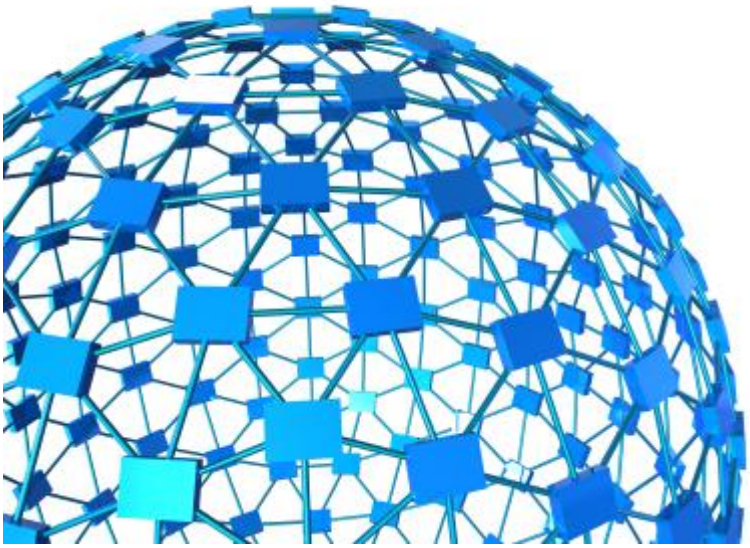
The MUO Network Manual



By Stefan Neagu

Tux Geek

This page intentionally left blank

Table of Contents

Why a Guide about Networking?

Networking is still a delicate subject for many people. Today, everyone needs to know how to set up a local or home network, share printers, share internet connection and protect their privacy online using services like VPN or encrypting your network traffic.

You're not alone. Most of the people I know that don't work in technology-related positions don't know what even the simplest of acronyms mean or how to set up a wireless network at home. This guide aims to provide you with all the basics you need to deal with networking related tasks.

Apart from the concepts and terminology, this guide is aimed at Windows users. Linux users will have a networking chapter in another upcoming eBook.

Networking Basics

Before diving in to the how-to part of this guide, it is essential to know some basic terms and acronyms. You don't need to learn them immediately, just look them up as you encounter them in the guide. This will help you make logical connections between the terminology and real-life situations.

Note: At the editor's request many of the terminology here is very simplified. A full unabridged explanation is available on Wikipedia and on the day of publication on [tuxgeek.me].

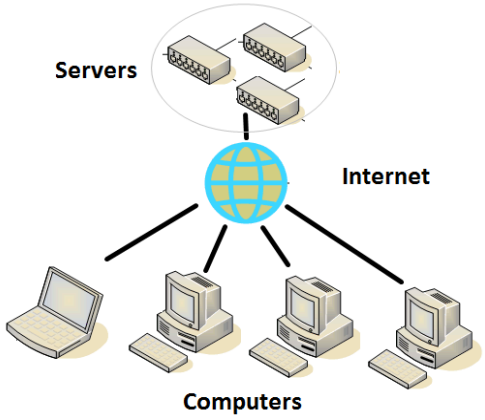
1. Computer Network – computers that are linked to each other (by a physical transport layer) using Optical fiber, Ethernet, Wireless LAN, HomePNA or Power Line. By connecting computers or network-capable appliances you can choose to share and access resources and information.

2. LAN - A local area network is a computer network with a limited range, usually considered to be less than 1KM. Common examples where a LAN might be implemented are at home, office, or small group of buildings, such as a school, or an airport. LANs are characterized by high speed data transfer rates.

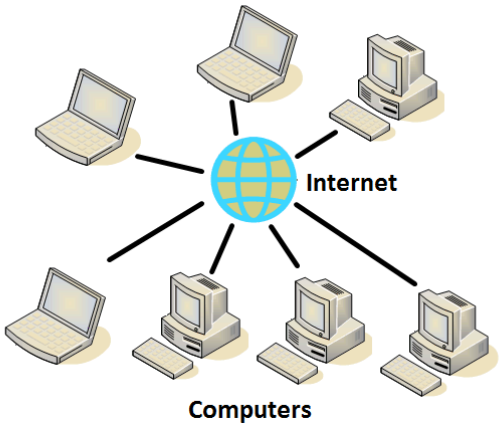
3. Network Architecture –

- The client-server architecture differentiates client systems from server systems. A common example that illustrates this model are websites. Your computer establishes a connection to the MakeUseOf server which sends back the web page over the Internet. An analogy would be broadcasting (one to many distribution model). This model is illustrated in the first image.
- A peer-to-peer (or P2P) architecture uses the cumulative bandwidth of network participants rather than centralized resources (servers). On a peer to peer network every participant is both a client and a server. This architecture is widely used in various file sharing software, including the notorious BitTorrent protocol. This model is illustrated in the second image.

The client-server architecture



A peer-to-peer (or P2P) architecture



MAC Address - Media Access Control address (MAC address) is a unique identifier assigned to network adapters, similar to your unique Social Security Number.

Network Card – otherwise known as a network adapter, is a piece of computer hardware that enables computers to communicate to each other.

Network Bridge - A network bridge connects multiple network segments. Consider it to be like a traffic police man directing traffic in an intersection.

Network Switch – A network switch usually forwards all the traffic by using MAC addresses to differentiate between peers.

TCP/IP - The Transmission Control Protocol is one of the main protocols of the Internet Protocol Suite, with which it works in tight integration. It's like a computer program that makes the internet work.

Ethernet Cable – is a twisted pair (4 pairs) high signal integrity cable type with the RJ45. It is also known as CAT5 cable.

DHCP - DHCP basically takes care of various settings automatically, so you don't have to read a 300 page book to set up a network.

WiFi - is a trademark of the Wi-Fi Alliance for products based on the IEEE 802.11 (W-LAN) standards. This certification warrants interoperability between different wireless devices. There are many variations of IEEE 802.11. The most important and current standards are contained in this table:

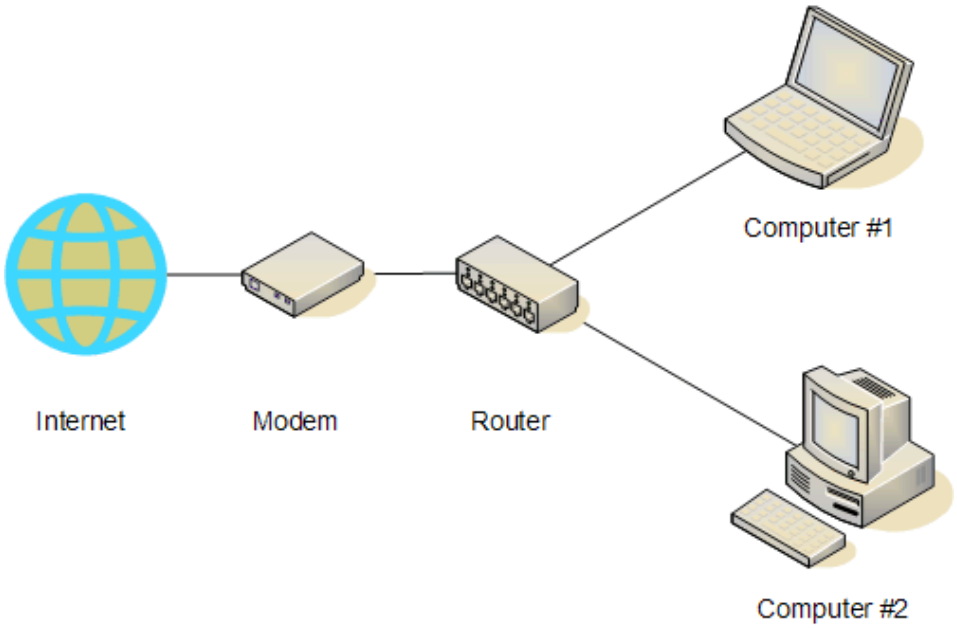
Name	Frequency	Release Date	Speed	Range(Indoors/Outdoors)
802.11N	2,4Ghz	January 2010*	600 Mbits/s	38 Meters/250 Meters
802.11G	2,4Ghz	June 2003	54 Mbits/s	70 Meters/140 Meters
802.11Y	3,7Ghz	November 2008	54 Mbits/s	50 Meters/5000 Meters

802.11n is the standard most used today and is recommended if you're trying to set up a wireless network. *The standard is set to be ratified in Jan 2010, all the currently available wireless routers are certified using Draft specifications.

Set up a local wired network

Setting up a wired network is not as common as it used to be a few years back. Wired connections still have the best bandwidth and are not affected by common household RF(radio-frequency) interference. However, it can be inconvenient to install Ethernet cables around the house, so wireless is slowly gaining in popularity. If your house doesn't have Ethernet cables in the walls and the appropriate wall plugs, you should consider the wireless alternative.

Here's how the network topology will look like:



1. Buy a router with a number of ports close to the number of computers. For most people an 8-port router will suffice. You can start your search by looking at the Newegg page for wired networking. A good choice would be the LINKSYS BEFSR81. This router will connect to your existing internet connection via an Ethernet cable. It will also connect to your other computers through the same type of cable.
2. Connect the cable to the port available on your computer, as shown in the picture below. Do this for all the computers you wish to connect.

3. Connect the other end of the cable to the router. Afterward, connect the internet cable to the indicated port.

In 99% percent of the cases, this is all you need to do in order to set up a network. The router and computer is already set up to use DHCP and should configure automatically.

4. If your computer doesn't automatically recognize the internet connection, you need to apply the settings your ISP (Internet Service Provider) gave to you when you registered to the router. This may be a PPPOE username/password combination or another validation method. The router manual contains instructions on how to access the configuration application of the router. These days, router interfaces are user friendly and are easily configured, just refer to the manual.

Once the network is set up, read through the sections that explain how to share files and do other network related tasks.

Modems are devices that negotiate a connection between your internet service provider and a network interface (computer, laptop, router). Most routers have integrated modem capabilities (for PPOE connections for example), but cannot interface directly to connections that don't use the RJ-45 connector. That's why usually internet providers have a modem that connects the internet line with the router from where connection distributed to all connected PCs. Also modems do not usually have the capability to connect to multiple computers at the same time but routers do. That's why when you want to use one internet line for multiple PCs you almost always need a router.

Set up a local wireless network

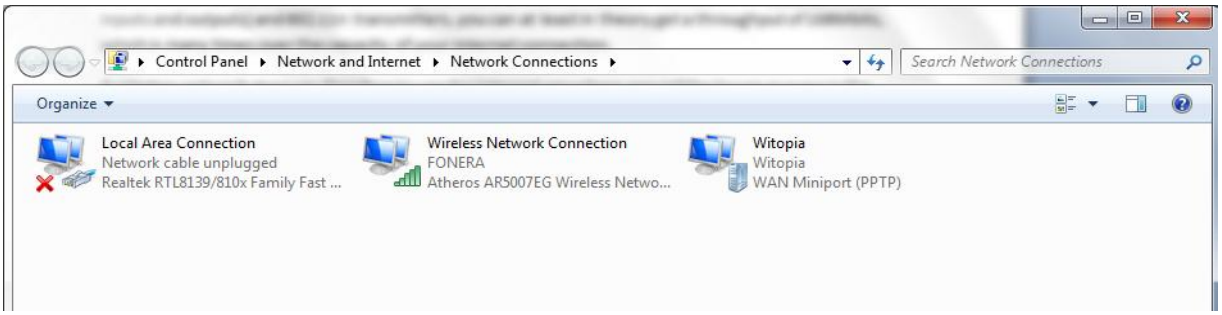
Wireless networks today offer enough speed to satisfy even the most prolific file-sharing, movie streaming, network backup fanatic. Using the latest generation of wireless routers, equipped with MIMO(multiple inputs and outputs) and 802.11n transmitters, you can at least in theory get a throughput of 108Mbits, which is many times over the capacity of your internet connection.

A wireless network gives you freedom to use the Internet anywhere around the house or even in the backyard. Considering how many mobile devices support wireless networking today, it's a good investment for the future.

Wireless networks are slower and less reliable than wired connections. Some security researchers consider that wireless is an inherently flawed technology – data can be trapped and analyzed later without the need of a physical tap. Setting up a wireless network is hassle free and can be easily upgraded later, no need to change the cables in all of your house.

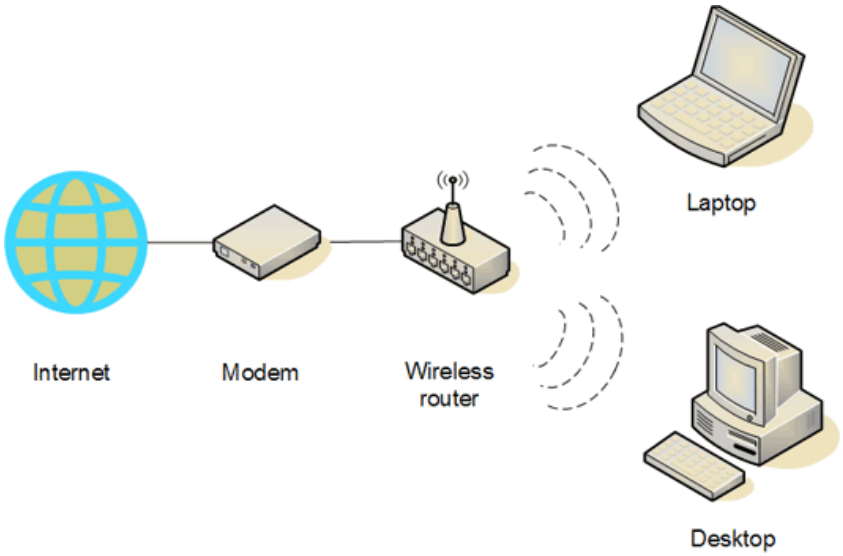
In order to set up a wireless network you need a router and a device with a wireless network adapter. This could be your PC, laptop or iPod touch. A good place to start shopping for a wireless router is the Newegg page [http://www.newegg.com/Store/Category.aspx?Category=41&name=Wireless-Networking]. A good wireless router is the LINKSYS WRT610N available here [http://www.newegg.com/Store/Category.aspx?Category=41&name=Wireless-Networking].

Now go to Control Panel and check to see if you have a wireless network adapter already installed. Most of the laptops and netbooks these days come with an inetrnal wireless network adapter (look for ON/OFF WLAN switch).



If not, visit the Newegg page and buy one of the USB adapters. They are fairly cheap and most work directly out of the box. PC/Cardbus/ExpressCard adapters are also available for purchase. A good choice would be the D-Link WUA-1340 available here.

Let's take a look at how the network topology is going to be:



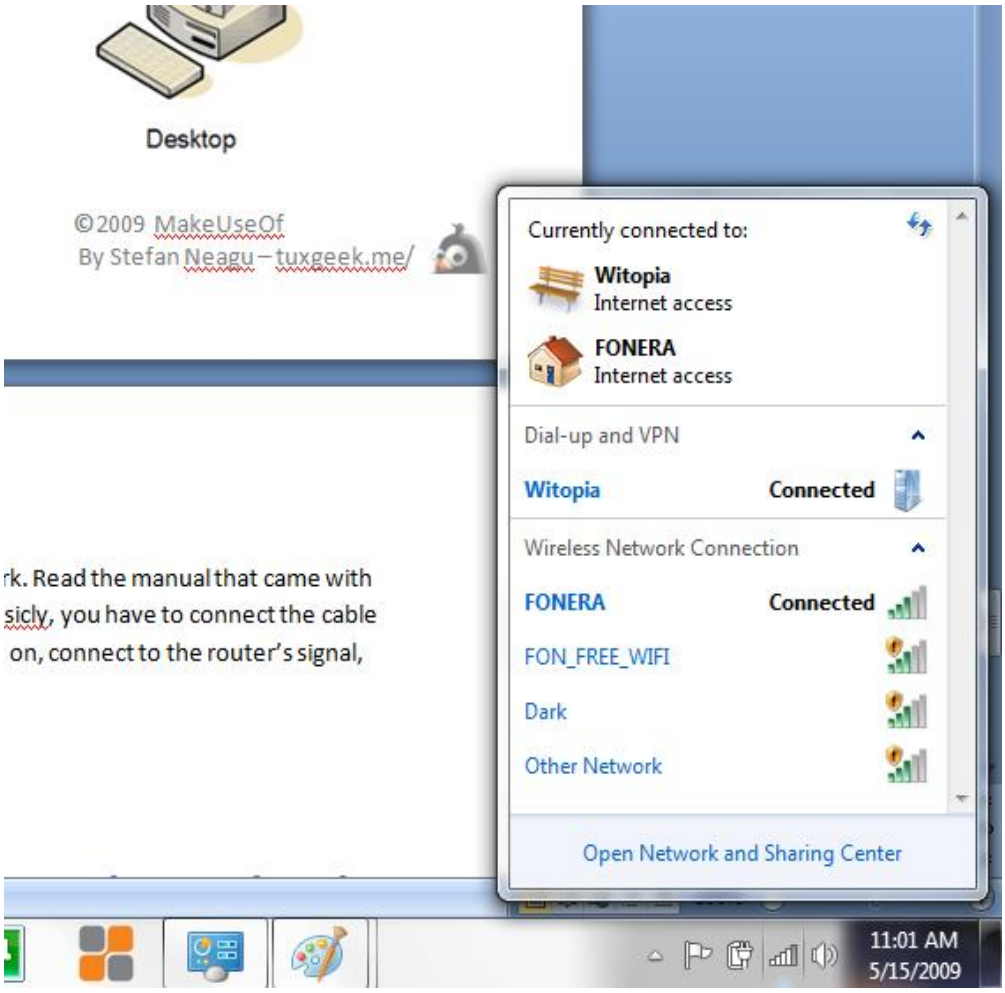
Once you have all the hardware you're ready to set up the network. Read the manual that came with the router and connect your internet connection to the router. Basically, you have to connect the cable from your cable/DSL router to the wireless router, turn the router on, connect to the router's signal, access a web configuration page and do some minor tweaks.

Modern wireless routers are extremely easy to configure, and most come with wizards and walkthroughs that explain everything as you go along. Here is a screenshot of my configuration panel that I access by typing 192.168.10.1 in the address bar of my browser. That address is the IP address of the wireless router, and may be different for your router, but it is clearly pointed out in the router's manual.Here are some links to sites that provide addresses:

- http://www.makeuseof.com/dir/router-passwords-default-passwords-routers/
- http://www.makeuseof.com/dir/cirtnet-lookup-default-passwords-electronic-devices/

The La Fonera 2.0 router is a perfect example of an easy to use web configuration application. Simply click on Settings>Internet>Connection Type>Username/Password.

If all your computers are 802.11N compatible, you'll also want to lock the network mode to N. This will disable access to the network to any non-N adapter which will prevent the network from downgrading the speed to the lower specifications. Particularly useful if you're going to set up an open wireless network – which doesn't require a password and allows anyone in range to connect (common for coffee shops, public places).



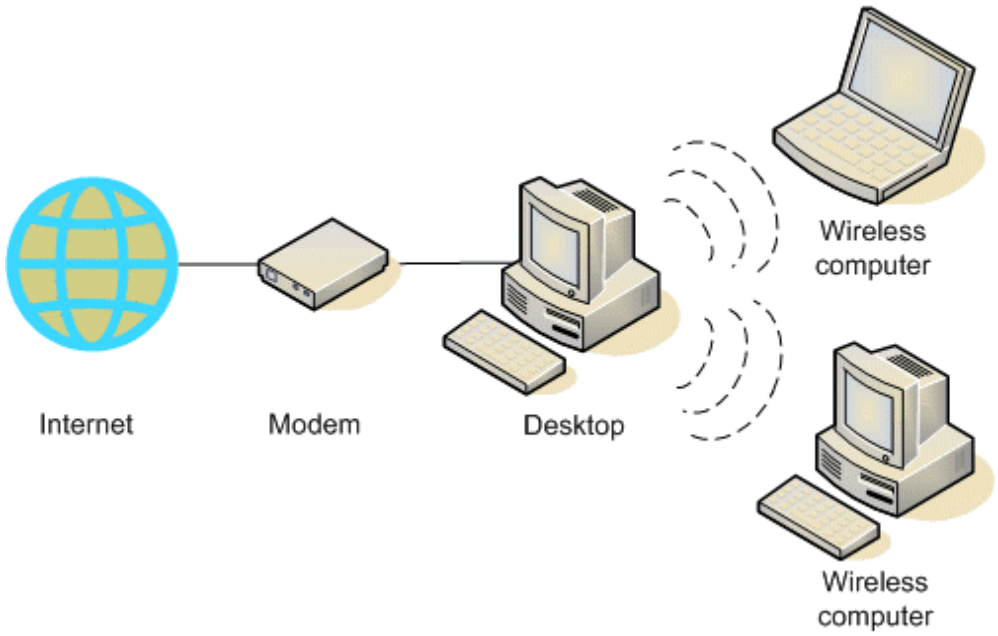
Back in Windows, you can either click on the taskbar icon, which is available on all versions of Windows since 2000 or bring up the control panel. Depending on your version, either right-click on the wireless network adapter and select **Connect**, or use the **Connect to a network** link.

Screenshots presented are from the upcoming Windows 7 operating system. In Windows 7 networking gets a much needed facelift and small usability enhancements. For example, the jumplist containing network connections.

Set up an ad-hoc wireless network

Not very well known and understood are the so called ad-hoc networks. Ad-hoc networks are wireless networks created between two or more computers which instead of having a dedicated router, they have a computer that takes care of that task.

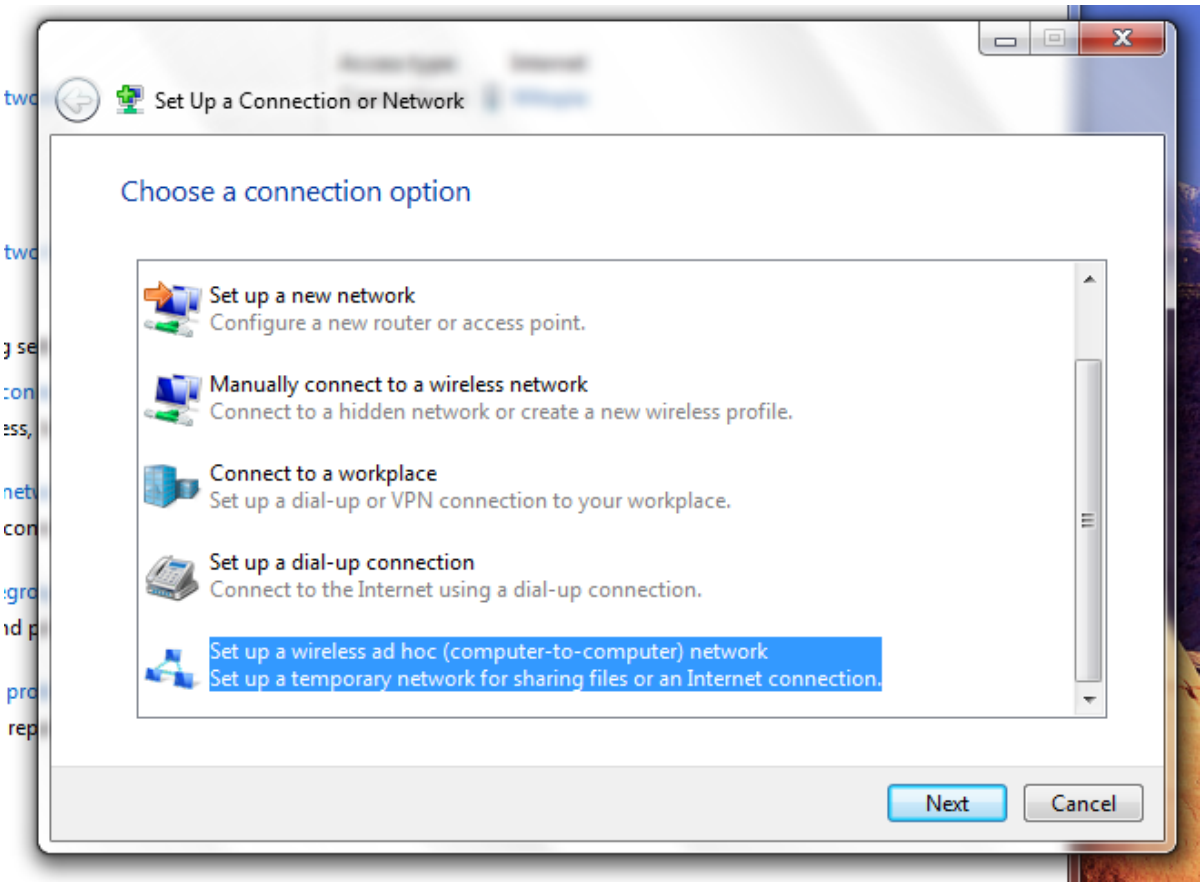
Combined with the ICS(Internet Connection Sharing) wizard – it's a fast and no-cost alternative to a router. Using an older computer equipped with a decent MIMO wireless card to provide the router capabilities is not as easy as using a standalone router.

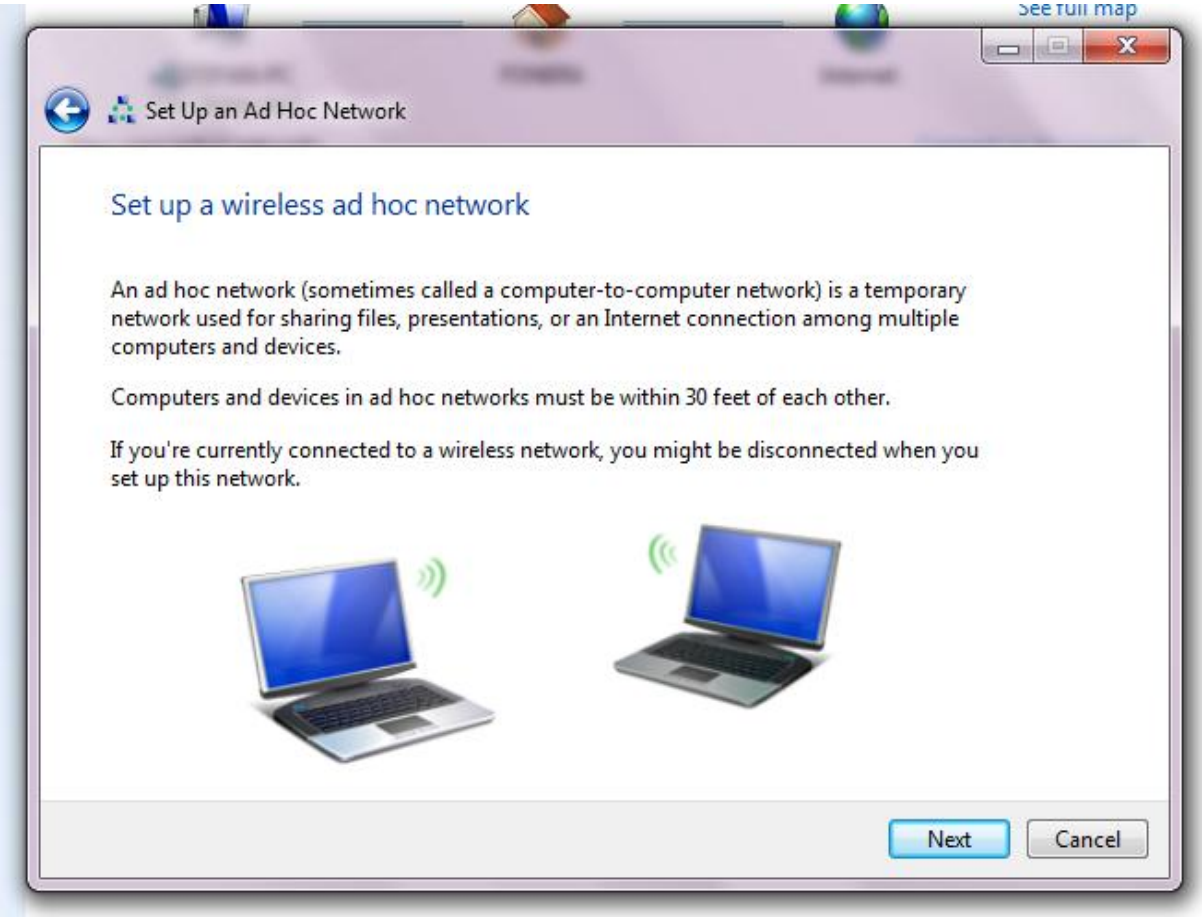


It's important to bolt down the computer with a decent security suite, a stateful packet inspection firewall and always keep it up to date with patches. I use the Yoggie Gatekeeper Pro to protect the network and also have Kaspersky AV on each of the Windows machines as a backup. Having a real computer on the job gives you flexibility – printer sharing, networked storage – but it can make it easier for hackers to get into your network.

Geeks usually set the computer-router with a Linux distribution, and for good reasons, but it is still difficult to get right and sometimes updates mess up the configurations and packages. Also, you may find that your card will work slower or not at all because of missing or incompatible drivers.

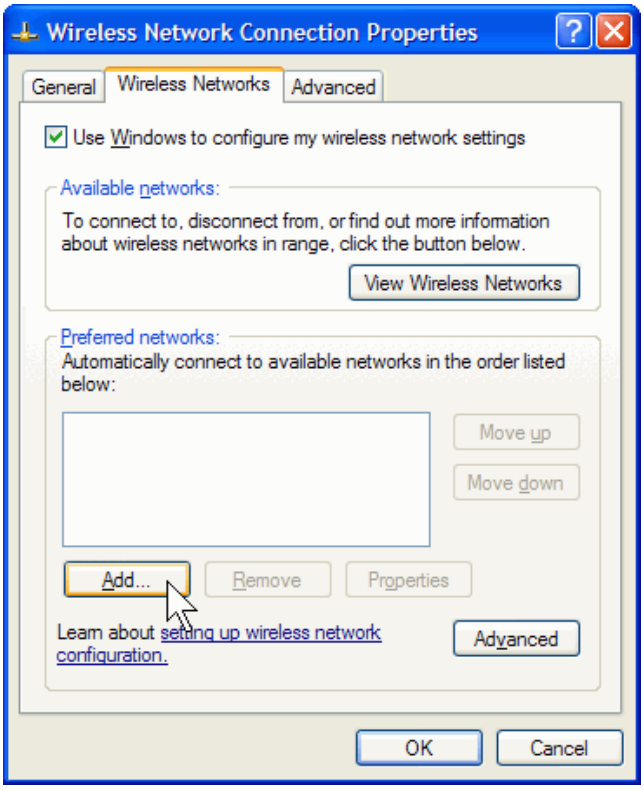
To create an ad-hoc network you need to have at least two network adapters, one that connect to the internet and a second which connects to the internal network. Ad-hoc networks are very easy to set up in Windows Vista and Windows 7 from Network and Sharing Center>Set Up a Connection or Network> Ad-hoc Network. All you have to do on these systems is read the short instructions presented on the screen.

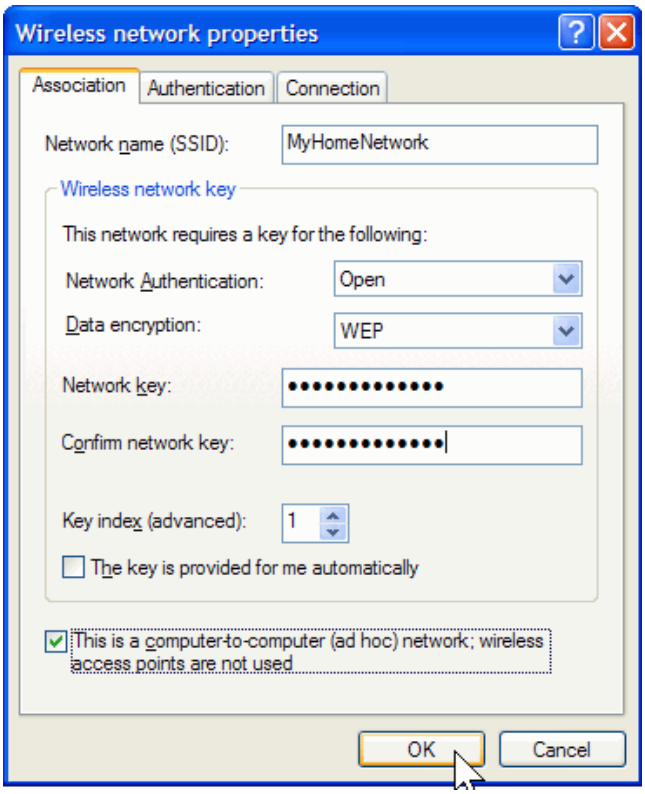

Set Up a Connection or Network
Choose a connection option
Set up a new network
Configure a new router or access point.
Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.
Set up a dial-up connection
Connect to the Internet using a dial-up connection.
Set up a wireless ad hoc (computer-to-computer) network
Set up a temporary network for sharing files or an Internet connection.
Next
Cancel


Set Up an Ad Hoc Network
Set up a wireless ad hoc network
An ad hoc network (sometimes called a computer-to-computer network) is a temporary network used for sharing files, presentations, or an Internet connection among multiple computers and devices.
Computers and devices in ad hoc networks must be within 30 feet of each other.
If you're currently connected to a wireless network, you might be disconnected when you set up this network.
Next
Cancel

Setting up an ad-hoc network on Windows XP is a little more complicated.

1. Right-click your wireless network connection, and then click **Properties**.
2. In the **Wireless Network Connection Properties** dialog box, click the **Wireless Networks** tab.
3. On the **Wireless Networks** tab, under **Preferred networks**, click **Add**.



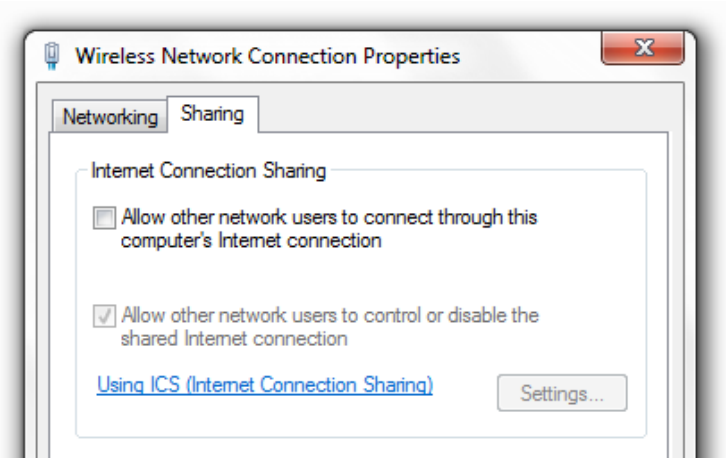


4. In the **Wireless network properties** dialog box, on the **Association** tab, type the name of your ad hoc wireless network in **Network name (SSID)** box.
5. Clear the **The key is provided for me automatically** check box and select the **This is a computer-to-computer (ad hoc) network** check box.
6. (optional) Create a 13-digit password and type it in both the **Network key** and **Confirm network key** boxes. For the best security, include letters, numbers, and punctuation. Then click **OK**.
7. Click **OK** again to save your changes.

Internet Connection Sharing

To use Internet Connection Sharing to share your Internet connection, the host computer must have at least two adapters. One of them needs to connect to the internal network (that has other PCs that want to use its internet connection), and the other must provide an internet connection. The configuration process takes place on the host computer.

1. Log on to the host computer as Administrator.
2. Click Start and then click Control Panel.
3. Click Network and Internet Connections.
4. Click Network Connections.
5. Right-click the connection that you use to connect to the Internet.
6. Click Properties.
7. Click the Advanced tab.



8. Under Internet Connection Sharing, select the Allow other network users to connect through this computer's Internet connection check box. Click OK.

   You receive the following message:

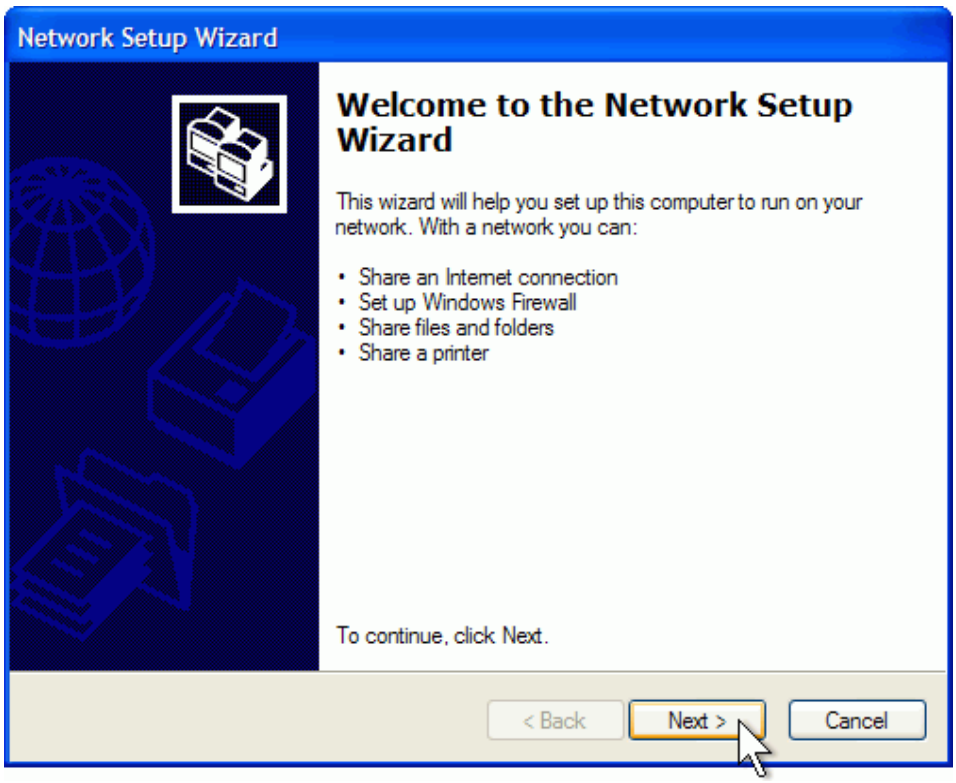
   When Internet Connection Sharing is enabled, your LAN adapter will be set to use IP address 192.168.0.1. Your computer may lose connectivity with other computers on your network. If these other computers have static IP addresses, it is a good idea to set them to obtain their IP addresses automatically. Are you sure you want to enable Internet Connection Sharing?

9. Click Yes.

Connecting to other computers, and sharing files and printers

Sharing files and printers on newer versions of Windows doesn't require you to run this wizard. If you're running on Vista or Windows 7, skip over these instructions.

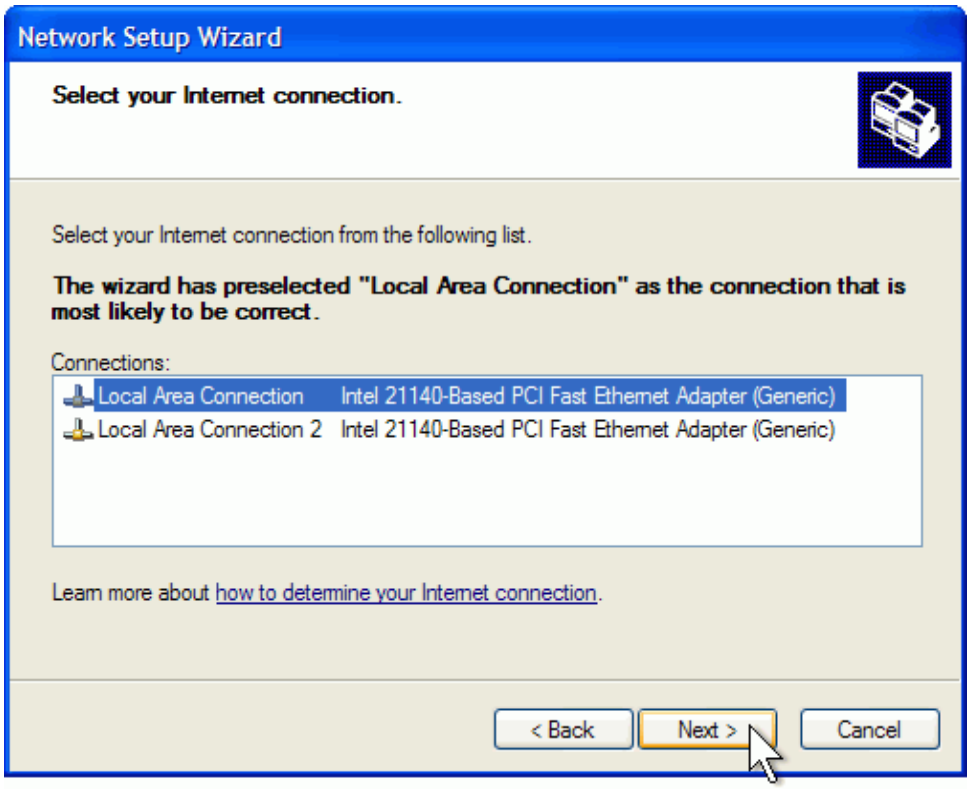
1. Log on as a member of the Administrators group.
2. Click **Start**, and then click **Control Panel**.
3. Click **Network and Internet Connections**.
4. Under **or pick a Control Panel icon**, click **Network Setup Wizard**.
5. The Network Setup Wizard starts. On the **Welcome** page, click **Next**.



6. On the **Before you continue** page, click **Next**.
7. If the wizard informs you that it has found disconnected hardware, make sure your network adapter is connected as described in Add a computer to your network. It's okay to have a disconnected network adapter if you're using a wireless network connection or if you connect to the network using a USB (Universal Serial Bus) cable. If you're sure everything has already been properly connected, select **Ignore disconnected network hardware**. Otherwise, connect your network cables, and leave the check box cleared. Then click **Next**.
8. If you connect your computer directly to the modem provided by your ISP, click **This computer connects directly to the Internet**. If you connect

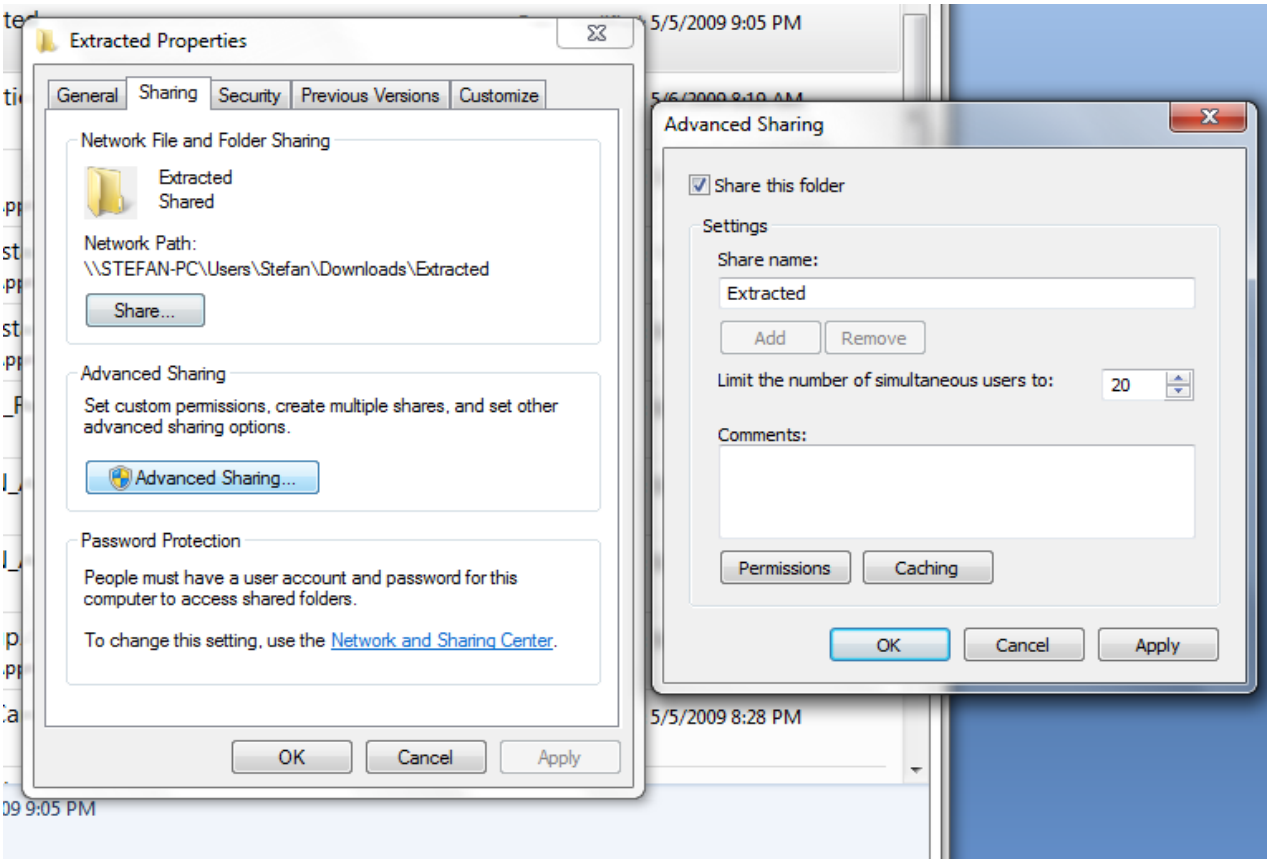
your computer to a router, click **This computer connects to the Internet through a residential gateway**. If you're not sure, leave the default setting. Then click **Next**.

9. If the **Select your Internet connection** page appears, click **Next**.



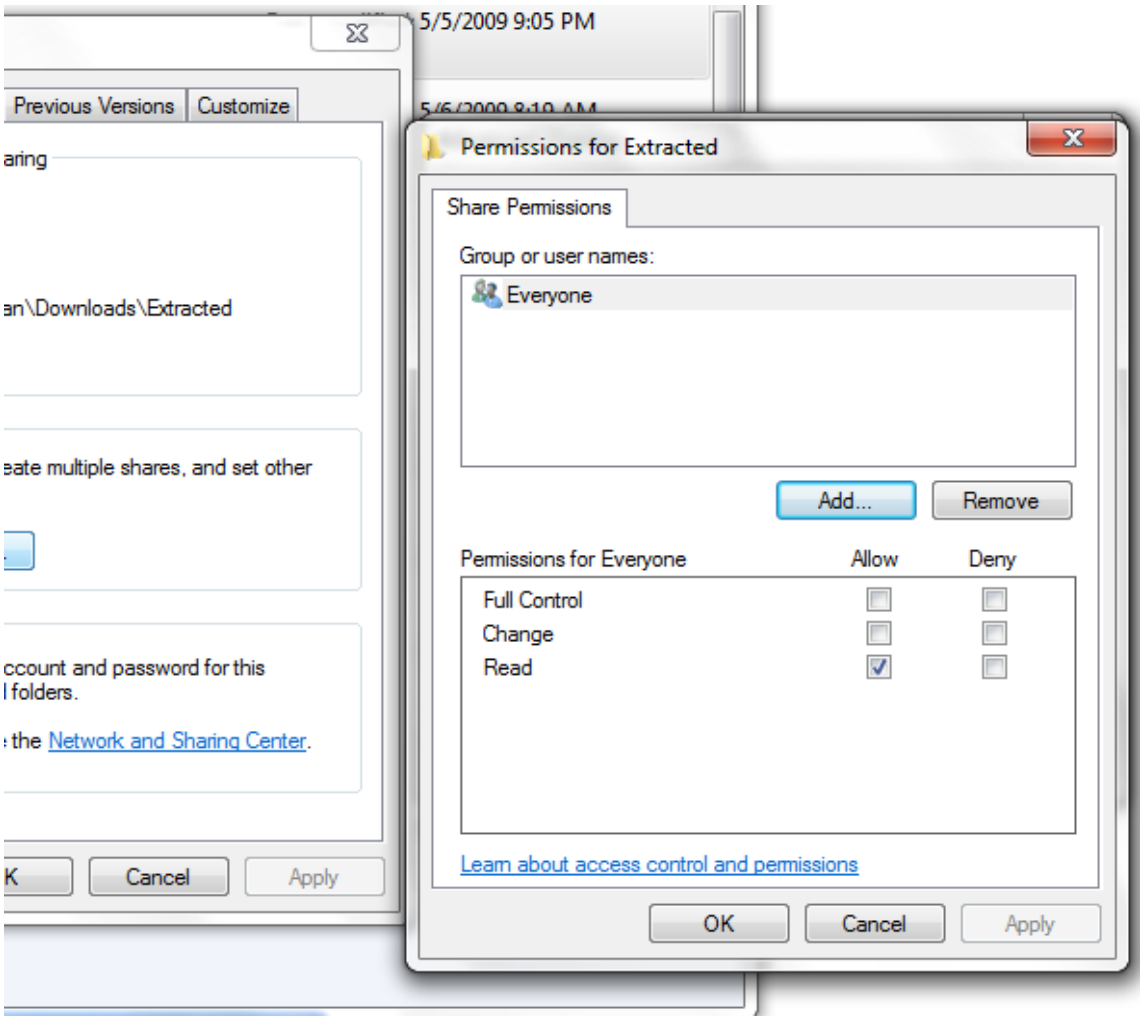
10. On the **Give this computer a description and name** page, type a computer description (such as "Kid's Computer") and computer name (such as "Desktop"). Click **Next**.
11. On the **Name your network** page, type **Workgroup**. Then click **Next**.
12. If you have files or a printer that you want to share with other computers on your home network, select **Turn on file and printer sharing**. Otherwise, leave **Turn off file and printer sharing** selected. Then click **Next**.
13. On the **Ready to apply network settings** page, click **Next**.
14. The **Network Setup Wizard** sets up your computer. On the **You're almost done** page, click **Just finish the wizard**. Then click **Next**.
15. On the **Completing the Network Setup Wizard** page, click **Finish**.
16. When prompted to restart your computer, save any open files, and then click **Yes**.

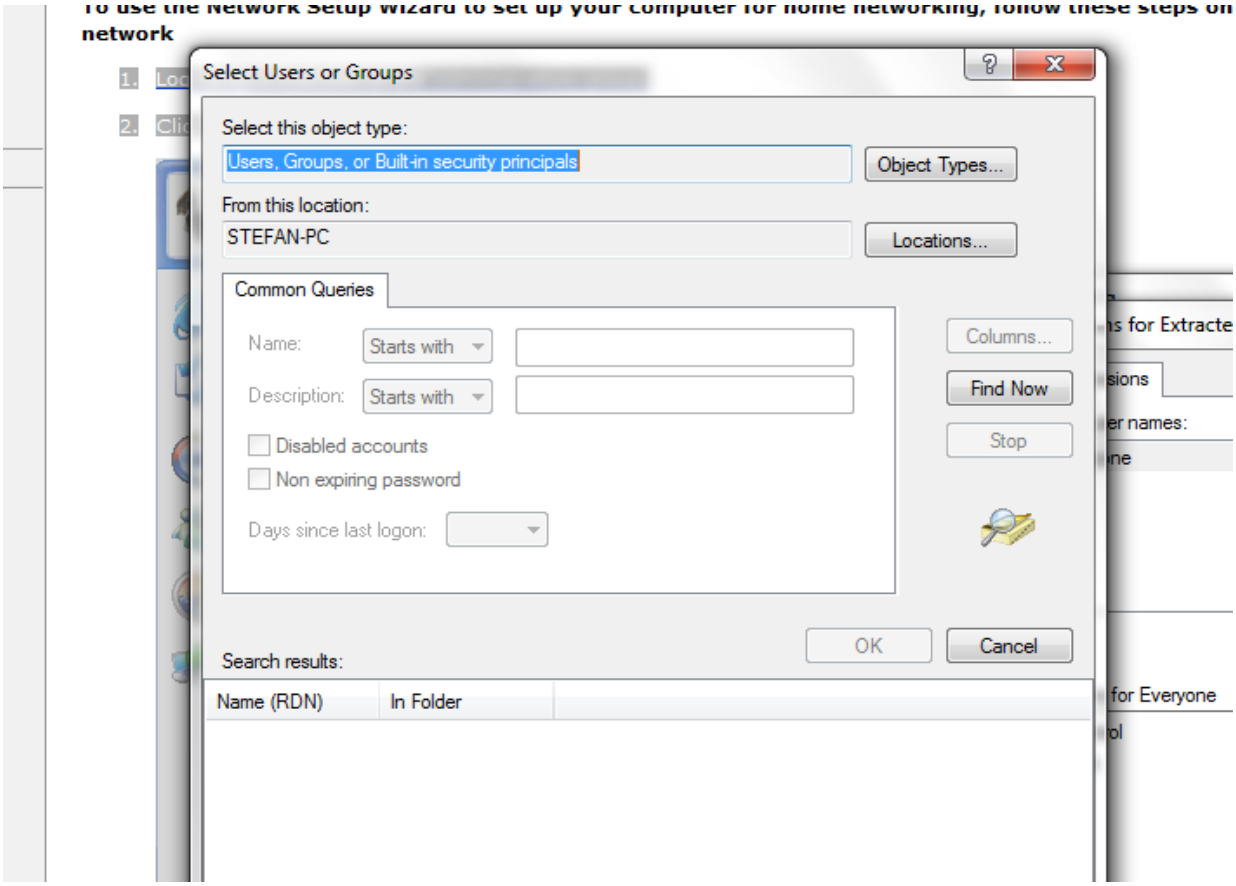
You need to run this wizard on each of the computers you want to be visible on the network. After completing this wizard, right click on any folder and then on **Properties**. Go to the **Sharing and Security** or just **Sharing** tab, depending on the operating system version.



Depending on where the folder is located, you'll need to configure additional settings. For example, if you want to share a folder which is in a protected area like **Documents**, the user who wishes to access that needs to have an account on the host computer.

You could authorize **Everyone** with Full-permissions (meaning that they will be able to view/edit/delete files) or Read-only if you're in a private network, like a WPA2 secured home network. You can also authorize any other visible (with Remote Desktop Connection on) accounts on the network from **Permissions>Add>Advanced**. They will appear in the box and then you can select and authenticate.

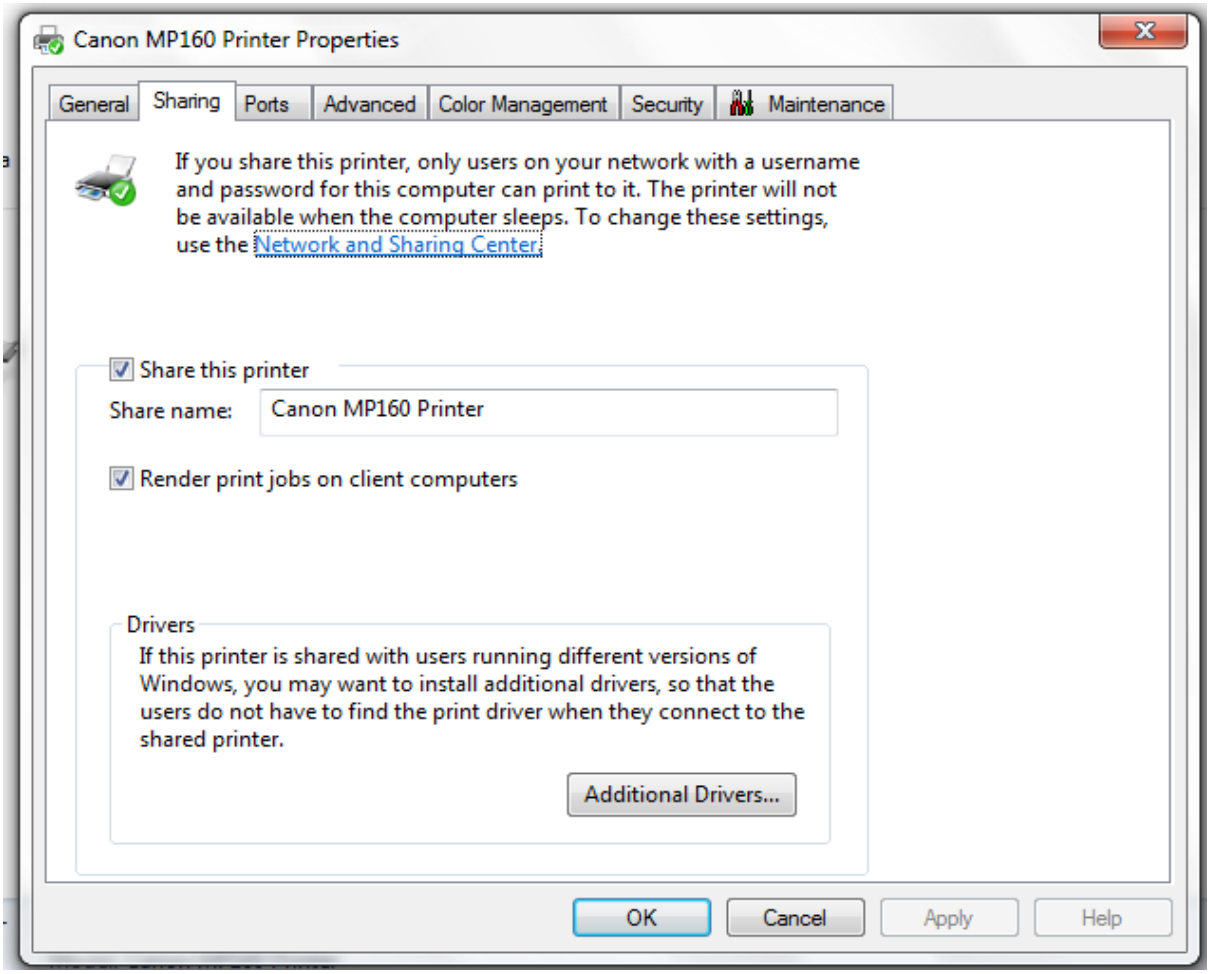

5/5/2009 9:05 PM
Previous Versions
Customize
aring
an\Downloads\Extracted
eate multiple shares, and set other
ccount and password for this
l folders.
the Network and Sharing Center.
K
Cancel
Apply
Permissions for Extracted
Share Permissions
Group or user names:
Everyone
Add...
Remove
Permissions for Everyone
Allow
Deny
Full Control
Change
Read
Learn about access control and permissions
OK
Cancel
Apply



If you ran the Network Setup Wizard like instructed before, your printer is already available on the network. Windows Vista and Windows 7 will share the printer automatically.

If for some reason that doesn't work you need to click Start>Control Panel>Printers and Other Hardware>Right Click on Printer Icon>Printer Properties>Share Printer. Type in a name for the printer and click OK.

On the other computers open Control Panel>Printers and Other Hardware>Add a Print> click Printer Connection and then browse the network for the printer.

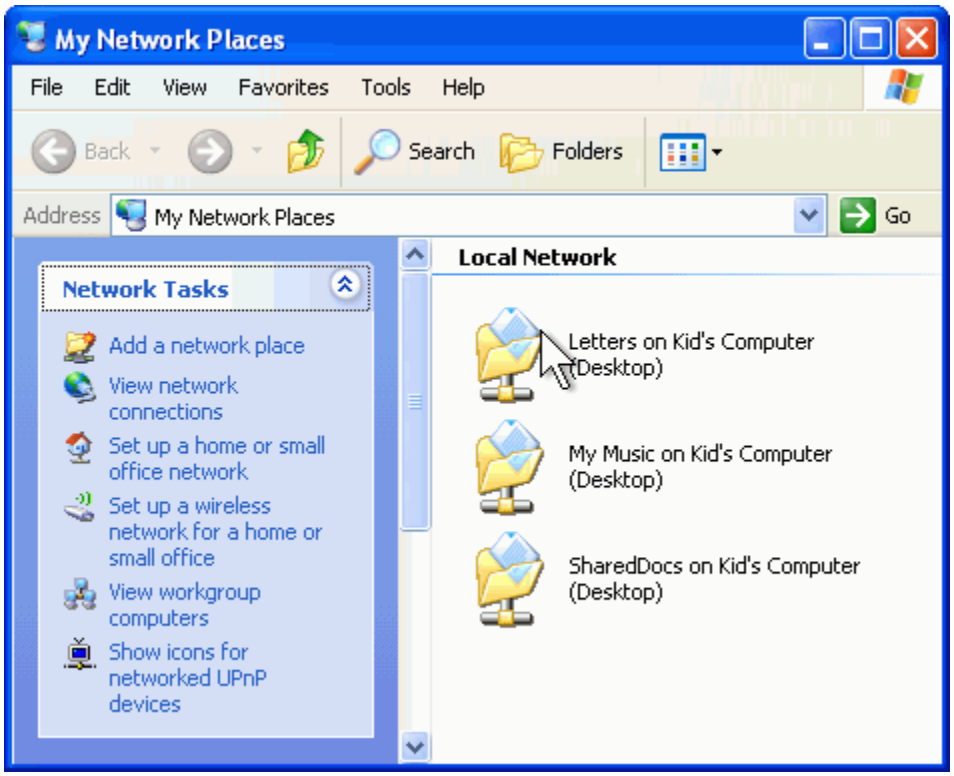


Open a shared folder

1.On your **desktop**, double-click **My Network Places**.

Note: If **My Network Places** is not on your desktop, click **Start**, and then click **My Network Places** on the **Start** menu.

2.In **My Network Places**, double-click the folder you want to open.



You'll see your files in the folder.

In Windows 7 type Network in the Start menu search box and hit enter.

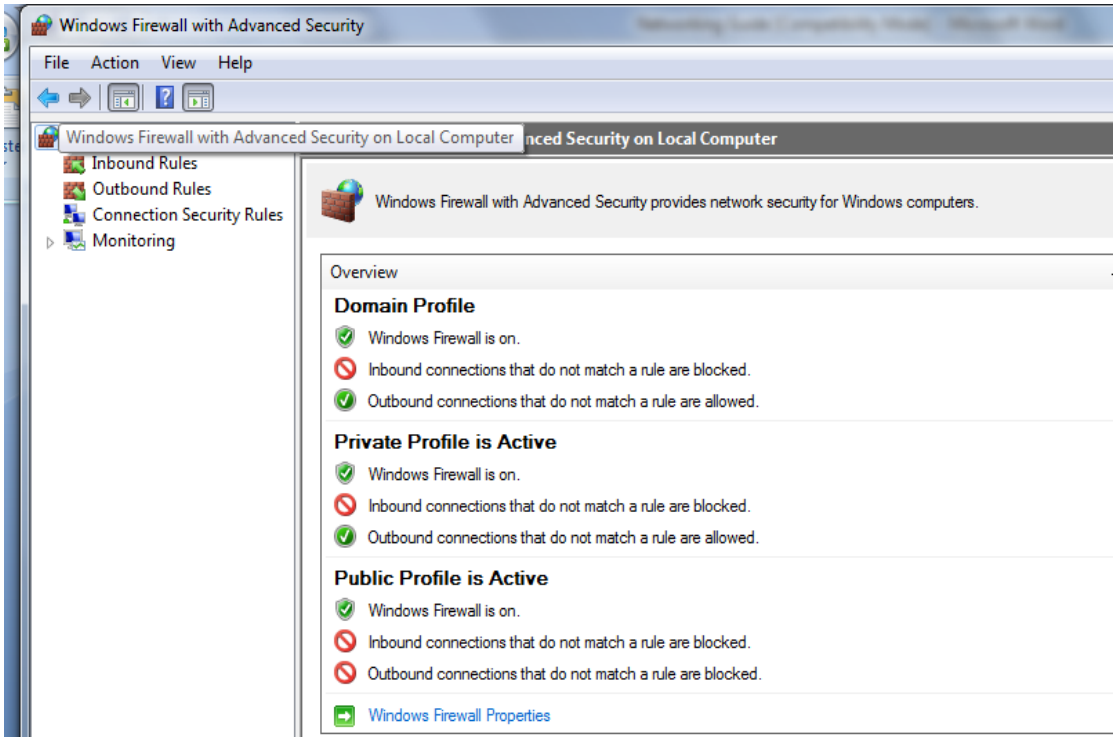
Security

Firewall: Why you need it, what is it, alternatives and configuration

A firewall is special kind of software that is designed to block unauthorized access while permitting safe communication. It discriminates between wanted and unwanted traffic by using a set of rules that can be modified by the user if he chooses to do so.Firewalls are available as separate hardware products like the Yoggie Gatekeeper products, integrated in the routers' software or standalone, as a software program on your computer. There are many advantages and disadvantages to each platform. Out of the three, the most secure is the hardware firewall. It also reduces the load on the computer, leaving more resources available for your applications.

Firewalls are frequently used to prevent unauthorized access of private resources, like those available on a company network (also known as intranet) from other users on the Internet. All communications entering or leaving the network pass through the firewall, which examines each message and blocks those that do not meet the specified security guidelines.

Windows XP, Vista and 7 have built-in firewalls, but just the latter can be considered to be actually useful by a security conscious person. While exposing quite a lot of functionality, the interface is not cluttered and is easy to use. For a comprehensive comparison chart on available firewall solutions I invite you to visit [en.wikipedia.org/wiki/Comparison_of_firewalls] .



Check out MakeUseof Poll on Firewalls: [http://www.makeuseof.com/tag/muo-polls-what-firewall-software-do-you-use/]

WEP, WPA, WPA2 and MAC Address Filtering

While wired connections are inherently safe because of the physical link, wireless networks are based on radio technology. This means that everyone in range of the transmitter – around 30-50 Meters – can listen to everything that is transmitted.

Hackers with software called network sniffers coupled with packet reassembly can recreate your traffic and steal your passwords, conversations, email, pictures and so on.

To protect the transmission security researchers created WEP(Wired Equivalent Privacy), a routine that encrypts your transmission before sending it to the router. But this encryption wasn't so great – it had numerous flaws – and could be cracked in less than 5 minutes. Researchers then came up with WPA(Wi-Fi Protected Access), a stronger encryption algorithm. This too has flaws and given enough time can be cracked as well. WPA2, the successor to WPA, is much improved and coupled with the AES(Advanced Encryption Standard) cipher is considered to be fully secure.

Another way of protecting networks in the old days was to use static IP addresses, hide the SSID(router name broadcast signal) and filter connection requests by checking the MAC address against a table stored in the router memory. This method is terribly flawed and can be bypassed in less than 10 minutes.

1. Hackers can sniff the network; capture unencrypted packets which contain the header with the IP address and the MAC address.
2. Using a simple command you can change the IP and MAC address of your network card to the one you captured.
3. Wireless scanners can be configured to show all available signals regardless if they router is broadcasting a name or not.

If you're like me and you love to tweak settings, make sure you set up the encryption to **WPA2 with AES,** change the default password to a string at least 8 characters long and which does not contain words from the dictionary. Details about the encryption technology are presented in the upcoming sections.

Check out this link for step-by-step instructions:
[http://www.makeuseof.com/tag/secure-your-wireless-network-here-is-why-and-how/]

VPN (Virtual Private Network)

A VPN is a method of connecting to a private network (for example, your office network) using public network (the Internet) as a carrier for the data.

VPNs use authenticated data transmission protocols to make sure that only authorized users can remotely connect to the network, and they use encryption to make sure that hackers cannot use the data intercepted while traveling over the Internet.

It is a great way to still have a secure encrypted link while at an open wireless access point. A VPN connection with a decent encryption setting can thwart any sniffing attack.

To configure a VPN in Windows XP, follow these instructions:

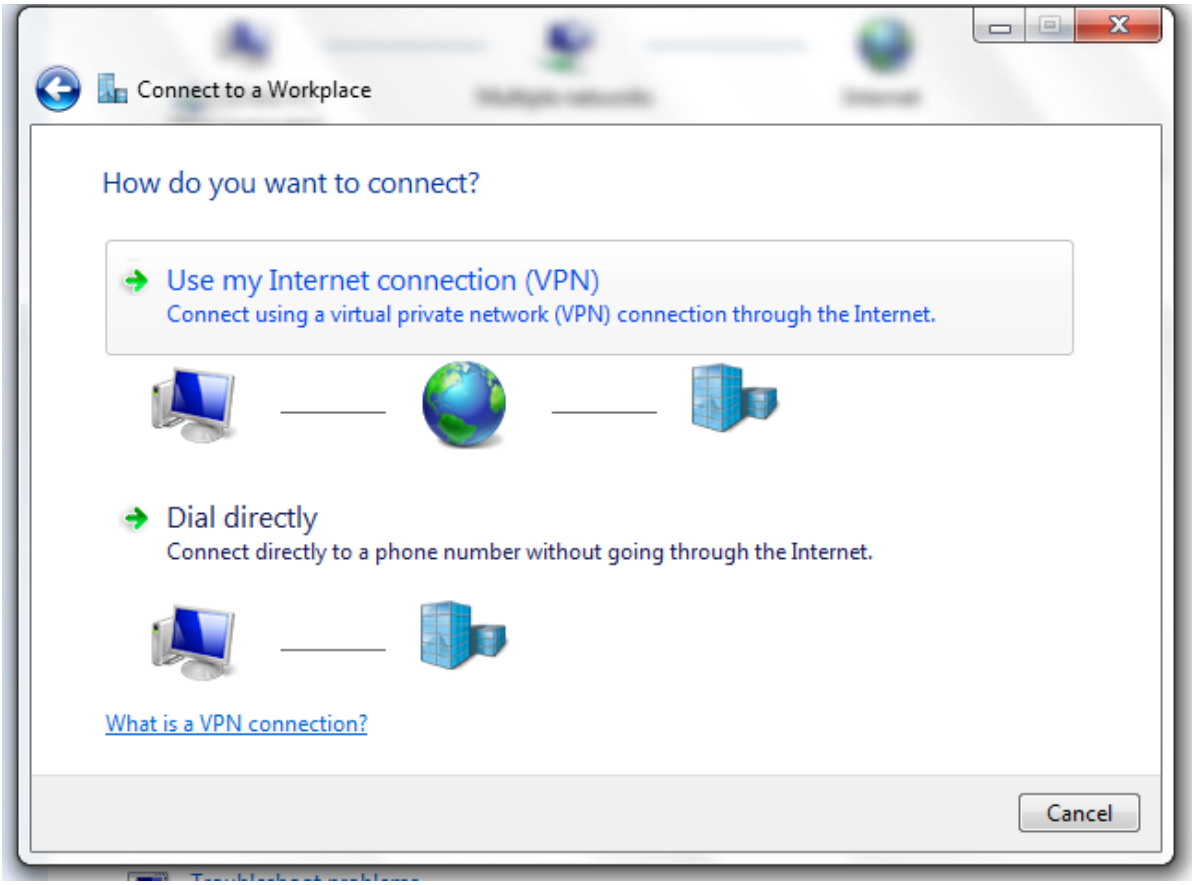
1. Click Start, and then click Control Panel.
2. In Control Panel, double-click Network Connections.
3. Click Create a new connection.
4. In the Network Connection Wizard, click Next.
5. Click Connect to the network at my workplace, and then click Next.
6. Click Virtual Private Network connection, and then click Next.
7. If you are prompted to, do one of the following:
8. If you use a dial-up connection to connect to the Internet, click Automatically dial this initial connection, and then click your dial-up Internet connection from the list.
9. If you use a full-time connection such as a cable modem, click Do not dial the initial connection.
10. Click Next.
11. Type the name of your company or type a descriptive name for the connection, and then click Next.
12. Type the host name or the Internet Protocol (IP) address of the computer that you want to connect to, and then click Next.
13. Click Anyone's use if you want the connection to be available to anyone who logs on to the computer, or click My use only to make it available only when you log on to the computer, and then click Next.

14. Click to select the Add a shortcut to this connection to my desktop check box if you want to create a shortcut on the desktop, and then click Finish.
15. If you are prompted to connect, click No.
16. In the Network Connections window, right-click the new connection.
17. Click Properties, and then configure more options for the connection:
18. If you are connecting to a domain, click the Options tab, and then click to select the Include Windows logon domain check box to specify whether to request Windows logon domain information before you try to connect.
19. If you want the computer to redial the connection if the line is dropped, click the Options tab, and then click to select the Redial if line is dropped check box.

To use the connection, follow these steps:

1. Use one of the following methods:
   - Click Start, point to Connect To, and then click the new connection.
   - If you added a connection shortcut to the desktop, double-click the shortcut on the desktop.
2. If you are not currently so, Windows offers to connect to the Internet.
3. After your computer connects to the Internet, the VPN server prompts you for your user name and password. Type your user name and password, and then click Connect. Your network resources should be available to you just like they would be with a direct connection.
4. To disconnect from the VPN, right-click the icon for the connection, and then click Disconnect.

On Windows Vista and Windows 7 all you have to do is go to **Network and Sharing Center>Set Up New Connection or Network>Connect to a workplace**. Simply follow the instructions presented for each step.



There are also programs like Hamachi that allow file sharing via VPN technology. It can be useful when trying to get to a file you have on the home computer from work. Hamachi basically simulates a local network. You may also use Hamachi to play multiplayer games with friends regardless of their location.

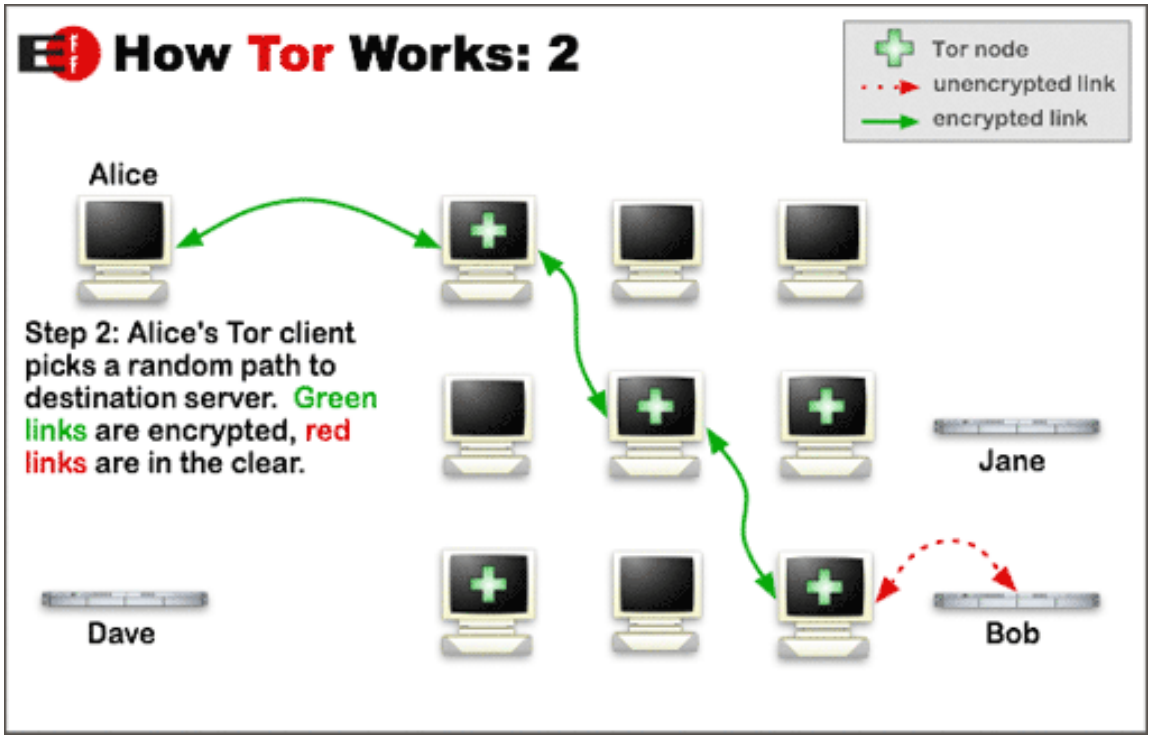
Protecting Your Identity Online

TOR

> ***Tor is free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as traffic analysis.***

Tor protects you by diverting the data stream through multiple relays that are set up by various users around the world. The data is always encrypted while en route. TOR protects anyone from spying on you and listening on your network traffic and piecing together information about what sites you visit, what you download, what messages you send via email and chat as well as hides your real physical location.

TOR is an essential tool for journalists and bloggers, human rights workers, law enforcement officers, soldiers, corporations, citizens of repressive regimes, or just ordinary citizens.



RDP(Remote Desktop Connection)

Remote Desktop, included with Windows, enables you to connect to your computer across the Internet from any computer with a Remote Desktop Client or an enabled Smartphone.

Once connected, Remote Desktop gives you control to the computer: mouse, keyboard and the same full-screen experience. There's a comprehensive guide for Windows XP available here. Configuration for newer systems remains the same.

There are several free remote desktop access applications and we mentioned quite a few of them on MakeUseOf: [http://www.makeuseof.com/tags/remote-control/]

Proxy Servers

A proxy server is a computer system or an application that acts as a mediator for requests from clients seeking resources from other servers. Instead of your computer, the server you are wanting to view sees the proxy.

A proxy server can be used to:

1. To enable anonymous surfing.
2. Speed up access to resources, mainly used by Internet Service Providers.

There are many articles discussing proxy servers available on MakeUseOf, including how to enable blocked websites and services that let you to surf internet anonymously: [http://www.makeuseof.com/tags/proxy/]

> Getting information off the Internet is like taking a drink from a fire hydrant.
>
> ~Mitch Kapor

Sources: Wikipedia, Computer Networks by Andrew S. Tanenbaum, Microsoft.com. All images licensed under Creative Commons Copyleft.

Visit MakeUseOf.com for daily posts on cool websites, free software and internet tips. If you enjoyed this guide/manual then subscribe to MakeUseOf.com (via feed or email) and get instant access to several other such guides and cheat sheets to your favorite programs.

- www.makeuseof.com (latest articles)
- www.makeuseof.com/dir/ (browser cool websites by category)
- www.makeuseof.com/most-popular/ (most popular articles)
- http://feedproxy.google.com/Makeuseof (feed)
- http://feedburner.google.com/fb/a/mailverify?uri=Makeuseof&loc=en_US (subscribe via email)

Don't miss out on our other cool manuals!

Subscribe via email or RSS to download!