**EXP1: various hard ware components on motherboard**

### 1. CPU (Central Processing Unit) chip:

CPU is the electronic circuitry in a computer that executes instructions that make up a program. It is also known as a central processor or the main processor. The CPU executes the basic logic, arithmetic, controlling as well as input/output (I/O) operations specified by the instructions in the desktop programs.

### 2. RAM (Random Access Memory) slots:

RAM is a kind of computer memory that can be read and written. It is mainly used to save data and machine code. A RAM device permits data to be read or written in nearly the same amount of time no matter where the data’s physical location is in the memory. Compared to the direct-access storage devices like hard drives, CD/DVD and magnetic tapes, RAM media is much faster for data reading and writing.

### 3. Southbridge/northbridge:

They are the two chips in the core logic chipset on the motherboard. Typically, the southbridge implements the slower capabilities of the motherboard in a northbridge/southbridge chipset computer architecture.

The northbridge, also known as host bridge or Memory Controller Hub, is connected directly to the CPU via the front-side bus (FSB). It is responsible for tasks requiring the highest performance. Together with the south bridge, they manage communications between the CPU and other **motherboard components**.

### 4. BIOS (Basic Input/Output System):

BIOS, also called system BIOS, PC BIOS or ROM BIOS, is firmware that is used to perform hardware initialization during the booting process; and to provide runtime services for operating system and programs. The BIOS firmware is the first software to run when powered on; it is re-installed on a PC’s system board.

### 5. I/O port:

Input/output ports are the connections between the CPU and peripheral devices on a motherboard. There are two complementary methods to perform input and output processes: memory-mapped I/O (MMIO) and port-mapped I/O (PMIO). Alternatively, you can use dedicated I/O processors, called channels on mainframe computers, which execute their own instructions.

### 6. USB (Universal Serial Bus):

USB is an industry standard that creates specifications for connectors, cables and protocols for connection; power supply (interfacing) and communication among computers, computer peripherals as well as other desktops. There are a great many USB hardware including several different connectors, of which USB-C is the latest kind.

### 7. CPU slot:

A CPU slot, also called a CPU socket or Processor socket, contains one or more mechanical components that provide mechanical and electrical connections between the PCB and a microprocessor (CPU). Therefore, you can install a CPU on a motherboard without soldering.

### 8. PCI (Peripheral Component Interconnect) slot:

Peripheral Component Interconnect is a local computer bus for connecting hardware to a computer. It supports all the functions of a processor bus. PCI is usually been called Conventional PCI to distinguish it from its successor PCI Express (PCIe, PCI-e or PCI-E).

PCI Express is a high-speed serial computer expansion bus standard designed to replace the older PCI, PCI-X and AGP bus standard. It is a general-use motherboard interface for the graphics card, SSDs, hard drives, Wi-Fi as well as Ethernet hardware connections.

### 9. AGP (Accelerated Graphics Port) slot:

AGP was designed as a high-speed point-to-point channel for connecting a video card (graphics card) to a computer system. Primarily, it was used to assist in the acceleration of 3D computer graphics. AGP is originally designed to be a descendant of the PCI series of connections for video cards. Yet, it was replaced by the PCIe slots.

### 10. ISA (Industry Standard Architecture) slot:

ISA is the 16-bit internal bus of IMB PC/AT and similar computers that are based on Intel 80286 and its immediate successors during the 1980s. It was backward compatible with the 8-bit bus of the 8088-based IBM PC largely.

There once was an attempt to extend ISA into a 32-bit bus, called Extended Industry Standard Architecture (EISA). The attempt wasn’t very successful and the EISA was largely replaced by the later VESA Local Bus and the PCI bus.

### 11. Parallel port:

A parallel port is a kind of interface for attaching peripherals on desktops. The name of this kind of port is derived from the way the data is sent. That is, the parallel ports send multiple bits of data at the same time. Serial interfaces, on the contrary, send bits one data at once. To achieve parallel data transfer, there are multiple data lines in the parallel port cables. The parallel port cable is larger than the cable of a contemporary serial port, which only has one data line within.

### 12. FDC (Floppy-Disk Controller):

FDC is a special-purpose chip and associated disk controller circuitry. It controls and directs reading from and writing to a computer’s [floppy disk drive](https://www.minitool.com/lib/floppy-disk.html) (FDD).

### 13. IDE (Integrated Drive Electronics) controller:

The devices used for connecting IDE, Ethernet, [FireWire](https://www.minitool.com/lib/firewire.html), USB and other systems can be called host adapter. So, the IDE controller refers to the host adapter. A host adapter, also called a host controller or a host bus adapter (HBA), connects a computer (acting as the host system) to other network and storage devices.

### 14. CMOS (Complementary Metal-oxide-semiconductor) battery:

CMOS battery, also called memory battery, clock battery or real-time clock (RTC), is generally a CR2032 lithium coin cell. The lifespan of the CMOS battery is estimated to be three years when the power supply unit (PSU) is unplugged or switch off.

### 15. Power supply connector:

A power supply provides the necessary electrical power to let the computer to work. It takes standard 110-Volt AC (Alternative Current) power to DC (Direct Current) power of 12 Volt, 5 Volt, 3.3 Volt, etc.

### 16. Mouse and keyboard ports:

All computers have a keyboard port connected directly to the motherboard. There are two types of connectors. The oldest one is a special DIN (Deutsches Institut für Normung) connector while the newest one is the mini DIN PS/2-style connector. Many PCs use the PS/2-style connectors for both keyboard and mouse; and the connectors are marked clearly for different usage.

### 17. DIP (Dual In-line Package) switch:

A DIP switch is a manual electric switch packaged with others in a standard dual in-line package. The term may refer to an individual switch or the whole unit. The DIP switch is designed to be used on a printed circuit board (motherboard) together with other electronic **motherboard components**. It is usually used to customize the behavior of an electronic device for specific situations.

### 18. Jumper:

A jumper is a short length of conductor that is used to close, open or bypass part of an electronic circuit. Typically, jumpers are used to set up or configure printed circuit boards like the motherboard.

### 19. Heat sink/heatsink (cooling system):

A heat sink is a passive heat exchanger that transfers the heat generated by **parts of motherboard** into a fluid medium like liquid or air. The fluid medium will dissipate away from the device. Thus, the temperature of the device is kept within a tolerable range. On the motherboard, the heatsink is usually used to cool CPU, GPU (graphics processing unit), chipsets and RAM modules.

### 20. Clock generator:

A clock generator is an electronic oscillator (circuit) that produces a clock signal for usage in synchronizing a circuit’s operation. The clock signal ranges between high and low frequencies, thus creating a metronome for the coordination of actions.

1. **Integrated Circuits (IC):** IC is also very important component of motherboard. [Integrated circuit](https://www.geeksforgeeks.org/types-of-integrated-circuits/) is used for data processing and storage.
2. **Power Connector:** The purpose of the power connector is to give power to the motherboard.
3. **Capacitor:** Two conducting plates and a thin insulator are placed together to form a capacitor. These components are contained in a plastic bag.
4. **Inductor (Coil):** A conducting wire is wrapped around an iron core to create an electromagnetic coil known as an inductor. It stores magnetic energy by functioning as an electromagnet or inductor.

**EXP2: using various options of cmos setup**

The CMOS (Complementary Metal-Oxide-Semiconductor) setup, often accessed via the BIOS or UEFI firmware interface, allows users to configure system hardware settings. These options vary by motherboard manufacturer, but here’s an overview of the most common categories and their purposes:

### ****1. Boot Configuration****

* **Boot Device Priority**: Choose the order in which devices (e.g., SSD, HDD, USB ) are checked for bootable media.
* **Fast Boot**: Enable/disable fast boot to speed up system startup.
* **UEFI/Legacy Boot Mode**: Select between UEFI or Legacy BIOS compatibility.
* **Secure Boot**: Secure the boot process against unauthorized software.

### ****2. Date and Time Settings****

* Set the system's current date and time, maintained by the CMOS battery.

### ****3. Advanced CPU Configuration****

* Enable/disable processor features:
  + **Hyper-Threading**
  + **Virtualization (VT-x, AMD-V)** for virtual machines.
  + **Overclocking Options**: Adjust CPU multiplier and voltage.
  + **Power Management**: Configure features like Intel SpeedStep or AMD Cool’n’Quiet.

### ****4. Memory (RAM) Configuration****

* **XMP Profiles**: Load pre-configured profiles for optimal RAM performance.
* **Memory Frequency and Voltage**: Manually adjust RAM settings.
* **Memory Channel Configuration**: Configure single, dual, or quad-channel setups.

### ****5. Storage Configuration****

* **AHCI/RAID Mode**: Set SATA controllers for AHCI (standard) or RAID (multi-drive setups).
* Configure NVMe settings for SSDs.
* View detailed information about connected storage devices.

### ****6. Integrated Peripherals****

* Enable/disable onboard devices:
  + USB Controllers
  + Audio Chipsets
  + Ethernet/Wi-Fi Adapters
  + SATA or NVMe controllers.
* Configure settings for specific ports (e.g., legacy USB support).

### ****7. Fan and Temperature Settings****

* Adjust fan speeds using **PWM profiles** or set custom curves.
* Monitor system temperatures for the CPU, GPU, and motherboard.
* Configure thermal shutdown thresholds.

### ****8. Power Management****

* Configure how the system behaves during power events:
  + **Restore on AC Power Loss**: Determines if the system restarts automatically after a power outage.
  + **Wake-on-LAN**: Allow the system to be powered on via network commands.
  + **Sleep Mode**: Adjust power-saving settings (S1, S3, S4, or S5 states).

### ****9. Security Settings****

* **Password Protection**:
  + Set a password to access the BIOS/UEFI or boot the system.
* **Drive Encryption**: Configure security keys for encrypted drives.
* **TPM (Trusted Platform Module)**: Manage cryptographic hardware for secure operations.
* Enable/disable **Secure Boot** to prevent unauthorized software from loading.

### ****10. Overclocking Options****

* Adjust settings for:
  + CPU clock speed, multiplier, and voltage.
  + GPU overclocking (if supported by the motherboard).
  + Memory timing and frequency.

### ****11. Diagnostic Tools****

* **Event Logs**: View hardware-related errors or power event logs.
* **Health Monitoring**: Check real-time system voltages, temperatures, and fan speeds.
* **POST (Power-On Self-Test)**: Enable/disable verbose boot logs.

### ****12. Exit Options****

* **Save Changes and Exit**: Save the current configuration and reboot.
* **Discard Changes**: Exit without saving.
* **Load Optimized Defaults**: Restore factory default settings.

### ****How to Access CMOS Setup****

1. Restart your computer.
2. Press the designated key during startup (common keys are **F2**, **DEL**, **F10**, or **ESC** depending on the motherboard manufacturer).
3. Navigate through menus using keyboard arrow keys or a mouse (in UEFI).

**Tips:**

* Be cautious while changing settings, especially in advanced sections like overclocking.
* Document or back up settings before making significant changes.

**EXP 3: Print the summary of your system Hardware and verify for correctness.**

To print the summary of your new system hardware and verify its correctness, you can use several methods depending on your operating system. Below are the steps for both Windows and Linux-based systems:

**Windows:**

System Information (GUI):

Press Win + R, type msinfo32, and press Enter.

This opens the System Information tool, where you can see detailed information about your system's hardware, including processor, memory, storage, and more.

Using Command Prompt (CLI):

Open the Command Prompt by pressing Win + R, typing cmd, and pressing Enter.

Run the following command to print a summary of your hardware:

System info

This command provides information such as OS version, memory, network adapter, and more.

Using PowerShell:

Open PowerShell (search for it in the Start menu).

Run the following command to get a summary of hardware:

Get-ComputerInfo

**Device Manager (GUI):**

Press Win + X and select **Device Manager**.

* This shows a tree view of your system’s components like processors, display adapters, disk drives, etc.

**Linux (Ubuntu/Debian-based):**

**Using lshw Command:**

Open the terminal.

Run the following command to display detailed hardware information:

sudo lshw

This will give a detailed list of your hardware components. You may need to install

lshw if it is not already installed:

sudo apt install lshw

**Using inxi (if installed):**

Run this command in the terminal:

inxi -F

It gives a summary of your hardware, including CPU, GPU, RAM, and storage.

**Using free and df for memory and disk:**

For memory usage:

free -h

For disk usage:

df -h

**Using neofetch (if installed):**

Neofetch provides a simple system summary with a nice graphical display.

Neofetch

**Verify Hardware Correctness:**

* **Cross-check system specs:** Compare the displayed information against the specifications provided by the manufacturer or documentation of your hardware. Ensure that the CPU, RAM, disk size, and GPU (if applicable) match what is expected.
* **Run hardware diagnostics:** Many systems offer diagnostic tools to test hardware performance (e.g., Windows Memory Diagnostic, memtest86, etc.).
* **Check BIOS/UEFI settings:** Verify that hardware is recognized correctly at the BIOS/UEFI level to ensure it's working as expected.

These steps should allow you to print and verify your system hardware summary across different platforms.

**EXP 4: Hard drive, optical drive installation.**

**Hard drive:**

Installing a hard drive in your system involves physical installation and software setup.

### ****Tools You Need:****

1. A screwdriver (usually Phillips-head).
2. Anti-static wrist strap (optional but recommended).
3. SATA cable (for internal drives, if not pre-installed).

**Steps to Install a Hard Drive:**

1. Power Down and Unplug the System

Shut down your computer completely.

Unplug the power cable and all peripherals (keyboard, mouse, etc.).

2. Open the Computer Case

Use a screwdriver to remove the side panel of the case.

Touch a metal surface to ground yourself or wear an anti-static wrist strap to prevent static electricity damage.

3. Locate the Hard Drive Bay

Identify the drive bay for your hard drive. Modern cases may have:

3.5-inch bays for standard hard drives.

2.5-inch bays for smaller drives (e.g., SSDs).

Some cases use screws, while others have tool-less brackets or trays.

4. Install the Hard Drive

For 3.5-inch HDD:

Slide the hard drive into the 3.5-inch bay. Align the screw holes on the drive with the bay.

Secure it with screws or use the case's tool-less mechanism.

For 2.5-inch SSD/HDD:

If your case doesn’t have a dedicated 2.5-inch bay, you might need a 2.5-inch-to-3.5-inch adapter.

Mount the drive and secure it with screws.

5. Connect the Drive

SATA Drives:

Plug one end of the SATA cable into the hard drive.

Connect the other end to a SATA port on the motherboard.

Attach a SATA power connector from the power supply to the drive.

NVMe SSD (M.2 Drives):

Locate the M.2 slot on your motherboard.

Insert the NVMe drive at an angle, then press it down and secure it with a screw.

6. Verify Connections

Ensure all connections are snug and secure:

SATA data cable (for standard drives).

SATA power cable (for standard drives).

Proper alignment in the M.2 slot (for NVMe drives).

7. Close the Case and Power Up

Reattach the side panel of the case.

Plug in the power cable and other peripherals.

Power on the system.

**Software Setup:**

Once the hardware is installed:

**For Windows:**

**Initialize the Drive:**

Open Disk Management:

Press Win + X and select Disk Management.

The new drive should appear as "Unallocated."

Right-click the unallocated space and select Initialize Disk.

Choose either MBR or GPT partition style (GPT is recommended for modern systems).

**Create a Partition and Format:**

Right-click the unallocated space and select New Simple Volume.

Follow the wizard to assign a drive letter and format the drive (choose NTFS for most use cases).

**Linux:**

Open a terminal and check if the drive is detected:

sudo fdisk -l

Partition and format the drive:

Use a tool like gparted (GUI) or fdisk (CLI).

Format it to a filesystem like ext4 or NTFS (if sharing with Windows).

### ****Verification****

* Ensure the drive appears in your OS and is accessible.
* Check its capacity to confirm it's set up correctly.

With these steps, your hard drive should be installed and ready for use!

**Optical drive:**

An **optical drive** is a device in a computer or standalone player that reads and/or writes data to optical discs using laser technology. Optical drives are commonly used to interact with various types of discs, such as CDs, DVDs, and Blu-rays. They are named "optical" because they use light (lasers) to read and write data.

**Types of Optical Drives:**

CD Drive (Compact Disc):

Reads and writes CDs.

Storage capacity: Up to 700 MB per disc.

DVD Drive (Digital Versatile Disc):

Reads and writes both CDs and DVDs.

Storage capacity:

Single-layer DVD: 4.7 GB.

Dual-layer DVD: 8.5 GB.

Blu-ray Drive:

Reads and writes CDs, DVDs, and Blu-ray discs.

Storage capacity:

Single-layer Blu-ray: 25 GB.

Dual-layer Blu-ray: 50 GB.

Combo Drives:

Can read and write multiple formats (e.g., a Blu-ray drive that reads Blu-rays and DVDs and writes CDs and DVDs).

**Installing an optical drive (such as a CD, DVD, or Blu-ray drive) in your system is a straightforward process.**

Tools You Need:

Phillips-head screw driver.

Anti-static wrist strap (optional, to avoid static damage).

**Steps to Install an Optical Drive:**

1. Turn Off and Unplug Your System

Shut down your computer and disconnect the power cord and all peripherals.

Ground yourself to discharge static electricity by touching a metal surface or wearing an anti-static wrist strap.

2. Open the Computer Case

Use a screwdriver to remove the side panel of your case.

Place the case on a stable surface.

3. Locate the Drive Bay

Find an available 5.25-inch drive bay in your computer case. This is where optical drives are typically installed.

Remove the bay's front cover if it has one (usually by pressing tabs or removing screws).

4. Insert the Optical Drive

Slide the optical drive into the drive bay from the front of the case.

Align the screw holes on the drive with the holes in the drive bay.

Secure the drive using screws or the tool-less mechanism provided by the case.

5. Connect the Cables

SATA Cable (Data):

Connect one end of the SATA data cable to the back of the optical drive.

Connect the other end to a free SATA port on the motherboard.

SATA Power Cable:

Connect a SATA power connector from your power supply to the back of the optical drive.

6. Verify Connections

Ensure both the SATA data cable and SATA power cable are securely attached.

Check that the drive is firmly mounted in the bay.

7. Close the Case and Reconnect Power

Reattach the side panel of your case.

Reconnect the power cord and peripherals.

8. Power On and Test

Turn on your computer.

The system should automatically detect the new optical drive.

For Windows:

Open File Explorer (Win + E) and check if the drive appears under "This PC."

For Linux:

Open your file manager to see if the drive is listed.

You can also use the terminal command:

lsblk

Insert a disc to test the drive's functionality.

**Troubleshooting:**

If the drive is not detected:

Check the SATA and power connections.

Ensure the drive is enabled in the BIOS/UEFI settings.

If the drive doesn't work:

Try using a different SATA port or cable.

By following these steps, you should have a fully functional optical drive installed in your system.

**EXP 5: How to recover lost data on hard drive.**

Recovering lost data on a hard drive depends on the cause of data loss (accidental deletion, formatting, corruption, or hardware failure).

1. Stop Using the Drive

If you’ve accidentally deleted files or formatted the drive, avoid writing new data to it. Writing new data could overwrite the lost files, making recovery difficult or impossible.

2. Determine the Cause of Data Loss

Accidental Deletion: Files removed from the recycle bin or deleted permanently.

Formatting: The drive was formatted but not physically damaged.

Corruption: The drive is inaccessible, and the file system is corrupted.

Hardware Failure: The drive is physically damaged or not recognized.

3. Recovery Methods:

A. Use Built-In Tools (For Accidental Deletion or Corruption)

Windows:

Check the Recycle Bin for deleted files.

Use the File History feature if enabled:

Right-click the folder where the lost file was stored.

Select Restore previous versions.

macOS:

Check the Trash for deleted files.

Use Time Machine backup if available:

Open Time Machine and navigate to the folder where the lost file was stored.

Select the file and click Restore.

Linux:

Check the Trash directory (~/.local/share/Trash/).

Use the extundelete or testdisk command-line tools for recovery.

B. Use Data Recovery Software

Windows/Mac/Linux:

Download and install reliable data recovery software:

Recuva (Windows)

EaseUS Data Recovery Wizard (Windows/Mac)

Disk Drill (Windows/Mac)

PhotoRec (Cross-platform, for advanced users)

Steps to follow with recovery software:

Install the software on a different drive (not the one where data was lost).

Scan the drive where the data was lost.

Preview and recover the files to a different storage device.

C. Repair Corrupted Drives

Windows:

* Use the chkdsk tool:

chkdsk D: /f /r

Replace D: with the drive letter.

* Try the Disk Management tool to reassign drive letters or initialize the disk.

Linux:

* Use fsck to repair file system corruption:

sudo fsck /dev/sdX

Replace /dev/sdX with the drive identifier.

D. For Hardware Failures

* If the drive makes clicking noises, is not recognized, or has physical damage:

Avoid using the drive to prevent further damage.

Consider professional recovery services, such as:

* DriveSavers
* Seagate Recovery Services
* Ontrack Data Recovery

4. Prevention Tips

Backups:

Regularly back up your data to an external drive or cloud service.

Avoid Formatting:

Double-check before formatting or partitioning a drive.

Antivirus:

Use reliable antivirus software to prevent malware-related data loss.

Disk Monitoring:

Use tools like CrystalDiskInfo to monitor drive health.

Recovering lost data requires prompt action and care to avoid overwriting or damaging the drive further.

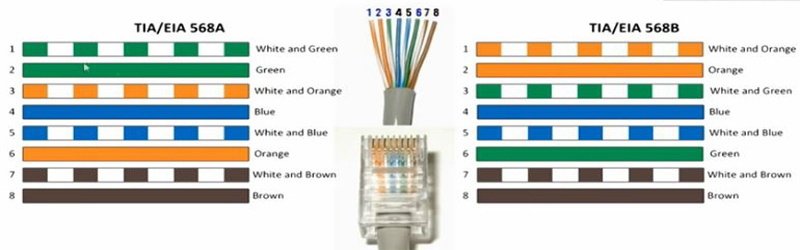
**Computer Networking:**

**EXP 6: Preparing the Ethernet cable for cross and direct connections using crimping tool and testusing LAN tester.**

**Crimping LAN Cables**

# Ethernet cable types

### There are 3 types of Cables.

[](https://kencorner.com/wp-content/uploads/2018/03/ethernet-cable-color-code.jpg)

## ****1. Straight Through Cables****

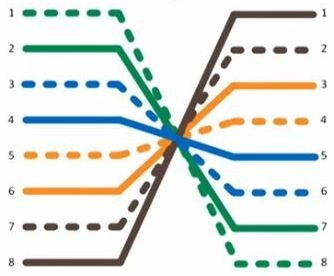
If we want to connect two different types of device then we can use straight-through cables.  
For example:  
> Connecting a router to a hub  
> Connecting a computer to a switch/router  
> Connecting a modem to a router

## ****2. Crossover Cables****

If we want to connect two same types of device then we can use crossover cables.  
For example:  
> Connecting a computer to a computer  
> Connecting a router to a router  
> Connecting a switch to a switch  
> Connecting a hub to a hub

## ****3. Rollover Cables****

This cables is used to connect computer to router’s console port.It is also called as console cable or yost cable.

[](https://kencorner.com/wp-content/uploads/2018/03/rollover_cable.jpg)

# Ethernet Cable Type

In computer networks, Cat-5, Cat-5e, and Cat-6 cables are mostly used. UTP cables are connected by RJ45 connectors.  
**Cable Type and  Speed**  
**CAT 3** 16Mbps  
**CAT 5** 100Mbps 1000Mbps (4 pairs)  
**CAT 5E** 1000Mbps  
**CAT 6** Up to 400MHz for super-fast broadband applications  
**Cat 7** cabling is also known as Class F.

**We will use  “Cat 6” cables for now.**

# Crimping tool rj45

[](https://kencorner.com/wp-content/uploads/2018/03/Tools-used-in-Lan-crimping-1.jpg)

**1)  rj45 Plug/Jack**

**2)  Ethernet cable**

[](https://kencorner.com/wp-content/uploads/2018/03/Tools-used-in-Lan-crimping-2.jpg)

**3)  LAN wire cutter**

**4)  rj45 Crimping tool**

**5)  rj45 Network LAN cable tester**

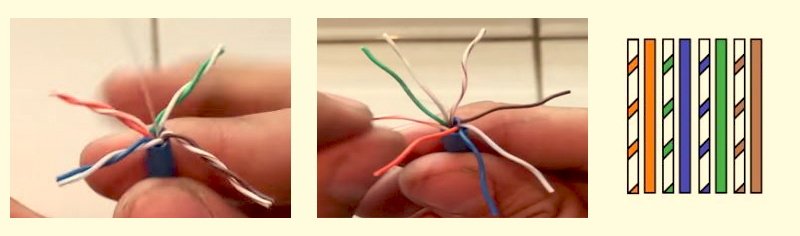
# How to make Ethernet cable

1. Take your LAN Cable and strip the outer cover be carefully in doing this or else the internal wire will be damage.

[](https://kencorner.com/wp-content/uploads/2018/03/Step1.jpg)

2. There will be 4 pair of twisted wire.

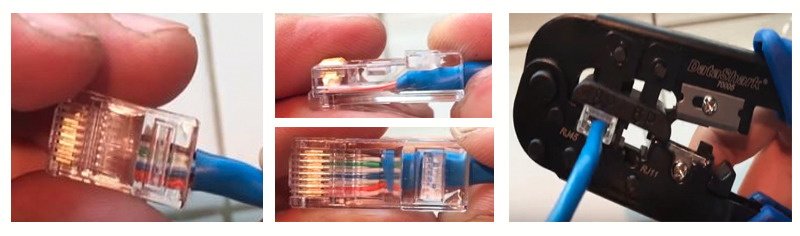
3. Unwind the twist cable and make it straight and cut the edge of wire.

[](https://kencorner.com/wp-content/uploads/2018/03/Step2.jpg)

4. Trim all the wires to the same length

[](https://kencorner.com/wp-content/uploads/2018/03/Step3.jpg)

5. Insert the wires into the RJ45 plug – make sure each wire is fully inserted to the front of the RJ45 plug and in the correct order.

[](https://kencorner.com/wp-content/uploads/2018/03/Step4.jpg)

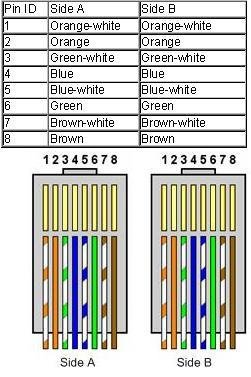
6. Now your LAN cable is ready you may now test the cable sing LAN tester.

**Note :**  
T568A and T568B are the two different colour codes used for pairing cable.  
T568B is mostly used one.

### ****Crimping a Straight through cable :****

Arrange all wire in the below manner and cut the edge ,be careful in doing so.Both end of cable must have same sequence of colored wire,please refer the below image.

**Both End of wire arrangement in cable is same.**

[](https://kencorner.com/wp-content/uploads/2018/03/straight-cable.jpg)

Now insert the cable into jack and then crimp the cable using crimping tool  
So now we crimped one side of the cable.so we can repeat the step for another side of cable.

### Crimping a Crossover cable :

Arrange the cable as shown in below image .

**Both End of wire arrangement in cable is different.**

Now cable is ready to use,You can test your cable using ” LAN Cable Tester” too.

**EXP:7 Installation of a switch and connecting systems to a network switch.**

**Switches:**

A switch is a network device. The main elements of a network are called Data Terminating Equipment. This term applies to computers, printers, faxes and any other pieces of equipment that serves the users of the network. The network that links these devices together is composed of cables and network equipment. A switch is the most commonly used network device. It makes connections between all the DTEs on the network, each of which is connected to the switch by a stretch of cable.

## 

## How to Install a Network Switch:

Network switches for home and small office use are typically stand-alone units, while switches for larger networks are usually rack-mounted. Either way, they typically use either Cat5 or Cat6 ethernet cables. Switches allow multiple computers to connect to a single Internet connection, but rather than simply passing the signal through, like a network hub, a switch can manage that network traffic. Switches differ in the way they handle network traffic, but all of them are installed in a very similar way.

### Step 1:

Provide power to the switch, if required. For a stand-alone switch, this simply means plugging in the power supply. For rack-mounted switches, this means using a slot that has power supplied to it.

##### Step2:

##### Connect the incoming network cable to the switch. Although any slot can be used on most network switches, it is a good idea to use the first slot so anyone can quickly identify the incoming cable. For home and small office applications, the incoming cable will be the one coming from your modem.

##### Step3:

Connect a Cat5 or Cat6 cable to another slot in the network switch. Connect the other end to a computer you want connected to the network.

**Step4:**



A Home / Office Switch

Repeat this process until all the computers are connected or all slots are filled.

## How to Connect an Ethernet Switch:



Home or Small Office Switch

A switch is a device that allows multiple computers to connect to one Internet connection. Unlike a network hub, which serves a similar purpose, a switch has the ability to manage the traffic that passes through it. A switch can be a stand-alone device, suitable for home or small office use, or rack-mounted for larger network applications. Switches also vary widely in traffic management capability. It's important to clearly define your requirements before you purchase a switch so you can buy the one best suited to your needs.

**Step1:**

Connect your modem to your Internet input line.Whether it is DSL, cable or satellite, your modem is the device that brings the signal into your network.

##### Step2:

##### Connect one end of an Ethernet cable to your modem. This will most likely be a Cat5 or Cat6 Ethernet cable. Connect the other end to your switch. Although not required, it's a good idea to connect this end to Slot 1 on your switch so you can quickly differentiate between incoming and outgoing cables.

##### 

##### Step3:

Connect one end of an other Ethernet cable to a different slot on your switch. Connect the other end of this cable to the Ethernet slot on a computer you wish to connect to the Internet.



Step4:Switch with one modem and two computers connected. Repeat Step 3 for all computers you wish to connect.

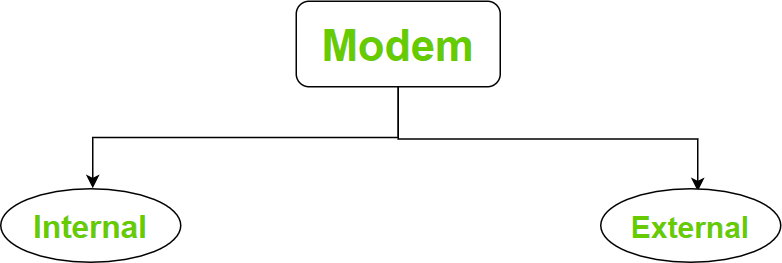


**EXP 8: Installation of a modem (internal, external or USB) and connecting to internet.**

### Modem:

### A modem is a hardware networking device whose basic functioning is to convert data to a signal. Modem is important so as to possess Internet access.

### Modem are of two types:



### Internal Modem:

As the name suggests internal modem is an internal part inside a computer. It usually comes with the computer and thattoo pre-installed. The best thing about internal modem is that itoperates with the computer’s power supply and doesn’t need an additional supply to work.

### External Modem:

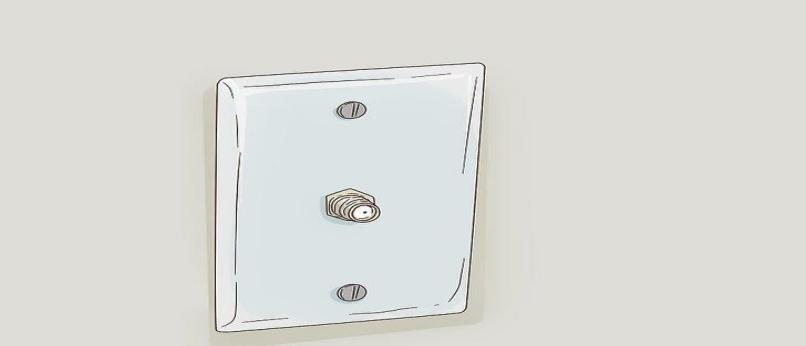
An external modem is quiet similar to the internal modem in that it also allows access to the Internet. The external modem is an external part of the computer. It can be used when a computer is unable to fit an internal modem inside of it. The modem typicallyconnectstothecomputer viaaserialorUSB cable, anditalsoneedsanexternalpowersupplyto operate.

## [How to Install a Modem](https://www.wikihow.com/Install-a-Modem)

## 

**Make sure that your modem will work with your Internet subscription.** While rare, some modems encounter issues when paired with a specific Internet company (e.g.,Comcast). Double-check your modem's compatibility with your current Internet subscription before buying (if possible).

* + If you find that your modemwon't work with your current subscription, try to exchange the modem for a different one that will work, or switch your Internet subscription.



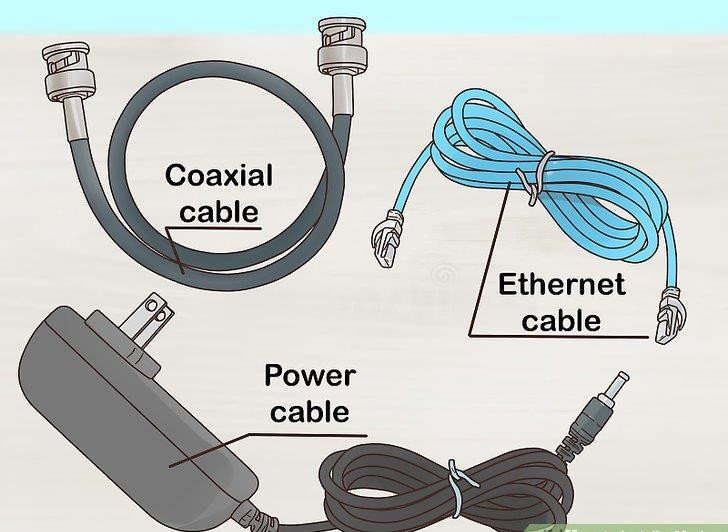
**Find your room's cable output.** The cable output resembles a metal cylinder with a small hole in the middle and screw threads all around the sides. You'll usually find cable outputs in the wall near the floor in living rooms and bedrooms.

* + In some cases, there will already be a cable connected to the cable outlet.

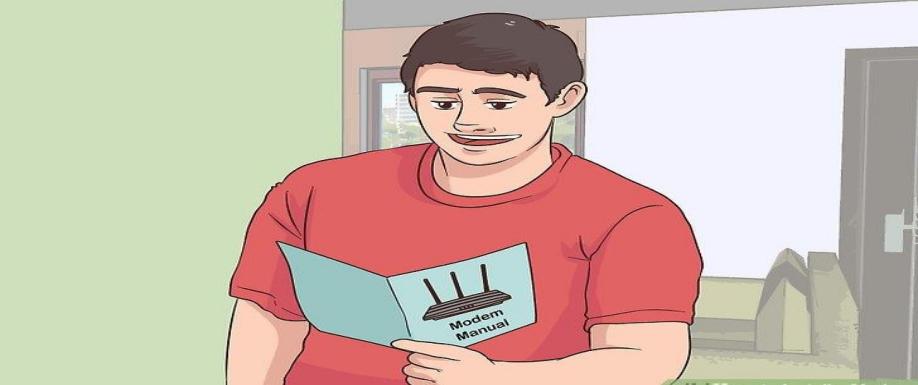
****

**Decide on a place to mount the modem.** The modem should be relatively highup (e.g., on top of a bookshelf), and it will need to be close enough to the cable output that you can connect it without stretching or bending the cable.

* + You'll also need to have a power outlet nearby.



**Make sure that you have all of the required cables.** A modem generally requires a coaxial cable to connect to the cable output, as well as a power cable to connect to an electrical out let. Both of thesecables should come with your modem, but if you bought it used, you may need to find replacement cables.

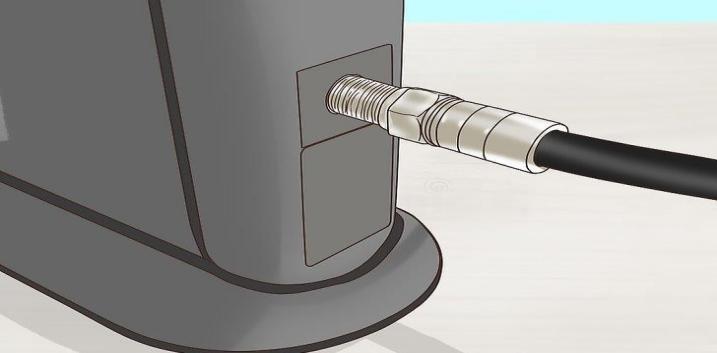
* + If you plan on attaching the modem to a router, you will also need an Ethernet cable.
  + Consider buying a longer coaxial cable if the one that you have is too short to allow you to mount properly your modem.

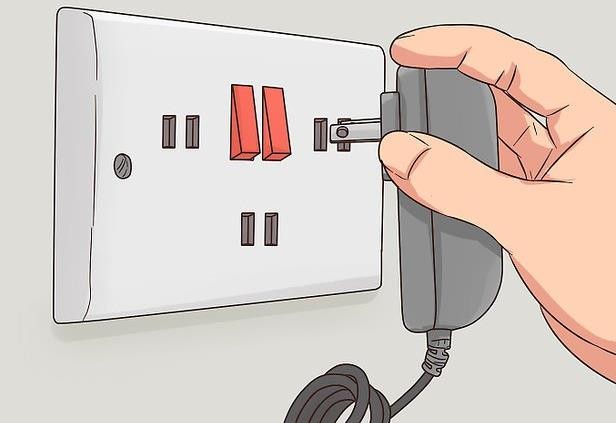
**Ready our modem's instructions.** Each modem is unique, and yours may require additional setup out side of this article's capacity. Reading your modem's manual will help make you aware of any additional steps that you have to take to install the modem.

##### Installing:

##### 

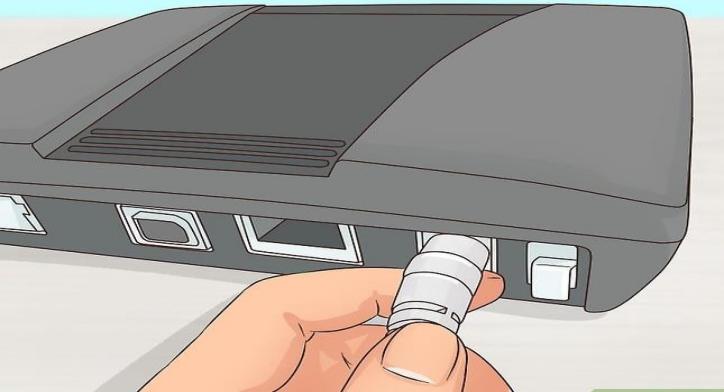
**Attach one end of the coaxial cable to the cable output.** The coaxial cable has a connection that resembles a needle on each end. This will plug into the cable output. Make sure that you screw the coaxial cable onto the cable outlet to ensure that the connection is solid.



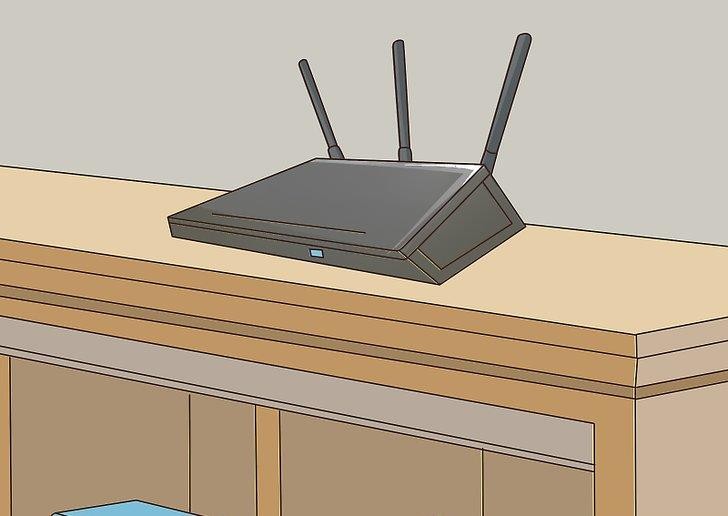
**Attach the other end of the cable to the input on your modem.** On the back of the modem, you should see an input that resembles the cable output cylinder. Attach the free end of the coaxial cable to this input, making sure to tighten as needed.

**Plug your modem's power cable into an electrical outlet.** A wall socket or a surge protector will do. It's important to plug the cable into the power out let be fore connecting it to the modem, since connecting the power cable tothe modem.

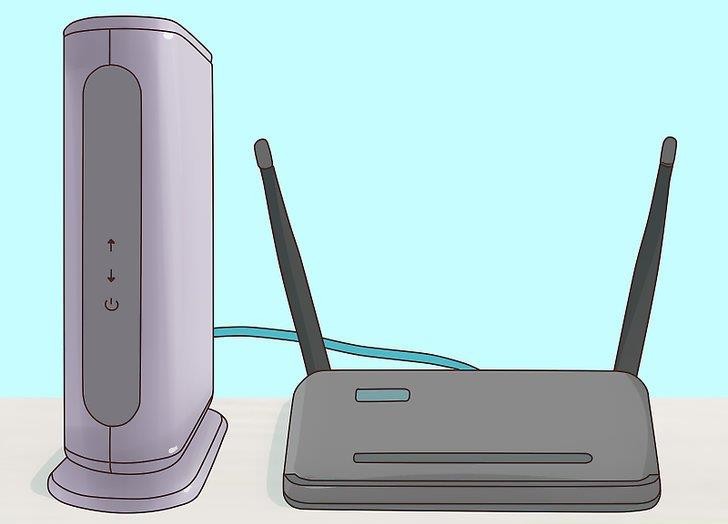
First can cause damage.



**Insert the modem power cable's freeend into the modem.** You'll usually find the power cable input port at the bottom of the back of the modem, but check your modem's documentation to confirm if you can't find the power port.



**Place your modem in its spot.** With the cables attached, gently move your modem into its designated position.You shouldn't feel any resistance from the cables.



**Attach the modem to a router.** If you have a Wi-Fi router that you want to use in conjunction with your modem, plug one end of an [Ethernet cable](https://www.wikihow.com/Set-up-Ethernet) into the square port on the back of the modem, then plug the other end into the "INTERNET" (or similarly labeled ) square port on the back of the router. As long as the router is plugged into a power source, the router should immediately light up.

* Give your modem and router a few minutes to boot up before attempting to [connect to Wi-Fi](https://www.wikihow.com/Connect-to-a-Wireless-Internet-Connection).
* You can also connect your computer directly to your modem via Ethernet if you have an Ethernet port enabled computer (ex. A PC or Ethernet Adapter for most Macs).

## How to set up and configure a USB modem on a Windows PC

[](https://www.hovatek.com/blog/bpyeki/uploads/2015/04/how-to-setup-and-configure-a-modem.jpg)

Its still the internet connection series and in this guide, we’ll be discussing how to setup / install and configure a USB modem (ie MTN, Airtel, GLO, Etisalat etc) on your Windows PC. If you choose to use Wi-Fi then consider reading these guides @[https://www.hovatek.com/blog/how-to-tether-share-an-internet-connection-on-an-android-phone-using- wi-fi-](https://www.hovatek.com/blog/how-to-tether-share-an-internet-connection-on-an-android-phone-using-%20%20%20%20%20wi-fi-)[bluetooth-and-usb-cord/](https://www.hovatek.com/blog/how-to-tether-share-an-internet-connection-on-an-android-phone-using-wi-fi-bluetooth-and-usb-cord/)and <https://www.hovatek.com/blog/how-to-share-an-internet-connection-data-plan-megabytes-between-android-and-pc/>

What are the problems commonly associated with USB modems ?

Some issues you might encounter are:

**Over heating**: The modem ( and some times the PC ) might over heat. Ensure the modem is connected to a good port when in use then disconnected and removed when not in use. You could also employ some PC cooling techniques( see <https://www.hovatek.com/blog/how-to-resolve-the-problem-of-an-overheating-laptop-pc/>)

**No/Low signal**: If the signal is weak, try changing ports and location. If the modem says Invalid SIM then its locked to another network and needs to be unlocked (see <https://www.hovatek.com/blog/how-to-unlock-a-modem/>)

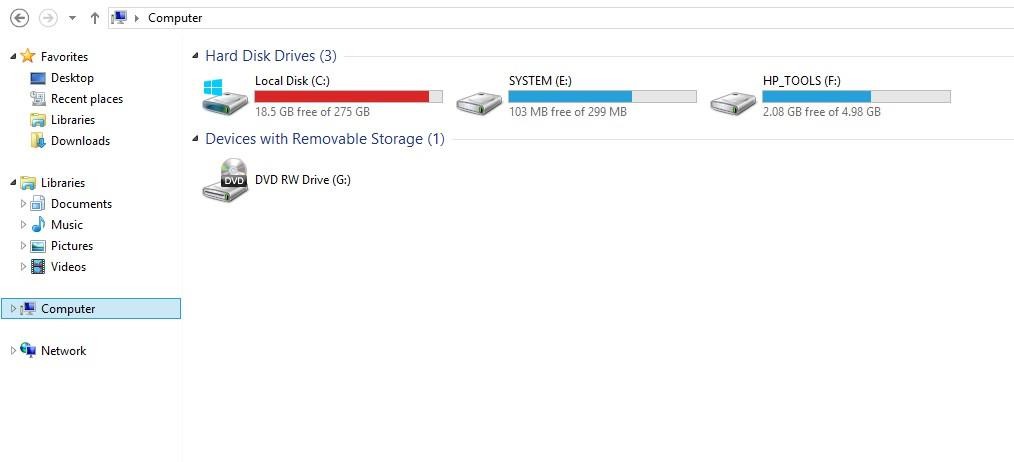
**Modem not detected:** This might be a hardware ( port / modem ) or driver issue.Try un installing the modem driver(under Device manager and then Programs)and manually installing (using a DVD, installer or another modem). Also, try other ports and the modem on another PC.

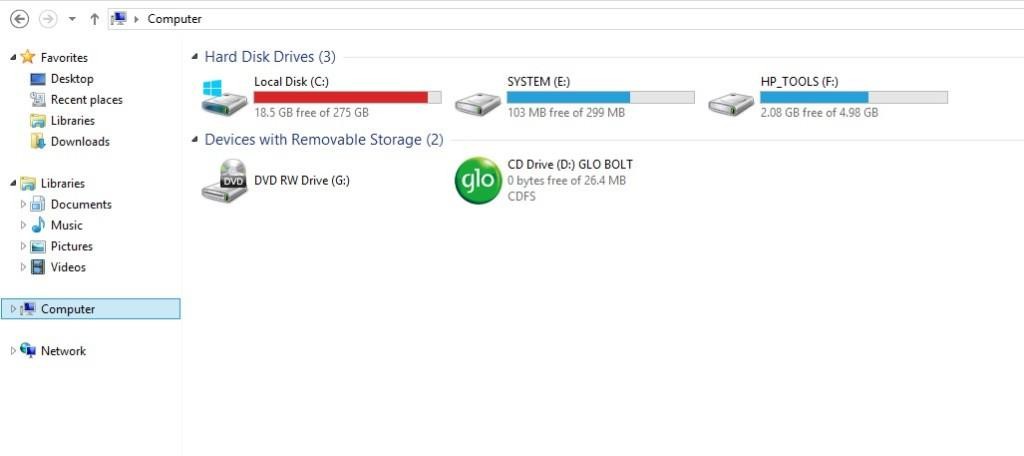
**Frequent disconnection:** This if often associated with the network but might also be due to a looseport/

Moving the modem while connected to the PC

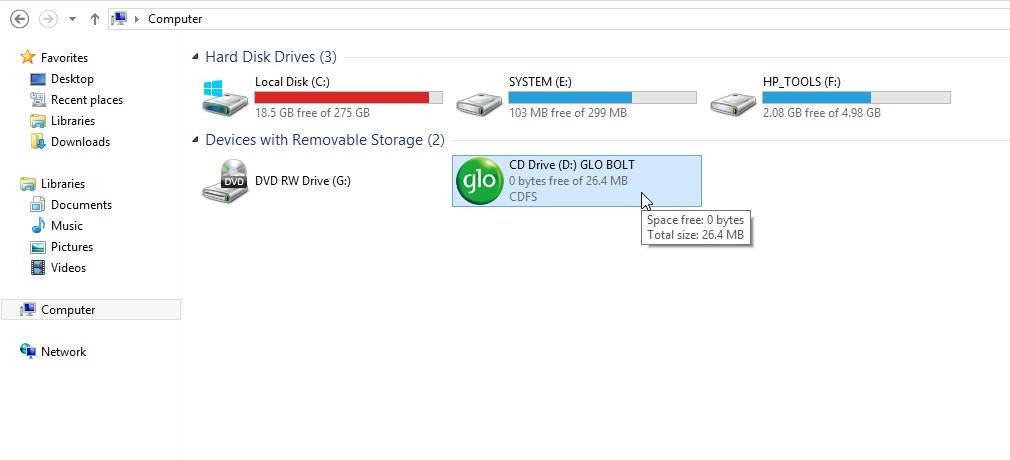
How do I setup / install a USB modem on aWindows PC?

We’ll be using an unlocked GLOBOL T modem for this guide so the technique should apply for many other such USB modems

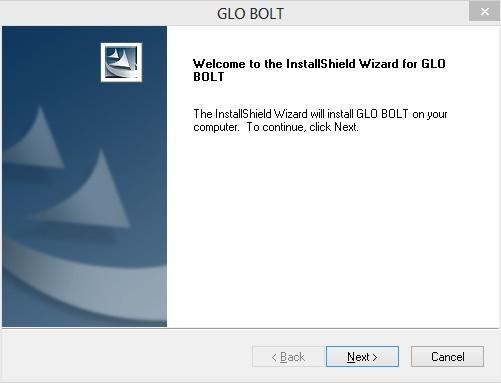
1. Goto My Computer
2. [](https://www.hovatek.com/blog/bpyeki/uploads/2015/04/how-to-install-a-modem-1.jpg)Connect the modem to the PC and wait for it to get detected (appear under MyComputer)

[](https://www.hovatek.com/blog/bpyeki/uploads/2015/04/how-to-install-a-modem-2.jpg)

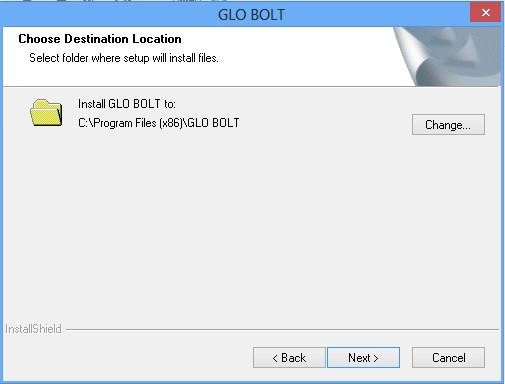
1. Double-click the Modem name to begin installation

[](https://www.hovatek.com/blog/bpyeki/uploads/2015/04/how-to-install-a-modem-3.jpg)

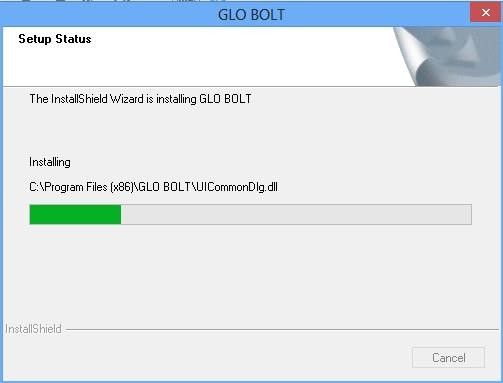
1. If prompted for permission to run auto run. Exe on your PC, select Yes
2. The installer wizard should appear, click Next

[](https://www.hovatek.com/blog/bpyeki/uploads/2015/04/how-to-install-a-modem-4.jpg)

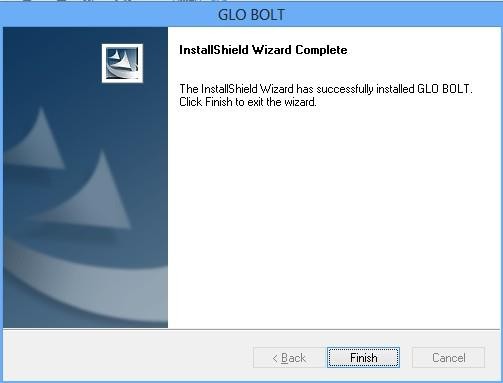
1. Leave the install location as default if you don’t know what this is and click Next

[](https://www.hovatek.com/blog/bpyeki/uploads/2015/04/how-to-install-a-modem-5.jpg)

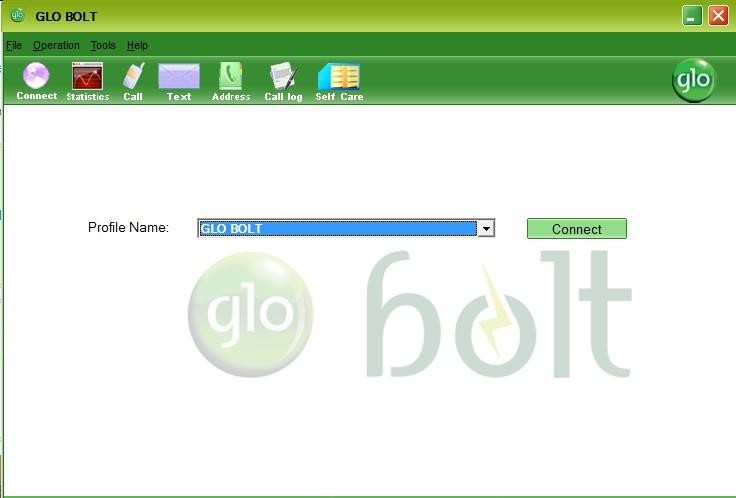
1. Installation should begin, wait till its complete

[](https://www.hovatek.com/blog/bpyeki/uploads/2015/04/how-to-install-a-modem-6.jpg)

1. Click Finish

[](https://www.hovatek.com/blog/bpyeki/uploads/2015/04/how-to-install-a-modem-7.jpg)

9. The modem’s dash board should automatically pop up.If it does n’t, launch it from your Desktop

[](https://www.hovatek.com/blog/bpyeki/uploads/2015/04/how-to-install-a-modem-8.jpg)

##### How do I configure the modem to surf the inter net with my SIM?

As earlier mentioned, we’ reusing an unlocked GLOBOL T modem for this guide so the exact steps might vary with USB modems but its the same principle. You however need to know your network’s APN details.for example:

*Note: If you’ reusing a modem that does n’t support SIM cards or using the networks’s SIM card on the Network’s branded modem then you shouldn’t need to configure. just click Connect to start surfing the internet.*

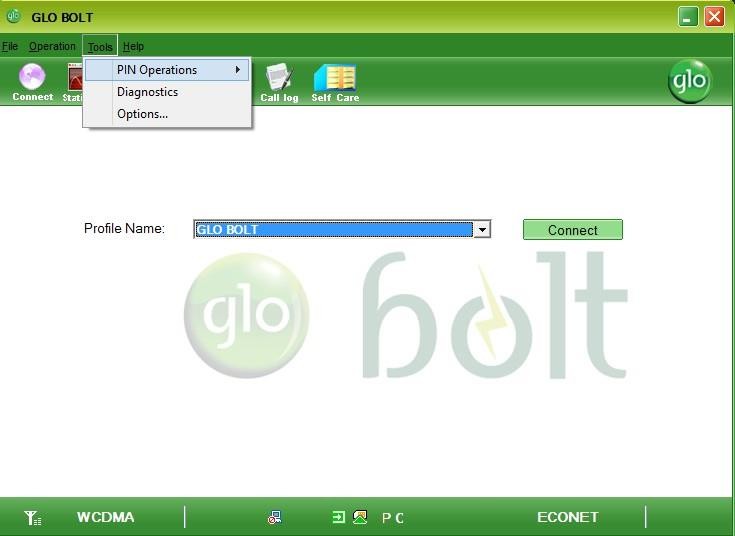
|  |  |  |  |
| --- | --- | --- | --- |
| Network | APN | Username | Password |
| MTN | web.gprs.mtnnigeria.net | web | web |
| Airtel | internet.ng.zain.com | notrequired | Notrequired |
| GLO | gloflat | flat | flat |
| Etisalat | etisalat.com.ng | Notrequired | not required |

Procedure

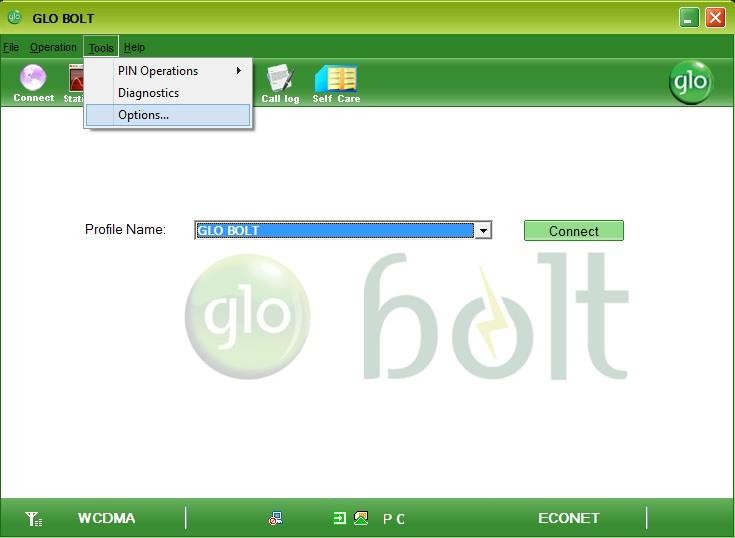
1. Launch the modem’s Dashboard

[](https://www.hovatek.com/blog/bpyeki/uploads/2015/04/how-to-configure-a-modem-1.jpg)

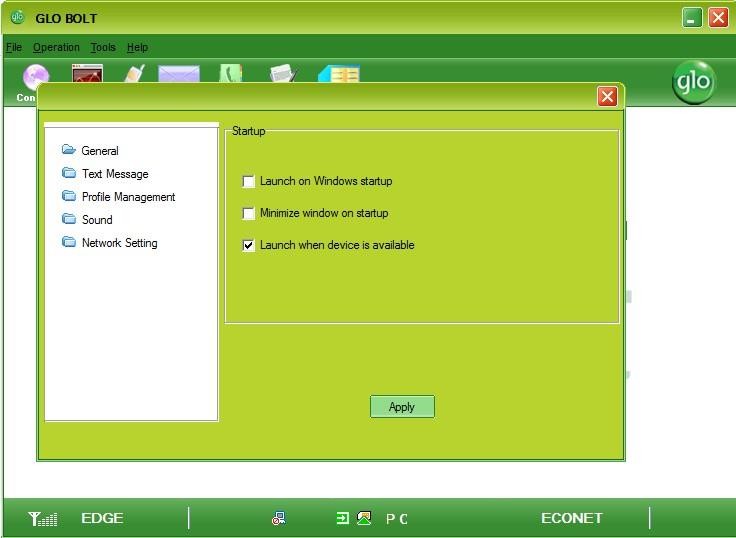
1. Click on the Tools tab

[](https://www.hovatek.com/blog/bpyeki/uploads/2015/04/how-to-configure-a-modem-2.jpg)

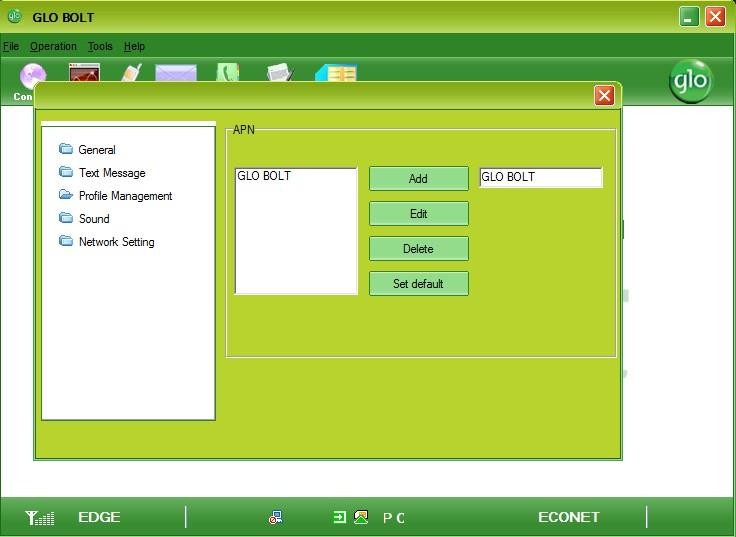
1. Select Options..

[](https://www.hovatek.com/blog/bpyeki/uploads/2015/04/how-to-configure-a-modem-3.jpg)

1. Click on Profile Management

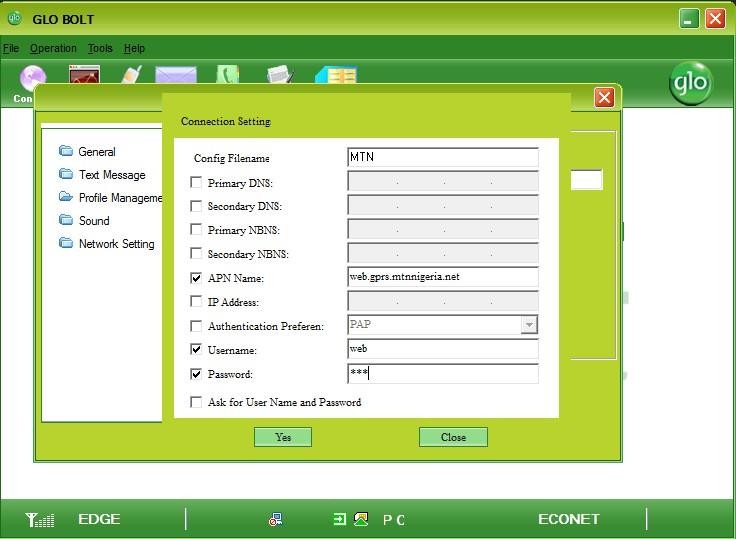
[](https://www.hovatek.com/blog/bpyeki/uploads/2015/04/how-to-configure-a-modem-5.jpg)

1. Click Add

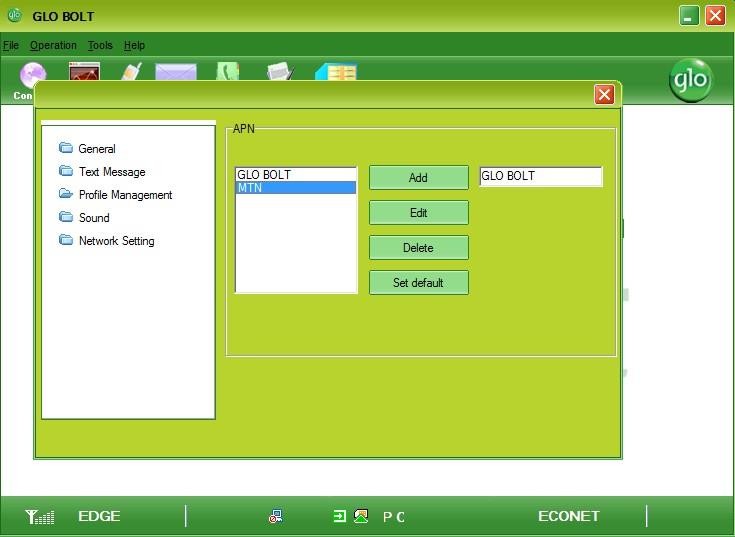
[](https://www.hovatek.com/blog/bpyeki/uploads/2015/04/how-to-configure-a-modem-6.jpg)

1. Enter the network’s APN details ( don’t tick user name and password if not required ) then click Yes or

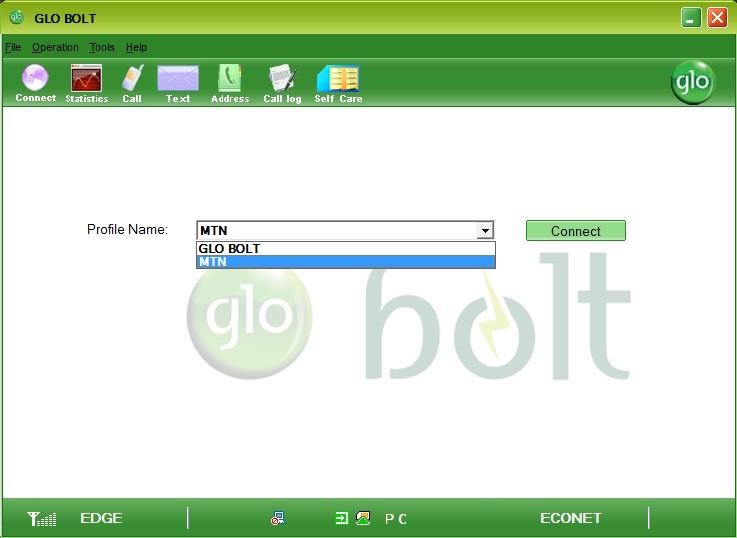
Save

1. [](https://www.hovatek.com/blog/bpyeki/uploads/2015/04/how-to-configure-a-modem-7.jpg)You could select the network by the left and click Set default to make it your default APN or just

Close the box

[](https://www.hovatek.com/blog/bpyeki/uploads/2015/04/how-to-configure-a-modem-8.jpg)

1. Select the APN from the drop down menu then click Connect

[](https://www.hovatek.com/blog/bpyeki/uploads/2015/04/how-to-configure-a-modem-9.jpg)

##### Exp9:Exercise onusingFTPforuploadinganddownloadingfiles.

FTP (File Transfer Protocol) is one of the most efficient methods for sending large files over the Internet. It also allows you to send multiple files, regard less of size, in on ego. In the following sections, I’ll draw up a step-by-step guide on how to transfer files using FTP. Learning how to FTP a file is not as difficult as you probably think.

##### Warning

Before you proceed, please note that the use of FTP is no longer recommended, especially if you transmit sensitive files. FTP is an insecure protocol that's vulnerable to man-in-the-middle and other attacks. To learn more about FTP's weaknesses and the more secure options for transferring files, please read the following articles:

##### Basic concept of an FTP file transfer

An FTP file transfer always involves at least two machines.This pair of machines can either be:

1. An [**FTP client**](https://www.jscape.com/products/file-transfer-clients/anyclient/)and an [**FTP server**](https://www.jscape.com/products/file-transfer-servers/jscape-mft-server/)or
2. Two FTP servers. A file transfer involving two servers is called a [**server to server file transfer**](https://www.jscape.com/blog/you-know-it-s-time-to-implement-server-to-server-file-transfer-when).

This post focuses on scenario 1, which is illustrated below.

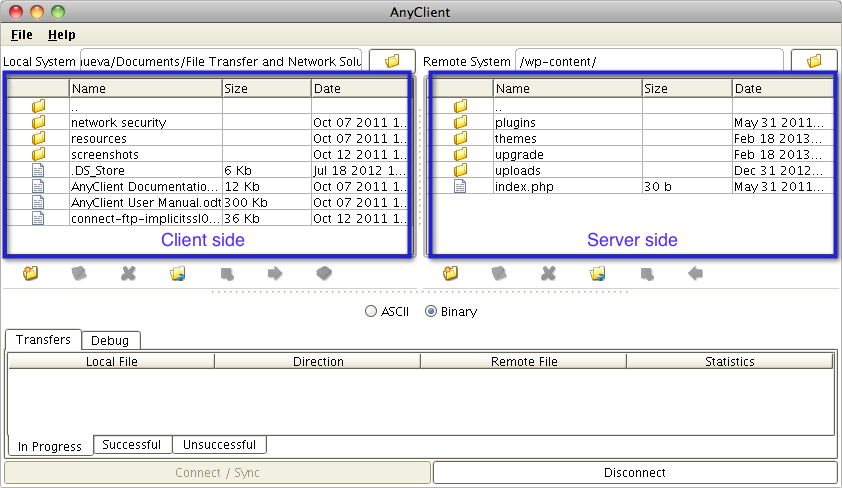
The client is the file transfer software used for uploading (sending) or downloading (retrieving) files to or

from the server. Itcanalsobeusedfornavigatingandbrowsingcertaindirectories foundon that’server.

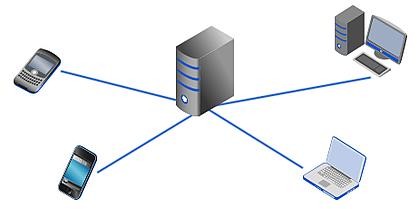
Thisiswhat you’llseeonatypical FTP client (see screenshot below).

Notice how an FTP client can display the directory contents (i.e., files and folders) of both the client and the server. Contents at the client side are usually labeled “ Local ”, while contents at the server side are usually

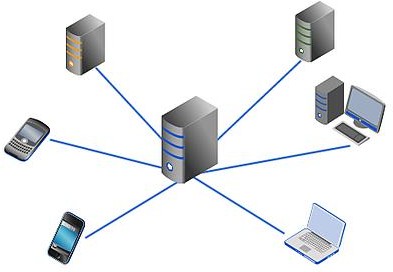
Labeled “Remote”.



Being a server, an FTP server can readily support multiple clients at the same time.



Once files have been uploaded to a server, those files can be accessed by other machines, including clients and other servers.



As an enduser wanting to transfer files via FTP, all you’ll have to be concerned with are the things you need

To do on the client side. That’s what we’ll be focusing on in the succeeding sections.

##### Basic requirements

So what’s the first thing you’ ll need to FTP a file? That’s right. If you’ve been paying attention earlier, you should know you’ll need an FTP client.

Next,you’llneedan accountonthatFTPserveryou’llbeconnectingto.Theadminofthatservershouldbeabletofurnish you with the following information:

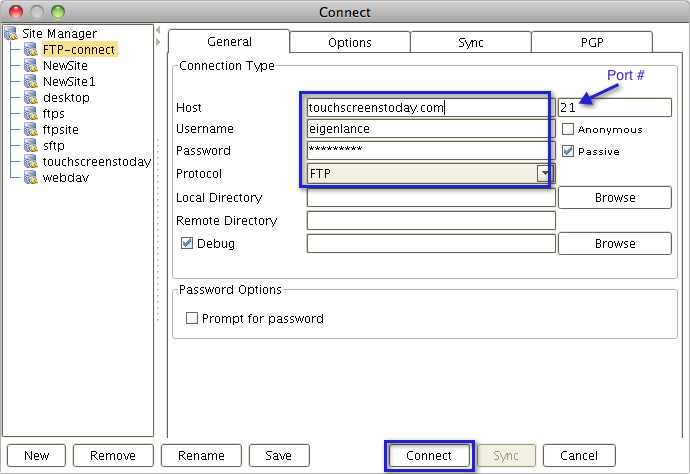
* 1. Your Username;
  2. Your Password; and
  3. The IP address / FTP site URL / host name of the FTP server Once you have those three, you’ll be good to go.

Note: I’ll beusing [**JSCAPE Any Client**](https://www.jscape.com/products/file-transfer-clients/anyclient/)for the rest of this tutorial.

##### How to connect to your FTP server:

Let me now show you how to connect to the FTP server. Here’s how to do it.

1. LaunchyourFTPclient.
2. Enteryourusernameand passwordintotheirrespective fields.
3. Enter the FTP server’s IP address (e.g. 192.168.0.150), FTP site URL (e.g.tp://touchscreenstoday.com), or hostname(e.g.touchscreenstoday.com).Inourexample,thisinformationisenteredintothefieldlabeledHost.
4. Ifyour FTPclientsupportsmultiplefiletransferprotocols,selectFTPasthe desired Protocol.
5. IfyourFTPclient doesnotautomatically enterthe portaddress, enterthenumber21.
6. Now,clicktheConnectbutton.



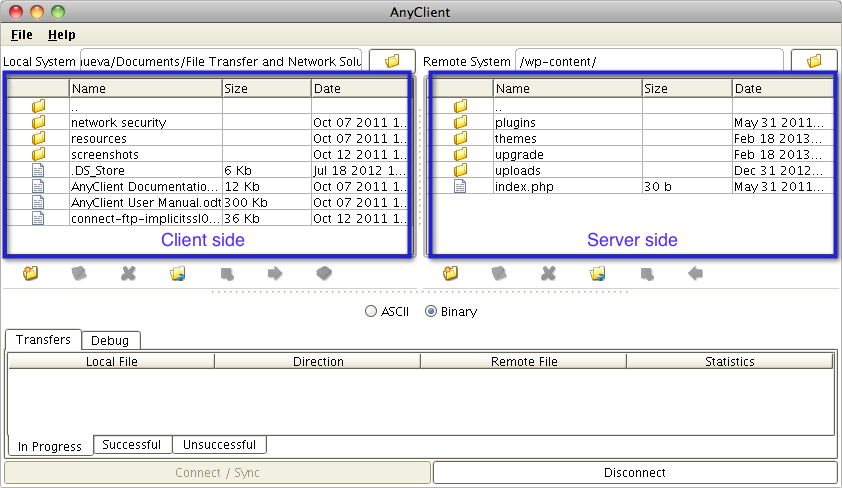
##### Navigating/BrowsingdirectoriesontheFTPserver

Once you’ve successfully connected, you can start browsing through the directories where you have been

granted access. MostFTPclientsallowyoutodouble-clickonafolderinordertoenterit. Tomoveupto

Thecurrentfolder’sparentfolder, you should click the corresponding button. In AnyClient, that would be

the folder labeled with ellipses (..)



##### UploadingandDownloadingafileto/from anFTPserver:

Touploadafile,yourcurrent directoryon theclientside(Local System)should be thedirectory that

HoldsthefileyouWanttoupload.Forexample,wewanttouploadthefilenamed“AnyClientUser

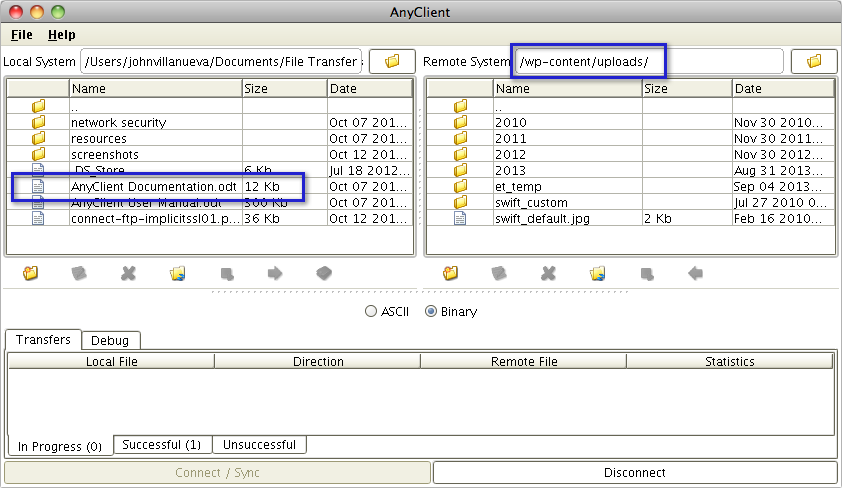
Manual.Odt”.Sowenavigatetothefolder that contains that file.

Next, moveto theserver side (RemoteSystem) and navigateto thetarget folder. This is the folder

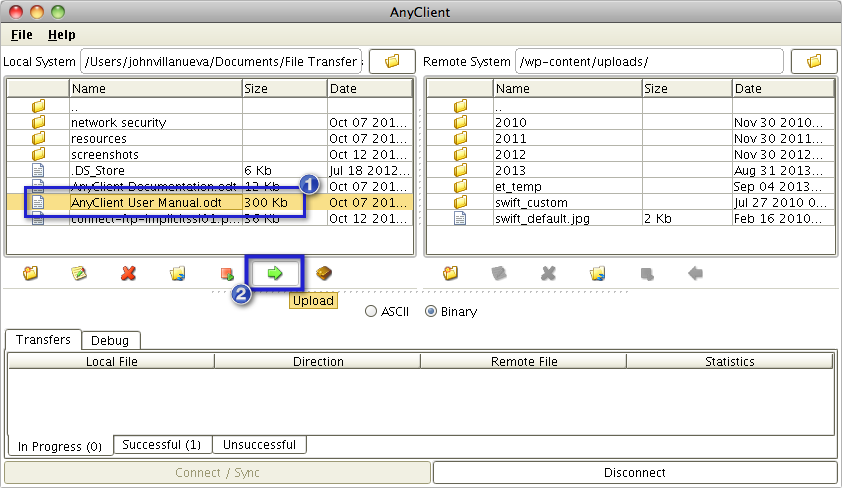
on the server whereyou wantyourfiletobestored.Again,tonavigate,just

Double-clickonthedesiredfolder.Inourexample,wewanttostoreour uploaded file into the

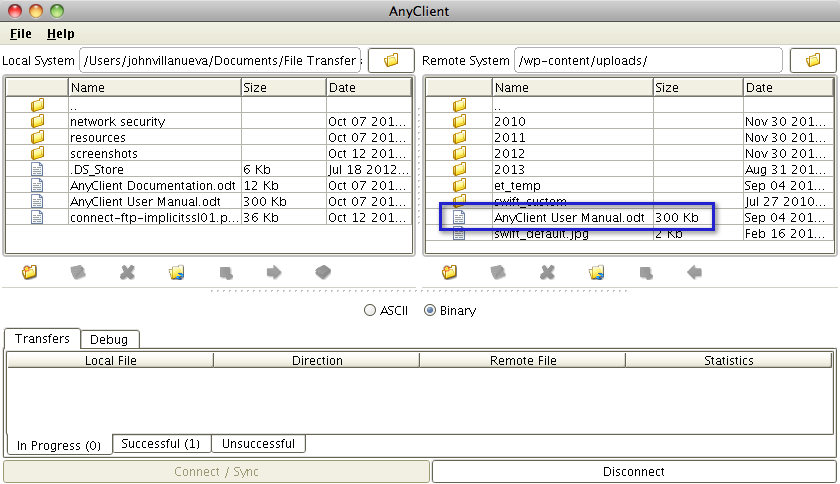
“uploads” folder as shown below.



Onceyou’redonewiththat,youcanthencommenceupload.Youmighthavetolookfortheuploadbuttonfirst.Once you’ve found it, select the file you want to upload and then click the Upload button.

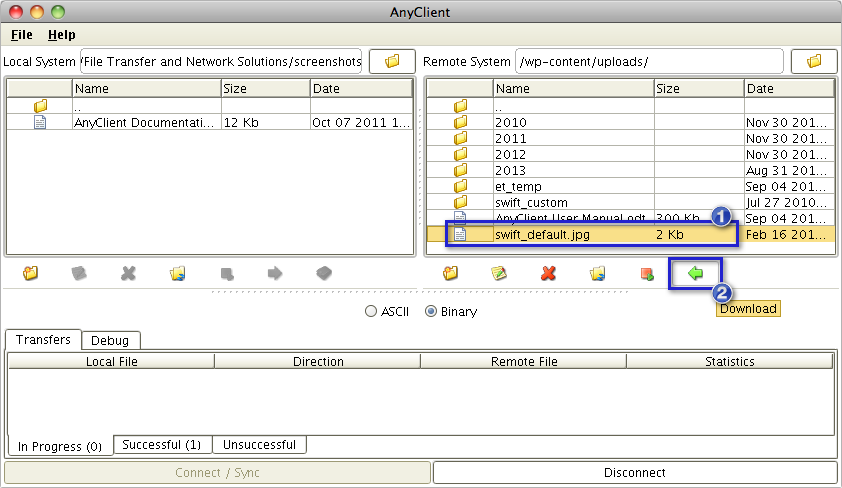


Here’sascreenshotshowingtheuploadedfile.



Theprocessfordownloadinga filefroman FTP serverisverysimilar. Just:

1. Navigateto theremotefolderwherethe fileyou want todownload is stored,
2. Navigatetothelocalfolder whereyouwant tostorethedownloadedfile,
3. Selectthefileyouwantto downloadfromtheremotefolder, and
4. ClicktheDownloadbutton.



That’sit.That'showeasyitistosendafilevia FTP.

**EXP 10: Installation and configuring the proxy server for internet access.**

If you employ a proxy server for Internet connectivity, you can configure the Manager or your devices to connect to thatserverforproxyservice.ThisisnecessaryifyouwanttodownloadupdatesdirectlytoManagerfromtheUpdateServeror if you want to download host reputation and country of origin information during integration with TrustedSource.

TheManagersupportsapplication-levelHTTP/HTTPSproxies,suchasSquid,IPlanet,MicrosoftProxyServer,and Microsoft ISA.

**NOTE:**TouseMicrosoftISA,youmustconfigurethisproxyserverwithbasicauthentication. NetworkSecurity Platform does not support Microsoft ISA during NTLM (Microsoft LAN Manager) authentication.

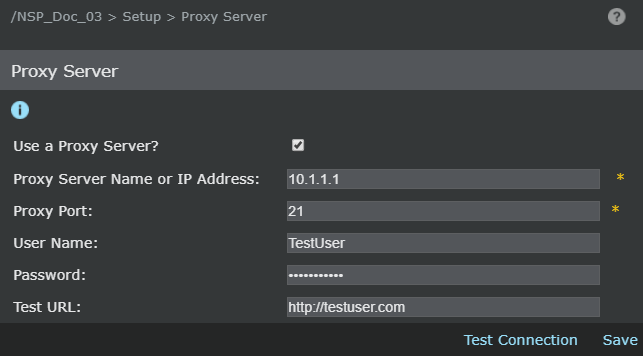
**NOTE:**SOCKS,anetwork-levelproxy,isnotcurrentlysupportedbyNetworkSecurity Platform.

Tospecify yourproxyserver, dothe following:

Task

LogintotheManagerinstance.

Select**Manager**→**<AdminDomainName>**→**Setup**→**ProxyServer**.The**ProxyServer**pageisdisplayed. Proxy Server Settings



Typethe**ProxyServerNameorIPAddress**.ThiscanbeeitherIPv4orIPv6address. Type the **Proxy Port** of your proxy server.

Type**User Name**and**Password**.

ProvidetheappropriateURL.Youmaytesttoensurethattheconnectionworksbyenteringa**TestURL**and

Clicking**Test Connection**.

Click**Save**to saveyoursettings.

WhentheManagerorthedevicemakesasuccessfulconnection,Itdisplaysamessageindicatingthattheproxyserver settings are valid.

### Howtofindproxysettingsin Windows:

Beforesettingupaproxyserver,youneedtochecktheproxysettingsonyourcomputer.Theinformation

Inproxysettings can help you determine which type of proxy server you can set up.

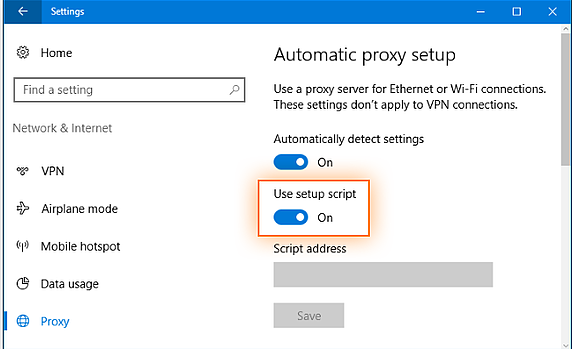
Here’showtofindproxy settingsonWindows:

1. Click **Start**andselect**Settings**(thegearicon)fromtheStart menu.
2. Choose**Network&Internet**.
3. Click**Proxy**intheleftpanel.
4. Hereyoucanfind theinformationyou needrelatedto automaticproxysettings andmanualproxysettings.

##### Howto setup aproxy serverinWindows:

Here'showto setupyourWindowsPC touseaproxyserver on Windows8 orWindows 10:

1. Pressthe**Windows**+**I**keys simultaneouslytoaccesstheWindowsSettings menu.
2. OnWindows10,click**Settings**>**Network &Internet**>**Proxy**.On Windows8,click **Settings**>**Network Proxy**.
3. UndertheManualSetupsection,setthe“UseaProxyServer”toggleto **On**.Makesurethe“Automaticallydetect settings” toggle is also on.
4. Bydefault,Windowsautomaticallycheckstoseeifyourbusiness,school,orlocalnetworkalreadyhasanautomatic proxy server setup ready to run for you. If it does, Windows tells you its name, and encourages you to follow its instructions.
5. Assumingthat Windowsfinds aPACfile, in theAutomaticProxySetup, set the**UseSetupScript**switch to **On**.



1. Enter the script address and click**Save**.

Congratulations!You'redoneandreadytoproxy.

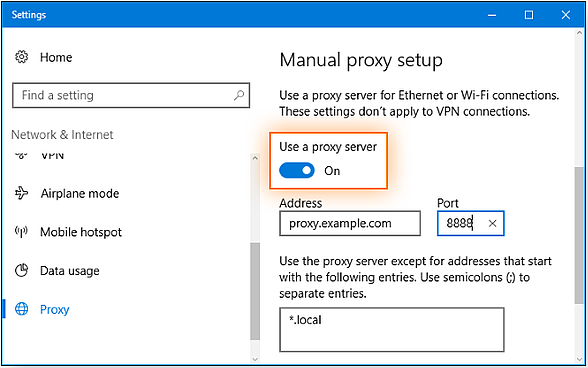
#### HowtomanuallysetupaproxyinWindows8orWindows10:

Noteveryorganizationsetsuptheprocessautomatically.Ifyouneedtosetupaproxy manuallyinWindows8or Windows 10, here’s how to do it.

1. ToaccesstheWindowsSettingsmenu, pressthe**Windows**+**I**keys simultaneously.
2. OnWindows10,click**Settings**>**Network&Internet**>**Proxy**.OnWindows8systems,

click**Settings**>**Network Proxy**.

1. Scrolldownto “Manualproxysetup”and setthe“UseaProxyServer”switchto**On**.



1. In the address field, type the proxy server name or IP address. In the Port field, enter the proxy port number. You canget these from your IT support tech.

5. If the proxy server is protected by a password, select the “Proxy server requires password” checkbox. Enter your

account name and password in the Username and Password fields.

6. Click **Save**.

That's all there is to it. You're now set up to use your proxy server on Windows. The next time you use the internet, you'll

be using the proxy server.

**How to set up a proxy server on a Mac running macOS**

Here's how to set up a proxy server on a Mac running macOS 10.15 Catalina. Other macOS versions use essentially the

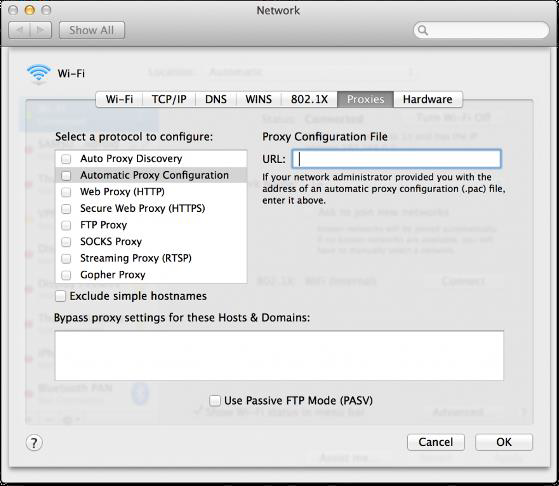
same commands.

1. Open System Preferences. One way to get there is to click on the **Apple menu** >**System Preferences**.

2. Choose the **Network icon** to adjust connectivity settings.

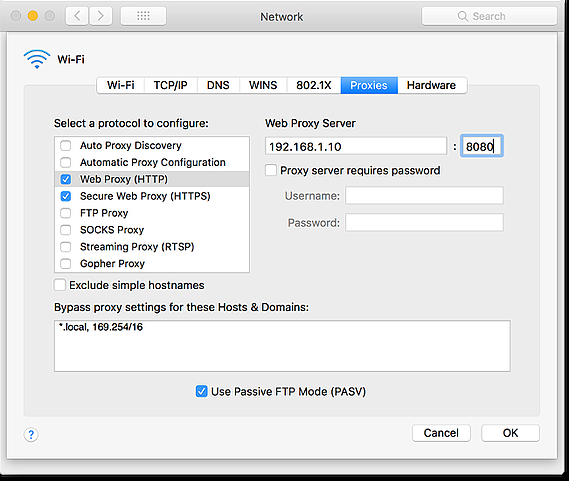
3. Select the type of network you use, which is usually Ethernet or Wi-Fi.

4. Click **Advanced** >**Proxies**.



1. To automatically configure your proxy server settings, select **Auto Proxy Discovery**. Click on **Secure Web Proxy**

**(HTTPS)**. Type in the proxy server address and its port number in the fields on the right.



1. To use a proxy auto-configuration (PAC) file, select **Automatic Proxy Configuration** and enter the proxy addressinto the URL field.

7. If the proxy server is protected by a password, select the “Proxy server requires password” checkbox. Enter youraccount name and password in the Username and Password fields.

8. Click **OK** to save the proxy setup.

You're now ready to surf the internet via your proxy.

**How to set up a proxy in Google Chrome**

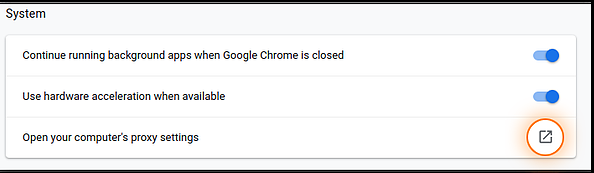
By default, Chrome uses your macOS or Windows proxy. To change your proxy settings from within Chrome, take the

following steps:

1. Open the Chrome toolbar and select **Settings**.

2. Scroll down to the bottom of the display. Click on **Show advanced settings...**

3. Scroll down to “System” and choose **Open your computer’s proxy settings.**



4. Next, go back to the instructions for your operating system listed above to set up your proxy server settings andfollow them.

In short, to set up a proxy server in Google Chrome, you're just doing the first few steps in the browser, and then

completing the process in your machine's operating system.

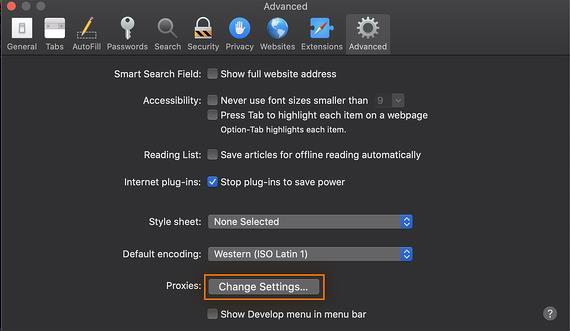
**How to set up a proxy server in Safari**

Like Chrome, Safari’s default setting is to follow the proxy configurations within your OS. Here’s how to change your

proxy settings from within Safari:

1. Click on **Safari** in the browser toolbar. Choose **Preferences**.

2. Click on the **Advanced** tab. Under “Proxies,” click **Change settings…**



3. Next, you must go back to the instructions for macOS listed above to set up your proxy server settings and followthem.

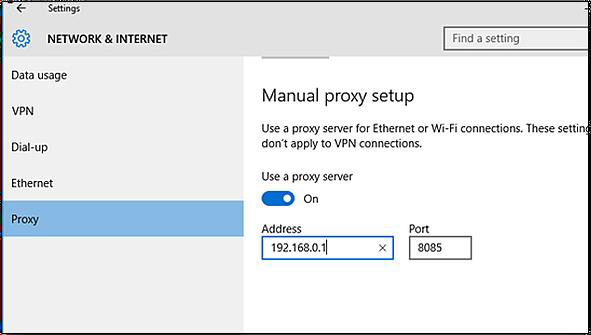
**How to set up a proxy server in Edge**

Edge is Windows 10's built-in web browser, and unless you tell it otherwise, it’ll use your proxy configurations inWindows. The latest versions of Edge are based on Chrome, so the configuration is similar. The following steps show youhow to set up a proxy from within Edge:

1. In Microsoft Edge, at the top-right corner, click the **Menu** button. Select **Settings**.

2. Scroll down to the Advanced settings section and click the **View advanced settings** icon.

3. Click the **Open proxy settings** button.



4. Next, go back to the instructions for Windows 10 listed above, then follow them to configure your proxy serversettings.

**How to set up a proxy server in Firefox**

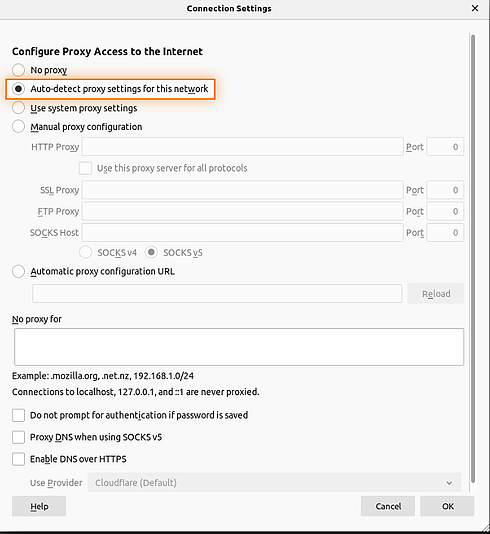
Unlike other web browsers, Firefox doesn't default to using your system's proxy settings. You’ll need to change your proxyfrom within Firefox:

1. Open the Firefox menu and select **Options**.

2. Click on the **Advanced** icon.

3. Select the **Network** tab.

4. In the Connection Settings, select, **Auto-detect proxy configuration for this network**. When prompted, enter theproxy address.



5. Alternatively, in the Connection Settings, you can select, **Use system proxy settings**. If you choose that option,

Firefox uses the proxy settings in your operating system.

6. Click **OK** to save your settings.

**How to set up a proxy server in Internet Explorer**

Please keep in mind that Internet Explorer is an outdated web browser. Instead, switch to a browser that’s still receiving

regular updates and support, such as Avast Secure Browser, Chrome, Edge, Firefox, or Safari. Though since quite a few

people and companies still use Internet Explorer (IE), you should know how to set things up when necessary.

As with other browsers, IE defaults to using your Windows proxy configurations. Here’s how to set your proxy up from

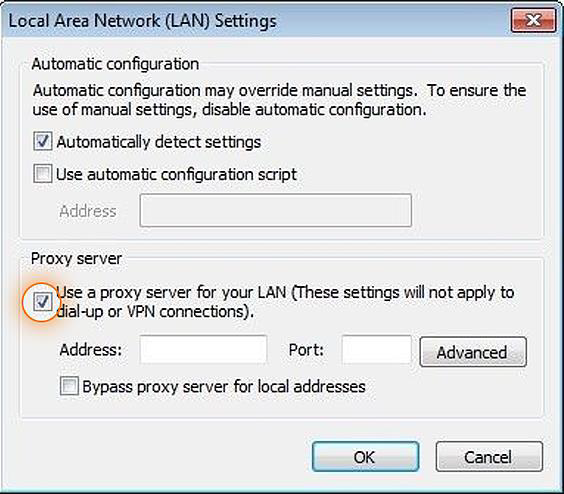
within IE.

1. Open the IE toolbar and select **Internet Options**.

2. Open the **Connections** tab.

3. Select **LAN Settings**.

4. Check the “Use a proxy server for your LAN” box.



5. When prompted, enter the proxy server name and port number.

6. Click **OK** to save your settings.

7.

**How to set up a proxy server in Android:**

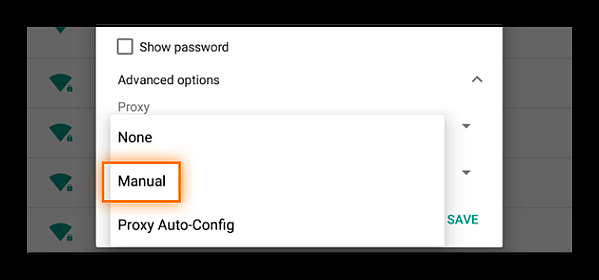
With Android, you must configure proxy settings for each network you use. In addition, the proxy will only be used byyour web browser. Other internet applications may choose to use or ignore the proxy based on their own internal settings.

This is another reason why VPNs tend to be better choices — when you use one, it covers all the internet traffic from yourdevice.

1. Open Android’s Settings and tap **Wi-Fi** to view a list of Wi-Fi networks.

2. Long-press the Wi-Fi network name for which you want to change the proxy settings. Tap **Modify Network**.

3. Tap **Advanced Options**.



4. Tap **Manual** to change your proxy's settings. Enter your hostname and proxy port.

OR

If you have a Proxy Auto-Config (PAC) file, select **Proxy Auto-Config** and Android will prompt you to enter the

PAC address.

5. Tap **SAVE**.

**How to set up a proxy server in iOS**

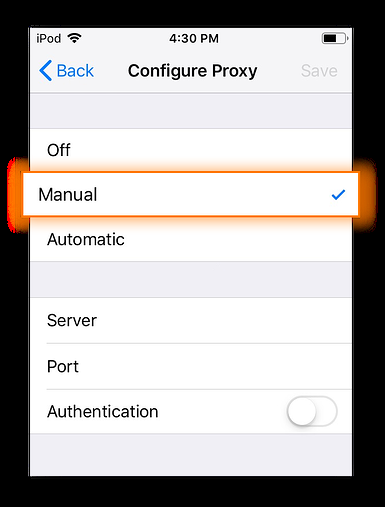
1. Go to **Settings** >**Wi-Fi**.

2. Select the active Wi-Fi connection.

3. Under HTTP proxy, click **Configure Proxy**.

4. Tap **Manual** to change your proxy's settings. Enter your host name, proxy port, and, if needed, your authentication

username and password.



OR

If your provider supports Web Proxy Auto-Discovery Protocol (WPAD), tap **Automatic**. If required, enter the Proxy

Auto-Config (PAC) file location.

1. Tap back to the Wi-Fi selection window

**EXP11: Exercise on Setting of particular IP address to an existing terminal system.**

**What is an IP address?**

IP address stands for “Internet Protocol address.” The Internet Protocol is a set of rules for communication over the

internet, such as sending mail, streaming video, or connecting to a website. **An IP address identifies a network or device**

**on the internet.**

The internet protocols manage the process of assigning each unique device its own IP address. (Internet protocols do other

things as well, such as routing internet traffic.) This way, it’s easy to see which devices on the internet are sending,

requesting, and receiving what information.

IP addresses are like telephone numbers, and they serve the same purpose. When you contact someone, your phone number

identifies who you are, and it assures the person who answers the phone that you are who you say you are. IP addresses do

the exact same thing when you’re online — that’s why **every single device that is connected to the internet has an IP**

**address**.

There are two types of IP addresses: IPv4 and IPv6. It’s easy to recognize the difference if you count the numbers. IPv4

addresses contain a series of four numbers, ranging from 0 (except the first one) to 255, each separated from the next by a

period — such as 5.62.42.77.

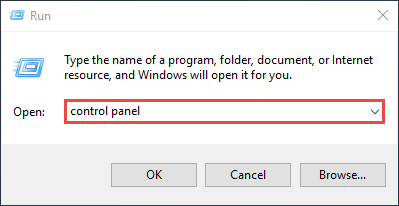
IPv6 addresses are represented as eight groups of four hexadecimal digits, with the groups separated by colons. A typical

IPv6 address might look like this: 2620:0aba2:0d01:2042:0100:8c4d:d370:72b4.

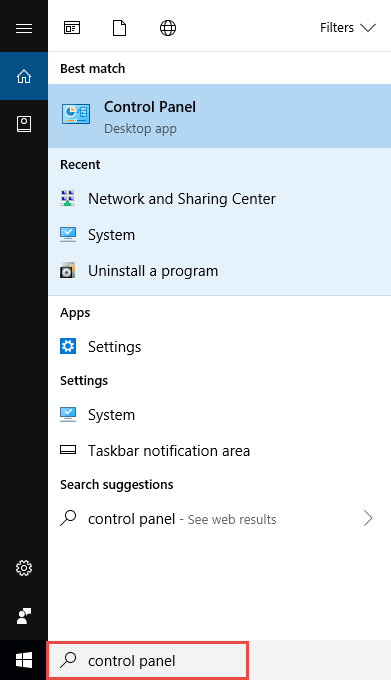
**How to set IP addresses to the computer systems in a LAN:**

**Step 1: Open the Control Panel**

Press “**Windows**+ **R**”, then a **Run** box comes out. Input **control panel** and press **Enter** to open the control panel.

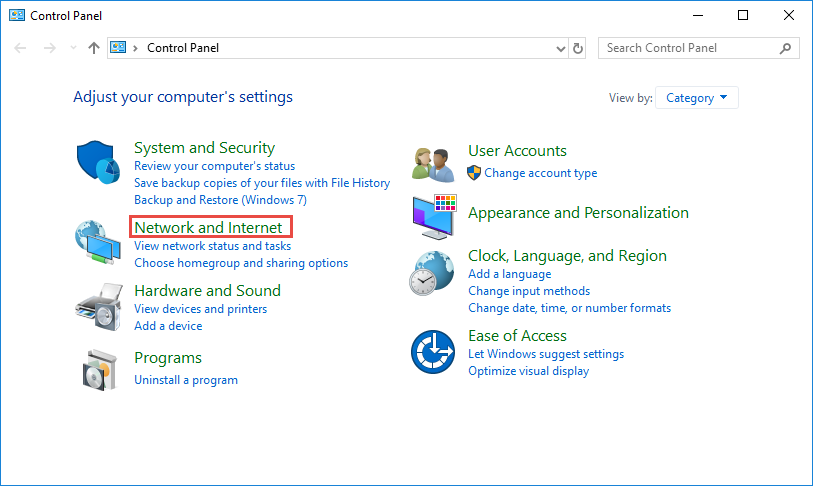


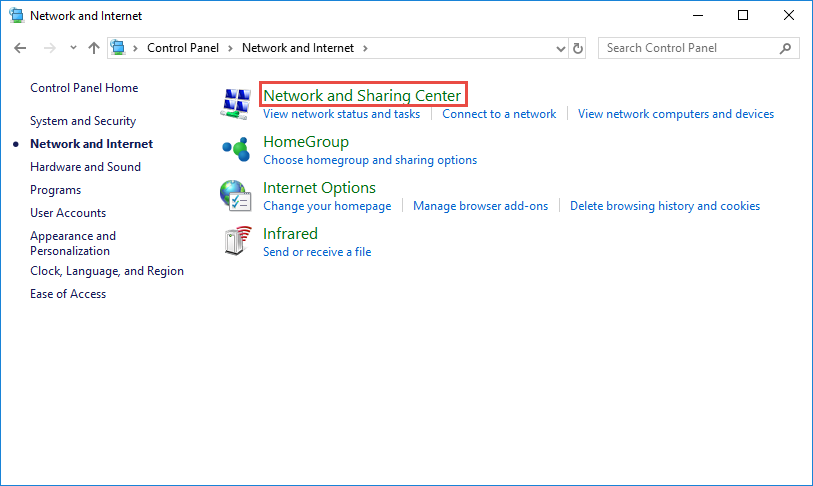
You can also type **control panel** in the search bar at the lower left of the screen and press **Enter** to open the control panel.



**Step 2: Go to Network Connections**

Go to **Network and Internet** >**Network and Sharing Center**.



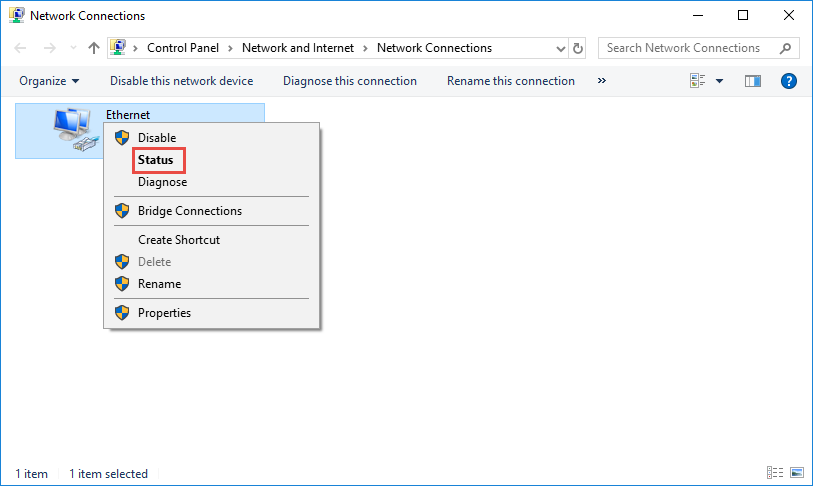


Select **Change adapter settings** on the left.

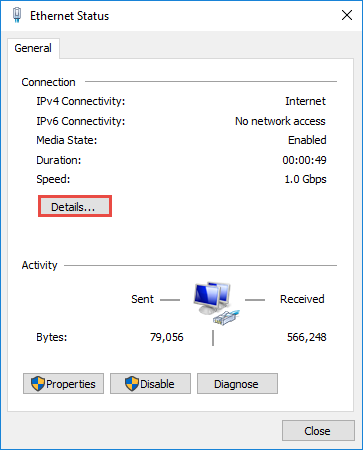


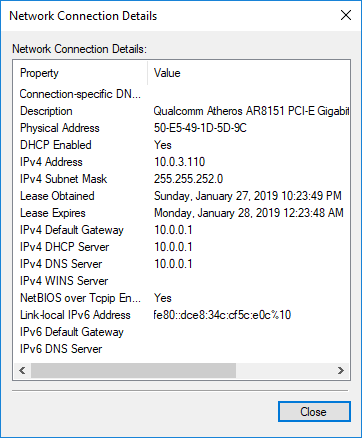
**Step 3: Find the IP address**

Right click the **Ethernet** icon and select **Status** from the context menu.



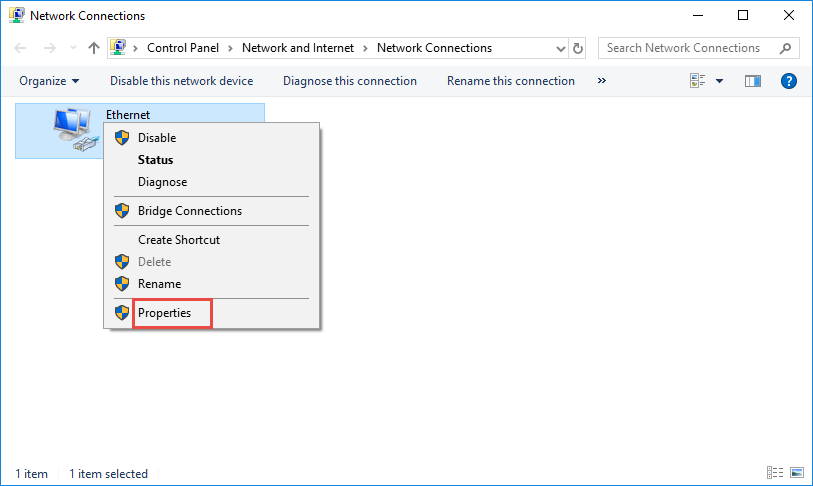
Then click **Details...** to view all detailed information of network connection.



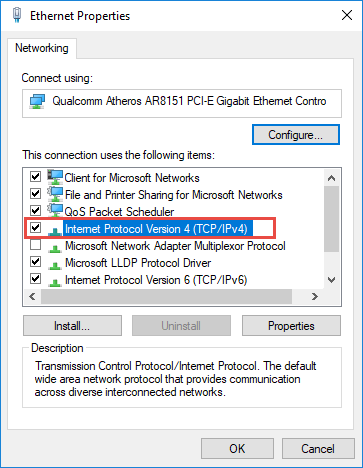


**Step 4: Set the IP address**

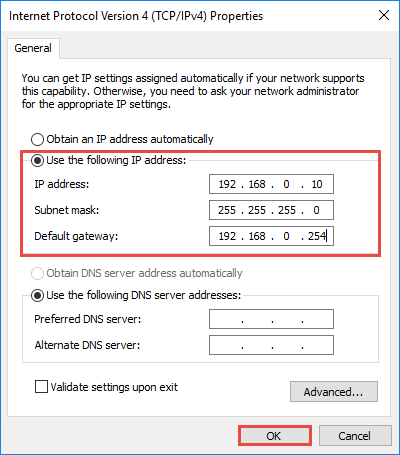
Right Click **Local Area Connection** and select **Properties**.



Then double click **Internet Protocol Version 4 (TCP/IPv4)**.



Select **Use the Following IP address:** and type in the **IP address**, **Subnet mask** and **Default gateway**. Click **OK** to apply the settings.



**Note**: If you need to set a static DNS server, select **Use the following DNS server address**: and input the address of DNS server. By default, the computer

obtains the address automatically

**CYBERSECURITY CONCEPTS:**

**SYMMETRIC KEY ENCRYPTION TECHNIQUES**

**EXP 12: perform encryption and decryption by using Caesar Cipher technique**

def caesar\_encrypt(plaintext, shift):

result = ""

for char in plaintext:

if char.isalpha():

shift\_base = 65 if char.isupper() else 97

result += chr((ord(char) - shift\_base + shift) % 26 + shift\_base)

else:

result += char

return result

def caesar\_decrypt(ciphertext, shift):

return caesar\_encrypt(ciphertext, -shift)

# Example usage

plaintext = "HELLO"

shift = 3

ciphertext = caesar\_encrypt(plaintext, shift)

print("Ciphertext:", ciphertext)

decrypted = caesar\_decrypt(ciphertext, shift)

print("Decrypted:", decrypted)

**Out Put:**

**Ciphertext: KHOOR**

**Decrypted: HELLO**

### ****How the Encryption Works (Example with "HELLO" and Shift = 3):****

| **Plaintext** | **H** | **E** | **L** | **L** | **O** |
| --- | --- | --- | --- | --- | --- |
| ASCII | 72 | 69 | 76 | 76 | 79 |
| Shifted | 75 | 72 | 79 | 79 | 82 |
| Ciphertext | K | H | O | O | R |

Each letter is shifted by **3 places forward**, and decryption shifts it **back by 3**.

**EXP 13: Exercise encryption and decryption by using Play fair Cipher technique**

def create\_playfair\_matrix(key):

matrix = []

key = ''.join(sorted(set(key.upper()), key=lambda x: key.index(x))) # Remove duplicates and maintain order

alphabet = "ABCDEFGHIKLMNOPQRSTUVWXYZ" # 'I' and 'J' are treated the same

key = key + alphabet

for char in key:

if char not in matrix:

matrix.append(char)

return matrix

def playfair\_encrypt(plaintext, key):

matrix = create\_playfair\_matrix(key)

plaintext = ''.join([c.upper() for c in plaintext if c.isalpha()])

if len(plaintext) % 2 != 0: # If odd length, add a filler letter

plaintext += 'X'

pairs = []

for i in range(0, len(plaintext), 2):

if plaintext[i] == plaintext[i + 1]: # If the same letter, add a filler

pairs.append(plaintext[i] + 'X')

else:

pairs.append(plaintext[i] + plaintext[i + 1])

ciphertext = ""

for pair in pairs:

row1, col1 = divmod(matrix.index(pair[0]), 5)

row2, col2 = divmod(matrix.index(pair[1]), 5)

if row1 == row2: # Same row

ciphertext += matrix[row1 \* 5 + (col1 + 1) % 5]

ciphertext += matrix[row2 \* 5 + (col2 + 1) % 5]

elif col1 == col2: # Same column

ciphertext += matrix[((row1 + 1) % 5) \* 5 + col1]

ciphertext += matrix[((row2 + 1) % 5) \* 5 + col2]

else: # Rectangle

ciphertext += matrix[row1 \* 5 + col2]

ciphertext += matrix[row2 \* 5 + col1]

return ciphertext

def playfair\_decrypt(ciphertext, key):

matrix = create\_playfair\_matrix(key)

pairs = [ciphertext[i:i + 2] for i in range(0, len(ciphertext), 2)]

plaintext = ""

for pair in pairs:

row1, col1 = divmod(matrix.index(pair[0]), 5)

row2, col2 = divmod(matrix.index(pair[1]), 5)

if row1 == row2: # Same row

plaintext += matrix[row1 \* 5 + (col1 - 1) % 5]

plaintext += matrix[row2 \* 5 + (col2 - 1) % 5]

elif col1 == col2: # Same column

plaintext += matrix[((row1 - 1) % 5) \* 5 + col1]

plaintext += matrix[((row2 - 1) % 5) \* 5 + col2]

else: # Rectangle

plaintext += matrix[row1 \* 5 + col2]

plaintext += matrix[row2 \* 5 + col1]

return plaintext

# Example usage

key = "KEYWORD"

plaintext = "HELLO"

ciphertext = playfair\_encrypt(plaintext, key)

print("Ciphertext:", ciphertext)

decrypted = playfair\_decrypt(ciphertext, key)

print("Decrypted:", decrypted)

**Out put:**

**Ciphertext: GYIZWZ**

**Decrypted: HELXOX**

**EXP 14:Exercise encryption and decryption by using Hill Cipher technique**

import numpy as np

def matrix\_inverse(matrix, mod=26):

det = int(np.linalg.det(matrix)) % mod

det\_inv = pow(det, -1, mod)

matrix\_adj = np.round(det\_inv \* np.linalg.det(matrix) \* np.linalg.inv(matrix)).astype(int) % mod

return matrix\_adj

def hill\_encrypt(plaintext, key\_matrix):

# Clean the plaintext

plaintext = ''.join([char.upper() for char in plaintext if char.isalpha()])

# If plaintext is odd-length, add padding

if len(plaintext) % 2 != 0:

plaintext += 'X'

# Convert letters to numbers

plaintext\_nums = [ord(char) - 65 for char in plaintext]

ciphertext\_nums = []

for i in range(0, len(plaintext\_nums), 2):

pt\_vector = np.array([[plaintext\_nums[i]], [plaintext\_nums[i + 1]]])

encrypted = np.dot(key\_matrix, pt\_vector) % 26

ciphertext\_nums.append(encrypted[0][0])

ciphertext\_nums.append(encrypted[1][0])

# Convert numbers back to letters

ciphertext = ''.join([chr(num + 65) for num in ciphertext\_nums])

return ciphertext

def hill\_decrypt(ciphertext, key\_matrix):

# Compute inverse of the key matrix

key\_inv = matrix\_inverse(key\_matrix)

ciphertext\_nums = [ord(char) - 65 for char in ciphertext]

plaintext\_nums = []

for i in range(0, len(ciphertext\_nums), 2):

ct\_vector = np.array([[ciphertext\_nums[i]], [ciphertext\_nums[i + 1]]])

decrypted = np.dot(key\_inv, ct\_vector) % 26

plaintext\_nums.append(decrypted[0][0])

plaintext\_nums.append(decrypted[1][0])

plaintext = ''.join([chr(num + 65) for num in plaintext\_nums])

return plaintext

# Example usage

key\_matrix = np.array([[6, 24], [1, 16]]) # Example 2x2 matrix for Hill Cipher

plaintext = "HELLO"

ciphertext = hill\_encrypt(plaintext, key\_matrix)

print("Ciphertext:", ciphertext)

decrypted = hill\_decrypt(ciphertext, key\_matrix)

print("Decrypted:", decrypted)

**OUT PUT:**

**Ciphertext: OFSFSG**

**Decrypted: HELLO**

**EXP 15: perform encryption and decryption by using Vigenere Cipher**

# Function to encrypt the message

def vigenere\_encrypt(plaintext, key):

encrypted\_text = []

key = key.lower()

key\_index = 0

for char in plaintext:

if char.isalpha():

shift = ord(key[key\_index % len(key)]) - ord('a')

if char.islower():

encrypted\_char = chr(((ord(char) - ord('a') + shift) % 26) + ord('a'))

elif char.isupper():

encrypted\_char = chr(((ord(char) - ord('A') + shift) % 26) + ord('A'))

encrypted\_text.append(encrypted\_char)

key\_index += 1

else:

encrypted\_text.append(char) # Non-alphabetic characters remain unchanged

return ''.join(encrypted\_text)

# Function to decrypt the message

def vigenere\_decrypt(ciphertext, key):

decrypted\_text = []

key = key.lower()

key\_index = 0

for char in ciphertext:

if char.isalpha():

shift = ord(key[key\_index % len(key)]) - ord('a')

if char.islower():

decrypted\_char = chr(((ord(char) - ord('a') - shift) % 26) + ord('a'))

elif char.isupper():

decrypted\_char = chr(((ord(char) - ord('A') - shift) % 26) + ord('A'))

decrypted\_text.append(decrypted\_char)

key\_index += 1

else:

decrypted\_text.append(char) # Non-alphabetic characters remain unchanged

return ''.join(decrypted\_text)

# Example usage

if \_name\_ == "\_main\_":

plaintext = "Hello World!"

key = "KEY"

encrypted = vigenere\_encrypt(plaintext, key)

print("Encrypted:", encrypted)

decrypted = vigenere\_decrypt(encrypted, key)

print("Decrypted:", decrypted)

**Out put:**

**Encrypted: Rijvs Uyvjn!**

**Decrypted: Hello World!**

The Vigenère cipher is a method of encrypting alphabetic text by using a simple form of polyalphabetic substitution. It employs a keyword to shift letters of the plaintext, making it more resistant to frequency analysis than simpler ciphers like the Caesar cipher.

**Encryption Process:**

**Preparation:**

* 1. **Plaintext:** The original message to be encrypted.
  2. **Key:** A chosen word or phrase used for encryption.

**Repeat the Key:** Extend the key so that its length matches the length of the plaintext. For example, if the plaintext is "attackatdawn" and the key is "LEMON", repeat the key to get "LEMONLEMONLE".

**Encrypt Each Letter:**

* 1. For each letter in the plaintext, determine its position in the alphabet (A=0, B=1, ..., Z=25).
  2. Do the same for the corresponding letter in the extended key.
  3. Shift the plaintext letter forward in the alphabet by the number of positions indicated by the key letter.
  4. If the end of the alphabet is surpassed, wrap around to the beginning.

**Decryption Process:**

**Preparation:**

* 1. Use the same extended key as in the encryption process.

**Decrypt Each Letter:**

* 1. For each letter in the ciphertext, determine its position in the alphabet.
  2. Subtract the position value of the corresponding key letter.
  3. If the result is negative, wrap around to the end of the alphabet.

**Example:**

* **Plaintext:** attackatdawn
* **Key:** LEMON
* **Extended Key:** LEMONLEMONLE
* **Ciphertext:** LXFOPVEFRNHR

**Encryption Steps:**

| **Plaintext Letter** | **Key Letter** | **Shift** | **Ciphertext Letter** |
| --- | --- | --- | --- |
| a | L | 11 | l |
| t | E | 4 | x |
| t | M | 12 | f |
| a | O | 14 | o |
| c | N | 13 | p |
| k | L | 11 | v |
| a | E | 4 | e |
| t | M | 12 | f |
| d | O | 14 | r |
| a | N | 13 | n |
| w | L | 11 | h |
| n | E | 4 | r |

**Decryption Steps:**

| **Ciphertext Letter** | **Key Letter** | **Shift** | **Plaintext Letter** |
| --- | --- | --- | --- |
| l | L | -11 | a |
| x | E | -4 | t |
| f | M | -12 | t |
| o | O | -14 | a |
| p | N | -13 | c |
| v | L | -11 | k |
| e | E | -4 | a |
| f | M | -12 | t |
| r | O | -14 | d |
| n | N | -13 | a |
| h | L | -11 | w |
| r | E | -4 | n |

**Security Considerations:**

While the Vigenère cipher was once considered secure, it is vulnerable to cryptanalysis, especially if the key is short or reused. Techniques such as the Kasiski examination and the Friedman test can be used to determine the key length and ultimately decrypt the message without knowing the key.

For enhanced security, it's crucial to use a long, non-repeating key, ideally as long as the plaintext itself. This approach transforms the Vigenère cipher into a one-time pad, which is theoretically unbreakable when the key is truly random and used only once.

In modern times, the Vigenère cipher is primarily of historical interest and is not used for serious encryption purposes due to its vulnerabilities.

**ASYMMETRIC KEY ENCRYPTION TECHNIQUES**

**EXP16 :Perform encryption and decryption using RSA public and private key.**

**!pip install pycryptodome**

from Crypto.PublicKey import RSA

from Crypto.Cipher import PKCS1\_OAEP

from Crypto.Random import get\_random\_bytes

from Crypto.Signature import pkcs1\_15

from Crypto.Hash import SHA256

# Generate RSA keys (public and private)

def generate\_rsa\_keys():

key = RSA.generate(2048) # 2048-bit key

private\_key = key.export\_key() # Export private key

public\_key = key.publickey().export\_key() # Export public key

return private\_key, public\_key

# Encrypt the message using the public key

def encrypt\_message(public\_key, message):

rsa\_key = RSA.import\_key(public\_key)

cipher = PKCS1\_OAEP.new(rsa\_key)

encrypted\_message = cipher.encrypt(message.encode())

return encrypted\_message

# Decrypt the message using the private key

def decrypt\_message(private\_key, encrypted\_message):

rsa\_key = RSA.import\_key(private\_key)

cipher = PKCS1\_OAEP.new(rsa\_key)

decrypted\_message = cipher.decrypt(encrypted\_message)

return decrypted\_message.decode()

# Digital Signature (sign a message with private key)

def sign\_message(private\_key, message):

rsa\_key = RSA.import\_key(private\_key)

h = SHA256.new(message.encode()) # Hash the message

signature = pkcs1\_15.new(rsa\_key).sign(h)

return signature

# Verify the digital signature (verify with public key)

def verify\_signature(public\_key, message, signature):

rsa\_key = RSA.import\_key(public\_key)

h = SHA256.new(message.encode()) # Hash the message

try:

pkcs1\_15.new(rsa\_key).verify(h, signature)

return True # Signature is valid

except (ValueError, TypeError):

return False # Signature is invalid

# Example usage

if \_name\_ == "\_main\_":

# Generate RSA keys (private and public)

private\_key, public\_key = generate\_rsa\_keys()

print("Private Key: ", private\_key.decode())

print("Public Key: ", public\_key.decode())

# Message to encrypt and sign

message = "This is a secret message."

# Encrypt and Decrypt

encrypted = encrypt\_message(public\_key, message)

print("\nEncrypted Message: ", encrypted)

decrypted = decrypt\_message(private\_key, encrypted)

print("\nDecrypted Message: ", decrypted)

# Sign the message

signature = sign\_message(private\_key, message)

print("\nSignature: ", signature)

# Verify the signature

is\_valid = verify\_signature(public\_key, message, signature)

print("\nIs the signature valid? ", is\_valid)

**Out put:**

**EXP 17: To perform the validation of the digital document using Digital signature standard encryptionand decryption.**

**!pip install cryptography**

from cryptography.hazmat.primitives.asymmetric import dsa

from cryptography.hazmat.primitives import hashes

# Step 1: Generate Key Pair

private\_key = dsa.generate\_private\_key(key\_size=2048)

public\_key = private\_key.public\_key()

# Step 2: Sign the Document

document = b"Hello, this is a digitally signed document!"

# Create a hash of the document

hasher = hashes.Hash(hashes.SHA256())

hasher.update(document)

document\_hash = hasher.finalize()

# Sign the document hash with DSA private key

signature = private\_key.sign(

document, # Original document, not the hash

hashes.SHA256() # Specify the hashing algorithm

)

# Step 3: Send (Document + Signature)

sent\_document = document

sent\_signature = signature

# Step 4: Verify Signature

try:

public\_key.verify(

sent\_signature, # Received signature

sent\_document, # Original document

hashes.SHA256() # Use the same hashing algorithm

)

print("✅ Signature is VALID. Document is authentic!")

except:

print("❌ Signature is INVALID. Document may be altered!")

**Out put:**

✅ Signature is VALID. Document is authentic!

❌ Signature is INVALID. Document may be altered!

**EXP18: To perform the procedure of installation process of antivirus to detect threats.**

Installing an antivirus is essential to protect your computer from malware, viruses, and other threats. Here’s a step-by-step guide:

## ****Step 1: Choose a Reliable Antivirus Software****

Some popular antivirus options:  
✅ **Free Antivirus:** Windows Defender (built-in), Avast, AVG.  
✅ **Paid Antivirus:** Norton, Bitdefender, McAfee, Kaspersky.

🔹 Visit the official website of the antivirus provider.  
🔹 Download the latest version for **Windows/macOS/Linux**.

**Example Websites:**

* **Windows Defender:** (Pre-installed on Windows 10/11)
* **Bitdefender:**[www.bitdefender.com](https://www.bitdefender.com)
* **McAfee:**[www.mcafee.com](https://www.mcafee.com)
* **Kaspersky:**[www.kaspersky.com](https://www.kaspersky.com)

## ****Step 2: Install the Antivirus Software****

1️⃣ Locate the downloaded **setup file** (e.g., antivirus\_setup.exe).  
2️⃣ Double-click to run the installation.  
3️⃣ Follow the **on-screen instructions**:  
✅ Accept Terms & Conditions  
✅ Choose **Standard** or **Custom Installation**  
✅ Allow the software to install necessary updates

## ****Step 3: Activate and Update the Antivirus****

1️⃣ After installation, **restart your computer** (if prompted).  
2️⃣ Open the antivirus application.  
3️⃣ **Sign in/Register** (if required).  
4️⃣ Update the virus database to get the latest security patches.

## ****Step 4: Perform a Full System Scan****

1️⃣ Open the **antivirus dashboard**.  
2️⃣ Click on **“Scan” or “Run a Full Scan”**.  
3️⃣ Wait for the scan to complete (this may take several minutes).  
4️⃣ The antivirus will show a **report of detected threats**.

✅ **Options if a threat is detected:**

* **Quarantine:** Isolates the infected file.
* **Delete:** Removes the malicious file permanently.
* **Ignore:** Keeps the file (not recommended unless sure it’s safe).

## ****Step 5: Enable Real-Time Protection****

1️⃣ Go to **Settings** in your antivirus.  
2️⃣ Turn on **Real-Time Protection** (if not enabled by default).  
3️⃣ Enable **Firewall Protection** for extra security.

## ****Step 6: Schedule Automatic Scans (Recommended)****

1️⃣ Open your antivirus settings.  
2️⃣ Set up **daily/weekly automatic scans**.  
3️⃣ Ensure automatic updates are enabled.

## ****Step 7: Keep Your System Safe****

✅ **Avoid downloading files** from unknown sources.  
✅ **Do not open suspicious email attachments**.  
✅ **Keep software updated** (OS, antivirus, browsers).

### ****Expected Output****

**If no threats are found:**

Your systemis clean! No threats detected.

**If threats are found:**

Warning: 5 threats detected!

[Action Required] Quarantine orDelete infected files.

## ****Conclusion****

By following these steps, your system stays protected from **viruses, malware, and cyber threats**.

**EXP 19: Learn the procedure to ensure security basic firewalls can be enabled in the system.**

Step-by-Step Procedure to Enable Windows Firewall for System Security

The Windows Defender Firewall is a built-in security feature in Windows that helps protect your system from unauthorized access, malware, and cyber threats. Here’s how to enable and configure it properly.

Step 1: Open Windows Security Settings

Press Win + S and type Windows Security, then press Enter.

Click on Firewall & network protection.

Step 2: Enable Firewall for All Networks

1. In the Firewall & network protection window, you will see three network types:

✅ Domain network (Used in office environments)

✅ Private network (For trusted home networks)

✅ Public network (For public Wi-Fi & untrusted networks)

1. Click on each network type and ensure Microsoft Defender Firewall is turned ON.

Expected Output:

Windows Defender Firewall is enabled for all networks.

Step 3: Enable Firewall via Control Panel (Alternative Method)

Open Control Panel (Win + R, type control, and press Enter).

Navigate to System and Security → Windows Defender Firewall.

Click Turn Windows Defender Firewall ON or OFF (on the left panel).

Select Turn On Firewall for both Private and Public networks.

Click OK to apply changes.

Step 4: Allow or Block Specific Apps Through Firewall

Go to Windows Security → Firewall & Network Protection.

Click Allow an app through firewall.

Click Change settings and check/uncheck apps to allow/block them.

Click OK to save changes.

Example:

Allow Google Chrome through Private Network.

Block Remote Desktop Connection on Public Network for security.

Step 5: Configure Advanced Firewall Rules (Optional)

Open Windows Defender Firewall from the Control Panel.

Click on Advanced settings (on the left).

Here, you can:

Create inbound/outbound rules for specific ports and applications.

Block unknown incoming traffic for better security.

Monitor firewall logs for suspicious activities.

Example Commands (for Advanced Users)

To block port 23 (Telnet):

New-NetFirewallRule -DisplayName "Block Telnet" -Direction Inbound -Protocol TCP -LocalPort 23 -Action Block

To allow port 443 (HTTPS):

Edit

New-NetFirewallRule -DisplayName "Allow HTTPS" -Direction Inbound -Protocol TCP -LocalPort 443 -Action Allow

Step 6: Test Firewall Protection

Open Command Prompt and check firewall status:

netsh advfirewall show allprofiles

If enabled, it will show:

State: ON

Try pinging your system from another device:

ping <your-IP-address>

If the firewall is active, the request should time out.

Use network scanning tools like nmap (from another device):

nmap -Pn <your-IP-address>

It should show filtered ports if the firewall is enabled.

Step 7: Enable Firewall Notifications & Automatic Updates

Go to Windows Security → Firewall & Network Protection.

Click Firewall Notification Settings and turn ON alerts for blocked apps.

Ensure Windows is up-to-date by enabling Windows Update under Settings → Update & Security.

Conclusion:

By enabling and configuring the Windows Defender Firewall, you:

✅ Prevent unauthorized access to your system.

✅ Block malware and cyber threats.

✅ Control which apps can access the internet.