CHAPTER-1

COMPUTER NETWORK

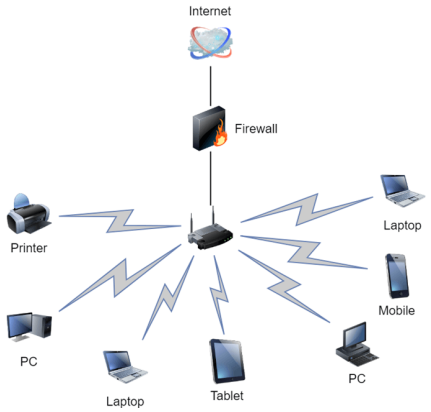
A computer network is a group of two or more interconnected computer systems. You can establish a network connection using either cable or wireless media. Every network involves hardware and software that connects computers and tools.

Advantages of a Computer Network

Here are the fundamental benefits of using Computer Networking :

- Helps you to connect with multiple computers together to send and receive information when accessing the network.
- Helps you to share printers, scanners, and email.
- Helps you to share information at very fast speed
- Electronic communication is more efficient and less expensive than without the network.

Computer Network Components :-



Switches

Switches work as a controller which connects computers, printers, and other hardware devices to a network in a campus or a building.

It allows devices on your network to communicate with each other, as well as with other networks. It helps you to share resources and reduce the costing of any organization.

Routers

Routers help you to connect with multiple networks. It enables you to share a single internet connection with multiple devices and saves money. This networking component acts as a dispatcher, which allows you to analyze data sent across a network. It automatically selects the best route for data to travel and send it on its way.

Servers:

Servers are computers that hold shared programs, files, and the network operating system. Servers allow access to network resources to all the users of the network.

Clients:
Clients are computer devices which access and uses the network as well as shares network resources. They are also users of the network, as they can send and receive requests from the server.

Transmission Media:
Transmission media is a carrier used to interconnect computers in a network, such as coaxial cable, twisted-pair wire, and optical fiber cable. It is also known as links, channels, or lines.

Access points
Access points allow devices to connect to the wireless network without cables. A wireless network allows you to bring new devices and provides flexible support to mobile users.

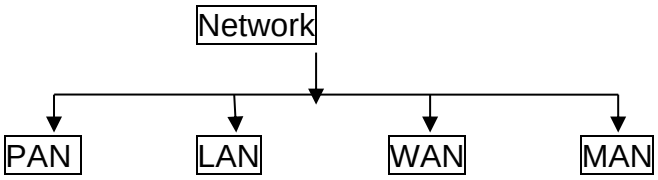
Shared Data:
Shared data are data which is shared between the clients such as data files, printer access programs, and email.

Network Interface Card:
Network Interface card sends, receives data, and controls data flow between the computer and the network.

Local Operating System:
A local OS which helps personal computers to access files, print to a local printer and uses one or more disk and CD drives which are located on the computer .

Types of Computer Networks

There are various types of computer networks are available. We can categorize them according to their size as well as their purpose.



PAN (Personal Area Network)

PAN is a computer network formed around a person. It generally consists of a computer, mobile, or personal digital assistant. PAN can be used for establishing communication among these personal devices for connecting to a digital network and the internet.

Characteristics of PAN

- It is mostly personal devices network equipped within a limited area.
- Allows you to handle the interconnection of IT devices at the surrounding of a single user.
- PAN includes mobile devices, tablet, and laptop.

- It can be wirelessly connected to the internet called WPAN.
- Appliances use for PAN: cordless mice, keyboards, and Bluetooth systems.

Advantages of PAN

Here, are important pros/benefits of using PAN network:

- PAN networks are relatively secure and safe
- It offers only short-range solution up to 10 meters
- Strictly restricted to a small area

Disadvantages of PAN

Here are important cons/ drawback of using PAN network:

- It may establish a bad connection to other networks at the same radio bands.
- Distance limits.

LAN (Local Are Network)

A **L**ocal **A**rea **N**etwork (LAN) is a group of computer and peripheral devices which are connected in a limited area such as school, laboratory, home, and office building. It is a widely useful network for sharing resources like files, printers, games, and other application. The simplest type of LAN network is to connect computers and a printer in someone's home or office. In general, LAN will be used as one type of transmission medium.

It is a network which consists of less than 5000 interconnected devices across several buildings.

Characteristics of LAN

Here are important characteristics of a LAN network:

- It is a private network, so an outside regulatory body never controls it.
- LAN operates at a relatively higher speed compared to other WAN systems.
- There are various kinds of media access control methods like token ring and Ethernet.

Advantages of LAN

Here are pros/benefits of using LAN:

- Computer resources like hard-disks, DVD-ROM, and printers can share local area networks. This significantly reduces the cost of hardware purchases.
- You can use the same software over the network instead of purchasing the licensed software for each client in the network.
- Data of all network users can be stored on a single hard disk of the server computer.

- You can easily transfer data and messages over networked computers.
- It will be easy to manage data at only one place, which makes data more secure.
- Local Area Network offers the facility to share a single internet connection among all the LAN users.

Disadvantages of LAN

Here are the important cons/ drawbacks of LAN:

- LAN will indeed save cost because of shared computer resources, but the initial cost of installing Local Area Networks is quite high.
- The LAN admin can check personal data files of every LAN user, so it does not offer good privacy.
- Unauthorized users can access critical data of an organization in case LAN admin is not able to secure centralized data repository.
- Local Area Network requires a constant LAN administration as there are issues related to software setup and hardware failures

WAN (Wider Area Network)

WAN (Wide Area Network) is another important computer network that which is spread across a large geographical area. WAN network system could be a connection of a LAN which connects with other LAN's using telephone lines and radio waves. It is mostly limited to an enterprise or an organization.

Characteristics of WAN:

- The software files will be shared among all the users; therefore, all can access to the latest files.
- Any organization can form its global integrated network using WAN.

Advantages of WAN

Here are the benefits/ pros of using WAN:

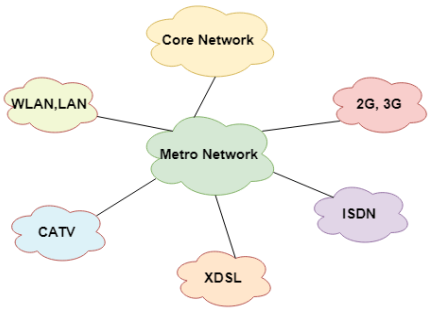
- WAN helps you to cover a larger geographical area. Therefore business offices situated at longer distances can easily communicate.
- Contains devices like mobile phones, laptop, tablet, computers, gaming consoles, etc.
- WLAN connections work using radio transmitters and receivers built into client devices.

Disadvantage of WAN

- The initial setup cost of investment is very high.
- It is difficult to maintain the WAN network. You need skilled technicians and network administrators.
- There are more errors and issues because of the wide coverage and the use of different technologies.

- It requires more time to resolve issues because of the involvement of multiple wired and wireless technologies.
- Offers lower security compared to other types of networks.

What is MAN?



A Metropolitan Area Network or MAN is consisting of a computer network across an entire city, college campus, or a small region. This type of network is large than a LAN, which is mostly limited to a single building or site. Depending upon the type of configuration, this type of network allows you to cover an area from several miles to tens of miles.

Characteristics of MAN

Here are important characteristics of the MAN network:

- It mostly covers towns and cities in a maximum 50 km range
- Mostly used medium is optical fibers, cables
- Data rates adequate for distributed computing applications.

Advantages of MAN

Here are pros/benefits of using MAN system:

- It offers fast communication using high-speed carriers, like fiber optic cables.
- It provides excellent support for an extensive size network and greater access to WANs.
- The dual bus in MAN network provides support to transmit data in both directions concurrently.
- A MAN network mostly includes some areas of a city or an entire city.

Disadvantages of MAN

Here are drawbacks/ cons of using the MAN network:

- You need more cable to establish MAN connection from one place to another.
- In MAN network it is tough to make the system secure from hackers .

CHAPTER-2

Topology

Network topologies describe the methods in which all the elements of a network are mapped. The topology term refers to both the physical and logical layout of a network.

Types of Networking Topologies
Two main types of networking topologies are 1) Physical topology 2) Logical topology

Physical topology:
This type of network is an actual layout of the computer cables and other network devices

Logical topology:
Logical topology gives insight's about network's physical design.

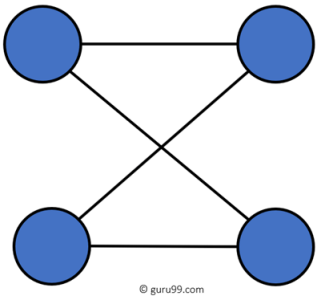
Different types of Physical Topologies are:

- P2P Topology
- Bus Topology
- Ring Topology
- Star Topology
- Tree Topology
- Mesh Topology
- Hybrid Topology

Point to Point
Point-to-point topology is the easiest of all the network topologies. In this method, the network consists of a direct link between two computers.

Advantages:

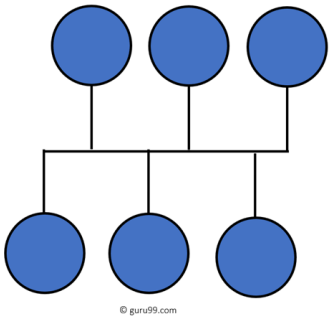
- This is faster and highly reliable than other types of connections since there is a direct connection.
- No need for a network operating system
- Does not need an expensive server as individual workstations are used to access the files
- No need for any dedicated network technicians because each user sets their permissions



Disadvantages:

- The biggest drawback is that it only be used for small areas where computers are in close proximity.
- You can't back up files and folders centrally
- There is no security besides the permissions. Users often do not require to log onto their workstations.

Bus Topology



Bus topology uses a single cable which connects all the included nodes. The main cable acts as a spine for the entire network. One of the computers in the network acts as the computer server. When it has two endpoints, it is known as a linear bus topology.

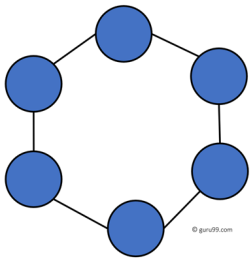
Advantages:
Here are pros/benefits of using a bus topology:

- Cost of the cable is very less as compared to other topology, so it is widely used to build small networks.
- Famous for LAN network because they are inexpensive and easy to install.
- It is widely used when a network installation is small, simple, or temporary.
- It is one of the passive topologies. So computers on the bus only listen for data being sent, that are not responsible for moving the data from one computer to others.

Disadvantages:
Here are the cons/drawbacks of bus topology:

- In case if the common cable fails, then the entire system will crash down.
- When network traffic is heavy, it develops collisions in the network.
- Whenever network traffic is heavy, or nodes are too many, the performance time of the network significantly decreases.
- Cables are always of a limited length.

Ring Topology



In a ring network, every device has exactly two neighboring devices for communication purpose. It is called a ring topology as its formation is like a ring. In this topology, every computer is connected to another computer. Here, the last node is combined with a first one.

This topology uses token to pass the information from one computer to another. In this topology, all the messages travel through a ring in the same direction.

Advantages:
Here are pros/benefits of ring topology:

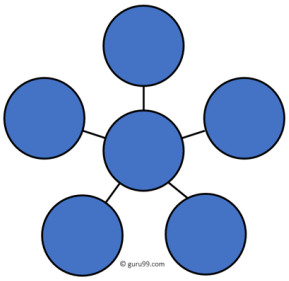
- Easy to install and reconfigure.
- Adding or deleting a device in-ring topology needs you to move only two connections.
- The troubleshooting process is difficult in a ring topology.
- Failure of one computer can disturb the whole network.
- Offers equal access to all the computers of the networks
- Faster error checking and acknowledgment.

Disadvantages:
Here are drawbacks/cons of ring topology:

- Unidirectional traffic.
- Break in a single ring can risk the breaking of the entire network
- Modern days high-speed LANs made this topology less popular.
- In the ring, topology signals are circulating at all times, which develops unwanted power consumption.
- It is very difficult to troubleshoot the ring network.
- Adding or removing the computers can disturb the network activity.

Star Topology

In the star topology, all the computers connect with the help of a hub. This cable is called a central node, and all other nodes are connected using this central node. It is most popular on LAN networks as they are inexpensive and easy to install.



Advantages:

- Easy to troubleshoot, set up, and modify.
- Only those nodes are affected, that has failed. Other nodes still work.
- Fast performance with few nodes and very low network traffic.
- In Star topology, addition, deletion, and moving of the devices are easy.

Disadvantages:

Here are cons/drawbacks of using Star:

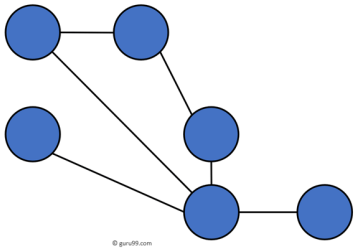
- If the hub or concentrator fails, attached nodes are disabled.
- Cost of installation of star topology is costly.
- Heavy network traffic can sometimes slow the bus considerably.
- Performance depends on the hub's capacity
- A damaged cable or lack of proper termination may bring the network down.

Mesh Topology

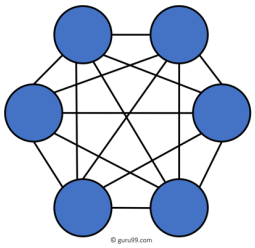
The mesh topology has a unique network design in which each computer on the network connects to every other. It is develops a P2P (point-to-point) connection between all the devices of the network. It offers a high level of redundancy, so even if one network cable fails, still data has an alternative path to reach its destination.

Types of Mesh Topology:

- **Partial Mesh Topology:** In this type of topology, most of the devices are connected almost similarly as full topology. The only difference is that few devices are connected with just two or three devices.



- **Full Mesh Topology:** In this topology, every nodes or device are directly connected with each other.



Advantages:

Here, are benefits of Mesh topology

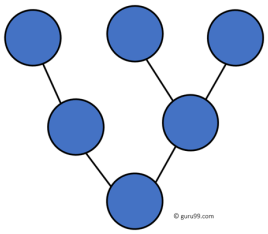
- The network can be expanded without disrupting current users.
- Need extra capable compared with other LAN topologies.
- Complicated implementation.
- No traffic problem as nodes has dedicated links.
- It has multiple links, so if any single route is blocked, then other routes should be used for data communication.
- P2P links make the fault identification isolation process easy.
- It helps you to avoid the chances of network failure by connecting all the systems to a central node.

Disadvantages:

- Installation is complex because every node is connected to every node.
- Dedicated links help you to eliminate the traffic problem.
- A mesh topology is robust.
- Every system has its privacy and security
- It is expensive due to the use of more cables. No proper utilization of systems.
- It requires more space for dedicated links.
- Because of the amount of cabling and the number of input-outputs, it is expensive to implement.
- It requires a large space to run the cables.

Tree Topology

Tree topologies have a root node, and all other nodes are connected which form a hierarchy. So it is also known as hierarchical topology. This topology integrates various star topologies together in a single bus, so it is known as a Star Bus topology. Tree topology is a very common network which is similar to a bus and star topology.



Advantages:

Here are pros/benefits of tree topology:

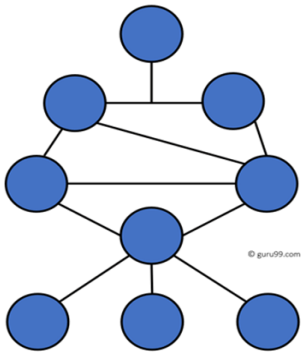
- Failure of one node never affects the rest of the network.
- Node expansion is fast and easy.
- Detection of error is an easy process
- It is easy to manage and maintain

Disadvantages:

Here are cons/drawback of tree topology:

- It is heavily cabled topology
- If more nodes are added, then its maintenance is difficult
- If the hub or concentrator fails, attached nodes are also disabled.

Hybrid Topology



Hybrid topology combines two or more topologies. You can see in the above architecture in such a manner that the resulting network does not exhibit one of the standard topologies.

For example, as you can see in the above image that in an office in one department, Star and P2P topology is used. A hybrid topology is always produced when two different basic network topologies are connected.

Advantages:

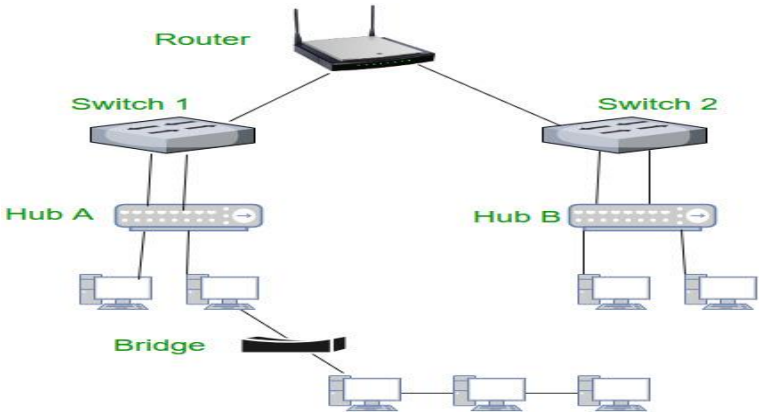
Here, are advantages/pros using Hybrid topology:

- Offers the easiest method for error detecting and troubleshooting
- Highly effective and flexible networking topology
- It is scalable so you can increase your network size

Disadvantages:

- The design of hybrid topology is complex
- It is one of the costliest processes

CHAPTER-3
Network Communication Devices



1. Repeater

A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

2. Hub

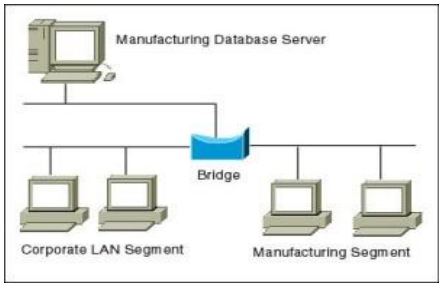
A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices.

Types of Hub

- **Active Hub:-** These are the hubs which have their own power supply and can clean, boost and relay the signal along with the network. It serves both as a repeater as well as wiring centre. These are used to extend the maximum distance between nodes.
- **Passive Hub :-** These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.

3. Bridge

A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.



4. Switch

A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

5. Routers

A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

6. Gateway –

A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

CHAPTER-4
CABLES & CONNECTORS

CABLES

Network cables are used to connect two or more computers or networking devices in a network. There are three types of network cables; coaxial, twisted-pair, and fiber-optic.

TYPES OF CABLES

COAXIAL CABLE –

It is a type of electrical cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Coaxial cable is a type of transmission line, used to carry high frequency electrical signals with low losses. It is used in such applications as telephone trunk lines, broadband internet networking cables, high speed computer data busses, carrying cable television signals, and connecting radio transmitters & receivers to their antennas.

Twisted Pair :-

Cable has pairs of wires with each pair twisted to eliminate electromagnetic interference and prevent crosstalk; each pair forms a circuit which can transmit data. At each end of the cable RJ-45 connectors are installed, The RJ-45 is an eight-wire connector used commonly to connect computers onto an Ethernet local-area network (LAN).

There are two sub-categories of Twisted Pair Cables as mentioned below

- Unshielded Twisted Pair Cable (UTP)
- Shielded Twisted Pair Cable (STP)

Unshielded Twisted Pair Cable (UTP) :-

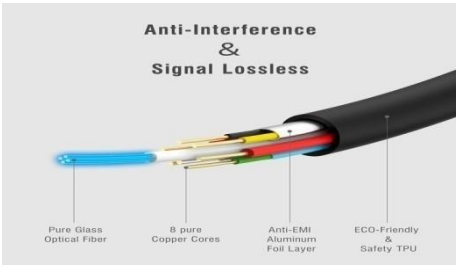
It is the most common type of cable used in networks. Almost all Ethernet LANs are built using UTP cables. UTP cables are thin and flexible and very cost effective which makes them the ideal choice for Ethernet cabling.

Shielded Twisted Pair Cable (STP) :-

It wraps each pair of wire in a metallic foil and further wraps all four pairs of wires in a metallic braid or foil, this further reduces the noise both within the cable from outside the cable. STP cable is more expensive then UTP cable and is much more difficult to install and manage. It also requires grounding at both ends of the metallic shield.

Fiber-Optic cable :-

A **fiber-optic cable**, also known as an **optical-fiber cable**, is an assembly similar to an electrical cable, but containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable[1] are used for different applications, for example, long distance telecommunication, or providing a high-speed data connection between different parts of a building.

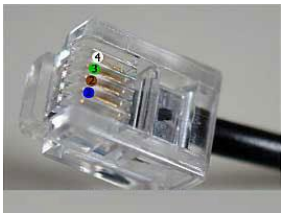


Connector

A device that terminates a segment of cabling or provides a point of entry for networking devices such as computers, hubs, and routers. Connectors can be distinguished according to their physical appearance and mating properties, such as jacks and plugs (male connectors) or sockets and ports (female connectors). They can also be distinguished by their different pinning configurations, such as DB9 and DB15 connectors, which have 9 and 15 pins, respectively.

Types of connectors

- **RJ11 (Registered Jack)**



RJ11 was originally designed by phone companies in the 70's and is used for analog voice lines. It is the standard telephone cable connectors; **RJ-11** has 4 wires.

- **RJ-45 (Registered Jack)**

The **RJ-45** connector is an eight-wire connector that is commonly used to connect computers to a local area network (LAN), particularly Ethernet LANs. Although they are slightly larger than the more commonly used **RJ-11** connectors,

- **SC/ ST**

SC/ST connectors are used for connecting fiber-optic cabling to networking devices. One is for transmitting data, and one is for receiving data. SC stands for subscriber connector / standard connector and ST stands for straight tip.

SC connector

ST connector

- **BNC (Bayonet Neill–Concelman)**

BNC connectors are attached to the ends of coaxial cables and can be used for connecting signals. On computer monitors, BNC connectors may be used as an alternative to VGA connectors in order to improve the quality of the video. BNC connectors can connect both analog and digital signals.

CHAPTER-5

OVERVIEW OF FRONT PANEL & BACK PANEL OF CPU

Front panel

- CD drive-This is the drive where any external CD/DVD can be inserted.
- Floppy disk drive - This the drive where any external floppy can be inserted.
- Power button - It is the button where the power can supply in to the system.
- Reset button – It is to restart the system.
- USB ports – It is used to attach any keyboard, mouse, printer, pen drive etc.
- Headphone / Mic port – it is use to attach headphone or speaker.
- Led - It is the indicator which shows the power supply current is going on into the system.

Back panel

- SMPS/Power supply – (switch mode power supply) It is having the 3 pin power connector, to supply AC current in to the system. This unit provides all the electrical power needed by all the components of the computer.

- Power supply cooling Fan – This fan cool the smps.

- PS/2 connector – This is 6 pin female port used to connect kbd and mouse.

- Serial com port – This is 9 pin male port used to connect kbd.

- VGA port – This is 15 pin female port used to connect VGA cable.

- Parallel port – This is 25 pin female port used to connect printer.

- USB port - This port can connect up to 127 peripherals (such as mouse, keyboard, printer, pendrive etc.) at once.

- RJ-45 LAN port – The Ethernet port accepts an Ethernet cable which allows you to communicate on a network that runs transmission control protocol/internet protocol (TCP/IP).

- Audio Jack - Mike in port (pink), Audio/Speaker output (green), Line in port (Blue)
- Expansion slots - An **expansion slot** is a socket on the motherboard that is **used** to insert an **expansion** card (or circuit board), which provides additional features to a computer such as video, sound, advanced graphics, Ethernet or memory.

- RJ 11 – Telephone modem card with RJ-11 female connectors to phone line and telephone. (broad band connection)

TYPES OF SWITCHES, PORTS & CONNECTORS OF CPU

Keyboard & Mouse : This Port is used to connect keyboard and mouse , now a day we use USB connector for keyboard and mouse

Serial or COM : It used to connect some types of modem, scanner, or digital camera

Parallel or Printer : You plug your printer into the parallel, or printer, port. But now printers may use a USB port

USB : Designed to replace older Serial and Parallel ports, the USB (Universal Serial Bus) can connect computers with a number of devices, such as printers, keyboards, mice, scanners, digital cameras, PDAs, and more

Video or Monitor : It used to connect your monitor into the video port

Line Out : It used to connect speakers or headphone into the Line Out jack

Line In : The Line In jack allows you to listen to your computer using a stereo system

Microphone : It used to connect a microphone into this jack to record sounds on your computer

Joystick or Game : If you have a joystick, musical (MIDI) keyboard, or other gaming device, this is where you plug it in

Phone or Modem : The phone or modem jack is where you plug your computer into a phone line

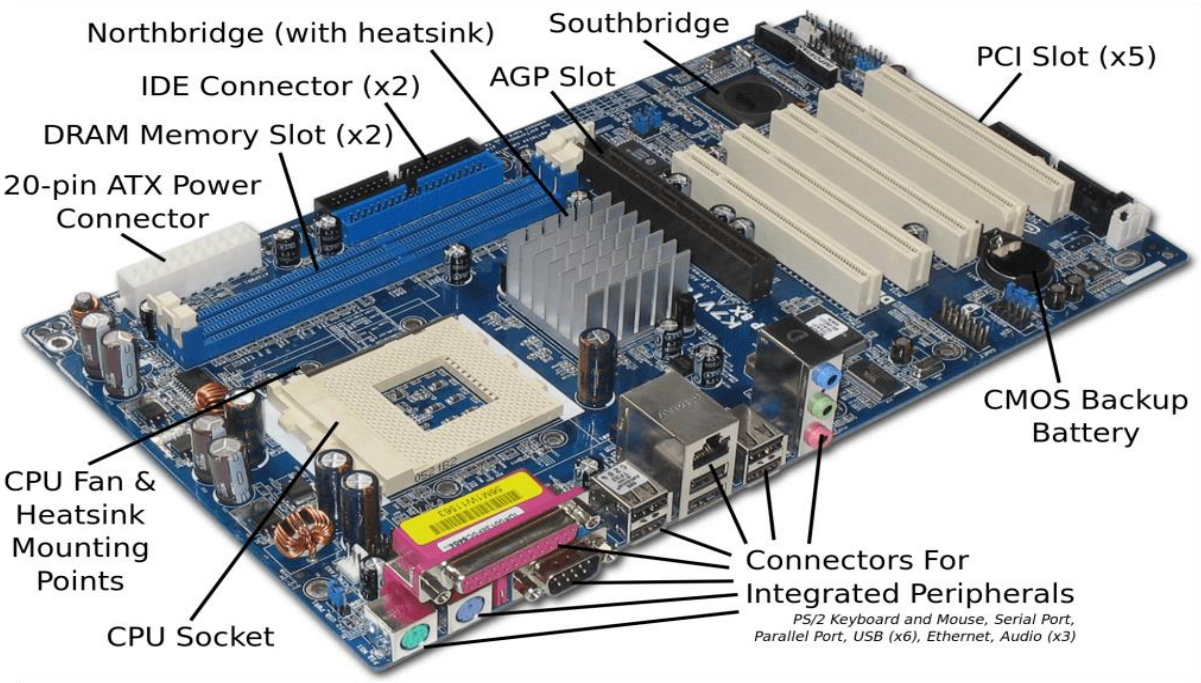
Network or Ethernet : You can connect your computer to a network by plugging in an Ethernet cable in this port

SCSI : It used to connect a hard drive, CD-ROM drive, or other device to a computer

CHAPTER-6
LAYOUT OF MOTHERBOARD WITH ITS COMPONENTS

Mother Board

A Computer Motherboard is commonly known as Main board or MB or System board or logic board is designed on PCB (Printed Circuit Board).That holds or connects all components and parts together on a single sheet. The Computer Motherboard holds all the circuitry to connect the various components of a computer system. Therefore it is also called as backbone of Personal computer system. **The Main board or Motherboard** is the main, cruical and important part of the computer system. It holds many important components such as Computer memory slots,cpu,sata IDE slots, expansions slots(PCI,AGP etc),capacitor's, resistor's ,BIOS chip etc The Computer main board is made up of thin sheet of non conductive material from plastic.



The motherboard may be characterized by the

1. Form factor
2. Chipset
3. Processor socket

Form factor : It refers to the motherboard's geometry, dimensions, arrangement and electrical requirements. Advanced Technology Extended (ATX) is the most common design of motherboard for desktop computers.

Chipset : It is a circuit, which is used to controls the of resources such as the bus interface with the processor, cache memory and RAM, expansion cards, etc. It used to coordinate data transfers between the various components of the computer.

The processor socket : It is a connector into which the processor is mounted. The Basic Input Output System (BIOS) and Complementary Metal – Oxide semiconductor (CMOS) are present on the motherboard.

Components of Motherboard

1. PCI Slot – Thos board has 2 PCI slots. These can be used for components such as Ethernet cards, sound cards, and modems.
2. PCI-E 16x Slot – There are 2 of them on this motherboard diagram, both are blue. These are used for your graphics card. With two of them onboard, you can run 2 graphics cards in SLI. You would only need this if you are a gamer, or working with high end video / graphics editing. These are the 16x speed versions, which are currently the fastest.
3. PCI-E 1x Slot – Single slot – In the PCI e 1x generation, each lane (1 x) carries 250 MB/s compared to 133 MB/s for the PCI slots. These can be used for expansion cards such as Sound cards, or Ethernet cards.
4. Northbridge – This is the Northbridge for this motherboard. This allows communication between the CPU and the system memory and PCI-E slots.
5. ATX 12V 2x and 4 Pin power connection – This is one of two power connections that supply power to the motherboard. This connection will come from your Power Supply.
6. CPU – Fan Connection – This is where your CPU fan will connect. Using this connection over one from your power supply will allow the motherboard to control the speed of your fan, based on the CPU temperature.
7. Socket – This is where your CPU will plug in. The orange bracket that is surrounding it is used for high end heat sinks. It helps to support the weight of the heat sink.
8. Memory slots – These are the slots for your RAM. Most boards will have 4 slots, but some will only have 2. The color coding you see on the motherboard diagram is used to match up RAM for Dual-Channel. Using them this way will give your memory a speed boost.
9. ATX Power connector – This is the second of two power connections. This is the main power connection for the motherboard, and comes from the power supply.
10. IDE connection – The IDE(Integrated Drive Electronics) is the connection for your hard drive or CD / DVD drive. Most drives today come with SATA connections, so you may not use this.
11. Southbridge – This is the controller for components such as the PCI slots, onboard audio, and USB connection.
12. SATA connections – These are 4 of the 6 SATA connections on the motherboard. These will be used for hard drives, and CD / DVD drives.
13. Front Panel connections – This is where you will hook in the connections from your case. These are mostly the different lights on your case, such as power on , hard drive activity etc.
14. FDD connection – The FDD is the floppy Disk controller. If you have a floppy disk drive in your computer, this is where you will hook it up.
15. External USB connections – This is where you will plug in external USB connections for your case or USB bracket.
16. CMOS battery – This is the motherboard's battery. This is used to allow the CMOS to keep it settings.

CHAPTER-7

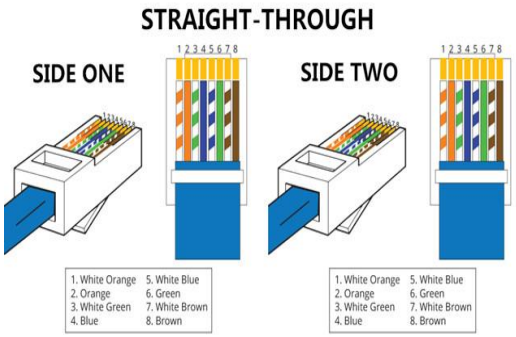
MAKING CROSS CABLE & STRAIGHT CABLE

What Is Straight-Through Cable?

A straight-through cable is a type of twisted pair cable that is used in local area networks to connect a computer to a network hub such as a router. This type of cable is also sometimes called a patch cable and is an alternative to wireless connections where one or more computers access a router through a wireless signal. On a straight-through cable, the wired pins match. Straight-through cable is a type of CAT5 with RJ-45 connectors at each end, and each has the same pin out. It is in accordance with either the T568A or T568B standards. It uses the same color code throughout the LAN for consistency. This type of twisted-pair cable is used in LAN to connect a computer or a network hub such as a router. It is one of the most common types of network cable.

A straight-through cable is used to connect the following devices.

- PC to Switch
- PC to Hub
- Router to Switch
- Switch to Server
- Hub to Server



Making Straight UTP Cable

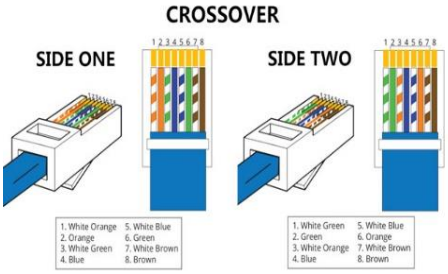
- Peel the end of the UTP cable, approximately 2 cm .
- Open the cable strands, align it
- Once the order is according to the standard, cut and flatten the ends of the cable ,
- Put the cable is straight and aligned into the RJ - 45 connector, and make sure all cables are in
correct position as follows :

Orange White on no 1
Orange on no 2
Green White on no 3
Blue on no 4
Blue White on no 5
Green on no 6
White Brown on no 7
Brown on no 8

- Make crimping using crimp tool
- Once finished at the end of this one , do it again at the other end cable

What Is Crossover Cable?
An Ethernet crossover cable is a type of Ethernet cable used to connect computing devices together directly. The internal wiring of Ethernet crossover cables reverses the transmit and receive signals. It is most often used to connect two devices of the same type: e.g. two computers (via network interface controller) or two switches to each other. A Crossover cable is a type of CAT 5 where one end isT568A configuration and the other end as T568BConfiguration. In this type of cable connection, Pin 1 is crossed with Pin 3, and Pin 2 is crossed with Pin 6.

The cross-over cable is used to connect the following devices.



Two computers
Two hubs
A hub to a switch
A cable modem to a router
Two router interfaces

Creating Cross UTP Cable
Creating a cross cable has almost the same steps with straight cable , the difference lies only in the color sequence from both ends of the cable . Unlike the straight cable that has the same color sequence at both ends of the cable , the cross cable has a different color sequences at both ends of the cable .

The first ends is same with straight cable :

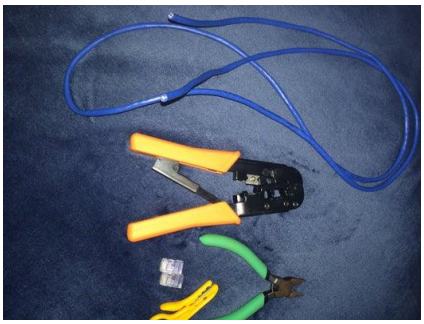
For the second end of the cable , the color composition is different from the first . the color arrangement is as follows :

Green White on no. 1
Green on no. 2
Orange White on no. 3
Blue on no. 4
Blue White on no. 5
Orange on no. 6
White chocolate on no. 7
Brown on no. 8

HOW TO MAKE ETHERNET CABLE

What are the tools are used for making Ethernet cable

CAT 6 CABLE
CRIMPING TOOL
WIRE CUTTER
SLIP CUTTER
RJ 45 CONNECTOR



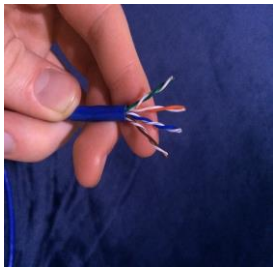
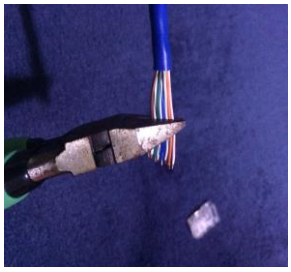
Step 1: Cable Inspection

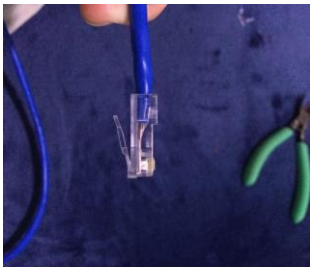
First, a Cat5e or Cat 6 cable will be required. This cable is mostly used with making an Unshielded Twisted Pair (UTP.) Make sure that the body of the wire has not been damaged, feel for lumps or anything unusual while examining the cables, as this can cause errors and may not even let your cable work. Also, avoid bending the cable to far past its bend radius because this can cause the copper inside to be damaged and not work correctly. The bend radius is usually where the cable jacket, will start to turn white.

Step 2: Stripping the Cable

Second, a cable stripper will be needed. Start by only stripping off about an inch of the jacket, to expose approximately an inch of wires. Be sure not to take off too much of the jacket, because it will have to be clamped down inside of an RJ45 connector. If there is too much wire, they might have to be shortened, by cutting them directly with wire cutters. After there is a correct amount of the wires exposed, unwind the copper wires twisted together on the inside, while starting with the correct colors left to right. There are a total of 8 copper wires inside of the jacket, each marked with a different color. The colors are orange-white, orange, green-white, blue, blue-white, green, brown-white, and brown, in that order, When unwinding them, try to bend them back and forth a bit, so the copper can flatten easier.

Step 3: Putting the Wires in the Connectors



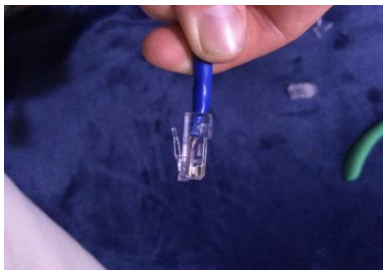
Next, this will need at least 2 RJ45 wire connectors, one for each side of the cable. After the wires have been spread apart, organize them into the correct color order of the desired cable. We are making the T-568B standard for a straight-through, which means that the color order for the wires is going to be the exact same on both sides. After the colors have been organized, if they don't all reach the same length, use wire cutters directly on the end, to make each wire the same length. Be careful not to trim the wires down too far, or the wires might not be long enough and might need to take a little bit more of the jacket off for the wires to be long enough to fit all the way into the RJ45 connector correctly. Once the wires are flat, in order, and can reach all the way to the end of the connector, start to put them into the RJ45 connectors. Make sure that the tab

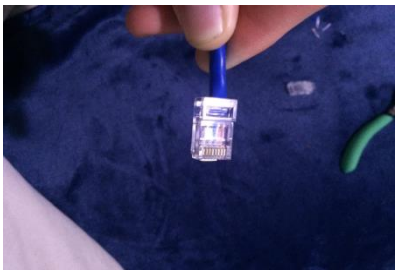
on the connector is facing down, and while holding the wires flat and in order, slide the wires down to the end of the connector, till you can see all of the copper wires at the end, through the end of the plastic. Remember that the jacket has to be inside the connector a bit, so the crimping tool will keep the wire inside the connector.

Step 4: Crimping the Connector

Then, RJ45 wire crimpers will be required, to hold the connector onto the cable. If the cable so far, has got all the wires correctly inside of the RJ45 connector, along with a bit of the cable jacket, then it should be ready to crimp the wire inside of the connector. The crimpers push down a wire locking piece inside, that cannot be undone. Note that, once the wire is crimped down correctly if there are errors with the connection and the wire doesn't work correctly, the only way to fix this is to cut off the RJ45 connector with wire cutters, and start from step 2, with a new RJ45 connector.

Step 5: Testing the Cable

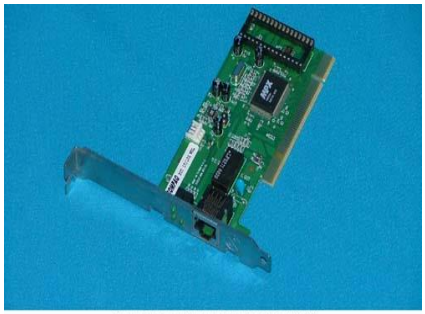




Last, in order to test the wire, either try using it on the live machines or use a cable tester to get detailed information about the wire in specific such as, what wires are where and how long is the whole cable. A tester can also determine what wires are in incorrect spots.

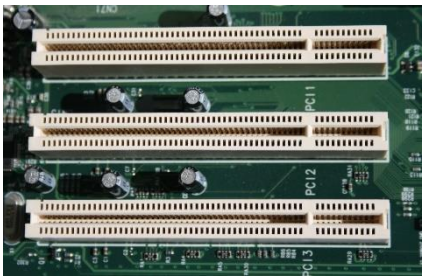
CHAPTER - 8
INSTALL & CONFIGURE NETWORK INTERFACE CARD

1. Read the user's guide and familiarize with the new card.
2. Power down PC and remove the AC power cord.
3. Open the computer case.
4. Find an available Peripheral Component Interconnect (PCI) slot on the motherboard and remove slot insert if one exists.

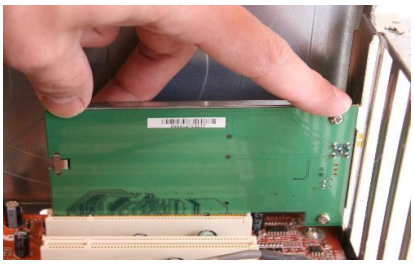


View of a typical Network Interface Card (NIC)

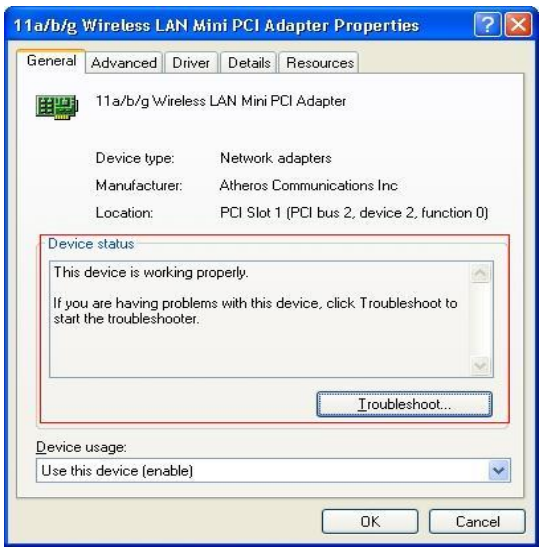
5. Carefully remove the network card from its static-proof plastic envelope, and slide it into the slot.
6. Seat the card in the slot firmly with gentle pressure along the length of the card, especially right about the slot itself.
7. Snugly, screw the card to the computer frame, but do not over tighten.
8. Close the computer case.
9. Plug your computer in and power it up.
10. The NIC comes with a disk containing the necessary drivers required for the software installation. Just install the driver software into the system.



To Check the NIC is working or not.



11. Click Start, then click Control Panel.
12. Click in Device Manager
13. Double-click Network Adapters.
14. It should appear the name of your Ethernet card.
15. Next, double click the name of your Ethernet adapter.
16. If the text in the "Device Status" box says "This device is working properly.", then you successfully installed the card and are finished.
17. If the text in the "Device status" box doesn't say "This device is working properly.", then write down on a piece of paper what it says and continue with next step.
18. Click the Troubleshoot. Button and follow instructions. Double check you followed the directions above. Install the most up to date device drivers.



IDENTIFY THE IP & CONFIGURE IP ADDRESS

1. Open the Control Panel.
2. Set View by to Category.
3. Click Network and Internet.

4. Click Network and Sharing Center.
5. On the left pane, click Change adapter settings.
6. Right-click the local area network connection that is connected to the radio hardware and select Properties.

    - If an unused network connection is available, the local area connection appears as Unidentified network.

    - If you plan to reuse your network connection, select the local area connection that you plan to use for the radio hardware.

    - If you have only one network connection, check if you can connect wirelessly to the existing local area network. If you can, you can use the network connection for the radio hardware.

    - You can use a pluggable USB to Gigabit Ethernet LAN adapter instead of a NIC. The instructions are the same.

7. On the Networking tab of the Properties dialog box, clear all options except Internet Protocol Version 4 (TCP/IPv4). Other services, particularly antiviral software, can cause intermittent connection problems with the radio hardware.

8. Double-click Internet Protocol Version 4 (TCP/IPv4).

9. On the General tab, select Use the following IP Address.

10. The default IP address is 192.168.1.101. The development computer network connection must be on the same subnet as the hardware board. To meet this requirement, a compatible IP address must be assigned to the development computer network connection. Set the network IP address to 192.168.1.x, where x is any number in the range 1 through 255, apart from 101.

11. Leave the subnet mask set to the default value of 255.255.255.0 and click OK.

Fig -1

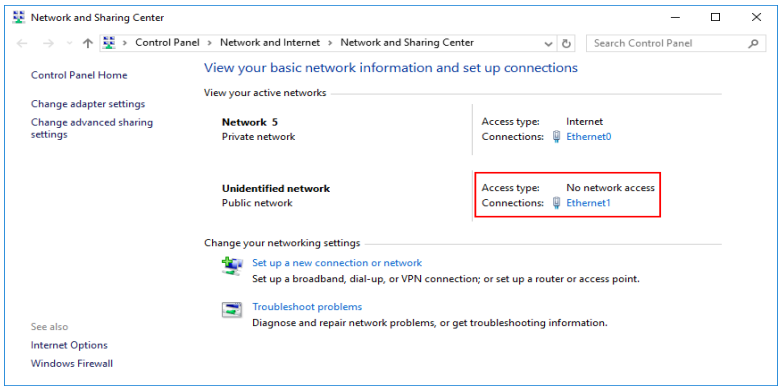


Fig-2

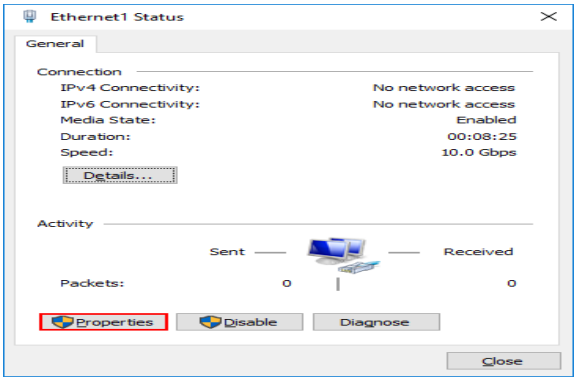


Fig-3

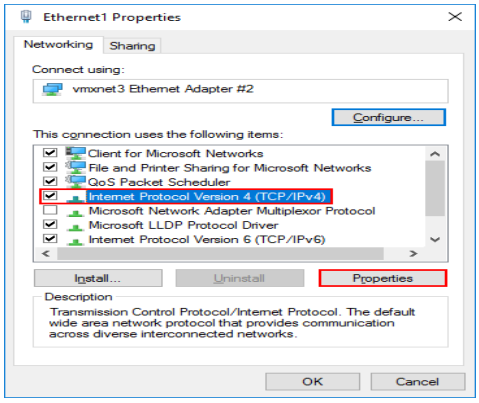
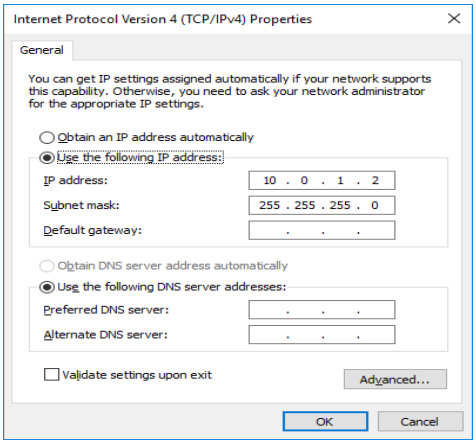


Fig-4



CHAPTER-9
MANAGING USER A/C IN WINDOWS

Go to the Control Panel from the Start Menu.

Click Add or remove **user accounts**. Going to **user accounts**.

The **Manage Accounts** pane will appear. You will see all of the **user accounts** here, and you can add more **accounts** or **manage** existing ones. The **Manage Accounts** pane.

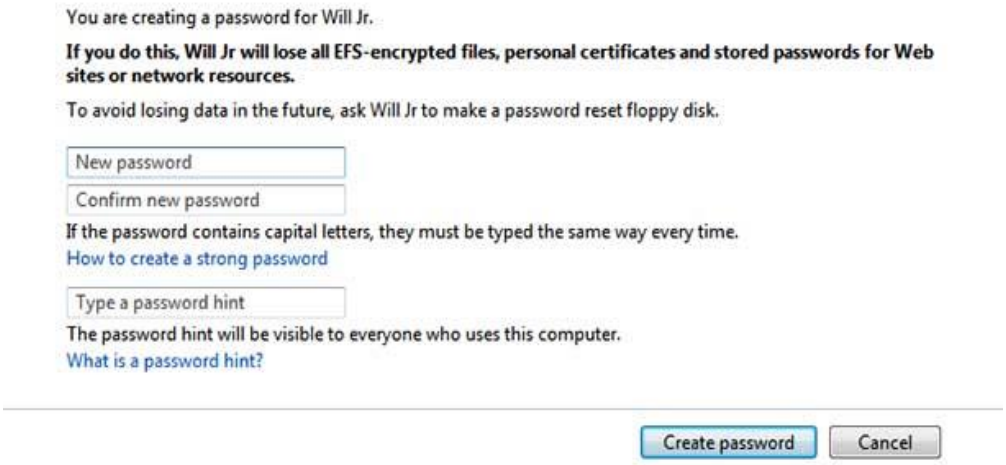
To create a new account:

1. From the **Manage Accounts** pane, click **Create a new account**.
2. Type an **account name**.
3. Select **Standard user** or **Administrator**.
4. Click **Create Account**.

Changing an account's settings
Once you've created a new account, you may want to add a **password** or make other changes to the account's settings.
To create a password:
From the **Manage Accounts** pane, click the account name or picture.

1. If you want, you can type a password hint to help you remember your password.
2. Click **Create password**.

3. To go back to the Manage Accounts pane, click **Manage another account**. Account passwords are **case sensitive**, which means capital and lowercase letters are treated as different characters. For example, **aBc1** is not the same as **abc1**.



MANAGING USER A/C IN LINUX

The Linux operating system was designed to be a multi-user OS. As such, one of the most common administrative tasks performed on a Linux machine is managing user accounts.

Background

A user account in Linux is the primary way of gaining access to a system — whether locally or remotely.

There are three main types of user accounts on a Linux system:

1. Root account — User with unlimited access to modify the Linux system.
2. System accounts — Used for running services or specific programs. Some of the most common ones include MySQL, mail, daemon, bin, etc.
3. User accounts — General users who have limited access to the system.

In Linux, most user information can be found in three files located at `/etc/passwd`, `/etc/shadow`, and `/etc/group`.

1. List All Users
To list all available users on a machine, you can run the following command:

```
$ compgen -u
```

Alternatively, you can output the users straight from the /etc/passwd file using the following command:

```
$ cat /etc/passwd
```

As you notice from the output, your list will contain the root user, several system users, and general user accounts. The output will be similar to this:

2. Create a User Account
One of the most common administrative tasks is adding users to a system. The simple command for that is useradd. For example, to add a user named Marion, we can run the following command:

```
$ sudo useradd -c "audit consultant" marion
```

The -c is an optional argument that allows you to add a comment associated with the user you are creating.

The useradd command takes other optional arguments too. You can take a look at them by running the following command:

```
man useradd
```

Tip: Debian-based systems have the adduser command as an alternative.

3. Change a User Password
To add a default password to the user we just created above, we can use the passwd command. The passwd command can also be used to modify the password of any user as follows:

```
$ sudo passwd marion
```

You will then be prompted to enter the password you wish to set. The output will be similar to this:

```
[redacted]@[redacted]iwa:~$ sudo passwd marion
New password:
Retype new password:
passwd: password updated successfully
```

4. Switching User Accounts

mentioned earlier, Linux is truly a multi-user OS. You can switch user accounts from the terminal as you wish (as long as you are allowed to do so).

To switch to the marion user account that we just created above, we can use the su command as follows:

```
$ su marion
```

You will then be prompted to enter the password of the user you are switching to.

If you successfully switched users, you can confirm your new identity by running the following command:

```
$ who am i
```

Your output should be similar to the one below:

```
$ whoami
marion
```

To switch back to the previous account, just type the exit command.

5. Modifying a User Account

The usermod command allows you to make changes to user accounts. It takes similar optional arguments as the useradd command.

For example, to modify the comment for the marion user account that we created above, you can do the following:

```
$ sudo usermod -c "New audit consulant comment" marion
```

To check if the comment was indeed modified, we can search for the user account name in the /etc/passwd file using the following command:

```
$ grep 'marion' /etc/passwd
```

```
[redacted]@[redacted]wa:~$ grep 'marion' /etc/passwd
marion:x:1001:1002:New audit consulant comment:/home/marion:/bin/sh
```

6. Delete a User Account

Deleting a user account from the command line is extremely easy. Therefore, you need to practice caution.

The userdel command is used to delete a user account. It only takes a single optional argument: -r. When the -r argument is specified, you delete the user's home directory and the mail spool.
To delete the user account that we created in this guide, do the following:

```
$ sudo userdel -r marion
```

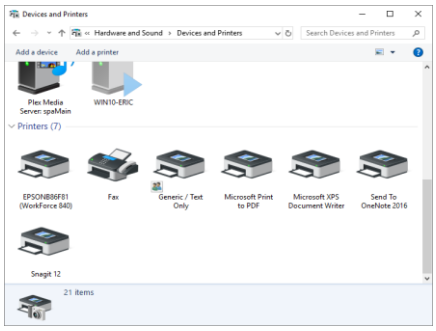
7. Running Commands as a Superuser
We have already used the command we will look at now, but I didn't really explain it. The sudo (superuser do) command allows you to run commands as the root user. You will be prompted to enter your user password to run this command.
If you can't run commands as the root user, you will be notified via the terminal that you cannot run sudo on the system.
To run elevated commands, use the sudo command followed by the elevated command you want to run. For example, to add a user, you can do this:

```
$ sudo useradd newuser
```

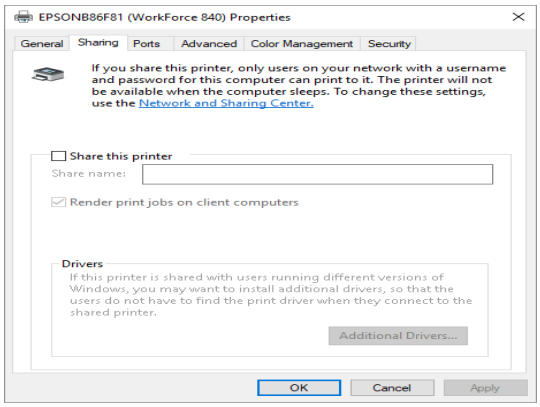
CHAPTER-10
SHARING HARDWARE RESOURCES ON A NETWORK

Printers

Network printers can be configured as shared devices so that others on the network can use them. If you are using Windows 7 go to **Start | Devices and Printers**. If you are using Windows 8 or Windows 10, display the control panel and click **View Devices and Printers** (under the Hardware and Sound heading). Windows displays the Devices and Printers dialog box. (See Figure 1.)



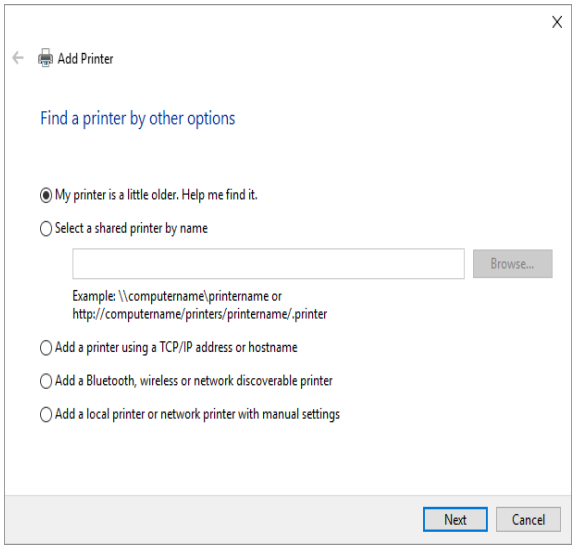
Right-click the printer you want to share and select Printer Properties from the Context menu. Windows displays the Properties dialog box for the selected printer. The contents of the dialog box vary depending on the capabilities of your printer. Make sure the Sharing tab is displayed. (See Figure 2.)



Click the Share this Printer check box and optionally change the Share Name of the printer.

Depending on the configurations of your particular systems you may either check or uncheck the Render Print Jobs on Client Computers check box. If checked, then all the processing required prior to queuing the print job occurs on the client computer. If unchecked, the computer hosting (serving) the printer does the processing for all print jobs sent through it.

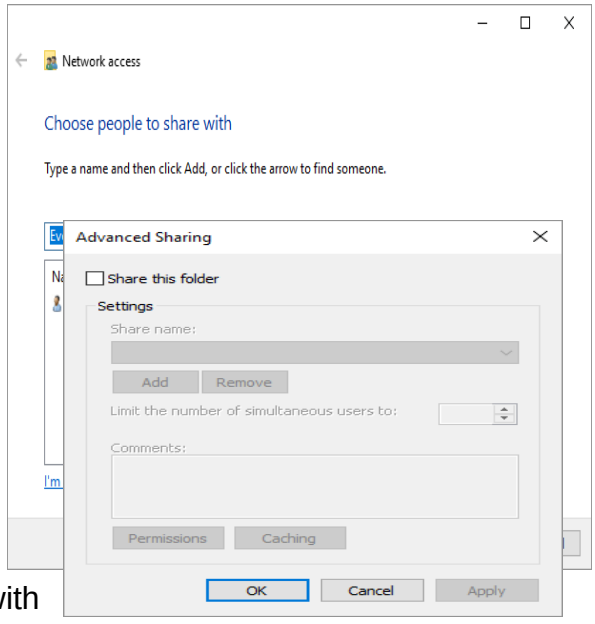
When you are done sharing the printer, click OK to close the printer's Properties dialog box. The printer is immediately made available to others on your network. In order to access the shared printer from a different system, go to that system and, if the system is using Windows 7, choose **Start | Devices and Printers** and click on Add a Printer. If the system is using Windows 8 or Windows 10, display the Control Panel and click **View Devices and Printers** (under the Hardware and Sound heading) and then click the Add a Printer option, at the top of the dialog box. Windows starts the Add Printer wizard. The Windows 10 system will perform a search for a device or printer to this PC. Click on The Printer I want isn't Listed if our printer isn't found. Windows displays the Find a Printer by Other Options section of the Add Printer wizard. (See Figure 3.)



Click the second option (Add a Network, Wireless or Bluetooth Printer if you are using Windows 7 or Windows 8) or click the fourth option (Add a Bluetooth, Wireless or Network Discoverable Printer) if you are using Windows 10, and the system immediately starts scanning the network for available printers. After all of the printers have been found, select the printer name that you want to use and click **Next**. The network printer is added to the computer's list of available printers. Click **Finish** to finish the process.

File Folders and Disk Drives

File folders and entire disks can also be shared among network-connected systems, and the procedure is similar to that of sharing a printer. Using Windows Explorer, right-click the folder you want to share with others on the network and select **Share With | Specific People** (Windows 7) or **Share | Specific People** (Windows 8). Windows then displays the File Sharing dialog box. If you are using Windows 10, display File Explorer and make sure the Share tab of the ribbon is displayed. Then right-click the folder you want to share with



others on the network and select **Give Access to | Specific People**. Windows then displays the Network Access dialog box. (The File Sharing and Network Access dialog boxes are essentially the same.) (See Figure 4.)

The dialog box looks like it does because I clicked the drop-down arrow to the left of the **Add** button and selected Everyone from the list. When I clicked the **Add** button, the group "Everyone" was added to the list of those allowed to access my folder.

When you add a person or a group to those permitted to access your folder, the permission level for your addition is set to "Read." If the group being added is "Everyone," then this allows everyone on the network to read from the shared folder. Clicking the down-arrow beside the Read setting (in the File Sharing dialog box) allows you to change the permission level to something else, such as to allow them to write to the folder. Once you've set the desired permission level, click the **Share** button to commit your changes.

Sharing an entire disk drive is similar to sharing a folder, but the mechanics are a bit different. Under Windows Explorer, right-click the disk drive you want to share and choose **Share With | Advanced Sharing** or **Share | Advanced Sharing** (Windows 8). If you are using Windows 10, display File Explorer, right-click the disk drive you want to share and choose **Give Access to | Advanced Sharing**. Windows displays the Sharing tab of the disk drive's Properties dialog box, and you should click the **Advanced Sharing** button within the dialog box. Windows then displays the Advanced Sharing dialog box. (See Figure 5.)

Click the Share this Folder check box (yes, I know it's not really a folder; it's a disk drive). You can then optionally change the Share Name. When ready to share, click **OK** to finish the process.

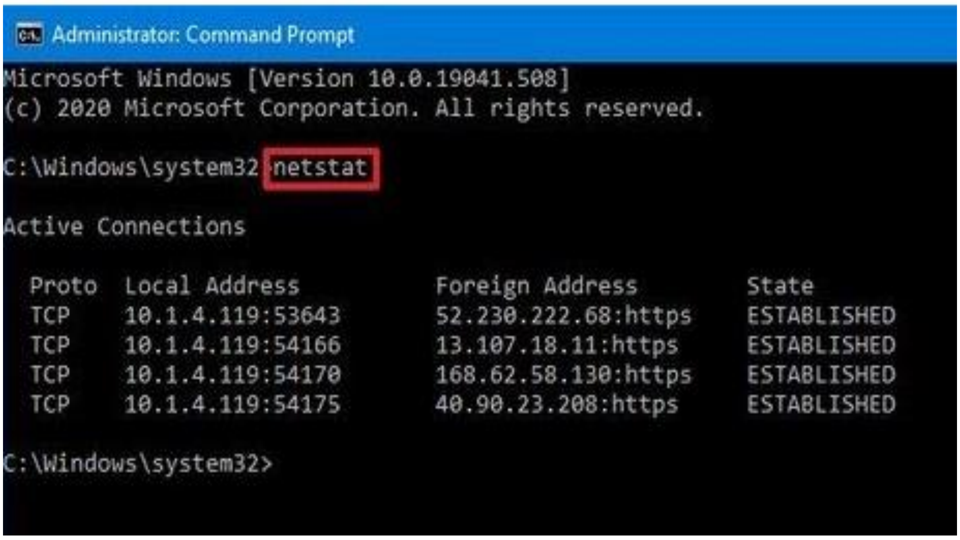
CHAPTER-11
NETSTAT

The network statistics (**netstat**) command is a networking tool **used** for troubleshooting and configuration, that can also serve as a monitoring tool for connections over the network. Both incoming and outgoing connections, routing tables, port listening, and **usage** statistics are common **uses** for this command.

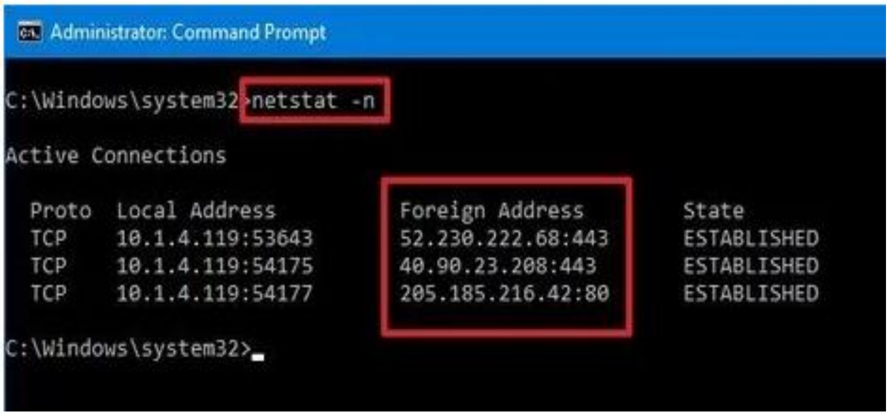
How to search netstat details on Windows 10

1. Open Start.
2. Search for Command Prompt, right-click the top result, and select the **Run** as administrator option.

3. Type netstat command to show all active TCP connections and press Enter:

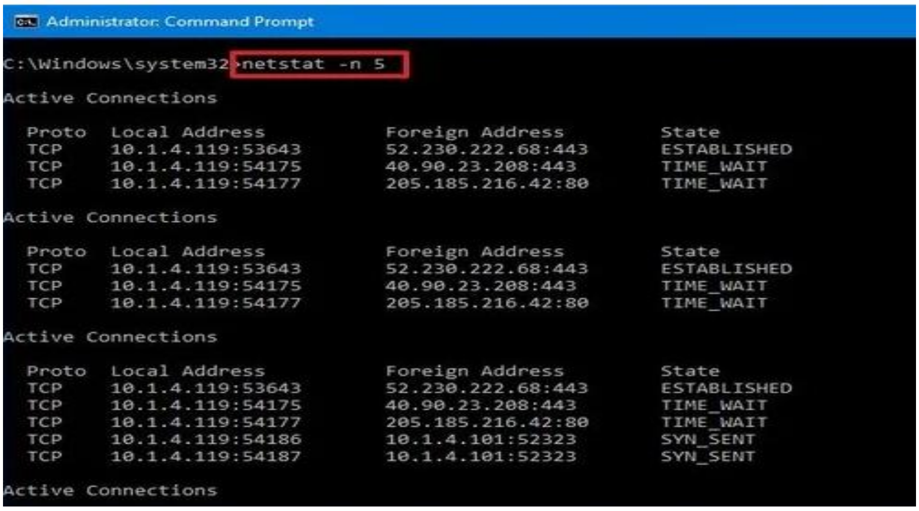


4. Netstat –n Type the command to display active connections showing numeric P address and port number instead of trying to determine the names



5. netstat -n INTERVAL   Type the command to refresh the information at a specific interval netstat -n 5

This example refreshes the command in question every five seconds:



Quick note: When using the interval parameter, you can terminate the command using the **Ctrl + C** keyboard shortcut in the console.

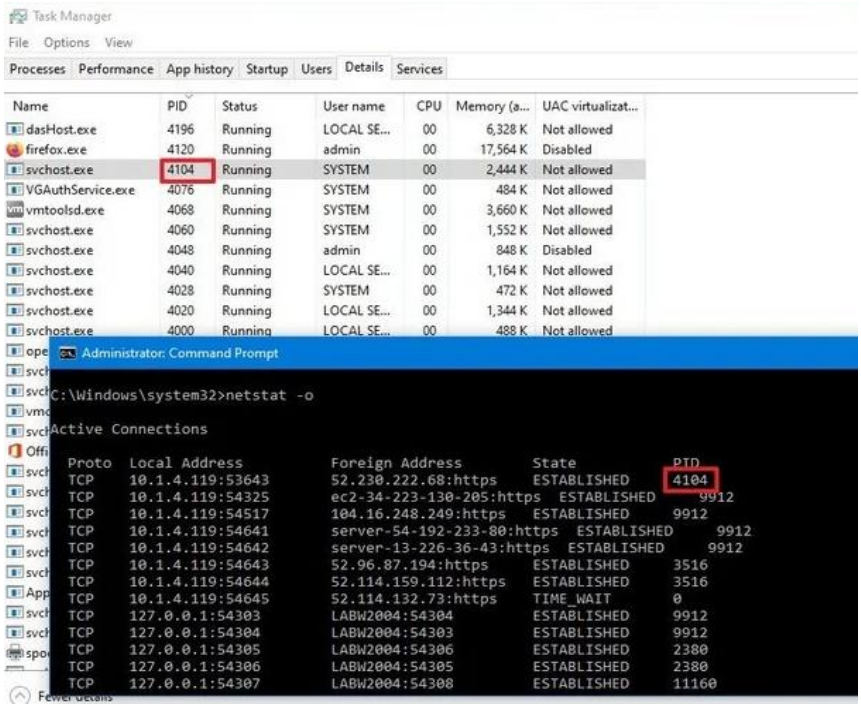
Once you execute the command, it'll return a list of all active connections in four columns, including:

- **Proto:** Shows the connection protocol (TCP or UDP).

- **Local Address:** Shows the computer's IP address followed by a semicolon with a port number of the connection. The double-semicolon inside brackets indicates the local IPv6 address, and "0.0.0.0" refers to the local address too.

- **Foreign Address:** Lists the remote device's IP (or FQDN) address with the port number after semicolon port name (for example, https, http, microsoft-ds, wsd).
- **State:** Indicates where the connection is active (established), the local port has been closed (time wait), and the program hasn't closed the port (close_wait). Other status include, closed, fin_wait_1, fin_wait_2, last_ack, listen, syn_received, syn_send, and timed_wait.

- Netstat –a : Show active and inactive connections
- Netstat –b : Show executable information
- Netstat – e : Show network adapter statistics
- Netstat –f : Show FQDNS(fully qualified domain name) for foreign addresses
- Netstat –n : Show the addresses and ports in numerical form. For example, 54.230.157.50:443.
- Netstat -o : command shows all active TCP connections like netstat, but with the difference that adds a fifth column to display the Process ID (PID) for each connection. The processes available in this view are the same in the "Details" tab of Task Manager, which also reveals the application using the connection.



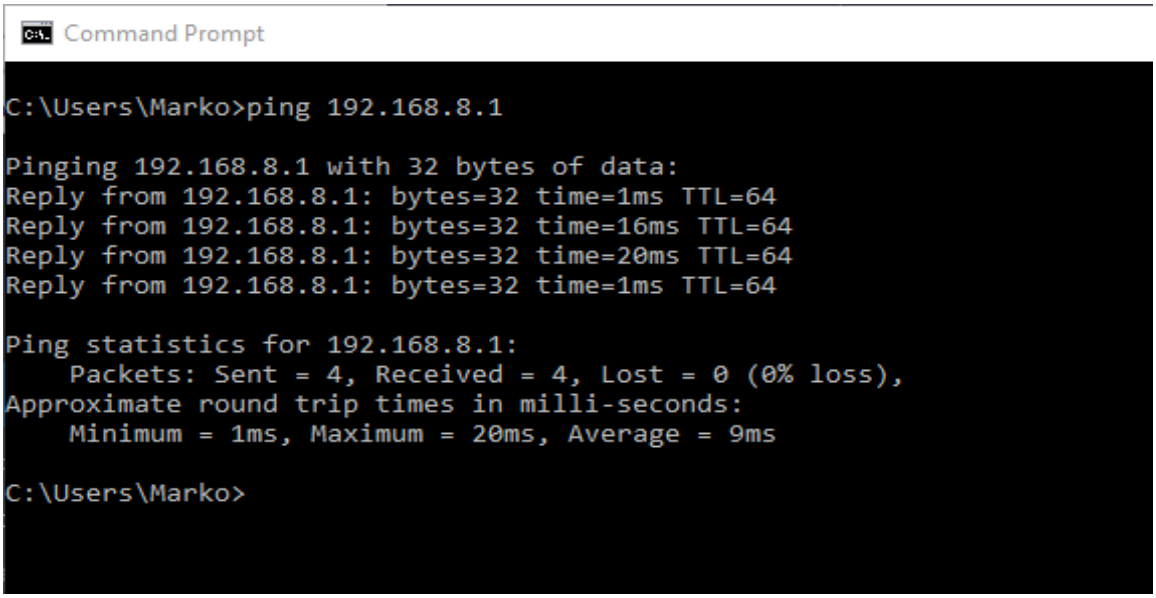
CONNECTIVITY TROUBLESHOOTING USING PING /IPCONFIG

Network troubleshooting tools necessity for every network administrator when getting started in the network field, It is important to a mass and number of tools that can be used to troubleshoot a variety of different network conditions.

PING

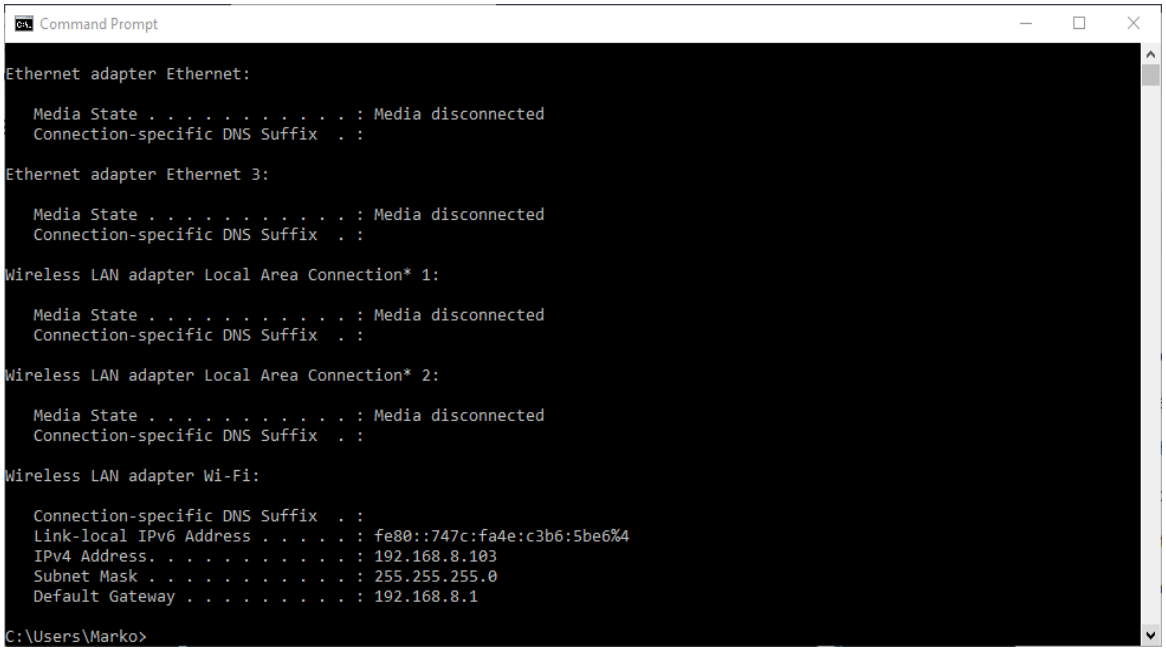
The ping command allows you to send a signal to another device ,and if that device is active, it will send a response back to the sender. The “Ping” command is a subset of the ICMP (internet control message protocol) and it uses what it called an “echo request”. So when you ping a device you send out an “echo request” , and if the device you Ping is active or online you get an echo response.

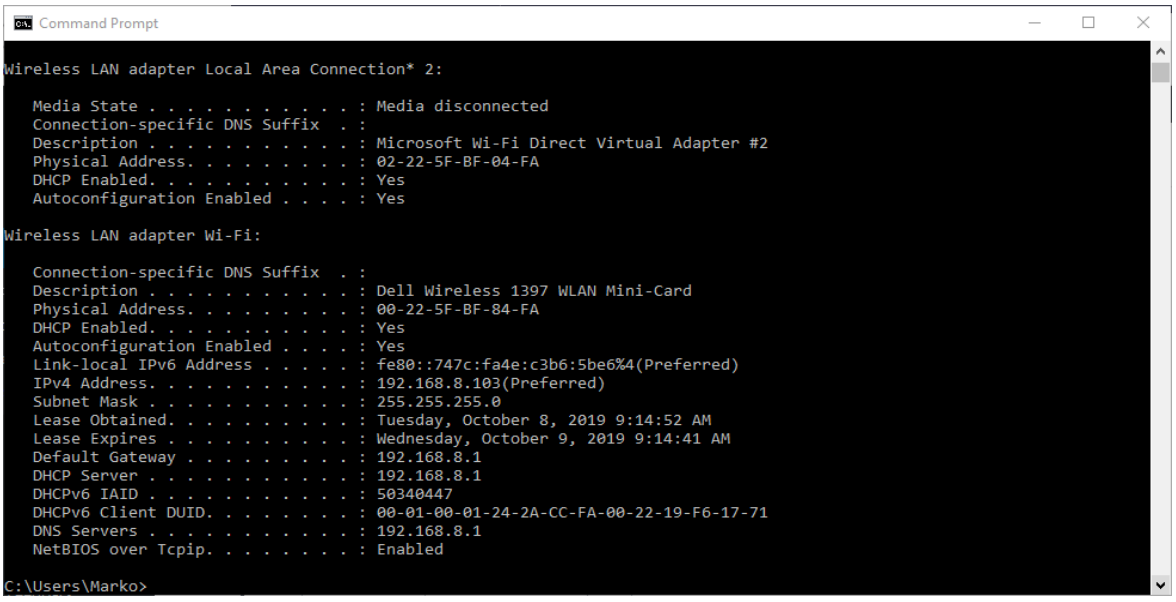
For example if you are local computer has internet connectivity issues, you can try to ping your router. If you get no response then you know that the router is what is giving you problems. Let's ping our router IP, which is reaches 192.168 router IP reaches 192.168 our router IP reaches 192.168 router IP reaches 192.168. 8.1 is our example and let's analyze the printout.



IPConfig

The IP config display the current information about your network such as IP and MAC address, and the IP address of your router. It can also display information about your DHCP and DNS servers. Let's see the basic output of “IPconfig”. Depending on the network connection type you may see different output for different connection. For example if you are connected to the network using Ethernet (you plug in your network cable to the RJ45 Jack) you will see IP information in the “Ethernet adaptor” section. In our case we are connected to the Wi-Fi (wireless) connection so get information there in our case. The local IPV4 of a computer is 192 168 8.103. We also see the subnet mask (255.255.255.0) which we can use to find the network address. We also see the default gateway IP (192.168.8.1) which is our router. To see detailed IP information we can use the “/all” switch together with “ipconfig” command (ipconfig /all).





CHAPTER -12
OPERATING SYSTEM, INSTALL OF OPERATING SYSTEM (WINDOWS 7)

Operating system

An **operating system** is the **most important software** that runs on a computer. It manages the computer's **memory** and **processes**, as well as all of its **software** and **hardware**. It also allows you to **communicate** with the computer

without knowing how to speak the computer's language. **Without an operating system, a computer is useless**.

INSTALLATION OF WINDOWS OS

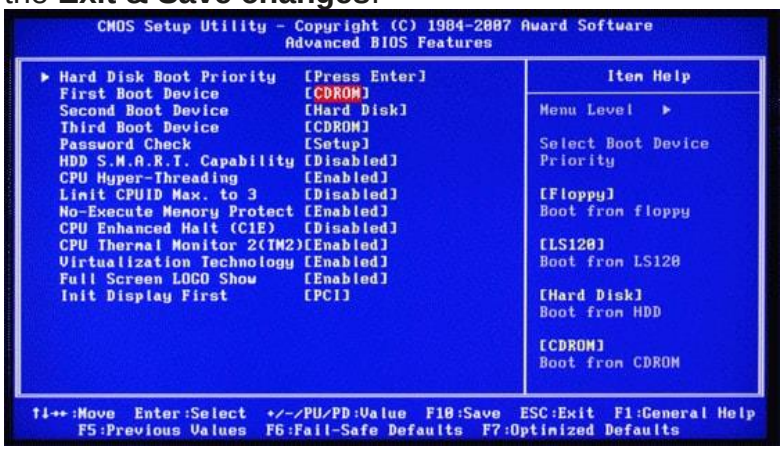
System requirements

Before you start installing your Windows 7, it is recommended that you check your hardware setup and find out if it corresponds to the recommended system requirements by Microsoft. The Windows 7 minimum system requirements are as follows:

- 1 gigahertz (GHz) or faster 32-bit (x86) or 64-bit (x64) processor;
- 1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit);
- 16 GB available hard disk space (32-bit) or 20 GB (64-bit)
- DirectX 9 graphics device with WDDM 1.0 or higher driver.

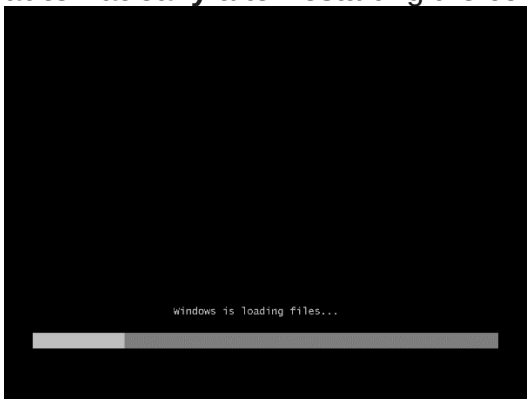
Booting your operating system using a DVD

Take out your Windows 7 DVD and insert it into the computer (if your computer does not have a DVD drive, please read the USB installation guide). If the installation does not run automatically, it is necessary to restart your computer and, in some cases, set up a booting priority in the BIOS (press the **Delete**, **F2** or **F12** button immediately after restarting the computer) so that your DVD drive is at the top of the list (Pic. 1). The BIOS version is based on your motherboard and the booting priority is usually found under the Boot option. Change the booting priority and confirm the changes by clicking the **Exit & Save changes**.



Running the installation

If the DVD booting setup was successful, the Windows 7 installation **should run automatically** after restarting the computer

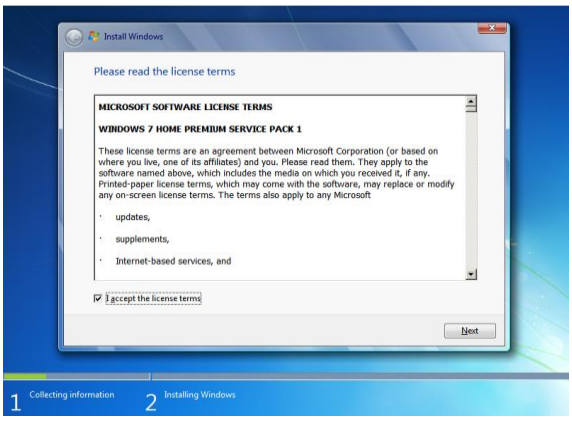


Language setting option

The first step is **choosing a language, time format, currency and keyboard layout**. Choose your language setting in the first step. This setting will carry on onto the next steps, so all you need to do is click **Next.**

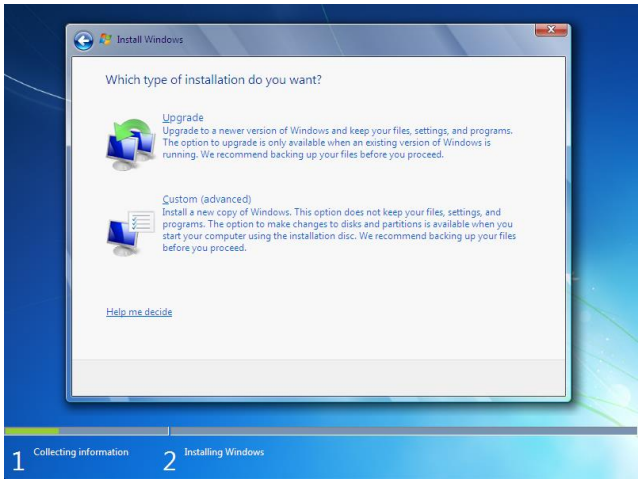
License terms acceptance

In the next step you have to click on **Install now** and then the **license terms must be accepted** by ticking the “I accept the license terms” checkbox. Then just click **Next to proceed.**



Which type of installation?

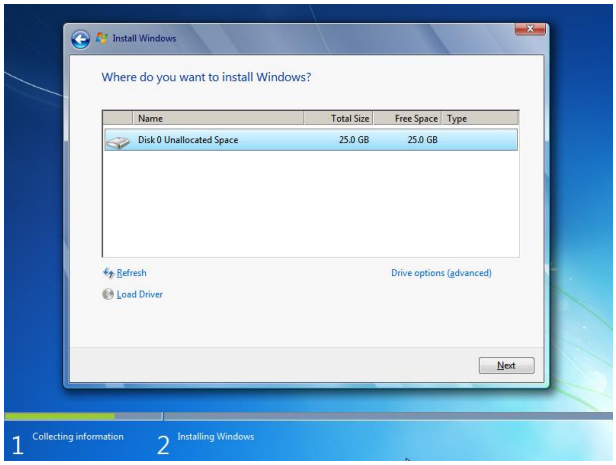
If you already have a previous version of Windows installed on your computer, the installation process will offer you a Windows 7 Upgrade option . In this case, we recommend choosing the **Custom** option and perform a complete reinstall. Before doing so, it is important to back up all important files and documents because all data will be deleted. You can use, for example, the Cobian backup application for preforming a backup. If you are installing Windows on a computer without an operating system, this option will not be available.

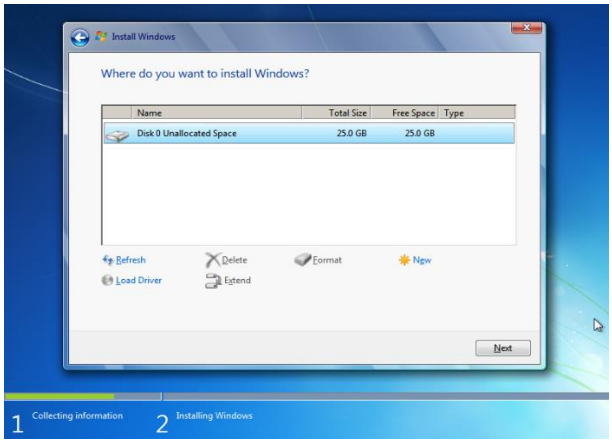


Where do you want to install Windows?

If you are installing Windows 7 **on a computer with a previous Windows version**, an allocated drive will be created for the installation. Click this drive and click on **Drive options (advanced)**, then click on **Remove**. Once you remove disks, a **Disk 0 Unallocated space** will remain. If you do not want to divide your disk into several drives, click **Next**.

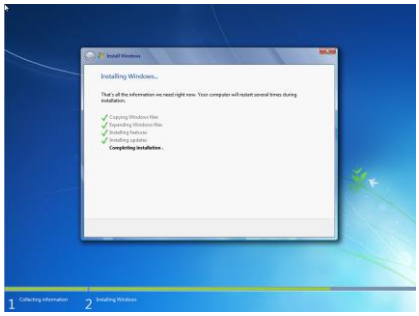
Warning! **If you have several disks** or allocated spaces in your computer, from which one is reserved for system files and others are for your files and documents which you want to keep, remove only the one which is reserved for the system files and click **Next**.





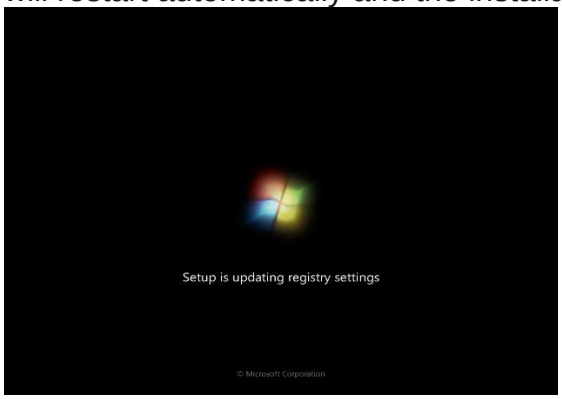
System installation

The next step is the actual installation, which includes copying of the files, installation of the features and updates). This step takes the most time but **should not take longer than 20 minutes**.



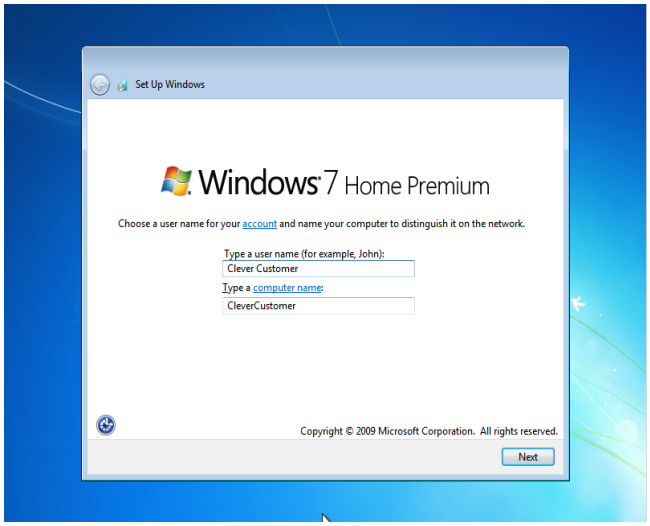
System restart

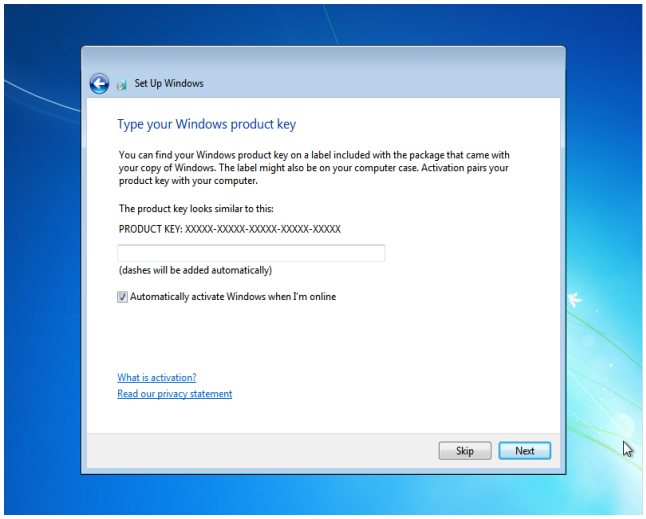
When the installation files are copied and features and updates installed, the computer will restart automatically and the installation will be completed .



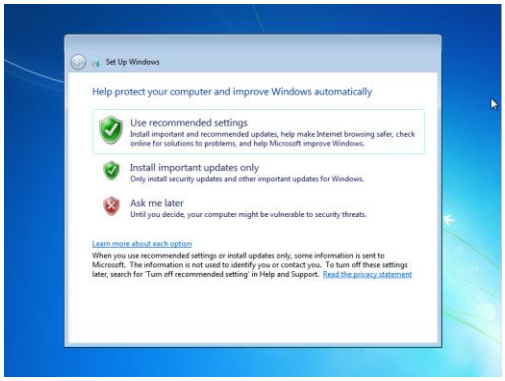
User setting

In the next two steps, you will choose your user name (which you will use for your Windows login. A computer name will be generated for you and can be changed according to your requirements. Clicking **Next** will take you to **setting up your password** . **Choose** your password, **retype** the password in the second line and type a **password hint**, to help you remember your password in case you forget it.



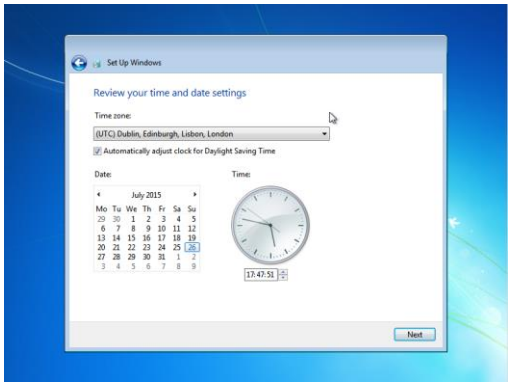


Help protect and improve Windows automatically
This step lets you choose the protection and automatic update options. We recommend using the **Recommended settings.**



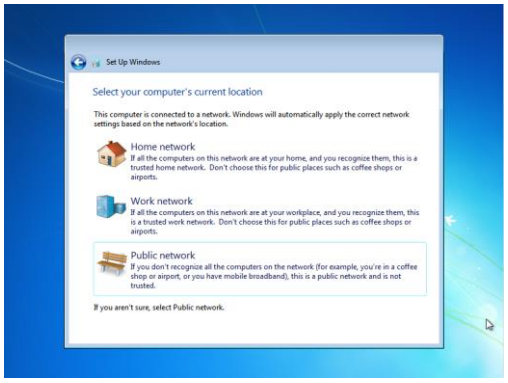
Time and date

In this step **check if the time and date is correct** and click Next.



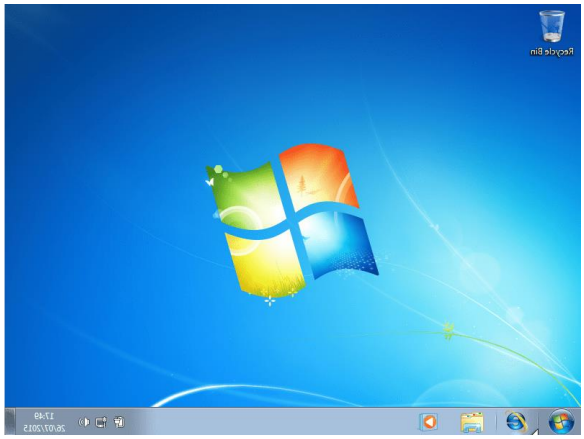
Network setup

If you are connected to a network, the **Choose a network type** window will pop up. Choose the network type and click **Next**.



Finishing the installation

Welcome! The installation process is complete. Just wait until your desktop is prepared.



System activation
Your system **must be activated within 30 days after installation**. The activation can be performed over the internet or phone.
Installing drivers and updates
Now you can personalise your computer and install all necessary updates and drivers. If you are connected to a network via an Ethernet cable, the updates and driver can be installed using the Windows Update application, which can be found in the Start menu.

CHAPTER-13
Network Operating System

Operating System (OS)

An Operating System(O.S.) is a System software that manages the hardware resources and provides services to the Application software. There are many types of operating systems depending upon its features and functionalities. They can be Batch O.S., Multitasking O.S., Multiprocessing O.S., Network O.S., Hybrid O.S., etc.

Network Operating System (NOS)

NOS is a computer operating system that facilitates to connect and communicate various autonomous computers over a network. An Autonomous computer is an independent computer that has its own local memory, hardware, and O.S. It is self capable to perform operations and processing for a single user. They can either run the same or different O.S.

The Network O.S. mainly runs on a powerful computer, that runs the server program. It facilitates the security and capability of managing the data, user, group, application, and other network functionalities. The main advantage of using a network o.s. is that it facilitates the sharing of resources and memory amongst the autonomous computers in the network. It can also facilitate the client computers to access the shared memory and resources administered by the Server computer. In other words, the Network O.S. is mainly designed to allow multiple users to share files and resources over the network. The NOSs can distribute their tasks and functions amongst connected nodes in the network, which enhances the system overall performance.

Types of Network Operating System

- **Peer to Peer NOS**
- **Client-Server NOS**

Peer-to-Peer **Network Operating System is an operating system in which all the nodes are functionally and operationally equal to each other.** No one is superior or inferior. They all are capable to perform similar kinds of tasks. All the nodes have their own local memory and resources. Using the Network O.S., they can connect and communicate with each other. They can also share data and resources with one another. One node can also communicate and share data and resources with a remote node in the network by using the authentication feature of the Network O.S. The nodes are directly connected with each other in the network with the help of a switch or a hub.

Advantages of the Peer-to-Peer NOS

- Easy to install and setup.
- The setup cost is low.
- There is no requirement for any specialized software.
- The sharing of information and resources is fast and easy.

Disadvantages of the Peer-to-Peer NOS

- The performance of autonomous computers may not be so good when sharing some resources.
- There is no centralized management.
- It is less secure.
- It does not have backup functionalities.
- There is no centralized storage system.

Client-Server **Networking Operating System operates with a single server and multiple client computers in the network.** The Client O.S. runs on the client machine, while the NOS is installed on the server machine. The server machine is a centralized hub for all the client machines. The client machines generate a request for information or some resource and forward it to the server machine. The server machine, in turn, replies to the client machine by providing appropriate services to it in a secure manner. The server machine is a very powerful computer, that is capable of tackling large calculations and operations. It can also have the ability to administer the whole network and its resources. It can be multiprocessing in nature, which can process multiple client requests at the same time. The N.O.S. enhances the reach of client machines by providing remote access to other nodes and resources of the network in a secure manner.

Advantages of the Client-Server NOS

- It has centralized control and administration.
- It has a backup facility for lost data.
- The shared data and resources can be accessed concurrently by multiple clients.
- It has better reliability and performance.

Disadvantages of the Client-Server NOS

- The setup cost is very high.
- There is a requirement of specialized software for client and server machines to function properly.
- There is a need for an administrator to administer the network.
- There may be network failure, in case of central server failure.
- A huge amount of client requests may overload the server.

the common functionalities of the NOS

- Data and Resource sharing
- Performance
- Security
- Robustness
- Scalability
- Memory management
-

Software Components

These are some programs which are installed on the network machines.

Networking Operating System– Novel Netware, MS Windows NT, MS Windows server (2000, 2003, 2008, 2016, 2019), Unix, Linux.

In client machines – any supportive Network OS are to be installed like Win8, win10.

Protocol Suite – OSI Model (Open System Interconnections), TCP / IP Model

Examples of Networking Operating System

- Microsoft Windows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows 2000
- Novell NetWare
- Mac OS X
- Linux
- UNIX

CHAPTER-14
INSTALL OF NOS

Windows NT Servers

The Windows Server operating system was first introduced in the 1990s, and Microsoft branded it with “NT” (short for “New Technology”) up until the year 2000. The company had several releases of the NT version of the operating system, as follows: Windows NT 3.1, Windows NT 3.5, 3.51, Windows NT 4.0

The Evolution of Windows Server

In 2000, the branding for Windows servers changed. Microsoft dropped the “NT” and released Windows Server 2000 to highlight its relevance for modern systems. After that, the server versions were named based on the year each edition was released.

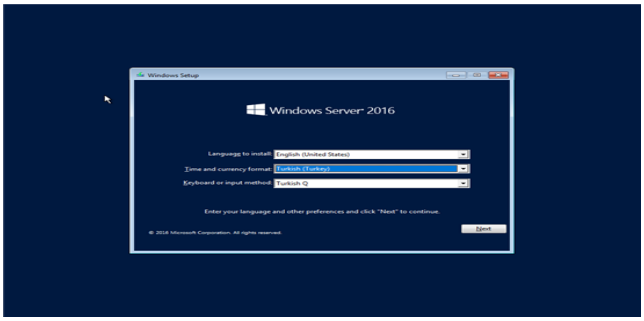
Windows Server 2000, Windows Server 2003, WS 2003 R2, WS 2008, WS 2008 R2, WS 2012, WS 2016, 2019 etc.

Installation of NOS

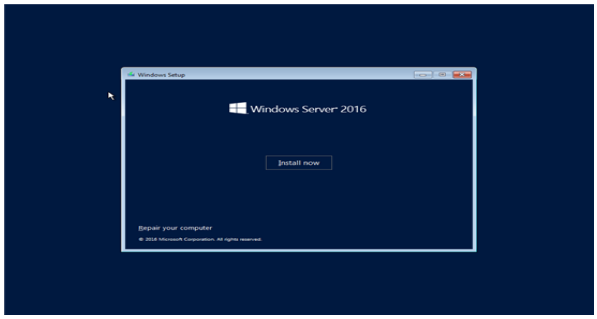
Windows Server 2016 Installation

First boot your system by using windows server 2016 installation disc .

Installation started now, on this screen we can able to configure language, region and time, keyboard settings. We should configure correct settings here and then select “Next” for continue.

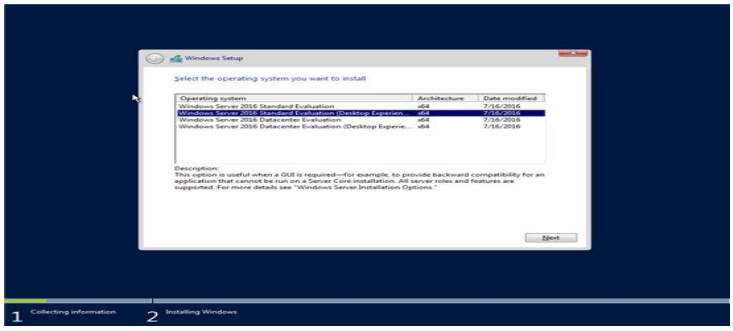


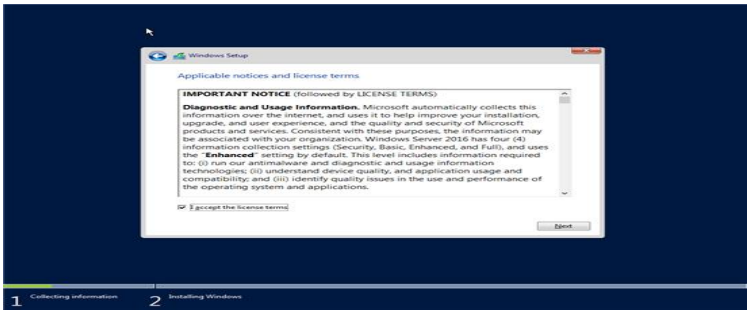
We should select “Install Now” in coming screen.



We can choose the Server 2016 version on this menu. We need Server 2016 Standard with GUI so selected “Server 2016 Standard (Desktop Experience).

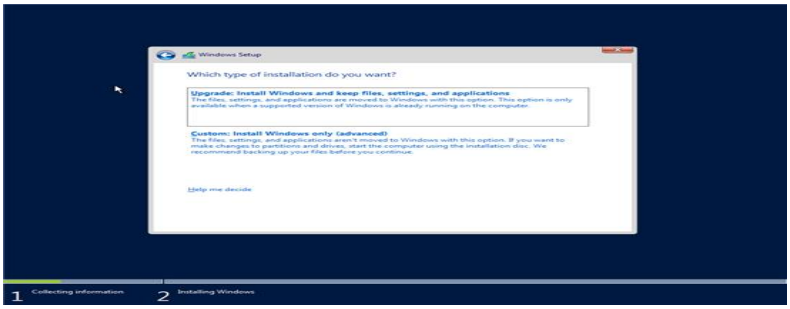
Also, if you need to install Server 2016 without GUI you should select “Windows Server 2016 Standard” here. Further Windows Server 2016 has different edition: Datacenter, Standard and Essentials editions.



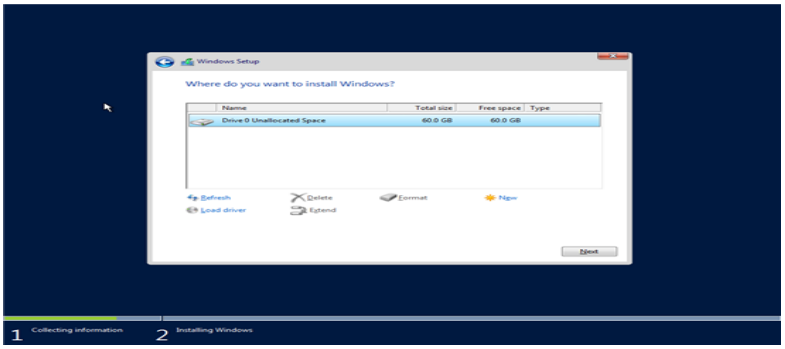


We can see the licence terms on this screen, select “I accept Licence Terms” then click Next to continue.

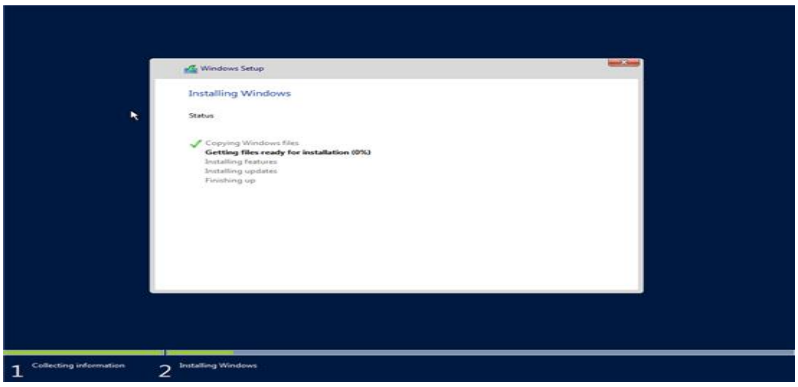
Select “Custom: Install Windows only (advanced)” here because we will do a clean installation OS. But if you need an in-place upgrade you should select “Upgrade: Install and Keep files, settings and applications” here. This option suitable for supported OS, features, services and roles. But keep in mind you should not prefer in-place upgrade for critical roles like Active Directory Directory Services, etc.



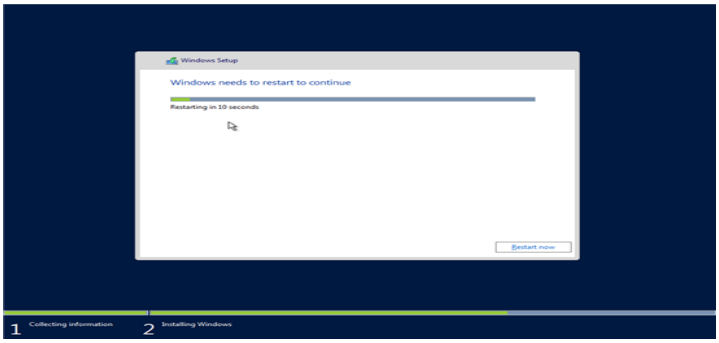
We can select and configure disc information on this screen. (You can set the installation disc, size, etc.) Used default settings here.



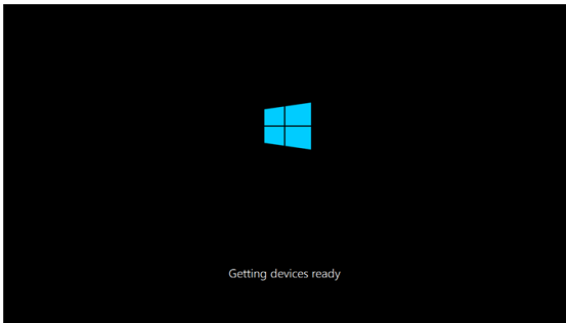
You can see that the necessary files are copied and the installation process is running on this screen



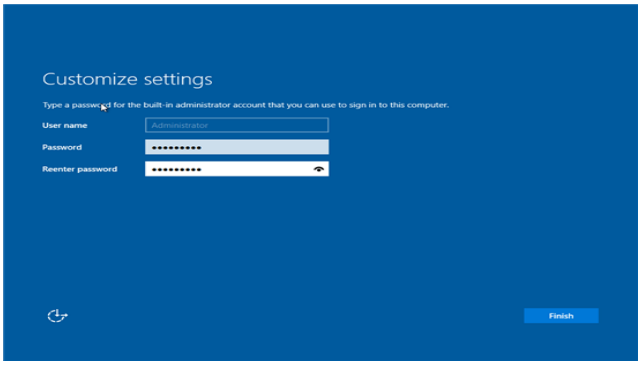
The installation process is done and rebooting.



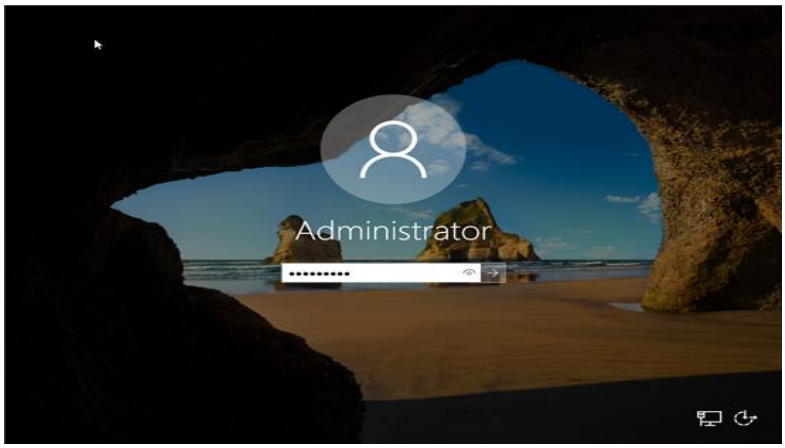
Screen showing that the necessary settings were made before the server was started.



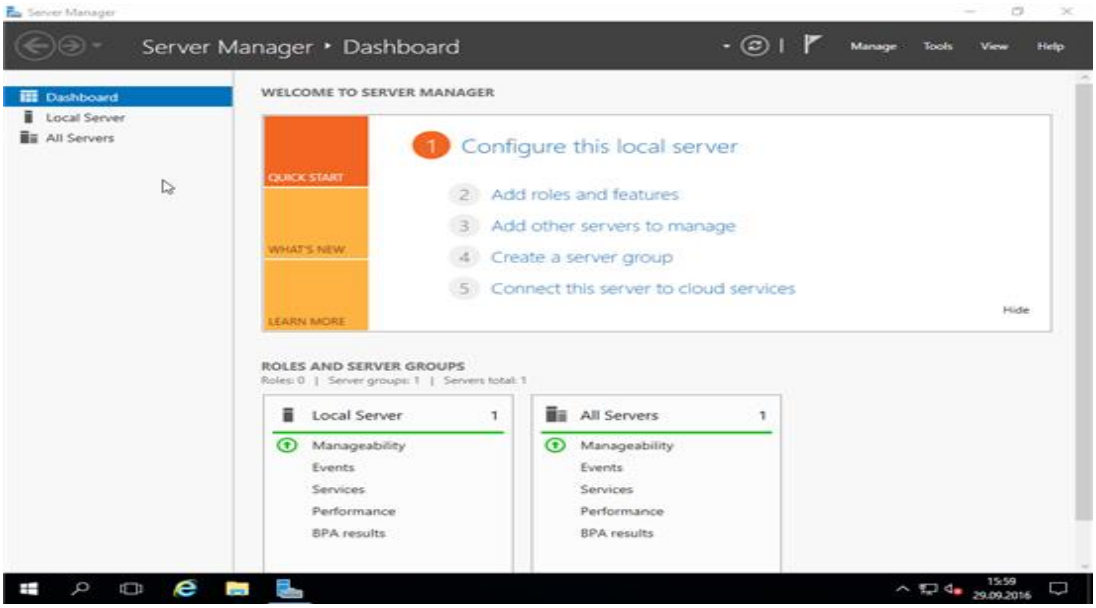
We can set a password for the local administrator account. You should configure a secure password for local admin.



On the login screen, we can login with “Administrator” account and related password.



And finally, you can see new Server 2016 interface. It’s similar to old Server 2012 interface but there are a lot of new features coming with Server 2016.



you should fully patch new Server 2016 before you add or configure roles, services.

CHAPTER-15

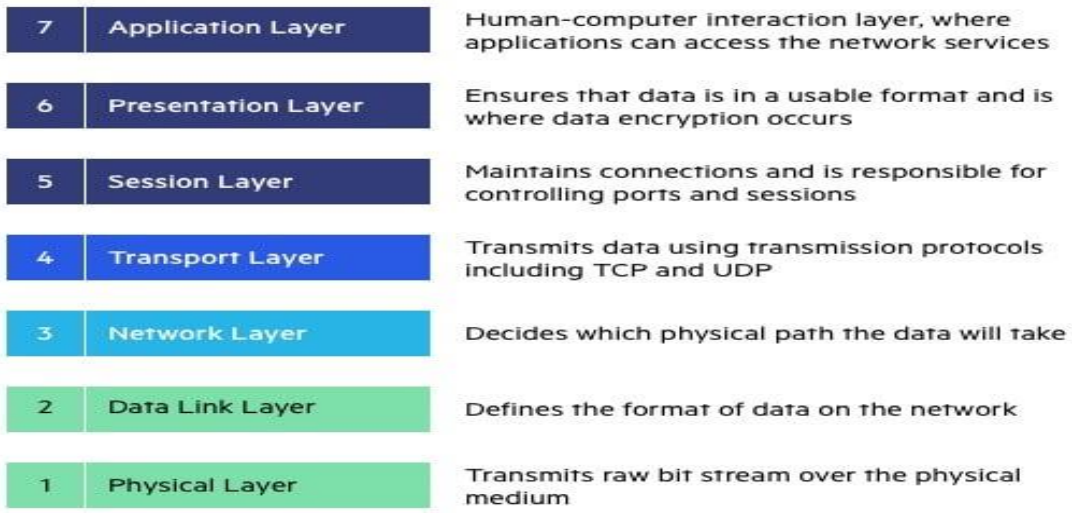
Layers of network

What Is the OSI Model

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. It was the first standard model for network communications, adopted by all major computer and telecommunication companies.

The OSI reference model describes how data is sent and received over a network. This model breaks down data transmission over a series of seven layers. Each layer has a responsibility to perform specific tasks concerning sending and receiving data. All of the layers are needed for a message to reach its destination.

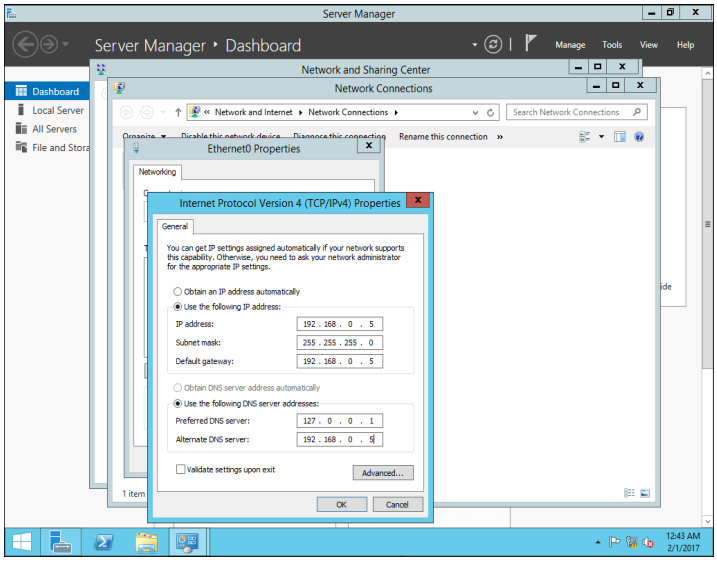
The OSI 7 Layers



Install and Configure (NOS) Windows Server 2016 Active Directory Domain Services (ADDS)

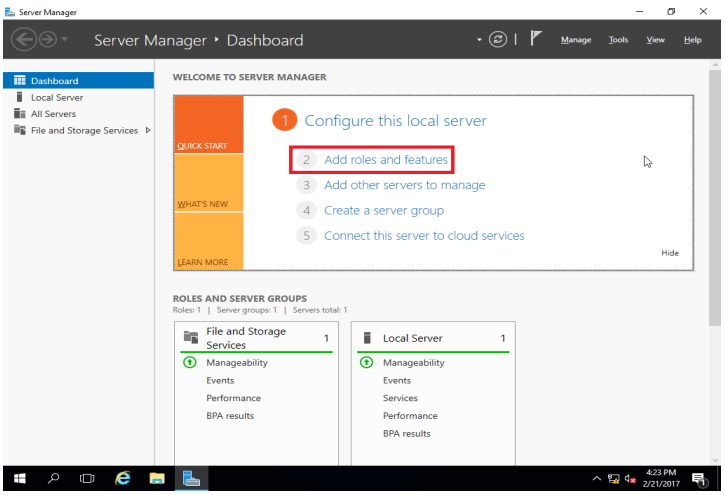
Some preparation:

- Create a strong password for the Administrator account (it will be Domain Admin in future);
- Install all updates;
- Rename your server by Corporate naming policy. (When you install Windows Server, a random name generated);
- Assign a static IP to your server.

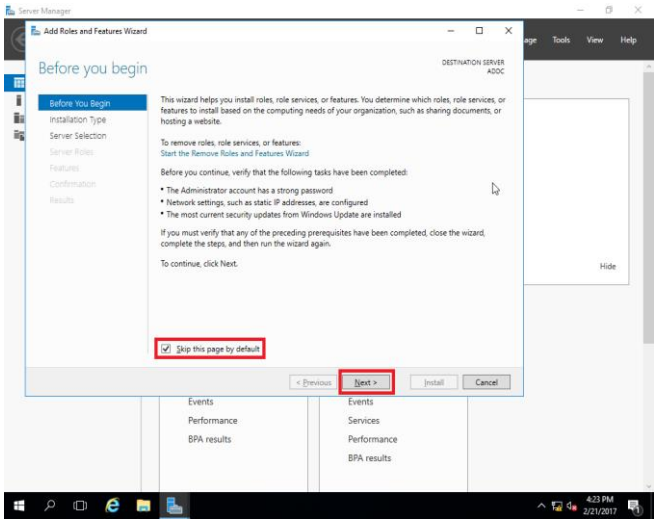


Installation

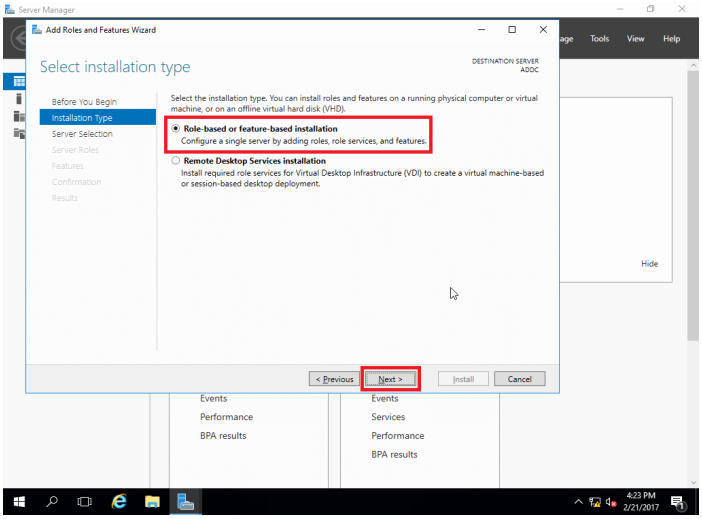
1. After Server Manager starts – click on **Add roles and features link**;



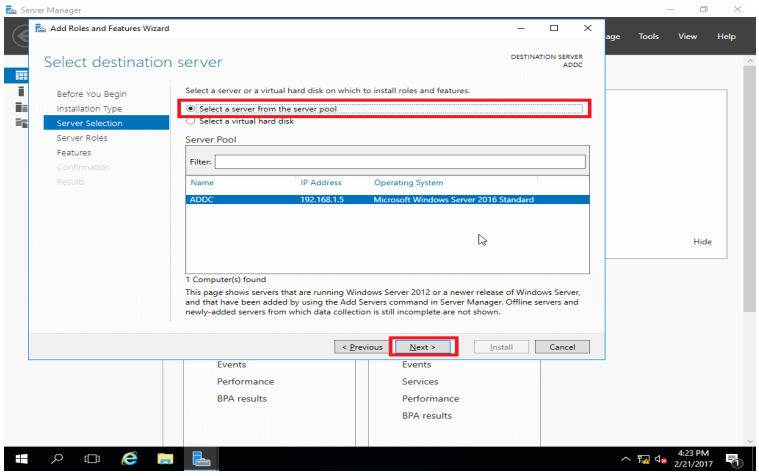
2. Click **Next** button on the wizard screen. Also, you may set check mark **Skip this page by default** and you don't see this step at next runtime;



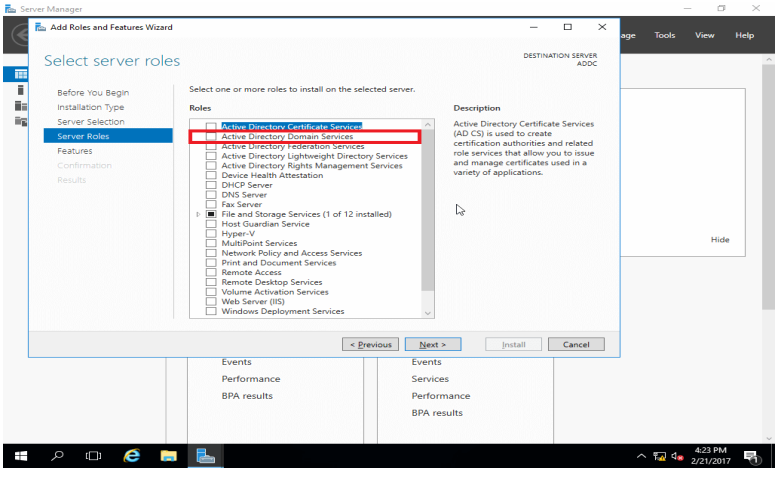
3. For installation type, select **Role-based or feature-based installation** and click **Next** button;



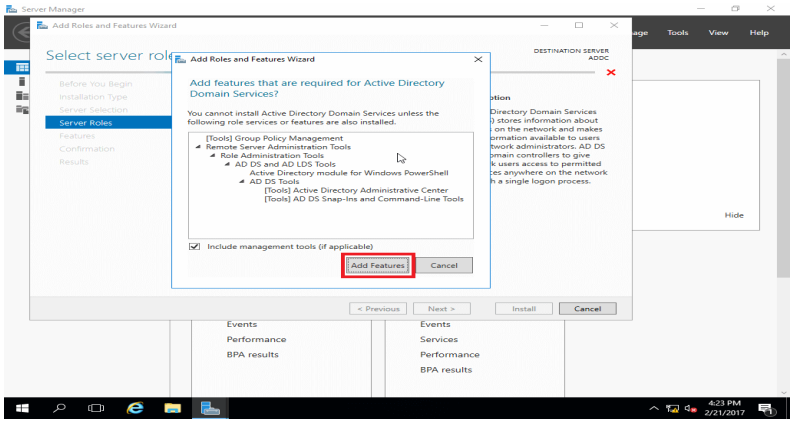
4. Choose option **Select a server from the server pool** (selected by default) and click **Next** button;



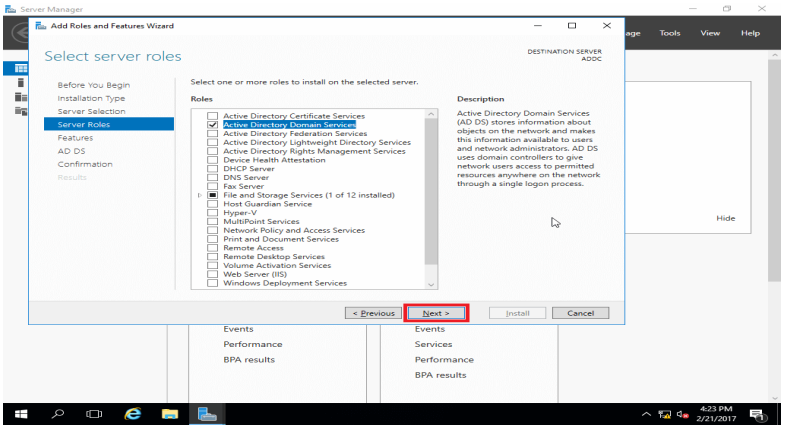
5. Click box for **Active Directory Domain Services**;



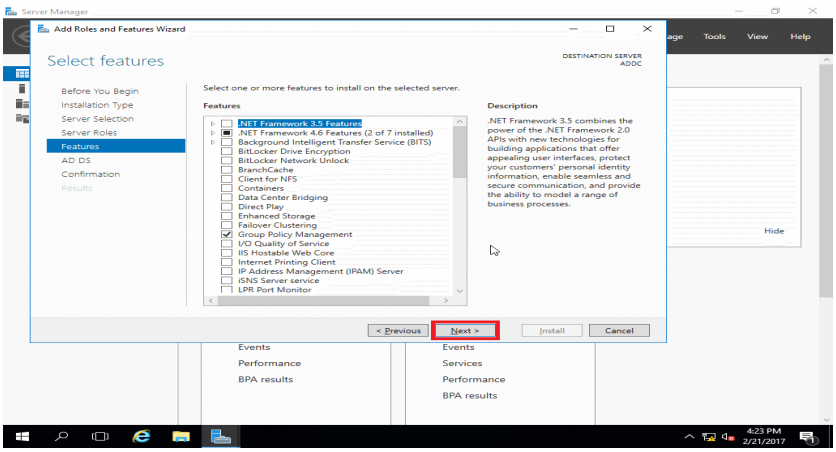
6. In the new pop-up window click **Add Features**;



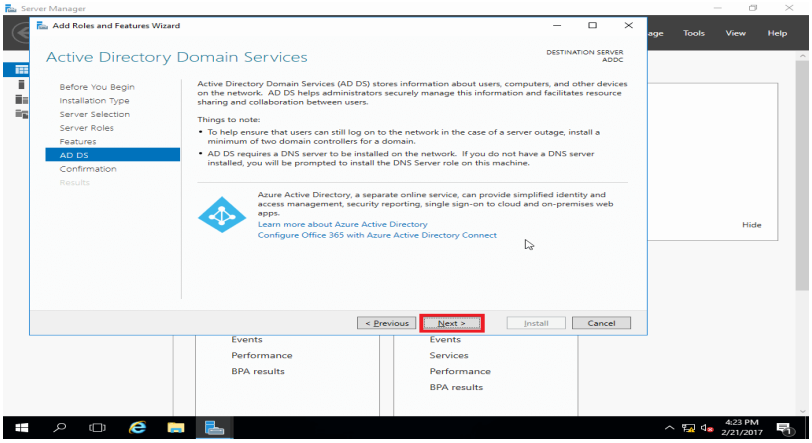
7. Click **Next** button;



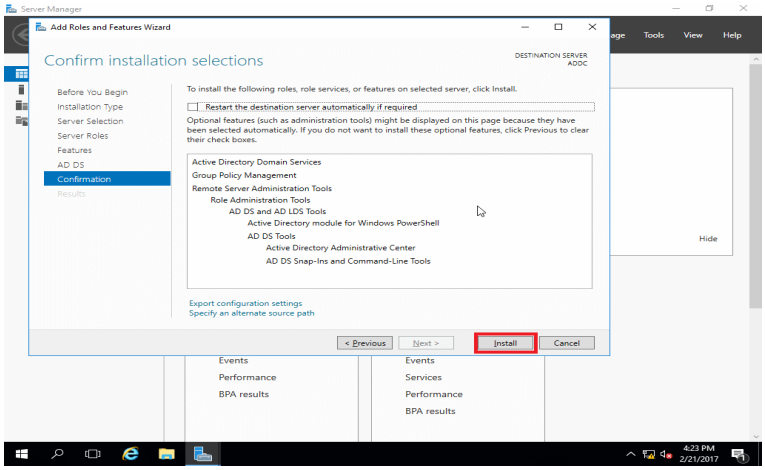
8. For Features, don't select anything, click **Next** button;



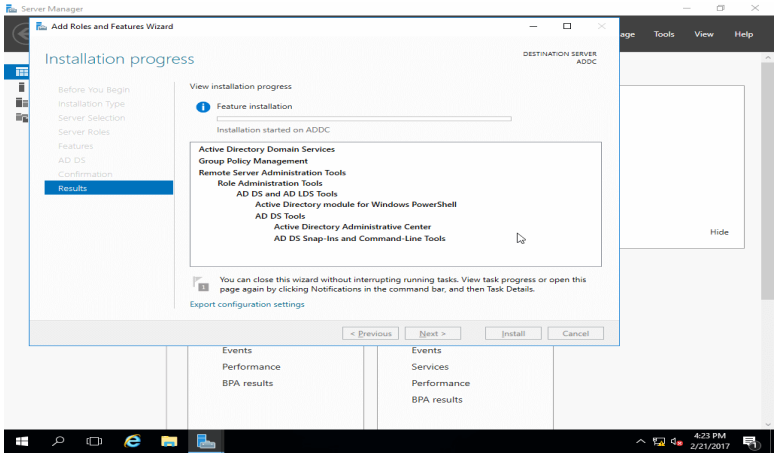
9. For Active Directory Domain Services click **Next** button;



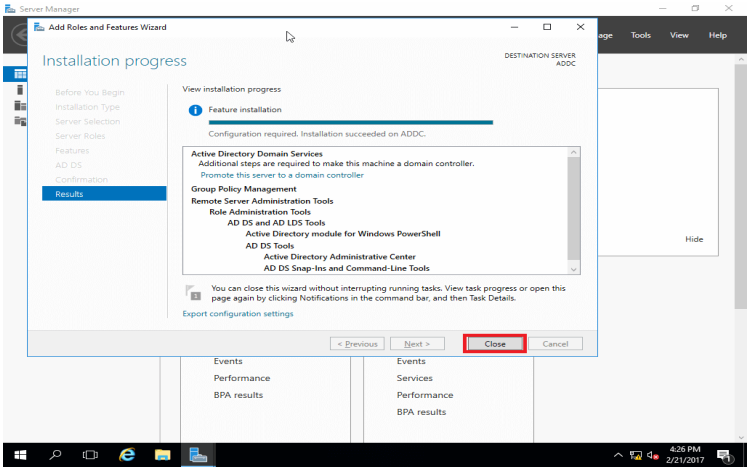
10. At the confirmation screen, you may decide whether to restart the destination server automatically or not, in my case, I don't set this option. Click **Install** button;



11. Installation begins;

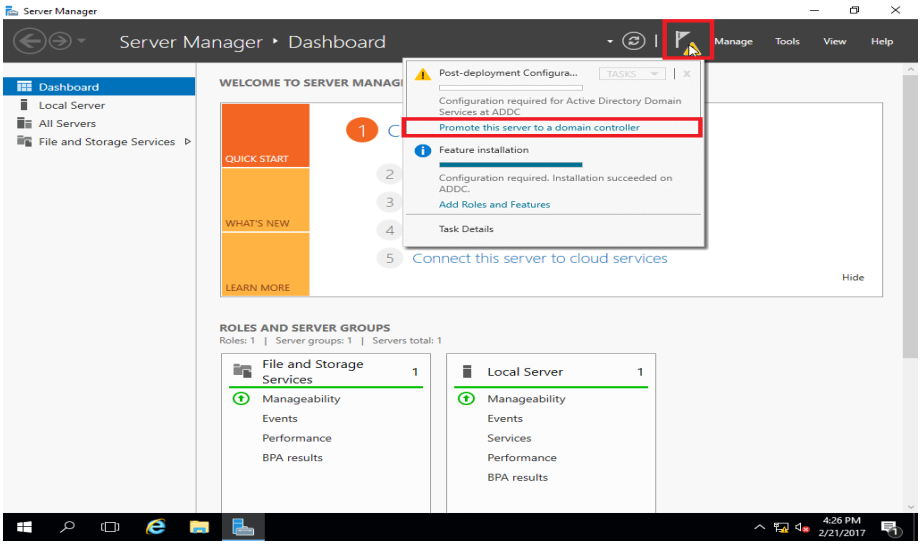


12. Once completed, click the **Close** button.

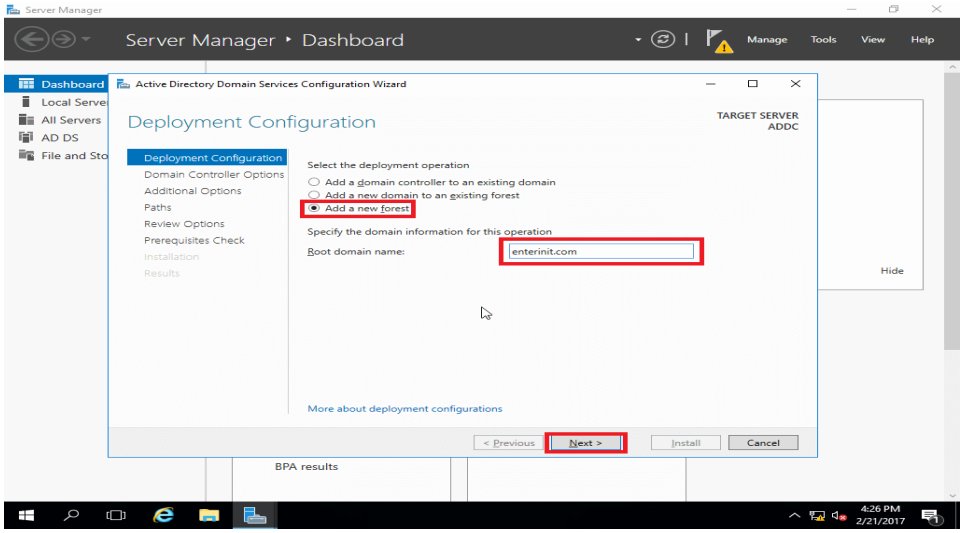


Configure ADDS

1. From the **Server Manager dashboard**, click the flag with the exclamation mark symbol. Click **Promote the server to a domain controller**;

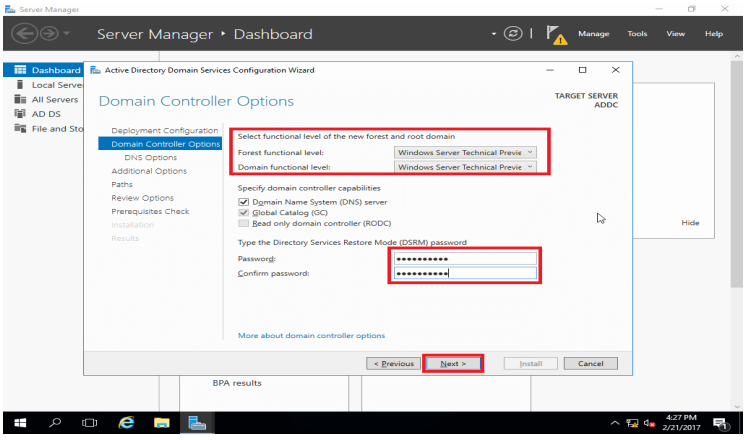


2. On the next screen, select the deployment operation that is needed. In this example, the **Add a new forest** is selected and the name **enterinit.com** is entered to create a new root domain. Click **Next** button;

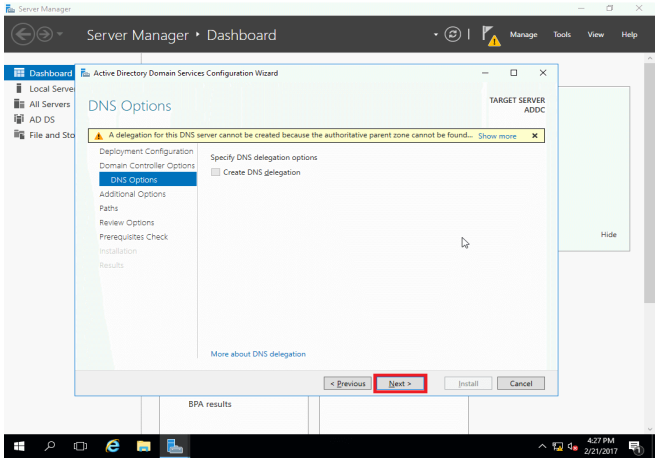


3. Since this will be the only domain controller in this lab example, both the forest and domain functional levels will remain at **Windows Server Technical Preview** (I use Windows Server 2016 from VLSC, but is recognized as Technical Preview). Leave checkbox on the **Domain Name System (DNS) Server** to make this system a DNS server. The option for GC is checked without the ability to modify since the first domain controller must be a **Global Catalog** server. The third option is unchecked and unmodifiable because the first domain controller cannot be a **Read-Only Domain Controller**;

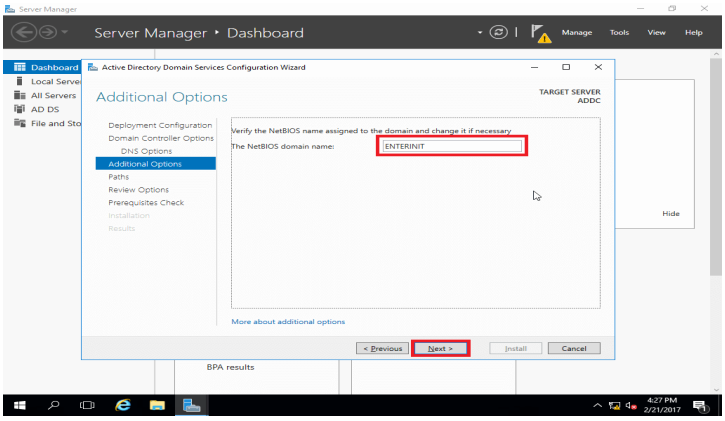
4. Enter a DSRM password and click **Next**;



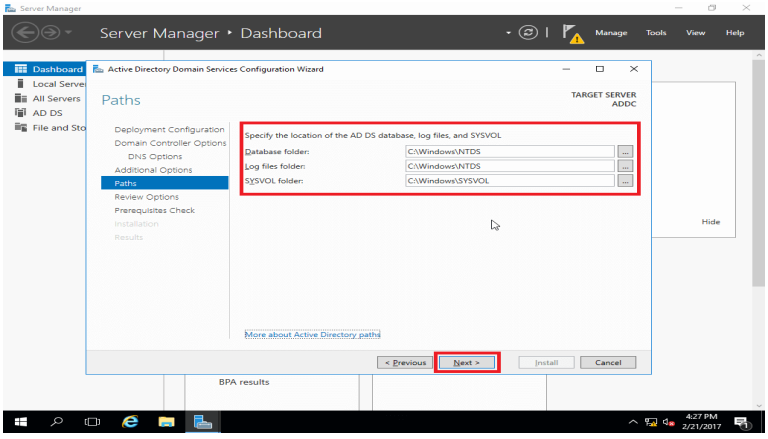
5. For DNS options, there is no existing DNS infrastructure since this is our first domain controller. So, the warning can be ignored. Click **Next** button;



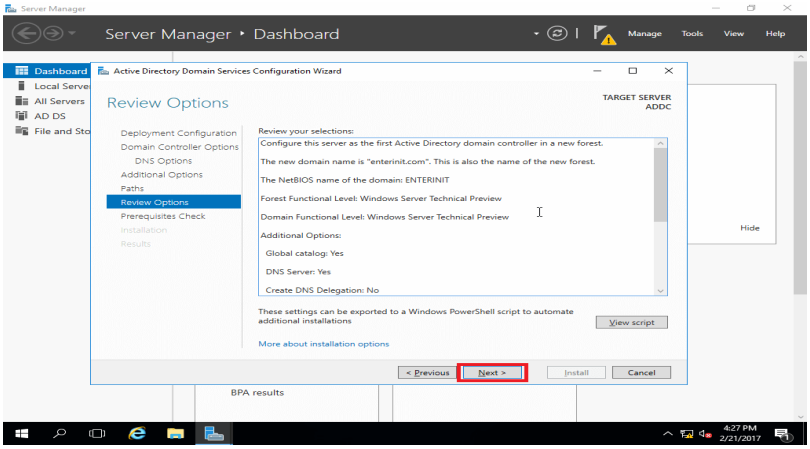
6. Enter **BIOS domain name** and click **Next** button;



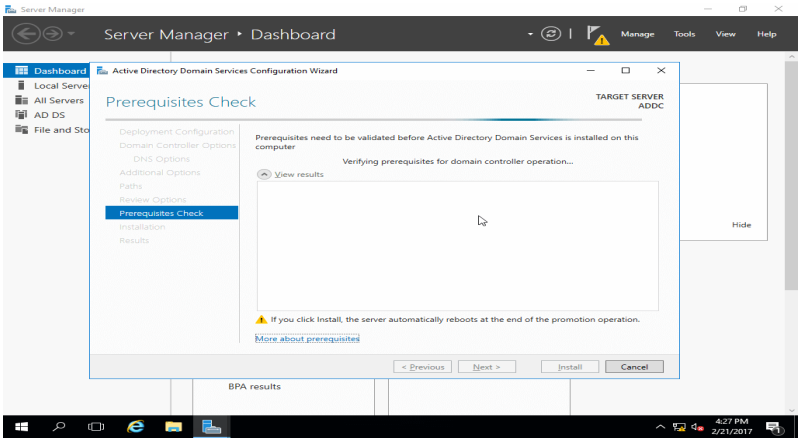
7. If you need you may change folders locations (**NOT RECOMENDED**), click **Next** button;



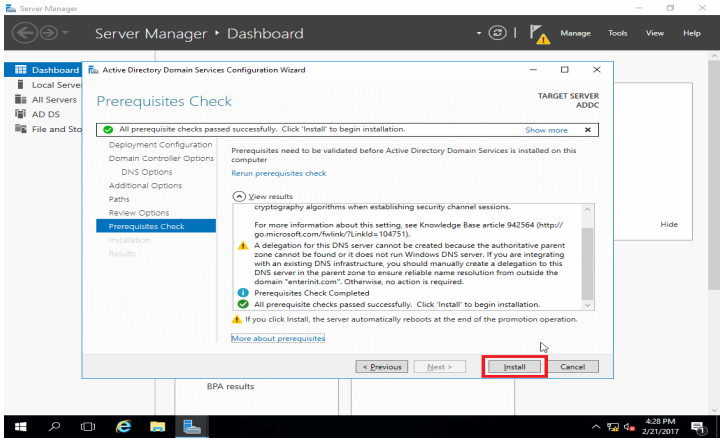
8. Review options. Please note that a PowerShell shell script is provided if you need to automate this on future installs. Click **View Script**. If needed, copy this script for future use. Close Notepad window and click **Next** button;



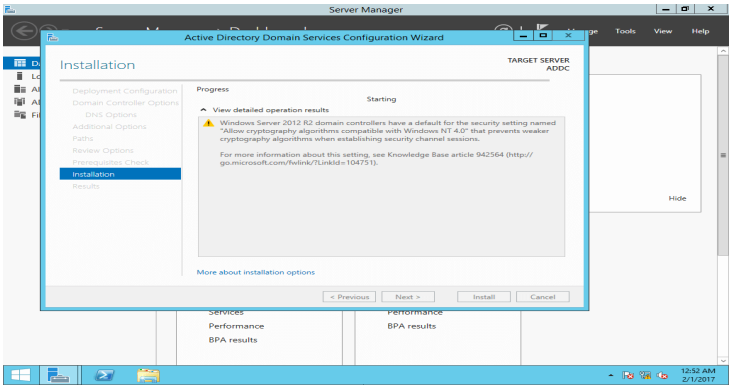
9. System check prerequisites;



10. If the prerequisites check passes, then click **Install** button;

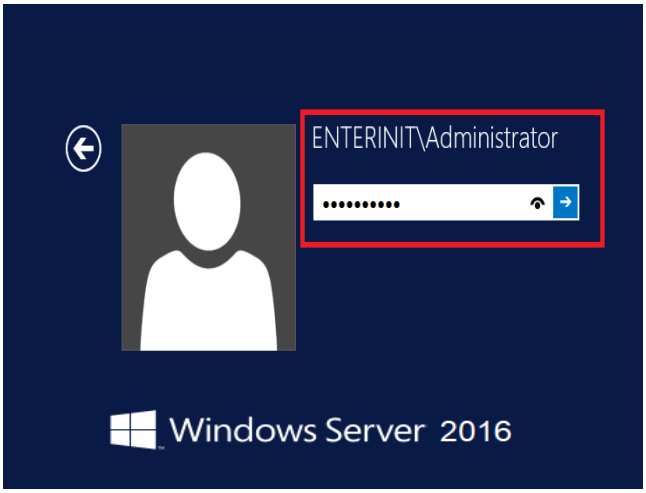


11. The installation will begin;



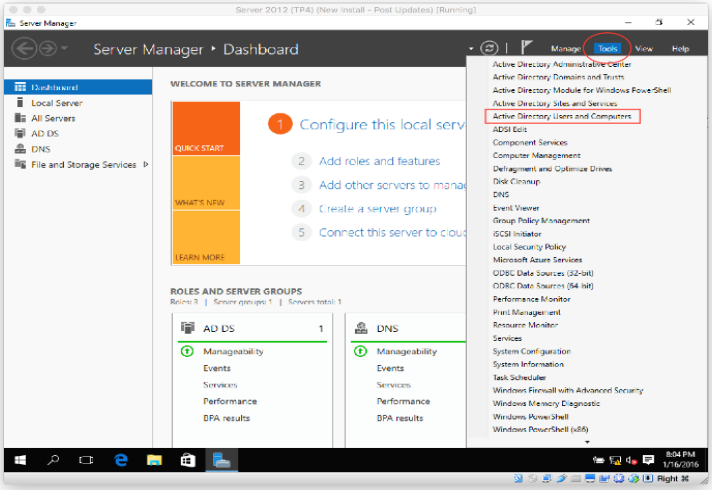
12. Once complete – system will be rebooted

13. After reboot you may sign to PC as **Domain Admin**;

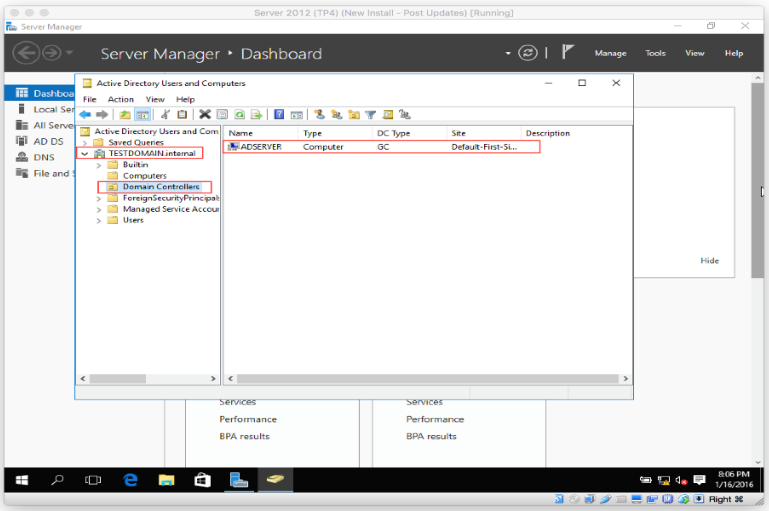


14. Let's verify Active Directory is setup and our server is classified as a DC (domain controller).

From within **Server Manager**, click **Tools** then **Active Directory Users and Computers**.

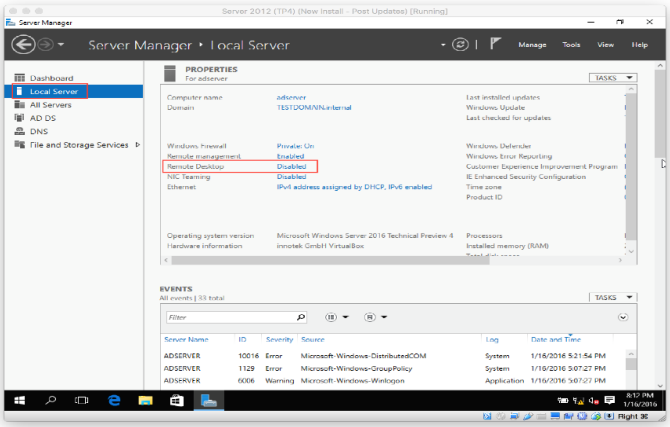


15. Expand the domain root (in my case, it's TESTDOMAIN.internal), then click on **Domain Controllers**.



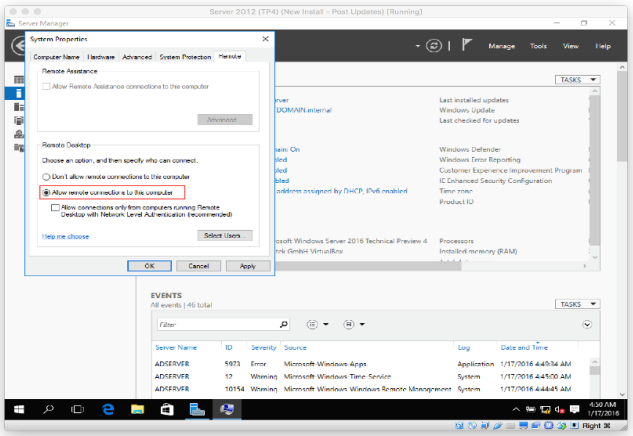
16. enable RDP (Remote Desktop Protocol).

- From **Server Manager Dashboard**, click **Local Server** then click **Disabled** next to Remote Desktop.



17. Select **Allow remote connections to this computer**

- **Uncheck** the option **Allow connections only from computers running Remote Desktop with Network Level Authentication**, then click **OK**.



We are done with the basic Active Directory setup!

CHAPTER-16
MODEM, ROUTER, SWITCH & CONFIGURATION

Routing & Switch

Routing and switches are two vital parts of any computer network. A switch is a piece of hardware that connects devices on a network, directing communications traffic within the network as terminals and hardware devices send data to one another. Routing is the part of the network protocol that directs individual packets of data to the right destination.

PRINICIPAL TERMS

bridge: a connection between two or more networks, or segments of a single network, that allows the computers in each network or segment to communicate with one another.

firewall: a virtual barrier that filters traffic as it enters and leaves the internal network, protecting internal resources from attack by external sources.

gateway: a device capable of joining one network to another that has different protocols.

node: any point on a computer network where communication pathways intersect, are redistributed, or end (i.e., at a computer, terminal, or other device).

packet forwarding: the transfer of a packet, or unit of data, from one network node to another until it reaches its destination.

packet switching: a method of transmitting data over a network by breaking it up into units called packets, which are sent from node to node along the network until they reach their destination and are reassembled.

Routing

Routing is the method by which a packet of data is transmitted to its destination. In computer networks, routing is accomplished by packet switching. This term describes how packets of data are moved from one node to another in a network. A network is made up of multiple nodes, which can be devices such as printers or computers. Nodes can also be network hardware such as switches, which direct network traffic. These devices communicate with each other by sending messages over the network. Each message is divided into units of data called “packets,” which are sent across the network individually and then reassembled once they all reach their destination. Each packet may take a different path to the destination, because when a packet reaches a node, it is forwarded to another node based on the state of the network at that instant. This is called **packet forwarding**.

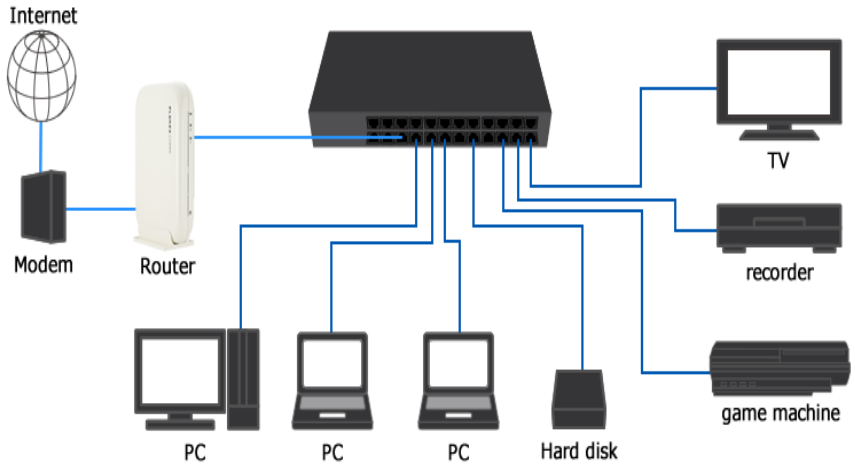
Network Switch vs Router

- Network switch and router are both computer networking devices that allow one or more computers to be connected to other computers, networked devices, or to other networks.
- While switches allow different devices on one network to communicate, routers allow different networks to communicate.
- Actually, a **switch creates networks while a router connects networks**.
- By the way, routers can be used in LANs, WANs, and MANs because they have both WAN and LAN ports, while switches can only be used in LANs.
- In addition, a router uses IP address for data transmission, while a network switch uses the MAC address.
- A **network switch** is used to connect multiple devices such as computers, printers, IP camera and modem on the same network within a building. In this way, these devices can share information and communicate with each other.
- A **router** is connected to a modem at one side and many other devices on the other side. Because the modem will only talk to the first computer that talks to it, the router at the position serves like a dispatcher to share the connection among all your devices. This enables all connected computers to share one single Internet connection.

Modem

Modem is short for "Modulator-Demodulator." It is a hardware component that allows a computer or another device, such as a router or switch, to connect to the Internet. It converts or "modulates" an analog signal from a telephone or cable wire to digital data (1s and 0s) that a computer can recognize. Similarly, it converts digital data from a

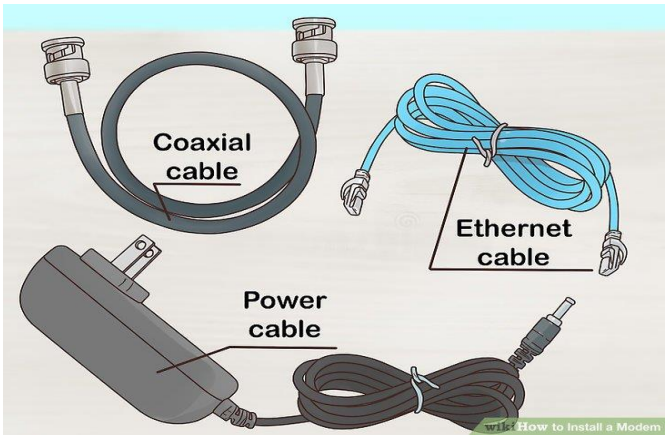
computer or other device into an analog signal that can be sent over standard telephone lines.



Configuring Modem , Router & Switch

How to install a modem for your home or workplace Internet. If you want to have Wi-Fi, you will need to buy a router and connect the modem to the router as well.

1. **Make sure that your modem will work with your Internet subscription.** While rare, some modems encounter issues when paired with a specific Internet company
2. **Find your room's cable output.** there will be a cable connected to the cable outlet.
3. **Decide the place to mount the modem.** U need to have a power outlet nearby.
4. **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 outlet. Both of these cables should come with your modem. If you plan on attaching the modem to a router, you will also need an Ethernet cable.
5. **Read your modem's user manual instructions.**
6. **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.



7. 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.

8. **Plug your modem's power cable into an electrical outlet.**

9. **Insert the modem power cable's free end into the modem.** You'll usually find the power cable input port at the bottom of the back of the modem.

10. Place your modem in its spot. With the cables attached, gently move your modem into its designated position.

11. **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 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.

- You can also connect your computer directly to your modem via Ethernet if you have an Ethernet port enabled computer.

How to configuring BSNL DSL W200-SY wireless modem.

1. The main line from Telephone pole will go to a small device called ADSL splitter. The splitter has one input i.e. main telephone line and two output, one is phone and other is the modem. You need to connect an RJ 11 cable coming out from the splitter '***Phone***' port to your Telephone and from splitter '***modem***' port to the ADSL modem. Now connect the one end of RJ45(LAN/Ethernet) cable to one of the LAN port of your modem and another end to your PC/Laptop.
2. Manually assigning IP to your PC/Laptop

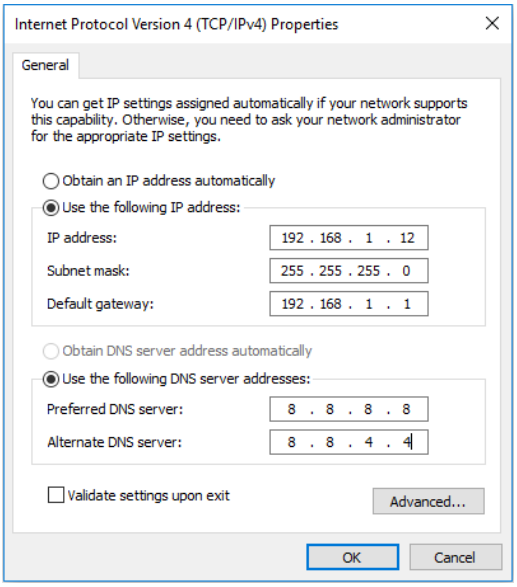
Now this step is not absolutely necessary for every ADSL modem but this particular modem of BSNL has a legacy of not being able to provide IP dynamically to its connected device. So it is always a good practice to assign IP manually to your PC/Laptop before using it. To do this:

A) Go to *Control panel* of your computer.

B) Go to Network and the internet → Network and sharing center → change adapter settings

C) Right click on "**Ethernet**" or **"Local Area Connection"** whatever it appears. On my Laptop, it is showing as Ethernet and someone else's PC it might show like 'Local Area Connection'. After right clicking on it select **Properties**. Now select **Internet Protocol version 4 (TCP/IP V4)** and then again **click on properties.**

Here you need to provide IP address manually. Follow the below given image and put it on your PC accordingly. Once you are done putting the IPs, **click OK.**



Now if you are connecting more than one PC/Laptop using the ethernet cable then you should assign different IP to each one of them. For example, if you are using 3 PC/Laptop connected via Ethernet cable then do it as mentioned below.

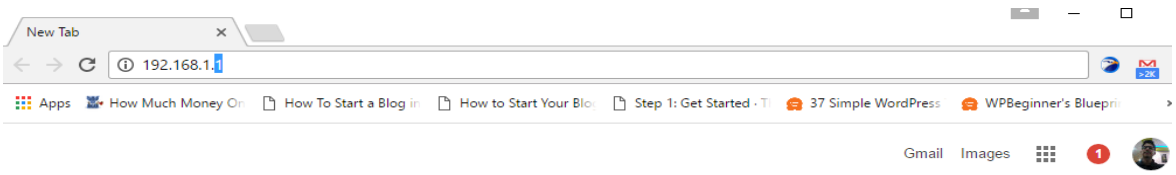
After assigning the IP we will now put your broadband user id and password in the modem.

You can assign any IP to your PC/Laptop ranging from 192.168.1.12 to 192.168.1.254. But please do remember the fact that you can not assign the same IP to two devices. If I put it in simple, assign one unique IP to each connected PC/Laptop. Otherwise, IP Conflict will occur.

1st PC/Laptop	IP address: 192.168.1.12 Subnet mask: 255.255.255.0 Default Gateway 192.168.1.1 Primary DNS: 8.8.8.8 Secondary DNS: 8.8.4.4
2nd PC/Laptop	IP address: 192.168.1.13 Subnet mask: 255.255.255.0 Default Gateway 192.168.1.1 Primary DNS: 8.8.8.8 Secondary DNS: 8.8.4.4
3rd PC/Laptop	IP address: 192.168.1.14 Subnet mask: 255.255.255.0 Default Gateway 192.168.1.1 Primary DNS: 8.8.8.8 Secondary DNS: 8.8.4.4

3. Configuring Your Modem

A) Type **192.168.1.1** on your PC browser(Google Chrome, Mozilla Firefox, Internet explorer etc)

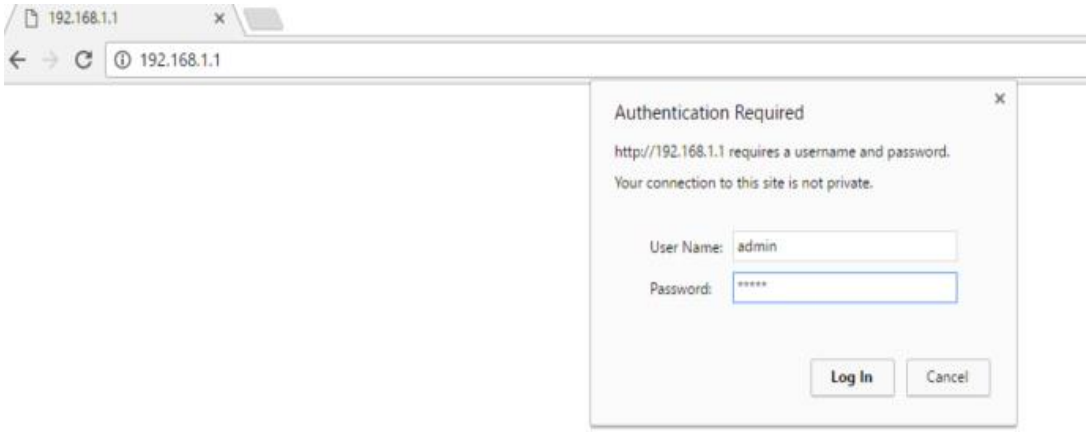


It will be asked for a username and password. Type

Usernae: admin

Password: admin

Press Enter now.



B) Now you will see a device **status** page.

C) Now click on **Interface setup** and then on **the internet**.

Here you need to select **ISP: PPPoA/PPPoE**

VPI=0, VCI= 35 And fill **service name: BSNL**

Username: this will be your broadband user id. BSNL(internet service provider) will provide this at the time of connection. Contact BSNL if you don't know the username.

Password: password

Once you get you get your username, put it on the appropriate field. After putting username and password click on SAVE button. This username and passwordd is provided by the ISP(BSNL) or any other.

D) Wifi Setup

To set up your wifi, click on wireless.

Check **Access Point Activated**.

Wireless Mode: 802.11 b+g+n

SSID: Put any name here. This will be your wifi access point name.(list of wifi name)

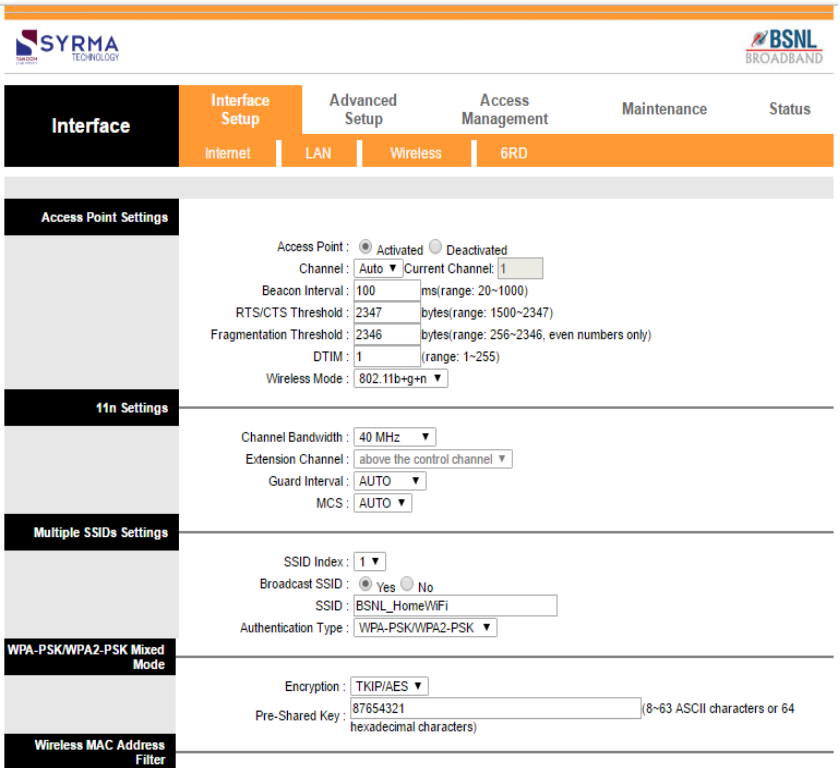
Authentication type: WPA-PSK/WPA 2 PSK

Encryption: TKIP/AES

Pre-shared key: This will be your wifi password.

Wireless Mac address Filter: Deactivated.

Now click on **SAVE** button and close the browser.



How to Configure Router Settings

Accessing Your Router

First, go to your settings and click on “**Network & Internet**.” Then select “**View your network properties**.” You should see “**Default gateway**” and a number beside it. This number is your router IP address. Type this address into your web browser’s search bar and a login or welcome page should appear.

From this point, you’ll need to log in as an administrator. Admin info should be on the back of the router.

Changing Router Login Info

- Access your router settings by inputting your router IP address into your browser
- Log in with router username and password
- Visit “Settings” and click on “Change Router Password”
- Input your chosen password (keeping in mind a strong password should have at least eight characters and feature letters, numbers, and special characters) and save the new settings

Changing Router IP Address

These instructions are for D-link routers, though the process is likely to be similar for other router types.

- Access your router settings by inputting your router IP address into your browser
- Log in with router username and password
- Visit “Settings” and click on “Network settings”
- Type in the new IP address under “Router Settings” and save the changes
- Note, you won’t be able to use the old IP address to access your router settings anymore

Changing SSID

- Access your router settings by inputting your router IP address into your browser
- Log in with router username and password
- Visit “Setup” and click on “Wireless settings”
- Input your new SSID and save the new settings
- You’ll then have to wait for your router to restart

Configuring Guest Wi-Fi and Multi-SSID

These following instructions are based on NETGEAR router settings, but again the process will be similar for other router types.

- Access your router settings by inputting your router IP address into your browser
- Log in with router username and password
- Visit “Guest Network” and make sure the “Enable SSID Broadcast” check box is ticked
- Name the guest network and select a security option, then click “apply” to save the settings

Activating Remote Management

- To access your router remotely, follow these instructions:
- Go to your router’s administration panel
- Visit “Settings,” then “Remote Management”
- Turn remote management on and save the settings

Gaining Visibility of Who Is Connected

- Access your router settings by inputting your router IP address into your browser
- Log in with router username and password
- Visit “My Network” or something similar. It may also be under “Attached devices”
- If you see an unfamiliar device you don’t think should be connected, ban its MAC address

Changing Wireless Band and Channel

Before changing your wireless band and channel, carefully consider what would be most suitable for your needs. For example, if you have a new router supporting 5GHz bands, this is probably a good choice for you as it will probably be less crowded. This means it’s a great option in densely populated areas. To change these settings, follow

the instructions above to access your router settings and visit “Wireless Settings.” You should be able to tweak band and channel from here.

Setting Up Parental or Employee Controls

Setting up filtering or monitoring controls is simple. These controls should be under router settings, though keep in mind they may have a dedicated category within the system. In some cases, you may want to download a specialized program to integrate with your router for more fine-tuned control. Either way, I’d recommend setting up a PIN or password for access to these controls, so users can’t change the settings themselves.

How to Set up a Network Switch With a Router

If we have a small business or have a large house – sometimes a wireless network just won’t cut it. By the time all devices have been connected, speed can be a real issue. Connecting all our devices via LAN is the preferred option to maintain and guarantee speed throughout our network.

That means If we have less than 4 devices to use in one network, we can use one router connecting a modem and don’t need to expend our network. However, when the number of devices is over 4, a network switch is necessary. We can use the network switch to expend our wired network with more ports. There are various switches of different port counts such as 8-port, 16-port, 32-port switch available in the market.

Our router only has 4 LAN ports ? Now what to do ? Well the quickest and cheapest option is to add a network switch to your setup. A network switch will take a connection from a single LAN port on your router and then provide a connection to the number of ports your switch has. So, if you have purchased a network switch with 8 ports, we take a single port from your router to the switch and then you can connect another 7 devices from the 7 remaining ports on your switch! It’s easy – this is how:

Steps to Set up a Network Switch With a Router

Step 1: Unplug all the power supplies of cable modem, network switch and wireless router.

Step 2: Connect your modem to the telephone wire. After that, connect one end of an Ethernet cable to the Ethernet port on the back of the modem.

Step 3: Plug the other end of the Ethernet cable connected with modem into your router’s WAN port.

Step 4: Use another Ethernet cable to connect one of your LAN ports in router to a network switch port.

Step 5: Plug the power supplies of three devices (modem, router & network switch).

After the setup, your network is expended and you can connect more than 4 devices using the internet. All you need is to connect the additional devices to the switch's normal port with straight cables.

Normally, the connection order of the devices is modem -> router -> switch -> devices.

There are various switches of different port counts such as 8-port, 16-port, 32-port switch available in the market.

CHAPTER – 17

Procedure to create a network (lan) using at least 6 computers

How to set up a LAN (Local Area Network) to connect multiple Windows PCs.

Method - 1

A. Setting Up the LAN

1. Determine the number of computers you want to connect. The number of computers you're connecting will determine the type of network hardware you'll need.If you are connecting four or less computers, you'll just need a single router, or one switch if you don't need internet.

If you're connecting more than four computers, you'll want a router and a switch, or just a switch if you don't need internet.

2. Determine your network layout. If your installing a permanent LAN solution, you'll want to keep cable length in mind. CAT5 Ethernet cables should not run longer than 250 feet. If you need to cover larger distances, you'll need switches at regular intervals, or you'll need to use CAT6 cables.You'll need one Ethernet cable for each computer you want to connect to the LAN, as well as an Ethernet cable to connect the router to the switch (if applicable).

3. Obtain the network hardware. To create a LAN, you'll need a router and/or

a network. These pieces of hardware are the "hub" of your LAN, and all of your

computers will be connected to them. The easiest way to create a LAN where

every computer has access to the internet is to use a router, and then add

a network switch if the router doesn't have enough ports. A router will automatically

assign an IP address to every computer that is connected to it.

Switches are similar to routers but do not automatically assign IP addresses. Switches typically have many more Ethernet ports than a router has.

4. Connect your modem to the WAN port on the router. This port may be labeled "INTERNET" instead. This will provide internet access to every computer that is connected to your LAN. You can skip this if you're setting up a LAN without internet access.

- You don't need a router at all to create a LAN, but it makes things easier. If you just use a network switch, you'll need to manually assign IP addresses to each computer after connecting them.

5. Connect the switch to a LAN port on the router. If you're using a network switch to connect more computers, connect it to one of the LAN ports on the router. You can use any open port on the switch to make the connection. When connected, the router will provide IP addresses for every computer that is connected to either device.

Method - 2

B. Connecting Your PC

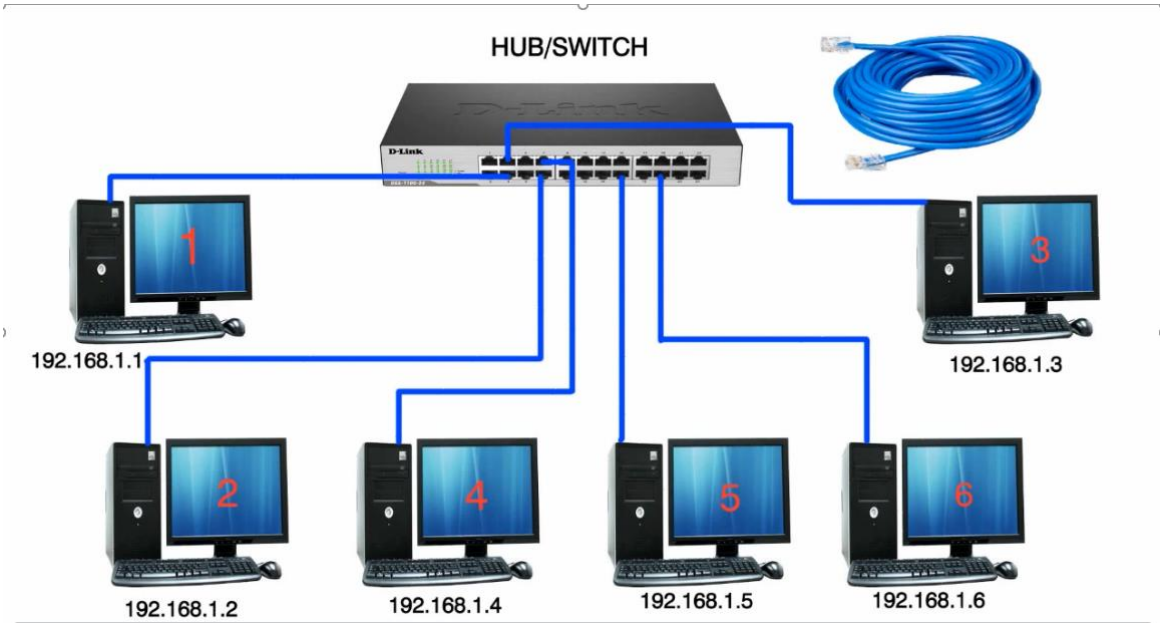
1. **Find the Ethernet port on your PC.** You can usually find this on the back of your desktop tower, or along the side or back of a laptop.Slim laptops may not have an Ethernet port, in which case you'll need to either use a USB Ethernet adapter or connect wirelessly if your router allows it.
2. **Plug one end of an Ethernet cable into your computer.** Make sure you're using an Ethernet cable (RJ45), not a telephone cable (RJ11).
3. **Plug the other end of the cable into an open LAN port.** This can be any open LAN port on either the router or the switch, depending on your LAN setup.
4. **Test out your network (router only).** If you're using a router, your work is complete. Once all of the computers are connected to a LAN port, they will be assigned IPs automatically and will appear on the network. If you set up your LAN for gaming, you should be able to start your LAN game and have each computer connect.If you're using a switch and no router, you'll still need to assign IP addresses to each computer.
5. **Enable file and printer sharing.** You won't be able to access resources on a networked computer until file and printer sharing is enabled. You can select specific files , folders, and drives to share on each computer, as well as share access to printer.

Method – 3

Assigning IP Addresses (No Router)

1. **Right-click on your network connection.** You'll see this in your System Tray. If you are connecting your computers through a switch with no router, you'll need to assign each computer on the network its own individual IP address. This process is handled automatically if you're using a router. Think of an IP address as a mailing address. Each computer on the network needs a unique IP address so that information sent across the network reaches the correct destination.

2. Click Open Network and Sharing Center.
3. Click the Ethernet link at the top of the window. You'll see this next to "Connections.“
4. Click Properties.
5. Click Internet Protocol Version 4 (TCP/IPv4). Make sure you don't uncheck it, just highlight it.
6. Click Properties.
7. Click the Use the following IP address radio button.
8. Type 192.168.1.50 into the IP address field.
9. Type 255.255.0.0 into the Subnet mask field.
10. Type 192.168.0.0 into the Default gateway field.
11. Click OK. This will save the settings for that computer. This computer is now configured on your network with a unique IP address.
12. **Open the Internet Protocol Version 4 properties on the next computer.** Follow the steps above on the second computer to open the Internet Protocol Version 4 (TCP/IPv4) Properties window.
13. **Click the Use the following IP address radio button.**
14. **Type 192.168.1.51 into the IP address field.** Notice that the final group of numbers has incremented by 1.
15. **Enter the same values for Subnet mask and Default gateway.** These values should be the same as they were on the first computer (255.255.0.0 and 192.168.0.0 respectively).
16. **Give each additional computer a unique IP.** Repeat these steps for each additional computer, incrementing the IP address by 1 each time (up to 255). The "Subnet mask" and "Default gateway" fields should be the same on each computer.



CHAPTER - 18
STUDY OF SCALING OF NETWORK

What is scalability?

In information technology, scalability (frequently spelled *scale ability*) has two usages:

1) The ability of a computer application or product (hardware or software) to continue to function well when it (or its context) is changed in size or volume in order to meet a user need. Typically, the rescaling is to a larger size or volume. The rescaling can be of the product itself (for example, a line of computer systems of different sizes in terms of storage, RAM, and so forth) or in the scalable object's movement to a new context (for example, a new operating system).
An example: In printing, scalable fonts are fonts that can be resized smaller or larger using software without losing quality.
2) It is the ability not only to function well in the rescaled situation, but to actually take full advantage of it. For example, an application program would be scalable if it could be moved from a smaller to a larger operating system and take full advantage of the larger operating system in terms of performance (user response time and so forth) and the larger number of users that could be handled.
It is usually easier to have scalability upward rather than downward since developers often must make full use of a system's resources (for example, the amount of disk storage available) when an application is initially coded. Scaling a product downward may mean trying to achieve the same results in a more constrained environment.
Scalability is the measure of a system's ability to increase or decrease in performance and cost in response to changes in application and system processing demands. Examples would include how well a hardware system performs when the number of users is increased, how well a database withstands growing numbers of queries, or how well an operating system performs on different classes of hardware. Enterprises that are growing rapidly should pay special attention to scalability when evaluating hardware and software.

Measures

Scalability can be measured in various dimensions, such as:

- *Administrative scalability*: The ability for an increasing number of organizations or users to easily share a single distributed system.
- *Functional scalability*: The ability to enhance the system by adding new functionality at minimal effort.
- *Geographic scalability*: The ability to maintain performance, usefulness, or usability regardless of expansion from concentration in a local area to a more distributed geographic pattern.
- *Load scalability*: The ability for a distributed system to easily expand and contract its resource pool to accommodate heavier or lighter loads or number of inputs. Alternatively, the ease with which a system or component can be modified, added, or removed, to accommodate changing load.
- *Generation scalability* refers to the ability of a system to scale up by using new generations of components. Thereby, *heterogeneous scalability* is the ability to use the components from different vendors.

Examples

- A routing protocol is considered scalable with respect to network size, if the size of the necessary routing table on each node grows as O(log *N*), where *N* is the number of nodes in the network.
- A scalable online transaction processing system or database management system is one that can be upgraded to process more transactions by adding new processors, devices and storage, and which can be upgraded easily and transparently without shutting it down.

The distributed nature of the Domain Name System allows it to work efficiently even when all hosts on the worldwide Internet are served, so it is said to "scale well".

What is Network Traffic?

Network traffic is the amount of data moving across a computer network at any given time. Network traffic, also called data traffic, is broken down into data packets and sent over a network before being reassembled by the receiving device or computer.Traffic is also related to security because an unusually high amount of traffic could be the sign of an attack.

Data Packets

When data travels over a network or over the internet, it must first be broken down into smaller batches so that larger files can be transmitted efficiently. The network breaks down, organizes, and bundles the data into data packets so that they can be sent reliably through the network and then opened and read by another user in the network. Each packet takes the best route possible to spread network traffic evenly.

Forwarding refers to the router-local action of transferring the packet from an input link interface to the appropriate output link interface.

Routing refers to the network-wide process that determines end-to-end paths that packets take from source to destination.

What is Port Forwarding?

In computer networking, **port forwarding** or **port mapping** is an application of network address translation (NAT) that redirects a communication request from

one address and port number combination to another while the **packets** are traversing a network gateway, such as a router or firewall. Port forwarding, or tunneling, is the behind-the-scenes process of intercepting data traffic headed for a computer's IP/port combination and redirecting it to a different IP and/or port. A program that's running on the destination computer (host) usually causes the redirection, but sometimes it can also be an intermediate hardware component, such as a router, proxy server or firewall.

How to Forward Ports on Your Router

How to Set Up Port Forwarding?

The traffic that passes through your router does so through ports. Every port is like a special pipe made for a specific kind of traffic. When you open a port on a router, it allows a particular data type to move through the router.

The act of opening a port, and choosing a device on the network to forward those requests to, is called **port forwarding**. Port forwarding is like attaching a pipe from the router to the device that needs to use the port—there's a direct line-of-sight between the two that allows data flow.

For example, FTP servers listen for incoming connections on port 21. If you have an FTP server set up that nobody outside your network can connect to, open port 21 on the router and forward it to the computer you use as the server. When you do this, that new, dedicated pipe moves files from the server, through the router, and out of the network to the FTP client that's communicating with it.

Every networking application needs a port to run on, so if a program or application isn't working when everything else is set up correctly, open the port on the router and forward requests to the right device (for example, a computer, printer, or game console). Port range forwarding is similar to port forwarding but is used to forward an entire range of ports.

Give the Device a Static IP Address

The device that will benefit from the port forward needs to have a static IP address. This way, you don't have to change the port forwarding settings each time it obtains a new IP address.

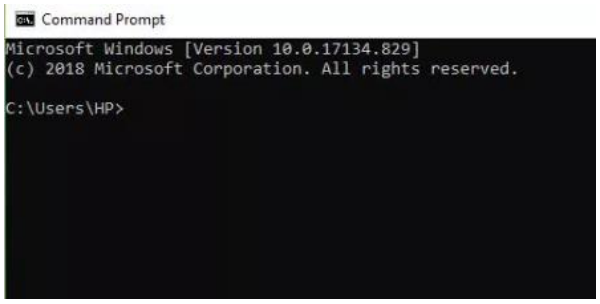
For example, if your computer runs torrenting software, assign a static IP address to that computer. If your gaming console uses a specific range of ports, it needs a static IP address.

There are two ways to do this: from the router and from the computer. When you set up a static IP address for your computer, it's easier to do it there.

USE YOUR COMPUTER TO SET UP A STATIC IP ADDRESS

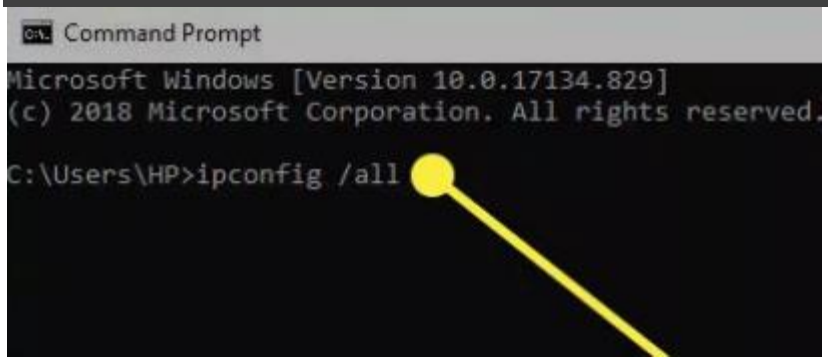
To set up a Windows computer to use a static IP address, first identify which IP address it's using currently.

1. Open Command Prompt on the computer.

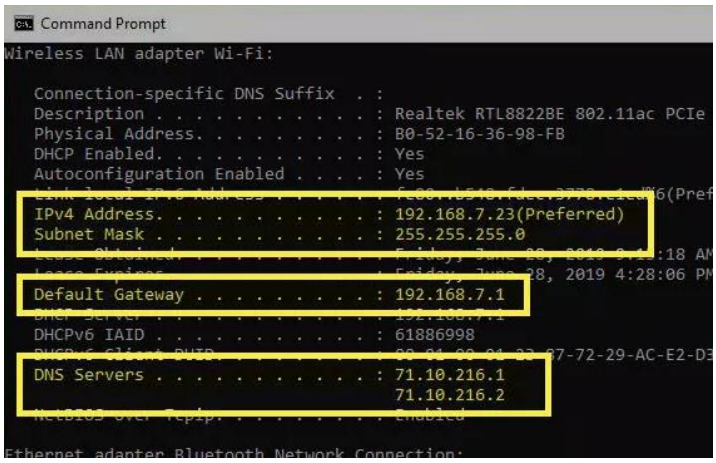


2. Type this command, then press **Enter**:

```
ipconfig /all
```

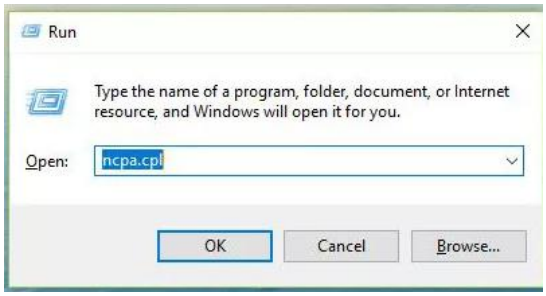


3. Record the following: **IPv4 Address**, **Subnet Mask**, **Default Gateway**, and **DNS Servers**.



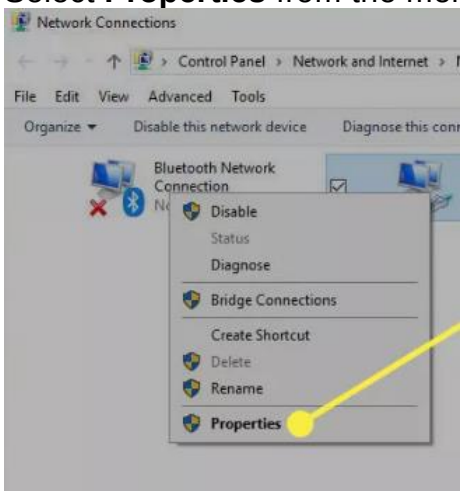
Now, you can use that information to set up the static IP address.

1. Open the **Run** dialog box (press **WIN+R**), enter **ncpa.cpl**, and select **OK** to open Network Connections.

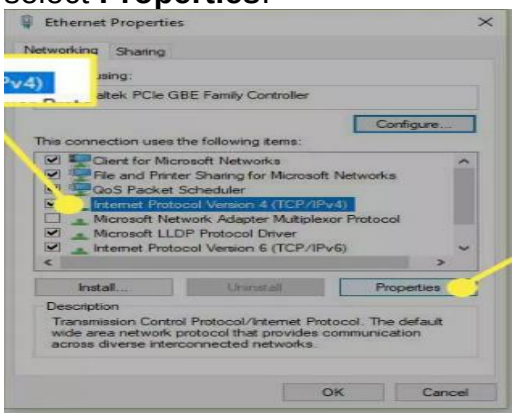


2. Right-click or tap-and-hold the connection that has the same name as the one you identified in Command Prompt. For example, **Ethernet0**.

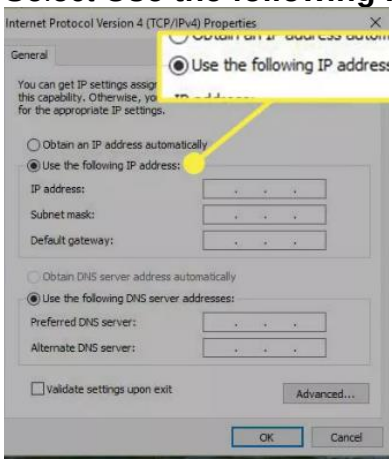
3. Select **Properties** from the menu.



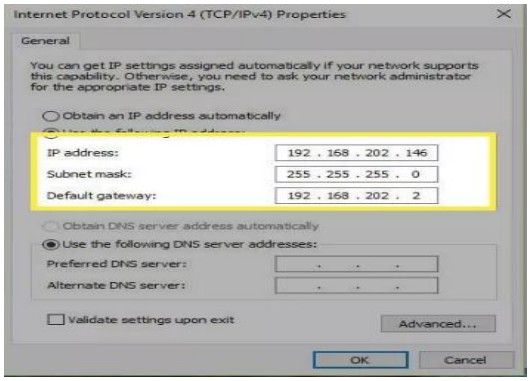
4. Choose **Internet Protocol Version 4 (TCP/IPv4)** from the list, then select **Properties**.



5. Select **Use the following IP address**.



6. Enter the details you copied from Command Prompt: IP address, subnet mask, default gateway, and DNS servers.

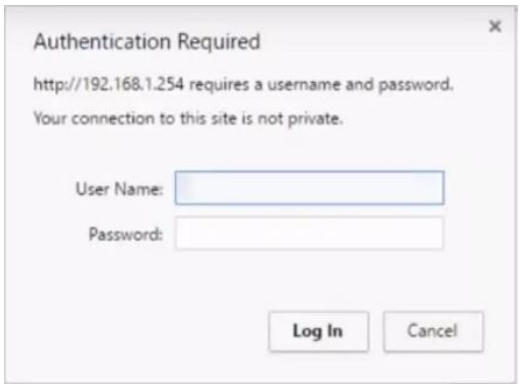


7. Choose **OK** when you're done.
   IMP : If you have several devices on your network that get IP addresses from DHCP, don't reserve the same IP address you found in Command Prompt. For example, if DHCP is set up to serve addresses from a pool between 192.168.1.2 and 192.168.1.20, configure the IP address to use a static IP address that falls outside that range to avoid address conflicts. For example, use 192.168.1.**21** or above. If you're not sure what this means, add 10 or 20 to the last digit in your IP address and use that as the static IP in Windows.

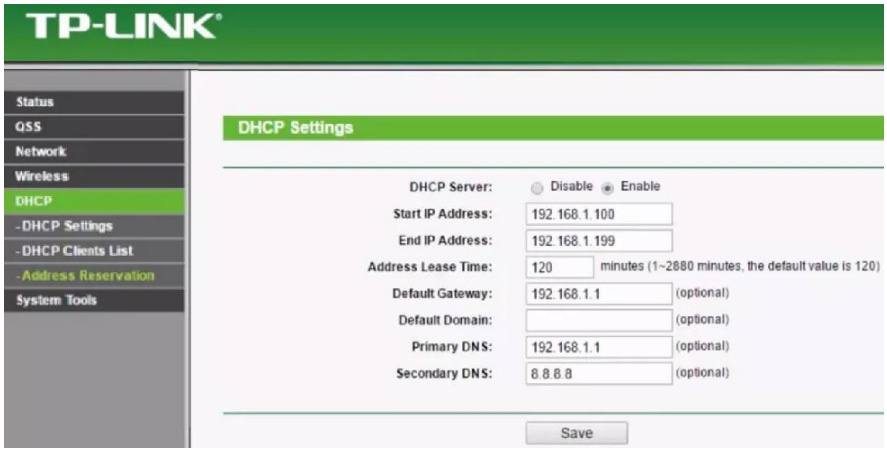
USE YOUR ROUTER TO SET UP A STATIC IP ADDRESS

Another option is to use the router to set up a static IP address. Do this when a non-computer device needs an unchanging address (like a gaming console or a printer).

1. Access the router as admin.



2. Locate a Client List, DHCP Pool, DHCP Reservation, or similar section of the settings. The section lists the devices currently connected to the router. The IP address of the device is listed along with its name.

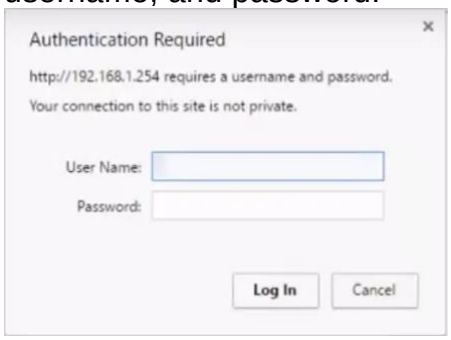


3. Look for a way to reserve one of those IP addresses to tie it with that device so that the router always uses it when the device requests an IP address. You might need to select the IP address from a list or choose **Add** or **Reserve**.

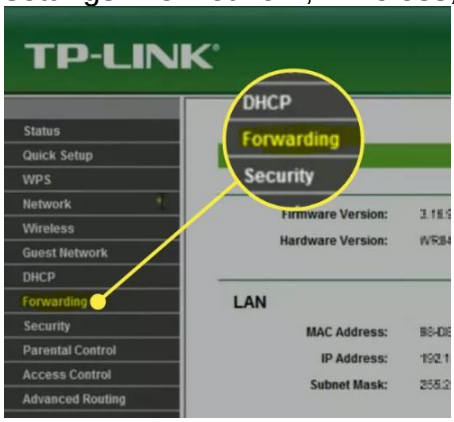
Set Up Port Forwarding

Now that you know the device's IP address and configured it to stop changing, access the router and set up the port forwarding settings.

1. Log in to the router as admin. You need to know the router's IP address, username, and password.

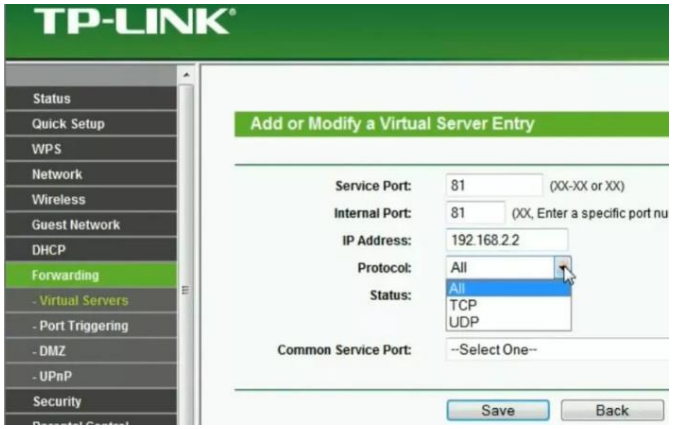


2. Locate the port forwarding options. These are different for every router but might be called something like Port Forwarding, Port Triggering, Applications & Gaming, or Port Range Forwarding. These might be buried within other categories of settings like Network, Wireless, or Advanced.

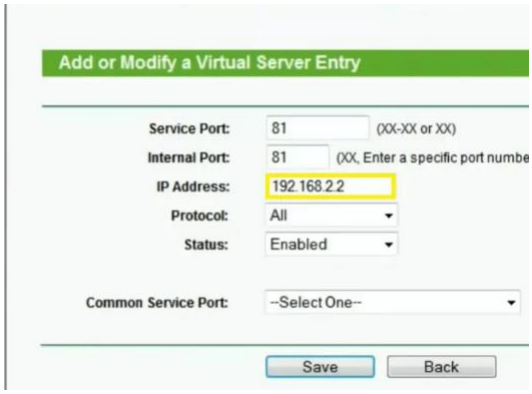


3. Type the port number or port range that you want to forward. If you're forwarding one port, type the same number under both the **Internal** and **External** boxes. For port ranges, use the **Start** and **End** boxes.

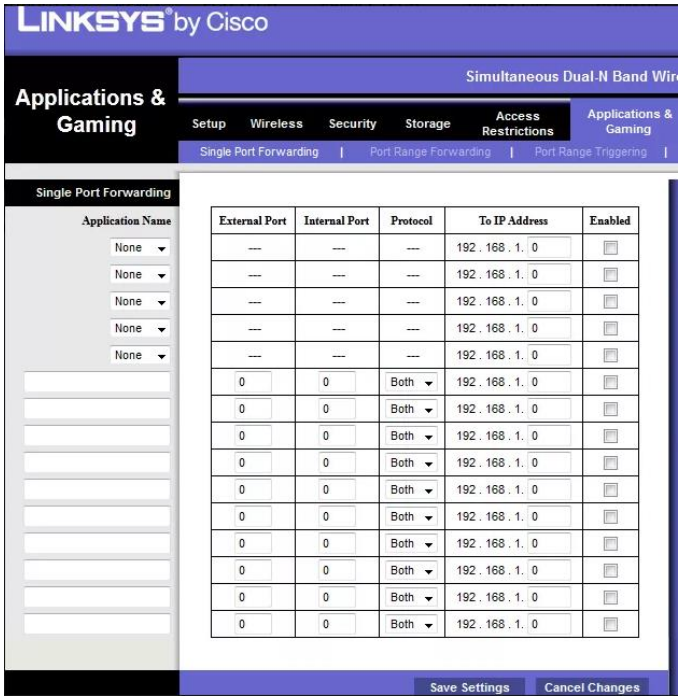
4. Choose a protocol, either TCP or UDP. Choose both, if needed. This information should be available from the program or game that explains the port number.



5. Type the static IP address you choose.



Enable the port forwarding rule with an **Enable** or **On** option.
Here's an example of what it looks like to forward ports on a Linksys WRT610N:



Some routers have a port forward setup wizard that makes it easier to configure. For example, the router might first give you a list of devices already using a static IP address and then let you choose the protocol and port number from there.

Here are some other port forwarding instructions that are more specific to these brands of routers: D-Link, NETGEAR, TP-Link, Belkin, Google, Linksys.

CHAPTER – 19
Study of IPV4 & IPV6

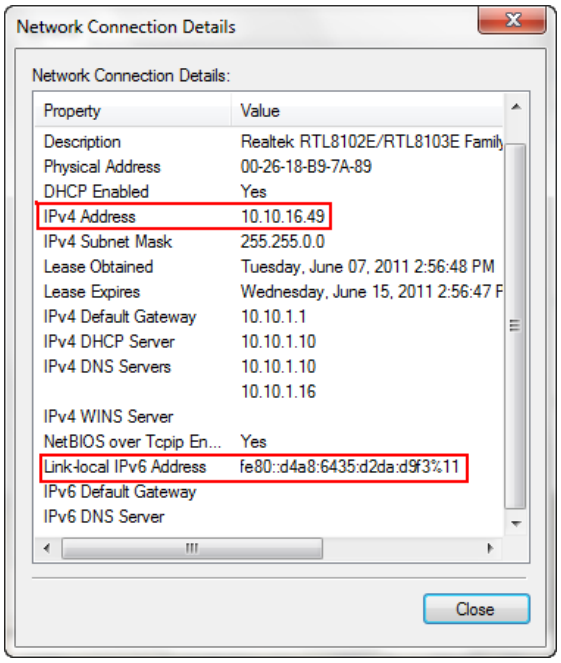
What is IP?

An IP stands for internet protocol. An IP address is assigned to each device connected to a network. Each device uses an IP address for communication. It also behaves as an identifier as this address is used to identify the device on a network. It defines the technical format of the packets. Mainly, both the networks, i.e., IP and TCP, are combined together, so together, they are referred to as a TCP/IP. It creates a virtual connection between the source and the destination.

IPv4 produces 4.3 billion addresses, and the developers think that these addresses are enough, but they were wrong. **IPv6** is the next generation of IP addresses. The main difference between IPv4 and IPv6 is the address size of IP addresses. The **IPv4** is a **32-bit** address, whereas **IPv6** is a **128**-bit hexadecimal address. IPv6 provides a large address space, and it contains a simple header as compared to IPv4.

The IPV4 is a protocol for use on packet-switched link layer networks(e.g. Ethernet). The IPV6 is more advanced and has better features as compared to IPV4. IPV4 & IPV6 is the appearance of the IP addresses. IPV4 uses four 1 byte decimal numbers,

separated by dot(i.e. **192.168.1.1**) while IPV6 uses hexadecimal numbers that are separated by colons (i.e. **fe80::d4a8:6435:d2d8:d9f3b11**).



Below is the summary of the differences between the IPv4 and IPv6:

	IPv4	IPv6
No. of bits on IP Address	32	128
Format	decimal	hexadecimal
Capable of Addresses	4.3 billion	infinite number
How to ping	ping XXX.XXX.XXX	ping6

Advantages of IPv6 over IPv4:

- IPv6 simplified the router's task compared to IPv4.
- IPv6 is more compatible to mobile networks than IPv4.
- IPv6 allows for bigger payloads than what is allowed in IPv4.
- IPv6 is used by less than 1% of the networks, while IPv4 is still in use by the remaining 99%.

How to configure IP

On Windows, setting a static IP address to your device is an essential configuration that may be required in many scenarios. For example, if you plan to share files or a printer on a local network or when trying to configure port forwarding.

If you do not assign a static IP address, services or a port forwarding configuration will eventually stop working. This is because, by default, connected devices use dynamic IP addresses assigned by the **Dynamic Host Configuration Protocol (DHCP)** server (usually the router), which can change as soon as you restart your machine, or after the dynamically assigned configuration expires.

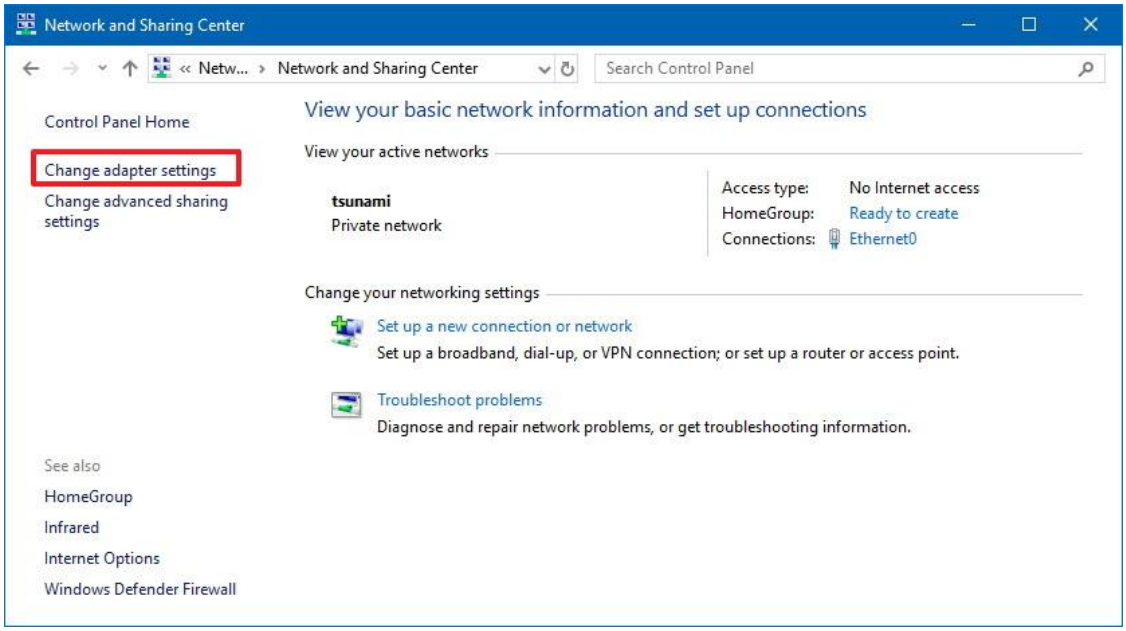
In this section we will learn the steps to set a static **IP (version 4)** address to your Windows device when it is providing a service on the network, or you are simply configuring port forwarding to your device on the router. (You can also configure your router to assign a static IP address using the DHCP settings.)

How to assign static IP address using Control Panel

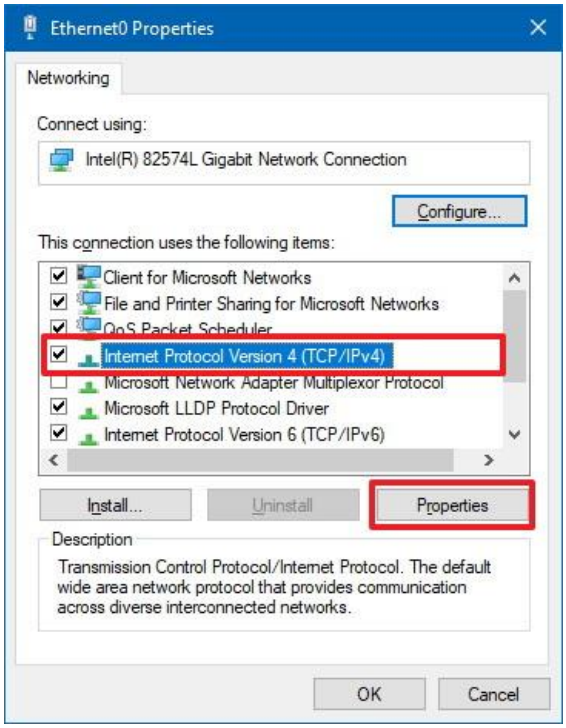
If Command Prompt is not for you, it's possible to use Control Panel to change the IP settings on Windows 10.

Use these steps to assign a static IP configuration using Control Panel:

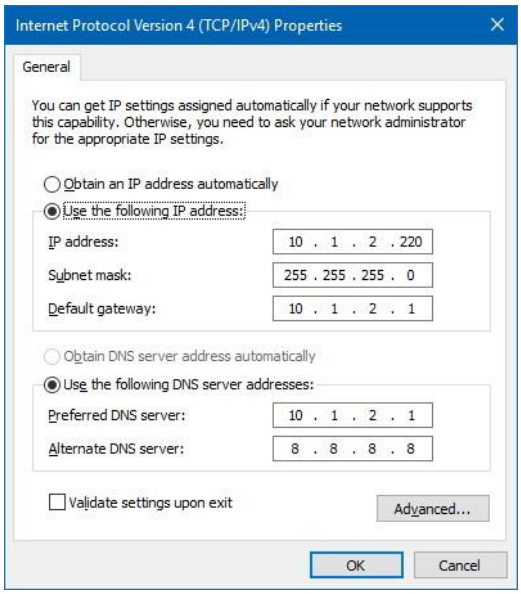
1. Open Control Panel.
2. Click on Network and Internet.
3. Click on Network and Sharing Center.
4. Click the Change adapter settings option on the left navigation pane.



5. Right-click the network adapter and select the Properties option.
6. Select the Internet Protocol Version 4 (TCP/IPv4) option.
7. Click the Properties button.



8. Select the Use the following IP address option.
9. Set the IP address (for example, 10.1.2.220).
10. Set the Subnet mask. Usually, on a home network, the subnet mask is 255.255.255.0.
11. Set the Default gateway. This address is typically your router's IP address (for example, 10.1.2.1).
12. Under the "Use the following DNS server addresses set Preferred DNS server" section, set the Preferred DNS server address, which is usually your router's IP address or IP address of the server providing DNS resolutions (for example, 10.1.2.1).
13. (Optional) Set the Alternative DNS server, which your computer will use if it cannot reach the preferred server.
14. Click the OK button.



15. Click the Close button again.

Once you complete the steps, you can open your web browser and try loading a website to see if the configuration is working.

CHAPTER - 20
Network Programming

Network Programming involves writing programs that communicate with other programs across a computer network. There are many issues that arise when doing network programming which do not appear when doing single program applications.

What does network programming do?
Computer network programming involves writing computer programs that enable processes to communicate with each other across a computer network.

Connection-oriented and connection less communications
Generally, most of communications can be divided into connection-oriented, and connection less. Whether a communication is a connection-oriented, or connection less, is defined by the communication protocol, and not by application programming interface (API). Examples of the connection-oriented protocols include Transmission Control Protocol (TCP) and Sequenced Packet Exchange (SPX), and examples of connectionless protocols include User Datagram Protocol (UDP), "raw IP", and Internetwork Packet Exchange (IPX).
Clients and servers
For connection-oriented communications, communication parties usually have different roles. One party is usually waiting for incoming connections; this party is usually referred to as "**server**". Another party is the one which initiates connection; this party is usually referred to as "**client**".

For connectionless communications, one party ("server") is usually waiting for an incoming packet, and another party ("client") is usually understood as the one which sends an unsolicited packet to "server".
Popular protocols and APIs
Network programming traditionally covers different layers of OSI/ISO model (most of application-level programming belongs to L4 and up). The table below contains some examples of popular protocols belonging to different OSI/ISO layers, and popular APIs for them.
[OSI/ISO LAYER] / [PROTOCOL] / [API]
L3(Network) / IP / Raw Socket
L4 (transport) / TCP, UDP, SCTP / Berkeley Sockets
L5 (session) / TLS / Open SSL
L7 (application) / HTTP / Various

CHAPTER-21

Network Troubleshooting

Basic Network Problems

- **Cable Problem**: The cable which is used to connect two devices can get faulty, shortened or can be physically damaged.
- **Connectivity Problem**: The port or interface on which the device is connected or configured can be physically down or faulty due to which the source host will not be able to communicate with the destination host.
- **Configuration Issue**: Due to a wrong configuration, looping the IP, routing problem and other configuration issues, network fault may arise and the services will get affected.
- **Software Issue**: Owing to software compatibility issues and version mismatch, the transmission of IP data packets between the source and destination is interrupted.
- **Traffic overload:** If the link is over utilized then the capacity or traffic on a device is more than the carrying capacity of it and due to overload condition the device will start behaving abnormally.
- **Network IP issue:** Due to improper configuration of IP addresses and subnet mask and routing IP to the next hop, the source will not be able to reach the destination IP through the network.

How to Troubleshoot a Network

Always start troubleshooting using these simple network troubleshooting steps to help diagnose and refine the issue.

1. Check the hardware. When you're beginning the troubleshooting process, check all your hardware to make sure it's connected properly, turned on, and working. If a cord has come loose or somebody has switched off an important router, this could be the problem behind your networking issues. There's no point in going through the process of troubleshooting network issues if all you need to do is plug a cord in. Make sure all switches are in the correct positions and haven't been bumped accidentally.

Next , turn the hardware off and back on again. This is the mainstay of IT troubleshooting, and while it might sound simplistic, often it really does solve the problem. Power cycling your modem, router, and PC can solve simple issues—just be sure to leave each device off for at least 60 seconds before you turn it back on.

2. Use ipconfig. Open the command prompt and type "ipconfig" (without the quotes) into the terminal. The Default Gateway (listed last) is your router's IP. Your computer's IP address is the number next to "IP Address." If your computer's IP address starts with 169, the computer is not receiving a valid IP address. If it starts with anything other than 169, your computer is being allocated a valid IP address from your router. Try typing in "ipconfig /release" followed by "ipconfig /renew" to get rid of your current

IP address and request a new one. This will in some cases solve the problem. If you still can't get a valid IP from your router, try plugging your computer straight into the modem using an ethernet cable. If it works, the problem lies with the router.

3. Use ping and tracert. If your router is working fine, and you have an IP address starting with something other than 169, the problem's most likely located between your router and the internet. At this point, it's time to use the **ping** tool. Try sending a ping to a well-known, large server, such as Google, to see if it can connect with your router. You can ping Google DNS servers by opening the command prompt and typing "ping 8.8.8.8"; you can also add "-t" to the end (ping 8.8.8.8 -t) to get it to keep pinging the servers while you troubleshoot. If the pings fail to send, the command prompt will return basic information about the issue.

You can use the **tracert** command to do the same thing, by typing "tracert 8.8.8.8"; this will show you each step, or "hop," between your router and the Google DNS servers. You can see where along the pathway the error is arising. If the error comes up early along the pathway, the issue is more likely somewhere in your local network.

4. Perform a DNS check. Use the command "nslookup" to determine whether there's a problem with the server you're trying to connect to. If you perform a DNS check on, for example, google.com and receive results such as "Timed Out," "Server Failure," "Refused," "No Response from Server," or "Network Is Unreachable," it may indicate the problem originates in the DNS server for your destination. (You can also use nslookup to check your own DNS server.)

5. Contact the ISP. If all of the above turn up no problems, try contacting your internet service provider to see if they're having issues. You can also look up outage maps and related information on a Smartphone to see if others in your area are having the same problem.

6. Check on virus and malware protection. Next, make sure your virus and malware tools are running correctly, and they haven't flagged anything that could be affecting part of your network and stopping it from functioning.

7. Review database logs. Review all your database logs to make sure the databases are functioning as expected. If your network is working but your database is full or malfunctioning, it could be causing problems that flow on and affect your network performance.

Tips For Network Troubleshooting

- Always use a high-level password to protect your network devices such as routers, switches and database servers as they store crucial data within themselves.

- Don't share your router login user ID and password with anyone in the organization or outside the organization.

- Properly log-out from the system once your job is done.
- Keep verifying your configuration **by show running-config command.**
- For assigning IP addresses and subnet mask to the devices for a network, always perform the IP planning first and then make a diagram of the connectivity of devices that you are using in the network.
- It is better if you use the routers or servers in the master-slave mode so that in the worst case if one goes down then the other will take up the load and your network will be kept alive.
- Avoid overloading your device with high traffic.

File sharing

Step in source computer

1. Open network and sharing center -> change advance sharing setting -> make the below option ON
   - Turn on network discovery
   - Turn on File and printer sharing
   - Turn on sharing so anyone with network access can read and write files in the public folder
   - Use 123 bit encryption to help protect file sharing connection
   - Turn off password protection sharing

2. Open this PC -> select the drive or folder to give sharing option -> right click -> share with -> advance sharing -> advance sharing -> click in share this folder check box -> permission -> full control -> apply -> ok.
3. In this properties dialog box -> click in security -> edit -> add -> type everyone -> ok -> select everyone -> full control -> apply -> ok -> close.
4.