

CertExams.com Lab Manual For Comptia® A+ Certification Exam

INTRODUCTION: To load or view any lab , please go to the left pane, and expand the topic by clicking on the “+” sign. Then, click on a given lab to “load” or “view” the lab. After loading the lab, you would be able to complete the lab instructions.

CONTENTS

1.PC Hardware

1.1 Identifying motherboard components

- 1.1.1 [Identify the components of an ATX \(Micro ATX\) motherboard](#)
- 1.1.2 [Identifying the display connector types](#)
- 1.1.3 [Identify the SATA2 connectors in a motherboard \(hotspot\)](#)
- 1.1.4 [Identify the PCI slots in a motherboard \(hotspot\)](#)
- 1.1.5 Identify the CMOS battery in a motherboard (hotspot)
- 1.1.6 Identify the 24-pin ATX power connector in a motherboard (hotspot).

1.2 Identifying DDR2/3 , SODIMM , and other memory modules

1.3 Identifying the features of memory types (such as DDR3 , DDR2 etc.)

1.4 Identify the components of Mini ITX motherboard

1.5 Identifying DDR3 DIMM and inserting it into a motherboard slot

1.6 Identify the graphics card and insert it into appropriate slot on the motherboard

1.7 Installing SATA hard drive to appropriate slot on the motherboard

1.8 Objective Test 1.

2. Networking

2.1 [Identifying Base-T Ethernet standards \(such as 802.2e , 802.3i etc. \) and their names](#)

2.2 [Arrange the color codes of the T568B connector in the correct order.](#)

2.3 [Identifying the fiber connector types \(such as ST , SC, FC etc\)](#)

2.4 Identifying the port numbers of a TCP/IP protocols

2.5 Identifying the features of TCP/IP protocols (such as HTTP, SMTP etc.)

2.6 Identifying functions of IPconfig labels (such as ipconfig , ipconfig/all etc.).

2.7 Identify the private IPv4 address.

2.8 Identifying speed ranges of 802.11 standards

2.9 Identifying characteristics of Internet WAN technologies

- 2.10 Identifying the network characteristics managed by QoS (such as Bandwidth , Jitter etc.)
- 2.11 Identifying twisted pair cable types(such as CAT3 , CAT5 etc.) with their speeds
- 2.12 Compare shielded vs unshielded twisted-pair cables
- 2.13 Identifying the IPv6 link local address
- 2.14 Objective Test 2

3. Laptops

- 3.1 Accessing special keyboard functions with the Fn key.
- 3.2 Objective Test 3.

4. Printers

- 4.1 Identify the basic components of a Laser printer
 - 4.1.1 Identify the laser printer components -1
 - 4.1.2 Identify the laser printer components - 2
 - 4.1.3 Identify the laser printer components - 3
- 4.2 Identifying the characteristics of various printer types (such as Laser , Inkjet etc.)
- 4.3 Identifying features of Laser printer components
- 4.4 Identifying features of laser printing process (such as cleaning, writing etc)
- 4.5 Objective Test 4.

5. Operating Systems

- 5.1 Identifying features (such as Event viewer , Bit-locker etc.) of windows OS
- 5.2 Identifying the features of networking command line tools (such as Copy , SFC etc.)
- 5.3 Identifying the Processes tab function of Windows Task manager in Windows 10/11 PC.
- 5.4 Identifying the options to open Local Users and Groups (Local) window in Windows 10/11 computer.
- 5.5 Identifying functions of “User and Groups” options in windows 10/11 PC
- 5.6 Identifying the features of NTFS permissions and Share permissions.
- 5.7 Identifying the System action resulting from different combinations of the duplex and speed modes.
- 5.8 Identifying the Recovery Console command tools and their respective features
- 5.9 Identifying the MSCONFIG options and their respective functions/features
- 5.10 Identifying the features of File attributes (such as Read-Only , System(S) etc.)
- 5.11 Identifying the windows OS “Power Options” and their features.
- 5.12 Identifying the features of File system types (such as FAT16 , FAT32 etc.)
- 5.13 Identifying the characteristics of Operating System Administrative tools
- 5.14 Identifying the features of Command line utilities (such as MSCONFIG,MMC) of Windows OS
- 5.15 Identifying features of Windows OS types
- 5.16 Identifying the display standards of Windows OS and their resolutions
- 5.17 NTFS permissions and Share permissions in Windows 10
 - 5.17.1. To share folders with other users on your network
 - 5.17.2. To change read only attributes on files and folders

5.17.3. To set, view, change, or remove file and folder permissions

5.18 Configuring Local Security Policy in Windows 10

5.18.1 Setting Account lockout policy

5.18.2 Setting Password policy

5.19 Configuring hardware settings using Device Manager

5.20 Troubleshooting startup issues using Bootrec.exe tool in windows RE(Recovery Environment)

5.21 Disabling start up program in Windows 10

5.22 Connecting to remote desktop in Windows 10

5.23 Changing the refresh rate in Windows 10

5.24 Changing Power Plan Settings in Windows 10

5.25 Creating new user account in Windows 10

5.26 Changing user account control settings in Windows 10

5.27 Changing user account password in Windows 10

5.28 Removing user account in Windows 10

5.29 Changing user account type in Windows 10

5.30 Creating a system image backup of Windows 10

5.31 Setting up and uploading files to OneDrive in Windows 10

5.32 Backup files to another drive in Windows 10

5.33 Restore the files backed-up before in Windows 10

5.34 Formatting hard drive in Windows 10

5.35 Turning On/Off BitLocker for Data Drive in Windows 10

5.36 Installing/Updating graphic card driver in Windows 10

5.37 Manage Location services in Windows 10

5.38 Manage app permissions for camera in Windows 10

5.39 Auto Lock using Screen Saver in Windows 10

5.40 Uninstall or remove apps and programs in Windows 10

5.41 To stop automatic updates in Windows 10

5.42 Objective Test 5

5.43 Microsoft Teams Labs

5.43.1 Creating a team using Microsoft Teams

5.43.2 Joining a meeting using Microsoft Teams

6. Security

6.1 Identifying Security threat features - 1(such as Malware , Spyware etc.)

6.2 Identifying Security threat features - 2 (such as Viruses , Worms etc.)

6.3 Identifying functions of digital security methods (such as Antivirus , Firewall etc.)

6.4 Identifying various features of physical security methods (such as Tokens , Biometrics etc.)

6.5 Identifying various features of data destruction/disposal methods (such as Low level format , Standard format etc.)

6.6 Set SSID on a generic WAP router.

6.7 Disabling SSID broadcast using the simulator.

6.8 Enabling the MAC address filtering in the WAP device.

6.9 Configure security encryption to WPA 2 with pass phrase

6.10 Pinging to DHCP server

6.11 Configuring Wireless Security on an Access Point (WEP)

6.12 Objective Test 6

7. Mobile Devices

7.1 Identifying the various methods to secure mobile devices (such as Passcode locks , Remote wipes etc.)

7.2 Steps to configure Email on android and iphone devices

7.3 Identifying the features of mobile devices (such as ARM , Bluetooth etc.)

7.4 Identifying basic features of mobile operating system (such as ACPI , OSPM etc.)

7.5 Connecting smart phone to a wireless network

7.6 Connecting smart phone to PoP3 email server

7.7 Objective Test 7

8. Troubleshooting

8.1 Identify the troubleshooting tools

8.2 Identifying the functions of various troubleshooting tools (such as Fixmbr , Fixboot etc.)

8.3 Identify the networking troubleshooting command

8.4 Troubleshoot WiFi connection on a Windows Workstation

8.5 Configuring IP address, subnet mask, default gateway statically on a Windows client

8.6 Objective Test 8

9. Appendix

9.1 Installing PATA/IDE drives

9.2 Installing SATA drive

9.3 SCSI drives

9.4 Inserting a memory card and reading its contents

9.5 Degaussing a CRT

9.6 Changing the relative position of the second monitor and changing its resolution to match native resolution

9.7 Stripping and terminating RJ-45 connector

9.8 Installing laptop memory

9.9 Replacing a laptop hard drive

9.10 Using a wireless toggle switch on a laptop to enable the NIC

9.11 Inserting and removing a PC Card (Card Bus or Express Card)

9.12 Using a docking station.

9.13 Replacing the laptop battery

9.14 Flushing the laptop's BIOS

9.15 Installing and sharing a printer and then testing its functionality

9.16 Changing the toner cartridge.

9.17 Troubleshoot hard drives and RAID arrays with appropriate tools

9.18 Troubleshoot printers with appropriate tools

9.19 Troubleshoot, and repair common laptop issues while adhering to respective features

9.20 Troubleshoot common problems related to motherboards, RAM, CPU and power with appropriate tools

9.21 Troubleshoot common video and display issues

9.22 User account creation , configuration and authentication in Windows 7

- 9.23 [Configuring windows 7 power options](#)**
- 9.24 [Configuring windows 7 update settings](#)**
- 9.25 [Configuring Local Security Policy in Windows 7](#)**
- 9.26 [Configuring hardware settings using Device Manager](#)**
- 9.27 [Disabling Startup Programs in Windows 7](#)**
- 9.28 [Changing the refresh rate in Windows 7](#)**
- 9.29 [Connecting to a remote desktop using windows 7](#)**

1. PC Hardware

1.1.1: Identify the components of an ATX (Micro ATX) motherboard -2

Description: This lab exercise helps to identify the parts of an ATX motherboard.

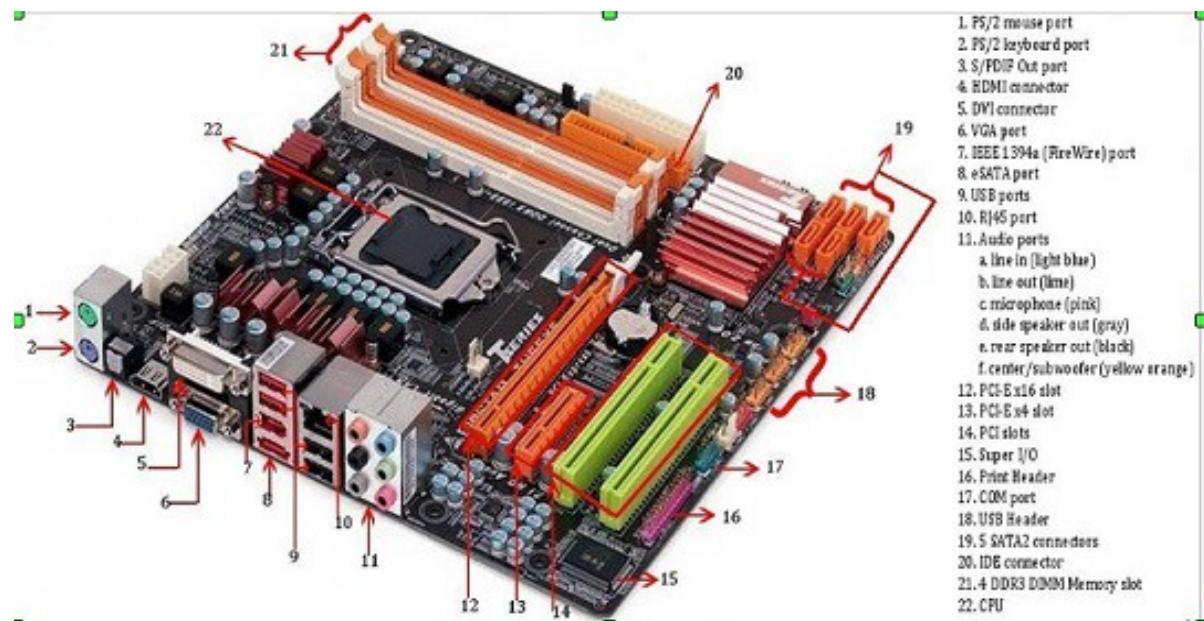
Instructions: 1. Part of an ATX motherboard figure is given below. Different parts are labeled as A, B, C, D, and E.

2. Drag and Drop the name of the components to their respective places.



Explanation:

Various motherboard parts are as shown in fig. below (BIOSTAR TH55XE MicroATX).



Below fig. Shows after dragging and dropping correct options on the image.



[Back](#)

1.1.2: Identifying the display connector types

Description: This lab exercise helps to identify the different display connector types.

Instructions: 1. Below figure shows the different display connector types labeled as A, B, C, D, E, F
 2. The name of the connector types are given as options.
 3. Drag and drop the name of the connector types to their respective places.

Explanation:

VGA: A Video Graphics Array (**VGA**) connector is a three-row 15-pin DE-15 connector. The 15-pin VGA connector was provided on many video cards, computer monitors, laptop computers, projectors, and high definition television sets. On laptop computers or other small devices, a mini-VGA port was sometimes used in place of the full-sized VGA connector.

HDMI(High-Definition Multimedia Interface) is a proprietary audio/video interface for transmitting uncompressed video data and compressed or uncompressed digital audio data from a Compliant source device, such as a display controller, to a compatible computer monitor, video projector, digital television, or digital audio device. HDMI is a digital replacement for analog video standards.

BNC Connector: The **BNC connector** is a miniature quick connect/disconnect radio frequency connector used for coaxial cable. BNC connectors are used with coaxial cable in radio, television, and other radio-frequency electronic equipment, test instruments, and video signals. The BNC was commonly used for early computer networks such as ARCnet, and the 10BASE2 variant of Ethernet. BNC connectors are made to match the characteristic impedance of cable at either 50 ohms or 75 ohms.

Display Port: **DisplayPort** is a digital display interface developed by the Video Electronics Standards Association (VESA). The interface is primarily used to connect a video source to a display device such as a computer monitor, though it can also be used to carry audio, USB, and other forms of data.

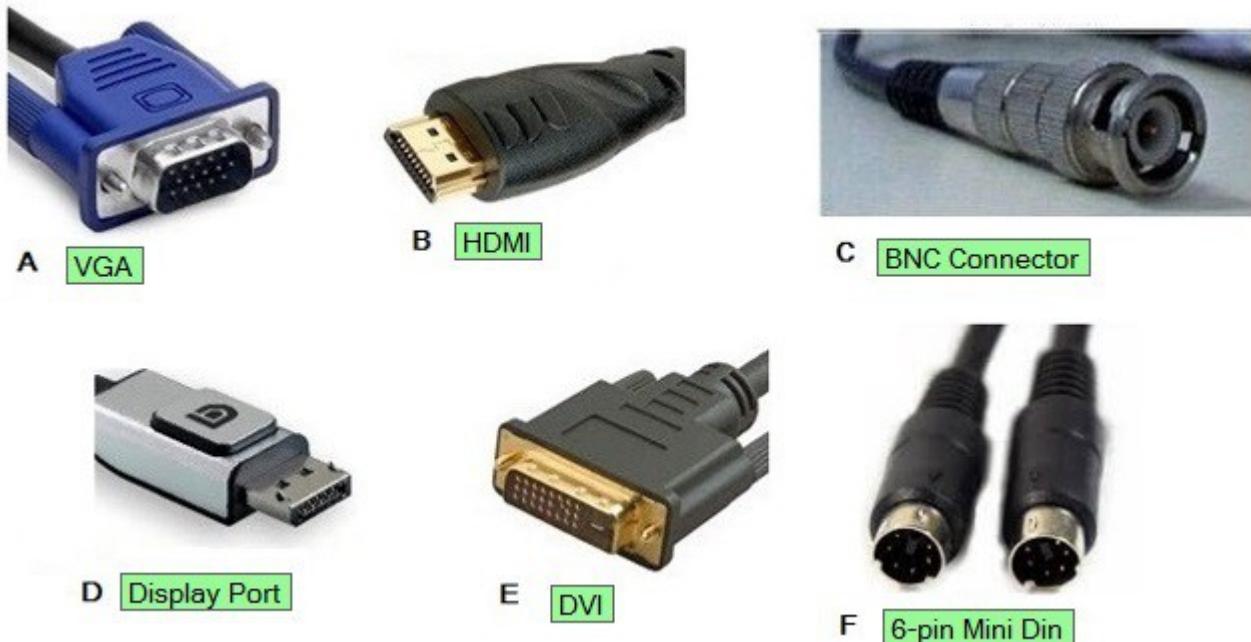
Display Port is backwards compatible with VGA, DVI and HDMI through the use of passive and active adapters.

Digital Visual Interface (DVI) is a video display interface developed by the Digital Display Working Group (DDWG). The interface is designed to transmit uncompressed digital video and can be configured to support multiple modes such as DVI-A (analog only), DVI-D (digital only) or DVI-I (digital and analog). The DVI

specification is compatible with the VGA interface. Although DVI is predominantly associated with computers, it is sometimes used in other consumer electronics such as television sets and DVD

6-Pin Mini Din Connector : The **mini-DIN** connectors are a family of multi-pin electrical connectors used in a variety of applications. Mini-DIN is similar to the larger, older DIN connector. Mini-DIN connectors are 9.5 mm in diameter and come in seven patterns, with the number of pins from three to nine. Each pattern is keyed in such a way that a plug with one pattern cannot be mated with any socket of another pattern.

Below fig. shows after dragging and dropping correct options on the image.



[Back](#)

1.1.3: Identify the SATA2 connectors in a motherboard (hotspot)

Description: This lab exercise helps to identify the SATA2 connector in a motherboard.

Instructions: 1. An ATX motherboard figure is given below

2. Click on the SATA 2 connector(s), if the clicked location is correct it indicates green mark, otherwise it indicates the red mark.



Explanation:

SATA is the faster serial version of the original parallel ATA (PATA) interface. Both SATA and PATA are "integrated drive electronics" (IDE) devices, which means the controller is in the drive, and only a simple circuit is required on the motherboard.

Serial ATA (Advanced Technology Attachment) (SATA) is a computer bus interface that connects host bus adapters to mass storage devices such as hard disk drives and optical drives.

Serial ATA replaces the older PATA, offering several advantages over the older interface: reduced cable size and cost (seven conductors instead of 40), native hot swapping, faster data transfer through higher signaling rates, and more efficient transfer through an (optional) I/O queuing protocol.

SATA host adapters and devices communicate via a high-speed serial cable over two pairs of conductors. To ensure backward compatibility with legacy ATA software and applications, SATA uses the same basic ATA and ATAPI command-set as legacy ATA devices.

Version	Bi-Directional speed	Year of introduction
SATAI	1.5Gbps	2002
SATAII	3.0Gbps	2003
SATAIII	6.0Gbps	2008

The below figure shows the SATA connector.



[Back](#)

1.1.4: Identify the PCI slots in a motherboard (hotspot)

Description: This lab exercise helps to identify the PCI slots in the motherboard.

Instructions: 1. An ATX motherboard figure is given below

2. Click on the PCI slots, if the clicked location is correct it indicates the green mark, otherwise it indicates the red mark.



Explanation:

A PCI or Peripheral Component Interconnect slot is a slot used to connect additional extension cards to a PC. PCI provides a shared data path between the CPU and peripheral controllers, such as the network and display.

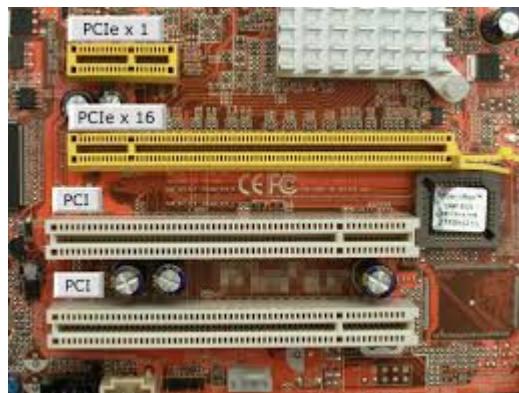
adapter (graphics card). However, with so many controller circuits built into the motherboard, the need for extra PCI slots in a PC has diminished considerably. Sound cards, TV tuners or modems are some examples of devices that use PCI slots.

Speed of PCI slot ranges from 133 megabytes/second of the PCI 2.0 up to 128 gigabytes/second for the PCI Express. Conventional PCI also has Plug and Play capabilities. PCI slots also use Error Correction Codes, or ECC, a technology that's also used in RAM memory modules to improve data integrity.

There are three types of PCI standards: Conventional PCI, PCI-X and PCI Express. Conventional PCI and PCI-X share the same architecture but have different features and specifications.

PCI-X is a generalization of the fast/wide/fast-wide variations. It uses the same physical slots as conventional PCI, but can negotiate speeds of 100MHz, 133MHz, 266MHz, or even 533MHz. There is also a narrow version of the slot - physically narrow, not the data width.

PCI-Express : This was originally called 3GIO. It is supposed to be "software compatible" with previous PCI standards, but it is otherwise completely different. The slots are smaller, and come in a variety of lengths. Signaling is both serial and parallel. There is serial signaling on each line, at 2.5GHz with an 8bits in 10bits encoding; and you can have up to 16 lines. It is also full-duplex - you can send data in both directions simultaneously. The different widths of PCI-Express are upwards compatible - cards should work in any slot equal to or wider than their own size. A 1x card should work in any width slot, a 4x card should work in 4x, 8x, and 16x slots, and so on.



[Back](#)

1.1.5: Identify the CMOS battery in a motherboard (hotspot).

Not Available in Demo Version

1.1.6: Identify the 24 pin ATX power connector in a motherboard (hotspot).

Not Available in Demo Version

1.2 Identifying DDR2/3 , SODIMM , and other memory modules

Not Available in Demo Version

1.3 Identifying the features of memory types (such as DDR3 , DDR2 etc.)

Not Available in Demo Version

1.4 Identify the components of Mini ITX motherboard

Not Available in Demo Version

1.5 Identifying DDR3 DIMM and inserting it into a motherboard slot

Not Available in Demo Version

1.6 Identify the graphics card and insert it into appropriate slot on the motherboard

Not Available in Demo Version

1.7 Installing SATA hard drive to appropriate slot on the motherboard

Not Available in Demo Version

1.8 Objective Test 1. Answer the following questions

Not Available in Demo Version

2.0 Networking

2.1 Identifying Base-T Ethernet standards (such as 802.2e, 802.3i etc) and their names

Description: This lab exercise helps you to learn the Base-T Ethernet standards and their descriptions.

Instructions: Drag and drop the Base-T Ethernet standards to their respective names.

Standard	Name
1. 802.3e	Star LAN
2. 802.3i	10 BASE-T
3. 802.3u	100 BASE-TX
4. 802.3ab	1000 BASE-T
5. 802.3an	10 G BASE-T

Explanation: The 100Base-T standard is made up of 3 versions:

100BASE-TX is full-duplex capable in point to point unshared applications because it uses 1 pair to receive and 1 pair to transmit. Designed to run over 2 pairs of category 5 unshielded twisted pair cable with RJ45 connectors and EIA/TIA 568B pinning. It can also be run on IBM type 1 shielded twisted pair (existing Token Ring wiring) with an impedance matching device and DB9 connectors or regular STP and DB9 connectors. Max segment length is 100m.

100BASE-T4 designed to run over 4 pairs of category 3, 4 or 5 UTP cable with RJ45 connectors and EIA/TIA 568B pinning. It can also be run over STP. 1 pair is used to receive while 3 pairs are used to transmit,

However full-duplex operation does NOT work because specific pairs are not designated to transmit or receive. Max segment length is 100m.

100BASE-FX designed to run over 2 strands of duplex multimode fiber optic cable. It's also full-duplex capable because it uses one strand for receive and one for transmit. Maximum cable segment varies depending on the cabling used. Singlemode (depending on the manufacturer) can exceed 10 km when full-duplex. Multimode maximum length is 412 meters for half-duplex and 2 km ful-duplex. Max length from station to repeater is 150 meters.

NOTE: For full-duplex operation on 100BASE -TX or FX:

- 1) Devices must support full-duplex
- 2) Connection must be unshared end to end.

[Back](#)

2.2 Arrange the color codes of the T568B connector in the correct order.

Description: This lab exercise helps to identify the color code of the T568B connector.

Instructions: 1. The following are the shuffled color codes used in the T568B connector

2. Arrange them in a proper sequence by dragging the text from left to a empty box given on the right

Shuffled order :

1. Orange
2. GreenWhite
3. OrangeWhite
4. BlueWhite
5. Blue
6. Brown
7. BrownWhite
8. Green

Correct Order is

1. OrangeWhite
2. Orange
3. GreenWhite
4. Blue
5. BlueWhite
6. Green
7. BrownWhite
8. Brown

Explanation:

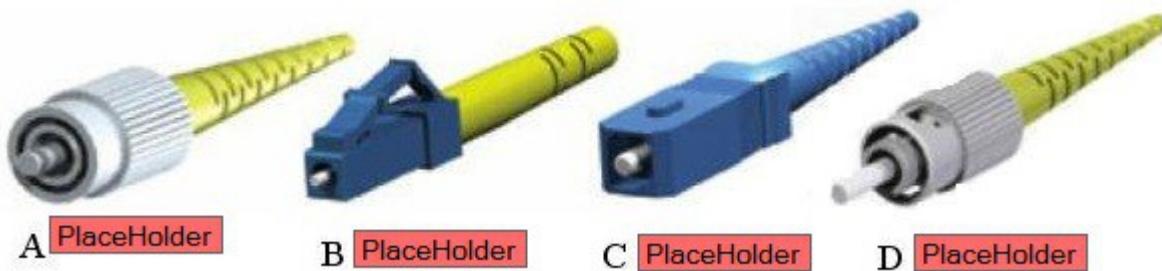


[Back](#)

2.3 Identifying the fiber connector types (such as ST , SC, FC etc)

Description: This lab exercise helps to identify the fiber connector types.

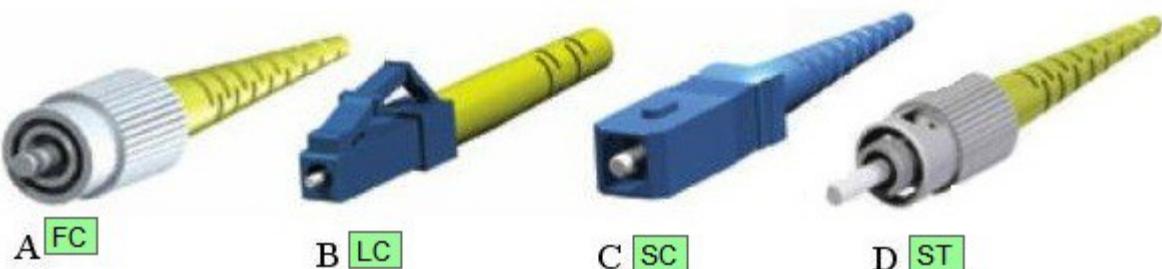
Instructions: 1. The below figure shows the different connector types labeled as A, B, C,D.
2. The name of the connector types are given as options
3. Drag and drop the name of the connector types into their respective places



Explanation:

1. ST connectors are the most common type of commercial fiber optic connector. These connectors utilize an exposed plastic tube housing the optical fiber. This requires a connection to a matching cable on the other side, incorporating a connector that mates to the other. These combine in a spring-loaded twist, reminiscent of BNC connectors, and are noted for their reliability.
2. SC connectors have the ferrule that houses the fiber mostly concealed. Probably the most similar commercial equivalent of To slink, SC connectors does not require a mating cable on the other side. Instead, these snap-on connectors simply push into their jacks with a click.
3. FC connector is similar to ST connectors, these fiber optic connector's screws into their mating jacks. Additionally, the tube surrounding the optical fiber is typically shrouded in ceramic or metal, as opposed to being fully exposed. The inner ring of the connector is keyed to ensure positive mating to its corresponding jack.
4. LC cables latch and release into their jacks in a manner similar to Ethernet connectors. Smaller in form than SC connectors, their durability is not compromised, nor is cost increased. Instead of snapping or thermoforming the connector to the cable, it is glued. This makes it a popular connector for field use.

Below fig. Shows after dragging and dropping correct option on the image.



[Back](#)

2.4 Identifying the port numbers of a TCP/IP protocols.

Not Available in Demo Version

2.5 Identifying the features of TCP/IP protocols (such as HTTP, SMTP etc.)

Not Available in Demo Version

2.6 Identifying functions of IPconfig labels (such as ipconfig , ipconfig/all etc.)

Not Available in Demo Version

2.7 Identify the Private IPv4 address

Not Available in Demo Version

2.8 Identifying speed ranges of 802.11 standards

Not Available in Demo Version

2.9 Identifying the characteristics of Internet WAN technologies

Not Available in Demo Version

2.10 Identifying the network characteristics managed by QoS (such as Bandwidth , Jitter etc.)

Not Available in Demo Version

2.11 Identifying twisted pair cable types (such as CAT3 , CAT5 etc.) with their speeds

Not Available in Demo Version

2.12 Compare shielded vs unshielded twisted-pair cable

Not Available in Demo Version

2.13 Identifying the IPV6 link local address .

Not Available in Demo Version

2.14 Objective Test 2 Answer the following questions

Not Available in Demo Version

3.0 Laptops

3.1 Accessing special keyboard functions with the Fn key

Description: This lab exercise helps you to get familiar with accessing special keyboard function key(Fn).

Instructions: Match (drag and drop) the Fn key given on the Column A with their respective functions given on the Column B

Column A	Column B
1. Fn+F3	A panel for selecting a power scheme appears.
2. Fn+F4	Put the computer in standby mode
3. Fn+F5	Enable or disable the built-in wireless networking features and the bluetooth features.
4. Fn+F7	Switching the display output location
5. Fn+F8	Change the settings of the Ultra Navigation pointing device.
6. Fn+F9	Open the ThinkPad Easy Eject Utility screen. Buttons for the following choices are displayed:
7. Fn+F12	Put the computer into hibernation mode
8. Fn + PgUp	Turn the Think Light on or off.
9. Fn+Home	The computer display becomes brighter.
10. Fn+End	The computer display becomes dimmer.

[Back](#)

3.2 Objective Test 3

1.A technician needs to upgrade the memory in a laptop. Which of the following memory types would be the correct type?

- A.RIMM
- B.DDR RAM
- C.SDRAM
- D.SODIMM

Answer: D

2.Which of the following is a feature of a Docking station?

- A. Provides additional connectivity options
- B. Expands the laptop memory
- C. Provides a built in tape drive
- D. Provides power surge protection

Answer: A

3. A technician has a laptop that is booting but nothing appears on the LCD. Which of the following should the technician press to make video transfer to the external monitor?

- A. Function keys
- B. Alt-insert keys

- C. Power button
- D. Control and escape keys

Answer: A

4.Which type of PC Card is used most often for expansion devices like NICs, sound cards, and so on?

- A. Type I
- B. Type II
- C. Type III
- D. Type IV

Answer: B Type II PC Card

5.How do laptop hard drives differ from desktop hard drives?

- A. Laptop hard drives use completely different standards from those used by desktop hard drives for communication with the host.
- B. Laptop hard drives are solid state; desktop hard drives have spinning platters.
- C. Laptop hard drives require a separate power connection; desktop hard drives are powered through the drive interface.
- D. The most common form factor of a laptop hard drive is about an inch smaller than that of a desktop hard drive.

Answer: D

Laptop hard drives commonly have a 2½" form factor. The most common form factor for desktop hard drives is 3½". Laptop hard drives use the same drive technologies as their desktop counterparts, such as serial and parallel ATA. As with desktop hard drives, laptop hard drives are available in both solid-state and conventional varieties. Unlike desktop hard drives, laptop hard drives do not have separate power connectors.

6. How do you upgrade BIOS?

- A. Remove and replace the CMOS chip with the newest version from the manufacturer.
- B. The BIOS is automatically upgraded each time you install the latest Windows service pack.
- C. BIOS cannot be upgraded. You must replace the motherboard.
- D. Download the BIOS upgrade from the BIOS manufacturer and then flash the BIOS.

Answer : D

7. Which type of battery is most commonly found in laptop computers?

- A. Li-Ion
- B. NiCad
- C. NiNH
- D. Lead Acid

Answer : A. Li-ion

8.Which type of memory is module is used in laptop computer RAM?

- A. SODIMM 204 pin DDR3
- B. DIMM 240 pin DDR3
- C.SIMM 72 pin
- D.SIMM 168 pin

Answer : A. SODIMM 204 pin DDR3

9. How many Type II PC cards can fit into a laptop access port?

- A. One
- B. Two
- C. Three
- D. Four

Answer : A. One

10. Which power option saves the current work to HDD?

- A. Sleep
- B. Hibernate
- C. Resting
- D. Away Mode

Answer : B. Hibernate

11. Which three hard drive characteristics are identified in BIOS?

- A. Manufacturer, date of installation, time to failure.
- B. Cylinders, sectors, and heads.
- C. Manufacturer, speed, and bytes used.
- D. Clusters, sectors, and speed

Answer : B. Cylinders, sectors, and heads.

12. The toggle switch marked 120/240V on the back of most system cases is used for:

- A. Users who play games and will be overclocking the system.
- B. Switching between electrical outlets in different countries.
- C. Peripherals that may drain power from the system.
- D. Assistance in troubleshooting power supply failures.

Answer : B. Switching between electrical outlets in different countries.

[**Back**](#)

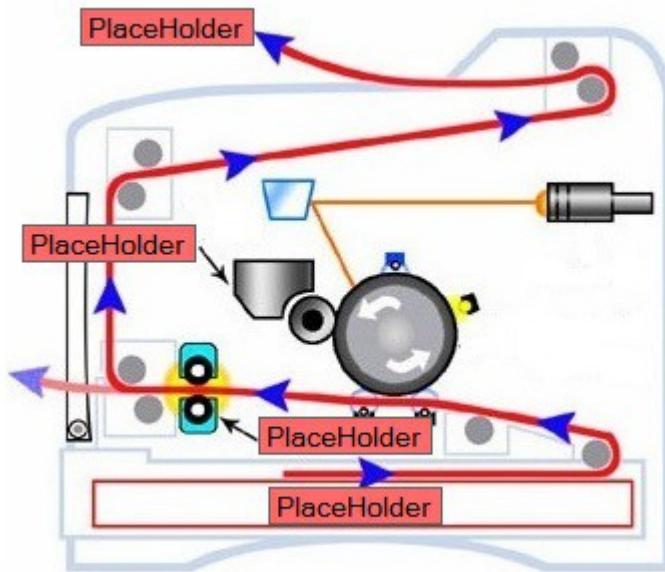
4.0 Printers

4.1 Identify the basic components of the LASER printer

4.1.1 Identify the laser printer components -1

Description: This lab exercise helps you to get familiar with laser printer components

Instructions: 1. The laser printer figure is given below
2. Drag and drop the component names into their respective places of laser printer.

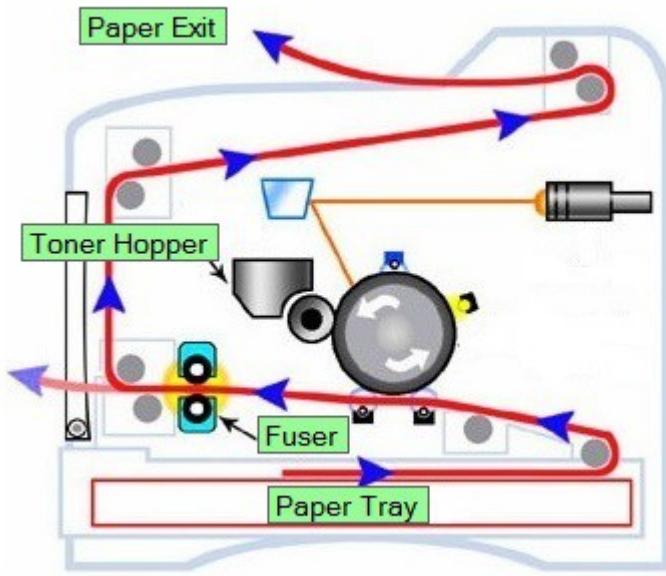


Explanation:

A laser printer is a popular type of personal computer printer that uses a non-impact (keys don't strike the paper), photocopier technology. When a document is sent to the printer, a laser beam "draws" the document on a selenium-coated drum using electrical charges. After the drum is charged, it is rolled in toner, a dry powder type of ink. The toner adheres to the charged image on the drum. The toner is transferred onto a piece of paper and fused to the paper with heat and pressure. After the document is printed, the electrical charge is removed from the drum and the excess toner is collected. Most laser printers print only in monochrome. A color laser printer is up to 10 times more expensive than a monochrome laser printer.

The laser printer is different from an inkjet printer in a number of ways. The toner or ink in a laser printer is dry. In an inkjet, it is wet. Over time, an inkjet printer is about ten times more expensive to operate than a laser printer because ink needs replenishing more frequently. The printed paper from an inkjet printer will smear if wet, but a laser-printed document will not. Both types of printer operate quietly and allow fonts to be added by using font cartridges or installing soft fonts. If your printing needs are minimal, an inkjet printer is sufficient. But if your printing volume is high, consider buying a laser printer.

Below fig. Shows after dragging and dropping correct option on the image.



[Back](#)

4.1.2 Identify the laser printer components -2

Not Available in Demo Version

4.1.3 Identify the laser printer components -3

Not Available in Demo Version

4.2 Identifying the characteristics of various printer types (such as Laser , Inkjet etc.)

Not Available in Demo Version

4.3 Identifying features of Laser printer components

Not Available in Demo Version

4.4 Identifying features of laser printing process (such as cleaning, writing etc)

Not Available in Demo Version

4.5 Objective Test 4 Answer the following questions

Not Available in Demo Version

5. Operating System

5.1 Identifying features (such as Event viewer , Bit-locker etc.) of windows OS.

Description: This exercise helps to know about the features supported in Windows XP/Vista/7 and their characteristics.

Instructions: 1. Various windows os features are given on the column A
2. Their functions/characteristics are given on the column B
3. Match (drag and drop) the feature given on the Column A with their respective functions given on the column B.

Column A

1. Bit-Locker
2. Shadow Copy
3. ReadyBoost
4. Windows Defender
5. Event viewer

Column B

1. Drive security and encryption program that protects drive content and data from any offline attack.
2. Allows taking manual or automatic backup copies or snapshots of computer files or volumes, even when they are in use.
3. It allows any compatible mass storage device to be used as a hard-drive memory cache for the purpose of increasing random read access speed to the hard drive.
4. An antispyware program for Windows that provides real-time protection and post infection scanning and removal.
5. A component you can use to view and manage event logs, gather information about hardware and software problems, and monitor security events.

Explanation

Bit-Locker: Bit-Locker lets you encrypt the hard drive(s) on your system and also helps to protect against unauthorized changes to your system such as firmware-level malware.

Shadow Copy: Shadow Copy(also known as Volume Snapshot Service, Volume Shadow Copy Service or VSS) is a technology that allows taking manual or automatic backup copies or snapshots of computer files or volumes, even when they are in use.

ReadyBoost: ReadyBoost is a feature uses a USB flash drive for caching. This allows to service random disk reads with performance that is typically 80-100 times faster than random reads from traditional hard drives.

Windows Defender: Windows Defender is malware protection. This software helps identify and remove viruses, spyware, and other malicious software.

Event viewer: Event Viewer is a tool that displays detailed information about significant events (for example, programs that don't start as expected or updates that are downloaded automatically) on your computer. Event Viewer can be helpful when troubleshooting problems and errors with Windows and other programs.

[Back](#)

5.2 Identifying the features of networking command line tools (such as Copy , SFC etc.)

Description: This exercise helps to know about the features of networking command line tools and their characteristics.

Instructions: 1. Various command line tools are given on the column A
2. Their functions/characteristics are given on the column B
3. Match (drag and drop) the feature given on the Column A with their respective functions given on the column B.

Column A

- 1. FORMAT
- 2. COPY
- 3. XCOPY
- 4. ROBOCOPY
- 5. DISKPART
- 6. SFC
- 7. CHKDSK

Column B

- 1. Carries out disk formatting
- 2. Allows the user to copy one or more files to an alternate location
- 3. Command copies multiple files or entire directory trees from one directory to another and for copying files across a network.
- 4. Used for Mirroring files or directories
- 5. Used to manipulate disk partitions
- 6. Allows users to scan for and restore corruptions in Windows system files.
- 7. It verifies the file system integrity of a volume and fixes logical file system errors.

Explanation

FORMAT: The FORMAT command is used to wipe data off disks and prepare them for new use. Before a hard disk can be formatted, it must have partitions created on it. The syntax for FORMAT is as follows:

FORMAT [volume] [switches]

The “volume” parameter describes the drive letter (for example, E :), mount point, or volume name.

COPY: COPY command makes a copy of a file in a second location. The syntax for COPY command is as follows: **COPY [filename] [destination]**

XCOPY: XCOPY command copies directories as well as files. The syntax is as follows:

XCOPY [source] [destination][switches]

ROBOCOPY: ROBOCOPY command is used for reliable copy or mirroring while maintaining the permissions, attributes, owner information, timestamps and properties of the objects copied.

DISKPART: The DISKPART command shows the partitions and lets you manage them on the computer’s hard drives.

SFC: The System File Checker (SFC) is a command line-based utility that checks and verifies the versions of system files on your computer. If system files are corrupted, the SFC will replace the corrupted files with correct versions. The syntax for the SFC command is as follows:

SFC [switch]

While the switches vary a bit between different versions of Windows,

CHKDSK: Chkdsk utility is used to create and display status reports for the hard disk. Chkdsk can also correct file system problems (such as cross-linked files) and scan for and attempt to repair disk errors.

5.3 Identifying the Processes tab function of Windows Task manager in Windows 10/11 PC.

Description: This exercise helps to know about the features of Processes tab columns of Task Manager.

Instructions: 1. Various Process tab column are given on the column A
2. Their functions/characteristics are given on the column B
3. Match (drag and drop) the feature given on Column A with their respective characteristics given on the column B.

Column A

- 1. Threads
- 2. Page Fault Delta
- 3. Page Faults
- 4. Process Identifier (PID)
- 5. Session ID

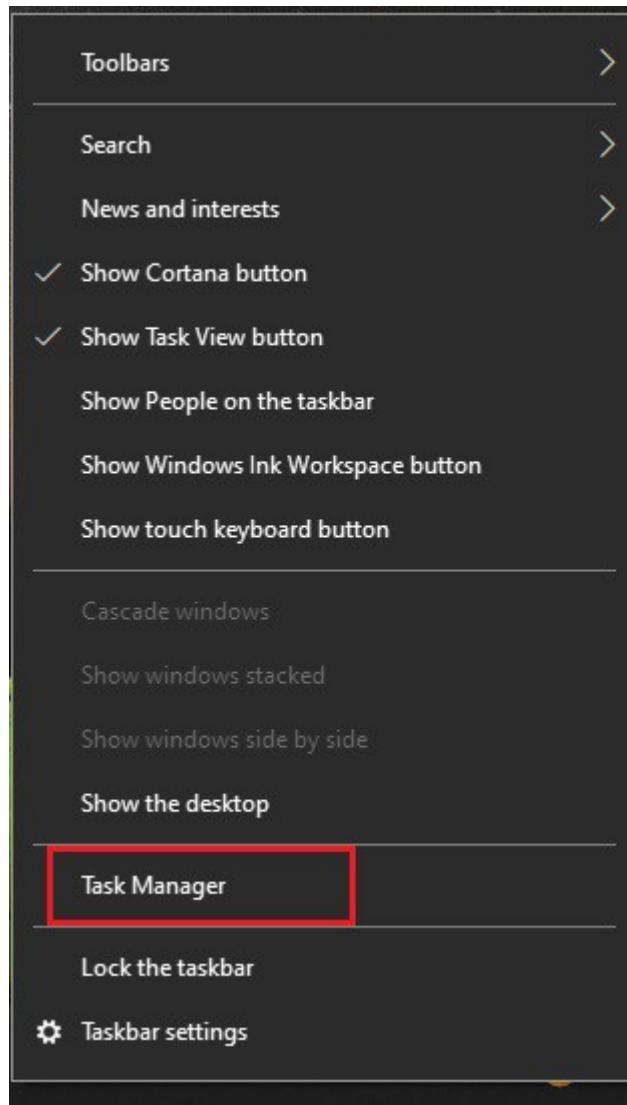
Column B

- 1. The number of threads running in a process.
- 2. The change in the number of page faults since the last update
- 3. The number of page faults generated by a process since it was started.
- 4. It is a number that uniquely identifies a process while it runs
- 5. It is a number that identifies the owner of the process.

Explanation

How to start the Windows Task Manager and an overview of its interface

The Windows Task Manager can be started by using two methods. The first, and easiest method, is to simply right click on the time shown in your Windows taskbar. When you right click the time, you will be shown a dialog box similar to the one below:



Simply left click on the Task Manager option and the Windows Task Manager will open.

The second method to start the Windows Task Manager is to click on the Start button and type in taskmgr.exe and press the Enter on your keyboard. If you are using Windows XP, then you will need to click on the Run option before typing taskmgr.exe. Once you press Enter on your keyboard, the program will start.

When the Windows Task Manager opens, it will open to the last tab that you viewed before you closed it in the past. If this is the first time you have run the program, then the Task Manager will start in the Applications tab as shown below.

The screenshot shows the Windows Task Manager window with the 'Processes' tab selected. The table lists various processes with columns for Name, PID, Status, User name, CPU, Memory (a...), Platform, and UAC virtualiza... . Notable entries include multiple instances of 'chrome.exe' and 'ApplicationFrameHo...', indicating a high number of browser tabs or background processes.

Name	PID	Status	User name	CPU	Memory (a...)	Platform	UAC virtualiza...
ApplicationFrameHo...	18096	Running	admin	00	812 K	64 bit	Disabled
armsvc.exe	4448	Running	SYSTEM	00	32 K	32 bit	Not allowed
browserhost.exe	15760	Running	admin	00	1,376 K	64 bit	Disabled
chrome.exe	10352	Running	admin	02	122,020 K	64 bit	Disabled
chrome.exe	19132	Running	admin	00	700 K	64 bit	Disabled
chrome.exe	18188	Running	admin	01	136,200 K	64 bit	Disabled
chrome.exe	5232	Running	admin	01	24,436 K	64 bit	Disabled
chrome.exe	16196	Running	admin	00	2,872 K	64 bit	Disabled
chrome.exe	4184	Running	admin	00	27,284 K	64 bit	Disabled
chrome.exe	9364	Running	admin	00	1,796 K	64 bit	Disabled
chrome.exe	12040	Running	admin	05	118,136 K	64 bit	Disabled
chrome.exe	10160	Running	admin	00	13,544 K	64 bit	Disabled
chrome.exe	11128	Running	admin	00	12,780 K	64 bit	Disabled
chrome.exe	13880	Running	admin	00	28,508 K	64 bit	Disabled
chrome.exe	18412	Running	admin	00	15,260 K	64 bit	Disabled
chrome.exe	11640	Running	admin	00	15,304 K	64 bit	Disabled
chrome.exe	16436	Running	admin	01	73,816 K	64 bit	Disabled
chrome.exe	14516	Running	admin	00	13,092 K	64 bit	Disabled
chrome.exe	3452	Running	admin	00	20,476 K	64 bit	Disabled
chrome.exe	13980	Running	admin	04	24,600 K	64 bit	Disabled
chrome.exe	17140	Running	admin	00	82,760 K	64 bit	Disabled
chrome.exe	9292	Running	admin	00	34,416 K	64 bit	Disabled
chrome.exe	11232	Running	admin	00	13,180 K	64 bit	Disabled

[Fewer details](#) [End task](#)

In Windows 10/11 Task Manager, you'll see a number of tabs, including "Performance", "App history", "Startup", "Users", "Details", "Services", and "Processes" tab. Typically, the Processes tab is the first place you want to go to determine which process is draining your computer's resources. This tab lists all the running processes in a single view grouped by "Apps", "Background processes" and "Windows Processes". On Windows 10, you can also find multiple instances or other processes under the same process, which helps you to better understand how they're organized and how they use system resources. In Task Manager, you can monitor processes running on your computer by adding columns to the information displayed on the Processes tab. These columns display information about each process, such as how much CPU and memory resources the process is currently using.

Process Tab: In the Processes tab, each app is listed with the percentage of CPU, memory, hard disk, and network resources being used in real time. You can sort the list by clicking the heading of the desired column in the table to find out which apps are using the most resources.

Performance tab: The Performance tab provides important information about the components and networks shown in thumbnails on the left side of the window. Click a thumbnail to view a graph and other information such as processor speed, amount of memory, and IP address associated with the CPU, memory, disk, Bluetooth, Wi-Fi, or Ethernet.

App history tab: The App history tab shows the cumulative activity for each of the app tiles. If you have limited data transfer each month, this information can be useful in helping you determine how much data transfer is still available.

Apps that use more processes or data are highlighted in a darker color.

Startup tab: If your computer is running slowly or if the startup process takes too long, select the Startup tab. The Startup tab shows the name and publisher of software that automatically opens when Windows starts. It also shows the status of software, whether a program is enabled or disabled, and the impact the software has on the startup time. In the Status column you can right-click a program and disable that program to improve startup times and computer performance. While disabling a program can improve startup time, the function provided by the program will not work unless you enable it again.

Users tab: The Users tab displays usage of CPU, memory, misc, and network by each user account on the system. Items that use a higher percentage of resources are highlighted in a darker color.

Details tab: The Details tab displays more descriptive information about processes.

Services tab: The Services tab displays the currently-running services.

To view processes currently running on your computer:

1. Open Task Manager by right-clicking the Task bar, and then clicking Start Task Manager.
2. Click the Processes tab. Task Manager shows the processes currently running under your user account.
3. You may add/remove the columns in processes tab by going to View → Select Columns

Features of the various Task Manager Process tab columns features are as given below:

1. Threads - The number of threads running in a process.
2. Page Fault Delta - The change in the number of page faults since the last update.
3. Page Faults - The number of page faults generated by a process since it was started.
4. Process Identifier (PID) - It is a number that uniquely identifies a process while it runs.
5. Session ID - It is a number that identifies the owner of the process.

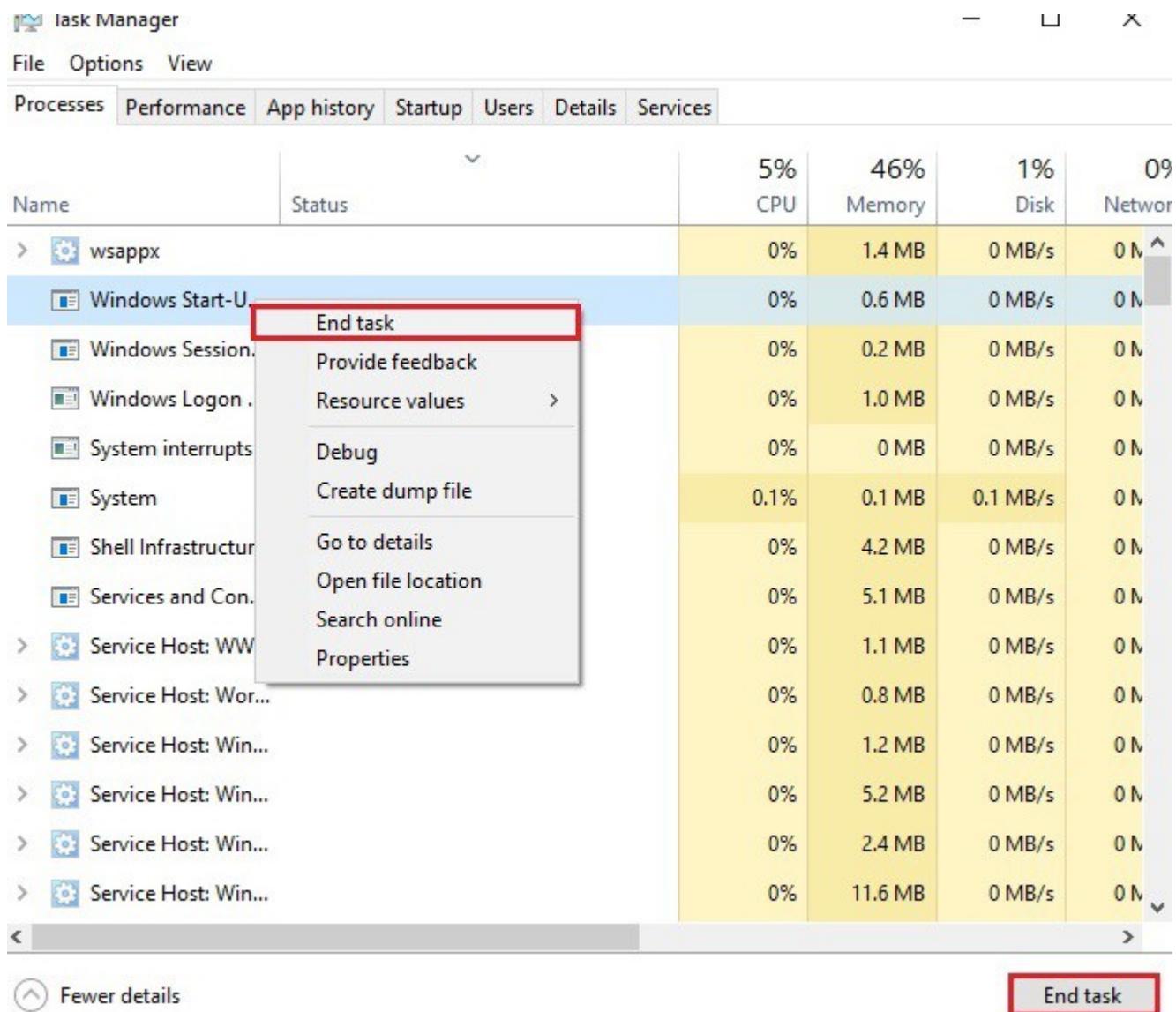
Stopping processes with high-resource usage

After you identify the problem, right-click the process, and select End task to terminate it. Alternatively, you can simply select the item and click the End task button in the bottom-right corner.

Task Manager also uses colors to highlight processes that use the most resources. You'll notice that as a process starts to consume more resources, the color begins to change from a light- to a dark-shade of orange, making it easier to tell which one is causing the problem.

Typically, when you're not actively using applications and your computer isn't working on anything specific, such as maintenance, your total CPU usage should be less than 30 percent. Applications that are running, even if you're not using them, and processes use part of your computer's memory, and that usage will increase as you use or launch more applications. Memory usually won't be an issue unless you run out of it, in which case your computer will start using virtual memory, and that can cause your PC to slow down. Generally speaking, depending on your system configuration, your total memory usage should be below 60 percent. If you're not copying files or rendering videos, disk usage should be below 5 percent.

Network connectivity is almost never the reason your system is slow, but there could be a problem in the network causing web content to take a long time to load. If you're having problems downloading files, and you see "Network" stuck at 0 percent, you may have an idea of what's going on.



[Back](#)

5.4 Identifying the options to open Local Users and Groups (Local) window in Windows 10/11 computer.

Description: This exercise helps to know the ways to open Local Users and groups window.

Instructions: 1. Various options to open the Local Users and groups window are given on the column A
2. Drag-n-drop the respective option to the Column B.

Column A	Column B
1. lusrmgr.msc in start → search box	1. lusrmgr.msc in start → search box
2. Administrative Tools-Computer Management	2. Administrative Tools-Computer Management
3. Control Panel → User Account	
4. Programs and Features	

Explanation

Option 1:

Open "Local Users and Groups Manager" in Computer Management

1. Open the Control Panel (icons view), and click/tap on the Administrative Tools icon.
2. Close the Control Panel window.
3. In Administrative Tools, click/tap on the Computer Management icon.
4. If prompted by UAC, click/tap on Yes.
5. Close the Administrative Tools window.
6. In the left pane of Computer Management, double click/tap on Local Users and Groups.

Option 2:

1. Press the Windows + R keys to open the Run dialog, type lusrmgr.msc, and press Enter.
NOTE: This file is located at C:\Windows\System32\lusrmgr.msc.
2. If prompted by UAC, click/tap on Yes.
3. You can now set and manage the Local Users and Groups settings on your computer to how you want them.

[**Back**](#)

5.5 Identifying functions of “User and Groups” options in windows 10/11 PC

Not Available in Demo Version

5.6 Identifying features of NTFS permissions and Share permissions

Not Available in Demo Version

5.7 Identifying the System action resulting from different combinations of the duplex and speed modes.

Not Available in Demo Version

5.8 Identifying Console command tools and their respective features

Not Available in Demo Version

5.9 Identifying the MSCONFIG options and their respective functions/features

Not Available in Demo Version

5.10 Identifying the features of File attributes (such as Read-Only , System(S) etc.)

Not Available in Demo Version

5.11 Identifying the windows OS “Power Options” and their features.

Not Available in Demo Version

5.12 Identifying the features of File system types (such as FAT16 , FAT32 etc.)

Not Available in Demo Version

5.13 Identifying the characteristics of Operating System Administrative tools

Not Available in Demo Version

5.14 Identifying the features of Command line utilities (such as MSCONFIG, MMC etc.) of Windows OS

Not Available in Demo Version

5.15 Identifying unique features of Windows OS types

Not Available in Demo Version

5.16 Identifying the display standards of Windows OS and their resolutions

Not Available in Demo Version

5.17 NTFS permissions and Share permissions in Windows 10

5.17.1 To share folders with other users on your network

Not Available in Demo Version

5.17.2 To change read only attributes on files and folders

Not Available in Demo Version

5.17.3 To set, view, change, or remove file and folder permissions

Not Available in Demo Version

5.18 Configuring Local Security Policy in Windows 10

5.18.1 Setting Account lockout policy

Not Available in Demo Version

5.18.2 Setting Password policy

Not Available in Demo Version

5.19 Configuring hardware settings using Device Manager

Not Available in Demo Version

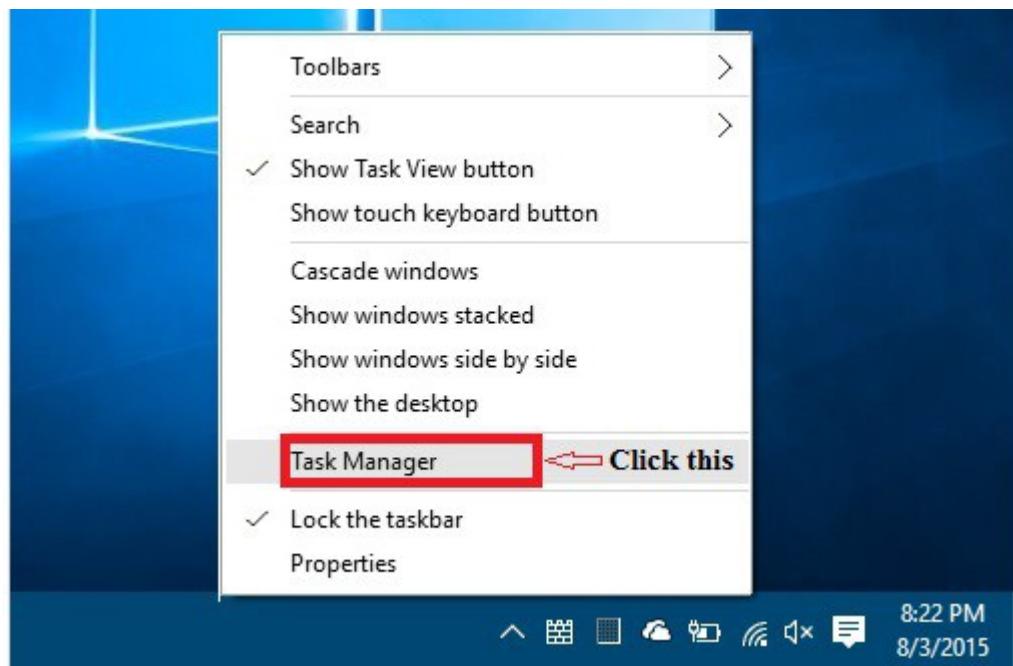
5.20 Troubleshooting startup issues using Bootrec.exe tool in windows RE(Recovery Environment)

Not available in Demo version

5.21 Disabling start up program in Windows 10

Description: This lab exercise helps how to disable startup programs in windows 10 OS. In this lab, disable a startup program “CCleaner”

Instructions: 1. In the given short cut menu click “Task Manager”



2. When Task Manager comes up, click the “Startup” tab and look through the list of programs that are enabled to run during startup. Then to stop them from running, right-click the program and select Disable.

Name	Status	11% CPU	40% Memory	86% Disk	0% Network
Click this					
Apps (1)					
> Task Manager		1.4%	17.3 MB	0.1 MB/s	0 Mbps
Background processes (40)					
> 64-bit Synaptics Pointing Enhanc...		0%	0.7 MB	0 MB/s	0 Mbps
> Adobe Acrobat Update Service (...)		0%	1.1 MB	0 MB/s	0 Mbps
> Antimalware Service Executable		6.3%	95.0 MB	1.1 MB/s	0 Mbps
CCleaner		0%	9.9 MB	0 MB/s	0 Mbps
> Cortana (3)		0%	50.0 MB	0 MB/s	0 Mbps
CTF Loader		0%	2.5 MB	0 MB/s	0 Mbps
Google Installer (32 bit)		0%	0.6 MB	0 MB/s	0 Mbps
Google Installer (32 bit)		0%	1.2 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks		0%	2.3 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks		0%	1.1 MB	0 MB/s	0 Mbps

3. In this simulator right click CCleaner and a popup menu appears click “Disable”. Click close button to close the application.

The screenshot shows the Windows Task Manager interface with the title bar "Task Manager Simulation". A note at the top right says "Note that only a few links are made active". The "Start-up" tab is selected. The table lists startup programs:

Name	Publisher	Status	Start-up impact
CCleaner	Piriform Ltd	Enabled	Not measured
Disable	ogitech, Inc.	Disabled	None
Open file location	Microsoft Corporation	Disabled	None
Search online	Realtek Semiconductor	Disabled	None
Properties	Microsoft Corporation	Disabled	None
Windows Defender notifications	Microsoft Corporation	Disabled	None

At the bottom left is a "Fewer details" button, and at the bottom right is a "Disable" button.

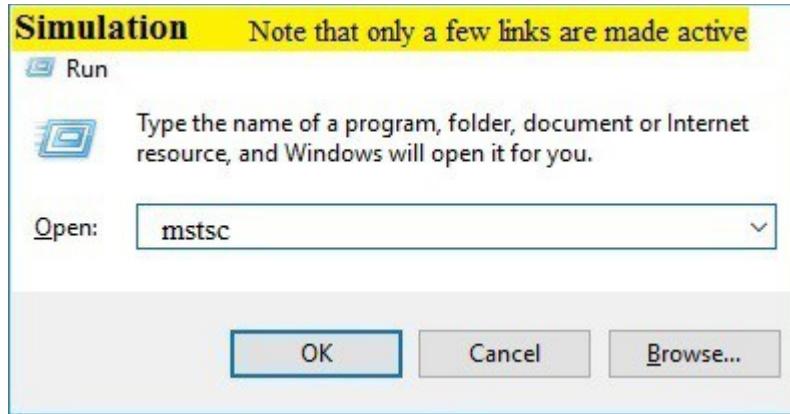
Explanation: Startup programs are programs which run when your computer starts / boots up. Startup programs can be antivirus programs, chat/messaging apps or background apps that can also continuously keep running on your computer. Start up programs impact computer boot time, and may make your computer boot slower. While some of startup programs like antivirus are important, you can make your computer boot faster by disabling unrequired startup programs.

[Back](#)

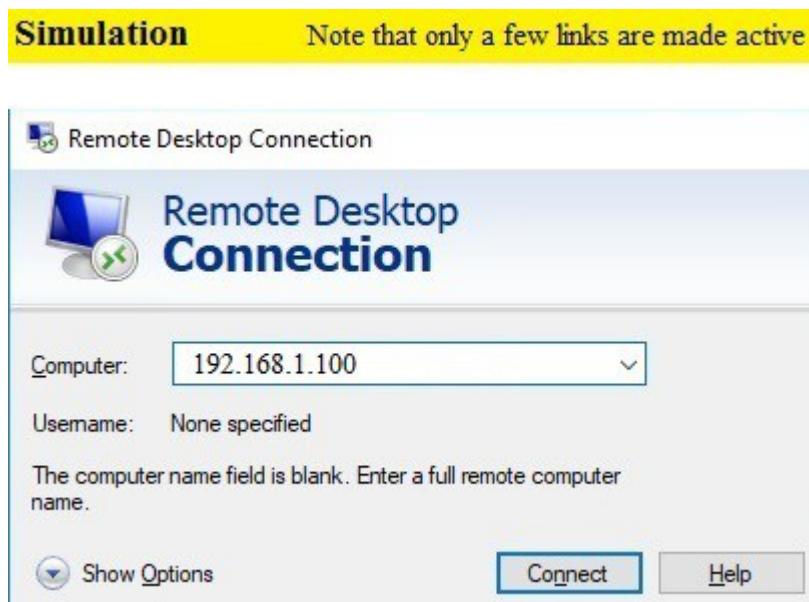
5.22 Connecting to remote desktop in Windows 10

Description: This lab exercise helps you to know how to connect to a remote desktop. Here, you connect to a remote computer given by the IP address 192.169.1.100.

Instructions: 1. On loading a lab exercise, in a given simulation type “ **mstsc** ” in the given Run dialog box and then click OK button



2. In Remote Desktop connection window type the address of the remote computer as 192.168.1.100 in computer text box and click “connect” button and then click close button to close the application.



Explanation: Remote Desktop can be used on any Windows platform, iOS or Android devices to connect to any other machine irrespective of the geographical location. Remote desktop is also known as Remote Desktop Services(RDS), or RDP(Remote desktop Protocol). It is one of the services offered from Microsoft Windows that allows a user to remote access any system from any other computer. Remote desktop allows users to connect to remote Window PCs and access resources from those machines. Terminal server is the server component of Remote Desktop Services. Software user-interface is transferred to the client system with Remote Desktop Services. These may arise a certain situations when one person sitting on a system may require data or information present on some other system or colleagues sitting in any organization can seek or ask for help irrespective of the geographical location, so here comes the wonderful use of the Remote desktop services, which can help user to retrieve information or seek help from anyone in any part of the world. Now access or connect to any computer or machine located at different places.

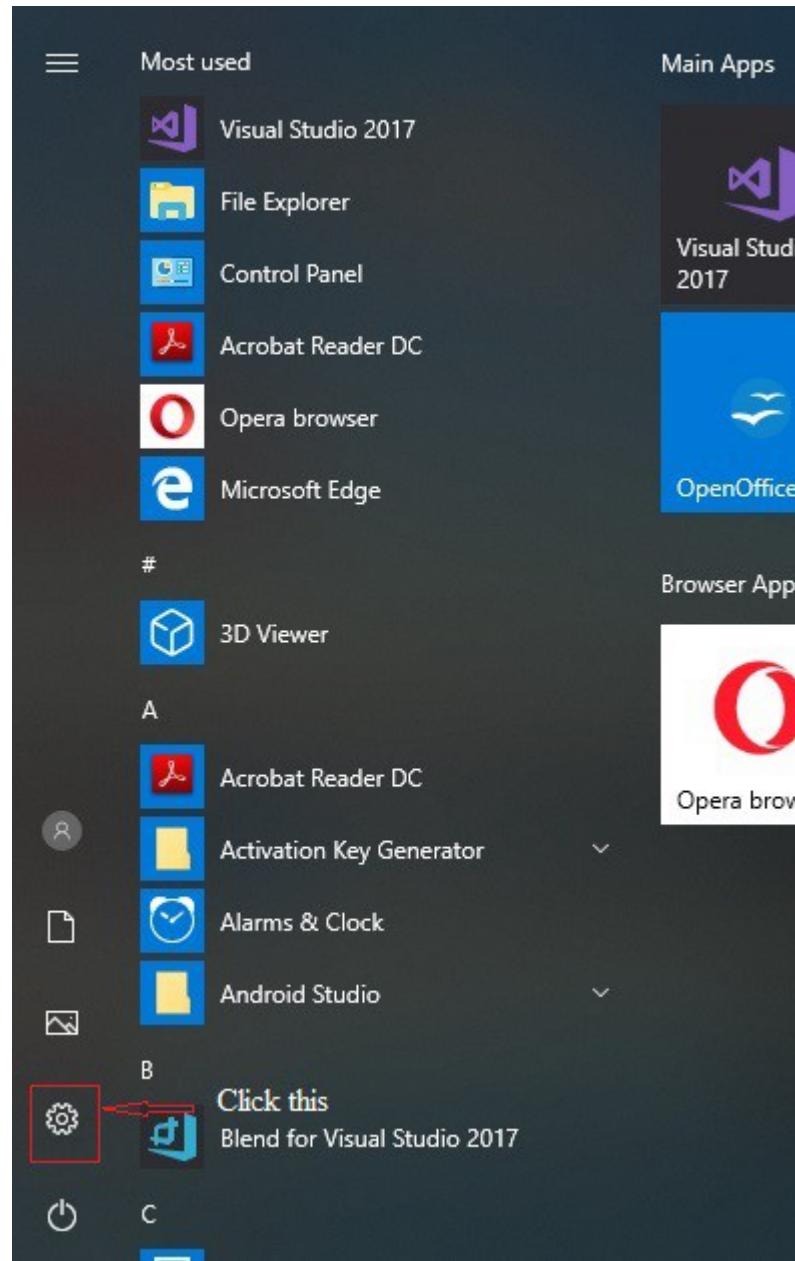
[Back](#)

5.23 Changing the refresh rate in Windows 10

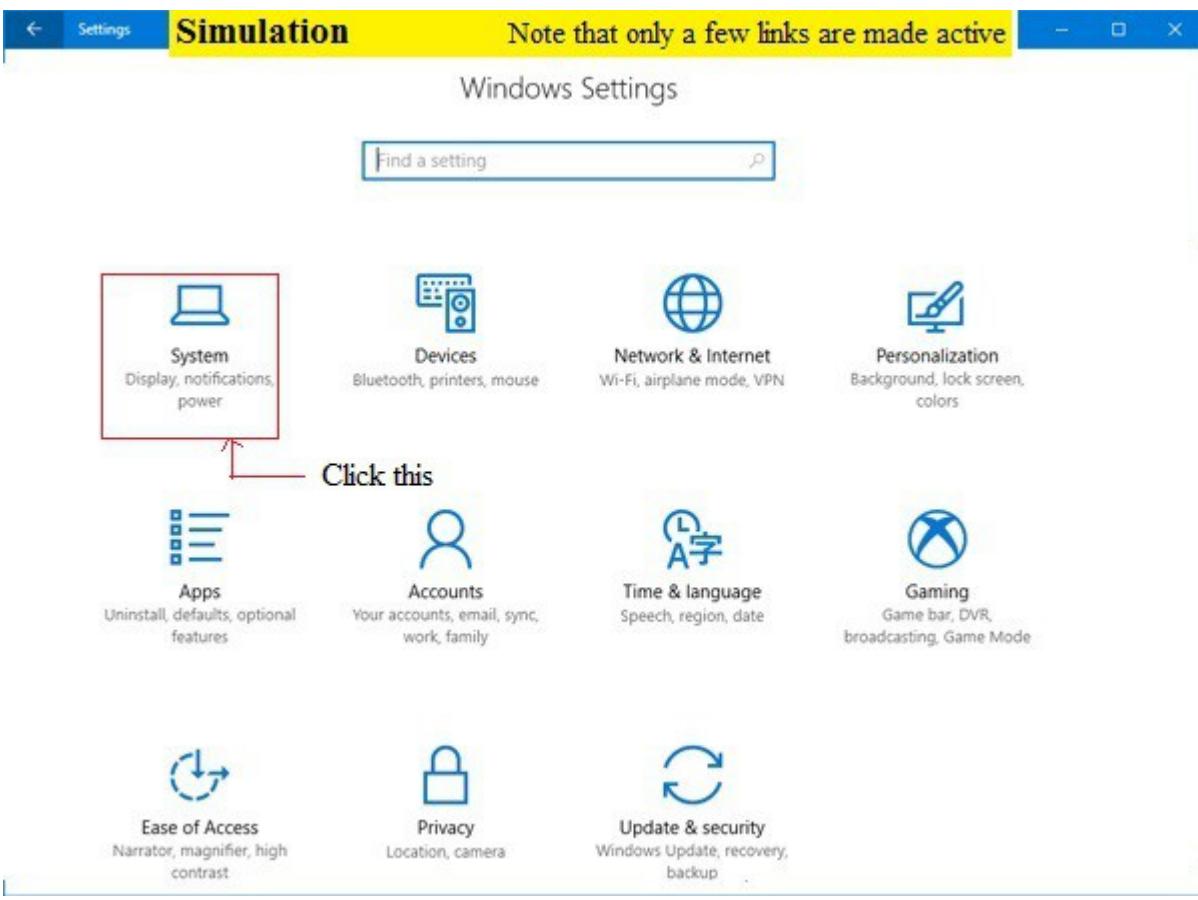
Description: The lab exercise explains how to change the monitor refresh rate in windows 10 OS. Here, you change the refresh rate to 60 Hertz.

Instructions:

1. On loading a lab exercise, in a given simulation start menu click **settings**



2. A settings app window appears , click on “System” icon



3. A display screen appears click “Advanced display settings” from right pane

Simulation Note that only a few links are made active

The screenshot shows the Windows Settings interface. On the left, under 'System', there's a 'Find a setting' search bar. Below it, a list of options includes: Display, Sound, Notifications & actions, Focus assist, Power & sleep, Battery, Storage, Tablet mode, Multi-tasking, Projecting to this PC, and Shared experiences. On the right, the 'Display' section is expanded, showing 'Scale and layout' settings like text size and resolution. Under 'Multiple displays', there's a 'Detect' button and a link to 'Advanced display settings'. A red box highlights the 'Advanced display settings' link, with a callout arrow pointing to it from the text 'Click this'.

Display
Scale and layout

Change the size of text, apps and other items
100% (Recommended)

Advanced scaling settings

Resolution
1366 × 768 (Recommended)

Orientation
Landscape

Multiple displays

Connect to a wireless display

Older displays might not always connect automatically. Select Detect to try to connect to them.

Detect

Advanced display settings

Click this

Graphics settings

4. In Advanced display settings click “**Display adaptor properties for Display 1**”

Simulation

Note that only a few links are made active

← Settings

 Advanced display settings

Display information



Display 1: Connected to Intel(R) HD Graphics

Desktop resolution 1366 × 768

Active signal resolution 1366 × 768

Refresh rate (Hz) 60 Hz

Bit depth 8-bit

Colour format RGB

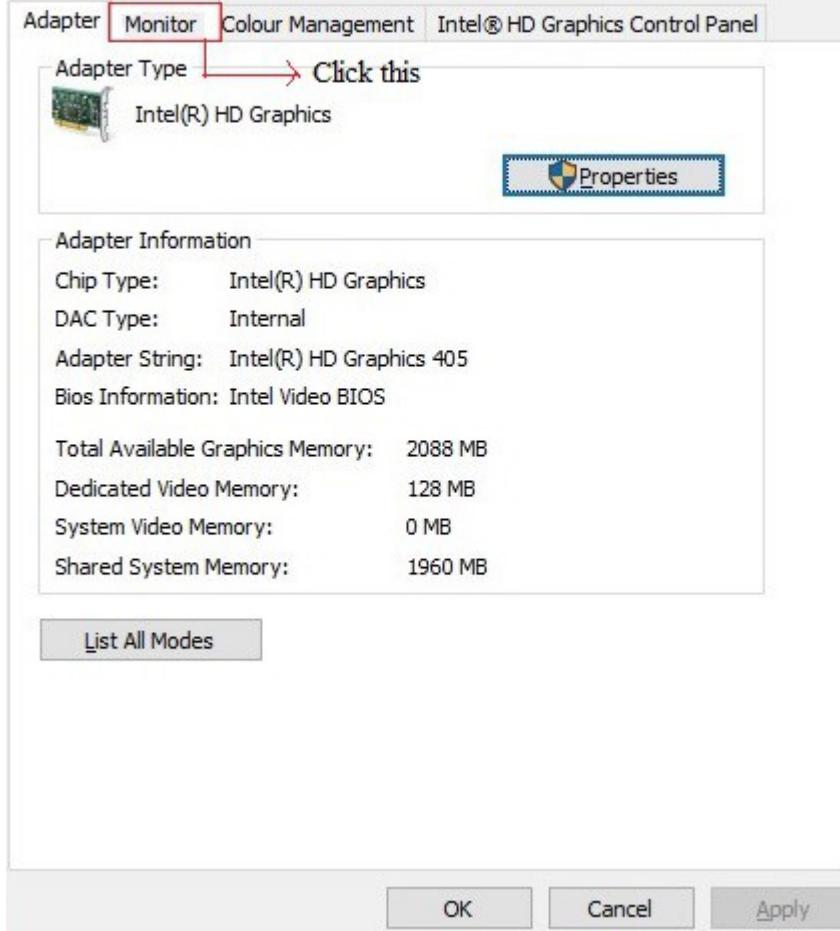
Colour space Standard dynamic range (SDR)

Display adaptor properties for Display 1  Click this5. Click the **Monitor** tab

Simulation

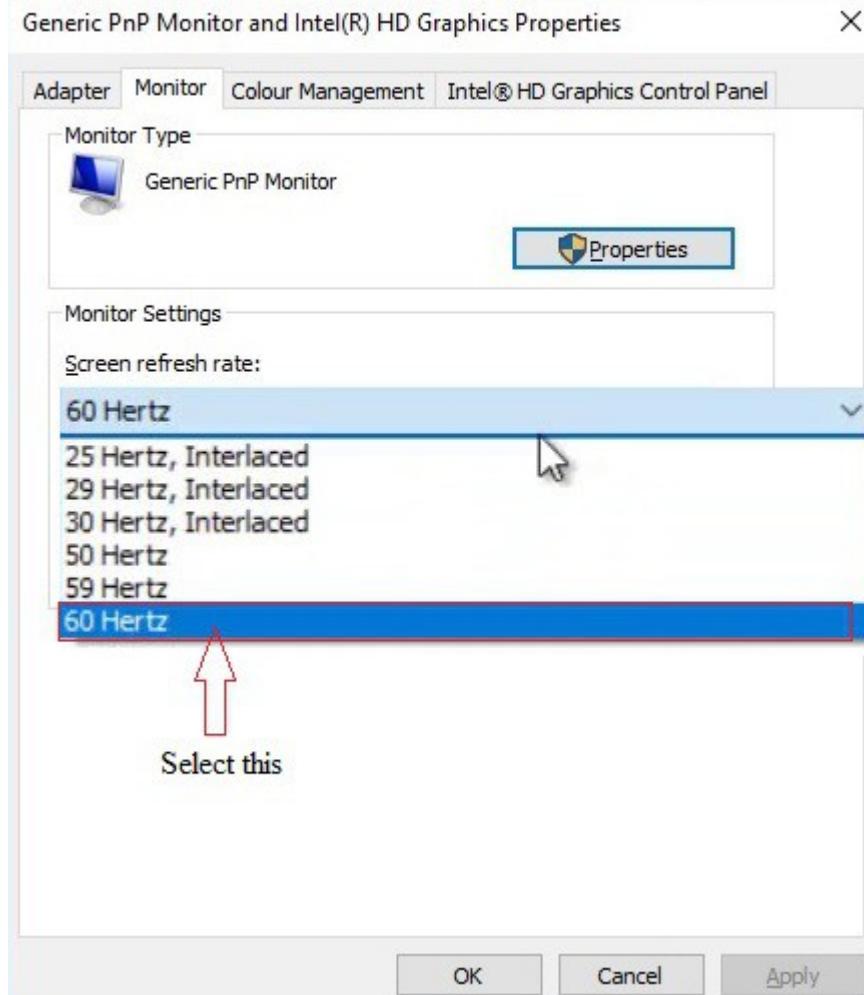
Note that only a few links are made active

Generic PnP Monitor and Intel(R) HD Graphics Properties



6. Under "Monitor Settings," use the drop-down menu to select the refresh rate , change the refresh rate to 60 Hertz click Apply button and then OK button.

Simulation Note that only a few links are made active



Explanation: Refresh rate refers to the number of times per second an image refreshes on the screen in a process measured in Hertz (Hz). The higher the refresh rate, the better the experience, while lower refresh rate usually results in screen flickering, and it can cause eye strain and headaches. Typically, a refresh rate of 60Hz is good enough for everyday computing tasks.

[Back](#)

5.24 Changing Power Plan Settings in Windows 10

Not Available in Demo Version

5.25 Creating new user account in Windows 10

Not Available in Demo Version

5.26 Changing user account control settings in Windows 10

Not Available in Demo Version

5.27 Changing user account password in Windows 10

Not Available in Demo Version

5.28 Removing user account in Windows 10

Not Available in Demo Version

5.29 Changing user account type in Windows 10

Not Available in Demo Version

5.30 Creating a system image backup of Windows 10

Not Available in Demo Version

5.31 Setting up and uploading files to OneDrive in Windows 10

Not Available in Demo Version

5.32 Backup files to another drive in Windows 10

Not Available in Demo Version

5.33 Restore the files backed-up before in Windows 10

Not Available in Demo Version

5.34 Formatting hard drive in Windows 10

Not Available in Demo Version

5.35 Turning On/Off BitLocker for Data Drive in Windows 10

Not Available in Demo Version

5.36 Installing/Updating graphic card driver in Windows 10

Not Available in Demo Version

5.37 Manage Location services in Windows 10

Not Available in Demo Version

5.38 Manage app permissions for camera in Windows 10

Not Available in Demo Version

5.39 Auto Lock using Screen Saver in Windows 10

Not Available in Demo Version

5.40 Uninstall or remove apps and programs in Windows 10

Not Available in Demo Version

5.41 To stop automatic updates in Windows 10

Not Available in Demo Version

5.42 Objective Test 5 Answer the following questions

Not Available in Demo Version

5.43 Microsoft Teams Labs

5.43.1 Creating a team using Microsoft Teams

Not Available in Demo Version

5.43.2 Joining a meeting using Microsoft Teams

Not Available in Demo Version

6. Security

6.1 Identifying Security threat features - 1 (such as Malware , Spyware etc.)

Description: This exercise helps to know about various security threats.

Instructions: 1.Various Security threats are given on the column A
2.Their features are given on the column B
3. Match (drag and drop) the Security threats given on Column A with their respective features given on the column B.

Column A

1. Social engineering
2. Malware
3. Rootkits
4. Phishing
5. Shoulder surfing

Column B

- 1.It is the use of deception and manipulation to obtain confidential information.
2. Software that is specifically designed to gain access or damage a computer without the knowledge of the owner.
3. Type of malicious software that is activated each time your system boots up.
4. E-mail fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients.
5. Act of obtaining personal or private information through direct

- observation.
6. Spyware
 6. Tracking software aids in gathering information about a person or organization without their knowledge.

Explanation:

Social Engineering: Social engineering is a process in which an attacker attempts to acquire information about your network and system by social means, such as by talking to people in the organization. Social engineering is grouped into three methodologies:

1. Phishing: The practice of sending emails appearing to be from reputable sources with the goal of influencing or gaining personal information.
2. Vishing: The practice of eliciting information or attempting to influence action via the telephone, may include such tools as “phone spoofing”.
3. Impersonation: The practice of pre-texting as another person with the goal of obtaining information or access to a person, company, or computer system.

Malware: "Malware" is a term for any software that gets installed on your machine and performs unwanted tasks, often for some third party's benefit. Malware programs can range from being simple annoyances (pop-up advertising) to causing serious computer invasion and damage (e.g., stealing passwords and data or infecting other machines on the network). Additionally, some malware programs are designed to transmit information about your Web-browsing habits to advertisers or other third party interests, unbeknownst to you.

Rootkits: A rootkit is a collection of tools (programs) that enable administrator-level access to a computer or computer network. Typically, a cracker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network.

Phising: The act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. Phishing email will typically direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and will capture and steal any information the user enters on the page.

Shoulder surfing: Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices.

Spyware: Spyware is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet (where it is sometimes called a spybot or tracking software), spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program.

6.2 Identifying Security threat features - 2 (such as Viruses , Worms etc.)

Description: This exercise helps to know about various security threats.

Instructions: 1. Various Security threats are given on the column A
2. Their features are given on the column B
3. Match (drag and drop) the Security threats given on Column A with their respective features given on the column B.

Column A	Column B
1. Viruses	1. Attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels.
2. Worms	2. Self-replicating virus that does not alter files but resides in active memory and duplicates itself.
3. Trojans	3. A program that appears legitimate but performs some illicit activity when run.

Explanation:

Virus: A computer virus is a program designed to harm or cause harm on an infected computer. It spreads through e-mail attachments, portable devices, websites containing malicious scripts and file downloads. A computer virus attaches itself to the host files and always activate whenever you open the infected files. The virus can replicate itself and then infect the other files on your computer causing more damage.

Worms: A computer worm is a self-replicating computer program that penetrates an operating system with the intent of spreading malicious code. Worms utilize networks to send copies of the original code to other computers, causing harm by consuming bandwidth or possibly deleting files or sending documents via email. Worms can also install back doors on computers.

Trojans: Trojans can illegally trace important login details of users online. For example E-Banking is very common among users, therefore, vulnerability of tracing your login details whenever your PC is working without any strong powerful anti-virus installed.

6.3 Identifying functions of digital security methods (such as Antivirus , Firewall etc.)

Not Available in Demo Version

6.4 Identifying various features of physical security methods (such as Tokens , Biometrics etc.)

Not Available in Demo Version

6.5 Identifying various features of data destruction/disposal methods (such as Low level format , Standard format etc.)

Not Available in Demo Version

6.6 Set SSID on a generic WAP router.

Not Available in Demo Version

6.7 Disabling SSID broadcast using the simulator.

6.8 Enable MAC Address filtering in the WAP device, so that the machines matching the MAC addresses are permitted to communicate using the wireless network. The following MAC addresses need to be allowed:

Not Available in Demo Version

6.9 Configure security encryption to WPA 2 with pass phrase.

Not Available in Demo Version

6.10 Pinging to DHCP server

Not Available in Demo Version

6.11 Configuring Wireless Security on an Access Point (WEP)

Not Available in Demo Version

6.12 Objective Test 6 Answer the following questions

Not Available in Demo Version

7. Mobile Devices

7.1 Identifying the various methods to secure mobile devices (such as Passcode locks , Remote wipes etc.)

Description: This exercise helps to know about the various methods to secure mobile devices and their features.

Instructions: 1. Various methods to secure mobile devices are given on the column A
2. Their features are given on the column B
3. Match (drag and drop) the method given on Column A with their respective features given on the column B.

Column A

1. Passcode locks
2. Remote wipes
3. Remote backup application
4. Failed login attempt restrictions

Column B

1. Implementing the Pattern, PIN, or Password you use to access the mobile device.
2. Instructions that are sent remotely to a mobile device that erase all the data in cases where the device is stolen.
3. Backing up the data with the iPhone by connecting the device to a Mac and using iTunes to manage the content
4. set to perform a remote wipe of the device after repeated failed login attempts.

Explanation:

Passcode locks: One of the most basic security measures is to implement a passcode lock on the device. This is akin to implementing the password you use to log on to your desktop or laptop. This can prevent someone from using the mobile device if it is stolen.

1. Setting the password on an Android phone is done by navigating to Settings Location & Security ⇒ Change Screen Lock. On the Change Screen Lock page, you can set the length of time the device remains idle until the screen locks as well as choose a method from None, Pattern, PIN, or Password. Select Password, and then enter the desired password.
2. On an iOS-based device, navigate to Settings ⇒ General ⇒ Passcode Lock to set the password and Settings ⇒ General ⇒ Auto-Lock to set the amount of time before the iPhone locks.

Remote wipes: A remote wipe refers to a system where an administrator has the ability to remotely delete data on a hardware device or system. Remote wipe features are often part of comprehensive security management systems that address issues like bring your own device (BYOD) policies or security gaps in distributed computing networks.

Remote backup application: Online backup, also known as remote backup, is a method of offsite data storage in which files, folders, or the entire contents of a hard drive are regularly backed up on a remote server or computer with a network connection.

Failed login attempt restrictions: This feature is available on a mobile device which can be set to perform a remote wipe of the device after repeated failed login attempts.

1. On the iOS, the Erase Data function can be set to perform a remote wipe after 10 failed passcode attempts. After 6 failed attempts, the iPhone locks out users for a minute before another passcode can be entered. And the device increases the lockout time following each additional failed attempt.
2. The Android does not have this feature built in but does provide the APIs that allow enterprise developers to create applications that will do this.

[Back](#)

7.2 Steps to configure Email on android mobile devices

Not Available in Demo Version

7.3 Identifying features of mobile devices (such as ARM , Bluetooth etc.)

Not Available in Demo Version

7.4 Identifying basic features of mobile operating system (such as ACPI , OSPM etc.)

Not Available in Demo Version

7.5 Connecting smart phone to a wireless network

Not Available in Demo Version

7.6 Connecting smart phone to PoP3 email server

Not Available in Demo version

7.7 Objective Test 7 Answer the following questions

Not Available in Demo Version

8. Troubleshooting

8.1 Identify the troubleshooting tools

Description: This exercise helps to know about the various troubleshooting tools and their features

Instructions: 1. Various troubleshooting tools are given below
2. Drag and drop the name of the tool to their respective places.



Explanation:

A **punch-down tool** is used when you are securing cables to the patch panel that have been run from the wall outlets into the switch room. A wire is pre-positioned into a slotted post, and then the punch-down tool is pressed down on top of the wire, over the post. Once the required pressure is reached, the internal spring is triggered, and the blade pushes the wire into the slot, cutting the insulation and securing the wire.

Toner probes (also called tone generators) are used to locate the correct cable coming into a patch panel from the wall outlet when connections have either not been labelled or the labels have been removed from the patch panel. They are two-piece units (sometimes called Fox and Hound) where one end sends a signal and the other end is used to locate the wires that contain the signal in the switch room.

A **crimper** is used to attach a connector to a cable by securing each wire (8 of them in a twisted-pair wire) to the proper connector in an RJ-45 connector. It usually also includes a stripper as well.

Loopback plugs are used to test the functionality of various types of ports, but their most common use is to test a network card. These plugs send a signal out of the card and then loop it back into the same card to test its operation. They look like an RJ-45 connector without the cable.

Parallel loop back tester will provide you with the ability to diagnose any problems with your DB25 parallel port or DB25 parallel cable. This loop back tester consists of a single DB25 male end for verifying accurate DB25 port functioning.

Below fig. shows after dragging and dropping correct option on the image.



[Back](#)

8.2 Identifying the functions of various troubleshooting tools (such as Fixmbr , Fixboot etc.)

Not Available in Demo Version

8.3 Identify the networking troubleshooting command.

Not Available in Demo Version

8.4 Troubleshoot WiFi connection on a Windows Workstation

Not Available in Demo Version

8.5 Configuring IP address, subnet mask, default gateway statically on a Windows client workstation.

Not Available in Demo Version

8.6 Objective Test 8 Answer the following questions

Not Available in Demo Version

9. Appendix

9.1 Installing PATA/IDE drives

Explanation: Parallel ATA (PATA) is an IDE standard for connecting storage devices like hard drives and optical drives to the motherboard. PATA generally refers to the types of cables and connections that follow this standard. It's important to note that the term Parallel ATA used to simply be called ATA. ATA was retroactively renamed to Parallel ATA when the newer Serial ATA (SATA) standard came into being.

PATA cables are long, flat cables with 40-pin connectors (in a 20x2 matrix) on either side of the cable. One end plugs into a port on the motherboard, usually labeled IDE, and the other into the back of a storage device like a hard drive. Some PATA cables have an additional connector midway through the cable for connecting yet another storage device.

PATA cables come in 40-wire or 80-wire designs. Most modern storage devices require the use of the more capable 80-wire PATA cable to meet certain speed requirements. Both types of PATA cables have 40-pins and look nearly identical so telling them apart can be difficult. Usually though, the connectors on an 80-wire PATA cable will be black, gray and blue while the connectors on a 40-wire cable will only be black.

[Back](#)

9.2 Installing SATA drive

Description: This lab exercise helps you to learn the installation procedure for SATA drives.

Instructions: 1. Power down your computer

2. Ground yourself
3. Find the hard drive bay
4. Disconnect the old hard drive (if replacing).
5. Remove the old hard drive.
6. Insert the new hard drive into an empty bay.
7. Secure the drive.
8. Connect the SATA cables to the hard drive.
9. Connect the data cable to the motherboard

Explanation:

Serial ATA (SATA) is an IDE standard for connecting devices like optical drives and hard drives to the motherboard. The term SATA generally refers to the types of cables and connections that follow this standard.

SATA cables are long, thin, 7-pin cables. One end plugs into a port on the motherboard, usually labeled SATA, and the other into the back of a storage device like a hard drive.

Serial ATA replaces Parallel ATA as the IDE standard of choice for connecting storage devices inside of a computer. SATA storage devices can transmit data to and from the rest of the computer over twice as fast as an otherwise similar PATA device.

[Back](#)

9.3 SCSI drives

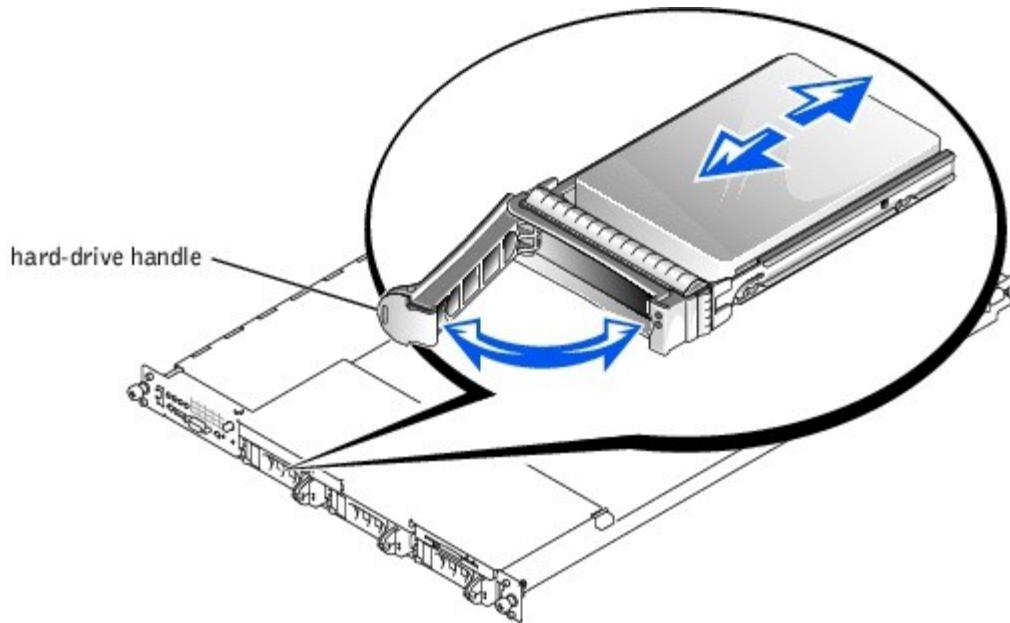
9.3a Installing SCSI drives on a bus

Description: This lab exercise helps to learn the installation procedure of SCSI drives on a bus.

Instructions:

Note : Hot-plug drive installation is not supported for systems without the optional ROMB card.

1. If the system does not have a ROMB card installed, shut down the system.
2. Remove the front bezel, if attached.
3. Open the hard-drive handle(see figure below)



4. Insert the hard drive into the drive bay. See fig above
5. Close the hard-drive handle to lock the drive in place.
6. Replace the front bezel, if it was removed in step 3.
7. If the hard drive is a new drive, run the SCSI Controllers test in the system diagnostics.

9.3b. Removing SCSI drives on a bus

Description: This lab exercise helps to learn the procedure to remove SCSI hard drive from a bus

NOTE: Hot-plug drive installation is not supported for systems without the optional ROMB card.

Instructions:

1. If the system does not have a ROMB installed, shut down the system.
2. Remove the front bezel, if attached.
3. For systems with a ROMB card, power down the hard-drive bay and wait until the SCSI hard-drive indicators on the drive carrier signal that the drive can be removed safely.
4. If the drive has been online, the green power on/fault indicator will flash as the drive is powered down. When both drive indicators are off, the drive is ready for removal.
5. Open the hard-drive handle to release the drive.
6. Slide the hard drive out until it is free of the drive bay.
7. Replace the front bezel, if it was removed in step 2.

[Back](#)**9.4. Inserting a memory card and reading its contents**

Description : This lab exercise helps to learn the procedure to insert a memory card and reading its contents.

Instructions : 1. Get a card reader device

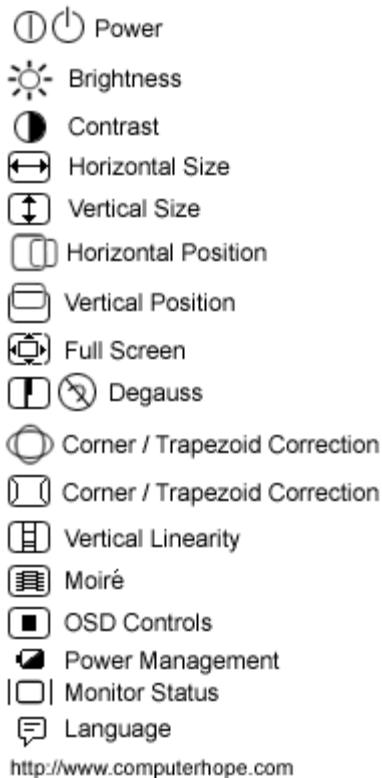
2. Connect the card reader to the computer. To do this, take an USB cable that can be easily recognized by the characteristic connectors. Sometimes, an additional power adapter will be supplied with a card reader device. In this case you need to find the port for the power adapter on the card reader device and then plug it in.
3. If you have installed the card reader correctly you should see blinking lights on the card reader device.
4. Remove your memory card from the device (a camera, a mobile phone and the like) and find an appropriate card reader slot. Keep in mind that the card reader may have several slots for the memory cards of various types and physical dimensions.

[Back](#)**9.5 Degaussing a CRT**

Description : Degaussing a computer monitor can help correct and fix any visual distortions being displayed on a CRT monitor and can also often improve the overall picture being displayed on the monitor.

Instructions :

- 1.To degauss the monitor, open the monitor setup through the buttons found on the front of the Monitor. Using the arrows or pressing the buttons multiple times will allow you to view all available options. One of the options should be degauss, the picture on the right shows what the degauss icons may look like.



2. Once selected, your monitor should make a loud noise and the display will appear to go distorted for a few seconds. If this occurs you've successfully degaussed your monitor.

[Back](#)

9.6 Changing the relative position of the second monitor and changing its resolution to match native resolution

Description: This lab exercise helps you to learn how to change the relative position of a second monitor and its resolution to match the native resolution.

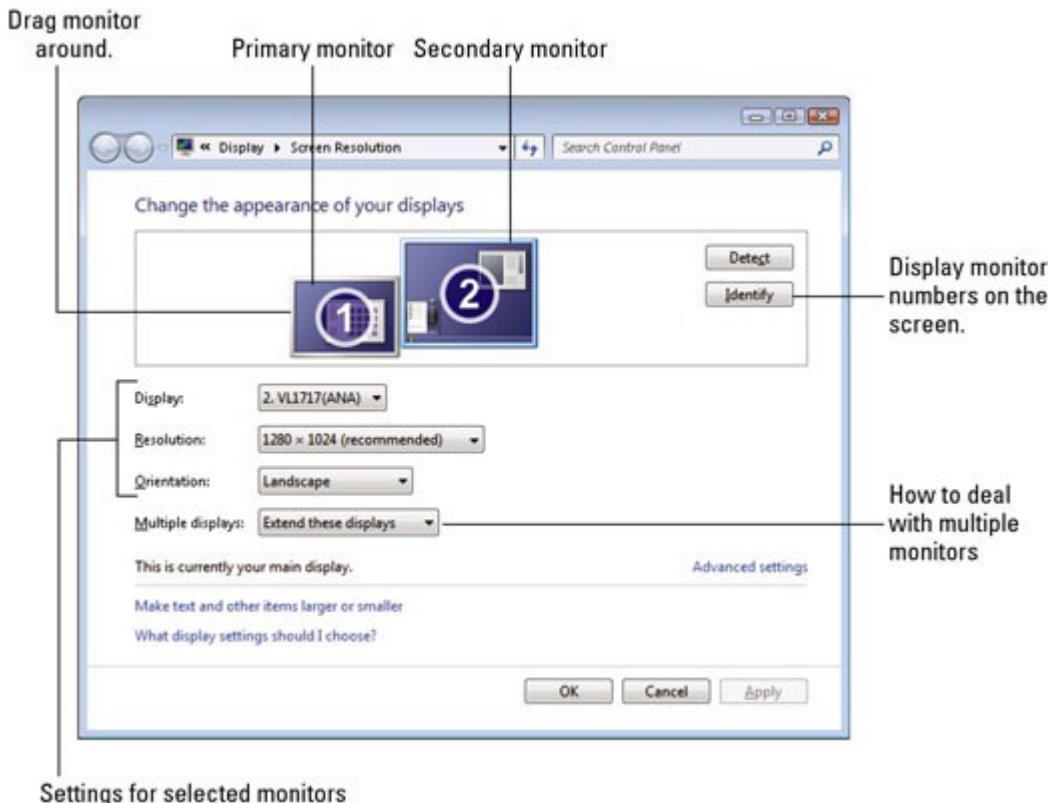
Instructions:

1. To use the second monitor, select it in the Screen Resolution window or Display Settings dialog box. What you do next depends on your version of Windows:

Windows 7: Choose an option from the button My Multiple Displays. Choosing Extend These Displays creates one large desktop across both monitors.

Windows Vista: Choose the option Extend the Desktop Onto This Monitor.

Windows XP: Choose the option Extend My Windows Desktop Onto This Monitor.



[Back](#)

9.7 Stripping and terminating RJ-45 connector

Description: This lab exercise helps you to learn strip and terminate the RJ-45 connector.

Instructions: 1. Using a Crimping tool trim the end of the cable you're terminating, to ensure that the ends of the conducting wires are even.



2. Being careful not to damage the inner conducting wires, strip off approximately 1 inch of the cable's jacket, using a modular crimping tool or a UTP cable stripper.



3. Separate the 4 twisted wire pairs from each other, and then unwind each pair, so that you end up with 8 individual wires. Flatten the wires out as much as possible, since they'll need to be very straight for proper insertion into the connector.



4. Holding the cable with the wire ends facing away from you. Moving from left to right, arrange the wires in a flat, side-by-side ribbon formation, placing them in the following order: white/orange, solid orange, white/green, solid blue, white/blue, solid green, white/brown, solid brown.

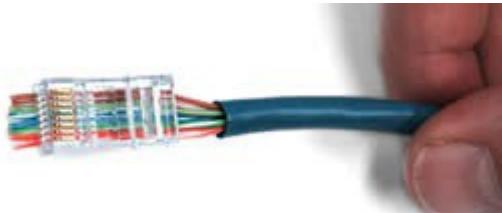


5. Holding the RJ45 connector so that its pins are facing away from you and the plug-clip side is facing down, carefully insert the flattened, arranged wires into the connector, pushing through until the wire ends emerge from the pins for strength of connection, also push as much of the cable jacket as possible into the connector.



6. Check to make sure that the wire ends coming out of the connector's pin side

are in the correct order; if not, remove them from the connector, rearrange into proper formation, and re-insert. Remember, once the connector is crimped onto the cable it's permanent. If you realize that a mistake has been made in wire order after termination, you'll have to cut the connector off and start all over again.



7. Insert the prepared connector/cable assembly into the RJ45 slot in your crimping tool. Firmly squeeze the crimper's handles together until you can't go any further. Release the handles and repeat this step to ensure a proper crimp.



8. If your crimper doesn't automatically trim the wire ends upon termination, carefully cut wire ends to make them as flush with the connector's surface as possible. The closer the wire ends are trimmed, the better your final plug-in connection will be.



9. After the first termination is complete, repeat process on the opposite end of your cable.

[Back](#)



9.8 Installing laptop memory

Description: This lab exercise helps you to learn how to install the laptop memory.

Instructions: 1. Save your work, shut down your computer, and close the display.

2. Disconnect all external devices attached to the laptop (like printers, flash drives, and headsets).
3. Unplug the A/C power cord and adapter.
4. Turn the laptop upside down on a flat surface.
5. Remove the laptop battery
6. Loosen the 3 screws on the memory module compartment
7. Remove the existing memory module(s)
8. Insert the new RAM module into the compartment
9. Align the tabs of the cover with the notches on the computer and close the cover.
10. Tighten the screws on the memory compartment.
11. Replace the battery, reattach the external devices, and plug the laptop back into the A/C outlet.
12. Start your computer

[**Back**](#)

9.9 Replacing the laptop hard drive

Description : This lab exercise helps you to learn how to replace the laptop hard drive.

Instructions:

1. Choose your drive well
2. Backup your files
3. Remove your old drive
4. Install your new drive
5. Configure the new drive

[**Back**](#)

9.10 Using a wireless toggle switch on a laptop to enable the NIC

Description: This lab exercise helps you to know how to enable the NIC in a laptop using a wireless toggle switch.

Instructions:

1. Press and hold the Fn key and then press the F2 key while still holding the Fn key. That will toggle the wireless off.
2. Press Fn+F2 again to toggle the wireless back on.

Note: Some laptops also have a dedicated ON/OFF switch for the wireless connections.
The below figure shows the symbol of wireless toggle switch.



[**Back**](#)

9.11 Inserting and removing the PC Card (Card Bus or Express Card)

9.11a Inserting a PC card

Description: This lab exercise helps you to learn how to insert a PC card.

Instructions: 1. Hold the PC Card label side up and its connectors facing the card slot.
2. Aligning the PC Card along the bottom of the slot, slide the PC Card until it is seated. Most cards are properly seated when the outer edge is flush with the casing of the laptop, but some cards are designed to protrude from the case.



9.11b Removing a PC card

Description: This lab exercise helps you to learn how to remove a PC card.

Instructions: 1. Select the Eject Hardware or Safely Remove Hardware icon in the task bar, select the card you want to remove, then remove the card. This protects your data and helps avoid unexpected problems. If needed, you can restart the card by reinserting it.
2. Press the eject button to extend the button, then press the button again to reject the PC Card.



[Back](#)

9.12 Using a docking station.

Description: This lab exercise helps you to know about the use of a docking station.

Explanation:

- A docking station is a hardware device that allows portable computers to connect with other devices with little or no effort.
- Docking stations enable users with a laptop computer to convert it into a desktop computer when at the office or at home. For example, a user could use their laptop while on the road and then when at the office connect the laptop to the docking station and use their 19" monitor, speakers, and office printer without having to transfer any of the data they may have been working on while on the road.
- The below picture is an example of a Dell docking station, this particular docking station enables the laptop to be directly connected to the docking station without the need of using any additional cables. Keep in mind that all docking stations are different.



Docking Station



Laptop with Docking station

Dock is the term used to describe the process of connecting a portable computer to a docking station.

[**Back**](#)

9.13 Replacing the laptop battery

Description: This lab exercise helps you to learn how to replace the laptop battery.

Instructions:

1. Turn off your laptop and disconnect the AC adapter.
2. Release the latch or other attachment devices that hold your battery in place.
3. Slide the old battery out of its compartment or storage bay.
4. Take the replacement battery out of the box.
5. Slide it into the notch or bay.

[**Back**](#)

9.14 Flashing the laptop's BIOS

Description: This lab exercise helps you to learn how to flash a laptop's BIOS.

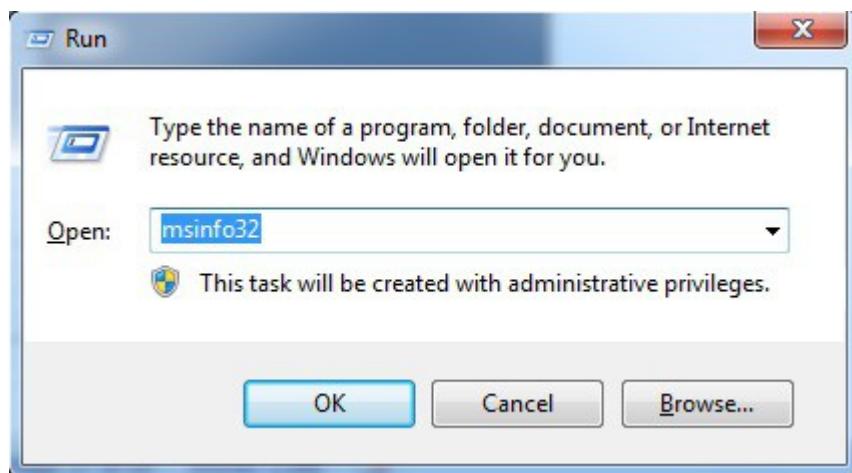
Instructions:

Step 1: Find the current BIOS version number

To find the current BIOS version, follow the steps below

- Windows 8: From the Start screen, type msinfo32. Click msinfo32 from the list of results.
- Windows 7 and Vista: Click Start, enter msinfo32 in the search field, and then select msinfo32.exe from the list of results

Windows XP: Click Start, select Run, enter msinfo32.exe in the Open field, and then click OK.



1. In the System Information window under the System Summary category, look for the BIOS Version/Date entry (see in the below figure). This is your current BIOS version.

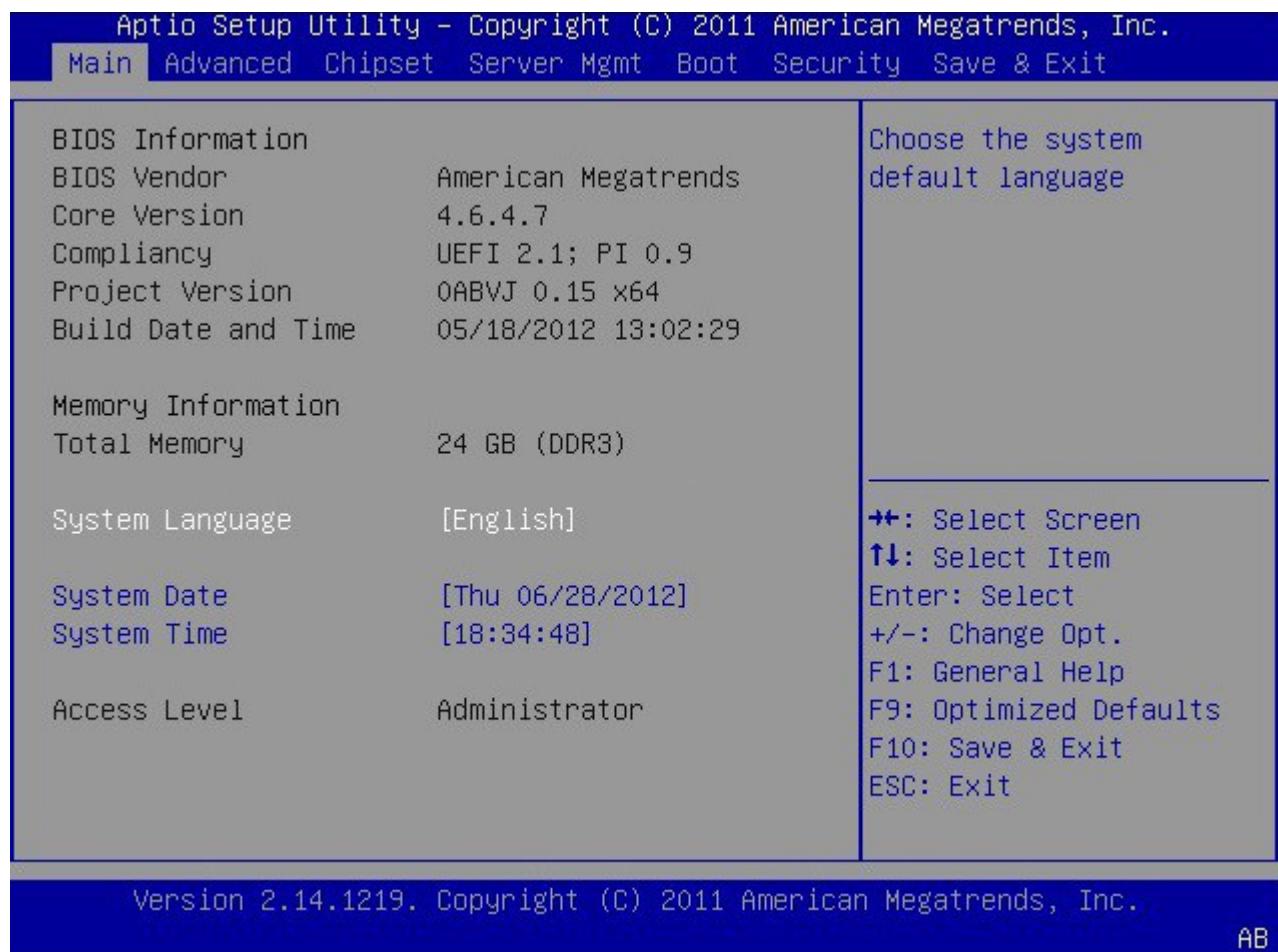
System Information	
File	Edit
System Summary	
Hardware Resources	
Components	
Software Environment	
	Item Value
	OS Name Microsoft Windows 7 Ultimate
	Version 6.1.7601 Service Pack 1 Build 7601
	Other OS Description Not Available
	OS Manufacturer Microsoft Corporation
	System Name ANAND
	System Manufacturer INTEL
	System Model DH61HO_
	System Type X86-based PC
	Processor Intel(R) Pentium(R) CPU G630 @ 2.70GHz, 2700 Mhz, 2 Cores, 2 Logical Proc...
	BIOS Version/Date Intel Corp. H0H610H-B6A/0010.3012.0424.1632, 4/24/2012
	SMBIOS Version 2.7
	Windows Directory C:\Windows
	System Directory C:\Windows\system32
	Boot Device \Device\HarddiskVolume1
	Locale United States
	Hardware Abstraction Layer Version = "0.1.7601.17314"
	User Name ANAND\Admini
	Time Zone India Standard Time
	Installed Physical Memory (RAM) 2.00 GB
	Total Physical Memory 1.90 GB
	Available Physical Memory 882 MB
	Total Virtual Memory 3.79 GB
	Available Virtual Memory 2.49 GB

2. Write down the BIOS version and continue to the next section.

Step 2: Download and install the BIOS update

To download and install the BIOS update for your computer, read and follow instructions on the download page carefully and complete the following steps:

1. Before installing the BIOS update, close any open programs and temporarily disable your anti virus software. Remember to re-enable the antivirus software after the installation is complete.
2. Click the Download link next to the BIOS update file for your computer.
3. When prompted, choose Run or Save depending on how you would like to install the updated. The Run button allows you to download and install the BIOS update from this screen.
4. If you want to install the BIOS update later, or if you are downloading the update to install on a different computer, choose Save to download and save the file to your computer or a removable storage device.
5. If you chose to Save the BIOS update file, navigate to where the file is stored, and double-click the file to begin installation. If you chose to Run the update, continue to step 5.
6. Agree to the terms and then follow the on-screen instructions to install the BIOS update. Do not interrupt the update process.
7. Allow the installation to complete all of its actions, and then restart the computer when prompted.



AB

9.15 Installing and sharing a printer and then testing its functionality

9.15a Installing a printer

Description: This lab exercise helps you to learn how to install a printer.

- Instructions:**
1. Connect the printer to your network by connecting one end of a Cat 5 cable to your router and the other end into the network port of your printer. Turn your printer on and wait for it to become ready.
 2. Get the IP address of your printer. The IP address is what will tell your computer where to find your printer on the network. All network printers allow you to print a configuration sheet which will list basic information about the printer along with the current network configuration.
 3. The last step is to add the printer to your computer. Click on Start, then Printers and Faxes.

9.15b Sharing a printer

Description: This lab exercise helps you to know about sharing a printer between the users.

- Instructions:**
1. Click on Start in the bottom left corner of your screen. A pop up list will appear.
 2. Select Control Panel from the pop up list. Type the word network in the search box.
 3. Click on Network and Sharing Center.
 4. Click on Change advanced shared settings, in the left pane.
 5. Click on the down arrow, which will expand the network profile.
 6. Select File and printer sharing and choose Turn on file and printer sharing. Click on save changes.

9.15c Testing the printer functionality

Description: This lab exercise helps you to know how to test the printer capabilities.

Instructions: To check printing capabilities, print a Self Test Report. To print this test follow the below steps:

1. Turn the printer on and place media in the tray.
2. Slide the paper guide all the way to the right.
3. Turn the printer on.
4. Print a Self Test Report by holding the Resume button for five seconds.
5. If the Self Test Report prints correctly, the printer is functioning properly.
6. If the Self Test Report is printed improperly, is missing colors or black, contains black streaking or white lines, go to the "Verify that the printer driver is installed correctly" section.
7. If the Self Test Report does not print, go to the "Verify if there is a paper jam" section.

9.16 Changing the toner cartridge.

Description: This lab exercise helps you to learn how to change the toner cartridge.

- Instructions:**
1. Remove the old toner cartridge from the printer by pulling the blue toner release lever located on the cartridge fully towards the front of the printer. Then lift the right-hand end of the cartridge and draw the cartridge to the right to release the left-hand end and withdraw from the printer.
 2. Dispose of the old toner cartridge in the plastic bag that came with the new cartridge.
 3. Gently shake the new cartridge from side to side several times to loosen and distribute the toner evenly inside.
 4. Remove the wrapping material and peel off the adhesive tape from the underside of the cartridge.
 5. Hold the new cartridge by its top center with the blue lever to the right and lower the cartridge into the printer over the image drum unit from which the old cartridge was removed. Insert the left end of the toner cartridge into the top of the image drum unit pushing it against the spring on the drum unit, then lower the right end of the cartridge down onto the image drum unit.
 6. Push the blue lever towards the rear of the printer, this will lock the cartridge into place and release toner into the image drum unit.

[Back](#)

9.17 Troubleshoot hard drives and RAID arrays with appropriate tools

Description: This exercise explains troubleshooting of hard drives and RAID arrays with appropriate tools.

- Instructions:**
1. If the CMOS setup is not properly setup the computer may ignore or not look at the CD-ROM as a bootable option. Verify in the CMOS that your settings are properly set to boot from the CD-ROM drive.
 2. The Complementary Metal-Oxide Semiconductor (CMOS) allows the computer to store the Real Time Clock (RTC) and other device information even after the computer is switched off and on. This is achieved by using a battery just for CMOS.
 3. Generally, these settings will be under the boot options. Setup your boot options similar to the below example.

- 1 - Floppy / LS120
- 2 - CD-ROM

3 - Network (if available)

4 - Hard Disk Drive

4. If CD-ROM is listed after a device that is bootable it will boot from the other device before the CDROM. Verify that the devices before CD-ROM, such as floppy, do not have bootable media in them.
5. If the SCSI bus termination is not done, SCSI devices on the bus will not function properly. This is due to reflection of the signals at the end of the bus. To prevent this, both ends of the SCSI bus needs to be terminated. If one end of the SCSI bus is terminated, you may find intermittent problems. Never terminate the bus at a device connected in between.
6. If you are creating a Striped volume on a new Windows 2000 machine, it can only be created on dynamic disks. However, if you are upgrading a Windows NT computer to Windows 2000, any existing stripe set will be supported.
7. If you are finding that the Logical Disk > %Free Space counter is less than 10%, you might need to make additional free space available. This can first be done cleaning up the disk of any unwanted files, duplicate files etc. If required, additional physical disk may be provided.
8. If you have a standard desktop PC that uses integrated drive electronics (IDE) disk drives, then these will be detected during setup. If, however, you use SCSI disks or have Redundant Array of Independent Disk (RAID) storage systems, you will see, shortly after the reboot, the following line of text displayed at the bottom of the screen:
9. "Press F6 if you need to install a third party SCSI or RAID driver..." Pressing F6 will start a dialog that allows you to configure and install the drivers for your SCSI or other disk subsystem controllers. This option is usually used on server platforms that use large-capacity, high-speed, fault-tolerant disk subsystems. For most PCs, however, you won't need to use this option.
10. If you want to format a drive and also make it bootable, you need to format with /s switch. By issuing this command, the boot files IO.SYS, MSDOS.SYS, COMMAND.COM get copied to the disk
11. It is obvious that you can get shock is due to sudden discharge of static electricity. Since the operator is touching the memory module when the discharge happened, it is most likely that the memory module may have internally damaged. This damage may or may not show up immediately. In any case, it always recommended to replace the statically damaged module with a good one. Follow anti-static precautions before touching any electronic components inside a PC.
12. It is recommended that the backup tape is stored at a location away from the building where the backup was taken. For most companies, backups contain important data and loosing backups may affect the continuity of one's business. If a backup is stored in the same building, it may get damaged in fire or any other natural calamities along with the computers. As a result, both the server, as well as back fail at the same time. Therefore, it is recommended to store the backup at a different location.
13. If the hard-disk is making sound, the most likely problem is that the hard disk read/write head is scratching the disk surface. It often results in the total failure of the disk. If you find that you can still read/write to the disk, backup the hard disk and replace immediately.

14. Low level formatting will erase the data on a hard drive permanently.

15. A hard disk should never be low level formatted at the customer premises. It is highly recommended that it is done at the manufacturer's or at any authorized center. It is very cumbersome to change the partition sizes, once the hard disk is partitioned and used. It may require backing up all the data and restoring after re partitioning.

[**Back**](#)

9.18 Troubleshoot printers with appropriate tools

Description: This exercise explains troubleshooting printers with proper tools.

Instructions:

1. Some of the frequently encountered problems using laser printers and probable causes are as given below.

I. Speckled Pages : The cause for this may be

- a. The failure to clean the drum after printing properly, or
- b. The drum might have developed scratches.

II. Blank Pages : The causes for white pages may be,

- a. The toner would have dried out, replace the toner.
- b. The transfer corona, that is responsible for transferring the toner to the drum might have failed.
- c. The High Voltage Power Supply (HVPS) failure will also result in white pages.

III. Ghosted Images: Ghosting occurs when previously printed pages are printed again, though much lighter than the present image. The most likely cause is that the erasure lamp might not be working properly, thus leaving some charges representing the earlier image left on the photosensitive drum before new image is written. Also check the cleaning blade, which is responsible for scaping the residual toner.

IV. Smudged images: If the fusing fails, the toner will not bond with the paper. Check the halogen lamp responsible for heating.

2. The following are the 6 steps in the ElectroPhotographic (EP) print process of Laser Printer:

a. Cleaning: Cleaning the photosensitive drum includes residual toner left on the drum and removing the electrical charges left out on the drum. The physical cleaning is done with a rubber blade and the electrical charge cleaning is done with erasure lamps.

b. Charging: The next step in printing, is to charge the photo sensitive drum with high negative charge, this is done with the help of a corona wire.

c. Writing: A laser (type 3) sweeps the entire length of the drum, creating the static image of the matter to be printed. The places where the laser travel, the highly charges are neutralized. Other places of the drum, it remains highly negatively charged.

d. Developing: Now drum gets in close proximity to the toner. Because the toner is negatively charged, it gets attracted to the areas where the drum is neutral. It will not be attracted to the

places where the drum is highly negatively charged. Thus the image of the page to be printed formed on the photosensitive drum.

e. Transferring: Now, the toner on the drum gets attracted toward the paper, by using highly positive charges developed on the surface of the paper. The "transfer corona" is used to generate highly positive charge on the paper surface and to attract the toner from the drum. Thus the image of the page to be printed formed on the paper. But still, the toner is loose and can get easily smeared.

f. Fusing: In order to permanently bond the toner particles to the paper, the paper is passed through rollers. One of the rollers, the non stick roller is heated by a high intensity lamp, generating the heat necessary to bond the toner to the surface of the paper.

3. When a printer is installed on a network, default printer permissions are assigned that allow all users to print. Because the printer is available to all users on the network, you might want to limit access for some users by assigning specific printer permissions. For example, you could give all non-executive users in a department the Print permission and give all managers the Print and Manage Documents permissions. You can also deny print permission to all others. In this way, all non-executive users and managers can print documents, but managers can also change the print status of any document sent to the printer.

4. Normally, the printer supplier provides a driver that goes with the XP OS. It is always preferable to use the driver supplied by the device manufacturer along with the printer.

[Back](#)

9.19 Troubleshoot, and repair common laptop issues while adhering to the appropriate procedures

Description: This exercise explains procedure to repair common laptop issues.

Instructions:

1. Laptops, being mobile, usually participate on more than one network, and often use a static IP address at one location and a dynamically assigned IP address at another. For example, your computer might use dynamic addressing (DHCP) at the office but need to use a static IP address when at home to connect to a broadband ISP.
2. Most laptop computers require a function key or software command to activate/deactivate the laptop video output signal. Usually, the activation/deactivation command acts as a toggle switch: repeat the command to display the image on the internal laptop display, the external display (projector) or both displays simultaneously. Examples: Acer: Fn+F5, Dell: Fn+F8 will activate/deactivate laptop/external display.
3. The nickel cadmium battery, known as NiCad , used to be the most common type of laptop battery. NiCad batteries could easily be ruined by being left on the charger after they had reached full charge, or by being recharged before they were completely dead. The latter problem, called the "memory effect," meant that if you recharged your laptop battery before it had run completely down, it would remember the point at which you put it back on the charger, and only discharge that far the next time you used it.
4. The nickel metal hydride (NiMH) laptop battery could hold considerably more power than NiCad, but they still had something of a memory effect, although to a lesser extent 5. Lithium ion (Li-Ion) is

the latest technology for laptop batteries. They are considerably lighter and does not exhibit memory effect. The Li-Ion laptop battery lasts considerably longer than its predecessors. If your laptop supports Li-Ion battery, then it is a recommended choice.

[Back](#)

9.20 Troubleshoot common problems related to motherboards, RAM, CPU and power with appropriate tools

1. On a personal computer, the general errors and the corresponding failures are shown below: 100-199 : System board failures 200-299 : Memory failures 300-399 : Key board failures 400-499 : Monochrome video problems 500-599 : Color video problems 600-699 : Floppy disk errors 1700-1799: Hard disk problems.
2. Some of the frequently encountered error codes and their corresponding error messages on a PC are given below.

Error Code----Error Message

- 161 - CMOS battery failure: Replace the CMOS battery
- 164 - Memory size error : If the error occurs after memory upgrade, run SETUP program.
- 201 - Memory test failed : RAM chips failed, one or more may need to be replace.
- 301 - Keyboard error: You may have to check the key board

3. The IRQ numbers and relevant Standard Device Assignment are given below. It is important to memorize these values before going to the exam, as there would be 5-10 questions on IRQs, and conflicts. IRQ----Standard Device Assignment 0-System timer 1-Keyboard 2-Cascade to IRQ9. Can't be used. 3-COM ports 2 and 4 4-COM ports 1 and 3 5-Parallel Port LPT2. Very often used for sound cards. 6-Floppy drive controller 7-Parallel Port, LPT1 8-Real time clock 9-Unassigned (Also redirected from IRQ2) 10-Available 11-Available. SCSI adapter will usually use this IRQ. 12-Mouse or touch pads 13-Math co-processor. 14-Primary hard-disk IDE controller 15-Secondary hard-disk IDE controller.

4. A toner probe is an electronic test instrument to help trace wires. One part (the tone generator) induces a tone on a pair of wires, and with the other you part (the tone probe) you can detect the tone at the other end to trace where the wires go. You can trace wires through walls using a tone probe, and determine which pair is carrying the signal you induced at the other end.

5. A cable tester is used to verify that all of the intended connections exist and that there are no unintended connections in the cable being tested. When an intended connection is missing it is said to be "open". When an unintended connection exists it is said to be a "short" (as in short circuit). If a connection "goes to the wrong place" it is said to be "miswired" (the connection has two faults: it is open to the correct contact and shorted to an incorrect contact).

6. The main difference between a cable tester and a toner probe is that in the former, you have access to the both ends of the cable at the same time, and you normally to Open or Short testing (to determine right pins are connected), and in the latter, you dont have simultaneous physical access to both ends of the cable. An AT computer will have two interrupt controllers. The second interrupt controller needs to deliver the interrupts through the primary interrupt controller. IRQ2 had been identified for this purpose on the primary and IRQ9 on the secondary interrupt controllers. In other words, IRQ2 and IRQ9 are cascaded.

- 7.** AT style systems use two power connectors, P8 and P9 to connect to the motherboard. ATX systems use only one P1 connector to connect to the motherboard.
- 8.** If you are getting a keyboard error, you need to do one of the following things: a. Check if the keyboard needs to be cleaned b. Check if the keyboard cable has become loose c. Check if one or more of the keys are stuck d. If required, replace the keyboard.
- 9.** The battery is supposed to provide backup in the event of any power failure, typically up to 2 hours or more.
- 10.** The best ways to find whether a new hardware is supported by your Windows OS is to check the manufacturer's documentation first, and then the Hardware Compatibility List (HCL). 11. The inverter board is responsible for converting low voltage DC power to high voltage AC, necessary to light up the back-light bulb. If the inverter board is bad, the LCD screen (back-light bulb) will not light up when you turn on the laptop, but you still should be able to see a very dim image on the screen.
- 11.** The inverter board is responsible for converting low voltage DC power to high voltage AC, necessary to light up the back-light bulb. If the inverter board is bad, the LCD screen (back-light bulb) will not light up when you turn on the laptop, but you still should be able to see a very dim image on the screen.
- 12.** The most likely cause for excessive paging is insufficient Memory. Increase the physical Memory on your computer.
- 13.** Date and Time Not Set is the most common error that occurs when the BIOS battery is drained. You need to replace the CMOS battery.
- 14.** The most likely cause for sporadic movement of mouse is dirt. If dirt has entered the mouse, clean the dirt with IPA, or cotton wetted in soap water.
- 15.** The most likely problem is conflicting IRQs. Since the mouse is working until the modem is used, the IRQ/IO address of modem may be conflicting with that of the mouse.
- 16.** The motherboard displayed has the following expansion slots:
- PCI slots : 5 (distinguished by white color, usually the number of PCI slots available on a motherboard varies from 3 to 6)
 - ISA slots: 2 (distinguished by black color, longer than PCI slots, placed next to PCI slots.)
 - AGP slot: 1 (The single slot, next to 5 white PCI slots is AGP slot in brown color. Note that there will be only one AGP slot)
- 17.** To obtain BIOS string ID: a. Power off the system b. Either unplug your keyboard or hold down one of the keys on the keyboard c. Power-on the system and you should get a keyboard error d. The string in the lower left hand corner of your computer screen represents the BIOS String ID.
- 18.** It is also possible to read the BIOS information by going to the BIOS set-up of the PC by pressing appropriate key (usually Del key) during boot up.
- 19.** Various POST (Power On Self Test) error codes and their description is as below: Code 01: Undetermined problem Code 02: Power Supply error Code 1xx: System board errors Code 2xx:

Memory (RAM) errors Code 3xx: Keyboard errors Code 6xx: Diskette Drive errors x is any single digit integer.

20. The following are true about backup:

- a. Full backup: Here all files that have been chosen for backup are backed up, irrespective of whether the archive bit is set or not set. Archive bit is set (ON) after backup.
- b. Incremental backup: Here only the files that have been created or have changed since the previous full or incremental backup will be backed up. The archive bit is set after a file is backed up.
- c. Incremental backup will backup files that have changed since previous full or incremental backup.
- d. Differential backup: Here, the files that have changed or created since the last full backup will be backed up. Note that, unlike Incremental backup, the archive bit is not set on a differential backup. The result of this is that the next differential backup will include files that were backed up during earlier Differential backups.

21. UPS usually contains a filter to smooth the noise, and this filter is called noise filter.

[**Back**](#)

9.21 Troubleshoot common video and display issues

Description: This exercise explains troubleshooting common video and display issues.

Instructions:

1. Monitors accumulate very high static charges and need to be handled very carefully. Before attempting any repair, it is imperative to discharge any accumulated charges on the monitor. You can use a jumper, one end of which is grounded, and touch the other end of the jumper wire to the anode of the monitor. While doing so, ensure that you are not in direct contact with the jumper wire or the anode. You can use a screw driver or a nose pliers with rubber handle for this purpose. A "POP" sound can be heard when the static charges accumulated on the anode lead getting grounded through the jumper wire
2. Never wear a wrist strap when working on monitors. Monitors contain very high voltages, sometimes fatal to human, even when the power is turned off. If you are wearing wrist strap, the human body work as a conduit to discharge the electric charge
3. When you are installing a different SVGA monitor, it is unlikely that the new monitor has the same capabilities as the old one. As a result, the image on the screen may not be readable. In such instances, change the video resolution to Standard VGA before installing the new monitor. You can change the resolution appropriately after the image on the screen is readable with the new monitor. It may also be necessary to load appropriate device driver, if you are installing a different display adapter.
4. The most probable cause that the screen is dumping garbled characters is that the communication settings are not correct. Check the speed, parity, start/stop bits etc. If the serial port parameters are correct, then you need to check the cable, such as straight/cross cable and the pin connections.

5. The problems such as video card, network card, and modem card can be resolved by booting to Safe Mode. While in Safe Mode, troubleshoot the problem.

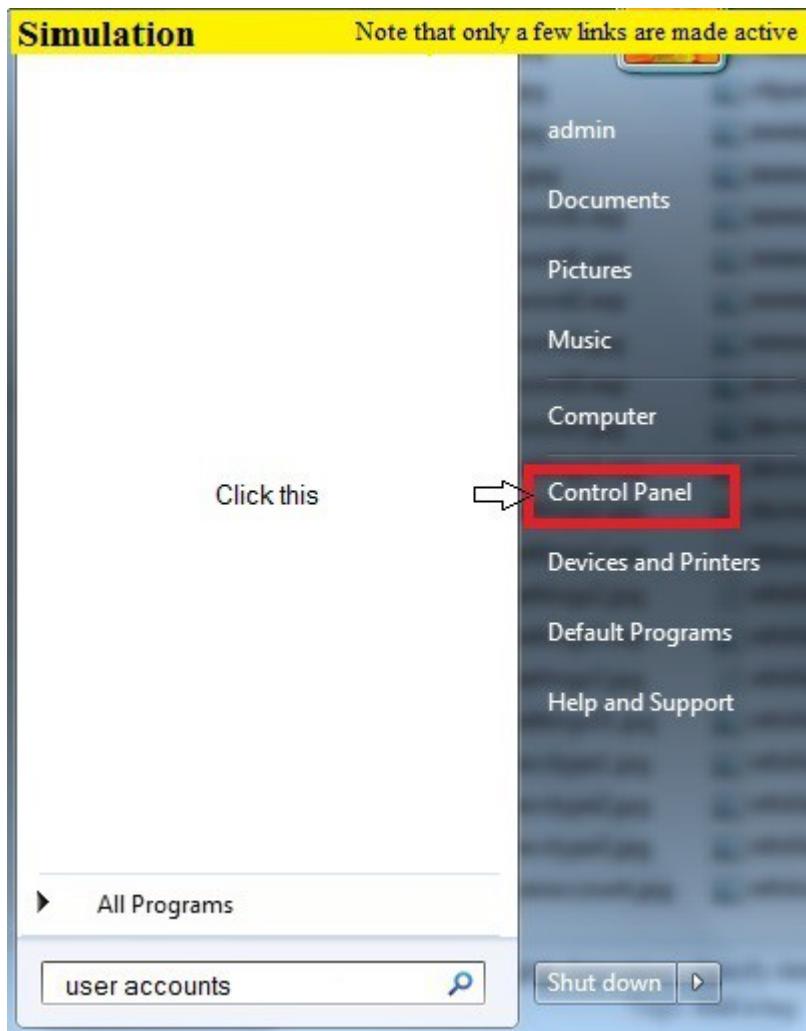
[Back](#)

9.22 User account creation , configuration and authentication in Windows 7

9.22.1 Creating a new user account

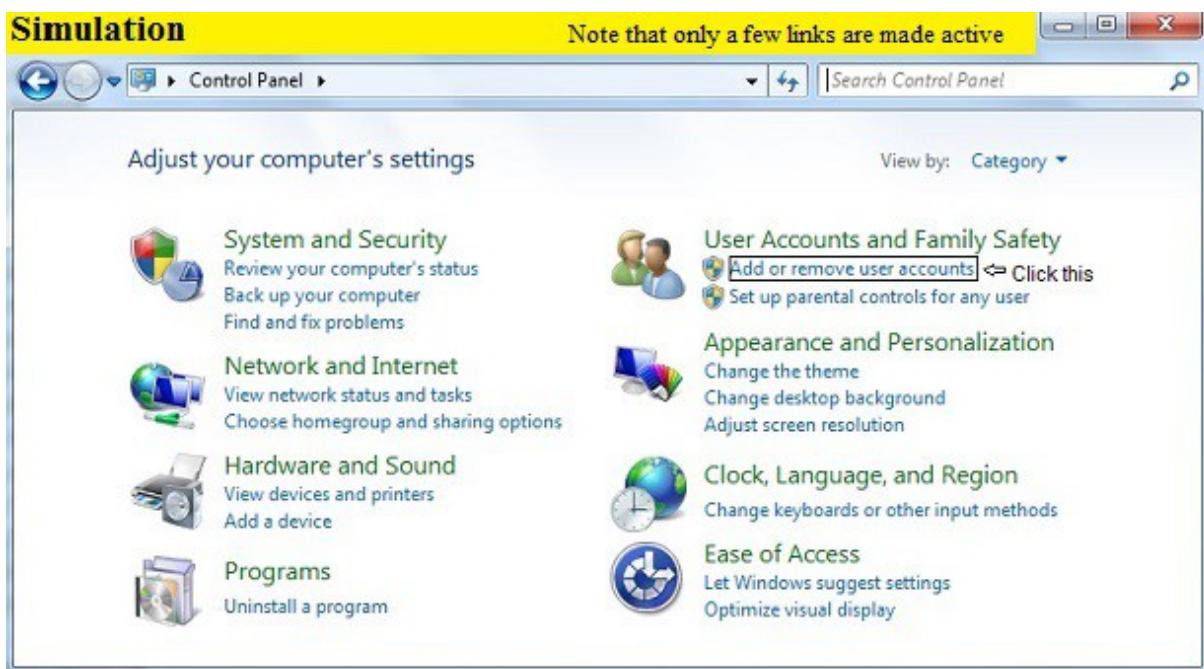
Description: This lab exercise explains how to create a new user account in windows 7

Instructions: 1. On loading a lab exercise, in a given simulation start menu either type “user accounts” in search box or click control panel option

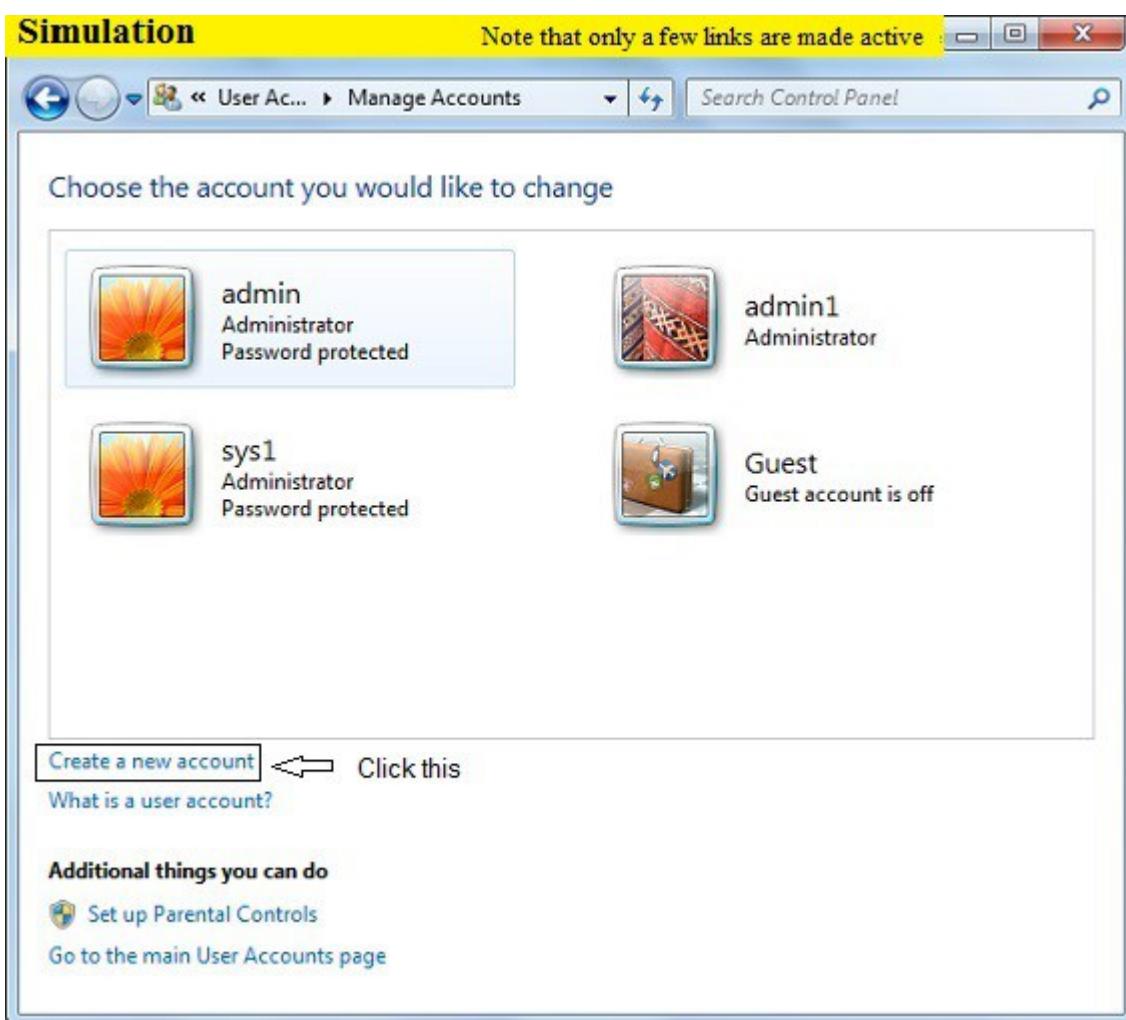


Go to step 2 if control panel option is clicked , otherwise go to step 3

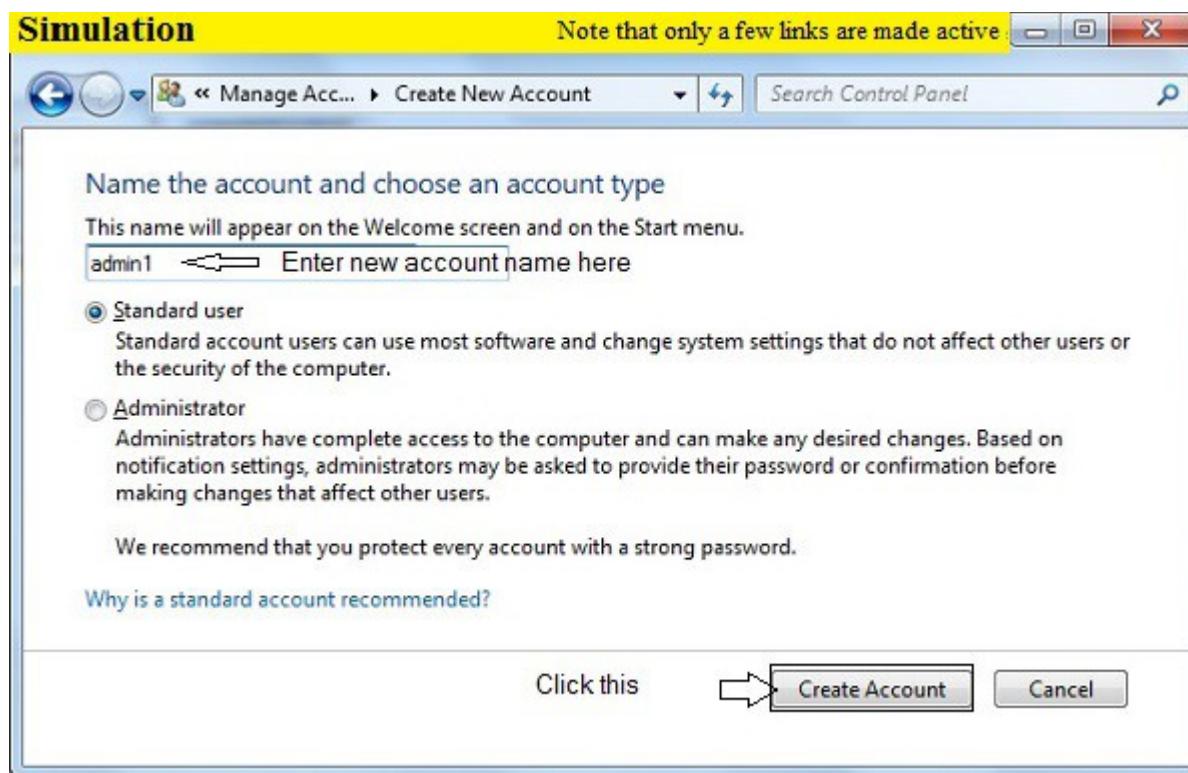
2. In control panel click Add or remove user accounts options.



3. You will now be in the Manage Accounts control panel, to create a new account, click on the Create a new account option.



4. You will now be at the Create New Account screen. In the New account name field enter the name of the new account as “admin1” and click Create Account button.



5. Your new account will have been created and you will see it listed in the Manage Accounts screen.

9.22.2 To change user account password

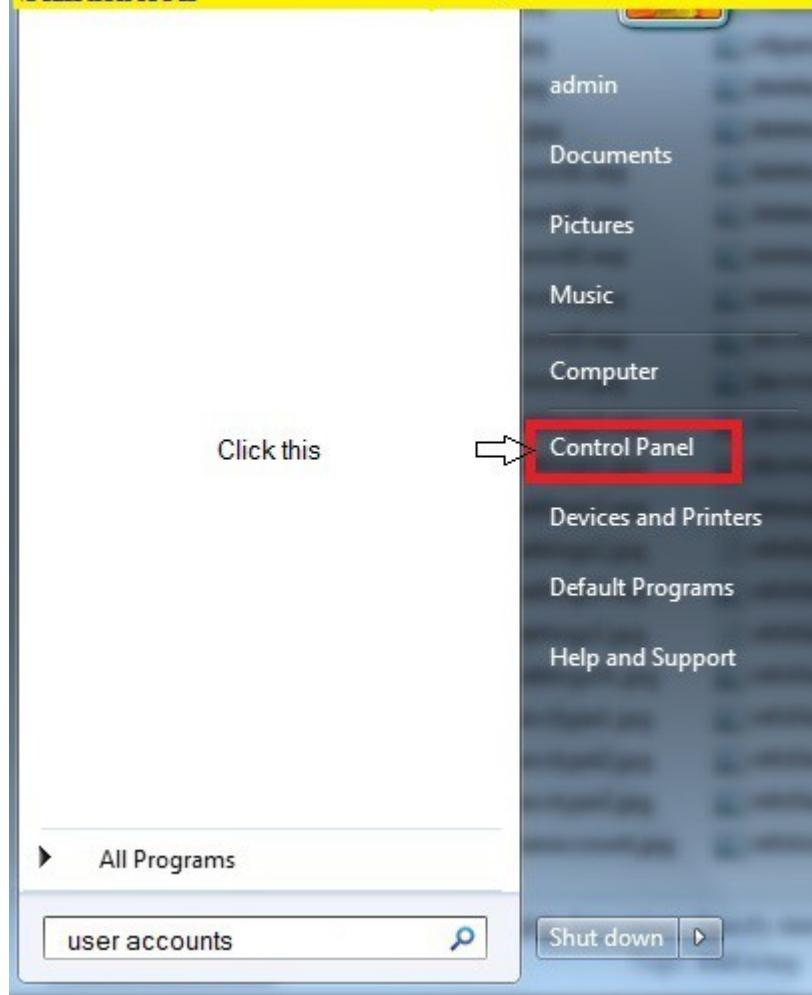
Description: This lab exercise explains changing user account password settings in windows 7.

Instructions: 1. On loading a lab exercise, in a given simulation start menu either type user accounts in search box or click control panel option

go to step 2 if control panel is clicked otherwise go to step 3

Simulation

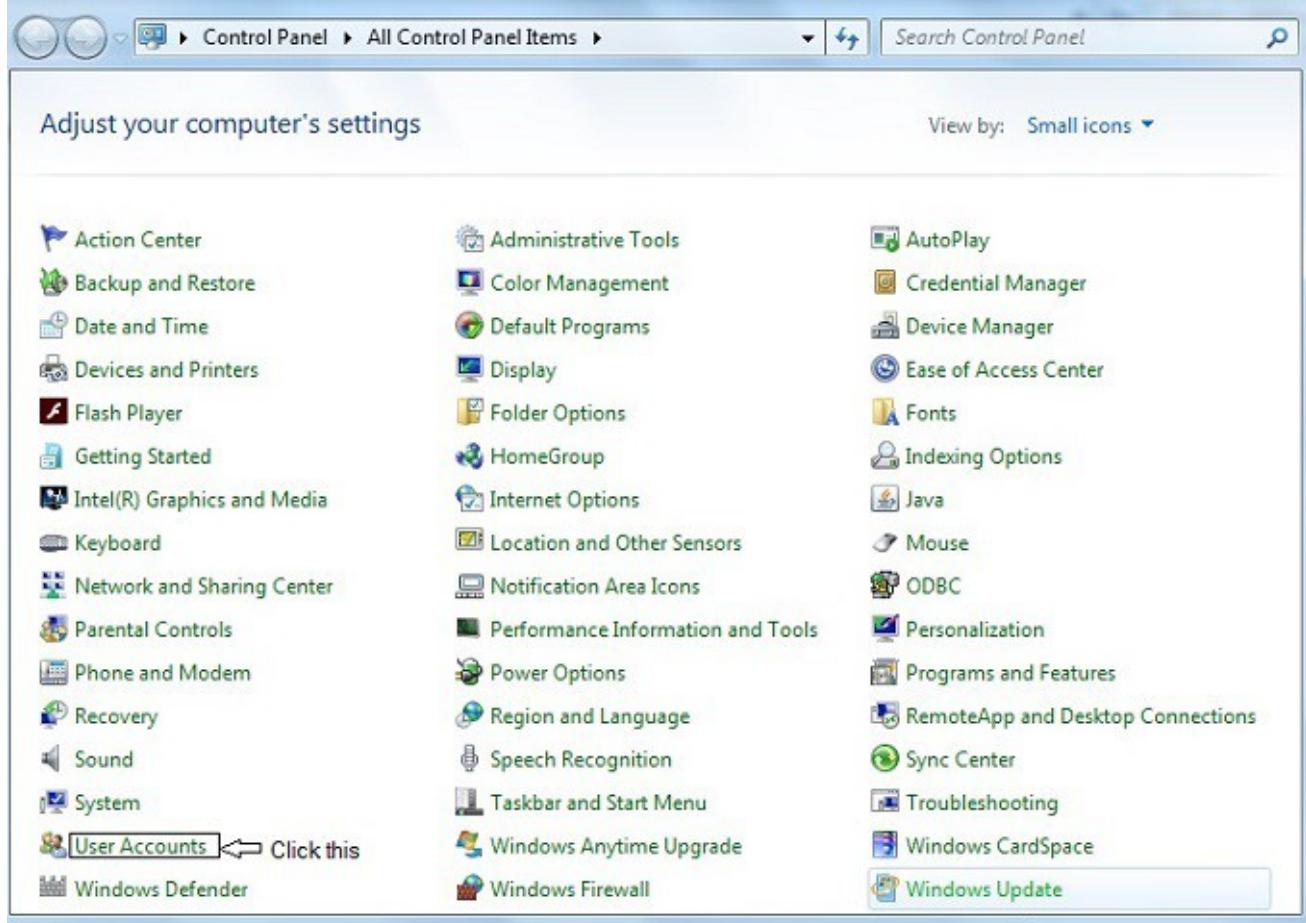
Note that only a few links are made active



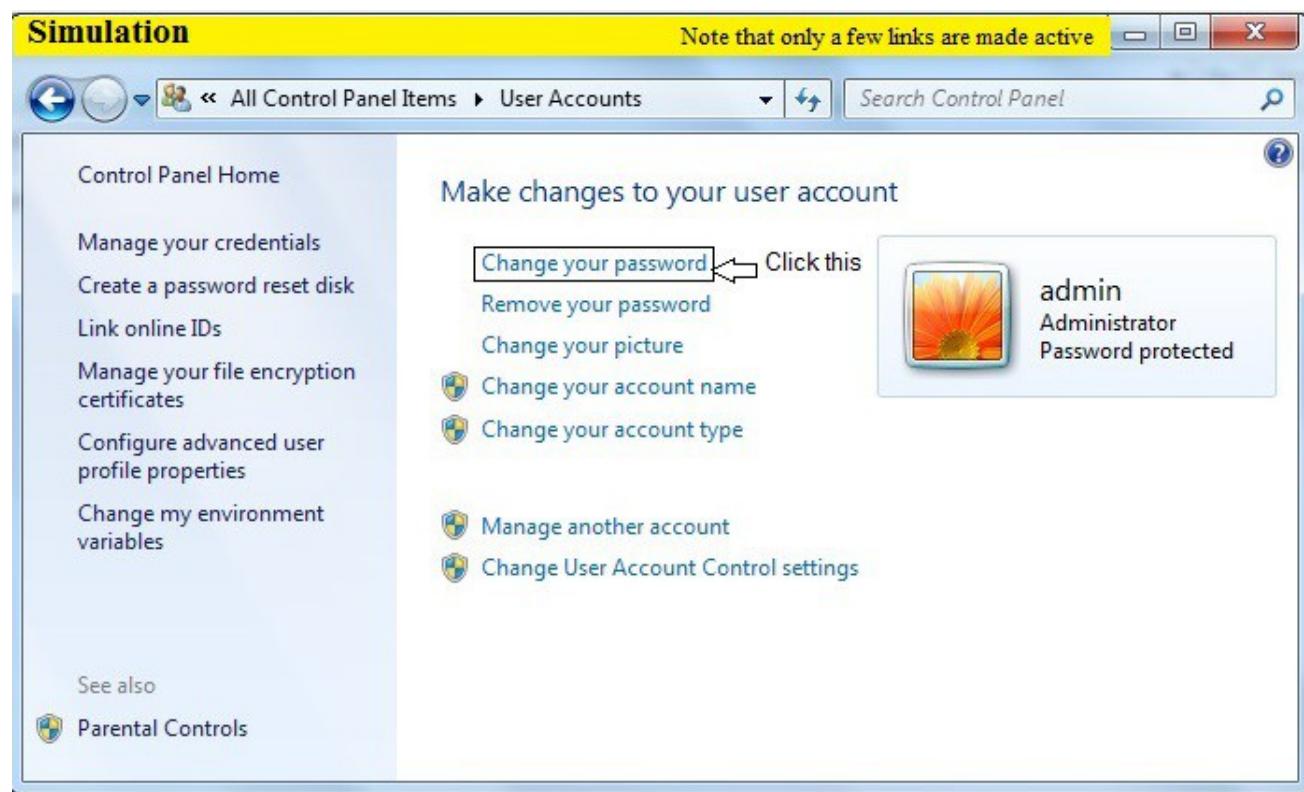
2. In control panel window click User Accounts options

Simulation

Note that only a few links are made active



3. In Make changes to user account screen click change your password option



4. In Change your Password window enter current password as “certexams” , new password as “certexam” and confirm password as “certexam” and click Change password button.



Explanation: You can keep your computer more secure by changing your Windows password regularly and by using a strong password

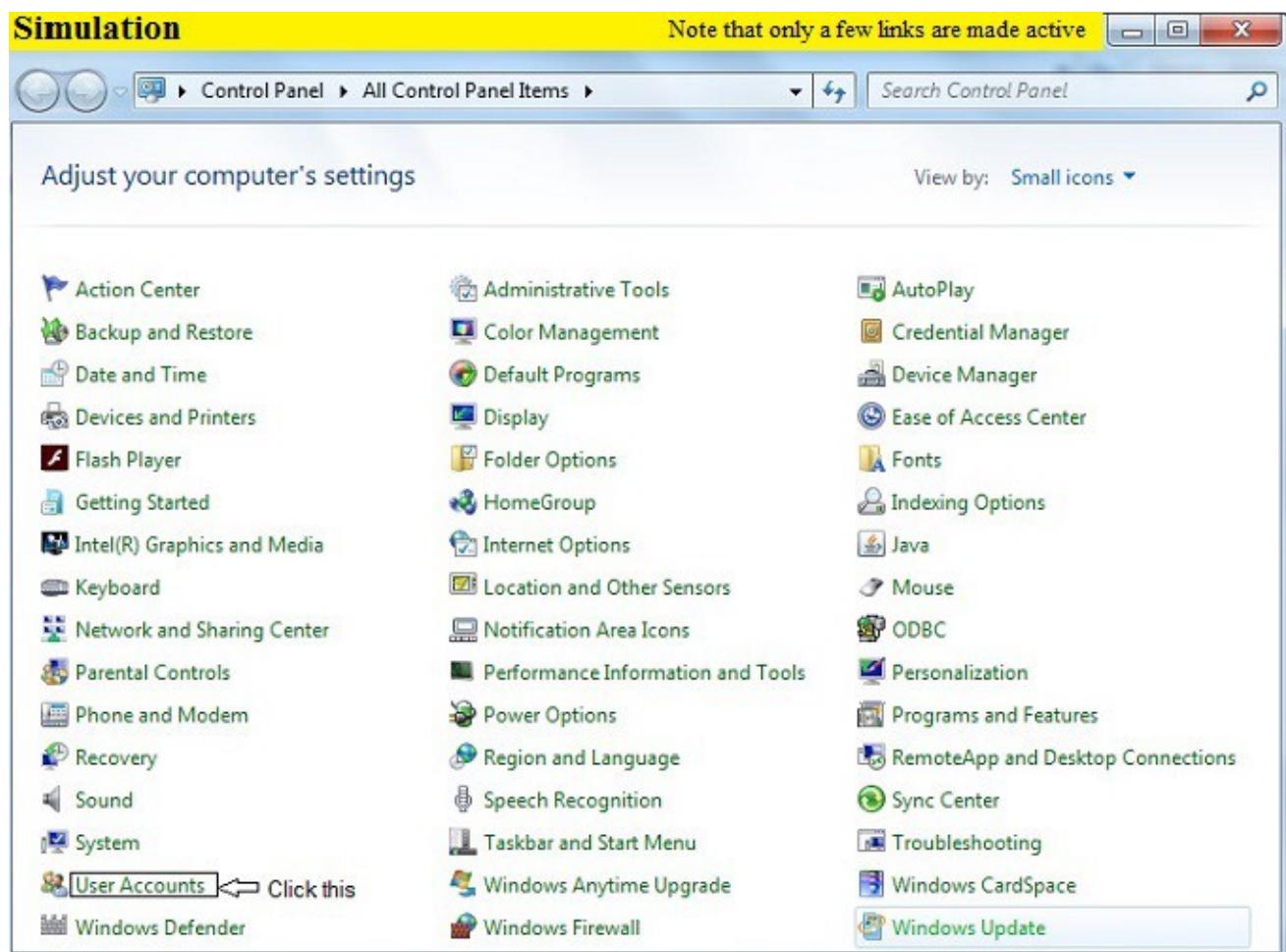
9.22.3 To change user account control settings

Description: This lab exercise explains the procedure on how to change the UAC settings

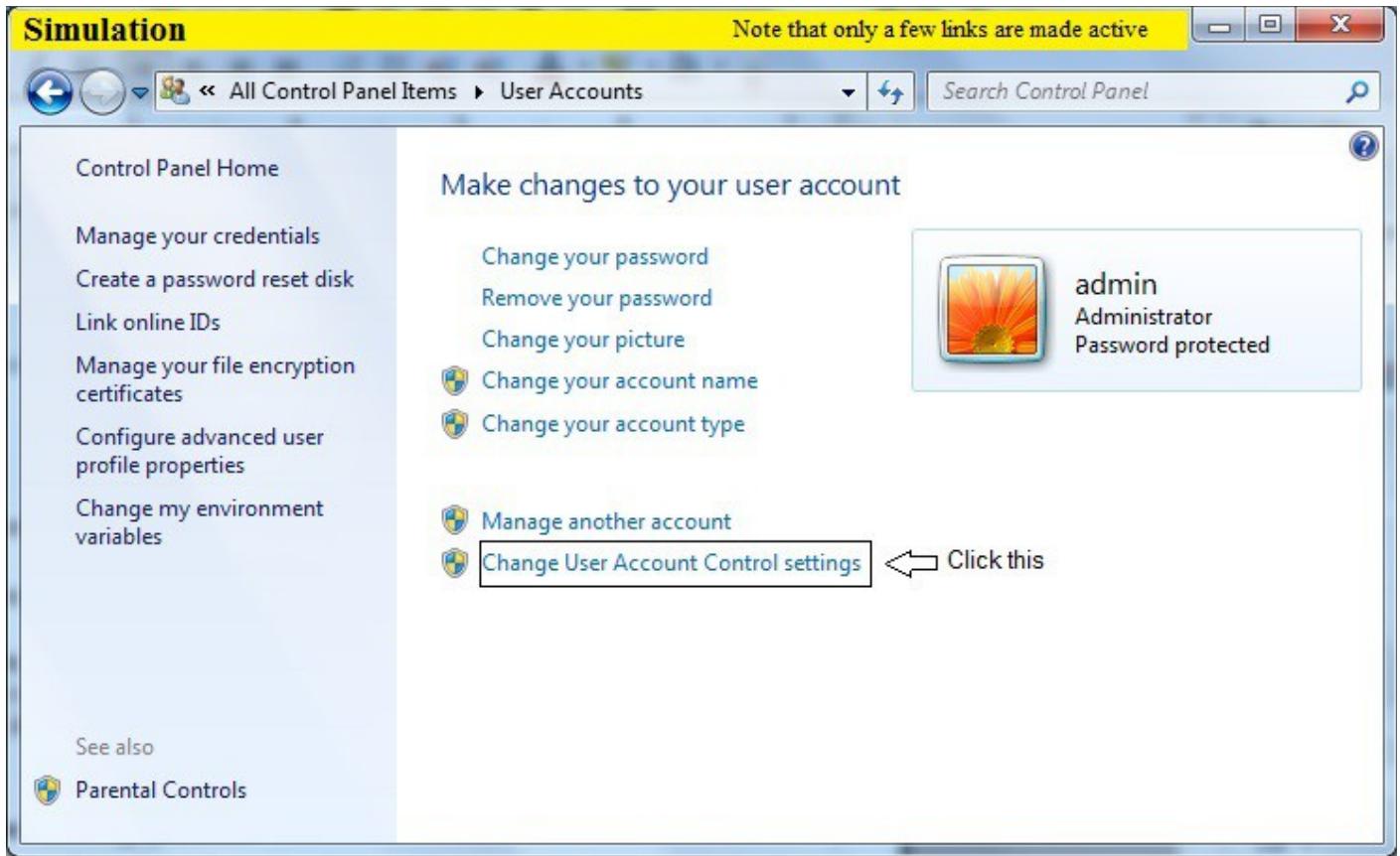
Instructions: 1. On loading a lab exercise, in a given simulation start menu either type user accounts in search box or click control panel option

Go to step 2 if control panel is clicked otherwise go to step 3

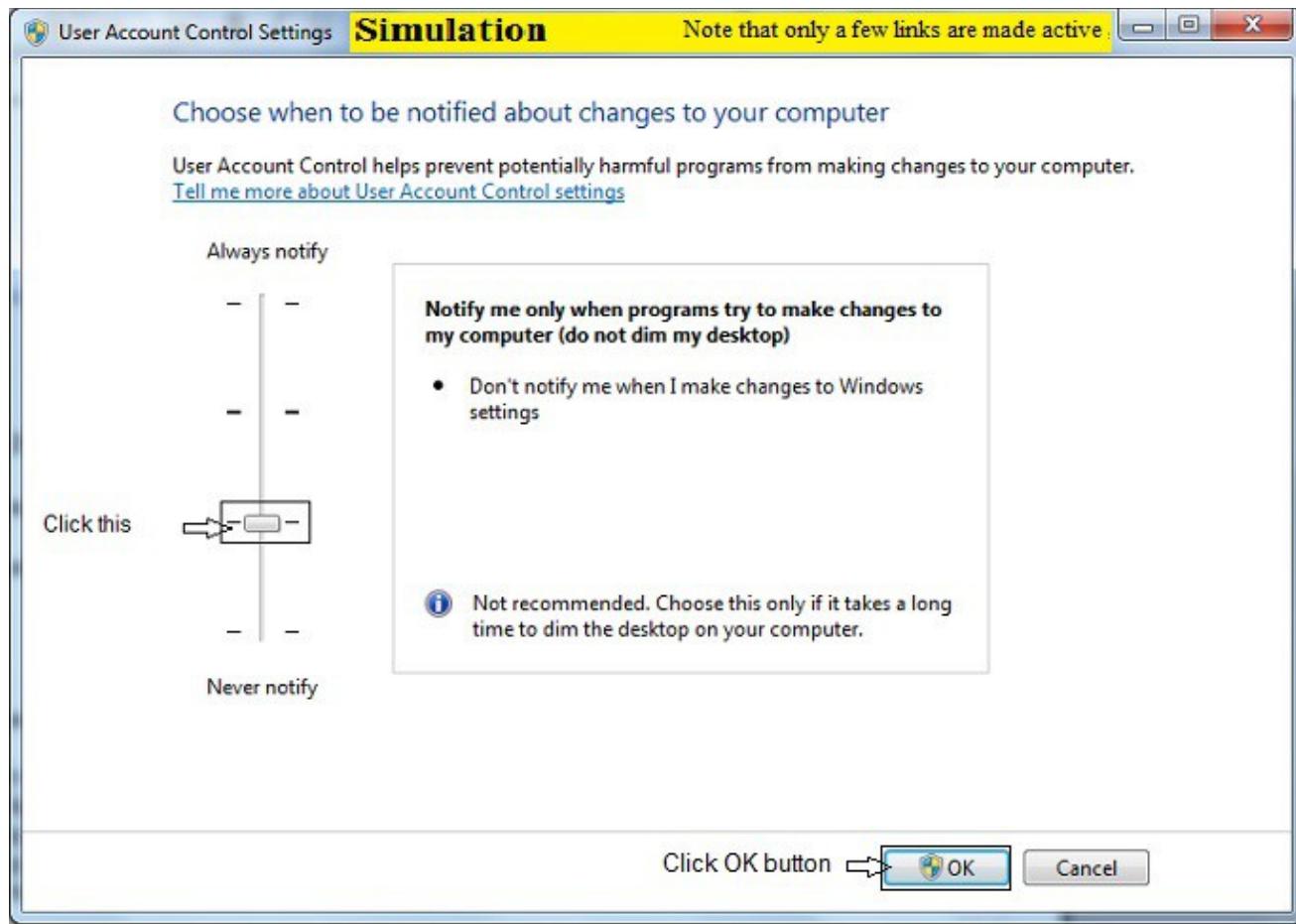
2. In control panel window click User Accounts



3. In Make changes to your user account click Change User Account Control settings



4. In User Account Control Settings window click Notify option and click OK button



Explanation: User Account Control Settings (UAC) can help to prevent unauthorized changes to your computer. UAC notifies you when changes are going to be made to your computer that require administrative level permission. These types of changes can affect the security of your computer or can affect the settings for other people that use the computer

9.22.4 To change the user account type

Description: This lab exercise helps to know about changing the user account type

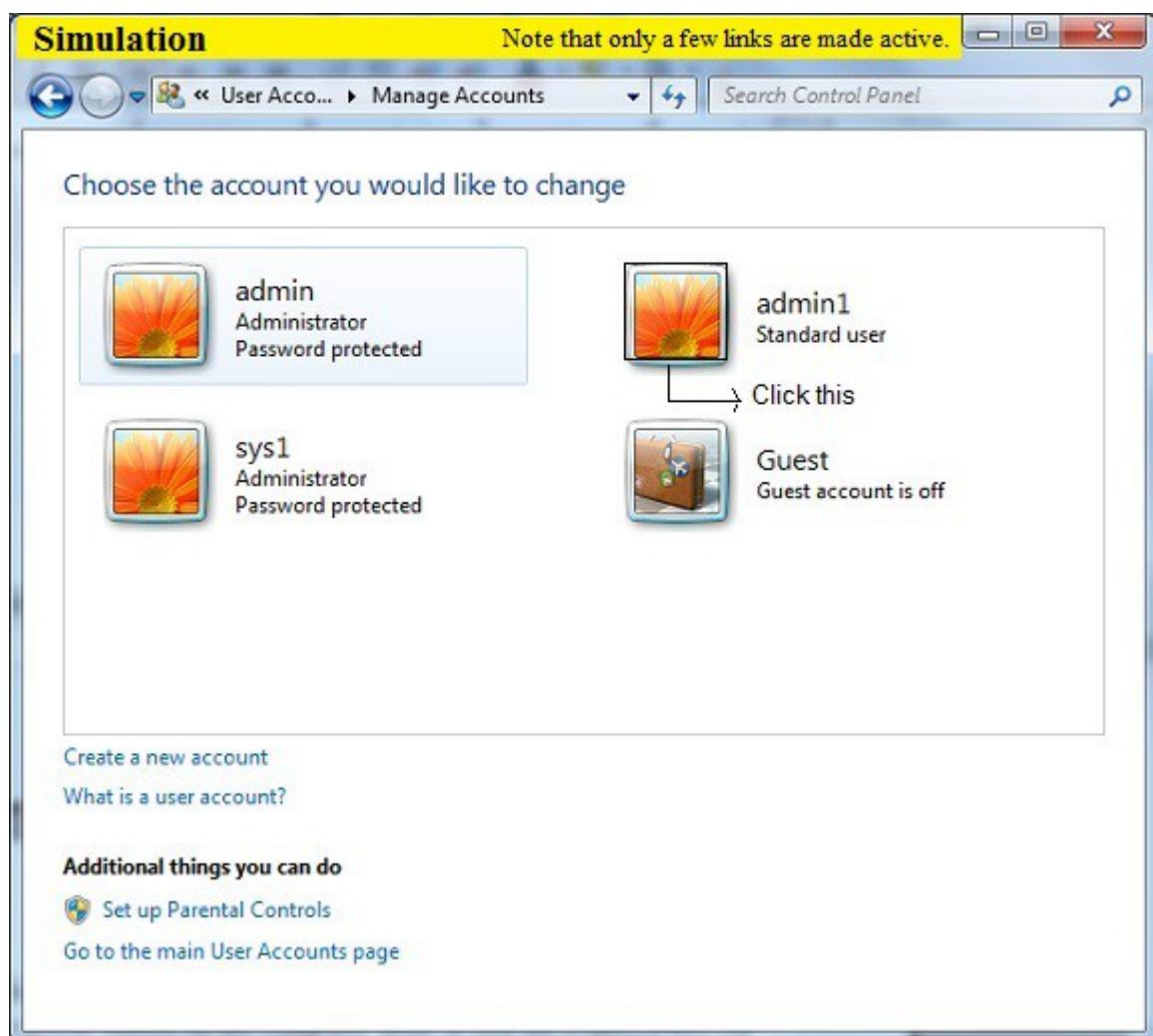
Instructions: 1. On loading a lab exercise, in a given simulation start menu either type “user accounts” in search box or click control panel option

Go to step 2 if control panel is clicked otherwise go to step 3

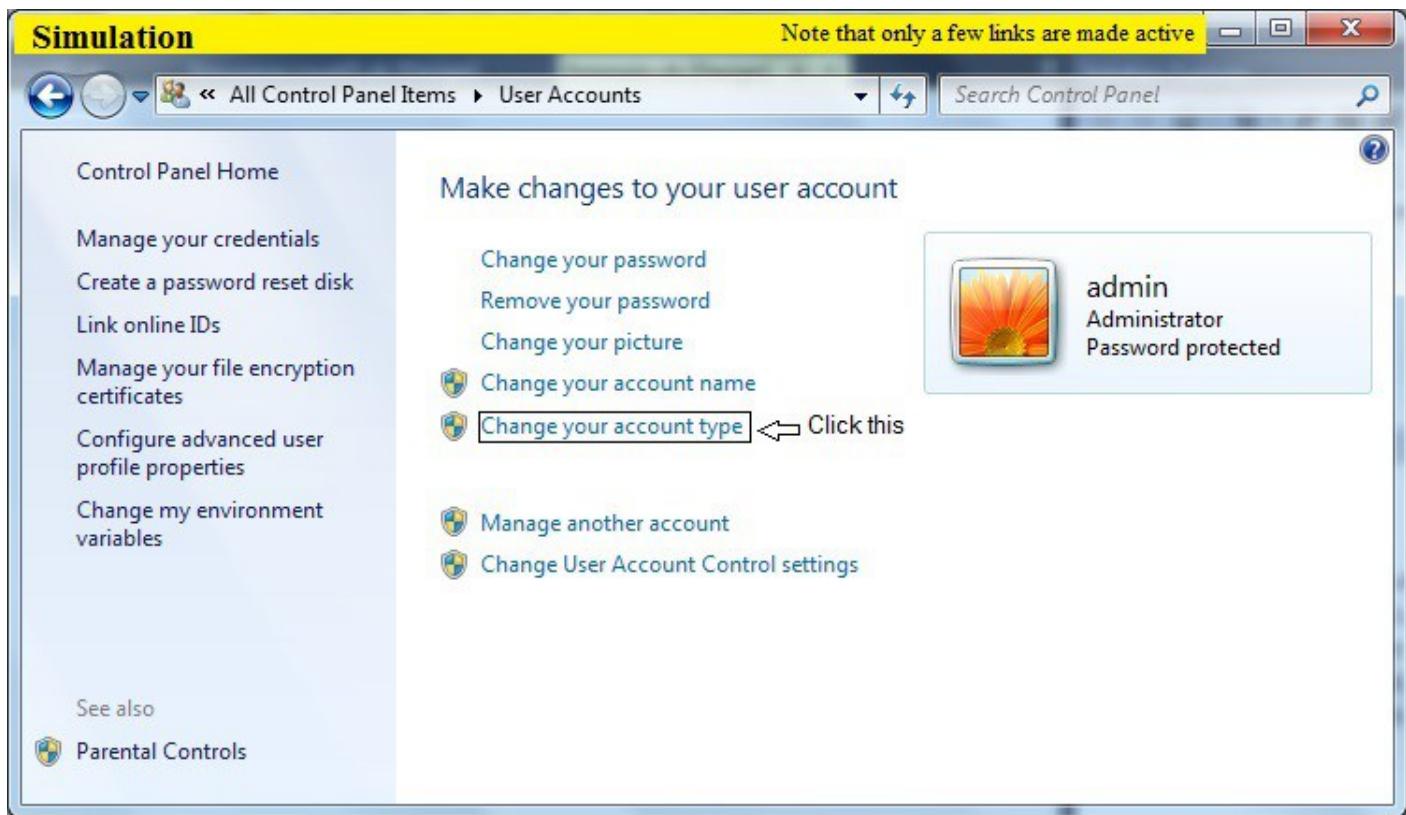
2. In a given control panel items window click Add or remove user accounts



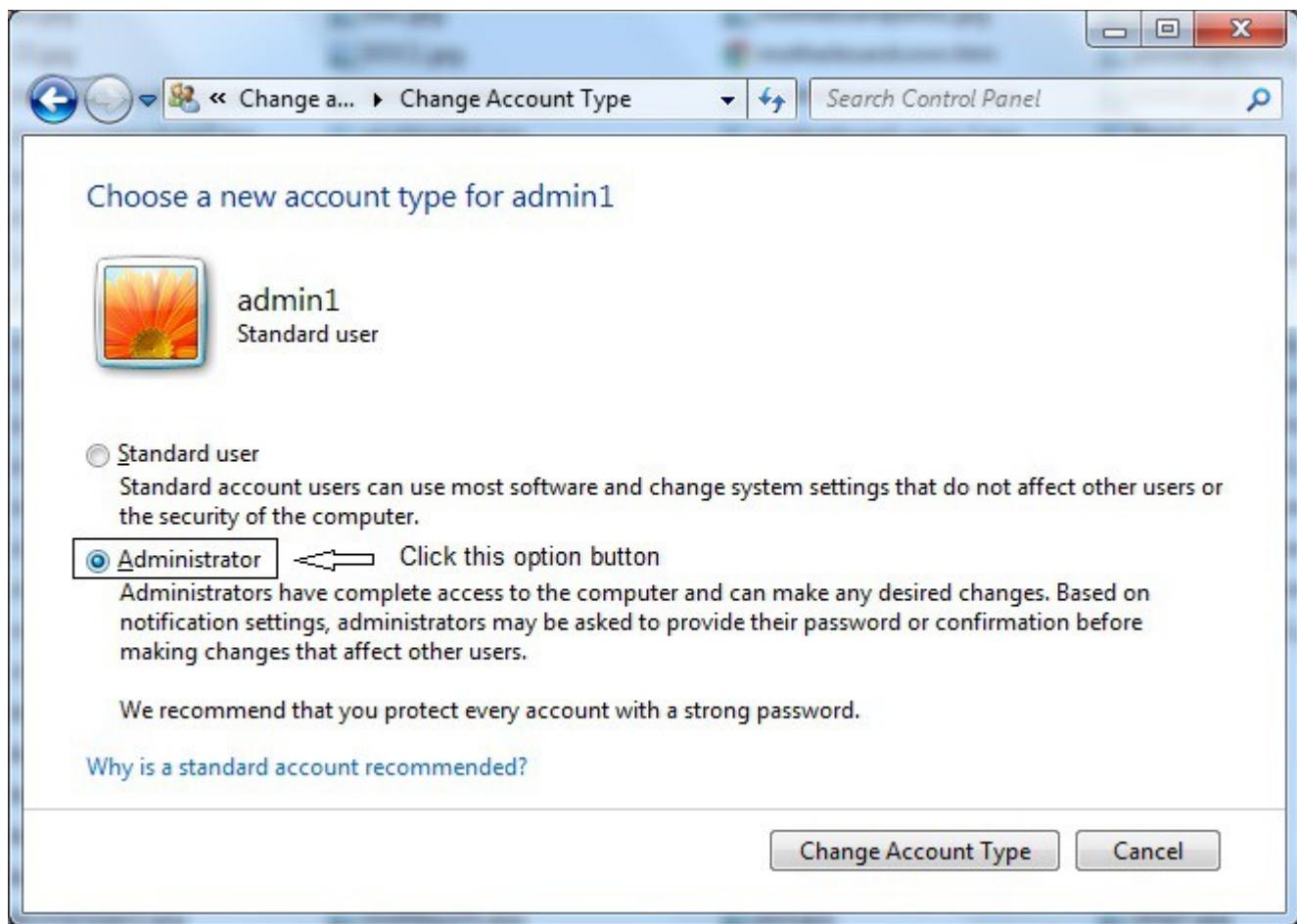
3. In Manage Accounts window click the icon or picture Admin1



4. In Make changes to admin1's account click Change the account type



5. In Change Account Type window click Administrator option button and click Change Account Type button



Explanation: With windows 7 everyone who uses the computer can have their own user account. This allows each one to have his or her own settings. There are two type of accounts

1. Standard: These are the basic accounts we use normal. As a standard user you can do just about anything you would need to do such as running a software or personalizing your desktop. Using standard account will help to keep your computer more safe.

2. Administrator: These are the special accounts that are used for making certain changes to system settings or managing other people's accounts.. They have full access to every setting on the computer. Every computer will have one administrative account.

9.22.5 Removing user accounts

Description: This lab exercise explains about removing or deleting an user accounts

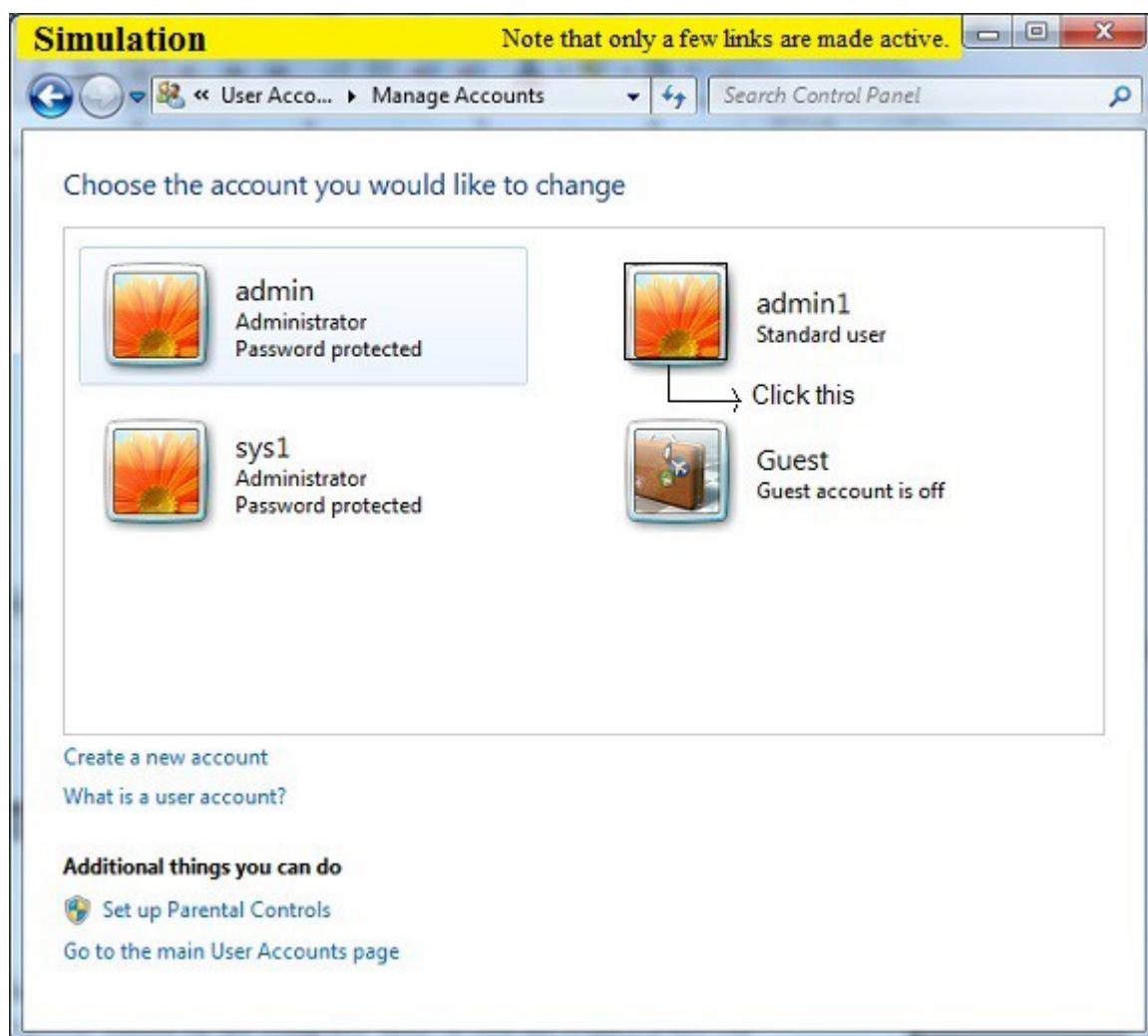
Instructions: 1. On loading a lab exercise, in a given simulation start menu either type user accounts in search box or click control panel option

go to step 2 if control panel is clicked otherwise go to step 3

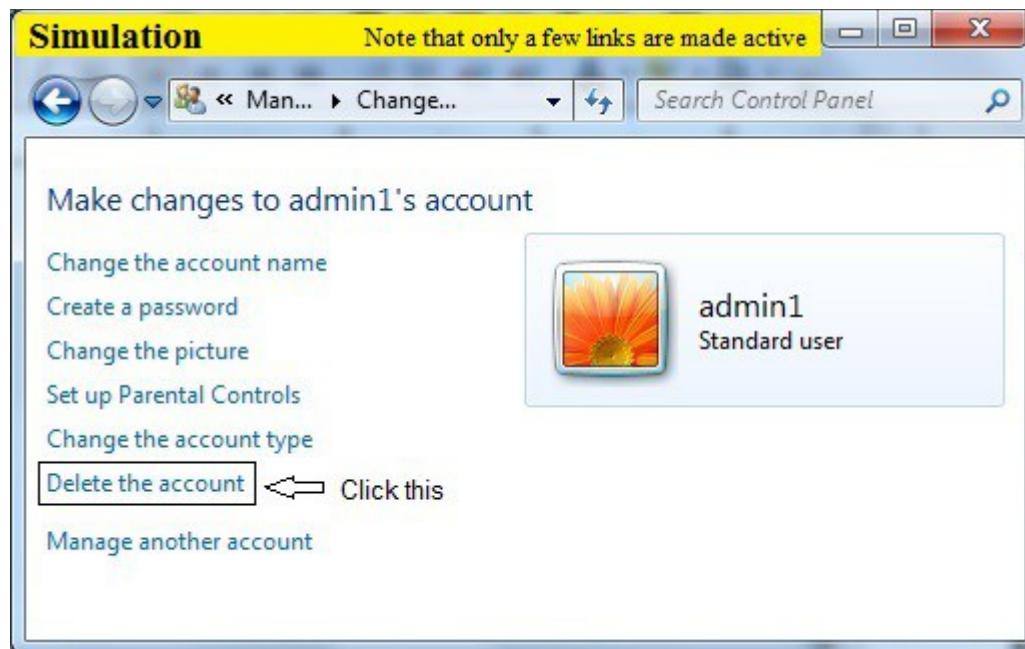
2. In control Panel window click the option Add or remove user accounts



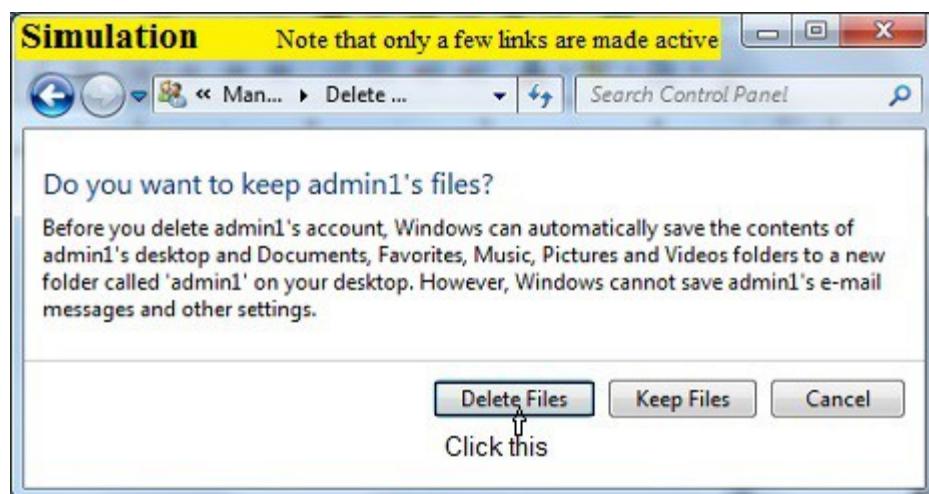
3. In Manage Accounts window click the icon or picture Admin1



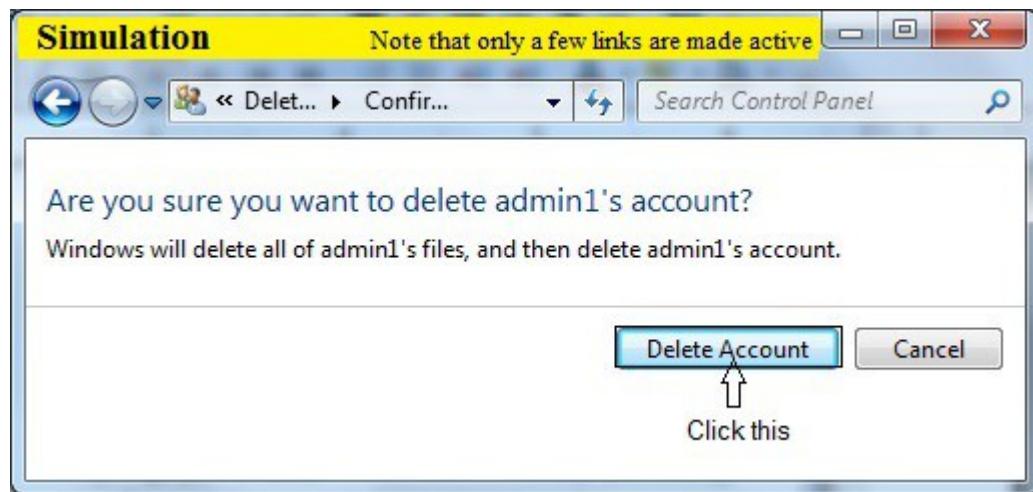
4. In Make changes to admin1 account click Delete the account option



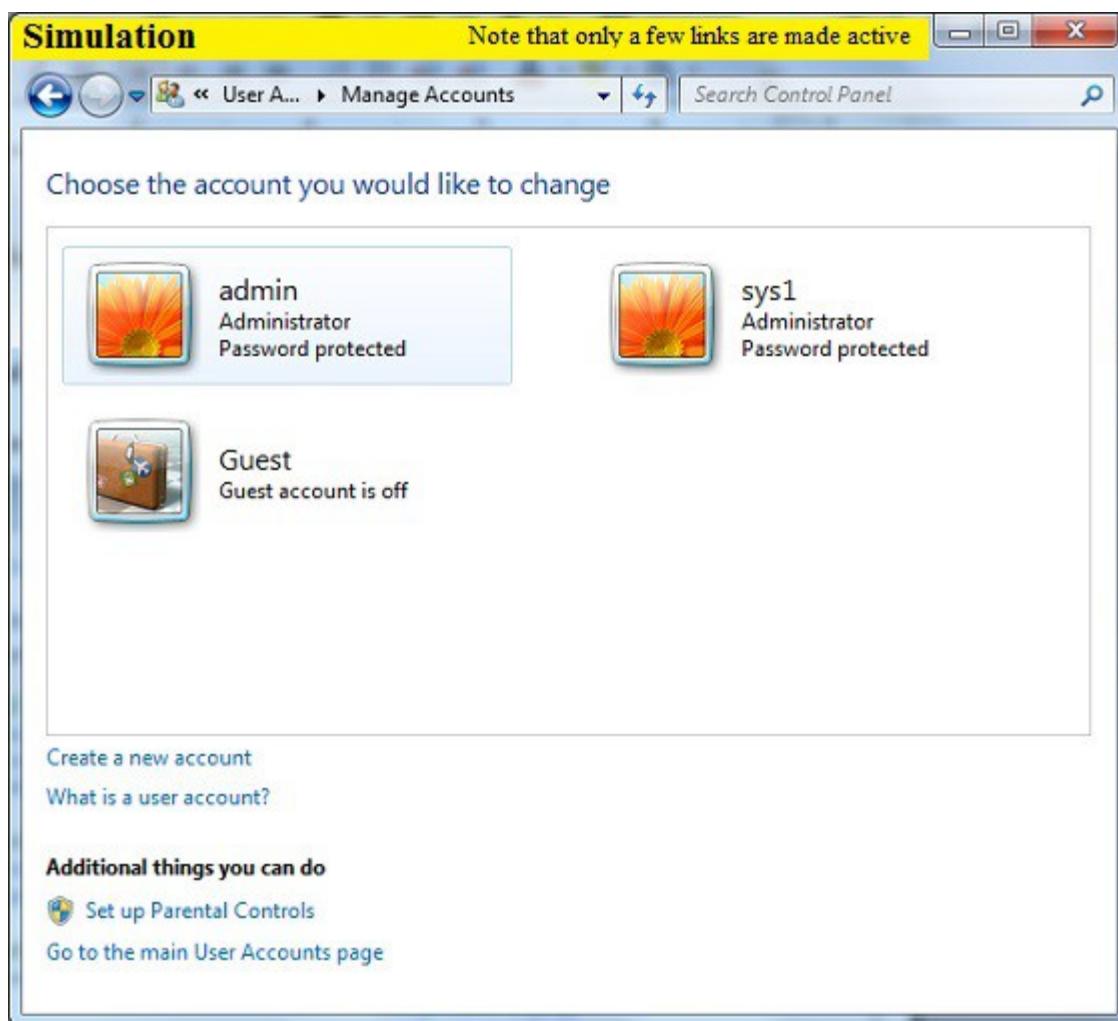
5. Click on the option to Delete the account and the Delete Account window will load asking you to choose whether or not to delete or keep the user's files. Click Delete Files button.



6. The final window for removing the account asks you to confirm that you want to delete the account. Click Delete Account button, the user's account will be deleted



7. After clicking the Delete Account button, the user's account will be deleted and the Manage Accounts window will reload showing the remaining accounts.



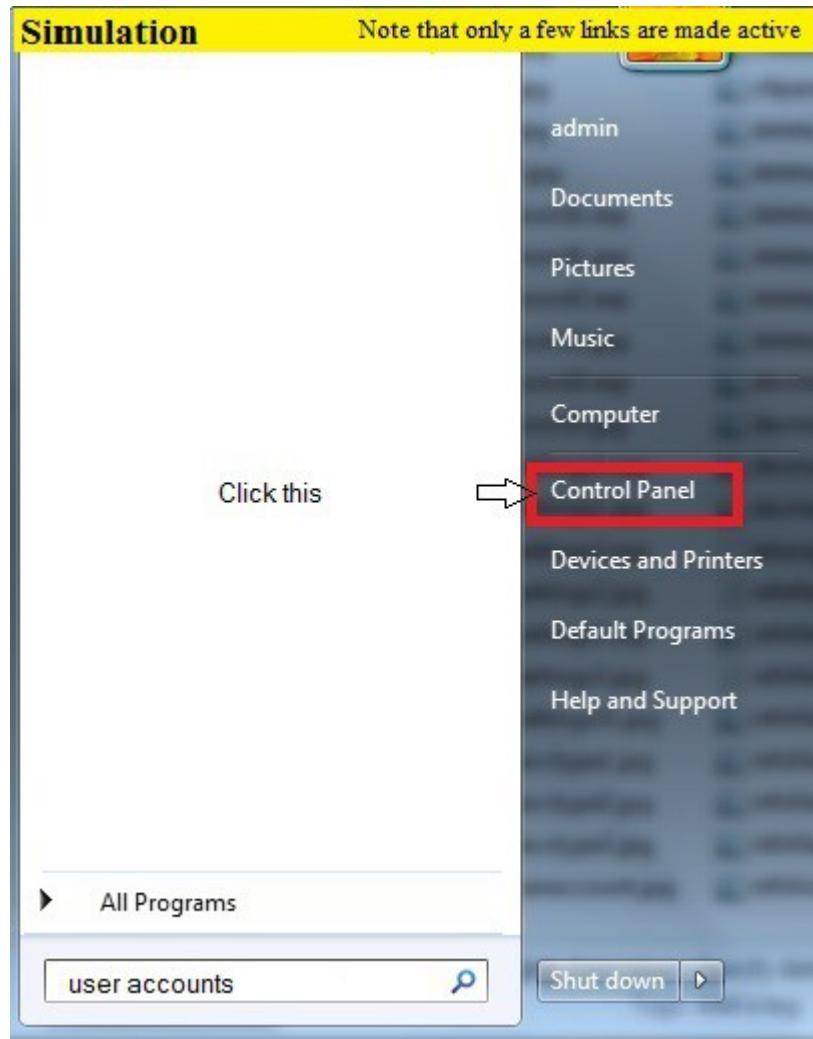
Explanation: User account on computer that is not being used can be permanently removed by deleting it.

[Back](#)

9.23 Configuring windows 7 power options

Description: This lab exercise explains about power options in window7

Instructions: 1. On loading a lab exercise, in a given simulation start menu either type power settings or power options in search box or click control panel option

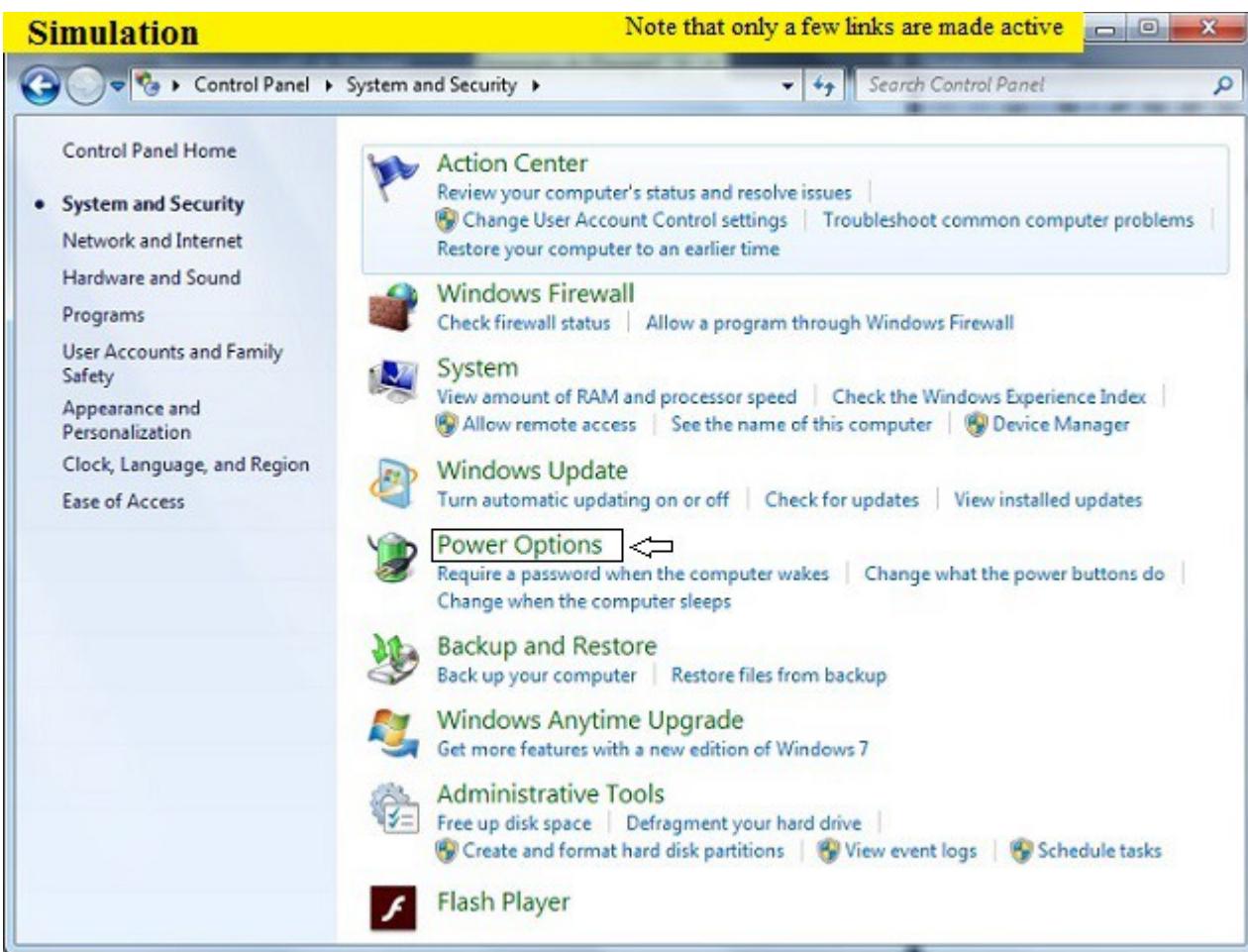


Go to step 2 if control panel is clicked otherwise go to step 4

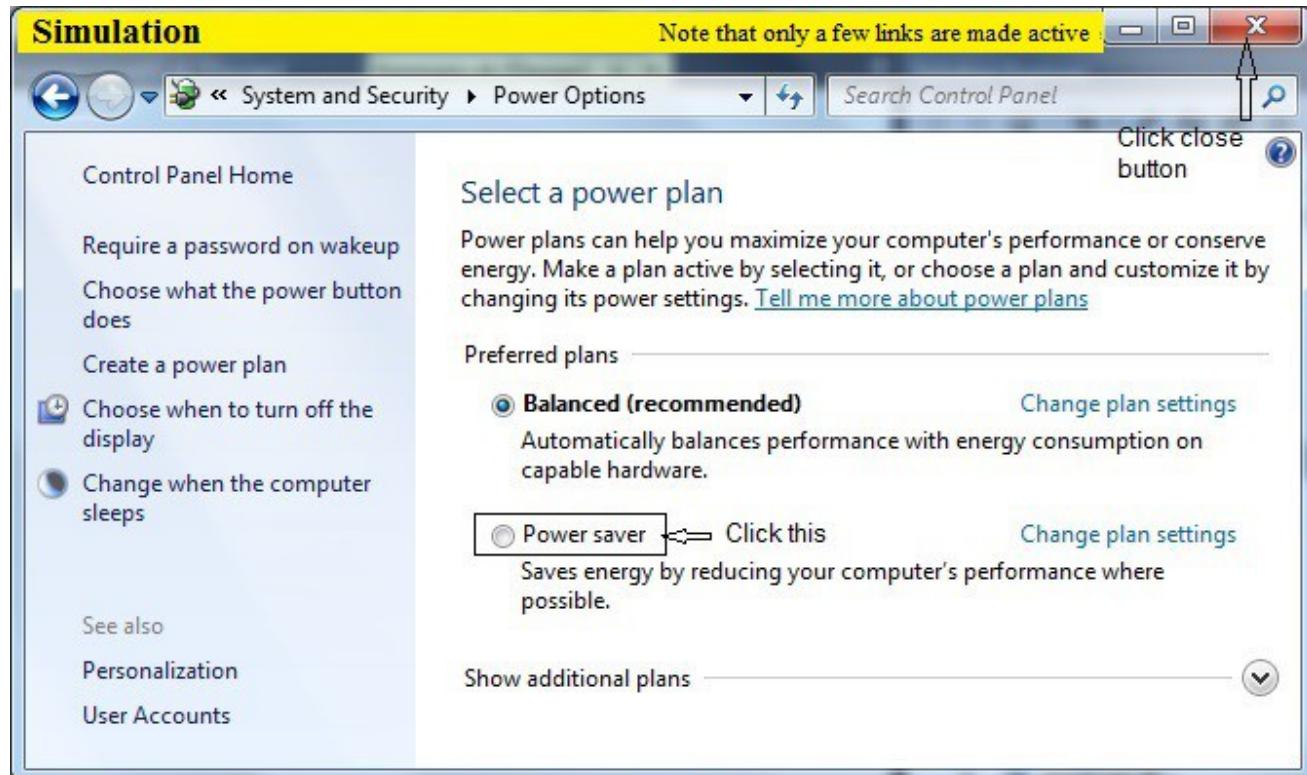
2. In a given control Panel window click the option System and Security



3. In System and Security screen click Power Options



4. In Power Options screen click the option button Power Saver and then click close button.



Explanation: Power plan is a collection of hardware and system settings that manage how your computer uses and conserves power. Power plans can save energy, maximize system performance or balance energy conservation with performance. The default power plans Balance and Power Saver meet most people's needs.

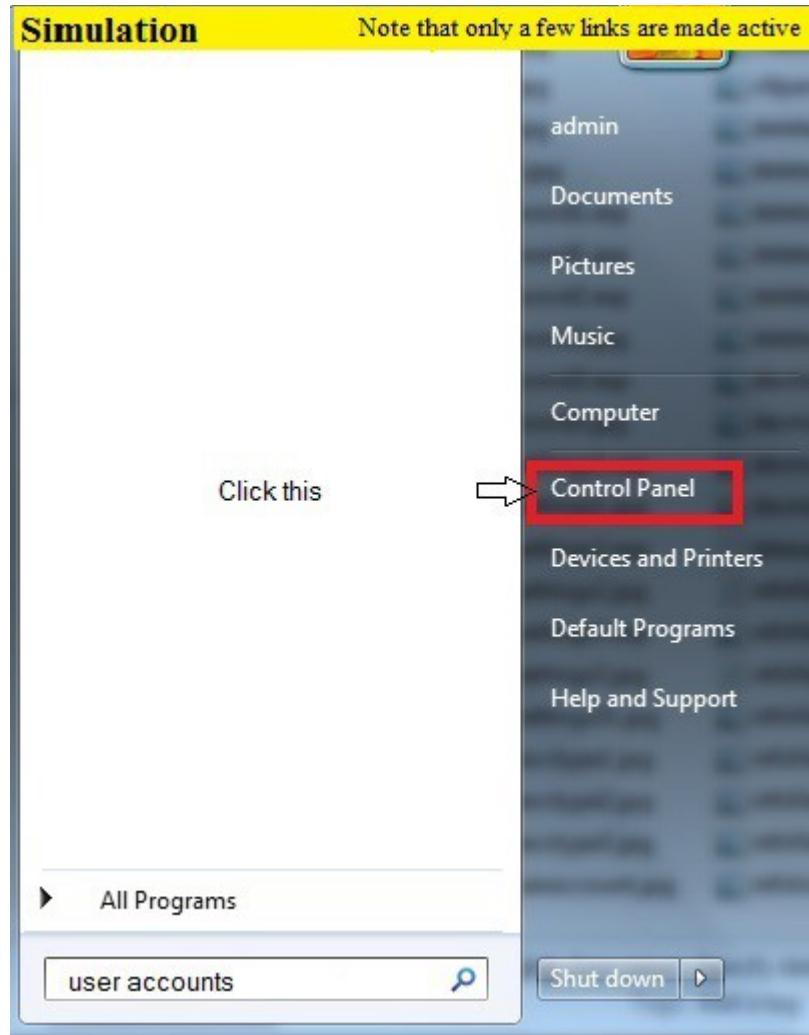
[Back](#)

9.24 Configuring windows 7 update settings

9.24.1 Turning ON/OFF recommended updates

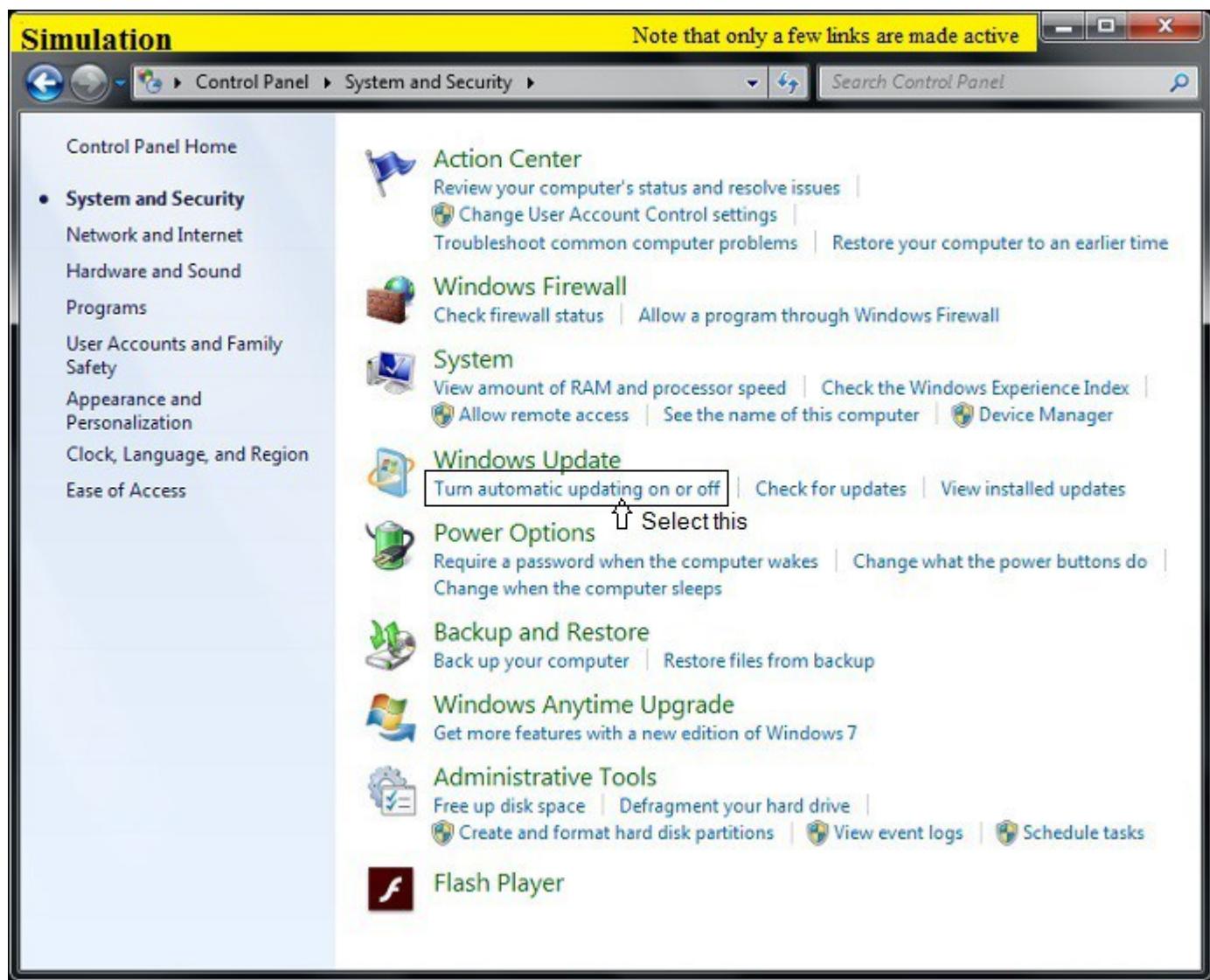
Description: This lab exercise explains turning ON/OFF recommended updates in windows 7 OS

Instructions: 1. On loading a lab exercise, in a given simulation start menu click control panel option or type “windows update” in search box

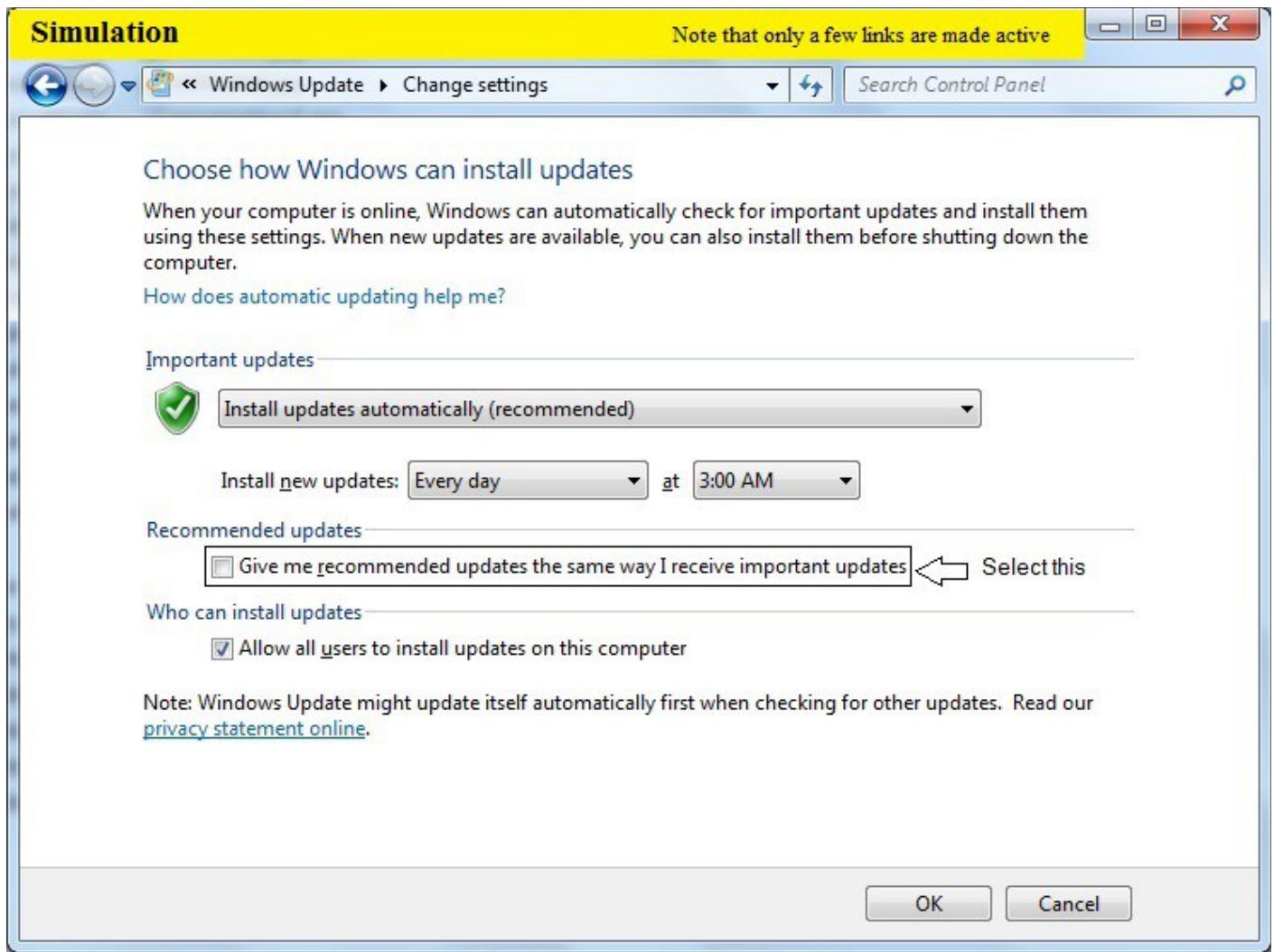




3. Under Windows Update, click Turn automatic updating on or off.



5. Under Recommended updates, select the “**Give me recommended updates the same way I receive important updates**” check box and click OK button



9.24.2. Turning ON/OFF automatic updates

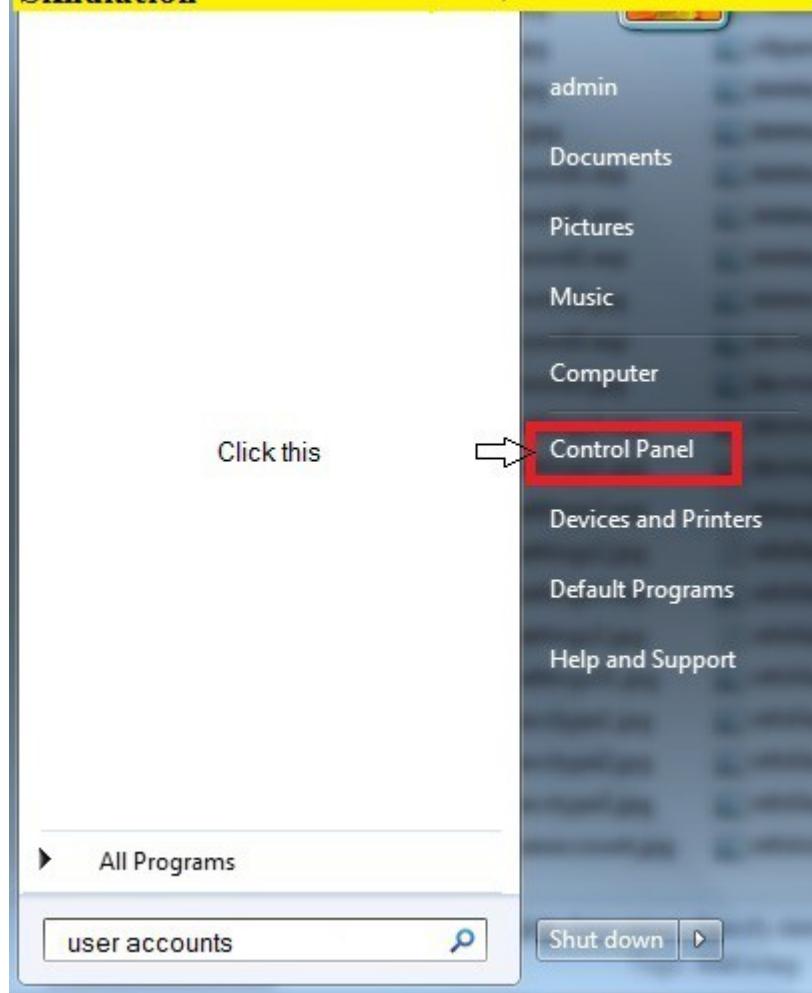
Description: This lab exercise explains turning ON/OFF automatic updates in windows 7 OS

Instructions: 1. On loading a lab exercise, in a given simulation start menu click control Panel option or type “windows update “ in search box

if control panel is clicked go to step 2,3 and 5 otherwise go to step 4 and step 5

Simulation

Note that only a few links are made active



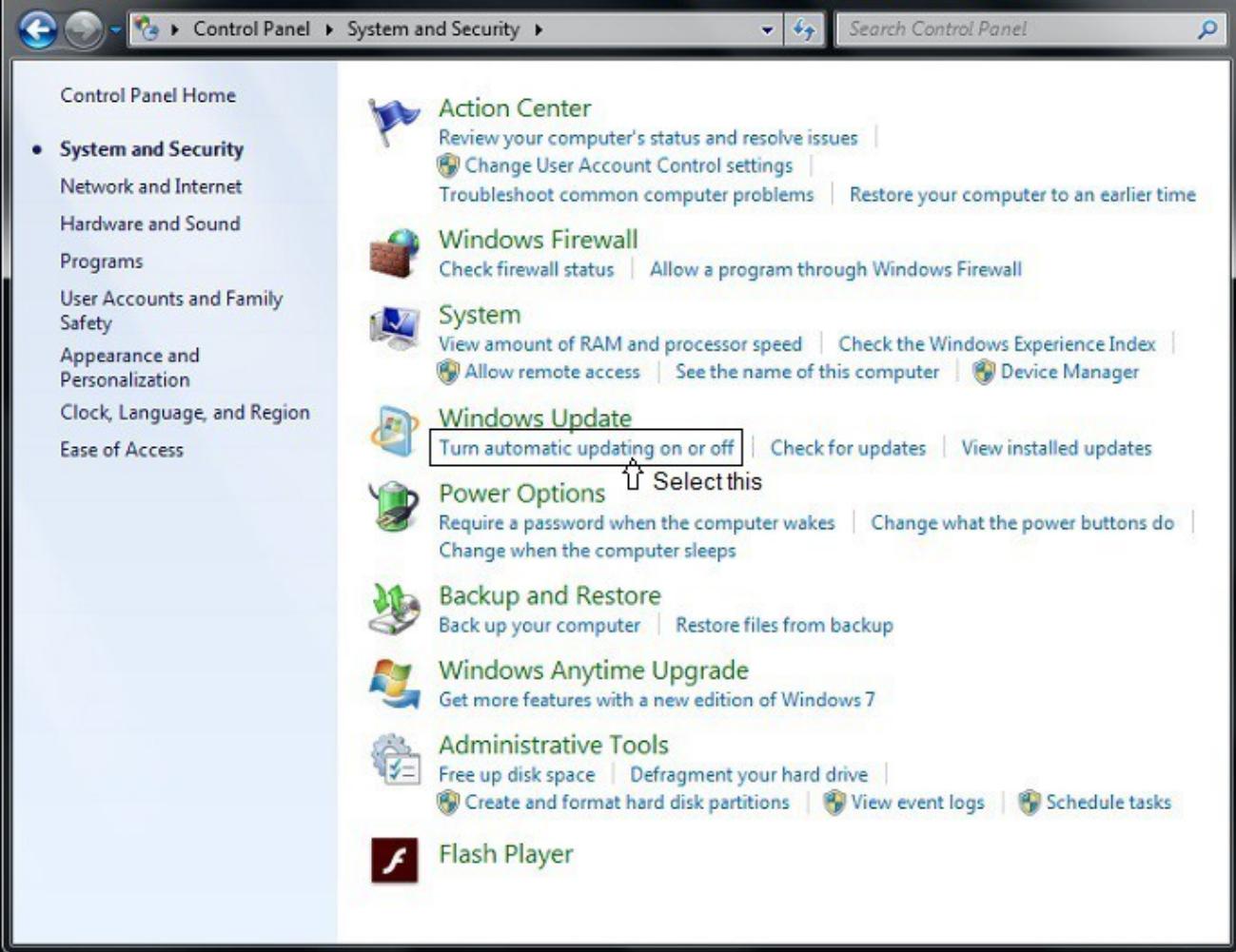
2. In control panel window click “System and security”



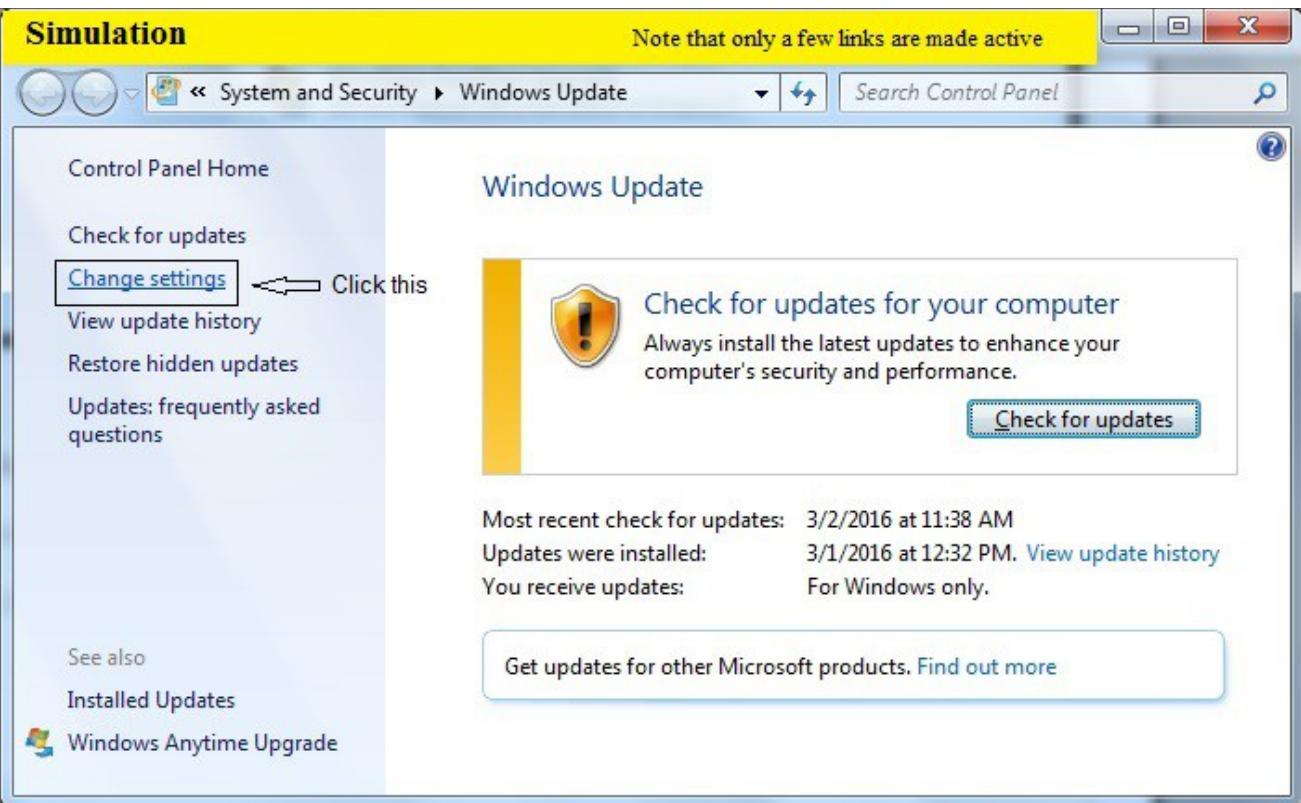
3. Under Windows Update, click “Turn automatic updating on or off”.

Simulation

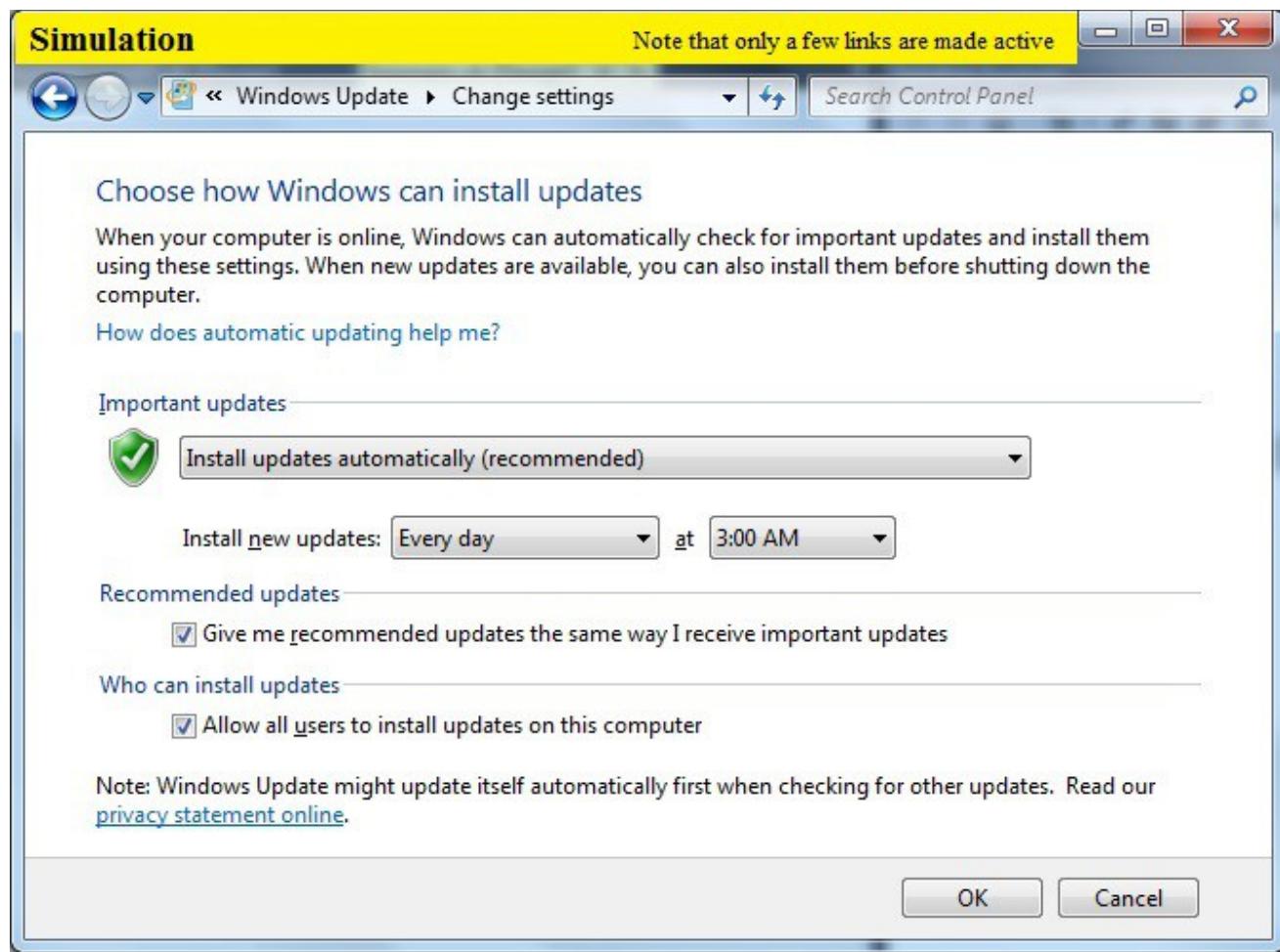
Note that only a few links are made active



4. Click **change settings** in windows update screen



5. From the drop-down menu, click Install updates automatically (recommended) and Click OK button.



Explanation: To have Windows install important updates as they become available, turn on automatic updating. Important updates provide significant benefits, such as improved security and reliability. You can also set Windows to automatically install recommended updates, which can address non-critical problems and help enhance your computing experience.

[Back](#)

9.25 Configuring Local Security Policy in Windows 7

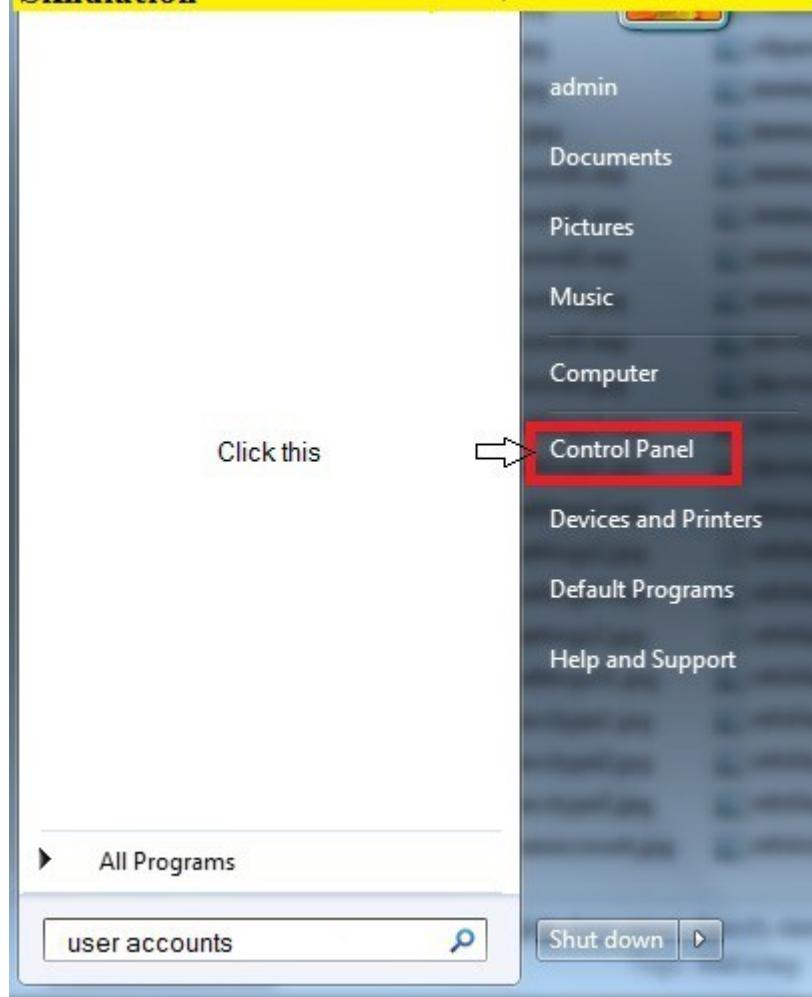
9.25.1 Setting Account lockout policy

Description: This lab exercise helps to set account lockout threshold policy in windows 7

Instructions: 1. On loading a lab exercise, in a given simulation start menu type “local” or “policy” or “sec” in search box or click control panel option.

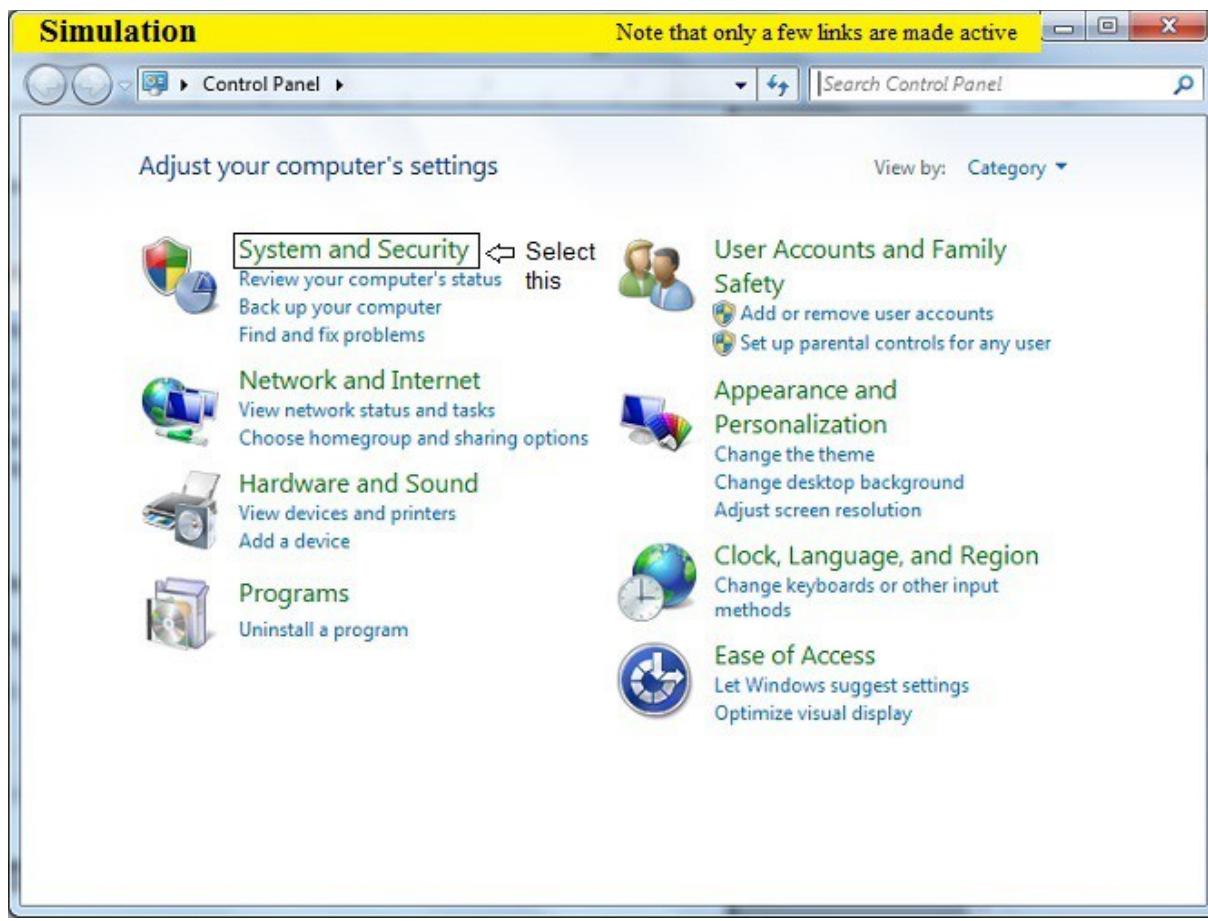
Simulation

Note that only a few links are made active

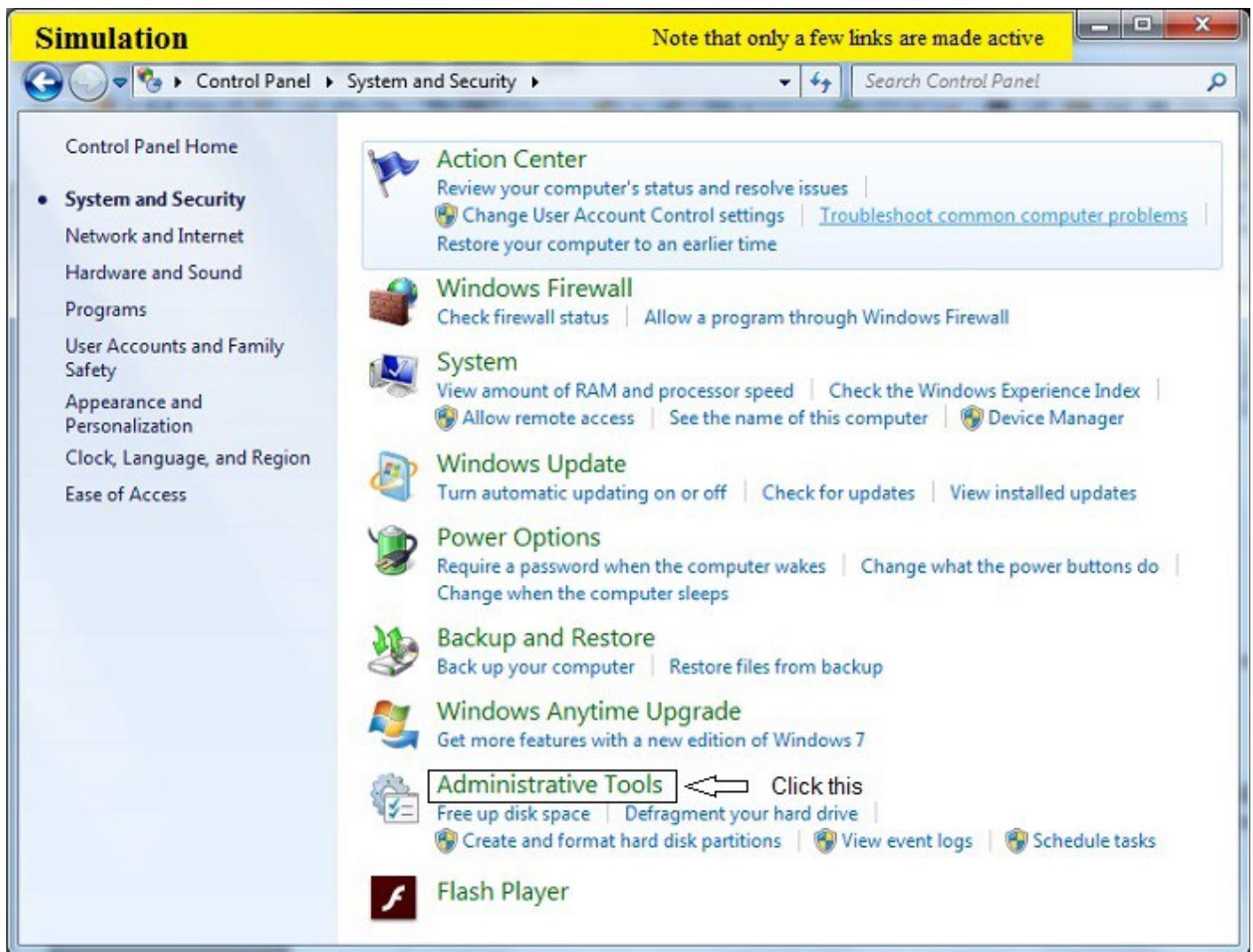


Go to step 2 if control panel is clicked otherwise go to step 5

2. In control panel window click System and Security .



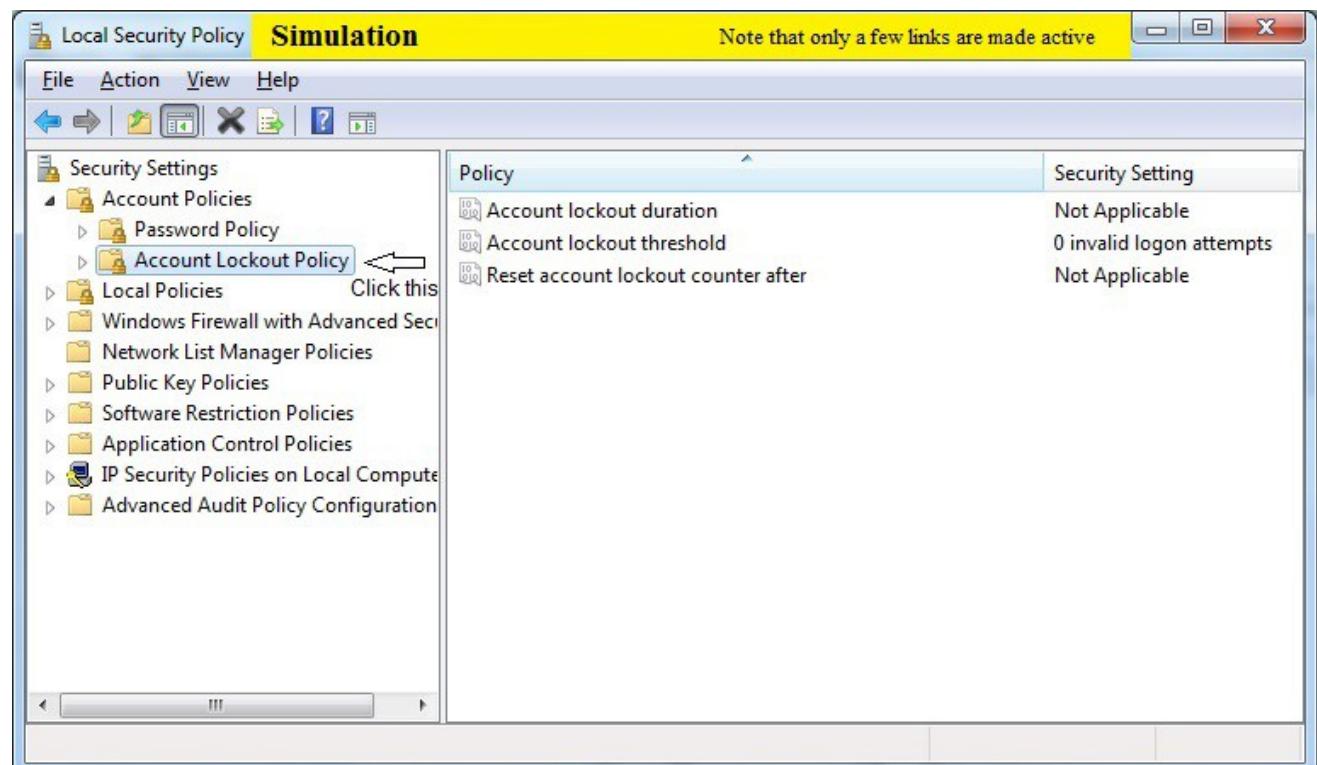
3. In System Security window click Administrative Tools



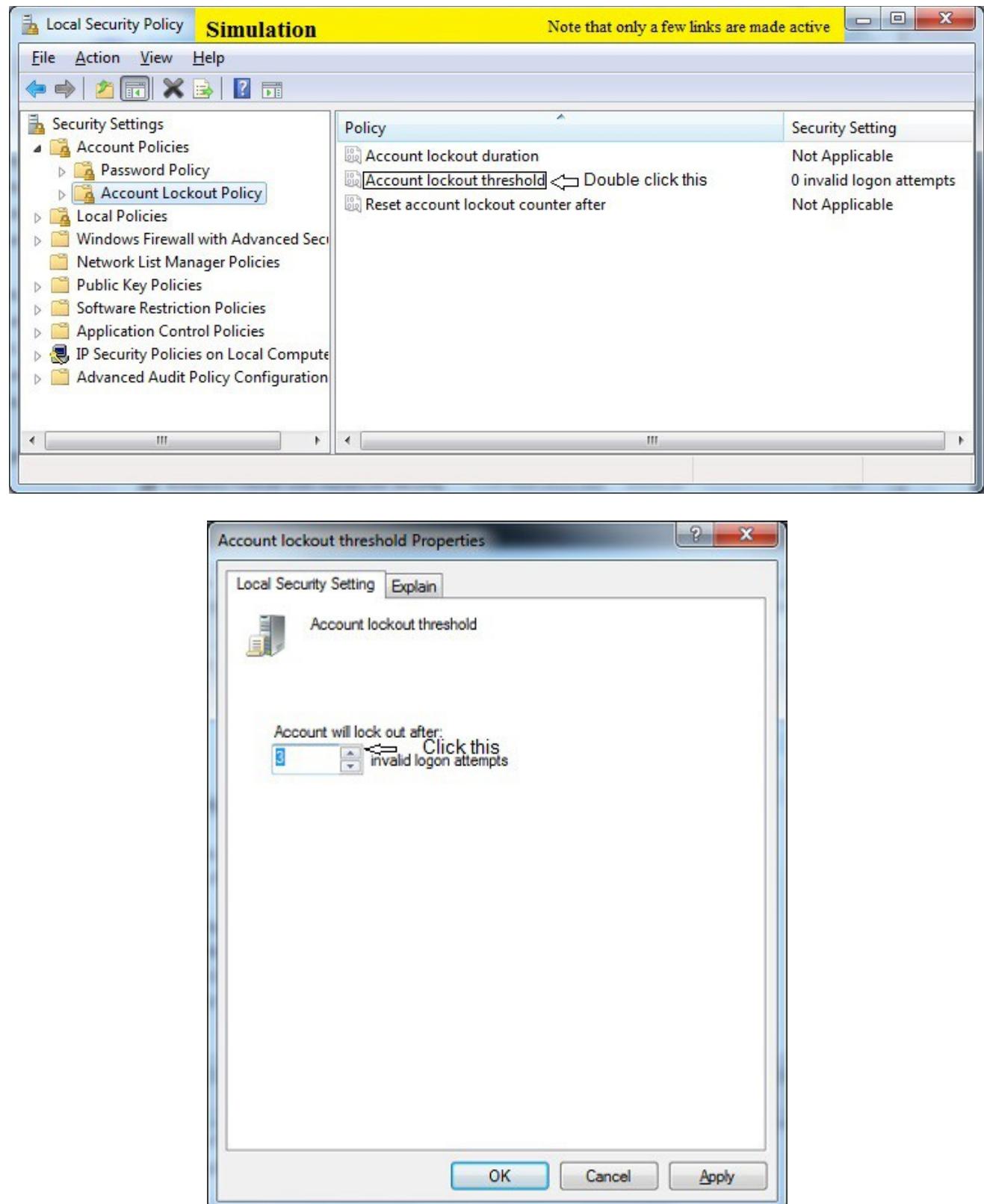
4. In Administrative Tools window double click Local Security Policy



5. Under Account Policies click on Account Lockout Policy you will see three policies in the right pane. Double Click Account lockout threshold.



6. In Account lockout threshold properties window click up arrow button and enter 3 as account will not lockout. Click Apply and then OK button.



Explanation: Someone who attempts to use more than a few unsuccessful passwords while trying to logon to your system might be a malicious user who is attempting to determine an account password by trial and error. Windows domain controller keeps track of logon attempts and domain controller

can configured to respond to this type of potential attack by disabling the account for a preset period of time. Account lockout policy setting control the threshold for this response and actions to be taken after the threshold is reached. There are 3 types of Account lockout policies they are Account lockout duration, Account lockout threshold and reset account lockout counter after

The account lockout duration: This policy allow to specify a time frame after which the account will automatically unlock and resume normal operation.

Account lockout threshold: This policy specifies the number of failed login attempts allowed before the account is locked out.

Reset account lockout counter after : This policy defines a time frame for counting the incorrect login attempts. If the policy is set for 1 hour and account lockout threshold is set for 3 attempts a user can enter the incorrect login information 3 times within 1 hour.

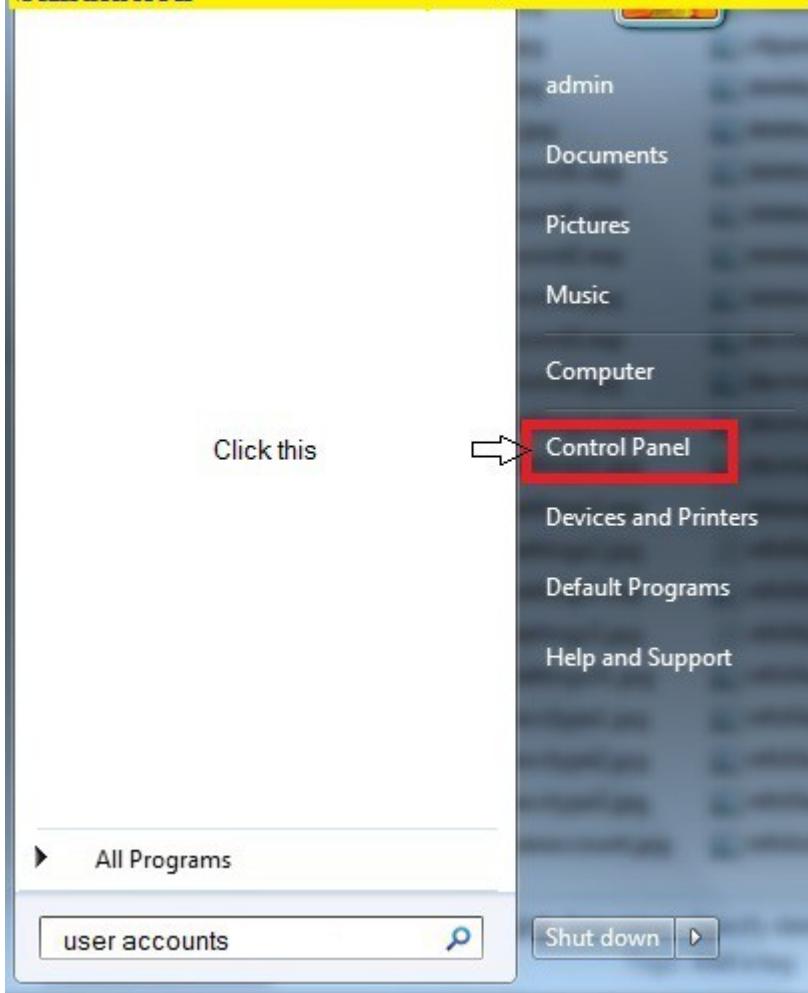
9.25.2 Setting Password policy

Description: This lab exercise helps to enable or disable password must meet complexity requirement in windows 7.

Instructions: 1. On loading a lab exercise, in a given simulation start menu type “local” or “policy” or “sec” in search box or click control panel option.

Simulation

Note that only a few links are made active

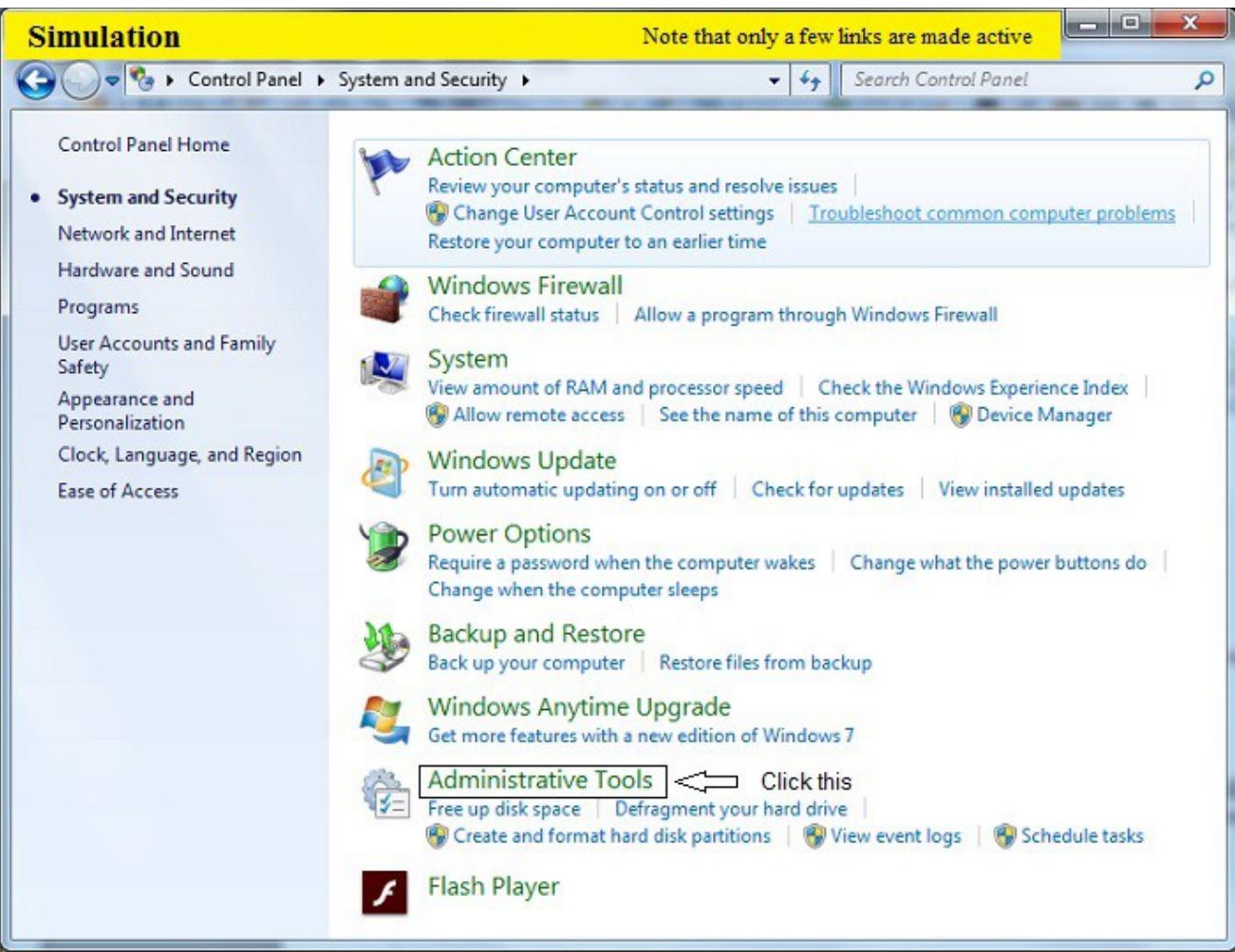


Go to step 2 if control panel is clicked otherwise go to step 5

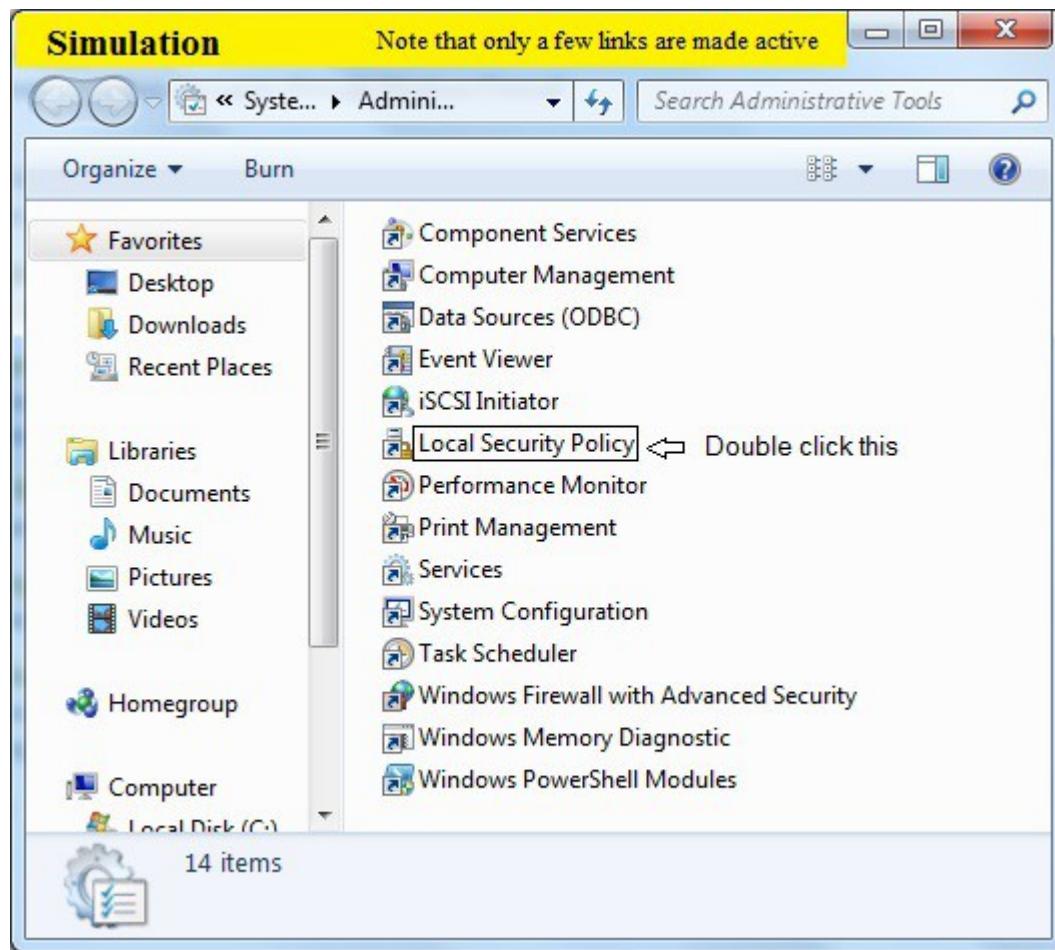
2. In control panel window click System and Security



3. In System Security window click Administrative Tools



4. In Administrative Tools window double click Local Security Policy

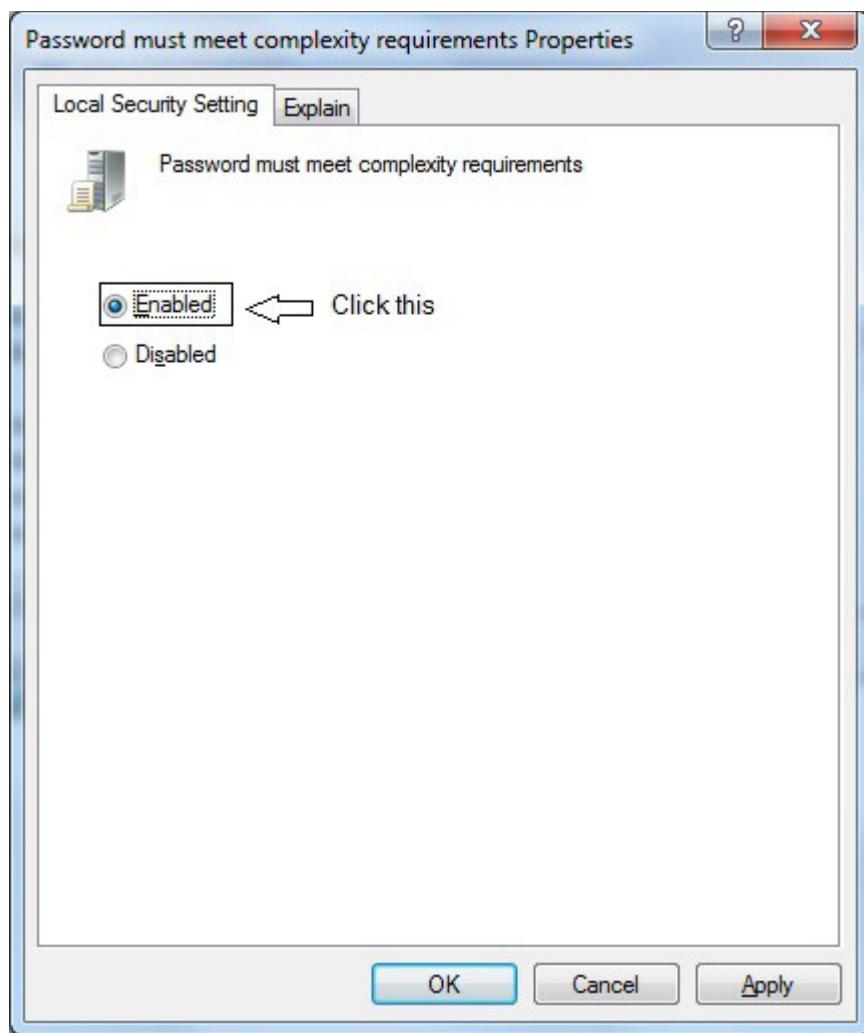
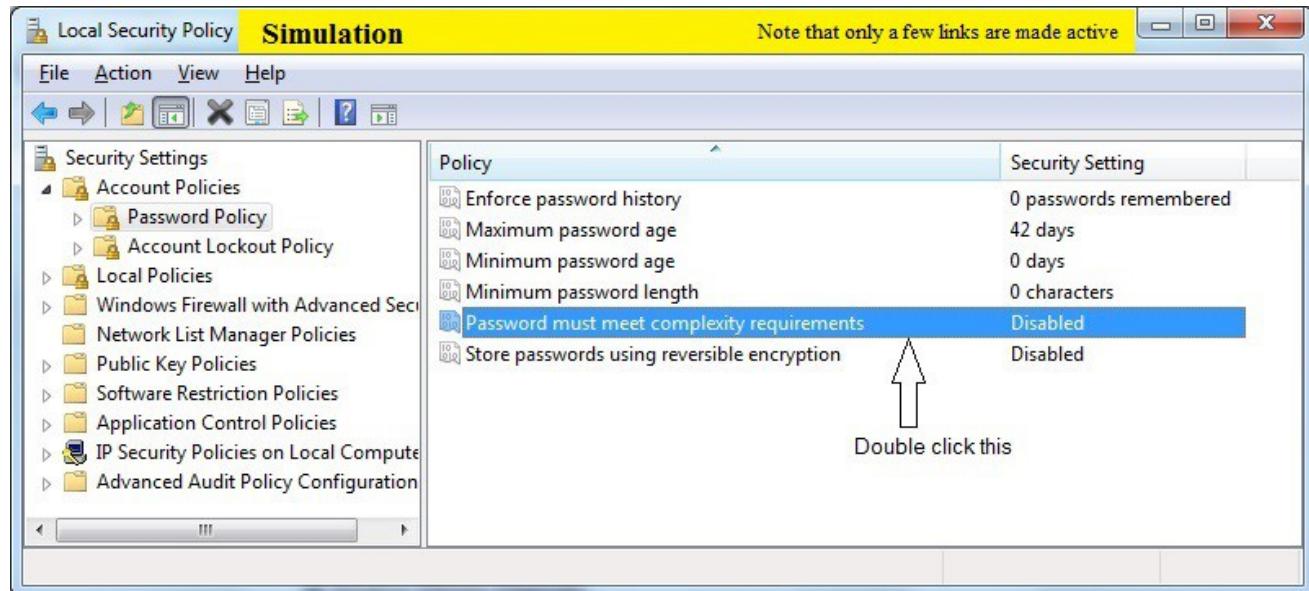


5. Under Account Policies click on Password Policy you will see six policies in the right pane. Double Click “Password must meet complexity requirements”

The screenshot shows the "Local Security Policy" snap-in window. The left pane displays a tree view of security settings, with the "Account Policies" node expanded. The "Password Policy" item under "Account Policies" is selected and highlighted with a blue border and a callout bubble pointing to it with the text "Click this". The right pane lists six policies with their corresponding security settings:

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
>Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

6. In Password must meet complexity requirements Properties click Enabled radio button and then click Apply and then click OK button.



Explanation: If your computer is on a domain only your network administrator can change password policy settings. You can help to protect your computer by customizing your password policy settings that is allow the user to change the password regularly,minimum length for password and requiring passwords to meet certain complexity requirements. Complexity requirements are enforced when

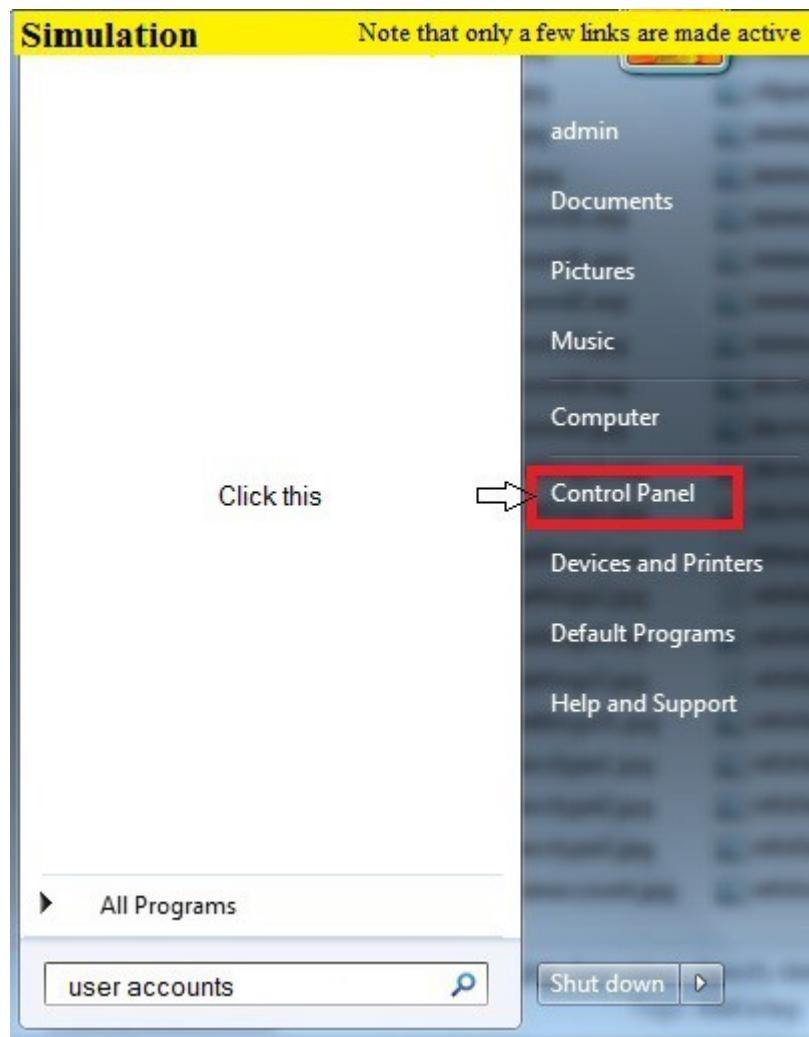
passwords are changed or created.

[Back](#)

9.26 Configuring hardware settings using Device Manager

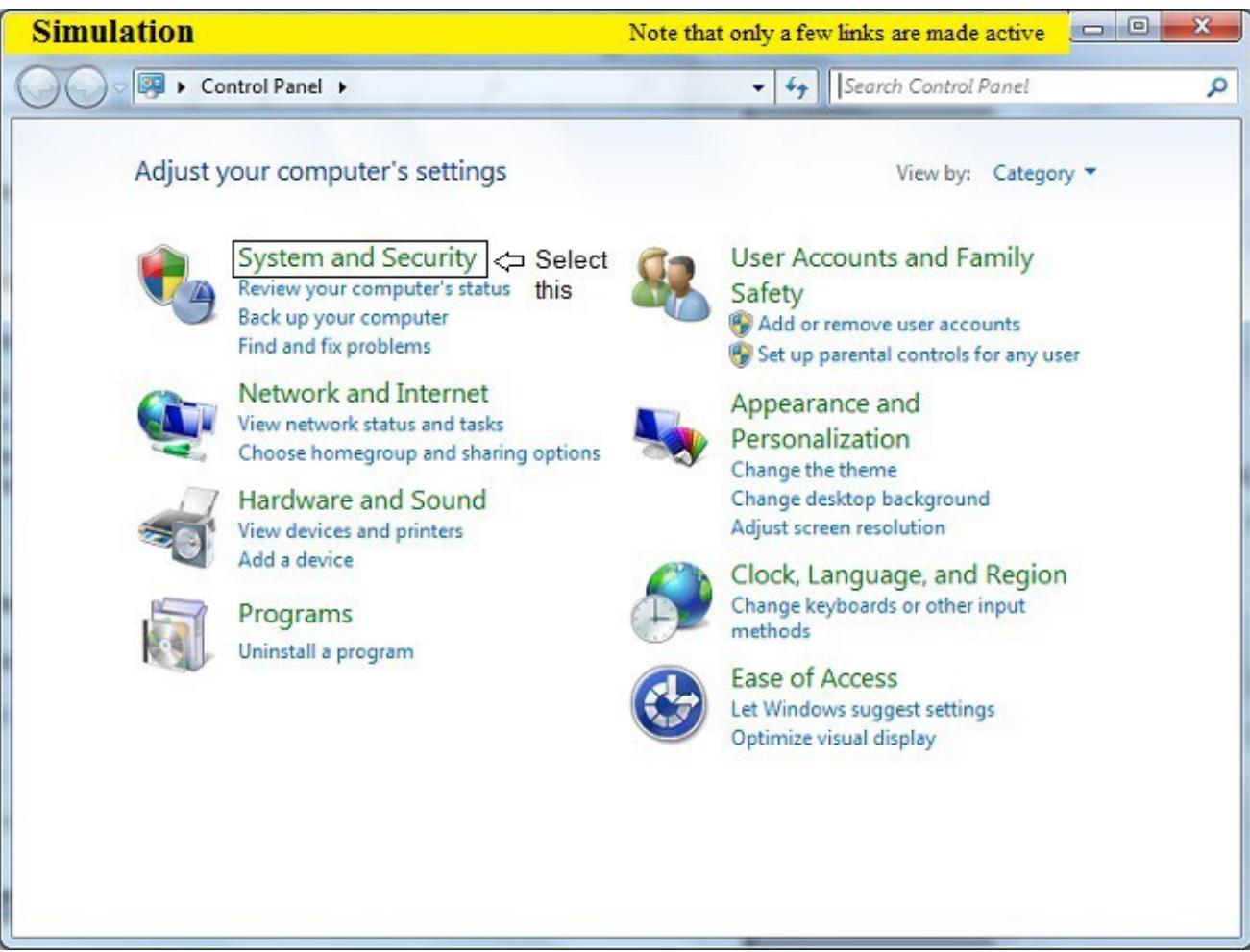
Description: This lab exercise helps to change the hardware settings using device manager

Instructions: 1. On loading a lab exercise, in a given simulation start menu type device manager in search box or click control panel option.

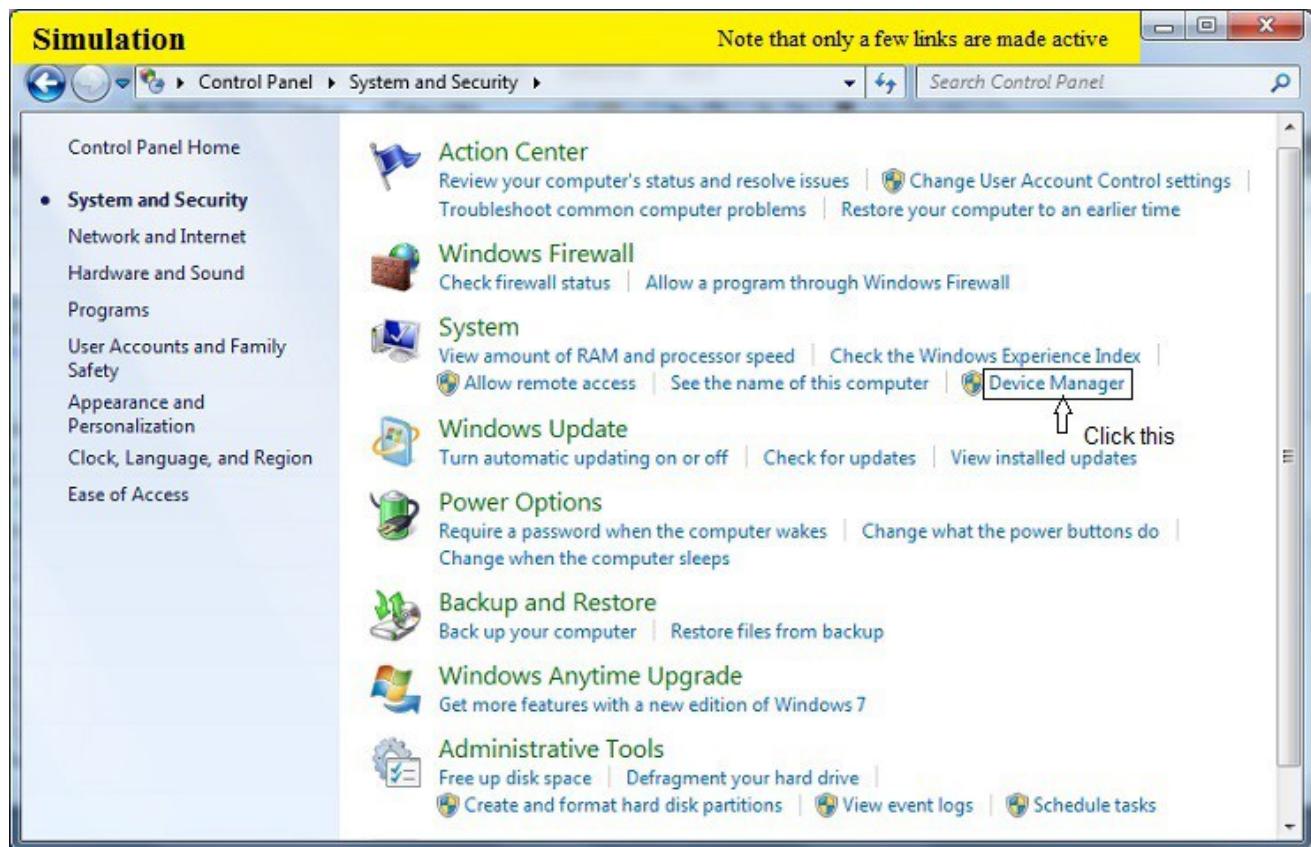


Go to step 2 if control panel is clicked other wise go to step 4

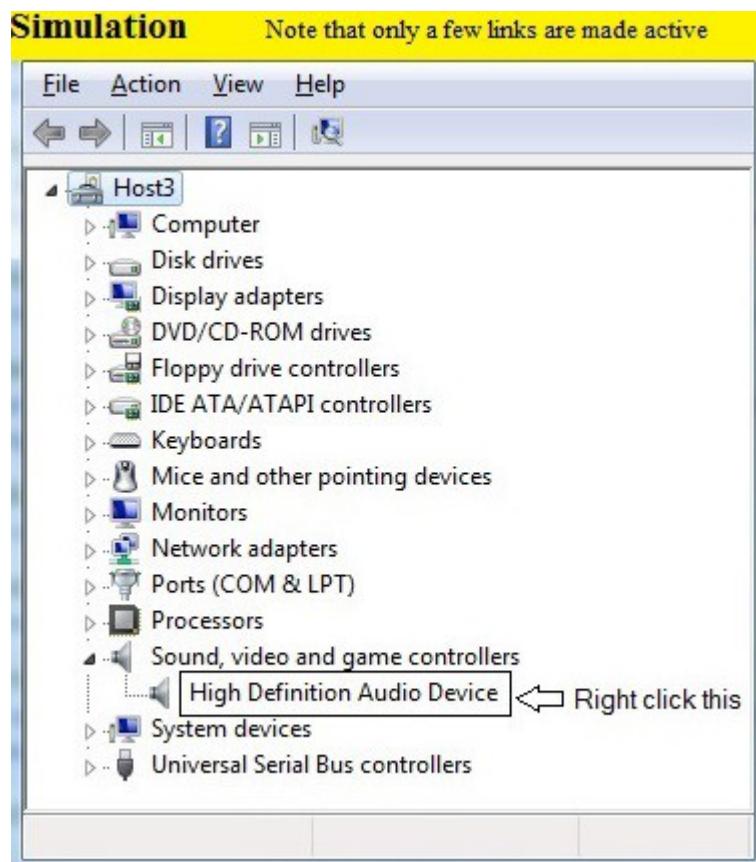
2. In control panel window click System and security.



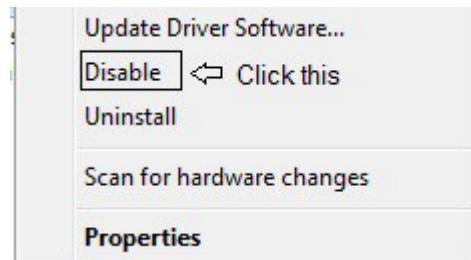
3. In System Security window click Device Manager



4. In Device Manager window right click High Definition Audio Device



5. A pop up menu appears click Disable , you are prompted with message click Yes button.



Explanation: Device Manager provides a graphical view of the hardware that is installed on your computer. All devices communicate with Windows through a piece of software called a device driver. You can use Device Manager to install and update the drivers for your hardware devices, modify hardware settings for those devices, and troubleshoot problems.

We can use Device Manager to:

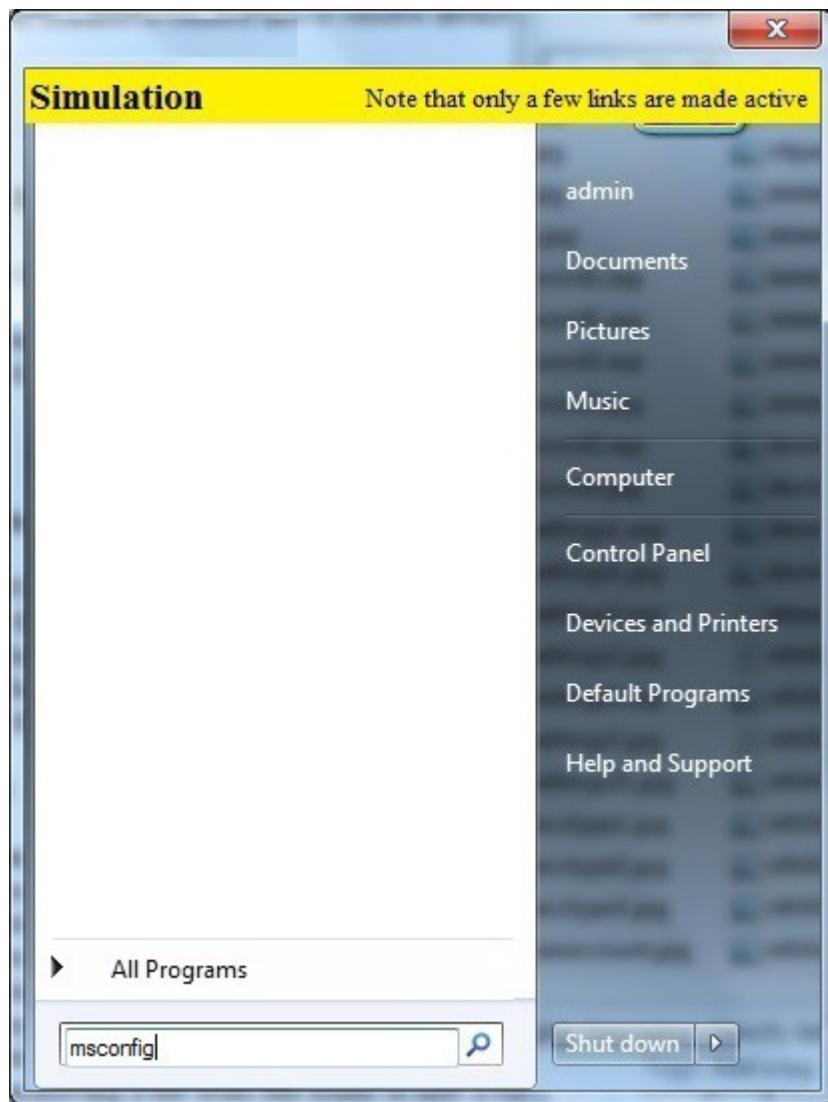
1. Determine whether the hardware on your computer is working properly.
2. Change hardware configuration settings.
3. Identify the device drivers that are loaded for each device, and obtain information about each device driver.
4. Change advanced settings and properties for devices. Install updated device drivers.
5. Enable, disable, and uninstall devices.
6. Roll back to the previous version of a driver.
7. View the devices based on their type, by their connection to the computer, or by the resources they use.
8. Show or hide hidden devices that are not critical to view, but might be necessary for advanced troubleshooting.
9. You will typically use Device Manager to check the status of your hardware and update device drivers on your computer. Advanced users who have a thorough understanding of computer hardware might also use Device Manager's diagnostic features to resolve device conflicts and change resource settings.

[Back](#)

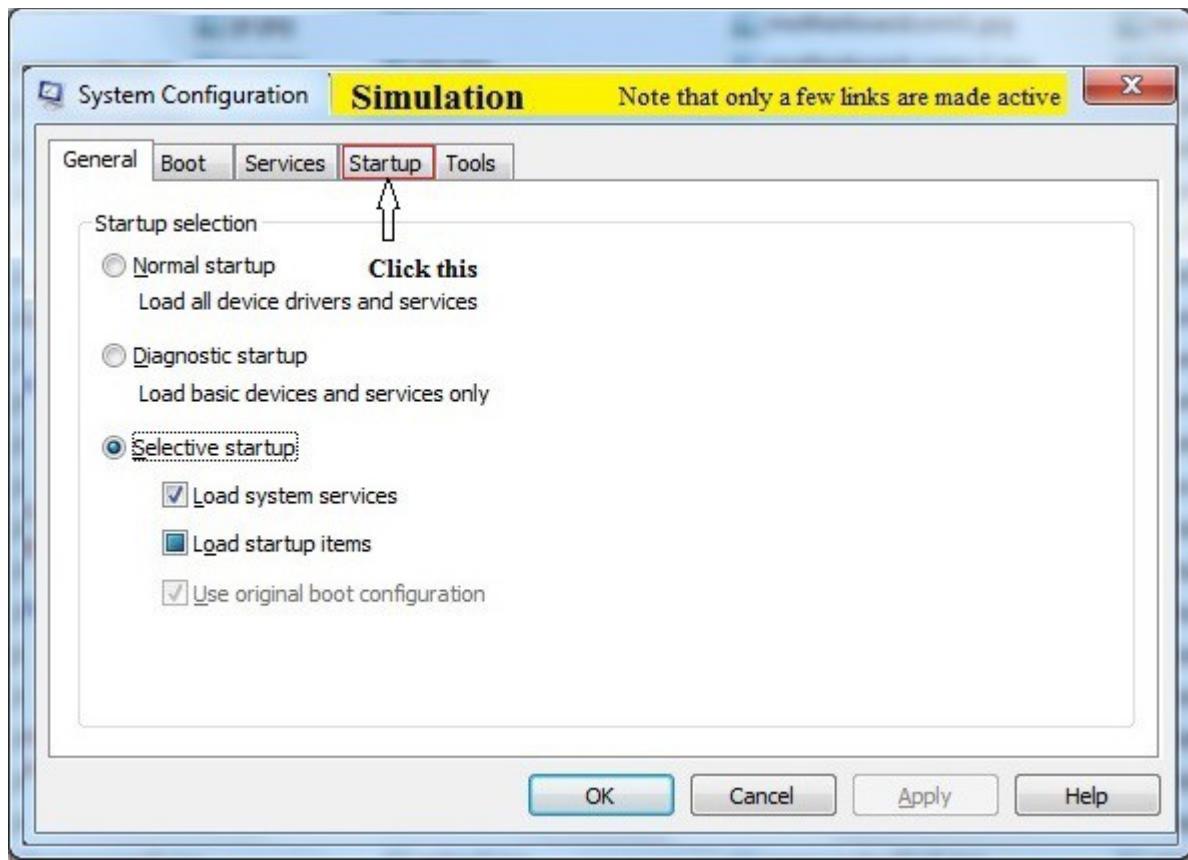
9.27 Disabling Startup Programs in Windows 7

Description: This lab exercise helps to disable startup programs in windows 7

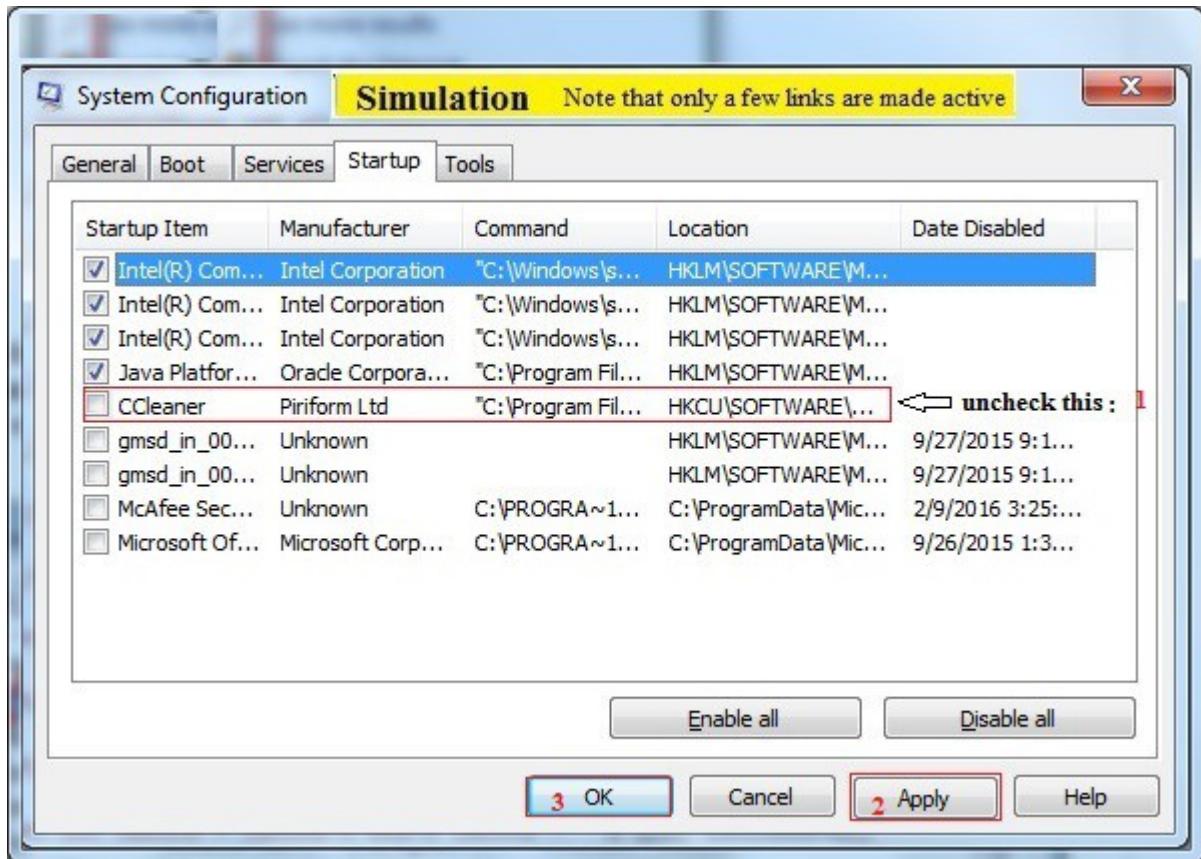
Instructions: 1. On loading a lab exercise, in a given simulation start menu type “ msconfig” in search box.

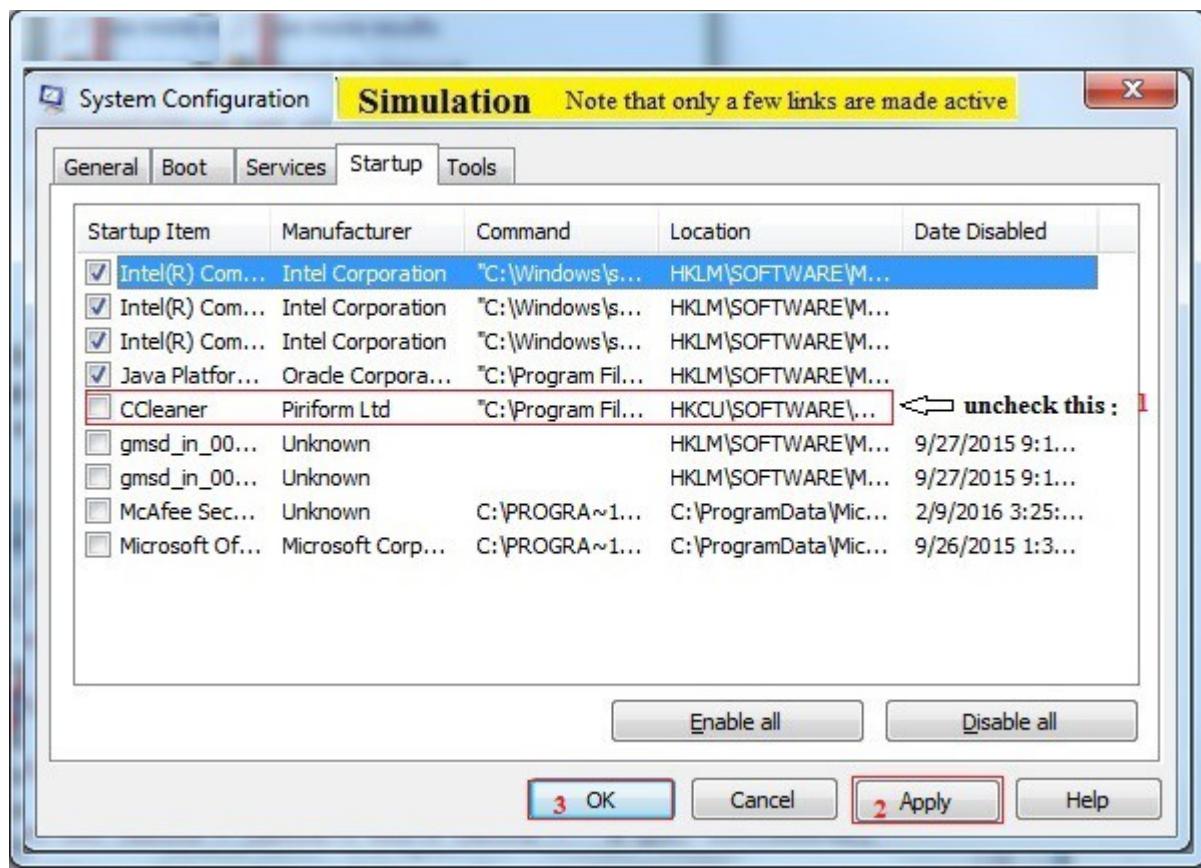


2. From within the System Configuration tool, *Click Startup tab*.



3. And then *Uncheck* the program box “Ccleaner” to prevent from starting when Windows starts. Click Apply button and then OK to save changes when finished.





Note: Now that you've saved changes Restart Windows and the selected programs should no longer automatically start up.

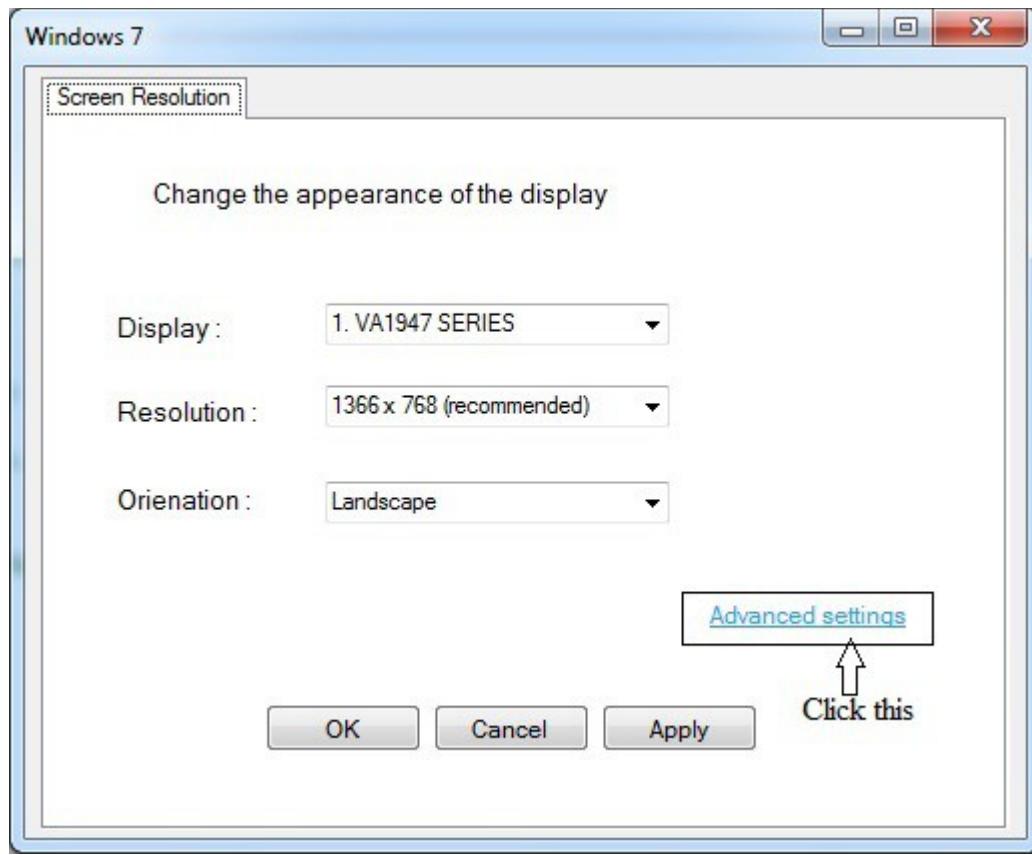
Explanation: Startup programs are programs which run when your computer starts / boots up. Startup programs can be antivirus programs, chat/messaging apps or background apps that can also continuously keep running on your computer. Start up programs impact computer boot time, and may make your computer boot slower. While some of startup programs like antivirus are important, you can make your computer boot faster by disabling unrequired startup programs. Next time you start your computer, disabled startup programs will not start, and your computer will start relatively faster.

[**Back**](#)

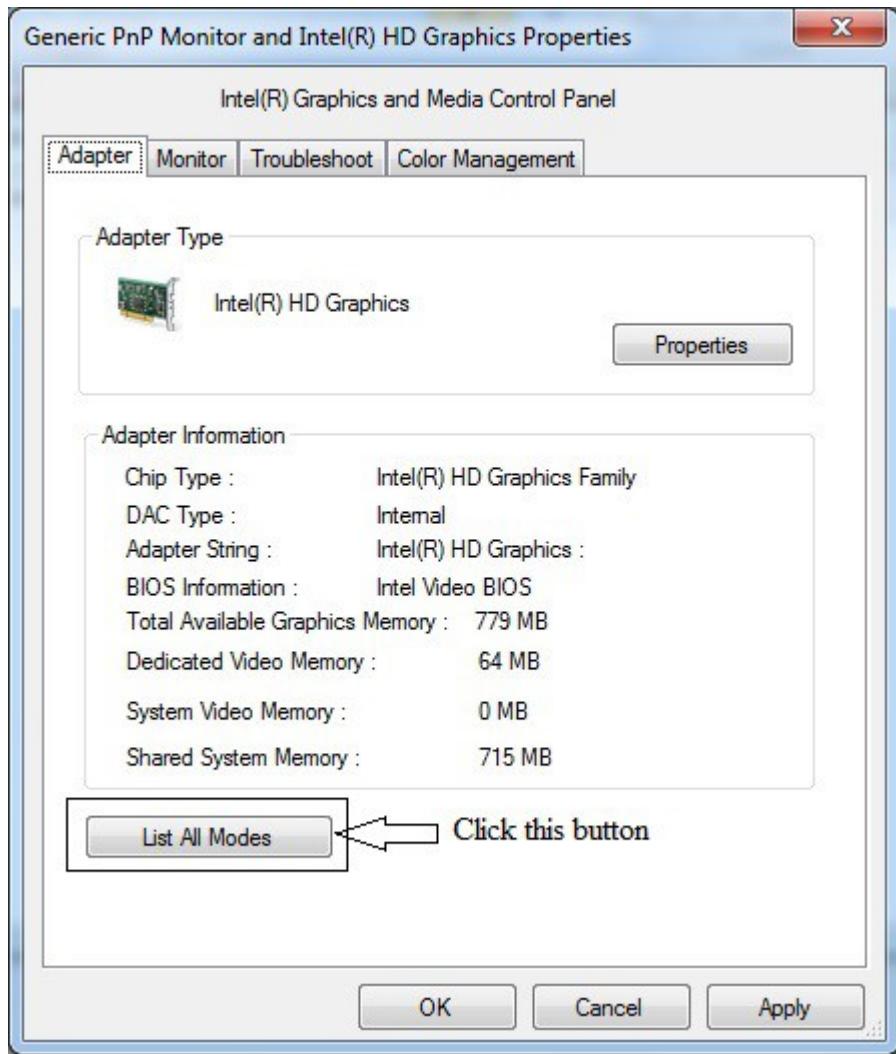
9.28 Changing the refresh rate in Windows 7.

Description: This lab exercise helps you to learn how to change the refresh rate in Windows 7.

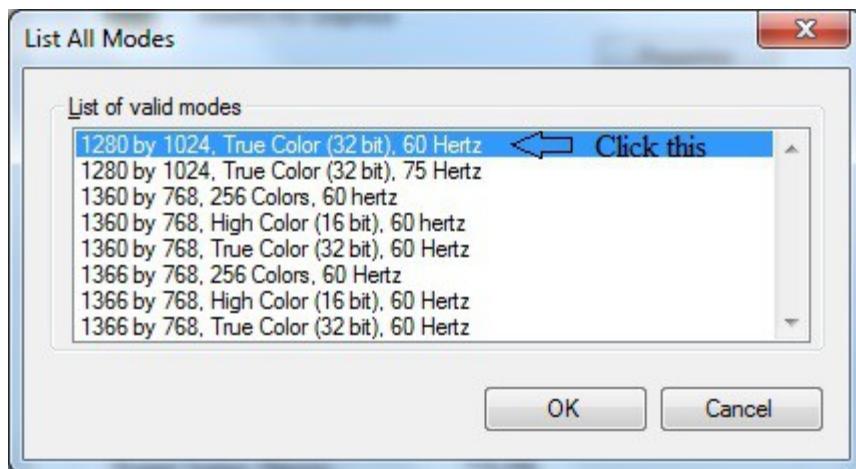
Instructions: 1. On loading a lab exercise, in a given simulator window click on the Advanced settings link.



2. To Select from a List of All Display Modes
 - a) Click on the Adapter tab, and click List All Modes button.



- b) Select the display mode with the screen resolution, color depth, and screen refresh rate as 1280 by 1024, True Color (32 bit), 60 Hertz, from list of valid modes drop down and then click OK button.



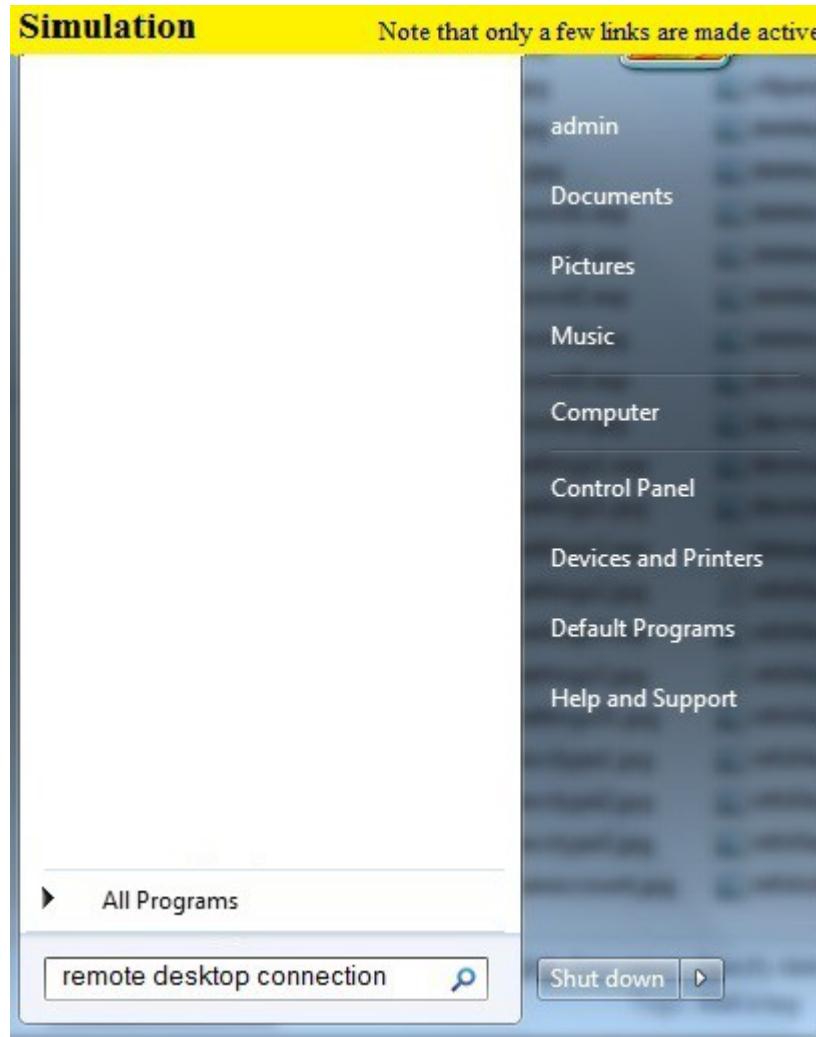
3. Click Apply and then OK button in Adapter tab window and also click apply and OK button in windows 7 window.

[Back](#)

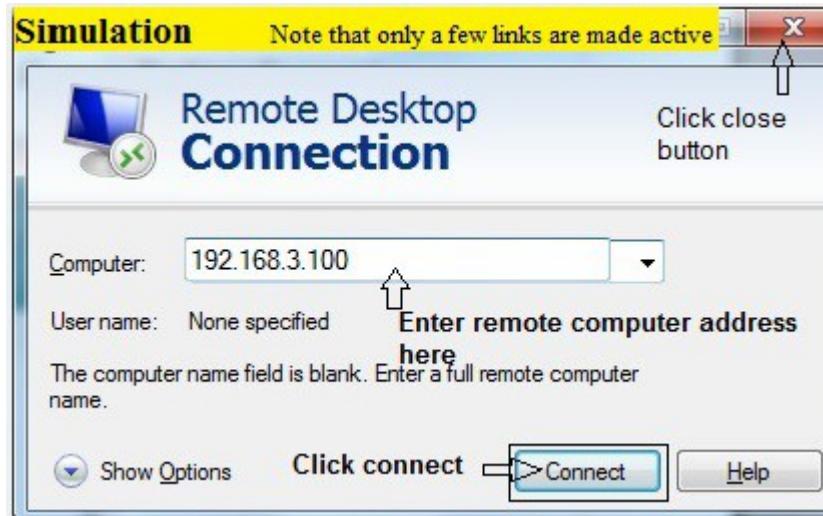
9.29 Connecting to a remote desktop using windows 7

Description: This lab exercise helps you to know how to connect to a remote desktop

Instructions: 1. On loading a lab exercise, in a given simulation start menu, type “*remote desktop connection*” in the given search box and hit enter button.



2. In Remote Desktop connection window type the address of the remote computer as 192.168.3.100 in computer text box and click connect button and then click close button



Explanation: With remote desktop connection we can connect to a computer running windows from another computer running windows that is connected to a same network. To connect to a remote computer , that computer must be turned on , it must have network connection, remote desktop must be enabled, you must have network access to the remote computer and you must have permission to connect.

[**Back**](#)