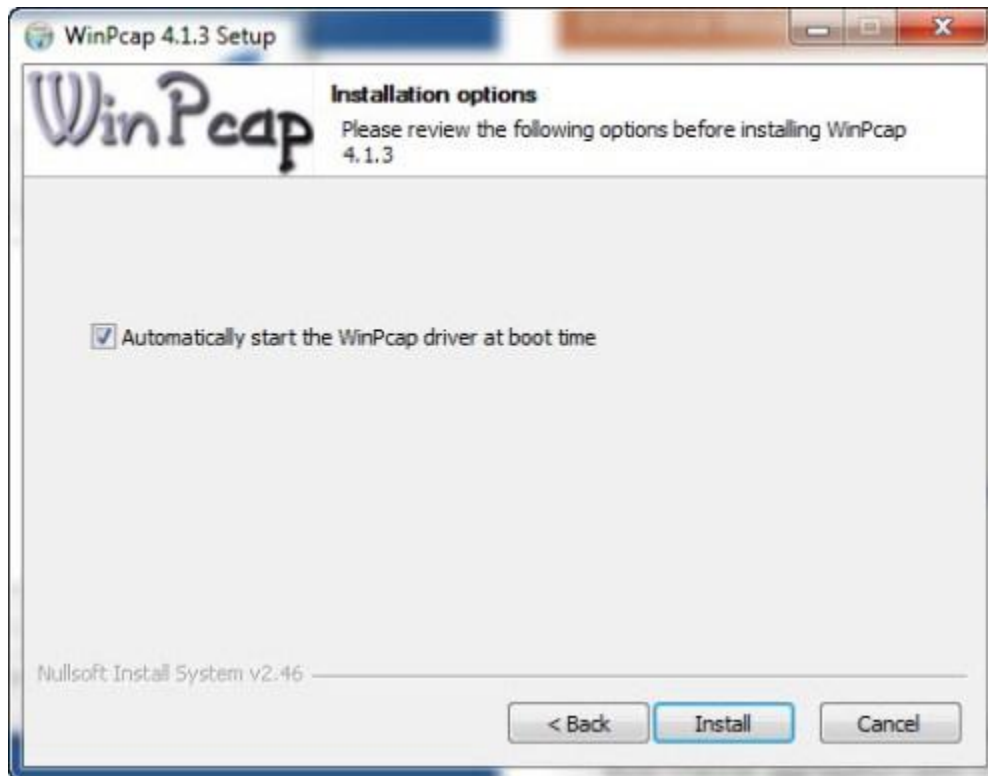
Wireshark won't install unless WinPcap is installed. Watch out for a second install to be launched. If you're not looking for it, you could miss it.



I Agree



## Install



## Finish



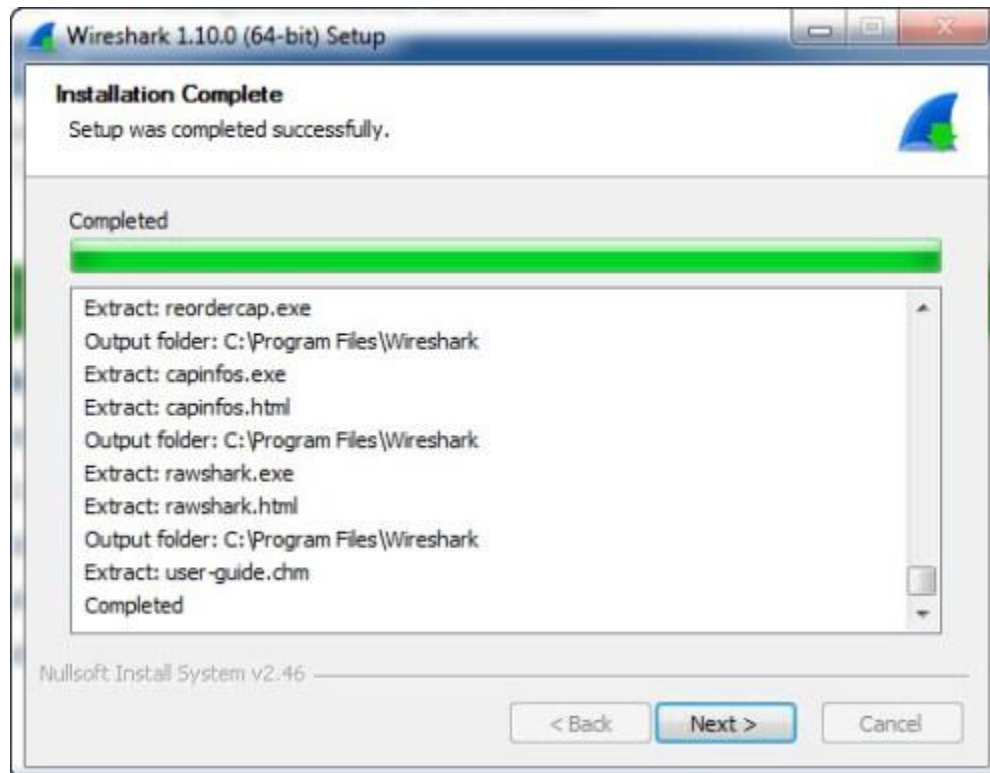
That's it!

Wireshark will now completely install for you.

If the install hangs half way through, it's because WinPcap has not been installed yet.

\*\*\*\*\*

Next







\*\*\*\*\*

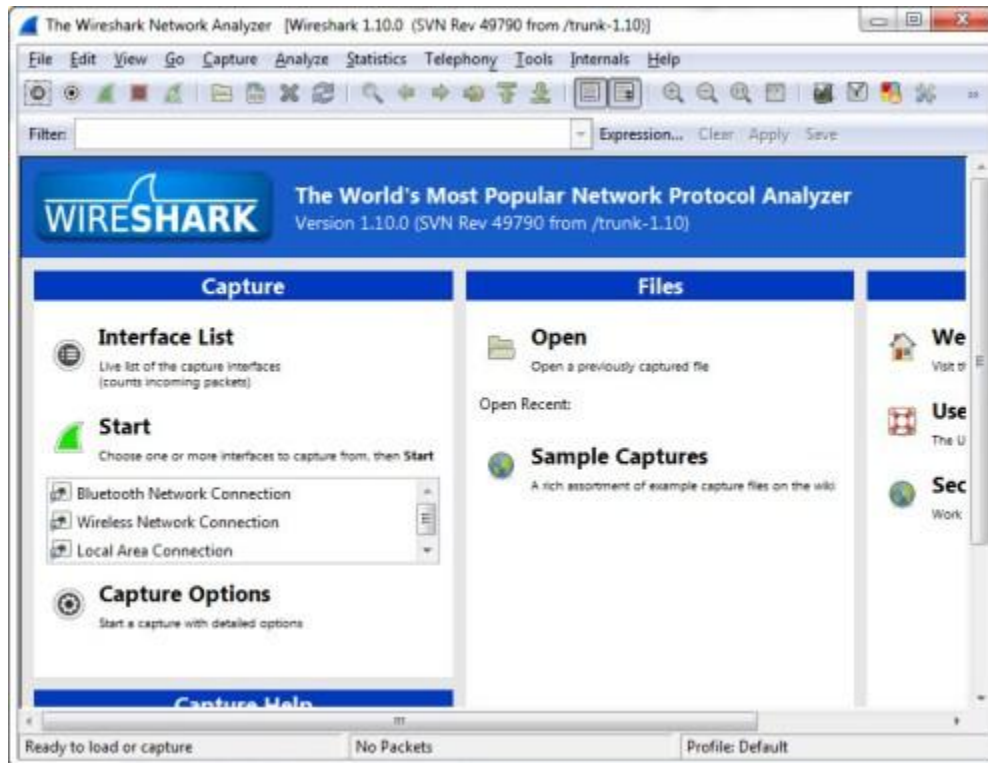
## Launch Wireshark

**Start > All Programs > Wireshark Icon**



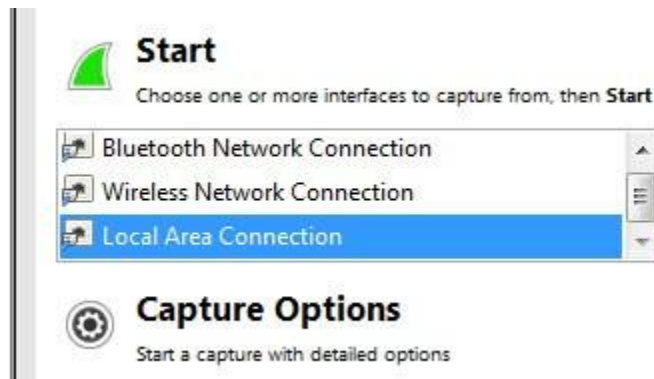


## Wireshark launches



Select your Interface (ie Wired or Wireless)

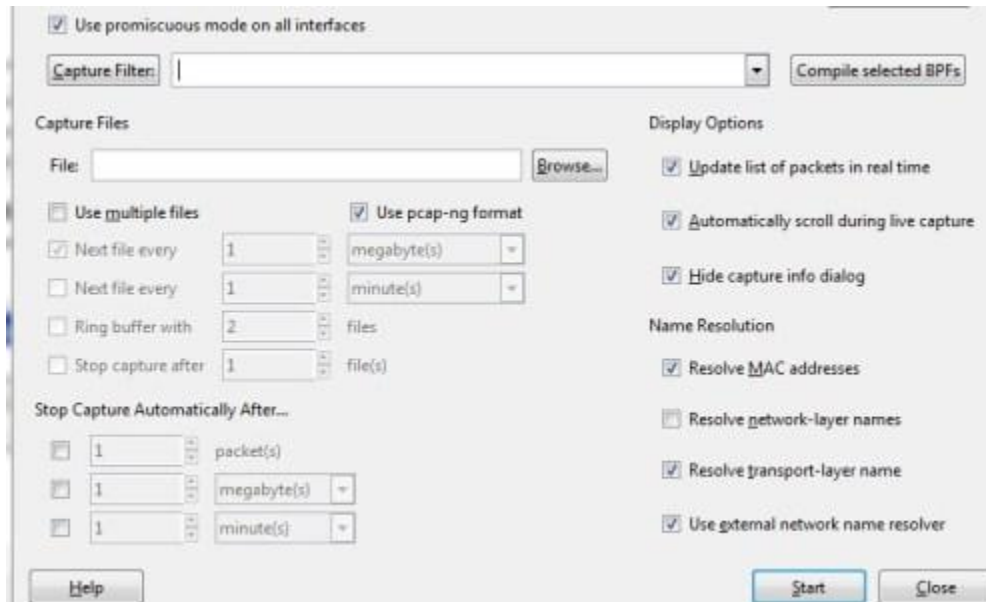
Then Capture Options



## Promiscuous Mode > Start

Promiscuous mode means that it picks up packets and data for all devices on the network

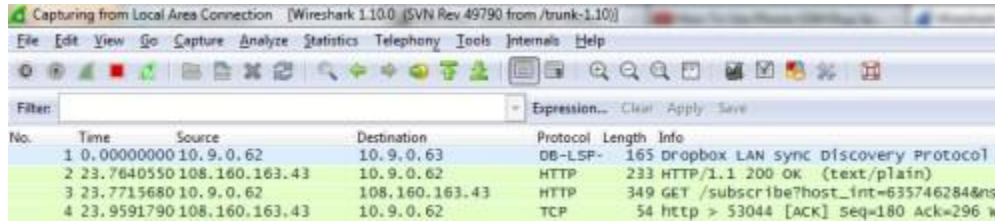
That's it – Wireshark will now listen in to all transmissions



\*\*\*\*\*

## Wireshark launches – by default it's split into 3 panes

### The top pane shows IP's & protocols



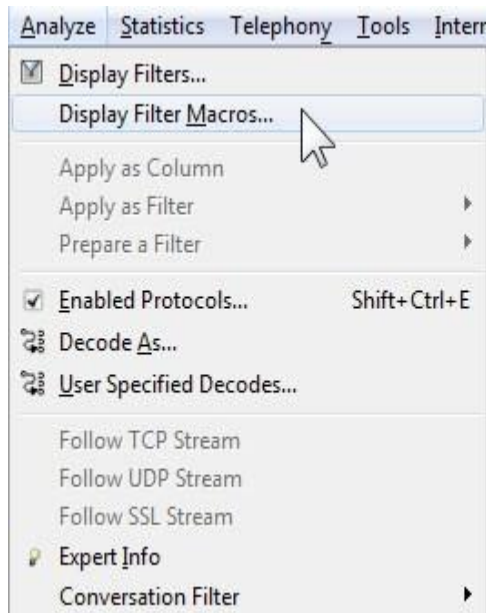
No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	10.9.0.62	10.9.0.63	DB-LSP	165	Dropbox LAN sync Discovery Protocol
2	23.7640550	108.160.163.43	10.9.0.62	HTTP	233	HTTP/1.1 200 OK (text/plain)
3	23.7715680	10.9.0.62	108.160.163.43	HTTP	349	GET /subscribe?host_int=635746284&ns
4	23.9591790	108.160.163.43	10.9.0.62	TCP	54	http > 53044 [ACK] Seq=180 Ack=296 W

\*\*\*\*\*

You can filter these results by protocol and by IP, and I'll cover that another time.

For now, select the Protocol header – and your results will sort by protocol.

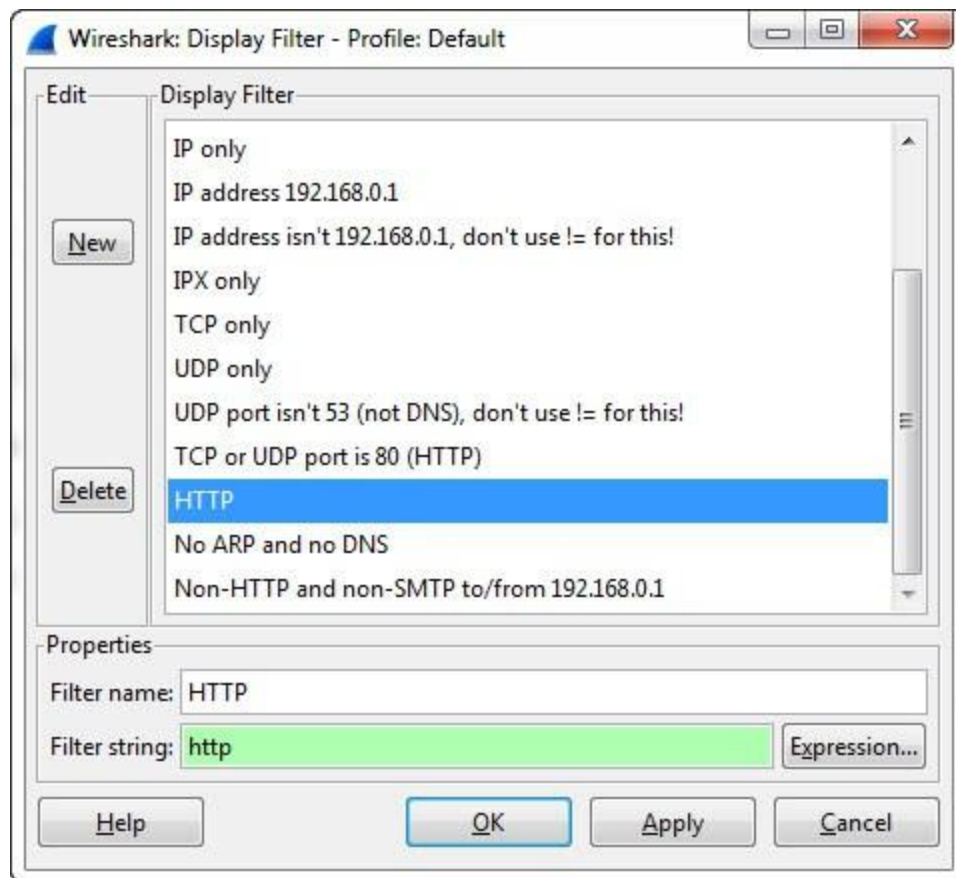
## ANALYSE > Display Filter



## HTTP

Select HTTP

OK



HTTP ONLY is now displayed

Capturing from Local Area Connection [Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
2	23.7640550	108.160.163.43	10.9.0.62	HTTP	233	HTTP/1.1 200 OK (text/plain)
3	23.7715680	10.9.0.62	108.160.163.43	HTTP	349	GET /subscribe?host_int=63574
15	79.4591610	108.160.163.43	10.9.0.62	HTTP	233	HTTP/1.1 200 OK (text/plain)
18	79.4674050	10.9.0.62	108.160.163.43	HTTP	349	GET /subscribe?host_int=63574
24	135.169066	108.160.163.43	10.9.0.62	HTTP	233	HTTP/1.1 200 OK (text/plain)
25	135.176526	10.9.0.62	108.160.163.43	HTTP	349	GET /subscribe?host_int=63574
32	190.503487	108.160.163.43	10.9.0.62	HTTP	233	HTTP/1.1 200 OK (text/plain)
35	190.511568	10.9.0.62	108.160.163.43	HTTP	349	GET /subscribe?host_int=63574
41	245.785651	108.160.163.43	10.9.0.62	HTTP	233	HTTP/1.1 200 OK (text/plain)
42	245.792606	10.9.0.62	108.160.163.43	HTTP	349	GET /subscribe?host_int=63574
60	301.556164	108.160.163.43	10.9.0.62	HTTP	233	HTTP/1.1 200 OK (text/plain)
61	301.563846	10.9.0.62	108.160.163.43	HTTP	349	GET /subscribe?host_int=63574
64	357.122929	108.160.163.43	10.9.0.62	HTTP	233	HTTP/1.1 200 OK (text/plain)
67	357.128140	10.9.0.62	108.160.163.43	HTTP	349	GET /subscribe?host_int=63574
68	357.511375	108.160.163.43	10.9.0.62	HTTP	233	[TCP Retransmission] HTTP/1.1
70	357.632037	10.9.0.62	108.160.163.43	HTTP	349	[TCP Retransmission] GET /sub

## PRACTICAL 7: To configure Wireless Local Loop.

**Wireless local loop (WLL)**, is a term for the use of A wireless communications link as the "last mile First mile" connection for delivering plain old Telephone service (POTS) and/or broadband Internet to telecommunications customers. Various Types of WLL systems and technologies exist.

**Narrowband** – offers a replacement for existing telephony Services

**Broadband** – provides high-speed two-way voice and data Service

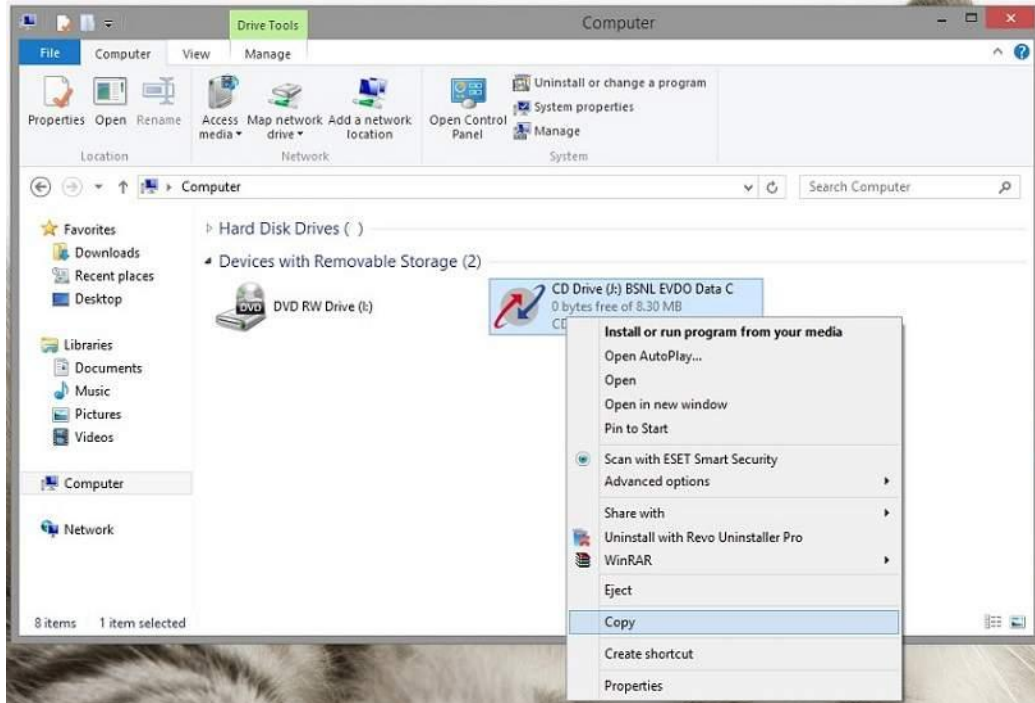
### Install BSNL EVDO Modem in Windows 8

Before proceed to installation make sure,

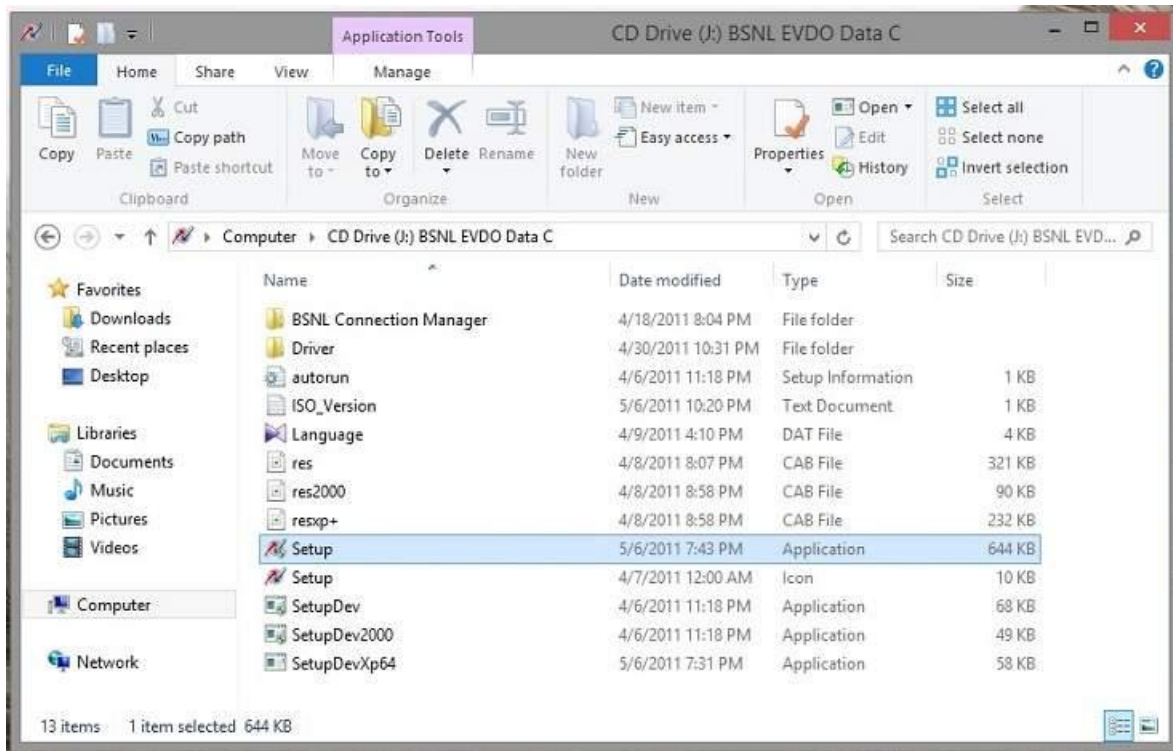
1. Windows 8 is updated with all its device drivers.
2. No issues found in Device Manager.

**Step 1#** Even if after a successful installation in normal way, most of the users face ‘Device Not Detected’ Problem. This happens due to unavailability of modem’s device drivers.

**Step 2#** Let’s start the installation, Insert EVDO Modem into the USB port in Laptop or Computer and go to ‘My Computer’, you will find a CD Drive named ‘BSNL EVDO Data Card’. **Back up the modem** installation files and folders (required): Right click on the icon and copy paste it in any drive except C partition.



**Step 3#** Now go to backed up data folder or CD Drive in My Computer and click Setup file icon to start the modem installation.



**Step 4#** Whole installation will take few minutes or seconds to complete depending upon the Computer or Laptop configuration, Don't worry just take a cup of Cold Coffee and wait.



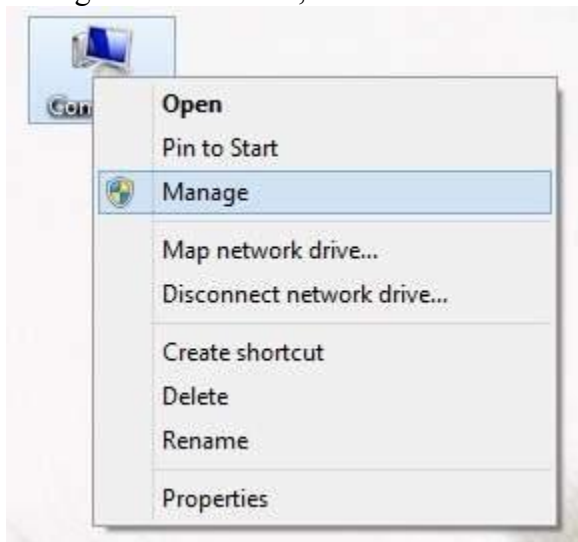


**Step 5#** After successful installation open BSNL EVDO Dashboard just by clicking on the Desktop's BSNL icon, What happen ?? same 'Device Not detected' issue!!!



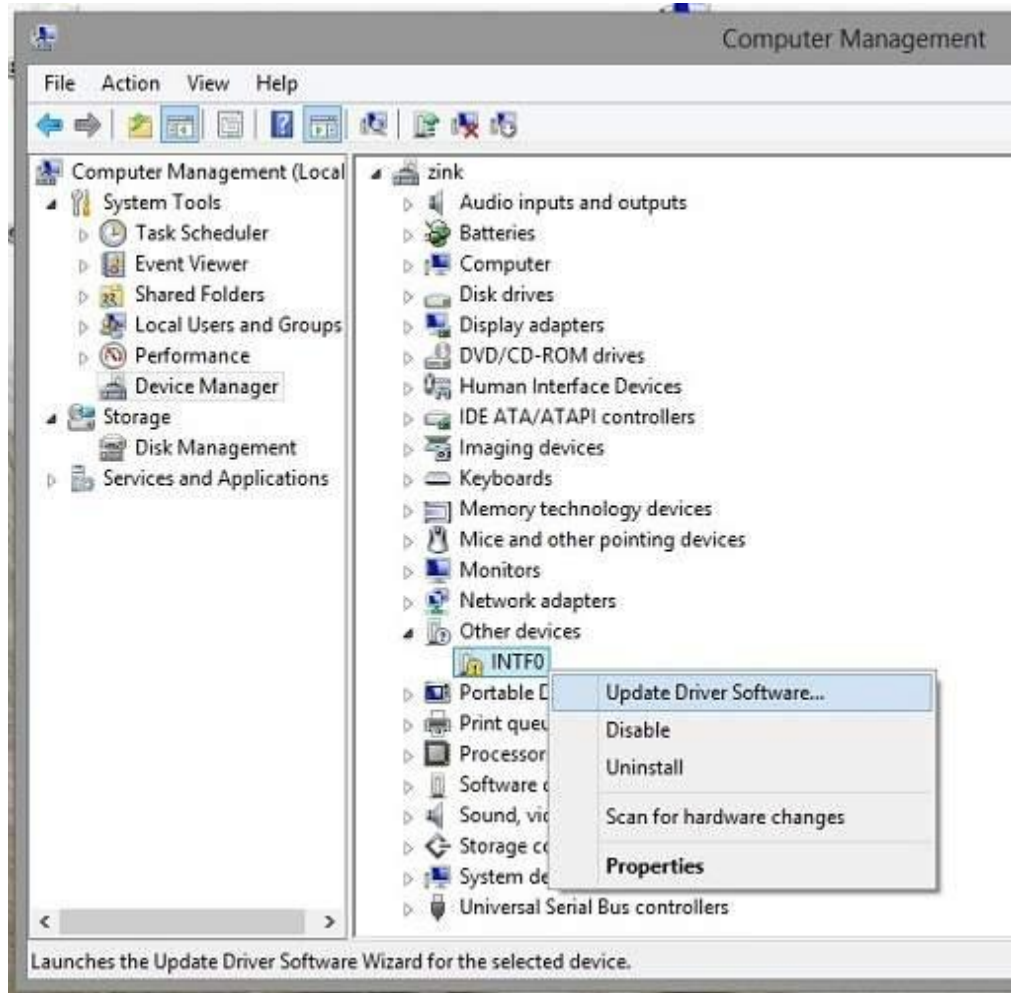
**Step 6#** Ok Here is the **solution for EVDO connecting issue in Windows 8.**

Right click on My Computer Icon and select 'manage' option, it will open 'Computer Management' Window,



Now select ' Device Manager' and find out the the devices on right pane which have not been updated with proper driver software. It may be INTF0 or UE100 USB ETS or

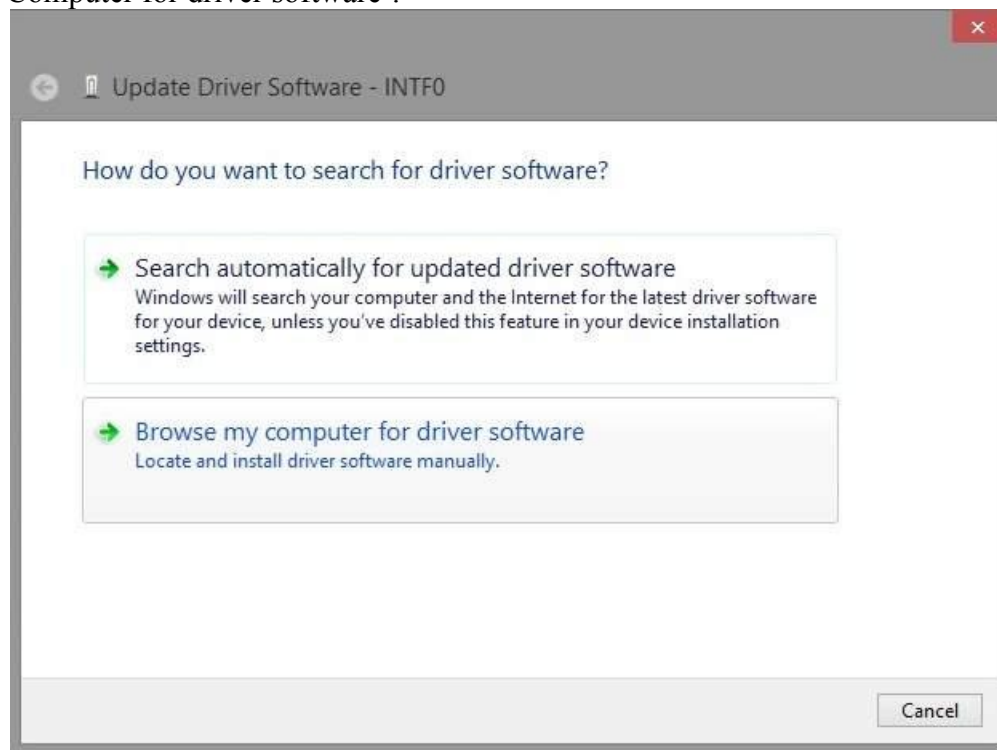
Win\_Mux\_Device\_01/02 etc



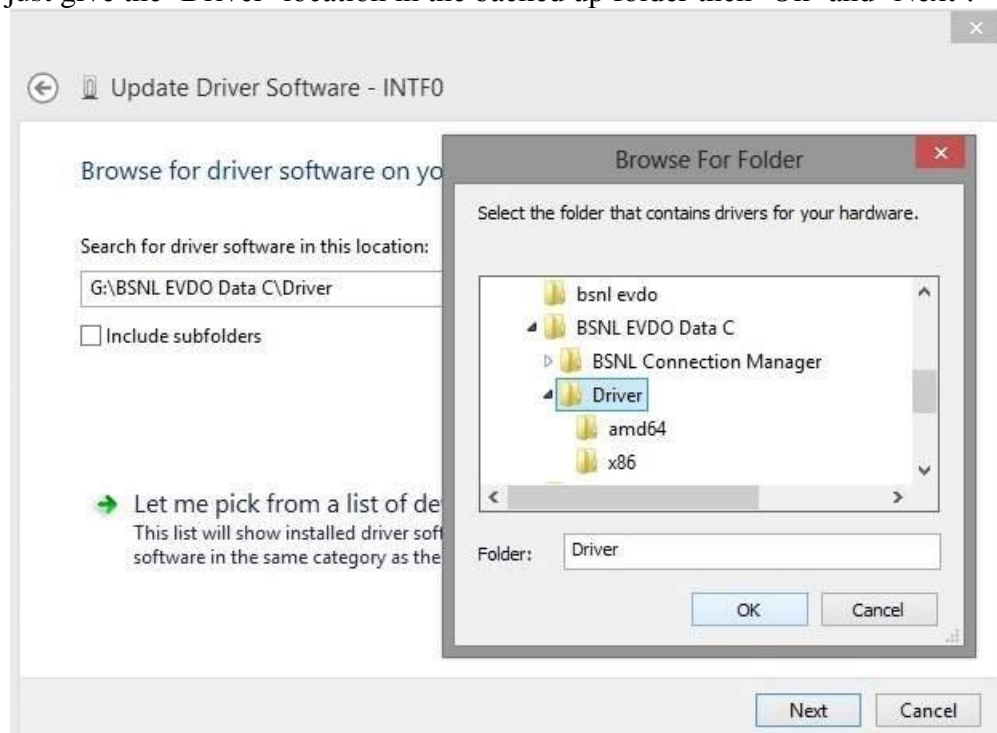
Right click on the device and select 'Update Device Driver Software' option. In next windows which ask to select option to search for software drivers: just select 2nd option- 'Browse my



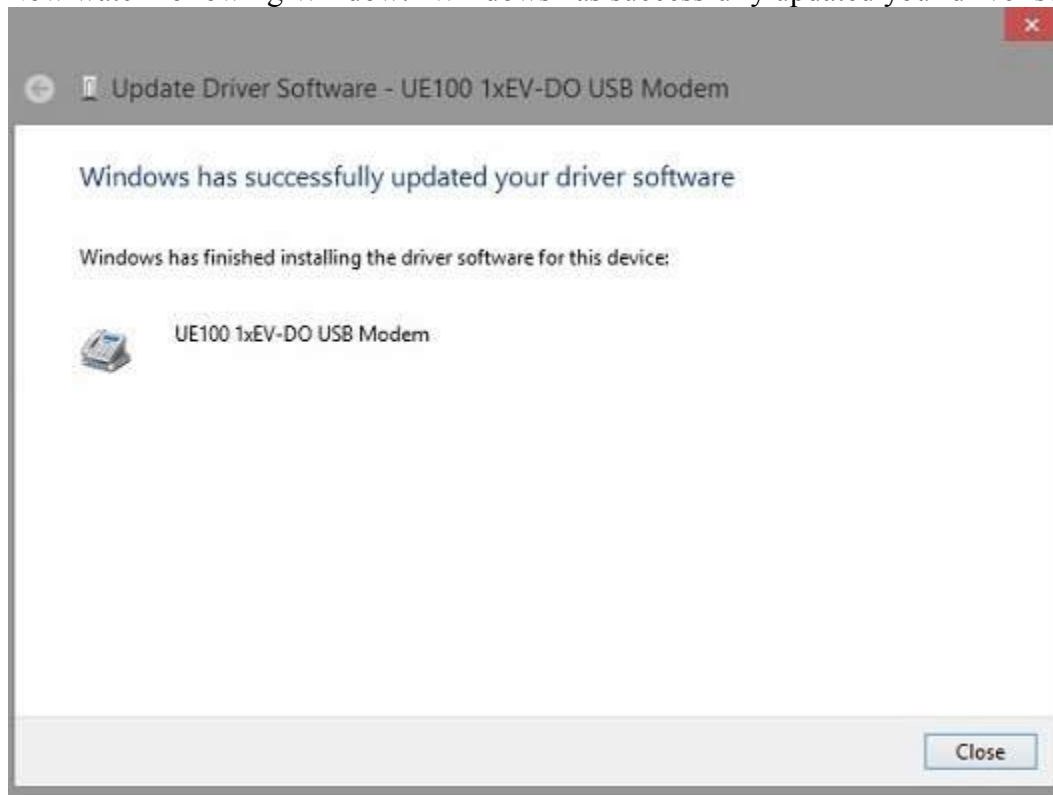
Computer for driver software’.



Now installation will ask to browse the drivers software location in your computer, Don't worry just give the 'Driver' location in the backed up folder then 'Ok' and 'Next'.



Now watch following Window: 'Windows has successfully updated your driver software'.

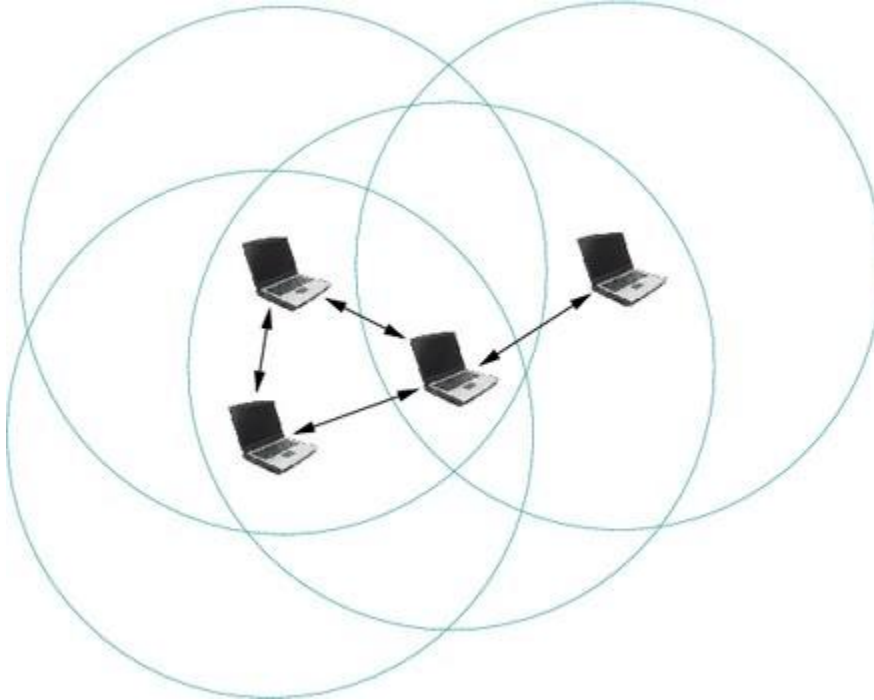


Now you have **successfully install BSNL EVDO modem in Windows 8.**

## PRACTICAL 8 -To Configure Ad Hoc Wireless Network

**Suitable for:** High Power & High Gain Wireless, 300Mbps Wireless N Adapters, 150Mbps Wireless N Adapters, 54Mbps Wireless G Adapters

The Ad Hoc mode, also called peer to peer mode, allows nodes to communicate directly (point-to-point) without the need for an AP, as in the following Figure. There is no fixed infrastructure. Nodes need to be in range with each other in order to communicate. For more information about an Ad Hoc network, please refer to the interpretation from [Wikipedia](#).



Ad Hoc mode

An Ad Hoc WiFi network should at least consist of 2 clients. In this tutorial, we also take just two computers for instance: computer A and computer B.

**NOTE:** Before we proceeding, please make sure the **Windows Zero Configuration (WZC)** service is started. If you are not sure about this, please click [here](#) to check the settings.

### Part 1: Create an Ad Hoc network profile on computer A

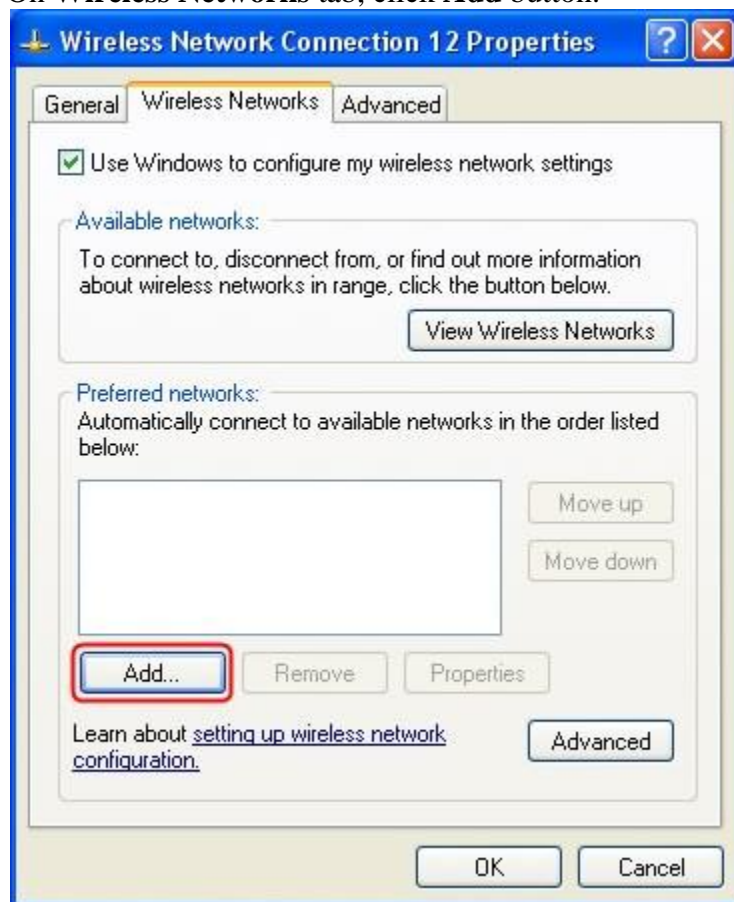
#### Step 1

Go to **Control Panel -> Network Connections** and find **Wireless Network Connection**. Right click Wireless Network Connection and select **Properties**.



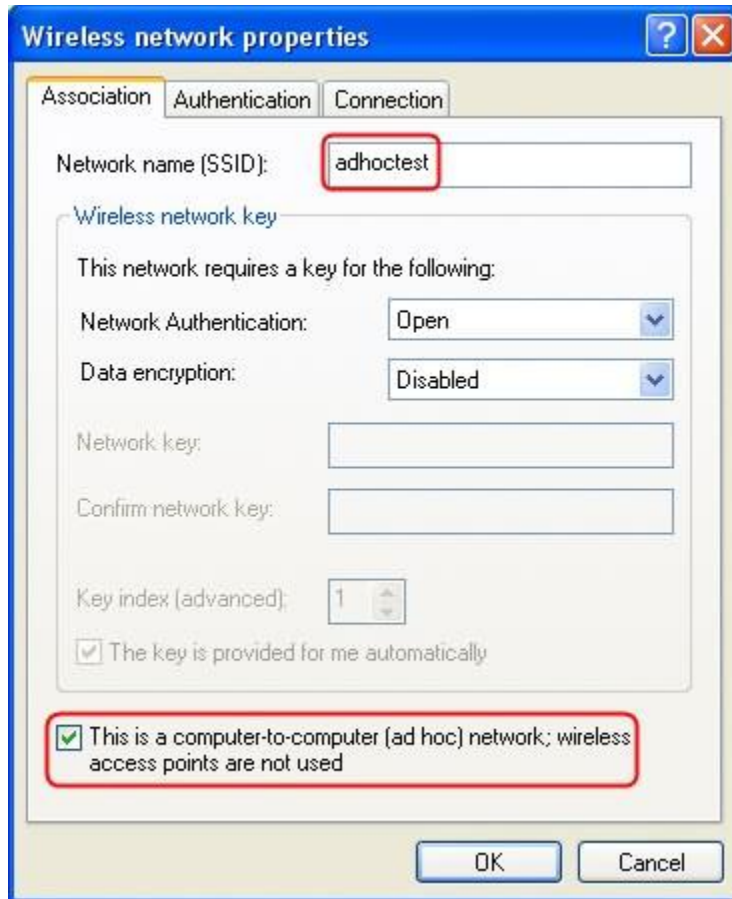
## Step 2

On **Wireless Networks** tab, click **Add** button.



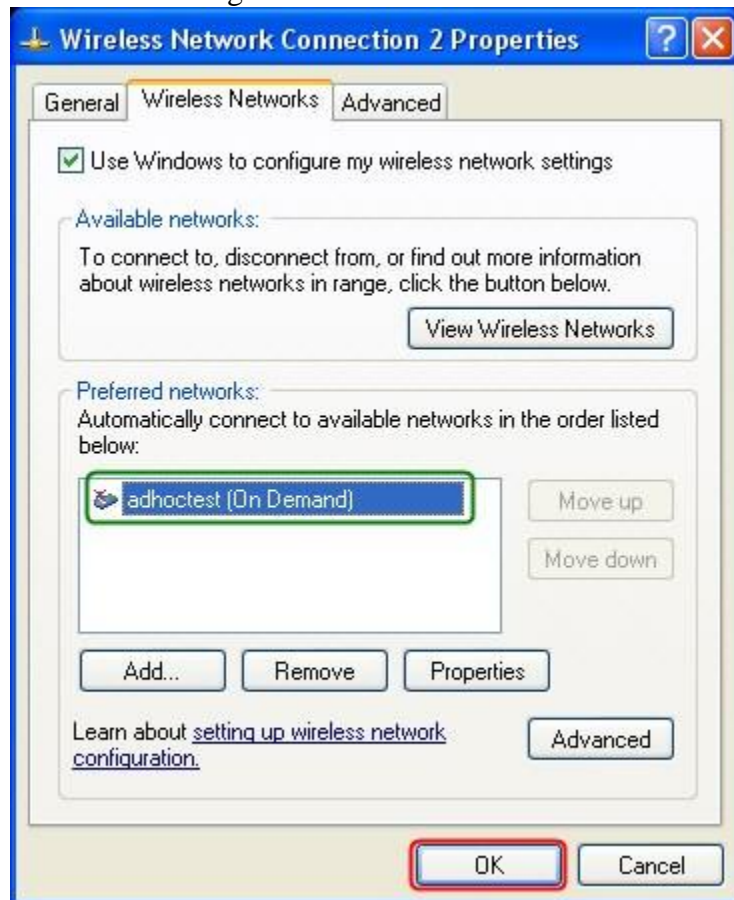
### Step 3

On **Association** tab of **Wireless network properties** window, please type a phrase for **Network Name [SSID]**. In our scenario, we take *adhoc*test for example. Then go to the bottom and tick **This is a computer-to-computer [ad hoc] network; wireless access points are not used**. Then click **OK**.



#### Step 4

After Step 3, there should be a profile named **adhoc**test in **Preferred Networks**. Click **OK** to save all the settings.



## Part 2: Manually configure an IP address on computer A

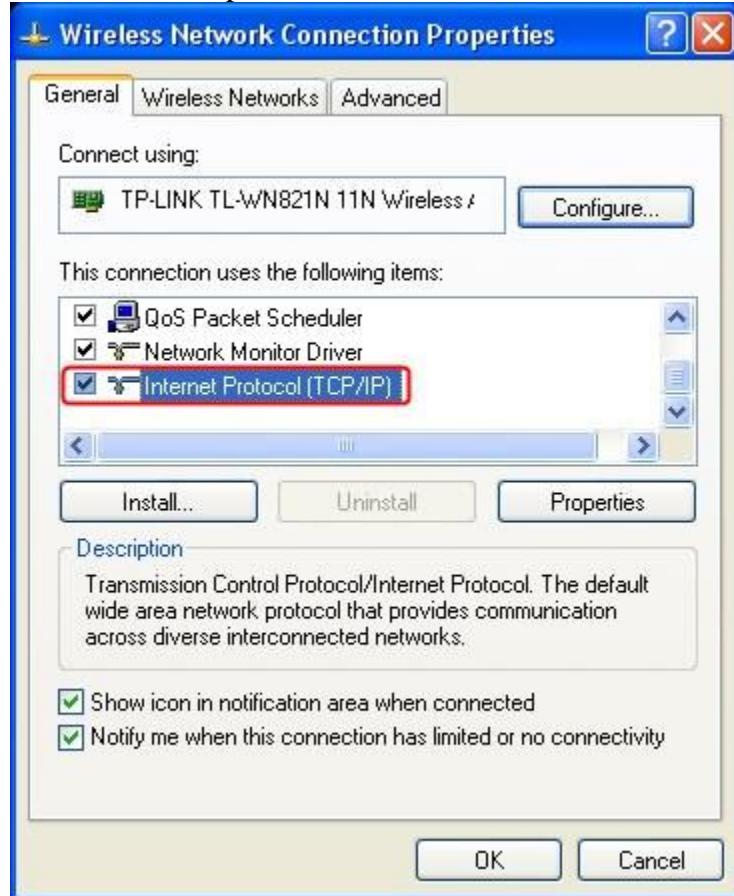
#### Step 5

Right click **Wireless Network Connection** and select **Properties**.



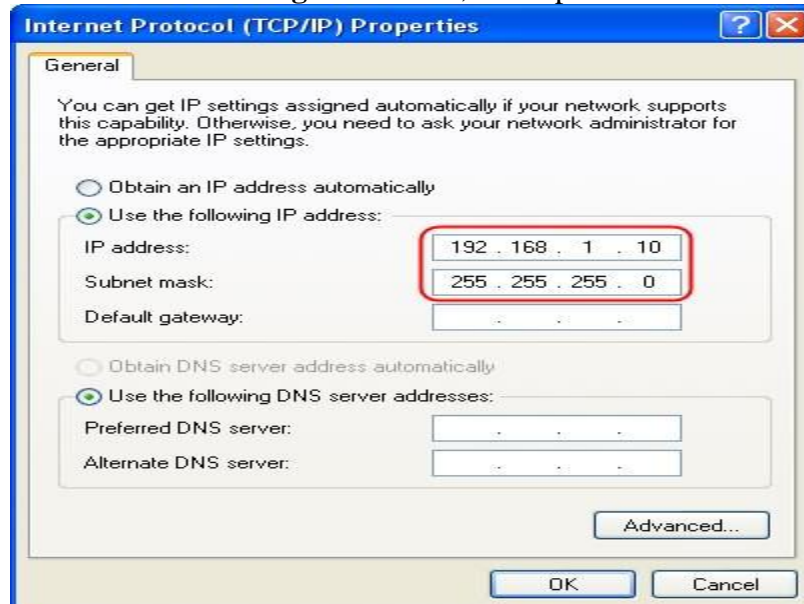
## Step 6

On **General** tab, please double click **Internet Protocol (TCP/IP)**.



## Step 7

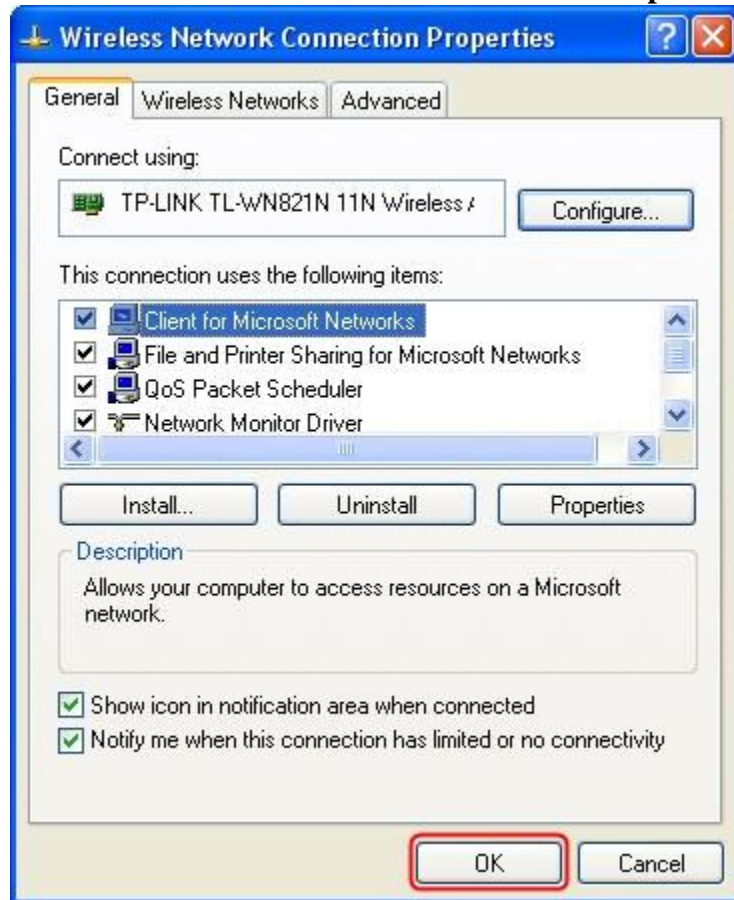
Tick **Use the following IP address**, and input the **IP address** and **Subnet mask**. Then click **OK**.





### Step 8

Click **OK** on **Wireless Network Connection Properties** window.



## Part 3: Scan for Ad Hoc network on computer B

### Step 9

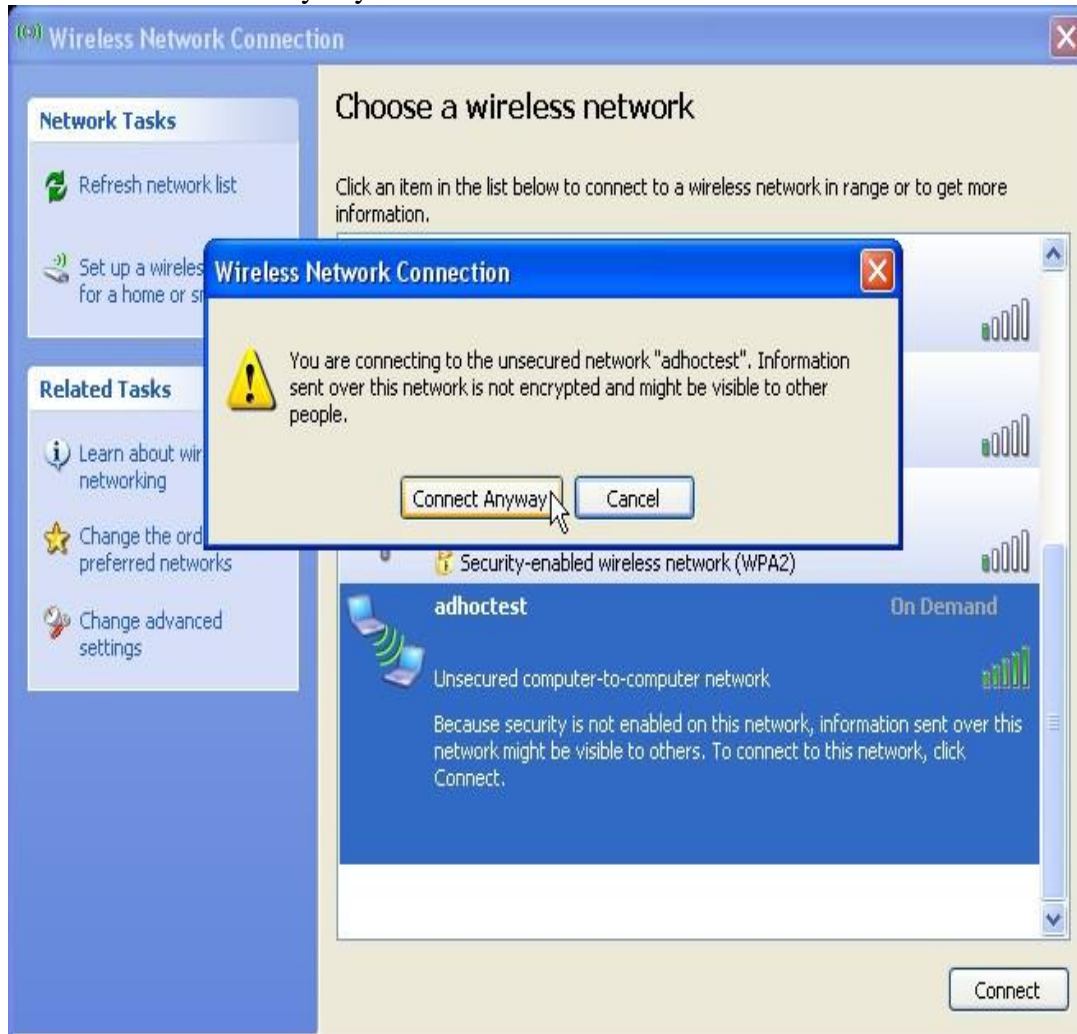
Right click **Wireless Network Connection**, select **View available wireless networks**





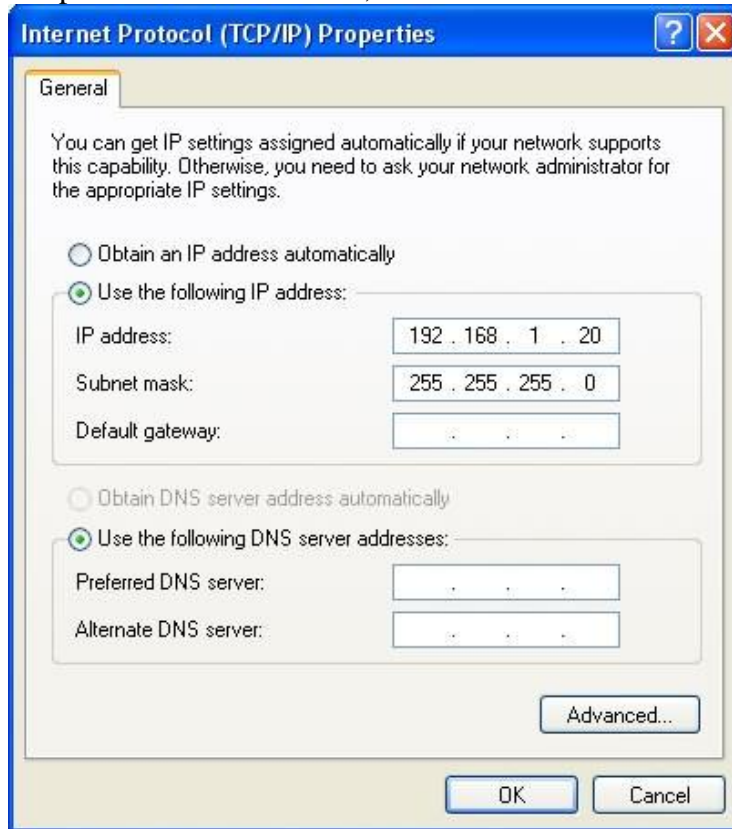
### Step 10

Find **adhoctest**(which is set up on computer A) network in the scan window. Then double click it and click connect Anyway?

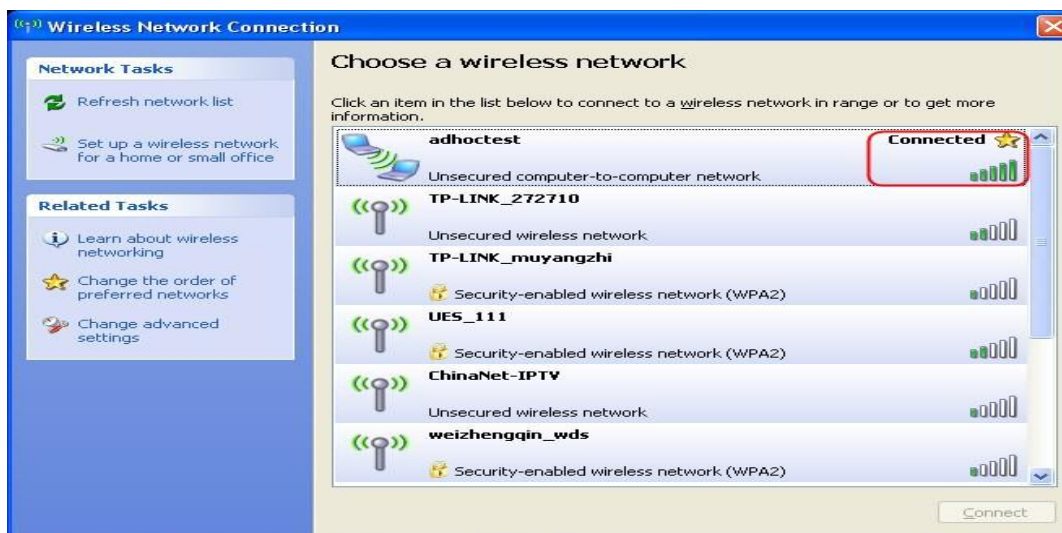


## Part 4: Manually configure an IP address on computer B

The steps are the same as which were done on computer A (**Step 5** to **Step 8**). The point is that we need assign a different IP address for computer B, and it must be in the same subnet with computer A. In our scenario, we can take 192.168.1.20/255.255.255.0.



Here until, all the basic settings for building an Ad Hoc network have been finished. If we open the network scan window again, we can see the **adhoctest** network says **Connected**.



## **PRACTICAL 9 – To Configure WLAN**

### **Pre-requisite:**

1. Wireless LAN adapter must support WPA2. Please refer to respective manufacturer.
2. Prior to this setup attempt, user system has been known to be authenticated successfully with NTU domain via LAN network. A user profile is created automatically upon successful authentication via LAN.

### **Advantages:**

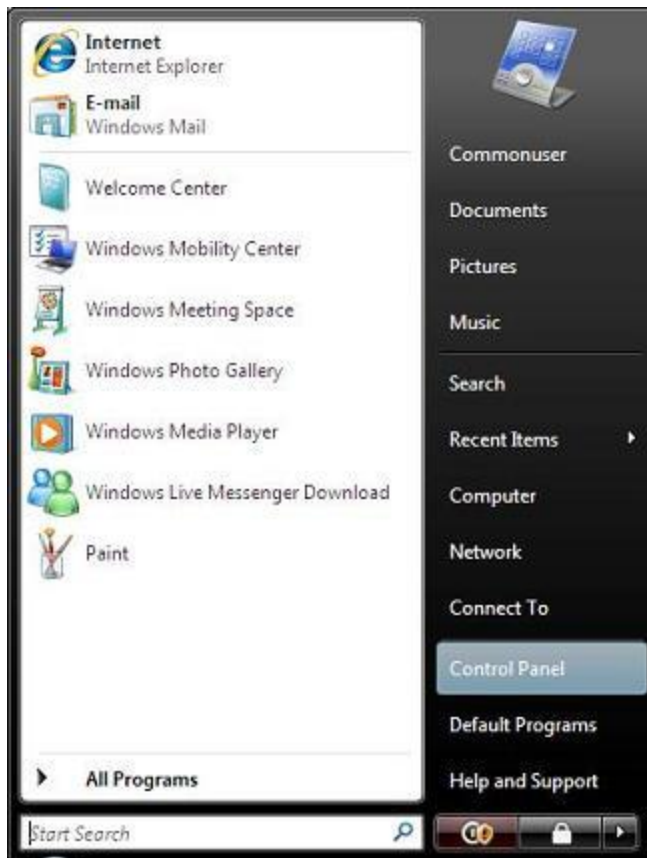
1. Wireless traffic is encrypted and is more secured compared to that of Open web-authentication (i.e. SSID: **NTUWL**). Strong encryption (AES) is used to ensure high data security in network traffic over the air.
2. WPA2 has a stronger cipher than WPA and conforms to 802.11i standard. Therefore, WPA2 offers higher security and interoperability than WPA.
3. User will need to login once to his/her system without the needs to re-enter credential to access Internet.
4. User systems will be able to roam and join the NTU wireless network automatically whenever his/her systems are in the wireless coverage range without the hassle of manual re-login.

### **Setting Up:**

1. At Windows desktop, click on Vista button



2. and navigate to **Control Panel** as shown below.



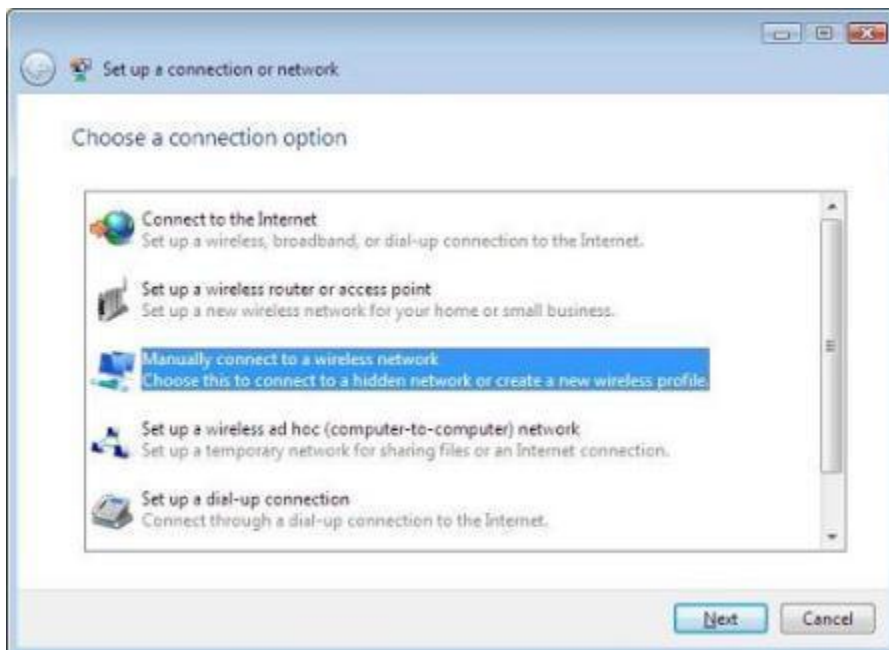
3. At **Control Panel** menu, click on **View network status and tasks** as shown below.



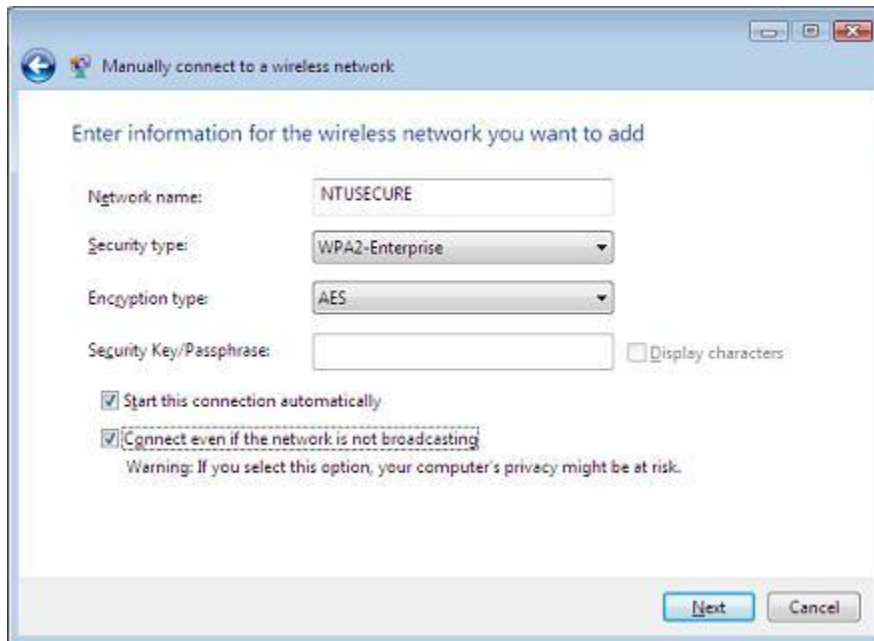
4. On the left panel, click on **Set up a connection or network**.



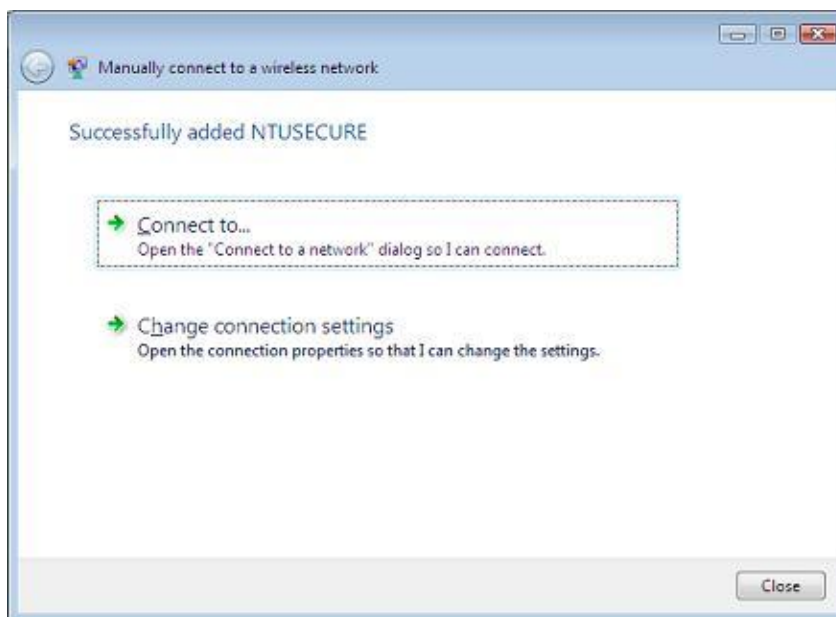
5. Select  **Manually connect to a wireless network**.



6. Set the **Network Name** for NTUSECURE (must be in uppercase), **Security type** for **WPA2-Enterprise** and **Encryption type** for **AES**.
7. Check the checkboxes ☒ **Start with this connection automatically** and ☒ **Connect even if the network is not broadcasting**. Click **Next** to proceed.

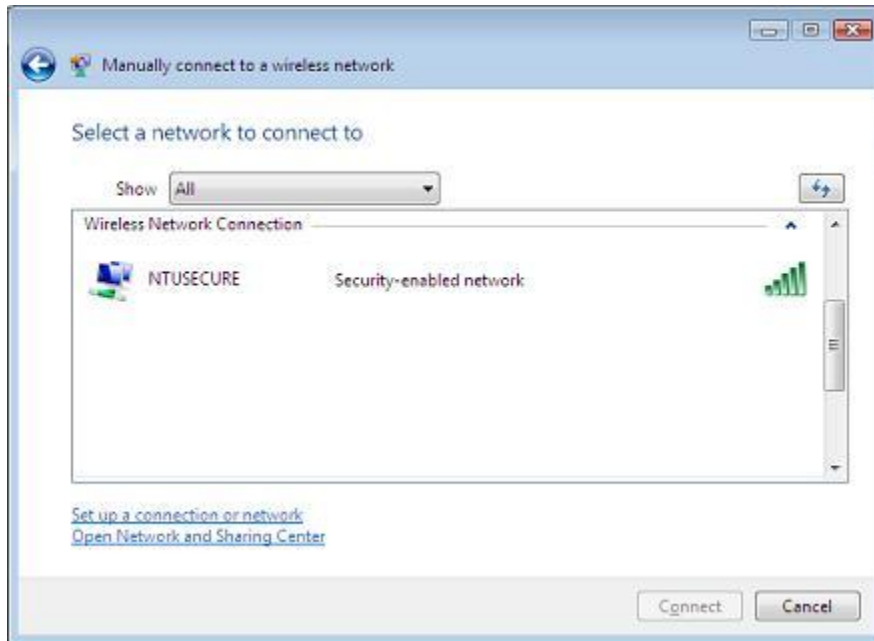


8. Click **Connect to...** to proceed connecting to wireless network.

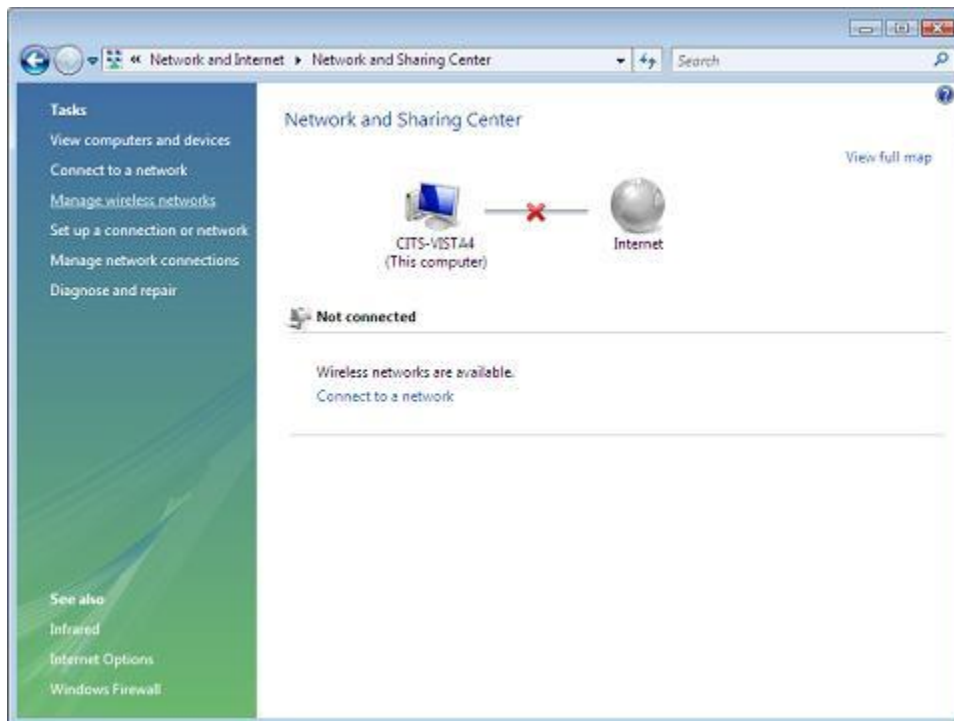




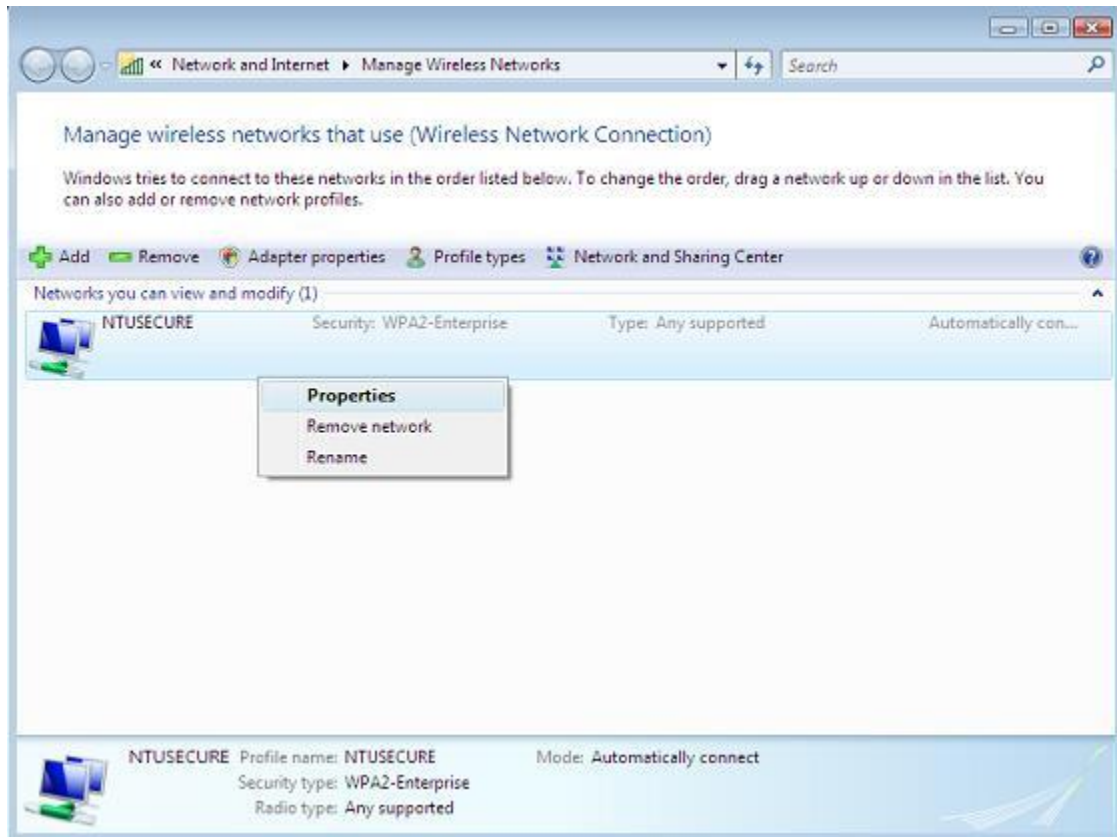
9. The initial wireless **NTUSECURE** status is **Security-enabled network** as shown in the following. Click **Cancel** to close the menu.



10. At **Network and Sharing Center** menu, click **Manage wireless networks**.

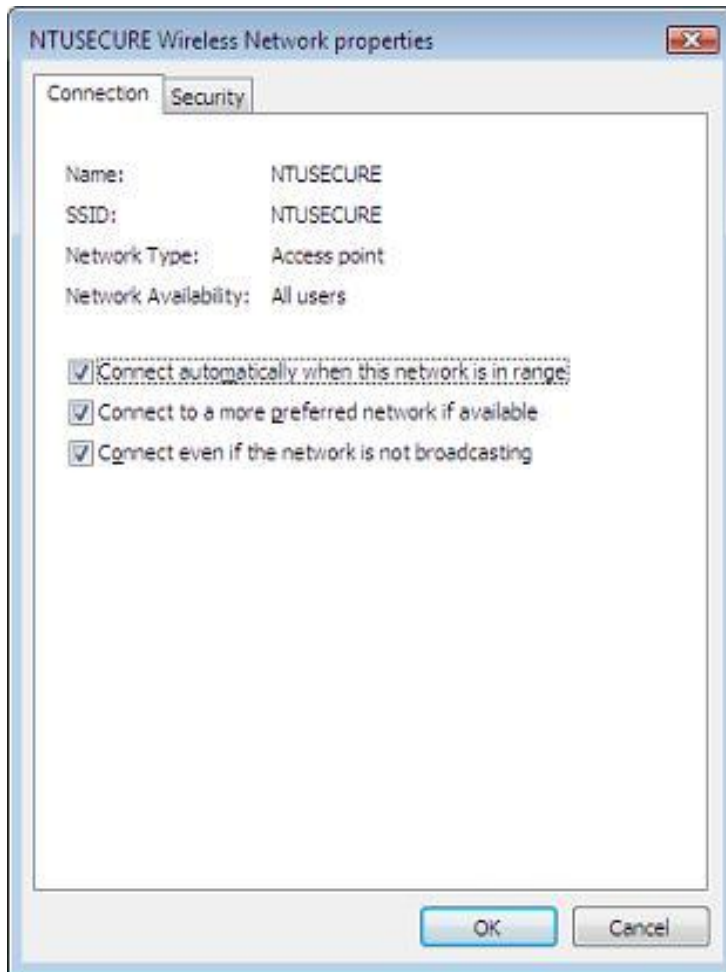


11. Right-click the highlighted **NTUSECURE** and select **Properties** as shown below.

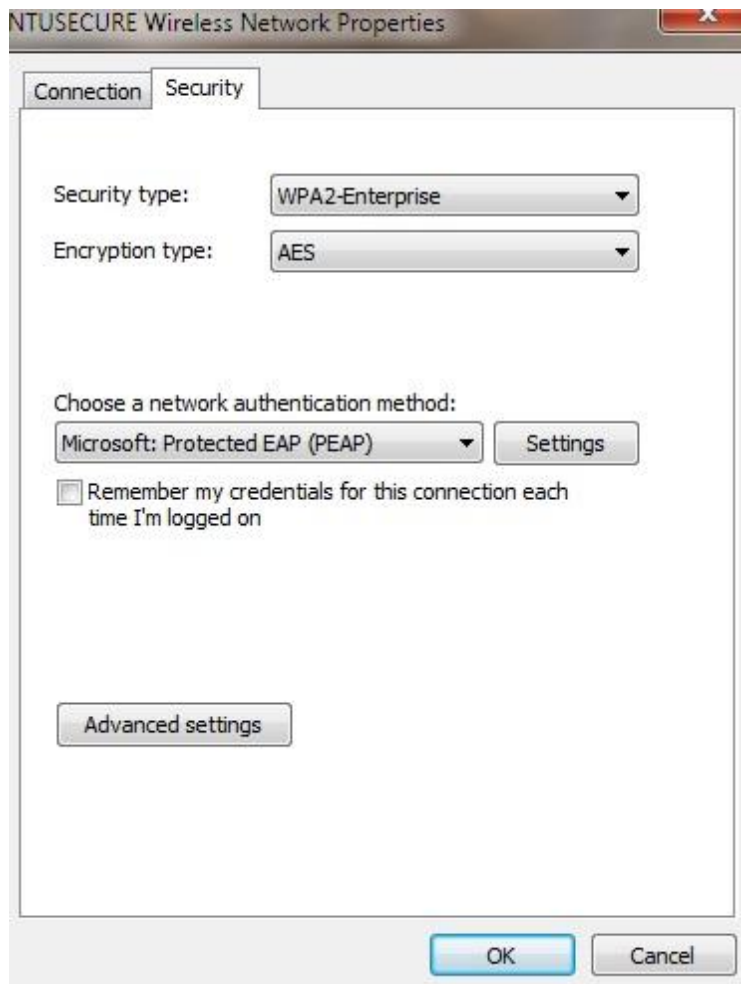




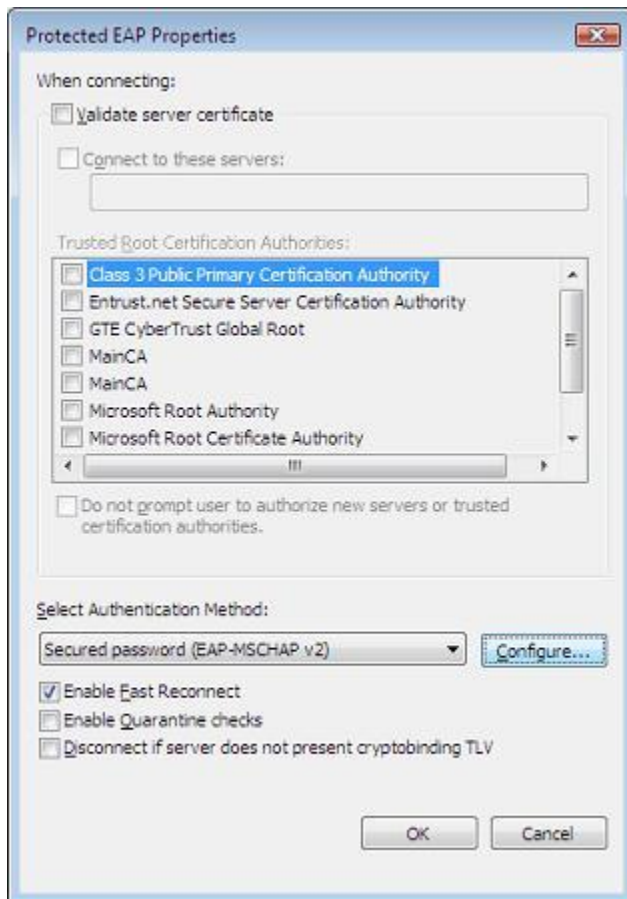
12. Ensure all the checkboxes are ticked. Proceed to click on **Security** tab.



13. Ensure settings are as the following. Click **Settings...** to proceed.



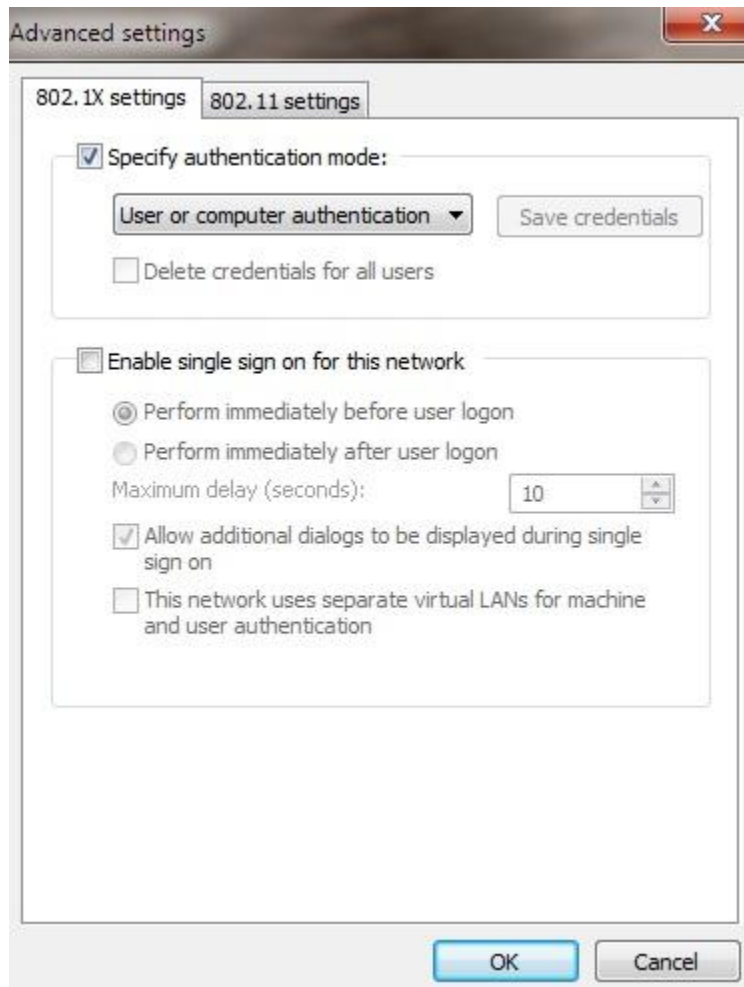
14. Ensure only checkbox ☒ **Enable Fast Reconnect** is checked. The rest of the checkbox MUST be uncheck. Click on **Configure ...** to proceed.



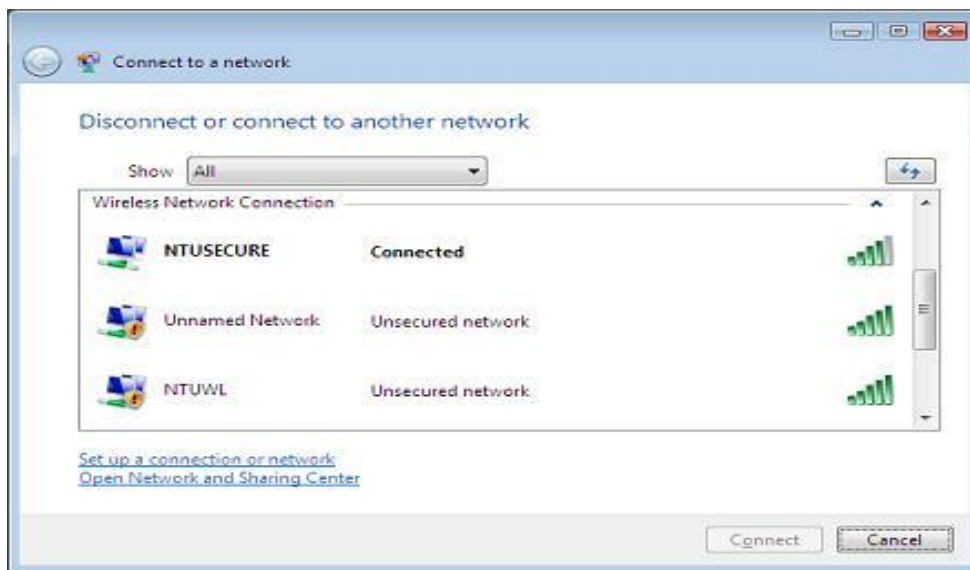
15. If you are staff and your PC is join to domain, Check the checkbox ☒. Click OK to close. Do not check it if your machine is not join to domain.



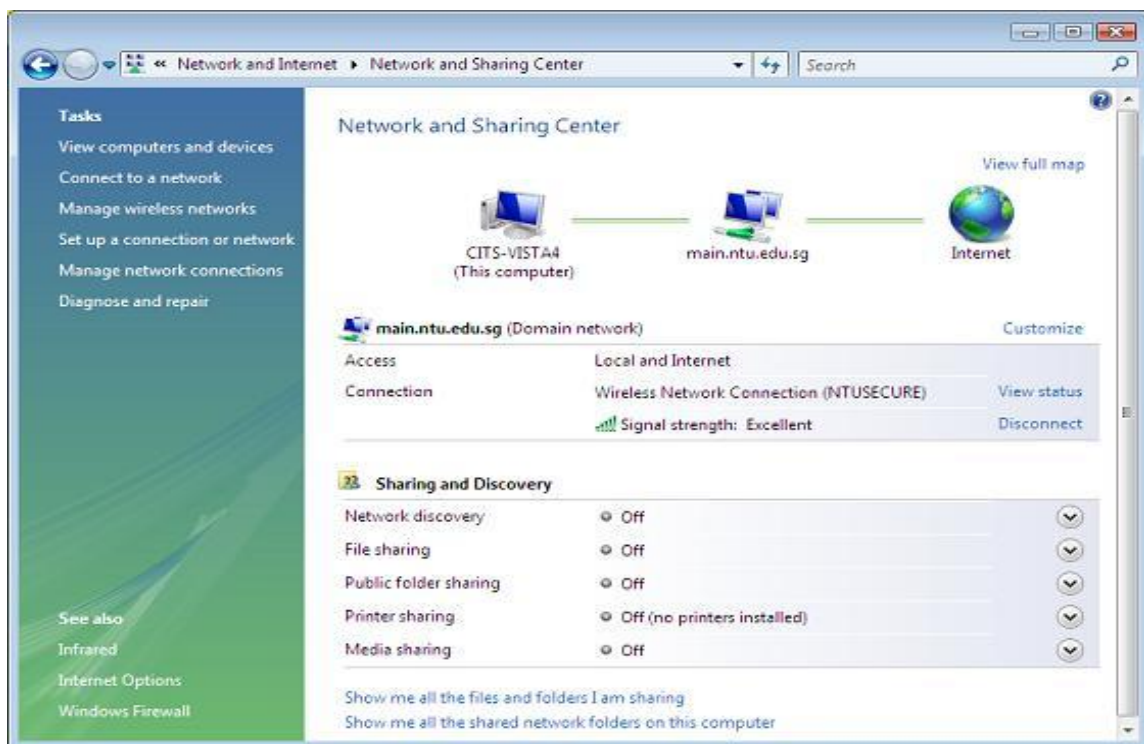
16. Return to Security Tab, under Advance Settings, check **Specify authentication mode** and select **User or computer authentication**. Proceed to click Ok to close configuration menus. Restart the computer and login to computer using domain user name.



17. Navigate to reach the following menu. If the configuration is successful, the network **NTUSECURE** status is **Connected**.




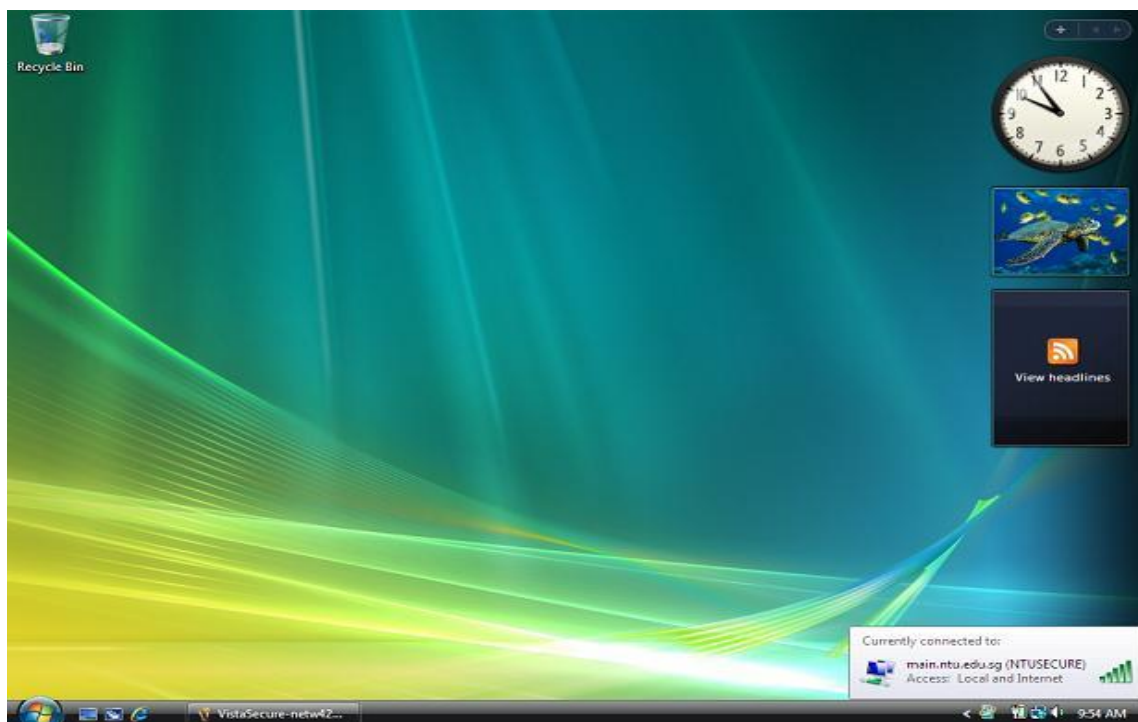
18. Navigate to reach the following menu. At **Network and Sharing Center** menu, click Internet icon to test Internet browsing.



19. For a successful Internet connection, the following default web page of Internet Explorer will be displayed.



20. At desktop, you can also move your mouse cursor to icon  at system tray to check the network status as shown in the following. If the connection status is **Access: Local and Internet**, you have logged on to NTU wireless network successfully.



Congratulations. You have completed the configuration.