MODULE 3:

CONFIGURING COMPUTER SYSTEMS AND NETWORKS

Content Standard	Performance Standard
The learner demonstrates understanding of the underlying concepts and principles on configuring computer systems and networks.	The learner independently demonstrates skills in configuring computer systems and networks as prescribed by TESDA Training Regulations.

Number of Sessions (Time Allotment): 72 Hours (2 Quarters)

•Introduction

Welcome to the next level of your modular training in Computer Hardware Servicing (CHS) under the Information and Communications Technology (ICT) Course. In this module, you will have a great deal of understanding of Configuring Computer Systems and Networks.

At the end of this module you will be able to apply the knowledge and skills on planning and preparing for configuration, configure computer systems and networks and inspecting configured computer systems and networks. Those skills are essential for you to pass the National Certification II in Computer Hardware Servicing.

In this module, topics will be introduced progressively for easy understanding. After carefully answering the pre assessment exercises, reading all the lessons, answering all the guide questions, skilfully performing all the activities, showing evidences of learning and finally answering the summative test you will gain a considerable knowledge and skills in configuring computer systems and networks essential to be successful in computer hardware servicing as one of the career option in ICT.

Reminder! Just follow the instructions given in this module. Now let us start exploring new things in this module.

There are three learning objectives (LO) in this module: (1) plan and prepare for configuration; (2) configure computer systems and networks; and (3) inspect and test configured computer systems and networks. These three learning objectives (LO) contain sub-topics that discuss the details on *configuring computer systems and networks*. This module has four essential parts, namely: what to KNOW, what to PROCESS, what to REFLECT and UNDERSTAND and finally, what to TRANSFER.

The competencies for this module are the following:

LO 1. Plan and Prepare for Configuration of Computer Systems and Networks

- Follow Occupational Health and Safety (OHS) procedures in planning and preparing for configuration of computer systems and networks;
- Prepare computer systems tools, devices, equipment and materials;
- Check computer systems and networks configuration against specified requirements; and
- Identify the procedures in using the tools and equipment.

LO 2. Configure Computer Systems and Networks

- Follow OHS procedures in configuring computer systems and networks;
- Inspect networking devices, media and connectors;
- Create cross-over and straight-through cables;
- Assign IP address to clients and servers;
- Configure the assigned IP address to clients and servers;
- Enable network security to the computer systems; and
- Configure file and printer sharing.

LO 3. Inspect and Test Configured Computer Systems and Networks

- Follow OHS procedures in testing systems and networks;
- Test computer systems and networks in accordance with the job requirements; and
- Accomplish technical reports on the tests conducted.

In order to master the listed competencies, you must gain knowledge of the topics under what to KNOW, perform activities required under what to PROCESS, accomplish additional tasks under what to REFLECT and UNDERSTAND and finally show some evidences of your learning by transferring what you have learned to a different context under what to TRANSFER.

Pre Assessment

Before you proceed to the core of this module, challenge yourself first and dig deep into your mind in order to answer the pre assessment exercises prepared for you. Take time to answer it!

A. Paper and Pencil Test
General Directions: Read the items very carefully. Write your answer in a clean sheet of paper.

Test I. True or False
Directions: Write **TRUE** if the statement is correct and **FALSE** if otherwise.

_____1. A safe workplace is clean, organized and well-lit.

_____2. One must unplug the power from the source before opening a case and performing services.

_____3. It is a best practice that a fire extinguisher and first aid kit be available in the workplace.

_____4. You are allowed to open the power supply or a monitor.

_____5. You can bring food and drinks inside the laboratory.

_____6. The key to a well-tuned computer system is the proper configuration.

_____7. Boot log stores all information from the boot process.

_____8. Registry is a collection of database of configuration of database of configuration in Windows Operating System.

_____9. The shortcut of Microsoft Configuration is Ipconfig.

_____10. Configuration is the way a system is set up.

Test II. Multiple Choice

Directions: Write the letter of the correct answer in a clean sheet of paper.

1. What boot configuration utility allows setting the programs that will run at startup?
   a. Ipconfig   c. msconfig
   b. regedit   d. dxdiag
2. What application allows you to edit the registry?
   a. Ipconfig   c. msconfig
   b. regedit   d. dxdiag
3. Which of the following enables you to test sound and graphics output?
   a. Ipconfig   c. msconfig
   b. regedit   d. dxdiag
4. Which of the following is an applet that controls the look of windows?
   a. Appearance and Themes   c. Performance and Maintenance
   b. Network and Internet   d. Sounds, Speech and Audio
5. Which of the following applets does not belong to performance and maintenance category?
   a. Administrative tool   c. Power Options
   b. Automatic Updates   d. System
6. Which of the following is a wizard used to configure MS Windows for vision, hearing and mobility needs?
   a. Accessibility Option   c. Sounds, speech and audio
   b. Security Center   d. User Accounts
7. Which of the following tab in direct X Diagnostic tool displays your current audio settings?
   a. Input   c. Sound
   b. Music   d. System
8. Which of the following networking cable category is the most commonly used?
   a. Cat3   c. Cat 5 and 5e
   b. Cat 5   d. Cat 6
9. What copper-cored cable is surrounded by a heavy shielding?
   a. coaxial cable   c. optical fiber
   b. fiber optics   d. twisted pair
10. What Ethernet cable is used to connect two devices directly?
    a. cross- over   c. both A and B
    b. straight-through   d. none of the options
11. Which of the following is a number used to identify a device on a network?

Computer Hardware Servicing

a. Default gateway   c. IP address

b. DNS Server   d. Subnet mask

12. In which of the following IP address classes does 192.168.1.105 belong to?

a. Class A   c. Class C   e. Class E

b. Class B   d. Class D

13. What command is used to test the ability of the source computer to reach a specified destination computer?

a. Ipconfig   c. Ping

b. Msconfig   d. Regedit

14. What do you call an approach to computer networking where all computers show equivalent responsibility for processing data?

a. Client server   c. Peer to client

b. Peer to peer   d. None of the options

15. Which of the following is an example of a Class A subnet mask?

a. 255.0.0.0   c. 255.255.255.0

b. 255.255.0.0   d. 255.255.255.255

Test III. Matching Type

Directions: Match Column A with Column B. Write the letter of your answer in a separate paper.

A	B
1. Copper cabling used for telephone communication	a. Crimping tool
2. Standard Ethernet cable	b. Cross-over
3. Cable that has a very thin core	c. Fiber-optic
4. Cable that has a thicker core	d. Ipconfig
5. Tool used for crimping RJ45	e. Multi-mode
6. Connector for Cat 5e cable	f. Ping
7. Set of rules	g. Protocol
8. Indicates the network portion of an IP address	h. RJ45
9. Command used find out the IP address	i. Single-mode
10. Glass or plastic conductor	j. Straight-through
	k. Subnet mask
	l. Twisted pair

Test IV. ACRONYMS

Directions: Give the complete meaning of the following acronyms. Write your answer in a separate sheet of paper.

1. UTP
2. STP
3. IP
4. TCP /IP
5. HTTP
6. FTP
7. SSH
8. IMAP
9. SMTP
10. DHCP
11. DNS
12. TTL
13. LAN
14. VPN
15. NIC

B. Skills Checklist

Configuration Skills

Directions: Below is a matrix containing the most important skills that one must have to configure computer systems and networks successfully. Check (/) the appropriate column which describes the level of your confidence in performing the given tasks.

Competencies	I can do it confidently 3	I can do it confidently but with assistance 2	I am not confident 1
1. I can use the different tools for configuration.			
2. I can inspect networking devices and connectors.			
3. I can create a cross-over and straight-through Ethernet cable.			
4. I can test the functionality of an Ethernet cable.			
5. I can assign and			

configure IP address.			
6. I can execute the IPconfig command properly.			
7. I can manage to create a peer-to-peer networking.			
8. I can configure Network Interface Card using DHCP.			
9. I can enable a firewall.			
10. I can configure file and printer sharing.			
TOTAL			
GRAND TOTAL			

Add all the scores to get the grand total and then divide it by the total number of items. Refer to the verbal interpretation on the table below to determine your initial competency on configuration of computer systems and networks.

Numerical and Verbal interpretation

Numerical Value	Verbal Interpretation
2.51 – 3.00	Confident
1.76- 2.50	Confident but needs assistance
1.00 – 1.75	Not yet Confident

Don't feel bad if you got a "not yet confident" in all of the competencies. Bear in mind that this is just a pre assessment of the knowledge and skills on the lessons to be presented. Also, it will guide and inspire you to study harder as you go along with the lessons.

The following topics familiarize you with the tasks involved in planning and preparing for configuration of computer systems and networks. All you need to do is to carefully read all the topics and apply the skills you have gained through the distinct activities provided in this module. Good luck and have fun while learning!

Lesson 1. Plan and Prepare for Configuration

This lesson is intended to develop your skills in planning and preparing for configuration of computer system and networks. At the end of this lesson you are expected to:

- ✓ Familiarize, follow and apply OHS in configuring computer systems and networks;
- ✓ Prepare materials and tools for configuration;
- ✓ Check and adhere to the standard operating procedures and requirements in computer system and network configuration; and
- ✓ Identify the procedures in using the tools for configuration.

•What to KNOW

Safety Procedures

It is essential to maintain safe working conditions to prevent accidents and injury to any person or damage to any object in a work area. New staff and visitors must be informed of the appropriate safety procedures. Any transgression of the procedures must be reported.

As an aspiring computer technician, you should be aware of all possible dangers in the workplace. It is a must to follow proper procedures for handling computer equipment. Failure to follow the prescribed safety procedures could result in fines, criminal convictions, and damage to equipment, claims for damage from the owner of the property and data, injury, or death.

A safe work space is clean, organized, and well-lit. The disposal or recycling of hazardous computer components must be done properly. Make sure to follow regulations that govern how to dispose specific items. When an organization violates these regulations, there can be legal consequences.

To keep you safe, this module provides the general and fire safety guidelines that protects the technician and the equipment.

General Safety Guidelines

Follow the basic safety guidelines to prevent cuts, burns, electrical shock, and damage to eyesight. As a best practice, make sure that a fire extinguisher and first aid kit are available in case of fire or injury. Here are some general safety guidelines:

- Remove your watch or any other jewelry and secure loose clothing.
- Turn off the power and unplug equipment before opening the case and performing service.
- Cover any sharp edges inside the computer case with tape.
- Never open a power supply or a monitor.
- Do not touch areas in printers that are hot or those which use high voltage.
- Know where the fire extinguisher is located and learn how to use it.
- Know where the first aid kit is located.
- Keep food and drinks out of your workspace.
- Keep your workspace clean and free of clutter.
- Lift heavy objects with sturdy leg support to avoid back injury.

Fire Safety Guidelines

Follow fire safety guidelines to protect equipment and lives. Turn off and unplug the computer before beginning a repair to avoid damage to the computer or electric shock to the technician. Fire can spread rapidly and be very costly. Proper use of a fire extinguisher can prevent a small fire from getting out of control. When working with computer components, always consider the possibility of an accidental fire and prepare how to react. If there is a fire, you should follow these safety procedures:

- Always have a planned fire escape route before beginning any work.
- Never fight a fire that is out of control or not contained.
- Get out of the building quickly in case of an out-of-control fire.
- Contact emergency services immediately for help.

Computer Hardware Servicing

Peer-to-Peer Activity

General Directions: Get a partner to perform the next activity. Identify whether each statement is true or false. Gather picture evidences that make it **true** or **false**. On the third column, show the effects of not following the safety precautions through a picture presentation.

Example:
Turn off the power and unplug equipment before opening the case and performing service.

Answer	Picture Presentation	
	Evidence	Effect
True		

	TRUE OR FALSE	**EVIDENCE**	**Effect**
1. A safe workplace is clean, organized and well-lit.			
2. Before opening the case and performing services, one must unplug the power from the source.			
3. It is a best practice that a fire extinguisher and first aid kit be available in the workplace.			
4. You are allowed to open the power supply or a monitor.			
5. You can eat inside the laboratory.			

Research and Investigate

Directions: Form a group of five members and research on the different safety precautions used in computer laboratory. Interview/Observe a practitioner while lending a quality service in computer hardware servicing. Use a video camera to record the event stressing the safety guidelines and procedures in the laboratory. You will be rated according to the following rubrics:

Video Documentation of Computer Laboratory Safety Precautions

Criteria	Poor (70-75)	Good (76-85)	Excellent (86-100)
Content/Information (50%) • Technically sound information • Coherence of information	The provided information was not necessary or not sufficient to the computer laboratory safety precautions.	The provided information was, for the most part, necessary and sufficient to the computer laboratory safety precautions.	The provided information was necessary and sufficient to the computer laboratory safety precautions.
Quality of Video (30%) • Clarity and cohesiveness of the video • Organization and coherence of ideas	It lacks clarity and/or does not present ideas in a coherent way.	Most part is well organized, clear and presents ideas in a coherent way.	The video was well organized, clear and presents ideas in a coherent way.
Interview on practitioner (20%) • Congruency of questions to the topic • Clarity of questions	Questions were not congruent with the topic and were not delivered clearly.	Most of the questions were congruent with the topic and delivered clearly.	All of the questions were congruent with the topic and delivered clearly.

What to TRANSFER

Application of Safety Procedures While Accomplishing a Task

Directions: After the interview and observation with a practitioner, your group will showcase what you have learned through a role playing. You will be rated based on the Rubrics written below:

Rubrics for Role Playing

Criteria	Excellent 4	Good 3	Fair 2	Weak 1
Content (40%) -Conveys full understanding of the content				
Enthusiasm (10%) -Facial expression and body language generates strong enthusiasm				
Interest and Purpose (10%) -Displays interesting purpose				
Speak Clearly (10%) -Group members speaks clearly at all times				
Volume (10%) -Loud volume				
Preparedness (10%) -Group is prepared with props and costumes				
Cooperation (10%) -displays teamwork				

Computer Hardware Servicing

•What to KNOW

Prepare Materials and Tools Used for Configuration

A key to a well-tuned, trouble-free system is proper configuration. In order to accomplish this, you must start by understanding its configuration. It can be difficult to figure out all the devices in your system and the resources they are using.

To assist in this, several software tools have been created. These are typically called *diagnostic utilities or programs*. Some of them are built-in to your operating system and others are available either for free download or commercial purchase.

Some of the built-in tools used in Microsoft system configuration involves Microsoft System Configuration, Register Edit, Direct X and Control Panel Applets.

1. Microsoft System Configuration: This boot configuration utility allows you to set the programs that will run at startup and to edit configuration files. It also offers simplified control over Windows Services.

System Configuration Utility consists of five functional tabs such as General, Boot, Services, StartUp and Tools. The succeeding table describes the use and functionality of each tab:

Table 1. General Tab of System Config Utility

Tab	Function and Description
General	The general tab is the default tab in the System configuration and shows how the computer will start, by default Normal startup should be selected. List of choices for startup configuration: • *Normal Startup.* Starts Windows in the usual manner. Use this mode to start Windows after you are done using the other two modes to troubleshoot the problem. • *Diagnostic Startup.* Starts Windows with basic services and drivers only. This mode can help rule out basic Windows files as the problem. • *Selective Settings.* Starts Windows with basic services and drivers and the other services and startup programs that you select.
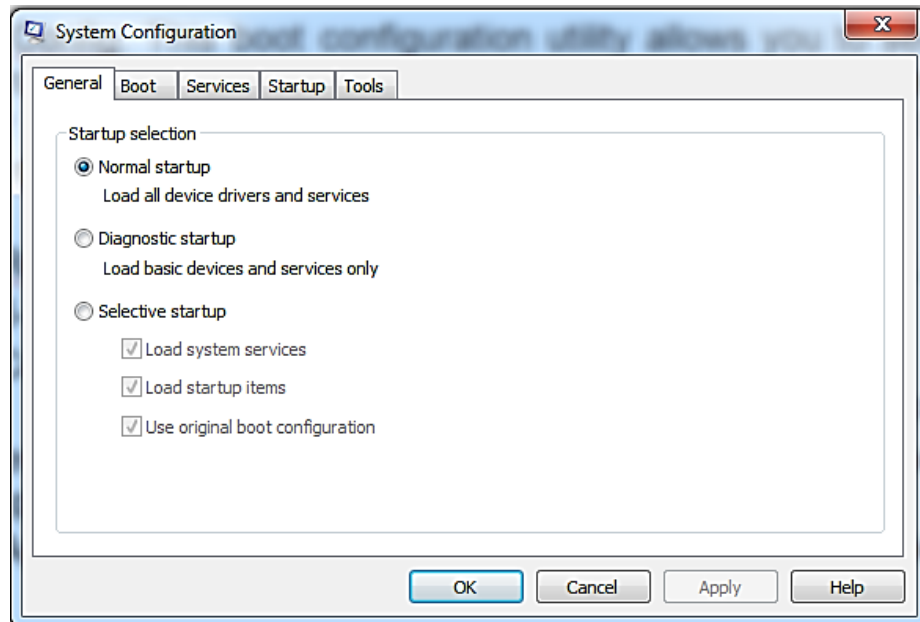
Figure 4. General Tab

Table 2. Boot Tab of System Config Utility

Tab	Function and Description
Boot	This tab allows you to make the same adjustments you can make in the Windows boot.ini file without having to edit the file. It shows configuration options for the operating system and advanced debugging settings, including the following: • Safe boot (Minimal): Boots the Windows graphics user interface in safe mode running only critical system services. Networking is disabled. • Safe Boot (Alternate Shell): Boots the Windows Command Prompt in safe mode running only critical system services. Networking and the graphical user interface are disabled. • Safe Boot (Active Directory Repair): Boots the Windows graphical user interface in safe mode running critical system services and Active Directory. • Safe boot (Network): Boots the Windows graphical user interface in safe mode running only critical system services. Networking is enabled. • No GUI boot. Does not display Windows splash screen when booting.

Computer Hardware Servicing

	• **Boot Log.** Stores all information from the boot process in the file %SystemRoot% Ntbtlog.txt. • **Base Video.** Boots to the Windows graphical user interface in minimal VGA mode. This loads standard VGA drivers instead of display drivers specific to the video hardware on the computer. • **OS boot information.** Shows driver names as drivers are being loaded during the boot process. • **Make all boot settings permanent.** Does not track changes made in System Configuration. Options can be changed later using System Configuration, but must be changed manually. When this option is selected, you cannot roll back your changes by selecting Normal startup on the General tab.
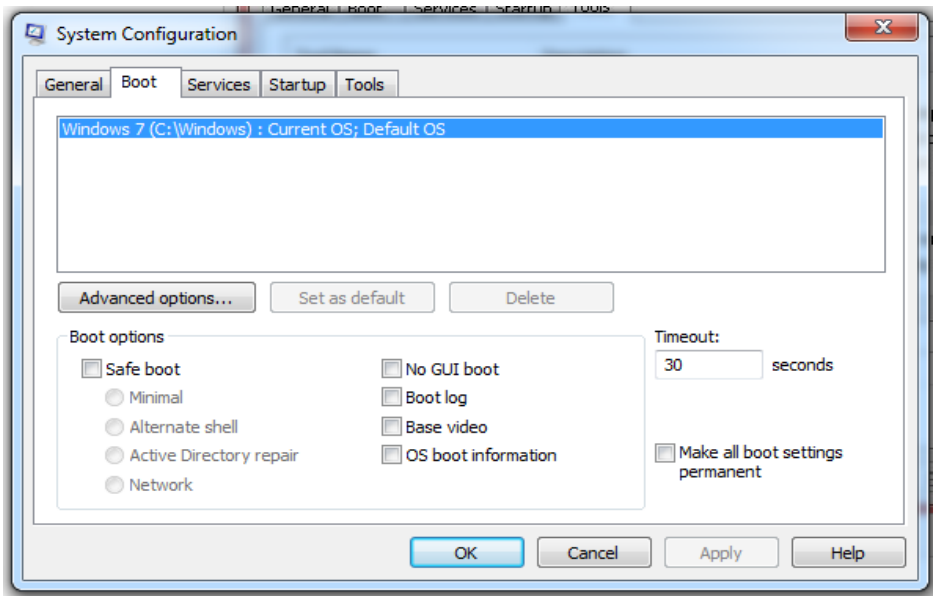
Figure 5. Boot Tab

Table 3. Services Tab of System Config Utility

Tab	Function and Description
Services	The Services tab allows you to enable or disable any of the Microsoft Windows services or other program services running on the computer. It lists all the services that start when the computer boots, along with their status (Running or Stopped). By checking the "Hide all Microsoft services" box at the bottom of the window, you can see all non-Windows

Computer Hardware Servicing

services such as driver services and program services that are often the cause of startup problems. Unchecking a box will disable the service from starting.

Warning:
Disabling services that normally run at boot time might cause some programs to malfunction or result in system instability. Do not disable services in this list unless you know they are not essential to your computer's operation. Selecting Disable all will not disable some secure Microsoft services required for the operating system to start.
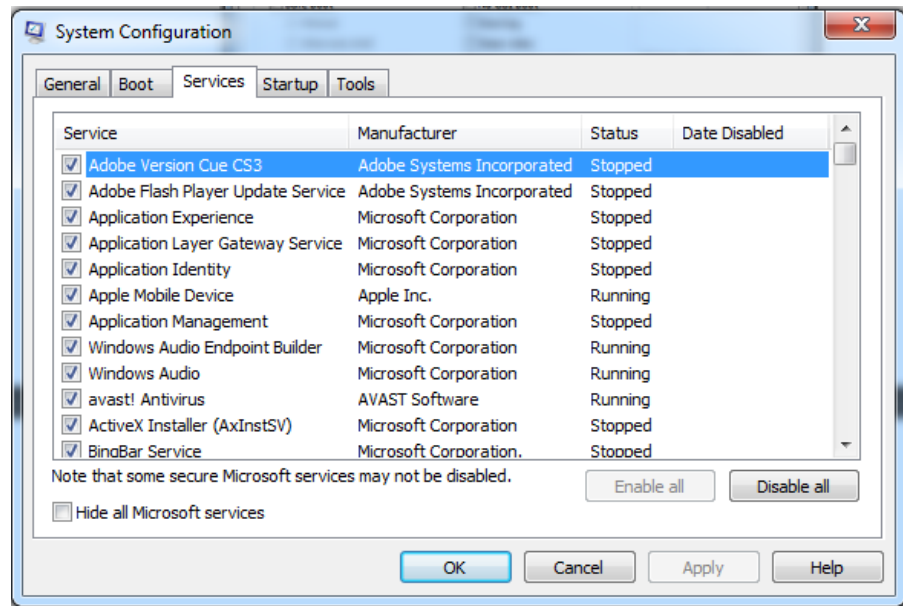
Figure 6. Services Tab

Table 4. Start Up Tab of System Config Utility

Tab	Function and Description
Startup	The Startup tab is one of the most frequent reasons most Windows users enter the System Configuration utility. In the Startup tab, you will be able to see the list of applications that run when the computer boots, along with the name of their publisher, the path to the executable file, and the location of the registry key or shortcut that causes the application to run. These startup programs are often one of the biggest causes for a computer to startup and run slow. You can clear the check box for a startup item to disable it on your next boot. If you have chosen Selective startup on the General Tab, you must either choose Normal startup on the

51

General tab or select the startup item's check box to start it again at boot time. If you suspect an application has been compromised, examine the Command column to review the path to the executable file.

Windows 8 Microsoft has removed this Startup feature in the System Configuration utility and moved it into the Windows 8 Task Manager. Uncheck any program that you want to disable from starting up each time.

Note:
Disabling applications that normally run at boot time might result in related applications starting more slowly or not running as expected.
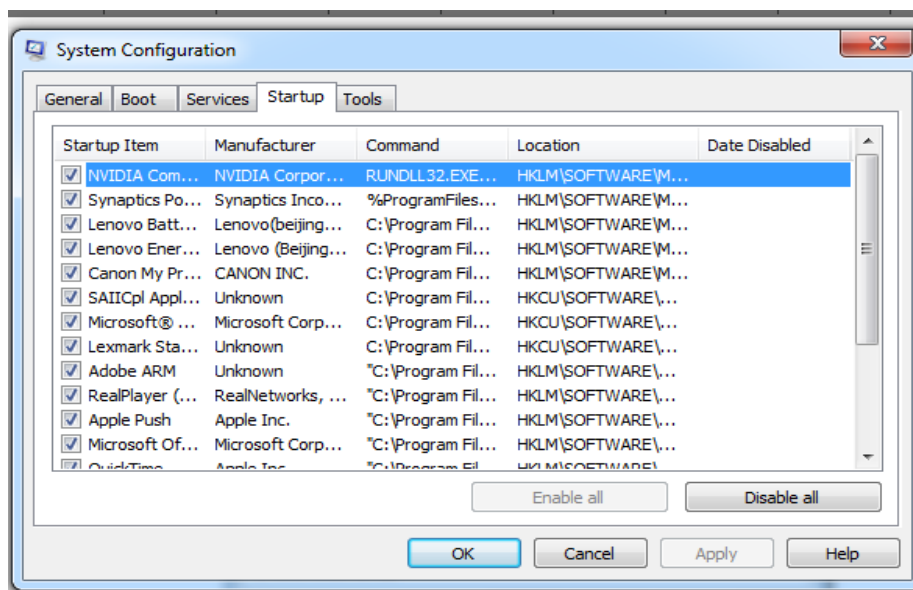
Figure 7. Startup Tab

Table 5. Tools Tab of System Config Utility

Tab	Function and Description
Tools	This Provides a convenient list of diagnostic tools and other advanced tools that you can run.
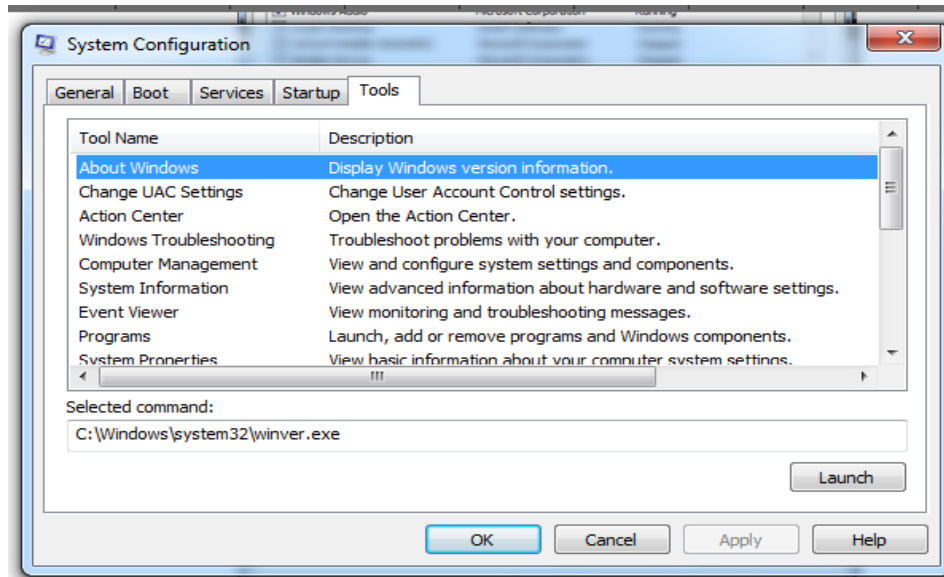
Figure 8. Tools Tab

2. Register edit: This application allows you to edit the registry.

The Windows Registry, usually referred to as "the registry," is a collection of databases of configuration settings in Microsoft Windows operating systems.

In Windows 2000 and Windows XP, the Registry is stored in several Hives, located in the following path: \windows\system32\config and \Documents and Settings\ {username} folders.

Structure of the Registry

1. The Registry has a hierarchical structure, like the directories on your hard disk. Each branch (denoted by a folder icon in the Registry Editor, see below) is called a *key*. Each key can contain other keys, as well as Values. Each value contains the actual information stored in the Registry. There are three types of values: String, Binary, and DWORD - the use of these depends upon the context.

2. There are six main branches (five in Windows 2000 and Windows XP), each containing a specific portion of the information stored in the Registry. They are as follows:

   o HKEY_CLASSES_ROOT - this branch contains all of your file types as well as OLE information for all your OLE-aware applications.

Computer Hardware Servicing

- o HKEY_CURRENT_USER - this branch points to the part of HKEY_USERS appropriate for the current user.
- o HKEY_LOCAL_MACHINE - this branch contains information about all of the hardware and software installed in your computer. Since you can specify multiple hardware configurations, the current hardware configuration is specified in HKEY_CURRENT_CONFIG.
- o HKEY_USERS - this branch contains certain preferences (such as colors and control panel settings) for each of the users of the computer. In Windows 95/98/Me, the default branch here contains the currently-logged in user. In Windows 2000/XP, the default branch here contains a template to be used for newly-added users.
- o HKEY_CURRENT_CONFIG - this branch points to the part of HKEY_LOCAL_MACHINE appropriate for the current hardware configuration.
- o HKEY_DYN_DATA (Windows 95/98/Me only) - this branch points to the part of HKEY_LOCAL_MACHINE, for use with Windows' Plug-&-Play subsystem.

3. Direct X Diagnostic: The **Microsoft DirectX Diagnostic Tool** provides you with information about the DirectX API components and drivers on your system. It enables you to test sound and graphics output and Microsoft DirectPlay service providers. You can use the diagnostic tool to gather information about your system to use for diagnostic purposes.

   If you are experiencing problems when running Microsoft **DirectX** applications, the DirectX Diagnostic Tool can help you find the source of the trouble such as incorrect versions of DirectX components, lack of hardware acceleration, devices that are not connected and unsigned drivers.
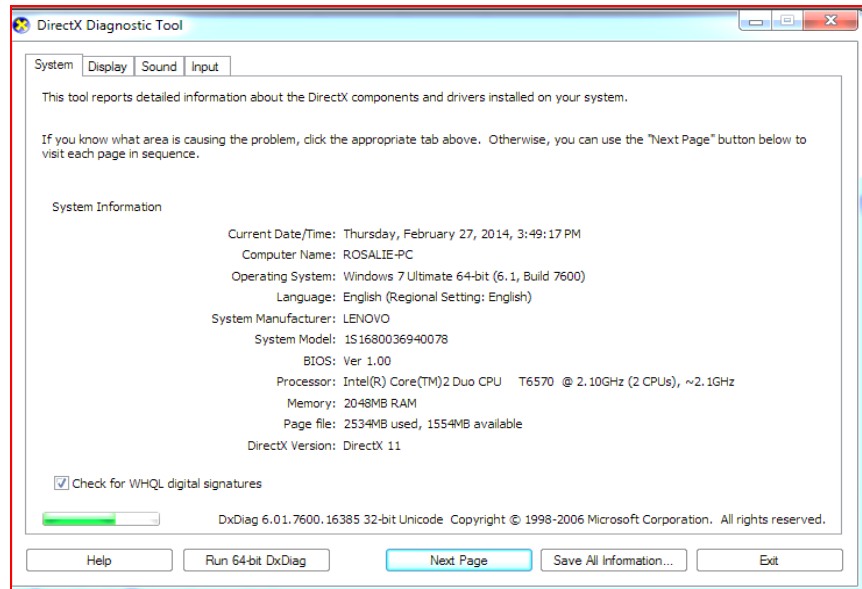
Figure 9. DX Diagnostic Tool

4. Control Panel applets

The names of various applets in the Control Panel differ slightly depending on the version of Windows installed. In Windows XP, the icons are grouped into categories:

- **Appearance and Themes**: Applets that control the look of windows:
  - ✓ Display
  - ✓ Taskbar and Start menu
  - ✓ Folder options
- **Network and Internet Connections**: Applets that configure all the connection types:
  - ✓ Internet options
  - ✓ Network connections
- **Add or Remove Programs**: An applet to add or remove programs and windows components safely
- **Sounds, Speech, and Audio Devices**: Applets that control all the settings for sound:
  - ✓ Sounds and audio devices
  - ✓ Speech
  - ✓ Portable media devices
- **Performance and Maintenance**: Applets to find information about your computer or perform maintenance:
  - ✓ Administrative tools
  - ✓ Power options
  - ✓ Scheduled tasks
  - ✓ System

Computer Hardware Servicing

- **Printers and Other Hardware**: Applets to configure devices connected to your computer:
  - ✓ Game controllers
  - ✓ Keyboard
  - ✓ Mouse
  - ✓ Phone and modem options
  - ✓ Printers and faxes
  - ✓ Scanners and cameras
- **User Accounts**: Applets to configure options for users and their e-mail:
  - ✓ E-mail
  - ✓ User accounts
- **Date, Time, Language, and Regional Options**: Applets to change settings based on your location and language:
  - ✓ Date and time
  - ✓ Regional and language options
- **Accessibility Options**: A wizard used to configure windows for vision, hearing, and mobility needs
- **Security Center**: Applet used to configure security settings for:
  - ✓ Internet options
  - ✓ Automatic updates
  - ✓ Windows firewall

•What to PROCESS

I. MS Configuration Command Classification

Directions: There are five functional tabs in MS Configuration utility, namely General, Boot, Services, Startup and Tools. Classify the following items according to the tabs they belong to. Write your answer on a separate paper.

1. Event Viewer
2. Safe Boot
3. List of services that start when computer boots
4. Make all boot settings permanent
5. Normal startup
6. No GUI Boot
7. OS Boot information
8. Hide All Microsoft Services
9. Convenient List of Diagnostic Tools
10. Base Video

II. Applet Grouping

Directions: Complete the diagram of various Control Panel Applets with the components included in their category.

Appearance and Themes
1. _____
2. _____
3. _____

Network and Internet Connections
1. _____
2. _____

Sounds, Speech, and Audio Devices
1. _____
2. _____
3. _____

Printers and Other Hardware
1. _____
2. _____
3. _____
4. _____
5. _____

Security Center
1. _____
2. _____

Research and Explore

Directions: Conduct a research that identifies other available tools used for computer system and network configuration. Use some other resources like the World Wide Web and interview a practitioner (preferably an IT specialist or a computer technician) to find out the different tools they use for configuration. Your research will be rated according to the following criteria:

Rubrics for Term or Research Paper

Qualities & Criteria	Poor (70-74)	Good (75-79)	Very Good (80-89)	Excellent (90-100)
Format/Layout (15%) • Presentation of the text • Structuring of text • Requirements of length, font and style followed	Followed poorly the requirements related to format and layout.	Some format and layout related requirements were met.	Most format and layout related requirements were met.	All the requirements related to format and layout were strictly followed.
Content/Information (50%) • All elements of the topics are addressed • The information is technically sound • Information based on careful research • Coherence of information	The research was not objective and poorly addresses the issues referred in the proposed topic. The provided information was not necessary or not sufficient to discuss these issues.	The research was objective and for some part addresses an in-depth analysis The provided information was, for some part, necessary and sufficient to discuss these issues.	The research was objective and for the most part addresses an in-depth analysis of most issues referred in the proposed topic. The provided information was, for the most part, necessary and sufficient	The research was objective and addresses with an in-depth analysis all the issues referred in the proposed topic. The provided information was necessary and sufficient to discuss

			to discuss these issues.	these issues.
Quality of Writing (25%) • Clarity and cohesiveness of sentences and paragraphs • No errors in spelling, grammar and use of English • Organization and coherence of ideas	The essay was not well written, and contains many spelling errors, and/or grammar errors and/or use of English errors. It lacks clarity and/or does not present ideas in a coherent way.	The essay was well written for some part, without spelling, grammar or use of English errors. The essay is for some part well organized, clear and presents ideas in a coherent way.	The essay was well written for the most part, without spelling, grammar or use of English errors. The essay is for the most part well organized, clear and presents ideas in a coherent way.	The essay was well written from start to finish, without spelling, grammar or use of English errors. The essay was well organized, clear and presents ideas in a coherent way.
References (10%) • Soundness of references	References were not appropriately used and cited.	Some of the references were appropriately used and cited.	Most of the references were appropriately used and cited.	All of the references were appropriately used and cited.

Computer Hardware Servicing

What to TRANSFER

Oral Presentation

Directions: After the thorough research and exploration, you have to present your work individually in an oral presentation. Your performance will be rated based on the rubrics provided in this section.

Rubrics for Oral Presentation					
CRITERIA	**B** (70- 74)	**D** (75-79)	**AP** (80-84)	**P** (85-89)	**A** (90-100)
1. Gave an interesting introduction					
2. Presented clear explanation of topic					
3. Presented information in a logical manner					
4. Used complete sentence					
5. Offered a concluding statement					
6. Spoke clearly, correctly, distinctly, and confidently					
7. Maintained eye contact					
8. Maintained good and proper posture					
9. Utilized audio-visual materials					
10. Answered questions sufficiently and received comments openly					
Total					
Grand Total					

Legend:
B- Beginner   **P**- Proficient
D- Developing   **A**- Advance
AP- Approaching Proficiency

Procedures in Using Computer System Configuration Tools

As a future computer technician you must be diligent and eager to know the different procedures in using the tools for computer system configuration. This will help and guide you to carry out a particular job in a proper manner. Once you already identify them, you must also acquire the necessary and appropriate skills to apply them in actual situations.

This part of the module present some of the required procedures in computer system configuration. Take note that you need to exert extra effort in finding out some procedures which are not in this module. This is your chance to explore and learn through your own experience.

The subsequent sections below present the various procedures in using Computer System Configuration Tools:

1. Accessing and using Microsoft System Configuration
   - Click on **Start Button**
   - In the Search Box, type Run
   - In the Run window, type **msconfig**, and press **Enter**.
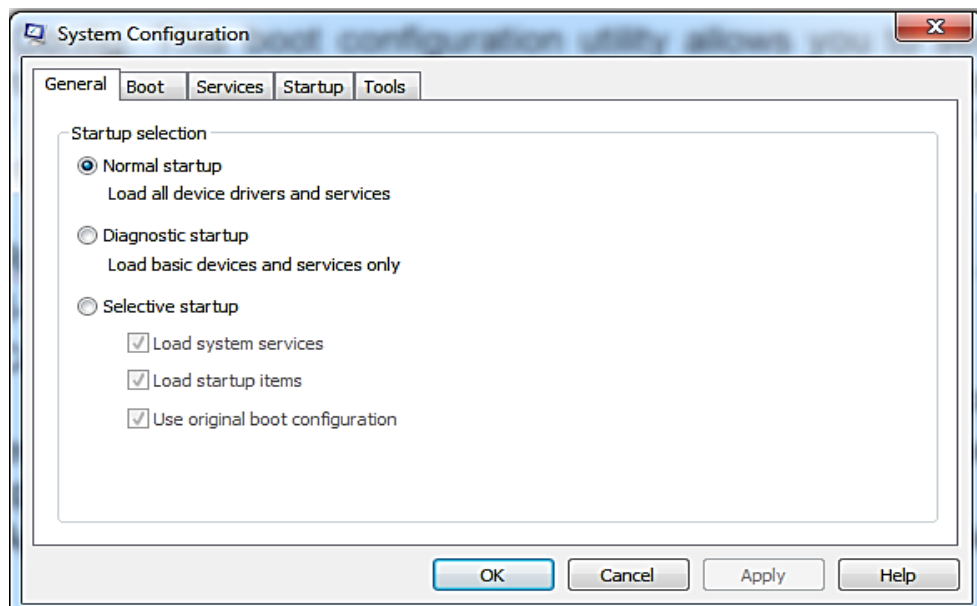
Figure 10. General Tab of Microsoft system configuration

2. Accessing and using Regedit:
   - Click on **Start Button**
   - In the search box, or *Run* window, type the following:
     regedit and then press **Enter**.
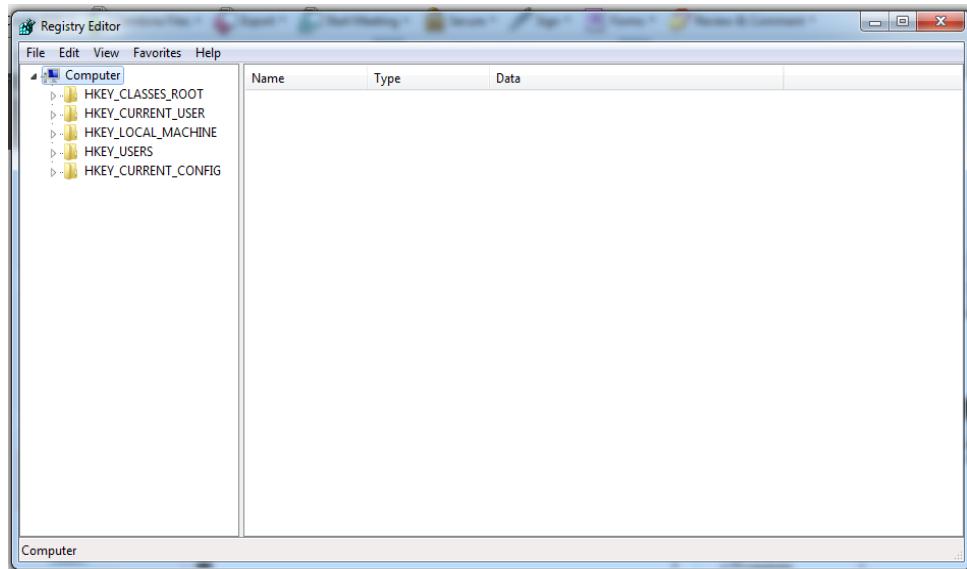
Figure11. Registry Editor Window

Using the Registry Editor

The Registry Editor (regedit.exe) is included in Windows to enable you to view and edit the contents of the Registry. When you open the Registry Editor, you will see a window divided into two panes. The left side shows a tree with folders (see Structure of the Registry above), and the right side shows the contents (values) of the currently selected folder (key).

✓ To expand a certain branch, click on the little plus sign [+] on the left of any folder, or just double-click on the folder.

✓ To display the contents of a key (folder), just click the desired key, and look at the values listed on the right side.

✓ You can add a new key or value by selecting New from the Edit menu.

✓ You can rename any value and almost any key with the same method used to rename files; right-click on an object and click rename, or click on it twice (slowly), or just press F2 on the keyboard.

Computer Hardware Servicing

✓ Lastly, you can delete a key or value by clicking on it, and pressing Delete on the keyboard, or by right-clicking on it, and choosing Delete.

Caution: Using regedt32.exe or regedit.exe incorrectly might cause configuration problems that may require you to reinstall the operating system.

3. Accessing and Using Direct X Diagnostic

You can test **Microsoft DirectDraw** and Direct3D on each monitor attached to your system. You can also test DirectSound on each wave output device, and **DirectMusic** on each music port.

To run the DirectX Diagnostic Tool (DX Diagnostic Tools Window of Windows XP differs from Windows 7 but it does the same function):
- Click on Start Button, type Run on the search box.
- On the Run window, Type in **dxdiag** and click Ok or press Enter, as shown in Figure 9, Run Dialog Box.
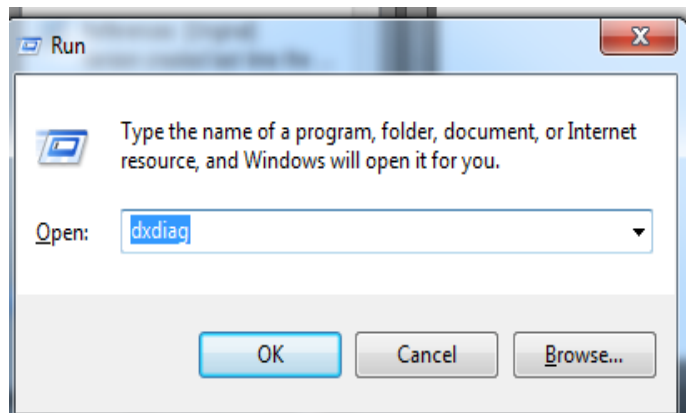
Figure12. Run Dialog Box

- Next you will see a new window with various tabs.
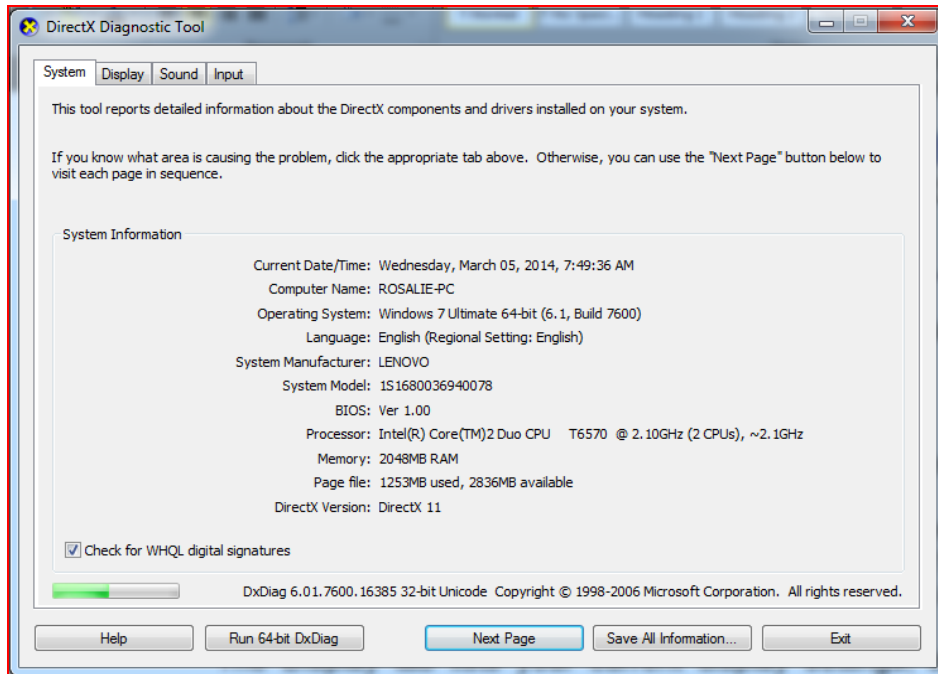
Figure13. System Tab of DX Diagnostic Tool

❖ The **System** tab shows information about your computer and displays the version of DirectX installed on your computer.
❖ The **DirectX Files** tab shows the file name and the version number for each DirectX file installed on your computer. It also shows the file names and the version numbers of other files that are used by games that are running under DirectX.
❖ The **Display** tab lists your current display settings, and allows you to disable DirectDraw, Direct3D, and AGP Texture Acceleration. You can also test DirectDraw and Direct3D from the Display tab which will indicate that the DirectX Graphics runtime files are installed and operating correctly. It will also display your device's available memory and can tell you if your video driver has passed Microsoft's Windows Hardware Quality Labs testing standard. The DirectX Diagnostic Tool, however, cannot report memory that is in use at the time that it starts and you may see less memory reported than your video card actually has.
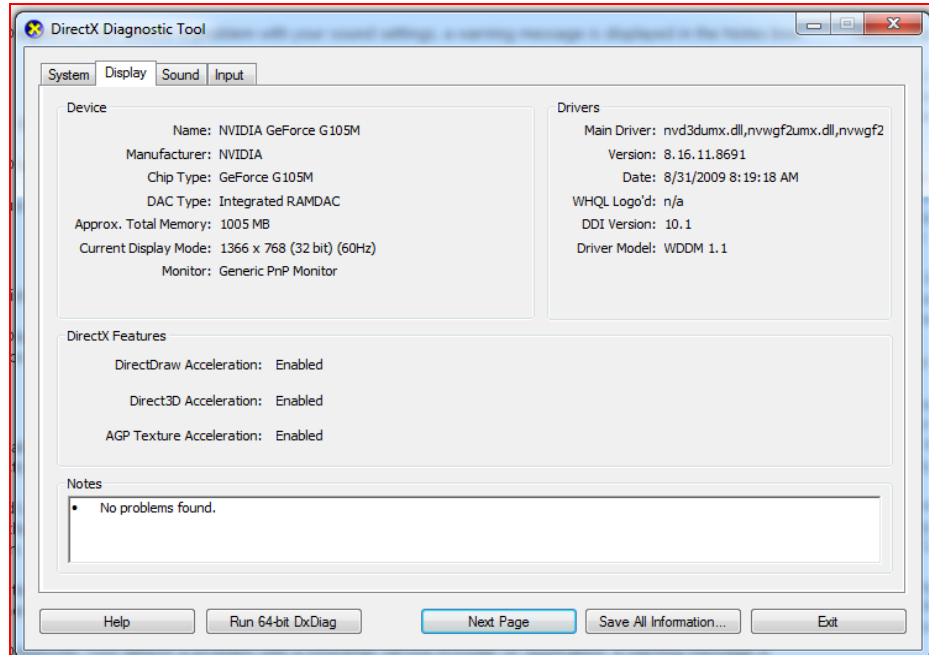
Figure14. Display Tab of DX Diagnostic Tool

❖ The **Sound** tab displays your current audio settings and allows you to test DirectSound. It will tell you if the audio driver are signed, meaning that it has passed Microsoft's Windows Hardware Quality Labs testing standard. The Hardware Sound Acceleration Level slider is used to correct audio glitches that might be caused by some audio drivers. You can adjust the slider settings and see if it provides better results in your application. Be sure not to lower it too much or you may disable some audio features of your system. If the tool detects a problem with your sound settings, a warning message is displayed in the Notes box.

❖ The **Music** tab displays your current **MIDI** settings, and allows you to test the DirectMusic component of DirectX. Click on the Test DirectMusic button to perform the test. If the DirectX Diagnostic Tool detects a problem with DirectMusic, a warning message is displayed in the Notes box.
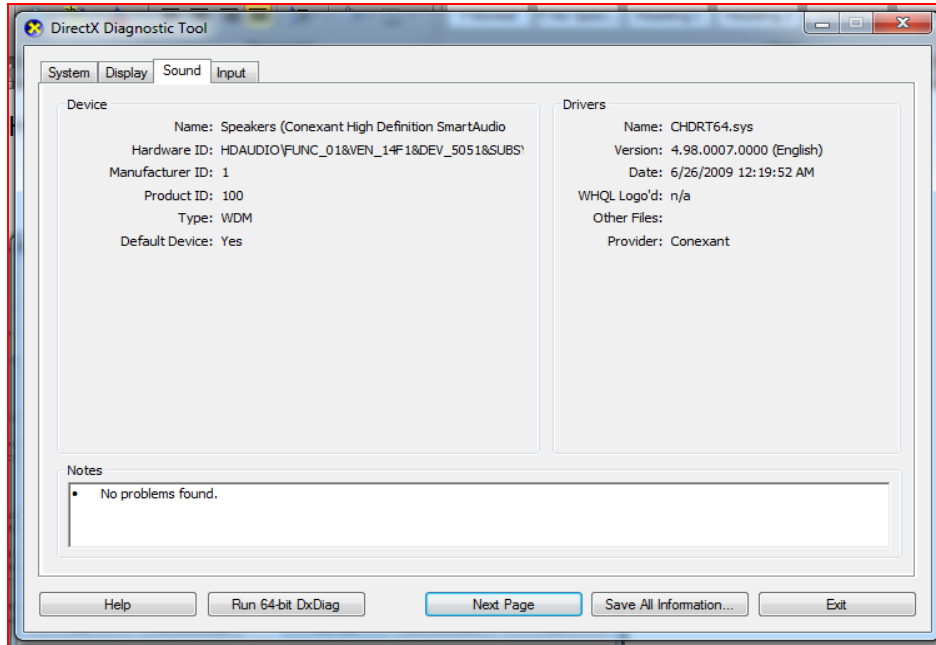
Figure15. Sound Tab of DX Diagnostic Tool

❖ The **Input** tab lists the input devices connected to your computer such as USB and PS2 devices. It also displays the input drivers installed on your computer. If the DirectX Diagnostic Tool detects a problem with an input device or an input device driver, a warning message is displayed in the Notes box.
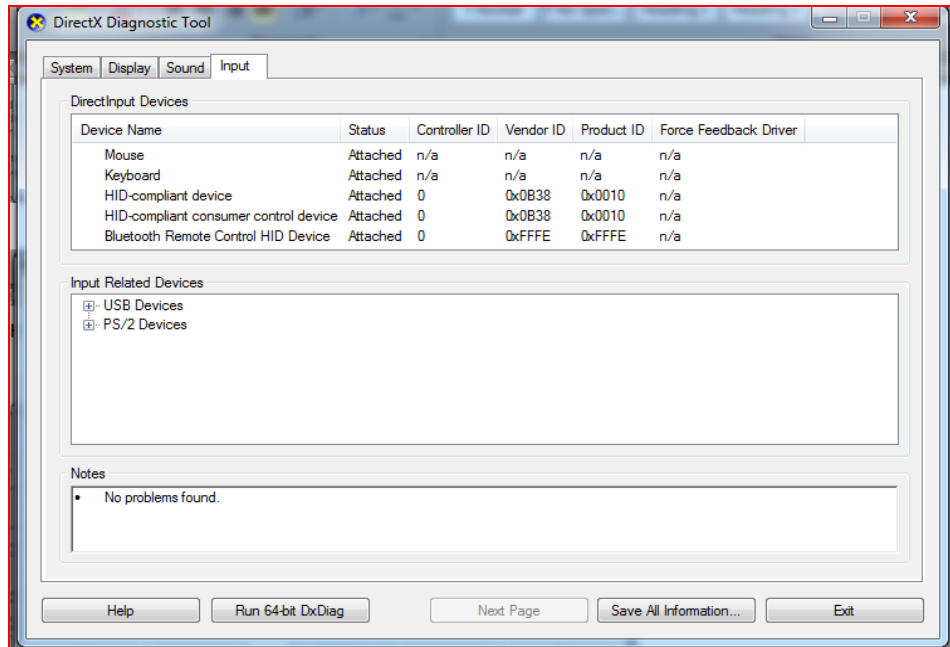
Figure16. Input Tab of DX Diagnostic Tool

❖ The **Network** tab lists the registered DirectPlay Service Providers. These are the connection methods that DirectPlay will operate across. A registry problem here can normally be resolved by reinstalling DirectX. A registry error here can normally be resolved by removing and reinstalling that application. If the DirectX Diagnostic Tool detects a problem with a DirectPlay Service Provider or Application, a warning message is displayed in the Notes box.

❖ The **More Help** tab allows you to further troubleshoot problems that the other tabs could not resolve. Features include the **DirectX troubleshooter,** sound troubleshooter, system information tool and the override tool which will override DirectDraw's refresh rate.

Windows Registry Backup and Recovery

Directions: In this activity you will back up a computer registry. You will also perform a recovery of a computer registry. The registry is also called System State data. You will be given 1 hour to accomplish this activity.

Recommended Equipment:
> A computer system running Windows XP is required for this exercise.

Procedures:
Step 1
- ✓ Log on to the computer as yourself.
- ✓ Click **Start > Run**.
- ✓ Type **ntbackup** and then click **OK**. The "Backup or Restore Wizard" window appears.
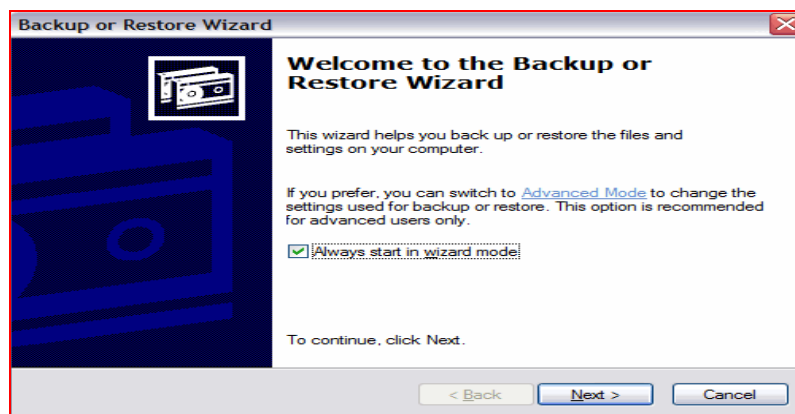
Figure 17. Backup or Restore Wizard

Step 2
- ✓ Click **Advanced Mode**.
- ✓ The Backup Utility window appears.
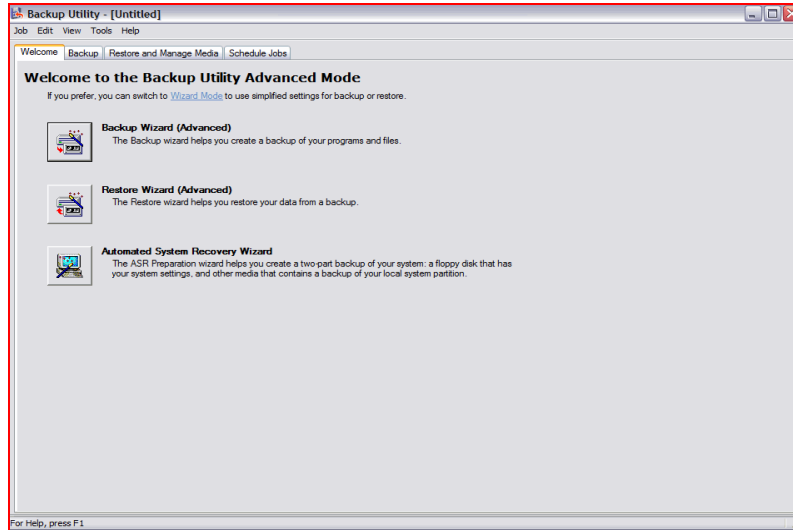
Figure 18. Backup Utility Window

Step 3
- ✓ Click **Backup Wizard**.
- ✓ The "Welcome to the Backup Wizard" window appears.
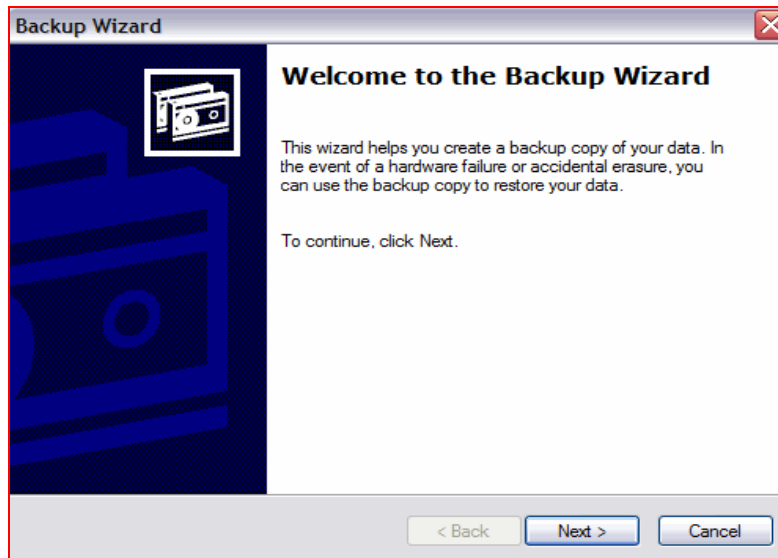
Figure 19. Backup Restore Wizard Window

Step 4
- ✓ Click **Next**.
- ✓ Click the **Only back up the System State data** radio button.
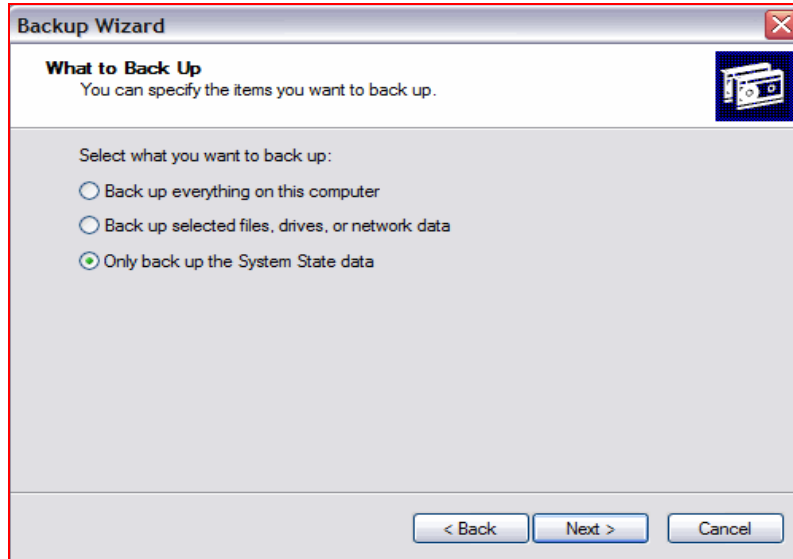
Figure 20. Choose "Only backup system state data"

Step 5
- ✓ Click **Next**.
- ✓ The "Backup Type, Destination, and Name" window appears.
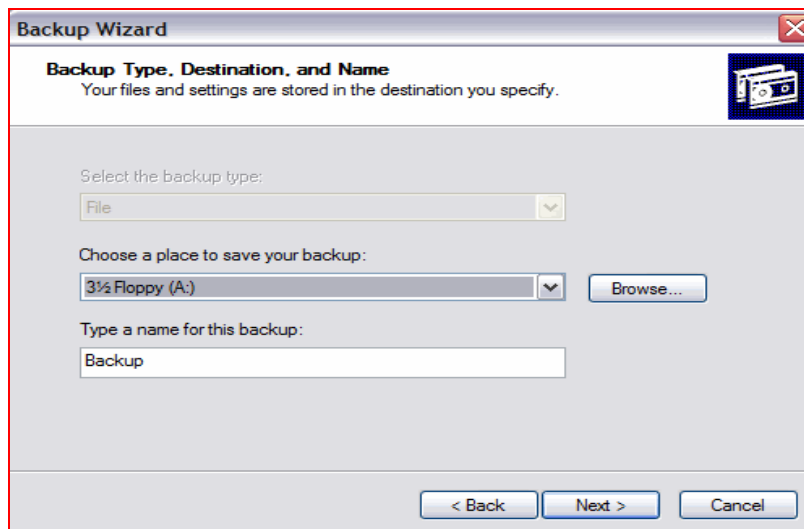
Figure 21. Backup Type Destination, and Name" Window

Step 6
- ✓ Click **Browse.**

✓ If you are asked to insert a disk into the floppy disk drive, click **Cancel**.
✓ The "Save As" dialog box appears.
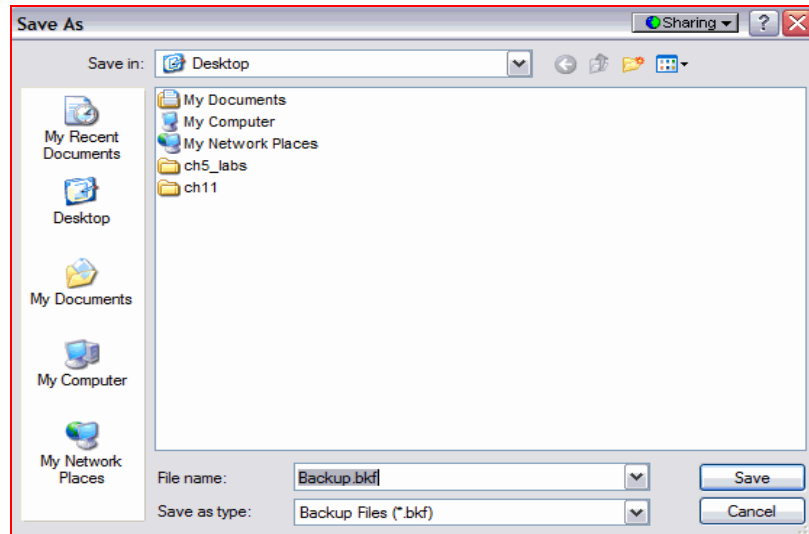
Figure 22. Save As Dialog Box

Step 7
✓ Click the **My Documents** icon on the left side of the "Save As" dialog box.
✓ Click **Save**.
✓ The "Backup Type, Destination, and Name" window re-appears.

Step 8
✓ Click **Next**.
✓ The "Completing the Backup Wizard" appears.

Figure 23. Completing the Backup Wizard Window

Step 9
- ✓ Click **Advanced.**
- ✓ The "Type of Backup" window appears.
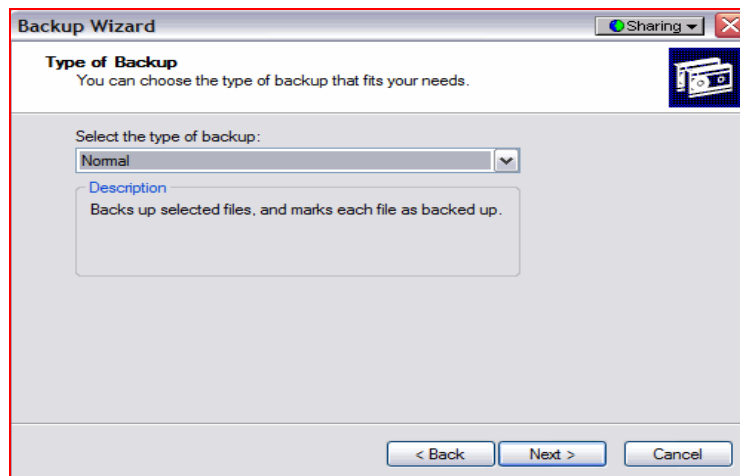
Figure 24. Type of Backup Window

- ✓ The default backup type is "Normal". If available, make sure that "Backup Migrated Remote Storage Data" is not checked.

Step 10
- ✓ Click **Next**.
- ✓ The "How to Backup" window appears.

Computer Hardware Servicing
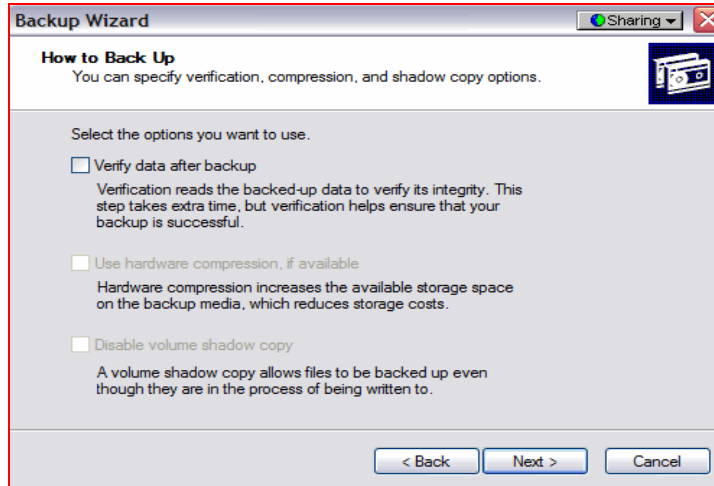
Figure 25. How to Backup Window

Step 11
- ✓ Click the **Verify Data After Backup** check box, and then click **Next**.
- ✓ The "Backup Options" window appears.
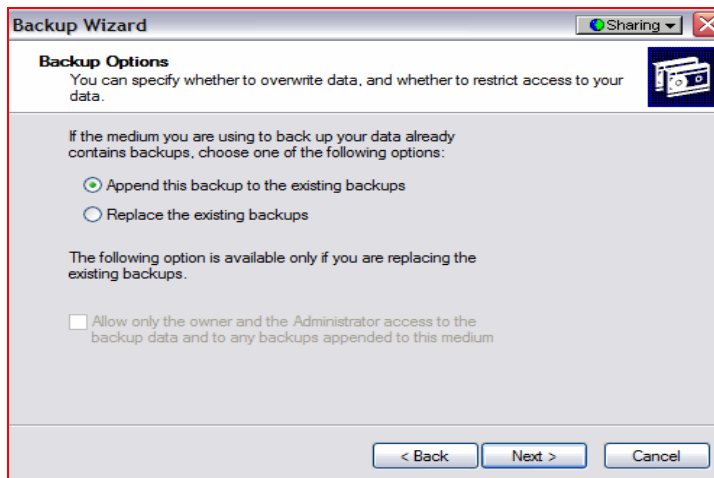
Figure 26. Backup Options Window

Step 12
- ✓ Click **Replace the existing backups**, and then click **Next**.
- ✓ The "When to Back Up" window appears.

Computer Hardware Servicing
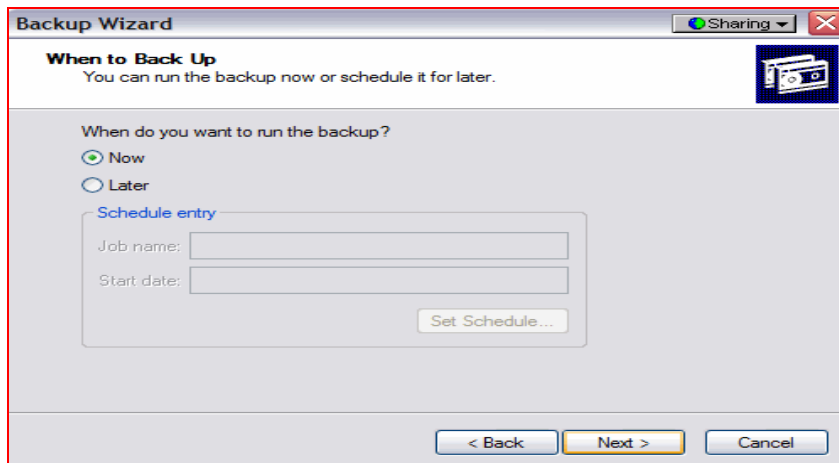
Figure 27. When to Backup Window

Step 13
- ✓ At the "When To Back Up" window, click **Now** and then click **Next**.
- ✓ The "Completing the Backup Wizard" window appears.

Figure 28. Completing the Backup Window

Step 14
- ✓ Click **Finish**.
- ✓ The "Backup Progress" window appears.

Computer Hardware Servicing
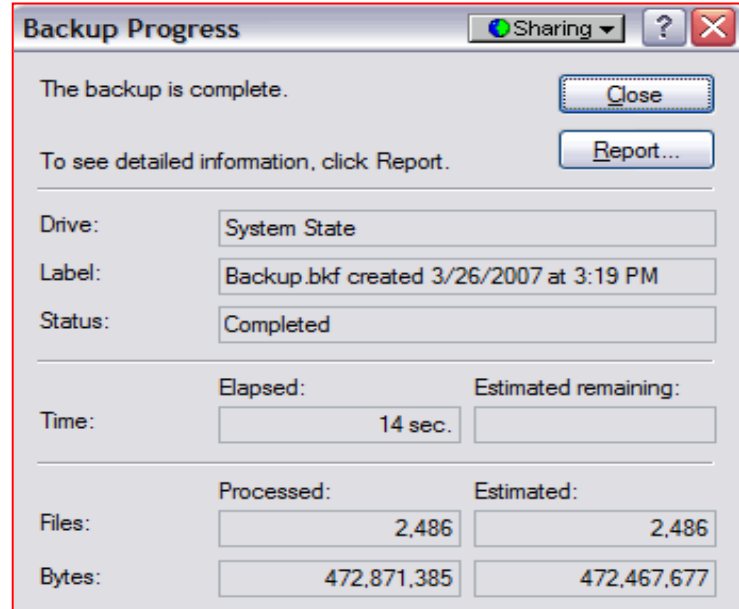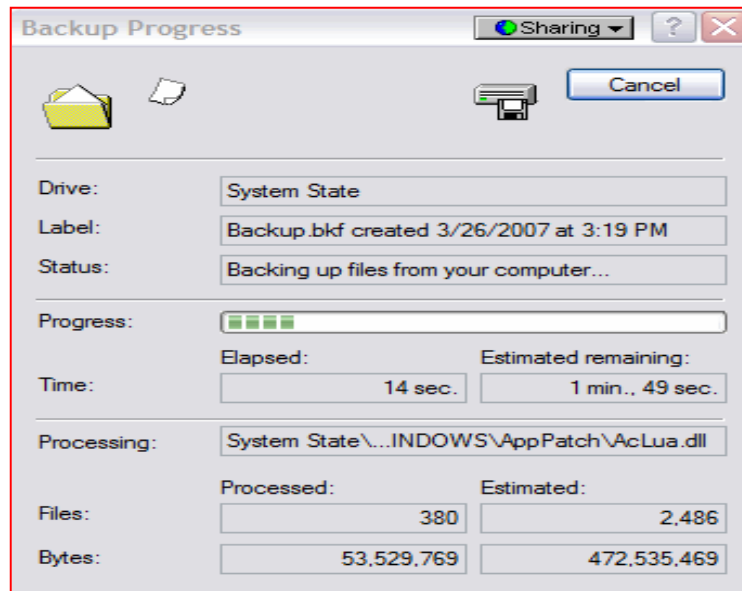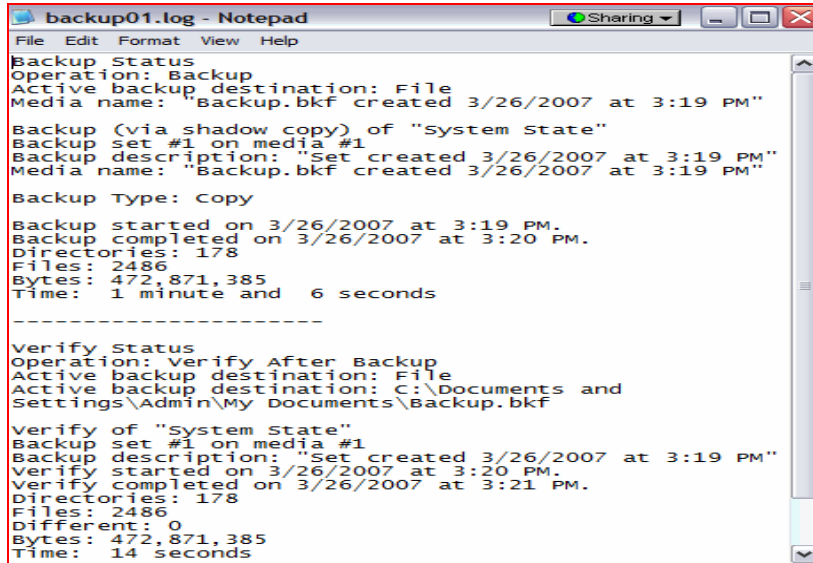
Figure 29. Backup Progress Window

✓ The "Backup Progress" window indicates that the backup is complete.

Step 15
✓ Click **Report**.
✓ The Notepad application window appears containing the report.

Figure30. Notepad Application Window

✓ Close Notepad.
✓ In the Backup Progress dialog box, click **Close**.
✓ Close the Backup Utility.

Step 16

✓ Click **Start >Run.**
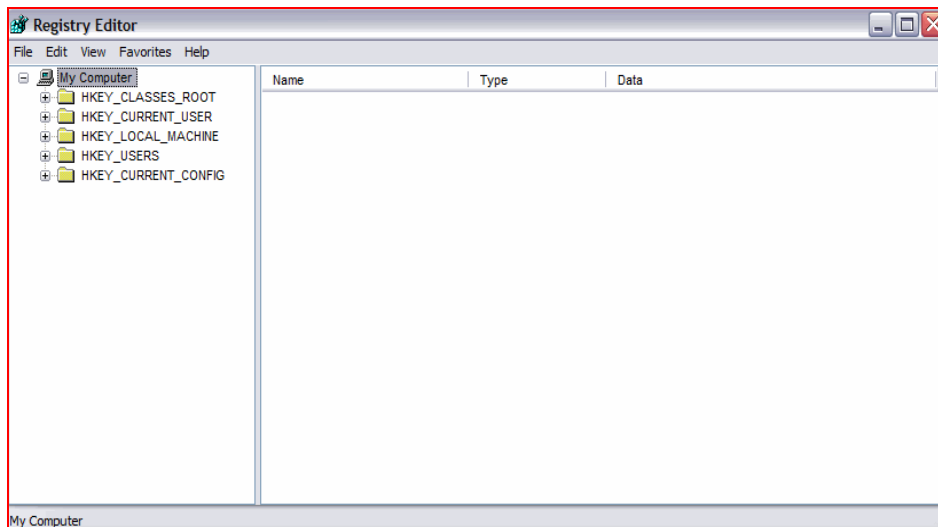✓ Type **regedit** in the "open" field. The Registry Editor window appears.

Figure 31. RegEdit Window

Step 17
- ✓ Expand the **HKEY_CURRENT_USER** Registry Key.
- ✓ Expand the **Control Panel** Registry Key.
- ✓ Expand the **PowerCfg** Registry Key.
- ✓ Right-Click the **Screen Saver. Stars** Registry Key.
- ✓ Click **Delete.**
- ✓ Click **File > Exit** in the Registry Editor window.
- ✓ Browse to the "My Documents" folder and locate the "backup.bkf" file.
- ✓ Double-click the backup file to bring up the Backup Utility Wizard.
- ✓ Click **Next**.

Step 18
- ✓ Click the **Restore files and settings** radio button and then click **Next**.
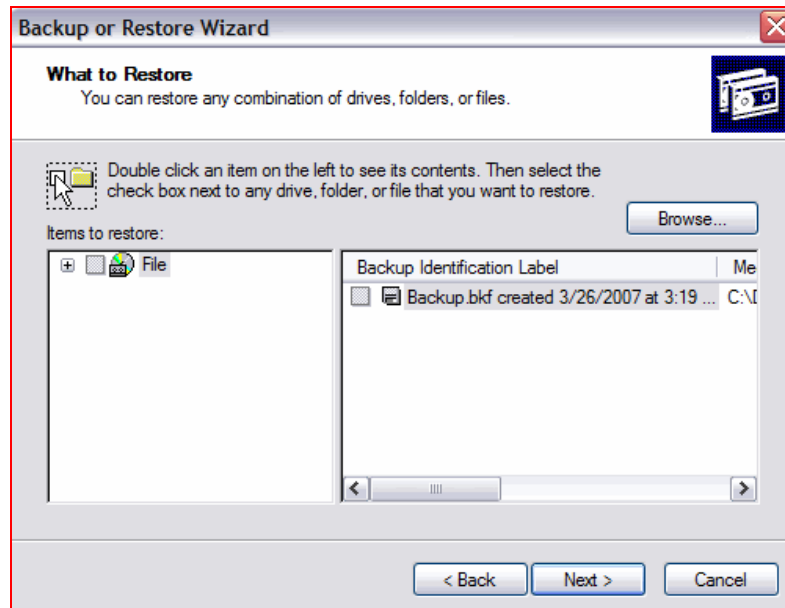- ✓ The "What to Restore" window appears.

Figure 32. What to Restore Window

Step 19
- ✓ Expand the file.
- ✓ Expand the backup.bkf file.
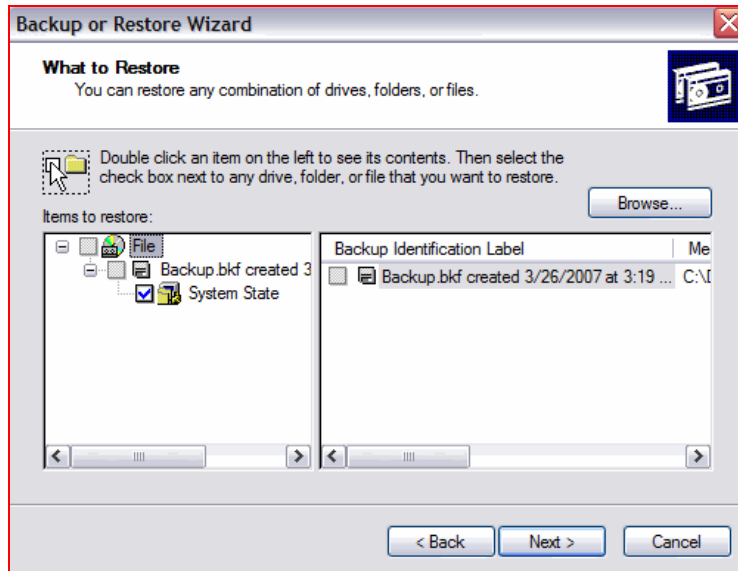- ✓ Click the **System State** check box.

Figure 33. Click System State Check box

Step 20
- ✓ Click **Next**.
- ✓ The "Completing the Backup or Restore Wizard" window appears.
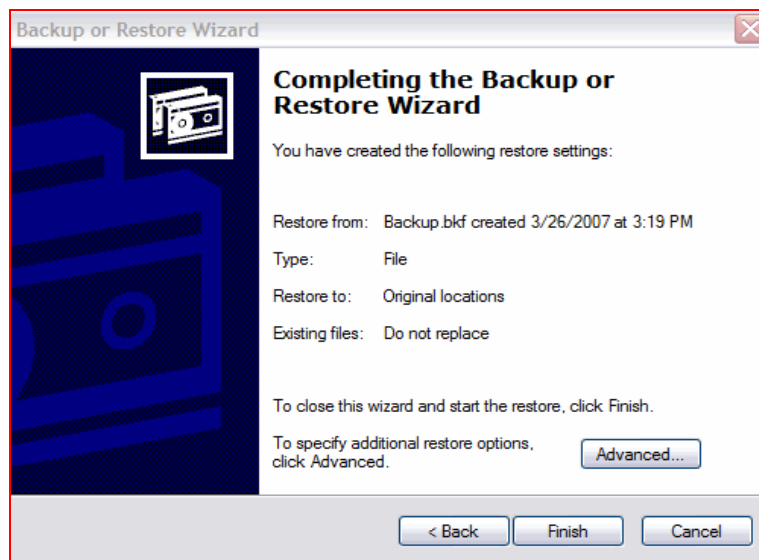

Figure 34. Completing the Backup or Restore Wizard Window

Step 21
- ✓ Click **Advanced**.
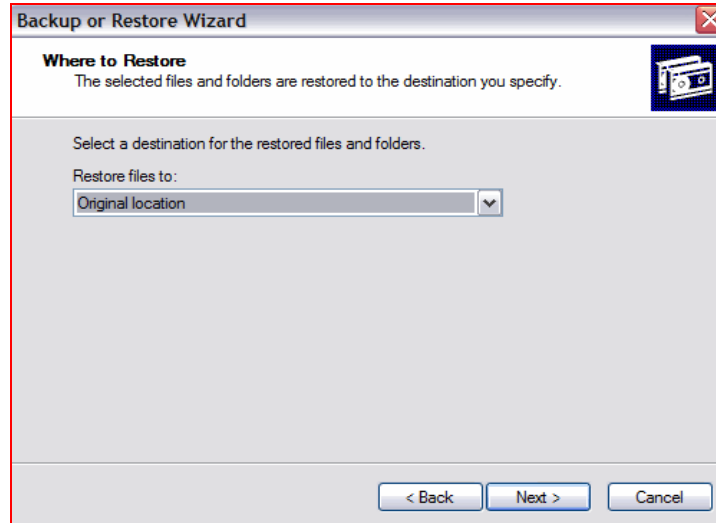- ✓ The "Where to Restore" window appears.

Figure 35. Where to Restore Window

Step 22
- ✓ The default restoration location is "Original location".
- ✓ Click **Next**.
- ✓ The "Restoring System State will always overwrite current System State unless restoring to an alternate location." Warning window appears.
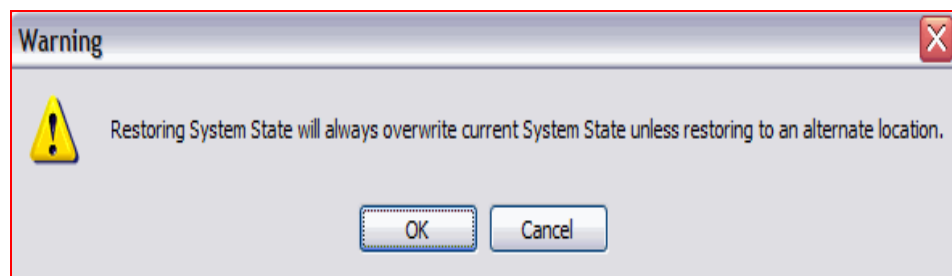- ✓ Click **OK**.

Figure 36. "Restoring System State will always overwrite current System State unless restoring to an alternate location" Warning Window

Step 23
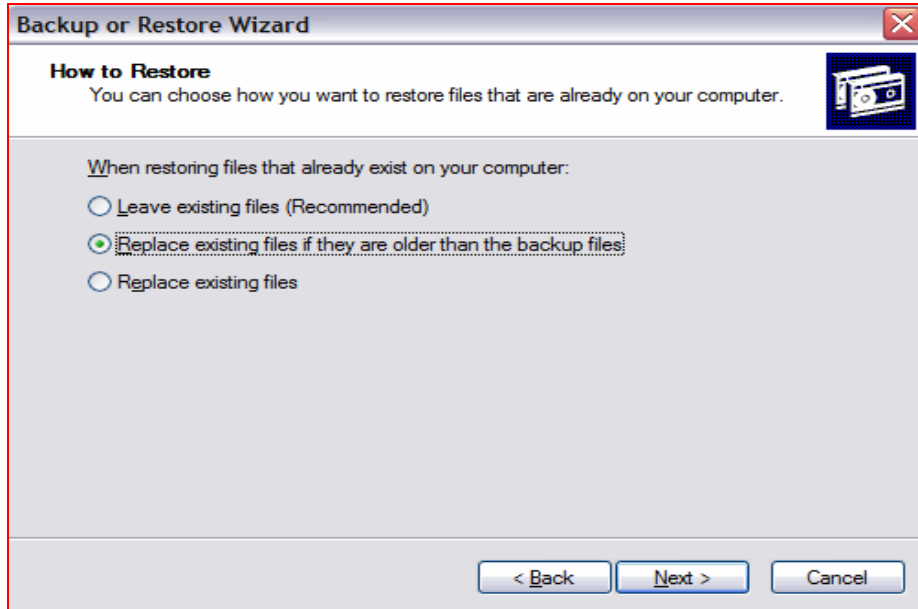- ✓ Click the **Replace existing files if they are older than the backup files** radio button.

Figure 37. How to Restore Window

Step 24
- ✓ Click **Next**.
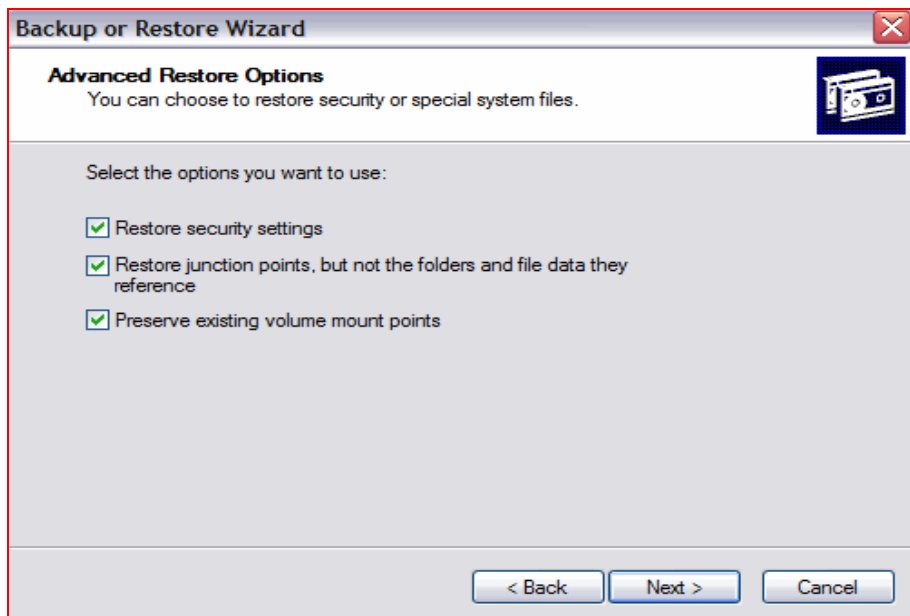- ✓ The "Advanced Restore Options" window appears

Figure 38. Advanced Restore Options Window

- ✓ Be sure that all three check boxes are selected, and then click **Next**.
- ✓ Click **Finish**.
- ✓ The system recovery begins by copying the files back to the computer.
- ✓ When prompted to restart the computer, click **Yes**. The computer will restart.

Step 25
- ✓ Click **start > Run.**
- ✓ Type **regedit** in the "Open" field.
- ✓ Click **OK**.
- ✓ You should see the "Screen Saver Stars" Registry key in the Registry Editor application window.
- ✓ Click **File > Exit**.

Finish

Performance Rubrics for
Windows Registry Backup and Recovery

CRITERIA	Excellent 4	Good 3	Fair 2	Poor 1
Safety Procedures (15%) -Applied / manifested safety precautions while working				
Adherence to the Procedures (30%) **-**Followed the procedures systematically				
Workmanship (15%) **-**Utilized organized materials and tools while accomplishing the task and exhibited time management				
Quality of work (40%) **-**the windows registry was fully backed up				

Computer Hardware Servicing

After dealing with the preparations for configuration, you can now proceed with the next section of this module which is Configuring Computer System and Network.

This lesson is designed to give you the proper procedures used in configuring computer systems and networks. At the end of this lesson you should be able to:

- ✓ Inspect networking devices and connectors;
- ✓ Create a cross-over and straight-through Ethernet cables;
- ✓ Assign and configure IP address to clients and servers;
- ✓ Create a peer-to-peer network;
- ✓ Enable network security; and
- ✓ Configure file and printer sharing.

Lesson 2. Configure Computer System and Network

System Configuration is the way a system is set up, it is the collection of components that make up the system. Configuration can refer to either hardware or software, or the combination of both. For instance, a typical configuration for a PC consists of 32MB (megabytes) main memory, a floppy drive, a hard disk, a modem, a CD-ROM drive, a VGA monitor, and the Windows Operating System.

Many software products require that the computer has a certain *minimum configuration.* For example, the software might require a graphics display monitor and a video adapter, a particular microprocessor, and a minimum amount of main memory capacity.

When you install a new device or program, you sometimes need to configure it, which means that you need to set various switches and jumpers (for hardware) and to define values of parameters (for software). For example, the device or program may need to know what type of video adapter you have and what type of printer is connected to the computer. Thanks to technological advancements, such as plug-and-play, much of this configuration is now performed automatically.

Safety Precautions Related to Networks

Installing network cables, whether copper or fiber-optic, can be dangerous. Often, cables must be pulled through ceilings and walls where there are obstacles or toxic materials. You should wear clothing such as long pants, a long-sleeved shirt, sturdy shoes that cover your feet, and gloves to protect you from those toxic materials. Most importantly, wear safety glasses. If possible, ask building management, or someone responsible for the building, if there are any dangerous materials or obstacles that you need to be aware of before entering the ceiling area.

Safety precautions when using a ladder:
- Read the labels on the ladder, and follow any safety instructions written on it.
- Never stand on the top rung of the ladder. You could easily lose your balance and fall.
- Make sure that people in the area know you will be working there.
- Cordon off the area with caution tape or safety cones.
- When you are using a ladder that leans up against a wall, follow the instructions written on the ladder, and have someone hold the ladder to help keep it steady.

Safety rules when working with cables:
The tools required to install copper and fiber-optic cable may cause danger through improper use. When working with cables, strictly follow these safety rules:
- Make sure that the tools you are using are in good working condition.
- Watch what you are doing, and take your time. Make sure that you do not cut yourself or place anyone in danger.
- Always wear safety glasses when cutting, stripping, or splicing cables of any kind. Tiny fragments can injure your eyes.
- Wear gloves whenever possible, and dispose any waste properly.

Use common sense when installing cables and fixing network problems. Call for assistance for tasks that you cannot do on your own.

Fiber-Optic Safety

Fiber-optic cables are useful for communications, but they have certain hazards:

- Dangerous chemicals
- Tools with sharp edges
- Light which you cannot see that can burn your eyes
- Glass shards produced by cutting fiber-optic cable that can cause bodily harm

Specific types of tools and chemicals are used when working with fiber-optic cable. These materials must be handled with care.

Chemicals

The solvents and glues used with fiber optics are dangerous. You should handle them with extreme care. Read the instructions on the label, and follow them carefully. Also, read the material safety data sheet (MSDS) that accompanies the chemicals to know how to treat someone in case of emergency.

Tools

When working with any tool, safety should always be your first priority. Any compromise in safety could result in serious injury or even death. The tools used for working with fiber optics have sharp cutting surfaces that are used to scribe glass. Other tools pinch cables with high pressure to fasten connectors to them. These tools can produce shards of glass that can splinter and fly into the air. You must avoid getting them on your skin and in your mouth or eyes.

Glass Shards

The process of cutting and trimming the strands of fiber-optic cables can produce tiny fragments of glass or plastic that can penetrate your eyes or skin and cause severe irritation. The fibers can be extremely difficult to see on your skin because they are clear and small. When you work with fiber-optic cabling, the working surface should be a dark mat so that you can see the tiny glass or plastic fragments. The mat should also be resistant to chemical spills.

You should keep the work area clean and neat. Never pick up fiber-optic fragments with your fingers. Use tape to pick up small fragments, and dispose them off properly. Use a disposable container, such as a plastic bottle with a screw-on lid, to store fiber fragments. Close the lid tightly before disposing the container.

Harmful Light

Protect your eyes from the harmful light that may be in the fiber-optic strands. The light is a color that humans cannot see. It can damage your eyes before you can feel it. When you use a magnifier to inspect fiber-optic cable and connectors, the light emitted from the fiber could be directed into your eyes. When working with fiber, be sure to disconnect the light source. Use special detectors to help you tell if a fiber is energized.

Caution:

Obtain proper training before you attempt to cut, strip, or splice fiber-optic cable. An experienced technician should supervise you until you become adequately skilled.

•What to KNOW

Networking Devices, Media and Connector

To make data transmission more extensible and efficient than a simple peer-to-peer network, network designers use specialized network devices such as hubs, switches, routers, and wireless access points to send data between devices. You have already discussed in your Grade 9 CHS class the different devices used in networking and which provides you the knowledge on the common networking cables that are essential in putting up a network.

Common Network Cables

Until recently, cables were the only medium used to connect devices on networks. A wide variety of networking cables are available. Coaxial and twisted-pair cables use copper to transmit data. Fiber-optic cables use glass or plastic to transmit data. These cables differ in bandwidth, size, and cost. You need to know what type of cable to use based on the job requirements. You also need to be able to troubleshoot and repair problems along the way.

Twisted Pair

Twisted pair is a type of copper cabling that is used for telephone communications and most Ethernet networks. A pair of wires forms a circuit that transmits data. The pair is twisted to provide protection against *crosstalk*, the noise generated by adjacent pairs of wires in the cable. Pairs of copper wires are encased in color-coded plastic insulation and are twisted together. An outer jacket protects the bundles of twisted pairs.

Figure 39. UTP and STP Cable

When electricity flows through a copper wire, a magnetic field is created around the wire. A circuit has two wires, and in a circuit, the two wires have oppositely-charged magnetic fields. When the two wires of the circuit are next to each other, the magnetic fields cancel each other out. This is called the cancellation effect. Without the cancellation effect, your network communications become slow because of the interference caused by the magnetic fields.

The two basic types of twisted-pair cables are as follows:
- *Unshielded twisted pair (UTP)* is the cable that has two or four pairs of wires. This type of cable relies solely on the cancellation effect produced by the twisted-wire pairs that limits signal degradation caused by electromagnetic interface (EMI) and radio frequency interference (RFI). UTP is the most commonly used cabling in networks. UTP cables have a range of 328 feet (100 m).
- With *shielded twisted pair (STP)*, each pair of wire is wrapped in metallic foil to better shield the wires from noise. Four pairs of wires are then wrapped in an overall metallic braid or foil. STP reduces electrical noise from within the cable. It also reduces EMI and RFI from

outside the cable. Although STP prevents interference better than UTP, STP is more expensive because of the extra shielding. It is also more difficult to install because of the thickness. In addition, the metallic shielding must be grounded at both ends. If it is improperly grounded, the shield acts like an antenna, picking up unwanted signals.

Category Rating

UTP comes in several categories that are based on two factors:
- The number of wires in the cable
- The number of twists in those wires

1. Category 3 is the wiring used for telephone systems and Ethernet LAN at 10 Mega byte per second (Mbps).
2. Category 3 has four pairs of wires.
3. Category 5 and Category 5e have four pairs of wires with a transmission rate of 100 Mbps.
4. Category 5 and Category 5e is the most common network cables used.
5. Category 5e has more twists per foot than Category 5 wiring.

These extra twists further prevent interference from outside sources and from the other wires within the cable.

Some Category 6 cables use a plastic divider to separate the pairs of wires, which prevents interference. The pairs also have more twists than Category 5e cable.

Coaxial Cable

Coaxial cable is a copper-cored cable surrounded by a heavy shielding. Coaxial cable is used to connect the computers to the rest of the network.

Source: www.phoneam.com
Figure 40. Coaxial Cable

Coaxial cable uses "British Naval Connectors (BNC)" or "Bayonet Neill-Concelman" connectors, at the ends of the cables to make the connection. Several types of coaxial cable exist:

- **Thicknet (10BASE5)** is a coaxial cable used in networks operating at 10 Mbps, with a maximum length of 500 meters.
- **Thinnet (10BASE2)** is a coaxial cable used in networks operating at 10 Mbps, with a maximum length of 185 meters.
- **RG-59** is most commonly used for cable television in the U.S.
- **RG-6** is higher-quality cable than RG-59, with more bandwidth and less susceptibility to interference.

Fiber-Optic Cable

An optical fiber is a glass or plastic conductor that transmits information using light. **Fiber optic cable** has one or more optical fibers enclosed in a sheath or jacket. Because it is made of glass, fiber-optic cable is not affected by EMI or RFI. All signals are converted to light pulses to enter the cable and are converted back into electrical signals when they leave it. This means that fiber-optic cable can deliver signals that are clearer, and can go farther, without compromising the clarity of signals.
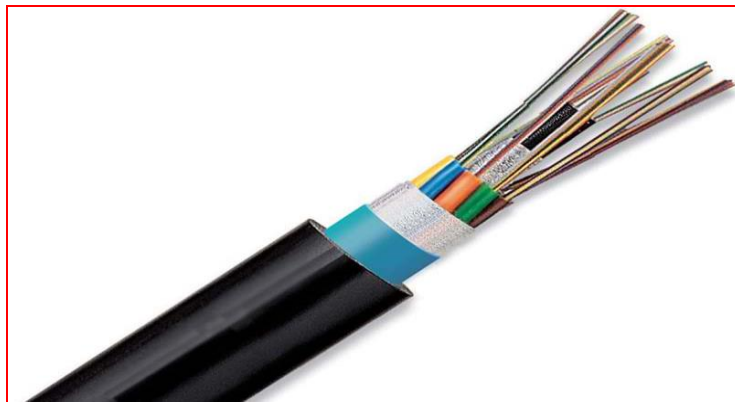
Source: www.picstopin.com
Figure 41. Fiber Optic Cable

Fiber-optic cable can reach distances of several miles or kilometers before the signal needs to be regenerated. Fiber-optic cable usually is more expensive to use than copper cable, and the connectors are more costly and harder to assemble. Common connectors for fiber-optic networks are SC, ST, and LC. These three types of fiber-optic connectors are half-duplex, which allows data to flow in only one direction. Therefore, two cables are needed.

These are the two types of glass fiber-optic cable:

- *Multimode* is the cable that has a thicker core than single-mode cable. It is easier to make, can use simpler light sources such as Light Emitting Diodes (LEDs), and works well over distances of a few kilometers or less.
- *Single-mode* is the cable that has a very thin core. It is harder to make, uses lasers as a light source, and can transmit signals dozens of kilometers with ease.

Creating Ethernet Cable

Ethernet cabling has been the standard in networking installation for years. It is the fastest way of connecting PC to a peer or to your router or a central switch. This section of the module will bring you back to the procedures in creating an Ethernet cable specifically straight-through and cross-over. Try to recall the procedures as you go on with the lesson.

Fabricating an Ethernet Cross-over and Straight-through Cable

In an Ethernet networking environment – like in a home or an office with multiple PCs that are wired – the computers need to be connected to a central router to allow data transfer. The router takes all the bits being sent out by the computers and relays them onto the other devices on the network.

The *straight-through* Ethernet cable is used in local area network to connect a PC to a network hub and router. This is the standard cable used for almost all purposes.

A *cross-over cable,* on the other hand, can be used to connect two network devices directly, without the need for a router in the middle. It simply reverses some of the pins so that the output on one computer is being sent to the input of another.

Bear in mind that safety precautions must always be applied and observed during the fabrication of the said cables. Also, materials and tools to be used must always be complete and functional to save time, money and effort.

The following items are the materials and tools used for making Ethernet cables:

- ✓ Ethernet Cable Category 5e or Cat5e- standard wire for cabling;
- ✓ RJ45 crimpable connectors for Cat5e;
- ✓ RJ45 Crimping tool;
- ✓ Wire cutter, stripper or pliers; and
- ✓ Ethernet cable tester.

Cable Fabrication Procedures

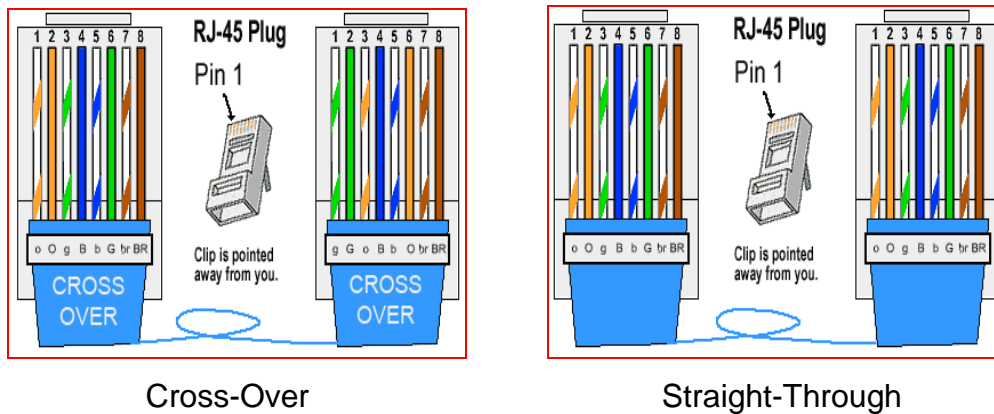Cross-Over   Straight-Through

Figure 42. Cross-Over and Straight-Through Color Coding

The picture below will serve as your guide in making the two important Ethernet cables.

1. Cut into the plastic sheath **1 inch** from the end of the cut cable. The crimping tool has a razor blade that will do the trick with practice.
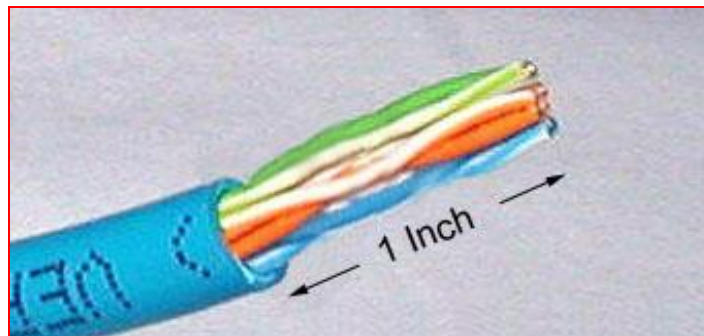
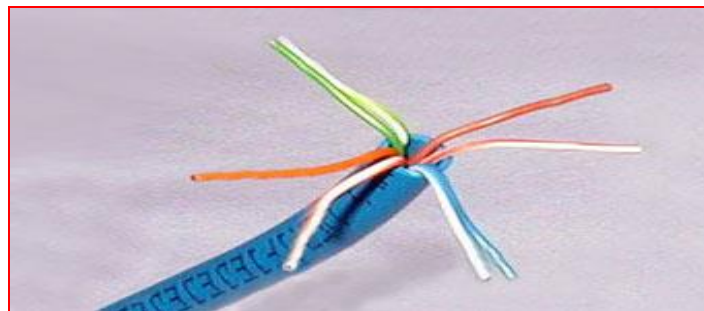

Figure 43. Step 1

2. Unwind and pair the similar colors.

Figure 44. Step 2

Computer Hardware Servicing

3. Pinch the wires between your fingers and straighten them out as shown. The color order is important to do this correctly.

Figure 45. Step 3

4. Use wire cutter to make a straight cut across the wires **1/2 inch** from the cut sleeve to the end of the wires.
5. Push the wires into the connector. Each wire fits into a slot in the RJ45 connector. Note the position of the blue plastic shielding. Also note how the wires go all the way to the end.

Figure 46. Step 5

6. Take view from the top. Make sure the wires are all the way in. There should be no short wires.

Figure 47. Step 6

7. Crimping the Cable – carefully place the connector into the Ethernet Crimper and cinch down on the handles tightly. The copper splicing tabs on the connector will pierce into each of the eight wires. There is also a locking tab that holds the blue plastic sleeve in place for a tight compression fit. When you remove the cable from the crimper, that end is ready to use.

Figure 48. Step 7

8. For a standard "Straight-Through" cable, repeat all steps and wire color order on the other end of cable. For a cross-over cable - the other end will have a different color order as shown by the crossover picture on page 84.

9. Make sure to test the cables before installing them. An inexpensive Ethernet cable tester does this quite well.

Figure 49. Step 9

Criss-Cross Puzzle

Directions: Complete the criss-cross puzzle and familiarize yourself of the cables being described. Write your answer in a clean sheet of paper.

CABLES
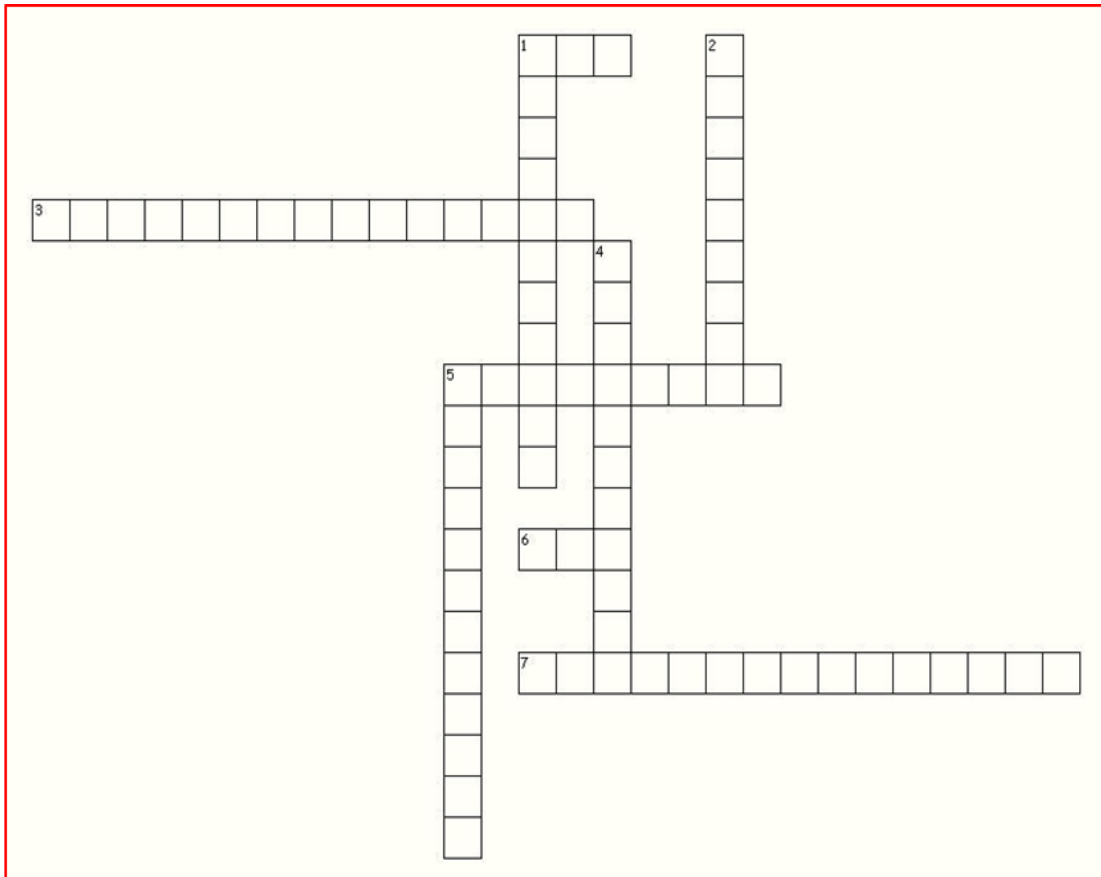
Across
1. each pair of wires is wrapped in metallic foil
3. one or more optical fibers enclosed in a sheath or jacket
5. used to connect two devices directly
6. cable that has two or four pairs of wires
7. the standard cable used for almost all purposes

Down
1. cable that has a very thin core
2. cable that has a thicker core
4. used for telephone communications and Ethernet networks
5. copper-cored cable

Now that you are equipped with the knowledge on the different cables used in networking, you also need to know that fiber technologies and connectors have changed through the years. In these videos, you will learn about the different fiber connectors, copper connectors and their characteristics. To watch the video presentations just type in the following URL:

1) http://www.professormesser.com/n10-005/copper-connectors/

2)http://www.professormesser.com/n10-005/copper-connectors/

3.http://www.professormesser.com/n10-005/utp-stp-and-coaxial-cabling/

I hope you learned a lot from the video presentations. After watching the videos, answer the following guide questions and submit it to your teacher. Write your answer in a clean sheet of paper. Good Luck!
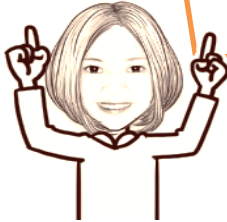
Here are the questions:

1. What are the different types of fiber connectors? Cite their advantages and disadvantages.

   _____
   _____
   _____
   _____.

2. List down the different types of connectors.

   _____
   _____
   _____
   _____

3. What are the characteristics of UTP, STP and coaxial cable?

   _____
   _____
   _____
   _____

Create your own Ethernet Cable

Directions: Prepare the following tools and materials in fabricating your own cross-over and straight-through cables.

Materials:
- ✓ 6 meters Ethernet Cable Category 5e or Cat5e-standard wire for cabling;
- ✓ RJ45 crimpable connectors for Cat5e;

Tools:
- ✓ RJ45 Crimping tool;
- ✓ Wire cutter, stripper or pliers; and
- ✓ Ethernet cable Tester / LAN Tester

Reminder / Caution: Be careful when using the tools.

Follow the procedures cited in this module and apply the safety precautions to avoid injury or any unwanted incident. You will be given 30 minutes to complete the task. You will be rated using the performance rubrics found on the next page.

Procedures:
1. Cut into the plastic sheath **1 inch** from the end of the cut cable. The crimping tool has a razor blade that will do the trick with practice.
2. Unwind and pair the similar colors.
3. Pinch the wires between your fingers and straighten them out as shown on page 90. The color order is important to do this correctly.
4. Use scissors to make a straight cut across the wires **1/2 inch** from the cut sleeve to the end of the wires.
5. Push the wires into the connector. Note the position of the blue plastic shielding. Also note how the wires go all the way to the end.
6. Take view from the top. Make sure the wires are all the way in. There should be no short wires.
7. In crimping the cable – carefully place the connector into the Ethernet Crimper and cinch down on the handles tightly. The copper splicing tabs on the connector will pierce into each of the eight wires. There is also a locking tab that holds the blue plastic sleeve in place for a tight compression fit. When you remove the cable from the crimper, that end is ready to use.

8. For a standard straight-through cable, repeat all steps and wire color order on the other end of cable. For a cross-over cable, the other end will have a different color order as shown in the cross-over picture on page 89.
9. Make sure to test the cables before installing them. An inexpensive Ethernet cable tester does this quite well.

Performance Rubrics for
Creating a Cross-Over and Straight-Through Ethernet Cables

CRITERIA	Excellent 4	Good 3	Fair 2	Poor 1
Safety Procedures (15%) -Applied / manifested safety precautions while working				
Adherence to the Procedures (30%) -Followed the procedures systematically				
Workmanship (15%) -Organized materials and tools while accomplishing the task and has time management				
Quality of Product (40%) -Produced a fully functional Ethernet Cable				

Internet Protocols

A protocol is a set of rules. A letter sent through the postal system also uses protocols. Part of the protocol specifies where on the envelope the delivery address needs to be written. If the delivery address is written in the wrong place, the letter cannot be delivered. Internet protocol works in a similar way. Internet protocols are sets of rules governing communication within and between computers on a network. Protocol specifications define the format of the messages to be exchanged.

Timing is crucial to network operation. Protocols require messages to arrive within a certain amount of time so that computers do not wait indefinitely for messages that may have been lost. Therefore, systems maintain one or more times during transmission of data. Protocols also initiate alternative actions if the network does not meet the timing rules. Many protocols consist of a suite of other protocols that are stacked in layers. These layers depend on the operation of the other layers in the suite to function properly.

The main functions of protocols are:
- Identifying errors
- Compressing the data
- Deciding how the data should be sent
- Addressing the data
- Deciding how to announce sent and received data

To understand how networks and the Internet work, you must be familiar with the commonly used protocols. These protocols are used to browse the web, send and receive e-mail, and transfer data files. You will encounter other protocols as your experience in IT grows, but they are not used as often as the common protocols described here:
- **TCP/IP:** The Transmission Control Protocol /Internet Protocol (TCP/IP) suite of protocols has become the dominant standard for internetworking. TCP/IP represents a set of public standards that specify how packets of information are exchanged between computers over one or more networks.

- **IPX/SPX:** Internetwork Packet Exchange/Sequenced Packet Exchange is the protocol suite originally employed by Novell Corporation's network operating system, NetWare. It delivers functions similar to those included in TCP/IP. Novell in its current releases supports the TCP/IP suite. A large installed base of NetWare networks continues to use IPX/SPX.
- **NetBEUI:** NetBIOS Extended User Interface is a protocol used primarily on small Windows NT networks. NetBEUI cannot be routed or used by routers to talk to each other on a large network. NetBEUI is suitable for small peer-to-peer networks, involving a few computers directly connected to each other. It can be used in conjunction with another routable protocol such as TCP/IP. This gives the network administrator the advantages of the high performance of NetBEUI within the local network and the ability to communicate beyond the LAN over TCP/IP.
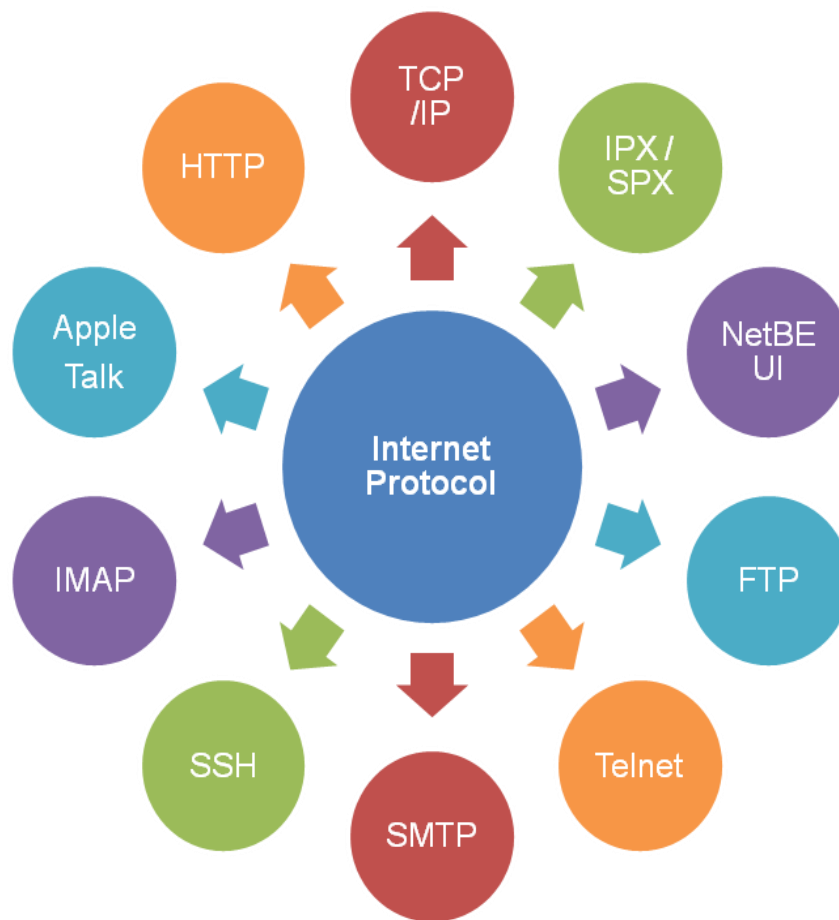
Figure 50. Commonly Used Internet Protocol

- **AppleTalk:** AppleTalk is a protocol suite used to network Macintosh computers. It is composed of a comprehensive set of protocols that span the seven layers of the Open Systems Interconnection (OSI) reference model. The AppleTalk protocol was designed to run over LocalTalk, which is the Apple LAN physical topology. This protocol is also designed to run over major LAN types, notably Ethernet and Token Ring.
- **HTTP:** Hypertext Transfer Protocol governs how files such as text, graphics, sound, and video are exchanged on the World Wide Web (WWW). The Internet Engineering Task Force (IETF) developed the standards for HTTP.
- **FTP:** File Transfer Protocol provides services for file transfer and manipulation. FTP allows multiple simultaneous connections to remote file systems.
- **SSH:** Secure Shell is used to securely connect to a remote computer.
- **Telnet:** It is an application used to connect to a remote computer that lacks security features.
- **POP3:** Post Office Protocol is used to download e-mail from a remote mail server.
- **IMAP:** Internet Message Access Protocol is also used to download e-mail from a remote mail server.
- **SMTP:** Simple Mail Transfer Protocol is used to send e-mail to a remote e-mail server.

The more you understand about each of these protocols, the more you will understand how networks and the Internet work.

IP Addressing

An *IP address* is a number that is used to identify a device on the network. Each device on a network must have a unique IP address to communicate with other network devices. Network devices are those that move data across the network, including hubs, switches, and routers. On a LAN, each host (device that sends or receives information on the network) and network device must have an IP address within the same network to be able to communicate with each other.

A person's name and fingerprints usually do not change. They provide a label or address for the person's physical aspect—the body. A person's mailing address, on the other hand, relates to where the person lives or picks up mail. This address can change. On a host, the Media Access Control

(MAC) address is assigned to the host Network Interface Card (NIC) and is known as the physical address. The physical address remains the same regardless of where the host is placed on the network in the same way that fingerprints remain with someone regardless of where he or she goes.

An IP address consists of a series of 32 binary bits (1s and 0s). It is very difficult for humans to read a binary IP address. For this reason, the 32 bits are grouped into four 8-bit bytes called octets. An IP address, even in this grouped format, is hard for humans to read, write, and remember. Therefore, each octet is presented as its decimal value, separated by a decimal point or period. This format is called dotted-decimal notation. When a host is configured with an IP address, it is entered as a dotted-decimal number, such as 192.168.1.5.

Imagine if you had to enter the 32-bit binary equivalent of this: 11000000101010000000000100000101. If you mistyped just 1 bit, the address would be different, and the host may not be able to communicate on the network. The logical 32-bit IP address is hierarchical and is composed of two parts. The first part identifies the *network*, and the second part identifies a *host* on that network. Both parts are required in an IP address. For example, if a host has an IP address of 192.168.18.57, the first three octets, 192.168.18, identify the network portion of the address, and the last octet, 57, identifies the host. This is called *hierarchical addressing*, because the network portion indicates the network on which each unique host address is located. Routers only need to know how to reach each network, not the location of each individual host.

Table 6. Five Classes of IP Address

IP Classes	Purpose
Class A	Used for large networks, implemented by large companies and some countries
Class B	Used for medium-sized networks, implemented by universities
Class C	Used for small networks, implemented by ISPs for customer subscriptions
Class D	Used for special use for multicasting
Class E	Used for experimental testing

Subnet Mask

The *subnet mask* indicates the network portion of an IP address. Like the IP address, the subnet mask is a dotted-decimal number. Usually all hosts within a LAN use the same subnet mask. Table 3 shows default subnet masks for usable IP addresses that are mapped to the first three classes of IP addresses:

- **255.0.0.0:** Class A, which indicates that the first octet of the IP address is the network portion
- **255.255.0.0:** Class B, which indicates that the first two octets of the IP address are the network portion
- **255.255.255.0:** Class C, which indicates that the first three octets of the IP address are the network portion

Table 7. Default Subnet Masks for Usable IP Addresses

Class A	Network	Host		
Octet	1	2	3	4

Class B	Network		Host	
Octet	1	2	3	4

Class C	Network			Host
Octet	1	2	3	4

Class D addresses are used for multicast groups. There is no need to allocate octet or bits to separate network and host addresses. Class E addresses are reserved for research use only.

IpConfig

Ipconfig is a command used to find out the IP address of a certain network you are connected to.

How to use the ipconfig command?
1) Click on Start Button, then type cmd (command prompt) on the search box.
2) A black screen will appear as shown in the figure below.
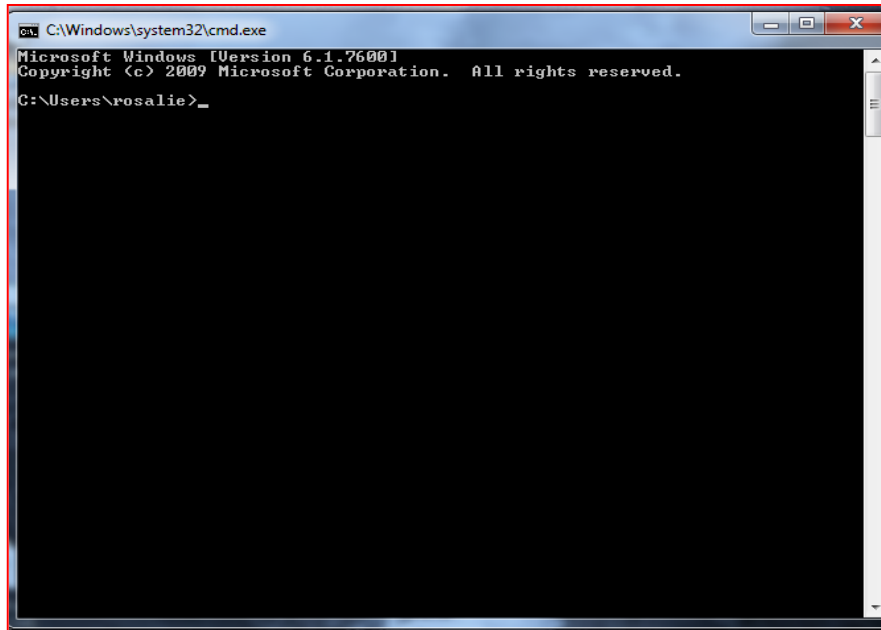
Figure 51. Command Prompt Window

3) Type ipconfig and press enter. The figure below shows the IP configuration window using the ipconfig command. The information from this window will be useful because it shows the IP address, subnet mask and default gateway of a network you are connected to.
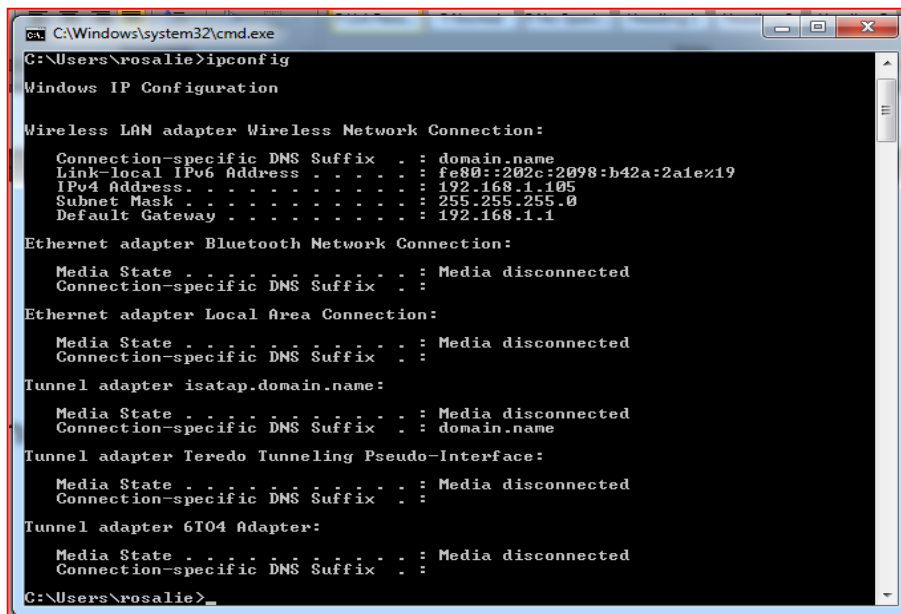
Figure 52. IP Configuration in CMD Window

Assigning a static IP Address

In a home network with several computers and devices, it is ideal to assign each of them a specific address. This is for the purpose of avoiding problems when you do troubleshooting which requires figuring out the IP address of each of them. It is also a means to prevent address conflicts between the devices. You can also manage them with ease if you have assigned their own addresses.

Here are the procedures in assigning an IP Address on a windows base computer system:

1. Open the Control Panel's Network Connections icon.

2. Open the icon representing your computer's network connection.

3. Click the Properties button in the Status dialog box.

4. From the list of items, choose Internet Protocol (TCP/IP).
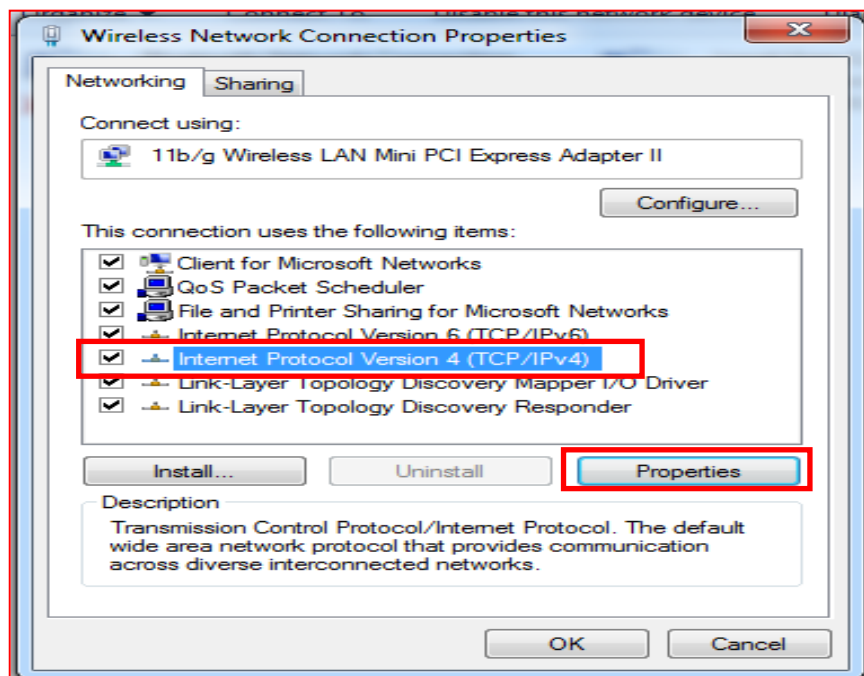
Figure 53. Wireless Network Connections Properties Dialog Box

5. Click the Properties button. The Internet Protocol (TCP/IP) Properties dialog box appears.
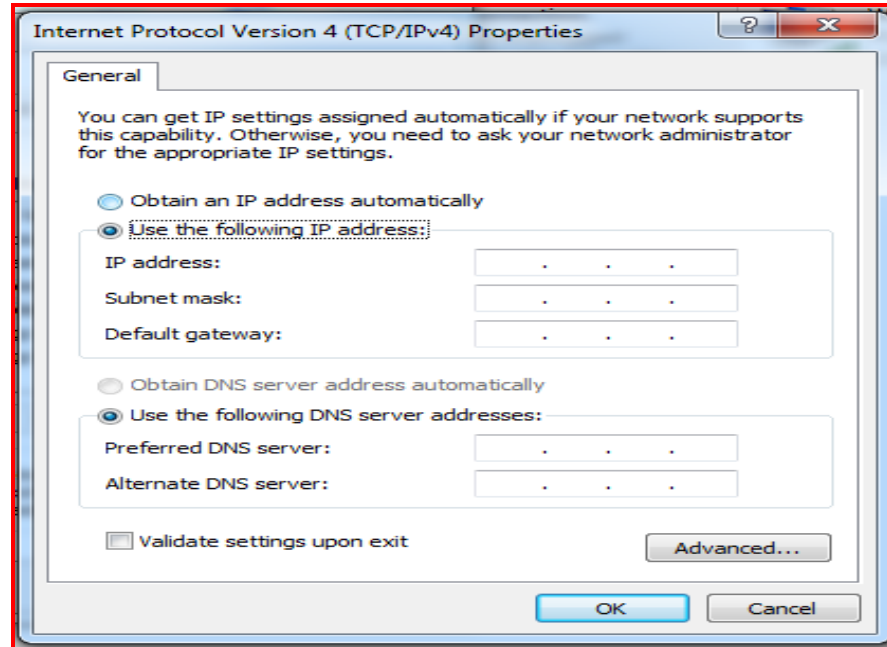
Figure 54. TCP / IPV4 Dialog Box

6. Type the IP address for your computer. Enter the appropriate IP Address in the IP address section.
7. Type a subnet mask. The value used on a local network is commonly 255.255.255.0, but it can be different, such as 255.255.255.127.
8. Type the default gateway address. The default gateway is the router, so type the router's address. Figure 54 shows an example of assigning an IP Address, Subnet mask and default gateway.
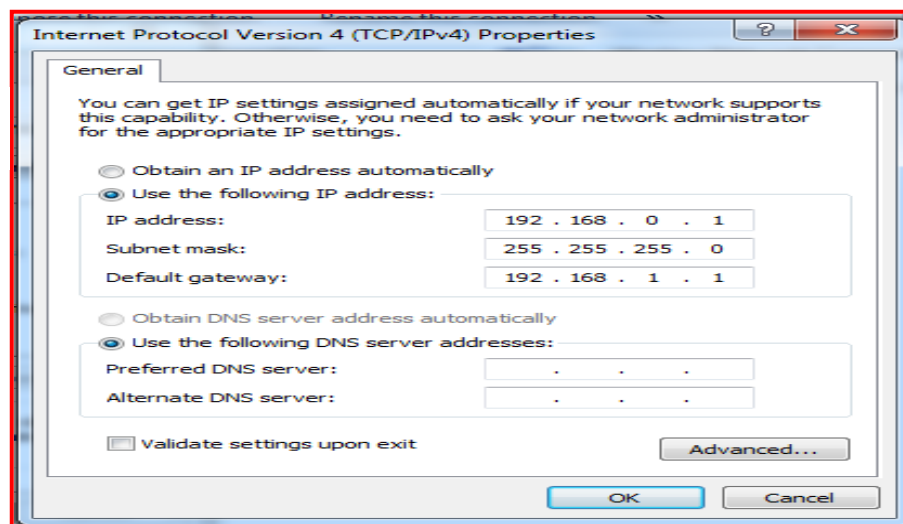
Figure 55. Assigning an IP Address

Computer Hardware Servicing

9. Type the address for the preferred **DNS server.** The address should be obtained from your Internet Service Protocol. It is used to help your computer find web pages and other addresses on the internet.
10. Type the address for the alternate DNS server.
    The alternate Domain Name System (DNS) server's IP address is something that your ISP provides.
11. Click OK to confirm the settings.
12. Close all other open dialog boxes and windows.

Assigning a Dynamic IP Address
   If more than a few computers comprise the LAN, manually configuring IP addresses for every host on the network can be time-consuming and prone to errors. In this case, using a Dynamic Host Configuration Protocol (DHCP) server would automatically assign IP addresses and greatly simplify the addressing process.
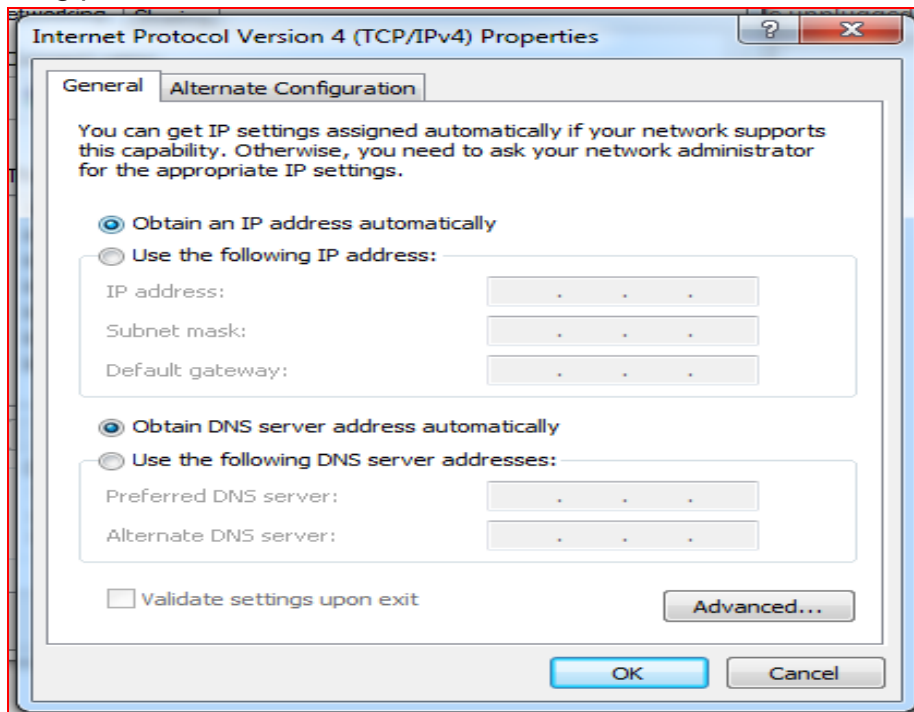
Figure 56. Assigning a Dynamic IP Address

   Dynamic Host Configuration Protocol (DHCP) is a software utility used to dynamically assign IP addresses to network devices. This dynamic process eliminates the need to manually assign IP addresses. A DHCP server can be set up and the hosts can be configured to automatically obtain

an IP address. When a computer is set to obtain an IP address automatically, the other entire IP addressing configuration boxes are dimmed or disabled. The server maintains a list of IP addresses to assign, and it manages the process so that every device on the network receives a unique IP address. Each address is held for a predetermined amount of time. When the time expires, the DHCP server can use this address for any computer that joins the network.

These are the IP address information that a DHCP server can assign to hosts:

- IP address
- Subnet mask
- Default gateway
- Optional values, such as a Domain Name System (DNS) *server* address

The DHCP server receives a request from a host. The server then selects IP address information from a set of predefined addresses that are stored in a database. After the IP address information is selected, the DHCP server offers these values to the requesting host on the network. If the host accepts the offer, the DHCP server leases the IP address for a specific period of time.

Using a DHCP server simplifies the administration of a network because the software keeps track of IP addresses. Automatically configuring TCP/IP also reduces the possibility of assigning duplicate or invalid IP addresses. Before a computer on the network can take advantage of the DHCP server services, the computer must be able to identify the server on the local network. You can configure a computer to accept an IP address from a DHCP server by clicking the *Obtain an IP address automatically* option in the NIC configuration window, as shown in Figure 56.

If your computer cannot communicate with the DHCP server to obtain an IP address, the Windows operating system automatically assigns a private IP address. If your computer is assigned an IP address in the range of 169.254.0.0 to 169.254.255.255, it can communicate with only other computers in the same range. An example of when these private addresses would be useful is in a classroom lab where you want to prevent access outside to your network. This operating system feature is called Automatic Private IP Addressing (APIPA). APIPA continually requests an IP address from a DHCP server for your computer.

Computer Hardware Servicing

Ping

The ping is a Command Prompt command used to test the ability of the source computer to reach a specified destination computer. The ping command is usually used as a simple way to verify that a computer can communicate over the network with another computer or network device.

The ping command operates by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination computer and waiting for a response. How many of those responses are returned, and how long it takes for them to return, are the two major pieces of information that the ping command provides.

Table 8. Ping Command Syntax

Syntax	Description
-t	Using this option will ping the *target* until you force it to stop using Ctrl-C.
-a -	This ping command option will resolve, if possible, the hostname of an IP address *target*.
-n *count*	This option sets the number of ICMP Echo Request messages to send. If you execute the ping command without this option, four requests will be sent.
-l *size*	Use this option to set the size, in bytes, of the echo request packet from 32 to 65,527. The ping command will send a 32 byte echo request if you do not use the **-l** option.
-f	Use this ping command option to prevent ICMP Echo Requests from being fragmented by routers between you and the *target*. The **-f** option is most often used to troubleshoot Path Maximum Transmission Unit (PMTU) issues.
-i *TTL*	This option sets the Time to Live (TTL) value, the maximum of which is 255.
-v *TOS*	This option allows you to set a Type of Service (TOS) value. Beginning in Windows 7, this option no longer functions but still exists for compatibility reasons.
-r *count*	Use this ping command option to specify the number of hops between the computer and the *target* computer or device that you would like to be recorded and displayed. The maximum value for *count* is 9 so use the tracert command instead. If you are interested in viewing all hops between two devices.
-s *count*	Use this option to report the time, in Internet Timestamp format, that each echo request is received and echo reply is sent. The maximum value for *count* is 4 which means that only

	the first four hops can be time stamped.
-w *timeout*	Specifying a *timeout* value when executing the ping command adjusts the amount of time, in milliseconds, that ping waits for each reply. If you do not use the **-w** option, the default timeout value is used which is 4000, or 4 seconds.
-R	This option tells the ping command to trace the round trip path.
-S *srcaddr*	Use this option to specify the source address.
-4	This forces the ping command to use IPv4 only but is only necessary if *target* is a hostname and not an IP address.
-6	This forces the ping command to use IPv6 only but as with the **-4** option, is only necessary when pinging a hostname.
target	This is the destination you wish to ping, which is either an IP address or a hostname.
/?	Use the help switch with the ping command to show detailed help about the command's several options.

Using the ping Command

Ping is one of your most important tools in troubleshooting Internet problems. It shows you whether the Domain Name Server is working, whether the computer you are trying to talk to is reachable, and how long it takes to get there. It does this at a very low level — only the most basic Internet functions have to be up and running.

1) Click on Start Button, then type cmd (command prompt) on the search box.
2) A black screen will appear as shown in the figure below.
3) Type ping followed by the IP address you desire to verify. The figure below shows the screen of the ping command and its output.

Figure 57. Step 3

Figure 58. Pinging

This output shows several things:

✓ **Decoding names to network addresses —** A domain name server (DNS) resolves machine names to numeric addresses. A single machine can have many names, all of which resolve to the same Internet address. In the example just given, the name www.google.com resolves to the Internet address 122.2.152.23.

✓ **Round-trip response time —** The parts of the replies that say things like time=105ms show you how long it took from the time the client machine sent out the ping message until a reply came back (1 ms is 1 millisecond, or one thousandth of a second). The variability in the times

you see reflects that networks do not always respond identically. Differing amounts of traffic on the communication lines or differing loads on the server are common causes. You will see very different response times depending on the access equipment you use.

✓ **Routing hop count —** The part of the replies that says TTL=50 tells you about the route the message took from one point to another. The acronym *TTL* stands for *Time to Live*, which is a measure of how many rerouting from one point to another the packet has to go through before IP declares it undeliverable. The number following TTL (called the *hop count*) is a number that usually starts at 255 and counts down by one every time the message gets rerouted through an intermediary computer.

•What to PROCESS

I. Protocols

Directions: In this worksheet, write the name of the protocol and the default port(s) for each protocol definition in the table. Do this on your notebook.

Be prepared to discuss your answers in front of the class.

Protocol Definition	Protocol	Default Port(s)
Provides connections to computers over a TCP/IP network		
Sends e-mail over a TCP/IP network		
Translates URLs to IP address		
Transports Web pages over a TCP/IP network		
Automates assignment of IP address on a network		
Securely transports Web pages over a TCP/IP network		
Transports files over a TCP/IP network		

II. Identifying IP Address Classes

Directions: In this worksheet, your teacher will write several IP addresses with their appropriate subnet masks. You will copy the IP address and Subnet Mask. You will write which IP Address Class is appropriate in the IP Address Class column in the chart below. An example has been provided for you.
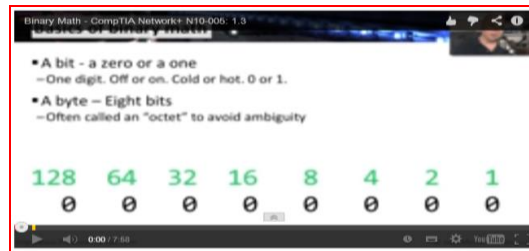
Be prepared to discuss the IP Address Class you select.
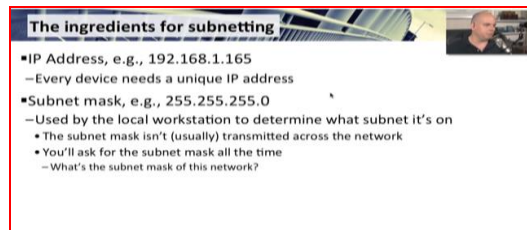
IP Address	Subnet Mask	IP Address Class
10.0.0.0	255.0.0.0	**A**

· **What to REFLECT / UNDERSTAND**

To deepen your understanding with regard to the Internet Protocols, IP Address and subneting, utilize the Internet and the website *www.professormesser.com*, watch and learn from the video presentations. Use the URLs below:

1. http://www.professormesser.com/n10-005/binary-math-2/

2. http://www.professormesser.com/n10-005/ip-classes/

Computer Hardware Servicing

3. http://www.professormesser.com/n10-005/networkingprotocols/

4. http://www.professormesser.com/n10-005/subnetting/
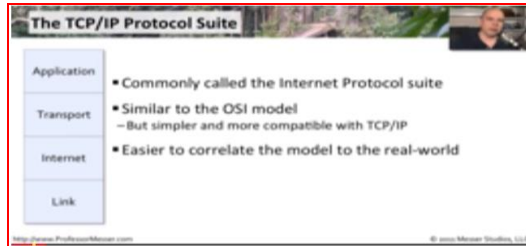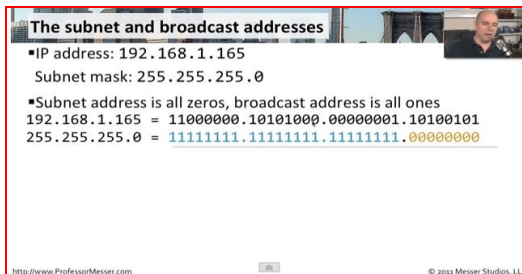
Reflection on the video presentations

Directions: Answer the essential questions below based on the video presentations you had watched. Write your answer in a clean sheet of paper.

1. What are the procedures involved in calculating IP address and the procedures in converting IP address to binary and vice versa?

   _____
   _____
   _____

   What are the different IP Classes? Discuss each briefly and give examples.

   _____
   _____
   _____

2. What are the distinguished Internet Protocols? Describe each.

   _____
   _____
   _____

3. What are the necessary procedures in calculating subnet mask or simply subneting? Show an example solution for the calculation.

   _____
   _____
   _____

Computer Hardware Servicing

Configure an Ethernet NIC to use DHCP

Directions: Configure an Ethernet NIC to use DHCP to obtain an IP address. You need to follow the procedures given below and apply safety precautions in accomplishing this task. While doing the activity, you have to answer activity questions written after every step. Write your answer in a clean sheet of paper. Your performance will be rated based on the performance rubrics.

Rubrics for Configuration

Criteria	B (70-74)	D (75-79)	AP (80-84)	P (85-89)	A (90-100)	Total (=score x %)
Proper Configuration (30 %) (The configured hardware was properly configured according to job specification.)						
Adherence to the Procedures (30%) (The specified job was done by following the procedures. Safety measures were observed during the activity.)						
Quality of Work (30%) (The device was configured properly.)						
Comprehension (10%) (Interview / Guide questions were answered correctly according to the job requirements.)						
					Grand Total	

Legend:
        B- Beginner
        D- Developing
        AP- Approaching Proficiency
        P- Proficient
        A- Advance

Recommended Equipment
- Linksys 300N router
- A computer running Window XP Professional
- Ethernet patch cable

Procedures:
Step 1
- ✓ Plug one end of the Ethernet patch cable into "Port 1" at the back of the router.
- ✓ Plug the other end of the Ethernet patch cable into the network port on the NIC in your computer.
- ✓ Plug in the power cable of the router if it is not already plugged in.
- ✓ Turn on your computer and log on to Windows as an administrator.
- ✓ Click **Start.**
- ✓ Right-click **My Network Places**, and then choose **Properties**.
- ✓ The "Network Connections" window appears.
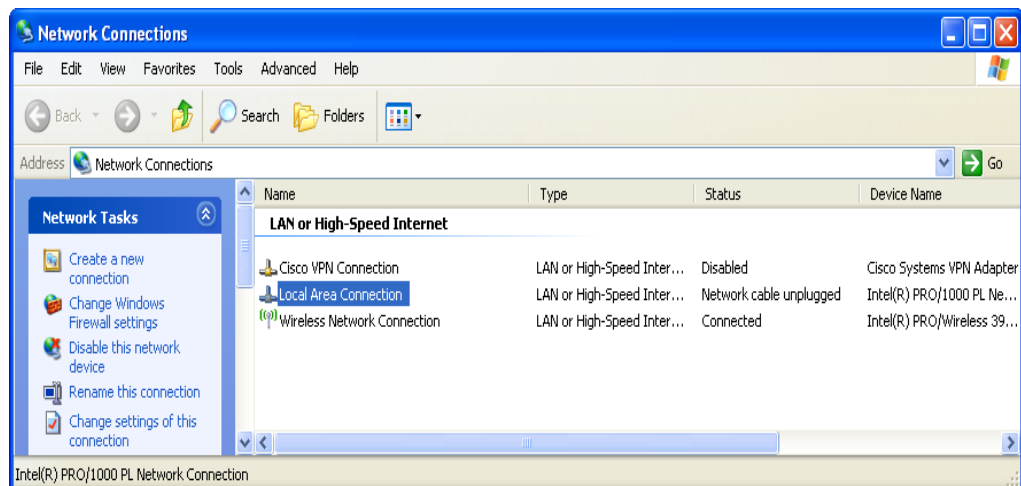
Figure 59. My Network Places

Computer Hardware Servicing

Step 2
- ✓ Right-click **Local Area Connection**, and then choose **Properties**.
- ✓ The "Local Area Connection Properties" window appears.
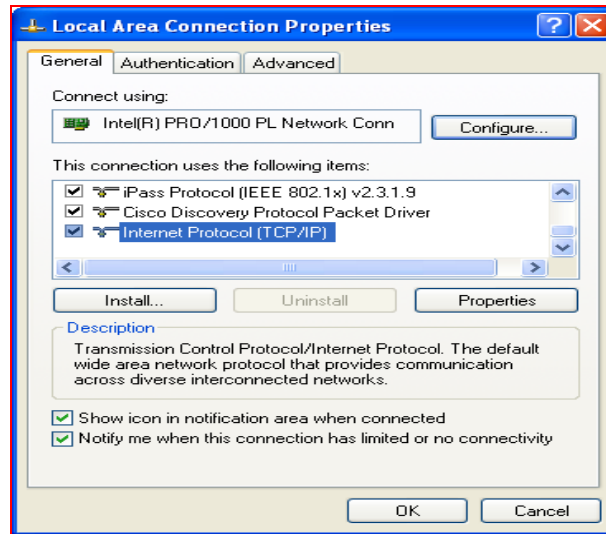
Figure 60. Local Area Connection Properties

Activity Questions:

1. What is the name and model number of the NIC in the "Connect using:" field?
2. What are the items listed in the "This connection uses the following items:" field?

Step 3
- ✓ Choose **Internet Protocol (TCP/IP)**.
- ✓ Click **Properties**.
- ✓ The "Internet Protocol (TCP/IP) Properties" window appears.
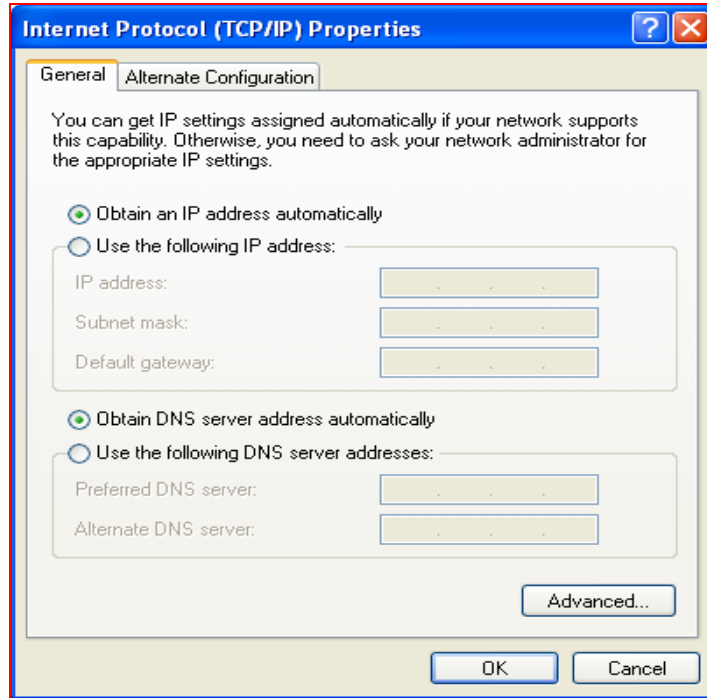
Figure 61. Internet Protocol (TCP/IP) Properties

Activity Question:

3. What is the IP address, Subnet mask, and Default gateway listed in the fields of the "Use the following IP address:" area? Answers may vary. If the computer is configured to obtain an IP address automatically, there will be no information in the fields.

✓ Click the **Obtain an IP address automatically** radio button.
✓ Click **OK**. The "Internet Protocol (TCP/IP) Properties" window closes.
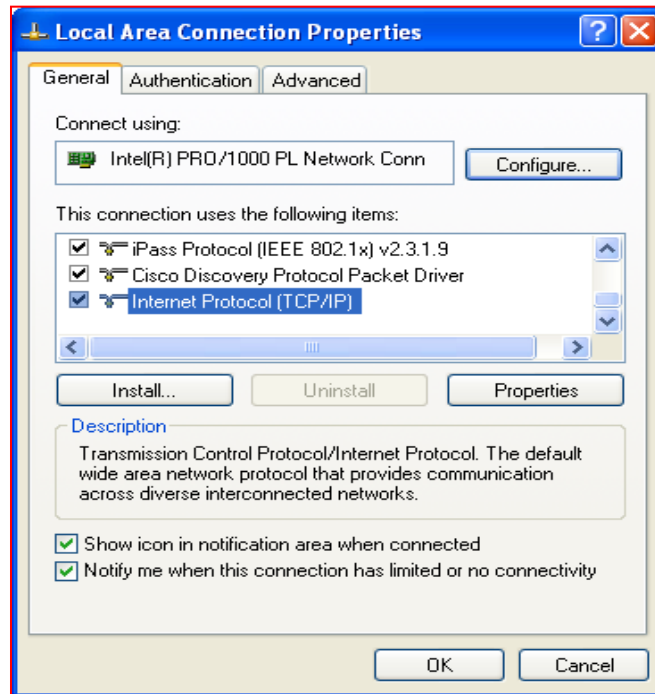
Figure 62. Local Area Connection Properties Window

- ✓ Click **OK.**
- ✓ Restart your computer.

Step 4
- ✓ Log on to Windows as an administrator.
- ✓ Check the lights at the back of the NIC. These lights will blink when there is network activity.
- ✓ Choose **Start > Run**.
- ✓ Type **cmd** and click **OK**.
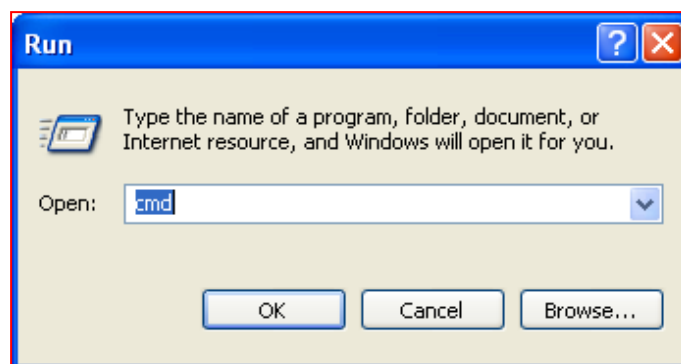
Figure 63. Run Window

- ✓ **Type ipconfig/all**, and then press the **Enter** key.

Figure 64. ipconfig all window

Activity Questions:
1. What is the IP address and subnet mask of the "Ethernet Adapter Local Area Network Connection"?
2. What is the IP address of the DHCP server?
3. On what date was the Lease obtained?
4. On what date will the Lease expire?

Computer Hardware Servicing

Task 2
Configure Wireless Router
Directions: Configure and test the wireless settings on the LinksysWRT300N.

Recommended Equipment
- A computer with Windows XP Professional / Windows 7
- A Wireless NIC installed
- An Ethernet NIC installed
- Linksys WRT300N Wireless Router
- Ethernet patch cable

Step 1

✓ Connect the computer to one of the **Ethernet** ports on the wireless router with an Ethernet patch cable.
✓ Plug in the power of the wireless router. Boot the computer and log in as an administrator.

Step 2

✓ Choose **start > Run**, and type "cmd". Press the **Return key**.
✓ Type **ipconfig**.
✓ What is the default gateway for the computer?

Step 3

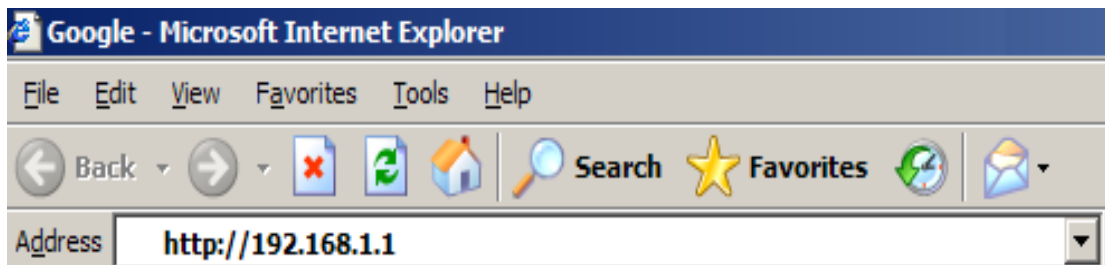✓ Open your browser. Type "192.168.1.1" in the "Address" field, and then press **Return**.

Figure 65. Browser Window
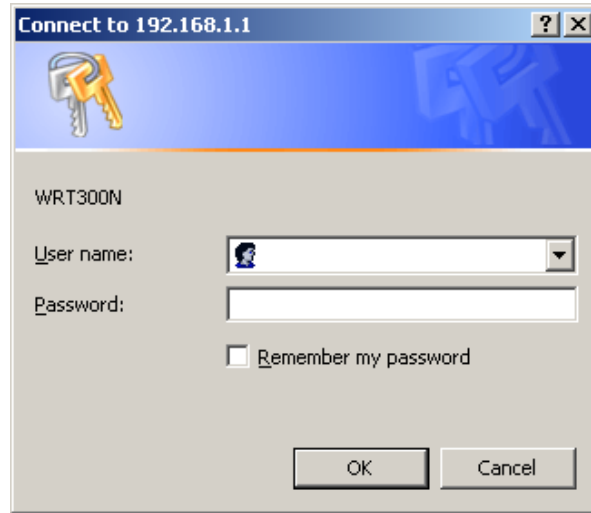
✓ The "Connect to 192.168.1.1" window appears.

Figure 66. Connect to 192.168.1.1 Window

- ✓ Type "admin" in the "Password" field.
- ✓ The Setup screen appears.

Step 4

- ✓ Click the "Wireless" tab.
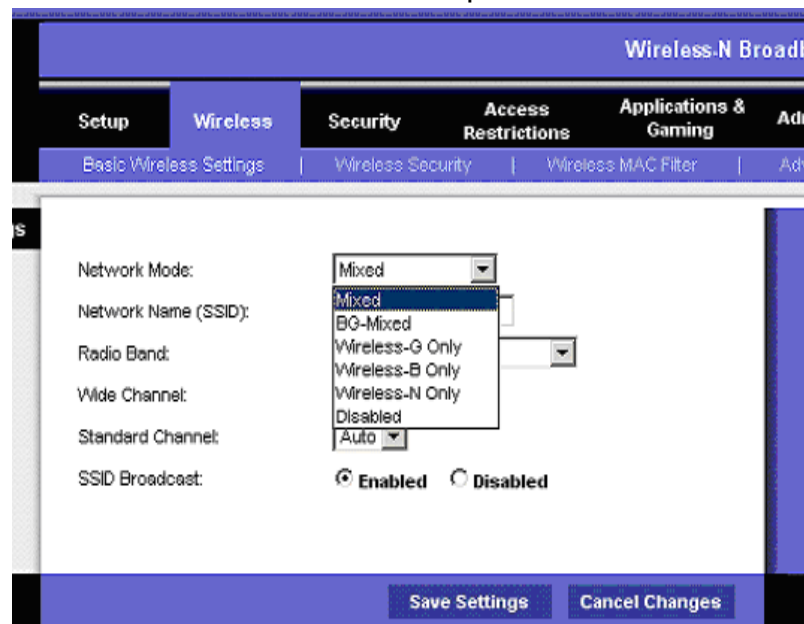- ✓ Choose "Mixed" in the "Network Mode" drop-down box.

Figure 67. Wireless Tab Window

- ✓ Type "CHS#" in the "Network Name (SSID)" field, where # is the number assigned by your instructor.

Computer Hardware Servicing

- ✓ Click **Save Settings**.
- ✓ The "Settings are successful" screen appears.

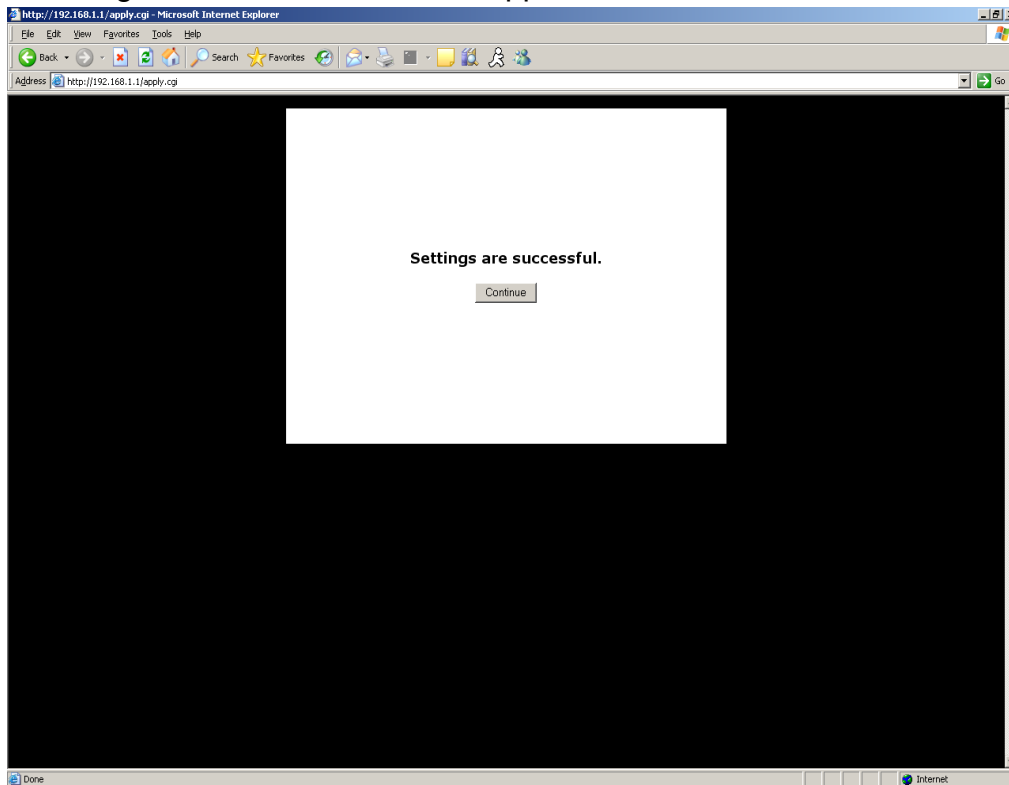
Figure 67. Settings are Successful Window

- ✓ Click **Continue**, and then close the browser window.

Step 4

- ✓ Unplug the Ethernet patch cable from the rear of the computer.
- ✓ Choose **Start**, and then right-click **My Network Places**. Choose **Properties**.
- ✓ Double-click the wireless adapter, and then select **View Wireless Networks**.
- ✓ Choose **CHS**, and then click the **Connect** button.
- ✓ Open Internet Explorer, and then connect to the wireless router.
- ✓ Log in to the wireless router.
- ✓ Close Internet Explorer.

Peer-to-Peer Network

In a ***peer-to-peer network***, devices are connected directly to each other without any additional networking devices between them, as shown in Figure 68. In this type of network, each device has equivalent capabilities and responsibilities. Individual users are responsible for their own resources and can decide which data and devices to share. Because of that, the network has no central point of control or administration.
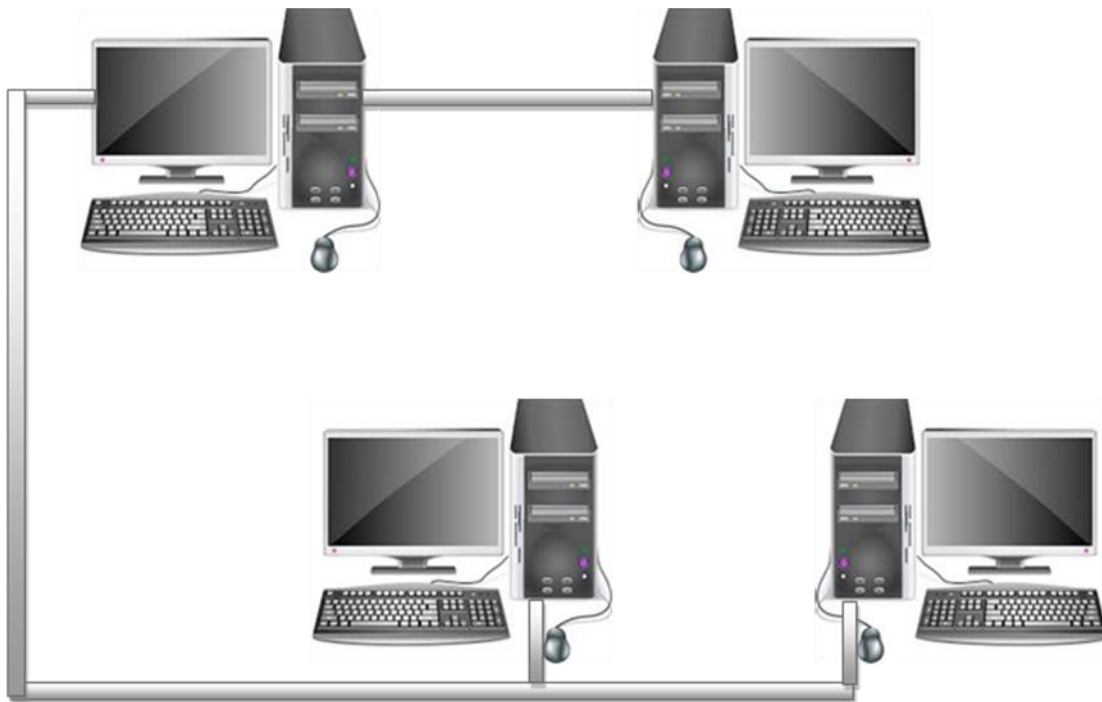

Figure 68. Peer-to-Peer Network

It allows certain files and folders to be shared with everyone or with selected users. Peer-to-peer networks are quite common in small offices that do not use a dedicated file server. Files and folders can be configured to allow network users to copy them, but not alter them in their original location, which is a common safety precaution. However, files and folders can also be assigned a "read/write" status that allows either selected users or all users on the network to change them.

Peer-to-peer networking differs from client-server networking, where certain devices have responsibility for providing or "serving" data and other devices consume or otherwise act as "clients" of those servers.

Setting up a peer-to-peer network in Windows XP

The steps described below are provided as a general guide that will work for most home networking situations. However, it may not work for all scenarios.

Do the following steps to set up your own inclusive home network:

1. Make sure both systems have Network Interface Cards (NICs) installed and are using the proper cables.

> **NOTE:** For a direct network cable connection between two PCs (not with a hub, switch or router), you need to have a cross-over cable.

2. For PCs with Windows XP, the home networking wizard can be used to set up Windows for your network.
   a. Click **Start**, and then **Control Panel**.
   b. Select **Network and internet connections**.
   c. Double-click **Network setup wizard** and follow the on-screen instructions.

> **NOTE**: If the Network setup wizard is unsuccessful, continue with the steps below.

3. Click **Start**, **Control Panel**, **Network and Internet Connections**, and then **Network Connections**. At Network Connection Windows, you will see the *Local Area Connection **Icon, Right click** it and select **Properties**.* Local Area Connection window appears.
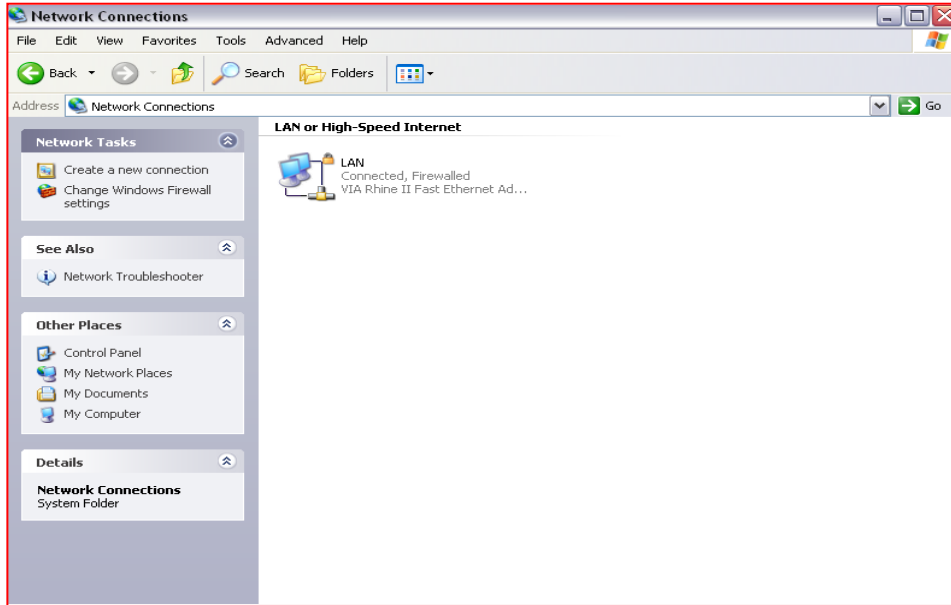
Figure 69. Network Connection Window

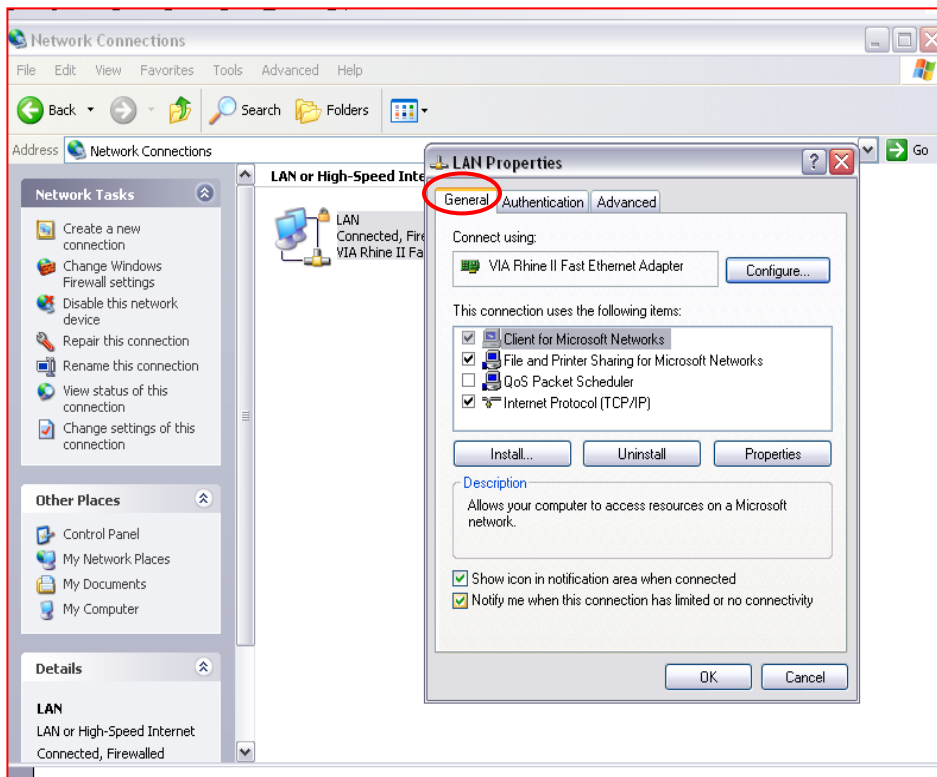4. Click on the **General** tab.

Figure 70. LAN Properties General Tab

5. A device name should appear under "connect using." If not, there is a hardware issue and Windows is not recognizing the network hardware. This issue must be fixed before continuing.

    a. At the General Tab, Put a check mark at the following:
- Client for Microsoft Network
- File and Printer Sharing for Microsoft Network
- Internet Protocol (TCP/IP)

    b. Put a check mark saying ***Show icon in notification area when connected.***

    c. Select the *Internet Protocol (TCP/IP)* and click the *Properties* button

NOTE: If any of the above component is not installed, install them by selecting **Add** or **Install**, and then selecting the missing component, and clicking **Add**.
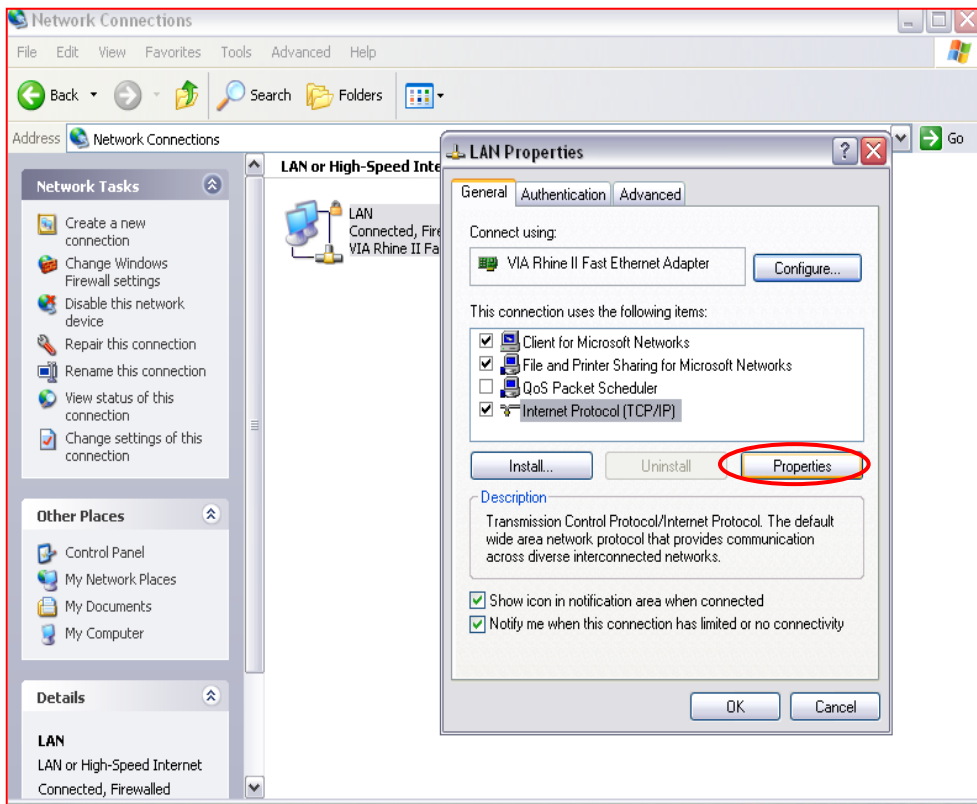

Figure 71. TCP/IP- Properties

d. At the IP Address tab, select **Specify IP Address**.

e. Enter 192.168.0.1 as the unique IP Address for the first machine. For each other PC add one to the last number in the IP address. For example,

- KIDSPC1 = 192.168.0.1 ,
- MOMSPC2 = 192.168.0.2 ,
- and WORKPC3 = 192.168.0.3 .

NOTE: 192.168.0.x is an IP Address reserved for private networks and is not routable to the Internet.
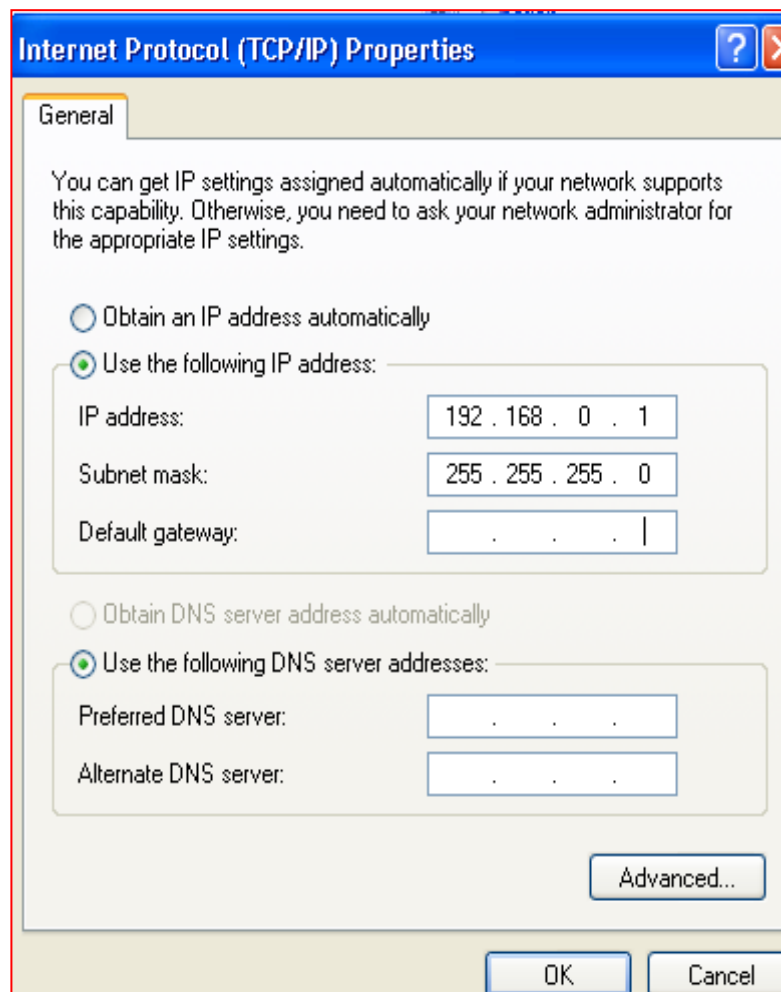

Figure 72. Assigning IP Address and Subnet Mask

6. In the Subnet mask field enter: 255.255.255.0
   All PCs on the same network use the same subnet mask. Click the *Ok* button to finish configuration and to close the Local Area Connection Properties windows.

> **Note**: The Domain Name System (DNS) is optional. If you have a DNS system and your connected to ISP you can input an IP address which came from the DNS server.

7. Click the **Computer Name** tab and click the **Change** button.
8. Enter a name that describes the PC in the Computer Description field. For example, KIDSPC1, MOMSPC2, or WORKPC3.
9. Enter the workgroup name for your network. Use the same workgroup name for all PCs on the network. Spelling is important in this step.
10. Repeat these steps for each PC on the network.
11. Wait two minutes after Windows opens on all PCs, and then double-click the **Network Neighborhood** icon on the desktop. If all went well, you should see all the PC names on the network when files and folders are being shared. If you do not see them, press F5 to refresh the screen.
12. If after refreshing the network window, the other PCs still do not appear, check the firewall settings that may be interfering with the communication.

Setting up a Peer-to-Peer network in Windows 7

If you are going to work with Windows 7 operating system, the following procedures are used to set up a peer-to-peer network:

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

Figure 73. Step 1

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

Figure 74. Step 2

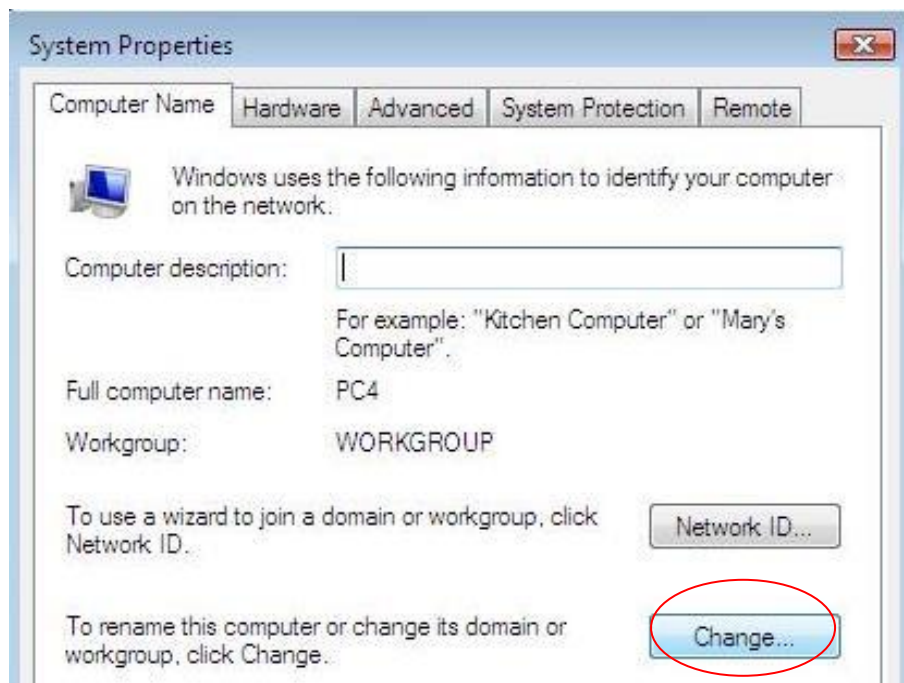3. Click or select Change.

Figure 75. Step 3

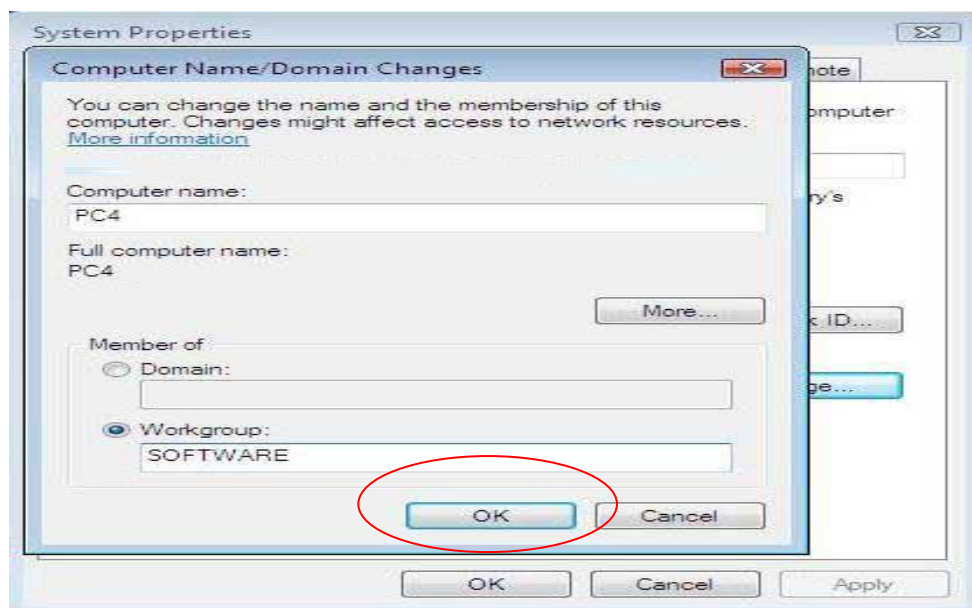4. Change computer name and workgroup name. Then, click OK.

Figure 76. Step 4

5. Save the change (A Reboot will be required).
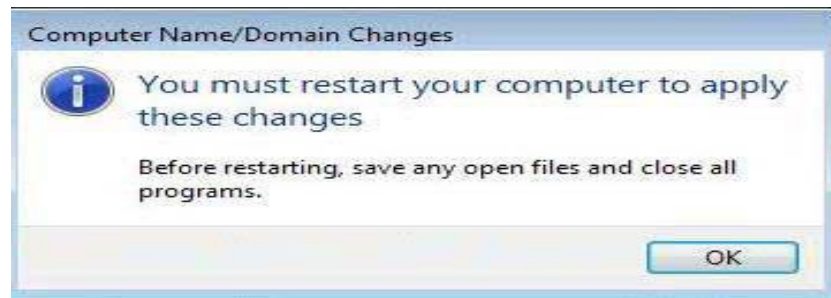
Figure 77. Step 5

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

Figure 78. Step 6

7. Turn on Network discovery, File sharing, Printer Sharing.
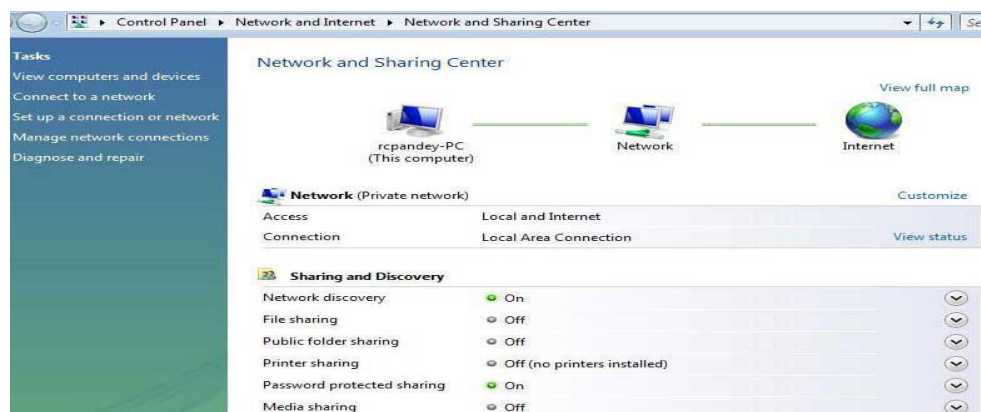
Figure 79. Step 7

8. Click on Manage network connections.
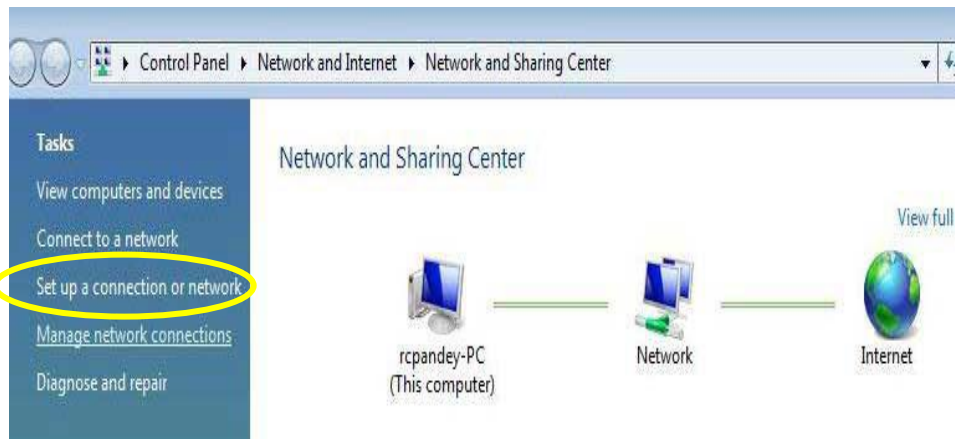
Figure 80. Step 8

9. Select Local Area Connection ==> Properties

Figure 81. Step 9

10. Select Internet Protocol version 4 (TCP/IPv4) ==> properties.
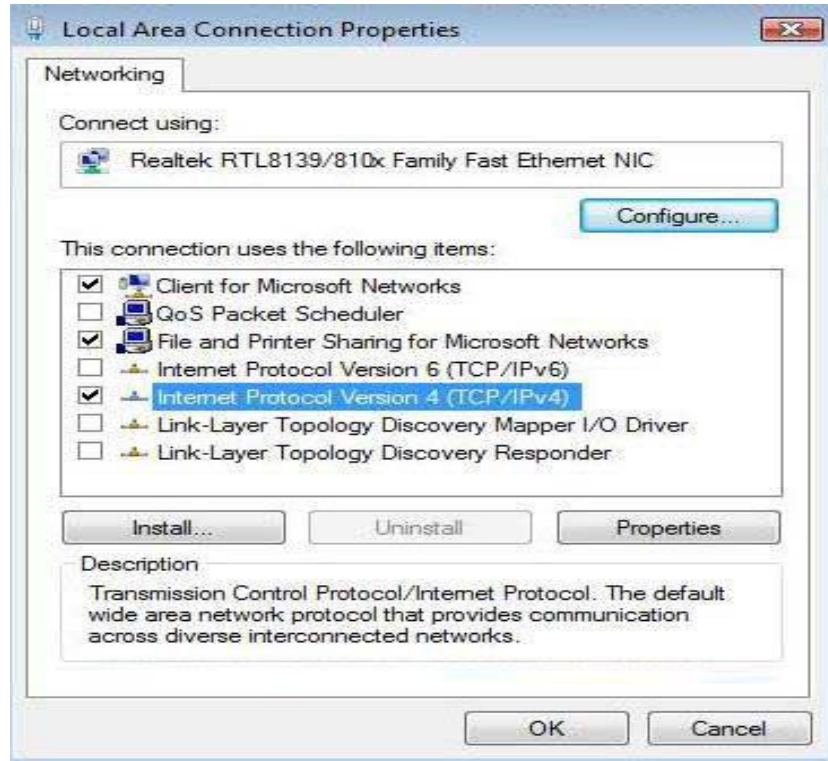
Figure 82. Step 10

11. Now enter the assigned IP address and then click OK.
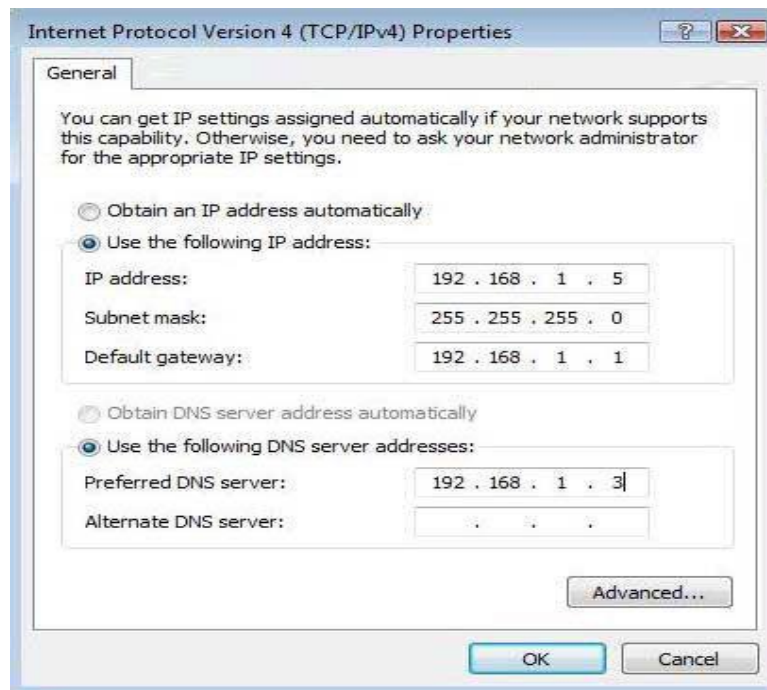
Figure 83. Step 11

12. Now open My network place ==> Click to change then Select Turn on network discovery and file sharing.
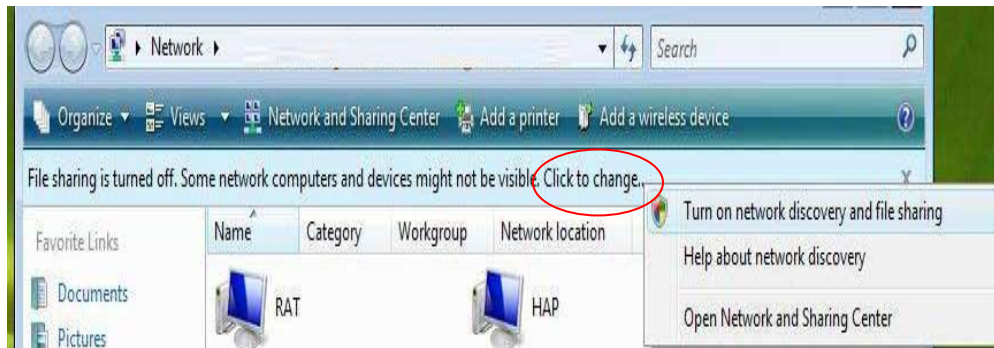
Figure 84. Step 12

13. If you could see all computers in My Network place, you have successfully configured a workgroup.
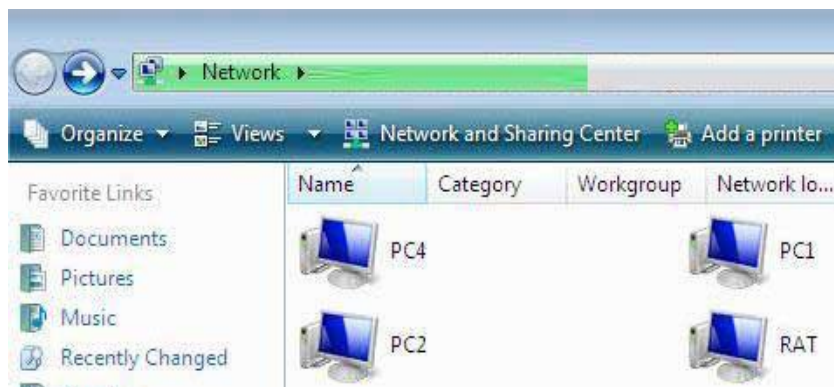
Figure 85. Step 13

Client-Server Network

In a **client/server network**, the server provides the requested information or service to the client. Servers on a client/server network commonly perform some of the processing work for client machines, such as sorting through a database before delivering only the records requested by the client.
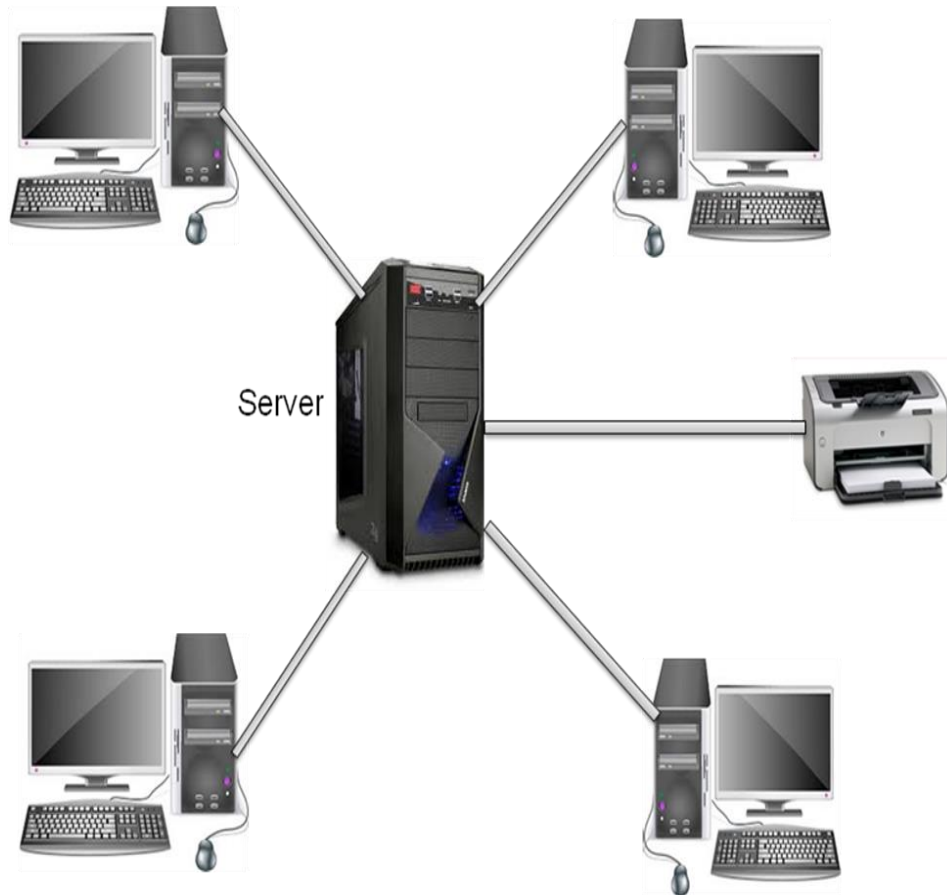
Figure 86. Client/Server Network

One example of a client/server network is a corporate environment in which employees use a company e-mail server to send, receive, and store e-mail. The e-mail client on an employee computer issues a request to the e-mail server for any unread e-mail. The server responds by sending the requested e-mail to the client.

In a client/server model, the servers are maintained by network administrators. Data backups and security measures are implemented by the network administrator. The network administrator also controls user access to

Computer Hardware Servicing

the network resources. All the data on the network is stored on a centralized file server. Shared printers on the network are managed by a centralized print server. Network users with the proper permissions can access both the data and shared printers. Each user must provide an authorized username and password to gain access to network resources that he or she is permitted to use. For data protection, an administrator performs a routine backup of all the files on the servers. If a computer crashes, or data is lost, the administrator can easily recover the data from a recent backup.

 •What to PROCESS

Comparison

Directions: Using the table below, cite the features of peer-to-peer and client /server network.

Peer-to-peer Network	Client/Server Network
1. 2. 3. 4. 5.	

 • What to REFLECT / UNDERSTAND

Peer-to-peer study

Directions: Have a partner. Using different references available such as articles, books, internet and publications, investigate and search for the advantages and disadvantages of peer-to-peer network. You will present your output in front of the class and you will be rated according to the rubrics for research and rubrics for oral presentation.

Rubrics for Research Study

Qualities & Criteria	Poor (0-74)	Good (75-79)	Very Good (80-89)	Excellent (90-100)
Format/Layout (15%) • Presentation of the text • Structuring of text • Requirements of length, font and style followed	Followed poorly the requirements related to format and layout.	Some format and layout related requirements were met.	Most format and layout related requirements were met.	All the requirements related to format and layout were strictly followed.
Content/Information (50%) • All elements of the topics are addressed • The information is technically sound • Information based on careful research • Coherence of information	The research was not objective and poorly addresses the issues referred in the proposed topic. The provided information was not necessary or not sufficient to discuss these issues.	The research was objective and for some part addresses an in depth analysis The provided information was, for some part, necessary and sufficient to discuss these issues.	The research was objective and for the most part addresses an in-depth analysis of most issues referred in the proposed topic. The provided information was, for the most part, necessary and sufficient to discuss these issues.	The research was objective and addresses with an in-depth analysis all the issues referred in the proposed topic. The provided information was necessary and sufficient to discuss these issues.

| Quality of Writing (25%)

- Clarity and cohesiveness of sentences and paragraphs
- No errors in spelling, grammar and use of English
- Organization and coherence of ideas	The essay was not well written, and contains many spelling errors, and/or grammar errors and/or use of English errors. It lacks clarity and/or does not present ideas in a coherent way.	The essay was well written for some part, without spelling, grammar or use of English errors. The essay is for some part well organized, clear and presents ideas in a coherent way.	The essay was well written for the most part, without spelling, grammar or use of English errors. The essay is for the most part well organized, clear and presents ideas in a coherent way.	The essay was well written from start to finish, without spelling, grammar or use of English errors. The essay was well organized, clear and presents ideas in a coherent way.
References (10%)

- Soundness of references | References were not appropriately used and cited. | Some of the references were appropriately used and cited. | Most of the references were appropriately used and cited. | All of the references were appropriately used and cited. |

Rubrics for Oral Presentation					
CRITERIA	B (70- 74)	D (75-79)	AP (80-84)	P (85-89)	A (90-100)
1. Gave an interesting introduction					
2. Presented clear explanation of topic					
3. Presented information in logical manner					
4. Used complete sentence					
5. Offered a concluding summary					
6. Spoke clearly, correctly, distinctly, and confidently					
7. Maintained eye contact					
8. Maintained acceptable posture.					
9. Utilized audio-visual aids					
10. Handled questions and comments confidently					
Total					
Grand Total					

Legend:

B- Beginner
D- Developing
AP- Approaching Proficiency
P- Proficient
A- Advance

Hands-on Activity

Directions: Follow and perform the prescribed procedures in setting up a peer-to-peer and client/server network for Windows XP and Windows 7. You will be rated base on the performance indicators below:

Performance Indicators for Setting- up a peer-to-peer and client/server network

Indicators	Poor (70- 74)	Fair (75-79)	Good (80-84)	Very Good (85-89)	Excellent (90-100)	Total (score x %)
Safety Procedures (15%) -Applied / manifested safety precautions while working						
Adherence to the Procedures (30%) -Followed the procedures systematically						
Workmanship (15%) -Organized materials and tools while accomplishing the task and has time management						
Quality of Service (40%) -Had set-up a fully functional peer-to-peer and client/server network.						
					Grand Total	

Network Security

As a future Computer Technician you need to understand computer and network security. Failure to implement proper security procedures can affect users, computers, and the general public. Private information, company secrets, financial data, computer equipment, and items about national security are placed at risk if proper security procedures are not followed.

The Importance of Security in Computer System and Networks

Computer and network security help keep data and equipment safe by giving only the appropriate people access. Everyone in an organization should give high priority to security, because everyone can be affected by a lapse in security.

Theft, loss, network intrusion, and physical damage are some of the ways a network or computer can be harmed. Damage or loss of equipment can mean a loss of productivity. Repairing and replacing equipment can cost the company time and money. Unauthorized use of a network can expose confidential information and reduce network resources.

An attack that intentionally degrades the performance of a computer or network can also harm an organization's production. Poorly implemented security measures that allow unauthorized access to wireless network devices demonstrate that physical connectivity is not necessary for security breaches by intruders.

A technician's primary responsibilities include data and network security. A customer or an organization may depend on you to ensure that their data and computer equipment are secure. You will perform tasks that are more sensitive than those assigned to the average employee. You may have to repair, adjust, and install equipment. You need to know how to configure settings to keep the network secure, but still keep it available to those who need to access it. You will ensure that software patches and updates are applied, antivirus software is installed, and antispyware software is used. You may also be asked to instruct users on how to maintain good security practices with computer equipment.

Security Attacks

To successfully protect computers and the network, a technician must understand both of the following types of threats to computer security:

- **Physical:** Events or attacks that steal, damage, or destroy such equipment as servers, switches, and wiring.
- **Data:** Events or attacks that remove, corrupt, deny access to, allow access to, or steal information.

Threats to security can come from inside or outside an organization, and the level of potential damage can vary greatly. Potential threats include the following:

- ✓ **Internal:** Employees who have access to data, equipment, and the network. Internal attacks can be characterized as follows:
  - ❖ *Malicious threats* are when an employee intends to cause damage.
  - ❖ *Accidental threats* are when the user damages data or equipment unintentionally.
- ✓ **External:** Users outside an organization who do not have authorized access to the network or resources. External attacks can be characterized as follows:
  - ❖ Unstructured attacks, which use available resources, such as passwords or scripts, to gain access to and run programs designed to vandalize.
  - ❖ Structured attacks, which use code to access operating systems and software.

Physical loss or damage to equipment can be expensive, and data loss can be detrimental to your business and reputation. Threats against data are constantly changing as attackers find new ways to gain entry and commit their crimes.

Viruses, Worms, and Trojan Horses

Computer viruses are created with malicious intent and sent by attackers. A *virus* is attached to small pieces of computer code, software, or document. The virus executes when the software is run on a computer. If the virus spreads to other computers, those computers could continue to spread the virus.

A virus is transferred to another computer through e-mail, file transfers, and instant messaging. The virus hides by attaching itself to a file on the computer. When the file is accessed, the virus executes and infects the computer. A virus has the potential to corrupt or even delete files on your

computer, use your e-mail to spread itself to other computers, or even erase your hard drive. Some viruses can be exceptionally dangerous. The most damaging type of virus is used to record keystrokes. Attackers can use these viruses to harvest sensitive information, such as passwords and credit card numbers. Viruses may even alter or destroy information on a computer. Stealth viruses can infect a computer and lay dormant until summoned by the attacker.
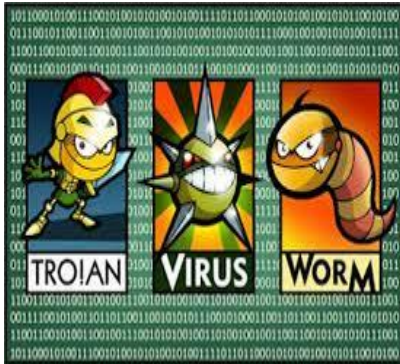
A *worm* is a self-replicating program that is harmful to networks. A worm uses the network to duplicate its code to the hosts on a network, often without any user intervention. It is different from a virus because a worm does not need to attach to a program to infect a host. Even if the worm does not damage data or applications on the hosts it infects, it harms networks because it consumes bandwidth.

A *Trojan horse* technically is a worm. It does not need to be attached to other software. Instead, a Trojan threat is hidden in software that appears to do one thing, and yet behind the scenes it does another. Trojans often are disguised as useful software. The Trojan program can reproduce or replicate like a virus and spread to other computers. Computer data damage and production loss could be significant. A technician may be needed to perform the repairs, and employees may lose or have to replace data. An infected computer could be sending critical data to competitors while at the same time infecting other computers on the network.

Security Procedures

You should use a security plan to determine what will be done in a critical situation. Security plan policies should be constantly updated to reflect the latest threats to a network.

A security plan with clear security procedures is the basis for a technician to follow. Security plans should be reviewed each year. Part of the process of ensuring security is conducting tests to determine areas where security is weak. Testing should be done on a regular basis. New threats are released daily.

Regular testing provides details of any possible weaknesses in the current security plan that should be addressed. A network has multiple layers of security, including physical, wireless, and data. Each layer is subject to

security attacks. The technician needs to understand how to implement security procedures to protect equipment and data.

Source: www.computerflu.com
Figure 87. Most Commonly Known Anti Virus Software

Virus protection software, known as ***antivirus software***, is software designed to detect, disable, and remove viruses, worms, and Trojans before they infect a computer. Antivirus software becomes outdated quickly, however. The technician is responsible for applying the most recent updates, patches, and virus definitions as part of a regular maintenance schedule. Many organizations establish a written ***security policy*** stating that employees are not permitted to install any software that is not provided by the company. Organizations also make employees aware of the dangers of opening e-mail attachments that may contain a virus or worm.

Data Encryption

Encrypting data involves using codes and ciphers. ***Data encryption*** can help prevent attackers from monitoring or recording traffic between resources and computers. It may not be possible to decipher captured data in

Computer Hardware Servicing

time to make any use of it. A security alert may inform you that you are using an encrypted connection.

A virtual private network (VPN) is an encryption system that protects data as though it resides on a private network. The data actually travels over the Internet or another unsecured public network.

Port Protection

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

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

How to Enable Firewall for Windows XP?

The proceeding section provides the procedures for enabling windows XP firewall:

1. Click Start Button then choose **Control Panel**.

Figure 88. Control Panel

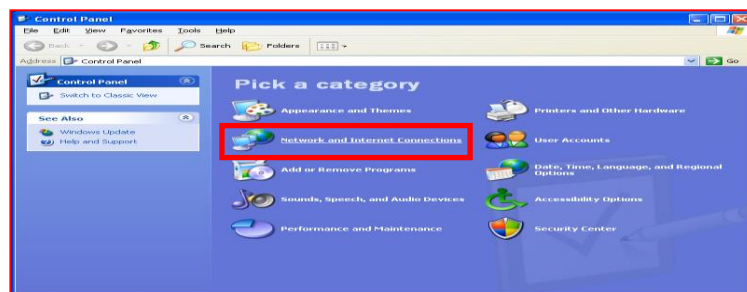2. Click the "**Network and Internet Connections**" option.

Figure 89. Control Panel Window

Computer Hardware Servicing

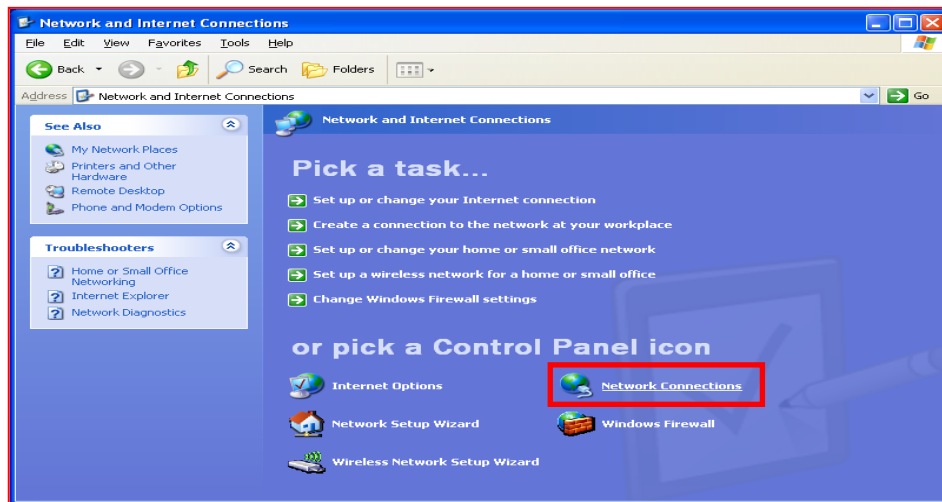3. Then click the "Network Connections" option.

Figure 90. Network and Internet Connections

4. Double click the icon labeled "Local Area Connection". The icon may have a number after it, for example "Local Area Connection 5". Click on Properties button.
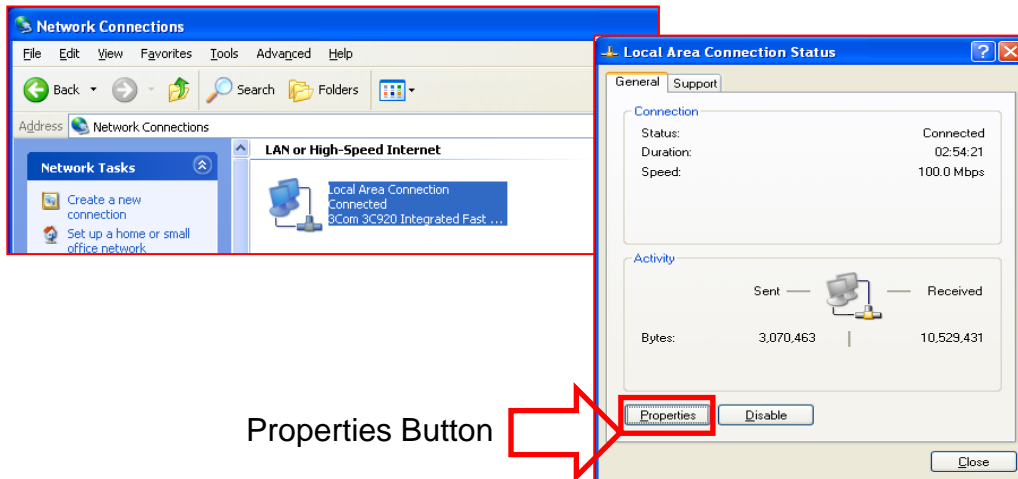

Properties Button

Figure 91. Local Area Network Connection Properties Window

5. On the "Advanced" tab, select "Protect my computer and network by limiting or preventing access to this computer from the Internet".
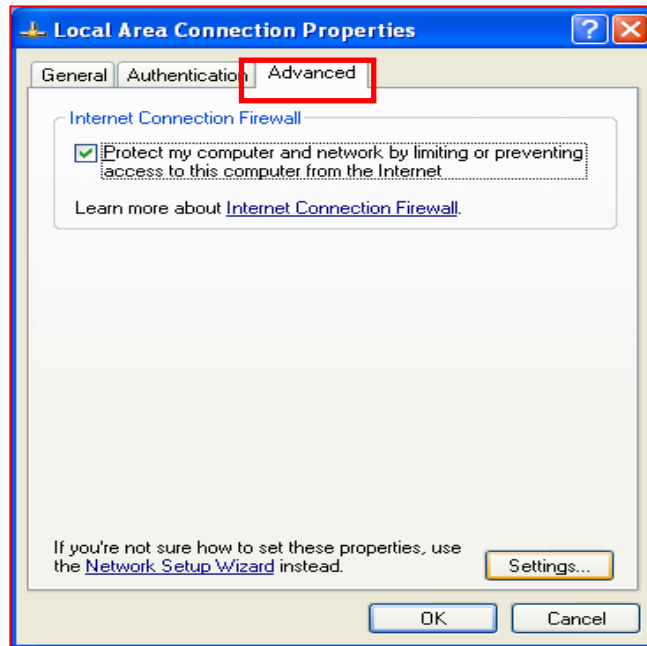
Computer Hardware Servicing

Figure 92. Local Area Network Connection Advance Tab

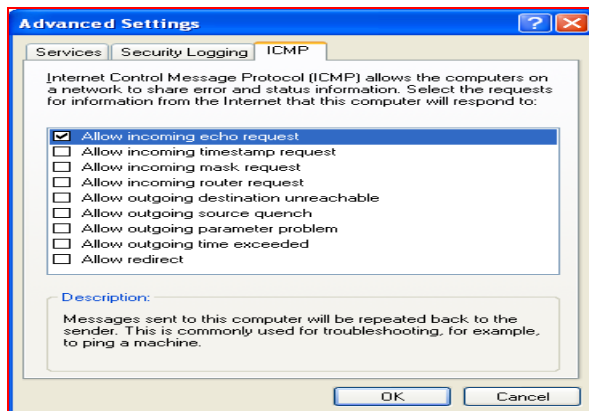6. Click Settings, then on the ICMP tab select "Allow Incoming echo request".

Figure 93. ICMP Tab

Enabling Windows 7 Firewall

1. Open Windows Firewall by clicking the **Start** button, and then clicking **Control Panel**. In the search box, type **firewall**, and then click **Windows Firewall**.
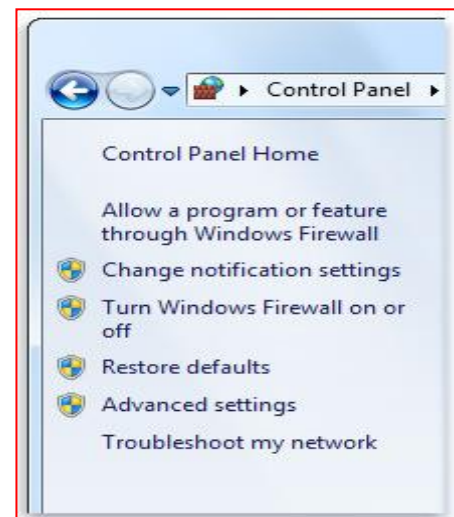

Figure 94. Windows 7 Control Panel

2. In the left pane, click **Turn Windows Firewall on or off**. If you're prompted for an administrator password or confirmation, type the password or provide confirmation. Turn Windows Firewall on or off link in Windows Firewall.

3. Click **Turn on Windows Firewall** under each network location that you want to help protect, and then click **OK**.

If you want the firewall to prevent all programs from communicating, including programs that you have previously allowed to communicate through the firewall, select the **Block all incoming connections, including those in the list of allowed programs** check box.

Wireless Security Techniques

Traffic flows through radio waves in wireless networks, so it is easy for attackers to monitor and attack data without having to connect to a network physically. Attackers gain access to a network by being within range of an unprotected wireless network. A technician needs to know how to configure access points and wireless network interface cards (WNIC) to an appropriate level of security.

When installing wireless services, you should apply the following wireless security techniques immediately to prevent unwanted access to the network:

- *Wired Equivalent Privacy (WEP)* was the first-generation security standard for wireless network. Attackers quickly discovered that 64-bit WEP encryption was easy to break. Monitoring programs could detect the encryption keys used to encode the messages. After the keys were obtained, messages could be easily decoded. In an attempt to overcome this weakness, most users employ a 128-bit key for WEP.
- Change the default administration password.
- Disable the broadcasting of the Service Set Identifier (SSID) to hide it from other users.
- Use MAC filtering to protect the network from other users.
- Change the default values of the SSID by entering the setup program for the access point and renaming the SSID.
- Update to the latest available firmware.
- Install or activate a firewall, and adjust the settings to eliminate all traffic except the desired network settings.
- Update to the latest available firmware.

- Install or activate a firewall, and adjust the settings to eliminate all traffic except the desired network settings.

An attacker can access data as it travels over the radio signal. However, you can use a wireless encryption system to encode data and thereby prevent unwanted capture and use of the data. Both ends of every link must use the same encryption standard. The following list describes the different levels of wireless security, from most secure to least secure:

- *Lightweight Extensible Authentication Protocol (LEAP)*: Also called EAP-Cisco, LEAP is a wireless security protocol created by Cisco to address the weaknesses in WEP and WPA. LEAP is a good choice when using Cisco equipment in conjunction with operating systems such as Windows and Linux.
- *Wi-Fi Protected Access (WPA)*: An improved version of WEP. It was created as a temporary solution until 802.11i (a security layer for wireless systems) was fully implemented. Now that 802.11i has been ratified, WPA2 has been released. It covers the entire 802.11i standard.
- **WEP 128:** An enhanced encryption protocol combining a 104-bit key and a 24-bit initialization vector.
- **WEP 64:** The first-generation security standard for wireless network. It could be exploited because of an encryption key that was vulnerable to decoding.
- **No security:** Although you can elect to implement no security whatsoever, you leave your wireless network completely vulnerable to attack.

In addition, **Wireless Transport Layer Security (WTLS)** is a security layer used in mobile devices that employ the Wireless Applications Protocol (WAP). Mobile devices do not have a great deal of spare bandwidth to devote to security protocols. WTLS was designed to provide security for WAP devices in a bandwidth-efficient manner.

To manually create a network profile using WEP shared key authentication:
1. Open Network and Sharing Center by clicking the **Start** button, and then clicking **Control Panel**. In the search box, type **network**, and then click **Network and Sharing Center**.
2. Click **Set up a new connection or network**.

3. Click **Manually connect to a wireless network**, and then click **Next**.
4. On the **Enter information for the wireless network you want to add** page, under **Security type**, select **WEP**.
5. Complete the rest of the page, and then click **Next**.
6. Click **Change connection settings**.
7. Click the **Security** tab, and then, under **Security type**, click **Shared**.
8. Click **OK**, and then click **Close**.

 •What to PROCESS

Short Quiz
Test I. Modified true or false
Directions: Write **SECURITY** if the underlined word on the subsequent statement makes it true and **VIRUS** if it is makes the statement a false one then write the correct term/word to correct it. (2 points each). Write your answer in a separate sheet of paper.
1. Computer and network <u>security</u> help keep data and equipment safe.
2. A technician's <u>secondary</u> responsibilities include data and network security.
3. Threats to security can come from <u>inside and outside</u> the organization.
4. Computer viruses are created and sent by attackers who have <u>malicious</u> intent.
5. A <u>virus</u> is transferred to another computer through e-mail, file transfer and instant messaging.

Test II. Matching Type
Directions: Match column A with column B in order to identify the term / word being described.

A	B
1. when an employee intends to cause damage	a. Accidental threats
2. when user damages data or equipment unintentionally	b. Antivirus software
	c. Data encryption
3. attached to small pieces of computer code, software and documents	d. Firewall
	e. Malicious threats
	f. Traffic
4. a self-replicating program that is harmful to network	g. Trojan horse
	h. Virus
5. it is technically a worm	i. VPN
	j. WPA

6. software designed to detect, disable and remove viruses 7. it involves using codes and ciphers 8. a way of protecting a computer from intrusion through the ports 9. an encryption system that protects data 10. data being transported on a network	k. WEP l. Worm

Test IV. Acrostic

Direction: Give the meaning of the acronyms given below:

1. VPN- _____
2. SSID- _____
3. WEP- _____
4. WPA- _____
5. WTLS- _____

What to REFLECT / UNDERSTAND

Research Firewalls

Directions: In this activity, you will use the Internet, newspaper, or a local store to gather information about hardware and software firewalls.

1. Using the Internet, research two different hardware firewalls. Based on your research, complete the table below.

Company/Hardware Name	Website URL	Cost	Subscription Length (Month/Year/Lifetime)	Hardware Features

2. Which hardware firewall would you purchase? List reasons for your choice.
3. Using the Internet, research two different software firewalls. Based on your research, complete the table below.

Company/Software Name	Website URL	Cost	Subscription Length (Month/Year/Lifetime)	Software Features

4. Which software firewall would you purchase? List reasons for your choice.

• What to TRANSFER

Configure Windows XP Firewall

Directions: In this hands-on activity you will explore the Windows XP Firewall and configure some advanced settings. There are essential questions that you need to answer while performing the activity.

Step 1
✓ Navigate to the Windows XP Firewall:
✓ **Start > Control Panel > Security Center**
✓ The Firewall indicator shows the status of the firewall. The normal setting is "**ON**".

Figure 96. Windows Security Center

✓ Access the controller for the firewall by clicking **Windows Firewall** at the bottom of the window.
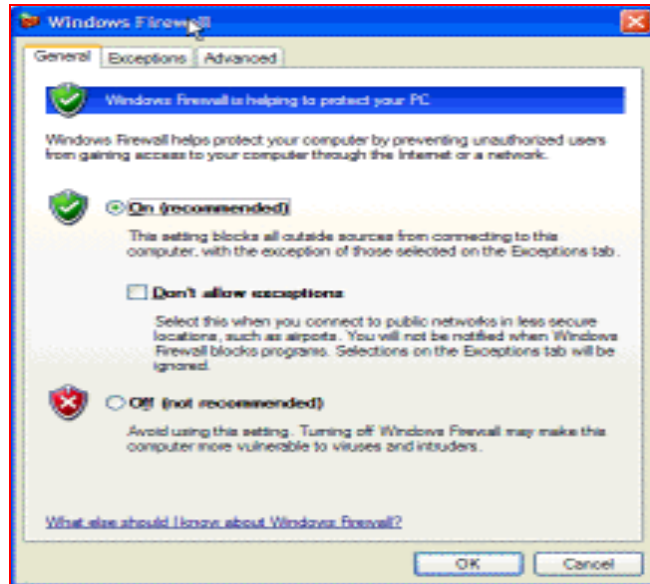
Step 2

Figure 97. Windows Firewall General Tab Window

Essential Questions:

In the space below, state why turning off the Windows Firewall is not advised.

_____

_____

Step 3

✓ From the Windows Firewall control menu select the **Exceptions** tab. Programs and services that Windows Firewall is not blocking will be listed with a checkmark.
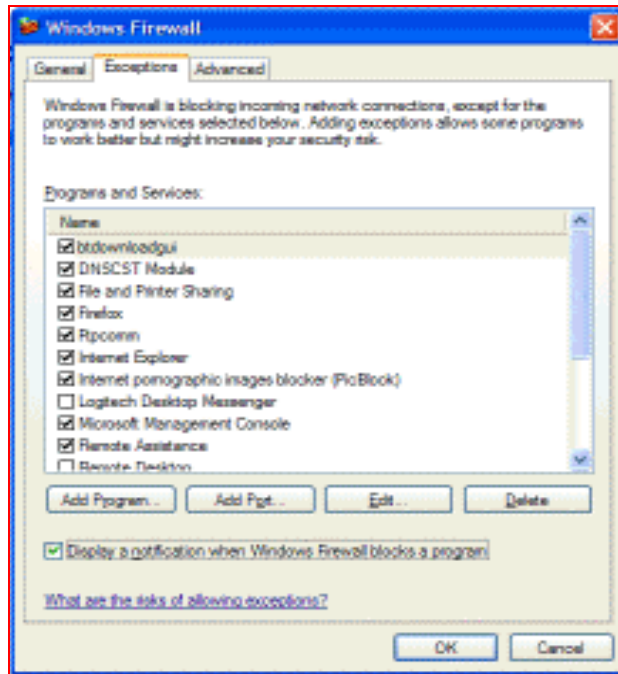
Figure 98. Windows Firewall Exceptions Tab Window

✓ You can add applications to this list. This may be necessary if your customer has an application that requires outside communications but for some reason the Windows Firewall cannot perform the configuration automatically. You must be logged on to this computer as an administrator to complete this procedure.

Essential Question:

Creating too many exceptions in your Programs and Services file can have negative consequences. Describe a negative consequence of having too many exceptions.

_____
_____
_____

Step 4

✓ From the Windows Firewall control menu select the **Advanced** tab to view the **Network Connection Settings**. Network Connection Settings displays the different connections configured for your computer.
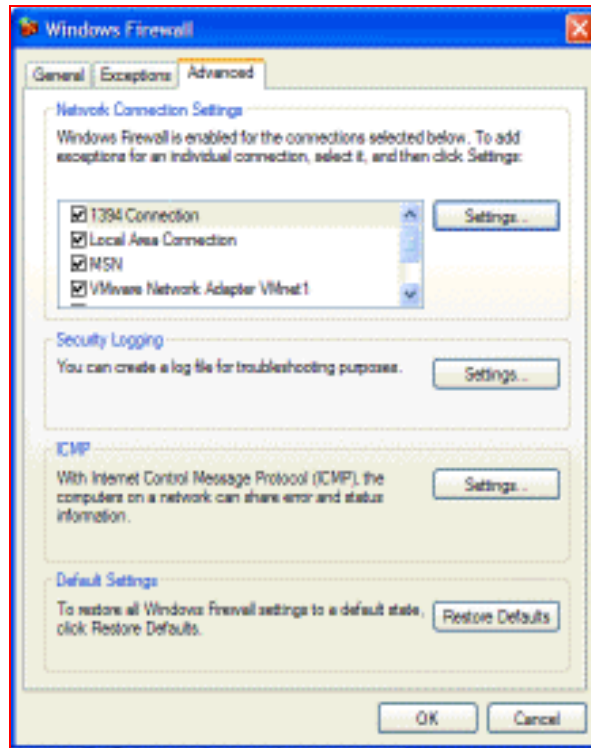
Figure 99. Windows Firewall Advance Tab Window

✓ Click the **Settings** button in the Network Connection Settings area. The Advanced Settings window has two tabs: Services and ICMP. Click the **Services** tab.

Essential Question:
In the space below, list the services that are available.

_____
_____
_____

Step 5

✓ There are many applications that users do not normally see that also need to get through the Windows Firewall to access your computer. These are the network level commands that direct traffic on the network and the Internet.

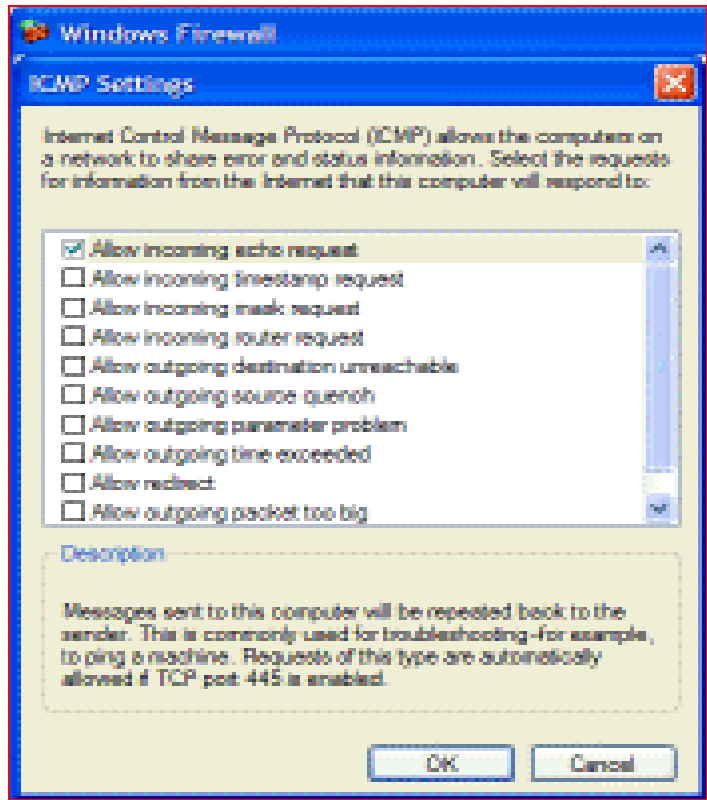✓ Under the ICMP heading, click the **Settings** button. You will see the menu where ICMP exceptions are configured.

Figure 100. ICMP Settings Window

✓ In the example here, allowing incoming echo requests is what allows network users to "ping" your computer to determine if it is present on the network and how fast information travels to and from it.

Essential Question:

In the space below, list the requests for information that your computer will respond to.

_____
_____
_____

File and Printer Sharing

File Sharing is sharing of or offering access to digital information or resources, including documents, multimedia (audio/video), graphics, computer programs, images and e-books. It is the private or public distribution of data or resources in a network with different levels of sharing privileges.

File sharing can be done using several methods. The most common techniques include the following:

- ✓ Removable storage devices
- ✓ Centralized file hosting server installations on networks
- ✓ World Wide Web-oriented hyperlinked documents
- ✓ Distributed peer-to-peer networks

Sharing Resources and Accessing Shared Resources

1. Open *My Computer,* double-click the C: drive, and create a new folder on the C: drive. Name it **Shared.** Right-click the Shared folder and select Properties.
2. In the Shared Properties dialog box, select the Sharing tab.
   - ✓ Notice that the Select the *Share This Folder* button.
   - ✓ Type the Share Name. Click *Apply* and the computer you are linked to should be able to view your Shared folder.
3. Right-click My Network Places, which should be located on your desktop. Select Properties.
4. Right-click your connection (look for a name like Local Area Connection) and again select Properties.
5. In your Local Area Connection Properties dialog box, select File and Print Sharing for Microsoft Networks and click OK. If you don't see an option for File and Print Sharing, click Install and select a service and then click Add. Now select the File and Print Sharing option.
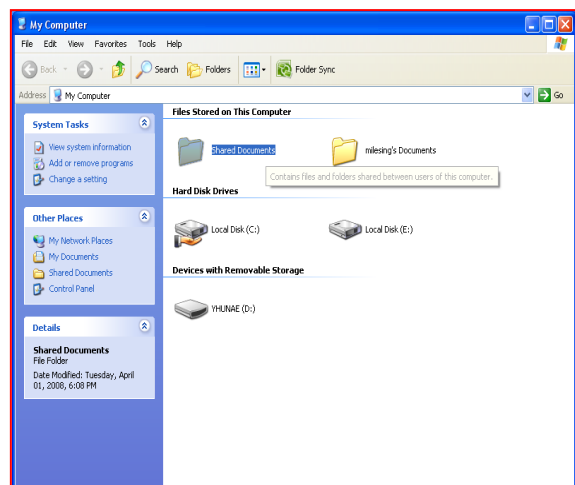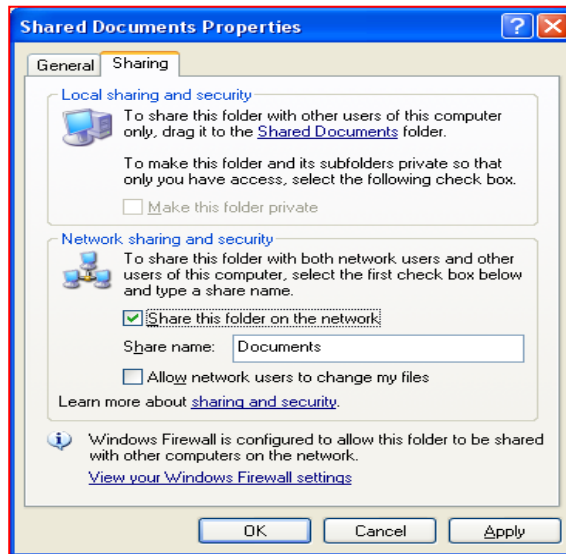

Figure 101. My Computer

Figure 102. Shared Document Properties

6. Open My Network Places- double-click the icon- and select the Entire Network option under Other Places at the left of the window. In the main (right-hand) pane, you should see one or more options. Double-click the Microsoft Windows Network icon.
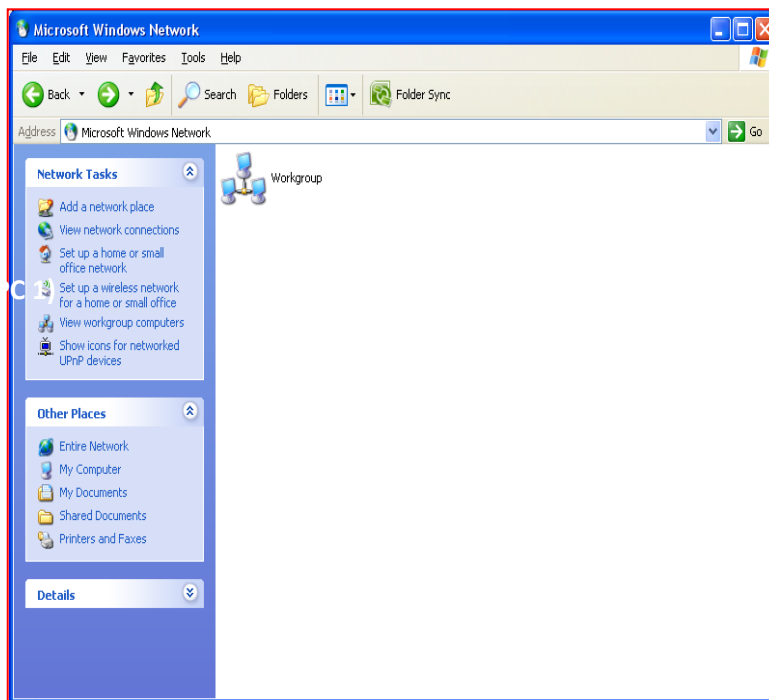

Figure 103. Microsoft Windows Network

Computer Hardware Servicing

7. You're now at the main network screen, where you should see what's called a workgroup. A workgroup is a basic group of computers connected to the same Ethernet network. Double-click the workgroup to see all the computers connected to your Ethernet network.
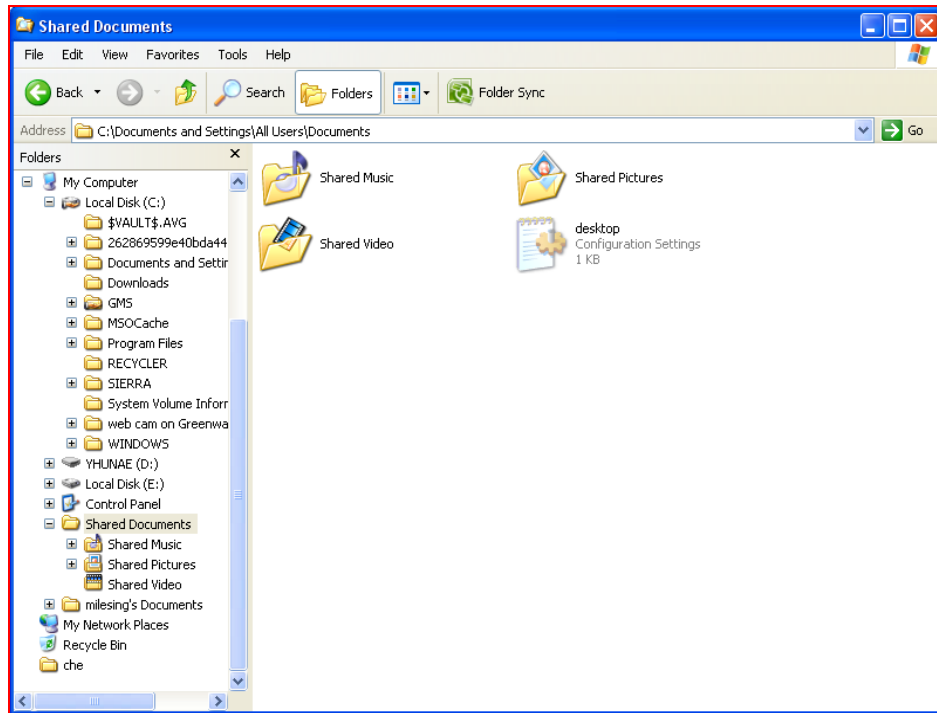

Figure 104. Shared Documents Window

At this point, you can access any of the other computers and see what folders they have shared. If you don't see any computer but your own, just wait a few minutes and refresh your screen. If you don't see other computers, then it's time to troubleshoot the network problems.

Printer Sharing

One of the primary reasons that networks were developed was to allow groups of computer users to share peripheral devices such as printer. Sharing a single printer among a group of users costs much less than buying a printer for each computer.

Low-cost printers usually require a separate print server to allow network connectivity because these printers do not have built-in network interfaces. The computer that is connected to the printer can serve as the print server. Most personal computer operating systems have built-in printer sharing capability.

Computer Hardware Servicing

Setting up printer sharing is simple with Windows XP. The following steps enable a computer to share a printer:

Step 1. Choose **Start > Printers and Faxes**.
Step 2. Right-click the printer, and choose **Properties**.
Step 3. Click the **Sharing** tab.
Step 4. Click the **Share this printer** radio button.
Step 5. Keep or change the share name.
Step 6. Click **Apply**.

All the computers that use the shared printer must have the correct drivers installed. Drivers for other operating systems can be installed on the print server.

To connect to the printer from another computer on the network, choose **Start > Printers and Faxes > Add Printer**. The Add Printer Wizard appears. Follow the steps using the wizard.

Essay Writing

Directions: Give an explanation on how you understand the subject. Provide at least 5 sentence response per item.

1. Cite the importance of file sharing and give an example scenario where its worth was proven.

_____
_____
_____
_____
_____

2. Cite the advantages and disadvantages of printer sharing.

Advantages	Disadvantages
Example Situation	Example **S**ituation

· What to REFLECT / UNDERSTAND

Read and Examine

Directions: Use other reference to understand more about printer sharing. Present your answer to the class.

1. What is a print server?
2. What are the functions of a print server?
3. What are the different types of print servers? Describe each.

Share a Folder, Share a Printer, and Set Share Permissions

Directions: In this activity, you will create and share a folder, share a printer, and set permissions for the shares. You will be given 30 minutes to complete the task. You will be rated based on the performance criteria provided below.

Recommended Equipment
- Two computers running Windows XP Professional that are directly connected to each other or through a switch or hub.
- A printer installed on one of the two computers.

Procedures:

Step 1
- ✓ Choose **My Computer > Tools > Folder Options**
- ✓ Click the **View** tab.
- ✓ Uncheck the "Use Simple File Sharing (Recommended)" checkbox, and then click **OK**.
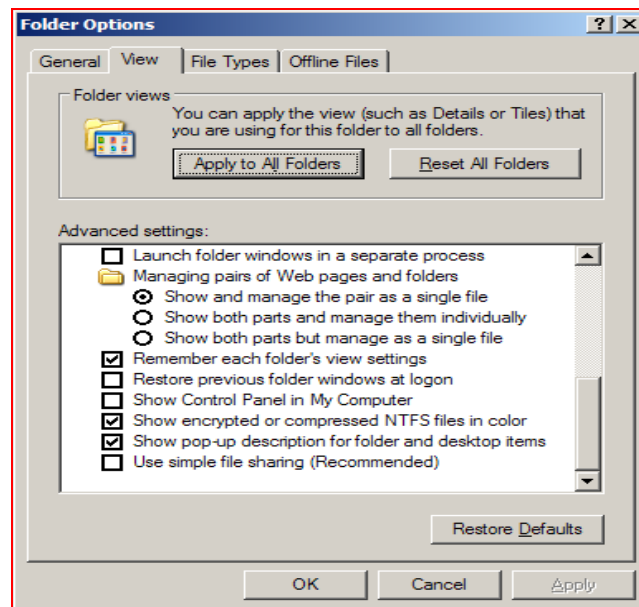

Figure 105. Folder Options Window

Step 2

- ✓ Right-click the **desktop**, and then choose **New > Folder**.
- ✓ Type **Example**, and then press the **Return** key.

- ✓ Open WordPad. Type "This is an example document".
- ✓ Save the file in the "Example" folder with the name "Brief.doc", and then close WordPad.

Step 3

- ✓ Right-click the **Example** folder, and then choose **Sharing and Security.**
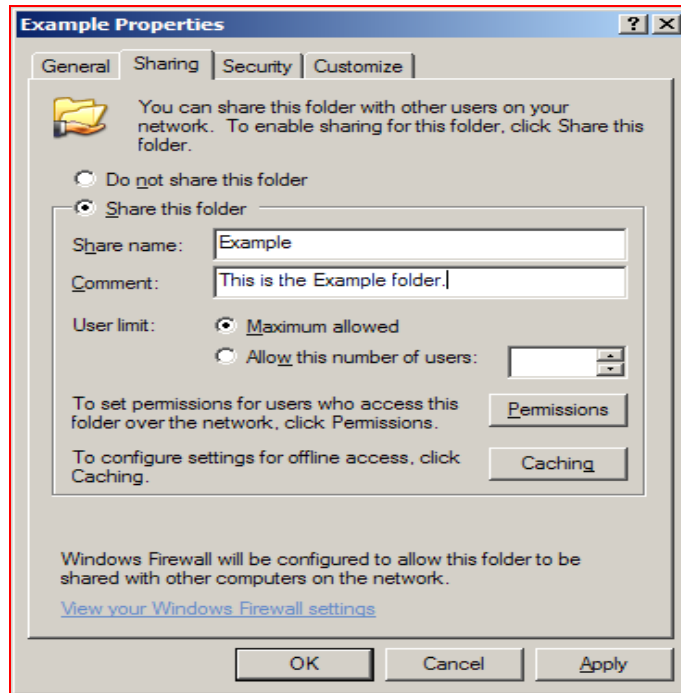- ✓ Click the **Share this folder** radio button, and then click **OK**.

Figure 106. Sharing Tab Window

- ✓ What is the icon of the "Example" folder?
- ✓ On the computer with the shared folder, right-click **My Computer**, and then click the **Computer Name** tab.

Step 4
- ✓ On the other computer, choose **Start > Run…**
- ✓ Type **\\computername\Example**, where computer name is the name of the computer with the "Example" folder, and then press the **Enter** key.
- ✓ Open the "Brief.doc" file.
- ✓ Delete the text in the "Brief.doc" file, and then choose **File > Save**.

✓ Click **OK**. Close WordPad, and then choose **NO** when prompted to save changes to the file.

Step 5

✓ Return to the computer with the shared folder.

✓ Right-click **Example folder > Sharing and Security**, and then click **Permissions**.

Step 6

✓ Open the Control Panel on the computer with the attached printer.

✓ Choose **Printers and Other Hardware > Printers and Faxes**.

✓ Right-click the icon of the installed printer, and then choose **Sharing…**.

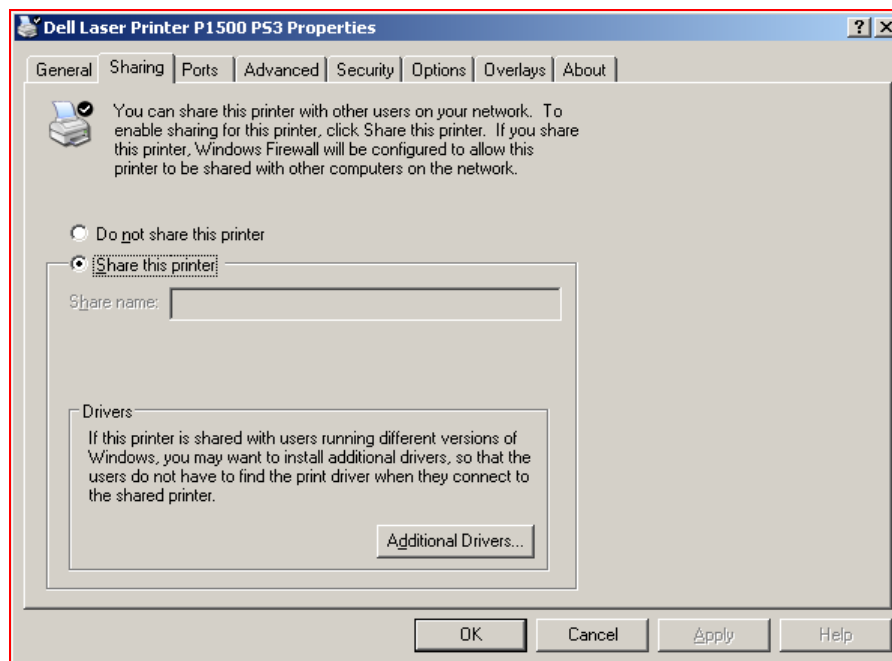✓ Click the **Share this printer** radio button, and then click **OK**.

Figure 107. Sharing Printer Tab Window

Step 7

✓ Return to the computer that is not directly connected to a printer.

✓ Open the Control Panel. Choose **Printers and Other Hardware > Printers and Faxes**.

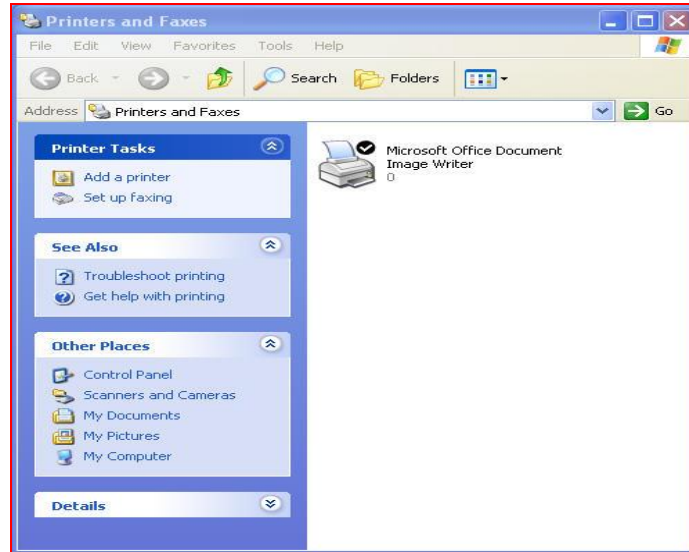✓ Choose **File > Add Printer** on the screen below.

Figure 108. Printer and Faxes Window

- ✓ The "Add Printer Wizard" window appears.
- ✓ Click **Next**.

Figure 109. Add Printer Wizard Window

- ✓ The Local or Network Printer of the Add Printer Wizard window appears. Click the **A network printer, or a printer attached to another computer** radio button, and then click **Next**.
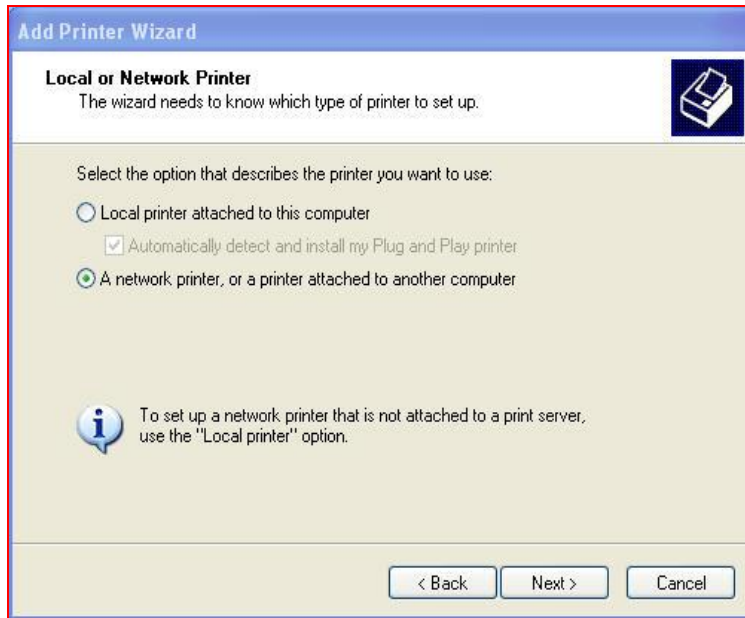
Figure 110. Local or Network Printer Option Window

✓ The "Specify a Printer" window appears.
✓ Click the **Connect to this printer** radio button, and then click **Next**.

Figure 111. Specify a Printer Window

✓ The Browse for a Printer window appears.
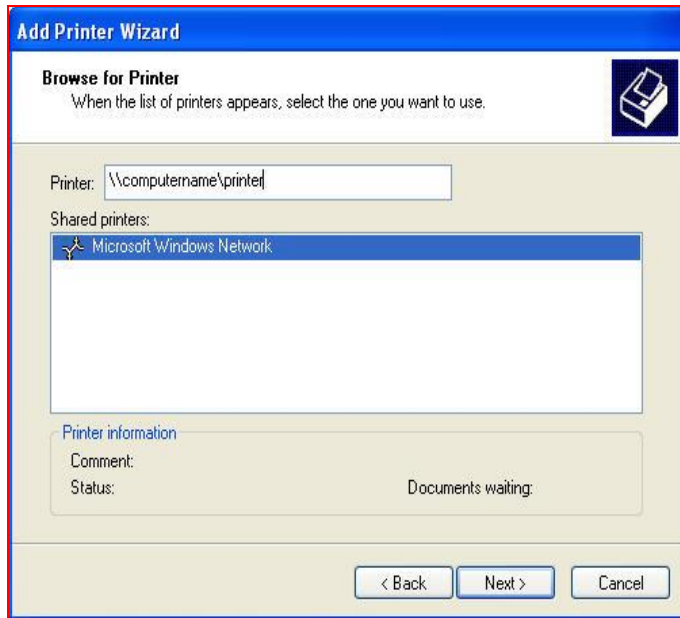
Figure 112. Browse for Printer Window

✓ Expand "Shared printers".
✓ Choose the printer from the list, and then click **Next**.
✓ The "Default Printer" screen of the "Add Printer Wizard" appears.
  Click **Next**.

Figure 113. Default Printer Screen

✓ The "Completing the Add Printer Wizard" window appears.

✓ Click **Finish**.

Figure 114. Completing the Add Printer Wizard Screen

Step 8
✓ Choose **Start > Printers and Faxes**.
✓ Right-click the printer you installed, and then choose **Properties**.
✓ The "Printer Properties" window appears.
✓ Choose the **General Tab**, and then click **Print Test Page**.

Figure 115. Printers and Faxes General Tab

✓ Click **OK** in the confirmation dialog box, and then click **OK** to close the printer properties window.
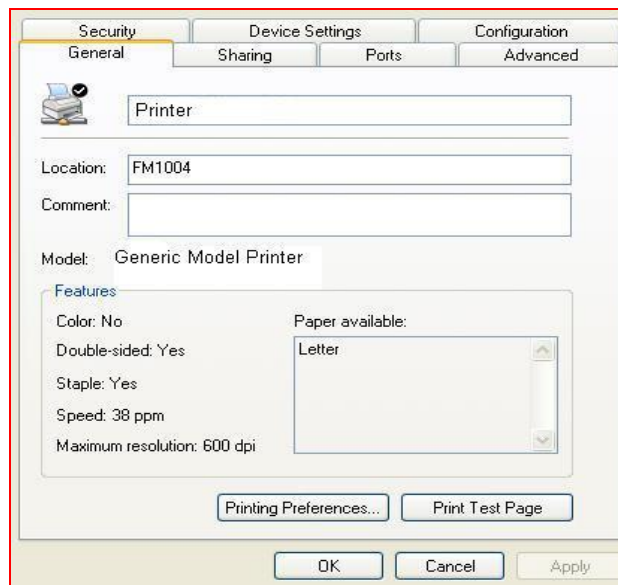
Step 9

✓ To test the functionality of file and printer sharing, you must be able to print a document or try the sample print feature of a printer.

Performance Rubrics for Sharing Files and Printer

CRITERIA	Excellent 4	Good 3	Fair 2	Poor 1
Safety Procedures (15%) -Applied/Observed safety precautions while working				
Adherence to the Procedures (30%) -Followed the procedures systematically				
Workmanship (15%) -Had organized materials and tools while accomplishing the task and has time management				
Functionality (40%) -Had set up a functional file and printer sharing system and was able to come up with a printed hard copy through it				

Computer Hardware Servicing

After having completed the configuration phase, you are now ready to face final chapter of configuration which is inspecting and testing configured computer system and networks. The lessons in this segment will focus on the guidelines and methods on inspecting and testing of computer system and networks. So at the end of this lesson you should be able to:

- ✓ follow OHS procedures in testing configured computer system and networks;
- ✓ testing configured computer system and networks; and
- ✓ accomplish a technical report.

Lesson 3. Inspect and Test Configured Computer System and Network

In general, testing is finding out how well something works. For human beings, testing tells what level of knowledge or skill has been acquired. In computer hardware and software development, testing is used at key checkpoints in the overall process to determine whether objectives are being met. For example, in software development, product objectives are sometimes tested by product user representatives. When the design is complete, coding follows and when finished, this is then tested at the unit or module level by each programmer; at the component level by the group of programmers involved; and at the system level when all components are combined together. At early or late stages, a product or service may also be tested for usability.

Safety Precautions

Occupational Health and Safety (OHS) Policy – An Information and Communication technology (ICT) student should know how to behave when working in the computer laboratory, and to accomplish task safely. Safety practices should be learned early and always adheres in working with any electrical and electronic device, including personal computers and its peripherals. This is for your protection as well as to the people working with you, and for the devices that you are using.

Occupational safety and health (OSH) is a planned system of working to prevent illness and injury where you work by recognizing and identifying hazards and risks. Health and safety procedure is the responsibility of all persons in the computer and technology industries**.** You must identify the hazards where you are working and decide how dangerous they are. Eliminate the hazard or modify the risk that it presents.

Occupational Health and Safety standards

Each student has a responsibility to their colleagues and their organization to report and act upon any potential workplace hazard. Students need to be aware of the *type of hazards* that are possibly present in their work environment.

Procedure

1. Identify the hazard.
2. Clear the area close to the hazard.
3. Partition the hazard off or clearly identify the area to protect other people from harm.
4. If the hazard can be easily and safely cleared, then do so.

If not…

5. Report the hazard to the appropriate person (such as teacher in charge, principal etc.) to obtain assistance.
6. After clearing the hazard, fill out the correct documentation to assist in identifying improved practice to reduce further incidence of hazards.

All hazards must be reported using an *Accidental Report form*. This enables us to track the kinds of hazards we have in our workplace, and take action when necessary to make it safer for all student and clients.

Accident Reports

Forms are used to give specific details with regards to accidents that happened in the laboratory during experiments.

Accident reports contain the following details:

- Name of the person injured
- Date and time of the accident
- Type of injury
- First aid given
- Action taken to prevent further accidents

Accident Report Sample Form

Form No:	**Accident Report Form**	Date:
		Rm. No:
Name:		Yr/Sec:
Type of Injury	Cause of Injury	Remedy

Hazardous substances

If the workplace hazard appears to be dangerous to staff and clients and professional assistance is required:

A. Call the supervisor or manager and advise them of the problem and the urgency of the matter.

B. Depending on the risk, an evacuation may be called.

C. Follow the evacuation procedure.

D. The supervisor or manager will call in the fire brigade or specialized personnel who will deal with the spill.

Fire Exits

All fire exits should be kept clear from any obstacles. All students have a responsibility to make sure that chairs, empty boxes or any other type of obstacle are not placed in or near fire exit doorways.

All corridors also need to have equipment stored on one side only to ensure that in the event of an emergency there is a clear exit.

Fire Safety Procedure

Each work area has a designated fire warden, who in the event of a fire will take charge. They are recognized by the use of the red hard hat they wear.

If you find the fire:

- Assess the danger prior to doing anything.
- If it is safe, assist anyone to move away from the vicinity of the fire.
- If it is possible, close the door to the fire area.
- Call for assistance. Verbally call FIRE, FIRE, in a loud and clear voice.
- Break the glass section of the fire alert call point.
- Call to the switch; ensure you know where the fire is, any other details that may be of assistance to the fire brigade. Details could be size of the fire, cause or type of fire, any people hurt or trapped, has anyone tried to put it out.
- If it is safe to do so, put out the fire with the correct extinguisher or fire hose.

If the designated fire officer is not present, someone quickly needs to take responsibility and:

1. Locate the source of the fire.
2. Locate any people.
3. Remove all people from the building.
4. Once outside, do a head count.
5. Notify the authorities.

Personal Safety While Working with PCs

Computer equipment can be dangerous, and you or others can be injured or even killed if you don't follow proper safety guidelines when working along with PCs. The following are some precautionary measures to take before working with any computer equipment:

- Wear shoes with non-conductive rubber soles to help reduce the chance of being shocked or seriously injured in an electrical accident.
- Do not work on components that are plugged into their power source.
- Do not remove expansion cards from a computer when it is turned on.
- Remove jewelries when working inside any computer-related equipment.
- Be sure not to pour water on electronic components.

•What to KNOW

Guidelines for Testing Configured Computer System and Network

Testing Your Computer Network

You've set up all your network switches, plugged in all the cables, and configured all your computers. One task remains before you can declare your network is finished: You must verify that the network works as expected.

Here are a few simple tests you can conduct to make sure your network is functional:

- **Check the physical connections.**

Check that the Link light — the little red or green light next to the RJ-45 port — is lit on every computer. You must check this light both on the computer itself and on the switch or router the computer is plugged into. If this light is not on, you have a connection problem — most likely a bad cable.

Computer Hardware Servicing

- **Verify that you can log in.**

   When you're sure the physical connections are good, you should attempt to log in to each of your network computers using a valid domain user account.

- **Check the network configuration.**

   Click the Start button, type cmd and press Enter. Then, enter the command ipconfig /all and press Enter.

   This command will spit out numerous lines of information. The line you're looking for should resemble this:

   IPv4 Address. . . . . : 192.168.1.125 (Preferred)

   If this part of the output does not show a valid IP address, you need to check that your IP configuration is set correctly and that your DHCP server is working.

- **Verify that the computers can ping each other.**

   Another basic test you should perform is to use the ping command from a command prompt to make sure that the computers on your network can contact one another.

   Do several ping tests. First, make sure that TCP/IP is up and running by having the computer try to ping itself. Open a command prompt and type ping local host. The output from this command will indicate whether or not the ping was successful.

   Next, try to ping your servers by name. For example, if your file server is named FileServer01, use the command ping FileServer01.

Writing a Technical Report on Test Conducted

Technical Report is any document that records the procedure adopted and results obtained from a scientific or technical activity or investigation. Use the following format for a technical report for your recently conducted test.

TECHNICAL REPORT ON TEST CONDUCTED

Name of Technician:_____

Date of Inspection: _____ **Time:** _____

Device Tested:	
Specification:	
Diagnosis:	
Action Taken:	
Remarks:	

Testing the Wireless NIC

Directions: In this activity, you will check the status of your wireless connection, investigate the availability of wireless networks, and test connectivity. After accomplishing the task you need to write a technical report regarding the test conducted.

Recommended Equipment

- A computer with Windows XP Professional installed
- A wireless NIC installed
- An Ethernet NIC installed
- Linksys WRT300N Wireless Router
- Internet connectivity

Step 1

- ✓ Disconnect the Ethernet patch cable from your computer.
- ✓ A red "X" appears over the "Local Area Connection" icon.

Figure 116. Local Area Connection- A Network Cable is Unplugged

- ✓ Hover over the "Wireless Network Connection" icon in the tray.

Figure 117. Wireless Network Connection Icon in System Tray

- ✓ Open a command window.
- ✓ Ping **127.0.0.1**.

Figure 118. Ping 127.0.0.1

✓ Use the ipconfig command.
✓ Get IP address of the default gateway.
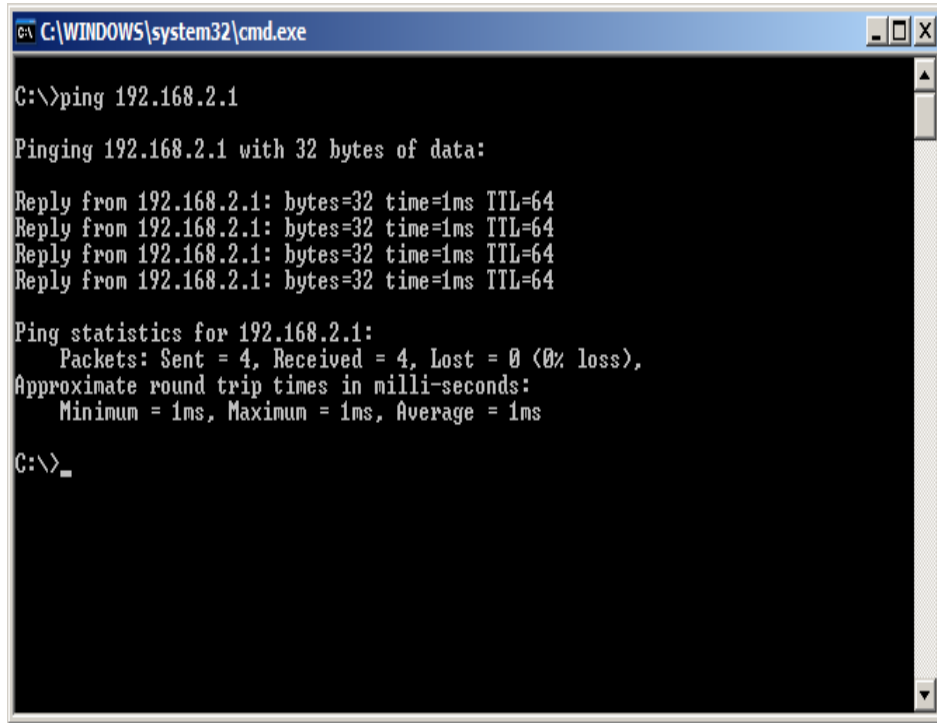
Figure 119. Ipconfig window

Computer Hardware Servicing

✓ Ping the default gateway.

Figure 120. Ping the Default Gateway

✓ A successful ping indicates that there is a connection between the computer and the default gateway.

Step 2

✓ Open a web browser.
✓ Type **www.google.com** in the "Address" field, and then press **Return**.

Step 3

✓ Open the **Network Connections** window.
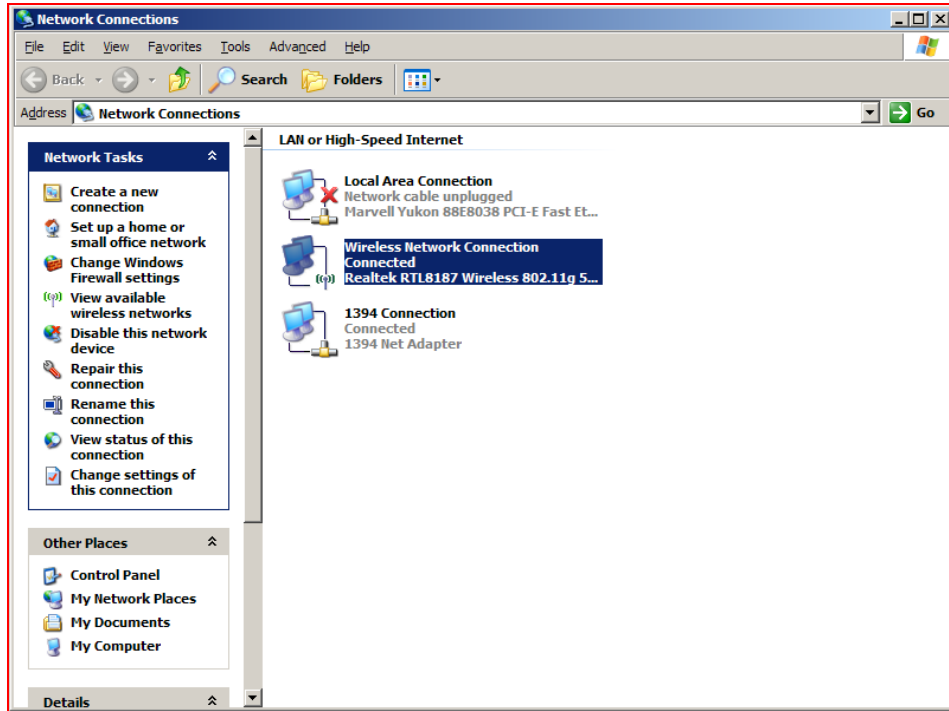
Figure 121. Network Connections Window

✓ Right-click the wireless connection and choose **Properties**.
✓ Click the **Wireless Networks** tab.
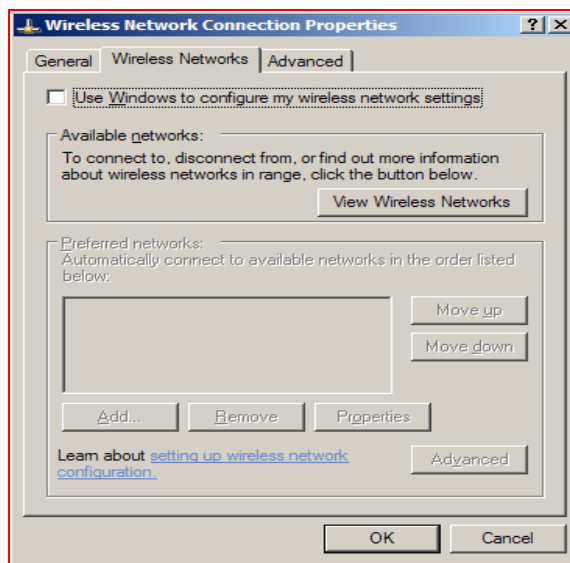
Figure 122. Wireless Networks Tab

✓ Click the **View Wireless Networks** button.

Computer Hardware Servicing

TECHNICAL REPORT ON TEST CONDUCTED

Name of Technician:_____
Date of Inspection: _____ **Time:** _____

Device Tested:
Specification:
Diagnosis:
Action Taken:
Remarks:

Computer Hardware Servicing

A.   Paper and Pencil Test

General Directions: Read the items very carefully. Write your answer in a clean sheet of paper.

Test I. True or False

Directions: Write TRUE if the proceeding statement is correct and FALSE if otherwise.

_____1. A safe workplace is clean, organized and well-lit.

_____2. One must unplug the power from the source before opening a case and performing services.

_____3. It is a best practice that a fire extinguisher and first aid kit must be available in the workplace.

_____4. You are allowed to open the power supply or a monitor.

_____5. You can bring food and drinks inside the laboratory.

_____6.The key to a well-tuned computer system is proper configuration.

_____7. Boot log stores all information from the boot process.

_____8. Registry is a collection of database of configuration in Windows operating system.

_____9. The shortcut of Microsoft Configuration is ipconfig.

_____10. Configuration is the way a system is set up.

Test II. Multiple Choice

Direction: Write the letter of the correct answer.

1. What boot configuration utility allows setting the programs that will run at startup?
     a. Ipconfig   c. msconfig
     b. regedit   d. dxdiag
2. What application allows you to edit the registry?
     a. Ipconfig   c. msconfig
     b. regedit   d. dxdiag
3. Which of the following enables you to test sound and graphics output?
     a. Ipconfig   c. msconfig
     b. regedit   d. dxdiag
4. Which of the following is an applet that controls the look of windows?
     a. Appearance and themes   c. Performance and Maintenance
     b. Network and Internet   d. Sounds, Speech and Audio

5. Which of the following applets does not belong to Performance and maintenance category?
    a. Administrative tool
    c. Power Options
    b. Automatic Updates
    d. System
6. Which of the following wizard is used to configure windows for vision, hearing and mobility needs?
    a. Accessibility Option
    c. Sounds, speech and audio
    b. Security Center
    d. User Accounts
7. A tab in direct X Diagnostic tool that displays your current audio settings.
    a. Input
    c. Sound
    b. Music
    d. System
8. Which of the following is the most commonly used networking cable category?
    a. Cat3
    c. Cat 5 and 5e
    b. Cat 5
    d. Cat 6
9. What do you call a copper-cored cable surrounded by a heavy shielding?
    a. coaxial cable
    c. optical fiber
    b. fiber optics
    d. twisted pair
10. What Ethernet cable is used to connect two devices directly?
    a. Cross-Over
    c. both A and B
    b. Straight-through
    d. None of the options
11. Which of the following is a number used to identify a device on a network?
    a. Default gateway
    c. IP address
    b. DNS Server
    d. subnet mask
12. In which of the following IP address does 192.168.1.105 belong?
    a. Class A
    c. Class C
    e. Class E
    b. Class B
    d. Class D
13. What command is used to test the ability of the source computer to reach a specified destination computer?
    a. Ipconfig
    c. Ping
    b. Msconfig
    d. Regedit
14. What do you call an approach to computer networking where all computers show equivalent responsibility for processing data?
    a. Client server
    c. Peer-to-client
    b. Peer to peer
    d. None of the options
15. Which of the following is an example of Class A subnet mask?
    a. 255.0.0.0.
    c. 255.255.255.0
    b. 255.255.0.0.
    d. 255.255.255.255

Test III. Matching Type

Direction: Match Column A with Column B.

A	B
1. Copper cabling used for telephone communication	a. Crimping tool
2. Standard Ethernet cable	b. Cross- over
3. Cable that has a very thin core	c. Fiber- optic
4. Cable that has a thicker core	d. Ipconfig
5. Tool used for crimping RJ45	e. Multi- mode
6. Connector for Cat 5e cable	f. Ping
7. Set of rules	g. Protocol
8. Indicates the network portion of an IP address	h. RJ45
9. Command used find out the ip address	i. Single- mode
	j. Straight-through
10. Glass or plastic conductor	k. Subnet mask
	l. Twisted pair

Test IV. ACRONYMS

Direction: Give the complete meaning of the following acronyms.

1. UTP
2. STP
3. IP
4. TCP /IP
5. HTTP
6. FTP
7. SSH
8. IMAP
9. SMTP
10. DHCP
11. DNS
12. TTL
13. LAN
14. VPN
15. NIC

B. **Skills Checklist**

Configuration Skills

Directions: Listed below are the most important skills one must have in order to configure computer systems and networks. The matrix lists the skills expected you to master. Check the appropriate column which describes the level of your confidence with the given skills.

Configuration Skills	I can do it confidently 3	I can do it but with assistance 2	I am not confident 1
1. I can use the different tools for configuration.			
2. I can inspect networking devices and connectors.			
3. I can create a cross-over and straight-through Ethernet cable.			
4. I can test the functionality of an Ethernet cable.			
5. I can assign and configure IP address.			
6. I can execute the ipconfig command properly.			
7. I can manage to create a peer-to-peer networking.			
8. I can configure Network Interface Card using DHCP.			
9. I can enable firewall			
10. I can configure file and printer sharing.			
TOTAL			
GRAND TOTAL			

Add all the scores to get the grand total and then divide it by the total number of items. Refer to the verbal interpretation on the next page to determine your initial configuration ability.

Computer Hardware Servicing

Numerical and Verbal interpretation

Numerical Value	Verbal Interpretation
2.51 – 3.00	Confident
1.76- 2.50	Confident but needs assistance
1.00 – 1.75	Not yet Confident