

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 7
 - 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 Flashing 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**

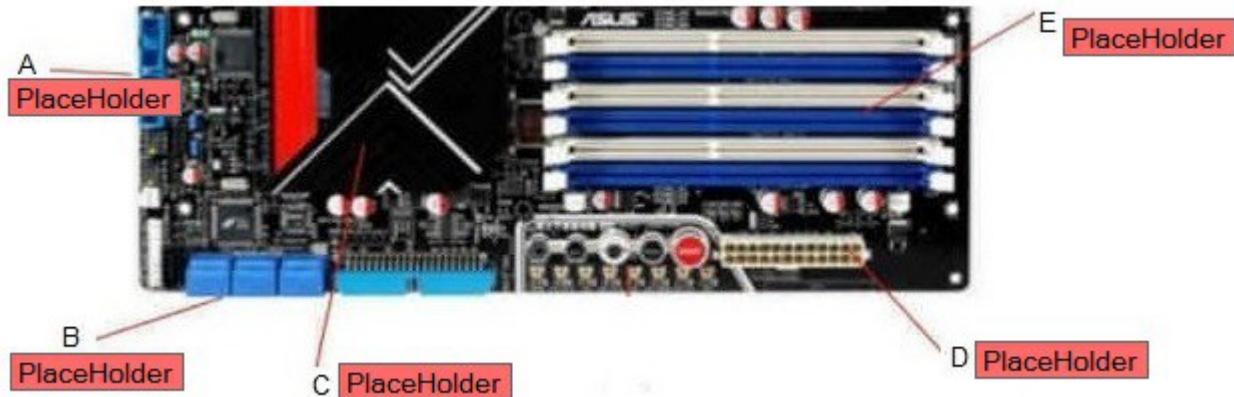
- [**9.25 Configuring Local Security Policy in Windows 7**](#)
- [**9.26 Configuring hardware settings using Device Manager**](#)
- [**9.27 Disabling Startup Programs in Windows 7**](#)
- [**9.28 Changing the refresh rate in Windows 7**](#)
- [**9.29 Connecting to a remote desktop using windows 7**](#)

1. PC Hardware

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

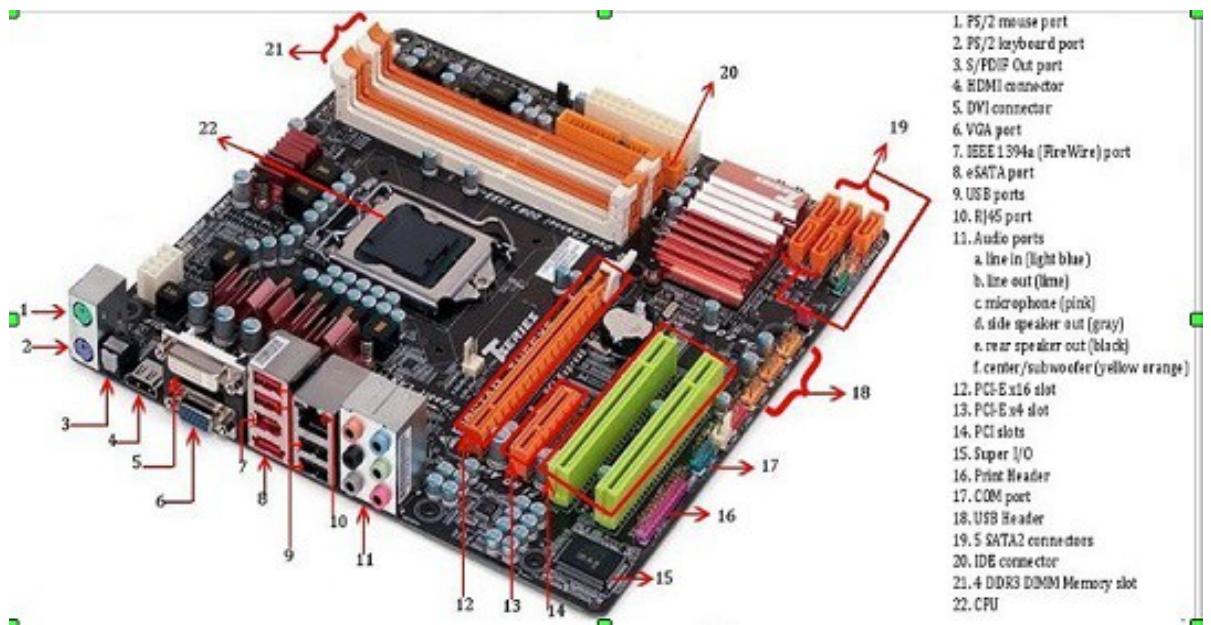
Description: This lab exercise helps to identify the parts of an ATX motherboard.

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.



A PlaceHolder



B PlaceHolder



C PlaceHolder



D PlaceHolder



E PlaceHolder



F PlaceHolder

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).

Description: This lab exercise helps to identify the CMOS battery in the motherboard.

Instructions: 1. An ATX motherboard figure is given below

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



Explanation:

CMOS (complementary metal-oxide-semiconductor) it is also called as non-volatile BIOS memory is the term usually used to describe the small amount of memory on a computer motherboard that stores the BIOS settings.

The CMOS is usually powered by a CR2032 cell battery. Most CMOS batteries will last the lifetime of a motherboard (up to 10 years in most cases) but will sometimes need to be replaced. Incorrect or slow system date and time and loss of BIOS settings are major signs of a dead or dying CMOS battery.



[Back](#)

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

Description: This lab exercise helps to identify the 24 pin ATX power connector in the motherboard.

Instructions: 1. An ATX motherboard figure is given below

2. Click on the ATX 24v power supply, if the clicked location is correct it indicates the green mark, otherwise it indicates the red mark.



Explanation:

The ATX standard has two different versions of the main power cable: the original 20 pin cable, and the newer 24 pin cable. The main ATX connector is a 20-pin connector. The four pins carrying power are 3.3 V, 3.3 V, 5 V, and 5 V. This allows the motherboard to pull about 20 to 30 watts.

The 24-pin ATX connector is simply the 20-pin connector along with the extra 4-pin connector on the side. This provides the 4 pins carrying power as ATX 20-pin connector plus an additional 4 pins with 5 V standby, 12 V, 12 V, and 3.3 V. The below shows the 24-pin ATX power connector.



[Back](#)

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

Description: This lab exercise helps to identify different memory modules.

Instructions: 1. Different memory modules are labeled as A, B, C, D, and E in the given figure.

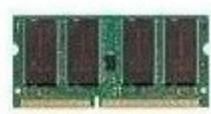
2. Drag and drop the name of the memory modules to their respective places.



A PlaceHolder



B PlaceHolder



C PlaceHolder



D PlaceHolder



E PlaceHolder

Explanation:

SDRAM DIMM (Dual In-line Memory Modules) SDRAM stands for Synchronous Dynamic Random Access Memory. DIMMs allow the ability to have two rows of DRAM chips. They are able to contain twice as much memory on the same size circuit board compared to SIMM (stands for Single Inline Memory Module, and not used now-a-days). In its basic form, DIMMs contain 168 pins and transfer data in 64 bit chunks. SDRAM DIMMs with 168 pins have two notches on the bottom of the PCB.

DDR DIMM: DDR DIMMs have 184 pins and may be identified by one notch at the bottom of the module. Note that DDR2 and DDR3 modules also have only one notch at the bottom of the board. However, they may be identified by the position of the notch. As may be observed, DDR (DDR1) modules have a notch slightly to the right in comparison with DDR2 memory module, and DDR3 has a notch to far left of the bottom of the module as may be seen in the figure above.

DDR3 DIMM Memory module : DDR3 memory modules are available in both DIMM and SO-DIMM form factors. DIMMs are commonly used for desktop PCs, while SO-DIMMs are typically used for laptops and all-in-one computers. While DDR3 DIMMs and SO-DIMM are the same size as their DDR2 counterparts, they are not compatible with DDR2 RAM slots. The connecting pins are arranged differently, so it is physically not possible to insert a DDR3 memory module into a DDR2 or DDR slot, and vice versa.

SO DIMM (Small Outline DIMM) SO DIMMs are commonly used in notebooks and are about half the size of normal DIMMs. 144-pin SO-DIMMs have a single notch near the center. 200-pin SO-DIMMs have a single notch nearer to one side. The exact location of this notch varies. 204-pin SO-DIMMs (DDR3) have a single notch closer to the center than on 200-pin SO-DIMMs. The 200-pin SO-DIMM may belong to types DDR or DDR2. The notch location is different in both the cases, and these two types of memory are not interchangeable.

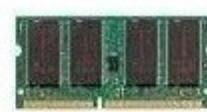
Below fig shows after dragging and dropping correct option on the image.



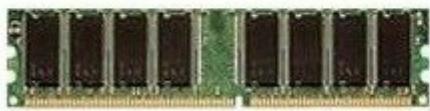
A 168 pin SDRAM DIMM



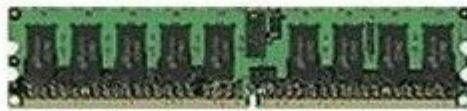
B 240 pin DDR3 DIMM



C 144 pin SDRAM SODIMM



D 184 pin DDR DIMM



E 240 pin DDR2 DIMM

[Back](#)

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

Description: This lab exercise helps to know the features of various memory types.

Instructions: 1. Different memory types are given on the column A.
2. Features of the memory types are given on the column B.
3. Match (drag & drop) the memory types given on the column A with their respective features given on the column B

Column A

1. DDR3
2. DDR2
3. DDR
4. SDRAM

Column B

1. 240 pin DIMM with quad, triple, or dual channels or be installed as a single DIMM
2. 240 pin DIMM can support dual channels or be installed as a single DIMM
3. 184 pin DIMM can support dual channels or be installed as a single DIMM
4. 168 pin DIMM with two notches on the module.

Explanation:

The computer main memory usually consists of some type of DRAM. Types of DRAM Packages and DRAM Memory are explained below:

- a. **168 pin DIMM (SDRAM):** It can run at much higher clock speeds than conventional memory. SDRAM actually synchronizes itself with the CPU's bus and is capable of running at 133 MHz and twice as fast EDO DRAM.
- b. **184 pin DIMM (DDR-SDRAM):** It supports data transfers on both edges of each clock cycle, effectively doubling the memory chip's data throughput. DDR-SDRAM is also called SDRAM II. DDR stands for Double Data Rate.
- c. **240 DIMM (DDR2-SDRAM):** It supports higher speeds than it's predecessor DDR SDRAM. DDR2 SDRAM is a double data rate synchronous dynamic random-access memory interface. It supersedes the original DDR SDRAM specification and has itself been superseded by DDR3 SDRAM. DDR2 is neither forward nor backward compatible with either DDR or DDR3.
- d. **240 DIMM (DDR3-SDRAM):** It supports speeds faster than DDR2 SDRAM. DDR3 SDRAM, an abbreviation for double data rate type three synchronous dynamic random access memory, is a modern kind

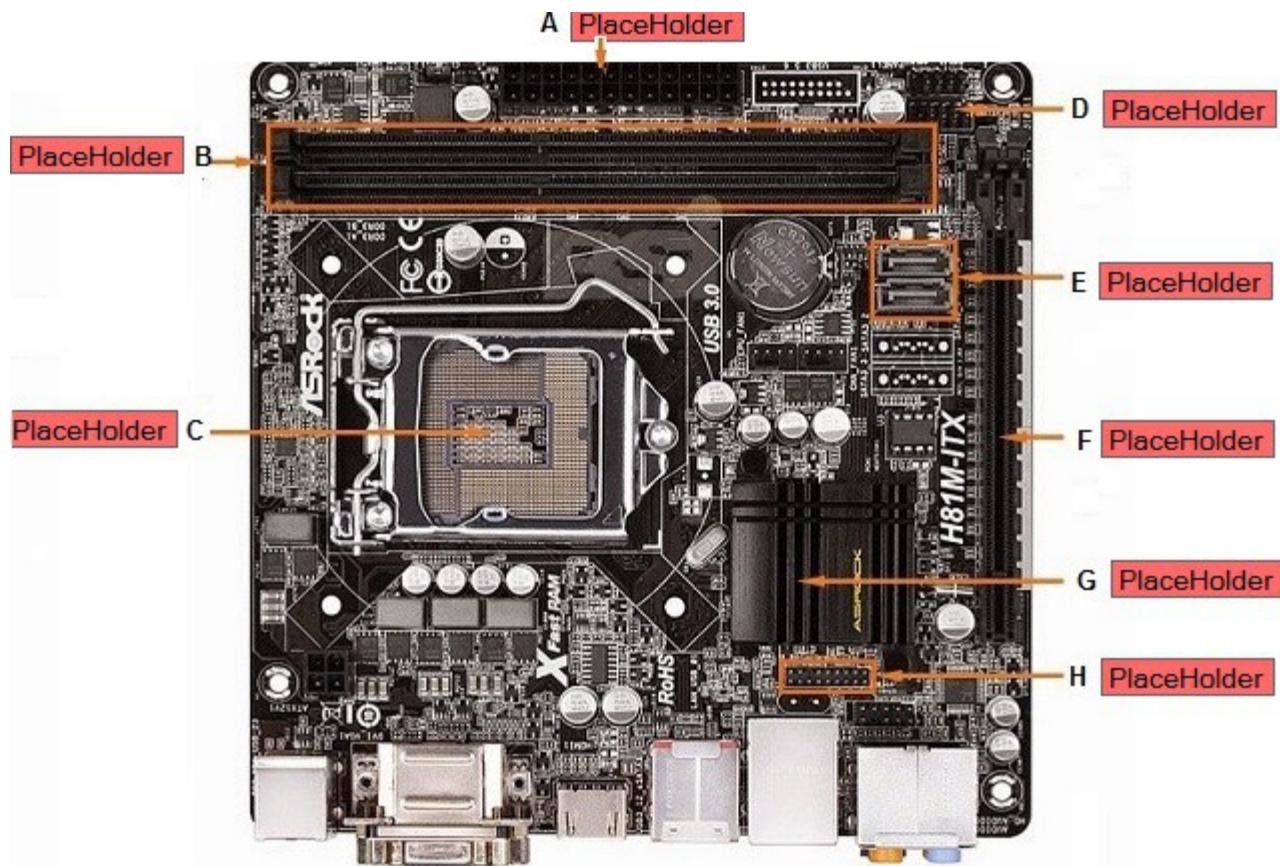
of dynamic random access memory (DRAM) with a high bandwidth interface, and has been in use since 2007. DDR3 SDRAM is neither forward nor backward compatible with any earlier type of random access memory (RAM) due to different signaling voltages, timings, and other factors.

[Back](#)

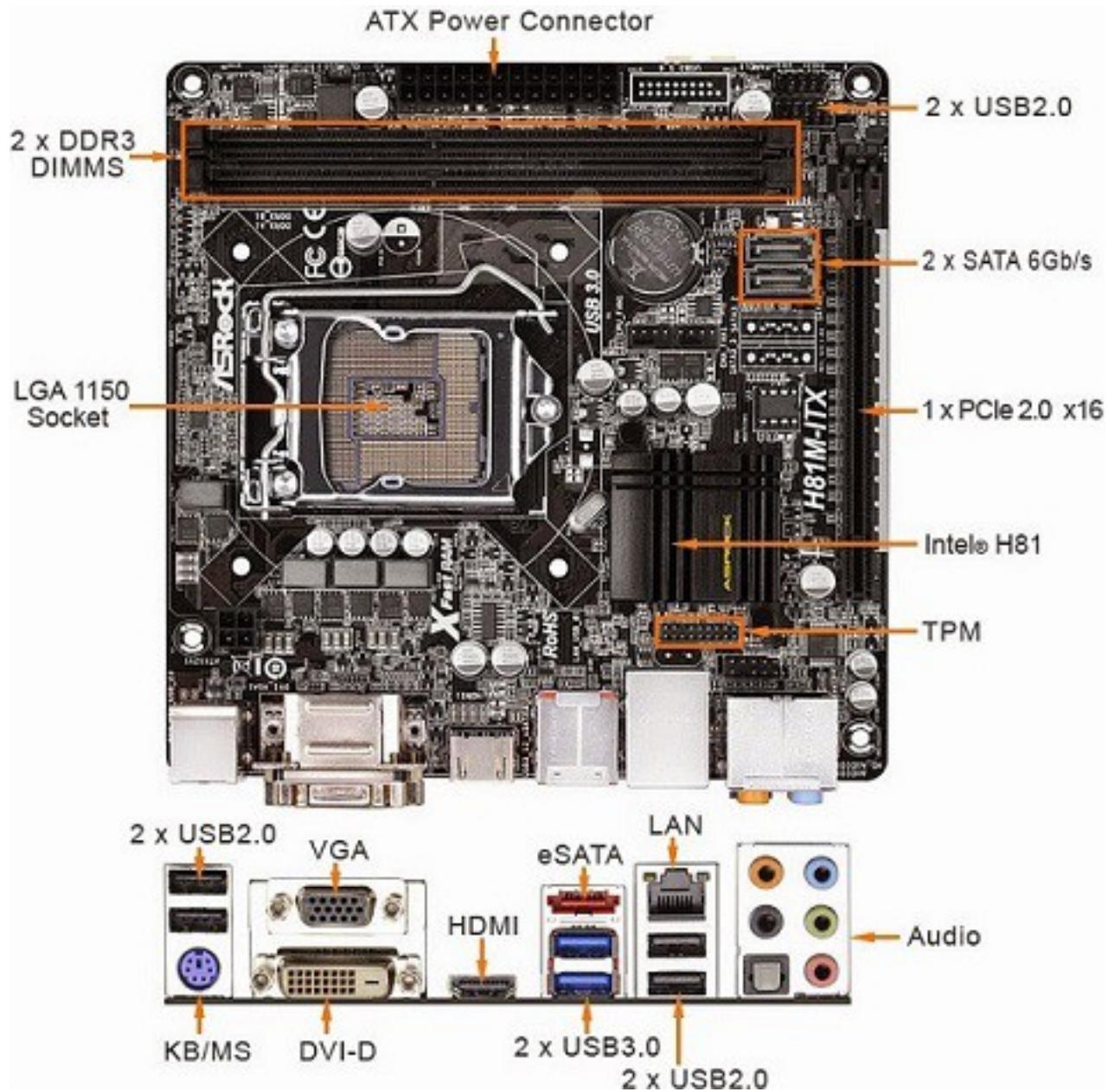
1.4 Identify the components of Mini ITX motherboard

Description: This lab exercise helps to identify the different components of Mini ITX motherboard

Instructions: 1. The below fig. shows Mini-ITX motherboard with different components
2. Drag and drop the component names into their respective options labeled as **A, B, C, D, E, F, G, H**



Explanation: Various components of Mini-ITX motherboard are as shown in the below figure



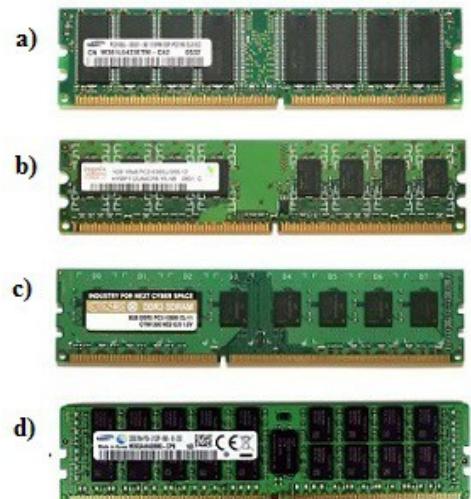
[Back](#)

1.5 Identifying DDR3 DIMM and inserting it into a motherboard slot

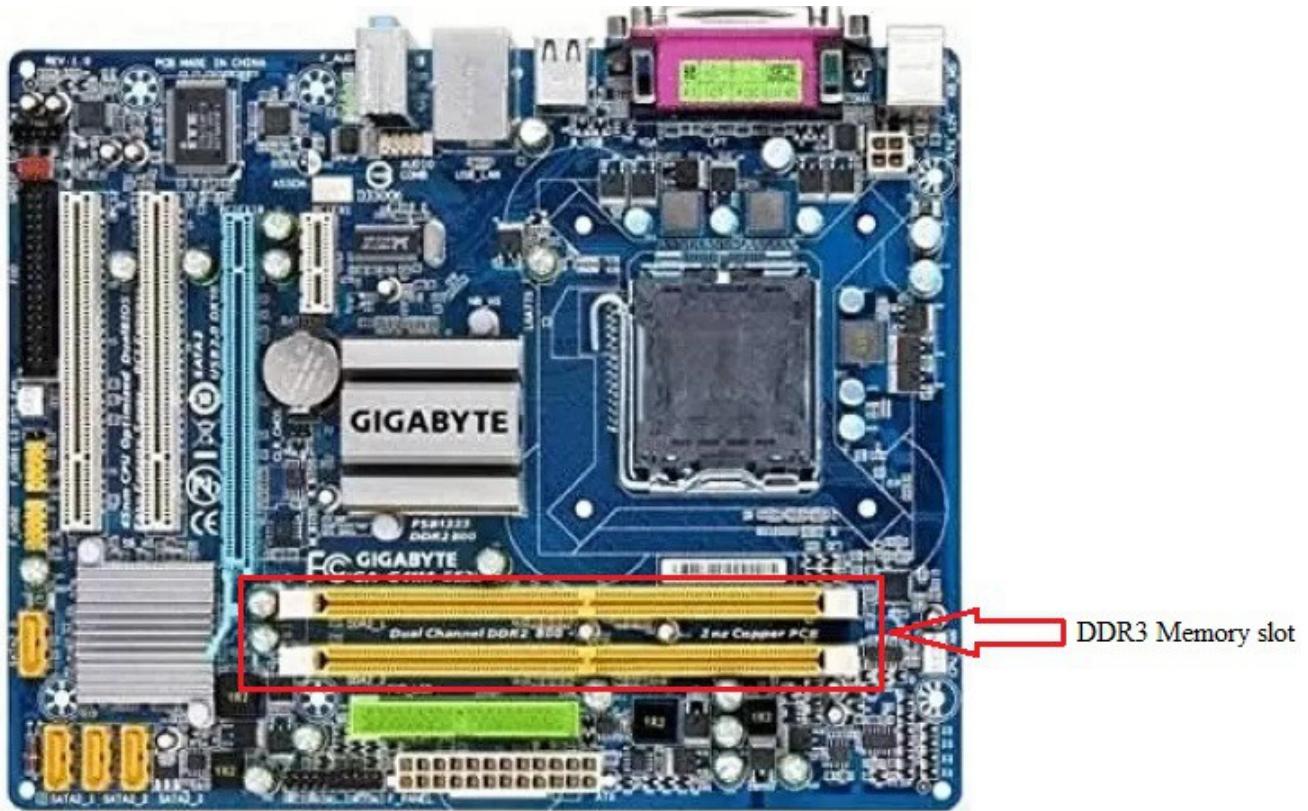
Description : This lab exercise helps to identify the DIMM memory slot

Instructions :

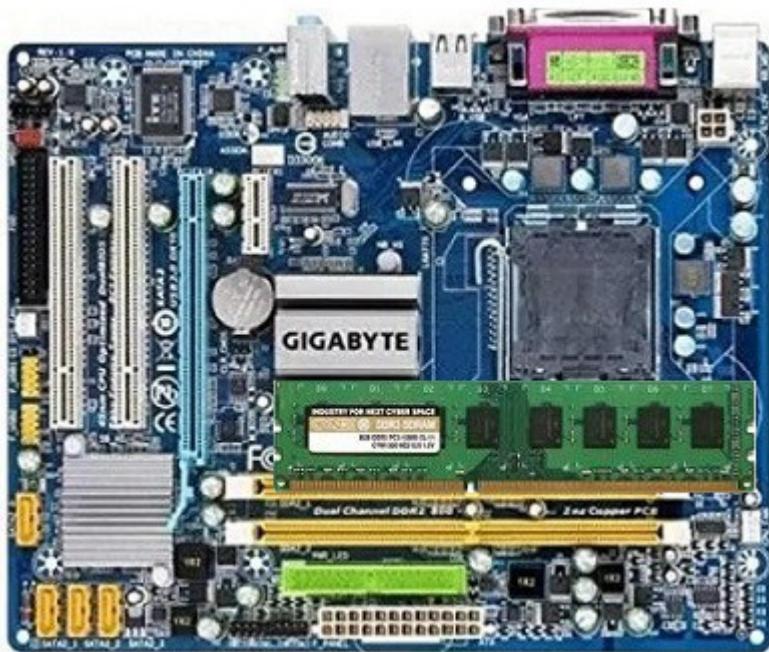
1. Select the DDR3 DIMM memory from the given list of image options.
2. Then Drag and Drop the selected image to appropriate DIMM memory slot in the motherboard.
3. Click “Click here to verify” button to verify your answer and then click “Exit” button.



Explanation: Below fig shows motherboard with DDR3 memory slot



After inserting ddr3 memory into a slot in the motherboard.



DDR SDRAM (Double Data Rate SDRAM): The next generation of SDRAM is DDR, which achieves greater bandwidth than the preceding single data rate SDRAM by transferring data on the rising and falling edges of the clock signal (double pumped). Effectively, it doubles the transfer rate without increasing the frequency of the clock. The transfer rate of DDR SDRAM is the double of SDR SDRAM without changing the internal clock. DDR SDRAM, as the first generation of DDR memory, the prefetch buffer is 2bit, which is the double of SDR SDRAM. The transfer rate of DDR is between 266~400 MT/s. DDR266 and DDR400 are of this type.



DDR2 SDRAM(Double Data Rate Two SDRAM): Its primary benefit is the ability to operate the external data bus twice as fast as DDR SDRAM. This is achieved by improved bus signal. The prefetch buffer of DDR2 is 4 bit(double of DDR SDRAM). DDR2 memory is at the same internal clock speed (133~200MHz) as DDR, but the transfer rate of DDR2 can reach 533~800 MT/s with the improved I/O bus signal. DDR2 533 and DDR2 800 memory types are on the market.



DDR3 DIMM Memory module: DDR3 memory modules are available in both DIMM and SO-

DIMM form factors. DIMMs are commonly used for desktop PCs, while SO-DIMMs are typically used for laptops and all-in-one computers. While DDR3 DIMMs and SO-DIMM are the same size as their DDR2 counterparts, they are not compatible with DDR2 RAM slots. The connecting pins are arranged differently, so it is physically not possible to insert a DDR3 memory module into a DDR2 or DDR slot, and vice versa.



DDR4 DIMM Memory module: Stands for "Double Data Rate 4." DDR4 is the fourth generation of DDR RAM, a type of memory commonly used in desktop and laptop computers. DDR4 is designed to replace DDR3, the previous DDR standard. Advantages include faster data transfer rates and larger capacities, greater memory density and more memory banks (16 rather than 8). DDR4 also operates at a lower voltage (1.2V compared to 1.5V), so it is more power-efficient.



Below are some notable DDR4 specifications:

- 64 GB maximum capacity per memory module (common capacities include 16 GB and 32 GB)
- 16 internal memory banks
- 1600 Mbps to 3200 Mbps data transfer rates
- 1.2 volts of electrical power required
- 288 pins in a regular DIMM, 260 pins in a SO-DIMM

DDR4 memory modules come in two primary form factors - DIMMs and SO-DIMMs. DIMMs are commonly used for desktop towers, while smaller SO-DIMMs are designed for laptops and all-in-one desktop computers. DDR4 DIMMs are the first to have a curved bottom edge, which makes it easier to insert them into and remove them from RAM slots on a motherboard. This and the unique position of the notch between the pins make it impossible to insert a DDR4 chip into an incompatible slot.

Faster speeds and increased memory bandwidth allow DDR4 SDRAM to keep up with modern processors, including multi-core CPUs. This prevents the memory from being a bottleneck as processing speeds and bus speeds increase.

NOTE: SDRAM must be matched with the specific requirements of a computer. When upgrading your memory, make sure you select the type (DDR2, DDR3, DDR4, etc) and speed (1600, 2400,

3200, etc) that is compatible with your computer.

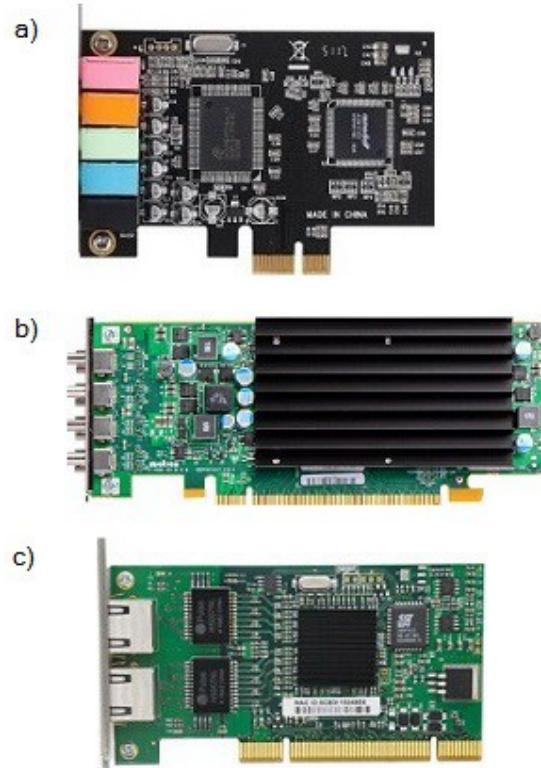
[Back](#)

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

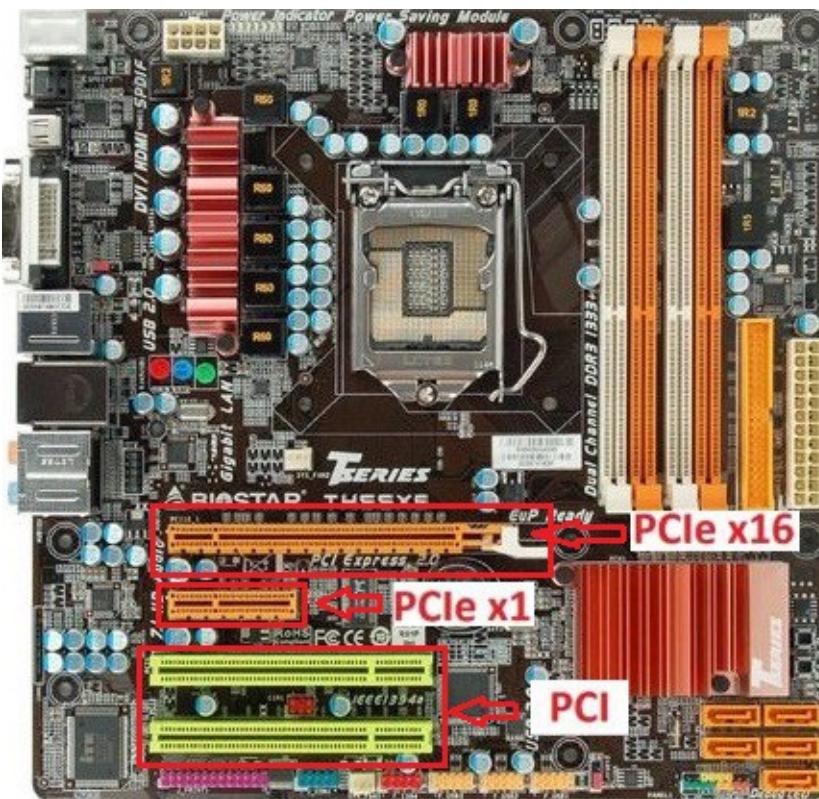
Description: The lab exercise help you in identifying the graphics card and inserting it to a appropriate slot on the motherboard.

Instructions:

1. Select graphic card with PCIeX16 interface from the given list of image options.
2. Drag and Drop the selected image to appropriate slot on the motherboard.
3. Click “Click here to verify” button to verify your answer and then click “Exit” button.



Explanation:The figure shows a Motherboard with PCIeX16 slots.



The graphics card has a PCIeX16 slot in the motherboard. All modern-day graphics cards come with a PCIeX16 connector and they install in the PCIeX16 slot on the motherboard. Slots are available in one-lane, two-lane, four-lane, eight-lane and 16-lane configurations, usually expressed as PCIe x1, x2, x4, x8 or x16. Speeds of PCIe interfaces are given below:

Below fig shows after dragging and dropping the graphic card to the PCIe X16 slot in the motherboard. Please note that the card is shown in horizontal position for the purpose of understanding. Otherwise, it is inserted in a vertical position



PCIe Version	Year	Data x'fer rate	1X	16X
PCIe 4.0	2017	16 GT/s	2 GB/s	32 GB/s
PCIe 5.0	2019	32 GT/s	4 GB/s	64 GB/s
PCIe 6.0	2021	64 GT/s	8 GB/s	128 GB/s

Various options available in drag n drop are briefly described below:

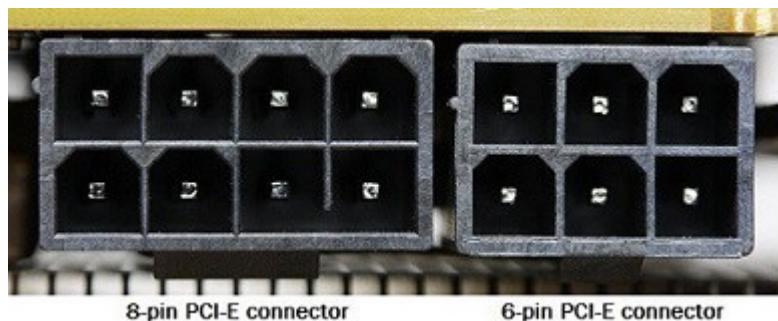


a) Graphic card: A graphics card is a major component of a PC and it generally consumes more power compared to other components. Entry-level graphics cards draw their power from the PCI Express x16 slot only but high-end graphics cards require external power from the PSU for their working. The external power for these high-end graphics cards comes from the 6-pin and 8-pin PCI-Express power connectors from the power supply.



PCI Express x16 connector: Every modern-day graphics card comes with a PCI Express x16 connector that goes in the PCI Express x16 slot of your motherboard. PCI Express x16 connector connects your graphics to the motherboard and is the only interface through which communication happens. A PCI Express x16 slot can

provide a maximum of 75 Watts to the graphics card which is enough for entry-level graphics cards. Even some mid-range graphics cards can also work on the power from the PCI Express x16 slot alone but higher mid-range graphics cards and high-end graphics cards require external power from the PSU through 6-pin or 8-pin power connectors. You can see these connectors below:



In fig b below you can see a typical PCI card, pointed out an alignment notch (A), this is used to align the card with the slot and take a look at the slot in fig a you can see how it is aligned with the card.





b) Sound Card: A sound card is an expansion card or integrated circuit that provides a computer with the ability to produce sounds that can be heard from the computer speakers, external speakers, and headphones. Sound Cards can also be referred to as sound board or an audio cord. A sound card allows you to have a better quality of sound, so that the sound coming out of the computer is clear. The point of the sound card or its function is so that you are able to listen to music, watch movies, audio conferencing, using it for presentations and many other things that we use sound for. There are two main types of sound cards, PCI and ISA.



c) Network Card: The figure shows a typical network card with RJ45 is a type of connector (not visible, though), commonly used for Ethernet networking. Network cards come in two main categories, 1) wired and 2) wireless.



Wireless NICs need to use wireless technologies to access the network, so they have one or more antennas sticking out of the card. You can see an example of this with the TP-Link PCI Express network card.

(Please note that the images have been resized for brevity and not actual size in the images)

[Back](#)

1.7 Installing SATA hard drive to appropriate slot on the motherboard

Description: Lab exercise explains identifying SATA power and data cable and connecting the same into appropriate slots on the motherboard and internal SATA hard drive.

Instructions:

Task1:

1. From the given list of images identify the SATA data cable.
2. Drag and Drop one end “EndA” to SATA hard drive and other end “EndB” to appropriate SATA connector slot in the motherboard.
3. Insert SATA data cable to any one , available SATA slot on the motherboard.

Task2:

1. Identify the SATA power cable from the list of given images.
2. Drag and Drop it to the appropriate slot on the SATA hard drive.

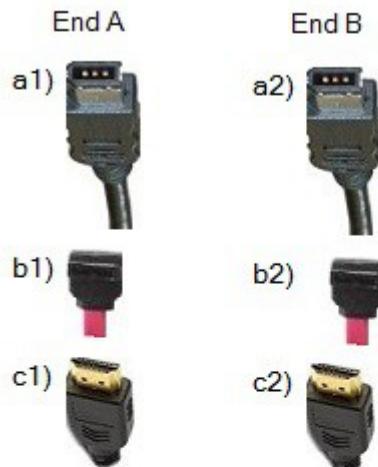
Task3:

1. Click the “Click here to verify” button to verify your answer.
2. Then click the “Exit” button.

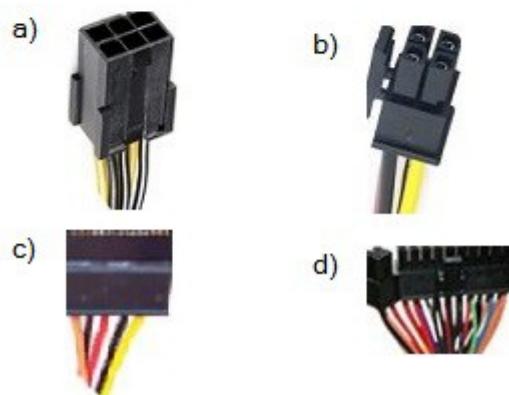
Note that both the motherboard and power supply unit will be inside a computer cabinet, but shown separately in the displayed figure for better understanding. The SATA power cable emanates from the power supply unit.



Data Cables

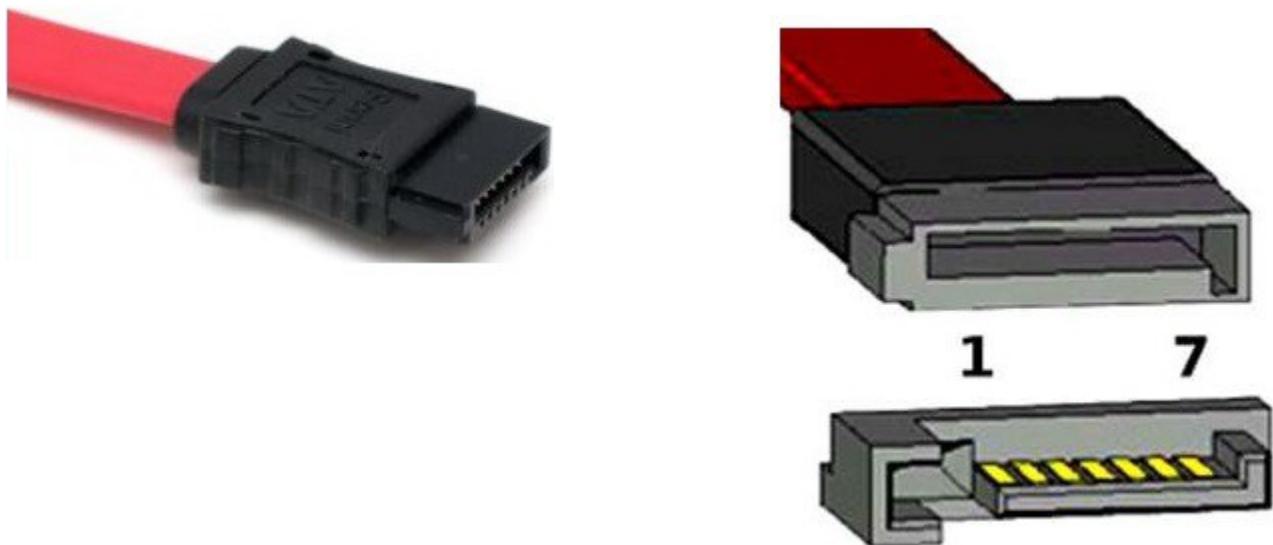


Power Cables



Explanation: In this lab, you need to identify appropriate SATA cables and the corresponding slots on the motherboard and disk drive. The figures below show the connectors that connects to the hard drive.

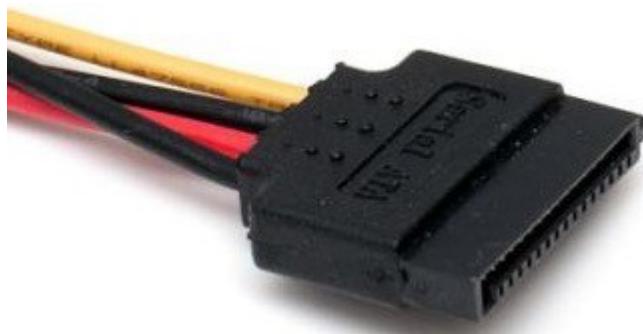
1. SATA data cable (7-pin):



SATA Data Pin out

Pin#	Signal Name	Signal Description
1	GND	Ground
2	A+	Transmit+
3	A-	Transmit-
4	GND	Ground
5	B-	Receive-
6	B+	Receive+
7	GND	Ground

2. The power connector (15-pin):



The SATA 15-pin power supply connector is one of the standard peripheral power connectors in computers. It's the standard connector for all SATA-based hard drives, SSDs and optical drives. SATA power cables come from the power supply unit. The connector is keyed so that it's not possible to insert it in the wrong orientation without breaking something.

SATA Power Pin out

Pin#	Signal Name	Signal Description
1	V33	3.3v Power
2	V33	3.3v Power
3	V33	3.3v Power, Pre-charge, 2nd mate
4	Ground	1 st Mate
5	Ground	2 nd Mate
6	Ground	3 rd Mate
7	V5	5v Power, pre-charge, 2 nd mate
8	V5	5v Power
9	V5	5v Power
10	Ground	2 nd Mate
11	Reserved	-

12	Ground	1 st Mate
13	V12	12v Power, Pre-charge, 2 nd mate
14	V12	12v Power
15	V12	12v Power

SATA features more pins than the traditional MOLEX connector:

- A third voltage is supplied, 3.3 V, in addition to the traditional 5 V and 12 V.
- Each voltage transmits through three pins ganged together, because the small contacts by themselves cannot supply sufficient current for some devices. (Each pin should be able to provide 1.5 A.)
- Five pins ganged together provide ground.
- For each of the three voltages, one of the three pins serves for hotplugging. The ground pins and power pins 3, 7, and 13 are longer on the plug (located on the SATA device) so they will connect first. A special hot-plug receptacle (on the cable or a backplane) can connect ground pins 4 and 12 first.
- Pin 11 can function for staggered spinup, activity indication, or nothing. Staggered spinup is used to prevent many drives from spinning up simultaneously, as this may draw too much power. Activity is an indication of whether the drive is busy, and is intended to give feedback to the user through a LED.

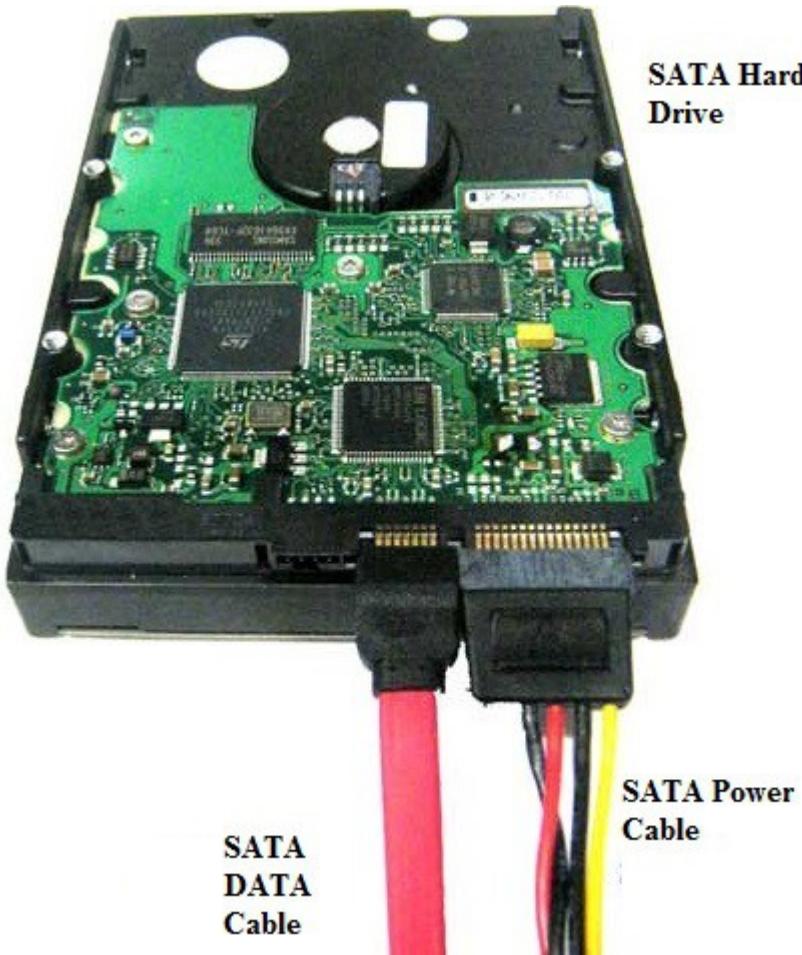
The figure below shows the motherboard and the disk drive after completing the cable connections. As usual, some distance is maintained between the female and male connectors for understanding purpose. For Drag n Drop of SATA data cable, any free SATA slot may be used.



Following instructions help you to insert SATA hard drive to your motherboard.

Step1: Turn off your computer and unplug it from mains power before you begin. Use of anti static wrist strap is recommended.

Step2: Insert one end of the SATA cable in the hard drive and the other end in the free SATA slot. Identify the SATA power cable emanating from the power supply and insert it into the matching slot on the hard drive.



The figure shows the SATA hard drive with both the DATA and Power cables inserted into SATA connector slots.

Typical connection of a hard drive using SATA cables. The red cable is SATA data, and the connector on the right is the power SATA cable. An older power supply might only have a ‘molex’ style power connector and not the SATA one shown above. Most hard drives will have the option for both Molex or SATA power connections, and you can use one or the other as you like. The two different types together look like this:

Fig: SATA Data cable , Power cable and hard disk interface physical map



These are the two options for connecting power to your hard drive. You only need to connect one or the other. The top plug is a “Molex” connector, and the bottom plug is SATA power. Once connected up power, then connect the data side of things. For this you need a SATA cable to connect your new hard drive to your motherboard. One end of the SATA cable will plug into your new hard drive, and the other needs to go to a SATA port on your motherboard.

Configuring the BIOS

Close your computer case and start your computer. Your computer may automatically detect your new drive. If your computer does not automatically detect your new drive, follow the steps below.

Restart your computer. While the computer restarts, run the system setup program by pressing a special key, such as DELETE, ESC, or F1 during the startup process. Within the system setup program, instruct the system to auto detect your new drive. Save the settings and exit the setup program. When your computer

restarts, it should recognize your new drive.

[Back](#)

1.8 Objective Test 1. Answer the following questions

1. Which of the following is the most common HDD motherboard connection port?

- A.RS-232
- B.DMM
- C.SATA
- D. Serial

Answer: C. SATA

2 Is DDR3 backward compatible With DDR2?

- A. Yes
- B. No

Ans: No

Explanation: No. DDR3 memory chips and modules are very different from DDR2. For example, DDR3 runs at a lower voltage (1.5V) than DDR2 (1.8V).

3.The computer shuts down unexpectedly every half hour. Which of the following could be the most probable cause of the issue?

- A. Malfunctioning processor cooling fan
- B. Faulty RAM
- C. Faulty hard drive
- D. Dead CMOS battery

Answer - A

Explanation: The most probable cause of a computer shutting down unexpectedly is a malfunctioning processor fan. In the absence of a component which can dissipate heat generated by the processor, the processor overheats. Eventually, when a threshold temperature is reached, the OS shuts down the computer.

4.Which of the following would BEST provide cooling to a processor?

- A. Case fan
- B. Heal sink
- C. Liquid cooling system
- D. CPU fan

Answer: C

5.Which of the following motherboard components quality can be measured using DPI?

- A. PS/2 port
- B. Audio interface
- C. Display adapter
- D. IEEE 1394 port

Answer: C

6.Which of the following memory types has the smallest form factor?(Select two)

- A.RIMM
- B.DIMM
- C. Micro DIMM
- D.SODIMM

Answer: C,D

Explanation: The SODIMM and Micro DIMM are the common laptop small-form factor memory standards. Of the two, Micro DIMM is smaller.

7. How many pins are on a DDR2 SO type laptop memory module?

- A.100
- B.168
- C.200
- D.204

Answer: 200

8. Which type of motherboard interface would you use for SLI graphics card configuration?

- A.ISA
- B.AGP
- C.PCI
- D. PCIe

Answer: D PCIe

9. What are the two most common HDD motherboard connection ports?

- A.RS-232, Serial
- B.DMM and ATA
- C.PATA and SATA
- D. Serial and PS2

Answer: C

10. What must be installed between a CPU and the heat sink?

- A. Electrical insulation pad
- B. Anti-vibration pad
- C. Thermo paste
- D. Liquid cooling oil

Answer : C

11.William purchased a new IDE hard drive and installed it on his computer. He switched ON and found that the new hard drive was not recognized. Which of the following should he check for FIRST?

- A. Jumpers on the hard drive
- B. Cable sequence
- C. Drivers that need to be loaded
- D. Hard drive manufacturer Website information

Answer - A -

Explanation: If a new hard drive is not recognized, the most crucial aspect to be checked for is the jumper setting on the hard drive. The jumper setting should be chosen to either Cable Select or Slave and Master, based on where the drive is connected.

12. After completing the installation of your internal and external SCSI devices that connects to

an Adapter AHA-1542s SCSI adapter, you find that none of the devices works. Which of the following should you do first to try and fix the problem?

- A. Disconnect all devices and start over.
- B. Remove the adapter and replace with a new one.
- C. Change the SCSI ID's
- D. Enable termination on the adapter.

Answer:D

Explanation: Some adapter cards like the Adapter AHA-1542s still need to have terminators installed. If you setup both internal and external devices and none of them work, try enabling termination on it to see if that fixes the problem. Incorrect Answers:A: Disconnecting all the devices and starting over will not solve the problem as you need to enable termination on the adapter. B: You do not have to remove and replace the adapter; you need to enable termination on it to make it function properly. C: Changing the SCSI IDs will not solve the problem when all that is necessary is to enable termination on the adapter to enable proper functioning of the SCSI devices.

13. A technician determines that a SCSI card needs an update to its embedded code. This is commonly referred to as updating the:

- A. driver
- B. operating system
- C. system
- D. firmware

Answer: D

14. Which of the following chipsets is responsible for controlling the data flow between a PATA optical drive and the processor?

- A. Northbridge
- B. BIOS
- C. Southbridge
- D. DMA controller

Answer: C

15. Which type of media is typically used for large data backups?

- A. CD ROM
- B. DVD-R
- C. DVD-RW
- D. Tape

Answer: D

16. When two EIDE drives are installed on the same motherboard port. How is the slave and master drive determined?

- A. The drive closest to the motherboard connection port is always the master.
- B. The jumper settings determine slave and master.
- C. Slave and master are configured manually during the BIOS setup.
- D. Modern EIDE drives are both masters.

Answer: B. The jumper settings determine slave and master

17. You have just replaced a 40 GB HDD with a newer 500 GB drive. After installing the 500 GB drive, the system only sees 137 GB. What is most likely causing the problem?

- A. The new 500GB drive has a section of bad sectors at approximately 137 GB track.
- B. The drive has been installed with the data cable on the wrong motherboard port.

C. The drive has a boot sector virus which has corrupted the MBR.

D. The BIOS does not support drives larger than 137 GB and needs to be upgraded.

Answer : D. The BIOS does not support drives larger than 137 GB and needs to be upgraded.

18. You suspect that the hard disk drive contains bad sectors or lost clusters. Which utility would you select to perform a hard disk repair for bad sectors or lost clusters?

A. Chkdsk

B. Fdisk

C. Sysconfig

D. Msconfig

Answer: A. Chkdsk

19. Which command is used to partition a hard disk?

A. Format

B. Partition

C. Fdisk

D. System Config

Answer: C. Fdisk

20. You have just replaced a customer's floppy drive with a new one. The new floppy drive LED stays on constantly after the computer is booted. What is most likely the problem?

A. The data cable connection is incorrectly connected backwards

B. The wrong type of power connector has been connected to the floppy drive.

C. The BIOS did not properly detect the new floppy drive.

D. The LED is being lit all the time is normal and indicates the drive is working correctly.

Answer: A. The data cable connection is incorrectly connected backwards

21. An expansion card that allows a computer to communicate with a server via unshielded twisted pair cable is known as:

A. A USB controller.

B. An AGP card.

C. A network interface card (NIC).

D. A cable modem.

Answer : C. A network interface card (NIC).

22. Which of the following power supply connectors would you use to supply power to a new HDD?

A. PCIe 6-pin

B. 20+4 pin

C. Floppy connector

D. SATA connector

Answer: D. SATA connector

[Back](#)

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 of 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:



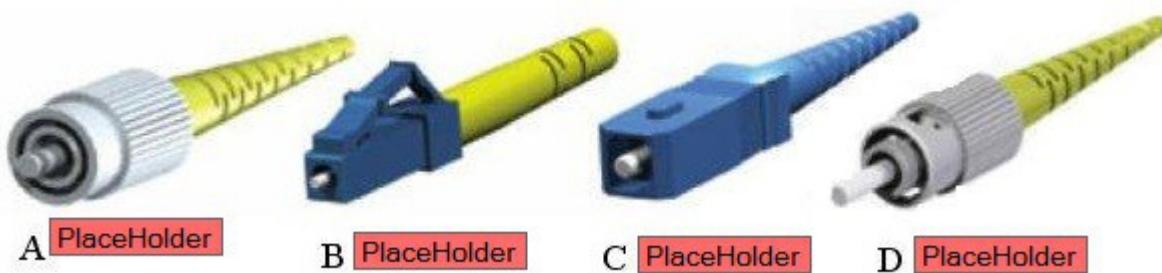
[Back](#)

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:

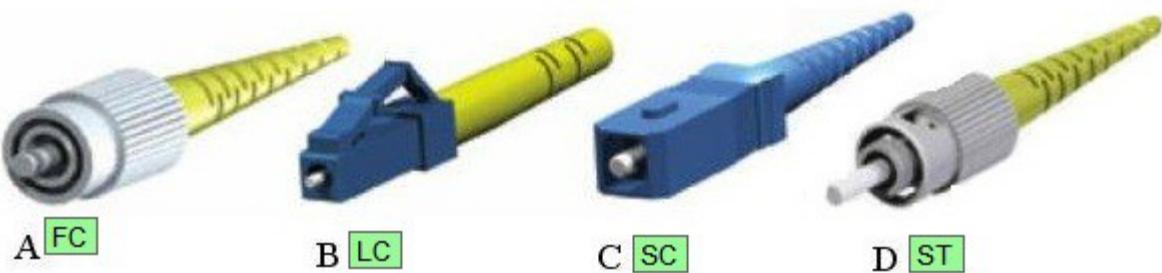
1. The below figure shows the different connector types labeled as A, B, C, D.
2. The name of the connector types are given as options
3. Drag and drop the name of the connector types into their respective places.



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.
- 5.

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



[Back](#)

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

Description: This lab exercise helps you to know the port numbers of a various TCP/IP protocols.

Instructions: 1. Names of the protocols are given on the column A.
2. Match (drag and drop) the protocol given on the column A with their respective

port numbers given on the column B.

Column A	Column B
1. FTP (File Transfer Protocol)	21
2. Telnet	23
3. SMTP (Simple Mail Transfer Protocol)	25
4. HTTP (Hyper Text Transfer Protocol)	80
5. POP3 (Post Office Protocol)	110
6. HTTPS (HTTP Secure)	443
7. DNS	53
8. IMAP	143

[Back](#)

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

Description: This lab exercise helps you to know about the descriptions of various TCP/IP protocols

Instructions: 1. Names of the protocols are given on the column A.

2. Drag and drop the protocol given on the column A to their respective features given on the column B.

Column A	Column B
1. HTTP	Set of rules for transferring files on the World Wide Web.
2. SMTP	A TCP/IP protocol used in sending and receiving e-mail
3. UDP	A communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP).
4. Telnet	A TCP/IP protocol for accessing remote computers
5. ICMP	A message control and error-reporting protocol between a host server and a gateway to the Internet
6. IGP	A protocol for exchanging routing information between gateways (hosts with routers) within an autonomous network
7. BGP	A protocol for exchanging routing information between gateway hosts(each with its own router) in a network of autonomous systems.

Explanation:

HTTP (Hypertext Transfer Protocol) : is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. As soon as a Web user opens their Web browser, the user is indirectly making use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols (the foundation protocols for the Internet).

SMTP (Simple Mail Transfer Protocol) : is a TCP/IP protocol used in sending and receiving e-mail.

However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, sendmail is the most widely-used SMTP server for e-mail. A commercial package, Sendmail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be setup to include POP3 support.

UDP (User Datagram Protocol): is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in.

Telnet: is a user command and an underlying TCP/IP protocol for accessing remote computers. Through Telnet, an administrator or another user can access someone else's computer remotely. On the Web, HTTP and FTP protocols allow you to request specific files from remote computers, but not to actually be logged on as a user of that computer. With Telnet, you log on as a regular user with whatever privileges you may have been granted to the specific application and data on that computer.

ICMP (Internet Control Message Protocol): is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the IP software and are not directly apparent to the application user.

IGP (Interior Gateway Protocol): is a protocol for exchanging routing information between gateways (hosts with routers) within an autonomous network (for example, a system of corporate local area networks). The routing information can then be used by the Internet Protocol (IP) or other network protocols to specify how to route transmissions.

BGP (Border Gateway Protocol): is a protocol for exchanging routing information between gateway hosts (each with its own router) in a network of autonomous systems. BGP is often the protocol used between gateway hosts on the Internet. The routing table contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen. Hosts using BGP communicate using the Transmission Control Protocol (TCP) and send updated router table information only when one host has detected a change. Only the affected part of the routing table is sent. BGP-4, the latest version, lets administrators configure cost metrics based on policy statements. (BGP-4 is sometimes called BGP4, without the hyphen.)

BGP communicates with autonomous (local) networks using Internal BGP (IBGP) since it doesn't work well with IGP. The routers inside the autonomous network thus maintain two routing tables: one for the interior gateway protocol and one for IBGP.

[Back](#)

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

Description: This lab exercise helps to learn about the various IPconfig labels and their descriptions.

Instructions: 1. Name of the Ipconfig label is give on the column A.
2. Match (drag and drop) the label given on the column A with their respective functions given on the column B.

Column A	Column B
1. ipconfig	1. displays the summary IP information for the system

- | | |
|-------------------------|---|
| 2. ipconfig /all | 2. displays the detailed IP information for the system |
| 3. ipconfig /displaydns | 3. displays the DNS resolver cache entries for the system |
| 4. ipconfig /flushdns | 4. Flushes the DNS cache of the system |
| 5. ipconfig /renew | 5. This option re-establishes TCP/IP connections on all network adapters. |

Explanation:

/all : Displays the full TCP/IP configuration for all adapters. Without this parameter, ipconfig displays only the IP address, subnet mask, and default gateway values for each adapter. Adapters can represent physical interfaces, such as installed network adapters, or logical interfaces, such as dial-up connections.

/renew [Adapter]: Renews DHCP configuration for all adapters (if an adapter is not specified) or for a specific adapter if the Adapter parameter is included. This parameter is available only on computers with adapters that are configured to obtain an IP address automatically. To specify an adapter name, type the adapter name that appears when you use ipconfig without parameters.

/release [Adapter]: Sends a DHCPRELEASE message to the DHCP server to release the current DHCP configuration and discard the IP address configuration for either all adapters (if an adapter is not specified) or for a specific adapter if the Adapter parameter is included. This parameter disables TCP/IP for adapters configured to obtain an IP address automatically. To specify an adapter name, type the adapter name that appears when you use ipconfig without parameters.

/flushdns: Flushes and resets the contents of the DNS client resolver cache. During DNS troubleshooting, you can use this procedure to discard negative cache entries from the cache, as well as any other entries that have been added dynamically.

/displaydns : Displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local Hosts file and any recently obtained resource records for name queries resolved by the computer. The DNS Client service uses this information to resolve frequently queried names quickly, before querying its configured DNS servers.

/registerdns : Initiates manual dynamic registration for the DNS names and IP addresses that are configured at a computer. You can use this parameter to troubleshoot a failed DNS name registration or resolve a dynamic update problem between a client and the DNS server without rebooting the client computer. The DNS settings in the advanced properties of the TCP/IP protocol determine which names are registered in DNS.

/showclassid Adapter: Displays the DHCP class ID for a specified adapter. To see the DHCP class ID for all adapters, use the asterisk (*) wildcard character in place of Adapter. This parameter is available only on computers with adapters that are configured to obtain an IP address automatically.

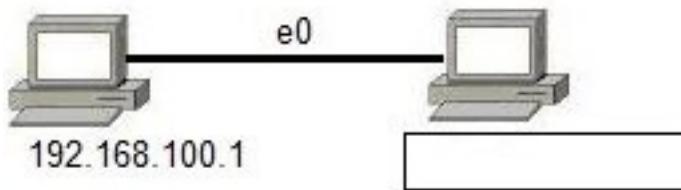
/setclassid Adapter [ClassID] : Configures the DHCP class ID for a specified adapter. To set the DHCP class ID for all adapters, use the asterisk (*) wildcard character in place of Adapter. This parameter is available only on computers with adapters that are configured to obtain an IP address automatically. If a DHCP class ID is not specified, the current class ID is removed.

[Back](#)

2.7 Identify the Private IPv4 address

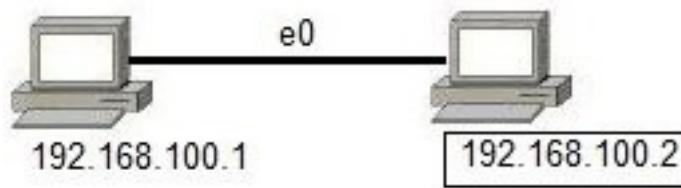
Description: This lab helps to identify the private IPv4 address of a device.

Instructions: Choose (drag and drop) the correct private IPv4 address of a second device from the options given in the below figure.



- Options are:**
- A. 10.10.1.1
 - B. 192.168.1.2
 - C. 192.168.100.2
 - D. 192.168.200.8

Image after choosing the correct option is as shown below:



[Back](#)

2.8 Identifying speed ranges of 802.11 standards

Description: This lab exercise helps you to know the speed ranges of a 802.11 standards.

Instructions:

1. Different 802.11 standards are given in the column A
2. Various speed ranges of 802.11 standards are given in the column B
3. Match (drag and drop) the standards given on the column A with their speed ranges given on the column B.

Column A

1. 802.11a
2. 802.11b
3. 802.11g
4. 802.11n
5. 802.11ac

Column B

1. Up to 54Mbps at 5 GHz
2. Up to 11 Mbps at 2.4 GHz
3. Up to 20+ Mbps at 2.4 GHz
4. Up to 600Mbps at 2.4GHz
5. Up to 6.9 Gbps at 5Ghz

Explanation: 802.11a standard provides wireless LAN bandwidth of up to 54Mbps in the 5GHz frequency spectrum. The 802.11a standard also uses orthogonal frequency division multiplexing (OFDM) for encoding rather than FHSS or DSSS.

802.11b standard provides for bandwidths of up to 11 Mbps (with fallback rates of 5.5, 2, and 1 Mbps) in the 2.4G Hz frequency spectrum. This standard is also called Wi-Fi or 802.11 high rates. The

802.11b standard uses only DSSS for data encoding.

802.11g standard provides for bandwidths of 20 Mbps+ in the 2.4 GHz frequency spectrum. This offers a maximum rate of 54 Mbps and is backward compatible with 802.11b.

A more recent wireless standard you need to know for the exam is 802.11n. The goal of the 802.11n standard is to significantly increase throughput in both the 2.4 GHz and the 5 GHz frequency range. The baseline goal of the standard was to reach speeds of 100 Mbps, but given the right conditions, it is estimated that the 802.11n speeds might be able to reach 600 Mbps. In practical operation, 802.11n speeds will be much slower.

802.11ac : The emerging Wi-Fi signaling standard, 802.11ac utilizes 5GHz channel. 802.11ac offers backward compatibility to 802.11b/g/n and bandwidth rated up to 6.9 Gbps at 5 GHz band. The speed is theoretical maximum and actual speeds will depend on several factors, like number of antennas, channel bandwidth, etc. For 160MHz channel, the speed is 867 Mbit/s, and 802.11ac can have up to 8 antennas at 160MHz channel, delivering 6.9Gbits/sec speed, theoretically.

<https://www.forbes.com/sites/gordonkelly/2014/12/30/802-11ac-vs-802-11n-wifi-whats-the-difference/#213154533957>

https://en.wikipedia.org/wiki/IEEE_802.11ac

[Back](#)

2.9 Identifying the characteristics of Internet WAN technologies

Description: This exercise helps to know about the internet WAN technologies and their characteristics.

Instructions: 1. The Internet WAN technologies are given on the column A

2. Characteristics of Internet WAN technologies are given on the column B
3. Match (drag and drop) the WAN technologies given on the column A with their respective characteristics given on the column B.

Column A

1. Packet Switching
2. Circuit switching
3. ISDN
4. FDDI

Column B

1. It is a technology whereby each packet of a data communication can take a separate route to its destination
2. It is a technology whereby a single communication channel is opened at the start of a session and that single channel is used throughout the communication.
3. It is an international standard for sending voice, data, and video over digital telephone lines or normal telephone wires.
4. Is a set of protocols used for sending digital data over a fiber optic cable. FDDI networks use a token-passing system and a dual ring topology.

Explanation:

Packet switching allows users to share common carrier resources so that the carrier can make more efficient use of its infrastructure. In a packet switching setup, networks have connections into the carrier's network, and many customers share the carrier's network. The carrier can then create virtual circuits between

customers sites by which packets of data are delivered from one to the other through the network.

Circuit Switching allows data connections to be established when needed and then terminated when communication is complete. This works like a normal telephone line works for voice communication.

Integrated Services Digital Network (ISDN) is a good example of circuit switching. When a router has data for a remote site, the switched circuit is initiated with the circuit number of the remote network.

Virtual private network (VPN) is a technology widely used in a public switched network (PSTN) to provide private and secured WAN for an organization. VPN uses encryption and other techniques to make it appear that the organization has a dedicated network, while making use of the shared infrastructure of the WAN.

WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer. Key technologies often found in WANs include SONET, Frame Relay, X.25, ATM and PPP.

ATM: A dedicated-connection switching technology that organizes digital data into 53-byte cell units. Individually, a cell is processed asynchronously relative to other related cells and is queued before being multiplexed over the transmission path. Speeds on ATM networks can reach 10 Gbps.

Frame Relay: (FR). A high-speed packet-switched data communications service, similar to X.25. Frame relay is widely used for LAN-to-LAN interconnect services, and is well suited to the bursty demands of LAN environments.

SONET/SDH: Synchronous Optical Network is an international standard for high speed communication over fiber-optic networks. The SONET establishes Optical Carrier (OC) levels from 51.8 Mbps to 10 Gbps (OC-192) or even higher. Synchronous Digital Hierarchy (SDH) is a European equivalent of SONET.

X.25: The X.25 protocol allows computers on different public networks to communicate through an intermediary computer at the network layer level.

PPP: A point-to-point link provides a single, pre-established WAN communications path from the customer premises through a carrier network, such as a telephone company, to a remote network. Point-to-point lines are usually leased from a carrier and thus are often called leased lines. For a point-to-point line, the carrier allocates pairs of wire and facility hardware to your line only.

[Back](#)

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

Description: This exercise helps to know about the network characteristics QoS.

Instructions: 1.The various network characteristics managed by QoS are given on the column A
2.The descriptions of the network characteristics are given on the column B
3. Match (drag and drop) the network characteristic given on the column A with their respective description given on the column B.

Column A

1. Bandwidth
2. Latency
3. Jitter
4. Reliability

Column B

1. The rate at which traffic is carried by the network.
2. The delay in data transmission from source to destination.
3. The variation in latency.
4. The percentage of packets discarded by a router.

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

Description: This exercise helps to know about different twisted pair cable types with their speeds

Instructions: 1.Different twisted pair cable types are given on the column A

2. Speeds of the cable types are given on the column B
3. Match (drag and drop) the twisted pair cable types on the column A with their speeds given on the column B

Column A	Column B
CAT3	Up to 16 Mbps
CAT5	Up to 100 Mbps
CAT5e	Up to 1 Gbps
CAT6	Up to 10 Gbps

Explanation: CAT6 is rated for gigabit Ethernet while CAT6e is thicker and rated for 10 gig Ethernet. Typically CAT5e is sufficient and can also handle gig Ethernet, but noise margin will be less.

	CAT3	CAT5	CAT5e	CAT6	CAT6e	CAT7
Speed	16 Mbps	100 Mbps	1000 Mbps	10/100/1000 Mbps and 10 Gbps	10/100/1000 Mbps and 10 Gbps	10/100/1000 Mbps and 10 Gbps
Limitation	Ineffective for Higher – speed networks often found in older 10 BaseT networks	Range of 100 meters	Range of 100 meters	Range of 100 meters	Range of 100 meters	Range over 100 meters

2.12 Compare shielded vs unshielded twisted-pair cable

Description: This lab exercise helps to know about STP and UTP cable characteristics

Instructions: 1. Match (drag and drop) the STP and UTP cables given on the column A with their characteristics given on the column B

Column A	Column B
STP	Heavier and more difficult to manufacture

More immune to interference and noise
Higher transmission rates over longer distances.
Used in more high-end applications.

UTP	Easy to handle and install. Cables are more prevalent in SOHO networks Cheapest form of cable available for networking purposes.
-----	--

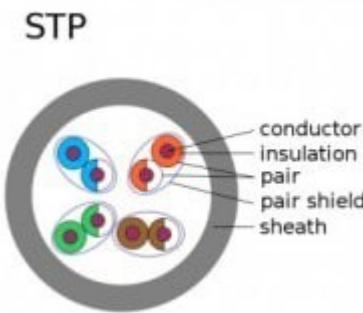
Explanation:

STP stands for Shielded Twisted Pair and UTP stands for Unshielded Twisted Pair.

Comparison between STP and UDP

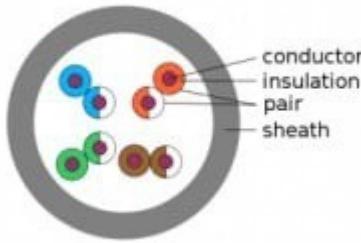
- 1) Physical: The only difference between the STP and UTP cable is the additional shielding material used in STP cables. The shielding covers the full length of the cable and protects it from any external interference.
- 2) Cost: Due to the additional material used in a STP cable, it costs more than the UTP cable.
- 3) Considerations: While using STP cable will yield maximum bandwidth despite external conditions, the shielding makes the cable heavier and more difficult to bend.
- 4) Use: UTP cable typically is used in homes and offices. Some large businesses also use the cable because it is cheaper. Large companies that require maximum bandwidth typically use STP cable. STP cable is used outside to better deal with the elements and equipment that may degrade bandwidth quality.

Shielded Twisted Pair (STP) cables reduce electrical noise and electromagnetic radiation. In other words, they help to keep the signal steady, and reduce interference with other devices. Given below is a diagram showing a typical shielded twisted pair cable



Unshielded Twisted Pair (UTP) cables do not have shielding to reduce interference. They are designed to cancel electromagnetic interference with the way the pairs are twisted inside the cable. Unshielded twisted cables are most widely used for office LANs, though recently wireless LANs are more widely used. Unshielded cables are lightweight, thin and flexible. They are also versatile and inexpensive. A typical UTP cable cross section is shown in the figure below:

UTP



[Back](#)

2.13 Identifying the IPV6 link local address .

Description: This lab exercise helps to identify the IPV6 link local address

Instructions:

1. A figure displays some of the IPV6 addresses
2. Click on the command which displays the corresponding output, if the clicked command is correct it indicates the green mark, otherwise it indicates the red mark.

- a. FE80::64 b. ::1 c. 127:0:0:1 d. ff02::2

Explanation: Link-local addresses (FE80::/64) : Auto-configured IPv6 address is known as Link-Local address. This address always starts with FE80. The first 16 bits of link-local address is always set to 1111 1110 1000 0000 (FE80). The next 48-bits are set to 0,

Link-local addresses are used for communication among IPv6 hosts on a link (broadcast segment) only. These addresses are not routable, so a Router never forwards these addresses outside the link.

Unicast loopback address : The IPv6 unicast loopback address is equivalent to the IPv4 loopback address, 127.0.0.1. The IPv6 loopback address is 0:0:0:0:0:1, or ::1.

Below fig. shows after identifying the correct command on the image.

- a. FE80::64 b. ::1 c. 127:0:0:1 d. ff02::2

[Back](#)

2.14 Objective Test 2 Answer the following questions

1. Which type of network cable uses an F-type connector?

- A. STP
- B. T567A
- C. Fiber
- D. Coaxial

Answer : A

2. What is the name of the technology that only lets specific wireless devices connect to a wireless access point?

- A. Channel selection
- B. MAC filtering
- C. Dynamic addressing
- D. Port forwarding

Answer : B. MAC filtering

3. Which device does not segment a network?

- A. Gateway
- B. Router
- C. Switch
- D. Hub

Answer : D. Hub

4. Which two types of connector is commonly used to make a physical connection from a computer to a cable modem? (Select two answers)

- A. RS232
- B. USB
- C. RJ-45
- D. BNC

Answer : B,C

5. ST connectors are used with which type of cable?

- A. UTP
- B. STP
- C. Fiber optic
- D. ATA data cables

Answer : C

6. Which two are common network configurations?

- A. Peer-to-peer and work group.
- B. Work group and stand alone.
- C. Work group and Domain
- D. Domain and Client /Server.

Answer : C. Work group and Domain

7. Which of the following is the connector used for 100Base-T Ethernet cables?

- A. RJ-11
- B. BNC
- C. RJ-58

D. RG-45

Answer : RG-45

RJ-45 is the eight-pin connector used for data transmission over twisted-pair wiring. RJ-45 is the connector used on 100Base-T Ethernet cables. Incorrect answers:A: The connector on the end of the cord that runs from the phone to the wall is an RJ-11 connector.B: BNC connectors are used for Thinner (10Base-2) Ethernet connections. C: RG-58 is coaxial cable. It is not a connector.

7.You are working with graphic translations. Which layer of the OSI model is responsible for code formatting and conversion and graphic standards.

- A. Network layer
- B. Session layer
- C. Transport layer
- D. Presentation layer

Answer: D

8. In which layer data is grouped into frames?

- A. physical
- B. data link
- C. network
- D. transport

Answer: B. Data link

9. In OSI network architecture, the dialogue control and token management are responsibility of

- A. Session layer
- B. Network layer
- C. Transport layer
- D. Data link layer

Answer: A

10. Which answer correctly lists the OSI PDUs in order?

- A. Data,Packet,Frame,Segment,Bit
- B. Bit,Data,Packet,Segment,Frame
- C. Data,Segment,Packet,Frame,Bit
- D. Bit,Frame,Segment,Packet,Data

Answer: C

Data is encapsulated, so that must come first. Segment next(Transport layer), then Packet (Internet layer), then frame(Network Access layer), then transmit bits.

11. Which type of device automatically issues IPv4 addresses?

- A.WINS server
- B.DHCP server
- C.DNS server
- D. NetBIOS server

Answer: B.DHCP server

12. Which type of address must be manually configured?

- A.APIPA
- B. Static
- C. Dynamic
- D.DHCP

Answer: B. Static

13. Which protocol is designed to support network file sharing?

- A.SNMP
- B.SMB
- C.SSH
- D.SFTP

Answer: B. SMB

14. Which protocol or standard is designed to allow a user to connect a wireless device to a secure wireless device without the need to enter a pass phrase or key? The device typically uses a push button.

- A. Mac filter
- B. Dynamic addressing
- C.WPS
- D.FTP

Answer: C. WPS

15. A computer is not connecting to the Internet but is connecting to local network shares. You inspect a computer assigned IP address and see that it is 169.254.10.1. What is the most likely problem?

- A. The network card is defective.
- B. The WINS server is down.
- C. The DHCP server has failed.
- D. The network cable has become disconnected from the PC.

Answer: C. The DHCP server has failed.

16. What is the loop back address associated with IPv4?

- A.192.168.0.1
- B.127.0.0.1
- C.10.0.0.1
- D.255.255.255.255

Answer: B.127.0.0.1

17. Which protocol is used to map all local network addresses to one single Internet address?

- A.DMA
 - B.TCP
 - C.NAT
 - D.UDP
- Answer : C. NAT**

18. Which command will reveal the assigned IP address of a computer network adapter?

- A. Ipconfig
- B. Nslookup
- C. Ipv4/config
- D. Config/IP

Answer: A. IPCONFIG

19. Which protocol is used to establish a connection with an ISP when using a dialup modem?

- A. HTML
- B. DNS

- C. TCP/IP
- D. PPP

Answer : D.PPP

20. Ports 0-1023 are known as?

- A. Registered Ports
- B. Dynamic Ports
- C. Well-known Ports
- D. Established Ports

Answer : C

21. The transmission of bits is considered to be on which layer in the OSI model?

- A. Data-Link
- B. Application
- C. Layer 1
- D. Layer 2

Answer: C. Layer, also called

22. Which processes does TCP, but not UDP, use?

- A. Windowing
- B. Acknowledgments
- C. Source Port
- D. Destination Port

Answer: B

23.Which of the following services use TCP?

- 1. DHCP
- 2. SMTP
- 3. HTTP
- 4. TFTP
- 5. FTP

- A. 1 and 2
- B. 2,3 and 5
- C. 1,2 and 4
- D.1,3, and 4

Answer: B. 2,3, and 5

24.What is the approximate indoor range for 802.11g wireless adapters?

- A.24 feet
- B.120 feet
- C.10 meters
- D.100 meters

Answer: B

25. Which application would most likely require QoS to function properly?

- A. Telephone modem
- B. VoIP
- C. Email
- D. Instant Messaging

Answer: B. VoIP

26. Which type of security is designed for 802.11 devices?

- A.PPP
- B.SLIP
- C.WEP
- D.PGP

Answer: C.WEP

27. Which are the two major types of ISDN service available?

- A. Static and dynamic
- B. Fixed cost and variable
- C. BRI and PRI
- D.DSL and Cable

Answer: C. BRI and PRI

28. You can ping a computer using its IP address and receive a ping reply. You ping the same computer using its assigned name and receive a timed out message. What is most likely the cause?

- A. The network card is configured with a static IP address.
- B. The network card is configured using a dynamic IP address.
- C. The DNS service is not working correctly.
- D. The DHCP service is not working correctly

Answer: C. The DNS service is not working correctly.

29. What is the another name for a wireless access point security key?

- A. AES certificate
- B. Passphrase
- C. Audit String
- D. Encrypt-phrase

Answer: B. Passphrase

30. How can you ensure only certain computers are able to access a WAP?

- A. Switch Encryption
- B. Disable SSID
- C.ACL
- D. MAC Filtering

Answer: D

MAC Filters only allow computers on the list of allowed MAC Addresses to access the Wireless Access Point.

31. Which of the following is a best practice when implementing a basic wireless network?

- A. Disabling ESSID broadcast
- B. Configuring encryption with a WEP key and labeling the key on the WAP
- C. Adding two access points per area of service
- D. Not configuring the ESSID point

Answer: A. Disabling ESSID broadcast

32. Which of the following specifications of 802.11 can operate simultaneously at 2.4GHz and 5GHz?

- A. 802.11a
- B. 802.11b

- C. 802.11g
- D. 802.11n

Answer: D. 802.11n

33. Which of the following WAN technologies requires fiber optics?

- A. POTS
- B. SONET
- C. ADSL
- D. PSTN

Answer: B. SONET

[**Back**](#)

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

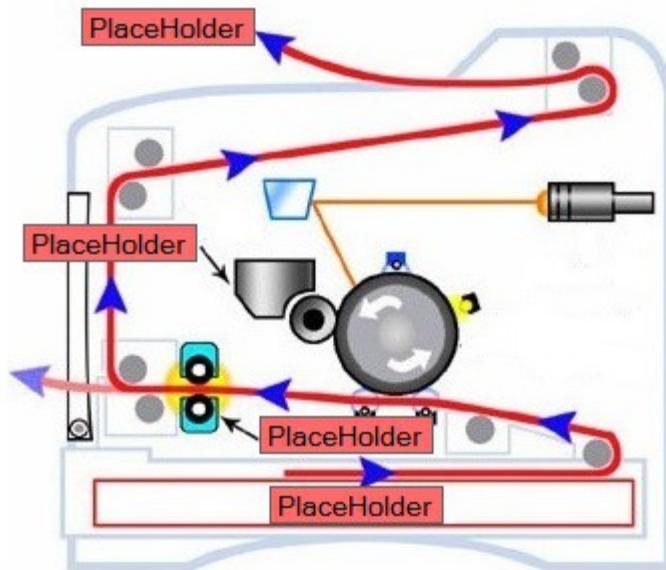
4.1 Identify the basic components of the LASER printer

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.

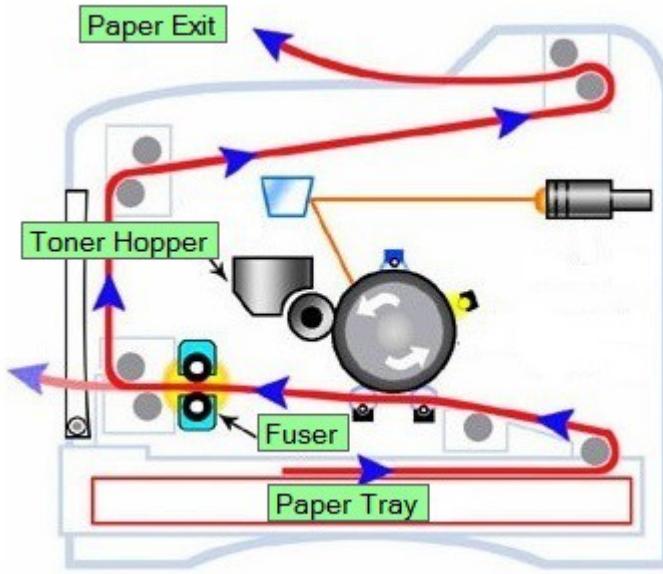


Explanation:

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 options on the image



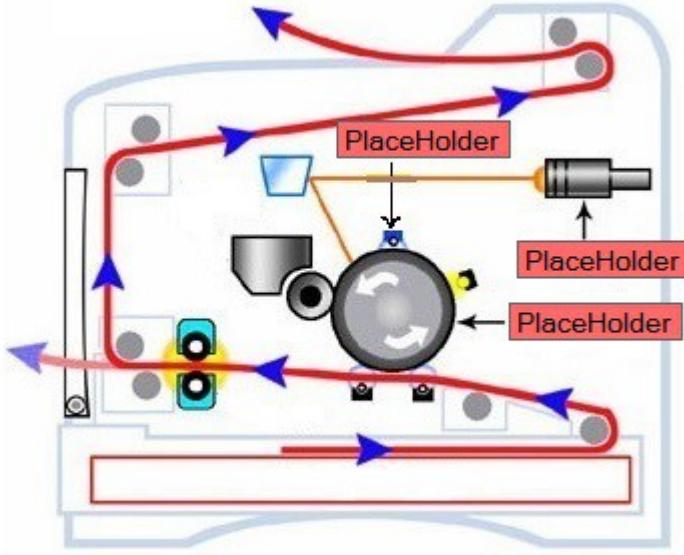
[Back](#)

4.1.2 Identify the laser printer components -2

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

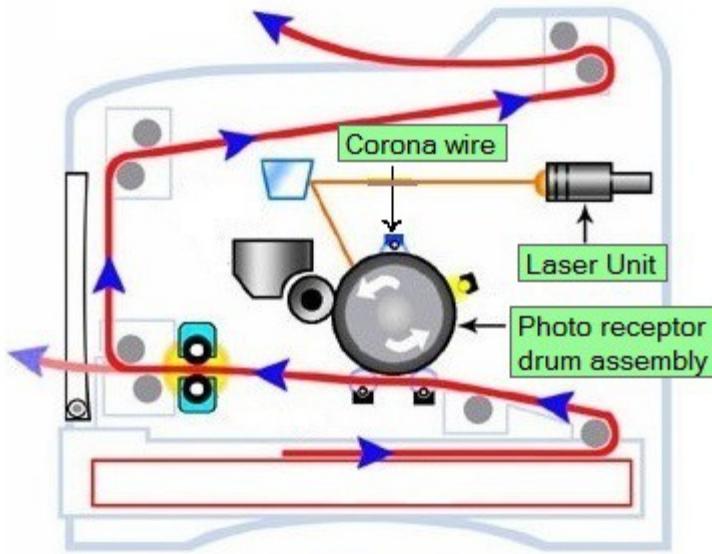
Instructions:

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



Explanation:

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

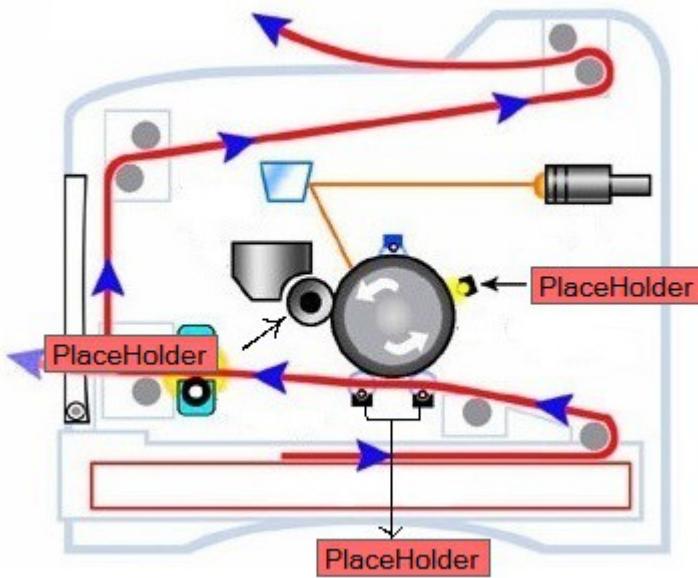


[Back](#)

4.1.3 Identify the laser printer components -3

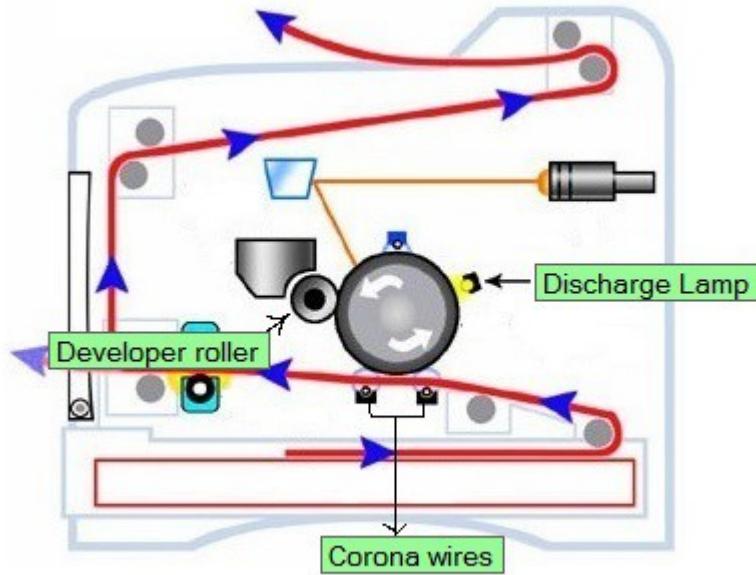
Description: This lab exercise helps you to get familiar with laser printer components

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



Explanation:

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



[**Back**](#)

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

Description: This lab exercise helps you to know about the printer types and their descriptions.

- Instructions:**
1. Names of the printer types are given on the column A.
 2. Match (drag and drop) the printer type given on the column A with their respective characteristics given on the column B.

Column A	Column B
1. Laser	1. Printer produces a backward image of the page to be printed on a cylinder using a laser.
2. Ink jet	2. Printers spray ink onto the paper to reproduce text and images
3. Thermal	3. The print mechanism feeds the paper next to a print head containing a sophisticated electronic heater, producing text and simple graphics on the tape.
4. Impact	4. Printers produce a printed page by striking an inked ribbon with a dot-matrix mechanism.

[**Back**](#)

4.3 Identifying features of Laser printer components

Description: This lab exercise helps you to know about the various components of the laser

Instructions: 1. Laser printer components are given on the column A.

2. Match (drag and drop) the laser printer component given on the column A with their respective features given on the column B.

Column A

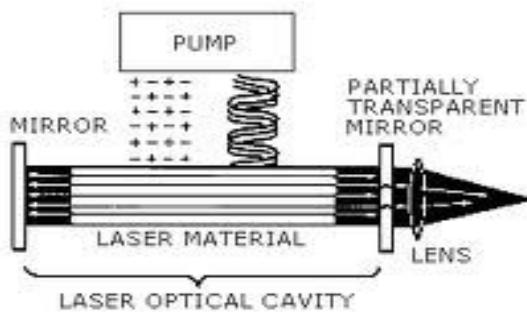
1. Lasing Material or active medium
2. External energy source
3. Optical resonator

Column B

- The active medium is excited by the external energy source(pump source) to produce population inversion.
- The excitation source, pump source provides energy which is needed for the population inversion and stimulated emission to the system.
- Provides the guidance about the simulated emission process. It is induced by high speed photons. Finally, a laser beam will be generated.

Explanation:

The below figure shows the various components of the laser.



[**Back**](#)

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

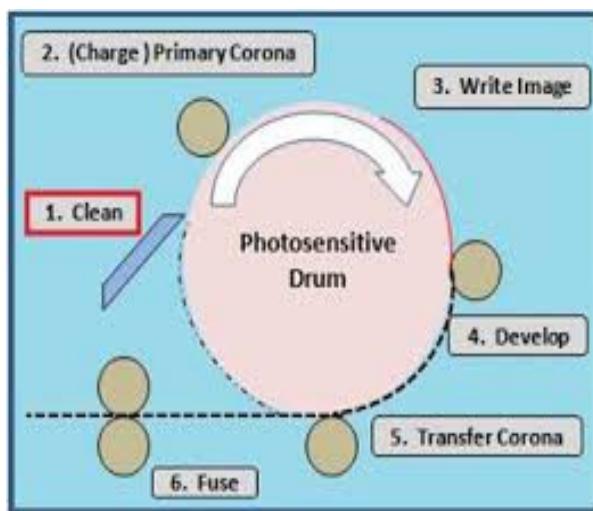
Description: This lab exercise helps you to know about the laser printing process with their descriptions

Instructions: 1. Laser printing process are given on the column A.
2. Match (drag and drop) the printing process given on the column A with their respective features given on the column B.

Column A	Column B
1. Cleaning	Excess Toner is scraped from the Photoelectric Drum.
2. Conditioning	A Uniform -600 Volt Charge is Placed on the Photoelectric Drum By The Primary Corona
3. Writing	Write An Invisible Electric Image on the photoelectric drum by causing the Drum surface, to be less negative wherever the laser beam hits
4. Developing	The toner is applied to the latent image on the drum.
5. Transferring	The toner attached to the latent image is transferred to the paper
6. Fusing	The toner is permanently fused to the paper.

Explanation:

The below figure shows the laser printing process:



- A drum assembly inside the printer receives a positive electrical charge from a wire with a current running through it.
- A laser then traces onto the drum the image to be printed, creating a negatively charged electrostatic image.
- Next, the drum gets coated in positively charged toner, which clings to the negatively charged image but nothing else.
- The paper is given its own negative charge that's stronger than the electrostatic image on the drum so it can pull the toner away from it.
- The drum rolls over the paper, transferring the image to the paper.

- The paper's electrical charge is discharged.
- The toner is fused to the paper.

[Back](#)

4.5 Objective Test 4 Answer the following questions

1.Which of the following would you find in the laser printer? (Select TWO)

- A. Laser scanner
- B. Ink ribbon
- C. Toner cartridge
- D. Daisy wheel

Answer: A,C

The laser printer consists of toner cartridge, fusing assembly, laser scanner; high-voltage power supply, DC power supply, paper transport assembly (including paper pickup rollers and paper registration rollers), corona, and printer controller circuitry. Incorrect Answers:B: The impact printer uses a mechanical device the drive forward until it hits unto the surface other ink ribbon. D: The Impact printer uses the daisy wheel

2.Which of the following is TRUE about the impact printer?

- A. It consists of a print-head
- B. It consists of toner powder
- C. It consists of an ink ribbon
- D. It consists of an ink cartridge

Answer:It consists of an ink ribbon

The impact printer uses a mechanical device the drive forward until it hits unto the surface of the ink ribbon. Incorrect Answers:A: The bubble-jet uses the ink cartridge, which consists of the print-head and ink supply. B: The laser uses the toner powder, which is made of plastic, metal, and organic material. D: The bubble-jet uses the ink cartridge, which consists of the print-head and ink supply.

3.Which of the following substance in the toner cartridge makes the toner “flows” better?

- A. Ink supply
- B. Polyester resins
- C. Iron oxide particles
- D. Carbon substance

Answer:B

The polyester resin makes the “flow” of the toner better. Incorrect Answers:A: The bubble-jet uses the ink cartridge, which consists of the print-head and ink supply. C: An iron oxide particle makes the toner sensitive to electrical charges. D: This gives the color to the toner.

4.In a laser printer, which of the following components carries the toner, before it is used by the EPprocess?

- A. The drum

- B. Developer
- C. Toner cartridge
- D. None of the above

Answer:B

The toner contains a medium called the developer (carrier), which “carries” the toner until it issued by the EP process. Incorrect Answers:A: This drum is coated with a photosensitive material that can hold a static charge C: The EP toner cartridge holds the toner. D: The toner contains a medium called the developer (carrier), which “carries” the toner until it issued by the EP process.

5.What is used to drain the charge in the paper when printing with a laser printer?

- A. Static-charge eliminator strip.
- B. The rubber cleaning blade.
- C. The iron particles in the toner.
- D. None of the above

Answer: Static-charge eliminator strip

In the corona assembly is a static-charge eliminator strip that drains away the charge imparted to the paper by the corona. If you do not drain away the charge, the paper would stick to the EP cartridge and jam the printer. Incorrect Answers:B: A rubber cleaning blade scrapes off any residual toner C: The iron oxide particles are used to make the toner sensitive to electrical charges. D: This is incorrect since one makes use of a static-charge eliminator strip to drain static charges in the paper.

6.Which is the latest type of printer interface?

- A. Serial
- B. SCSI
- C.USB
- D. Parallel

Answer: C

The USB interface is the latest of the serial interface and parallel interfaces. Incorrect Answers A: The serial interface is slower than the parallel interface, so the serial is not preferably used. B: The SCSI bus interface is a type of device management system. It was designed to attach peripheral devices to a PC's motherboard. D: The parallel interface is the standard interface.

7. Multi-part forms can be printed on _____.

- A.A laser jet printer
- B. An ink jet printer
- C.A dot matrix printer
- D.A bubble jet printer

Answer: C

8.If a printer is not printing full color correctly, which of the following steps can be taken to attempt to solve the problem?

- A. Calibrate the printer.
- B. Reinstall the drivers.
- C. Swap the color cartridges.
- D. Replace the toner cartridge.

Answer: A

9.The usual cause of the paper jams in Bubble-jet printers is caused through a worn pick up roller. What is the other common cause of paper jams in Bubble-jet printers?

- A. Too much ink on the page.
- B. The wrong type of paper
- C. When more than one page enter the system.
- D. None of the above.

Answer: B

Paper jams in bubble-jet printers are usually due to one of two things: a worn pickup roller, or the wrong type of paper. Incorrect Answers: A: If an ink cartridge becomes damaged, or develops a hole, it can put too much ink on the page and the letters will smear. C: This happens in laser printer when the pick up roller picks up more than one page. D: Paper jams in bubble-jet printers are usually due to one of two things: a worn pickup roller, other wrong type of paper.

10.What problem can be cause by the fusing assembly?

- A. It can cause a worn pickup assembly.
- B. The paper comes out with a smudged image, and toner rubs off.
- C. It causes a "misfeed" or "paper feed" error.
- D. None of the above

Answer: B

When the paper comes out with a smudged image, and toner rubs off, the problem is in the fusing assembly. Incorrect Answers: A: A worn pickup assembly can cause a paper jams. C: Paper jams in laser printers is when more than one piece of paper moves between the registration rollers and tries to go through the printer. This is also called a "misfeed" or "paper feed" error. D: When the paper comes out with a smudged image, and toner rubs off, the problem is in the fusing assembly.

11. A laser printer is centrally located in an office and used by many different people. The printer was working fine before lunch. When a client returns to resume more printing of documents they notice that the printer performance is sluggish. It is taking much longer to print a document than it did this morning. What most likely has caused the poor printer performance?

- A. The power cable to the printer is loose.
- B. The electrical power voltage level has dropped to an unacceptable level.
- C. The configuration of the printer has been modified by another user to print in high quality mode rather than draft.
- D. The paper train has excessive paper lint and needs to be cleaned and lubricated

Answer : C

[Back](#)

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 features 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.

[**Back**](#)

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 columns 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

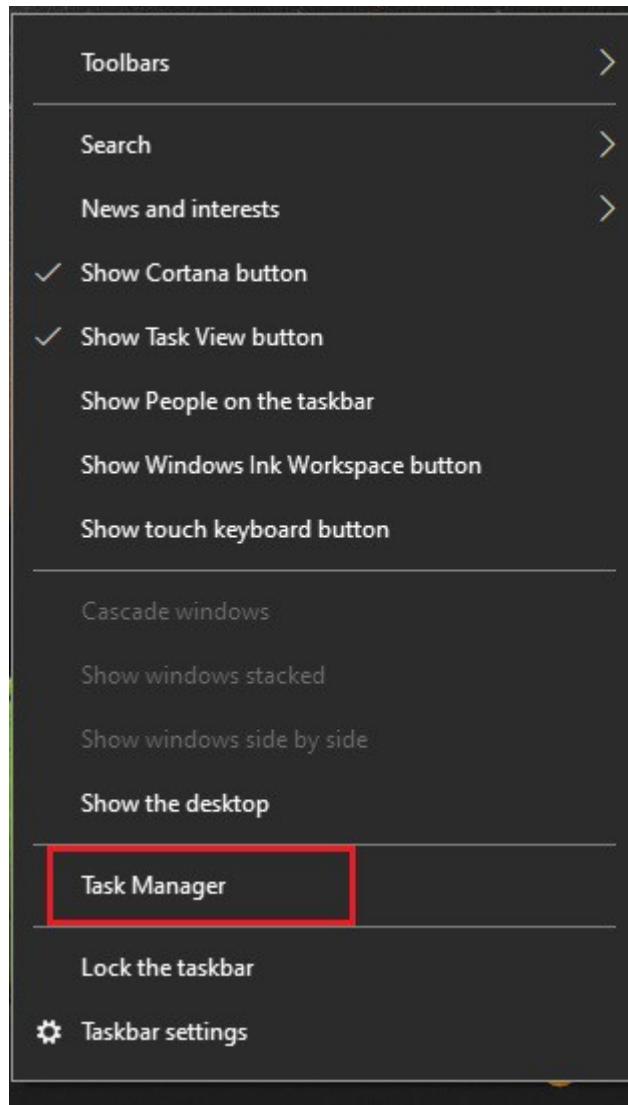
Column B

- 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.

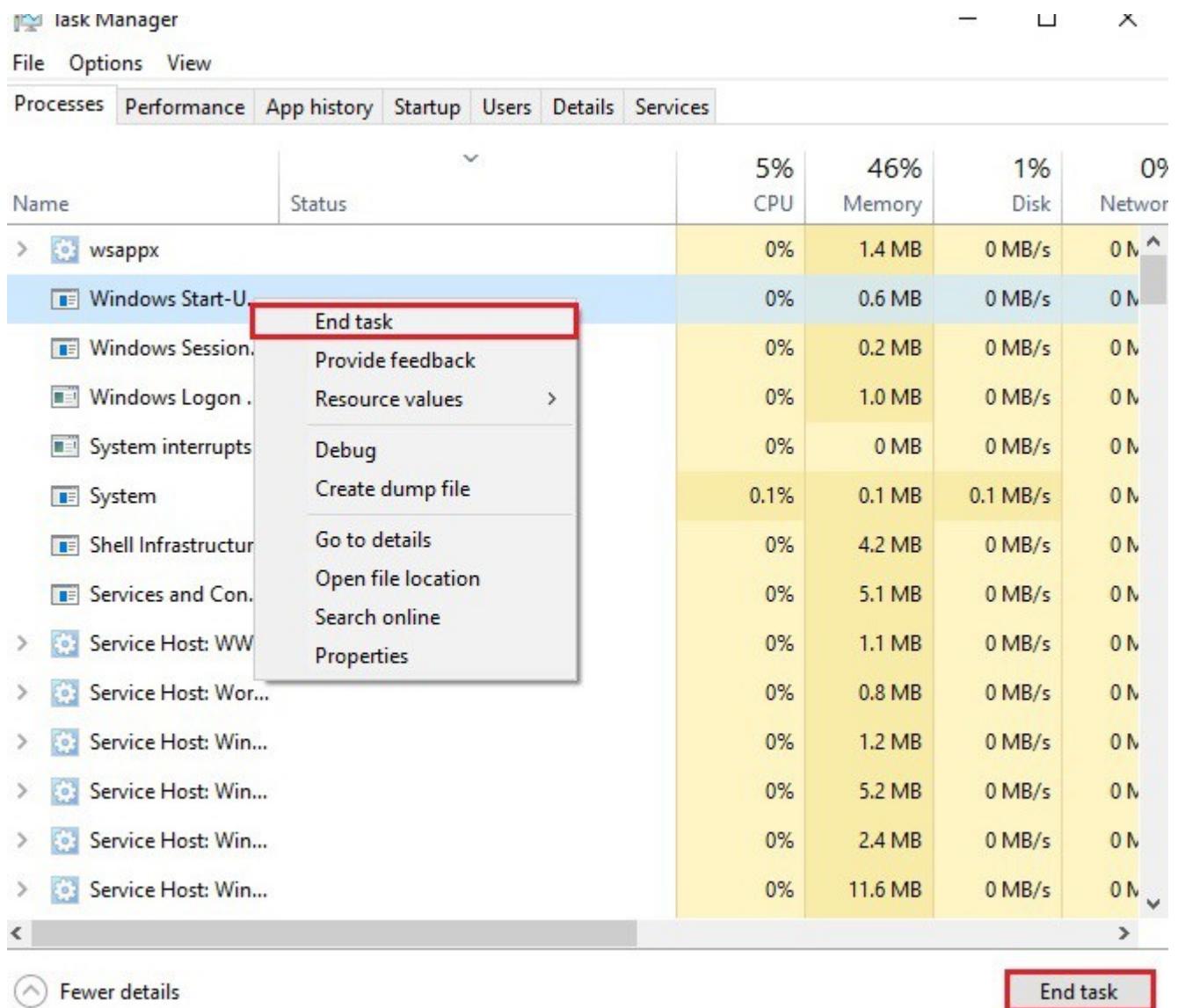
Stopping processes with high-resource usage

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

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

Column B

1. lusrmgr.msc in start → search box
2. Administrative Tools-Computer Management

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

Description: This exercise helps to know about the various options of “User and Groups” and their respective functions/features.

Instructions: 1.“User and Group” options 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. Administrator
2. Power User
3. Guest
4. Users

Column B

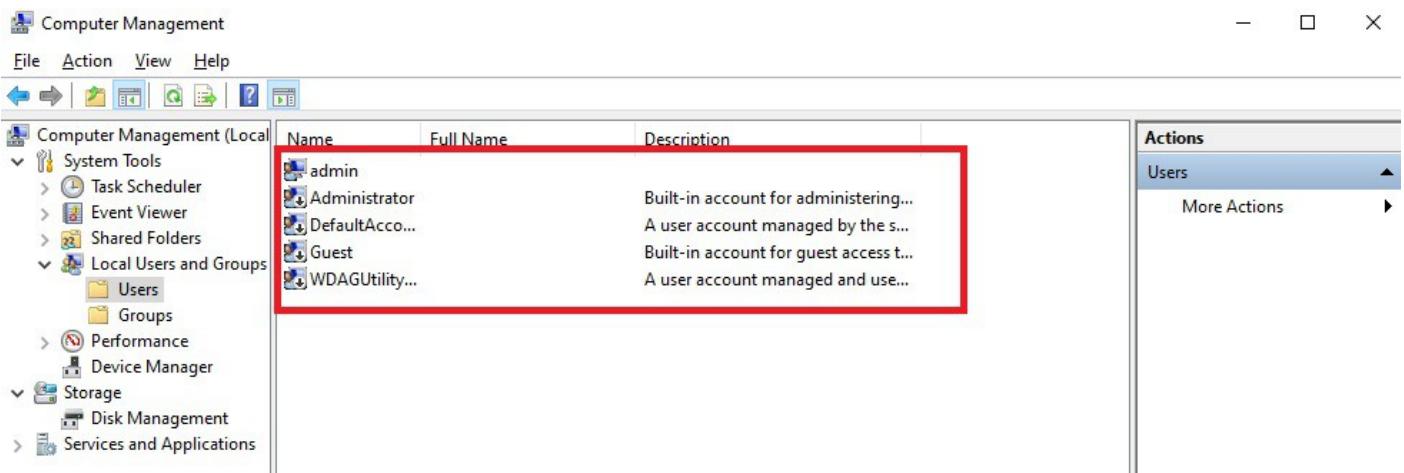
1. This type of user account has complete control over the PC and the user can install anything and make changes that affect all users of that PC.
2. This type of user has considerable experience with computers and utilizes the most advanced features of applications.
3. This type of account is only for users that need temporary access to the PC and the user can only use the software that's already installed on the PC and cannot make any changes to system settings.
4. This type of user account can only use the software that's already installed on the PC and change system settings that don't affect other users.

Explanation:

In Windows 10, the Local Users and Groups snap-in, also known as lusrmgr.msc, offers the best way to see all the users and groups configured on the system. To open this click Control Panel - System and Security - Administrative Tools - Computer Management , in Computer Management, select “Local Users and Groups” on the left panel.

The user accounts found on every Windows 10 computer

- All the user accounts you have created on your Windows 10 PC
- Administrator - a built-in account created by Windows 10 even if you use it or not, made by the operating system for administration purposes
- DefaultAccount - a user account that's managed by Windows 10
- Guest - another built-in account that can be used for guest access on the computer or domain
- WDAGUtilityAccount - managed and used by the Windows Defender antivirus in Windows 10 for running certain processes (like the Microsoft Edge browser) in sandboxed/virtualized environments.



On most Windows 10 PCs, you should have at least the following groups:

Access Control Assistance Operators - members of this group can run remote queries for authorization attributes and permissions on your Windows 10 computer. This group is used on computers that are part of domains, so it's mainly useful for network administrators in large companies.

Administrators – it includes all the user accounts with administrative permissions on your computer. The Administrators group can't be deleted or renamed.

Backup Operators – user accounts with permissions to perform backup and restore operations, using tools like Backup and Restore.

Cryptographic Operators – user accounts with permissions to encrypt or decrypt data, using tools such as BitLocker.

Device Owners - Windows 10 says that the members of this group can change system-wide settings. However, this group is not currently used in Windows 10.

Distributed COM Objects – this user group is harder to explain. It is used mostly for user accounts that need to participate in more complex scenarios, such as distributed computing across computers on a network. Therefore it is used in business environments.

Event Log Readers – this group gives permissions to its members to read Windows 10 event logs that show what is happening on the system.

Guests – are regular user accounts that cannot perform any administrative tasks on your computer. They can be used only for light computing activities such as browsing the internet or running the installed applications. They are not able to perform any modifications to the system's configuration, to access or modify another user's data, etc.

Hyper-V Administrators - gives its members unrestricted access to all the features available in Hyper-V.
IIS_IUSRS – this group is used only by the Internet Information Services you may choose to install using the Windows Features panel.

Network Configuration Operators – this group gives its users permission to configure networking features in Windows 10.

Performance Log Users & Performance Monitor Users – members are given permissions to perform advanced logging in Windows 10 and collect performance data.

Power Users – this user group was used in older versions of Windows to provide limited administrative permissions to specific user accounts. It is still present in Windows 10 but only to provide backward compatibility for old legacy applications.

Remote Desktop Users – this user group provides its members with permissions to logon remotely to the computer via the Remote Desktop.

Replicator – this user group is used in network domains, and it gives its members the permissions required to do file replication across the domains.

System Managed Accounts Group - the Windows 10 operating system manages the members of this group.

Users – It includes the standard user accounts defined on your Windows 10 computer or device. Its members do not have administrative permissions. They can only run installed applications and cannot make system changes that affect other users.

Name	Description	Actions
Access Control Assist...	Members of this group can remot...	Groups
Administrators	Administrators have complete an...	More Actions
Backup Operators	Backup Operators can override se...	
Cryptographic Operat...	Members are authorized to perfor...	
Distributed COM Users	Members are allowed to launch, a...	
Event Log Readers	Members of this group can read e...	
Guests	Guests have the same access as m...	
Hyper-V Administrators	Members of this group have com...	
IIS_IUSRS	Built-in group used by Internet Inf...	
Network Configuration...	Members in this group can have s...	
Performance Log Users	Members of this group may sche...	
Performance Monitor ...	Members of this group can acces...	
Power Users	Power Users are included for back...	
Remote Desktop Users	Members in this group are grante...	
Remote Management...	Members of this group can acces...	
Replicator	Supports file replication in a dom...	
System Managed Acc...	Members of this group are mana...	
Users	Users are prevented from making ...	
SQLServer2005SQLBro...	Members in the group have the re...	

[Back](#)

5.6 Identifying features of NTFS permissions and Share permissions

Description: This exercise helps to know about the functions of NTFS vs Share permissions.

Instructions: 1.NTFS permissions and Share permissions are given on the column A
 2.Their functions/characteristics are given on the column B
 3.Match (drag and drop) the item given on the Column A with their respective functions/features given on the column B.

Column A

- 1. NTFS Permission
- 2. Share Permission

Column B

- 1. Applies to the users who locally use the machine
- 2. Can control whether the user or a group is able to execute programs
- 3. This applies to a user accessing the folder directly on the hard drive while logged on to the machine.
- 1. Applies to user who remotely access the machine from a remote terminal
- 2. Can't control whether the user or a group is able to execute programs
- 3. This applies to a user accessing the share via a UNC, Network Neighborhood browsing , or mapped drive.

Explanation

With NTFS, files, directories, and volumes can each have their own security. NTFS's security is flexible and built in. Not only does NTFS track security in ACLs, which can hold permissions for local users and groups, but each entry in the ACL can specify what type of access is given—such as Read, Write, Modify, or Full Control. This allows a great deal of flexibility in setting up a network. In addition, special file-encryption programs were developed to encrypt data while it was stored on the hard disk.

Share permissions apply only when a user is accessing a file or folder through the network. Local

permissions and attributes are used to protect the file when the user is local. With FAT and FAT32, you do not have the ability to assign “extended” or “extensible” permissions, and the user sitting at the console effectively is the owner of all resources on the system. As such, they can add, change, and delete any data or file that they want.

<http://blogs.msmvps.com/acefekay/2011/02/04/share-permissions-and-ntfs-permissions-folder-access-control-amp-folder-permissions/>

[Back](#)

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

Description: This exercise helps to know about the system action resulting from different combinations of duplex and speed modes.

Instructions: 1. Different combinations of duplex and speed modes are given.
2. Drag and drop the respective System actions resulting from the combinations of duplex and speed modes.

Duplex Commands	Speed Commands	Resulting System Action
duplex auto	speed auto	
duplex auto	speed 100 or speed 10	
duplex half or duplex full	speed auto	
duplex half	speed 10	
duplex full	speed 10	
duplex half	speed 100	
duplex full	speed 100	

Explanation

Duplex Commands	Speed Commands	Resulting System Action
duplex auto	speed auto	Auto negotiates both speed and duplex modes.
duplex auto	speed 100 or speed 10	Auto negotiates both speed and duplex modes.
duplex half or duplex full	speed auto	Auto negotiates both speed and duplex modes.
duplex half	speed 10	Forces 10 Mbps and half duplex.
duplex full	speed 10	Forces 10 Mbps and full duplex.
duplex half	speed 100	Forces 100 Mbps and half duplex.
duplex full	speed 100	Forces 100 Mbps and full duplex.

<http://www.lab.dit.upm.es/~labrst/config/ciscopedia/duplex.htm>

[Back](#)

5.8 Identifying Console command tools and their respective features

Description: This exercise helps to know about the functions of recovery console commands.

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 recovery console command given on the Column A with their respective functions/characteristics given on the column B.

Column A	Column B
1. TASKKILL	1. Ends one or more tasks or processes by process ID (PID) or image name
2. BOOTREC	2. Troubleshoot and potentially fix errors that are preventing your computer to start.
3. SHUTDOWN	3. Allows you to shut down or restart a local or remote computer.
4. TASKLIST	4. Displays list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer.
5. MD	5. Creates a directory
6. RD	6. Deletes an empty directory
7. CD	7. Used to change the current working directory
8. DEL	8. Used to delete one or more files or directories from a file system

Explanation

TASKKILL: This is used to kill tasks or processes under windows from command line. Syntax is as follows:

`TASKKILL [/S system [/U username [/P [password]]]] { [/FI filter] [/PID processid | /IM imagename] } [/T] [/F]`

BOOTREC: Bootrec.exe can help you troubleshoot and repair things like the master boot record (MBR), the boot sector or the Boot Configuration Data (BCD) store. The Bootrec.exe tool supports the following options. /FixMbr, /FixBoot, /ScanOs, /RebuildBcd.

TASKLIST: Displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer. Syntax for Tasklist is as follows:

`TASKLIST [/S system [/U username [/P [password]]]] [/M [module] | /SVC | /V] [/FI filter][/FO format] [/NH]`

SHUTDOWN: Allows you to shut down or restart a local or remote computer. Used without parameters, shutdown will logoff the current user.

MD: MD(Make Directory) Creates a new folder. Syntax for MD is as follows:

`MD [drive:]path`

Where, the path can consist of any valid characters up to the maximum path length available

CD: CD(Change Directory) - Select a Folder (and drive). Syntax for CD is as follows:

`CD [/D] [drive:]path`

CD [..]

Where, /D : change the current DRIVE in addition to changing folder.

RD: This command is used to Delete folder(s). Syntax for RD is as follows:

RD pathname

RD /S pathname

RD /S /Q pathname

Where,

/S : Delete all files and sub-folders in addition to the folder itself. Use this to remove an entire folder tree.

/Q : Quiet - do not display YN confirmation

DEL: DEL (or ERASE) command is used to delete one or more files or directories. Syntax for DEL (or ERASE) is as follows :

DEL [options] [/A:file_attributes] files_to_delete

Where, files_to_delete : This can be a filename, a list of files or a Wildcard.

Options : /P Give a Yes/No Prompt before deleting.

/F Ignore read-only setting and delete anyway (FORCE)

/S Delete from all Sub-folders (DELTREE)

/Q Quiet mode, do not give a Yes/No Prompt before deleting.

/A Select files to delete based on *file_attributes*

file_attributes: R Read-only -R NOT Read-only

S System -S NOT System

H Hidden -H NOT Hidden

A Archive -A NOT Archive

[Back](#)

5.9 Identifying the MSCONFIG options and their respective functions/features

Description: This exercise helps to know about the features of MSCONFIG options.

Instructions: 1. MSCONFIG options are given on the column A

2. Their functions/characteristics are given on the column B

3. Match (drag and drop) the MSCONFIG options given on the Column A with their respective functions/characteristics given on the column B.

Column A

1. General

2. Boot

3. Services

4. Startup

5. Tools

Column B

1. Lists various Stuart configuration modes available for troubleshooting Windows startup issues.

2. Shows various configuration options and debugging settings

3. Lists all of the services that start when your computer starts along with each service's current status.

4. It allows you to quickly disable and prevent an application from starting when Windows starts.

5. It provides a list of diagnostic and informational tools and shows the location of these tools

Explanation

The Msconfig system configuration tool features different tabs based on the Windows version you are running, but the key ones are General, Boot, Services, Startup, and Tools.

General: On the General tab, you can choose the startup type. There are three sets of options: Normal, Diagnostic, and Selective. A normal startup loads all drivers and services, whereas a diagnostic startup only loads the basic drivers and services. Between the two extremes is the selective startup that gives you very limited options on what to load.

Boot: The Boot tab (called Boot.ini in Windows XP), shows the boot menu and allows you to configure parameters such as the number of seconds the menu should appear before the default option is chosen and whether you want go to Safe boot or not. You can toggle on/off the displaying of drivers as they load during start-up and choose to log the boot, go with basic video settings, and similar options.

Services: The Services tab shows the services configured and their current status. From here, you can enable or disable all and hide Microsoft services from the display (which greatly reduces the display in most cases).

Startup: The Startup tab shows the items scheduled to begin at startup, the command associated with them, and the location where the configuration is done (usually, but not always, in the Registry). From here, you can enable or disable all. If a particular startup item has been disabled in Windows 7 and Windows Vista, the date and time it was disabled will appear in the display.

Tools: The Tools tab contains quick access to some of the most useful diagnostic tools in Windows. You can launch such items as the Registry Editor as well as many Control Panel applets, and enable or disable UAC (User Account Control).

[**Back**](#)

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

Description: This exercise helps to know about the various File Attributes

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

Column A

1. Read-Only (R)
2. Hidden (H)
3. System (S)
4. Directory (D)
5. Archive (A)

Column B

1. This attribute will prevent software programs from saving changes to a file.
2. This attribute will be hidden from view under normal viewing conditions.
3. A file or directory used exclusively by the operating system which should not be altered or deleted.
4. This attribute is tagged to folders or sub-folders to differentiate them from files.
5. This attribute is used by software applications that modify files as well as backup software as a “communication link”.

Explanation

Read-Only (R): When set, indicates that a file should not be altered. Upon opening the file, file system API usually does not grant write permission to the requesting application, unless the application explicitly requests it. Read-only attributes on folders are usually ignored. Note that a Read-Only file will not prevent it from being deleted.

Hidden (H): A file marked with the hidden attribute will be hidden from view under normal viewing conditions.

System (S): When set, indicates that the hosting file is a critical system file that is necessary for the computer to operate properly. A file or directory used exclusively by the operating system which should not be altered or deleted.

Directory (D): This attribute is tagged to folders or sub-folders to differentiate them from files.

Archive (A): When set, it indicates that the hosting file has changed since the last backup operation. Windows' file system sets this attribute on any file that has changed. Backup software then has the duty of clearing it upon a successful backup.

[**Back**](#)

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

Description: This exercise helps to know about the various Power options

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

Column A	Column B
1. Hibernate	1. Saves the current session to hard drive before powering off the computer.
2. Sleep/Suspend	2. Saves the current session to memory and put the computer into a minimal power state.
3. Standby	3.Turns off the display and the hard drive for a pre-determined period of inactivity.

Explanation

Sleep mode is a power-saving state that is similar to pausing a DVD movie. All actions on the computer are stopped and any open documents and applications are put in memory. You can quickly resume normal, full-power operation within a few seconds. Sleep mode is basically the same thing as “Standby” mode. The Sleep mode is useful if you want to stop working for a short period of time. The computer doesn’t use much power in Sleep mode.

The **Hibernate mode** saves your open documents and running applications to your hard disk and shuts down the computer, which means once your computer is in Hibernate mode, it uses zero power. Once the computer is powered back on, it will resume everything where you left off. Use this mode if you won’t be using the laptop for an extended period of time, and you don’t want to close your documents.

Stand by is a mode the computer, monitor, or other device enters when idle for too long. This mode

helps conserve power when a computer or computer device is not in use without having to sacrifice the time it would take to turn off and on the computer. When in Stand by, the computer or monitor has a solid or flashing amber light, indicating that there is still power but the computer is in Standby mode.

[Back](#)

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

Description: This exercise helps to know about the different types of file systems and their features.

Instructions: 1. FAT 16/32 and NTFS File Systems are given on the column A
2.Their functions/features are given on the column B
3.Match (drag and drop) the file system types given on Column A with their respective functions/features given on the column B.

Column A	Column B
1. FAT16	1. a) Maximum volume size is 2GB. b) Files stored in this partition cannot exceed 2GB. c) Fault tolerance is average.
2. FAT32	2. a) Maximum volume size 2TB. b) Files stored in this partition cannot exceed 4GB. c) Fault tolerance is minimal
3. NTFS	3. a) Maximum volume size is 2TB. b) Files stored in this partitions can be as large as the partition c) Fault tolerance is maximum

http://www.adrc.com/ckr/ntfs_fat.html

[Back](#)

5.13 Identifying the characteristics of Operating System Administrative tools

Description: This exercise helps to know about the features of Administrative tools.

Instructions: 1.Various Administrative 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 Column A with their respective functions/characteristics given on the column B.

Column A	Column B
1. Computer Management	1. Manage local or remote computers by using a single window.
2. System Configuration	2. Identify problems that might prevent Windows from starting correctly.
3. Services	3. Manage the different services that run in the background on your computer.
4. Component services	4. Configure and administer Component Object Model (COM) components.
5. Data Sources	5. Allows ODBC - compliant applications to

- | | |
|------------------------|--|
| 6. Performance monitor | communicate with each other.
6. View advanced system information about the central processing unit (CPU), memory, hard disk, and network performance. |
|------------------------|--|

Explanation

The **Computer Management Console** is a power-packed interface and includes the following system tools: Device Manager, Event Viewer, Shared Folders, Performance/Performance Logs and Alerts (based on the OS you are running, you may also see Local Users and Groups, or Task Scheduler here as well). Computer Management also has the Storage area, which lets you manage removable media, defragment your hard drives, or manage partitions through the Disk Management utility. Finally, you can manage system services and applications through Computer Management as well.

MSCONFIG, known as the **System Configuration utility**, helps you to troubleshoot startup problems by allowing you to selectively disable individual items that normally are executed at startup. It works in all versions of Windows, although the interface window is slightly different among versions.

Services an MMC snap-in that allows you to interact with the services running on the computer. The status of the services will typically either be started or stopped, and you can right-click and choose Start, Stop, Pause, Resume, or Restart from the context menu. Services can be started automatically or manually, or they can be disabled. If you right-click on the service and choose Properties from the context menu, you can choose the startup type as well as see the path to the executable and any dependencies.

Component Services is an MMC snap-in that allows you to administer, as well as deploy, component services and configure behavior like security (Component Services is located beneath Administrative Tools).

ODBC Data Source Administrator (located beneath Administrative Tools) allows you to interact with database management systems.

Performance Monitor differs a bit in versions but has the same purpose throughout: to display performance counters. While lumped under one heading, two tools are available—System Monitor and Performance Logs And Alerts. System Monitor will show the performance counters in graphical format. The Performance Logs And Alerts utility will collect the counter information and then send it to a console (such as the one in front of the admin so they can be aware of the problem) or event log.

[**Back**](#)

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

Description: This exercise helps to know about the features of command line utilities.

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 command line tools given on the Column A with their respective features/functions given on the column B.

Column A

Column B

1. MSCONFIG	1. Configuration utility to troubleshoot the startup process.
2. REGEDIT	2. A tool used to make changes to the system registry.
3. SERVICES.MSC	3. Allows to interact with the services running on the computer.
4. MMC	4. Starts the management control, that allows to configure and monitor snap-ins.
5. MSINFO32	5. Displays a comprehensive view of your hardware, system components, and software environment.
6. DXDIAG	6. Tool used to test DirectX functionality and troubleshoot video or sound-related hardware problems.
7. MSTSC	7. Used to connect and login to a remote machine using the Remote Desktop Protocol (RDP)

Explanation

Msconfig configuration utility is useful for looking at start-related settings. The Msconfig system configuration tool features different tabs based on the Windows version you are running, but the key ones are General, Boot, Services, Startup, and Tools.

REGEDIT used to open and edit the Registry. Regedit does not have Save or Undo features (though you can import and export); once you make a change, you've made the change for better or worse, and this is not a place to play around in if you're not sure what you're doing. The Registry is divided into five "hives" that hold all settings. The two main hives are HKEY_USERS (which contains settings for all users) and HKEY_LOCAL_MACHINE (which contains settings for the machine itself). HKEY_CURRENT_USER is a subset of HKEY_USERS holding information only on the current user. HKEY_CURRENT_CONFIG and HKEY_CLASSES_ROOT are both subsets of HKEY_LOCAL_MACHINE for the current configuration.

SERVICES.MSC an MMC snap-in that allows you to interact with the services running on the computer. The status of the services will typically either be started or stopped, and you can right-click and choose Start, Stop, Pause, Resume, or Restart from the context menu.

MMC Starts the management console, allowing you to run any snap-in (such as SERVICES.MSC).

MSINFO32, the System Information dialog box, this tool displays a thorough list of settings on the machine. You cannot change any values from here, but you can search, export, save, and run a number of utilities. It is primarily used during diagnostics because it is an easy way to display settings such as IRQs and DMAs.

DXDIAG DirectX Diagnostic tool allows you to test DirectX functionality, with a focus on display, sound, and input. When started, you can also verify that your drivers have been signed by Microsoft. DirectX is a collection of APIs related to multimedia.

MSTSC Remote Desktop Connection Usage is used to configure remote desktop connections.

[Back](#)

5.15 Identifying features of Windows OS types

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

Instructions: 1. Windows OS types are given on the column A

- 2.Their features are given on the column B
3. Match (drag and drop) the OS types given on Column A with their respective features given on the column B.

Column A	Column B
Windows 11	<ol style="list-style-type: none"> 1. Only runs on devices with TPM 2.0 2. Only runs on devices with a minimum of 4GB RAM and 64GB storage. 3. Adjusted the Start menu to the center of the screen but it can be changed. 4. Integrated Microsoft Teams within it and there is no separate app in it. 5. Xbox tech to improve gaming 6.Better virtual desktop support
Windows 10	<ol style="list-style-type: none"> 1. Only runs on devices with TPM 1.2 or above. 2. Only runs on devices with a minimum of 2GB RAM and 32GB storage. 3. Adjusted the Start menu to the left of the screen. 4. Microsoft Teams need to be installed separately.

Explanation

Difference between Windows 11 and Windows 10

1. Design: A major difference between Windows 11 and Windows 10 is in its design. Windows 11 offers an interface that's more like a Mac, with pastel colors, rounded corners for all windows and a cleaner interface than its predecessor. Microsoft simplified the user interface as much as possible to create a clean space for work and play.

Start menu/taskbar: Microsoft has moved the Start menu along with the taskbar to the center of the screen;

Windows 11 also doesn't support live tiles. Live tiles display useful bits of information that users can view without opening the corresponding apps. For example, the weather live tile shows the forecast. Windows 10 is best for users who want to see information in their Start menus at a glance.

Snap Layouts: Another new feature in Windows 11 is Snap Layouts. This allows users to organize their apps and windows more efficiently by grouping them together. The Snap feature in Windows 10 requires users to arrange their windows manually by hovering to the left or right of the screen or by using keyboard combinations.

Microsoft Store: Microsoft has redesigned the Microsoft Store in Windows 11, making it easier for users to find apps and movies, for example. The Microsoft Store will allow users to download all the Windows apps in Windows 11 and Windows 10.

Android apps: The Microsoft Store will also include Android apps hosted on the Amazon App Store. Customers can use Android apps on Windows 10 with the Your Phone app that Microsoft rolled out last year. By bringing Android apps to Windows 11, Microsoft is meeting user demand to run smartphone apps on their desktops. Microsoft has replaced the Windows 10 Meet Now feature powered by Skype with the integration of Teams into the Windows 11 taskbar. This will make it easier for users to access the communication platform.

Touch/tablet mode: Microsoft is removing the tablet mode included in Windows 10 from Windows 11. The tablet mode in Windows 10 makes users' PCs more touch-friendly when they use their devices as tablets. However, Windows 11 acts more like an iPad. That means when users switch their PCs to tablets, they will receive an experience that's optimized for touch.

Windows 11 will also have larger touch targets and visual cues so users can easily resize and move windows.

Virtual desktops: Although Windows 10 included the Task View feature and allowed users to create multiple virtual desktops, the options were limited. Windows 11 users will be able to set up virtual desktops much like they do with Macs. Users can toggle between multiple desktops simultaneously for work, school, gaming and personal use.

Gaming upgrades: PC gaming should also improve with Windows 11. Auto HDR (high dynamics range) will also be baked into Windows 11, which should enhance the colors in many games. When a user plays on an HDR monitor, Auto HDR enhances the color range in many DirectX 11 and newer games -- even games where HDR settings weren't implemented. Xbox Game Pass will also be included in Windows 11.

Performance improvements: The new OS will include performance improvements, including faster logins with Windows Hello, faster web browsing and faster wake from sleep mode. Windows Hello is a biometrics-based technology that lets Windows 10 users authenticate secure access to their devices, apps and networks with iris scans, facial recognition or fingerprints.

[**Back**](#)

5.16 Identifying the display standards of Windows OS and their resolutions

Description: This lab exercise helps you to know the various display standards and their resolutions.

Instructions: 1. Name of the resolutions is given on the column A.
2. Match (drag and drop) the display standards given on the Column A with their respective resolution given on the Column B

Column A	Column B
1. HD	1. 1366X768 (16:9)
2. FHD	2. 1920 X 1080 (16:9)
3. HD+	3. 1600 X 90 (16:9)
4. SXGA	4. 1280 X 1024 (5:4)
5. VGA	5. 640 X 480 (4:3)
6. SVGA	6. 800 X 600 (4:3)
7. XGA	7. 1024 X 768 (4:3)

Explanation:

Resolution: Monitors display images with several characteristics that you can control: resolution, brightness and contrast, and color depth. Resolution and color depth are usually adjusted with the software driver that works with the computer's operating system through the graphics adapter card. In most Microsoft Windows operating systems you can adjust the resolution and color depth by going to the Start Menu > Settings > Control Panels > Display > Settings.

Resolution is how many pixels your screen displays for a given size dimension, and is given in pixel

dimensions, such as 640 x 480. Other popular sizes are 800 x 600 and 1024 x 768. For example, 800 x 600 means your monitor's screen will have 800 pixels on the long horizontal side and 600 pixels on the short vertical side. More resolution, such as 1024 x 768, means smaller pixels and finer detail.

Color depth describes how many colors that can be displayed on a monitor's screen. Color depth is usually talked about in bits. A bit is an abbreviation for "binary digit".

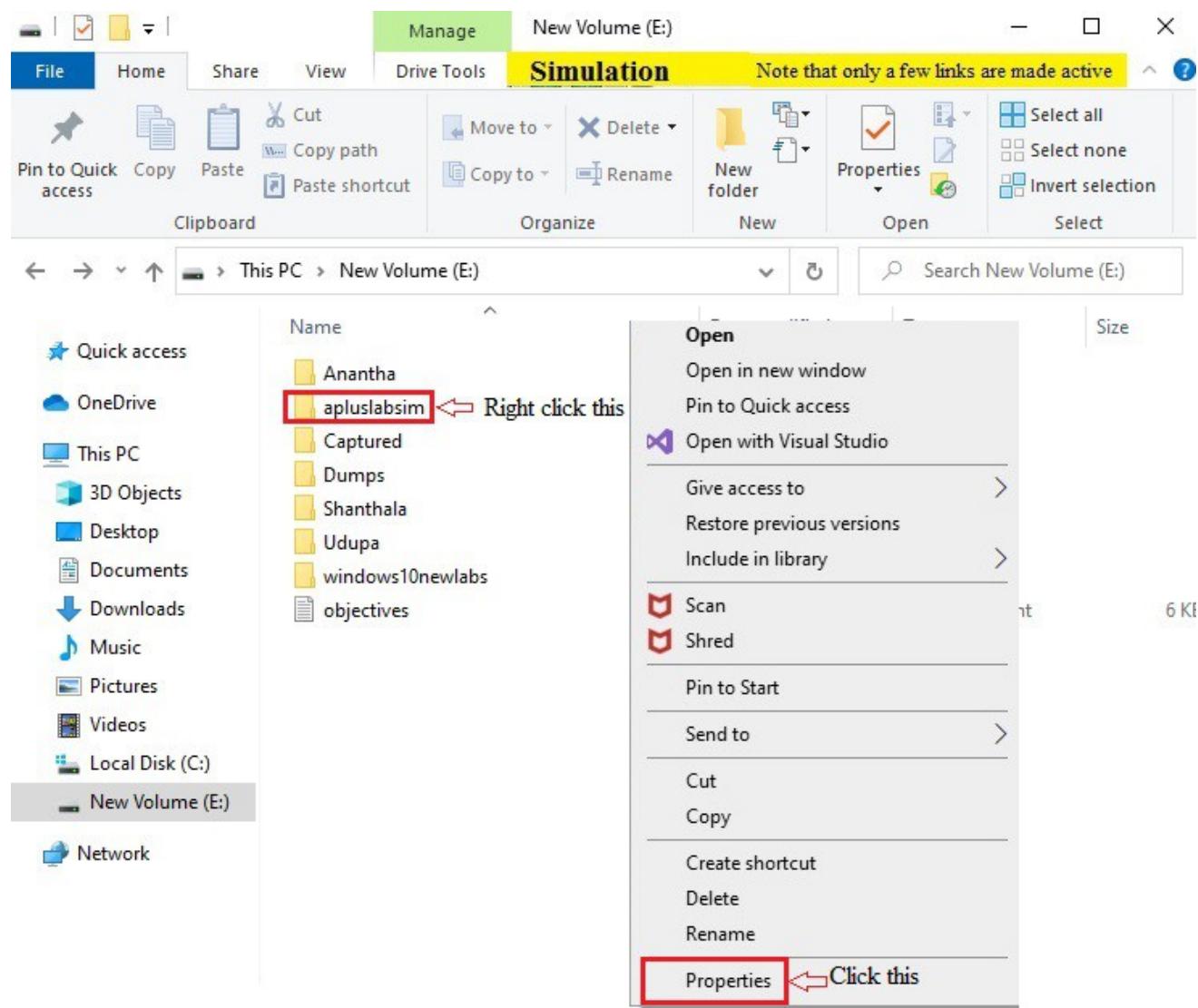
Computers speak a binary language of bits where there are only ones and zeros. Since there are only two numbers (1 and 0) the math is called "binary" (bi meaning two, like two wheels on a bicycle). Each of the three primary colors (Red, Blue and Green) has a number of bits that describes its color "depth", or the number of shades of that particular color that can be displayed. The number of colors are usually talked about in exponential notation, such as the number 2 raised to the second power (two squared, $2 \times 2 = 4$), or two to the eighth power ($2 \times 2 = 256$). The more bit depth a color has, the more shades of that color can be displayed. "True" color is also called 24-bit color. Here, each color is 8 bits, for a total of 24 bits. Since each color has 256 shades, we can multiply 256 for red, times 256 for green, times 256 for blue and get millions of colors, ($256 \times 256 \times 256 = 16,777,216$). Millions of colors are pretty much what's accepted for a monitor's colors to look "true" to the human eye.

[Back](#)

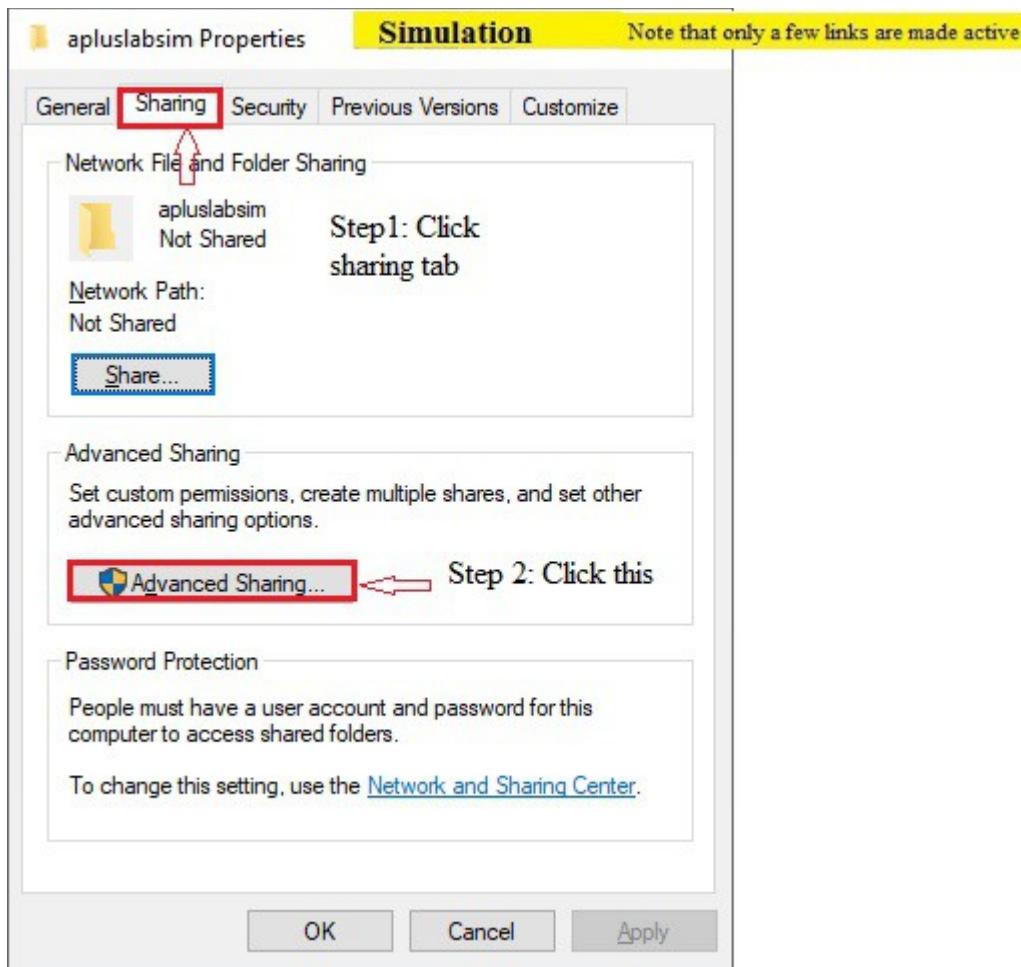
5.17 NTFS permissions and Share permissions in Windows 10

Description: This lab exercise helps you to know how to share the folder with other users on your network.

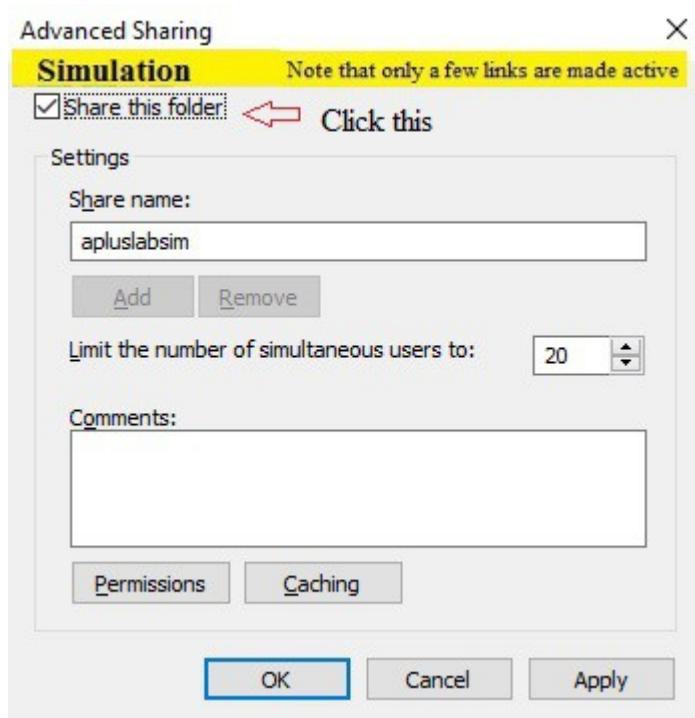
Instructions: 1. On a given file explorer in windows 10 right click on a folder you want to share.
2. In this lab exercise right click on folder “aplusLabsim” and a popup window appears click “Properties” option.



3. In properties dialog box click sharing tab and click Advanced Sharing button



4. In Advanced sharing window click share this folder checkbox , click apply button and then OK button.



Explanation: The File and Printer Sharing for Microsoft Networks component allows computers on a network to access resources on other computers using a Microsoft network. This component is installed and enabled by default. It is enabled per connection using TCP/IP and is necessary to share local folders.

The File and Printer Sharing for Microsoft Networks component is the equivalent of the Server service in Windows NT 4.0. Shared permissions are used to control access to shared folders when they are accessed over the network.

Share permissions:

1. Apply only to users who gain access to the resource over the network. They do not apply to users who log on locally, such as on a terminal server.
2. Apply to all files and folders in the shared resource.
3. Are the only way to secure network resources on FAT and FAT32 volumes, because NTFS permissions are not available on FAT or FAT32 volumes.

Specify the maximum number of users who are allowed to access the shared resource over the network.

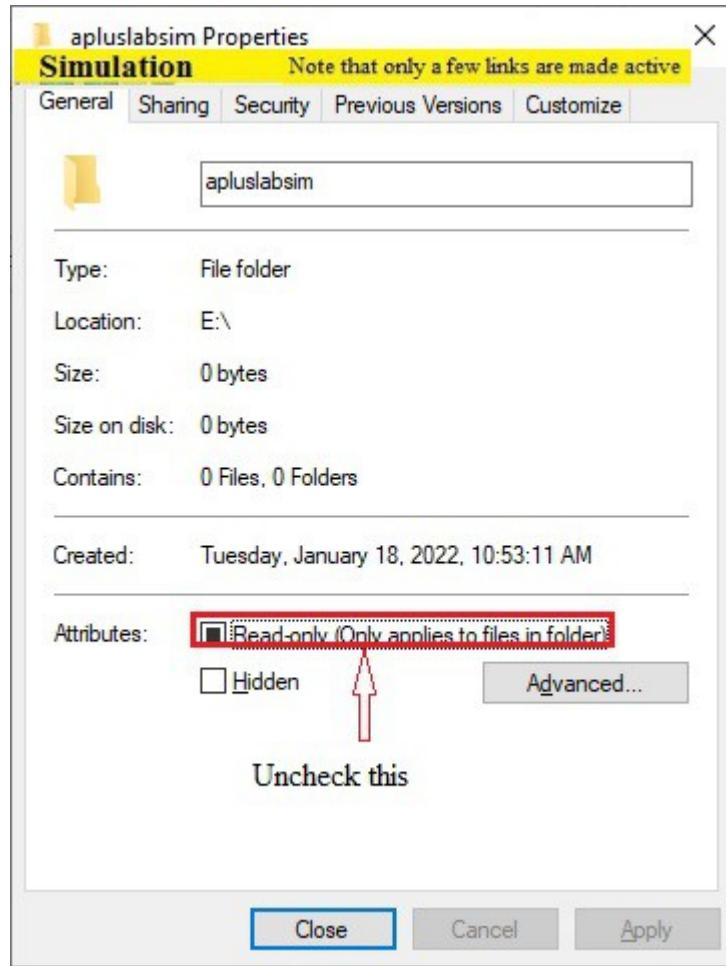
[**Back**](#)

5.19.2 To change read only attributes on files and folders

Description: This lab exercise helps you to know about changing the read only attributes of files and folders

Instructions:

1. In a given File Explorer window in Windows 10 right click on the folder "aplusLabsim" and click properties.
2. Remove the check mark by the Read Only item in the file's Properties dialog box.
The attributes are found at the bottom of the General tab and click Apply and then OK button.



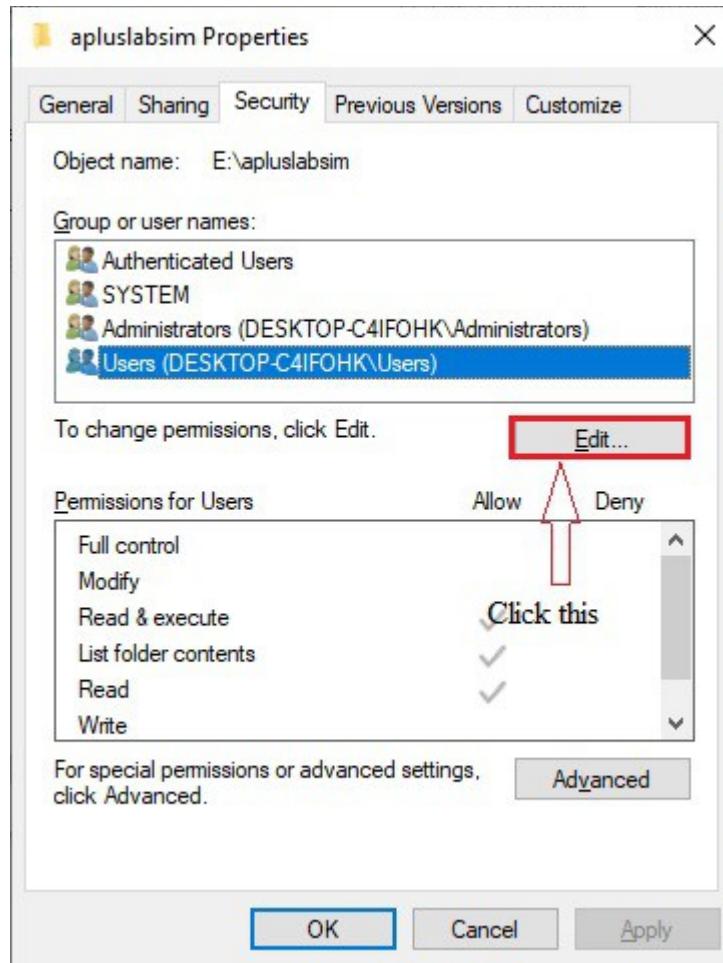
[**Back**](#)

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

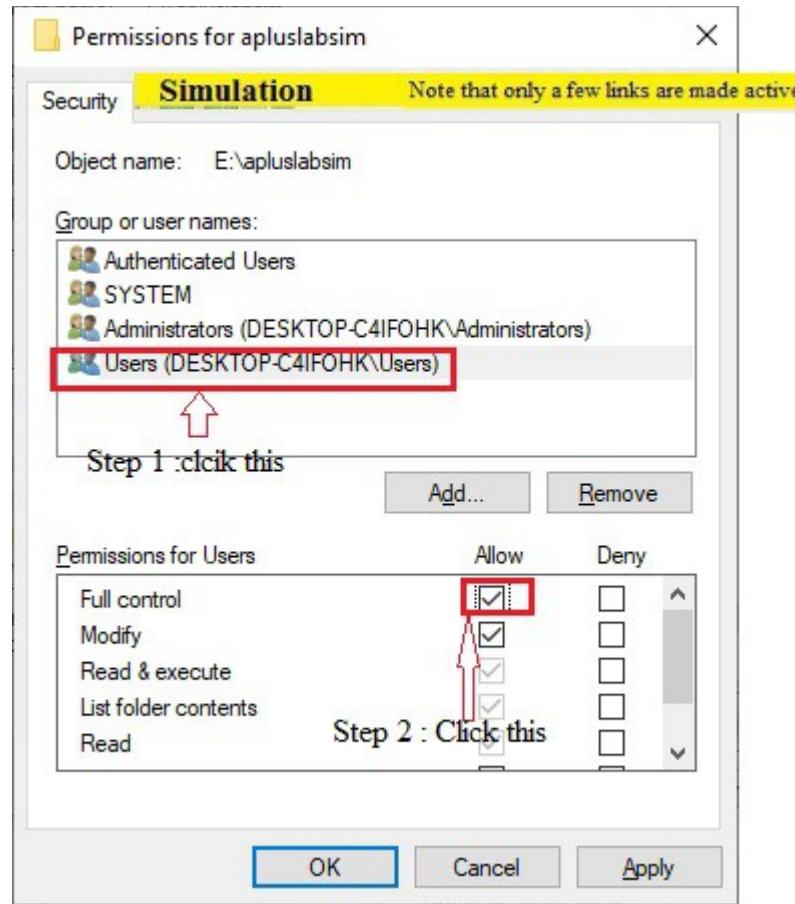
Description: This lab exercise helps you to know about setting folder permissions.

Instructions:

1. In a given File Explorer window in Windows 10 right click on the folder “AplusLabsim” and click properties.
2. Click the **Security** tab in Folder properties dialog box. In security tab click Edit button.



4. In Permissions window check mark the Full control in Allow column and click Apply and then OK button



Explanation: File system permissions are an essential method of securing one's private data. In Windows, you can set permissions on NTFS-formatted partitions/drives; other file systems, such as FAT/FAT32/exFAT do not support access restrictions, aka Access Control Lists (ACL).

[Back](#)

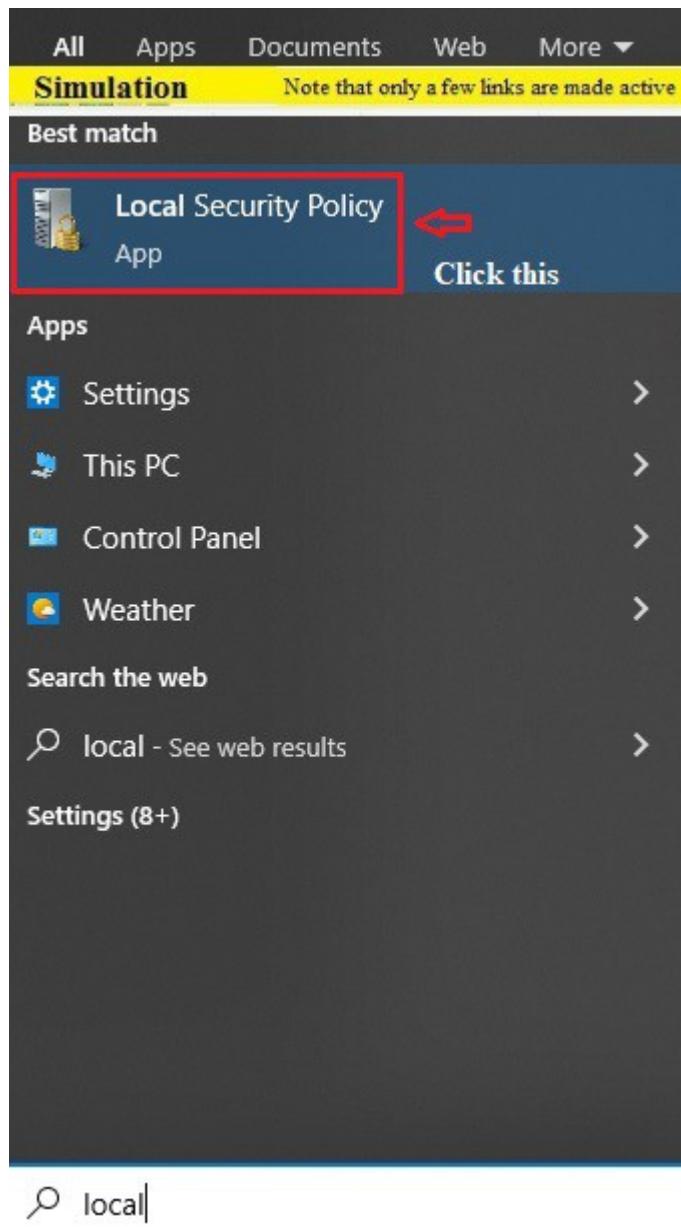
5.18 Configuring Local Security Policy in Windows 10

5.18.1 Setting Account lockout policy

Description: This lab exercise helps to set account lockout threshold policy in Windows 10

Instructions: 1. Start typing “local security policy” (without quotation marks) in the Search box on the left side of the Windows 10 taskbar. When the Local Security Policy (Desktop app) shows in the search results list, click on it to open it.

In this lab exercise, in given simulation Start menu click “**Local Security Policy**”



2. In Local Security Policy window in right pane double click on “Account policies”

Local Security Policy Simulation Note that only a few links are made active

File Action View Help

Security Settings

- > Account Policies
- > Local Policies
- > Windows Defender Firewall with Advanced Security
- > Network List Manager Policies
- > Public Key Policies
- > Software Restriction Policies
- > Application Control Policies
- > IP Security Policies on Local Computer
- > Advanced Audit Policy Configuration

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options policies
Windows Defender Firewall with Advanced Security	Windows Defender Firewall with Advanced Security
Network List Manager Policies	Network name, icon and location group policies.
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administration
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

Double click this

3. In next window double click on Account Lockout policy.

Local Security Policy Simulation Note that only a few links are made active

File Action View Help

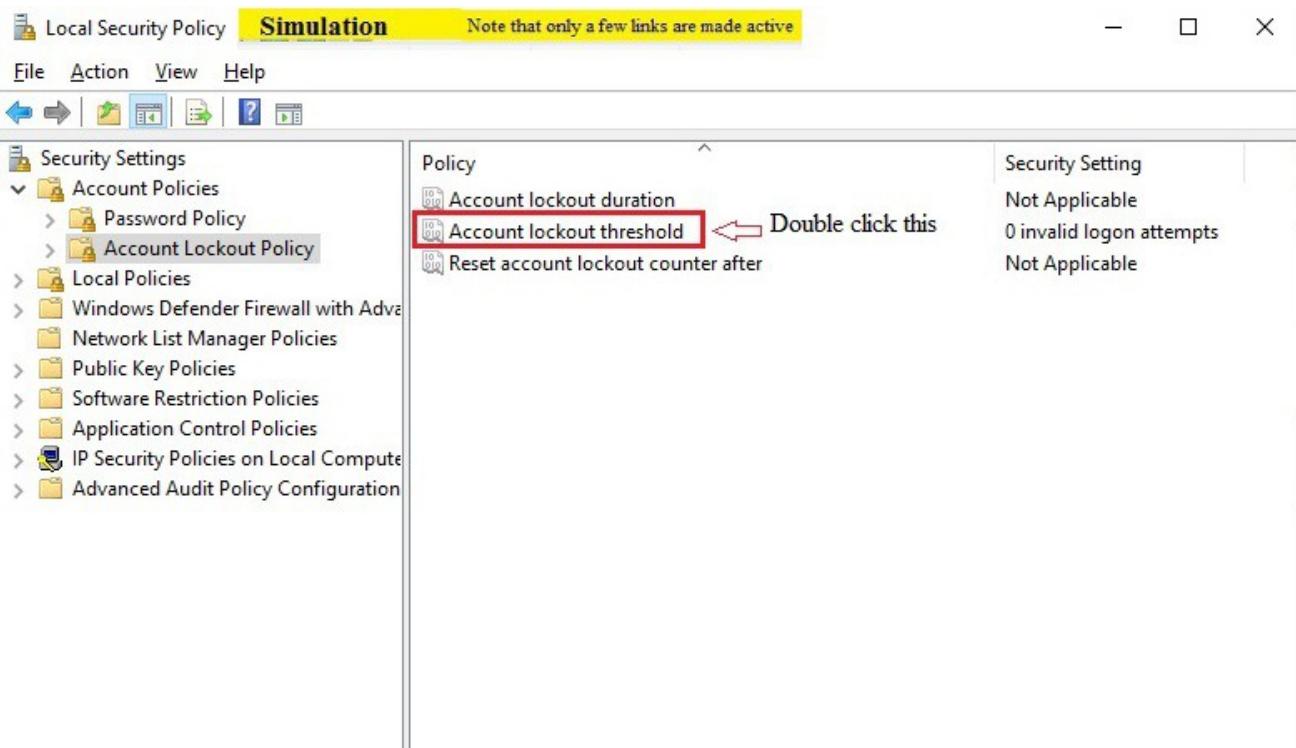
Security Settings

- > Account Policies
- > Local Policies
- > Windows Defender Firewall with Advanced Security
- > Network List Manager Policies
- > Public Key Policies
- > Software Restriction Policies
- > Application Control Policies
- > IP Security Policies on Local Computer
- > Advanced Audit Policy Configuration

Name	Description
Password Policy	Password Policy
Account Lockout Policy	Account Lockout Policy

Double click this

4. In next window double you will see three policies in the right pane. Double Click **Account lockout threshold**.



5. In Account lockout threshold properties window click up arrow button and enter 3 in “Account will lock out after” drop down.

Account lockout threshold Properties

Simulation

Note that only a few links are made active

Local Security Setting

Explain



Account lockout threshold

Account will lock out after:

3



invalid logon attempts

OK

Cancel

Apply

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.

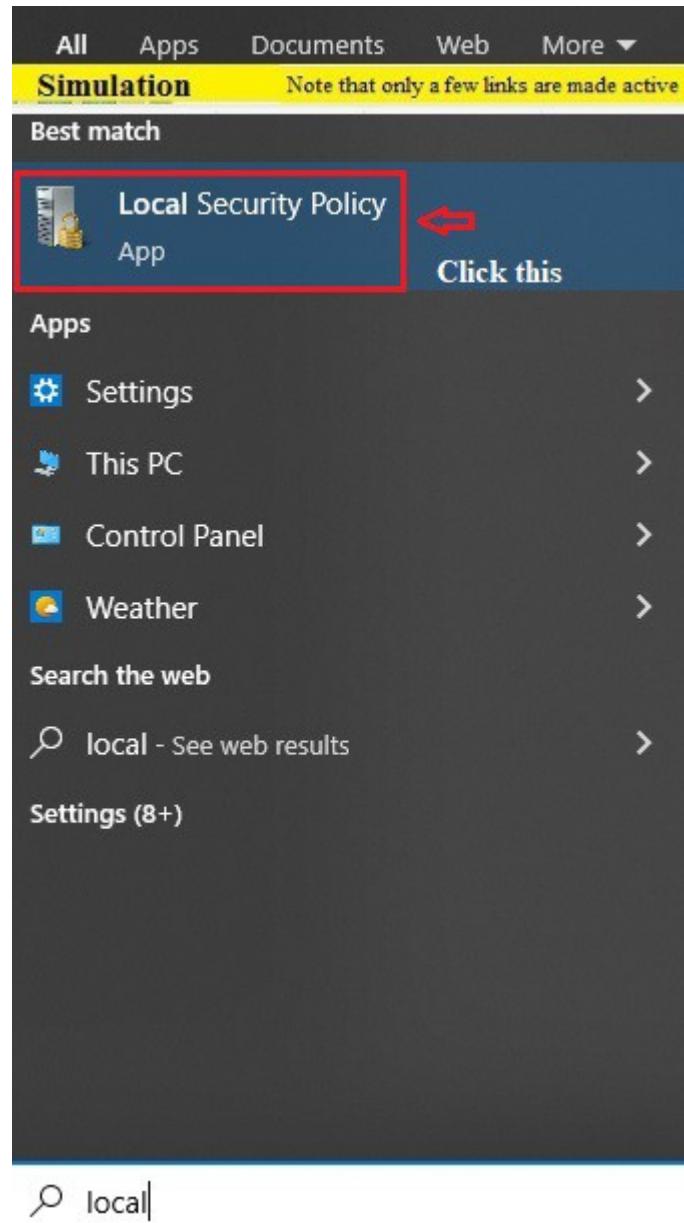
[Back](#)

5.23.2 Setting Password policy

Description: This lab exercise helps to enable or disable password must meet complexity requirement in windows 10

Instructions: 1. Start typing “local security policy” (without quotation marks) in the Search box on the left side of the Windows 10 taskbar. When the Local Security Policy (Desktop app) shows in the search results list, click on it to open it.

In this lab exercise, in given simulation Start menu click “Local Security Policy”



2. In Local security policy window double click on “Account Policies”

Local Security Policy **Simulation** Note that only a few links are made active

File Action View Help

Security Settings

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options policies
Windows Defender Firewall with Advanced Security	Windows Defender Firewall with Advanced Security
Network List Manager Policies	Network name, icon and location group policies.
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administration
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

Double click this

3. In next window double-click on “Password Policy”

Local Security Policy **Simulation** Note that only a few links are made active

File Action View Help

Security Settings

Name	Description
Account Policies	Password Policy
Local Policies	Account Lockout Policy
Windows Defender Firewall with Advanced Security	
Network List Manager Policies	
Public Key Policies	
Software Restriction Policies	
Application Control Policies	
IP Security Policies on Local Computer	
Advanced Audit Policy Configuration	

Double click this

4. In the next window you will see six policies in the right pane. Double Click “Password must meet complexity requirements”

Local Security Policy **Simulation** Note that only a few links are made active

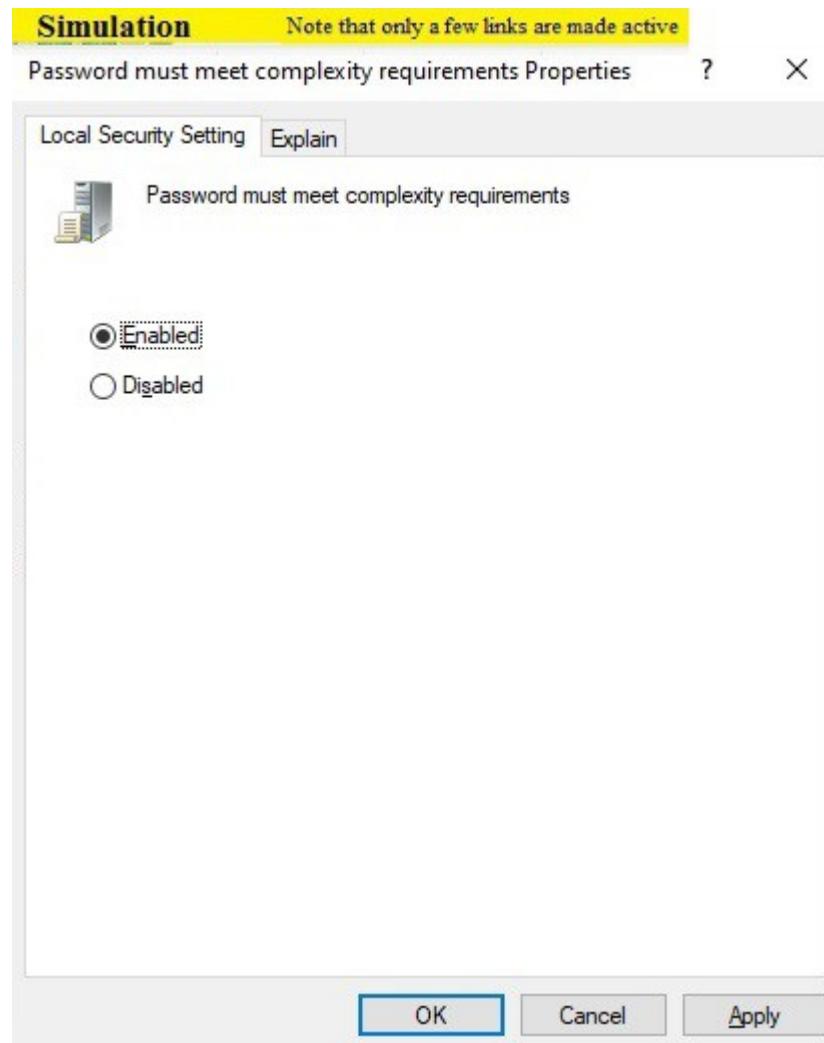
File Action View Help

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
Minimum password length audit	Not Defined
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Double click this

5. 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.

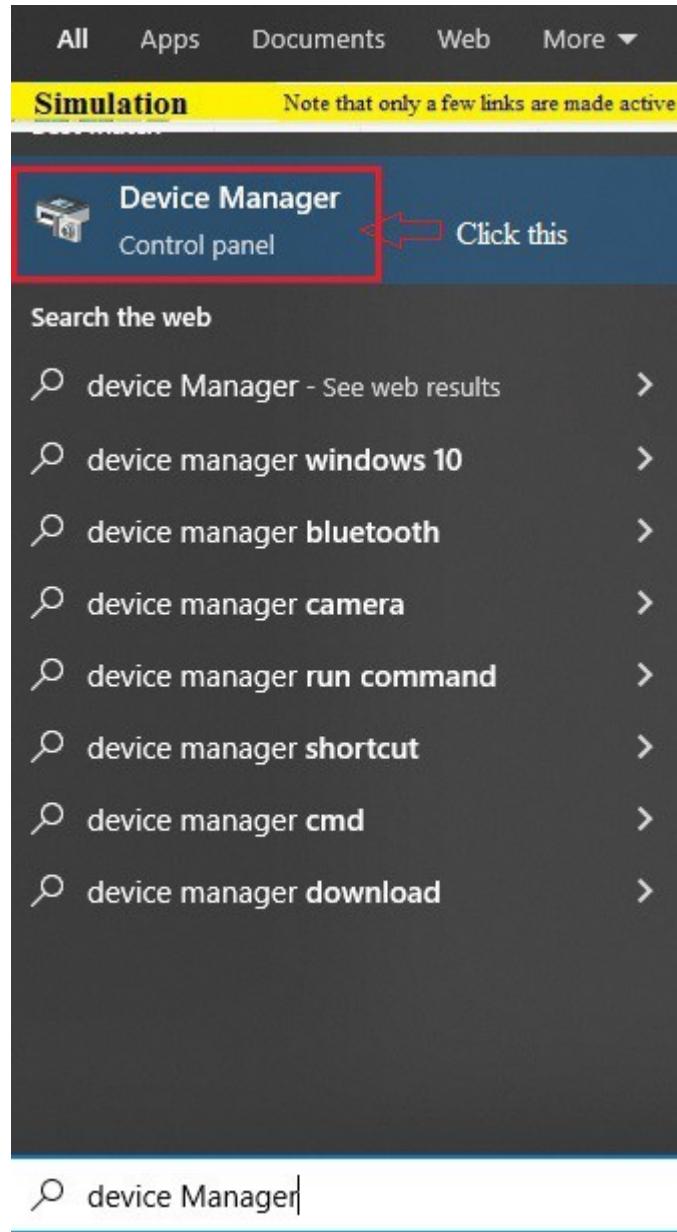
[**Back**](#)

5.24 Configuring hardware settings using Device Manager

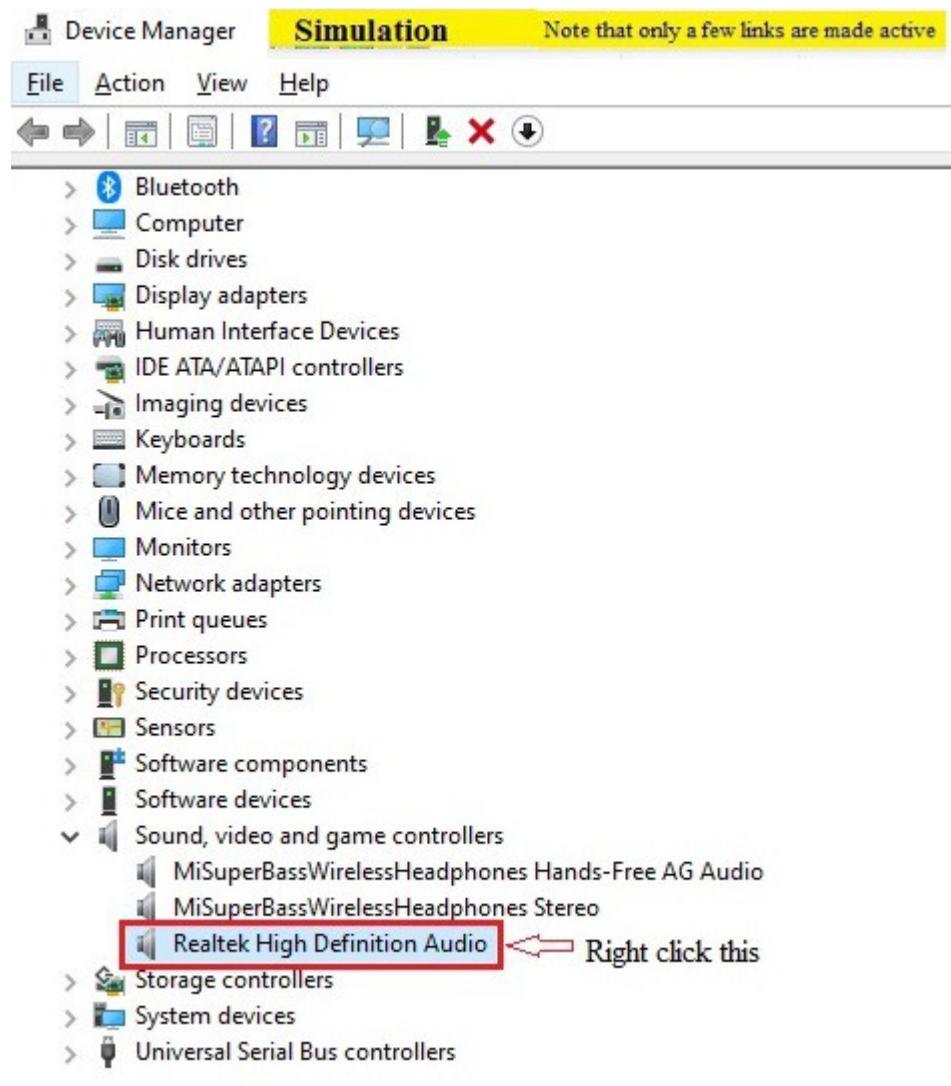
Description: This lab exercise helps to change the hardware settings using device manager

Instructions: 1. On the taskbar, in the Search field next to the Start button type "Device Manager" and then press Enter key to access Device Manager.

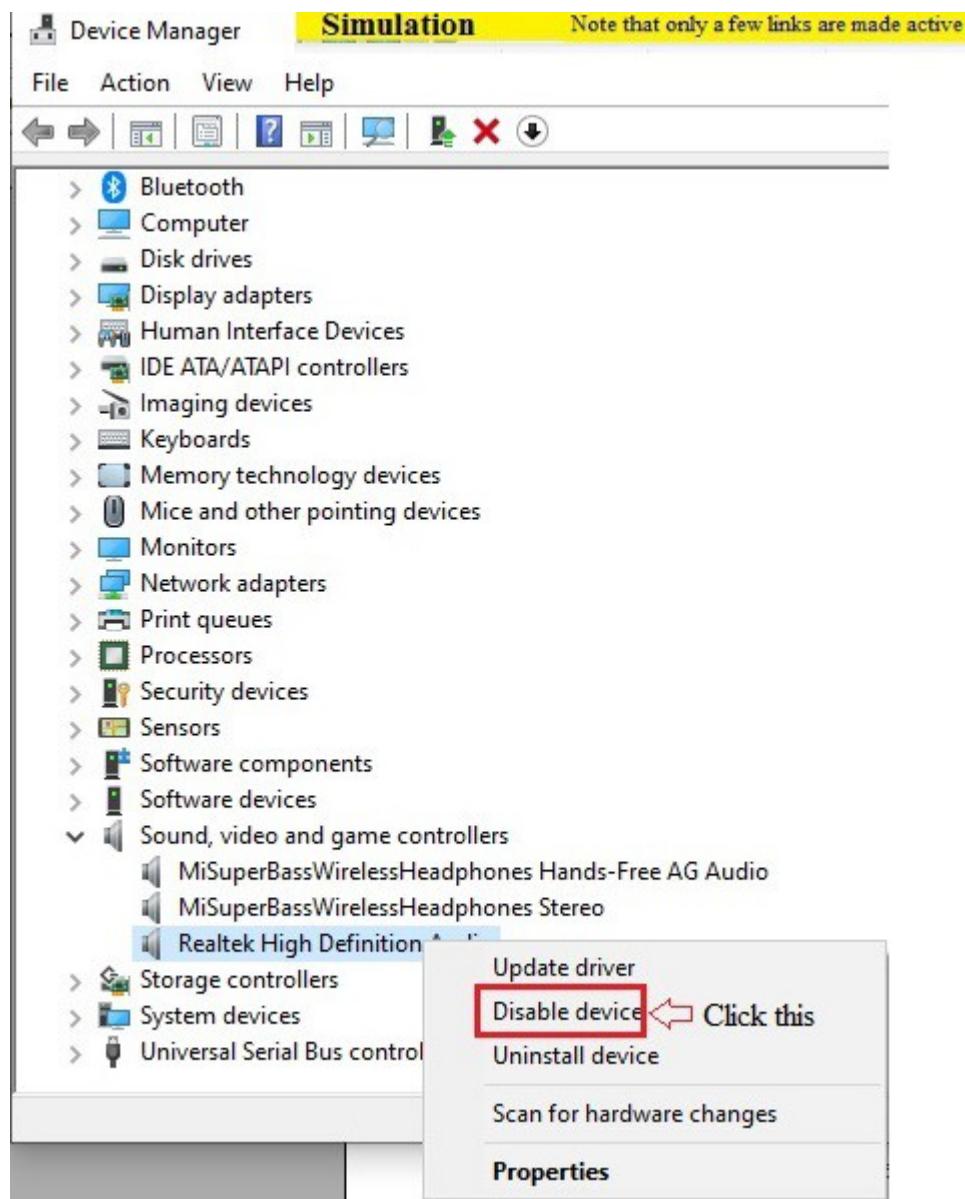
In this Simulation start menu click "Device Manager" option as shown below fig.



2. In Device Manager window under Sound,video and game controllers right click “Realtek High Definition Audio”



3. A pop up menu appears click “Disable device”, 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:

- a. Determine whether the hardware on your computer is working properly.
- b. Change hardware configuration settings.
- c. Identify the device drivers that are loaded for each device, and obtain information about each device driver.
- d. Change advanced settings and properties for devices. Install updated device drivers.
- e. Enable, disable, and uninstall devices.
- f. Roll back to the previous version of a driver.
- g. View the devices based on their type, by their connection to the computer, or by the resources they use.
- h. Show or hide hidden devices that are not critical to view, but might be necessary for advanced

troubleshooting.

- i. 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](#)

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

Description: This lab exercise explains how to use the Command Prompt to fix issues with your PC's boot records

Instructions: 1. In the given command prompt type the following commands one after the other

1. bootrec.exe /fixmbr
2. bootrec.exe /fixboot
3. bootrec.exe /rebuildbcd

Note : You can type “exit” command to close the command prompt window.

The screenshot shows a Windows Command Prompt window with the title bar 'S Command Prompt'. The window has a yellow header bar with the text 'Simulation' on the left and 'Note that only a few commands supported' on the right. The main area of the window is black and contains the following command-line session:

```
C:\windows\system32>bootrec.exe /fixmbr
The operation completed successfully
C:\windows\system32>bootrec.exe /fixboot

The operation completed successfully
C:\windows\system32>bootrec.exe /rebuildbcd

Scanning all disks for Windows installations.

Successfully scanned Windows installations.
Total identified Windows installations : 0
The operation completed successfully.
C:\windows\system32>exit
```

In the bottom right corner of the window, there is a 'Close' button.

Explanation: Bootrec.exe is the ultimate repair tool for boot problems in Windows

The first parameter of the Bootrec.exe tool is /FixMbr. It allows the repair of a corrupted or damaged Master Boot Record (MBR). Usually, you will use this parameter when you are faced with one of these error messages: "Operating System not found", "Error loading operating system", "Missing operating system" or "Invalid partition table". To start the repair process of the MBR, run the command: bootrec.exe /fixmbr.

The /FixBoot parameter writes a new boot sector to the system partition. The tool will use a boot sector that is compatible with your Windows version. Using this parameter is useful in the following situations:

- The boot sector has been replaced with a non-standard Windows boot sector;
- The boot sector is damaged;
- An earlier Windows operating system has been installed after your version of Windows was installed.

The *Boot Configuration Data (BCD)* contains a detailed list of what is supposed to load at startup. Microsoft indicates that a boot error can also be caused by missing or damaged files in the BCD. The /rebuildbcd parameter can be very useful when you must fix some errors by completely rebuilding the BCD. To completely rebuild the Boot Configuration Data, run this command: bootrec.exe /rebuildbcd.

If your computer has multiple operating systems installed but not all of them are available, use the /ScanOS option. Using this parameter on Bootrec.exe will launch a scan on all disks for any Windows

installations that are not currently included in the *Boot Configuration Data (BCD)*.

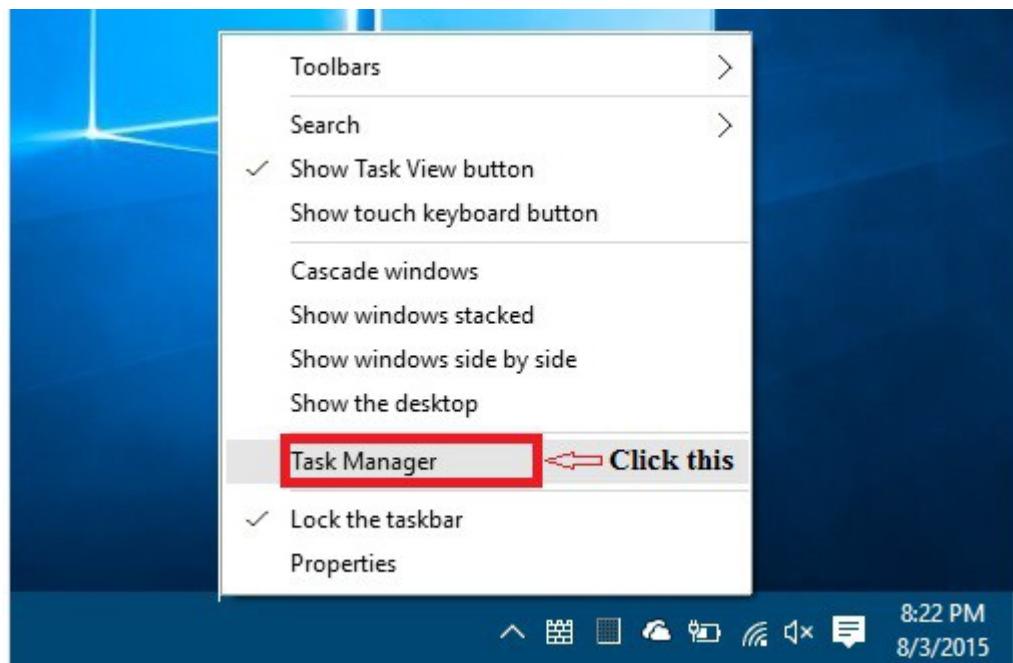
[Back](#)

5.21 Disabling start up program in Windows 10

Description: This lab exercise explains 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.

Task Manager

File Options View

Processes Performance App history Start-up Users Details Services

Click this

Name	Status	11% CPU	40% Memory	86% Disk	0% Network
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

Fewer details **End task**

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 menu bar includes "File", "Options", and "View". Below the menu is a tab bar with "Processes", "Performance", "App history", "Start-up" (which is selected), "Users", "Details", and "Services". A status message at the bottom right says "Last BIOS time: 5.4 seconds".

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			
Windows Defender notificati...	Microsoft Corporation	Disabled	None

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

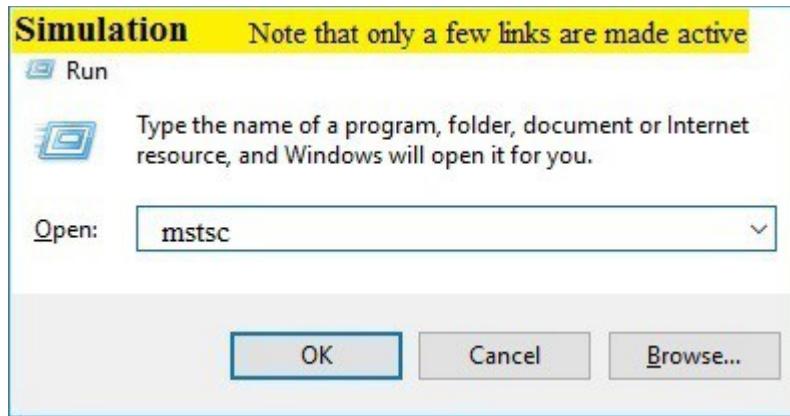
Explanation: Startup programs are programs which run when your computer starts / boots up. Startup programs can be antivirus programs, chat/messaging apps or background apps that can also continuously keep running on your computer. Start up programs impact computer boot time, and may make your computer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

[Back](#)

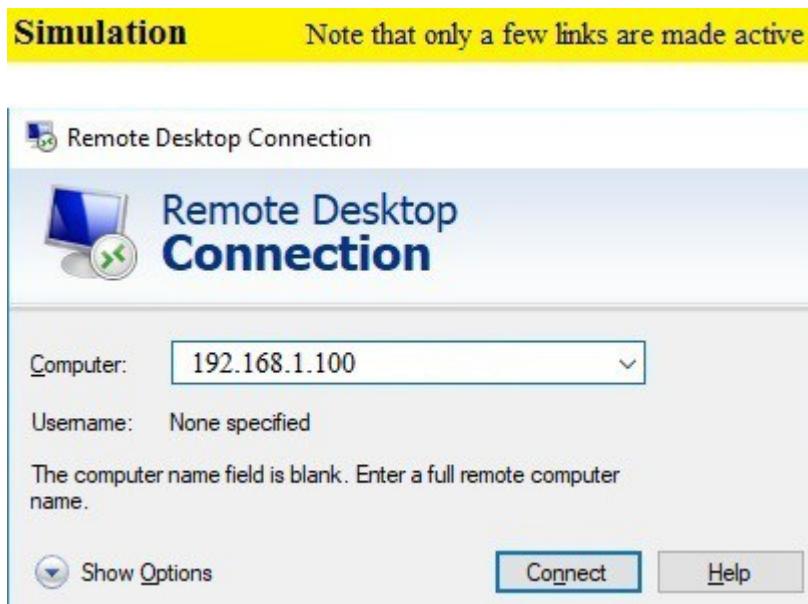
5.22 Connecting to remote desktop in Windows 10

Description: This lab exercise explains 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.

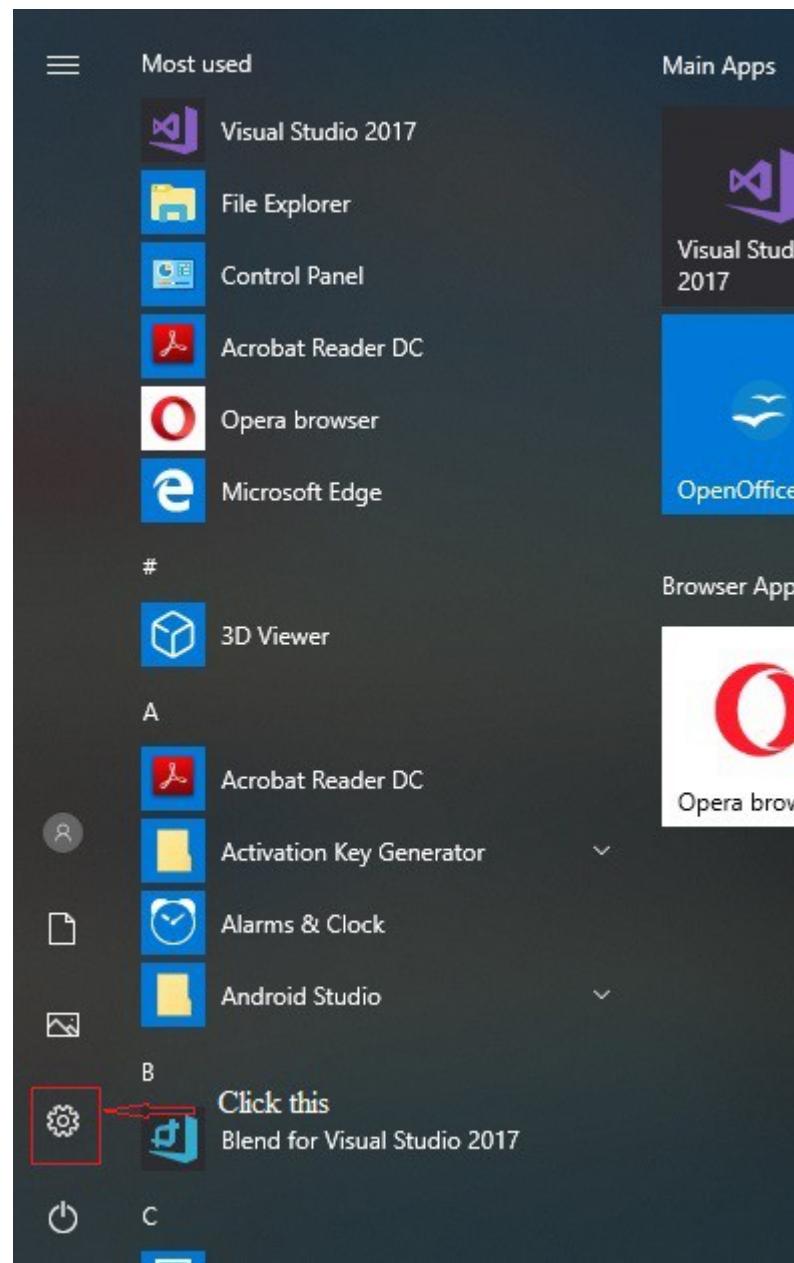
[Back](#)

5.23 Changing the refresh rate in Windows 10

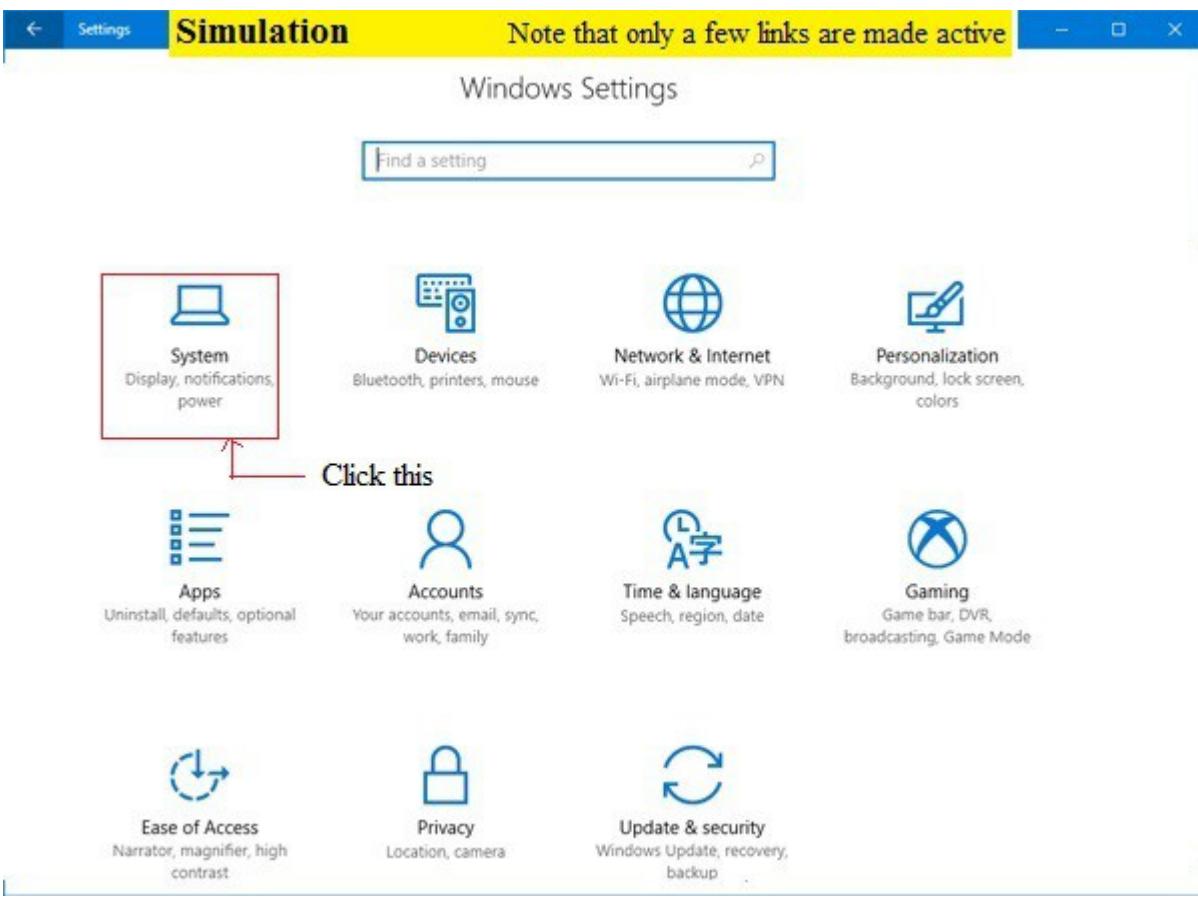
Description: The lab exercise explains how to change the monitor refresh rate in windows 10 OS. Here, you change the refresh rate to 60 Hertz.

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, a sidebar lists various system categories like Home, System, Display, Sound, etc. The 'Display' category is selected. On the right, under 'Display', the 'Scale and layout' section is active. It includes a dropdown for text size ('100% (Recommended)'), a link to 'Advanced scaling settings', and dropdowns for resolution ('1366 x 768 (Recommended)') and orientation ('Landscape'). Below this, the 'Multiple displays' section is shown, featuring a 'Detect' button and links for 'Advanced display settings' and 'Graphics settings'. A red box highlights the 'Advanced display settings' link, with a red 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 this

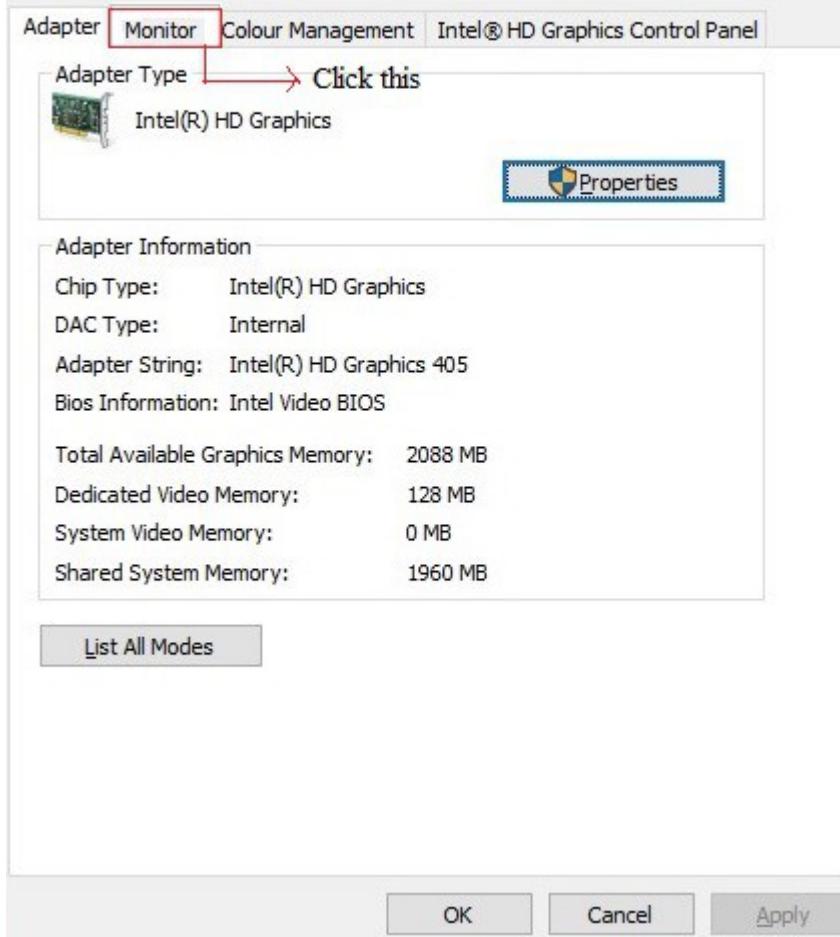
5. Click the **Monitor** tab

Simulation

Note that only a few links are made active

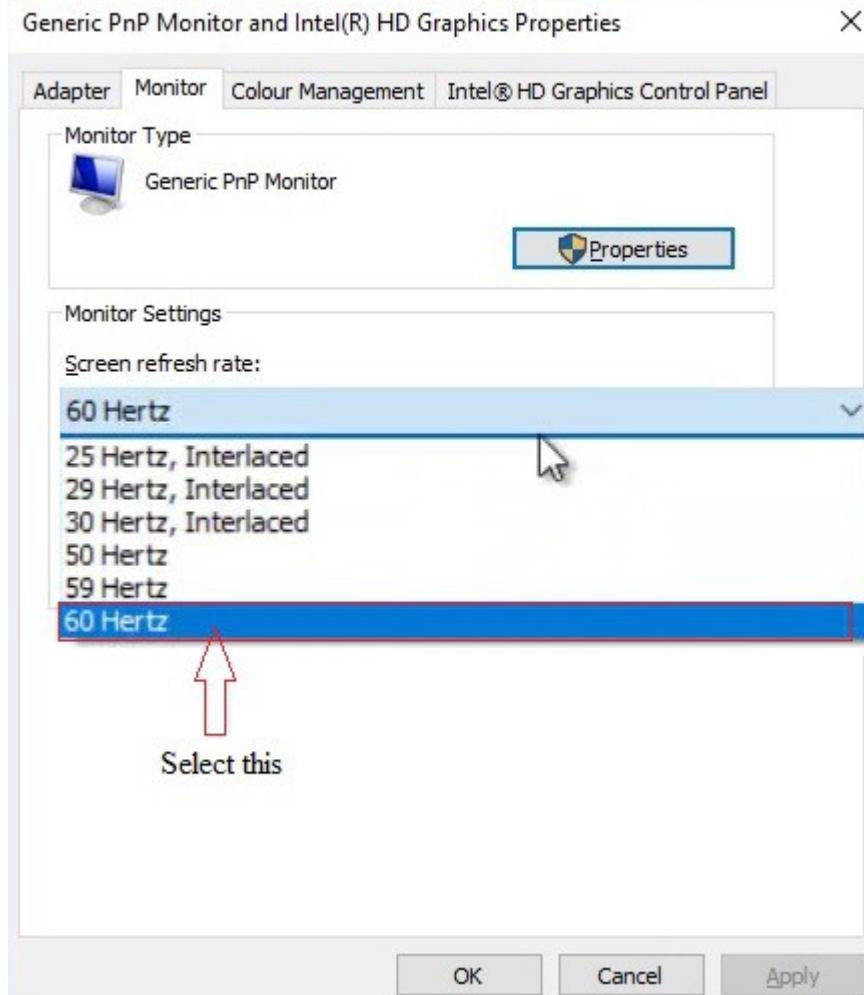
Generic PnP Monitor and Intel(R) HD Graphics Properties

X



- 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.

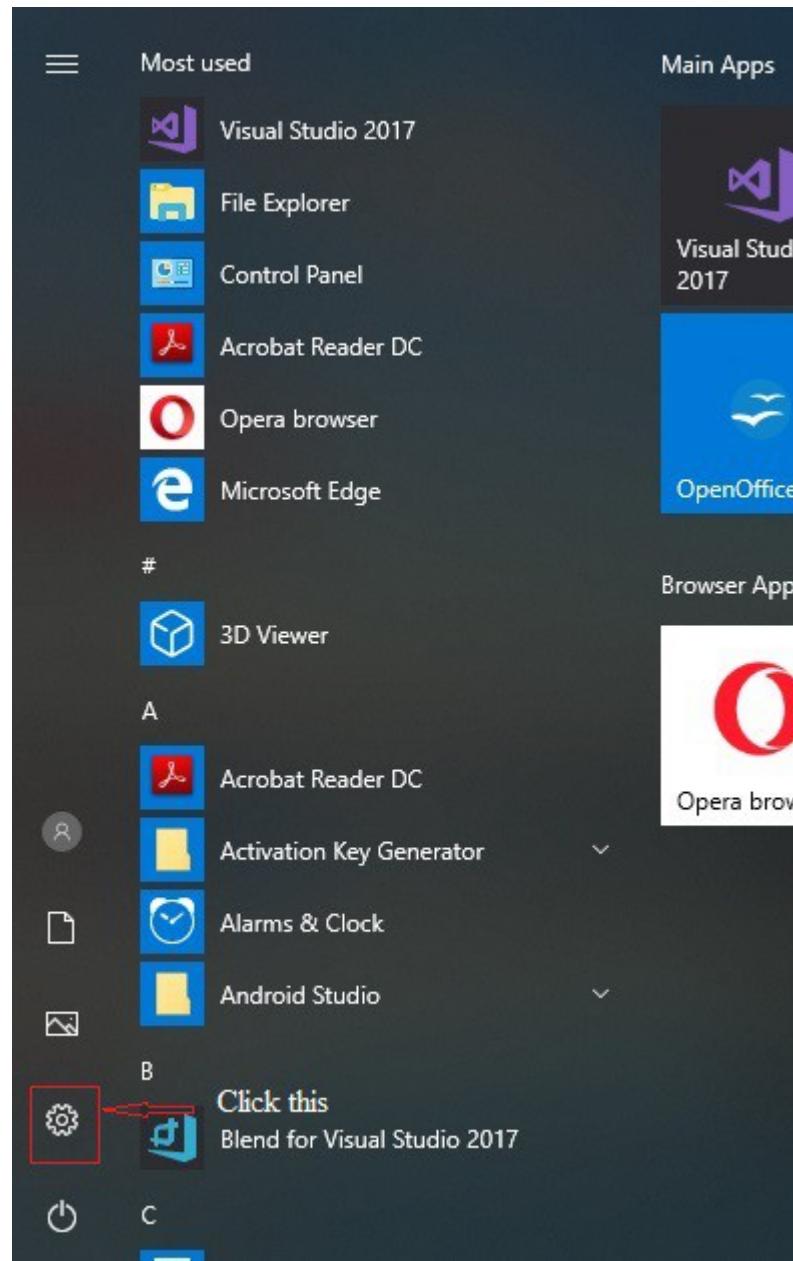
[Back](#)

5.24 Changing Power Plan Settings in Windows 10

Description: This lab exercise explains how to change the power plan settings in windows 10 OS. Here, you change the Power and sleep settings to 5 minutes and 2 hours.

Instruction:

1. In the given simulator start menu click **settings**



2. In the settings app click/tap on the **System** icon.

Windows Settings

Find a setting  Click this

3. Click/tap on Power & sleep on the left side.

The screenshot shows the Windows Settings application running in Simulation mode. The title bar indicates "Simulation" and includes a note: "Note that only a few links are made active". The left sidebar lists system settings: Home, Find a setting search bar, System, Display, Sound, Notifications & actions, Focus assist, Power & sleep (which is highlighted with a red box and a callout "Click this"), Battery, Storage, Tablet mode, Multi-tasking, and Projecting to this PC. The main content area is titled "Display" and contains sections for Brightness and colour, Change brightness (with a slider), Night light (switched off), Night light settings, Scale and layout, Change the size of text, apps and other items (set to 100% Recommended), Advanced scaling settings, Resolution (set to 1366 x 768 Recommended), Orientation (set to Landscape), and Multiple displays.

Display

Brightness and colour

Change brightness

Night light

Off

[Night light settings](#)

Scale and layout

Change the size of text, apps and other items

100% (Recommended)

[Advanced scaling settings](#)

Resolution

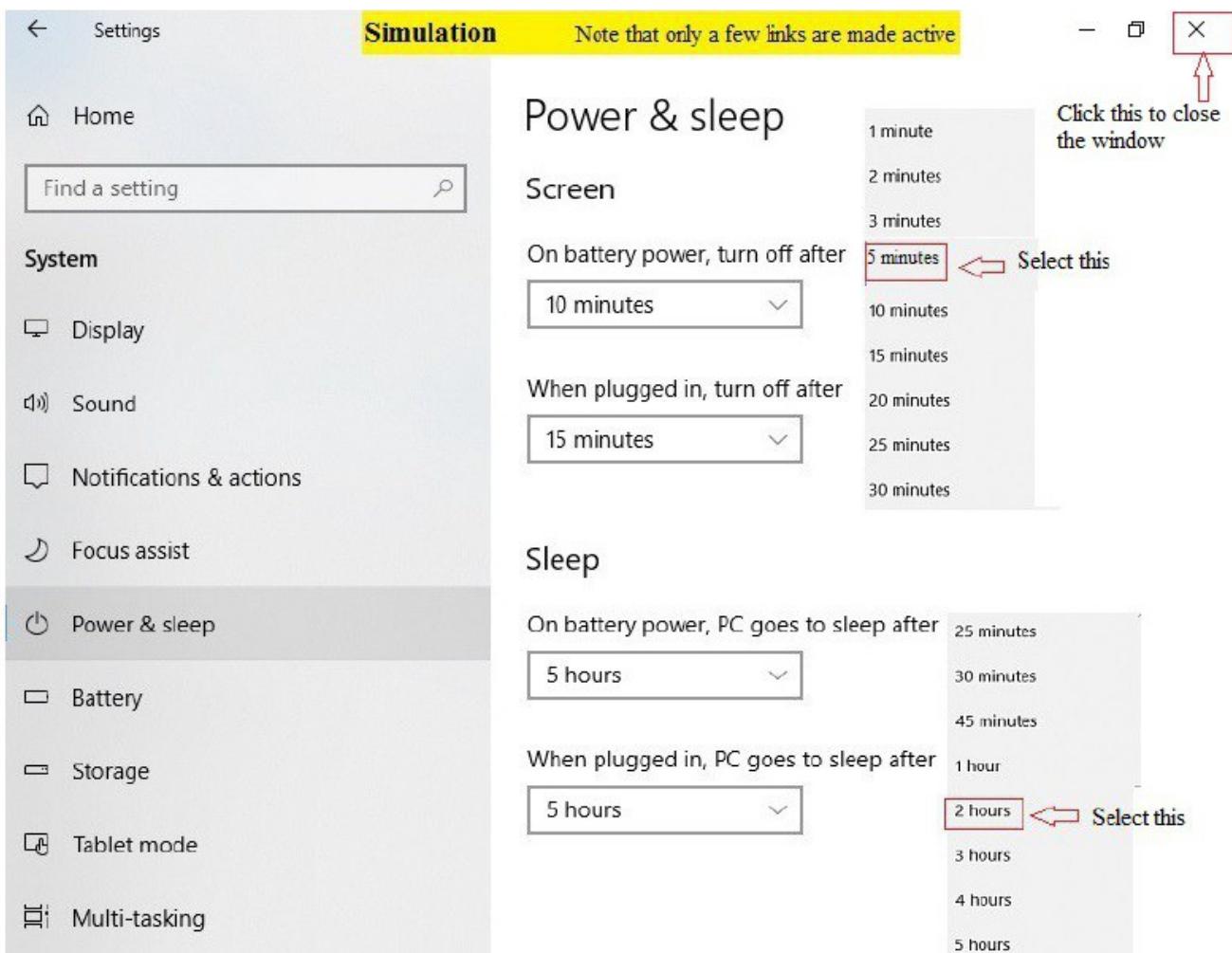
1366 × 768 (Recommended)

Orientation

Landscape

Multiple displays

4. On the right side Power and Sleep settings displayed , change the screen settings , “**On battery power, turn off after**” and “**When plugged in, turn off after**” to 5 minutes and sleep settings , “**On battery power, PC goes to sleep after**” and “**When plugged in, PC goes to sleep after**” to 2 hours. and then close the settings.



Explanation: A power plan is a collection of hardware and system settings that manages how your computer uses power. Power plans can help you save energy, maximize system performance, or achieve a balance between the two. All users (standard and administrator) will be able to make changes to any power plan settings.

Changes made to a power plan will affect all users that have chosen the same power plans their default active power scheme.

Windows 10 offers several power plans to help you manage how your device uses power. The different power settings can help you to control system performance, conserve battery life or both.

By default, Windows 10 comes with three power plans:

Balanced – the best plan for most users. This option automatically balances system performance and energy usage by adjusting to full performance when you need it and power-saving mode when you don't.

High performance – the best plan for maximizing screen brightness and increasing system performance. It uses more energy, however, so it will drain your battery the fastest.

Power saver – the best plan to extend your battery life. This option saves energy by reducing computer performance and screen brightness to give you the most juice from your current battery charge.

<https://www.tenforums.com/tutorials/2843-change-power-plan-settings-windows-10-a.html>

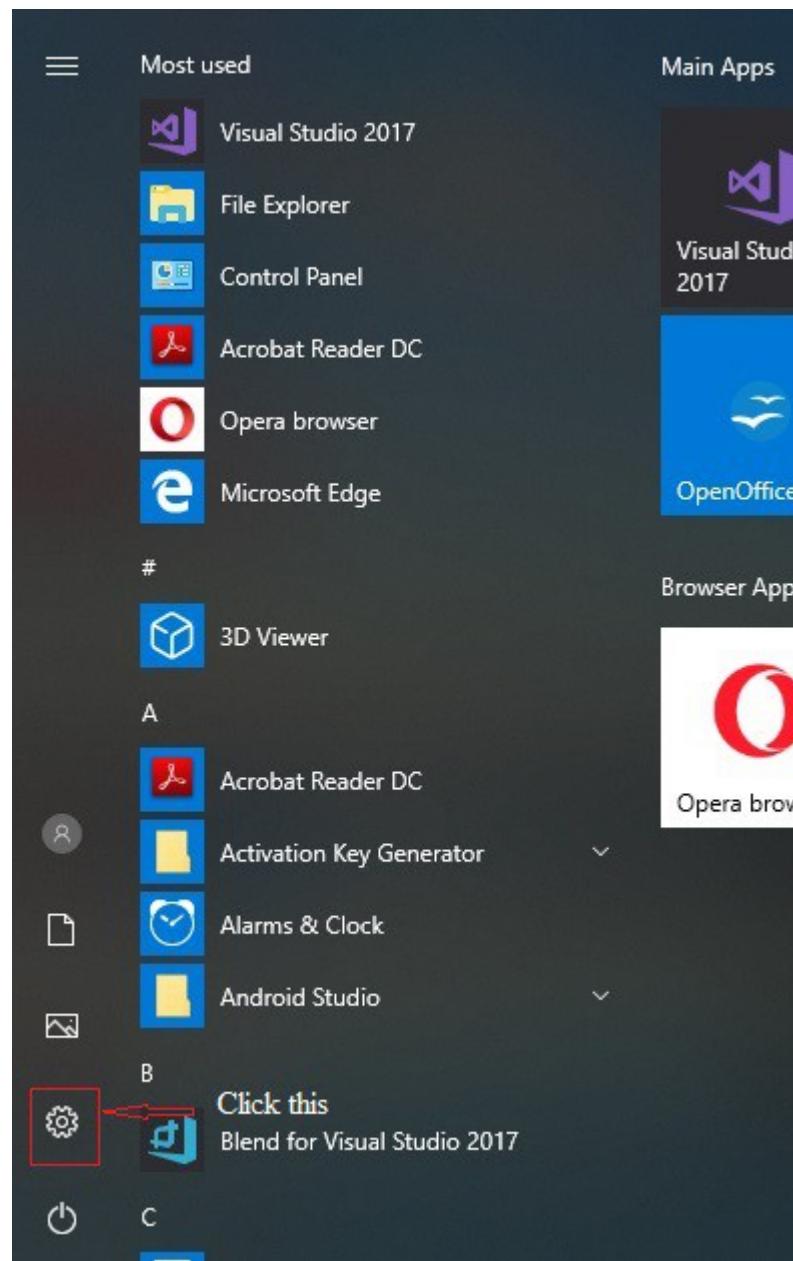
[Back](#)

5.25 Creating new user account in Windows 10

Description: The lab exercise explains how to create a new local user account in windows 10 OS. Here, you create a new user account with user name as “Test” and password as “pass”

Instructions:

1. In the give simulator start menu click **settings**



2. In the Settings window, click **Accounts** icon.

Simulation Note that only a few links are made active

Windows Settings

Find a setting

Phone
Link your Android, iPhone

Network & Internet
Wi-Fi, airplane mode, VPN

Personalization
Background, lock screen, colors

Click this

Accounts
Your accounts, email, sync, work, family

Apps
Uninstall, defaults, optional features

Time & Language
Speech, region, date

Gaming
Game bar, DVR, broadcasting, Game Mode

Ease of Access
Narrator, magnifier, high contrast

3. Select “Family & other people” from the left side.

[←](#) Settings

Simulation

Note that only a few links are made active

— □ ×

Home

Find a setting 

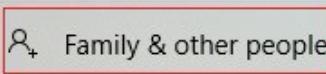
Accounts

Your info

Email & app accounts

Sign-in options

Access work or school

Family & other people   Click this

Sync your settings

Your info



ANANDSOFT

Local Account
Administrator

Windows is better when your settings and files automatically sync.
Use a Microsoft account to access all your stuff on all your devices
easily.

[Sign in with a Microsoft account instead](#)

Create your picture



Camera

4. Then click on “**Add someone else to this PC**”. It will be located under Other people on the right side.



Settings

Simulation

Note that only a few links are made active



Home

Find a setting

Accounts

Your info

Email & app accounts

Sign-in options

Access work or school

Family & other people

Sync your settings

Family & other people

Your family

Add your family so everybody gets their own sign-in and desktop. You can help kids stay safe with appropriate websites, time limits, apps, and games.



Add a family member

[Learn more](#)

Other people

Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family.



Add someone else to this PC

← Click this

[Set up assigned access](#)

4. Here, click on “I don’t have this person’s sign-in information”.

How will this person sign in?

Enter the email address or phone number of the person you want to add. If they use Windows, Office, Outlook.com, OneDrive, Skype, or Xbox, enter the email or phone number they use to sign in.

I don't have this person's sign-in information  Click this

[Privacy statement](#)

[Next](#)

[Cancel](#)

5. On the Let's create your account screen, select “**Add a user without a Microsoft account**”.

Simulation

Note that only a few links are made active

Let's create your account

Windows, Office, Outlook.com, OneDrive, Skype, Xbox. They're all better and more personal when you sign in with your Microsoft account.* [Learn more](#)

[Get a new email address](#) 

*If you already use a Microsoft service, go [Back](#) to sign in with that account.

[Add a user without a Microsoft account](#)  Click this

[Back](#)[Next](#)

6. In this step, fill the Username as “**Test**”, Password as “**pass**” and Re-enter password as “**pass**” for the new user account. now, click on **Next** button.

Simulation

Note that only a few links are made active

Create an account for this PC

If you want to use a password, choose something that will be easy for you to remember but hard for others to guess.

Who's going to use this PC?

Enter your user name.

Make it secure.

[Next](#)[Back](#)

7. After clicking “Next”, you’re back to the Accounts screen a new user account should now be listed.

Click close button to close the settings.

Other people

— 
Click this close
the settings

Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family.



Add someone else to this PC



Test

Local account

[Set up assigned access](#)

<https://merabheja.com/how-to-create-a-new-user-account-in-windows-10/>

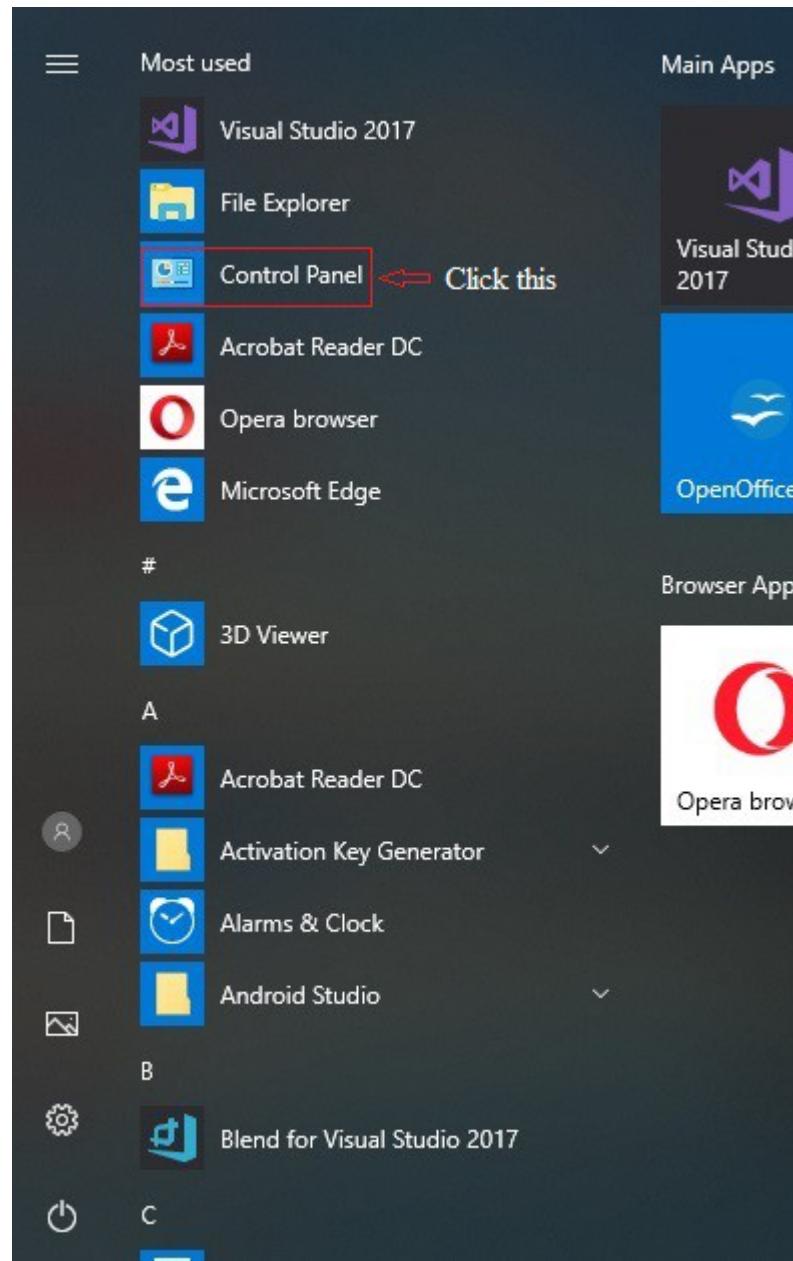
[Back](#)

5.26 Changing user account control settings in Windows 10

Description: The lab exercise explains how to change user account control settings on windows 10 OS. Here, you change the user account control settings from “Never Notify” to “Notify”

Instructions:

1. In the given start menu click **control panel**



2. In the control panel window click “System and Security”

< → ⏪ ⏩ Control Panel >

View by: Category ▾

Adjust your computer's settings

**System and Security**  Click this

Review your computer's status
Save backup copies of your files with File History
Back up and Restore (Windows 7)

**Network and Internet**

View network status and tasks

**Hardware and Sound**

View devices and printers
Add a device
Adjust commonly used mobility settings

**Programs**

Uninstall a program

**User Accounts**

Change account type

**Appearance and Personalisation****Clock and Region**

Change date, time or number formats

**Ease of Access**

Let Windows suggest settings
Optimise visual display

3. Under System and Security window click “Security and Maintenance”

System and Security **Simulation** Note that only a few links are made active

< → ⏪ ⏩ Control Panel > System and Security Search Control Panel

Control Panel Home

- **System and Security**
- Network and Internet
- Hardware and Sound
- Programs
- User Accounts and Family Safety
- Appearance and Personalization
- Clock, Language, and Region
- Ease of Access

Security and Maintenance  Click this

Security and Maintenance

Review your computer's status and resolve issues |
 Change User Account Control settings |
 Troubleshoot common computer problems

Windows Firewall

Check firewall status | Allow an app through Windows Firewall

System

View amount of RAM and processor speed |
 Allow remote access | Launch remote assistance |
 See the name of this computer

Power Options

Require a password when the computer wakes |
 Change what the power buttons do |
 Change when the computer sleeps

File History

Save backup copies of your files with File History |
 Restore your files with File History

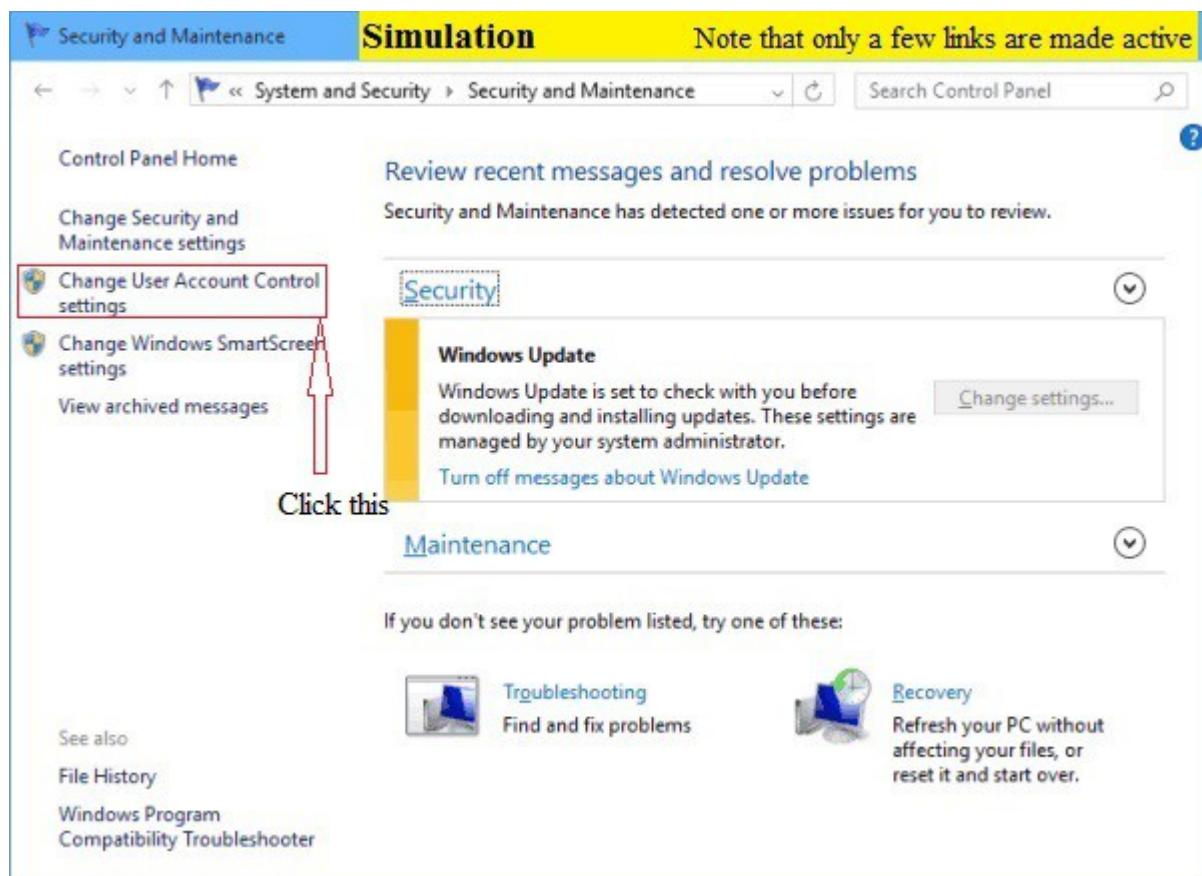
BitLocker Drive Encryption

Manage BitLocker

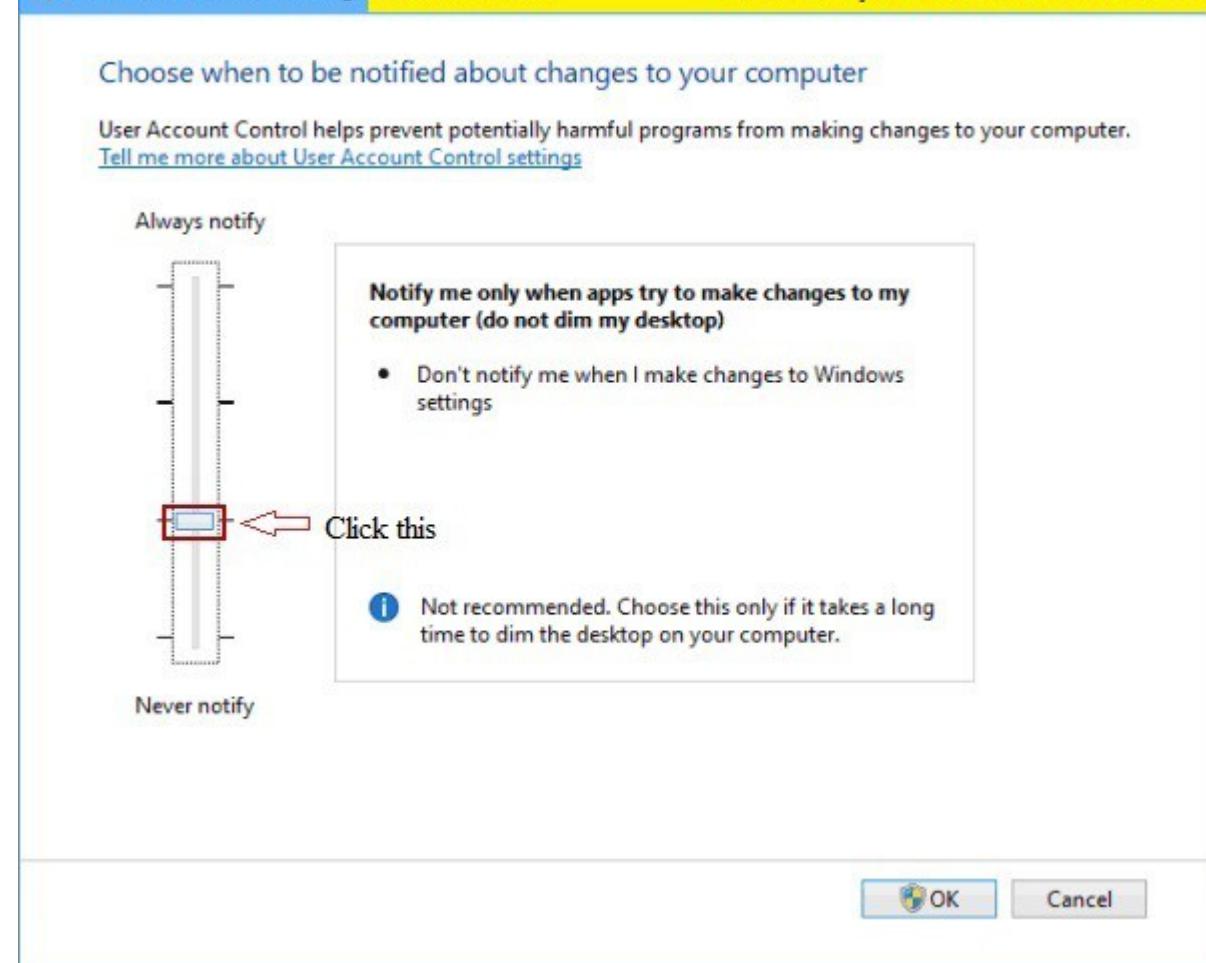
Storage Spaces

Manage Storage Spaces

4. Tap “Change User Account Control settings” on the left to continue.



5. Move the scale up or down to choose when to be notified about changes to your computer, in this lab click “Notify” and click OK button.



Explanation: User Account Control notifies you when potentially harmful programs try to make changes to your PC, and you can choose when to be notified about changes to your computer through changing its settings

1. By default, User Account Control will notify you only when apps try to make changes to your computer. And this setting is recommended if you use familiar apps and visit familiar websites, referring to the picture above.
2. If you move the scale to the top to select Always notify, you will be notified when apps try to install software or make changes to your PC and when you make changes to Windows settings. BTW, the setting is recommended if you routinely install new software and visit unfamiliar websites.
3. You can move the scale to choose the third option to ask User Account Control not to dim your desktop when notifying you about apps' up-coming changes to your computer if it takes a long time to dim the desktop.
4. Supposing that you don't want to be notified when apps try to install software and make changes to your PC and when you make changes to Windows settings, move the scale to the bottom to choose Never notify.

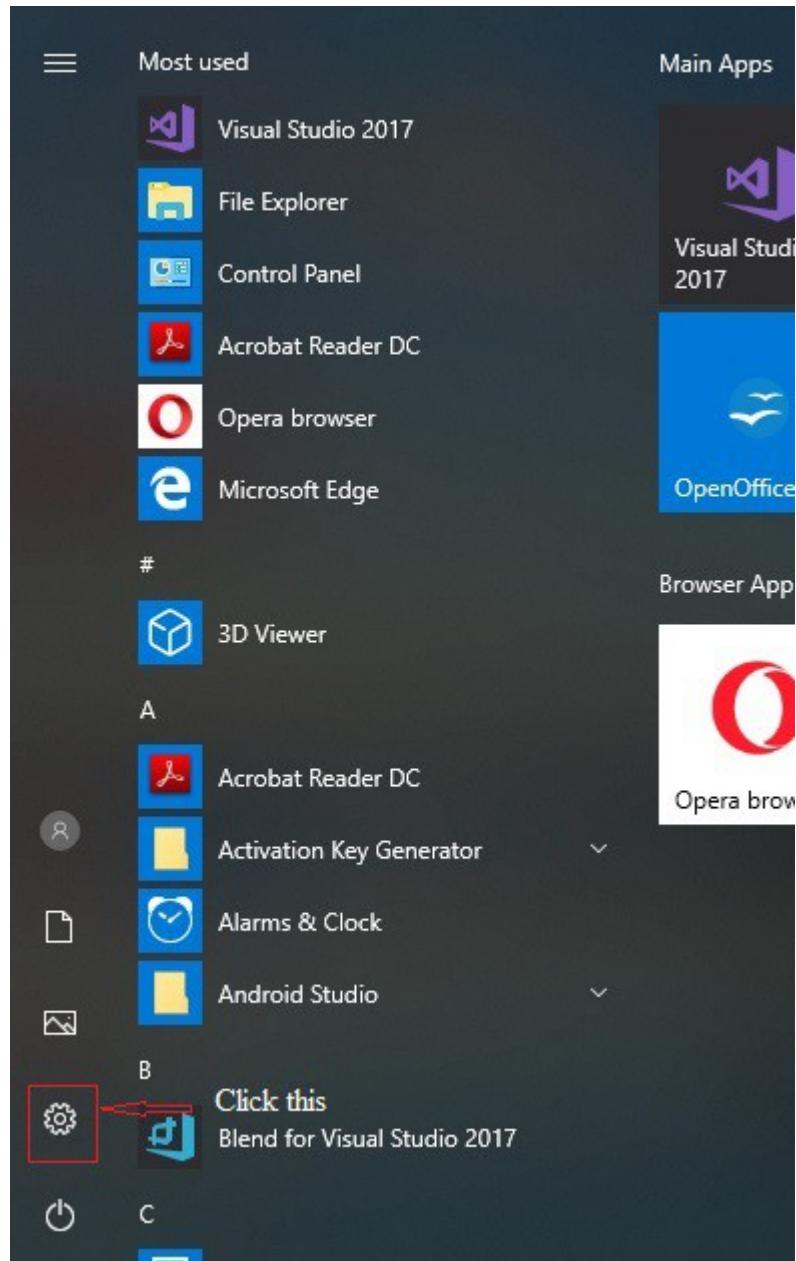
[Back](#)

5.27 Changing user account password in Windows 10

Description: The lab exercise explains how to change user account password in windows 10 computer. Here you change the user account password from “aplussim” to “apluslabsim”.

Instructions:

1. Click **settings** in a given start menu window.



2. Click “Accounts” icon from settings app

Simulation

Note that only a few links are made active

Windows Settings

Find a setting



Phone

Link your Android, iPhone



Network & Internet

Wi-Fi, airplane mode, VPN



Personalization

Background, lock screen, colors

Click this



Accounts

Your accounts, email, sync, work, family



Apps

Uninstall, defaults, optional features



Time & Language

Speech, region, date



Gaming

Game bar, DVR, broadcasting, Game Mode



Ease of Access

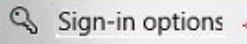
Narrator, magnifier, high contrast

3. Choose the “Sign-in Options” link from the Accounts window’s left edge.

Find a setting **Accounts**

Your info

Email & app accounts

Sign-in options   Click this

Access work or school

Family & other people

Sync your settings

Your info**ANANDSOFT**Local Account
Administrator

Windows is better when your settings and files automatically sync.
Use a Microsoft account to access all your stuff on all your devices
easily.

[Sign in with a Microsoft account instead](#)[Create your picture](#)

4. In the Password section on the window's right side, click the “Change” button.

← Settings

Simulation

Note that only a few links are made active

Home

Find a setting

Accounts

Your info

Email & app accounts

Sign-in options

Access work or school

Family & other people

Sync your settings

Sign-in options

Require sign-in

If you've been away, when should Windows require you to sign in again?

When PC wakes up from sleep

Windows Hello

Sign in to Windows, apps and services by teaching Windows to recognise you.

Windows Hello isn't available on this device.

See how it works and find compatible devices.

Password

Change your account password

Change

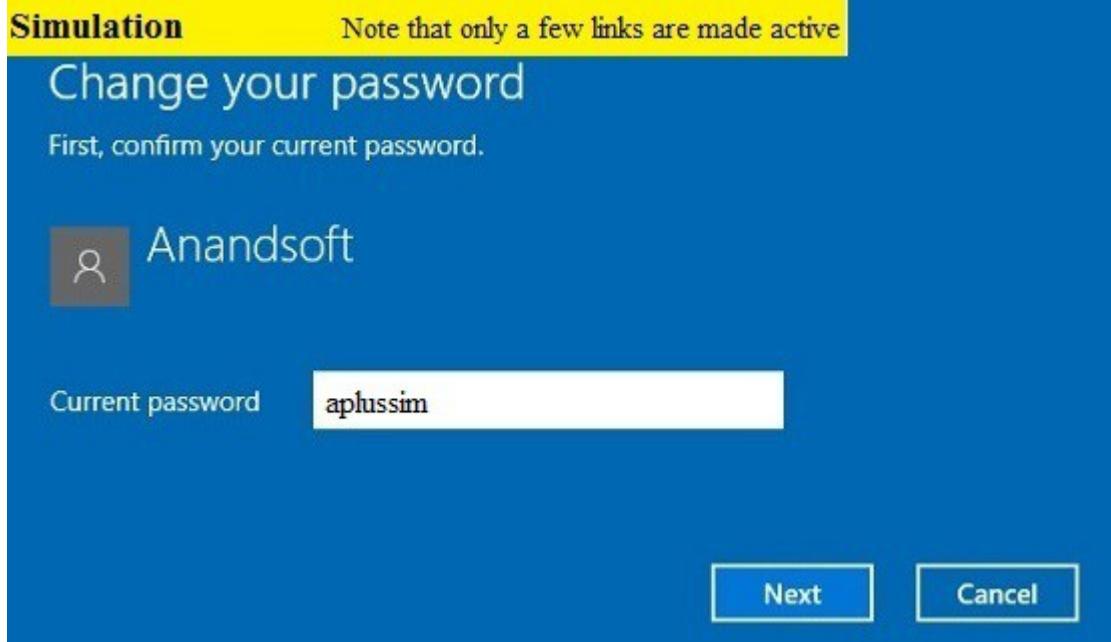
Click this

Update your security questions

PIN

Create a PIN to use in place of passwords. You'll be asked for this PIN when you sign in to Windows, apps and services.

5. In change your password window enter the current password as “aplussim” and click Next button



6. In the next Change your password screen enter New password as “apluslabsim” and retype the same password in Re-enter Password box and click Next.



Explanation: Microsoft account holders can change their passwords online. Local account holders can create or change a password as explained in this exercise.

[Back](#)

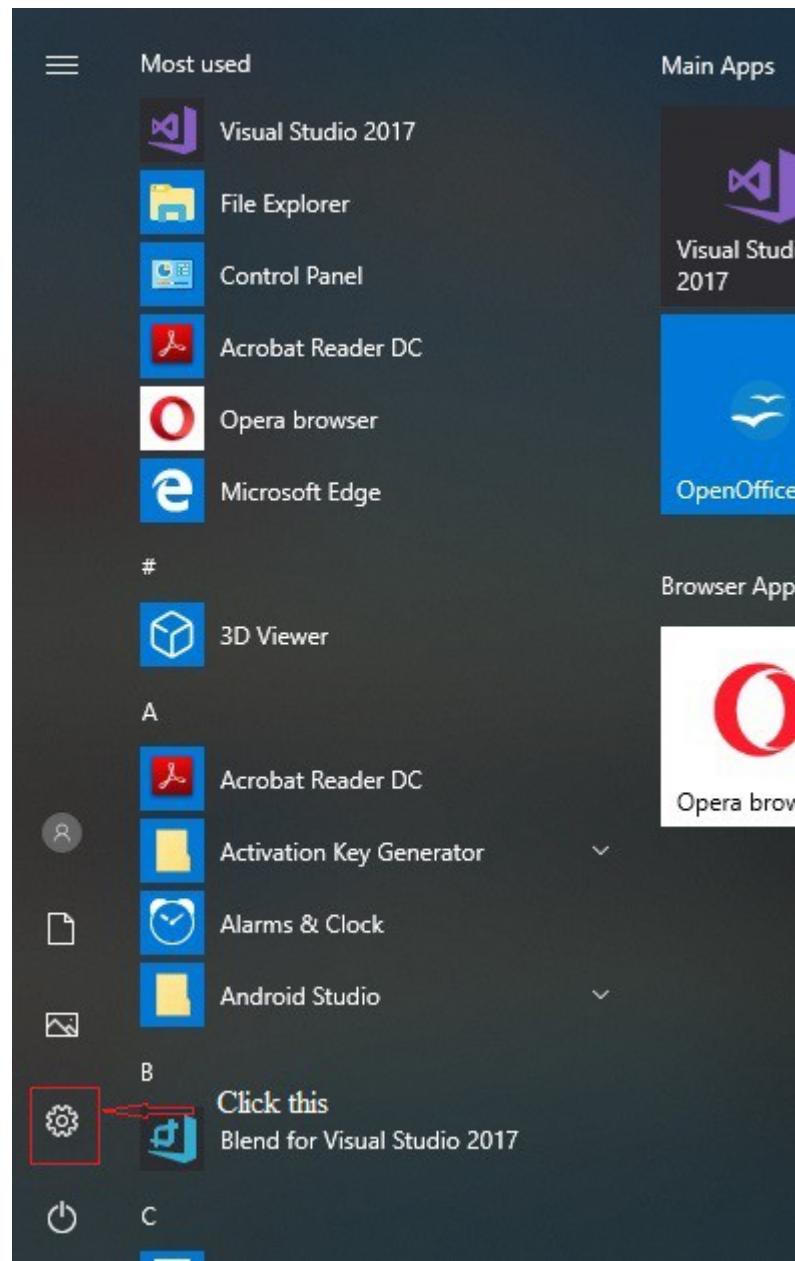
5.28 Removing user account in Windows 10

Description: The lab exercise explains how to delete/remove existing user accounts from windows

10 OS. Here, you delete a user account named “Test”.

Instructions:

1. In the given simulator start menu click **settings**.



2. Click “Accounts” icon from settings app.

Simulation

Note that only a few links are made active

Windows Settings

 **Phone**

Link your Android, iPhone

**Network & Internet**

Wi-Fi, airplane mode, VPN

**Personalization**

Background, lock screen, colors

Click this

**Accounts**

Your accounts, email, sync, work, family

**Apps**

Uninstall, defaults, optional features

**Time & Language**

Speech, region, date

**Gaming**

Game bar, DVR, broadcasting, Game Mode

**Ease of Access**

Narrator, magnifier, high contrast

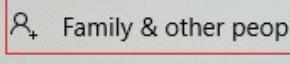
3. From the left-side menu, click “**Family & other people**”

← Settings **Simulation** Note that only a few links are made active — □ ×

Home

Find a setting

Accounts

- Your info
- Email & app accounts
- Sign-in options
- Access work or school
- Family & other people**  Click this
- Sync your settings

Your info



ANANDSOFT
Local Account
Administrator

Windows is better when your settings and files automatically sync.
Use a Microsoft account to access all your stuff on all your devices easily.

[Sign in with a Microsoft account instead](#)

Create your picture



Camera

4. This will take you to your family members associated with your Microsoft account with or without an account on your PC, as well as other users that aren't in your Microsoft family list who have their own login credentials. In this simulator lab select the user "**Test**" and hit **remove**

← Settings

Simulation Note that only a few links are made active

Home

Find a setting

Accounts

- Your info
- Email & app accounts
- Sign-in options
- Access work or school
- Family & other people**
- Sync your settings

Family & other people

Your family

Sign in with a Microsoft account to see your family here or add any new members to your family. Family members get their own sign-in and desktop. You can help kids to stay safe with appropriate websites, time limits, apps and games.

[Sign in with a Microsoft account](#)

Other people

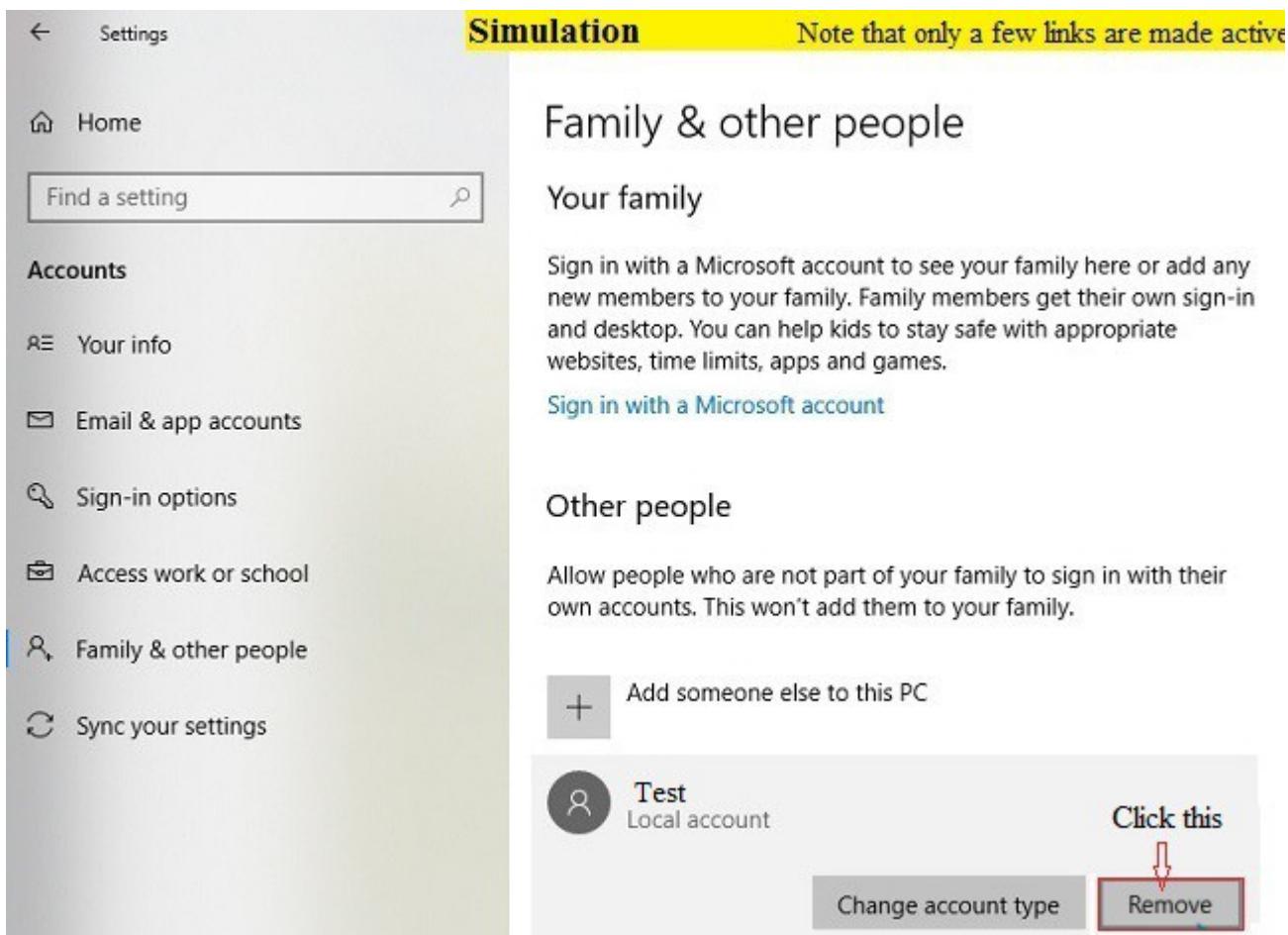
Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family.

+ Add someone else to this PC

 Test Local account

Click this

Change account type Remove



5. To make sure you're certain you want to remove the account and all of its files, apps, and settings, Windows will display a pop-up window to ask you to verify your intent on removing the user. Click **“Delete account and data”**. The account will be removed, and all offline files and apps will be removed from the device .

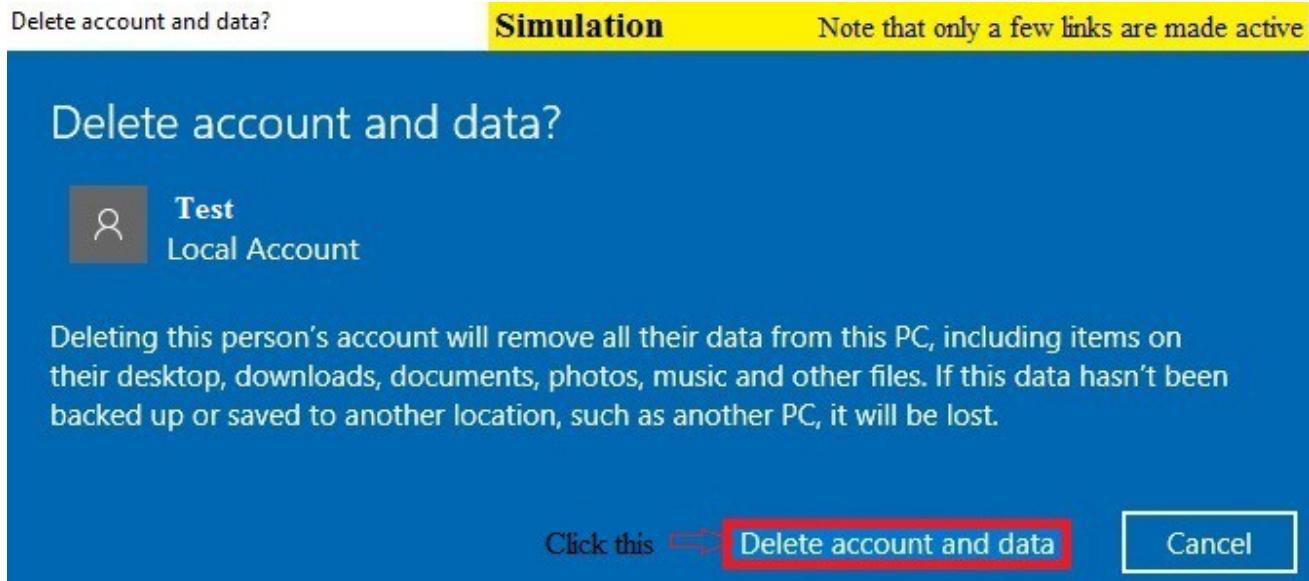
Delete account and data?

Simulation Note that only a few links are made active

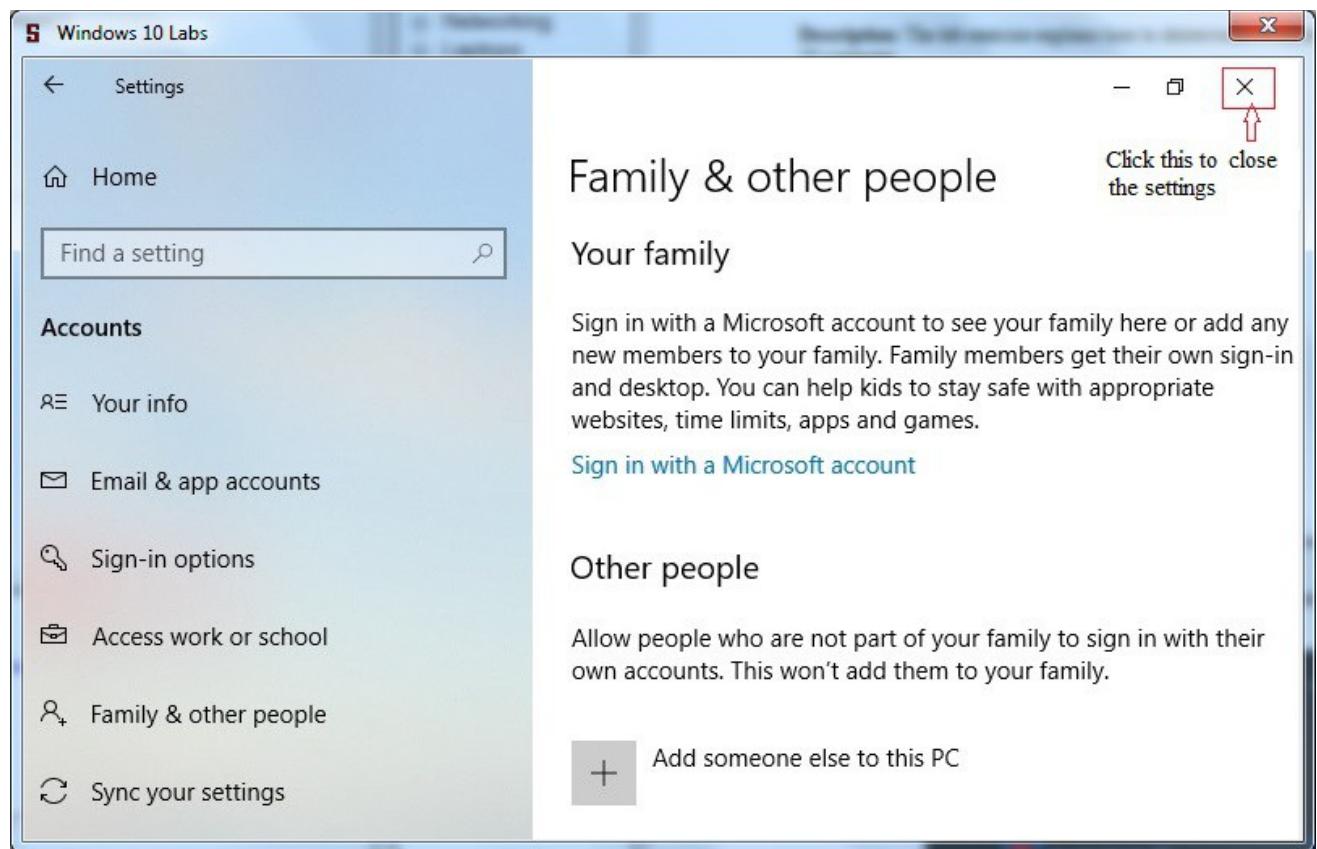
 Test Local Account

Deleting this person's account will remove all their data from this PC, including items on their desktop, downloads, documents, photos, music and other files. If this data hasn't been backed up or saved to another location, such as another PC, it will be lost.

Click this  **Delete account and data** Cancel



6. After this you will be back to Accounts screen where Test account has been removed , close the settings.



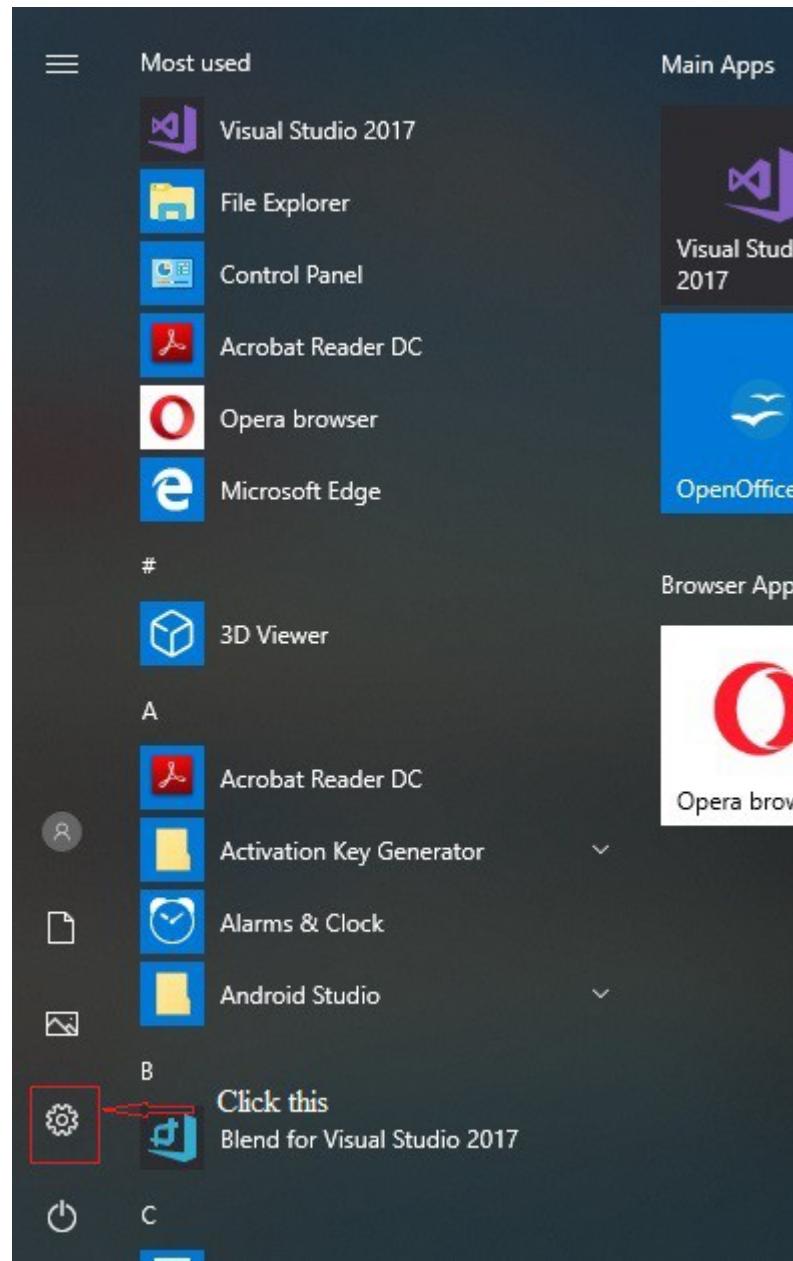
[Back](#)

5.29 Changing user account type in Windows 10

Description: The lab exercise explains how to change user account type in windows 10 OS. Here, you change the user account type from “Standard” to “Administrator”.

Instructions:

1. In the given start menu click **settings**



2. Click “**Accounts**” icon in the settings app

Simulation

Note that only a few links are made active

Windows Settings

Find a setting



Phone

Link your Android, iPhone



Network & Internet

Wi-Fi, airplane mode, VPN



Personalization

Background, lock screen, colors

Click this



Accounts

Your accounts, email, sync, work, family



Apps

Uninstall, defaults, optional features



Time & Language

Speech, region, date



Gaming

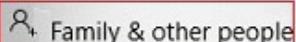
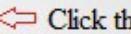
Game bar, DVR, broadcasting, Game Mode



Ease of Access

Narrator, magnifier, high contrast

3. Select “**Family and other people**” from the list on the left.

[Home](#) **Accounts**[Your info](#)[Email & app accounts](#)[Sign-in options](#)[Access work or school](#)[Family & other people](#)   Click this[Sync your settings](#)**Your info****ANANDSOFT**

Local Account

Administrator

Windows is better when your settings and files automatically sync.
Use a Microsoft account to access all your stuff on all your devices
easily.

[Sign in with a Microsoft account instead](#)**Create your picture**

Camera

4. Click on the account you want to change the type of from the right , here select “Test” and click “Change account type”

← Settings

Simulation Note that only a few links are made active

Home

Find a setting

Accounts

Your info

Email & app accounts

Sign-in options

Access work or school

Family & other people

Sync your settings

Family & other people

Your family

Sign in with a Microsoft account

Other people

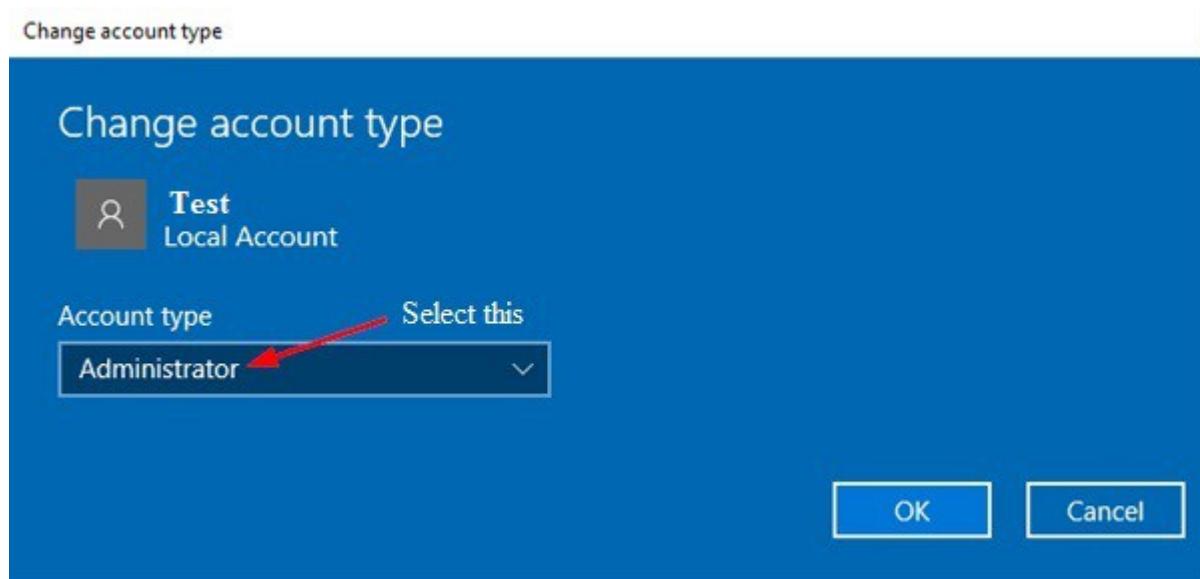
Add someone else to this PC

+ Test Local account

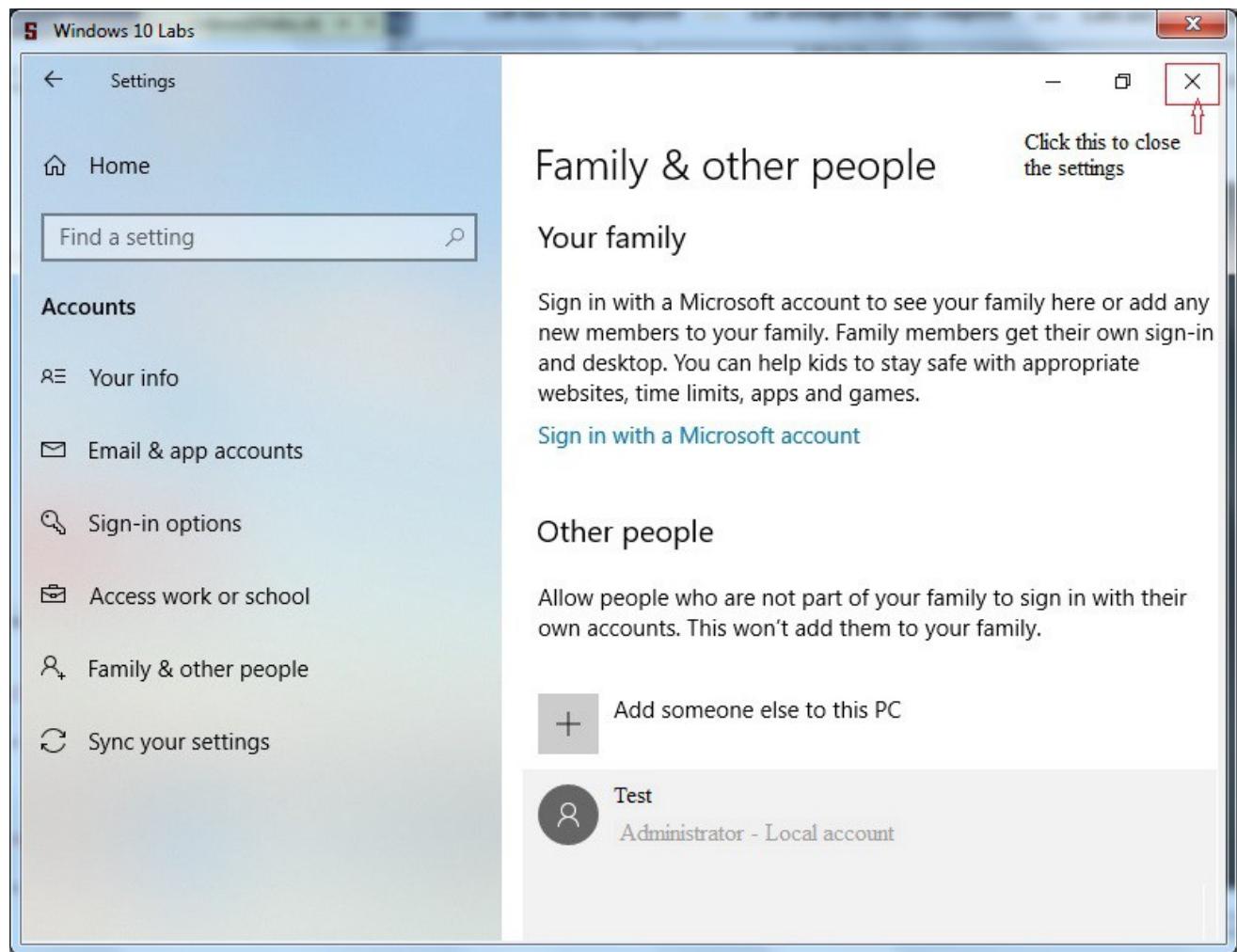
Click this step:1
Click this step: 2

Change account type Remove

5. In the Change Account type screen select “Administrator” from the drop-down menu and click OK button to complete the task.



6. After clicking “Next”, you’re back to the Accounts screen ,user account type has been changed to Administrator ,click close button to close the settings.



Explanation: Other ways to change user account type is explained below

1. Change a user account type on Control Panel

1. One of the great things about Windows is being able to accomplish the same task in a number of different ways.
2. If you're looking to change an account type using Control Panel, then you can use the following steps:
 3. Use the Windows key + X keyboard shortcut to open the Power User menu and select Control Panel.
 4. Click Change account type.
 5. Click the user account you want to change.
 6. Click Change the account type.
 7. Select Standard or Administrator.

8. Click the Change Account Type button to complete the task.

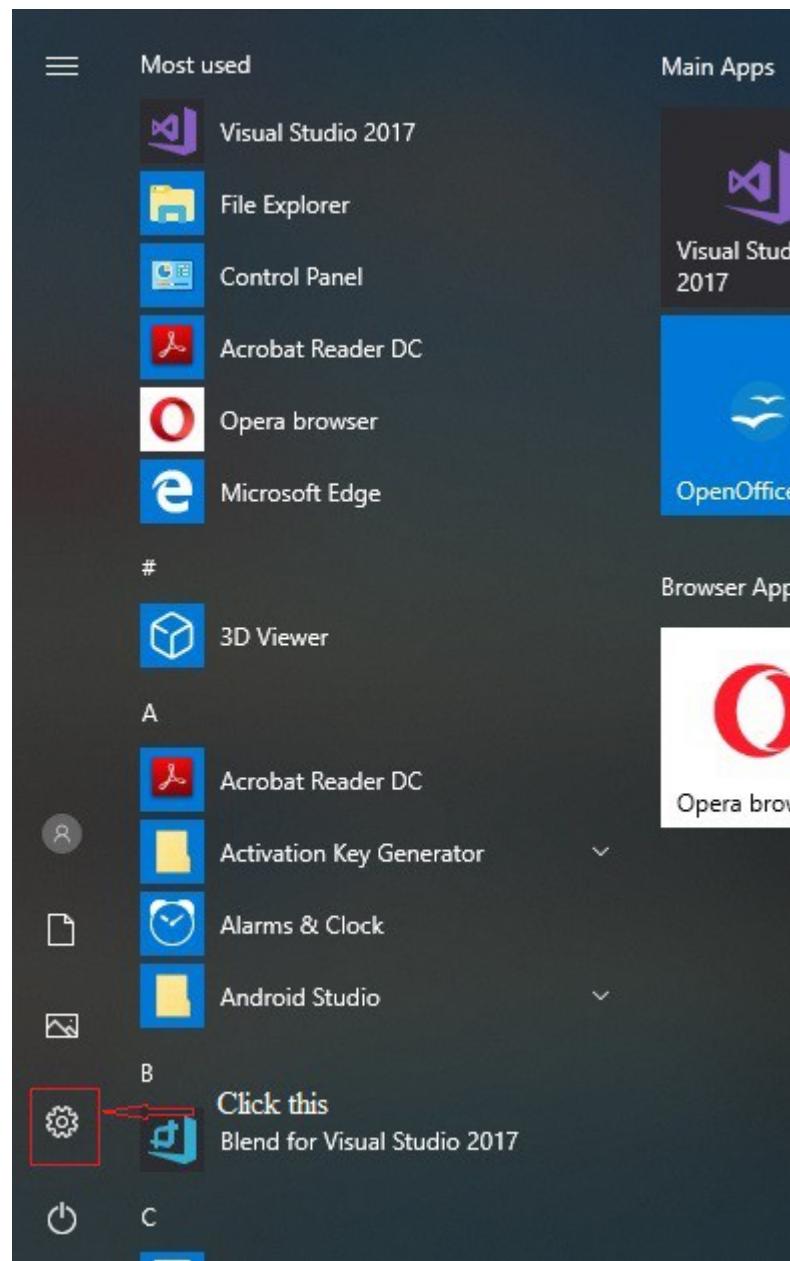
[Back](#)

5.30 Creating a system image backup of Windows 10

Description: The lab exercise explains how to create a system image backup of Windows 10 computer. Here, you are storing the image backup in “E:” drive.

Instructions:

1. In the given simulator start menu click “control panel”



2. In the control panel window click “System and Security”

Control Panel **Simulation** Note that only a few links are made active

← → ⏪ ⏩ Control Panel >

View by: Category ▾

Adjust your computer's settings



System and Security  Click this

Review your computer's status
Save backup copies of your files with File History
Back up and Restore (Windows 7)



Network and Internet

View network status and tasks



Hardware and Sound

View devices and printers
Add a device
Adjust commonly used mobility settings



Programs

Uninstall a program



User Accounts

 Change account type



Appearance and Personalisation



Clock and Region

Change date, time or number formats



Ease of Access

Let Windows suggest settings
Optimise visual display

3. Click on “Backup and Restore (Windows 7)”.

Control Panel\System and Security

← → ⏪ ⏩ Control Panel > System and Security >

Control Panel Home

• **System and Security**

Network and Internet

Hardware and Sound

Programs

User Accounts

Appearance and Personalisation

Clock and Region

Ease of Access



Security and Maintenance

Review your computer's status and resolve issues |  Change User Account Control settings | Troubleshoot common computer problems



Windows Defender Firewall

Check firewall status | Allow an app through Windows Firewall



System

View amount of RAM and processor speed |  Allow remote access | Launch remote assistance | See the name of this computer



Power Options

Change battery settings | Change what the power buttons do | Change when the computer sleeps



File History

Save backup copies of your files with File History | Restore your files with File History



Back up and Restore (Windows 7)  Click this

Back up and Restore (Windows 7) | Restore files from backup



Storage Spaces

Manage Storage Spaces



Work Folders

Manage Work Folders



Administrative Tools

Free up disk space | Defragment and optimise your drives |  Create and format hard disk partitions |  View event logs |  Schedule tasks

4. On the left pane of the next screen , click the “Create a system image link”.



See also

[Security and Maintenance](#)

[File History](#)

5. Under "Where do you want to save the backup? Under **On a hard disk** option select “E” drive from drop-down menu as storage to save the back up and click Next button.

Simulation

Note that only a few links are made active

X

← Create a system image

Where do you want to save the backup?

A system image is a copy of the drives required for Windows to run. It can also include additional drives. A system image can be used to restore your computer if your hard drive or computer ever stops working; however, you can't select individual items to restore.

On a hard disk  Click this

 New Volume (E:) 90.77 GB free  Select this

 The drive selected is on the same physical disk that is being backed up. If this disk fails, you will lose your backups.

On one or more DVDs

 DVD RW Drive (D:)

On a network location

 Select...

Next

Cancel

6. Click the “Start backup” button in the next screen.

Once you completed these steps, the wizard will proceed to create a full backup of your system, including everything that is stored on the main drive, as well as the system reserved partition.

[Create a system image](#)

Confirm your backup settings

Backup location:

New Volume (E:)

The backup could take up to 88 GB of disk space.

The following drives will be backed up:

- System Reserved (System)
- (C:) (System)
- Windows Recovery Environment (System)

[Start backup](#)[Cancel](#)

Explanation: While you can store the backup on a secondary drive, network location, and even use blank DVDs, it's best to connect to external storage, which you can quickly disconnect and store in a safe place.

To create a full backup using Windows 10's system image tool, you need to connect external storage with enough available space and then use these steps

During the backup process, Windows 10 will also use Shadow Copy, a technology that allows you to create a backup while files are still in use, which means that you can continue to work normally as the image is being created.

https://www.windowscentral.com/how-make-full-backup-windows-10#create_system_image_windows10

[Back](#)

5.31 Setting up and uploading files to OneDrive in Windows 10

Description: OneDrive is a file hosting service and synchronization service operated by Microsoft as part of its web version of Office. With OneDrive, you can sync files between your computer and the cloud, so you can get your files from anywhere - your computer, your mobile device, and even through the OneDrive website at OneDrive.com. If you add, change, or delete a file or folder in your OneDrive folder, the file or folder is added, changed, or deleted on the OneDrive website and vice versa. You can work with your synced files directly in File Explorer and access your files even when you're offline. Whenever you're online, any changes that you or others make will sync automatically.

This lab exercise demonstrates how to set up OneDrive and upload files to OneDrive in Windows 10.

Here, we do the following:

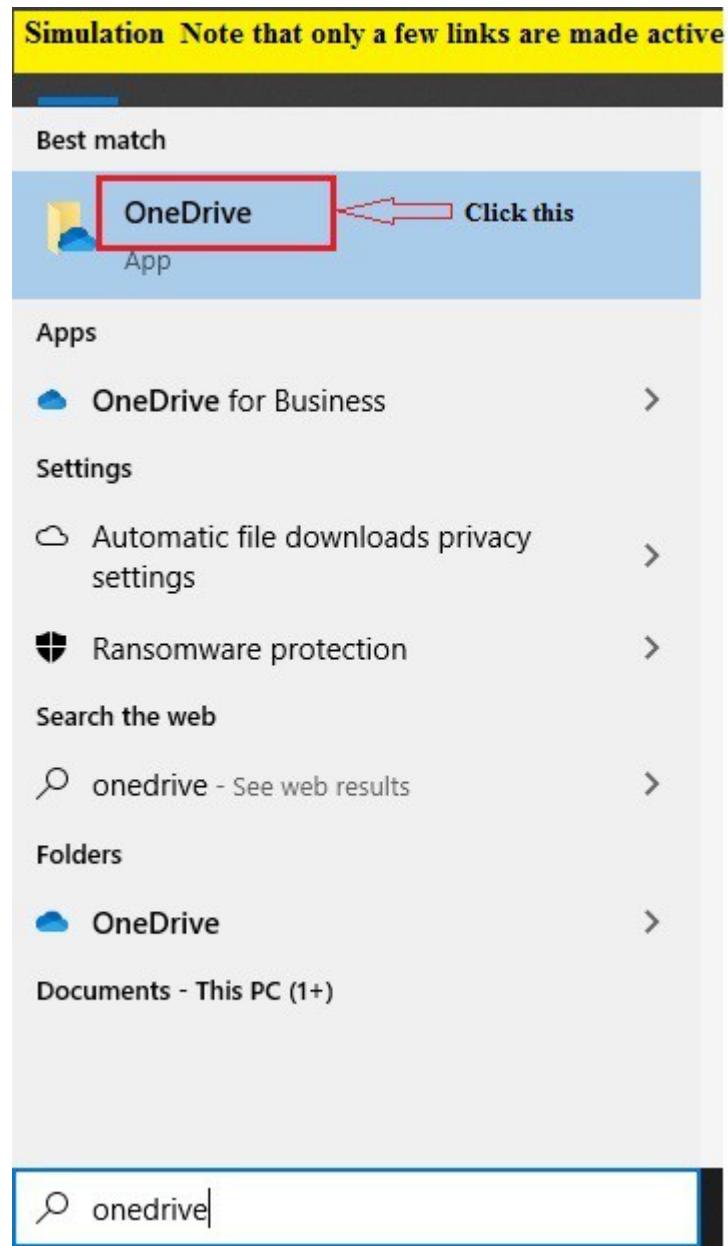
1. Login to the OneDrive account and setup.
2. Copy a folder “ccnalabs” in local “E” drive to be in sync with OneDrive folder on the web.
The contents of the folder E://ccnalabs are automatically copied to the OneDrive and synced.

Note: It has been assumed that you have already downloaded and installed OneDrive app from the corresponding Microsoft website, <https://www.microsoft.com/en-us/microsoft-365/onedrive/download>

Instructions:

Task1: Setting up OneDrive in Windows 10

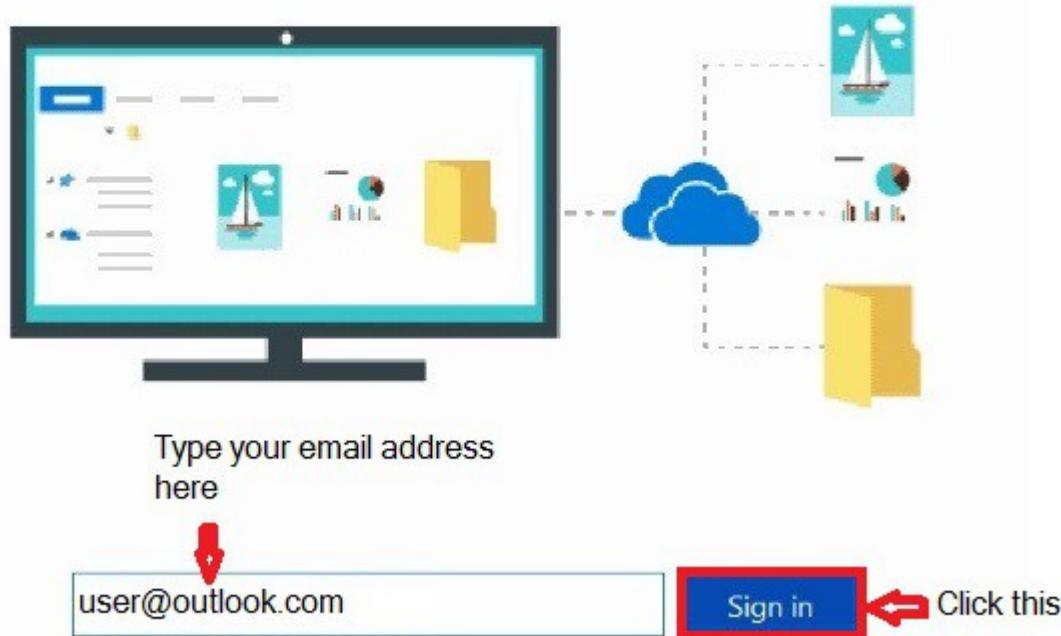
1. In this lab exercise we assume that OneDrive app is already installed in your Windows 10 system.
2. To access the OneDrive , in a given simulation Start Menu  click OneDrive. (Type OneDrive in the searchbox of your Windows 10 system).



3. Set up the OneDrive window appears, enter email address as "user@outlook.com" and click on the **Sign in** button.

Set up OneDrive

Put your files in OneDrive to get them from any device.



Clicking "Sign in" means you agree to the Microsoft [Services Agreement](#) and [privacy statement](#). OneDrive may also download and install its updates automatically.

4. Next, you will be prompted for password, enter your Microsoft account password as “pass” and click **Sign in** button.

That signs you into OneDrive account and syncs it to your PC. The signing-in process might take a couple of minutes in the actual system. Afterward, proceed to set up the newly-added OneDrive.

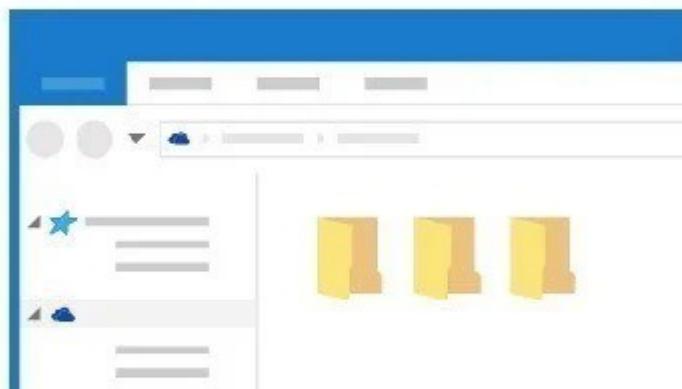


That signs you into OneDrive account and syncs it to your PC. The signing-in process might take a couple of minutes in the actual system. Afterward, proceed to set up the newly-added OneDrive.

Windows will show you the folder location of the new OneDrive account and other information. You can tap the **Change location** button if you want to modify the default folder of the new OneDrive account.

This is your OneDrive folder

Add files here so you can access them from other devices and still have them on this PC.



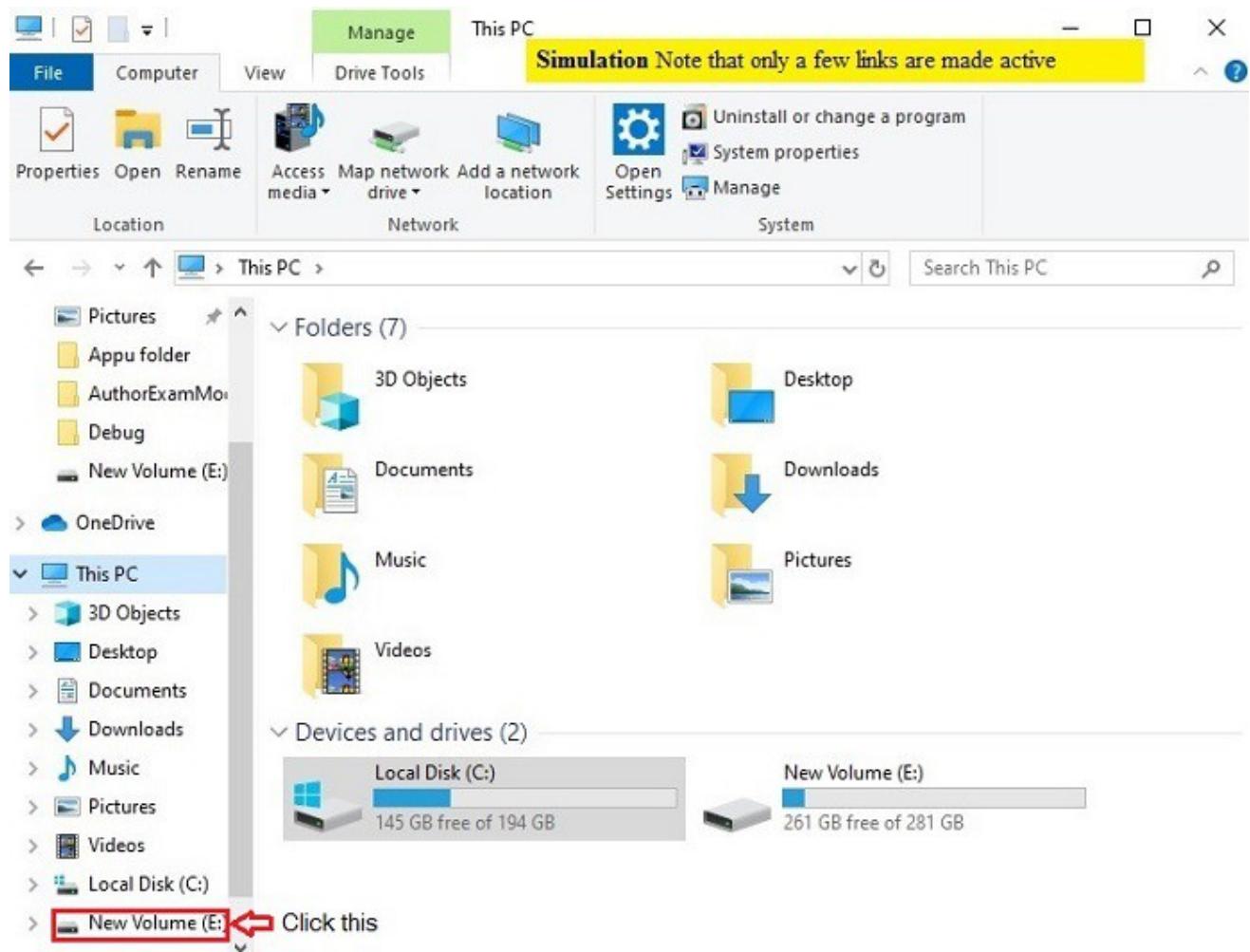
Next

Click this

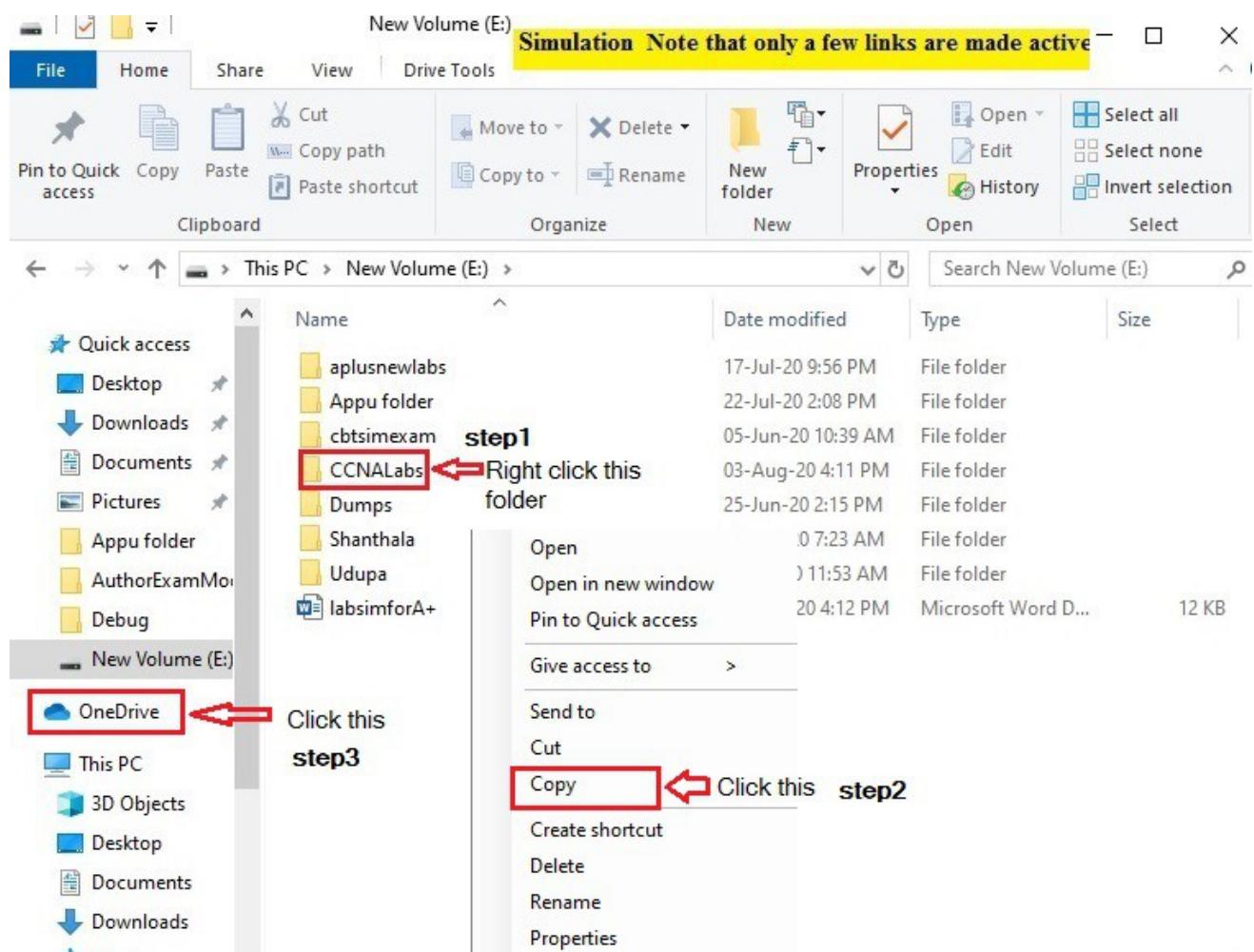
5. Click Next button to proceed.

Task2: Uploading files to OneDrive

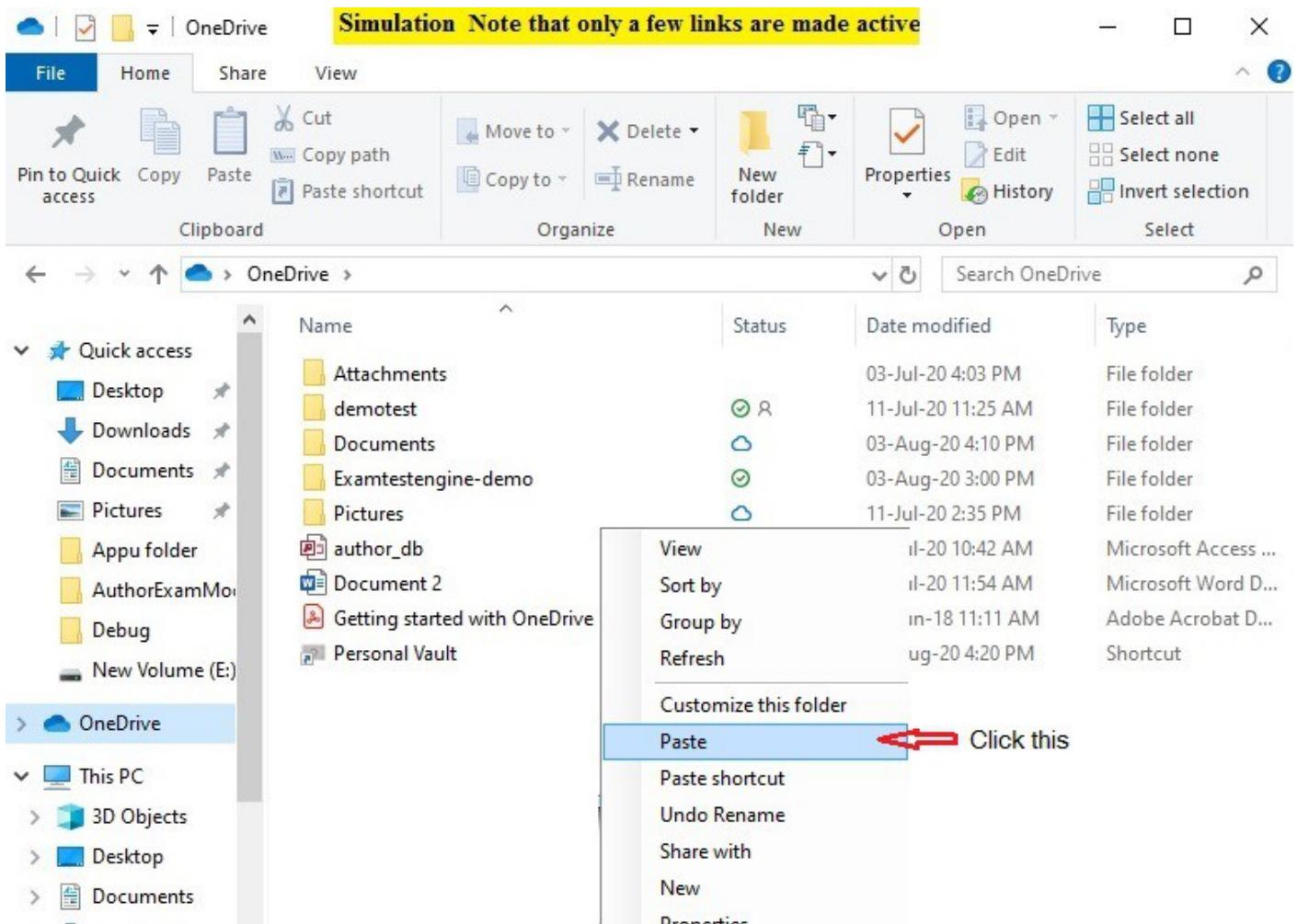
6. In the given Windows 10 File Explorer click E drive.



7. Right click the folder "ccnalabs" , a popup menu appears click Copy. To paste this to OneDrive, click OneDrive folder using leftpane.



8. In the OneDrive folder location right click a popup menu appears click Paste option.



9. The file will be copied to OneDrive folder. Click the Close button to complete the lab.

Explanation: OneDrive is Microsoft's cloud service for storing and sharing files. You can store business documents, presentations, pictures, videos, your personal folders and many other types of items. You can share anything from *OneDrive* using the *OneDrive* app for Windows, iOS, Android and so on.

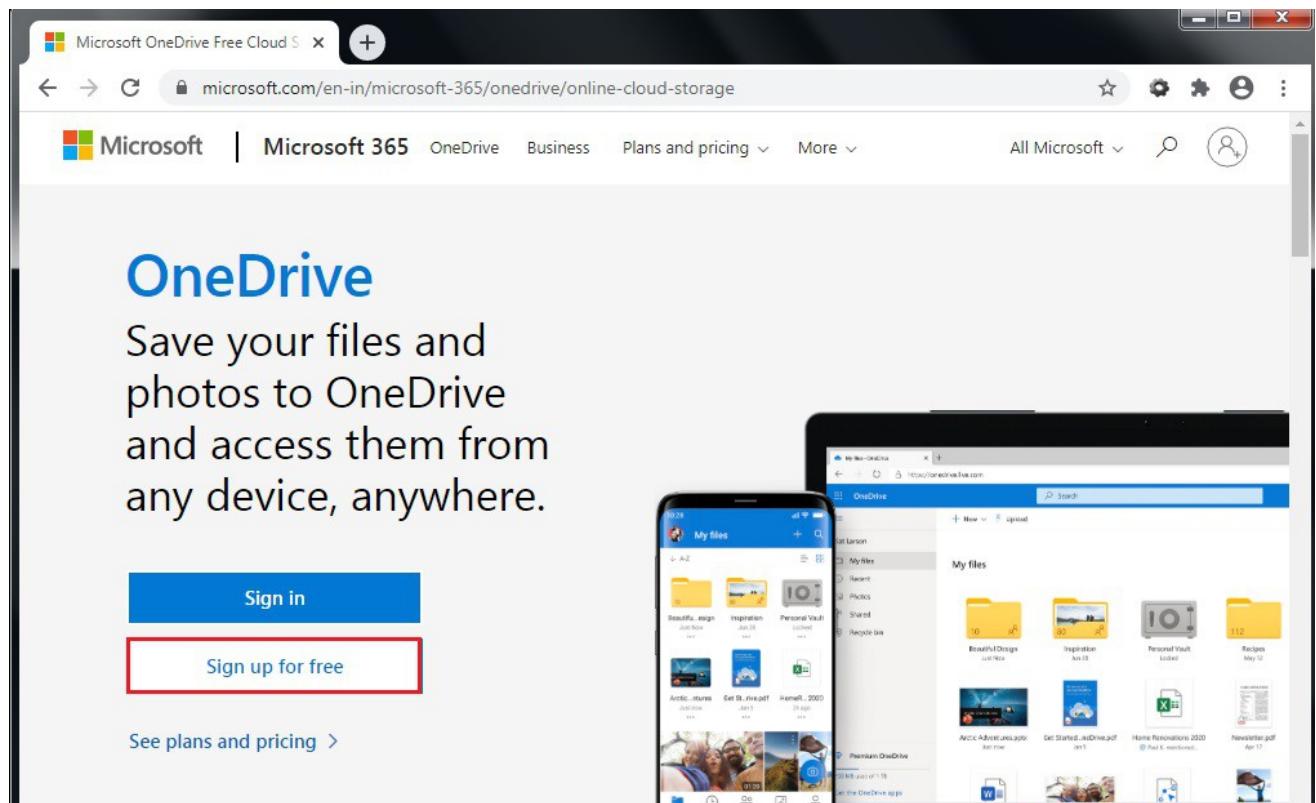
You can house your files in the cloud at a variety of online storage sites, including Dropbox, Google Drive, and iCloud, but only Microsoft OneDrive is built directly into Windows 10. With OneDrive, you can store your documents, photos, and other files online and sync them across multiple computers and devices. You can also easily share any file on OneDrive with other people.

1. How to create OneDrive account

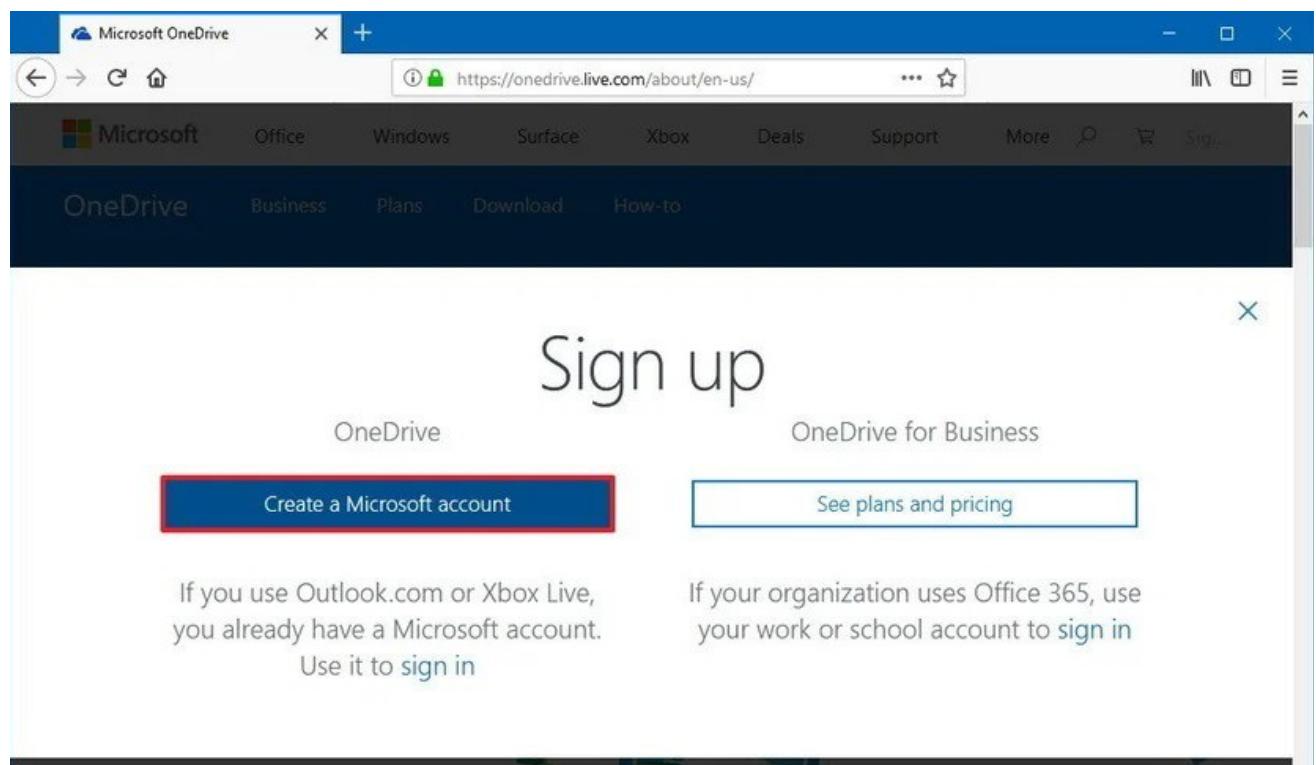
You're required to use a Microsoft Account to use OneDrive. If you already have a @outlook.com, @hotmail.com, or @live.com*email address, or an Xbox Live or Skype account, you already have a Microsoft account, and you can use that info to sign in.

If you don't have a Microsoft account , do the following.

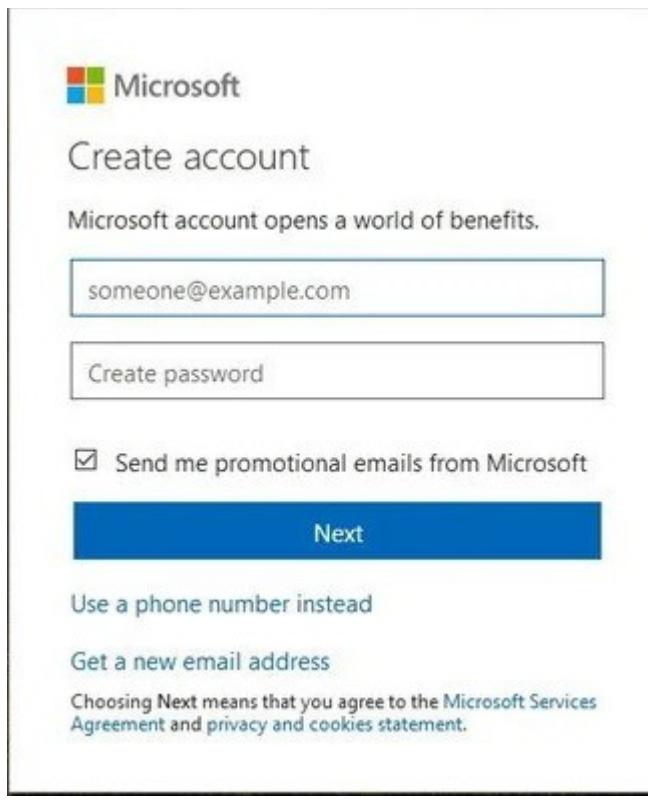
1. Visit “OneDrive.com” using your web browser.
2. Click the Sign up for free button.



3. Click the **Create a Microsoft account** button.



4. Create a new email address and password for the new account.
5. Click the **Next** button.



6. Continue through any additional on-screen instructions.

Set Up OneDrive: OneDrive is automatically available and ready to use in Windows 10. In fact, when you go through the Windows 10 setup, you're asked if you want to use OneDrive. If you missed that opportunity, you should still see an icon for OneDrive in the System Tray. If the icon does not appear, you'll need to trigger it manually from the OneDrive exe file.

To do this, open File Explorer. Make sure that hidden items are enabled (click the View menu and check the box for Hidden items). Then, drill down to the following location:

C:\Users\[YourUsername]\AppData\Local\Microsoft\OneDrive\

In that folder, double-click the OneDrive.exe file, and the icon will then appear in the System Tray. Right-click that icon and select Settings. Click the Settings tab and make sure the box to "Start OneDrive automatically when I sign in to Windows" is checked.

Sign Into OneDrive: At the Settings screen, click the Account tab and then select the button to Add an account. At the Set up One Drive screen, enter the email address for your Microsoft Account and click Sign in. Choose your type of OneDrive account - Personal or Work or School. Enter your password and click Sign in. Confirm the location that Microsoft has set for your One Drive folder.

You can change the location if you want. Otherwise, accept the default and click Next. Then click the button to Open my OneDrive folder.

Add Files to OneDrive : Select the folders and files you wish to add and sync to your One Drive storage. From File Explorer, move any folders and files you wish to synchronize into your OneDrive location. If you are signed in with a Microsoft account and have enabled OneDrive, you will see your OneDrive folders in File Explorer in Windows 10 appear in the Navigation pane at the left side of the

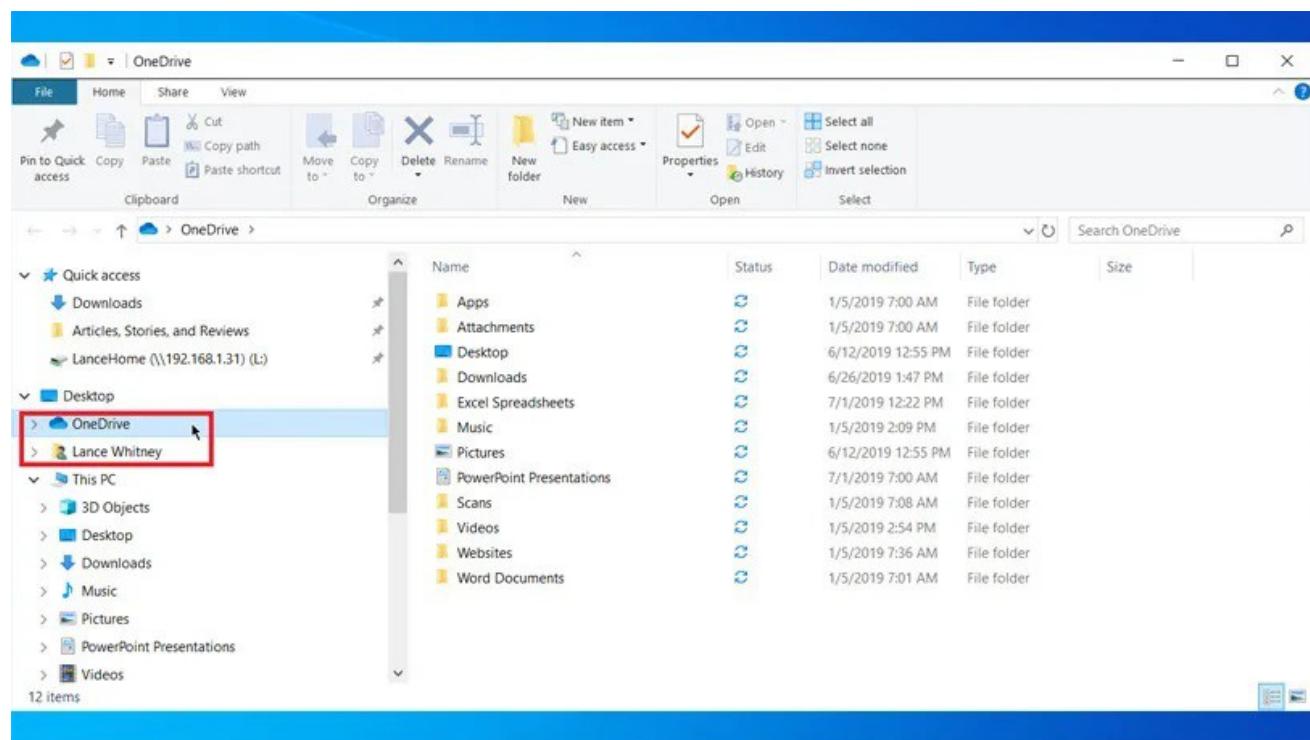
File Explorer window. This makes accessing your OneDrive files, and keeping them synched across your devices, easy. You can easily move or copy existing files to the OneDrive folders in File Explorer in Windows 10. Many applications, like Microsoft Office, also allow you to save directly to your OneDrive.

Open File Explorer (Windows key + E).

Click the OneDrive folder using the left pane.

Note: If you have multiple accounts configured on your device, the folders will be named accordingly: OneDrive - Personal for your regular account, and OneDrive - Family for business accounts.

Drag and drop or copy and paste content into the OneDrive folder.



Sync Files in OneDrive: Another way to select folders and files to sync in OneDrive is through the program's settings. Right-click the System Tray icon for OneDrive and select Settings. Click the Account tab and then select Choose folders. Here you'll see the files and folders that you moved into your OneDrive folder. If you wish to sync everything stored in your OneDrive folder, click the checkbox for Make all files available.

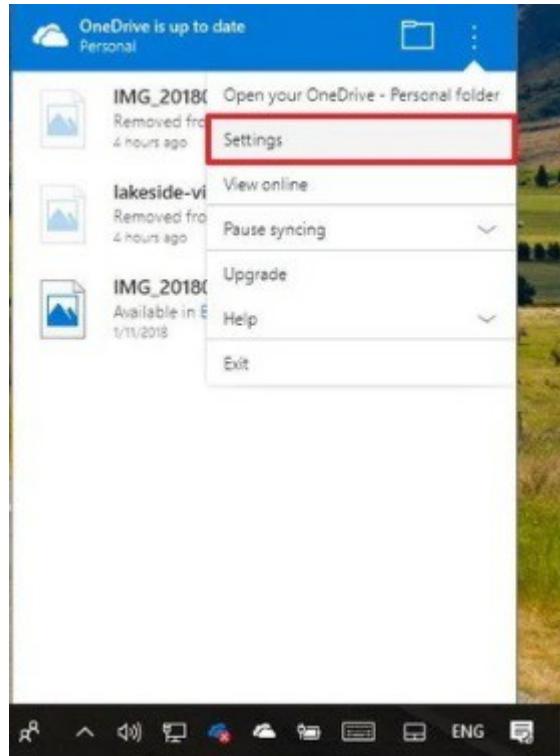
Otherwise, check the individual folders you wish to sync and uncheck any folders you don't want synced. Unchecked folders will remain on OneDrive but will be removed from your current PC and no longer synced online or across other OneDrive devices. Click OK when done.

How to choose which folders to sync from one drive

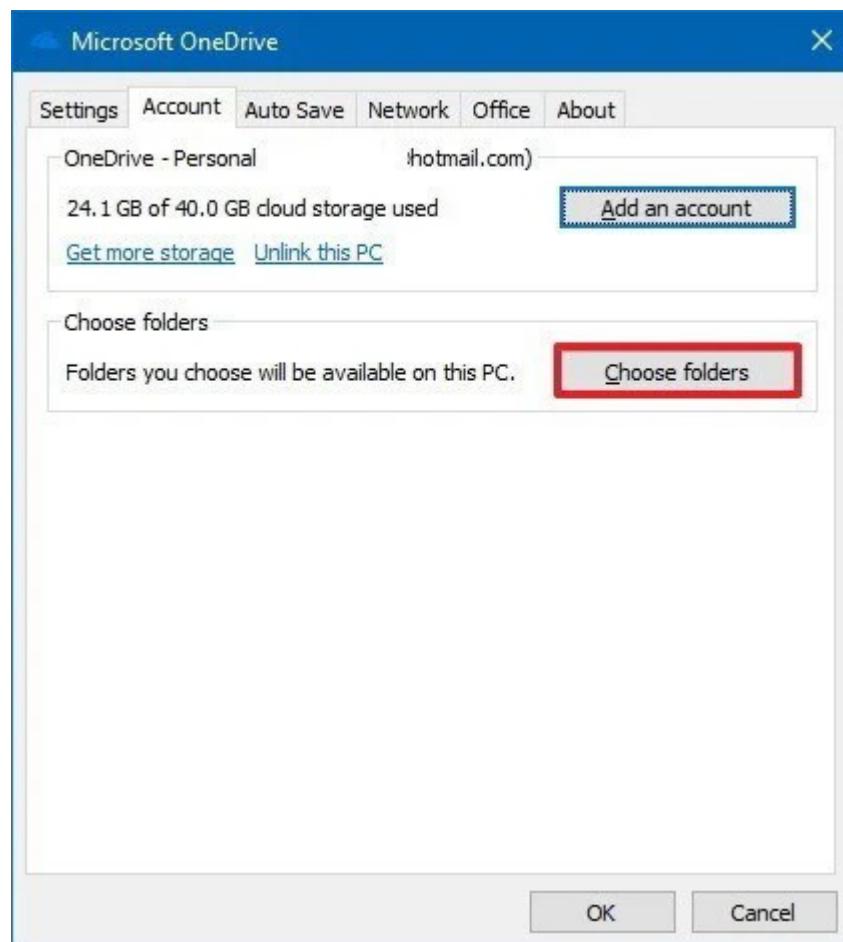
Click the cloud icon in the notification area.

Click the three-dotted menu button in the top-right corner.

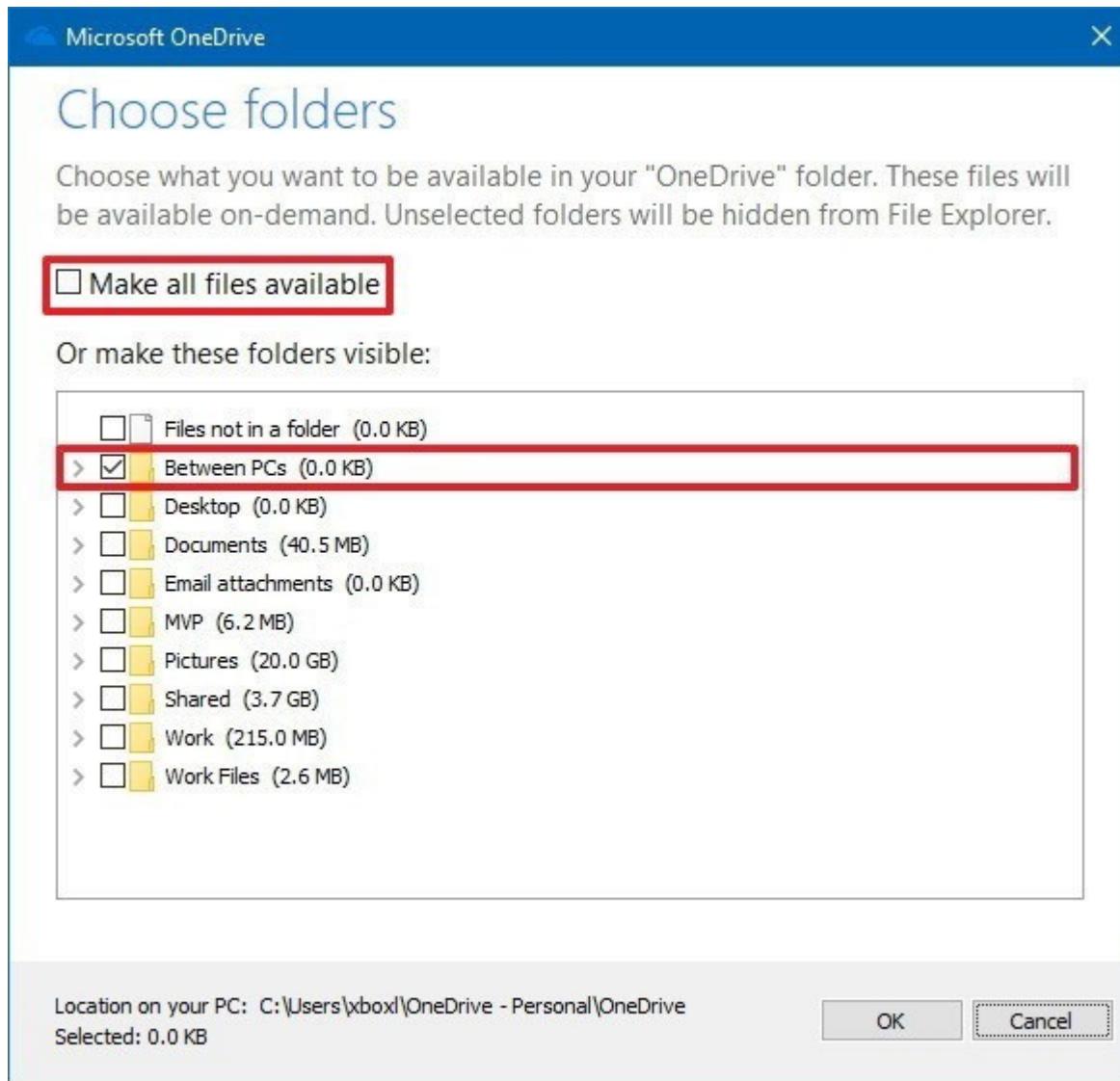
Click Settings.



4. In the "Account" tab, click Choose folders button.

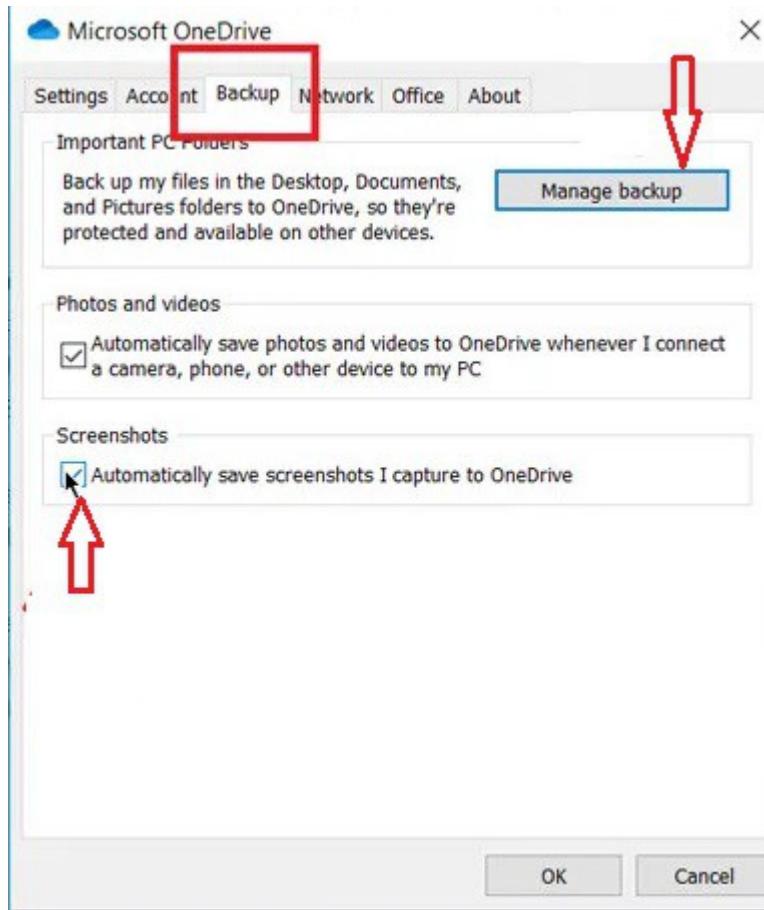


5. Clear the Make all files available option.
6. Check the folders you want to make visible.
7. Click OK.



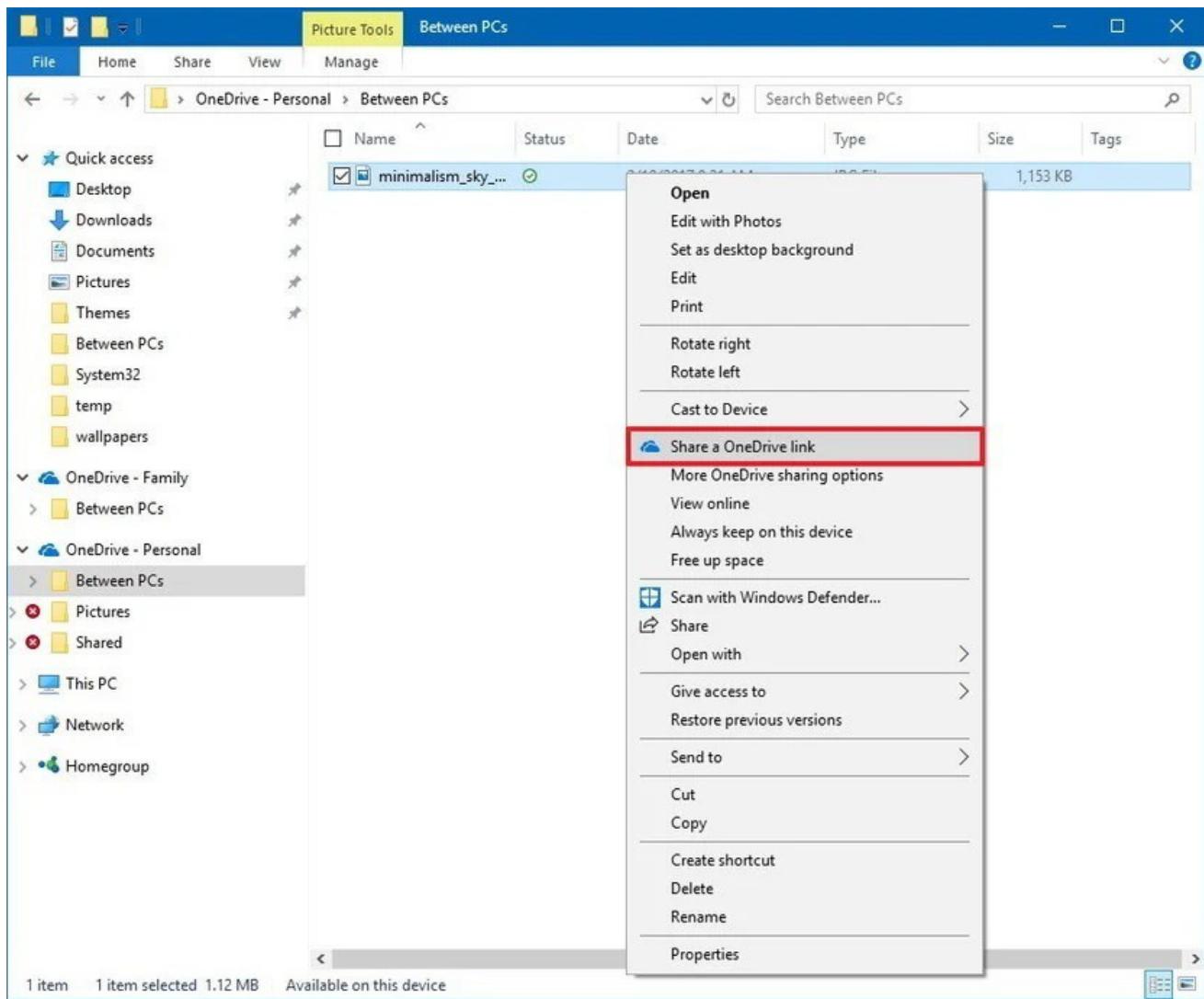
BackUp With OneDrive: After OneDrive is up and running, you can also use it to back up important folders. From the OneDrive program window, click the Backup tab. Click the button to Manage backup. You can opt to back up your desktop, your pictures folder, and your documents folder. Check the items you wish to back up and click the button to Start backup.

You can also opt to automatically save photos and videos to OneDrive whenever you connect a camera, phone, or other picture-taking device. Plus, you can automatically save screenshots to OneDrive. To enable either option, check the box next to it.



Share Files From File Explorer

You can share your OneDrive folders or files with other people either from File Explorer or from your online OneDrive site. In File Explorer, right-click the file you wish to share and select Share a OneDrive link from the pop-up menu. That generates a link you can email or share with someone else, giving that person the ability to read and edit that file. Enter the name or email address of the person you would like to share the document or folder. Enter the message (which is optional). Uncheck 'Allow editing' box if you would like users so that they can just view the document. Otherwise, leave it checked. Click Send.



[Back](#)

5.32 Backup files to another drive in Windows 10

Description: Windows Backup will backup all files in the libraries, folders, and drives you choose or let Windows choose. You will have a choice to include a system image in the backup. You can also choose to have these items be backed up on a regular schedule.

Here, we do the following tasks:

Task 1: Navigate to Update & security applet in Control Panel

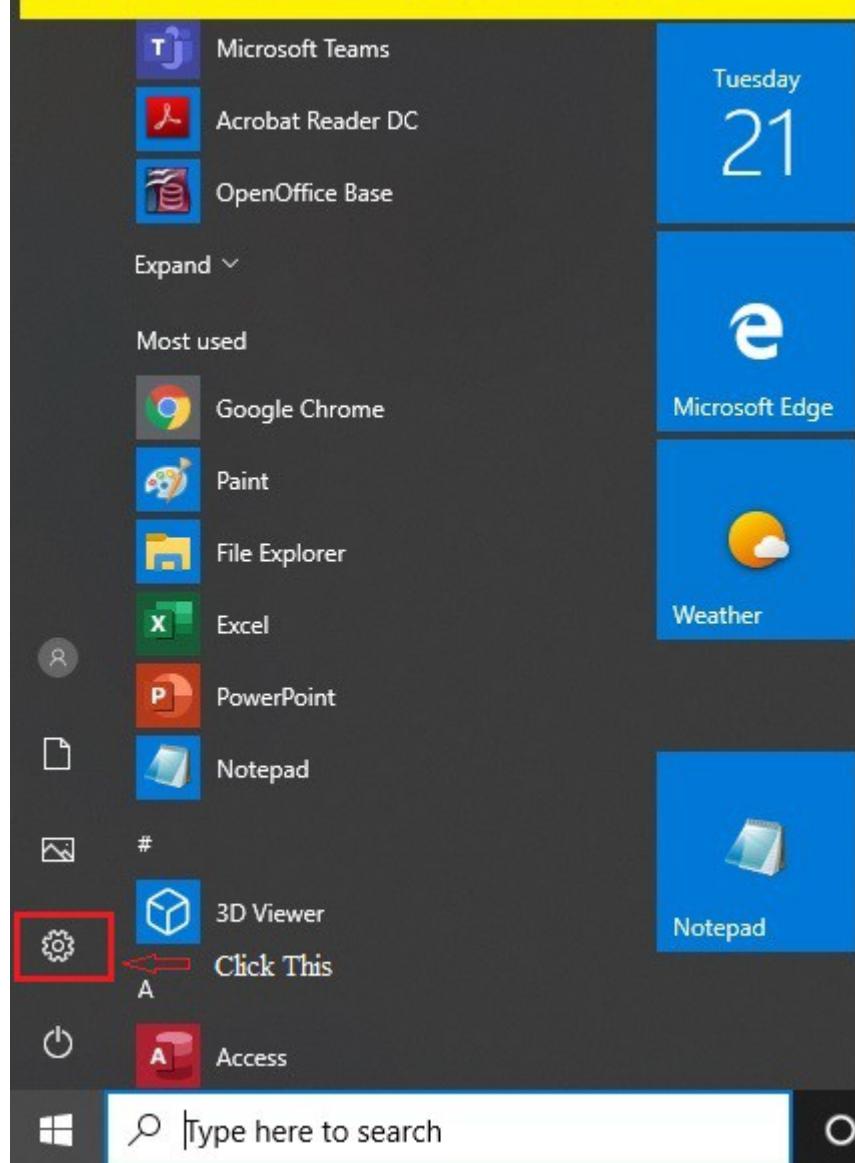
Task 2: Backup your files to USB device. (Assume that USB device is already inserted)

Lab exercise explains how to backup files to another drive in Windows 10

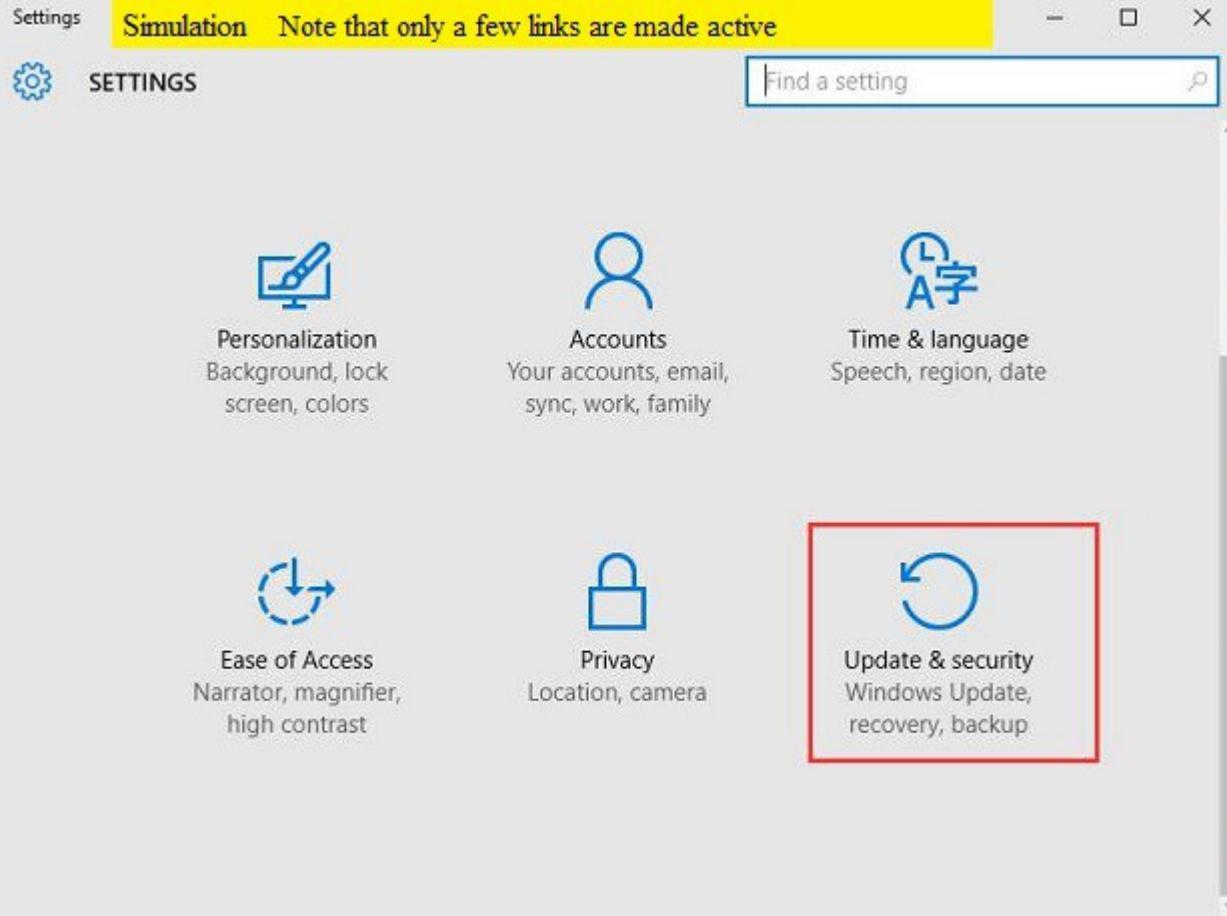
Instructions:

1. On loading the lab exercise click Settings  icon in the Start Menu 

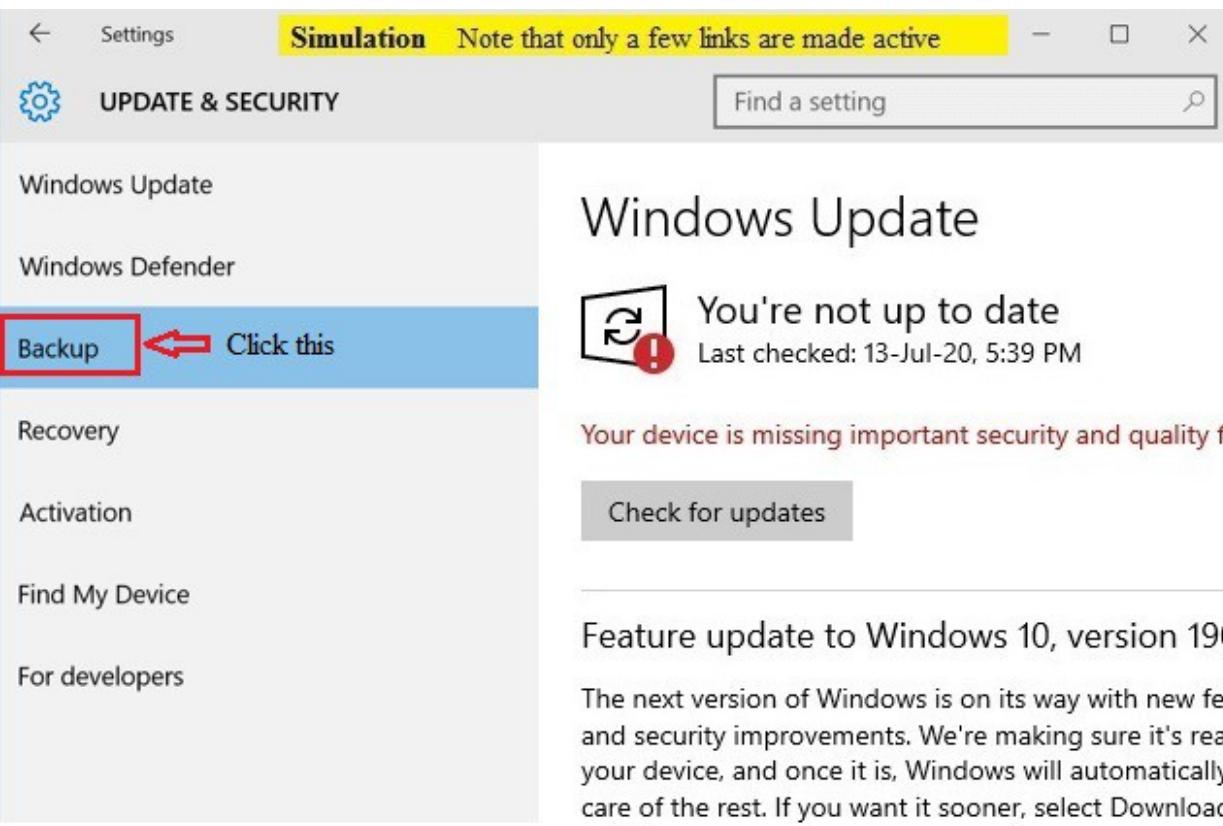
Simulation Note that only a few links are made active



2. Tap or click the "Update & security" button.

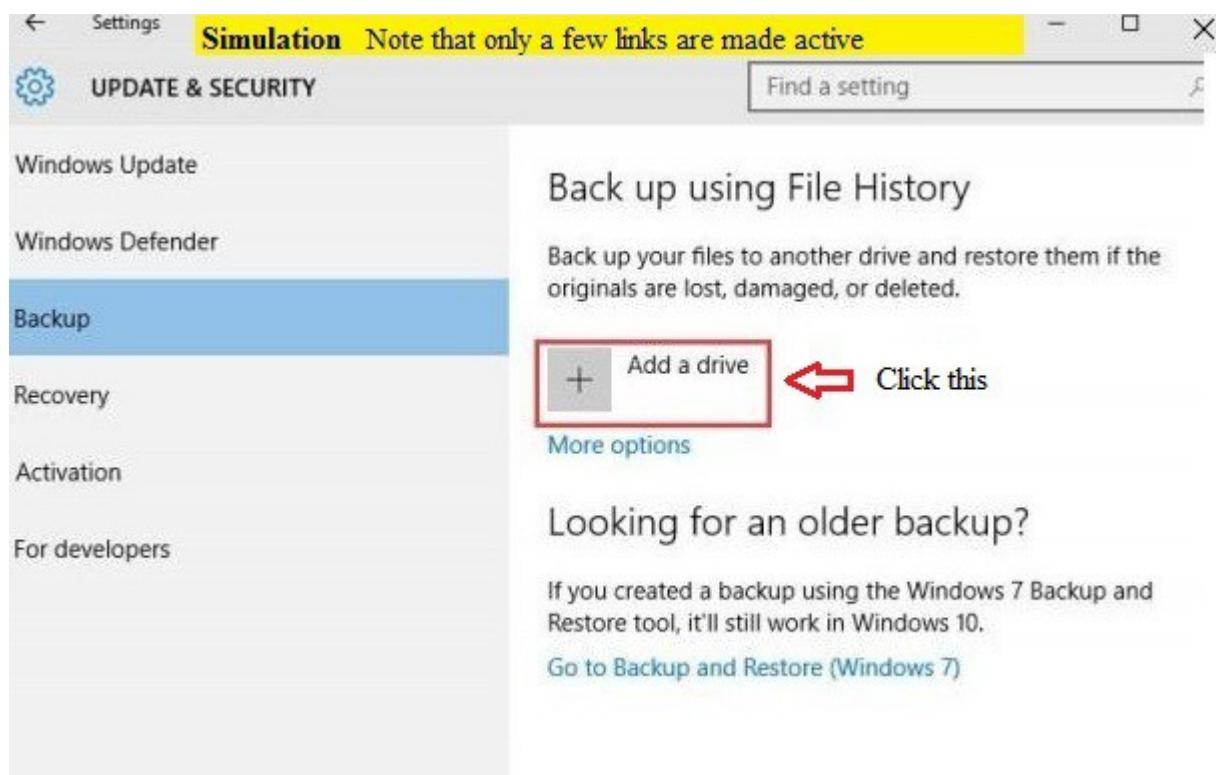


3. Then choose “Backup” on the left side of the panel.



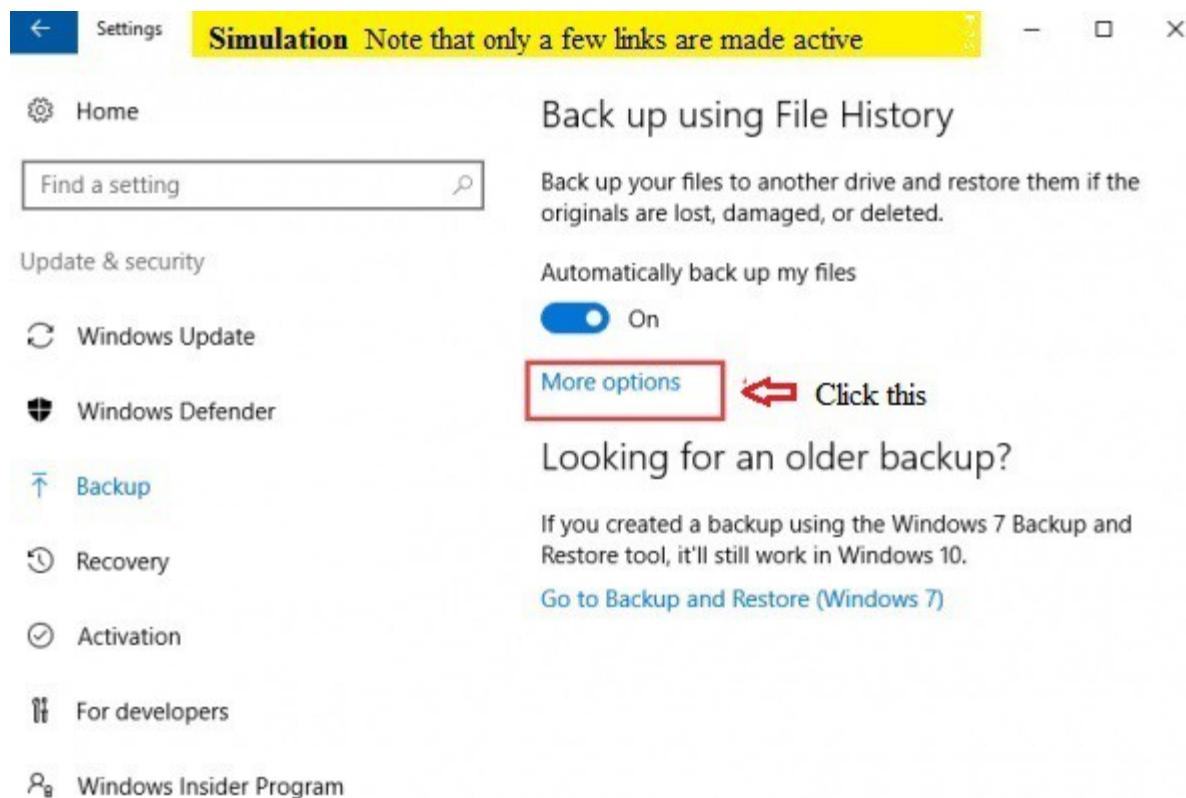
Note: In this lab exercise USB flash drive considered as an example

4. Then click the Add a drive option on the right side of the panel.

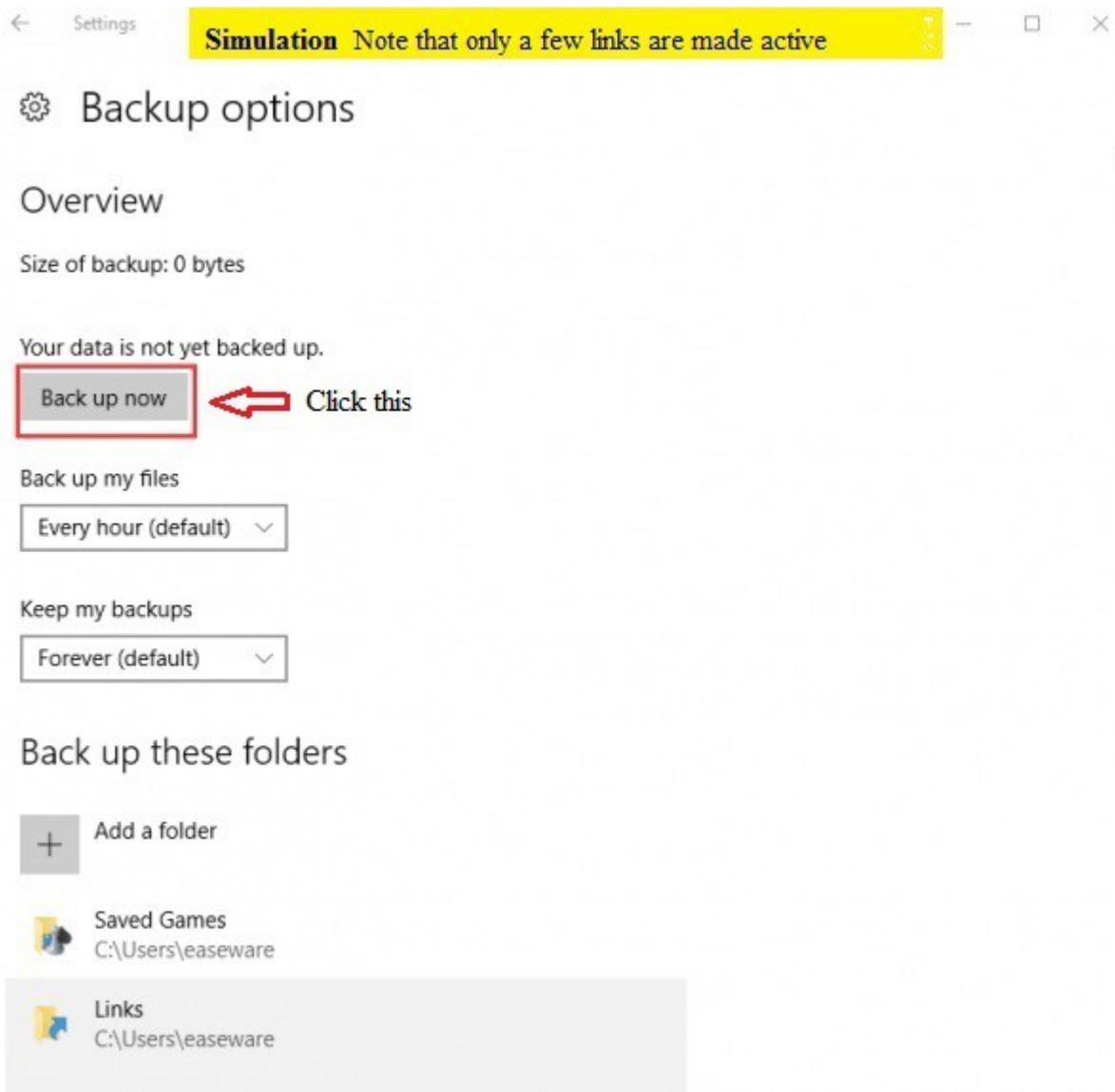


5. Wait for the system to help you find your drive. Then choose the correct drive that you would like to back up to. You can choose to backup your important files in your external USB drive, a network shared or network attached drive.

6. Tap or click “More options”



7. Click “Back up now” button.



Note: Scroll down and you can see the folders that you want to back up. You could click the **Add a folder** button to add more folders.

⚙️ Backup options

Keep my backups

Forever (default) ▾

Back up these folders

+ Add a folder

Saved Games
C:\Users\ easeware

Links
C:\Users\ easeware

Remove

Downloads
C:\Users\ easeware

Favorites
C:\Users\ easeware

Contacts
C:\Users\ easeware

OneDrive
C:\Users\ easeware

Or scroll down to the Exclude these folders section and click the Add a folder button to delete the folders that you don't want to back up.

Exclude these folders



Add a folder

Back up to a different drive

You'll need to stop using your current backup drive before you add a new one. This won't delete any files from your current backup drive.

[Stop using drive](#)

Related settings

[See advanced settings](#)

[Restore files from a current backup](#)

[Back](#)

5.33 Restore the files backed-up before in Windows 10

Description: Lab exercise demonstrates how to restore files that you had previously backed-up in Windows 10.

Here, we do the following tasks:

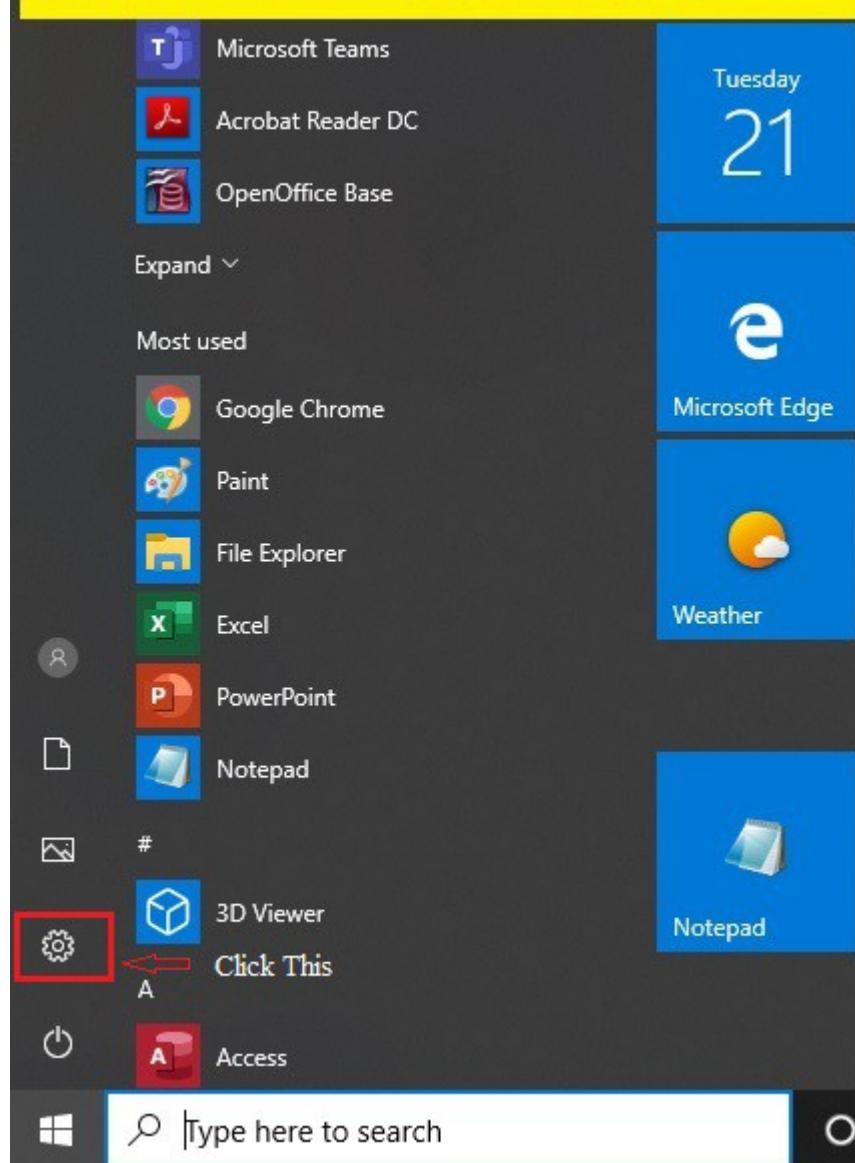
Task 1: Navigate to Update & security applet in Control Panel

Task 2: Select and restore files in a folder named “AplusLabs”

Instructions:

1. On loading the lab exercise click Settings  in the Start Menu 

Simulation Note that only a few links are made active



2. Tap or click the "Update & security" button.



Personalization
Background, lock
screen, colors



Accounts
Your accounts, email,
sync, work, family



Time & language
Speech, region, date



Ease of Access
Narrator, magnifier,
high contrast



Privacy
Location, camera



Update & security
Windows Update,
recovery, backup

3. Tap or Click the "Backup"

← Settings **Simulation** Note that only a few links are made active ×

 UPDATE & SECURITY Find a setting

Windows Update

Windows Defender

Backup  Click this

Recovery

Activation

Find My Device

For developers

Windows Update

 You're not up to date
Last checked: 13-Jul-20, 5:39 PM

Your device is missing important security and quality fixes.

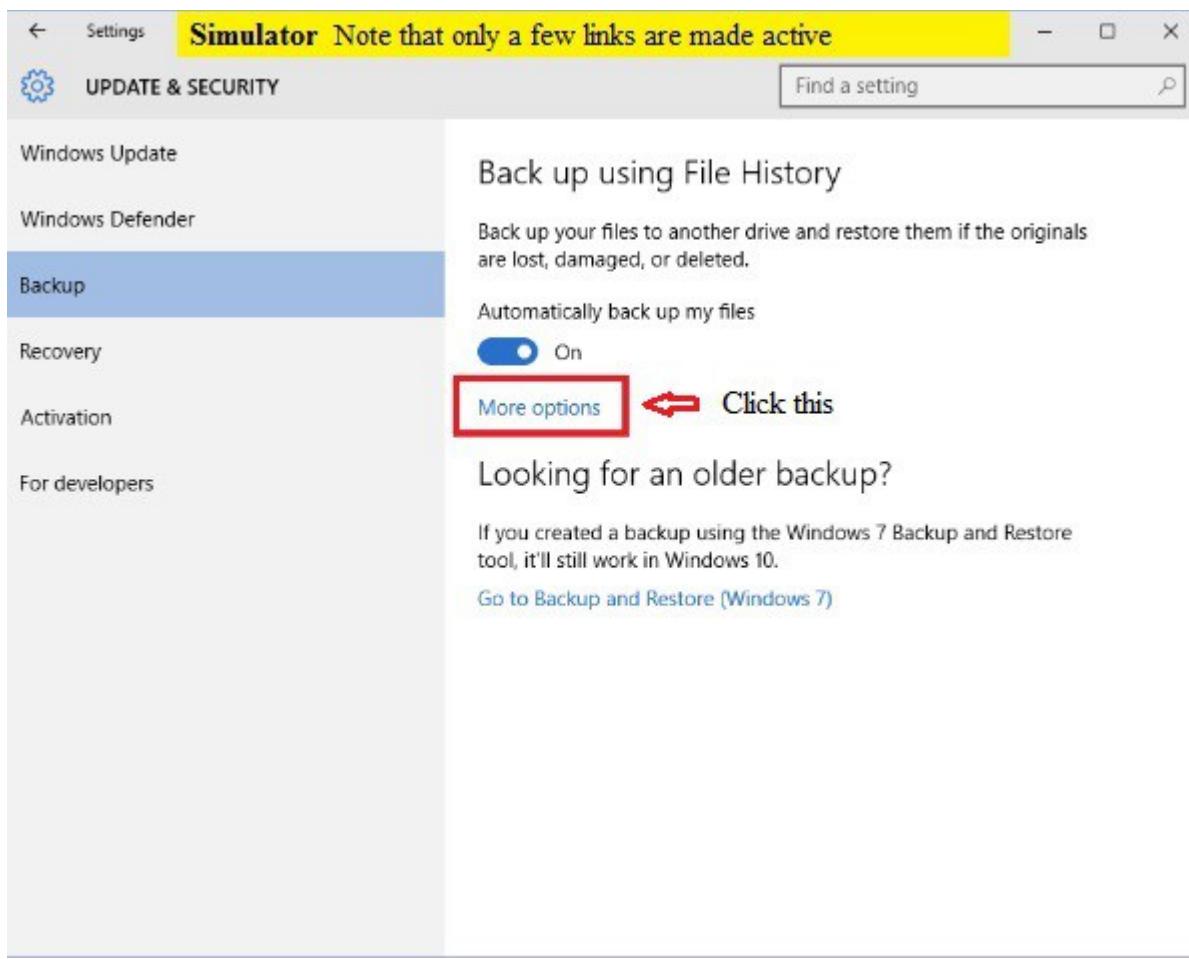
[Check for updates](#)

Feature update to Windows 10, version 1909

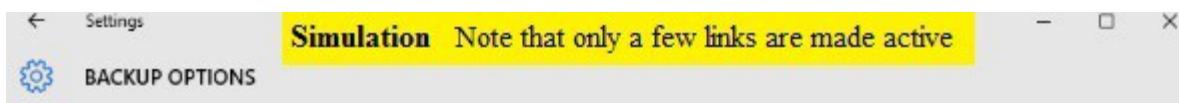
The next version of Windows is on its way with new features and security improvements. We're making sure it's ready for your device, and once it is, Windows will automatically take care of the rest. If you want it sooner, select Download and install now.

[Download and install now](#)

4. Tap or Click the "More options"



5. Click "Restore files from a current backup".



Exclude these folders

+ Add a folder

Back up to a different drive

You'll need to stop using your current backup drive before you add a new one. This won't delete any files from your current backup drive.

Stop using drive

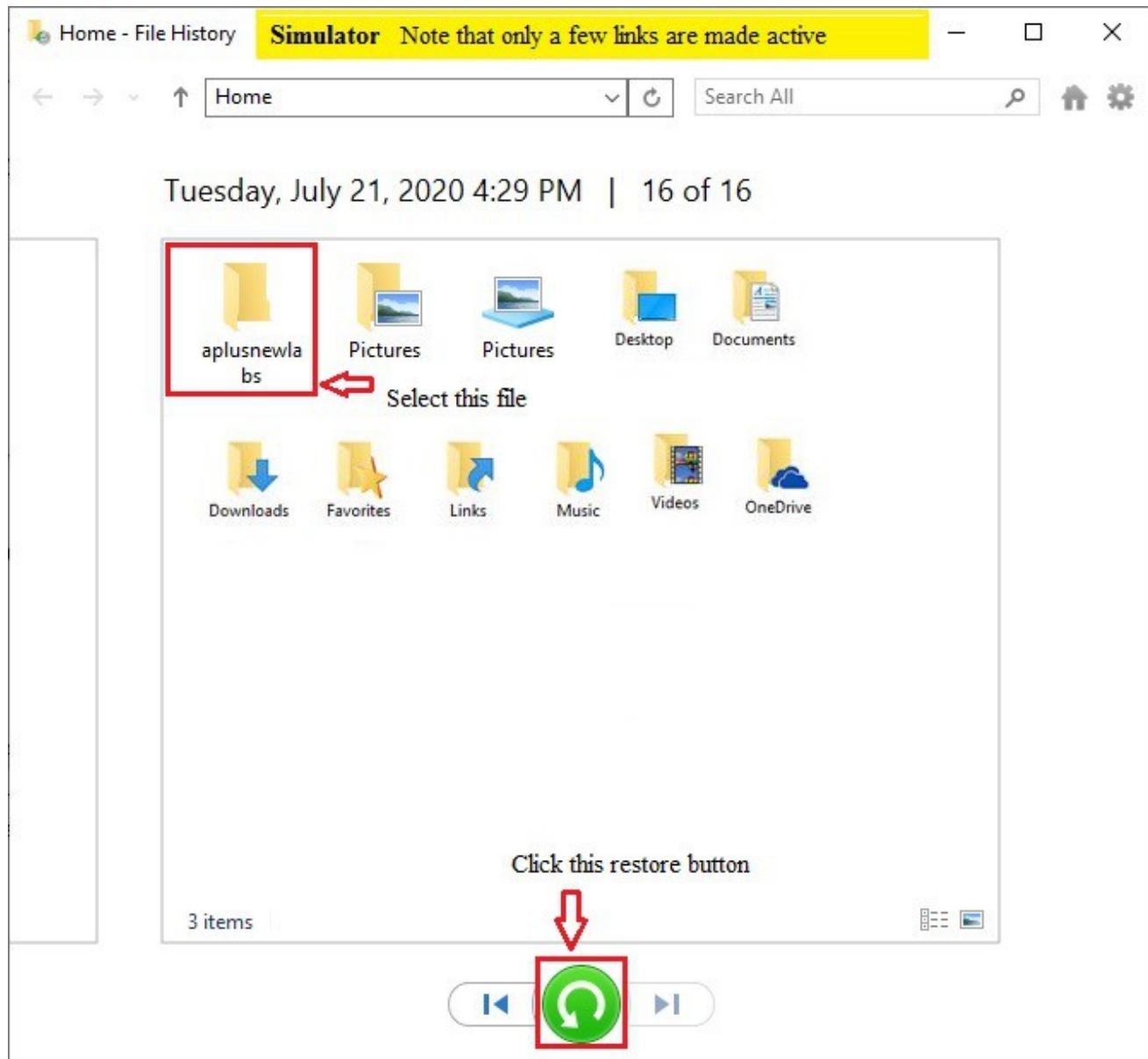
Related settings

[See advanced settings](#)

[Restore files from a current backup](#)

← Click this

6. Select “aplusnewlabs” folder from the available list of files and folders and click “Restore” button.



Explanation: The Windows 10 backup program, File History, saves the files that you've created. It doesn't back up your apps and programs. The apps and programs can always be reinstalled. But photos, videos, and documents can never be re-created.

To keep your files safe, File History automatically makes a copy of every file in your Documents, Music, Photos, and Videos folders. It copies all the files on your desktop, as well. And File History automatically makes those copies every hour.

File History makes your backups easy to see and restore, letting you flip through different versions of your files and folders, comparing them with your current versions. Should you find a better version, a press of a button brings that older version back to life.

[Back](#)

5.34 Formatting hard drive in Windows 10

Description: Lab exercise explains how to format a volume with NTFS in Windows 10 OS environment. In another exercise, we enable BitLocker which requires NTFS formatting of the disk

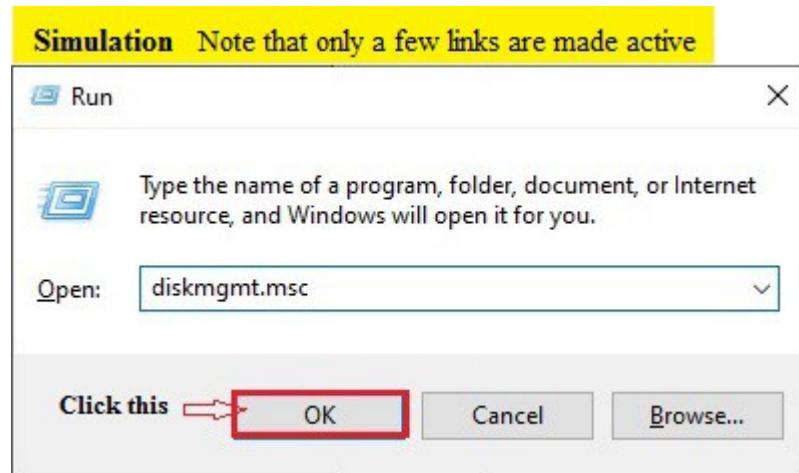
drive.

Task 1: Navigate to Disk Management using appropriate given option.

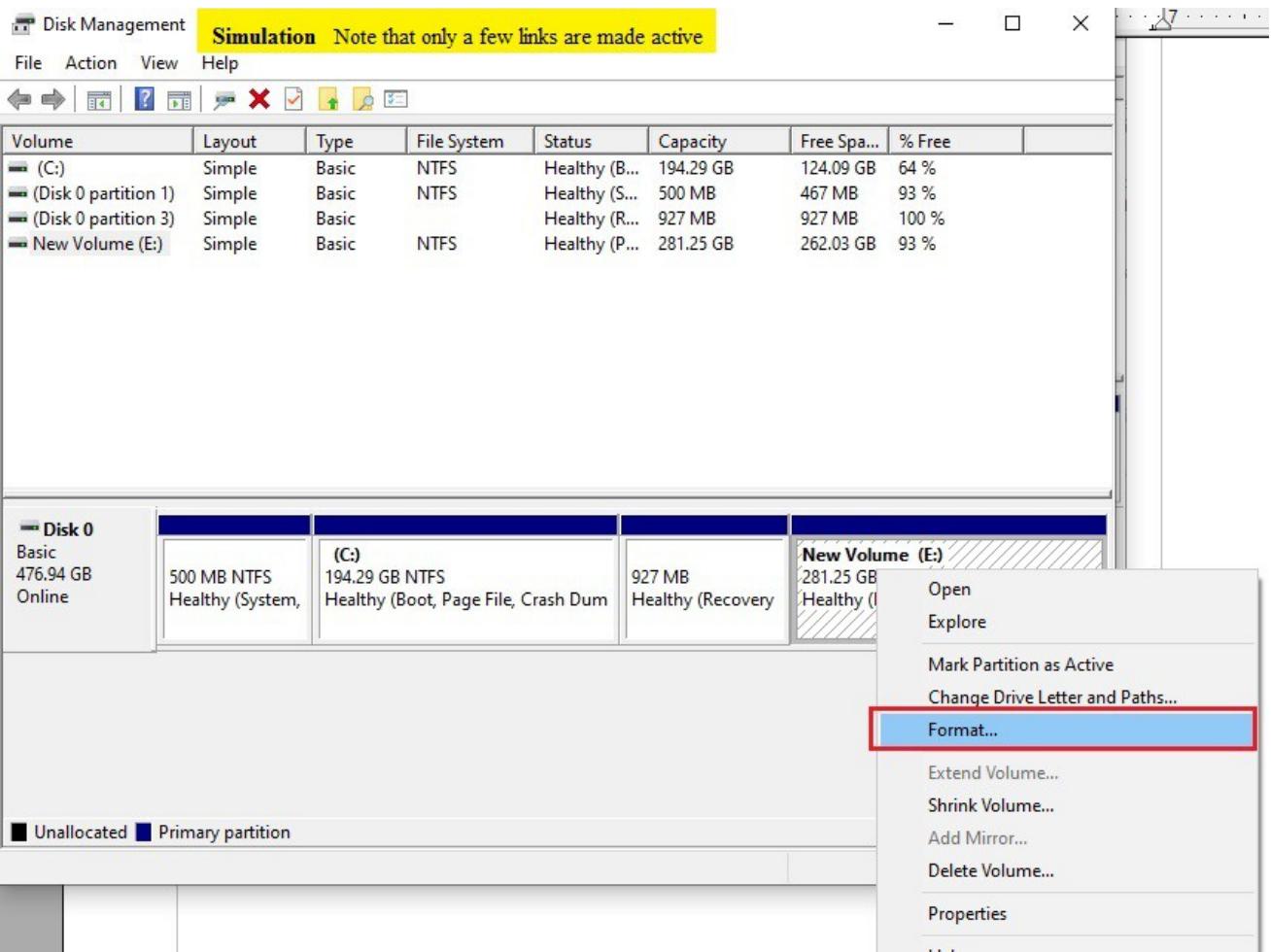
Task 2: Format “E” drive , and give the Volume label as “Data”.

Instructions:

1. After loading the lab exercise, in the resulting simulation run window, type “diskmgmt.msc” and hit Enter.

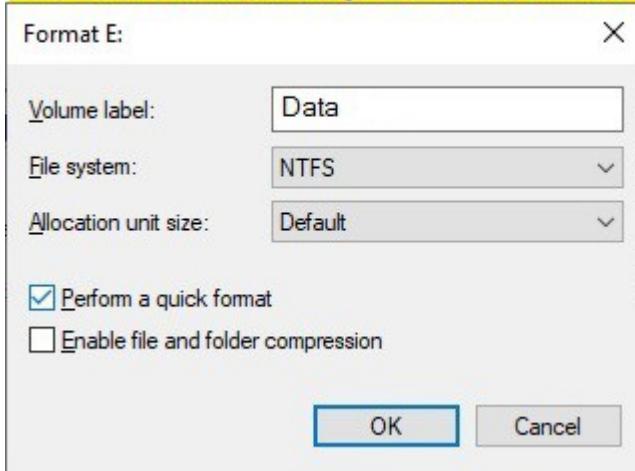


2. In the Disk Management window right click New Volume (E) hard drive and select “Format” option from the popup menu.



3. Format E drive window appears , in the "Value label" field, enter a descriptive name for the drive as “Data”, keep the remaining value as it is , that is
 1. Use the "File system" drop-down menu, and select NTFS (recommended for Windows 10).
 2. Use the "Allocation unit size" drop-down menu, and select the Default option.
 3. Check the Perform a quick format option.
4. Click OK button to format the selected drive.

Simulation Note that only a few links are made active



[Back](#)

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

Description: This lab exercise will show how to turn on or off BitLocker to encrypt operating system drives in Windows 10

Task 1: Open “Bitlocker Drive Encryption” by going to CP , using appropriate option.

Task 2: Turn on bitlocker for “E” drive , use password “mypass” as unlock password when prompted.

Task 3: Save recovery key to your cloud domain account.

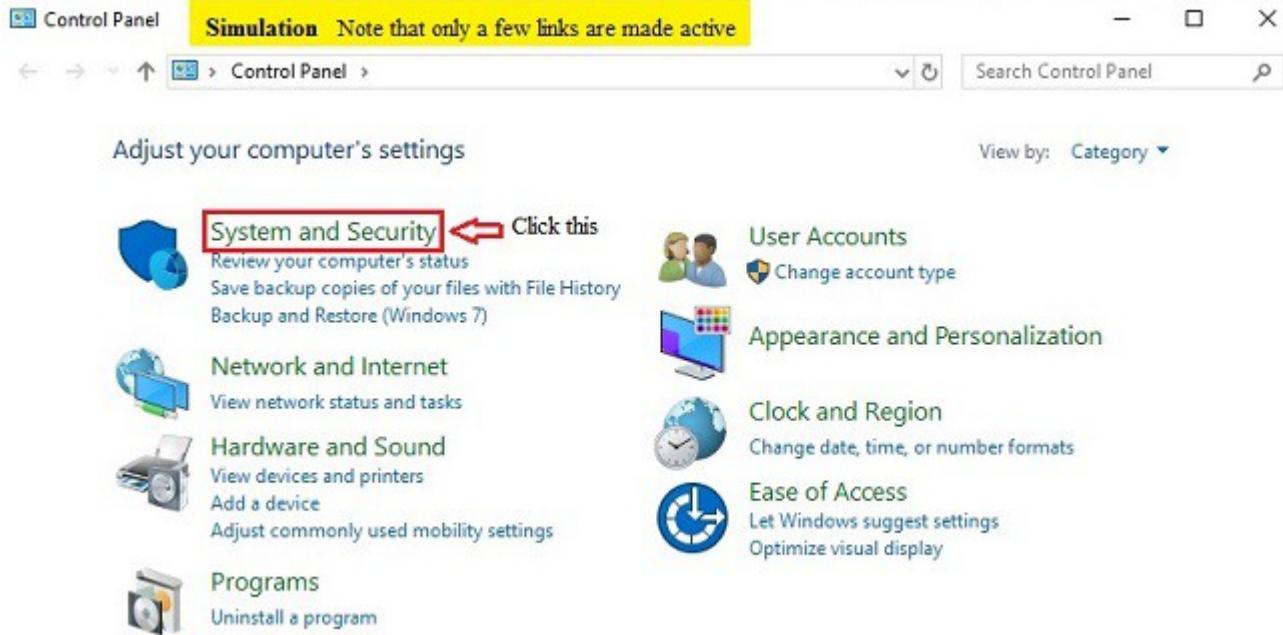
Task4: Select the encryption option "Encrypt used disk space"

Task 4: Select the encryption option as Encrypt used disk space only

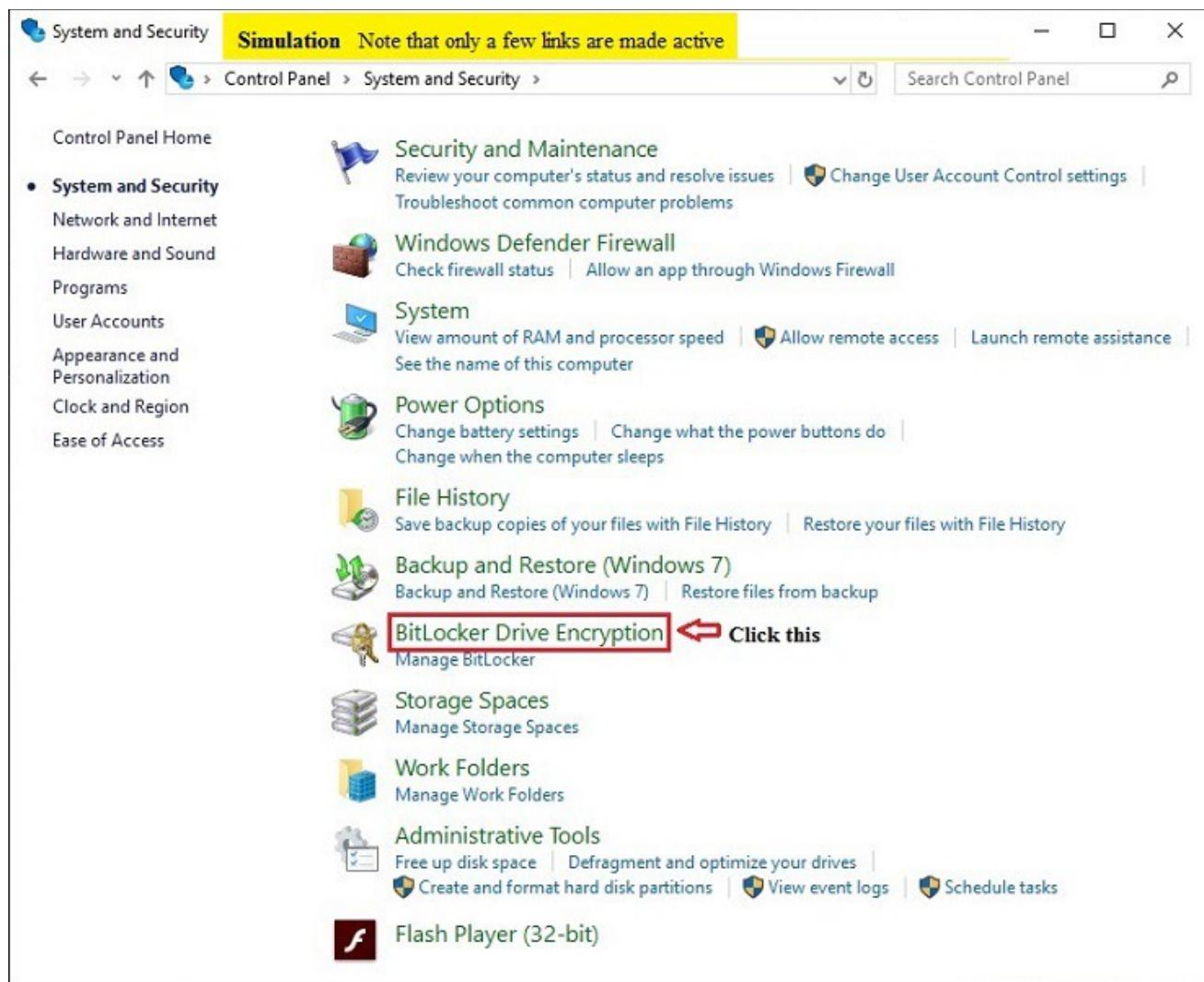
Instructions:

1. On loading a lab exercise, in a given simulation start menu click “System and Security” from the given control panel window.

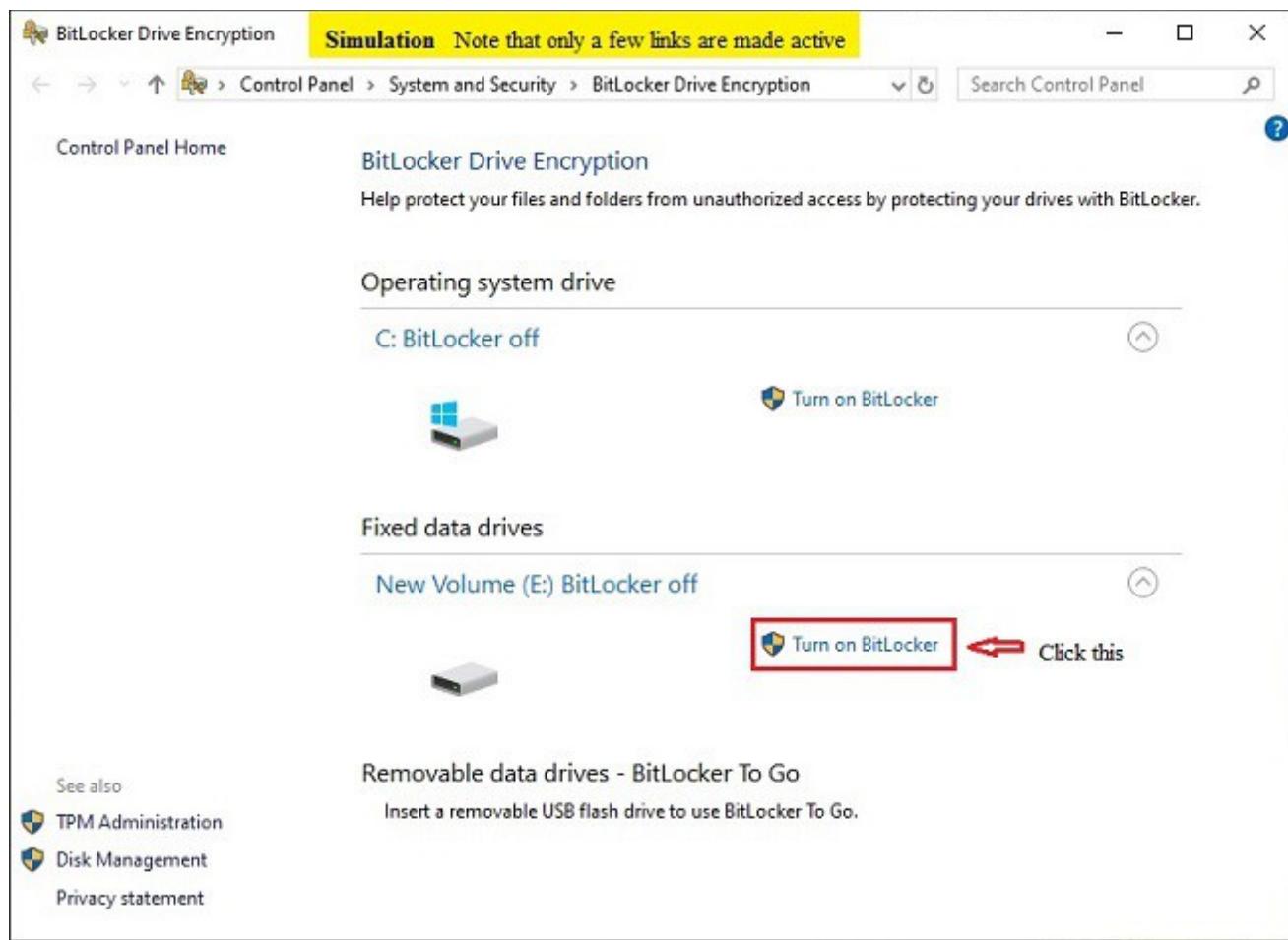
Note: You can also open , by typing bitlocker in the search bar of the start menu, and click Manage Bitlocker in your Windows 10 system.



2. Click BitLocker Drive Encryption.



3. In the BitLocker Drive Encryption window under “E” Drive, click Turn on BitLocker.



4. Choose how you want to unlock your drive during startup:

1. Use a password to unlock the drive.
2. Use my smart card to unlock the drive.

In this lab exercise , select the first option Use a password to unlock the drive , Enter a password as “mypass” that you'll use every time you boot Windows 10 to unlock the drive and click “Next button.

Simulation Note that only a few links are made active

X

← BitLocker Drive Encryption (E:)

Choose how you want to unlock this drive

Use a password to unlock the drive

Select this

Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.

Enter your password

Reenter your password

Use my smart card to unlock the drive

You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.

Click this

Next

Cancel

Note: Make sure to create a strong password mixing uppercase, lowercase, numbers, and symbols.

5. You will be given the choices to save a recovery key to regain access to your files in case you forget your password. Options include:

1. Save to your cloud domain account
2. Save to a USB flash drive
3. Save to a file
4. Print the recovery key

Important. Select the option that is most convenient for you, and save the recovery key in a safe place. Because if you forget your password or lose your USB flash drive and do not have the recovery key then your data will be lost forever.

Note: If you trust the cloud, you can choose to save your recovery key in your Microsoft account using the Save to your Microsoft account option. In which case, you can retrieve your encryption key at this location: <https://onedrive.live.com/recoverykey>.

In this lab exercise select the first option “Save to your cloud domain account” and click Next button.

Simulation Note that only a few links are made active

X

← BitLocker Drive Encryption (E:)

How do you want to back up your recovery key?

i Some settings are managed by your system administrator.

If you forget your password or lose your smart card, you can use your recovery key to access your drive.

→ Save to your cloud domain account

→ Save to a USB flash drive

→ Save to a file

→ Print the recovery key

Click this
↑

[How can I find my recovery key later?](#)

Click this

Next

Cancel

6. Select the encryption option that best suits your scenario:

1. Encrypt used disk space only (faster and best for new PCs and drives)
2. Encrypt entire drive (slower but best for PCs and drives already in use)

In this lab exercise select the first option and click Next button.

Simulation Note that only a few links are made active X

← BitLocker Drive Encryption (E:)

Choose how much of your drive to encrypt

If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.

If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected—even data that you deleted but that might still contain retrievable info.

Encrypt used disk space only (faster and best for new PCs and drives)

Select this

Encrypt entire drive (slower but best for PCs and drives already in use)

Click this

Next

Cancel

7. Choose between the two encryption options

1. New encryption mode (best for fixed drives on this device)
2. Compatible mode (best for drives that can be moved from this device)

Select the first option “New encryption mode” and click Next button

Simulation Note that only a few links are made active X

← BitLocker Drive Encryption (E:)

Choose which encryption mode to use

Windows 10 (Version 1511) introduces a new disk encryption mode (XTS-AES). This mode provides additional integrity support, but it is not compatible with older versions of Windows.

If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.

If this is a fixed drive or if this drive will only be used on devices running at least Windows 10 (Version 1511) or later, you should choose the new encryption mode

New encryption mode (best for fixed drives on this device)

Select this

Compatible mode (best for drives that can be moved from this device)

Click this

Next

Cancel

8. Click Start encrypting to finish the process.

Simulation Note that only a few links are made active X

← BitLocker Drive Encryption (E:)

Are you ready to encrypt this drive?

You'll be able to unlock this drive using a password.

Encryption might take a while depending on the size of the drive.

Until encryption is complete, your files won't be protected.

Click this

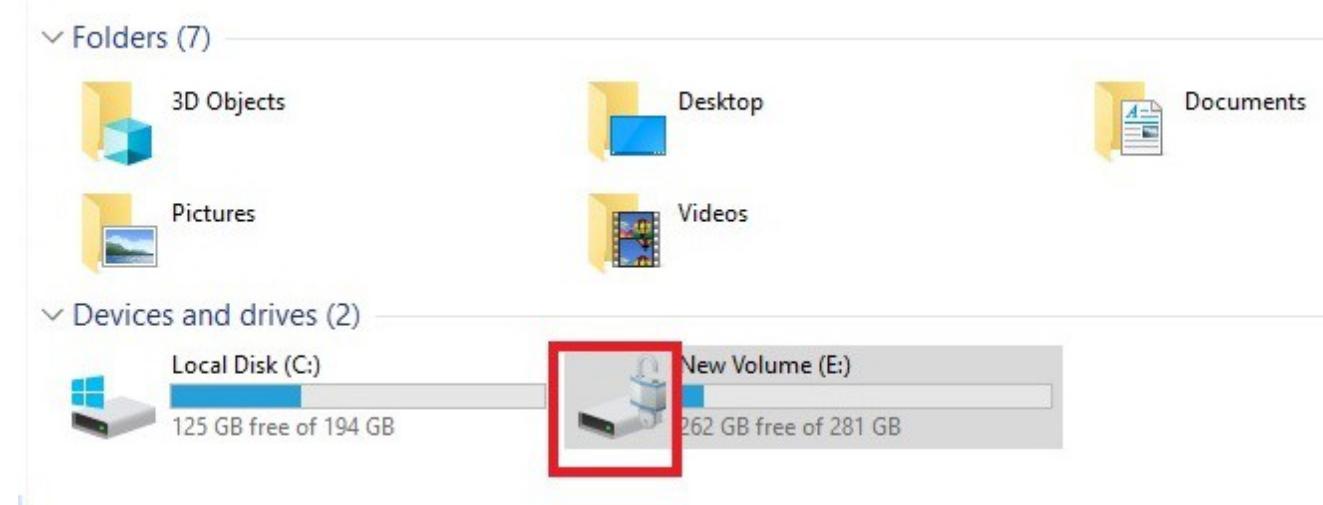
Start encrypting

Cancel

9. Bit locker Drive encryption window is displayed.



Finally, restart your computer to begin the encryption process. You can verify that BitLocker is turned on by the lock icon on the drive when you open This PC on File Explorer. As shown below.



Explanation: You can use BitLocker Drive Encryption to help protect your files on an entire drive. BitLocker can help block hackers from accessing the system files they rely on to discover your password, or from accessing your drive by physically removing it from your PC and installing it in a different one. You can still sign in to Windows and use your files as you normally would. New files are automatically encrypted when you add them to a drive that uses BitLocker. However, if you copy these files to another drive or a different PC, they're automatically decrypted. BitLocker can encrypt the drive Windows is installed on (the operating system drive) as well as fixed data drives (such as internal hard drives). You can also use BitLocker To Go to help protect all files stored on a removable data drive (such as an external hard drive or USB flash drive). BitLocker checks the PC during startup for any conditions that could represent a security risk (for example, a change to the BIOS software that starts the operating system when you turn on your PC, or changes to any startup files). If a potential security risk is detected, BitLocker will lock the operating system drive and you'll need a special BitLocker recovery key to unlock it. You can choose how to unlock the operating system drive when you turn on your PC with a PIN (requires TPM), password, or startup key on a connected USB flash drive.

How does it work:

BitLocker is used in conjunction with a hardware component called a Trusted Platform Module (TPM). The TPM is a smart card-like module on the motherboard that is installed in many newer computers by the

computer manufacturer. BitLocker stores its recovery key in the TPM (version 1.2 or higher). When you enable BitLocker, you create a personal identification number (PIN) that will be required to enter each time you startup your computer. While enabling BitLocker, a recovery key is generated. The recovery key is used to gain access to your computer should you forget your password. After the recovery key is generated you will be prompted to restart the machine. The encryption process begins when the computer reboots.

Note: You should print or save the recovery key and store it in a safe place apart from your computer.

Given below are the requirements for BitLocker to work in Windows 10:

1. BitLocker Drive Encryption is available only on Windows 10 Pro and Windows 10 Enterprise.
2. For best results your computer must be equipped with a Trusted Platform Module (TPM) chip. This is a special microchip that enables your device to support advanced security features.
3. You can use BitLocker without a TPM chip by using software-based encryption, but it requires some extra steps for additional authentication.
4. Your computer's BIOS must support TPM or USB devices during startup.
5. Your PC's hard drive must contain at least two partitions: a system partition, which contains the necessary files to start Windows, and the partition with the operating system. If your computer doesn't meet the requirements, BitLocker will create them for you. Additionally, the hard drive partitions must be formatted with the NTFS file system.

[**Back**](#)

5.36 Installing/Updating graphic card driver in Windows 10

Description: While Windows Update will update your computer system including the Device Drivers automatically, or the software updaters of your graphics hardware will inform you when updates are available, there may be a time when you may have to, update your systems video and graphic drivers, if you are facing issues like laptop screen brightness flickering or if you wish to get better performance out of your Windows 10/8/7 system.

Here, we do the following.

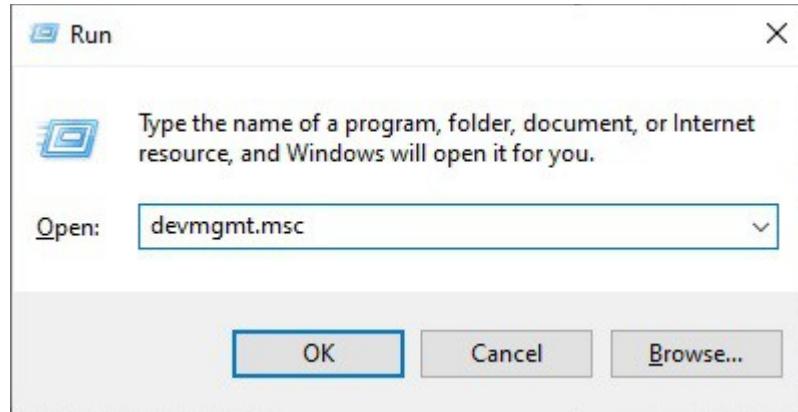
Task 1: Navigate to Device Management using appropriate given option.

Task 2: Update the driver for graphic card using appropriate options, to allow Windows 10 to find and install driver.

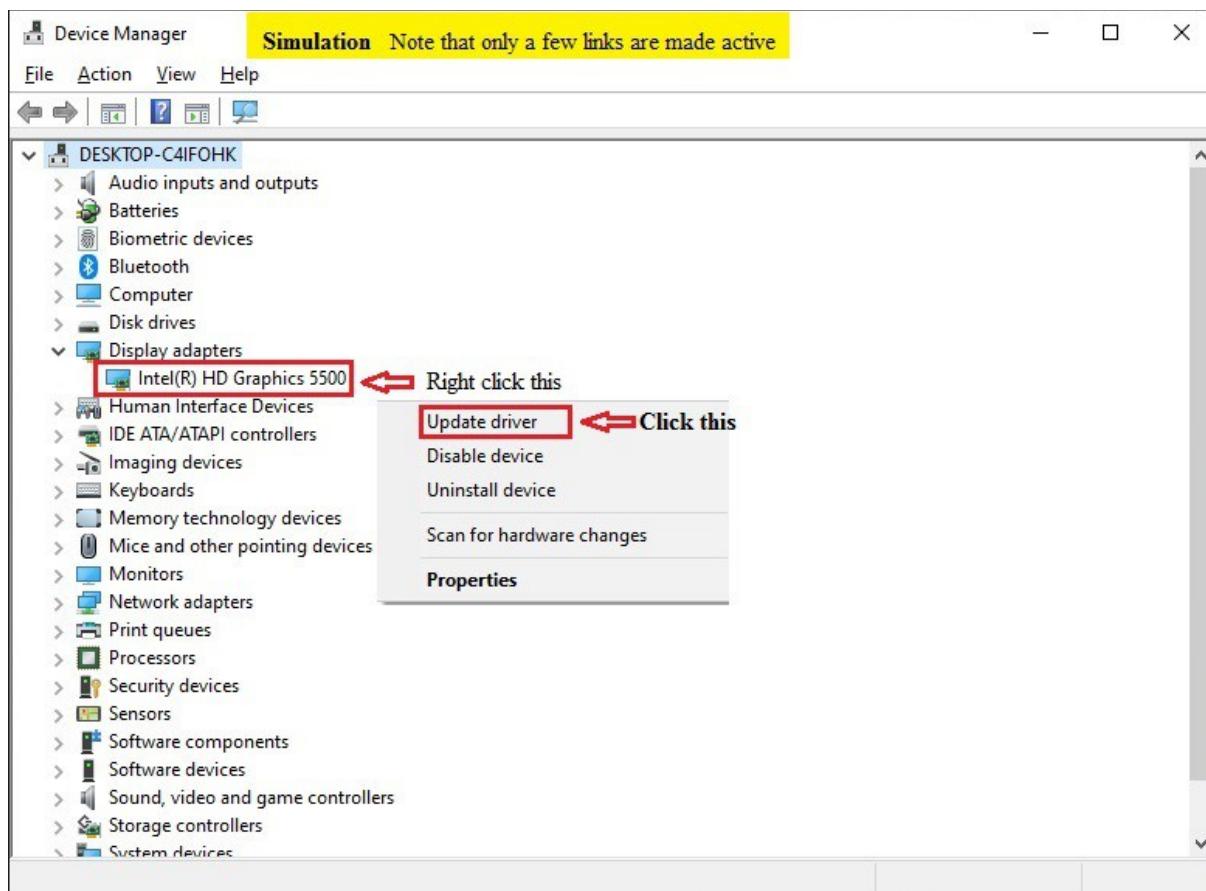
Lab Exercise explains how to update graphics card driver in Windows 10.

Instructions:

1. In the given run window (open the run window by pressing windows + R button in your Windows 10 system) type “devmgmt.msc” to open Device Manager.



2. Double click on the Display Adapters menu. Now already installed graphics cards will display as shown below, right click on the graphic card and select update driver from the popup menu.



3. In the next Update Drivers window, you will see two options. Click the first option “Search automatically for updated driver software”. Then Windows will find and install drivers for your video device automatically.

Simulation Note that only a few links are made active

X

← Update Drivers - Intel(R) HD Graphics 5500

How do you want to search for drivers?

→ [Search automatically for updated driver software](#)

Windows will search your computer and the Internet for the latest driver software for your device, unless you've disabled this feature in your device installation settings.

← Click this

→ [Browse my computer for driver software](#)

Locate and install driver software manually.

Cancel

By clicking on “Search automatically for updated driver software” the following screen appears which will allow Windows 10 to automatically search for driver updates and install the same, if available.

Click the close button to complete the lab.

Simulation Note that only a few links are made active



← Update Drivers - Intel(R) HD Graphics 5500

Click this

Searching online for drivers...

Cancel

Once installed, you will see “Windows has successfully updated your driver software” message. If updates are not available, you will see “No updates were found” message.

Note: You may also check for hardware changes in the Device Manager as shown below:



Explanation: Graphic card drivers are important to have installed and up to date for better performance and to ensure that the graphics card works as intended. Essentially, the driver software handles communication between Windows 10, games and applications, and the graphics card component.

In most circumstances, Windows Update won't find a new driver. However, the companies that manufacture the graphics hardware usually release updates monthly, with bug fixes and optimizations for new games. However, it takes a while for these changes to make their way through the Microsoft certification process (if the company even bothers).

In Windows Update, you usually see a date next to each entry. If your graphics driver is older than a year or so, Windows Device Manager can be used to upgrade to the latest driver.

Before you get started, it's wise to create a system recovery point. This backs up all your current drivers, allowing you to return to the previous state in case anything goes wrong. To create your backup, right-click on Computer (on your desktop) and select Properties. Click on the System Protection item on the left. In the next window, click on System Protection, select Create, and follow the instructions on the screen.

Note: You can refer to Inserting graphics card in a motherboard slot in the PC hardware lab section of this manual.

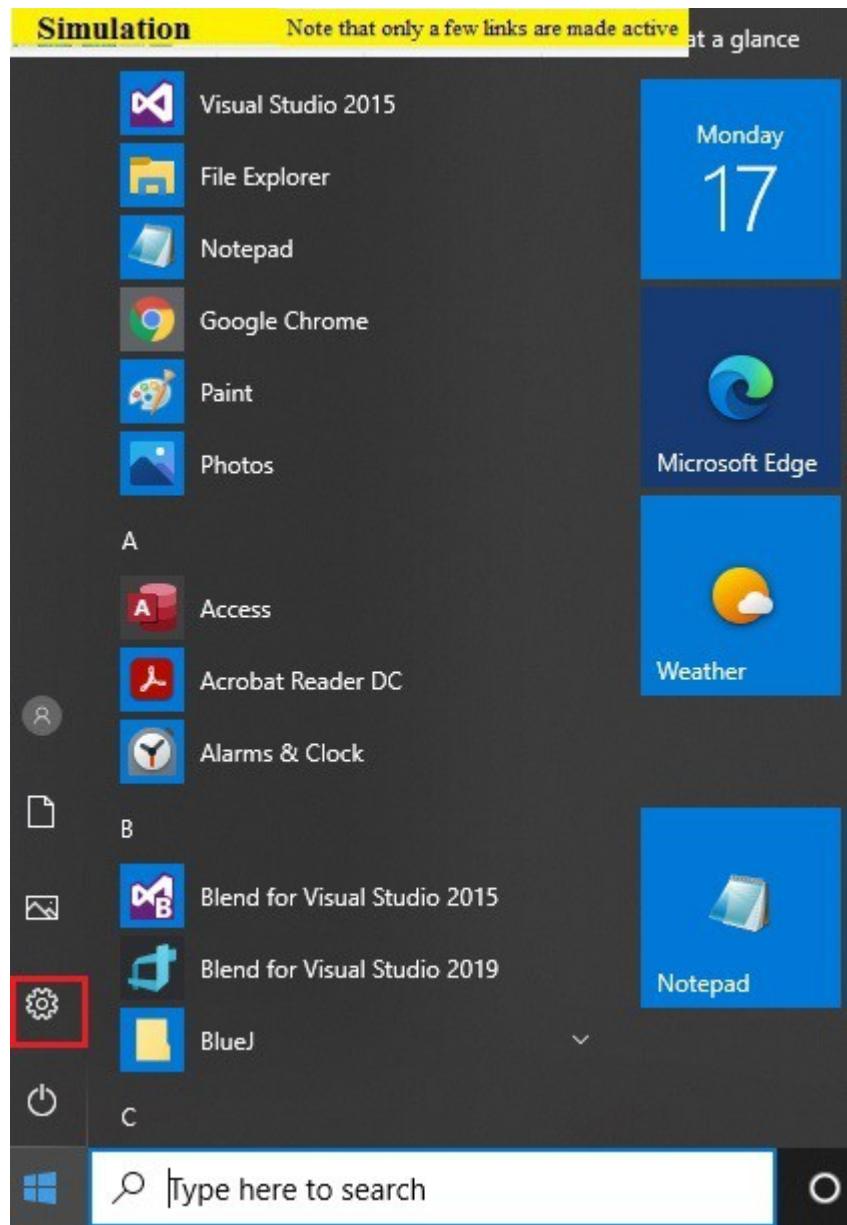
[Back](#)

5.37 Manage Location Services in Windows 10

Description: Lab Exercise explains how to turn the Windows location settings on or off:

Instructions:

1. From the Windows desktop, navigate: Start menu icon and click Settings icon



2. Select Privacy in the Windows Settings window.

Windows Settings

System

Display, sound, notifications,
power

Devices

Bluetooth, printers, mouse



Phone

Link your Android, iPhone



Network & Internet

Wi-Fi, airplane mode, VPN



Personalization

Background, lock screen, colors



Apps

Uninstall, defaults, optional
features

Accounts

Your accounts, email, sync,
work, family

Time & Language

Speech, region, date



Gaming

Game bar, captures,
broadcasting, Game Mode

Ease of Access

Narrator, magnifier, high
contrast

Search

Find my files, permissions



Cortana

Cortana language, permissions,
notifications

Privacy

Location, camera, microphone



Update & Security

Windows Update, recovery,
backup

3. Click **Location** in the left pane under App Permissions.

To set the location on or off, click Change button in 'Location for this device is on/off', then select the switch to turn on or off.

Home

Find a setting

Privacy

Windows permissions

General

Speech

Inking & typing personalization

Diagnostics & feedback

Activity history

App permissions

Location

Camera

Microphone

Location

Allow access to location on this device

If you allow access, you will enable Windows to use your device's capabilities to determine your location and Microsoft will use your location data to improve location services. People using this device will be able to choose if their apps have access to location by using the settings on this page. Denying access blocks Windows from providing location to Windows features, Microsoft Store apps, and most desktop apps.

Location for this device is on

[Change](#)

← Click this

Allow apps to access your location

If you allow access, you can use the settings on this page to choose which apps can access your device's precise location and location history to enable location-based experiences such as directions and weather. If you are signed in with a Microsoft account on this device, your last known location is saved to the cloud, and shared with other devices where you are signed in with your Microsoft account. Denying access only blocks the apps listed on this page from accessing your location.

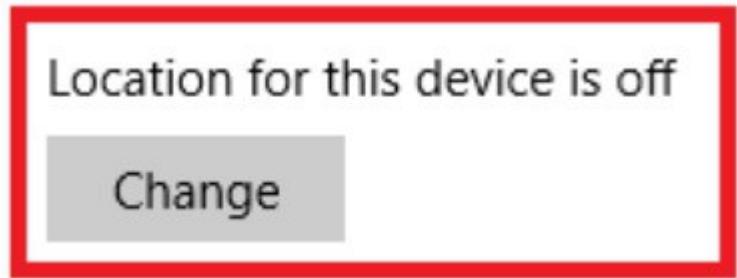
On

Some desktop apps may still be able to determine your location when settings on this page are off. [Find out why](#)

Location access for this device

On

Explanation: This is a global setting: only users with admin rights can change it. Failure to turn on this setting will leave location services disabled for all users. If you don't want any users on your machine to be able to use any form of location services,



Enable Location Services for a Specific User

Each user on the computer can enable or disable location services for their own account.

To enable location services for an individual user, go to Settings > Privacy > Location > Location service. Slide the toggle to the On or Off position, depending on your preferences.

Location service



Manage Which Apps Can Access Location Data

Once you've turned on location services for a user, you can establish which apps have access to their location data on a case-by-case basis. To change which apps can access the data, navigate to Settings > Privacy > Location > Choose apps that can use your precise location. Slide the toggle for each app to match your usage needs.

Location

Choose which apps can access your precise location

	App connector	<input type="checkbox"/> Off
	Camera	<input type="checkbox"/> Off
	Cortana	<input type="checkbox"/> Off
	Desktop App Web Viewer	<input type="checkbox"/> Off
	Mail and Calendar	<input type="checkbox"/> Off
	Maps	<input type="checkbox"/> Off
	Messaging	<input type="checkbox"/> Off
	Microsoft News	<input type="checkbox"/> Off

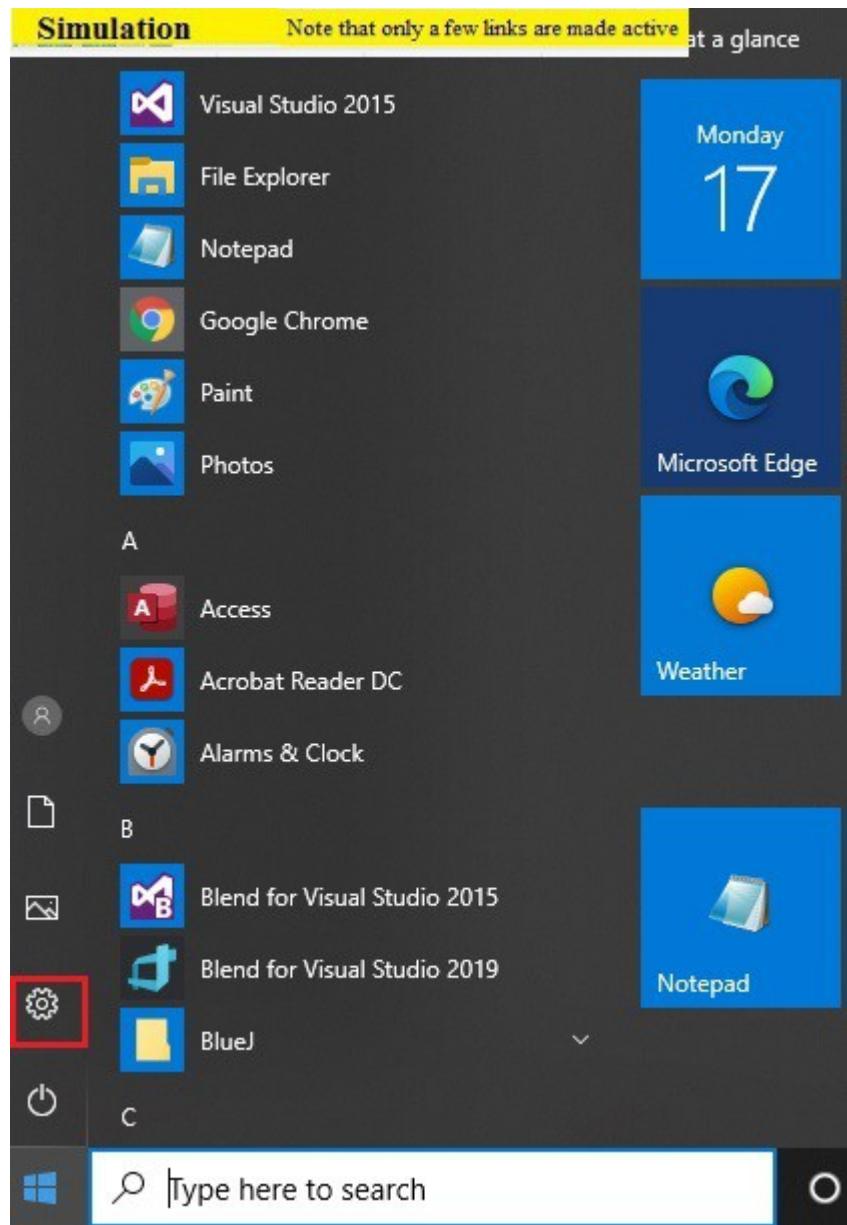
[Back](#)

5.38 Manage app permissions for camera in Windows 10

Description: Lab Exercise explains how to turn on app permissions for your camera in Windows 10 (system level).

Instructions:

1. From the Windows desktop, navigate Start menu icon and click Settings icon



2. Select Privacy in the Windows Settings window.

Windows Settings

System

Display, sound, notifications, power



Devices

Bluetooth, printers, mouse



Phone

Link your Android, iPhone



Network & Internet

Wi-Fi, airplane mode, VPN



Personalization

Background, lock screen, colors



Apps

Uninstall, defaults, optional features



Accounts

Your accounts, email, sync, work, family



Time & Language

Speech, region, date



Gaming

Game bar, captures, broadcasting, Game Mode



Ease of Access

Narrator, magnifier, high contrast



Search

Find my files, permissions



Cortana

Cortana language, permissions, notifications



Privacy

Location, camera, microphone

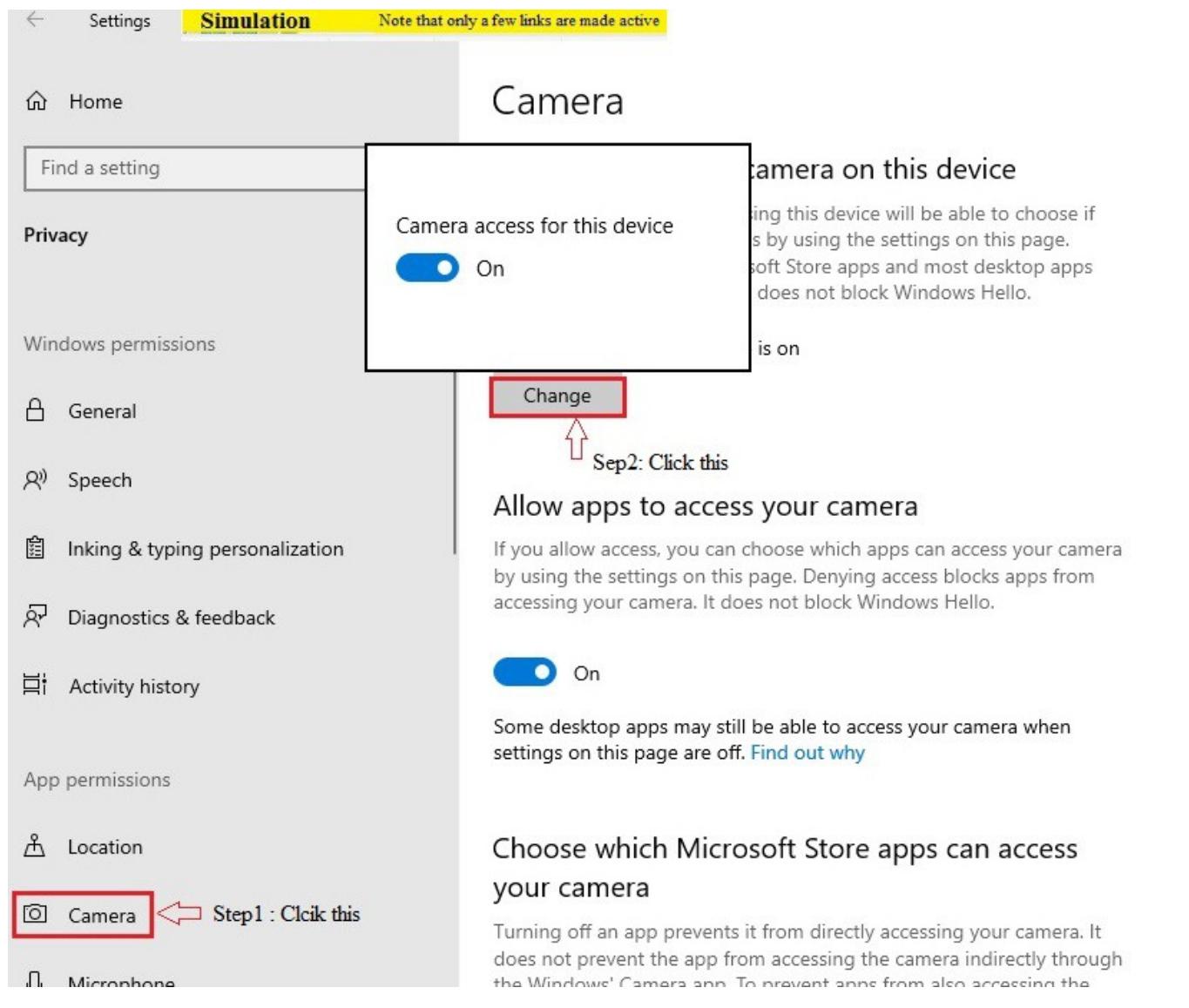


Update & Security

Windows Update, recovery, backup

3. Select Camera in the left pane under App Permissions.

In the right pane under “Allow access to the camera on this device” option select Change button and then select switch to turn on camera access feature.

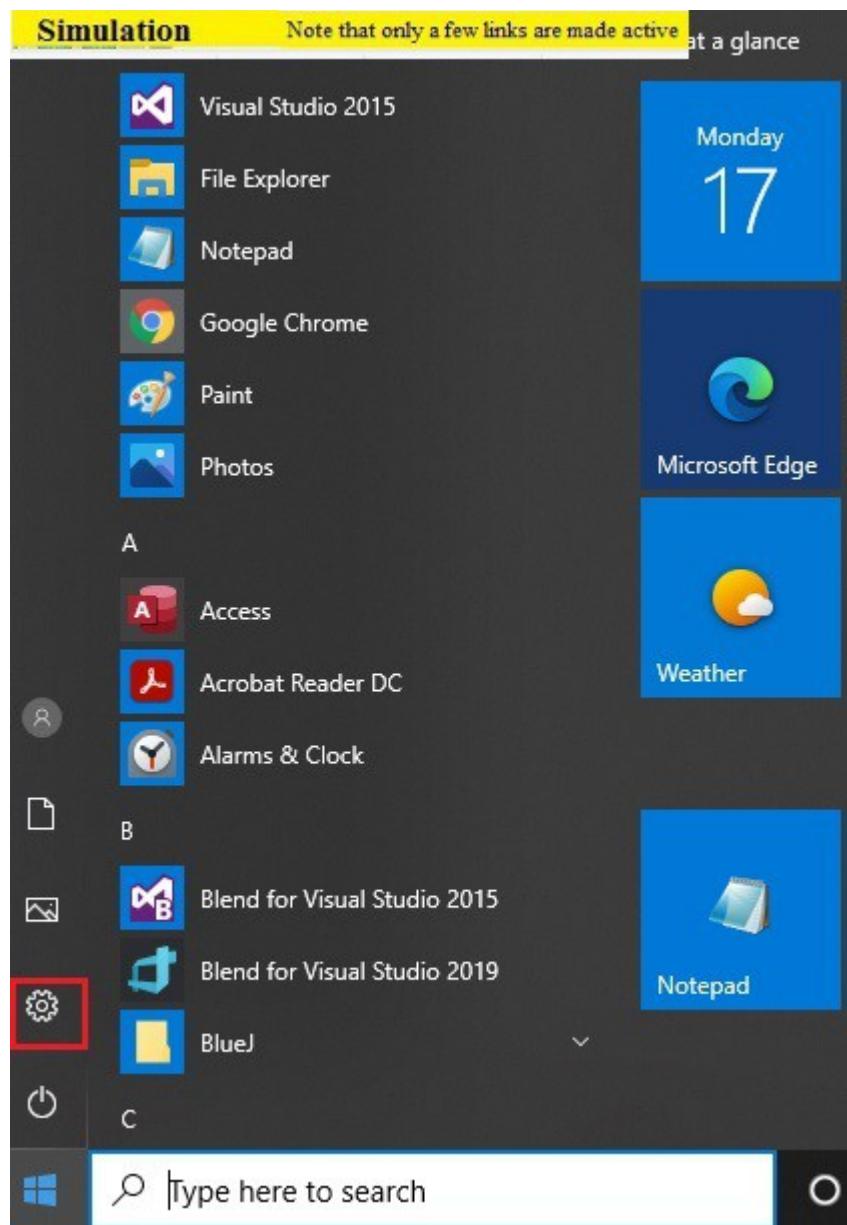


5.38 Auto Lock using screen saver in Windows 10

Description: The lab exercise explains how to automatically lock your system using Screen Saver in windows 10 system.

Instructions: 1. From windows 10 start menu click Settings icon

[Back](#)



2. In settings window click Personalization icon.

Simulation

Note that only a few links are made active

Windows Settings

 **System**Display, sound, notifications,
power**Devices**

Bluetooth, printers, mouse

**Phone**

Link your Android, iPhone

**Network & Internet**

Wi-Fi, airplane mode, VPN

**Personalization**

Background, lock screen, colors

**Apps**Uninstall, defaults, optional
features**Accounts**Your accounts, email, sync,
work, family**Time & Language**

Speech, region, date

**Gaming**Game bar, captures,
broadcasting, Game Mode**Ease of Access**Narrator, magnifier, high
contrast**Search**

Find my files, permissions

**Cortana**Cortana language, permissions,
notifications**Privacy**

Location, camera, microphone

**Update & Security**Windows Update, recovery,
backup

3. In the Personalization screen click Lock screen option.

Home

Find a setting

Lock screen

Preview



Personalization

Background

Colors

Lock screen

Themes

Fonts

Start

Taskbar

Background

Windows spotlight



4. In the right pane click Screen saver settings option.

In your Windows 10 system to access this feature Scroll down in right pane.

← Settings

Simulation

Note that only a few links are made active

Home

Find a setting



Personalization

Background

Colors

Lock screen

Themes

Fonts

Start

Taskbar

Lock screen

Background

Windows spotlight



Choose one app to show detailed status on the lock screen



Choose which apps show quick status on the lock screen



Show lock screen background picture on the sign-in screen



On

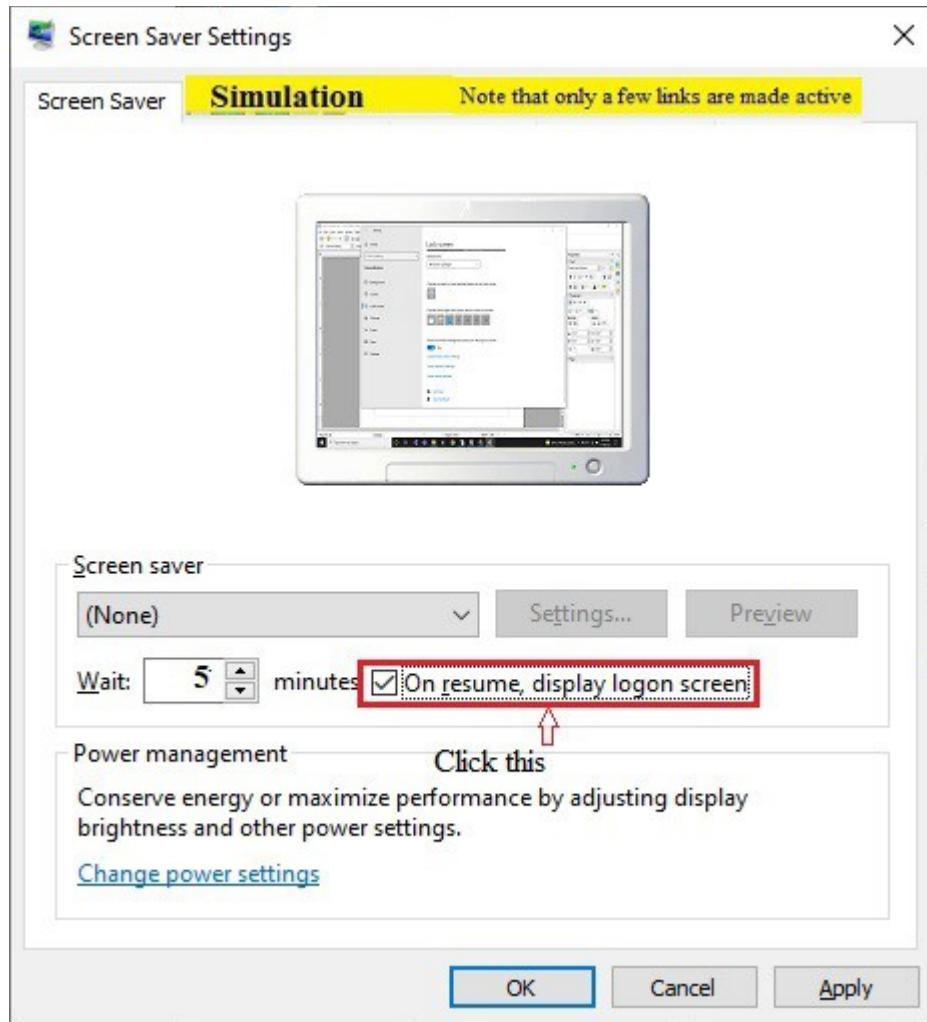
[Cortana lock screen settings](#)

[Screen timeout settings](#)

[Screen saver settings](#)

← Click this

5. Next, the Screen Saver Setting windows will come up. check the “On resume, display logon screen” box and set the “Wait” time to 5 minutes by clicking up arrow, and click Apply and then OK button.



[Back](#)

5.40 Uninstall or remove apps and programs in Windows 10

Description: This lab exercise explains uninstall and remove apps and programs in Windows 10 from settings page.

Instructions:

1. From the start menu click “Settings” icon
2. In the Settings window click “Apps” icon
3. You will be presented with “Apps & Features” window. In this window click the app you want to uninstall, a popup with 2 buttons displayed next to app , click “Uninstall” button.

In this lab exercise task is to uninstall **“Adobe Acrobat Reader DC”**

Windows Settings

 **System**

Display, sound, notifications, power

**Devices**

Bluetooth, printers, mouse

**Phone**

Link your Android, iPhone

**Network & Internet**

Wi-Fi, airplane mode, VPN

**Personalization**

Background, lock screen, colors

**Apps**

Uninstall, defaults, optional features

**Accounts**

Your accounts, email, sync, work, family

**Time & Language**

Speech, region, date

**Gaming**

Game bar, captures, broadcasting, Game Mode

**Ease of Access**

Narrator, magnifier, high contrast

**Search**

Find my files, permissions

**Cortana**

Cortana language, permissions notifications

**Privacy**

Location, camera, microphone

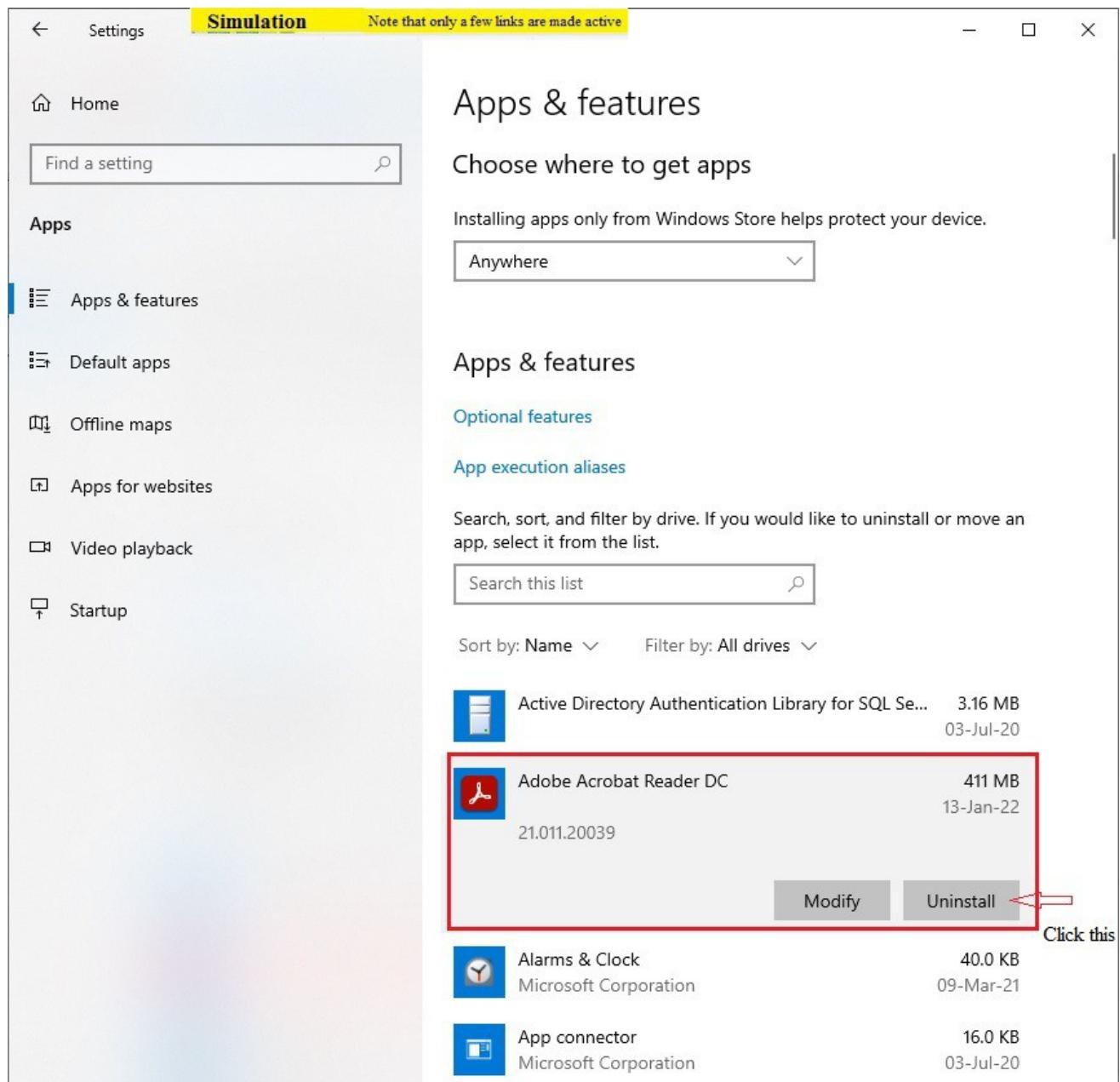
**Update & Security**

Windows Update, recovery, backup

3. You will be presented with “Apps & Features” window. In this window click the app you want to uninstall, a popup with 2 buttons displayed next to app , click “Uninstall” button.

In this lab exercise task is to uninstall **“Adobe Acrobat Reader DC”**

You will be provided with a popup saying “This app and its related info will be uninstalled “ click “Uninstall” button.



[Back](#)

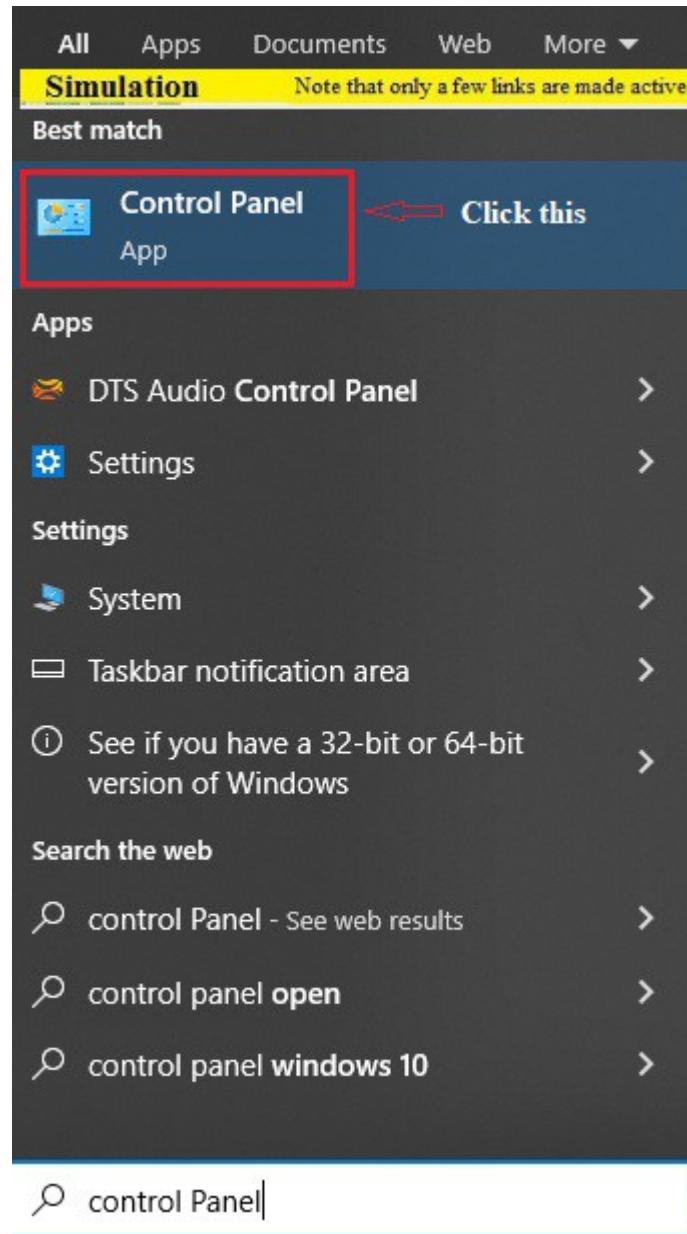
5.41 To stop automatic updates in Windows 10

Description: The lab exercise explains how to stop automatic updates in Windows 10

Instructions:

1. In a given Simulation start menu click Control Panel option.

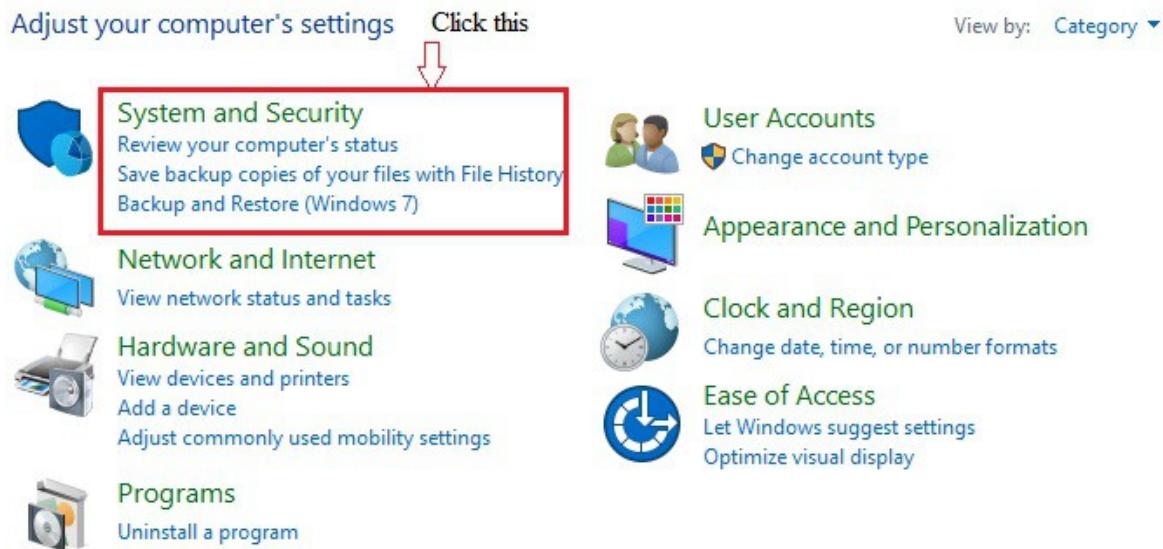
To access control Panel option in your Windows 10 system type “Control Panel” in search box and then click “Control Panel” option.



2. In Control Panel window click “**System and Security**”

Control Panel **Simulation** Note that only a few links are made active

← → ▴ ▾ Control Panel > Search Control Panel



3. In the next window click “**Administrative Tools**”

System and Security Simulation Note that only a few links are made active

Control Panel Home

• **System and Security**

- Network and Internet
- Hardware and Sound
- Programs
- User Accounts
- Appearance and Personalization
- Clock and Region
- Ease of Access

 **Security and Maintenance**
Review your computer's status and resolve issues |  Change User Account Control settings | Troubleshoot common computer problems

 **Windows Defender Firewall**
Check firewall status | Allow an app through Windows Firewall

 **System**
View amount of RAM and processor speed |  Allow remote access | Launch remote assistance | See the name of this computer

 **Power Options**
Change battery settings | Change what the power buttons do | Change when the computer sleeps

 **File History**
Save backup copies of your files with File History | Restore your files with File History

 **Backup and Restore (Windows 7)**
Backup and Restore (Windows 7) | Restore files from backup

 **BitLocker Drive Encryption**
Manage BitLocker

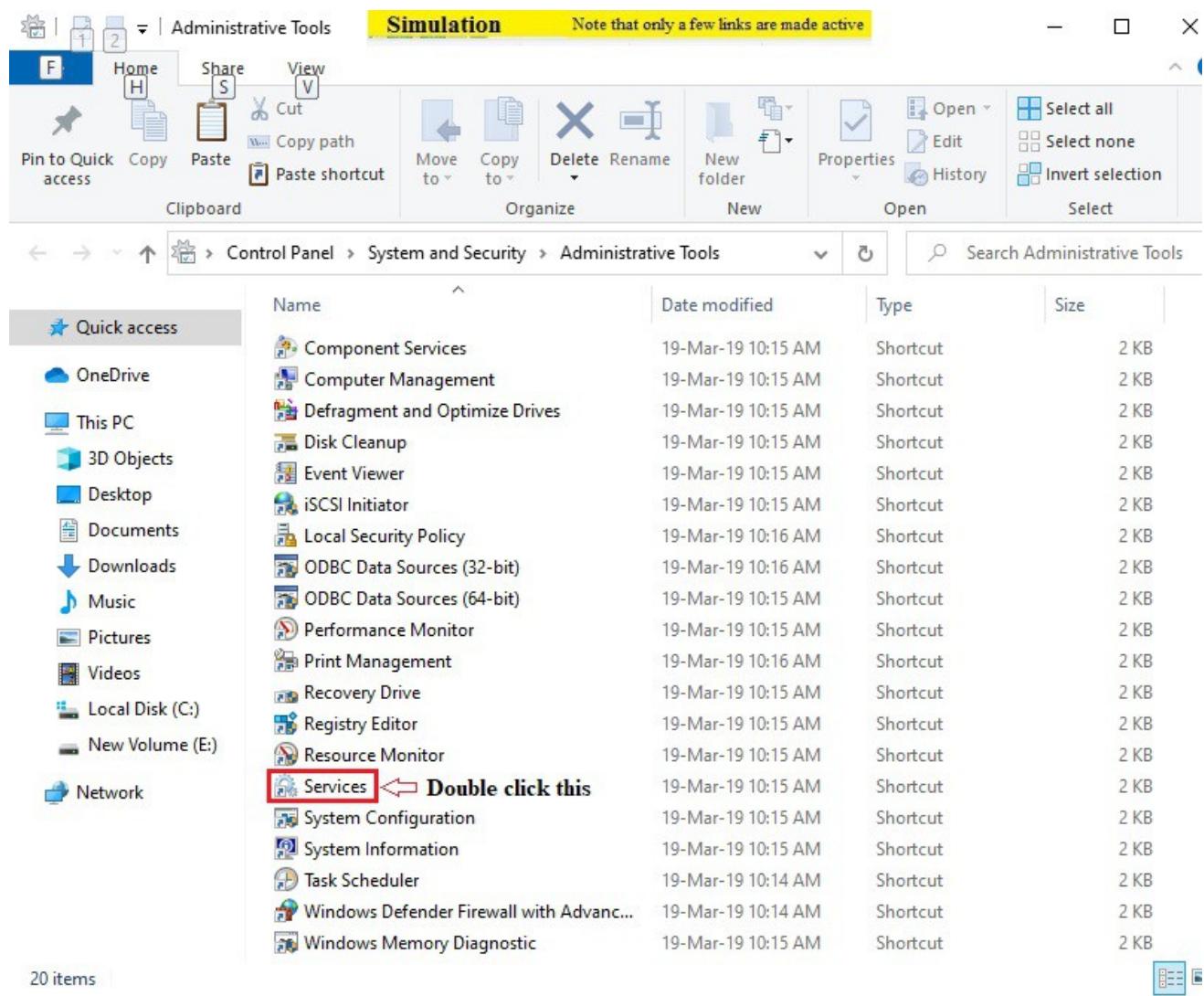
 **Storage Spaces**
Manage Storage Spaces

 **Work Folders**
Manage Work Folders

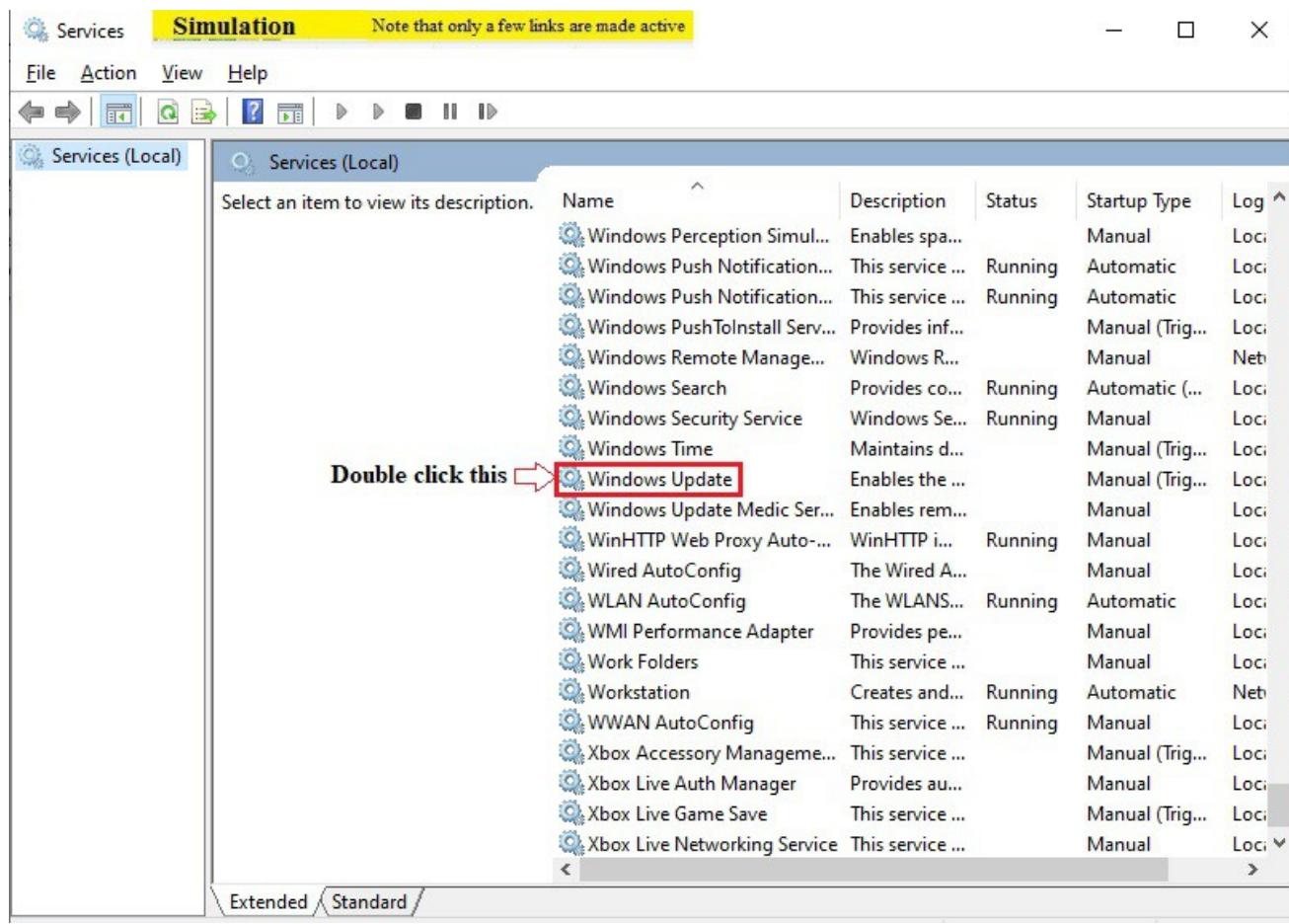
 **Administrative Tools**  Click this

Free up disk space | Defragment and optimize your drives |  Create and format hard disk partitions |  View event logs |  Schedule tasks

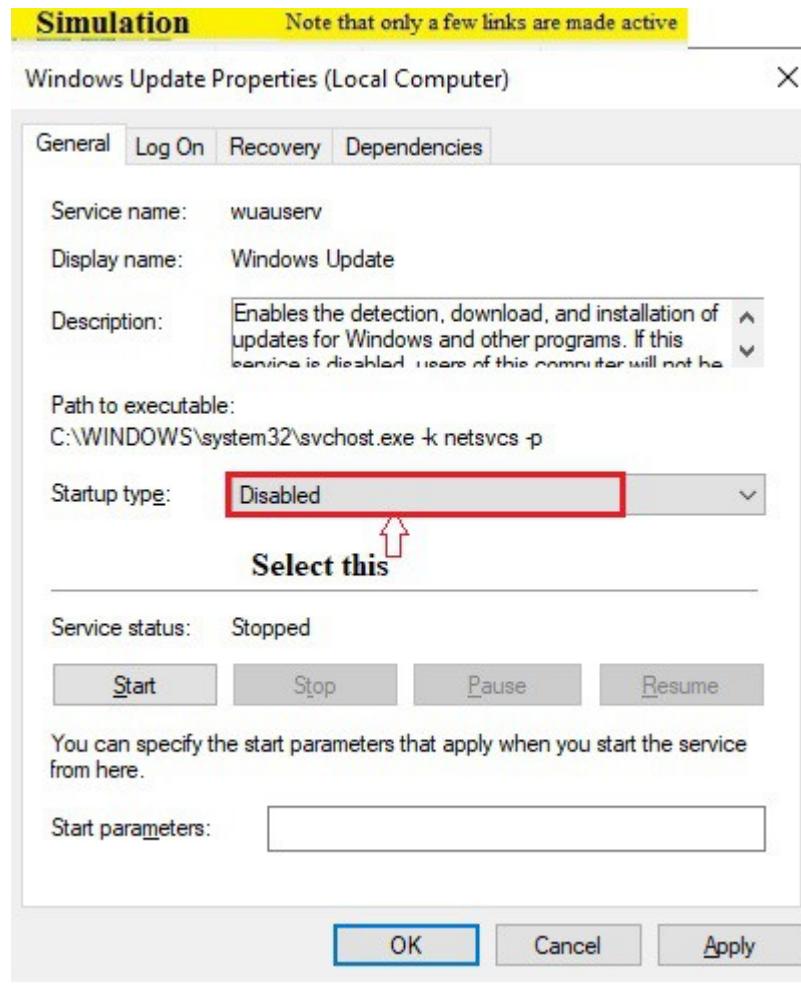
4. In the next window double click on “Services” option.



5. In services window scroll down to “**Windows Update**” in the resulting list and double click the Windows Update Entry



6. In the resulting dialog, select Startup Type to Disabled from drop down and then click Apply and then OK button.



Note: if the service is started, click 'Stop' button in the resulting window. (In your Windows 10 system).

Please Note: if you disable Windows 10 Updates, your system will be at risk from attack

1. Windows Defender will not be updated
2. Operating System patches will not be applied
3. You will not be able to use the Windows Store
4. Windows Apps will not update and possibly fail

On the plus side your hardware will continue to work!

[Back](#)

5.42 Objective Test 5 Answer the following questions

1. Windows 10 has a Refresh recovery option that helps you recover a PC that isn't behaving well. Using this recovery option you keep your personal files such as Music, Photos etc. but which of these will you lose?
 - A. Default Windows apps
 - B. OEM apps
 - C. Nothing
 - D. User installed apps

Answer: D

Explanation: Any user installed apps will be removed during the Refresh recovery option. It does however keep all of your personal files such as music, photos, videos etc. and it creates a file showing you all apps which were deleted (file on desktop).

2. An annoying piece of Firewall software runs everytime a Windows 10 workstation starts up. You want to make sure that this software does NOT run on startup, what should you do?

- A. Execute the msconfig.exe
- B. Modify the machine.config file
- C. Modify the app.config file
- D. Run the msinfo32.exe command

Answer: A

Explanation: msconfig.exe allows you to modify which programs run at startup.

3. Using a Windows 10 Provisioning Package you want to enroll a device into a subscribed service such as Intune. What is the name for this term?

- A. USMT
- B. Windows PE
- C. ICD
- D. MDM

Answer: D

Explanation: Mobile Device Management (MDM) - an industry term for the administration of mobile devices, such as smartphones, tablet computers, laptops and desktop computers.

4. Using a Windows 10 Provisioning Package you want to enroll a device into a subscribed service such as Intune. What is the name for this term?

- A. USMT
- B. Windows PE
- C. ICD
- D. MDM

Answer: D

Explanation: Mobile Device Management (MDM) - an industry term for the administration of mobile devices, such as smartphones, tablet computers, laptops and desktop computers.

5. Apps that are installed in the Windows image are called _____. These apps are staged in the image and are scheduled to be installed for every user of the Windows image at first logon or at the next logon, if the user account is already created.

- A. preloaded apps
- B. preinstalled apps
- C. provisioned apps
- D. intune apps

Answer: C

Explanation: Provisioned apps are specific to the PC and will not roam with the user. You can only install 24 provisioned apps in an image.

6. In Windows 8.1 the push-button recovery image was contained in a dedicated partition at the end of the hard drive. Rather than having to wipe and restore from an image, IT engineers could keep valuable data by using push-button recovery. In Windows 10, is the recovery image still stored in a dedicated partition?

A. Yes

B. No

Answer:B

Explanation: The partition and image no longer exist in Windows 10. Instead, the OS is rebuilt using existing files

7. What PowerShell command would you use to activate a sideloading product key?

- A. SideLoad /ipk <sideloading product key>
- B. Slmgr /ipk <sideloading product key>
- C. SideLoad /key <sideloading product key>
- D. Slmgr /key <sideloading product key>

Answer: B

Explanation: You would use the Software Licensing Management Tool (Slmgr) where <sideloading product key> is the 25 digit key to enable sideloading on the computer.

8. While booting Windows 10 computer you got an error message that Registry is corrupt. What should you do as a first step of troubleshooting?

- A. Boot to Recovery options
- B. Boot in Safe Mode
- C. Boot to Last Known Good Configuration
- D. Use Setup disks, and repair the installation
- E. Re-install the Operating System after formatting the drive

Answer:B

Explanation: If you fail to boot, first try to boot in Safe Mode. If it doesn't work, try booting to Last Known Good Configuration. If both fail, you can try using Recovery Console. You need to install the Recovery options for choosing this option on your Win 10 computer. If the option is not installed, you may get to the Recovery options by using the Win 10 installation CD ROM.

9. Your customer complains that his Windows 10 computer restarts immediately after a major error. What is likely cause?

- A. The hard disk corrupt
- B. The memory is corrupt
- C. The keyboard is not connected properly
- D. Automatic Restart option in Windows 10 is enabled

Answer:D

Explanation: The automatic restart option in Windows 10 is enabled by default. Errors might occur but not

display with Automatic restart enabled. Disable this option to allow the computer to display error messages instead of restarting.

1. In Windows, search for and open View advanced system settings.
2. Click Settings in the Startup and Recovery section.
3. Remove the check mark next to Automatically restart, and then click OK.

The ability to choose the restart options is very convenient as you can view any error messages and restore failed hardware.

10. You want to install device drivers for a new Network card on your windows 10 computer? Which tools do you use?

- A. Accessibility Options
- B. Device Manager
- C. Personalization
- D. Power Options

Answer: B

Explanation: The Device Manager lists all the hardware devices installed on your system. You can also update any existing drivers, as well as change the hardware settings. You use Add/Remove Hardware to install new hardware. Accessibility options is primarily used to configure the keyboard, display, and mouse options on a computer to accommodate the users who are physically handicapped. The Add/Remove Programs is used to install/uninstall 3rd party software.

11) **Which of the following data transfers will retain the current NTFS permissions of a file?**

- A. Copying the file to a different location on the same volume
- B. Moving the file to a different location on the same volume
- C. Moving the file to a different location on a different volume
- D. Copying the file to a different location on a different volume

Answer: B

Explanation:

1. When copying a file from one NTFS volume to a folder on another volume the file inherits the permissions of the destination folder.
2. When copying a file from one folder to new a folder on the same NTFS volume the file inherits the permissions of the destination folder.
3. When moving a file from one NTFS volume to a folder on another volume the file inherits the permissions of the destination folder.
4. When moving a file from one folder to new a folder on the same NTFS volume the file retains the permissions.

12) **The folder "Documents" is shared. The user can create and delete documents when on the local PC, but can only read documents when accessing them remotely. Which of the following should be adjusted?**

- A. Read Only Attribute
- B. Share Permissions
- C. Firewall Settings
- D. NTFS Permissions

Answer: B

Explanation:

Share permissions:

1. Apply only to users who gain access to the resource over the network. They do not apply to users who log on locally, such as on a terminal server.
2. Apply to all files and folders in the shared resource.
3. Are the only way to secure network resources on FAT and FAT32 volumes, because NTFS permissions are not available on FAT or FAT32 volumes.
4. Specify the maximum number of users who are allowed to access the shared resource over the network.

You can assign the following types of access permissions to shared folders or drives:

Read: Read is the default permission that is assigned to the Everyone group. Read allows: Viewing file names and sub folder names, Viewing data in files and Running program files

Change: Change is not a default permission for any group. The Change permission allows all Read permissions, plus: Adding files and sub folders, Changing data in files , Deleting sub folders and files

Full Control: Full Control is the default permission that is assigned to the Administrators group on the local computer. Full Control allows all Read and Change permissions, plus: Changing permissions (NTFS files and folders only).

13) Which of the following can be used as an appropriate boot device?

- A. DVD
- B. USB drive
- C. CD-ROM
- D. FDISK
- E. HDMI

Answer: B.

Explanation:

When you boot from a USB device, what you're actually doing is running your computer with the operating system that's installed on the USB device.

<http://pcsupport.about.com/od/tipstricks/ht/bootusbflash.htm>

14) Which of the following tabs under MSCONFIG would allow a technician to configure all of the applications that launch at boot?

- A. Startup
- B. Services
- C. Tools
- D. Boot

Answer: A

Explanation:

The Startup tab shows the items scheduled to begin at startup, the command associated with them, and the location where the configuration is done (usually, but not always, in the Registry). From here, you can enable or disable all. If a particular startup item has been disabled in Windows 10 and Windows 11, the date and time it was disabled will appear in the display.

15. Which is the correct path to view Windows Automatic Updates?

- A. Start | All Programs | Accessories | Administrator Tools | Windows Updates
- B. Start | All Programs | Windows Updates
- C. Start | Right-click Computer | Manage | Windows Updates
- D. Start | Right-click Computer | Windows Updates

Answer: B

16. Which command line tool is used to inspect and create a partition in Windows 10?

- A. Fdisk
- B. Format
- C. Diskpart
- D. Msinfo32

Answer: C

17. What is the default disk format option used for Windows 10?

- A. FAT16
- B. FAT32
- C. NTFS
- D. EFS

Answer: C

18. Which display resolution provides the least detail?

- A. VGA
- B. XGA
- C. SVGA
- D. UVGA

Answer: A

19. You are connecting your access point and it is set to root. What does Extended Service Set ID mean?

- A. That you have more than one access point and they are in the same SSID connected by a distribution system.
- B. That you have more than one access point and they are in separate SSIDs connected by a distribution system.
- C. That you have multiple access points, but they are placed physically in different buildings.
- D. That you have multiple access points, but one is a repeater access point

Answer: A, you have more than one access point and they are in the same SSID connected by a distribution system.

Explanation: Extended Service Set ID means that you have more than one access point and they all are set to the same SSID and all are connected together in the same VLAN or distribution system so users can roam.

20. When a user boots his computer, the monitor goes black. After investigating, you find out that he has set the refresh rate too high. How can you fix this problem?

- A. Reboot the computer
- B. Press F1 while booting
- C. Boot in VGA mode and change the refresh rate.
- D. Delete the boot.ini file

Answer: C

There is no way of entering a normal boot configuration when the refresh rate is set to a very high value. Enter the VGA mode that loads the generic video drivers and set the resolution to 640×480 at a refresh rate

of 60 Hz. This changes the refresh rate to an optimal value.

5.43 Microsoft Teams Labs

5.43.1 Creating a team using Microsoft Teams

Description: Microsoft Teams is an online communication and team collaboration tool that's part of the Microsoft Office 365 Suite.

This lab exercise demonstrates how to create teams in Microsoft Teams.

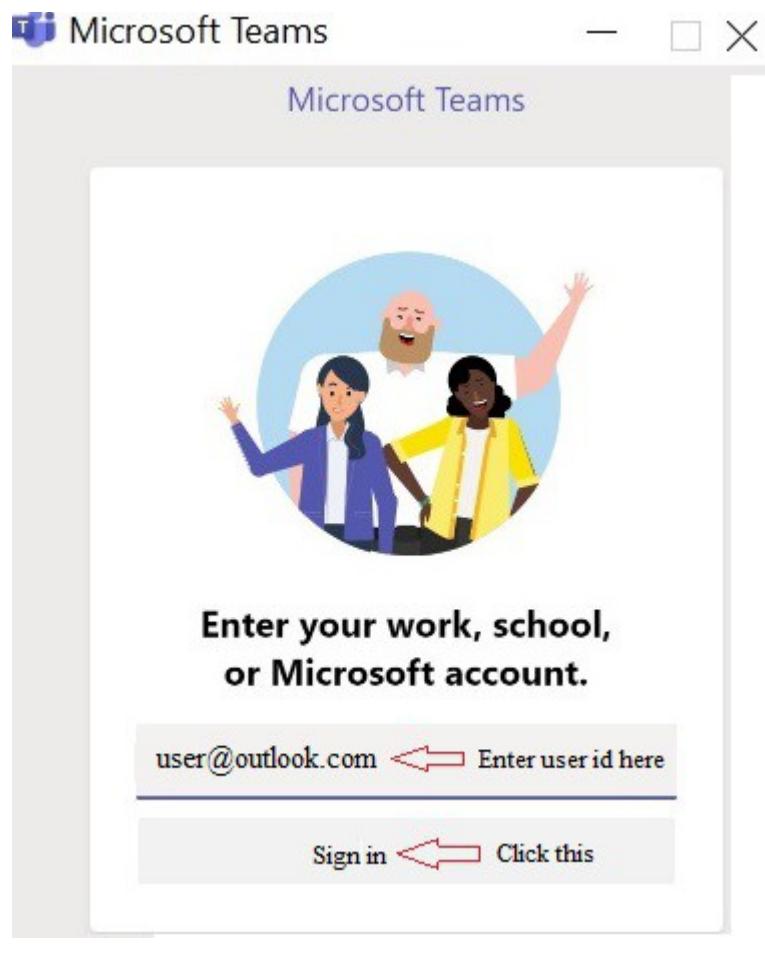
Note: It has been assumed that you already have account in Microsoft Teams and Microsoft Team App is downloaded and installed on your system.

Here we do the following

1. Login to your Microsoft Teams account.
2. Create new team by name Group1.

Instructions:

1. When the Teams app is first installed on your device, you may need to sign in again. Use the account that you created.
2. Enter the user id as “user@outlook.com” and click “Sign in “ button.



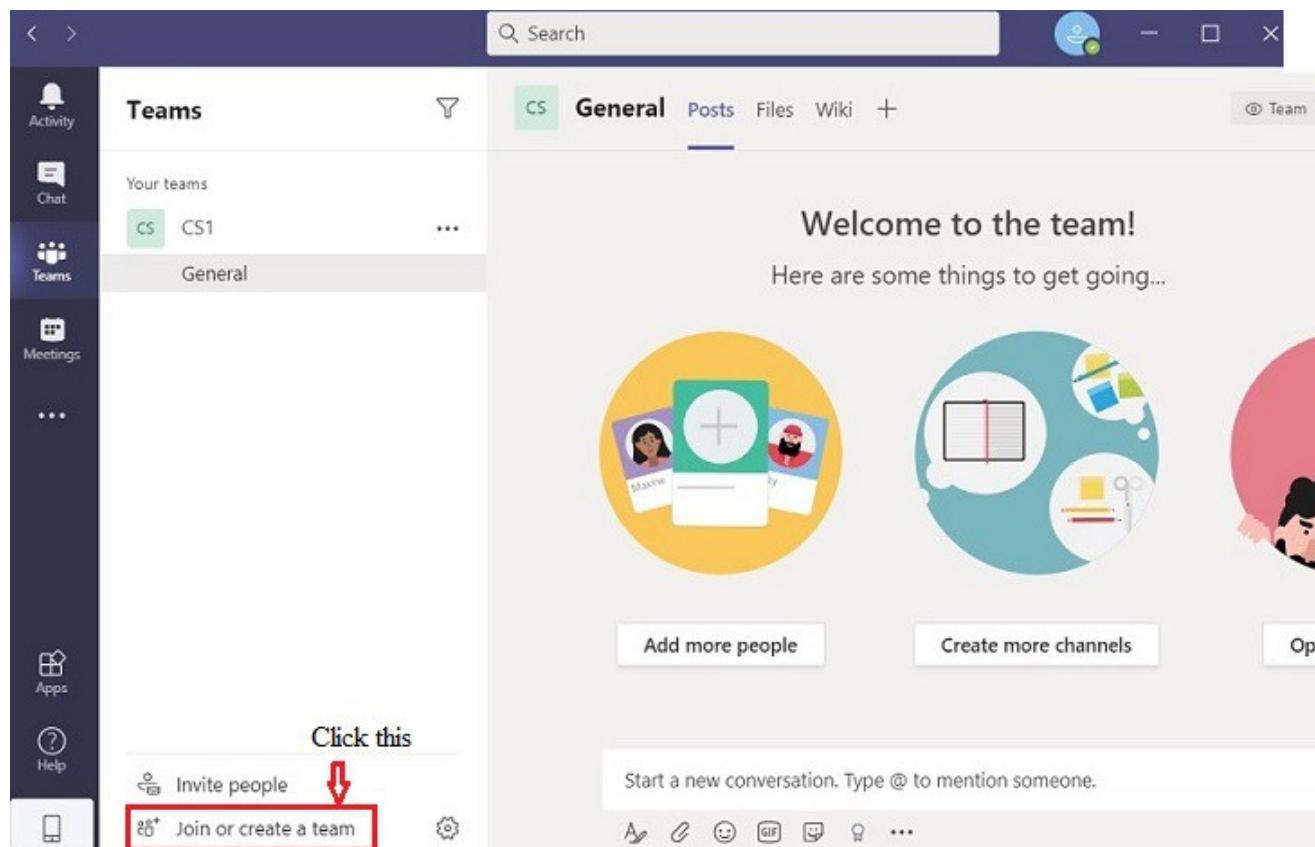
3. Next, you will be prompted for password, enter your Microsoft account password as “pass” and click **Sign in** button.



Now you should be able to access Microsoft Teams. With Microsoft Teams open to the Teams tab, look to the bottom of the space where all of your teams and channels are listed, where you'll find the Join or Create a Team button . It's here you can create teams, or join ones in your organization that

are open to everyone but aren't automatically joined when a new account is created.

4. To create a team , in the Microsoft Teams app click “Join or create a team” option at the bottom of the Teams sidebar on the left.



5. On the new screen that appears, click on the “Create team” button.

The screenshot shows the Microsoft Teams interface. On the left, there's a vertical sidebar with icons for Activity, Chat, Teams (which is selected), Meetings, Calls, Files, ..., Apps, Help, and a mobile device icon. The main area is titled 'Join or create a team'. It shows a 'Create a team' section with a plus sign icon, three dark circles, and a 'Create team' button. A red arrow points to the 'Create team' button with the text 'Click this' below it. At the bottom of the central panel, there are links for 'Invite people' and 'Join or create a team'.

6. On the following screen, you can choose:

- Build a team from scratch
- Create from an existing Office 365 group or team

If your team was using Office 365 before signing up for Teams, you may have existing groups that can be added using the “Create from...” option. Otherwise, go with “Build a team from scratch.”

click “Build a team from scratch” option.

The screenshot shows a 'Create your team' dialog box. It features a cartoon illustration of three people working together. Below the illustration, there are two main options: 'Build a team from scratch' (represented by a blue icon with a white plus sign) and 'Create from...' (represented by a green icon with a white arrow). A red arrow points to the 'Build a team from scratch' button with the text 'Click this'.

7. Next, define who's part of the Team.

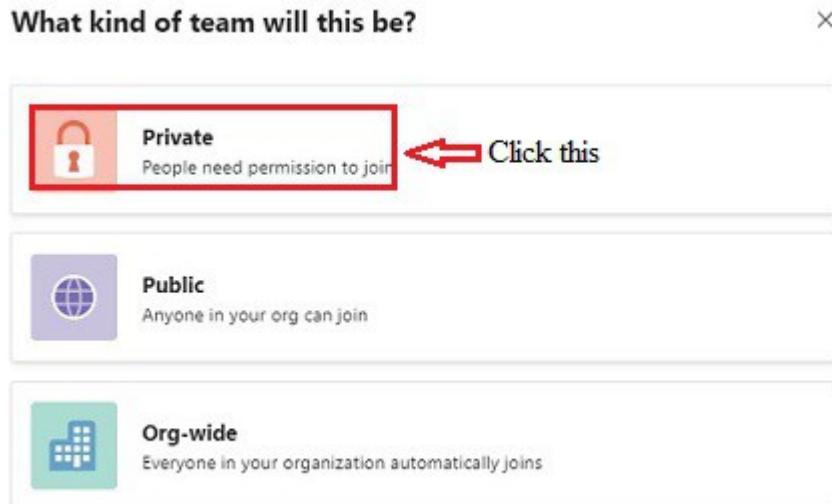
Make your choice based on how you want to organize your platform:

Private: If the team should only have a few specific members, select Private.

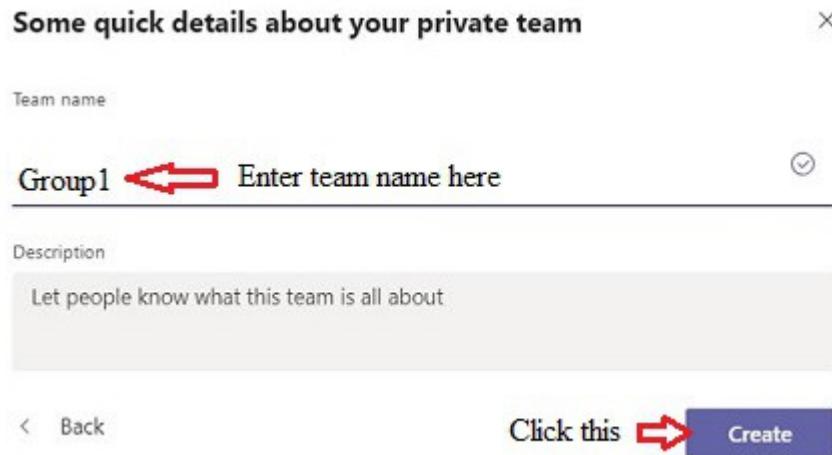
Public: Best for teams with changing members.

Org-Wide: If you want to host your entire organization as one “team” on the platform and use channels to divide departments, Org-wide is the ideal option.

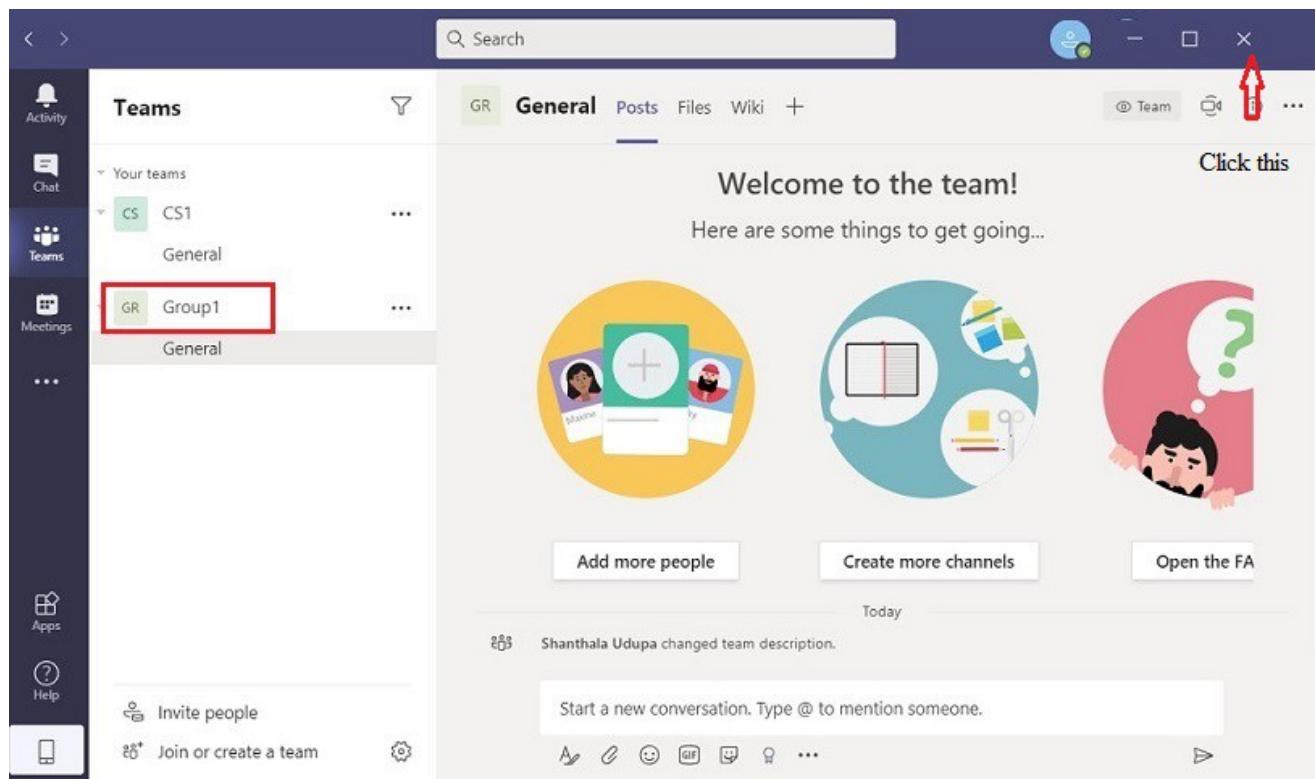
Click “Private”



8. Once you've chosen the type of team you want to create, you need to give it a name. Choose an appropriate team name. In this lab give the team name as “Group1” and click “Create” button.



9. Your new team will now appear on the left sidebar of your Teams app (“Group1” in the image below). Click Close button to complete the lab.



Explanation: Microsoft Teams is a collaboration app that helps your team stay organized and have conversations all in one place. Microsoft Teams is a digital hub that brings conversations, meetings, files, and apps together in one place. Because it's built on Office 365, schools benefit from integration with their familiar Office apps and services. It delivers enterprise-grade security and compliance that is extensible and customizable to fit the needs of every school.

With Microsoft Teams, your school or institution can create collaborative classrooms, connect in professional learning communities, communicate with school staff, coordinate research across institutions, or more easily facilitate student life efforts like clubs or extracurricular activities – all from a single experience in Office 365 for Education.

Microsoft Teams allow staff to focus on their roles as educator, researchers, and leaders in school or institution. Teams can help you:

- Create dedicated channels for specific tasks or teams.
- Record audio and video meetings.
- Easily share your screen with team members for detailed explanations.
- Quickly search through archives using its command box.
- Enabling Teams for your school
- Learning what kind of controls are available to manage Teams within your school
- Finding partner services through references to external documentation

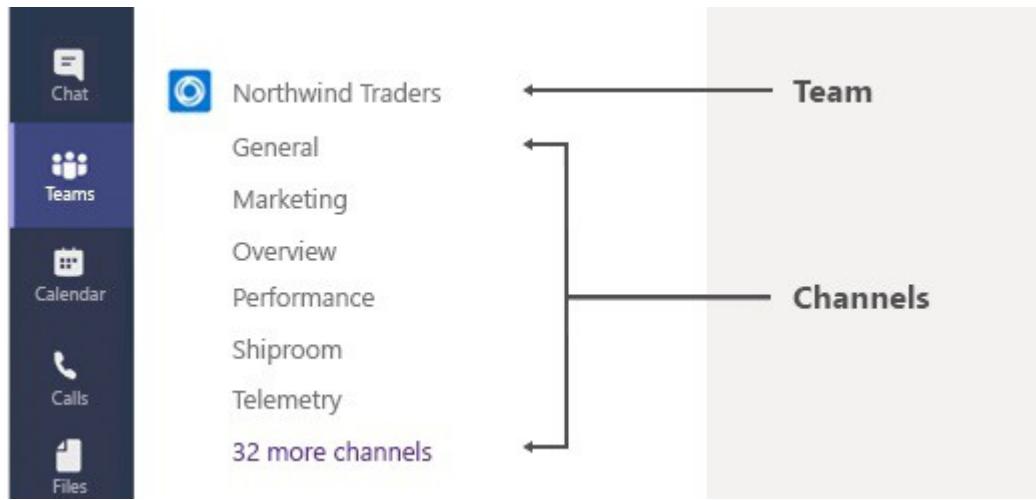
In Microsoft Teams, a Team is a group of people who collaborate together, usually consisting of the entire organization.

Features of Microsoft teams

Teams - Find channels to belong to or create your own. Inside channels you can hold on-the-spot meetings,

have conversations, and share files. A team is a group of people gathered to get something big done in your organization. Sometimes it's your whole organization.

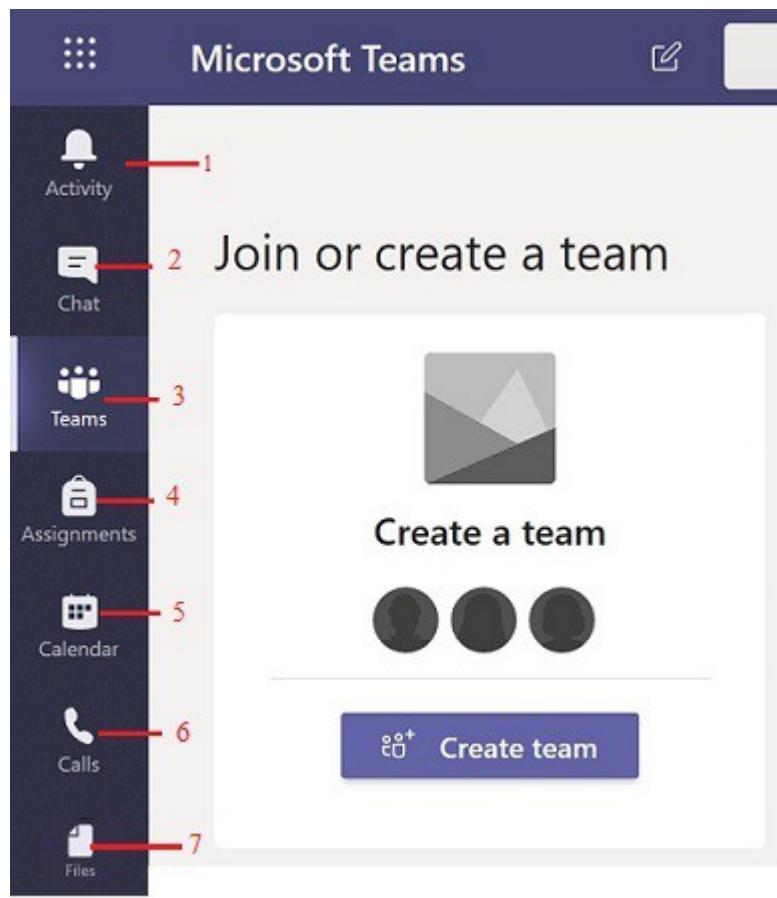
Teams are made up of channels, which are the conversations you have with your teammates. Each channel is dedicated to a specific topic, department, or project.



By default, all members of a team can create channels. A standard channel is open for all members and anything posted is searchable by others. If you need a smaller audience for a specific project, you can create a private channel for your team.

Channels: Channels are dedicated sections within a team to keep conversations organized by specific topics, projects, disciplines whatever works for your team! Files that you share in a channel (on the Files tab) are stored in SharePoint. Channels are places where conversations happen and where the work actually gets done. Channels can be open to all team members or, if you need a more select audience, they can be private. Standard channels are for conversations that everyone in a team can participate in and private channels limit communication to a subset of people in a team. Channels are most valuable when extended with apps that include tabs, connectors, and bots that increase their value to the members of the team.

The below gives you a brief overview of each section:



1. Activity: The activity section will show all new activity taking place within your team. This could include

- File Uploaded
- New Calendar events
- Recorded video sessions
- Chat conversations

2. Chat: The chat section will allow you to have real-time conversations with others within the team. The primary intention of this function is to communicate with your students , if there are questions about assignments, schedules etc.

Note: In some teams, teachers have opted to disable this function. If this is the case, please communicate with your student's teacher via email.

Students should not be using the chat function to send private messages to their friends during instruction.

3. Teams: Once logged in, you will see one or more modules that represent grade level classes. (i.e. 1st Grade Team). Click on the box for your class. Please note that in the early stages of roll-out, grade level teachers will be team-teaching all classes together.

4. Assignments: Teachers may choose to use this function to post upcoming assignments for the class.

Students should submit completed assignments through this section, unless instructed otherwise by the teacher.

5. Calendar: User can see everything got lined up for the day or week. Or, schedule a meeting. This calendar syncs with your Outlook calendar.

6. Calls - In some cases, if your organization has it set up, you can call anyone from Teams, even if they're not using Teams.

7. Files: Documents related to class activity will be accessible in the Files folder. Please note:

- Files found in the “Class materials” folder are read-only instructional files and students cannot edit them.
- Files found outside of the “class materials” folder can be used collaboratively, and students have the ability to edit them at the teacher's direction.

[**Back**](#)

5.43.2 Joining a meeting using Microsoft Teams

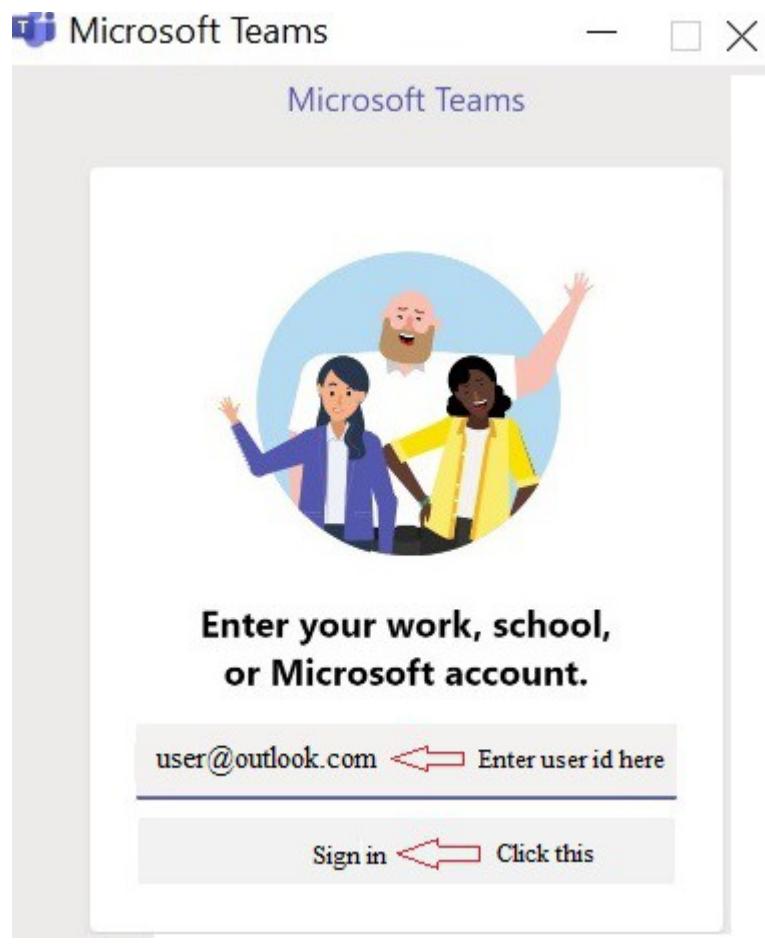
Description: The lab exercise demonstrates how to join Microsoft Teams meeting.

Here we do the following

1. Login your Microsoft Teams account provided by your organization.
2. Join Microsoft Teams Meeting by selecting ‘Calendar’ on the left side of the app.

Instructions:

1. Login to Microsoft Team using your login id as “user@outlook.com”



2. Enter you password as “pass”.



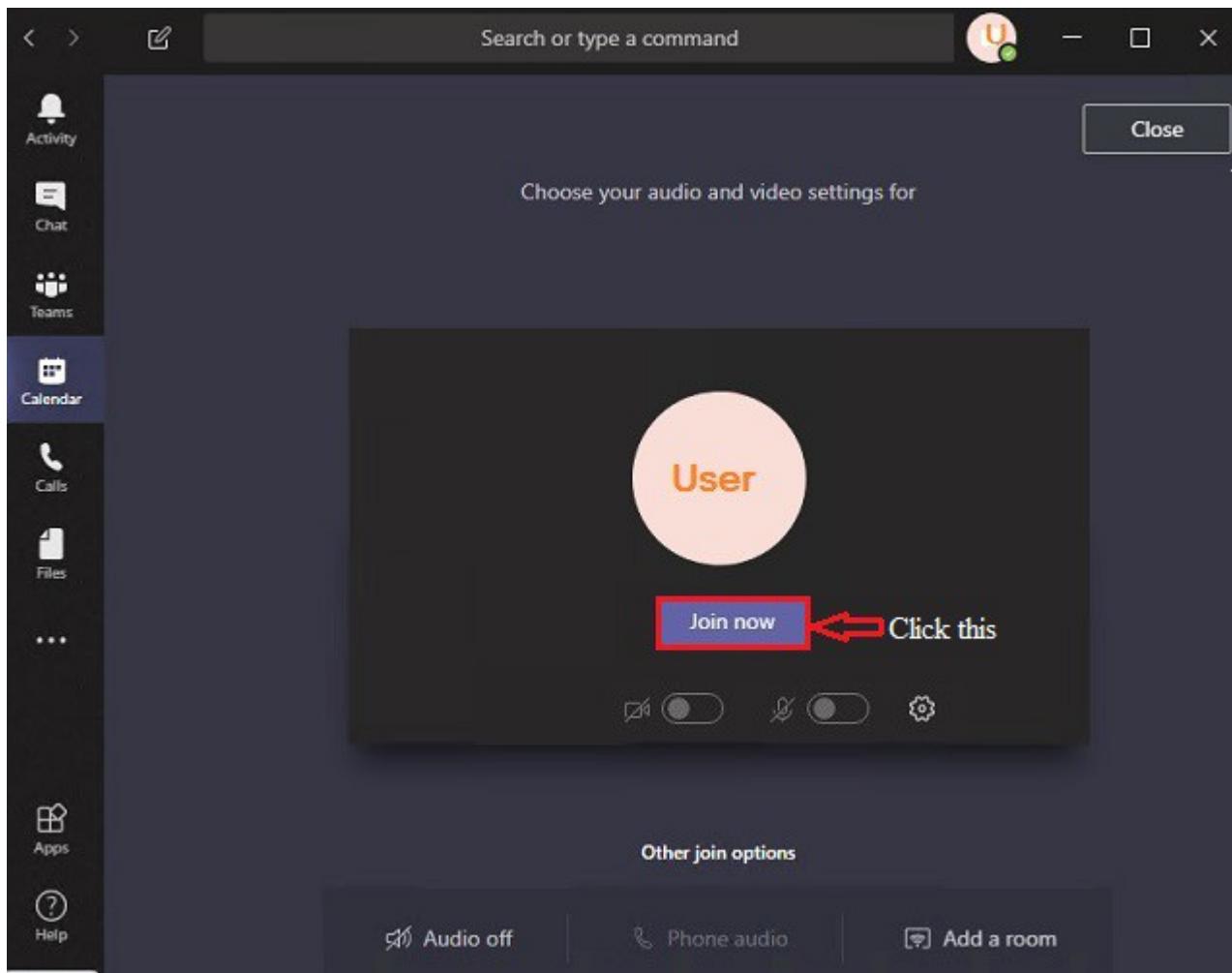
3. In the “Teams” application, you will see a number of tabs in the left hand side bar (Activity, Chat, Teams, Assignments, etc.). If a teacher has already added you to their class team, you will now see it listed. Select the meeting from "**Calendar**" in Microsoft Teams app:
Select **Calendar** on the left side of the app to see your meetings.

The screenshot shows the Microsoft Teams application window. On the left, there's a sidebar with icons for Activity, Teams, Assignments, **Calendar** (which is highlighted with a red box), Stream, Calls, ..., Apps, and Help. The main area shows a team named "General". A pinned message from "SS" says, "The meeting 'Group1 - Physics' has been cancelled" and "Replies are disabled". Below it, a "Meeting now" card for "Group1" shows a "Join" button and participant icons. A message from "Nandhi Darshan-Staff" at 8:27 AM says, "Scheduled a meeting" and lists an "August Test Meeting - CHEMISTRY, Group1" on Friday, August 28, 2020, at 2:15 PM. There are 9 replies from Nandhi Darshan. A note below says, "You've been muted, so you can't start a conversation". At the bottom, there are various message and file icons.

4. List of meeting scheduled displayed click on the individual meeting you'd like to join
Click on “Join” button.

The screenshot shows the Microsoft Teams calendar for August 2020. The sidebar on the left includes Activity, Teams, Assignments, **Calendar**, Stream, Calls, ..., Apps, and Help. The calendar view for August 2020 shows the days from Monday, August 24, to Friday, August 28. On Tuesday, August 25, there are three scheduled meetings: "Mathematics Group3 Cancelled" at 2 PM, "English Group1" at 3 PM, and "Physics Test Meeting" at 4 PM. The "English Group1" entry has a red box around the "Join" button, which is also highlighted with a red arrow and the text "Click this". The "Work week" option is selected at the top right.

5. After clicking the Join button, you will be directed to the meeting and asked to choose your audio and video settings before joining. Click the “Join now” button and you'll be placed into the meeting.



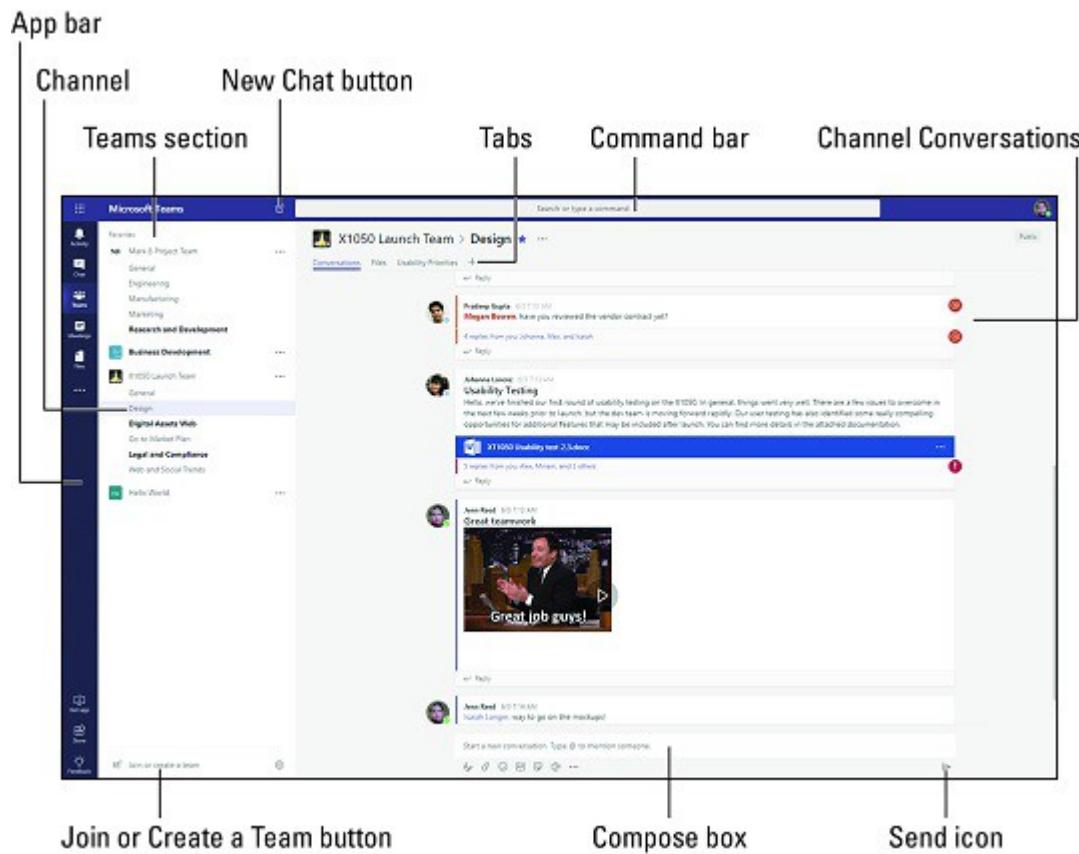
Explanation: Microsoft Teams is a collaboration app that helps your team stay organized and have conversations - all in one place. Here's a quick look at the left hand side of Teams.

Accessing Microsoft Teams

1. Open a web browser.
2. Navigate to <https://www.office.com/>
3. Note: It is not necessary to purchase an Office 365 subscription. Each student has a subscription provided by Lighthouse.
4. Login using your LCS Microsoft Office account credentials
 - a. Username for a student is: `firstname.lastname@lcstudent.net`
 - b. Password: Password is same as students use for Accelerated Reader and computer lab. If your student does not know their password, each teacher has a list of their students' passwords. You may email your student's teacher to request the password or email support@lcschool.org.
5. Once logged in, you will see a menu of available office applications. Select “Teams”.
6. This will launch the application in your browser.

7. For accessing MS Teams in the future, you may utilize the browser version (as is detailed above) or you may choose to download the Teams client to install on your computer.
8. If you choose to download the client to your computer, click on the icon on the bottom left corner of the page that displays a computer monitor with a down arrow. (Example below)
9. App download is encouraged if possible as some web functionality may be limited when access through a web browser.
10. MS Teams can be accessed through any device – computer, tablet, iPhone

The below gives you a brief overview of each section:



App bar: Here you can navigate to the various sections in Teams. From the top, you'll see the following icons:

- **Activity** is where you'll find mentions, replies, and other notifications.
- **Chat** is where you'll see your recent one-on-one or group chats and your Contacts list.
- **Teams** displays all the Teams you are a member of.
- **Meetings** is synched with your Outlook calendar and displays all your upcoming meetings.
- The new '**Calendar**' app that will replace Meetings retains existing functionality while introducing a range of new features:

- Three new types of calendar views: Day, Work week and Week view (default).
- Users will have the ability to go back or forward in time in their calendar to see any past or future meeting respectively.
- Users will be able to perform key actions on meetings such as Join, RSVP, Edit, and Cancel from the right-click menu on meetings displayed.
- Meetings on the calendar will light up to indicate when someone joins it online.
- User's current exchange setting for working hours and working days of the week will be respected in this new calendar.
- Users will be able to schedule events on their calendar without adding any attendees in the Teams scheduling form.
- Non-Teams meetings can also be edited and updated from Teams as part of this release.

- Files aggregates all the files from all the Teams you are a member of. It is also where you access your personal OneDrive for Business storage.
- [...] includes links to apps that are tied to Teams and the channels within Teams.
- Store takes you to apps and services that can be integrated into Teams.
- Feedback takes you to the Microsoft Teams user voice page where you can leave feedback about the service.

Teams section: Above, the Teams icon is selected in the App bar, so the list of the teams we are members of are displayed here.

Channel: A dedicated section within a Team to organize conversations and tasks into specific topics or projects.

Join or Create a Team button: Clicking this button takes you through the process of creating or joining a team. This button is only visible when the Teams icon is selected in the App bar.

New Chat button: Clicking this button selects the Chat icon in the App bar and allows you to start a new chat with an individual or a group.

Command bar: This bar at the top is used to query apps or perform a search in Teams.

Tabs: Switch between different Teams pages with these tabs. Conversations and Files are automatically included; the + sign tab allows you to add shortcuts to content in Teams.

Channel Conversations: This section displays all the conversations in the selected channel. Chats in Channel Conversations are persistent, so if you've been away, it's easy to scroll through to get caught up when you get back. Chats can include visual indicators such as the @mention, which indicates that the chat specifically mentions a user, or a red bang to indicate high importance. Take note that chats are open by design so everyone in the team has visibility to the conversation to help speed up the decision-making process when needed.

Compose box: This is where you can type a message to start a conversation. You can send a quick chat or expand the Compose box to access rich formatting tools.

Send icon: When you're ready to share your chat, click the Send icon to post your chat to the team.

[Back](#)

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	Column B
1. Social engineering	1. It is the use of deception and manipulation to obtain confidential information.
2. Malware	2. Software that is specifically designed to gain access or damage a computer without the knowledge of the owner.
3. Rootkits	3. Type of malicious software that is activated each time your system boots up.
4. Phishing	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. Shoulder surfing	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.

[Back](#)

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

1. Viruses
2. Worms
3. Trojans

Column B

1. Attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels.
2. Self-replicating virus that does not alter files but resides in active memory and duplicates itself.
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.

[**Back**](#)

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

Description: This exercise helps to know about various digital security methods and their features.

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

Column A	Column B
1. Antivirus	1. Type of utility used for scanning and removing viruses from your computer.
2. Firewall	2. A system designed to prevent unauthorized access to or from a private network.
3. Antispyware	3. Type of software that is designed to detect and remove unwanted pop-ups, slow performance, and security threats caused by spyware programs.
4. User authentication	4. A process that ensures and confirms a user's identity.

Explanation:

Antivirus: Anti-virus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more.

Firewall: A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several types of firewall techniques that will prevent potentially harmful information from getting through:

- Packet Filter:** Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
- Application Gateway:** Applies security mechanisms to specific applications, such as FTP and

Telnet servers. This is very effective, but can impose a performance degradation.

3. **Circuit-level Gateway:** Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
4. **Proxy Server:** Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

Antispyware: Anti-spyware software detects spyware through rules-based methods or based on downloaded definition files that identify common spyware programs. Anti-spyware software can be used to find and remove spyware that has already been installed on the user's computer, or it can act much like an anti-virus program by providing real-time protection and preventing spyware from being downloaded in the first place.

User authentication: Authentication begins when a user tries to access information. First, the user must prove his access rights and identity. When logging into a computer, users commonly enter usernames and passwords for authentication purposes. This login combination, which must be assigned to each user, authenticates access. However, this type of authentication can be circumvented by hackers. A better form of authentication, biometrics, depends on the user's presence and biological makeup (i.e., retina or fingerprints). This technology makes it more difficult for hackers to break into computer systems

[**Back**](#)

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

Description: This exercise helps to know about various physical security methods and their features.

Instructions: 1. Various physical security methods are given on the column A
2. Their features are given on the column B
3. Match (drag & drop) the physical security method given on the column A with their respective features given on the column B

Column A

1. Tailgating
2. Biometrics
3. Key fobs
4. Tokens
5. Privacy filters
6. RFID badge

Column B

1. Type of utility used for scanning and removing viruses from your computer.
2. Authentication technique that rely on measurable physical characteristics that can be automatically checked.
3. A small hardware device with built-in authentication mechanisms.
4. Process of substituting a sensitive data element with a non-sensitive equivalent that has no extrinsic or exploitable meaning or value
5. A panel that is placed over a display to make it difficult or impossible for someone to see the screen without being directly in front of the display.
6. Used for identification purposes and to speed up a registration process by reducing wait time and long lines since they are read instantly.

Explanation:

Tailgating: is the term used for someone being so close to you when you enter a building that they are able to come in right behind you without needing to use a key, a card, or any other security device.

Biometrics: It is the identification of a person by the measurement of their biological features. For example,

a user identifying themselves to a computer or building by their finger print or voice is considered a biometrics identification. When compared to a password, this type of system is much more difficult to fake since it is unique to the person. Various commonly used biometric devices are:

1. **Face scanner:** Biometric face scanners identify a person by taking measurements of a person face.
2. **Hand scanner :** A biometric hand scanner will identify the person by the palm of their hand.
3. **Finger scanner :** biometric finger scanner identifies the person by their finger print.
4. **Retina or iris scanner:** A biometric retina or iris scanner identifies a person by scanning the iris or retina of their eyes.
5. **Voice scanner:** a voice analysis scanner will mathematically break down a person's voice to identify them.

Key fobs: A key fob is a small electronic security device with built-in authentication protocols or mechanisms to allow whoever possesses it to enter a secured network or location in order to access data or services. A key fob is designed to be small so that it can be carried around inconspicuously just like a key chain, hence the name key fob.

Tokens: Physical tokens are anything that a user must have on them to access network resources and are often associated with devices that enable the user to generate a one-time password authenticating their identity. Secure ID, from RSA, is one of the best known examples of a physical token

Privacy filters: Privacy filters are either film or glass add-ons that are placed over a monitor that prevent the data on the screen from being readable when viewed from the sides. Only the user sitting directly in front of the screen is able to read the data.

RFID badge: A smart card is a type of badge or card that gives you access to resources, including buildings, parking lots, and computers. It contains information about your identity and access privileges. Each area or computer has a card scanner or a reader in which you insert your card. RFID (Radio Frequency Identification) is the wireless, no-contact, technology used with these cards and their accompanying reader. The reader is connected to the workstation and validates against the security system. This increases the security of the authentication process, because you must be in physical possession of the smart card to use the resources

[Back](#)

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

Description: This exercise helps to know about various data destruction/disposal methods and their features.

Instructions: 1.Various data destruction/disposal methods are given on the column A
2.Their features are given on the column B
3.Match (drag and drop) the data destruction/disposal methods given on the Column A with their respective features given on the column B.

Column A

1. Low level format

Column B

1. The process of outlining the positions of the tracks and sectors on the hard disk, and writing the control structures that define where the tracks and sectors are.

- | | |
|--------------------|--|
| 2. Standard format | 2. The process of writing the file system structures on the disk that let the disk used for storing programs and data. |
| 3. Overwrite | 3. Program or utility that repeatedly overwrites the data on a computer's hard drive with gibberish. |
| 4. Drive wipe | 4. Hardware can be recycled, if a piece of hardware that's no longer being used doesn't contain any data of a sensitive or proprietary nature. |

Explanation:

A **low-level format** (typically only accomplished in the factory) can be performed on the system, or a utility can be used to completely wipe the disk clean. This process helps ensure that information doesn't fall into the wrong hands.

Standard format: The process of writing the file system structures on the disk that let the disk used for storing programs and data.

Overwrite: Overwriting the drive entails copying over the data with new data. A common practice is to replace the data with 0s. A number of applications allow you to recover what was there prior to the last write operation, and for that reason, most overwrite software will write the same sequence and save it multiple times.

Drive wipe: a piece of hardware that's no longer being used doesn't contain any data of a sensitive or proprietary nature, that hardware can be recycled (sold to employees, sold to a third party, donated to a school, and so on). That level of assurance can come from wiping a hard drive or using specialized utilities.

[**Back**](#)

6.6 Set SSID on a generic WAP router.

Description: This lab exercise helps you to know how to set the SSID on the generic WAP router.

Instructions: To set SSID (network name), perform the below steps (these steps are generic in nature, and likely to change from one device type to another):

Note: Please click on the "Load lab" button. You will be presented with appropriate interface to answer the question. You need to navigate to the proper menu tab and perform the task

- Step 1: Access the router's web-based setup page.
- Step 2: When the router's web-based setup page appears, click Wireless tab
- Step 3: Click Basic Wireless Settings, in that look for SSID(network Name)
- Step 4: Enter the SSID name to "aplussim" in the box provided.
- Step 5: Click on Save Settings

Explanation :A Service Set Identifier (SSID) is essentially the "name" that you give to a wireless network. Any wireless device that you want to connect to the wireless network must know the SSID for that network. The SSID is controlled by the wireless access point (WAP) for the network. An

SSID may be any combination of ASCII characters (i.e., any combination of letters, numbers, punctuation marks, etc.).

[Back](#)

6.7 Disabling SSID broadcast using the simulator.

Description: This lab exercise helps you to know how to disable the SSID broadcast.

Instructions: To disable SSID (network name), perform the below steps (these steps are generic in nature, and likely to change from one device type to another):

Note: Please click on the “Load lab” button. You will be presented with appropriate interface to answer the question. You need to navigate to the proper menu tab and perform the task

Step 1: Access the router's web-based setup page.

Step 2: When the router's web-based setup page appears, click Wireless, look for Basic wireless Settings tab.

Step 3: select Disable option button of the SSID Broadcast.

Step 4: Click on Save Settings

Explanation : One way to secure your wireless network is to disable the SSID broadcast. This procedure prevents other users from detecting your SSID or your wireless network name when they attempt to view available wireless networks in your area.

[Back](#)

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:

- a. 18:F4:6A:1A:A2:12
- b. 1E:F4:6A:1A:A2:12
- c. 1F:F4:6A:1A:A2:12
- d. 1D:F4:6A:1A:A2:12

Instructions: To enable MAC address filtering and to allow the devices with matching MAC addresses, perform the below steps (these steps are generic in nature, and likely to change from one device type to another)

Note: Please click on the “Load lab” button. You will be presented with appropriate interface to answer the question. You need to navigate to the proper menu tab and perform the task

Step1: Access the router's web-based setup page.

Step2: When the router's web-based setup page appears, click Wireless tab

Step3: In wireless window click Wireless MAC Filter tab and click option button “Premit only” and then click “Edit MAC Filter List” button in Wireless MAC Filter window.

Step4: In MAC Address Filter List window enter the above given MAC addresses and click Save Settings button and again click Save Settings button in Access Point main window

6.9 Configure security encryption to WPA 2 with pass phrase.

Note: Please click on the “Load lab” button. You will be presented with appropriate interface to answer the question. You need to navigate to the proper menu tab and perform the task

Instructions :

- Step 1: Access the router's web-based setup page.
- Step 2: When the router's web-based setup page appears, click Wireless, and in wireless window click Wireless Security tab and select WPA2 -PSK as encryption mode from Security mode drop down and enter “APLUS” as Pass Phrase and click Save Settings button

Explanation: You need to know how to configure basic security setting such as WPA (Short for Wi-Fi Protected Access) or WPA2. You can typically select the appropriate setting from a drop down box and then enter the appropriate pass phrase. The settings entered on the access point must be used on all devices that connect to the access point.

Both WPA and WPA2 operate in either Personal or Enterprise modes. Most home and small business networks use Personal mode using a pass phrase or password. Big enterprises add additional security to WAPs with WPA Enterprise or WPA2 Enterprise. Enterprise mode provides additional security by adding an authentication server such as RADIUS, and requiring each user to authenticate with a username and password.

Enterprise mode requires a server typically configured as a Remote Authentication Dial-In User Service (RADIUS) server, which is configured separately from the access point. The RADIUS server has access to the user's authentication credentials and can verify when a user has entered authentication information correctly.

6.10 Pinging to DHCP server

Description: Verify DHCP configuration parameters using appropriate command on the client computer. For this purpose, ping DHCP server by IP address from the remote workstation.

Configuration parameters:

DHCP Server IP address: 192.168.1.2

Subnet mask: 255.255.255.0

Default Gateway: 192.168.1.1

DHCP Parameters:

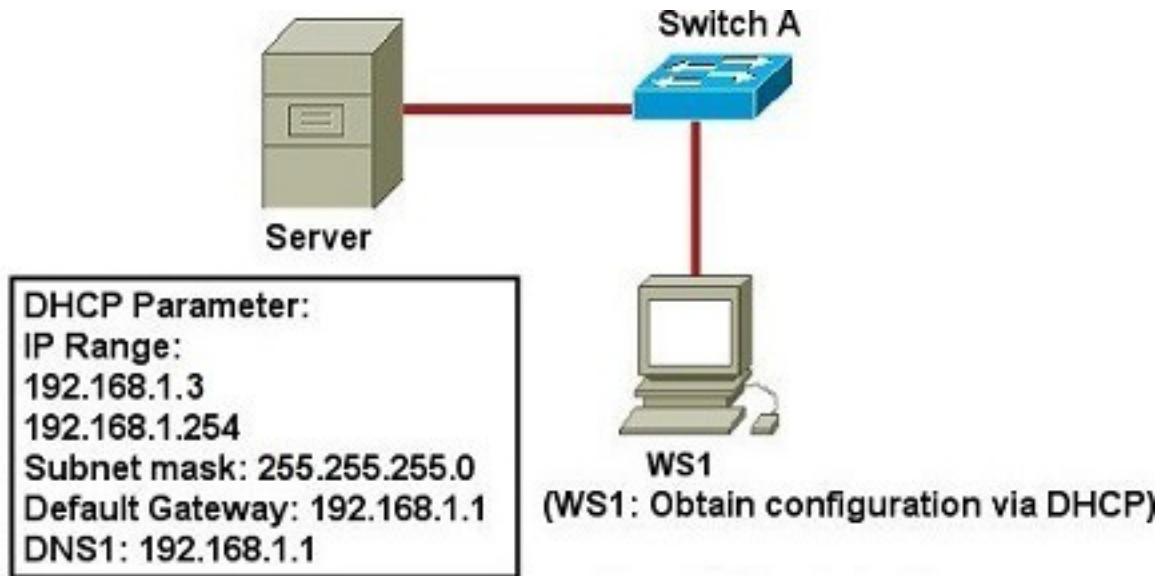
IP address range: 192.168.1.3 to 192.168.1.254

subnet mask: 255.255.255.0

Gateway: 192.168.1.1

DNS1: 192.168.1.1 DNS2: None.

Client (WS1) needs to be configured to obtain DHCP parameters automatically.



- Instructions:**
1. Click on Server this will open Windows Networking dialog box.
 2. Configure IP address, subnet mask and default gateway on the Server with 192.168.1.2, 255.255.255.0, and 192.168.1.1 respectively in DHCP Server IP settings tab.
 3. Click on DHCP scope tab and enter the Start IP address range 192.168.1.3 and End IP address as 192.168.1.254 , Subnet Mask 255.255.255.0 , Default-gateway 192.168.1.1 , DNS Primary as 192.168.1.1
 4. Click OK button
 5. Click on WS1 this will open Windows Networking dialog box. Click on Obtain IP Address automatically option button (if it has not selected already) and click OK button.
 6. Select WS1 from Select Device to configure and Ping Server (192.168.1.2) from WS1. Ping should be successful. If not, troubleshoot for the same)

[**Back**](#)

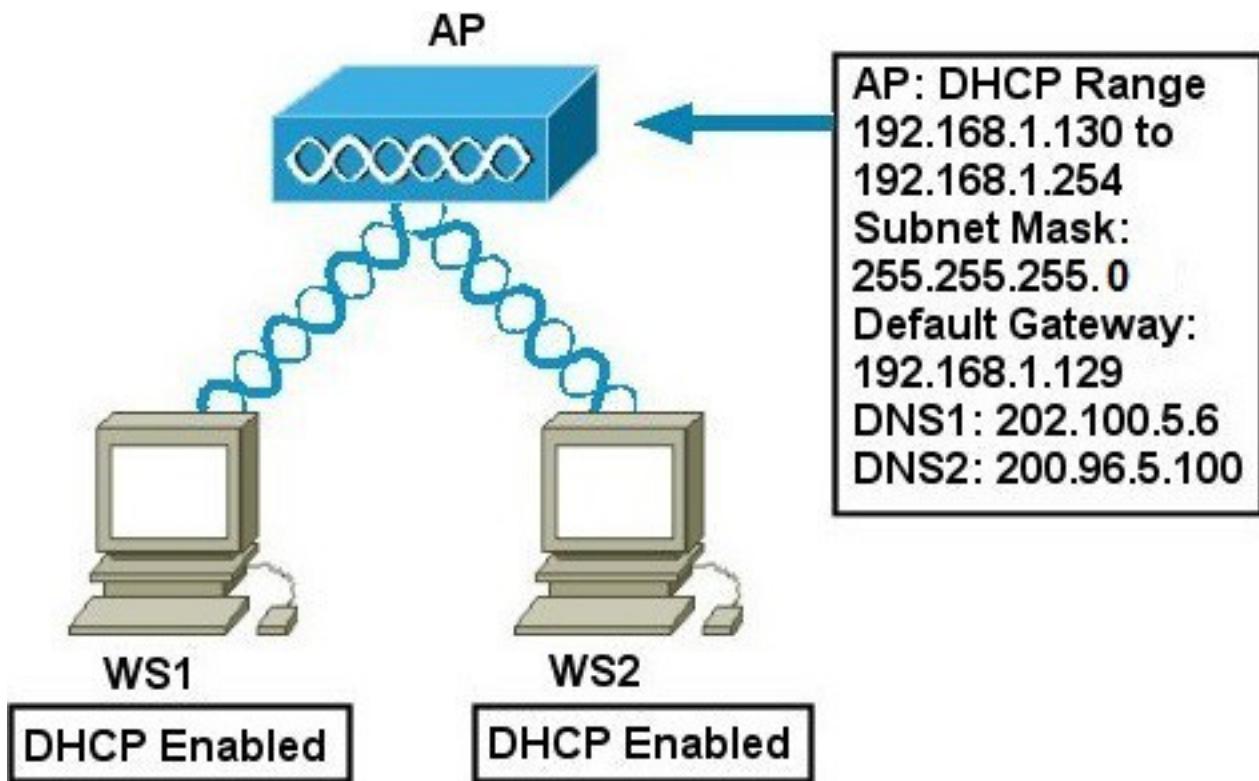
6.11 Configuring Wireless Security on an Access Point (WEP)

Description: Configure WEP security on AP . Verify that the communication will not take place between the PCs (PC1 and PC2) until the WEP key is provided. Use ping command to ping the Access Point (AP) from WS1. AP IP address: 192.168.1.131 subnet mask: 255.255.255.0

Instructions:

1. Click AP , this will open Access Point configuration window enter ip address 192.168.1.131 in Local IP address box , select 255.255.255.0 as subnet mask from subnetmask drop down , Click option button Enable from DHCP Server and enter starting ip address as 192.168.1.130 and maximum number of DHCP users as 254 ,

- enter static DNS1 as 202.100.5.6 and static DNS2 as 200.96.5.100
2. Click Wireless tab and in that click Wireless Security tab and select WEP from Security Mode drop down and enter password “Cert1” and click Save Settings button.
 3. Click WS1 this will open Windows Networking dialog box. Click on Obtain IP Address automatically option button (if it has not selected already) and click wireless button and check Network Name (SSID) is same as AP1 that is “CertExam”, Select WEP from Encryption drop down and enter password “Cert1” click OK button and then click OK button to close the WS1 configuration window
 4. Click WS2 and repeat step 3.
 5. Select WS1 from Select Device to configure and Ping AP by IP address (192.168.1.131) from WS1, it should succeed.
 6. If ping fails, check for SSID mismatch, or WEP mismatch and try again.
 7. Try ping from WS2 to AP by IP address. It should also succeed.



[Back](#)

6.12 Objective Test 6 Answer the following questions

1) Which of the following security threat does NOT use software to extract sensitive information ?

- A. Shoulder surfing
- B. Rootkits
- C. Malware
- D. Man-in-the-Middle exploits
- E. Grayware

Answer: A

Explanation:

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.

2) A company is experiencing issues with third parties tailgating authorized users during entry to secure server rooms. Which of the following would BEST alleviate this problem?

- A. Retinal scanners
- B. Mantraps
- C. Face reader
- D. Door locks
- E. Smart card badges

Answer: B

Explanation:

A mantrap is a small room with an entry door on one wall and an exit door on the opposite wall. One door of a mantrap cannot be unlocked and opened until the opposite door has been closed and locked. How it works is that when the first door is opened through fingerprint scanning the person being admitted passes into a room that contains a second, automatically locked door. When verified through biometric security the door then opens and the person is passed through.

3) The practice of following an authorized person through an entrance without using a badge to defeat security is called:

- A. Tailgating
- B. Spamming
- C. Shredding
- D. Phishing

Answer: A

Explanation:

Tailgating: is the term used for someone being so close to you when you enter a building that they are able to come in right behind you without needing to use a key, a card, or any other security device.

4) Which security measure is in place when a client is denied access to the network due to outdated antivirus software?

- A. IPsec
- B. DMZ
- C. NAC
- D. NAT

Answer: C

Explanation:

Network Access Control (NAC) defines a set of rules enforced in a network that the clients attempting to access the network must comply with. With NAC, policies can be enforced before or after end stations gain access to the network. NAC can be implemented as Pre-admission NAC, where a host must, for example, be virus free or have patches applied before it is allowed to connect to the network, and/or Post-admission

NAC, where a host is being granted/denied permissions based on its actions after it has been provided with the access to the network.

5) Which of the following tools allows for secure disposal of physical documents?

- A. Shredder
- B. Hard drive sanitation
- C. Degaussing tool
- D. Recycle Bin

Answer: A

Explanation: When it comes to DVDs and CDs, many commercial paper shredders include the ability to destroy them. Paper shredders, however, are not able to handle hard drives and you need a shredder created for just such a purpose.

[Back](#)

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

Description: This lab exercise helps to get familiar with configuration of Email on android mobile devices

Instructions: 1. The following are the shuffled email configuration on android mobile devices
2. Arrange them in a proper sequence by dragging the text from left to a empty box given on the right

1. Type your Email address and Password, and click next.
2. If you already have an email account setup, press Menu and tap Accounts. Press Menu again and tap Add account.
3. Open your device's email application
4. Enter the settings for your incoming server, depending on the type of email you have
5. Tap Next again. Name your account and enter the name you want to display on outgoing messages
6. Tap Done
7. Select Require sign-in and make sure your Username (your full email address) and Password are correct. Tap Next.
8. If you have IMAP, tap IMAP. If you're not sure, tap POP3. USE IMAP ONLY
9. Enter the settings for your outgoing server:

The correct order is

1. Open your device's email application

2. If you already have an email account setup, press Menu and tap Accounts. Press Menu again and tap Add account.
3. Type your Email address and Password, and click Next.
4. If you have IMAP, tap IMAP. If you're not sure, tap POP3. USE IMAP ONLY
5. Enter the settings for your incoming server, depending on the type of email you have
6. Enter the settings for your outgoing server:
7. Select Require sign-in and make sure your Username (your full email address) and Password are correct Tap Next
8. Tap Next again. Name your account and enter the name you want to display on outgoing messages
9. Tap Done

Explanation

http://pw2.com/pdf/android_setup.pdf

<http://www.ehostpk.com/clients/knowledgebase.php?action=displayarticle&id=37>

<https://mediateemple.net/community/products/dv/204643630/using-email>

<https://my.bluehost.com/cgi/help/android>

[Back](#)

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

Description: This exercise explains some of the features of mobile devices

Instructions: 1. Some of the features of mobile devices are given on the column A
 2. Their characteristics are given on the column B
 3. Match (drag & drop) the feature given on the column A with their respective characteristics given on the column B

Column A

1. ios Android OS
2. ARM
3. Bluetooth
4. Wi-Fi tethering
5. Configure a screen lock
6. POP3 and IMAP Connection

Column B

- 1.The common operating system used by mobile devices
2. A CPU used by mobile devices
3. To connect headset of your mobile
4. Other mobile devices to share your mobile's internet
5. Prevent person from accessing your mobile
6. A connection requires username, password, and SMTP server

Explanation:

1. ios Android OS: Google's **Android** and Apple's **iOS** are operating systems used primarily in mobile technology, such as smartphones and tablets. Android, which is Linux-based and partly open source, is more PC-like than iOS, in that its interface and basic features are generally more customizable from top to bottom.

However, iOS' uniform design elements are sometimes seen as being more user-friendly.

2. ARM: An ARM processor is one of a family of CPUs based on the RISC(reduced instruction set computer) architecture developed by Advanced RISC Machines (ARM).

ARM processors are extensively used in consumer electronic devices such as smartphones, tablets, multimedia players and other mobile devices, such as wearables. Because of their reduced instruction set, they require fewer transistors, which enables a smaller die size for the integrated circuitry (IC). The ARM processor's smaller size, reduced complexity and lower power consumption makes them suitable for increasingly miniaturized devices.

3. Bluetooth: Bluetooth is a wireless radio technology that allows many different **devices** to connect to each other and work together. It was originally invented as an affordable wireless alternative to wired keyboards, headphones, speakers, and other peripherals.

4. Wi-Fi tethering: Tethering is connecting one device to another. In the context of mobile phones and tablet computers, tethering allows sharing the Internet connection of the phone or tablet with other devices such as laptops. Connection of the phone or tablet with other devices can be done over wireless LAN (Wi-Fi), over Bluetooth or by physical connection using a cable, for example through USB.

If tethering is done over Wi-Fi, the feature may be branded as a mobile hotspot. Mobile hotspot is a feature present in smartphones nowadays which lets you convert your smart phone into a portable router. One can setup a password protection to it easily so that no one without the password can connect to your smart phones. The Internet-connected mobile device can act as a portable wireless access point and router for devices connected to it.

5. Configure Screen lock: Our smart phones carry a lot of personal information. All of your text messages, emails, notes, apps, app data, music, pictures, and so much more are all on there. While it's a very great convenience to have all of these on your phone, it's also a major security risk if all of this data is easily accessible. The best way to prevent simple unauthorized access is by setting some sort of lock on your phone. Two popular choices, especially on Android phones, are passwords and pattern

6. POP3 and IMAP Connection:

POP3:

Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client. POP3 allows you to download email messages on your local computer and read them even when you are offline."

IMAP

The Internet Message Access Protocol (IMAP) is a mail protocol used for accessing email on a remote web server from a local client. IMAP and POP3 are the two most commonly used Internet mail protocols for retrieving emails. Both protocols are supported by all modern email clients and web servers."

"Main difference between IMAP and POP3:

The POP3 protocol assumes that there is only one client connected to the mailbox. In contrast, the IMAP protocol allows simultaneous access by multiple clients. IMAP is suitable for you if your mailbox is about to be managed by multiple users."

[Back](#)

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

Description: This exercise explains some of the basic features of mobile operating systems

Instructions: 1. Some of mobile operating system 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	Column B
1. ACPI	1. Provides an open standard for device configuration and power management by the operating system
2. OSPM	2. An operating system technology that switches between different power states
3. AHCI	3. Is a technical standard defined by Intel that specifies the operation of Serial ATA (SATA) host bus adapters in a non-implementation-specific manner.
4. Gyroscope	4. re-alignment of screen orientation as the user turns his phone
5. icloud	5. A cloud storage and cloud computing service from Apple Inc
6. GPS	6. Is a network of satellites that transmit radio waves, providing location information to people on the ground.

Explanation:

1. Advanced Configuration and Power Interface (ACPI) : specification provides an open standard for device configuration and power management by the operating system.

2. Operating System Power Management (OSPM) : is an operating system technology for managing the power of the underlying platform and switching it between different power states. OSPM enables a platform or system to implement the most efficient power mode and is applicable across all devices and components within a platform/system. OSPM is also known as Operating System-directed configuration and Power Management.

3. The Advanced Host Controller Interface (AHCI) : is a technical standard defined by Intel that specifies the operation of Serial ATA (SATA) host bus adapters in a non-implementation-specific manner

4. Gyroscope: enables re-alignment of screen orientation as the user turns his phone

5. iCloud: is a cloud storage and cloud computing service from Apple Inc. The service allows users to store data such as music and iOS applications on remote computer servers for download to multiple devices such as iOS-based devices running iOS 5 or later, and personal computers running OS X 10.7.2 "Lion" or later, or Microsoft Windows (Windows Vista service pack 2 or later).

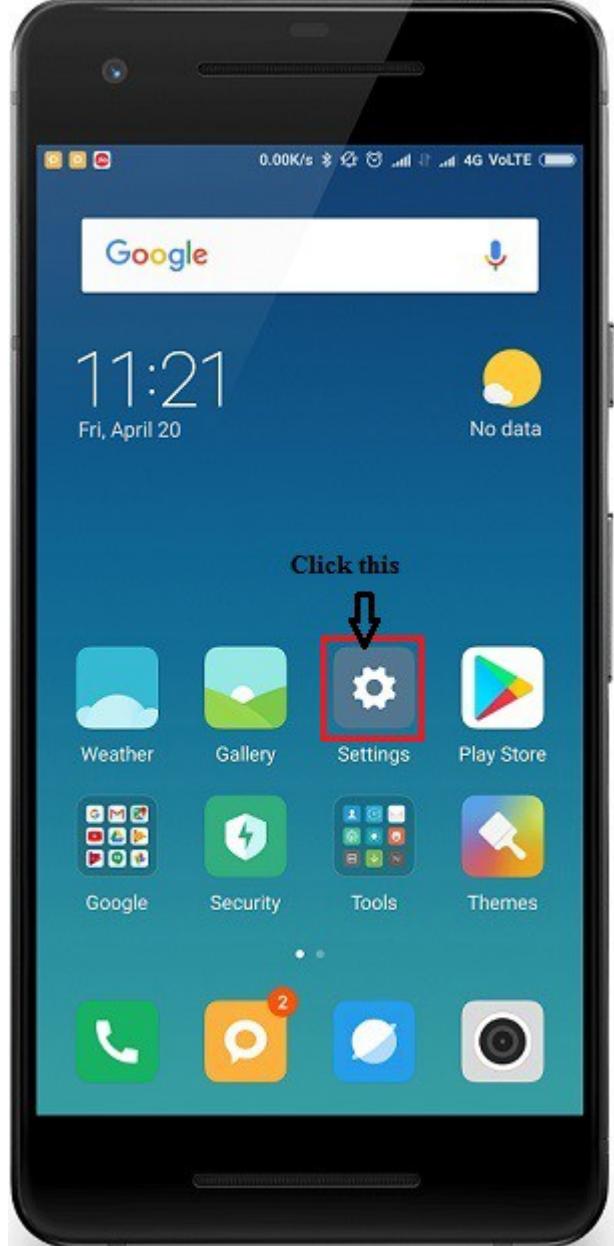
6. The Global Positioning System (GPS): is a space-based satellite navigation system that provides location and time information in all weather conditions, anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites. Most smart phones have GPS built in to the software.

[Back](#)

7.5 Connecting smart phone to a wireless network

Description: This lab exercise will help you to connect an Android device wirelessly to a router.

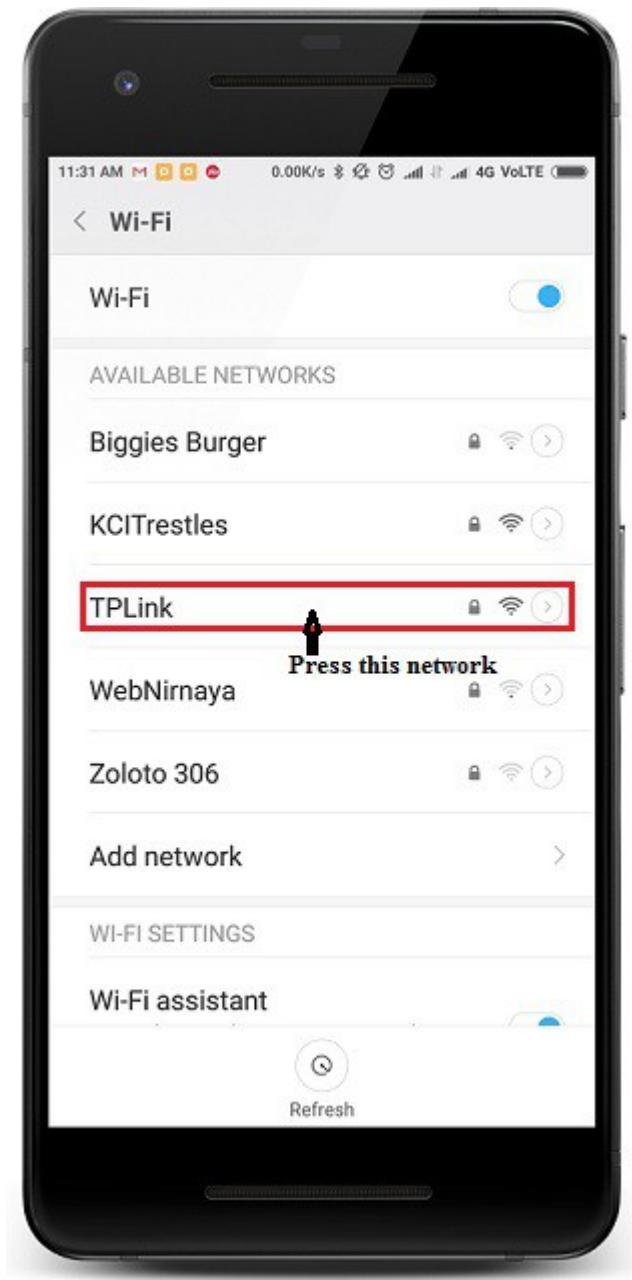
Instructions: 1. On loading a lab exercise, in a given simulation press settings button.



2. Under “Wireless and Networks”, then press Wi-Fi.



3. Press the Wi-Fi network name “TPLink” that you want to connect to.



4. Enter the Wi-Fi network password as “apluslabsim”, and press “Connect”. This will complete your connection to the wireless network.



[Back](#)

7.6 Connecting smart phone to PoP3 email server

Description: This lab exercise will help you to setup mobile phone for PoP3 email.

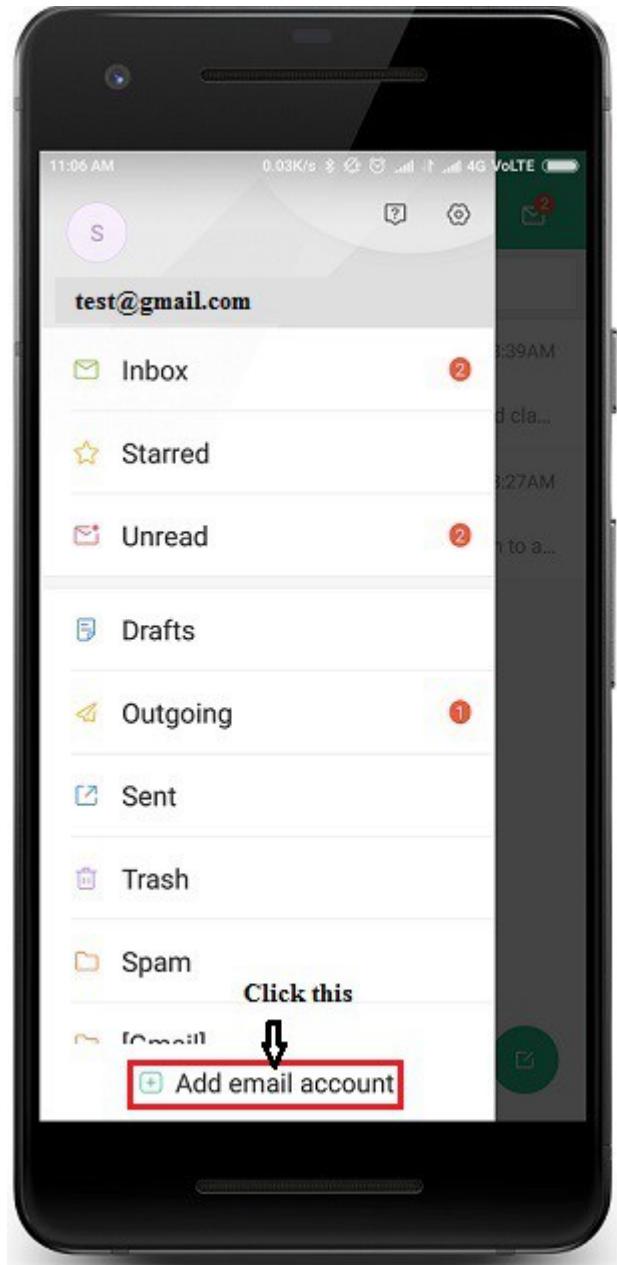
Instructions: 1. On loading a lab exercise, in a given simulation press tools button.



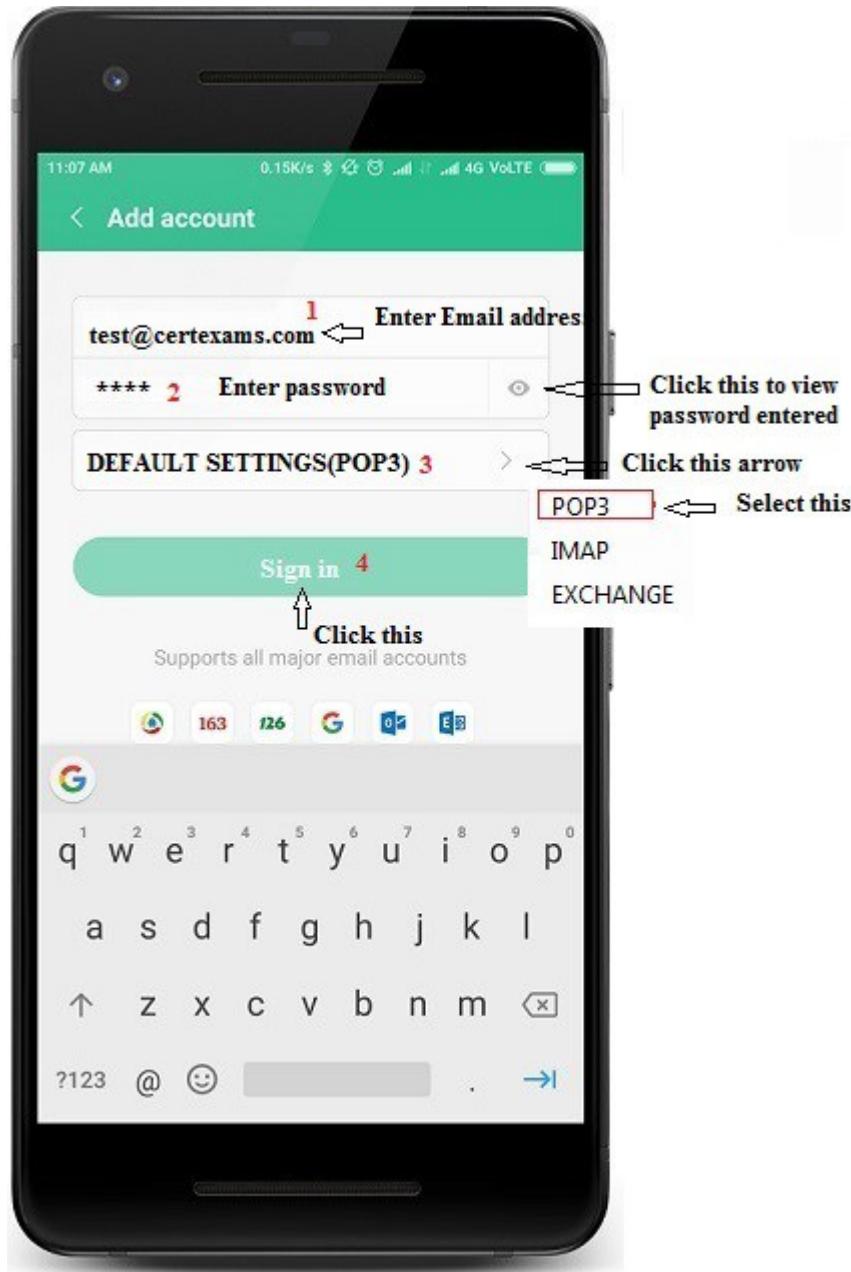
2. In the next screen click Mail option



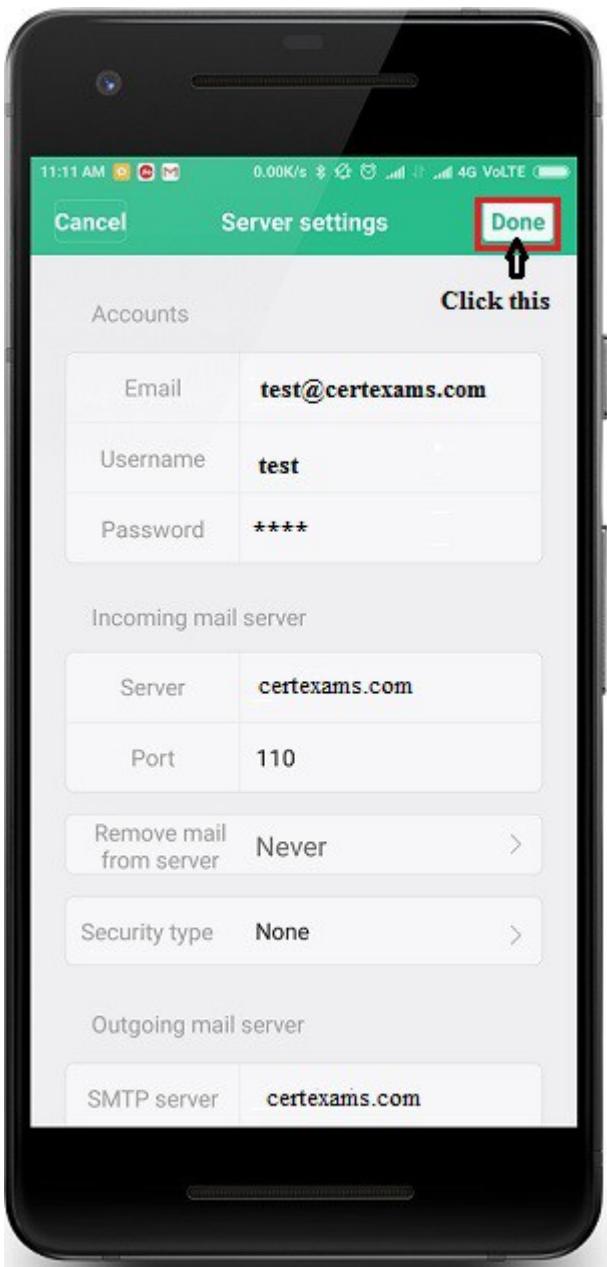
3. Click Add email account



4. In the Add Account screen enter the email address as “test@certexams.com” , password as “pass” and click arrow next to “Default Settings” and select POP3 from the popup list and then click Sign in.



5. The Mail app will configure the incoming and outgoing server settings for you automatically , as shown in the below screen click done this will complete the setup and your account is ready to use.



Note : test@gmail.com already existing gmail account , this lab explains adding one more email account.

Explanation: You can setup your mobile phone to send and receive email from your email accounts. Using POP3 (**Post Office Protocol version 3**), your email are retrieved and stored locally on your mobile phone and at the same time they're deleted from the server. It is therefore not possible to access your email from different devices.

[**Back**](#)

7.7 Objective Test 7 Answer the following questions

- 1) Which of the following software types would need to be installed on a mobile device to help prevent data from being viewed if the device is lost?

- A. Remote wipe
- B. GPS locator
- C. Remote backup application
- D. Antivirus

Answer A: Remote wipe

Explanation:

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.

2) Modern mobile devices have the capability to present landscape or portrait views of the device's screen based on the way the device is being held. Which of the following built-in functionalities allows for determining screen orientation in those devices?

- A. Hypervisor
- B. Geotracking
- C. Degaussing tool
- D. Accelerometer

Answer: D

Explanation:

An accelerometer is a sensor which measures the tilting motion and orientation of a mobile phone.

3) A user interface element on mobile devices controlling access to a device after the device is switched on is called:

- A. Accelerometer
- B. Single Sign-On (SSO)
- C. Lock screen
- D. Locator application

Answer: C

Explanation:

A **lock screen** is a user interface element used by various mobile devices. They regulate immediate access to a device by requiring that the user perform a certain action in order to receive access: such as entering a password, using a certain button combination, or by performing a certain gesture using a device's touchscreen.

4) The process of establishing connection between Bluetooth devices is commonly referred to as:

- A. Linking
- B. Degaussing
- C. Crosstalk
- D. Pairing

Answer: D

Explanation:

Establishing a connection between two Bluetooth devices is called pairing. For example, to pair a headset

with a phone, the phone is configured to "Discoverable" mode and the headset is setup to pair by pressing one or more keys for some number of seconds. The headset finds the phone and establishes a connection using an assigned passkey.

5) Which of the following refers to a mail server developed by Microsoft?

- A. Gmail
- B. PXE
- C. IMAP
- D. Exchange

Answer: D

Explanation:

Microsoft Exchange Server is a mail server developed by Microsoft which runs exclusively on the Microsoft Windows Server product line. The Microsoft Exchange client, was an email reader or user agent application.

[Back](#)

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 dropping correct options on the image.



[Back](#)

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

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

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

Column A

1. Fixmbr
2. Fixboot
3. Defrag
4. Safe mode
5. REGEDIT
6. REGSVR32

Column B

1. Used to repair the Master Boot Record (MBR) and to fix a problem with the hardware.
2. Used to write a new boot sector to the system partition and to fix the damage to the Windows boot sector
3. Reorganizes file storage on a disk to reduce the number of files that are stored non-contiguously.
4. Used to boot into if you suspect driver problems and want to load with a minimal set while you diagnose the problem.
5. Centralized database contains environmental settings for various Windows programs.
6. Used for registering and un-registering DLL's and ActiveX controls in the Registry.

Explanation:

1. FIXMBR command lets you repair a master boot record (MBR). The syntax for this command is:
FIXMBR [DeviceName]

If you omit the DeviceName parameter, FIXMBR rewrites the MBR on the boot device. You can specify a device name to write a MBR to a different drive (such as a floppy disk or secondary hard disk). You can use the MAP command to retrieve a list of device names. An example of a valid device name is \Device\HardDisk0.

2. FIXBOOT writes a new boot sector onto the system partition. The syntax for the command is:
FIXBOOT [drive:]

If you do not specify the drive: option, FIXBOOT writes the boot sector to the default boot partition. You can specify a different drive if you need to write a boot sector to a volume other than the default boot partition.

3. Defrag or Defragmentation is the process of locating the non-contiguous fragments of data into which a computer file may be divided as it is stored on a hard disk, and rearranging the fragments and restoring them into fewer fragments or into the whole file. Defragmentation reduces data access time and allows storage to be used more efficiently.

4. Safe mode: To access Safe Mode, you must press F8 when the OS menu is displayed during the boot process. A menu of Safe Mode choices appears, and you can select the mode you want to boot into. This is the mode to boot into if you suspect driver problems and want to load with a minimal set while you diagnose the problem.

5. REGSVR32 (Microsoft Register Server) is a command-line utility in Windows operating systems for registering and unregistering DLLs and ActiveX controls in the Registry. Regsvr32.exe is installed in the %systemroot%\System32 folder in Windows XP and later versions of Windows.

RegSvr32.exe has the following command-line options:

```
Regsvr32 [/u] [/n] [/i[:cmdline]] <dllname>
```

where, /u - Unregister server

/i - Call DllInstall passing it an optional [cmdline]; when it is used with /u, it calls dll uninstall

/n - do not call DllRegisterServer; this option must be used with /i

/s - Silent; display no message boxes

6. REGEDIT or Registry Editor is a tool intended for advanced users. It's used to view and change settings in the system registry, which contains information about how your computer runs. Windows refers to this information and updates it when you make changes to your computer, such as installing a new program, creating a user profile, or adding new hardware. Registry Editor lets you view registry folders, files, and the settings for each registry file.

[Back](#)

8.3 Identify the networking troubleshooting command.

Description: This lab exercise helps to identify the networking troubleshoot command.

Instructions:

1. A figure which displays an output of the troubleshooting command is given below.
2. Click on the command which displays the corresponding output, if the clicked command is correct it indicates the green mark, otherwise it indicates the red mark.

```
Tracing route to google.com [216.58.220.46]
over a maximum of 30 hops:
 1   6 ms    2 ms    1 ms  192.168.1.1
 2   3 ms    2 ms    3 ms  10.249.0.1
 3  62 ms    6 ms    9 ms  83.20-broadband.acttv.in [202.83.20.41]
 4   5 ms    3 ms    2 ms  83.26-broadband.acttv.in [202.83.26.2]
 5   5 ms    5 ms    8 ms  83.26-broadband.acttv.in [202.83.26.1]
 6   2 ms    2 ms    2 ms  83.20-broadband.acttv.in [202.83.20.66]
 7   8 ms    7 ms    5 ms  83.20-broadband.acttv.in [202.83.20.65]
 8  15 ms   15 ms   12 ms  83.20-broadband.acttv.in [202.83.20.50]
 9  12 ms   13 ms   18 ms  72.14.194.18
10  13 ms   11 ms   13 ms  72.14.233.204
11  12 ms   14 ms   12 ms  209.85.255.43
12  11 ms   11 ms   14 ms  maa03s18-in-f14.1e100.net [216.58.220.46]

Trace complete.
```

A) TRACERT B) NBTSTAT C) NETSTAT D) IPCONFIG /renew

Explanation:

The TRACERT diagnostic utility determines the route to a destination by sending Internet Control Message Protocol (ICMP) echo packets to the destination. In these packets, TRACERT uses varying IP Time-To-Live (TTL) values. Because each router along the path is required to decrement the packet's TTL by at least 1 before forwarding the packet, the TTL is effectively a hop counter. When the TTL on a packet reaches zero (0), the router sends an ICMP "Time Exceeded" message back to the source computer.

TRACERT sends the first echo packet with a TTL of 1 and increments the TTL by 1 on each subsequent transmission, until the destination responds or until the maximum TTL is reached. The ICMP "Time Exceeded" messages that intermediate routers send back show the route. Note however that some routers silently drop packets that have expired TTLs, and these packets are invisible to TRACERT.

TRACERT prints out an ordered list of the intermediate routers that return ICMP "Time Exceeded" messages. Using the -d option with the tracert command instructs TRACERT not to perform a DNS lookup on each IP address, so that TRACERT reports the IP address of the near-side interface of the routers.

TRACERT syntax: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

Parameters:

- d: Specifies to not resolve addresses to host names.

- h maximum_hops: Specifies the maximum number of hops to search for target.

- j host-list: Specifies loose source route along the host-list.

- w timeout: Waits the number of milliseconds specified by timeout for each reply.

- target_name: Name or IP address of the target host.

Below fig. Shows after identifying the correct networking command.

```

Tracing route to google.com [216.58.220.46]
over a maximum of 30 hops:

 1      6 ms      2 ms      1 ms  192.168.1.1
 2      3 ms      2 ms      3 ms  10.249.0.1
 3     62 ms      6 ms      9 ms  83.20-broadband.acttv.in [202.83.20.41]
 4      5 ms      3 ms      2 ms  83.26-broadband.acttv.in [202.83.26.2]
 5      5 ms      5 ms      8 ms  83.26-broadband.acttv.in [202.83.26.1]
 6      2 ms      2 ms      2 ms  83.20-broadband.acttv.in [202.83.20.66]
 7      8 ms      7 ms      5 ms  83.20-broadband.acttv.in [202.83.20.65]
 8     15 ms     15 ms     12 ms  83.20-broadband.acttv.in [202.83.20.50]
 9     12 ms     13 ms     18 ms  72.14.194.18
10    13 ms     11 ms     13 ms  72.14.233.204
11    12 ms     14 ms     12 ms  209.85.255.43
12    11 ms     11 ms     14 ms  maa03s18-in-f14.1e100.net [216.58.220.46]

```

Trace complete.

A) TRACERT

B) NBTSTAT

C) NETSTAT

D) IPCONFIG /renew

[Back](#)

8.4 Troubleshoot WiFi connection on a Windows Workstation

Scenario: WS3 is not able to communicate with WS4. Ping WS4 from WS3 is not successful. Verify the configuration on WS3/WS4 and ensure that ping works. DHCP is configured on client computers and working properly.

Requirements: For this purpose, WS3 SSID will be configured wrongly before hand. No communication takes place (ping fails). Then, bringup the wireless properties window on WS3 and configure SSID properly. Ping should be successful.

Access Point configuration:

SSID: CertExams, Password: cert1,

IP address: 192.168.1.2 , subnet mask: 255.255.255.0

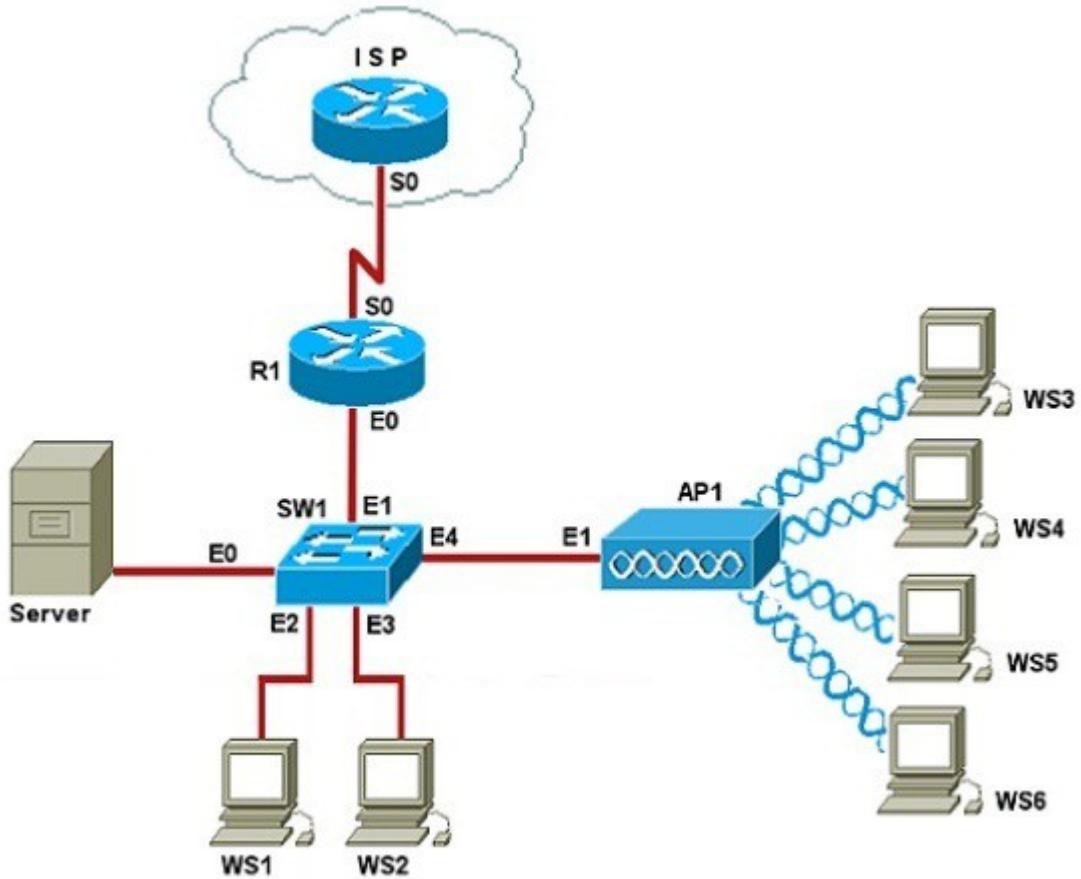
Default gateway: 192.168.1.1

DHCP Server is configured to provide DHCP parameters as below:

IP address range: 192.168.1.3 to 192.168.1.254

Subnet mask: 255.255.255.0

Default gateway: 192.168.1.1



Instructions:

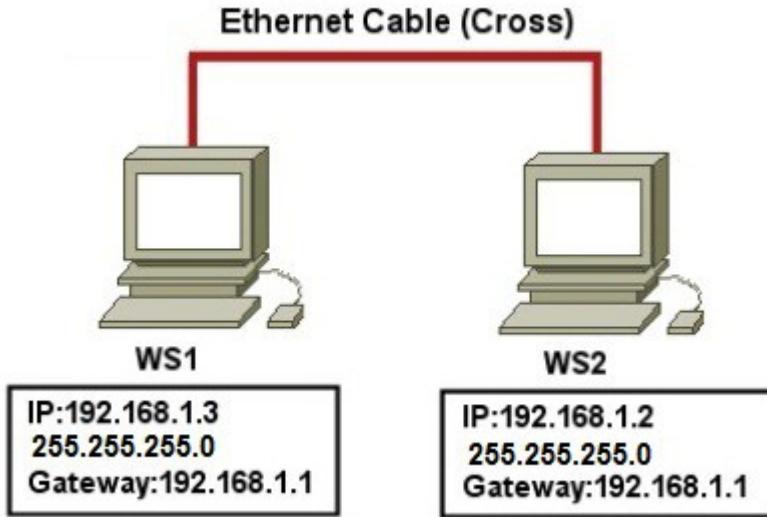
1. Click AP1 , this will open Access Point configuration window enter ip address 192.168.1.2 in Local IP address box , select 255.255.255.0 as subnet mask from subnet mask drop down , Click option button Enable from DHCP Server and enter starting ip address as 192.168.1.3 and maximum number of DHCP users as 254
2. Click Wireless tab enter Wireless Network Name (SSID) as “CertExams” , Click Wireless Security tab and select WEP from Security Mode drop down and enter “cert1” in Password field and click Save Settings button
3. Click WS3 this will open Windows Networking dialog box. Click on Obtain IP Address automatically option button (if it has not selected already) and click wireless button and enter Network Name (SSID) same as AP1 that is “CertExams” and select WEP from Encryption drop down and enter “cert1” in Password field and click OK button and then click OK button to close the WS3 configuration window.
4. Repeat steps 3 - 4 for WS4
5. Ping WS4 from WS3 and see that ping is successful

Notes: An SSID is the name of a wireless local area network (WLAN). All wireless devices on a WLAN must employ the same SSID in order to communicate with each other. SSIDs are case sensitive text strings. The SSID is a sequence of alphanumeric characters (letters or numbers). SSIDs have a maximum length of 32 characters.

[Back](#)

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

Description: This exercise explains how to configure ip address on windows (ip address, subnet mask, dns server, default gateway) client workstation.



Configure IP address, subnet mask, default gateway statically on Windows client workstation WS1 with the following IPv4 configuration settings:

IP address: 192.168.1.3
Subnet mask: 255.255.255.0
Default gateway: 192.168.1.1

Instructions:

1. Click WS1 from network diagram and in WS1 configuration window click the option button Use the following IP Address and configure IP address as 192.168.1.3 , Subnet mask 255.255.255.0 and default-gateway 192.168.1.1 and click OK button
2. Next, click on WS2, and configure IP address 192.168.1.2, Subnet mask 255.255.255.0 and default-gateway 192.168.1.1 and click OK button

[Back](#)

8.6 Objective Test 8 Answer the following questions

1) A user states their workstation will not reach the login screen. Which of the following commands can be used to write a new partition boot sector to the system partition in the Recovery Console?

- A. FIXMBR
- B. BOOTCFG
- C. FIXBOOT
- D. DISKPART

Answer: C

Explanation:

FIXBOOT writes a new boot sector onto the system partition. The syntax for the command is:

FIXBOOT [drive:]

If you do not specify the drive: option, FIXBOOT writes the boot sector to the default boot partition. You can specify a different drive if you need to write a boot sector to a volume other than the default boot partition.

2) Which of the following is the BEST tool to verify the cable is plugged into the correct port on the patch panel?

- A. Cable tester
- B. Wire strippers
- C. Crimper
- D. Toner probes

Answer: D

Explanation:

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.

3) A technician believes a machine loaded with Windows XP Professional has issues with file integrity of the core OS components. Which of the following commands could be used to both check and replace damaged files?

- A. SFC /SCANNOW
- B. CHKDSK /R /F
- C. FORMAT C:
- D. DISKPART

Answer: A

Explanation:

The System File Checker (sfc) command is a Command Prompt command that can be used to verify and replace important Windows system files. It is a very useful tool to use when you suspect issues with protected Windows files like many DLL files. Sfc Command Syntax is as follows:

sfc [/scannow] [/verifyonly] [/scanfile=file] [/verifyfile=file] [/offbootdir=boot] [/offwindir=win] [/?]

/scannow : This option instructs sfc to scan all protected operating system files and repair as necessary.

/verifyonly : This sfc command option is the same as */scannow* but without repairing.

/scanfile=file : This sfc option is the same as */scannow* but the scan and repair is only for the specified *file*.

/offbootdir=boot : Used with */offwindir*, this sfc option is used to define the boot directory (*boot*) when using sfc from outside of Windows.

/offwindir=win : This sfc option is used with */offbootdir* to define the Windows directory (*win*) when using sfc offline.

/? = Use the help switch with the sfc command to show detailed help about the command's several options.

4) A network security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network is commonly referred to as:

- A. MAC filtering
- B. SSID broadcast
- C. Encryption
- D. Static IP addressing

Answer: A

Explanation:

In computer networking, MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network.

MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists. While the restriction of network access through the use of lists is straightforward, an individual person is not identified by a MAC address, rather a device only, so an authorized person will need to have a whitelist entry for each device that he or she would use to access the network.

5) What is the name of the anti-malware software distributed with Windows?

- A. Event Viewer
- B. Windows Firewall
- C. Recovery console
- D. Windows Defender

Answer: D

Explanation:

Windows Defender is an antispyware program for Windows that provides real-time protection and post infection scanning and removal. Windows Defender succeeds Windows Antispyware, and is one of several competing packages from various vendors that protect against spyware and adware (generally lumped together and called "malware").

[Back](#)

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

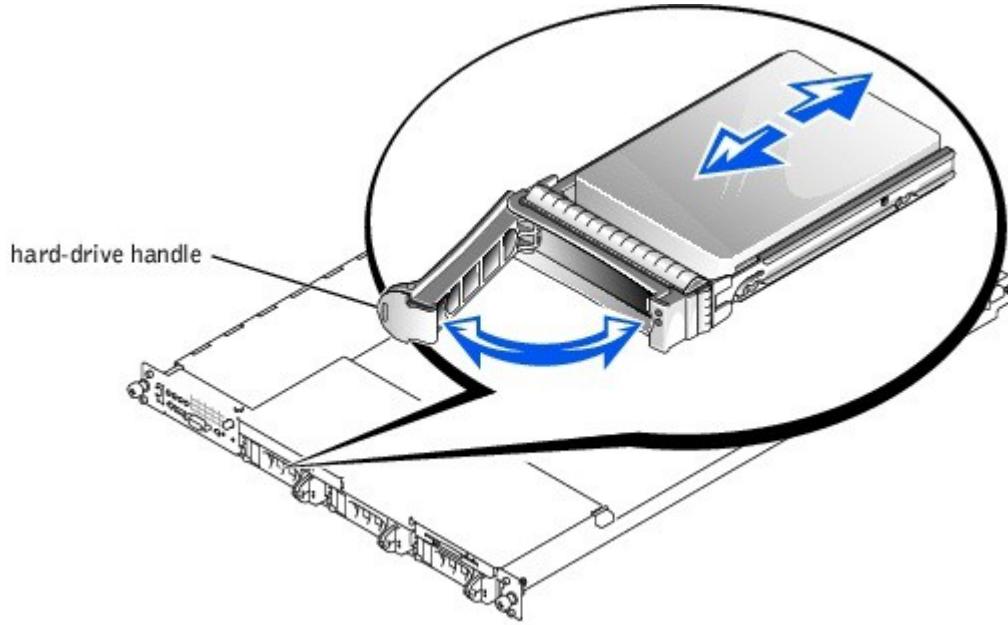
9.3a Installing SCSI drives on a bus

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.

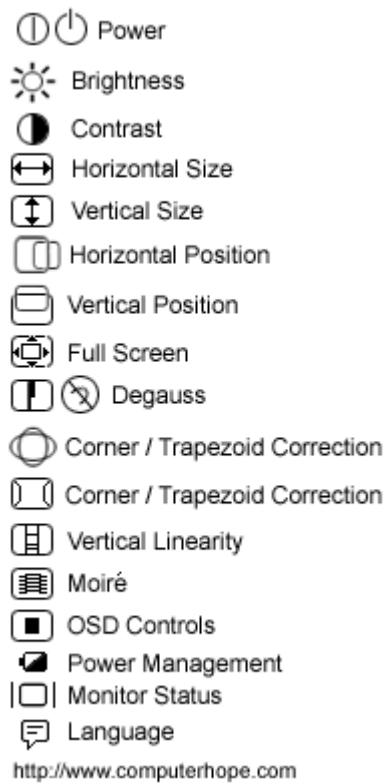
[Back](#)

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.

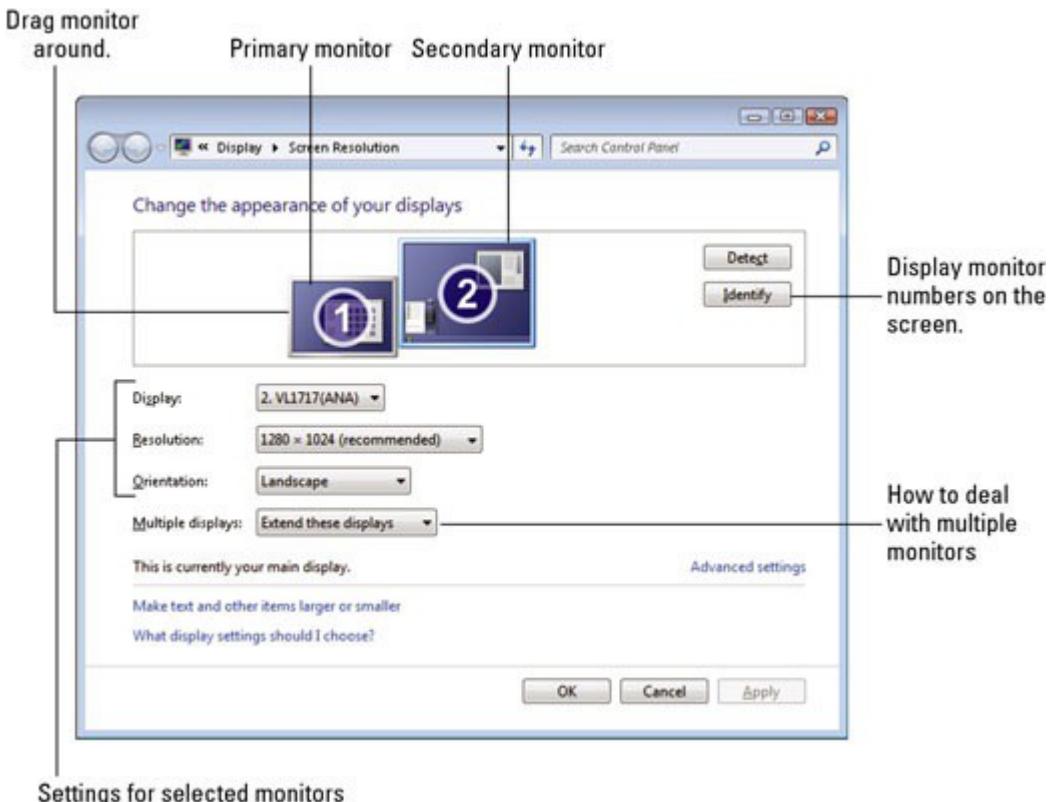
Instructions:

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.

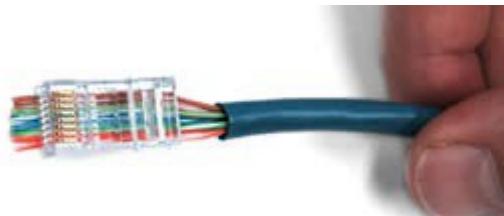


5. Holding the RJ45 connector so that its pins are facing away from you and the plug-clip side is facing down, carefully insert the flattened, arranged wires into the connector, pushing through until the wire ends emerge from the pins for strength of connection, also push as much of the cable jacket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

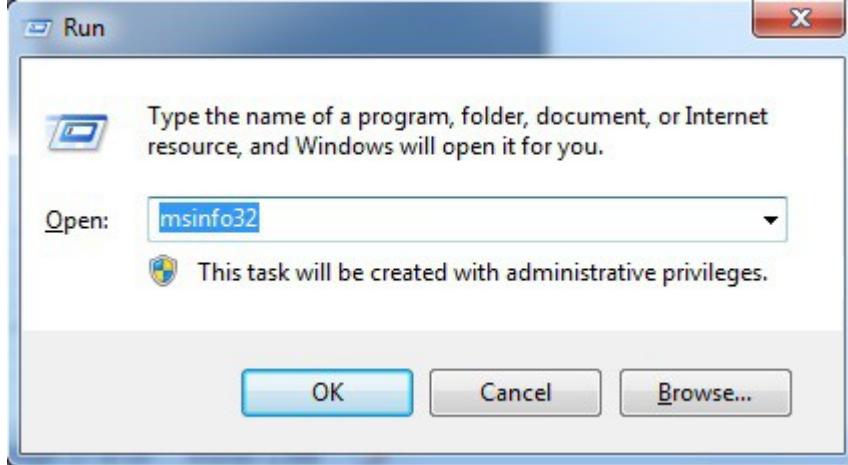
Instructions:

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
View	Help
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 Core(s), 2 Logical Proc...
BIOS Version/Date	Intel Corp. H0H610H86A.0010.2012.0424.1632, 4/24/2012
SMBIOS Version	2.7
Windows Directory	C:\Windows
System Directory	C:\Windows\system32
Boot Device	1Device\HarddiskVolume1
Locale	United States
Hardware Abstraction Layer	Version = "6.1.7601.17914"
User Name	ANAND\Admini
Time Zone	India Standard Time
Installed Physical Memory (RAM)	2.00 GB
Total Physical Memory	190 GB
Available Physical Memory	882 MB
Total Virtual Memory	3.79 GB
Available Virtual Memory	2.49 GB

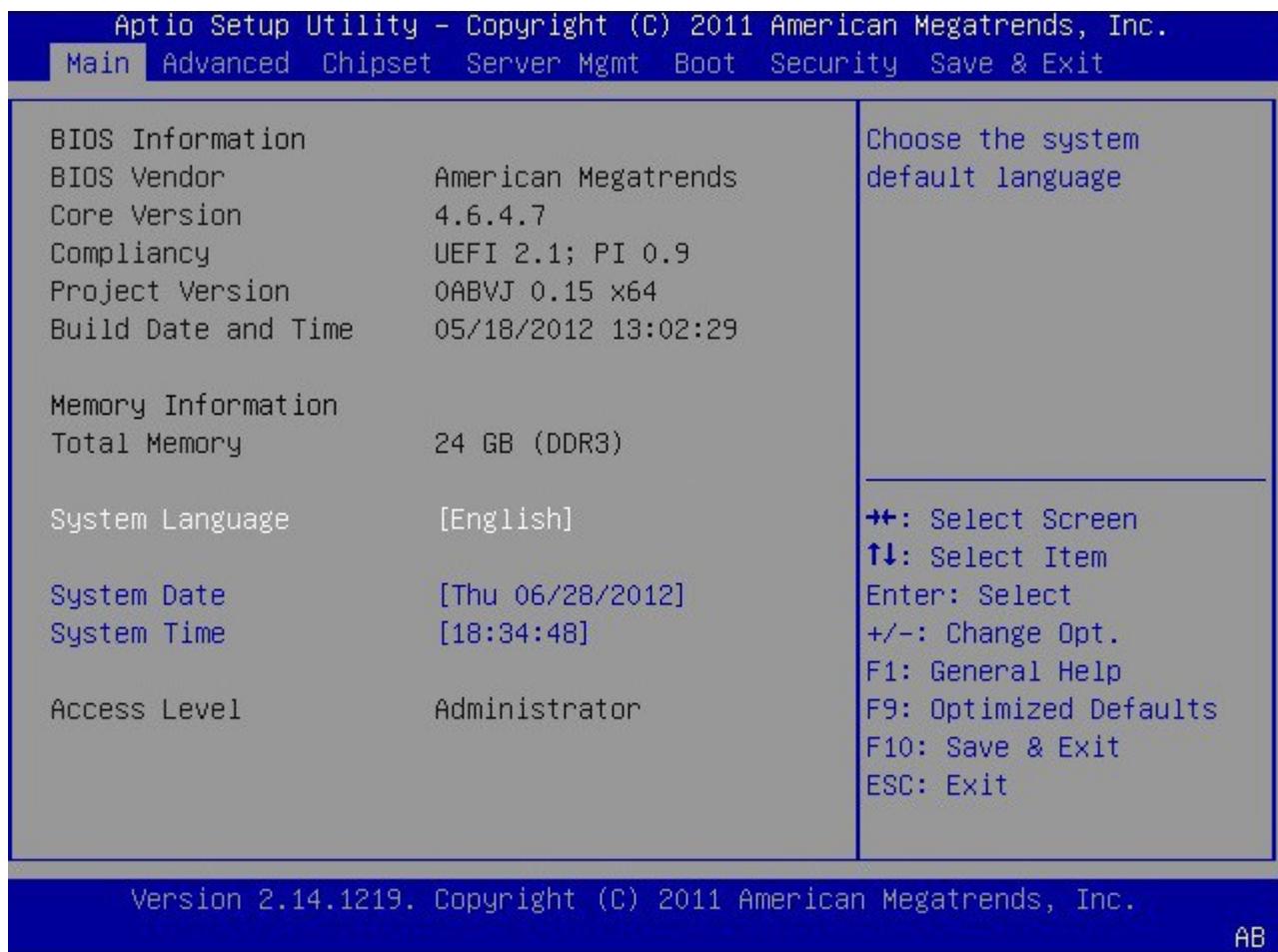
2. Write down the BIOS version and continue to the next section.

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.



[Back](#)

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.

[**Back**](#)

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.

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.

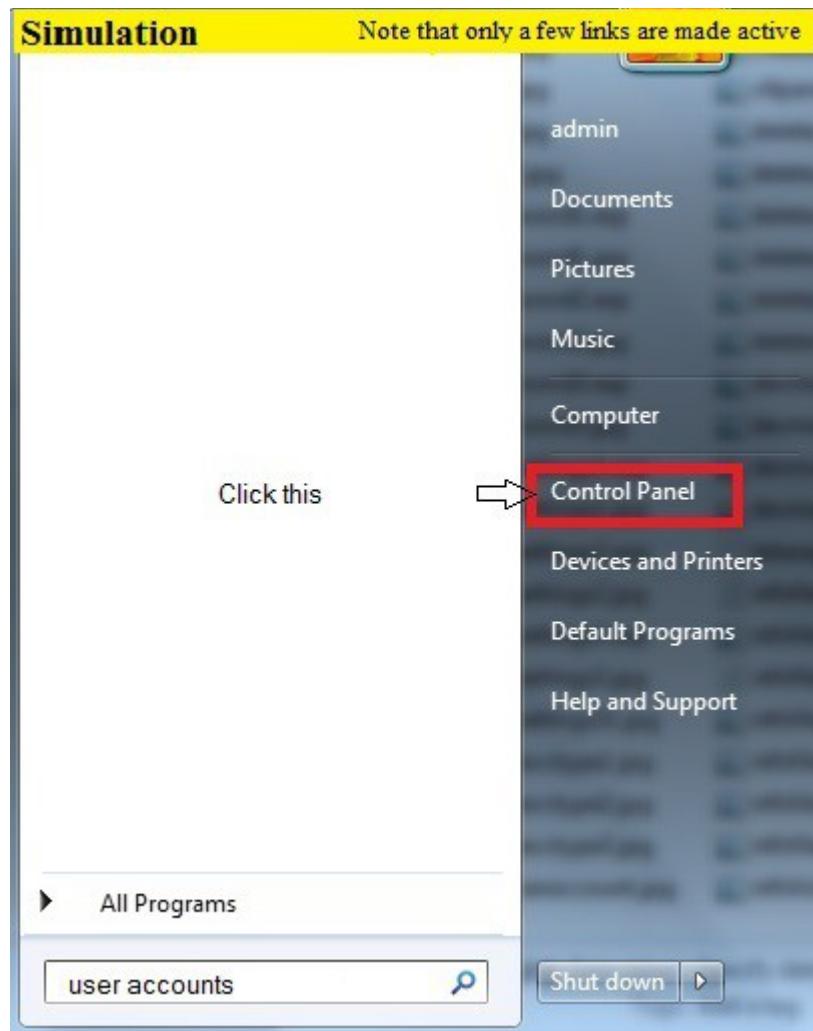
[Back](#)

9.22 User account creation , configuration and authentication in Windows 7

9.22.1 Creating a new user account

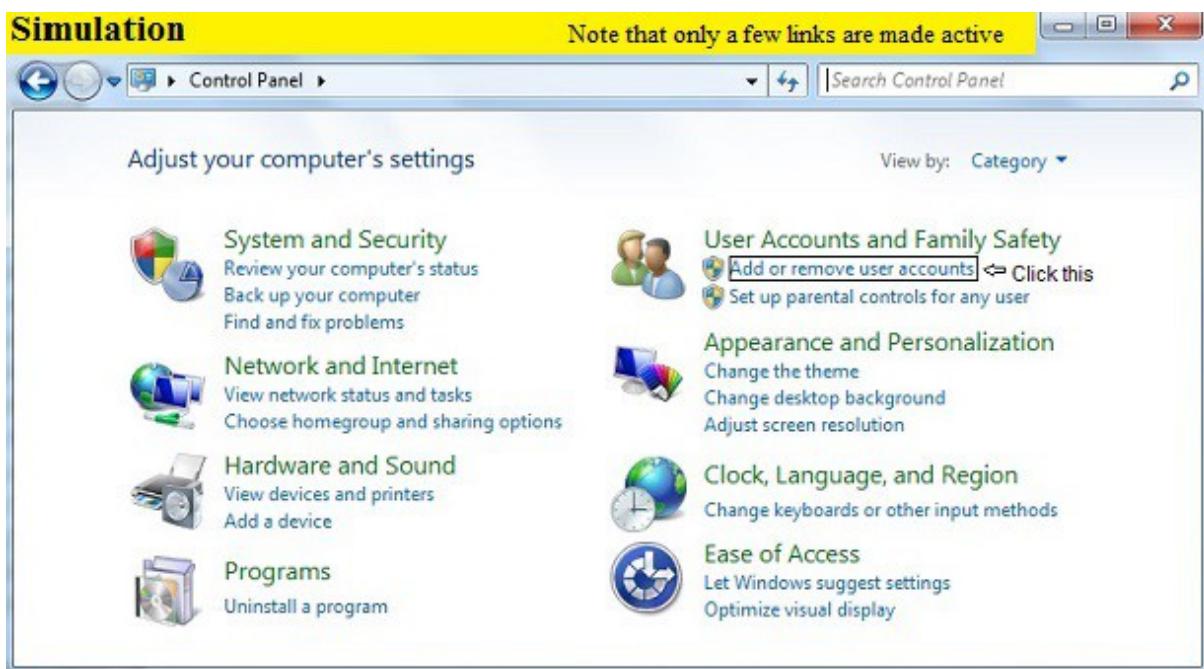
Description: This lab exercise explains how to create a new user account in windows 7

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

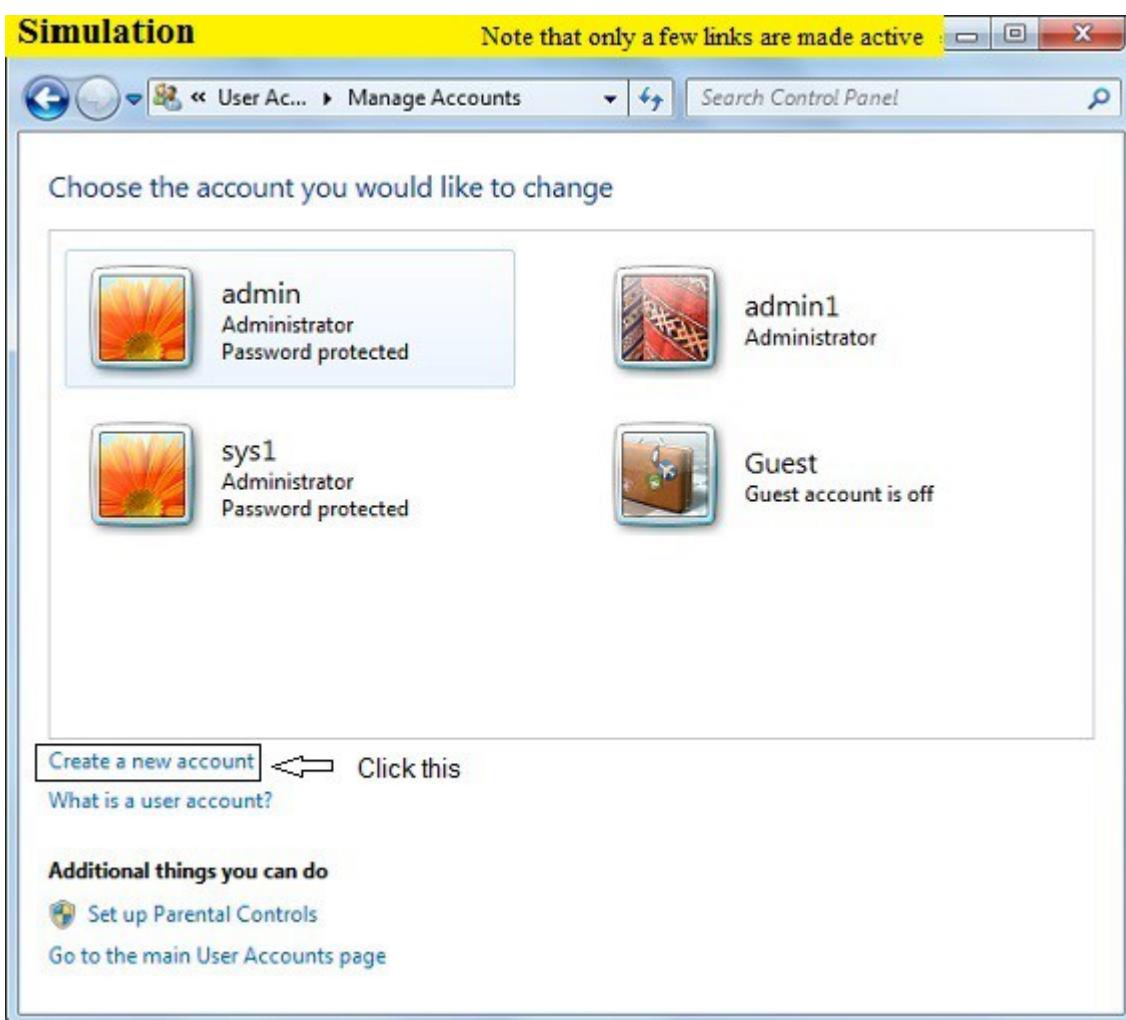


Go to step 2 if control panel option is clicked , otherwise go to step 3

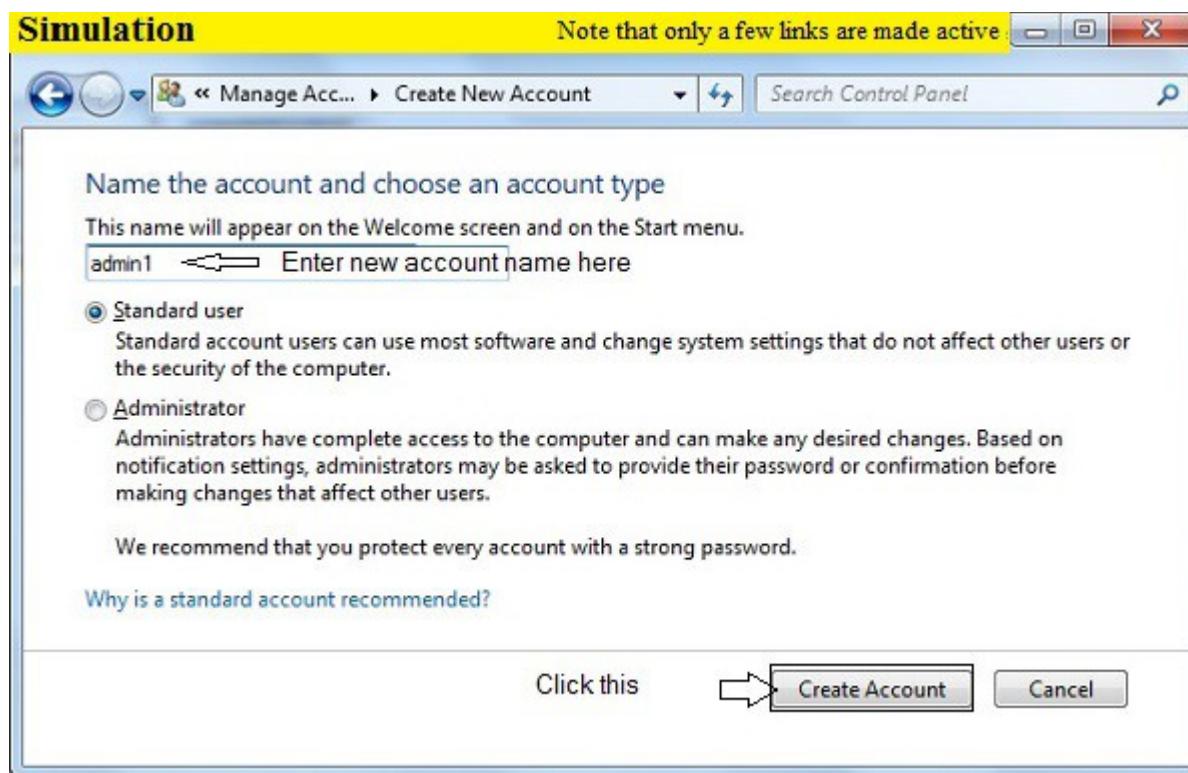
2. In control panel click Add or remove user accounts options.



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

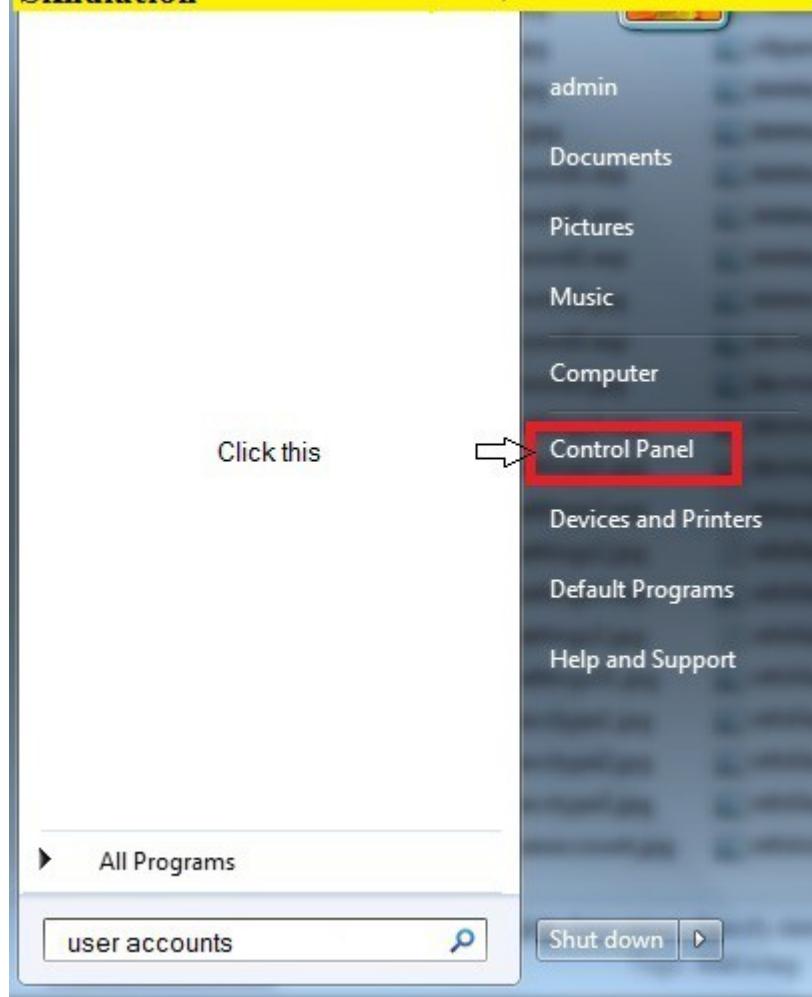
Description: This lab exercise explains changing user account password settings in windows 7.

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

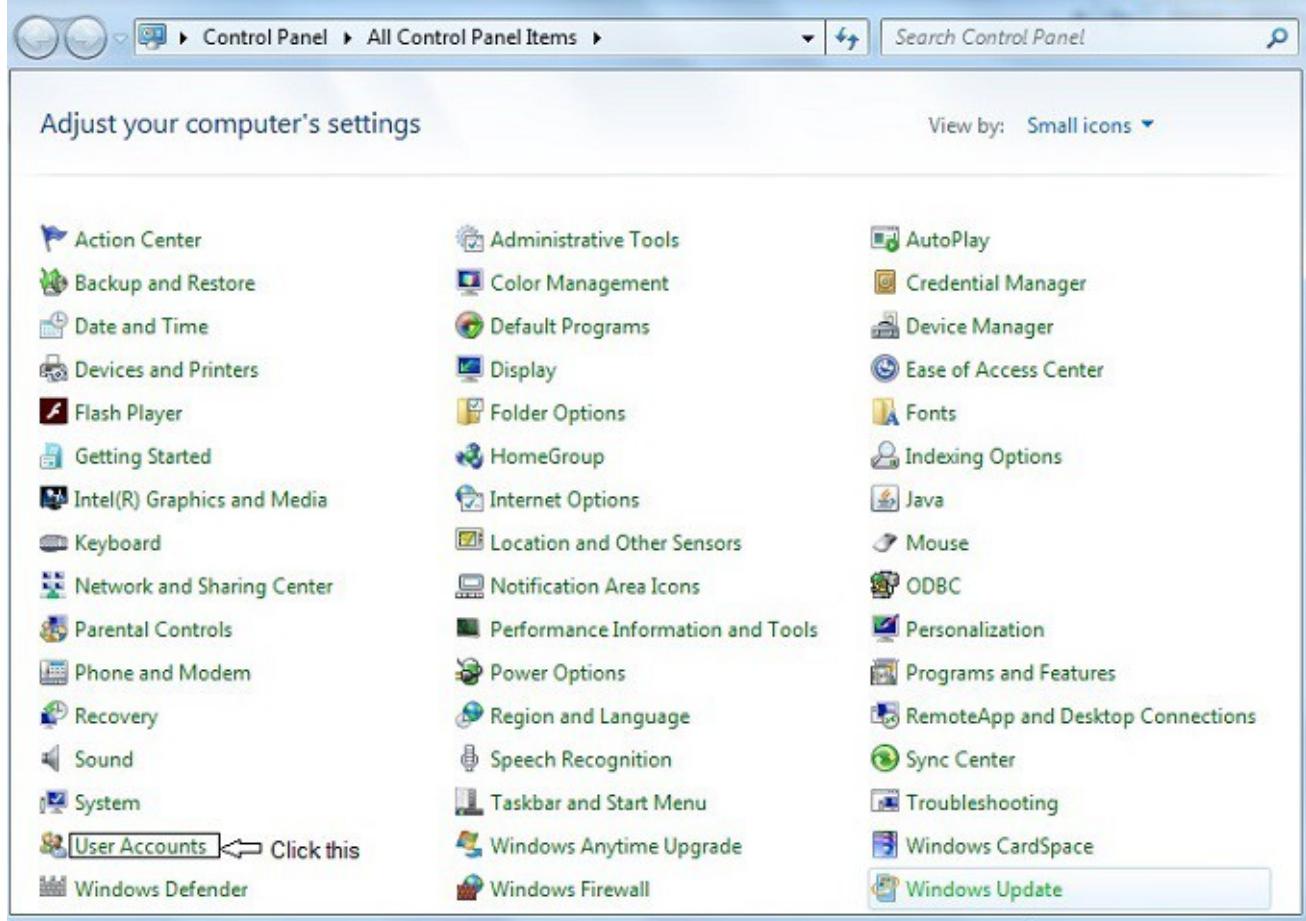
Note that only a few links are made active



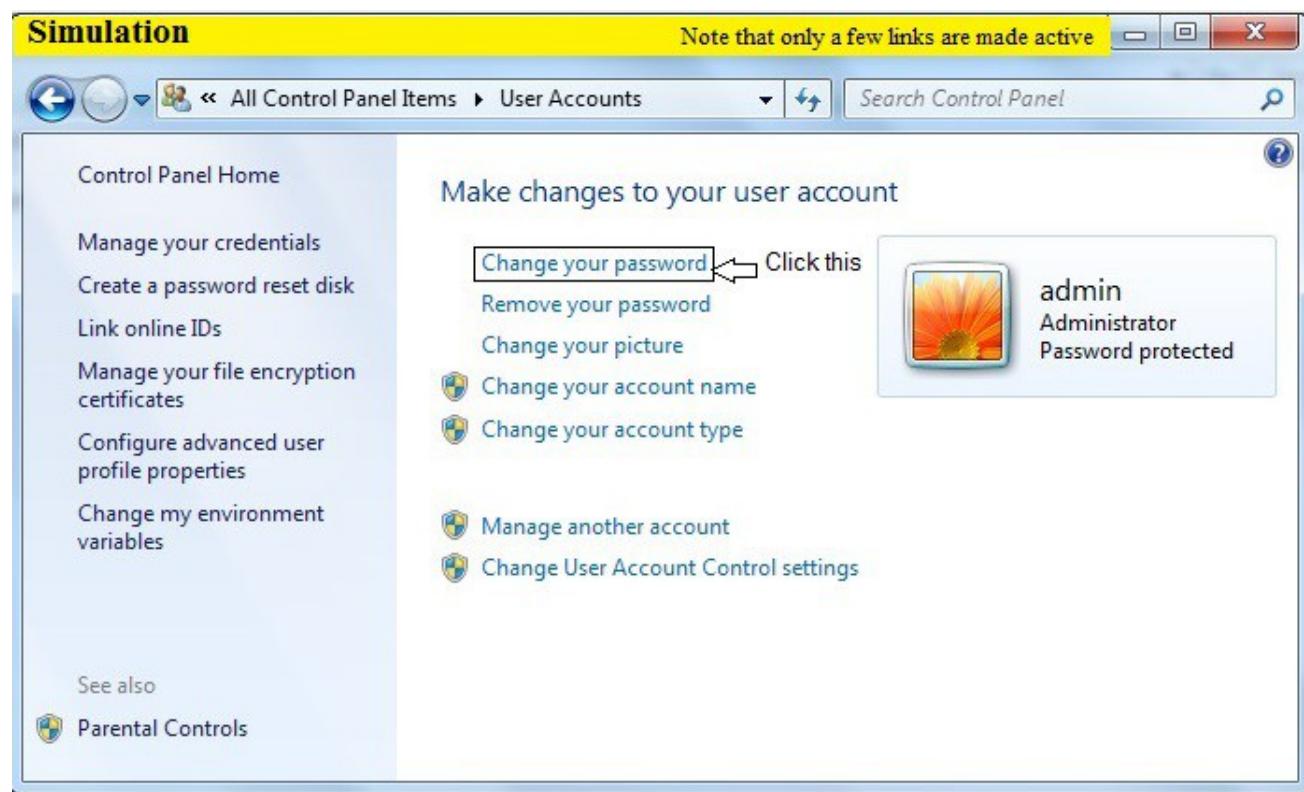
2. In control panel window click User Accounts options

Simulation

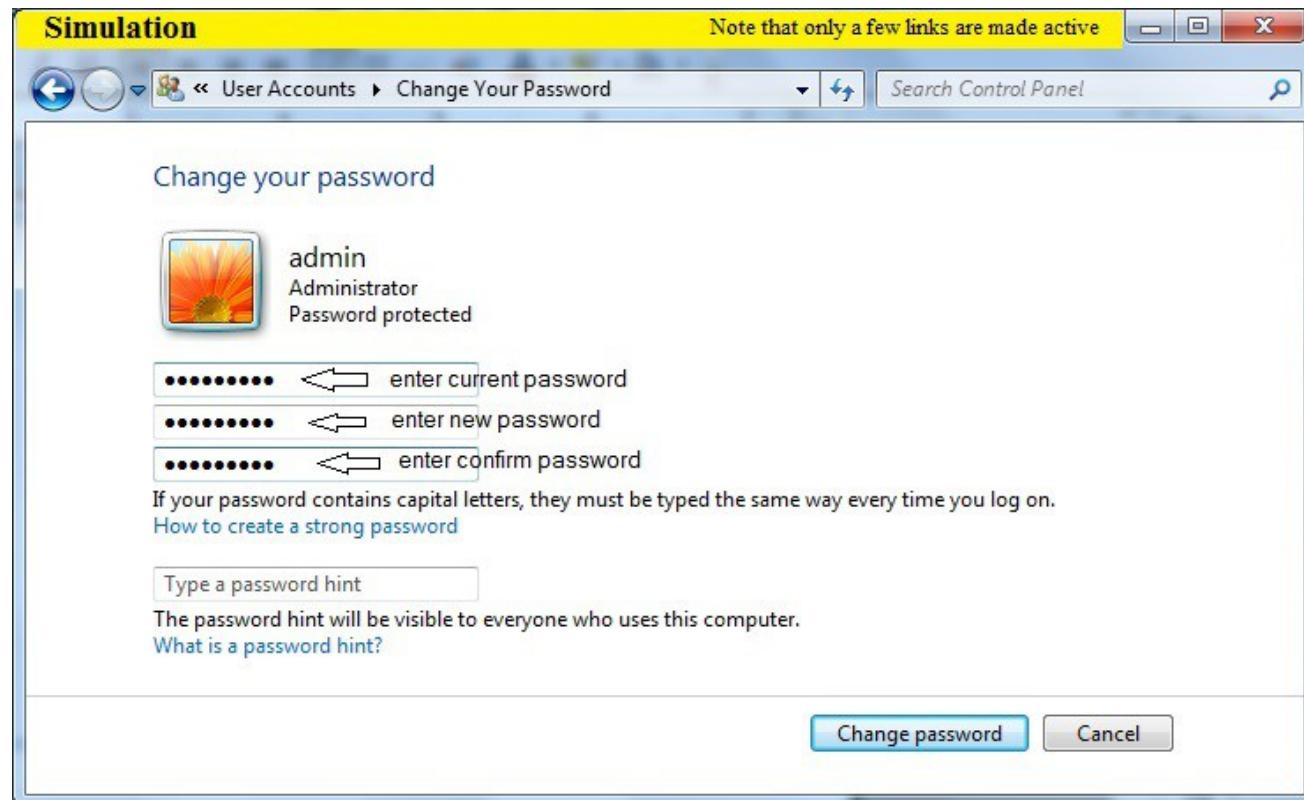
Note that only a few links are made active



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

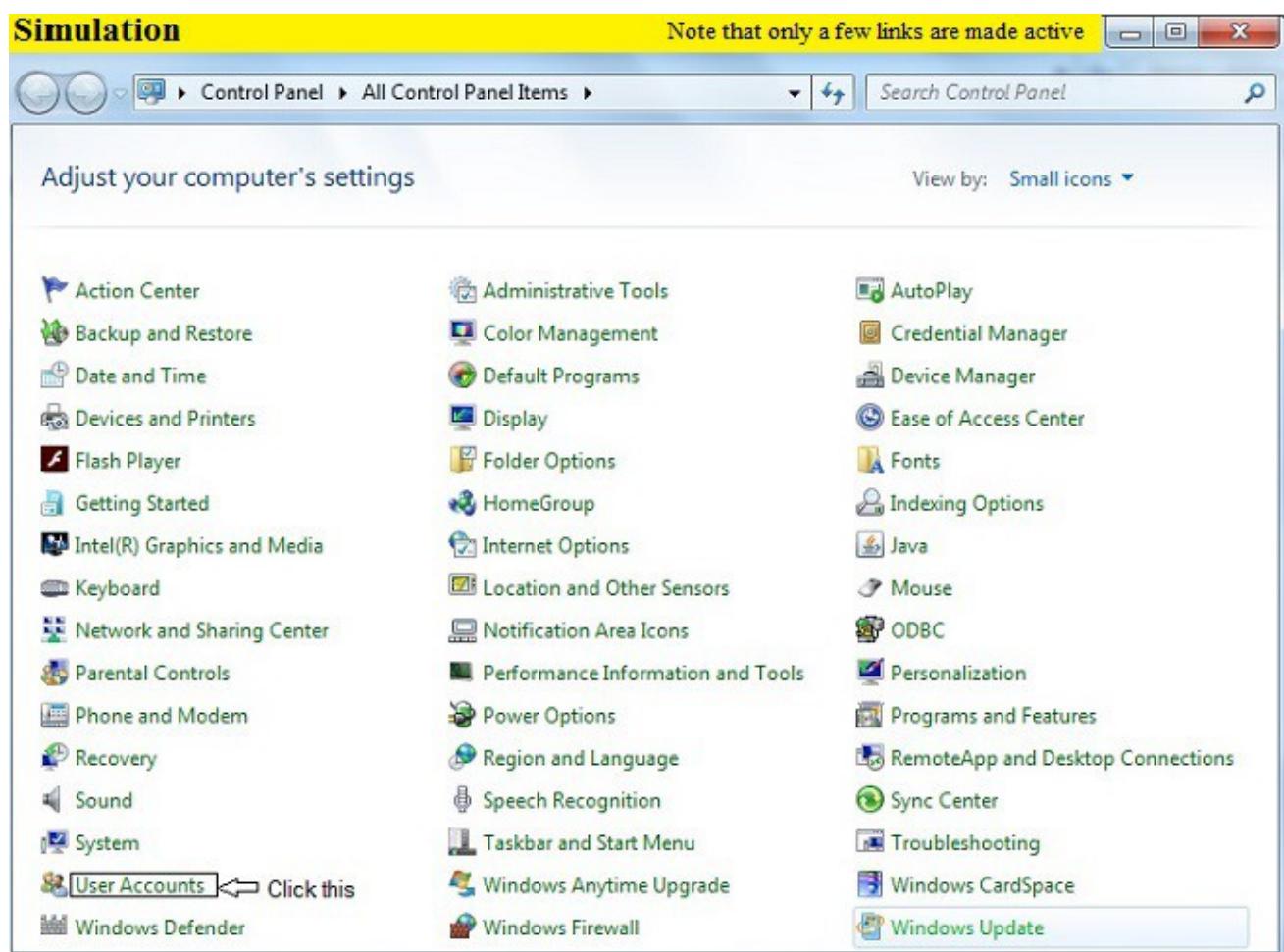
9.22.3 To change user account control settings

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

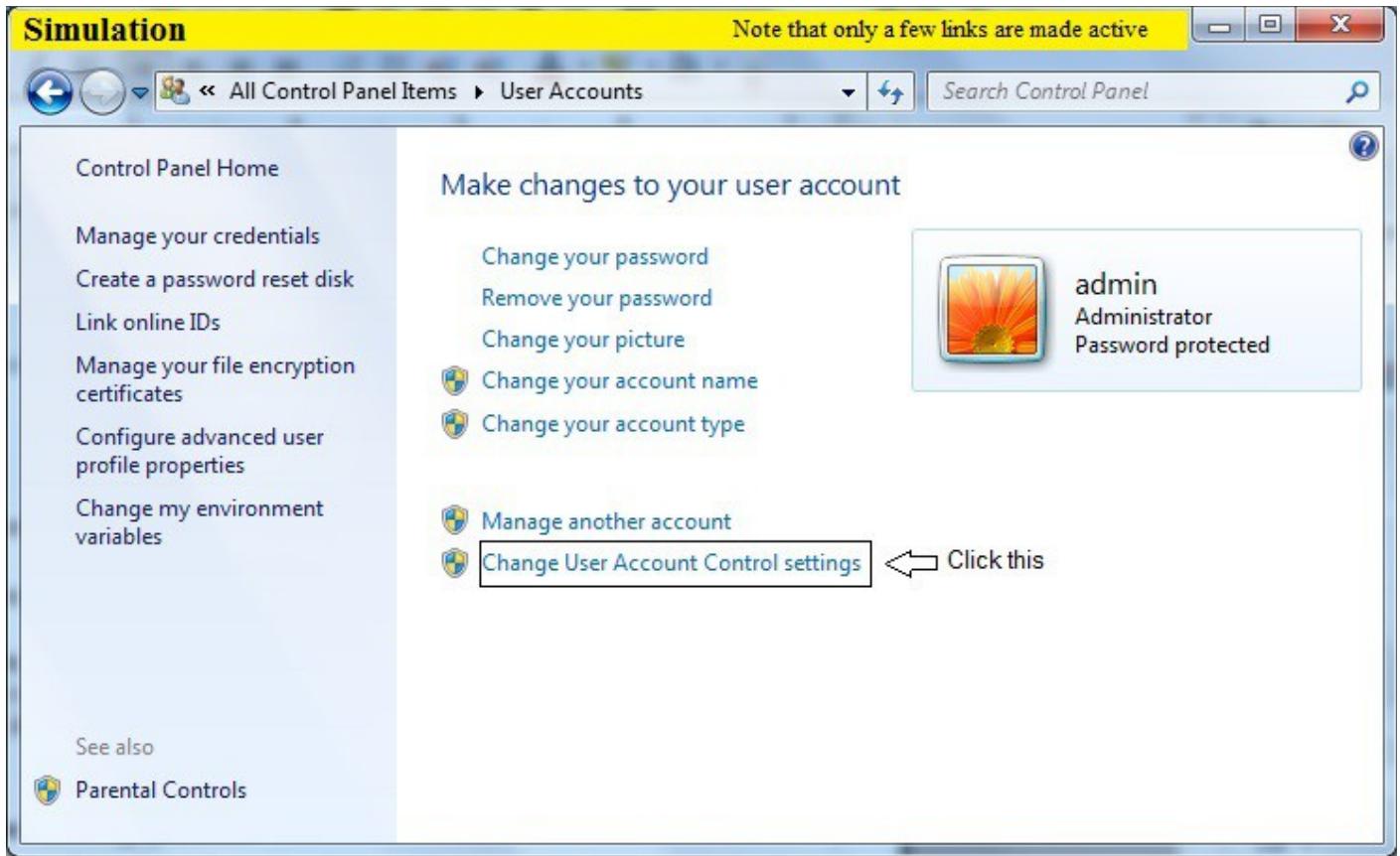
Instructions: 1. On loading a lab exercise, in a given simulation start menu either type user accounts in search box or click control panel option

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

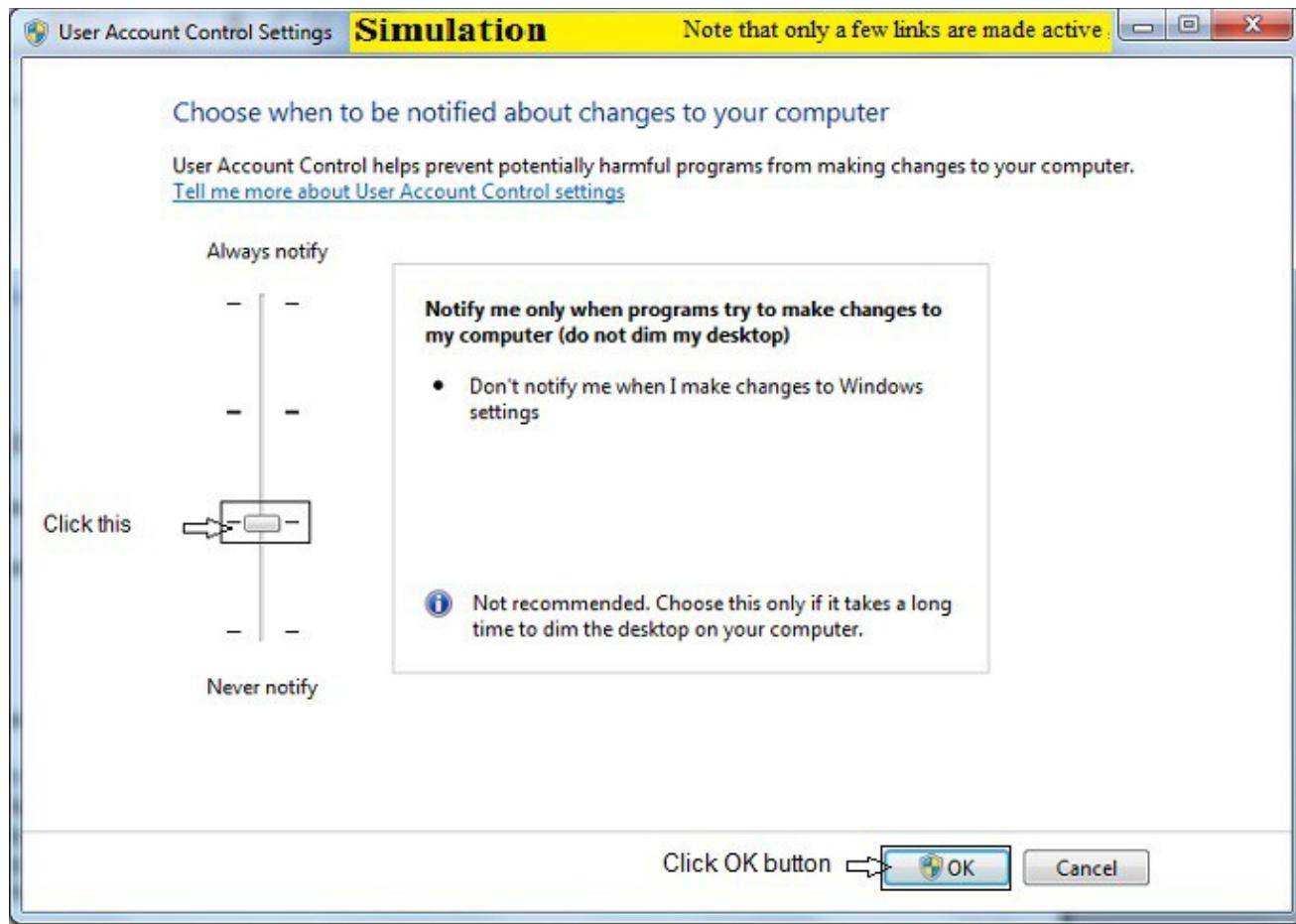
2. In control panel window click User Accounts



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

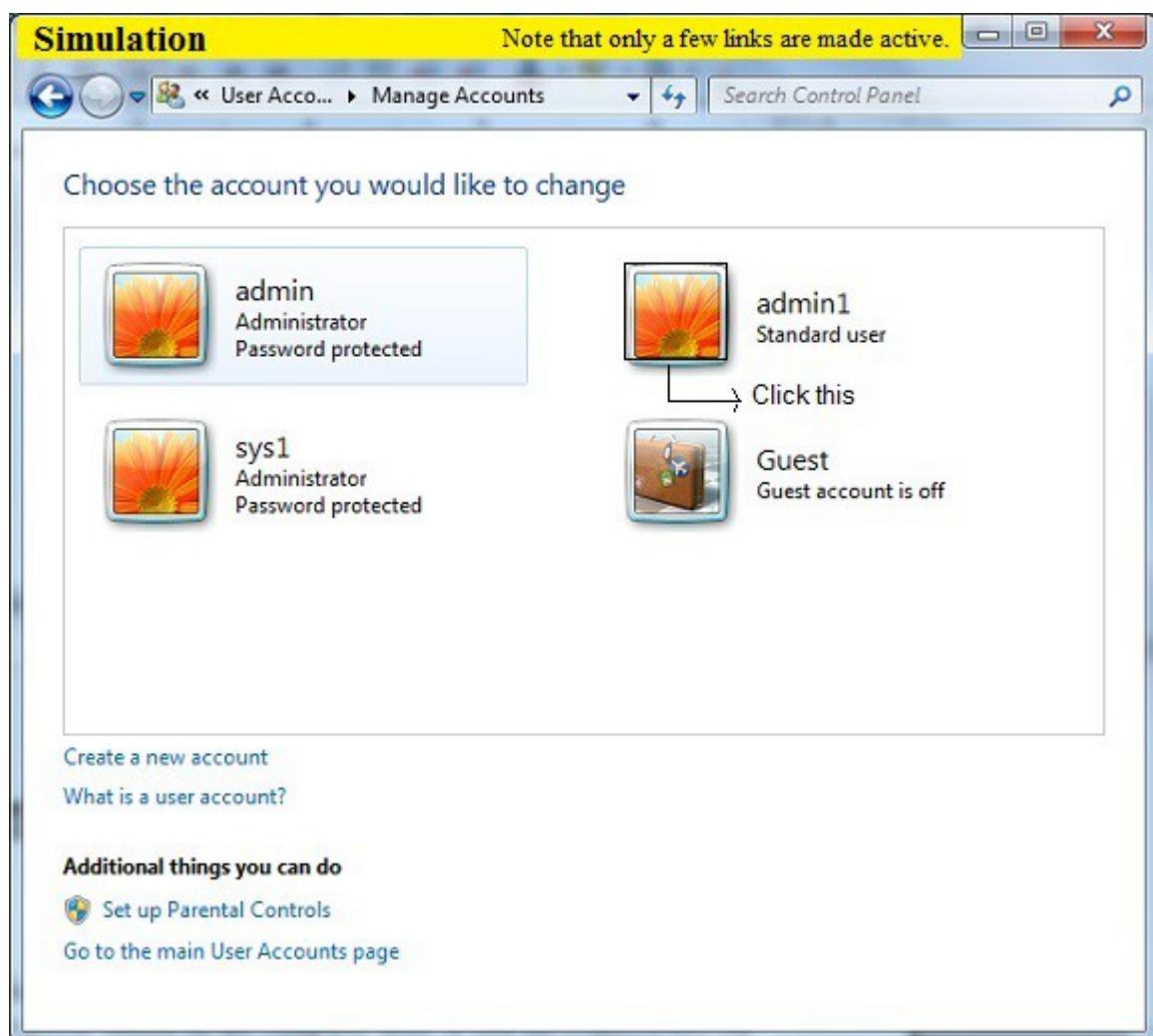
Instructions: 1. On loading a lab exercise, in a given simulation start menu either type “user accounts” in search box or click control panel option

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

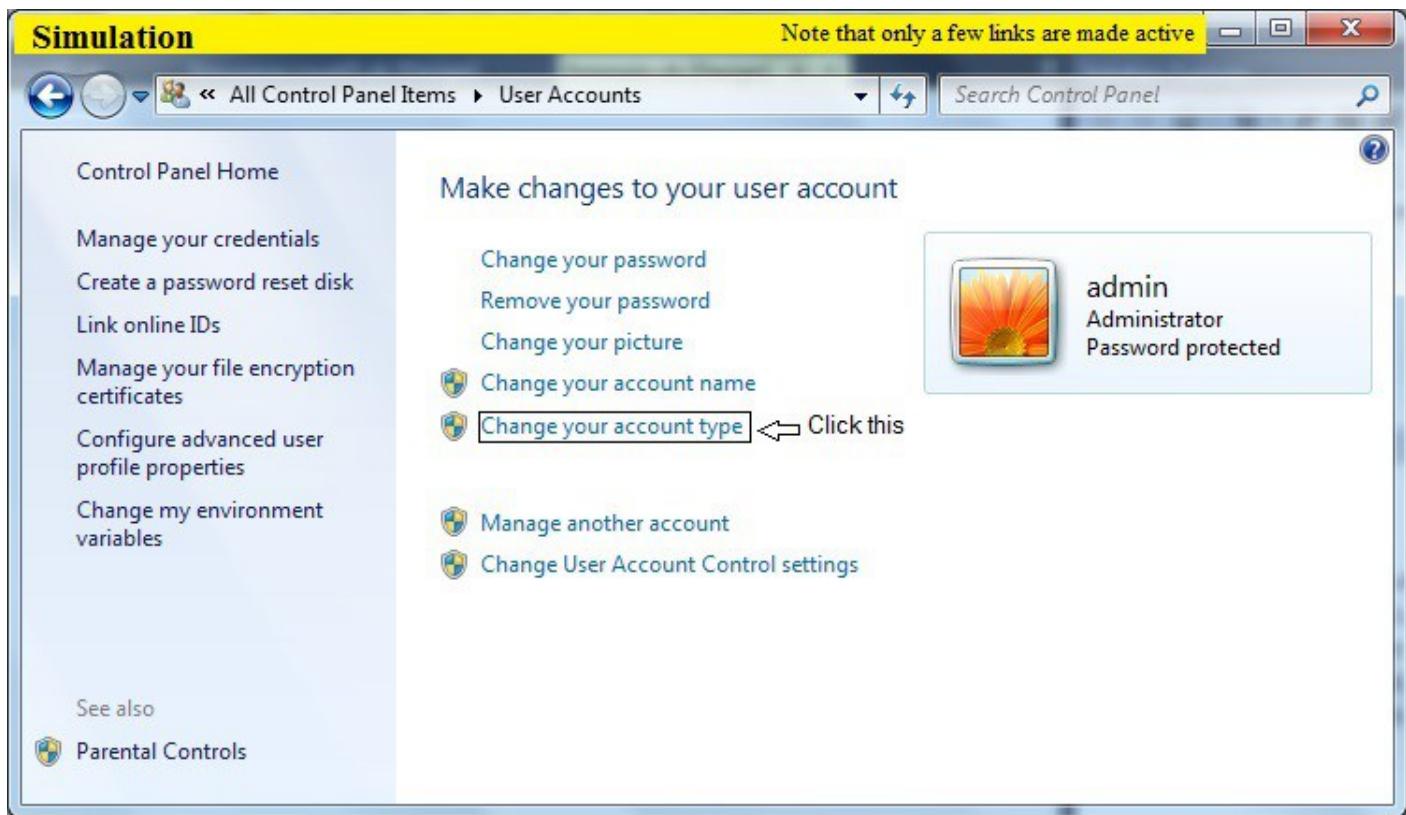
2. In a given control panel items window click Add or remove user accounts



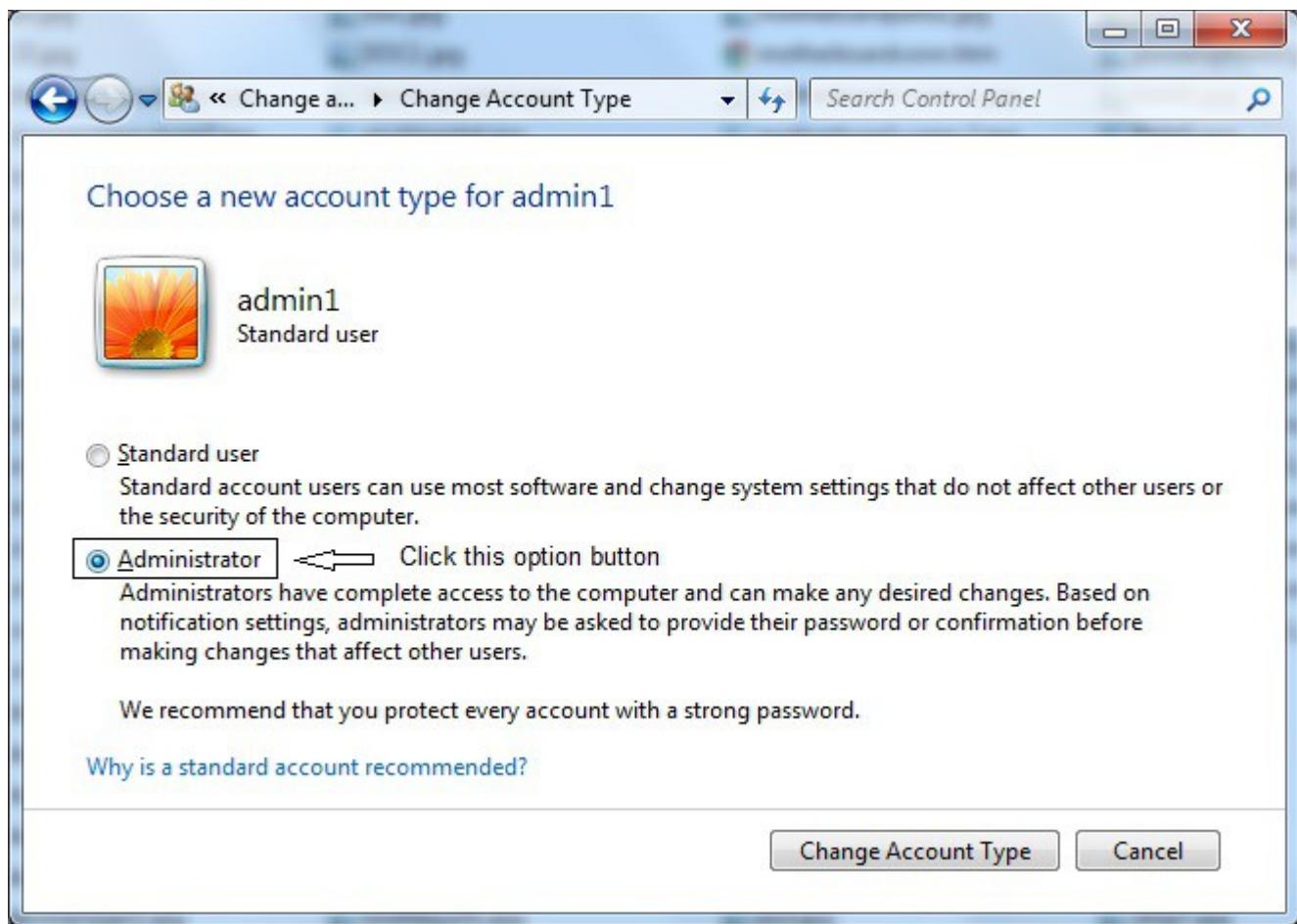
3. In Manage Accounts window click the icon or picture Admin1



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

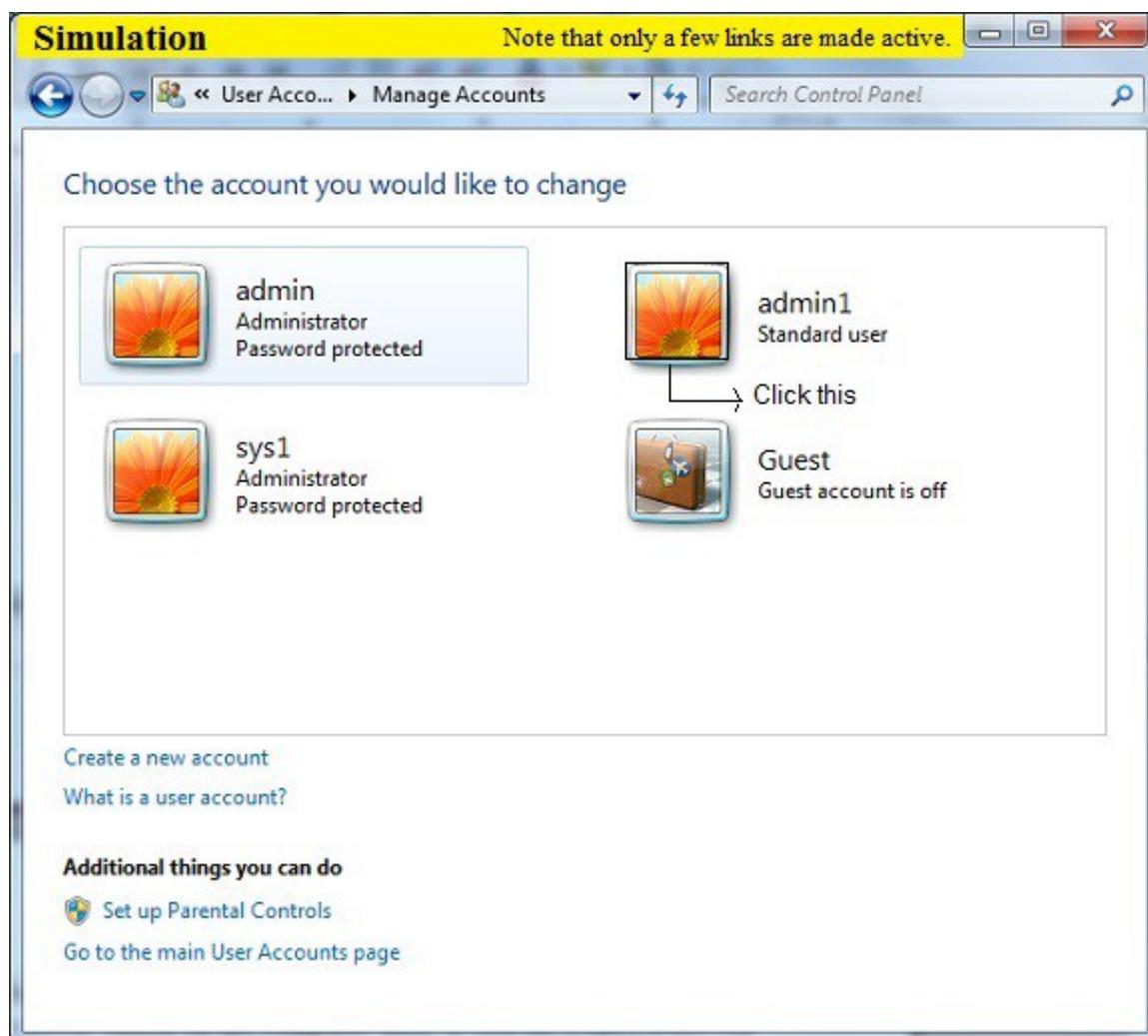
Instructions: 1. On loading a lab exercise, in a given simulation start menu either type user accounts in search box or click control panel option

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

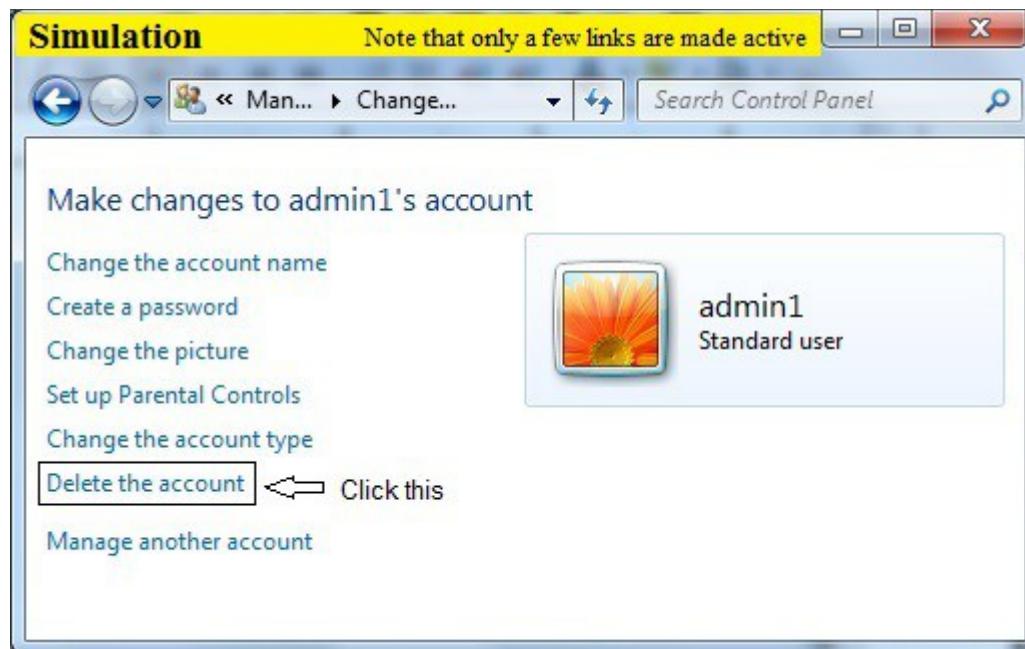
2. In control Panel window click the option Add or remove user accounts



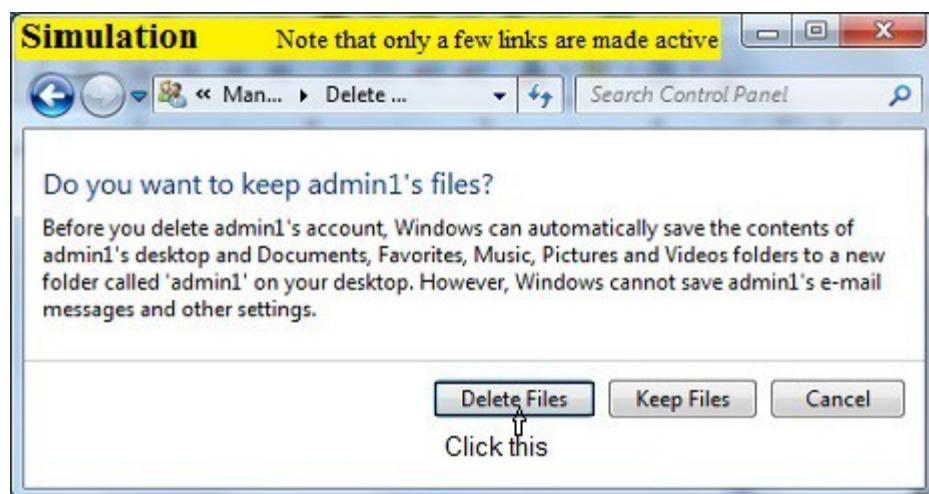
3. In Manage Accounts window click the icon or picture Admin1



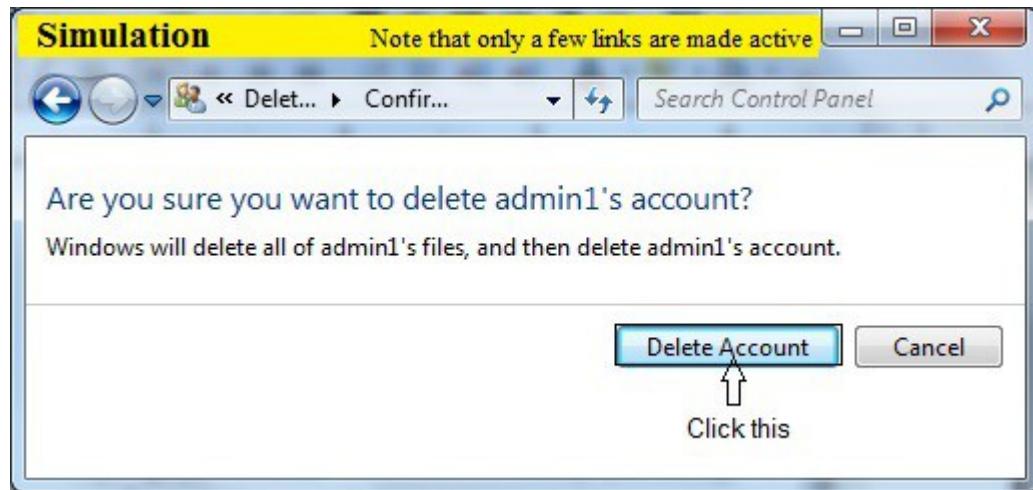
4. In Make changes to admin1 account click Delete the account option



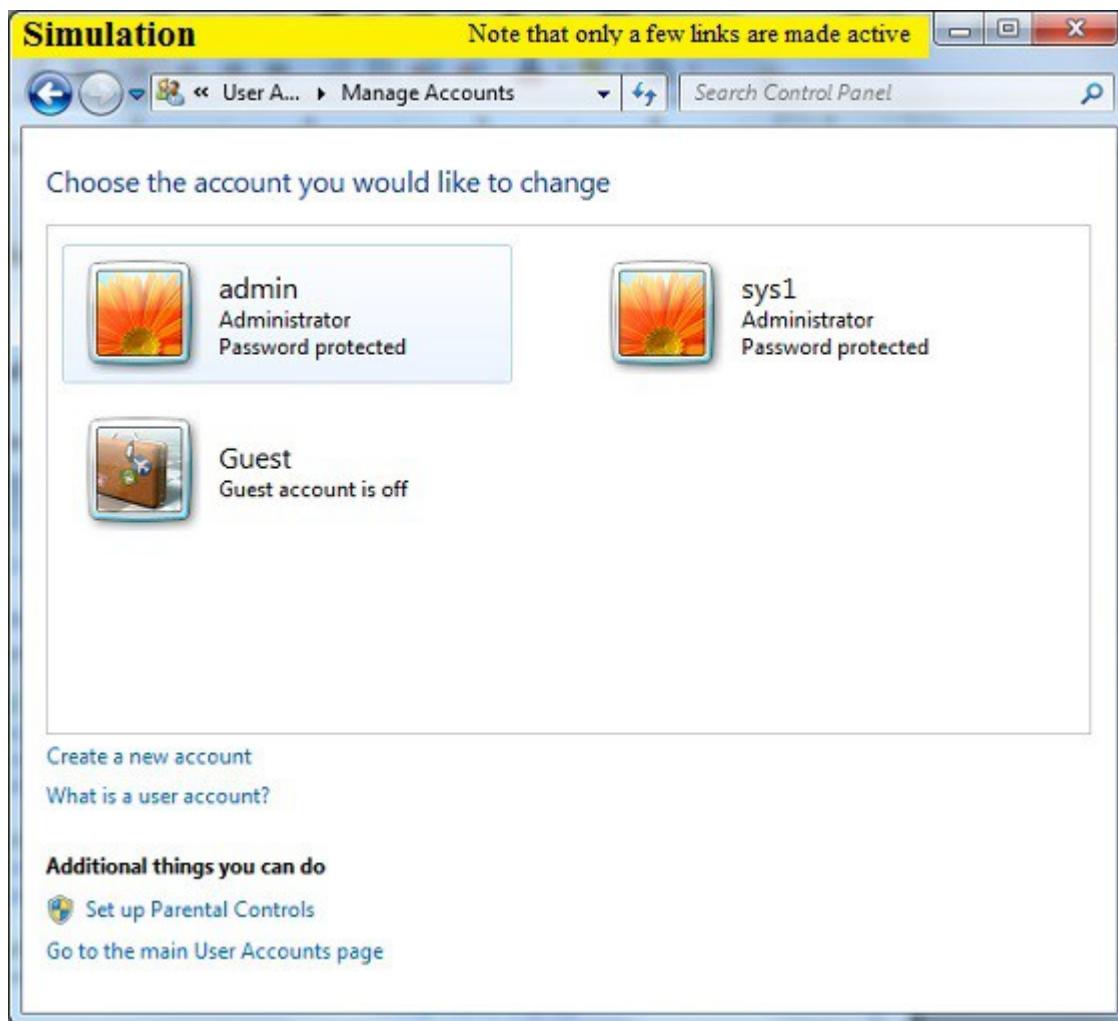
5. Click on the option to Delete the account and the Delete Account window will load asking you to choose whether or not to delete or keep the user's files. Click Delete Files button.



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.



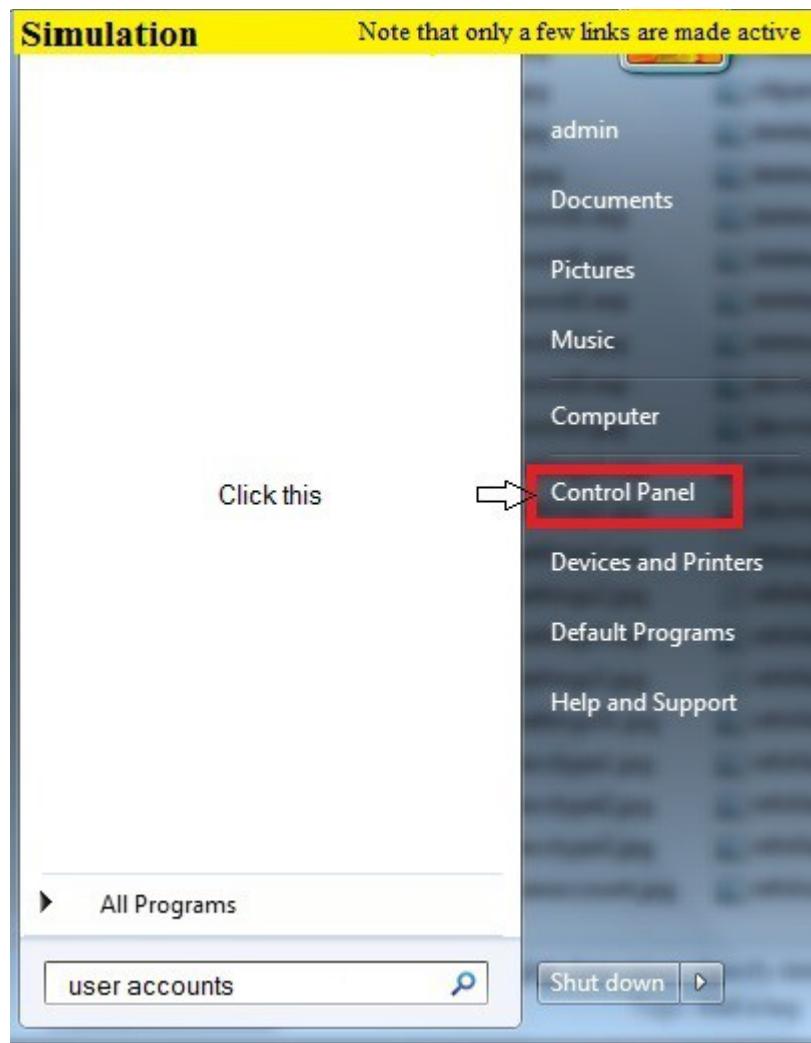
Explanation: User account on computer that is not being used can be permanently removed by deleting it.

[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

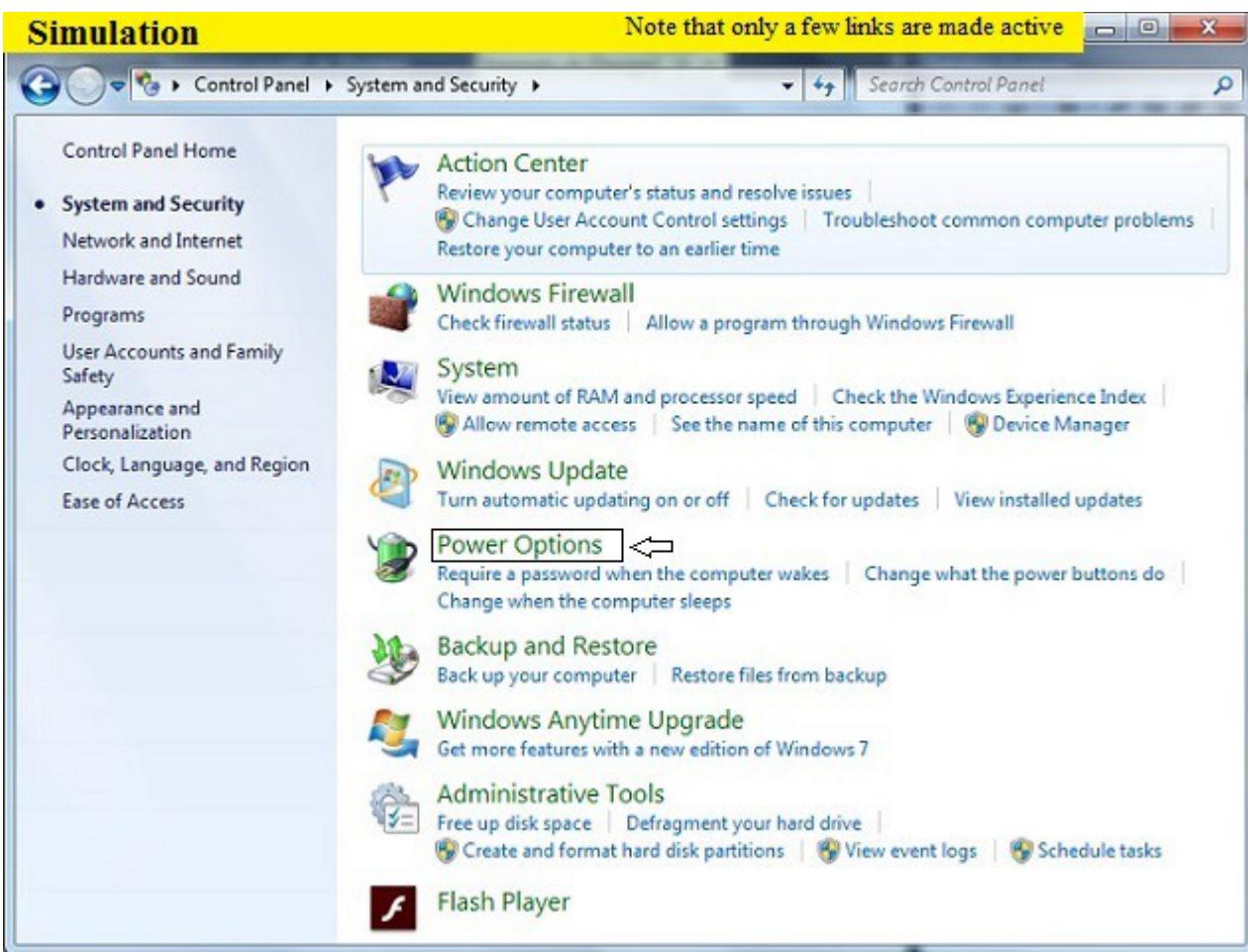


Go to step 2 if control panel is clicked otherwise go to step 4

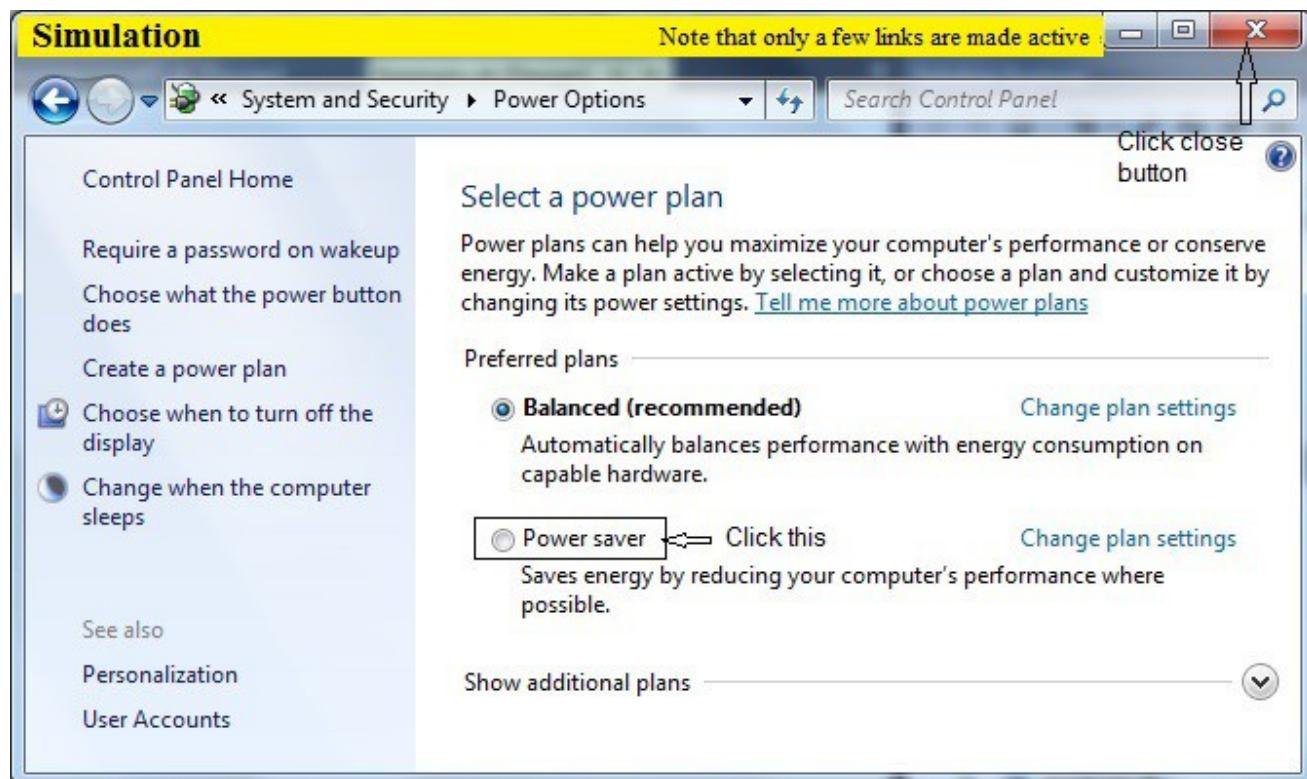
2. In a given control Panel window click the option System and Security



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.

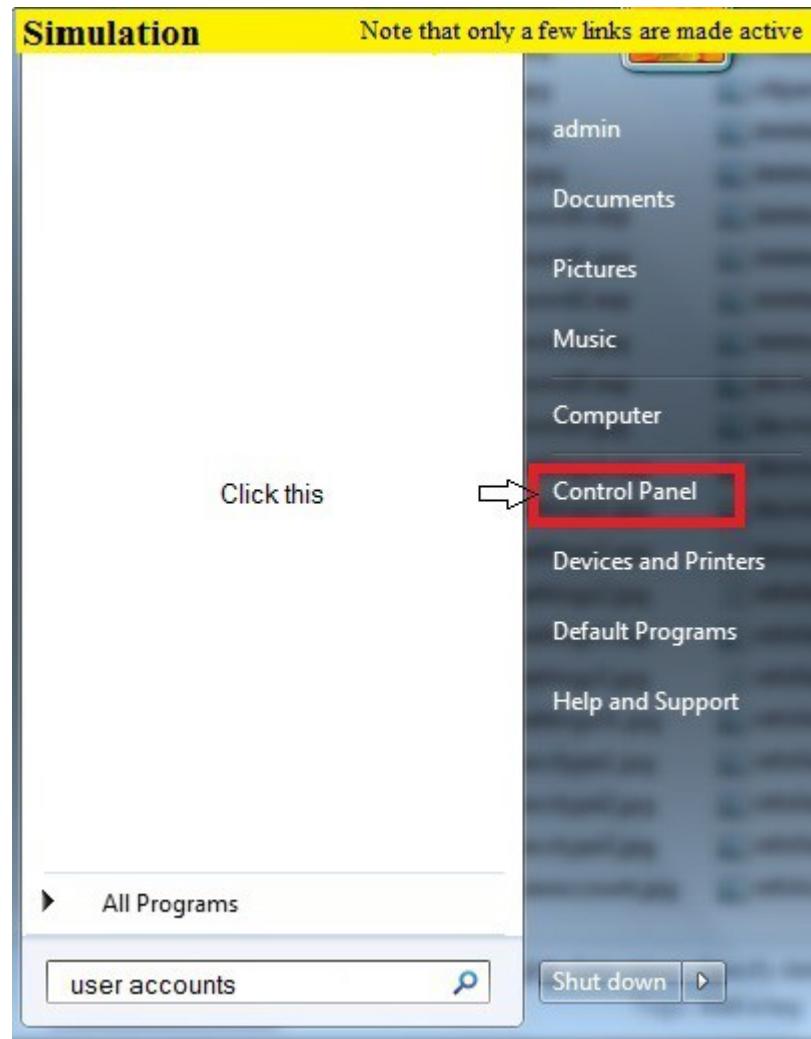
[Back](#)

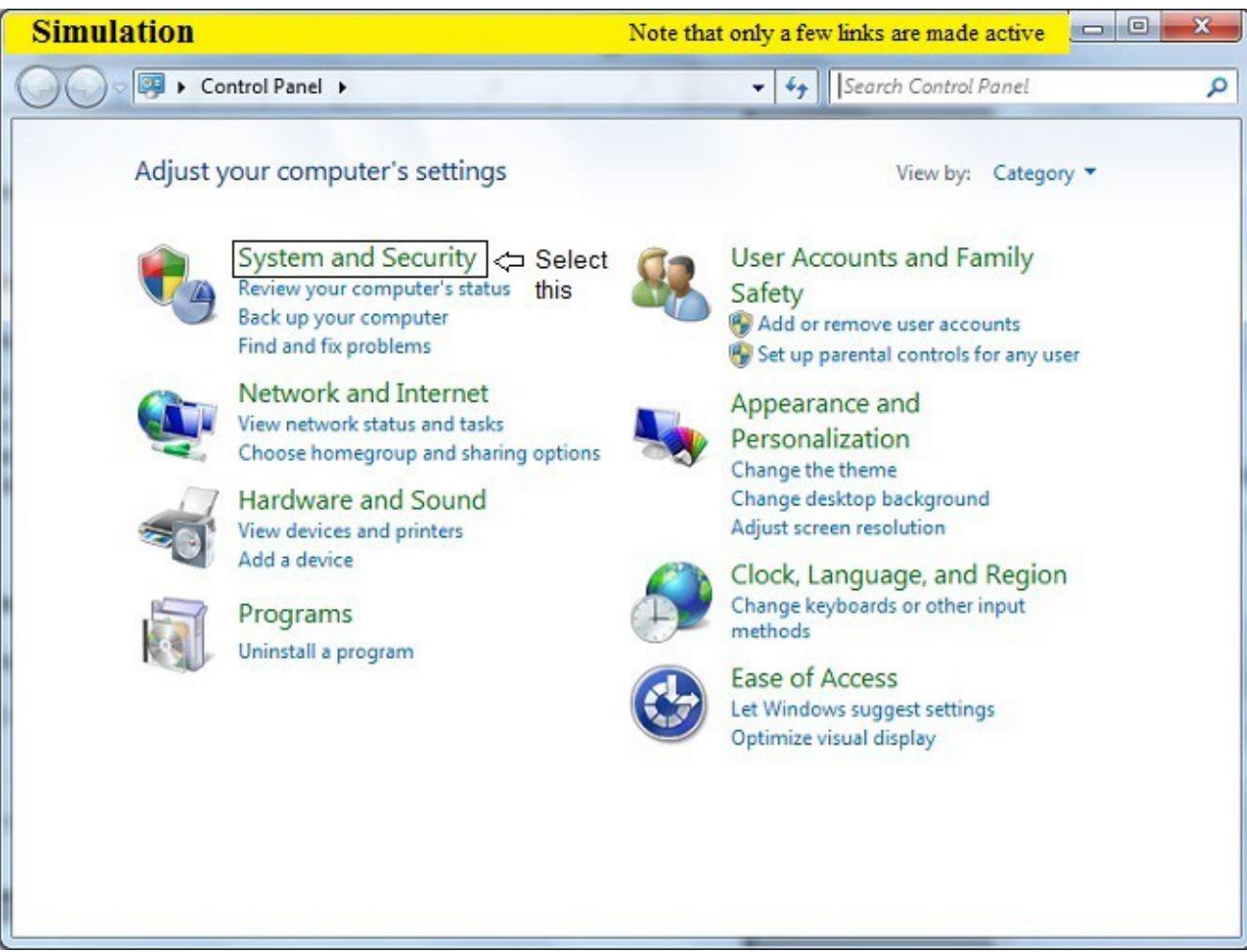
9.24 Configuring windows 7 update settings

9.24.1 Turning ON/OFF recommended updates

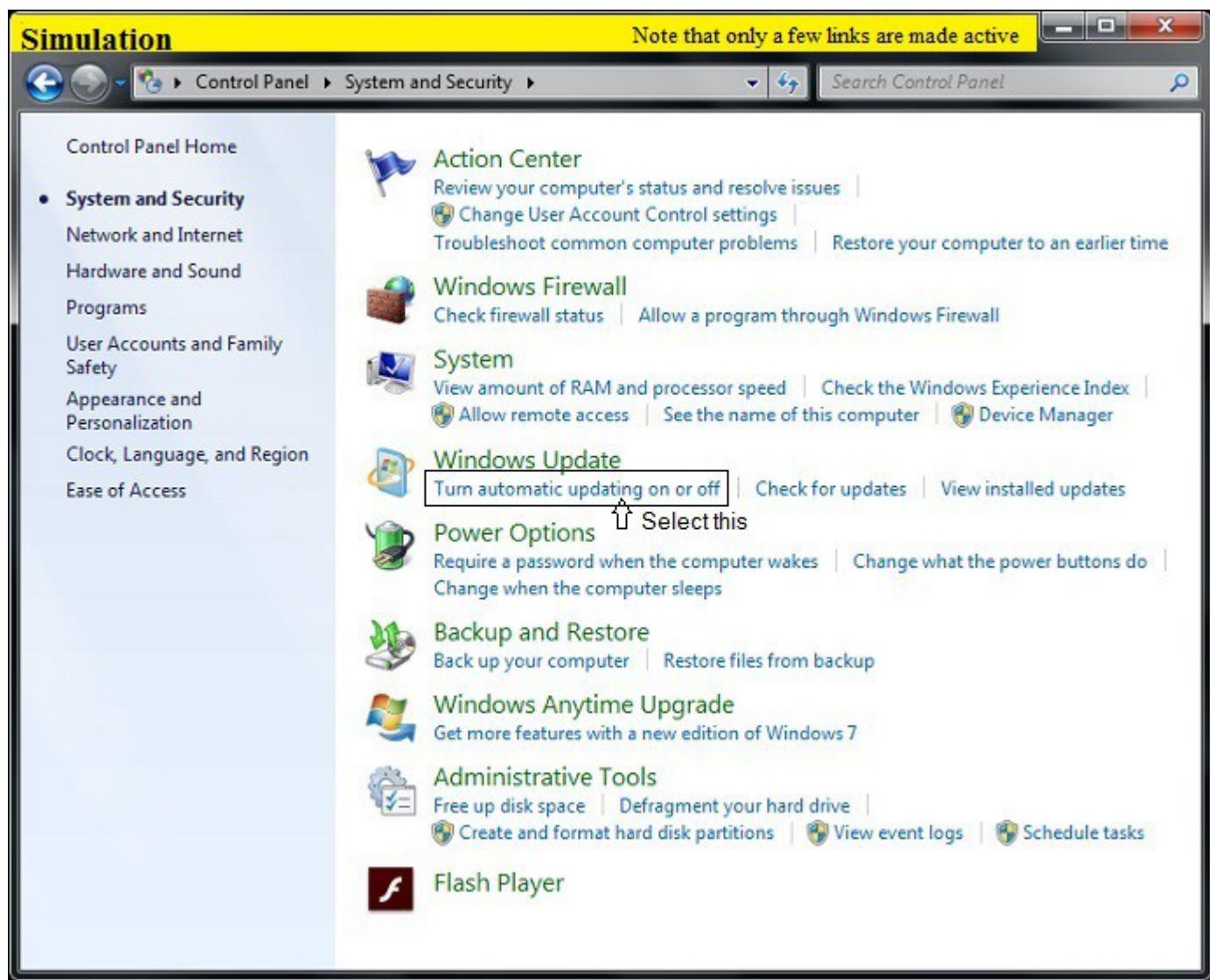
Description: This lab exercise explains turning ON/OFF recommended updates in windows 7 OS

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

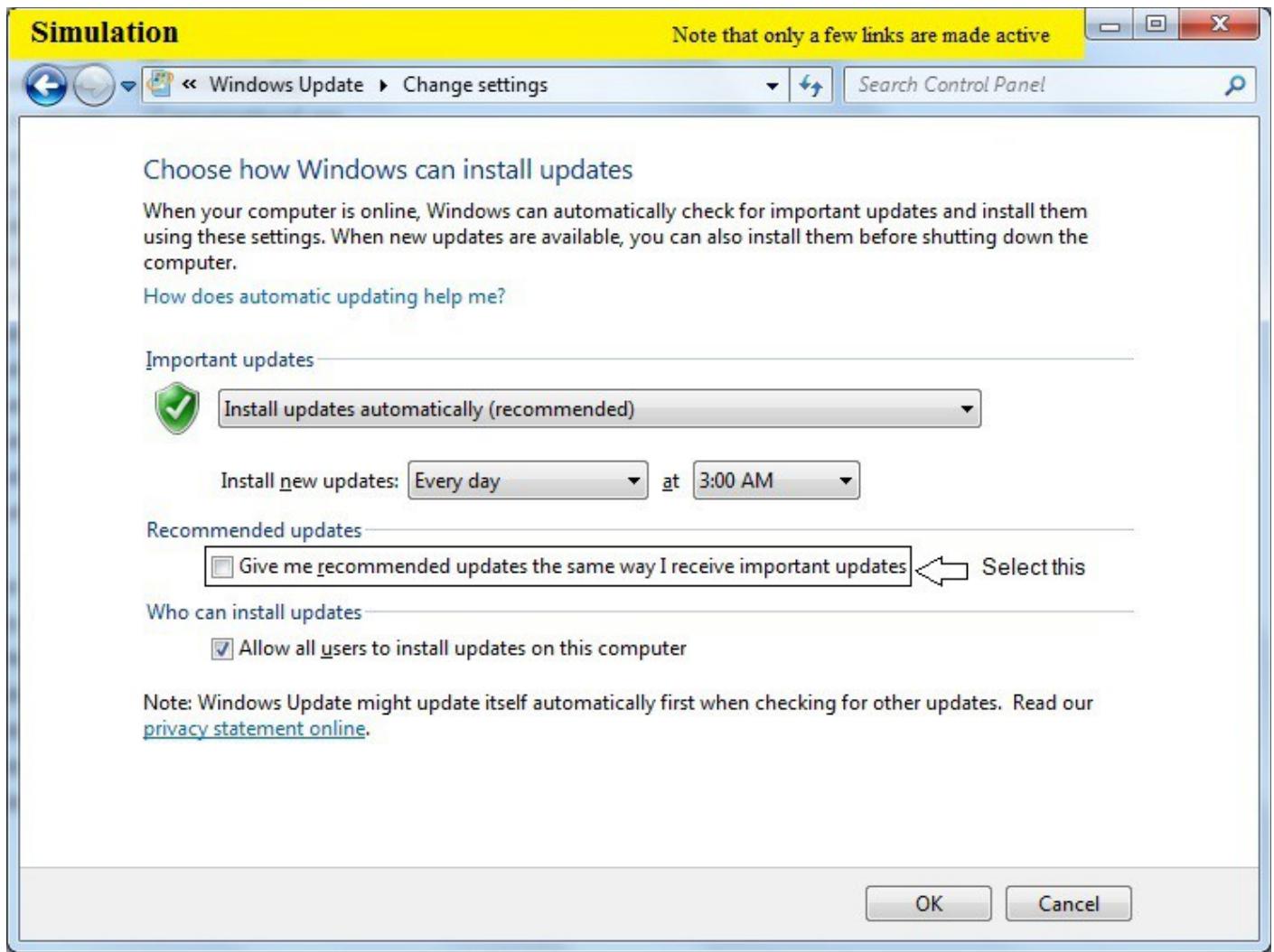




3. Under Windows Update, click Turn automatic updating on or off.



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

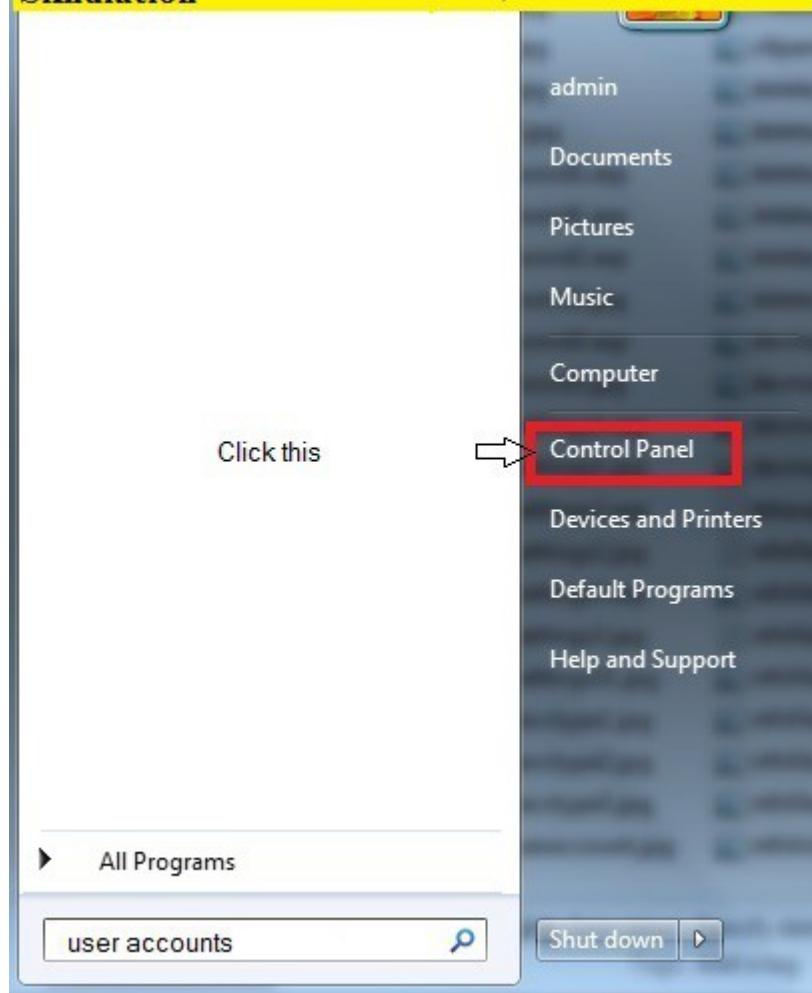
Description: This lab exercise explains turning ON/OFF automatic updates in windows 7 OS

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

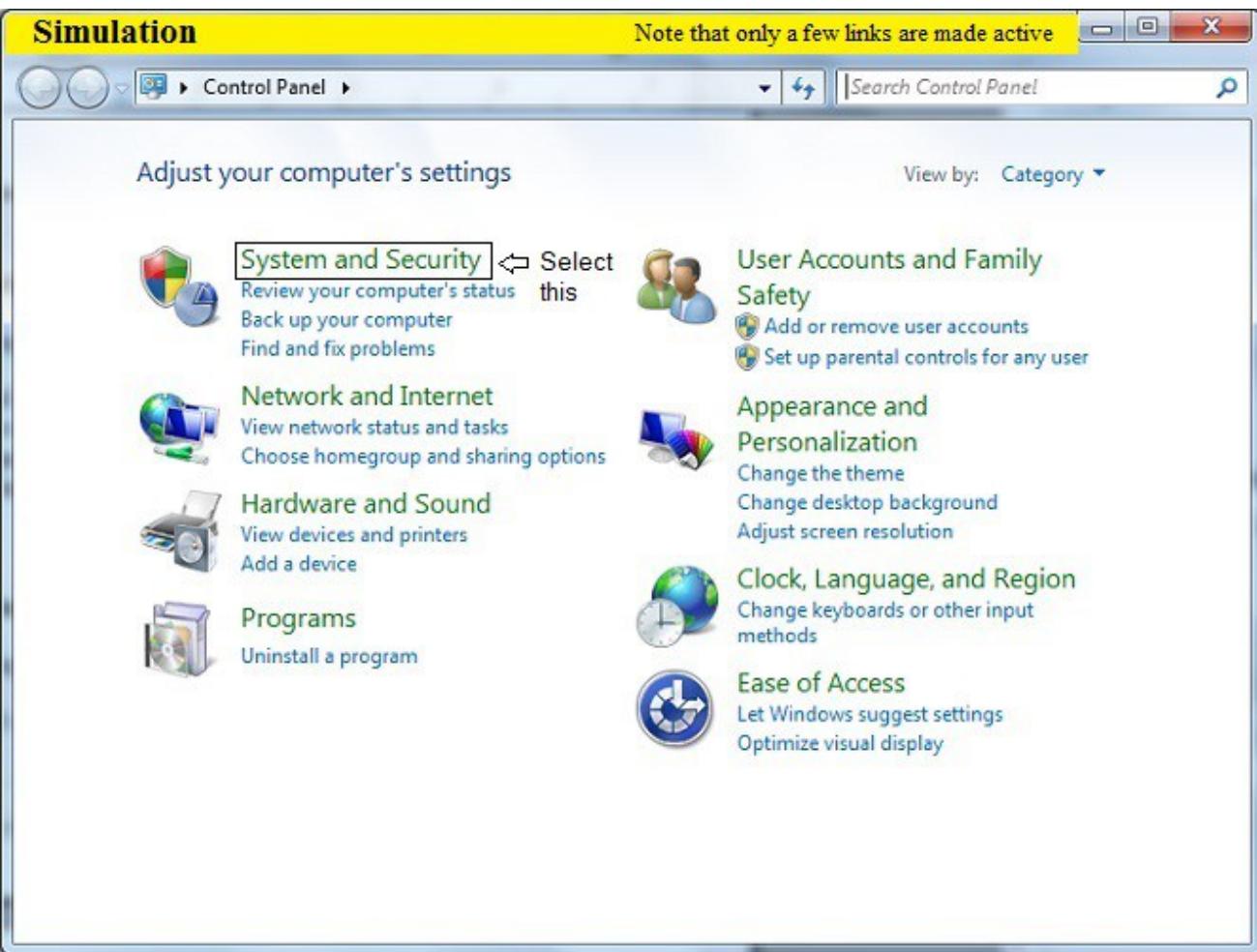
if control panel is clicked go to step 2,3 and 5 otherwise go to step 4 and step 5

Simulation

Note that only a few links are made active



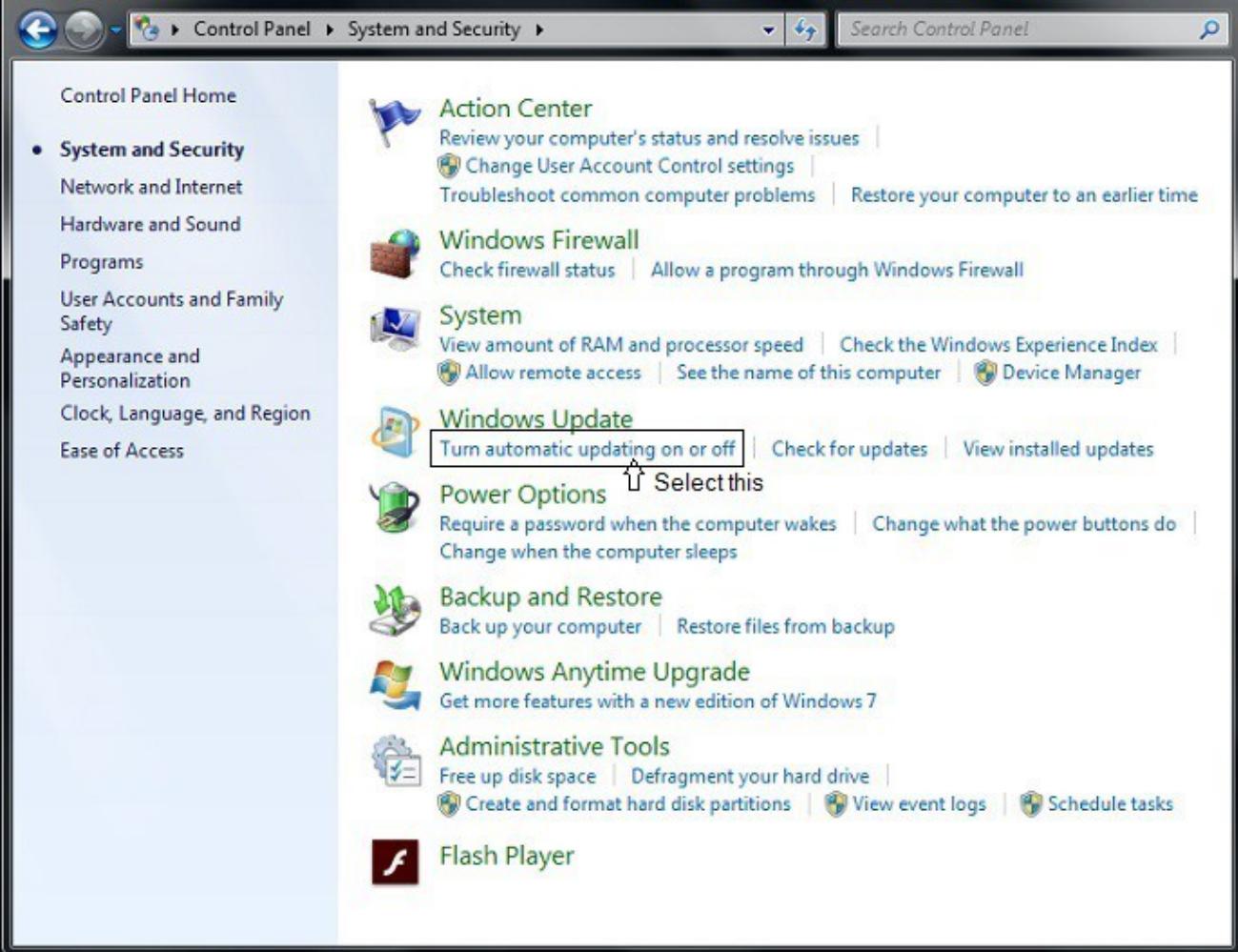
2. In control panel window click “System and security”



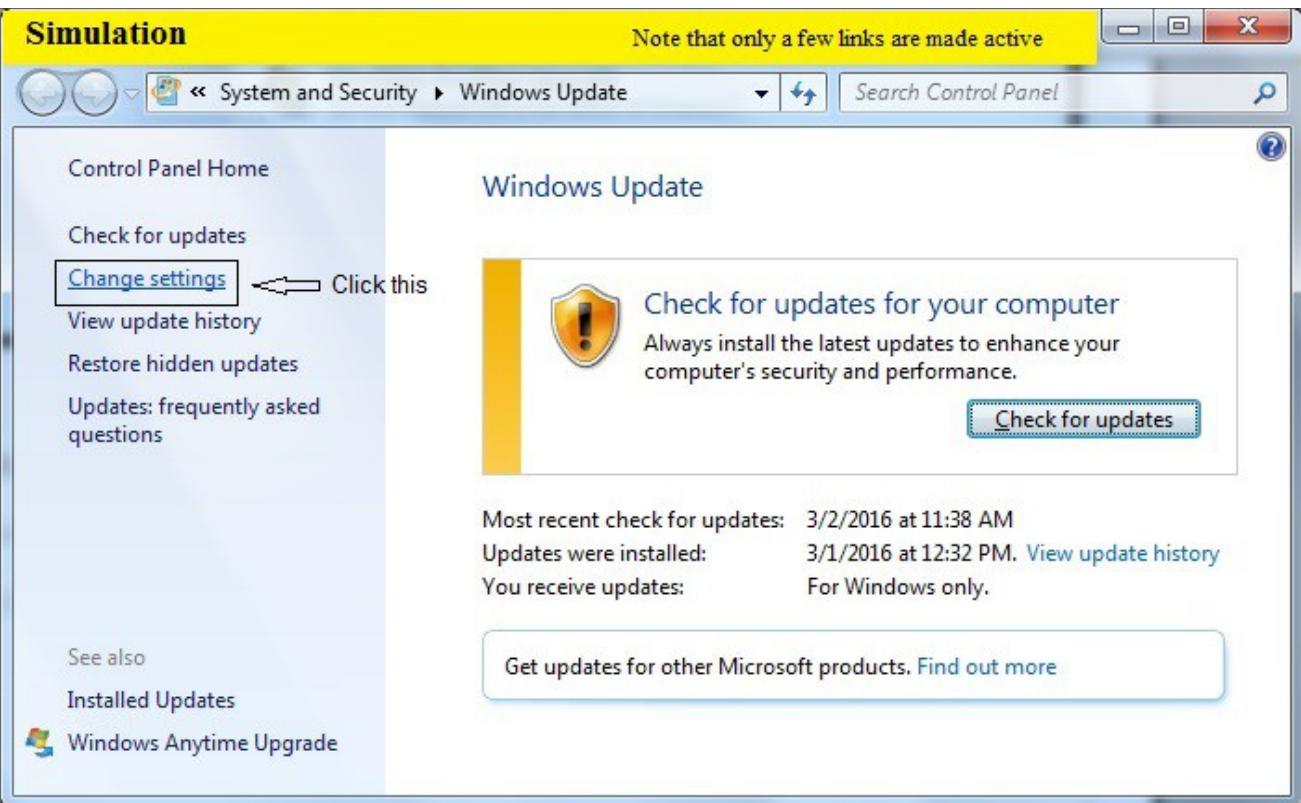
3. Under Windows Update, click “Turn automatic updating on or off”.

Simulation

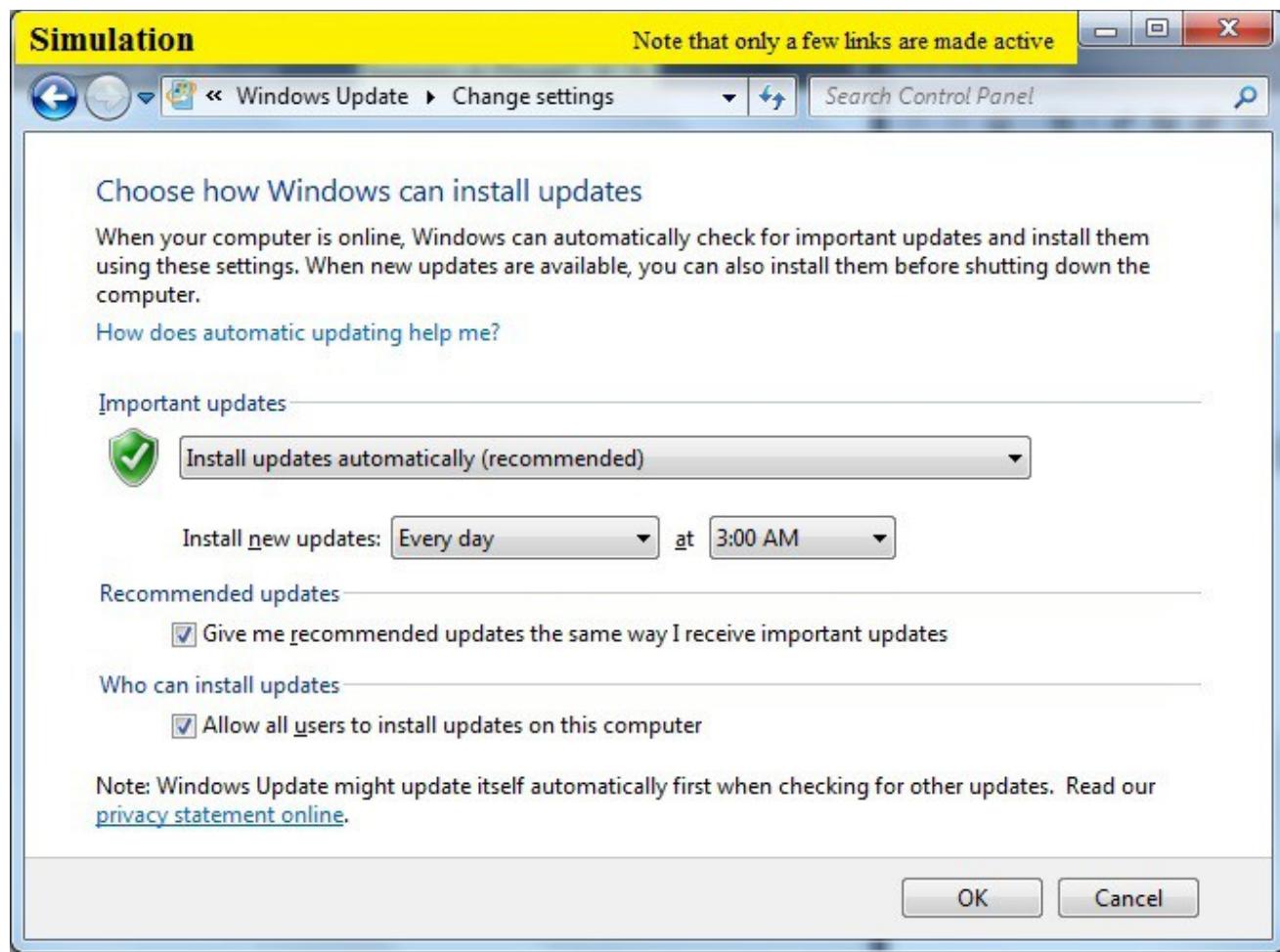
Note that only a few links are made active



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

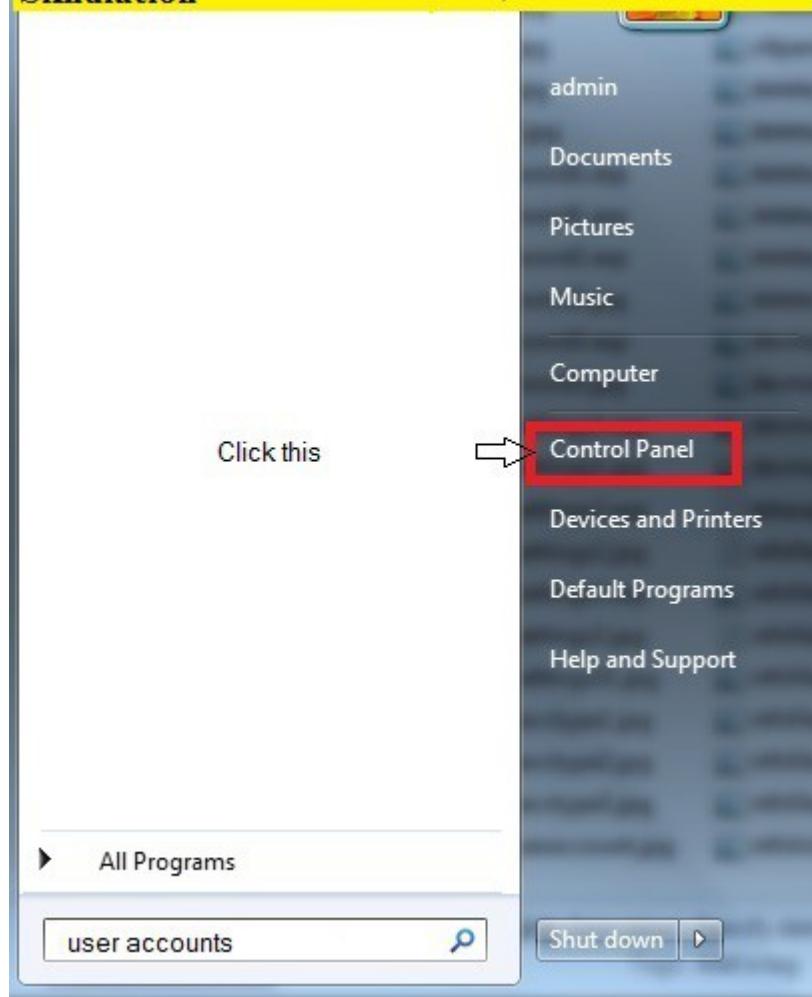
9.25.1 Setting Account lockout policy

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.

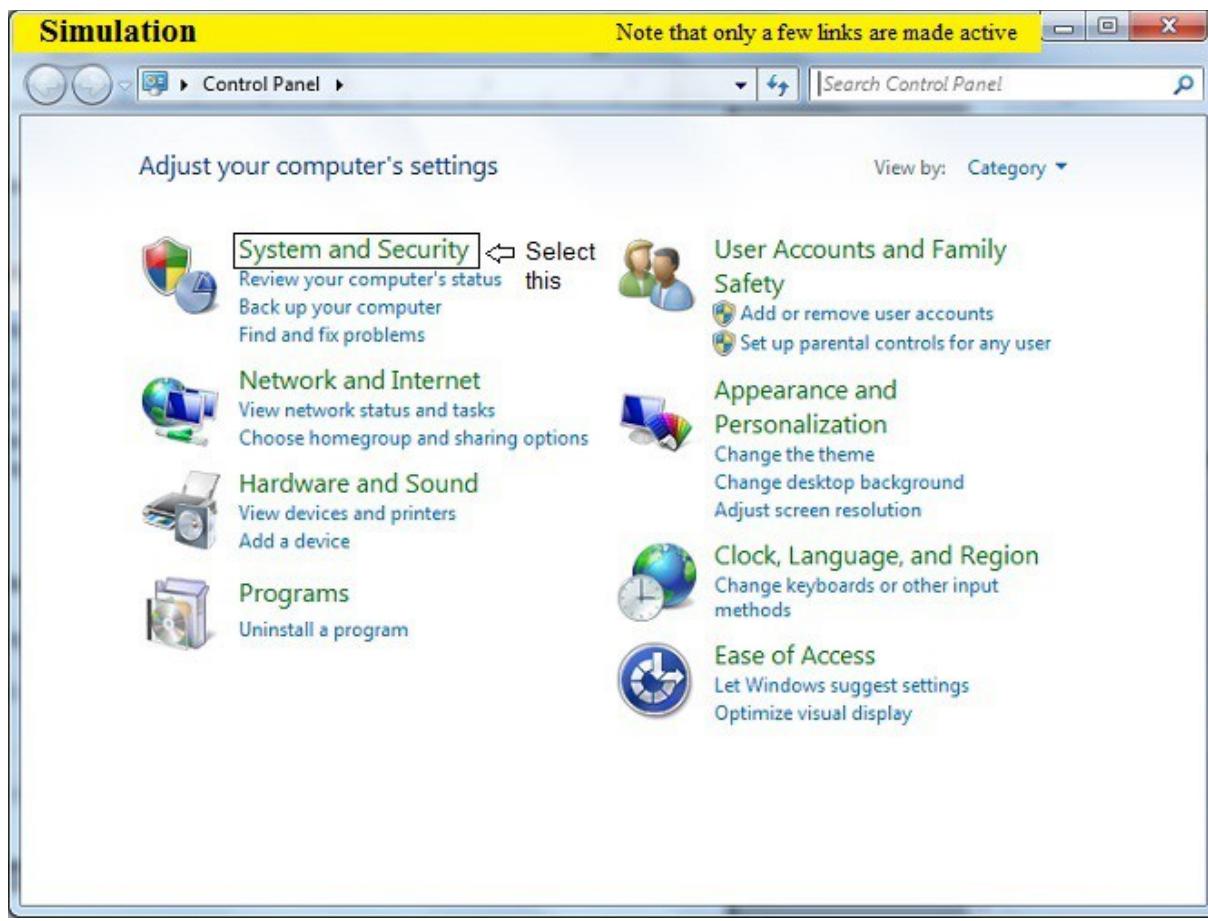
Simulation

Note that only a few links are made active

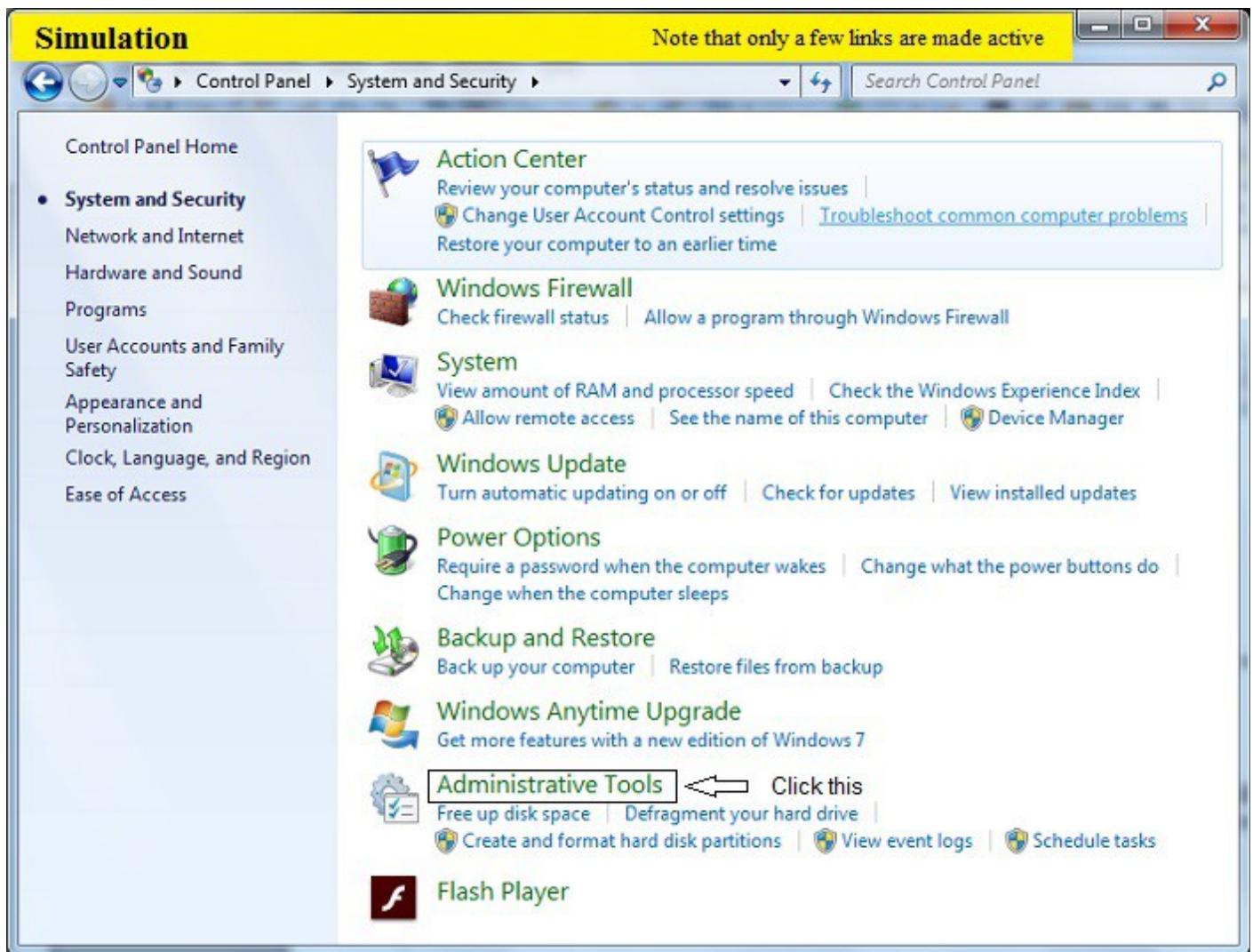


Go to step 2 if control panel is clicked otherwise go to step 5

2. In control panel window click System and Security .



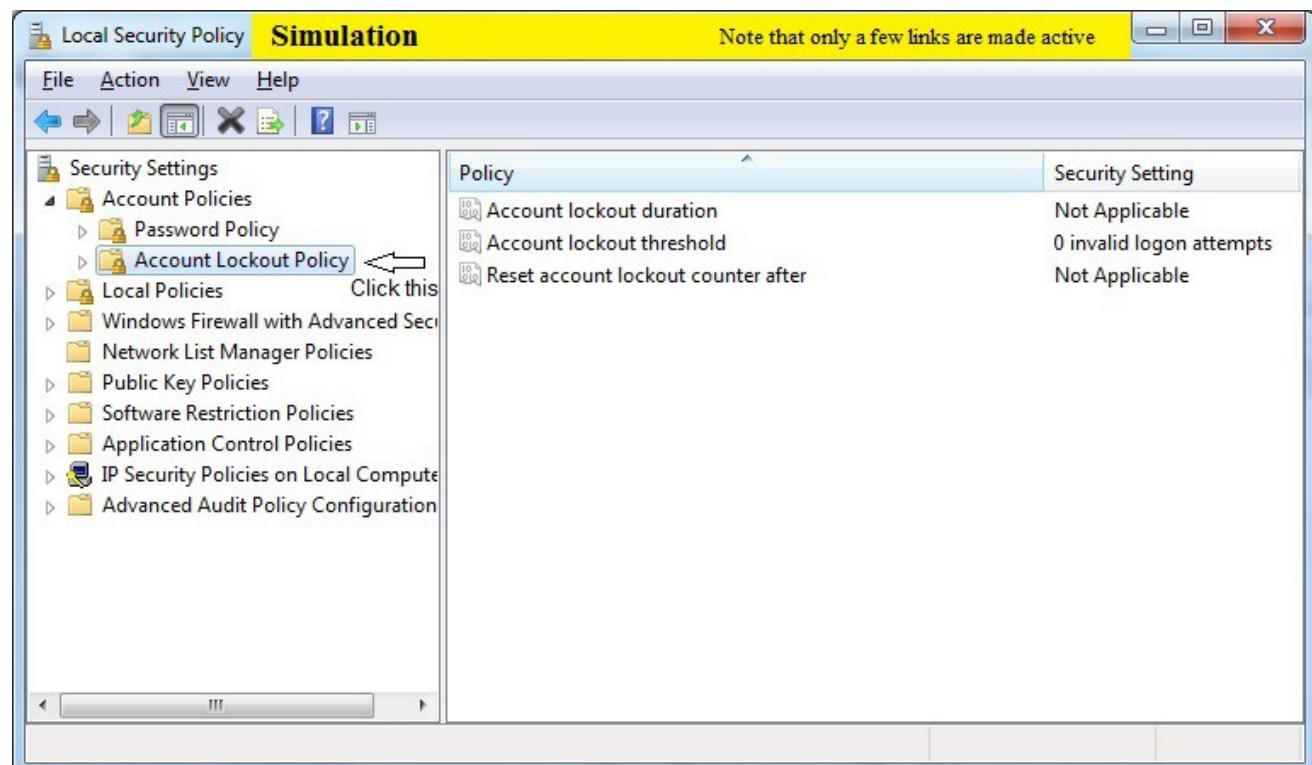
3. In System Security window click Administrative Tools



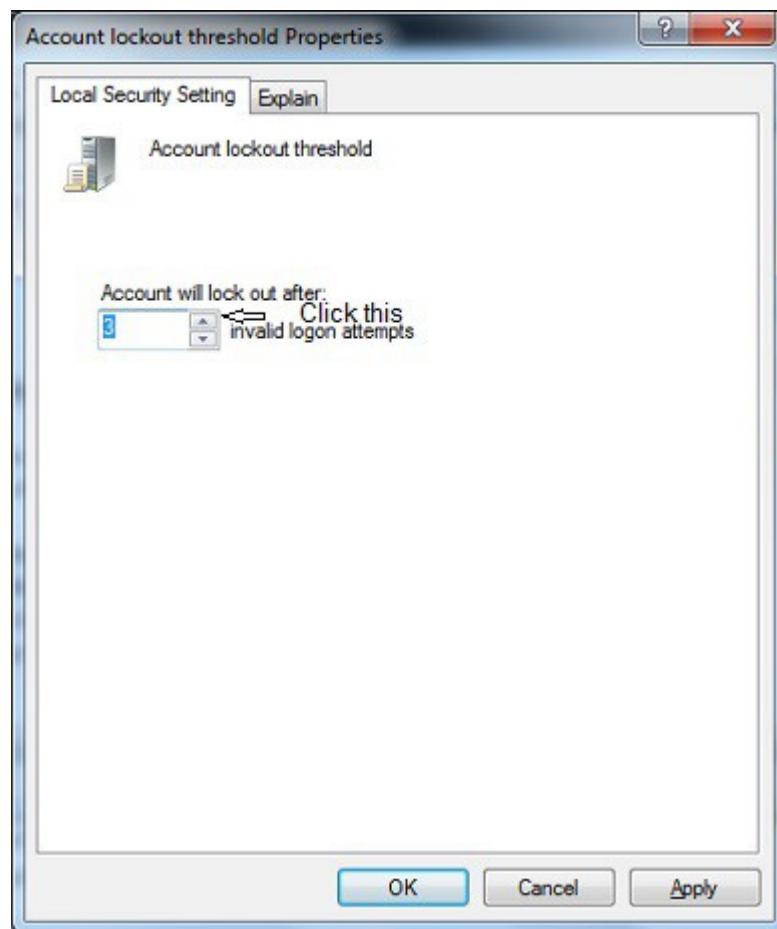
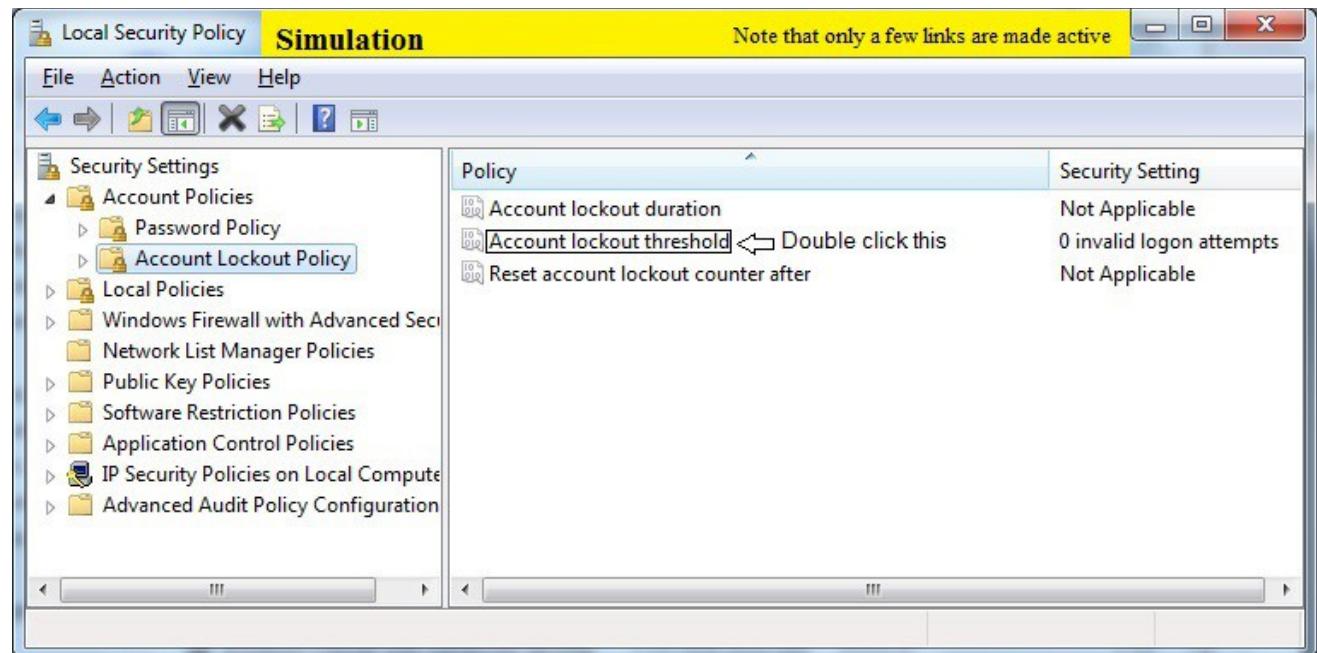
4. In Administrative Tools window double click Local Security Policy



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 be configured to respond to this type of potential attack by disabling the account for a preset period of time. Account lockout policy setting controls 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 allows 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.

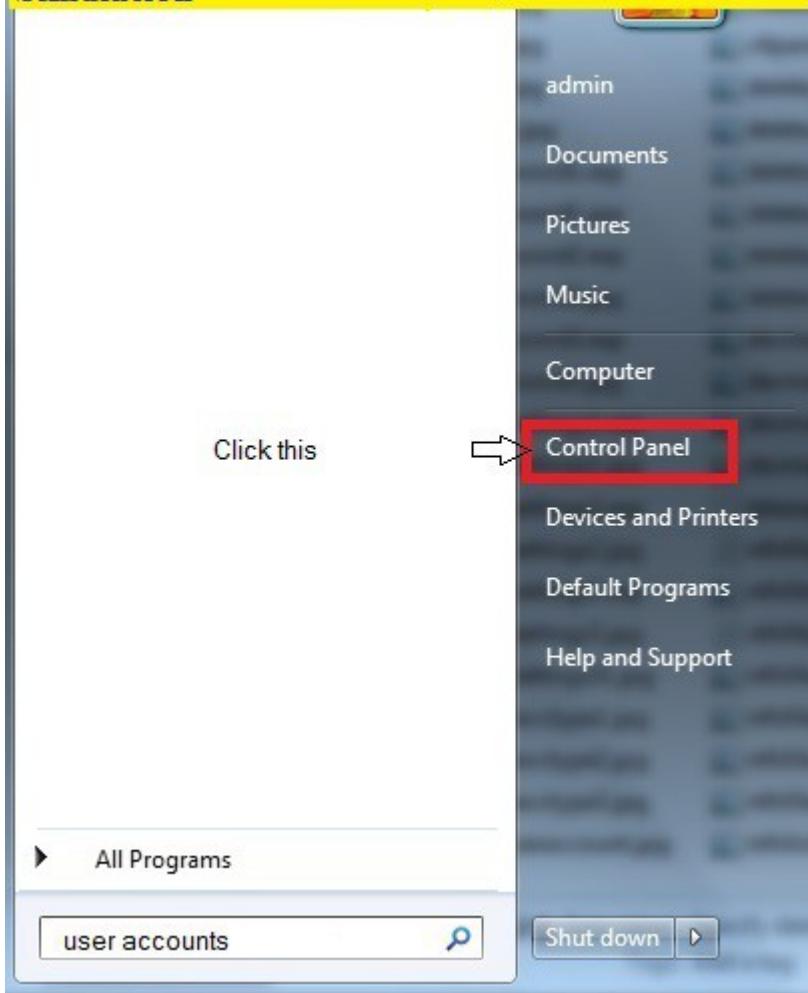
9.25.2 Setting Password policy

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

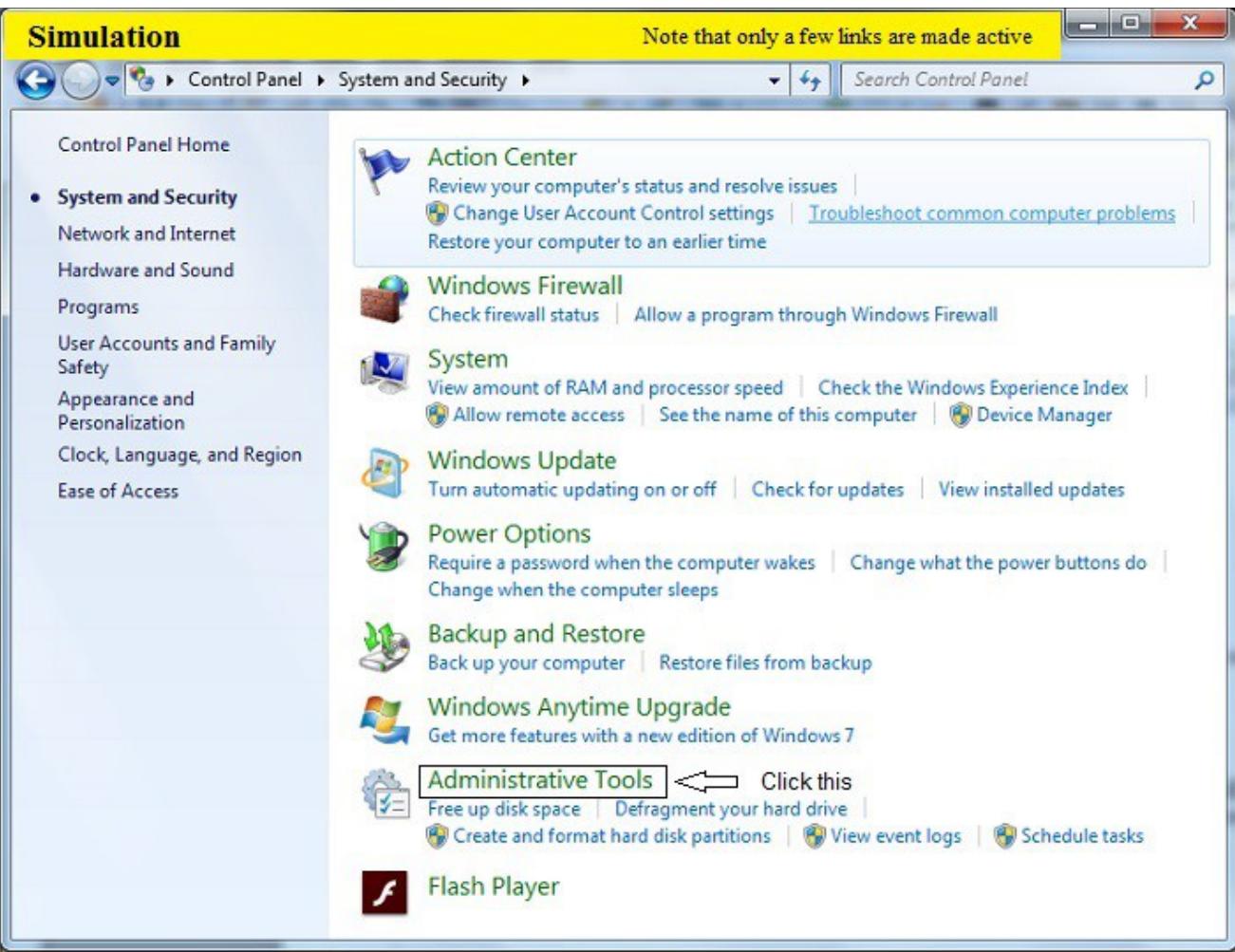


Go to step 2 if control panel is clicked otherwise go to step 5

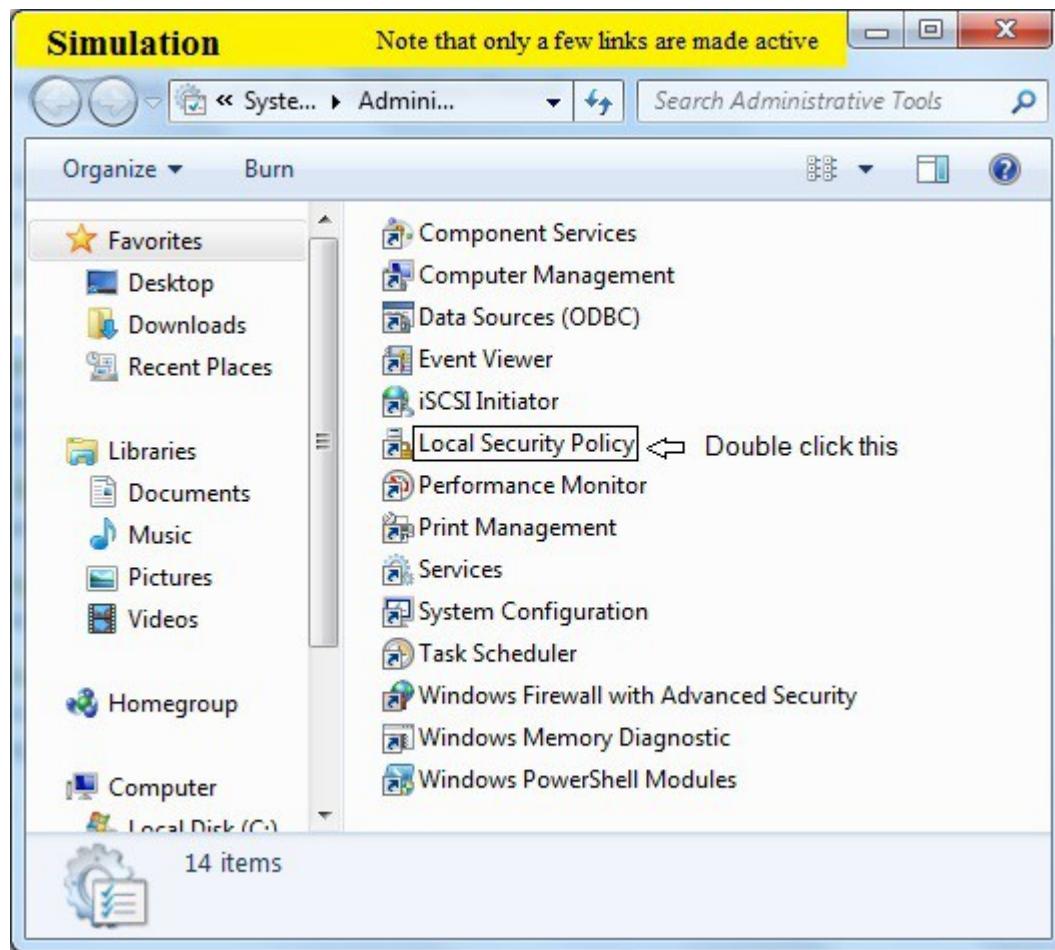
2. In control panel window click System and Security



3. In System Security window click Administrative Tools



4. In Administrative Tools window double click Local Security Policy

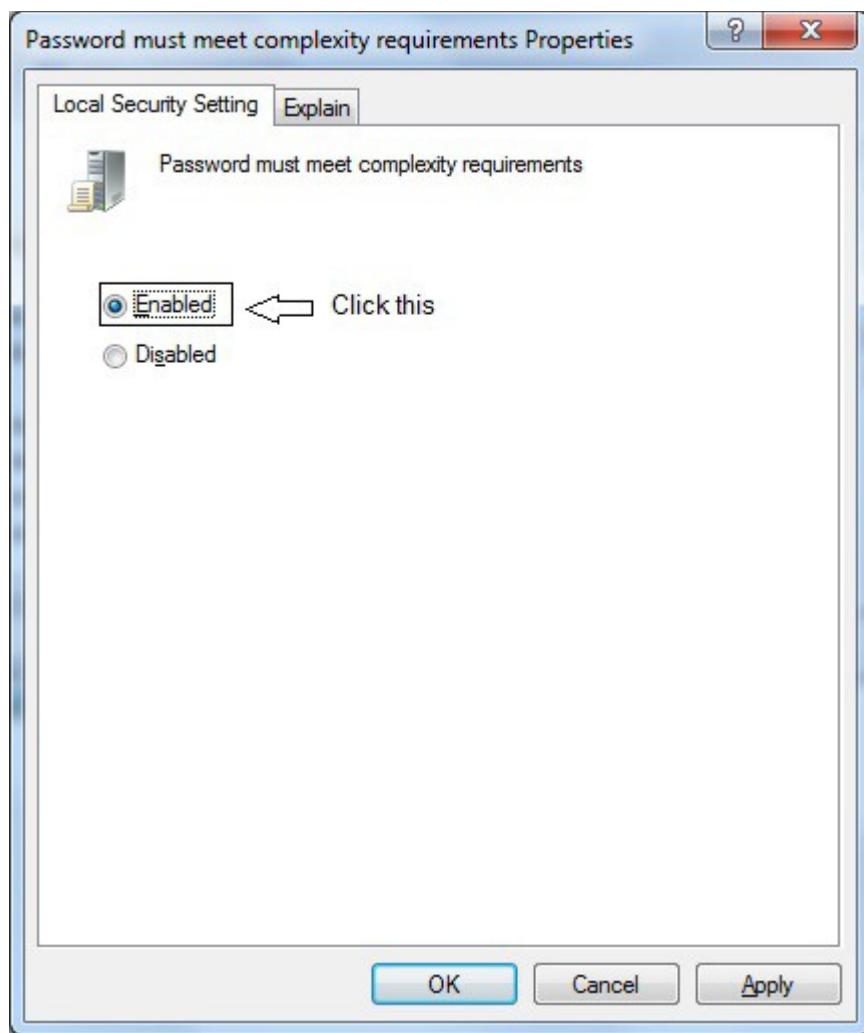
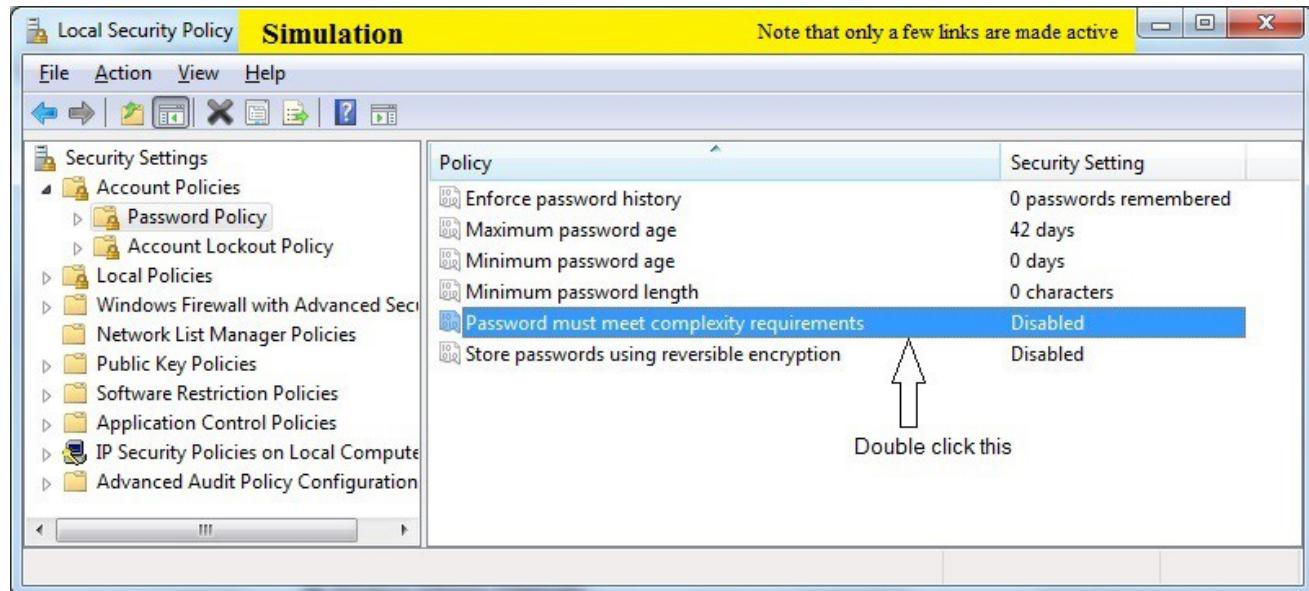


5. Under Account Policies click on Password Policy you will see six policies in the right pane. Double Click “Password must meet complexity requirements”

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

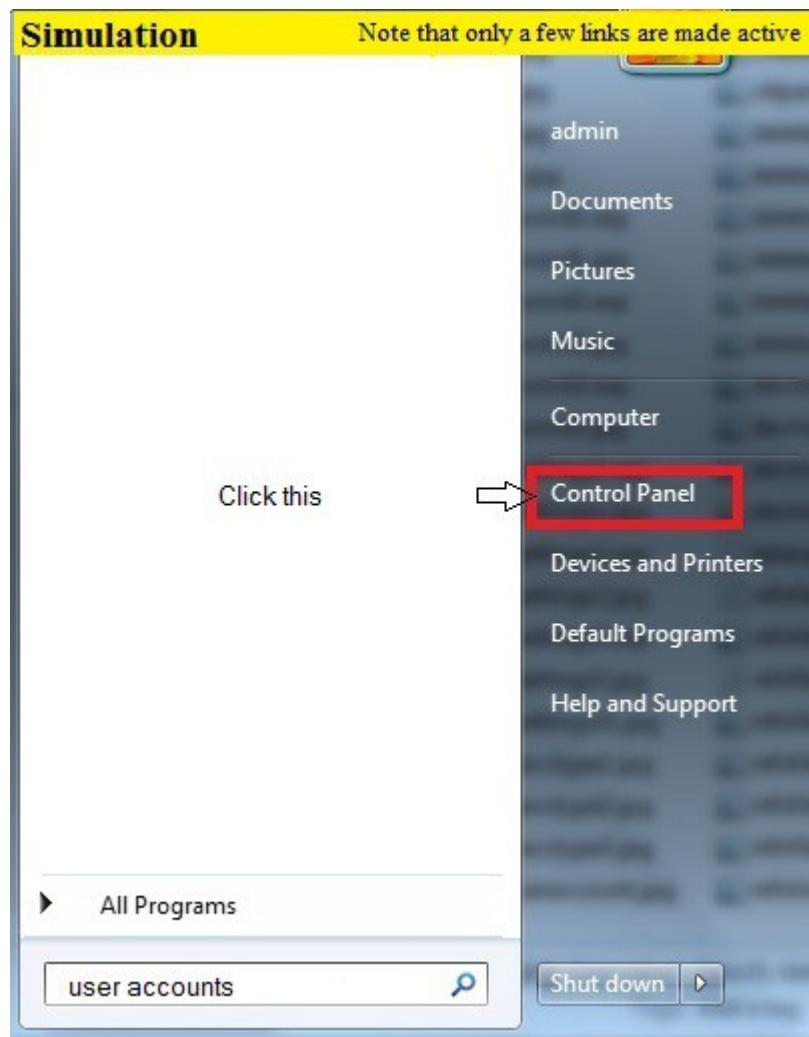
passwords are changed or created.

[Back](#)

9.26 Configuring hardware settings using Device Manager

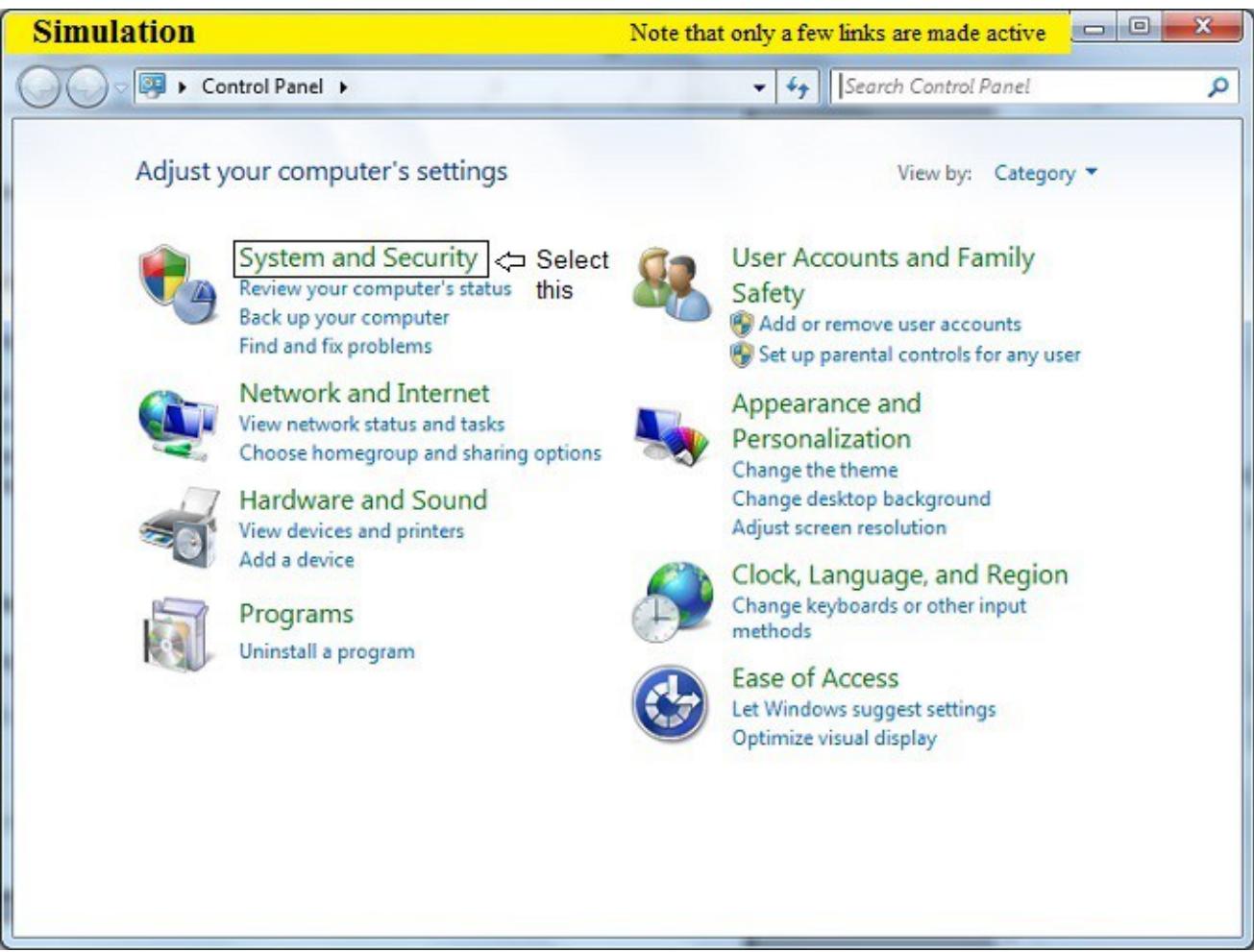
Description: This lab exercise helps to change the hardware settings using device manager

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

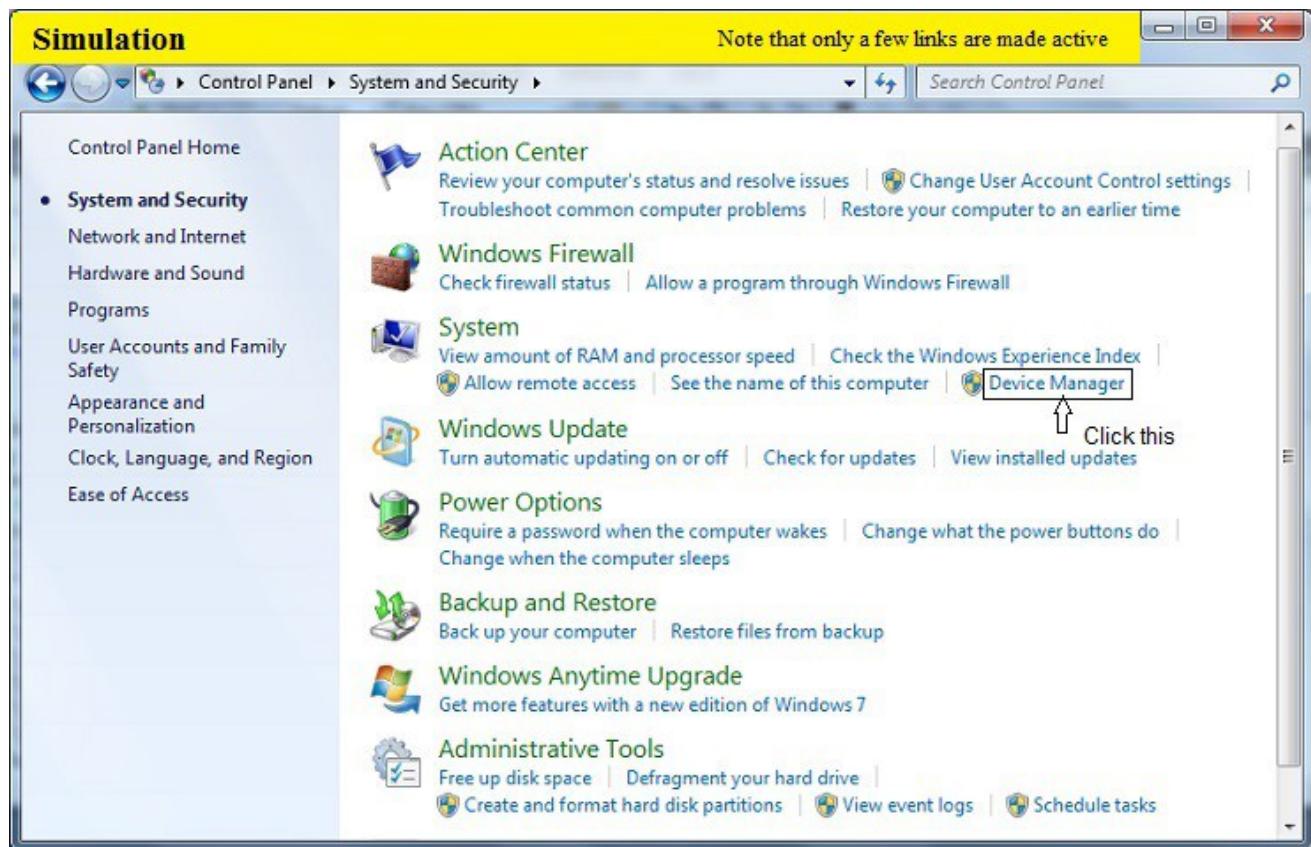


Go to step 2 if control panel is clicked other wise go to step 4

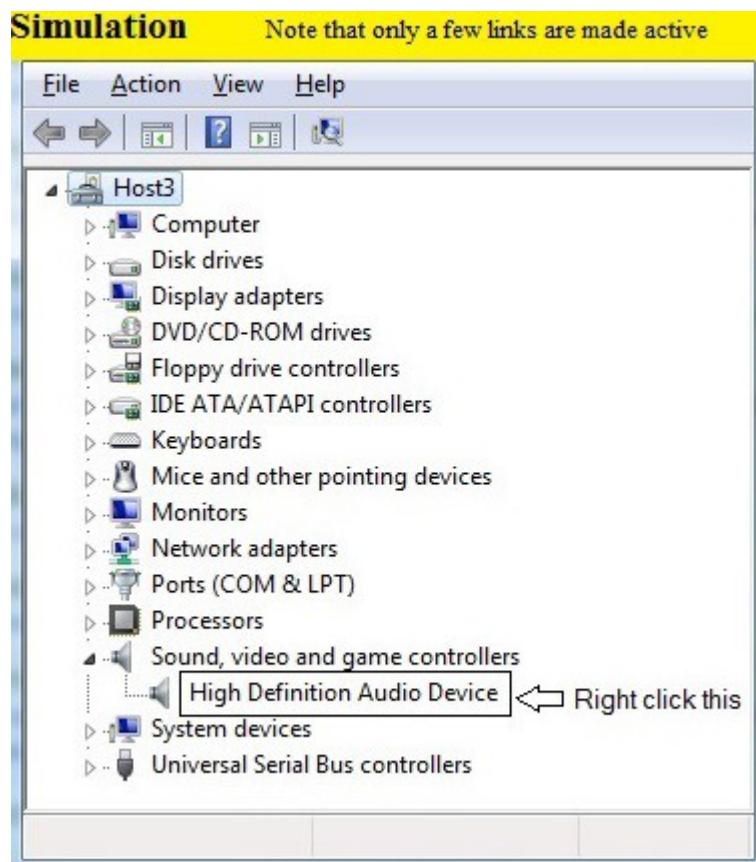
2. In control panel window click System and security.



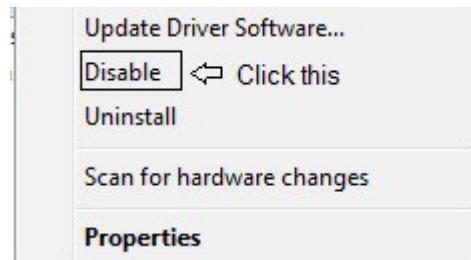
3. In System Security window click Device Manager



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:

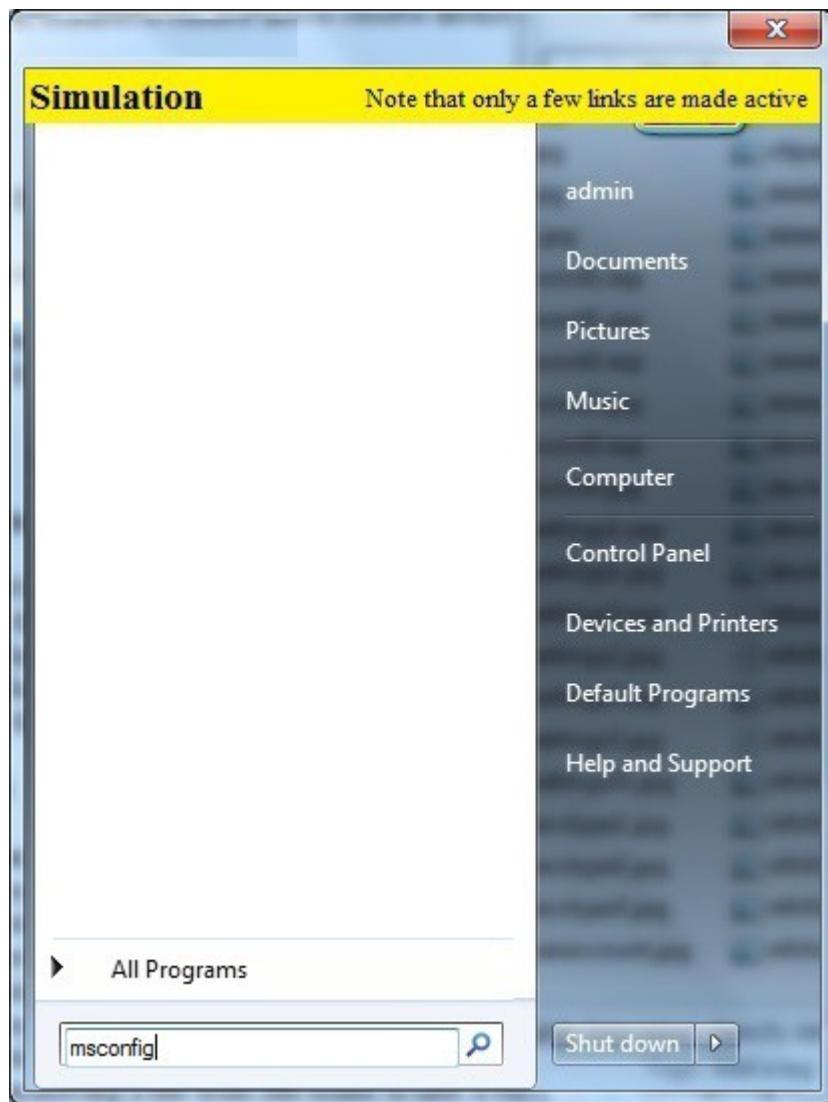
1. Determine whether the hardware on your computer is working properly.
2. Change hardware configuration settings.
3. Identify the device drivers that are loaded for each device, and obtain information about each device driver.
4. Change advanced settings and properties for devices. Install updated device 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](#)

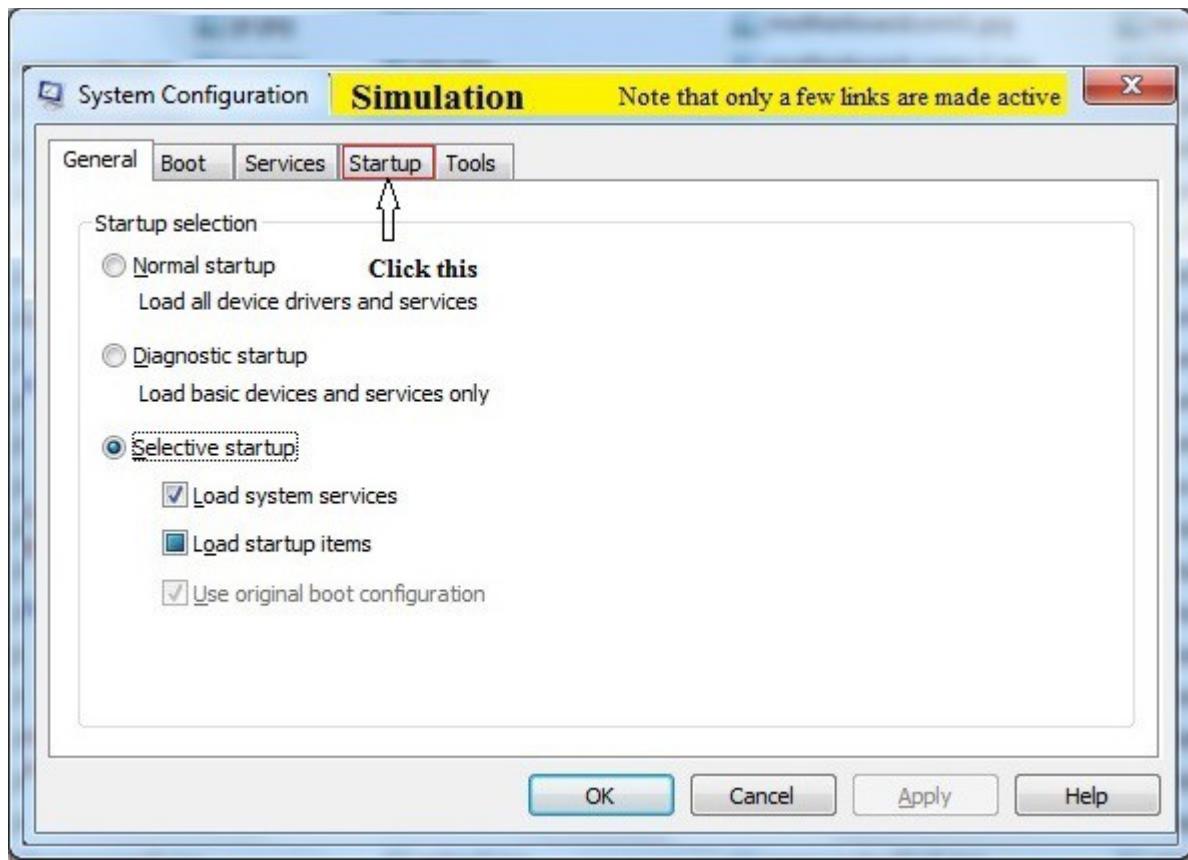
9.27 Disabling Startup Programs in Windows 7

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

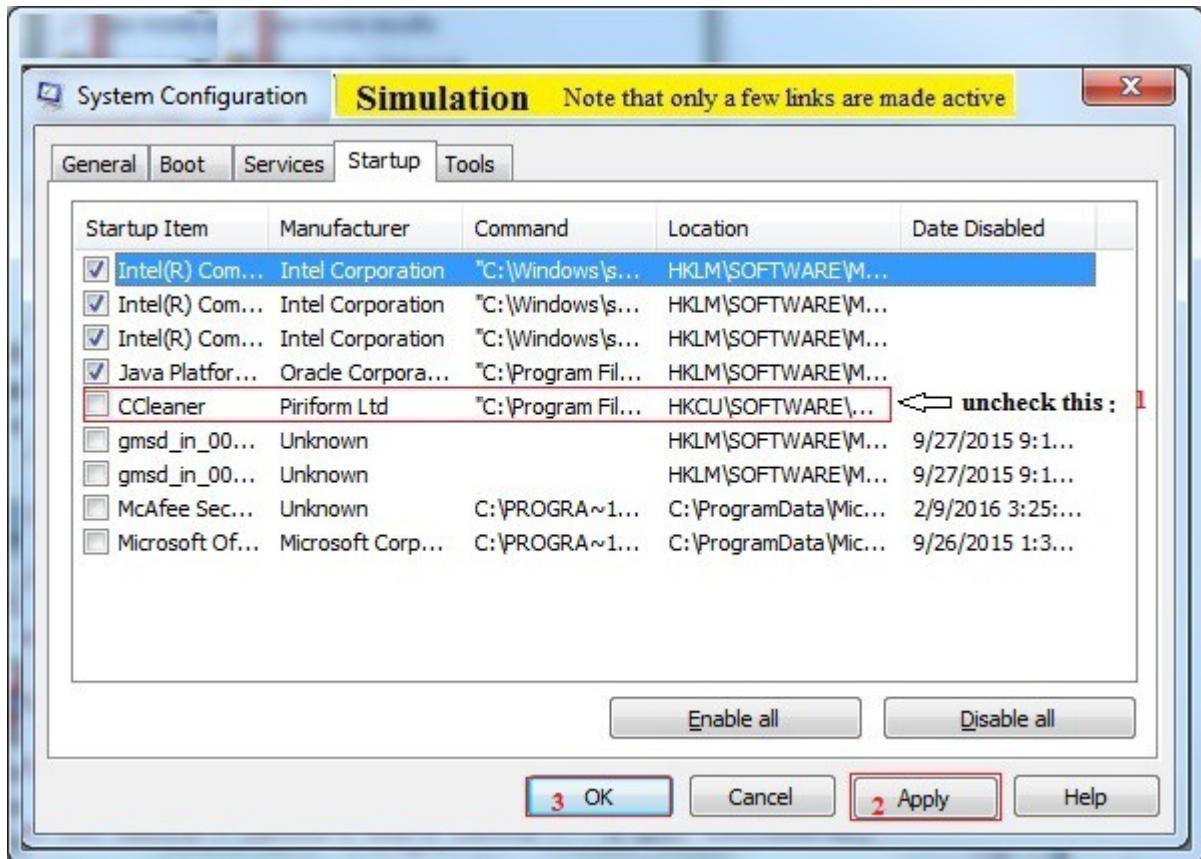
Instructions: 1. On loading a lab exercise, in a given simulation start menu type “ msconfig ” in search box.

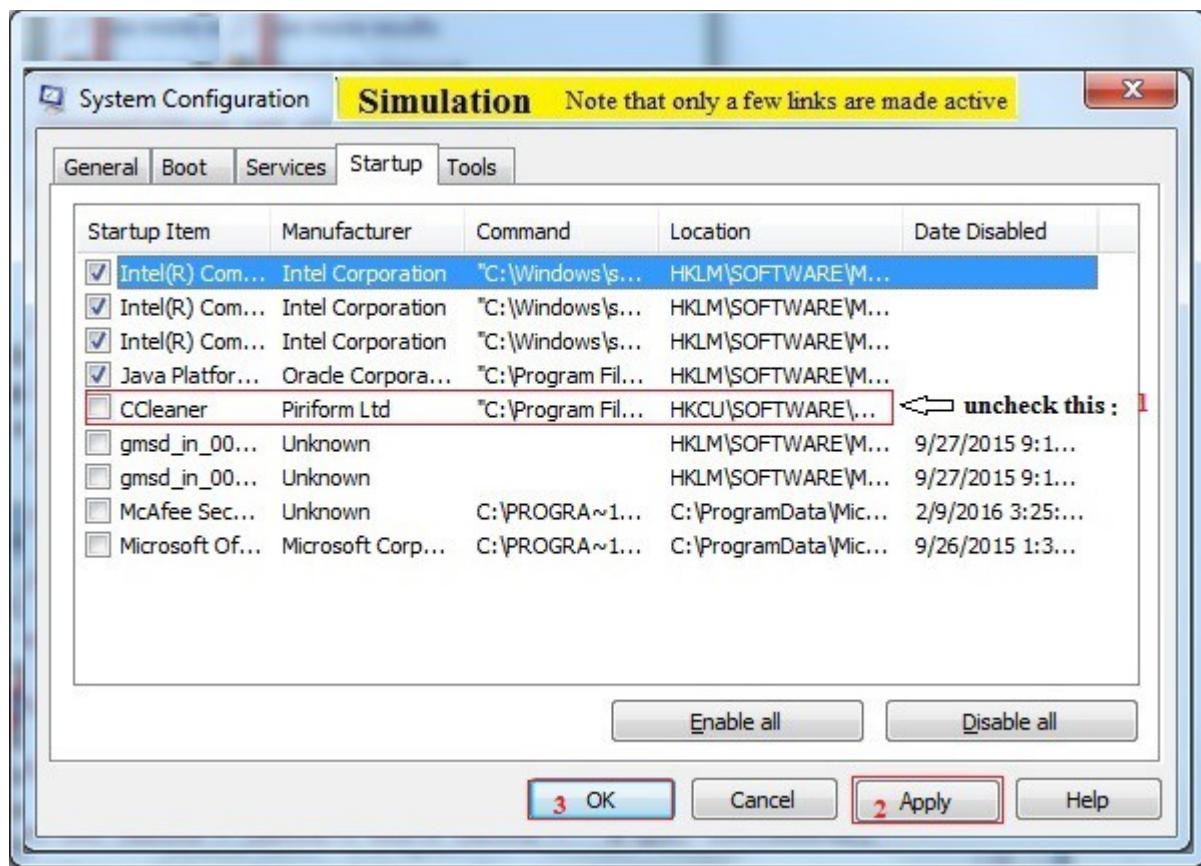


2. From within the System Configuration tool, *Click Startup tab*.



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.

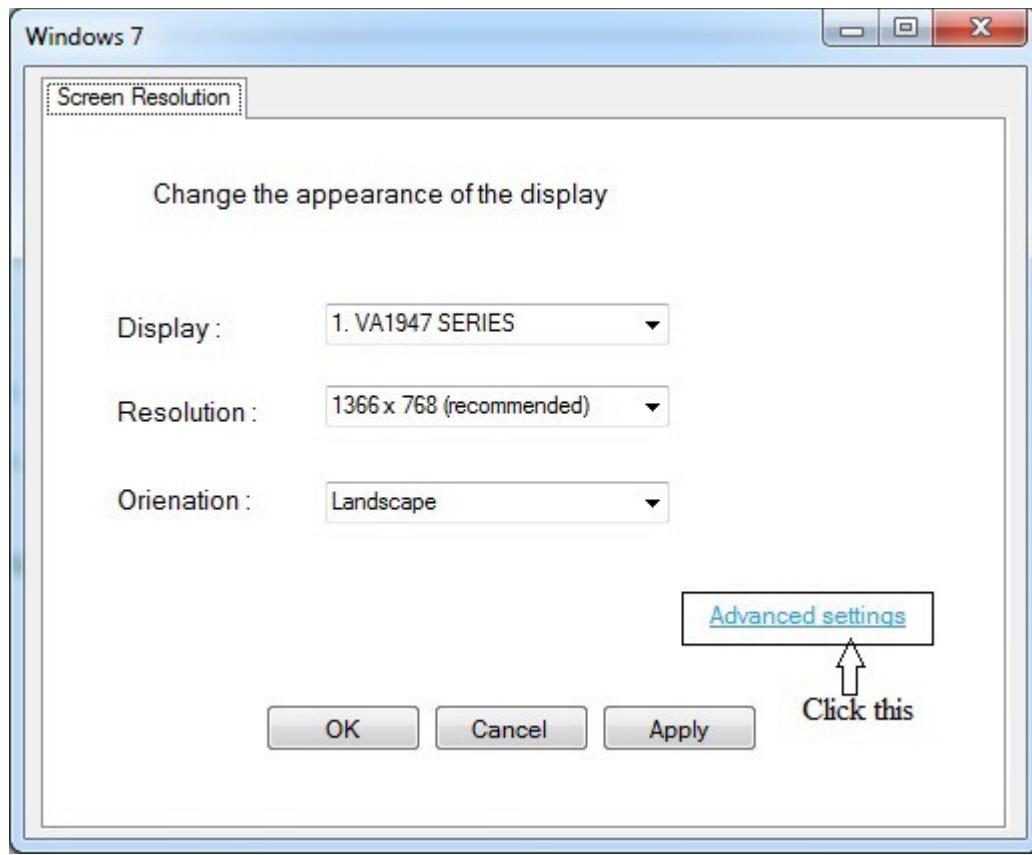
Explanation: Startup programs are programs which run when your computer starts / boots up. Startup programs can be antivirus programs, chat/messaging apps or background apps that can also continuously keep running on your computer. Start up programs impact computer boot time, and may make your computer 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**](#)

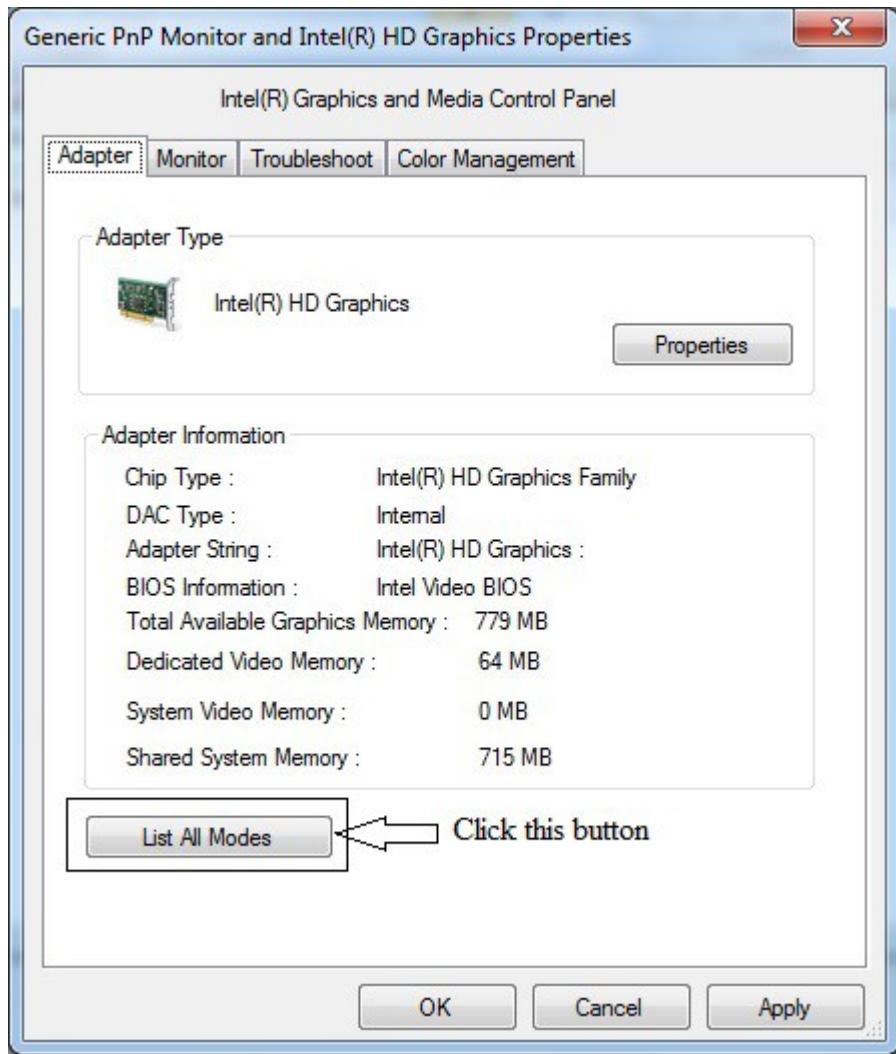
9.28 Changing the refresh rate in Windows 7.

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

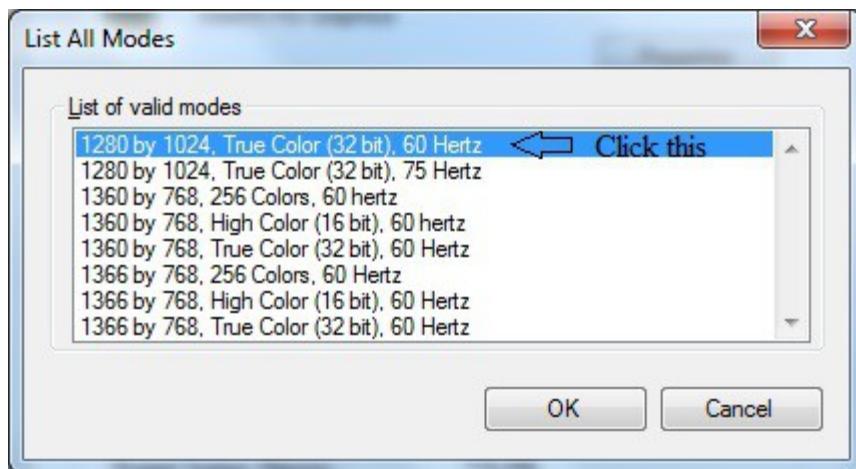
Instructions: 1. On loading a lab exercise, in a given simulator window click on the Advanced settings link.



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.



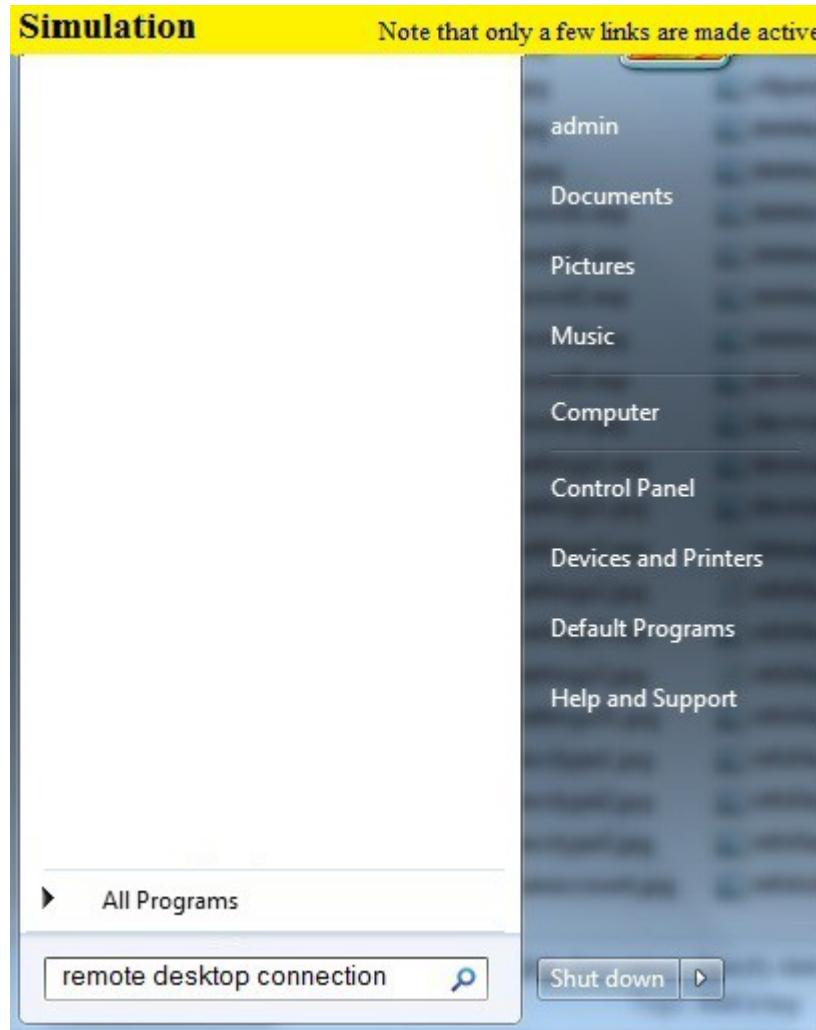
3. Click Apply and then OK button in Adapter tab window and also click apply and OK button in windows 7 window.

[Back](#)

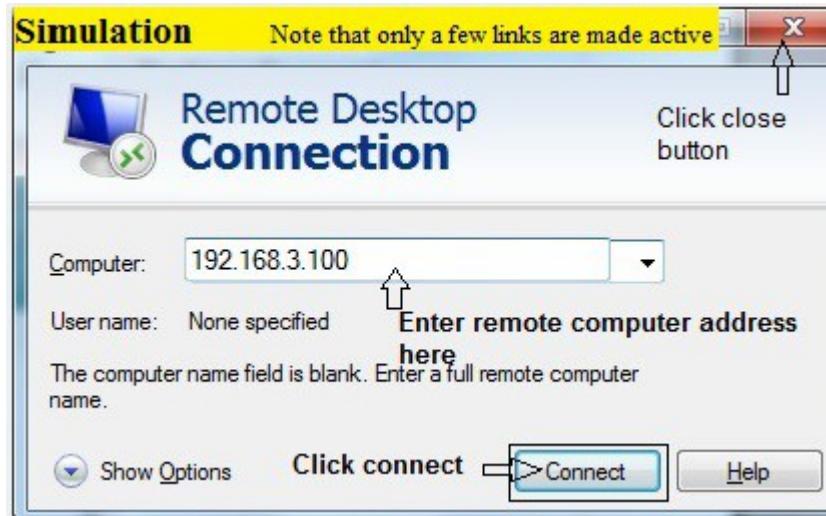
9.29 Connecting to a remote desktop using windows 7

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**](#)