Securing Network Connections

Module 7

Simplifying Security.

Certified Secure Computer User

Module 7: Securing Network Connections

Exam 112-12

Module Objectives

A fast Internet connection always enhances a browsing experience; at the same time, a fast Internet connection is also a great tool for attackers looking for **vulnerable machines**. Attackers may use it to infiltrate a user's computer and steal personal information or use the computer to disguise attacks they launch on other computers. Users are at risk of being attacked whenever they are connected to the Internet, therefore, and it is necessary for the users to **safeguard** their **network connections**.

This module will familiarize you with:

- Home Network
- Steps for Home Networking
- Wireless Networks
- Setting Up a Wireless Network
- Common Threats to Wireless Network
- Securing Wireless Network
- Using the Network with Windows 7
- Using the Network with MAC OS X
- Network Security Threats
- Securing Network Connections
- General Security Practices in Home Networking
- Network Adapters
- Troubleshooting with Network Adapters
- Network Security Checklist

Module Flow

Home and Wireless Networks

Setting Up a Wireless Network

Wireless Network Security

Using the Network with Windows 7

Using the Network with MAC OS X

Securing Network Connections

Network Adapters

Troubleshooting with Network Adapters

Home Network

Home computers are **widely used** to send emails, school work, and instant messages, as well as to download music and videos, shop, and play games. Understandably, there is an increasing trend of having multiple computers in a single household. However, multiple users in a household can **optimize** their **experiences** with computers through a **home network**. A home network can let them share:

- Files and documents
- An Internet connection
- Printers and scanners
- Stereos, TVs, and game systems
- DVD/CD burners

A simple home network is depicted in the following figure.

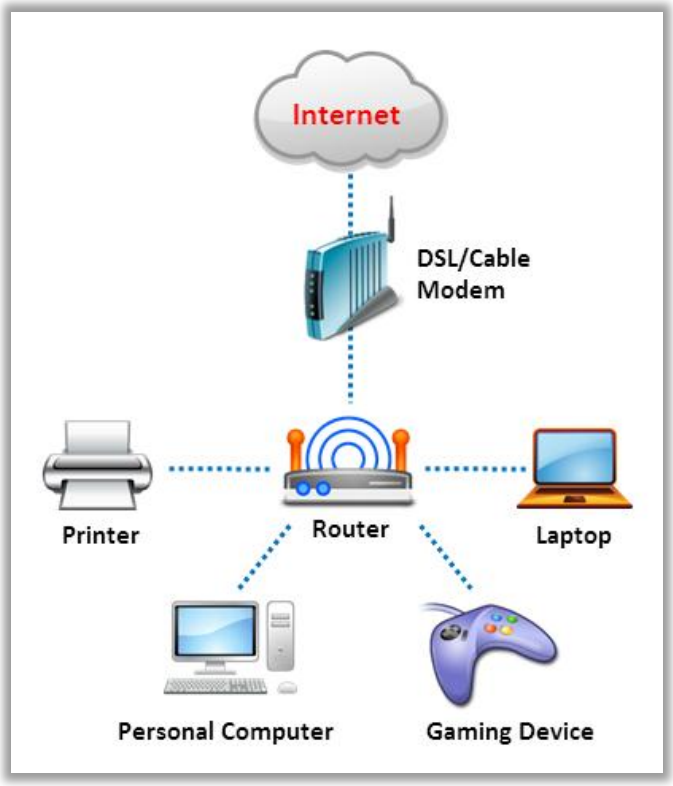


Figure 07-01: Simple Home Network

Network Devices

A network is a place where different systems are connected. Network security is the process of preventing and detecting unauthorized access over a network and ensuring that the network is secure. Some network devices include:

- **Router:**

  Routers are used for connecting the modem to the network. It determines the **next network point** to which a packet should be forwarded to its destination. Routers can access the address of a network layer and can have incorporated software that helps them **identify** the **possible paths** between the addresses and the appropriate channels to transmit data.

- **Hub/Switch:**

  A network hub/switch is a device that **directs** the **incoming data** from any of multiple input ports to the **specific output port** that will take the data toward its intended destination. A hub contains multiple ports. When a packet arrives at one port, it is copied to other ports so that all segments of the local area network (LAN) can see all packets.

- **Converter:**

  Converters are used to connect several types of cables within an existing network. They get data from a cable and **convert the signal for analog transmission** on another type of cable. Usually, the network media converters are used to connect newer gigabit Ethernet (1000 Mbps) cabling to older 10Base-T or 100Base-T networks.

- **NICs:**

  A network interface card (NICs) is a device that **joins computers** to LANs. Networked terminals communicate with each other using an existing protocol or a compliant language for sending data packets between the different terminals, known as nodes. The network interface card acts as the connection for the machine to both transmit and receive data on the LAN.

- **Modem:**

  A modem is used to connect the system to the network (Internet). The term “modem” means **modulator-demodulator**. It is a device that **converts digital signals into analog** and vice versa. The signals from a computer are in digital form, but the signals that are transferred over the telephone lines are in analog form. The modem is responsible for this conversion.

- **Access point:**

  The access point is wireless communications hardware that creates a **central point of wireless connectivity**. Similar to a “hub,” the access point is a common connection point for devices in a wireless network.

- **Gateway:**

  A gateway is any device that connects different network environments.

- **Transceiver:**

  A transceiver is a network device that has **both a transmitter and a receiver**. The transmitter is used to transmit analog or digital signals, and the receiver is used to receive analog or digital signals. These devices are built-in NICs.

- **Cable:**

  A cable is used to connect one network device to another.

- **Terminals:**

  Terminals are the hardware devices used to **enter data** into computer or to **display data** from the computer. These depend on the format of the data they handle. For example, an older terminal contains a typewriter keyboard for input and a typewriter printing device for alphanumeric output. A new variant contains the keyboard for input and a television-like screen to display the output.

Steps for Home Networking

Home networking is a method of connecting computers and other electronic devices to communicate with one another. Networking allows a user to share an Internet connection, files and documents, printers and scanners, etc.

To set up a home network, you should need at least the following configuration:

- At least two computers with a LAN card each to set up a network
- One router to connect the Internet and computers
- One Internet subscription line

To set up a home network:

- Note all of the computers and hardware.
- Purchase the required hardware.
- Check for a network interface card on each computer; if not available, fix them.
- Ensure that the computers and all other network devices are connected using cables.
- Select one computer as the host and connect it to the Internet.
- Connect the other computers to the host using the switch/router.
- Install network adapters through the network setup wizard on all computers.
- Restart all computers and you can start sharing the files and accessing the Internet.

Wireless Networks

Wireless networks are used to connect the computers to each other **without any cables**. They have become popular due to ease of installation and the increasing popularity of laptop computers. Restaurants, hotels, business centers, apartment complexes, and individuals often provide wireless access with little or no protection. The network is referred to as a **service set identifier** (SSID). All devices on the wireless network must use the same SSID to communicate with each other.

The major advantage of wireless networks is **user mobility** that is within the range of a particular network. A network has sufficient bandwidth to enable a wide range of applications and services such as police radios, palm pilots, and cell phones.

The main concern has to do with the mobility of users who expect flawless reception between access points. It is not necessary to re-login and restart network applications. A wireless exchange is possible only if the access points exchange data with every transfer of one user to another. Wireless networks provide the freedom to roam with uninterrupted connectivity.

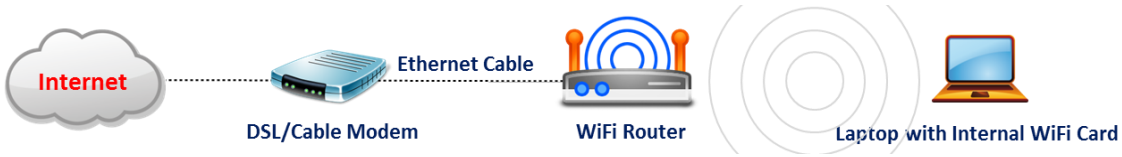


Figure 07-02: Wi-Fi Network

Setting Up a Wireless Network in Windows 7

To set up a wireless network in Windows 7, you should have a wireless router, wireless adapter, and Internet connection.

Wireless Router

A wireless router helps to convert the signals coming across your Internet connection into a wireless broadcast. It works like a cordless phone **base station**. Make sure that you are using a wireless router and not a wireless access point.

Wireless Network Adapter

A wireless network adapter is used to connect your computer to the wireless router. In a newer configuration of computers, wireless capabilities are built in. You should have network adapters for every computer on your network.

Steps to set up a Wireless Network in Windows 7 include:

- In the **Start** search box type ***Network*** and select **Network and Sharing Center.**
- Click **Set up a new connection or network.**
- Click **Set up a new network** and click **Next.**

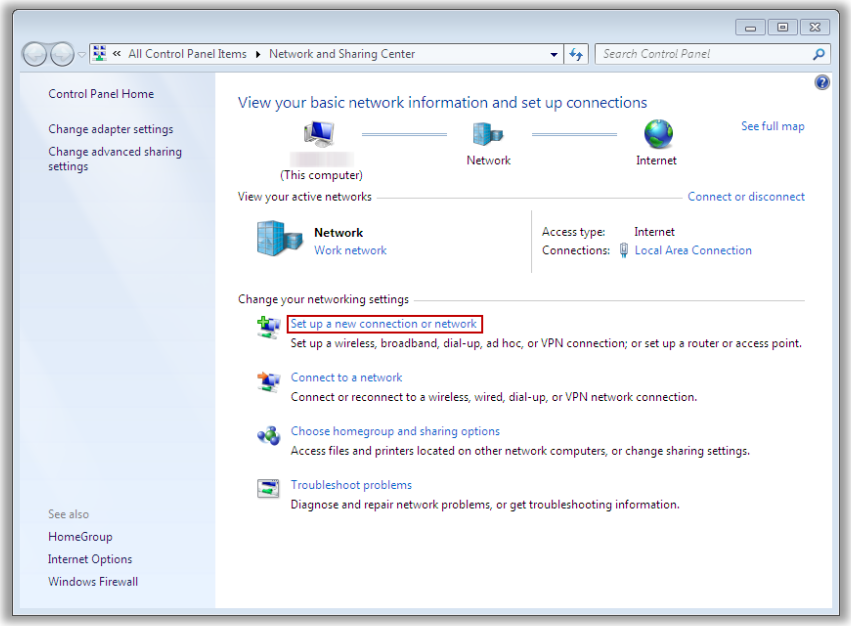


Figure 07-03: Wireless Network Setup in Windows 7

Changing Wireless Networking Configuration in Windows 7

Steps to change wireless networking configuration in Windows 7 include:

- Select **Manage Wireless Network** from **Network and Sharing Center.**
- Click **Add** if you are asked **How do you want to add a Network?** Select **Manually create a network profile.**

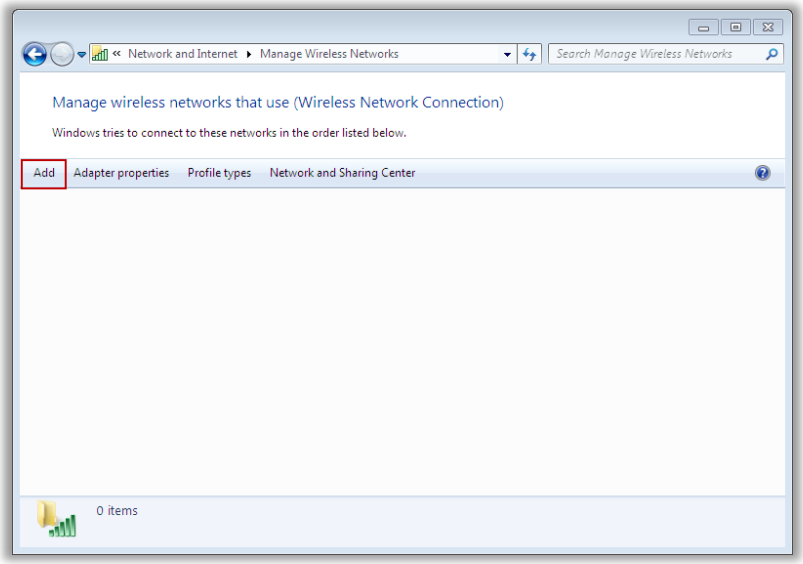


Figure 07-04: Managing Wireless Network Setup in Windows 7

Changing Wireless Networking Configuration in Windows 7

- Fill in the wireless network information that you want to add.
- Check the options **Start this connection automatically** and **Connect even if the network is not broadcasting** and click **Next.**
- Select **Change connection settings.**
- Uncheck the option **Connect to a more preferred network if available** in the **Connection** tab.
- Select the **Security** tab next to **Microsoft Protected EAP (PEAP)** and click **Settings.**

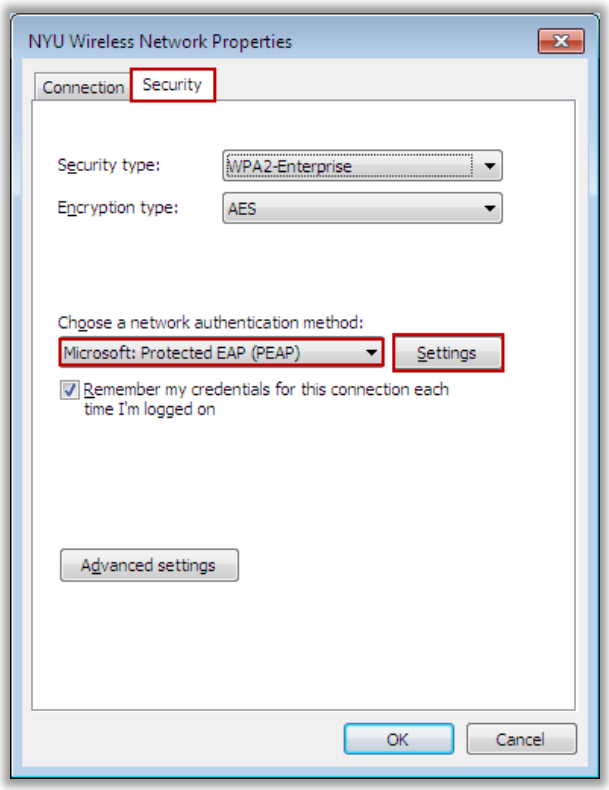


Figure 07-05: Changing Wireless Configuration in Windows 7

Following are the steps to change the wireless networking configuration in Windows 7:

- **Protected EAP properties** pops up. Check the option to **Validate server certificate.**
- In **Trusted Root Certification Authorities,** check **Class 3 Public Primary Certification Authority.**
- In Select **Authentication Method**, select **Secured Password (EPA-MSCHAP v2)** and click the **Configure** button.

- Uncheck **Automatically use my Windows logon name password (and domain if any)** and click **OK** to dismiss each of the open windows.
- A balloon will appear near the system tray that reads, **Additional information is required to connect to name which you have provided.** Click the balloon.
- Enter your **NETID and password**. After validating, another balloon appears at the system tray that says, **Additional information is required to connect.**
- Click the balloon → **OK** to agree and validate the server certificate
- After few minutes, you will be connected to your wireless network.

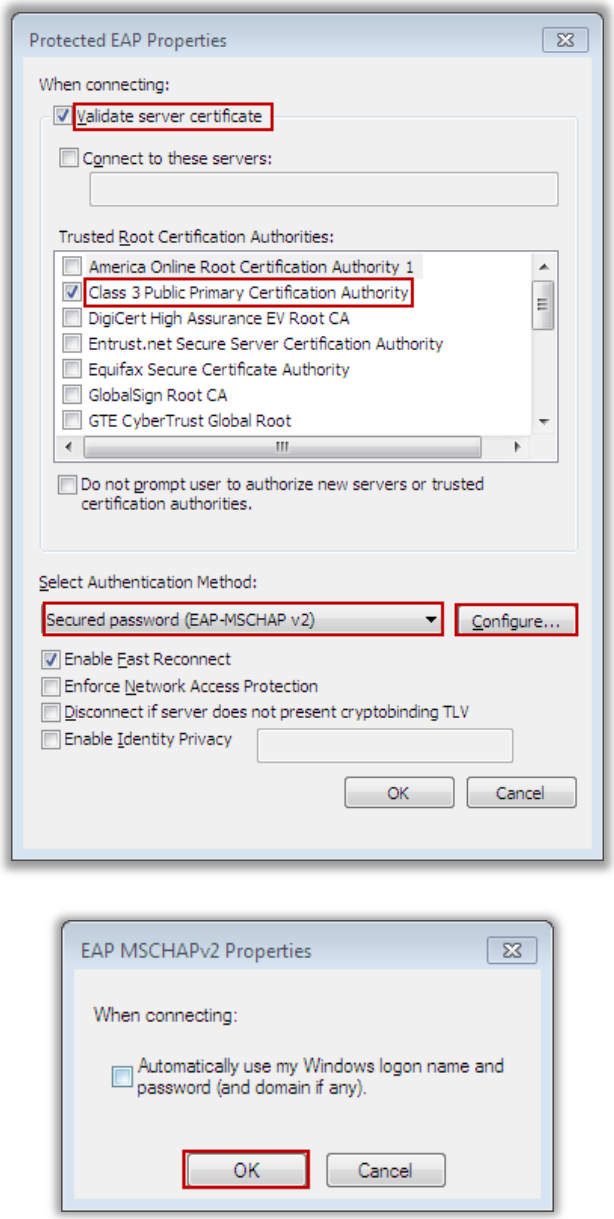


Figure 07-06: Protected EAP Properties in Windows 7

Setting Up a Wireless Network in Mac

Steps to set up a wireless network in Mac include:

- Click **Network Pane** in system preferences and choose **AirPort** entry.
- Check the **Show AirPort Status in Menu Bar** check box.
- Close the system preferences.
- Click the **AirPort** status icon in the menu bar.
- Click **Create network** and enter a name for the network.
- Check the **required password** check box.
- Enter a **password** for your network and then enter it again to confirm it.
- Click **OK.**

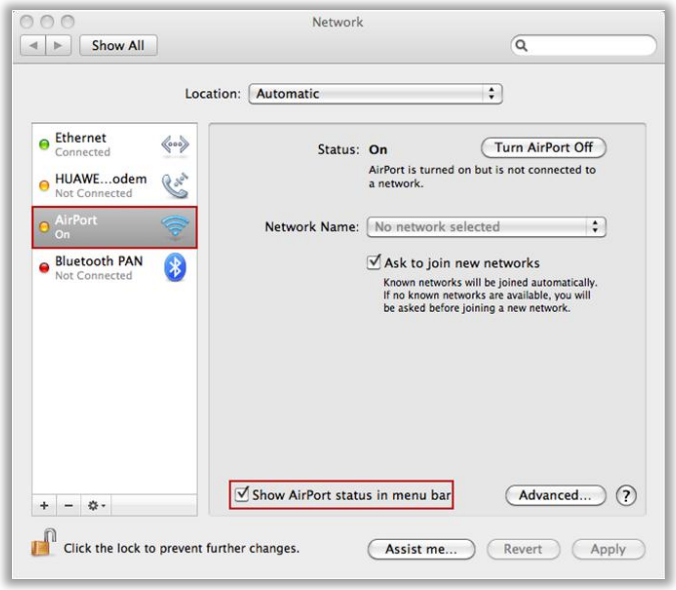


Figure 07-07: Setting Up Wireless Network in Mac

Changing Wireless Networking Configuration in Mac

Steps to change wireless networking configuration in Mac include:

- Go to the upper right **Airport** icon.
- Select the **UConnect** option from the drop-down menu.
- Complete the **User Name** and **Password** fields, select **Automatic** for **802.1x,** and check **Remember this Network**.
- Click **OK.**

- Accept the verify certificate by clicking **Continue.**

Note: You should connect to UConnect shortly. If this does not happen, check your profile.

- Go to **System Preferences** and click **Network.**
- Verify that you are connected.
- Select **Airport** to the left and click **Advanced.**
- Click on the **802.1X** tab and select the **WPA: UConnect** profile.
- Verify that **PEAP** is the only **Protocol** checked.
- Select the **Configure Trust** button.
- Select the **Servers** tab. Click the **+** and select one of the available servers**.** Click **OK.**
- Hit **OK** twice and click **Apply.**

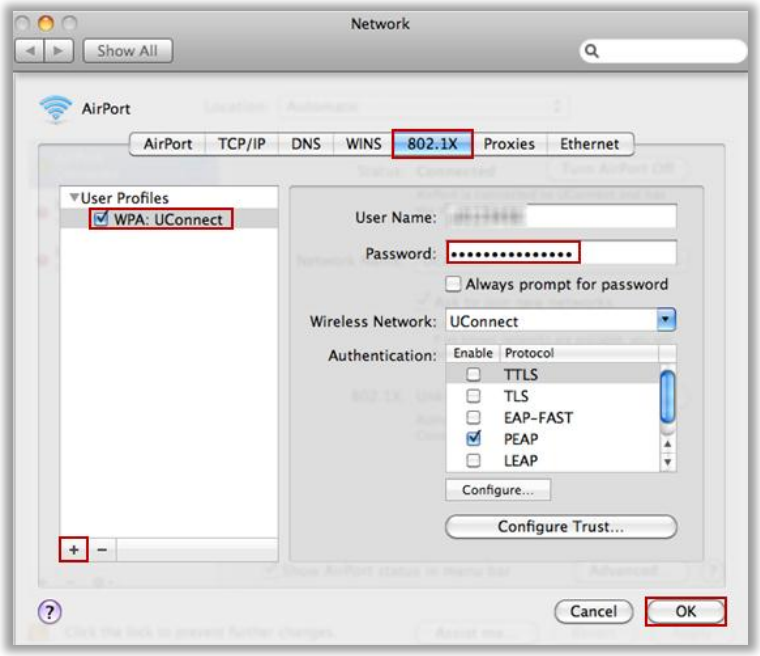


Figure 07-08: Changing the Wireless Networking Configuration in Mac

Common Threats to Wireless Network

Threats to a wireless network are largely unpredictable. However, the common threats to wireless networks include:

- **Eavesdropping:** Attackers can use a variety of tools to find wireless access points where they can pick up an SSID broadcast.

- **Data interception and modification:** Attackers who gain access to a network can insert a rogue computer to intercept, modify, and relay communications between two legitimate parties.
- **Denial of service:** Attackers can shut down access points by jamming the air with noise, rerouting connections to dead ends, or disconnecting valid clients.
- **Spoofing:** Even if the user disables broadcasting or turns on Media Access Control (MAC) filtering on the wireless access point, attackers can use antennas to capture users' signal, determine SSID or valid MAC address, and then use it to impersonate an authorized client.
- **Freeloading:** An attacker can use the network as a free access point to the Internet.
- **Rogue WLANs:** Attackers can easily install unauthorized WLANs on the network.

An attacker can exploit weaknesses in a wireless network to:

- Read user email and instant messages as they travel across the network.
- Monitor the websites visited by the user.
- Copy users' usernames and passwords.
- View files on the computers and spread malware.
- Disclose user confidential information.
- Interrupt the wireless service and implement unauthorized WLAN.
- Send spam or perform illegal activities with a user's Internet connection.
- Slow the user's Internet performance.

Securing Wireless Network

Wireless security refers to a set of control procedures, policies and tools employed to protect a wireless network and its associated devices from **damage** and **unauthorized access**. The following is a set of recommendations to secure a wireless network:

- Turn off the network during extended periods of non-use.
- Revisit the WLAN network design for incorrect access point placement.
- Do not connect to unprotected wireless networks in public places.
- Change the default SSID.
- Change the default administrator passwords (and usernames).

  Disable or **turn off SSID broadcast** for the network to make the network invisible to attackers.
- Enable MAC Address filtering to keep track of all network MAC devices connecting to the router.

- Data transmitting over wireless networks should be encrypted to prevent eavesdropping, interception, and data modification.
- Network-level denial of service attacks are prevented by using user authentication.
- Unauthenticated access to the wireless network can be prevented by using a virtual private network (VPN) connection and **IPSEC**.
- VPNs keep communications safe by creating secure tunnels through which the encrypted data travels.
- A network should be scanned using software scanning tools to locate and shut down rogue WLANs.
- If the user is connected to an unprotected wireless network at public places, do not visit a website that requires a password unless the website is encrypted.

Using the Network with Windows 7

Setting up the PC's Name and Workgroup Name in Windows 7

It is highly recommended to assign a computer and work group name in Windows 7 because it allows other computers to easily access your computer and shared files or printer by using your computer name.

You should assign a unique computer name to each computer; you can group all home computers under the same workgroup.

To set up the PC's name and workgroup name in Windows 7:

- Go to **Start** → **Control Panel** and double-click the **System** icon
- Click **Change Settings** on right pane
- In the **System Properties** dialog box, click the **Computer Name** tab
- Click the **Change** button
- Give the computer a new name and a new workgroup name
- Click **OK** to save your changes

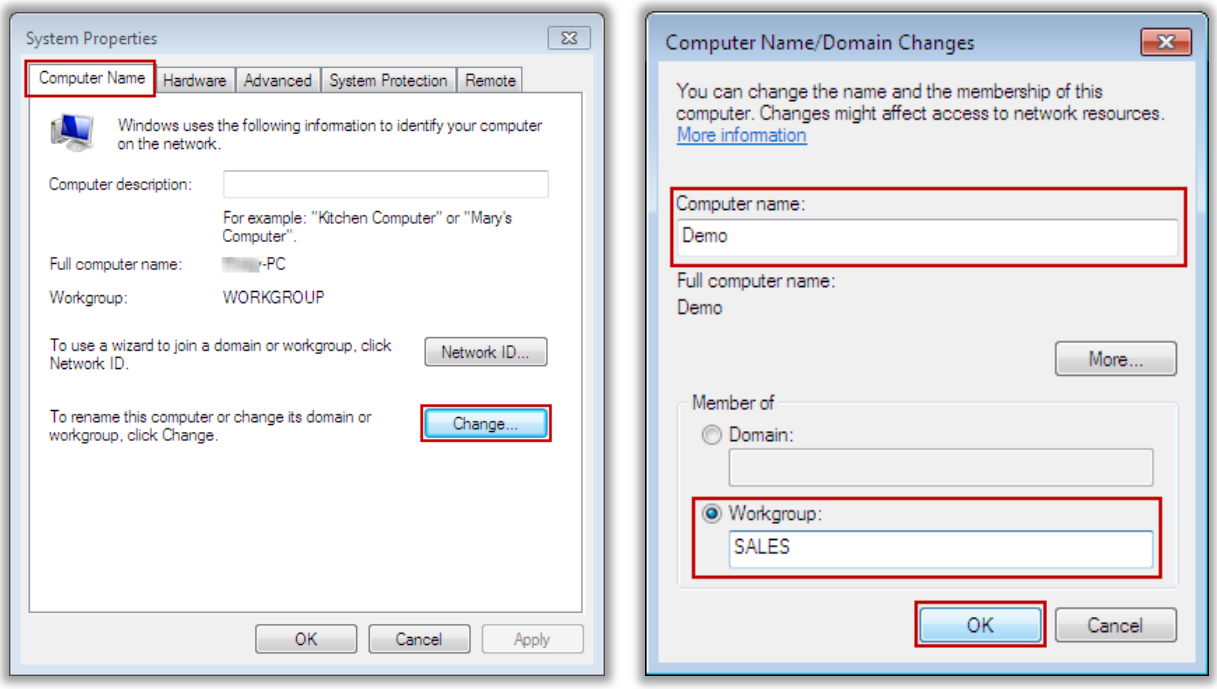


Figure 07-09: Assigning a PC's Name and Workgroup Name in Windows 7

Sharing

Sharing the data, such as files and printers, over a network is also called file sharing. Attackers who can access a single computer in a network can also access information from other computers in the network. Files can only be shared when stored within a folder. Once the folder is shared on the network, it is referred to as a **shared folder**. The owner of the folder can **limit users' access** to both this shared folder and the files it contains. Access to the shared folder is sometimes regulated by **password protection**, account or security authorizations, or locking the file to prevent more than one user at a time from making changes.

The term **file sharing** also refers to the users being granted the same or different levels of **access privilege**. The files may be stored in a particular system, also known as the server, and can be accessed by more than one user, depending on the levels of access privilege. The user must keep the following points in mind when sharing a folder:

- Only folders can be shared, not files.
- Shared folders are available only to users capable of accessing the network server on which the folder is stored.
- When a copy of the shared folder is created, the copy is not automatically shared.
- When a shared folder is moved from its original position, it will no longer be shared.

Transferring Files

File transfer is the process of **communicating** with two computers or more to send a file between them. There are various ways of transferring files. A file can be transferred through email or messengers (Yahoo and MSN), which **scan for viruses** using an email virus scanner. The user must ensure that he or she scans the file for viruses and malware before and after acquiring or transferring the file. A file can also be transferred using FTP, Telnet, and web folders. The user must use a valid user name and **strong password** on FTP, Telnet, and web folders to ensure **authorized access** of the files to be transferred. This will enhance the security as no other user can access files stored at these location.

Transferring of files can also happen through **peer-to-peer** (P2P) networks. There are numerous peer-to-peer applications available on the Internet, including emule, BearShare, Warez, Morpheus, and KaZaA. These P2P applications are configured by default such that all members in the network can access each other's hard drives and folders by default. Theses settings can be disabled to avoid anyone else accessing the user's hard drive.

Simple File Sharing in Windows 7

Steps to set up file sharing in Windows 7 include:

- Confirm that you have enabled file and printer sharing on a network card.
- Go to **Start → Control Panel → Network and Sharing Center.**
- Click **Change adapter settings.**
- The **Network Connections** window will appear. Right-click the network adapter (can be a wireless adapter or a wired Ethernet adapter) in use and select **Properties.**
- The network card's properties window will appear. Check **File and Printer Sharing for Microsoft Networks,** and click **OK.**

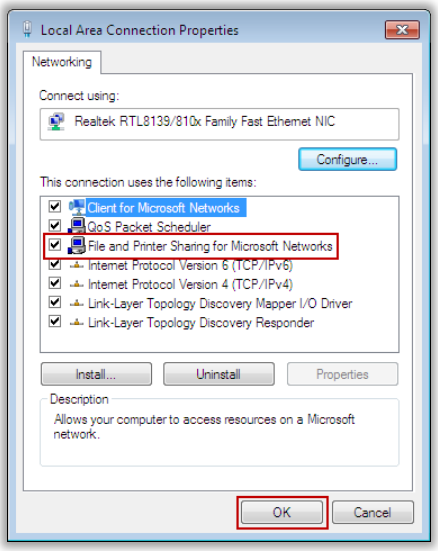


Figure 07-10: Wireless Network Setup in Windows 7

- Select the appropriate network location type before enabling file sharing, mostly home network or work network type.
- Click **Change advanced sharing settings.**
- Locate your current set profile (home or network), and turn on/off the following settings.
  - Turn on file and printer sharing.
  - Turn off password protected sharing.
- Click **Save changes.**

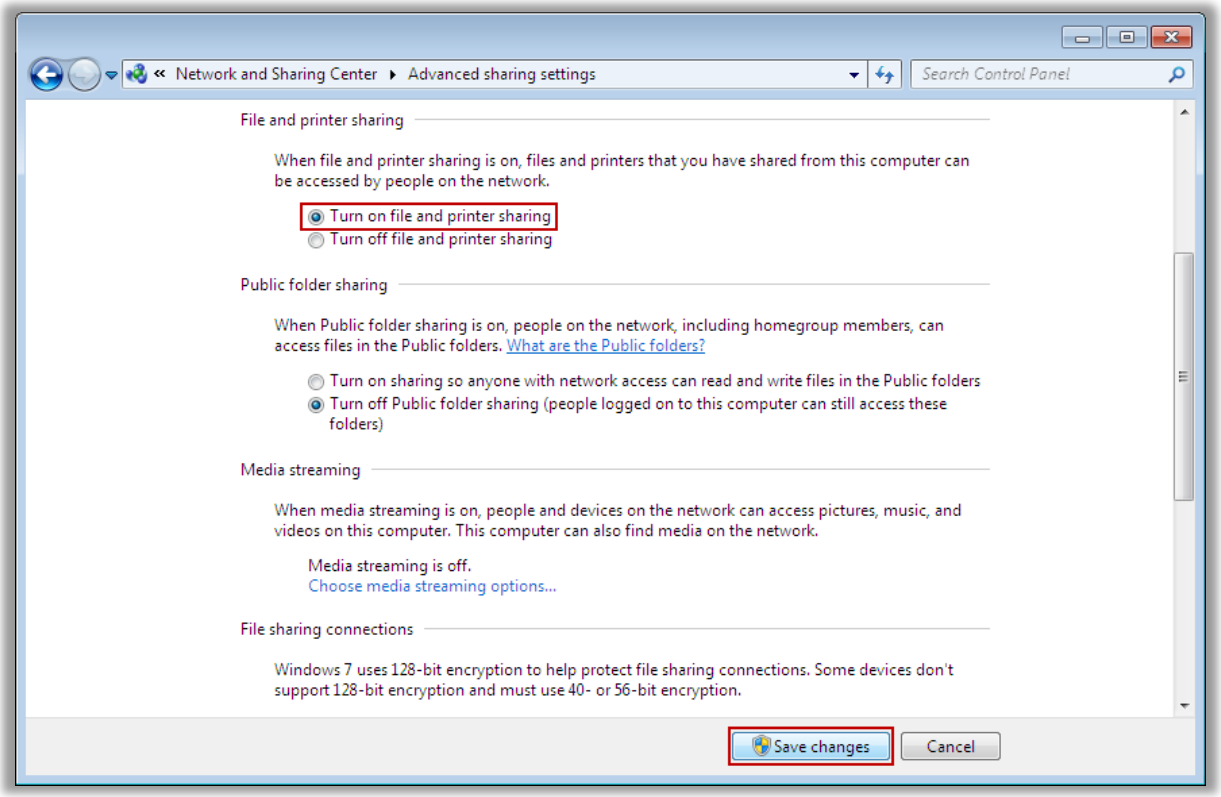
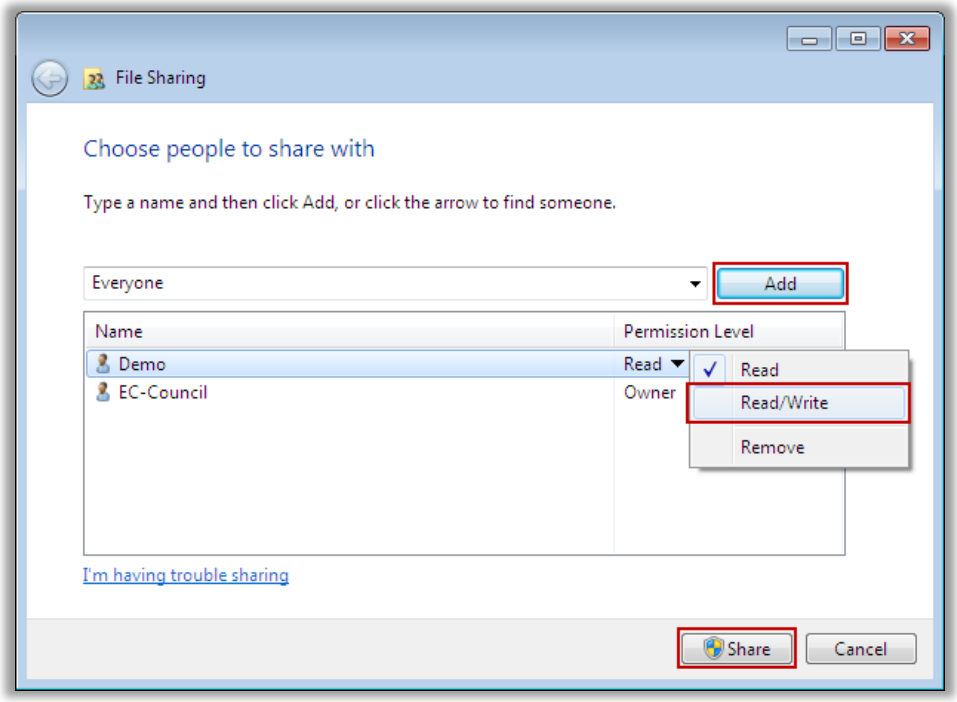
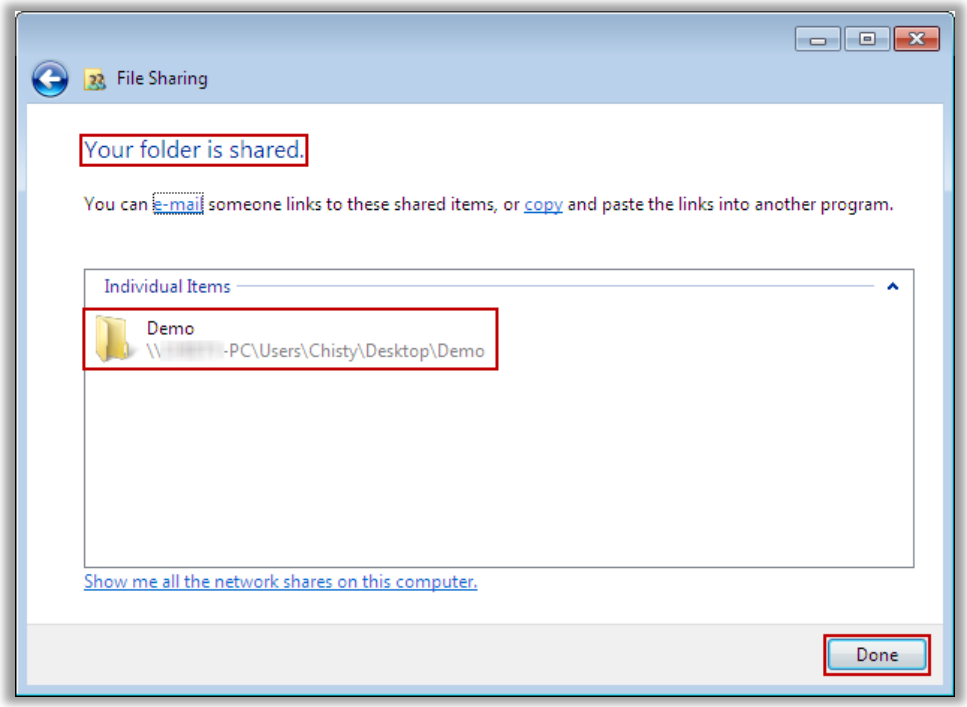


Figure 07-11: Wireless Network Setup in Windows 7

- Right-click the folder you plan to share, select **Share with,** and click **Specific people.**
- The **File Sharing** window will appear. Here, select or type the people you would like to share the file/folder with and click **Add.** Set the permission level and click **Share.**
- The next window will tell you that your file/folder is shared. Click **Done** to close the window
- Right-click the shared folder and click **Properties**. Then go to the **Sharing** tab, which indicates that the folder is shared.

- Click the **Security** tab. Check the group or user names that are allowed to access the file/folder, and ensure that the user/group you allowed access during the sharing process is listed here as well.





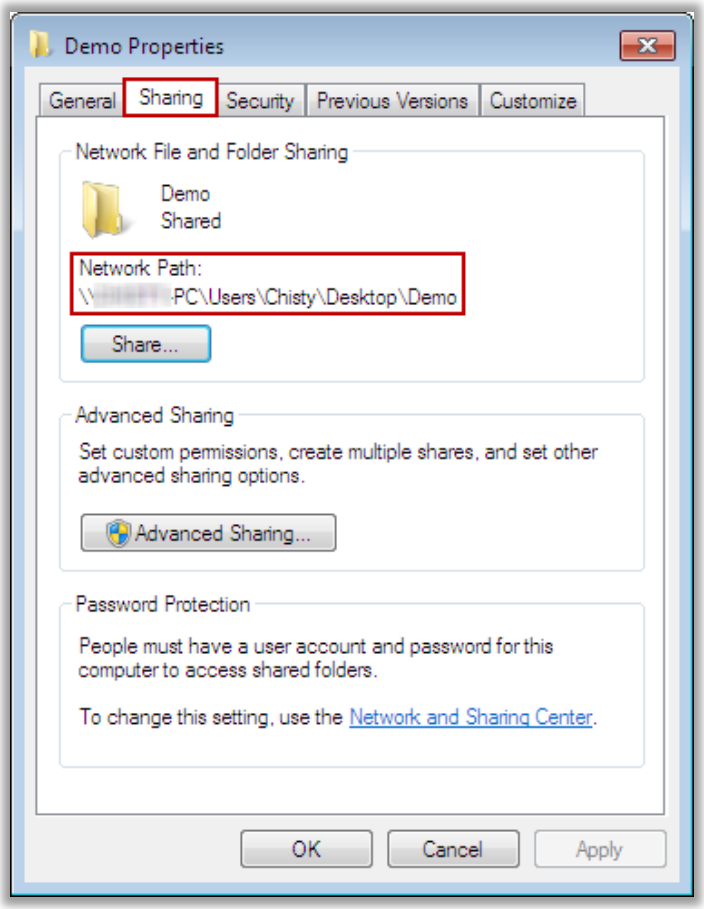


Figure 07-12: Simple File Sharing in Windows 7

Hiding a Shared Disk or Folder

Steps to hide a shared disk or folder include:

- Go to **Windows Explorer** (**Start** → **Computer**) → **Organize** → **Folder and Search Options.**
- To hide the empty drives, extensions for the known file types, and protected OS files, check mark the respective options.
- To show hidden files, folders, and drives, enable the **Show hidden files, folders, and drives option.**
- To not show hidden files, folders, and drives enable the **Don't show hidden files, folders, or drives** option.

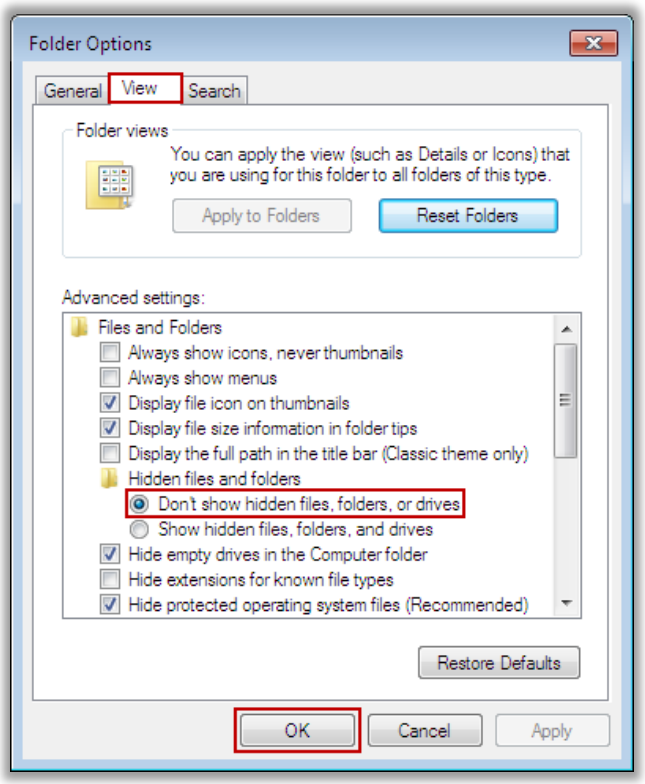


Figure 07-13: Hiding Shared Disk or Folder

How to Share Printer in Windows 7?

The steps to share printer in Windows 7 include:

- Go to **Start → Devices and Printers.**
- Right-click the printer to be shared, and then click on the **Properties.**
- Select the **Sharing** tab and check **Share this printer** to share the printer.
- Type in a new name in the **Share name** field to change the printer name on the network; however, this will not change the printer name on the computer.
- Click **Apply.**
- If the other users using different version of Windows want to access the printer, then they need to install a printer driver themselves.
- Click **Additional Drivers** and check the additional driver to be installed.
- The user will be prompted to install the additional drivers after clicking **OK.**

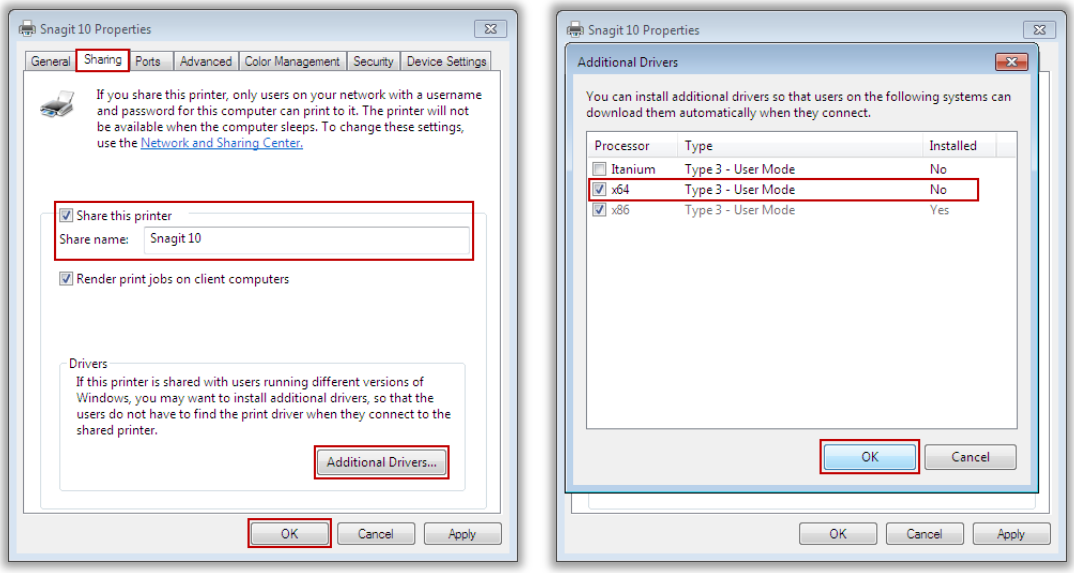
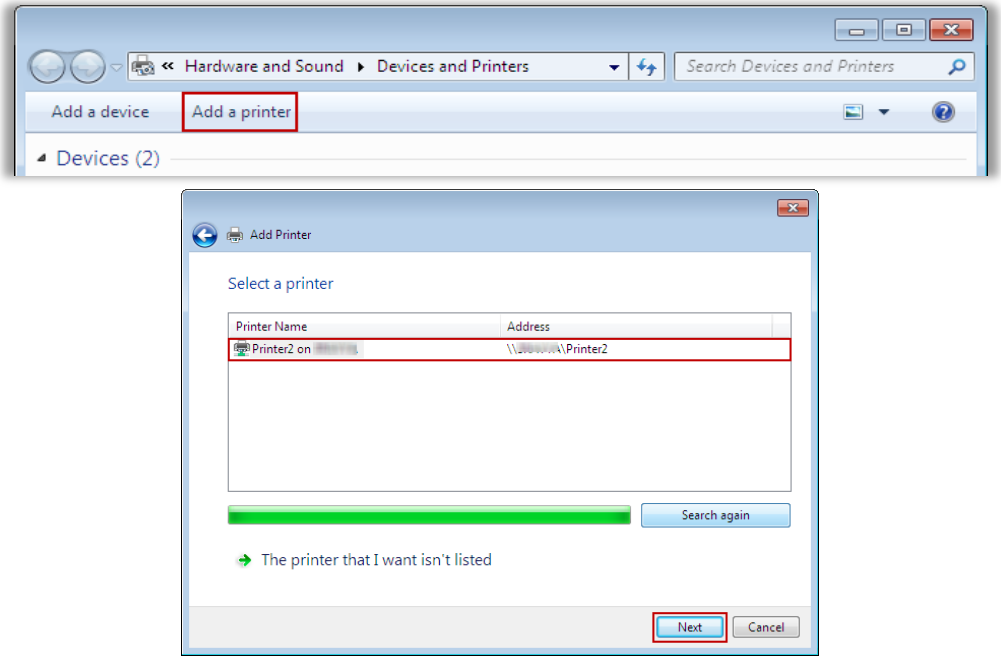


Figure 07-14: Sharing Printer in Windows 7

Using Printers on Other PCs

The steps to share printer on other PCs include:

- Go to **Start → Devices and Printers.**
- Double-click the selective printer or click **Add a Printer** to browse for it.
- Select a printer from the list displayed and click **Next.**
- Now Windows will try to connect to the printer of choice.
- Install the software for the printer when prompted.



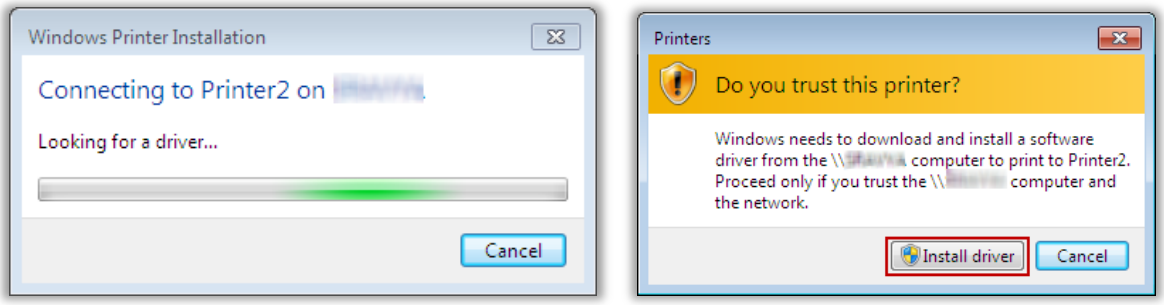
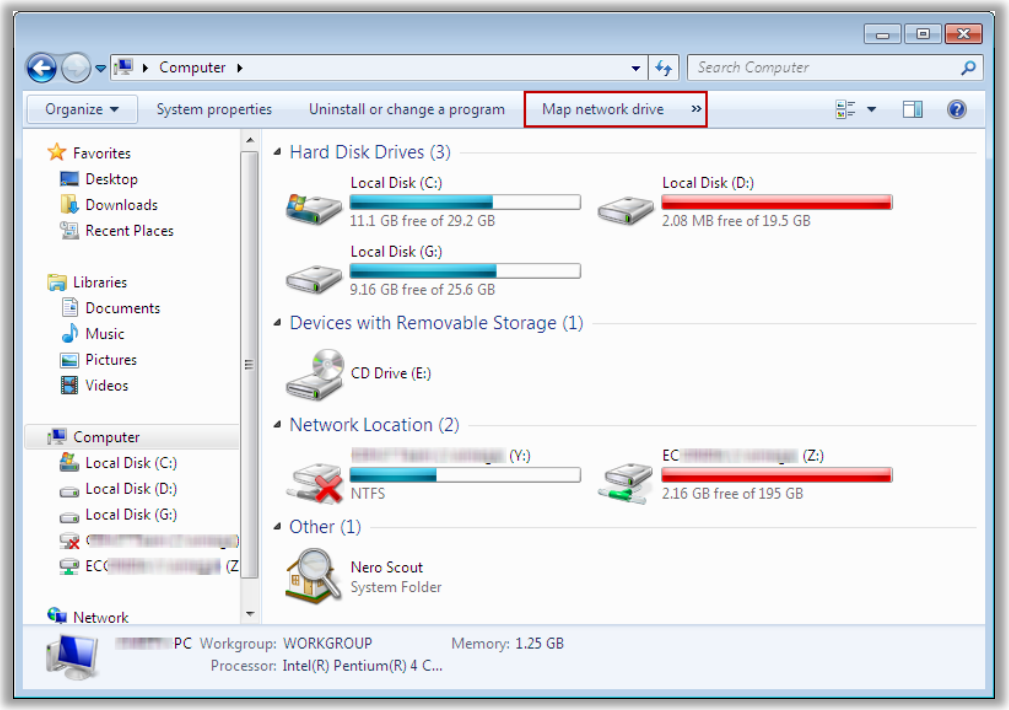


Figure 07-15: Using Printers on Other PCs

Accessing Files on Other PCs

To assign a letter to a particular shared disk or folder on the network:

- Go to **Start → Computer → Map network drive.**
- Using the drop-down list, choose a drive letter.
- Indicate which folder or disk you want this letter to represent.
- To make this letter assignment "stick," turn on **Reconnect at logon.**
- Click **Finish.**



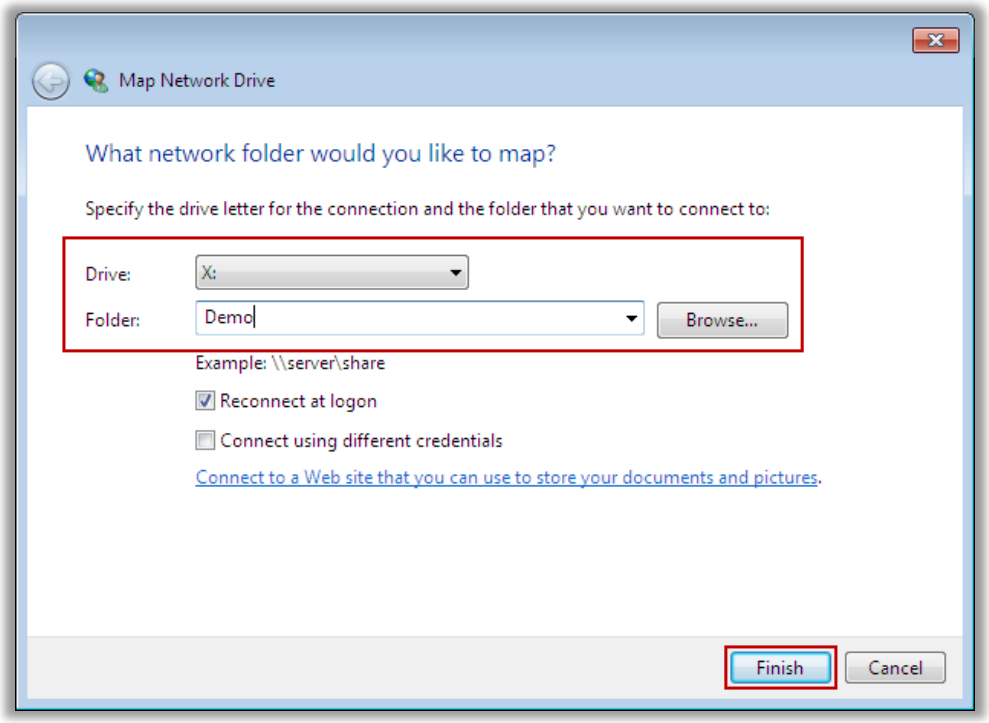


Figure 07-16: Accessing Files on Other PCs

Windows Easy Transfer

Windows Easy Transfer is a **Microsoft application** that helps in transferring personal files, email, data, files, media, and settings stored on the system running Windows to another system running Windows. Programs (applications) cannot be transferred. It transfers:

- User accounts
- Files and folders
- Program data files and settings
- Email messages, settings, and contacts
- Photos, music, and videos
- Windows settings
- Internet settings

Windows Easy Transfer Methods:

Windows Easy Transfer provides a number of ways for users to connect two computers to transfer the data. Some of the key features of these easy transfer methods are:

- An easy transfer cable is a special USB cable that is designed to work with Windows Vista and Windows Easy Transfer.

- If the user already has a wired or wireless network, this is a great way to transfer all of the data.
- It can copy the data to a removable hard disk and then copy data from that disk to a new computer.
- It can use a computer's CD or DVD burner to transfer user data.

Figure 07-17: Windows Easy Transfer

Using the Network with MAC OS X

Setting Up the PC's Name in Mac OS X

The steps to set up a PC's name in Mac OS X include:

- Go to **Apple** menu → **System Preferences.**
- From the **Internet & Network** section of the **System Preferences** window, select the **Sharing** option.
- At the top of the **File Sharing** dialog box, in the **Computer Name** field, type the new name for your Mac.
- Close the **File Sharing** dialog box.

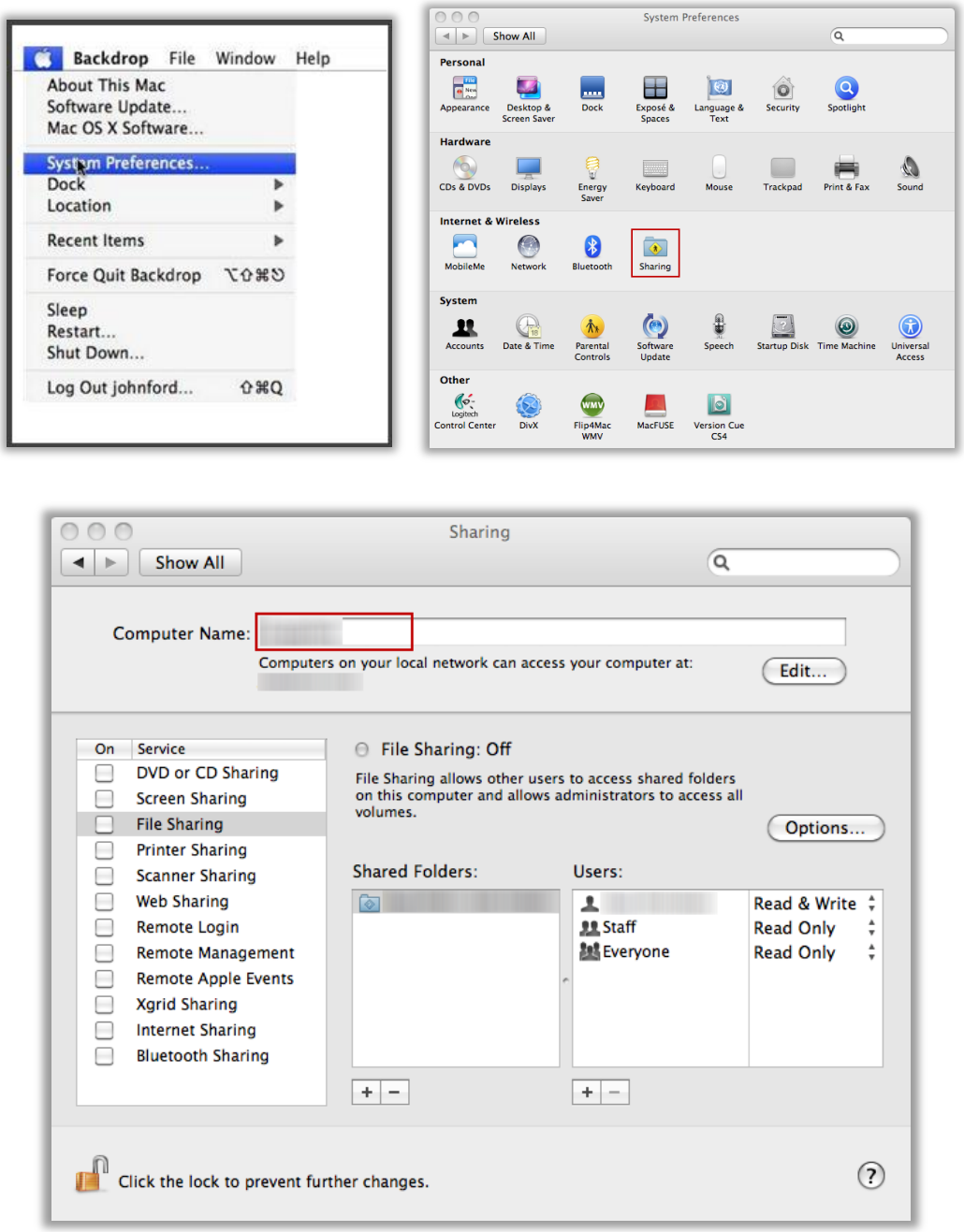


Figure 07-18: Setting a PC's Name in Mac OS X

Setting Up the Workgroup Name in Mac OS X

The steps to set up work group name in Mac OSX:

- Open **System Preferences** from the **Apple** menu.
- Open the **Network** icon in the **Internet & Network** area.
- Select the network connection you use to connect to the Windows network.

- Click the **Advanced** button and then click the **WINS** tab.
- Type the name of the workgroup in the **Workgroup** field.
- Click **OK** to save the changes.
- **Restart** your computer to join the workgroup that you have specified.

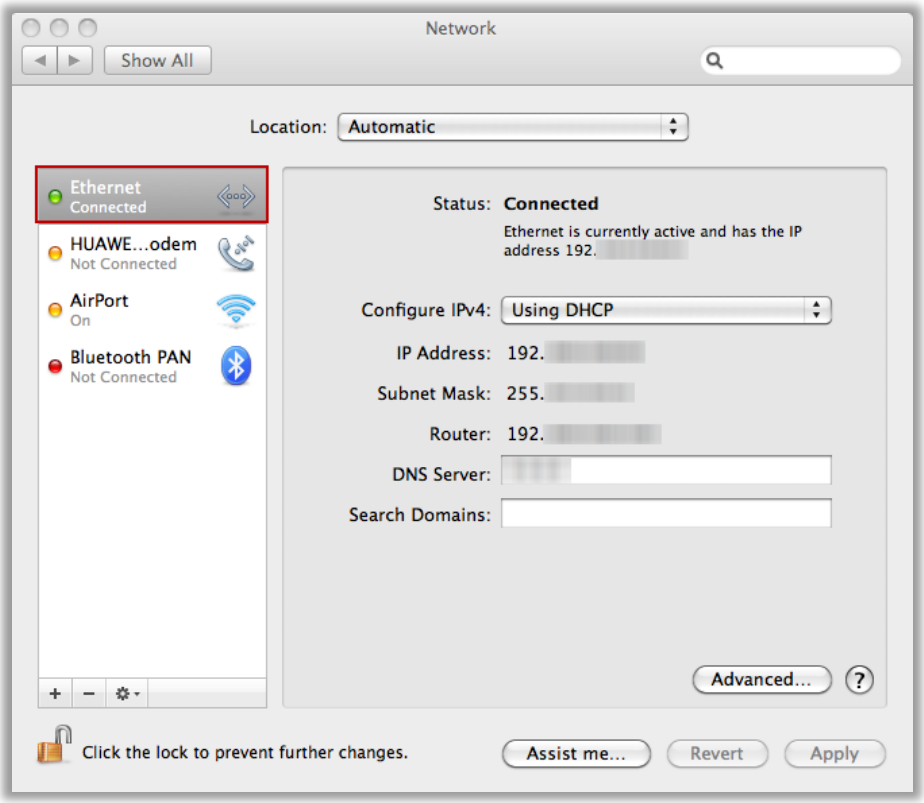


Figure 07-19: Setting up a Workgroup Name in MAC OS X

Creating User Accounts and Groups in MAC OS X

In Mac OS X, accounts are either two types—Administrator and Standard.

- Administrators can Install new programs, fonts, make changes to certain System Preferences panels, use the **NetInfo Manager** and **Disk Utility** programs, create new folders outside of their Home folder, and manage other users accounts
- Users with Standard accounts have everyday access to their own Home folders, and to some of the System Preferences, but most other areas of the Mac are off-limits

Creating an Account:

- Choose **Apple** menu → **System Preferences.**

- Click the **Accounts** and then click the **+** button beneath the list of accounts.

Name the Account:

- On the first tab of the **Accounts** dialog box, fill in information for the new account holder (name, short name, password, and verify).
- Check the **Allow user to administer this computer** box to give the user administrative privileges.

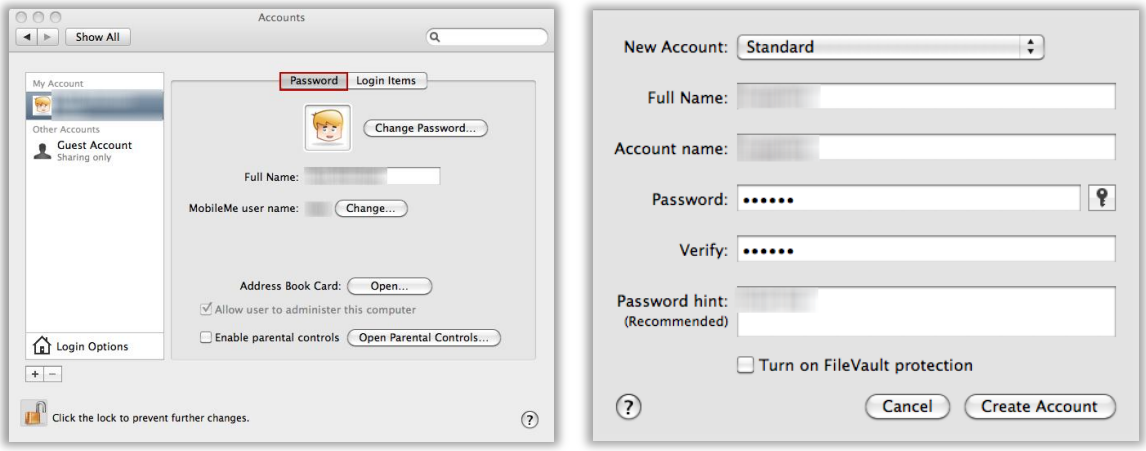


Figure 07-20: Creating an Account in Mac OS X

Creating User Accounts and Groups in Mac OS X

The steps to create user accounts and groups in Mac OS X:

Editing an Account:

- Go to **System Preferences** → **Accounts** and select the account you want to change.

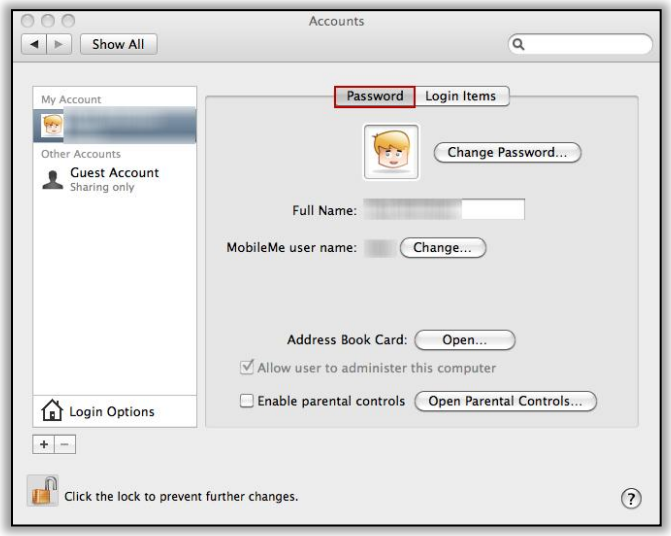


Figure 07-21: Editing an Account in Mac OS X

Deleting an Account:

- Choose **Apple** menu → **System Preferences.**
- Click the **Accounts** icon, select the account name to delete, and then click the – button beneath the list.
- Now Mac asks what to do with all of the deleted account's files and settings:
  - If you click the **Delete Immediately** button, the documents will be gone forever.
  - In contrast, if you click the **OK** button, it preserves the deleted account's folders on the Mac in a tidy digital envelope.

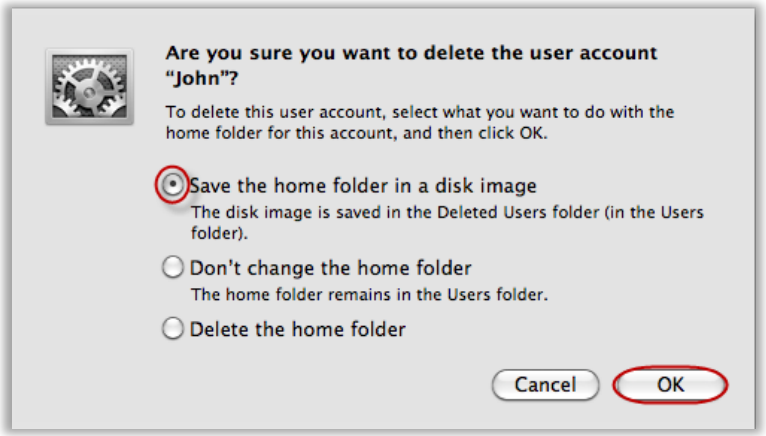


Figure 07-22: Deleting an Account in Mac OS X

The Guest Account:

- Launch System Preferences, either by clicking the **System Preferences** icon in the Dock, or by selecting **System Preferences** from the **Apple** menu**.**
- Click the **Accounts** icon, located in the **System** area of the **System Preferences** window.
- Click the lock icon in the bottom left corner. When prompted, supply your administrator username and password.
- From the list of accounts, select **Guest Account.**
- Check the **Allow guests to connect to shared folders** box.
- Click the lock icon in the bottom left corner.

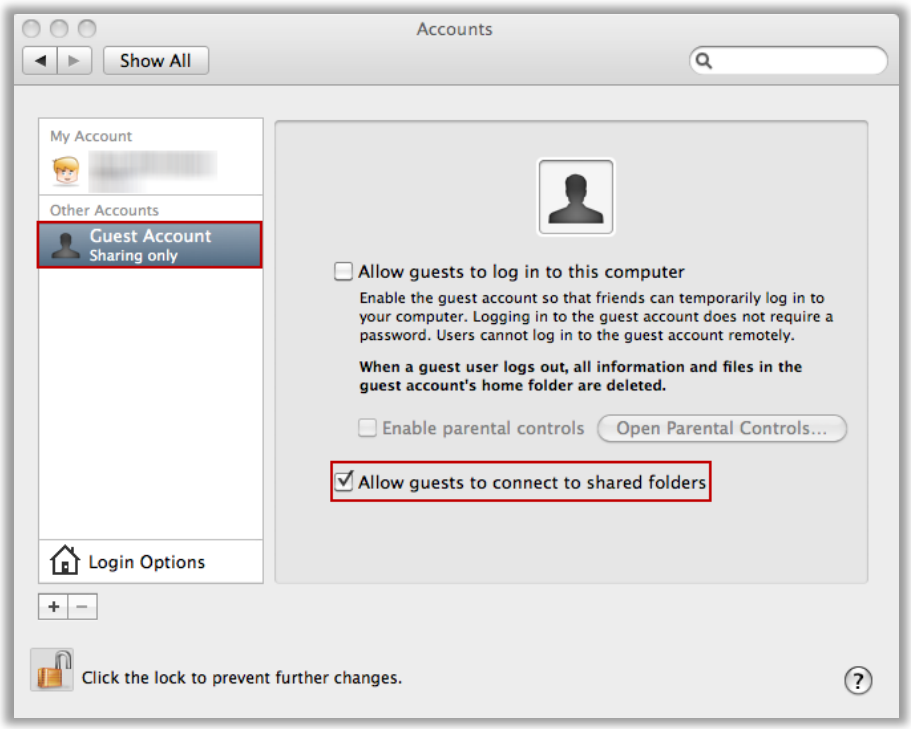


Figure 07-23: Guest Accounts in Mac OS X

Sharing Files and Folders in Macintosh OS X

To share Files and Folders in Macintosh OS X, follow these steps:

- Choose **Apple** menu → **System Preferences** to open the system preferences program.
- Click the **Sharing** icon.
- Check the **Personal File Sharing** box.

Permissions control in Mac OS X:

When connected to a remote Mac:

- An **Administrator account holder** sees the names of each drive on the remote Mac as well as the Home folder. By opening a Mac's hard drive, administrators can view all Home folders on that Mac.
- A **Standard account holder** sees only the names of the **Home** folders on the remote Mac and has free access only to his or her own **Home** folder. In all other **Home** folders, he can only access the **Public** folder.
- A **Guest account holder** sees only the names of the **Home** folders on the remote Mac. In each **Home** folder, all he or she can see is the **Public** folder.

Changing access permissions for a file or folder:

- Choose **File → Get Info**. When the Info dialog box appears, expand the **Ownership & Permissions** panel; then expand the **Details** section.
- This displays three pop-up menus—**Owner**, **Group**, and **Others**.
- For instance, click the **Owner** drop-down list and specify the access permission (read only, write only, read and write, or no access).
- Finally, click the **Apply** button.

Figure 07-24: Sharing Files and Folders in Mac OS X

Printer Sharing in Macintosh OS X

The steps to share printer in Mac OSX include:

- Click **Sharing** from the **System Preferences** window.
- Check the **Printer Sharing** option to enable it.
- Click **Print & Fax** icon in the **System Preferences** window.
- Click the **+** button.
- Click the **Default** button from the browser window.

- Click the shared printer you wanted to use and then click the **Add** button.

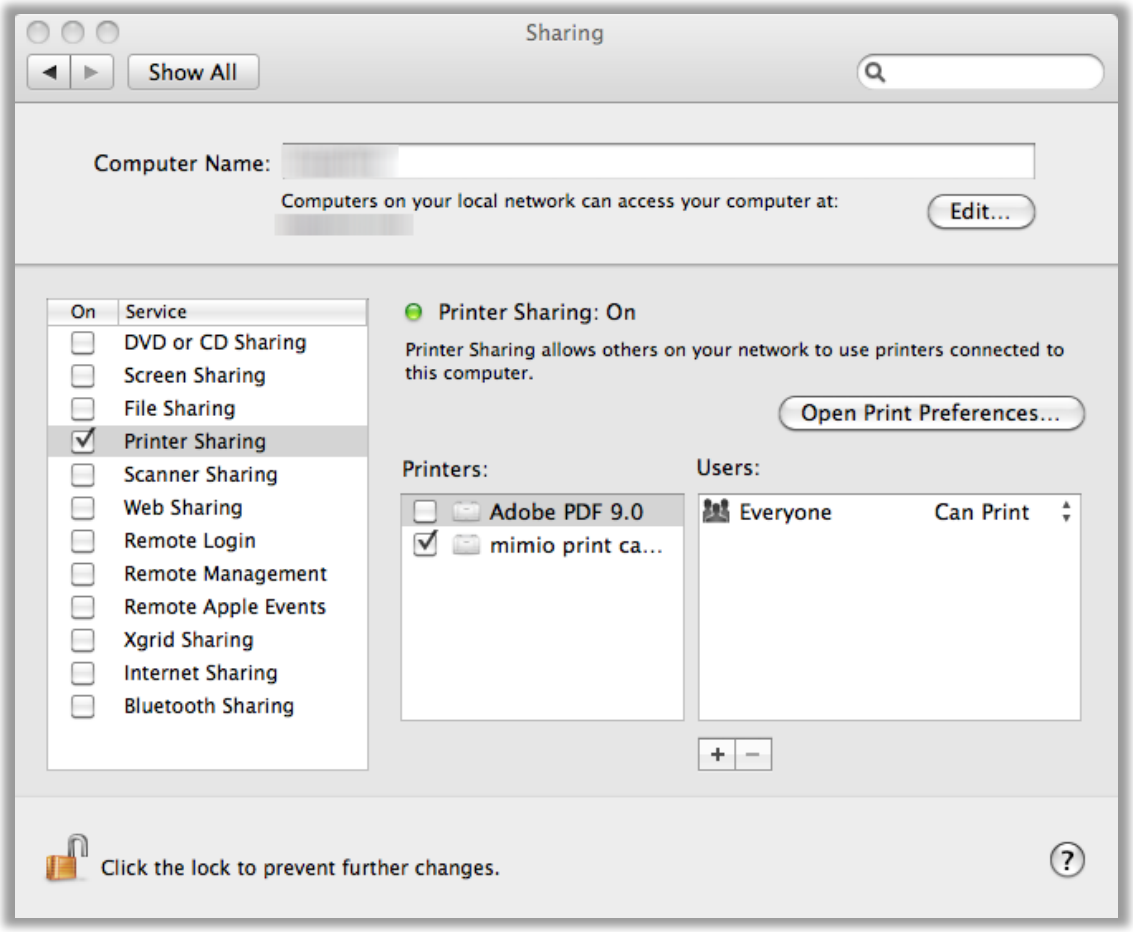


Figure 07-25: Sharing Printers

Accessing Other Macs on Your Network

To access other Macs on your network, you need to follow these steps:

- Click **Go** and **Connect to Server** in the Snow Leopard menu
- Enter the IP address of the server
- Click **Connect**

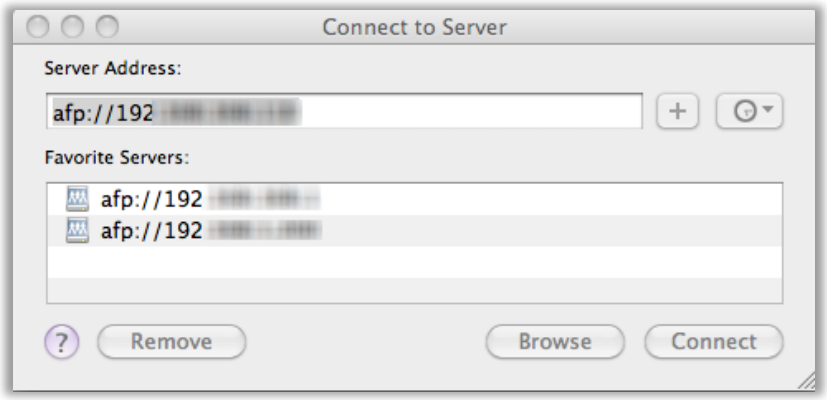


Figure 07-26: Accessing Other Macs on Network

Network Security Threats

Malware:

- Email, instant messaging, and file sharing programs have traditionally been used to spread viruses, worms, backdoors, rootkits, Trojans, and spyware from computer to computer.

Sniffing:

- Unsecured network connections such as Wi-Fi access points are used by hackers to set up packet sniffers to monitor all traffic that comes and goes in a network.

Denial of Service:

- Denial of service leads the computer to crash or to become so busy in processing data that it cannot be used.

Mobile code (Java, JavaScript, and ActiveX):

- Intruders use a mobile code to gather information such as the websites visited or to run malicious code on your computer.

Email spoofing:

- An email message that appears to have originated from one source when it was really sent from another to trick the user into exposing sensitive information.

Chat clients:

- Chat clients allow the exchange of executable code that may be malicious.

Being an intermediary for another attack:

- Intruders use compromised computers as launching pads for attacking other systems.

Backdoor and remote administration programs:

- BackOrifice, Netbus, and SubSeven are the tools commonly used by intruders to attack Windows computers.

Cross-site scripting:

- A malicious web developer may attach a script to something sent to a website, such as a URL that is transferred to your browser when the website responds to you.

Unprotected Windows shares:

- Unprotected Windows networking shares can be exploited by intruders to place distributed attack tools for Windows-based computers attached to the Internet.

Securing Network Connections

Use a Firewall

A firewall is a part of a computer system/network that is designed to **block unauthorized access**. It controls traffic coming into and leaving the system by permitting authorized communications. It hides a user's home network from the outside world. It can be in either **hardware or software**. It is recommended to use personal firewall on all computers. It monitors all the requests coming into the system, alerts the user, and asks permission to allow/block them. A firewall can also be a secure, reliable, and trusted machine placed between private and public networks. It is configured with a **set of rules** to trace the network traffic. Firewalls are responsible for the traffic allowed to **pass**, **block**, or **refuse**. It is also placed inside the organization to protect some departments of the organization. There are many ways to construct a firewall. The most complicated arrangement is the perimeter network. Two machines can act as filters and are called **chokes**. These chokes allow pre-defined traffic to pass through the network. Network servers such as mail gateways or web proxy servers, are placed between these chokes. This type of system allows for much control over who can make a connection from inside to outside and from outside to inside the perimeter. A firewall working closely to the router examines every packet before forwarding it. Firewalls also work with the **proxy server**, which makes requests in place of the workstation. Many features are included in the firewall such as logging, reporting, automatic alarms at the time of attack, and a graphical user interface (GUI) to control it.

Examples of software firewalls include:

- Windows Firewall
- Norton Personal Firewall
- McAfee Personal Firewall
- Sunbelt Personal Firewall
- ZoneAlarm
- Comodo Personal Firewall

Figure 07-27: Firewall

Use Anti-Virus Protection

Anti-virus is a software used to **detect viruses** and protect the system from threats. It should be used at the server. Viruses can be detected using **specific** or **generic** methods. Generic methods look for a virus-like performance rather than for a specific virus. Because of this, a virus is not named, but the user is warned of a possible virus infection. Also, the generic method can raise false alarms, so it is not considered as effective as a specific method. Other than commercial anti-virus programs, which come at a cost, many other anti-virus programs can be downloaded from the Internet for free.

Many Trojan backdoor programs, such as BO2k, Sub7, Hack-a-tac, and Netbus, have a well-known way of manipulating the system. An anti-virus program that scans for such attacks on the hard drive can easily recognize this mode of operation. Due to new application-level Trojan backdoor tools, it is imperative for the user to load the **most recent version** of this anti-virus software. While anti-virus software provides good protection, the user must also be cautious about what programs are being run on the machine. The anti-virus should be configured to scan:

- All work stations
- The complete network at regular intervals
- All incoming and outgoing traffic
- Email attachments
- Downloads
- Browsing

AVG Anti-Virus:

Source: http://www.grisoft.com

AVG Anti-Virus is the product of the Grisoft Company. It can be downloaded from www.grisoft.com. Like any other anti-virus software, it detects and removes viruses from a system.

Features:

- Downloads program and software updates from high-speed servers
- Detects the Internet connection to download the updates
- Works with multiple languages
- Detects, cures, and deletes the corrupted files or puts them in the Virus Vault

Kaspersky Anti-Virus 2011

Source: http://www.kaspersky.com

Kaspersky Anti-Virus provides a user with traditional anti-virus protection based on the latest protection technologies. The user can work, communicate, surf the Internet, and play online games on the computer safely and easily.

Features:

- Three protection technologies against new and unknown threats:
  - Hourly automated database updates
  - Preliminary and ongoing behavior analysis
  - On-going behavior analysis
- Provides protection from viruses, Trojans, worms, spyware, and adware
- Real-time scanning for email, Internet traffic, and files
- Provides protection from viruses when using ICQ and other IM clients

Norton Anti-virus

Source: http://www.symantec.com

Norton antivirus, a product of Symantec Corporation, can be downloaded from www.symantec.com. It can detect and remove viruses and other malicious codes from a system.

Features:

- Protects system from various viruses

- Loads in memory after Windows start-up
- Checks for viruses each time the software is used
- Examines all malicious activities on the network
- Updates virus definitions automatically
- Detects and repairs viruses in all incoming and outgoing emails messages and instant messenger attachments
- Defends against unauthorized use by protecting the password
- Monitors every new behavior, other than normal, to find new and unknown viruses
- Monitors network's traffic for malicious activity

Use Strong Passwords

A password is the first line of defense, and the user should ensure that the passwords selected for all user accounts are strong. While creating a password, the user should remember that the passwords should be:

Easy to remember: The password must be something that the user can remember, but not related to the user (such as date of birth, maiden name, or spouse name). Similarly, it should not contain bank information (e.g., Credit card number or PIN number).

Contain long and multiple symbols: A strong password is 8–10 digits long with letters, numbers, and characters (special characters can be used, but the password should be easy to remember).

Be frequently changing: Create a schedule to change the password periodically and use strong encryption algorithms to encrypt the password storage files such as a security account manager (SAM) and passwd.conf file.

Withstand filters and resist crackers: Use a filter that operates in real time and enforces some level of length and complexity on passwords. Run a cracker periodically on user-owned password files and change the password if the cracker is able to crack the password.

Make Regular Backups

Regular backups help to **avoid the loss of critical data** or files, which can be accidentally deleted or corrupted. It helps to restore data during security issues. Particularly, users should **back up the settings** and **configurations** of routers and firewalls. Also, they should create a book disk before a security event occurs, which helps in recovering the system when it is damaged or compromised.

The user can store backed-up data on many **different types of media**, including a different hard disk, rewriteable CD-ROMs/DVD-ROMs, tape drives, and compact storage media such as jump

drives. Prominently, Windows offers several ways to back up the data. Deciding when and how to back up the data relies on a number of issues. Selecting the correct backup options for a specific situation can help to ensure that information is properly protected from disaster. Windows uses the **Windows backup and restore center** for file backup, which keeps data safe from user errors and hardware and software failures.

The main reasons to backup data include:

- **Restoring the critical data after data loss:** The disaster condition may lead to the loss of critical information of the organization. But if the information has a backup copy, it would offer business continuity and thus allow restoring the information.
- **Restoring files when they are accidentally deleted or corrupted:** Because of improper password handling or during transmission/storage, it is possible for files to be corrupted or deleted. This discards the request of accessing the files by the authorized party. If this condition arises, backup would be an advantage and it helps in restoring those files.

Know about Encryption

Encryption is the conversion of data into an unreadable form called a cipher text. Unencrypted data is called plaintext. It **protects sensitive information** that is transmitted online. It is an effective way to achieve data security. Web browsers will encrypt text automatically when connected to a secure server. Encryption can be defined as protection by **camouflaging** data within a file or message so that unauthorized users cannot use it. File encryption is a type of file protection that **disguises the data** within a file or message so that the specific information included within the file or message cannot be read or understood by unauthorized users. A key is used to encode the data, and neither the file nor the key contents can be read by anyone who does not have the key. File encryption can be local, where a file that is on a disk is protected, or it can be used when a file is being transmitted over a network connection. Encryption consists of two types:

- **Asymmetric Encryption:**

  In asymmetric encryption, the user uses two keys. One key is used for encryption, and other key is used for decryption. One of the two keys must be kept secret. Asymmetric encryption is also called public key cryptography.

- **Symmetric Encryption:**

  Symmetric encryption uses only one key for encryption and decryption. The key must be kept secret. The sender and the receiver must share the key.

Identify a Secure Website

A visit to an unsecure website may lead to risk. Therefore, it is necessary for the user to know the difference between secure and unsecure websites. Secured websites can be

identified if:

- The URL contains **https://**
- The **lock** icon is present at the bottom right hand side of the browser

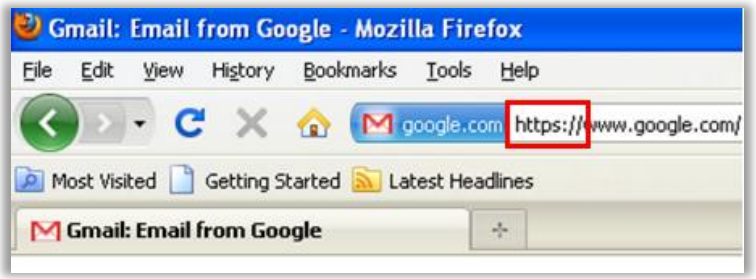


Figure 07-28: Screenshot of Gmail

Figure 07-29: Screenshot of a Webpage

General Security Practices in Home Networking

A home network allows computers to communicate with one another. To avoid the potential risks associated with data sharing over the Internet, all the users should:

- Use anti-virus software on all systems
- Use a personal firewall software package
- Do not open email attachments coming from unknown senders and disable scripting features in email programs
- Never run a program unless the sender/company is a trusted source
- Keep all applications, including the operating system, patched
- Turn off the system or disconnect its Ethernet interface when not in use
- Turn off Java, JavaScript, and ActiveX to keep the user from being vulnerable to malicious scripts (refer Module 04: Internet Security)
- Make regular backups of critical data

- Windows operating systems contain an option to Hide file extensions for known file types; disable this option display file extensions
- Make a boot disk to recover the system when it is damaged or compromised

Network Adapters

Checking Network Adapter

Steps to follow for checking a network adapter include:

- Go to **Start → Control Panel → Network and Sharing Center**
- Click **Manage Network Connections**

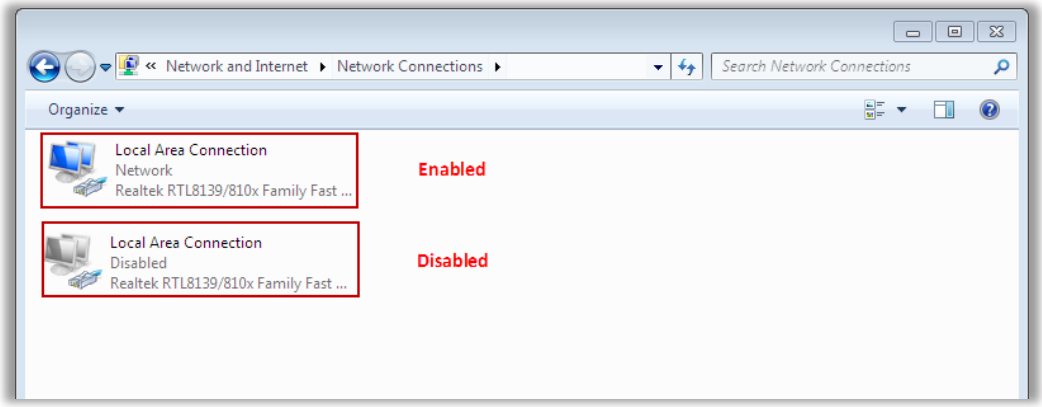


Figure 07-30: Network Connections

Network Setup Wizard

Steps to set up the network wizard:

- Go to **Start → Control Panel → Network and Sharing center → Set up a new connection or network → Connect to the Internet → Next**
- In the **Connect to the Internet** window, click **Set up a new connection anyway** and then click **Next**
- Select the connection type in **How do you want to connect** wizard and click **Next**
- Enter **User Name**, **Password,** and **Internet Service Provider (ISP)**
- Type the connection name, check **Allow other people to use this connection,** and click **Connect**

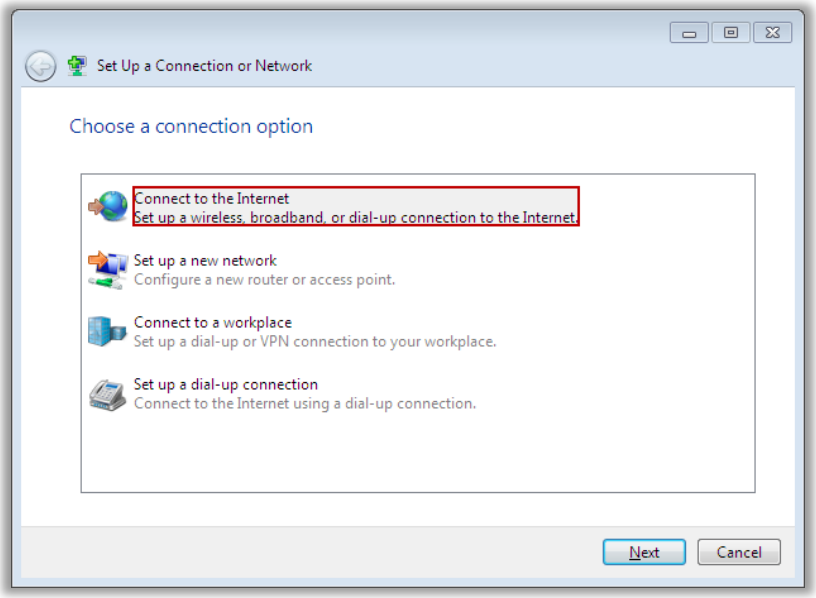


Figure 07-31: Network Setup Wizard

The steps to setup a network:

- If connected successfully, the window will display with **The connection to the Internet is ready to use**. Click **Close**
- Click **Yes** to restart the computer

How to Isolate Networking Problems (Windows 7): Network Adapter

To isolate networking problems in Windows XP network adapter:

- Go to **Start → Control Panel**
- Click **Network and Sharing Center**
- Click **Manage Network Connections**
- In the **Network Connections** window, examine the status of the network adapter

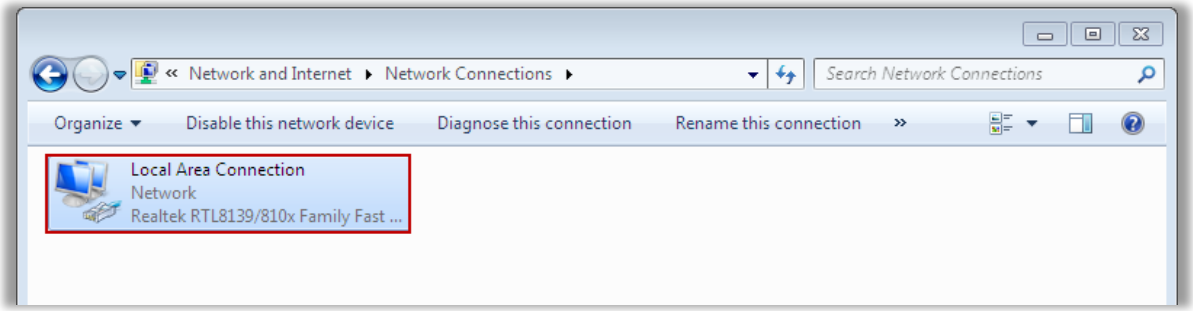


Figure 07-32: Network Connections

Network Adapter Status

See the following screenshot for the status of network adapter.

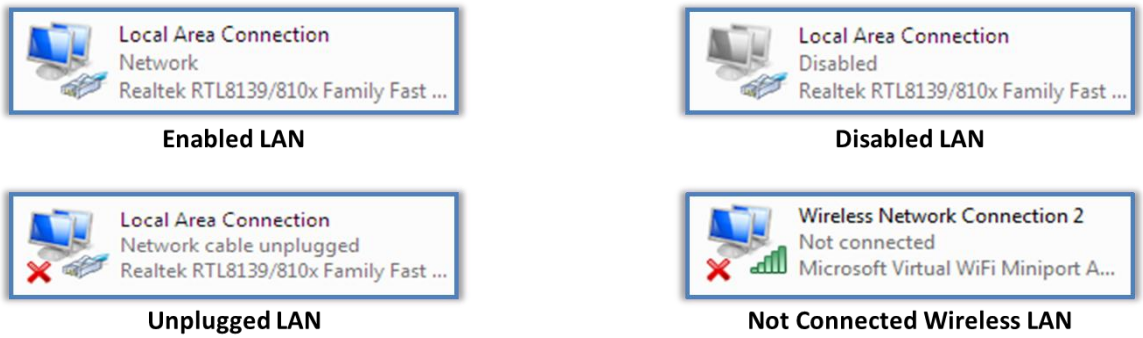


Figure 07-33: Status of Network Adapter

Troubleshooting with Network Adapters

Network Adapter is Unplugged

To verify whether the network adapter is unplugged, follow these steps:

- Verify that both ends of the network cable are properly connected.
- If the cable is properly connected, verify that the modem and router are plugged in and turned on.
- If the user has more than one network port available in the router, plug the cable into a different port. If the network connection works, then the original port on the router is faulty.
- Replace the network cable with a new cable. The user might have a faulty network cable.
- The network adapter on the system might have failed.

Network Adapter has Limited or No Connectivity

The network adapter sometimes fails to recognize the network connections and displays an error message like **Network adapter has limited or no connectivity.** The following steps may help solve the issue:

- In the **Network Connections** window, right-click the **Network Adapter**, and then click **Repair.**
- Unplug the modem; the modem is the device that is connected directly to the phone line (if the user has DSL) or cable connection.

- If the user has a router connected to the modem, unplug it and plug it back in again after some time.
- Restart the system.
- If the network adapter still shows **Limited or no connectivity** and the user has customized the router's configuration, verify that the router has dynamic host configuration protocol (DHCP) enabled.
- Enable DHCP, and then restart the computer.
- If the user is using a router, unplug the network cable that connects the modem to the router, and connect the computer directly to the modem. Now, restart the computer. If the computer connects properly after restarting, the problem is with the router.
- If the problem persists, contact the ISP for support.
- When there is limited or no connectivity, it may be due to a:
  - Failed Internet connection
  - Misconfigured router
  - Misconfigured network adapter

Network Adapter is Connected, but User cannot Reach the Internet

When the network adapter is connected, but the user cannot reach the Internet:

- First check whether the Internet is accessible; check for some websites such as www.microsoft.com, www.eccouncil.org.
- Unplug the modem, wait a minute, and then plug the modem back in.
- If the router is connected to the modem, unplug it, and reconnect it after a minute.
- Restart the computer.
- If the user has configured the system previously with a static IP address, he or she probably needs an automatic IP address at home.

Module Summary

A firewall is a part of a computer system or network that is designed to block unauthorized access.

The router acts as a shield to the network and manages all communications.

Wireless networks are used to connect the computers to each other without any cables.

Eavesdropping, data interception and modification, denial of service, spoofing, freeloading, and rogue WLANs are the common threats to the wireless network.

Windows Easy Transfer helps in transferring personal files, email, data, files, media, and settings from an old computer to a new one.

Sniffing, malware, email spoofing, chat clients, cross-site scripting, unprotected Windows shares, and mobile code are some of the network security threats.

Secure network connections using firewall, anti-virus, using strong passwords, regular backups, encryption, and so on.

Network Security Checklist

The network security checklist includes:

- ☐ Schedule regular backups of data files.
- ☐ Change network device passwords on a routine basis.
- ☐ Regularly update the operating system and other software with the latest patches.
- ☐ Block all access to the network infrastructure from the outside.
- ☐ Run performance monitoring software to alert you if something abnormal happens on the servers or network.
- ☐ Install anti-virus software on all workstations.
- ☐ Configure servers to scan both incoming and outgoing files.
- ☐ Scan all incoming and outgoing emails and attachments.