

Installation Technician Computing and Peripherals

(Job Role)

Sector: Electronics and Hardware

Reference Textbook for Class XII

Vocational Education

INDEX

Unit	Unit name	Page number
1	Computer network essential	1-17
2	Installation and Configuration of windows server	18-42
3	Installation and configuration of Linux server	43-49
4	IT security fundamental	50-60
5	Basics of ITIL V3	61-68

Unit 1: - Computer Network Essentials.

1.1 Introduction to Computer Networks

We are living in a connected world. Information is being produced, exchanged, and traced across the globe in real time. It's possible as almost everyone and everything in the digital world is interconnected through one way or the other.

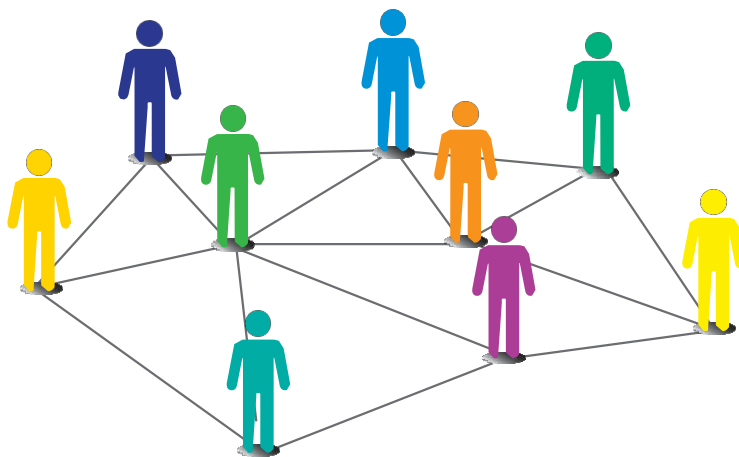


Figure 1.1: Interconnection forming a social network

A group of two or more similar things or people interconnected with each other is called network (Figure 1.1). Some of the examples of network in our everyday life includes:

- ✓ Social network
- ✓ Mobile network
- ✓ Network of computers
- ✓ Airlines, railway, banks, hospitals networks

A computer network (Figure 1.2) is an interconnection among two or more computers or computing devices. Such interconnection allows computers to share data and resources among each other. A basic network may connect a few computers placed in a room.

The network size may vary from small to large depending on the number of computers it connects. A computer network can include different types of hosts (also called nodes) like server, desktop, laptop, cellular phones.

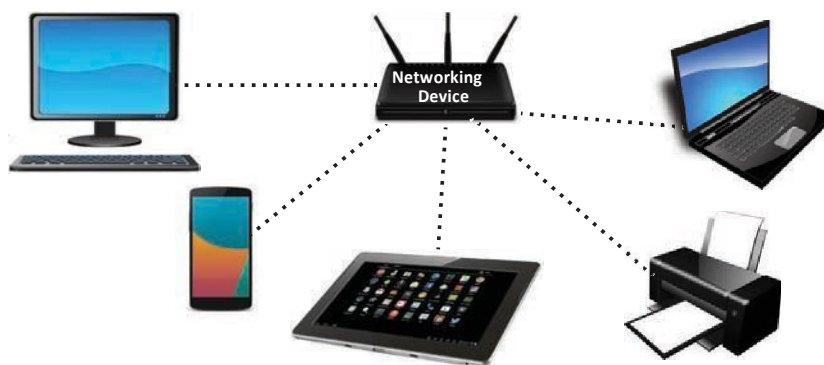


Figure 1.2: A computer network

Apart from computers, networks include networking devices like switch, router, modem, etc. Networking devices are used to connect multiple computers in different settings. For

communication, data in a network is divided into smaller chunks called packets. These packets are then carried over a network. Devices in a network can be connected either through wired media like cables or wireless media like air.

In a communication network, each device that is a part of a network and that can receive, create, store or send data to different network routes is called a node. In the context of data communication, a node can be a device such as a modem, hub, bridge, switch, router, digital telephone handset, a printer, a computer or a server.

Interconnectivity of computing devices in a network allows us to exchange information simultaneously with many parties through email, websites, audio/video calls, etc. Network allows sharing of resources. For example, a printer can be made available to multiple computers through a network; a networked storage can be accessed by multiple computers. People often connect their devices through hotspot, thus forming a small personal network.

1.2 Evolution of Networking

In the 1960s a research project was commissioned by Advanced Research Projects Agency Network (ARPANET) in the U.S. Department of Defence to connect the academic and research institutions located at different places for scientific collaborations. The first message was communicated between the University of California, Los Angeles (UCLA) and Stanford Research Institute (SRI). Slowly but gradually, more and more organisations joined the ARPANET, and many independent smaller networks were formed. Few of the milestones in the magnificent journey of evolution of computer networks is depicted in the timeline shown in Figure 1.3.

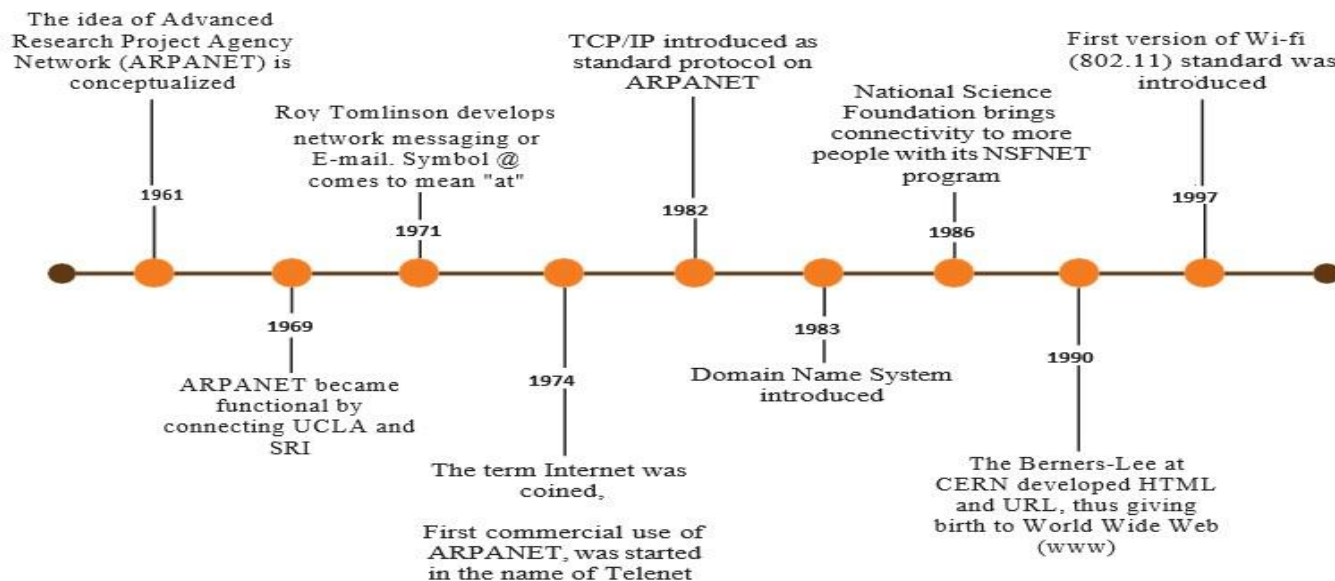


Figure 1.3: Timeline showing evolution of networking

1.3 Types of Networks

There are various types of computer networks ranging from network of handheld devices (like mobile phones or tablets) connected through Wi-Fi or Bluetooth within a single room to the millions of computers spread across the globe. Some are connected wireless while others are connected through wires.

Based on the geographical area covered and data transfer rate, computer networks are broadly categorised as:

- ✓ PAN (Personal Area Network)
- ✓ LAN (Local Area Network)
- ✓ MAN (Metropolitan Area Network)
- ✓ WAN (Wide Area Network)

1.3.1 Personal Area Network (PAN)

It is a network formed by connecting a few personal devices like computers, laptops, mobile phones, smart phones, printers etc., as shown in Figure 10.4. All these devices lie within an approximate range of 10 metres. A personal area network may be wired or wireless. For example, a mobile phone connected to the laptop through USB forms a wired PAN while two smartphones communicating with each other through Bluetooth technology form a wireless PAN or WPAN.



Figure 1.4: A Personal Area Network

1.3.2 Local Area Network (LAN)

It is a network that connects computers, mobile phones, tablet, mouse, printer, etc., placed at a limited distance. The geographical area covered by a LAN can range from a single room, a floor, an office having one or more buildings in the same premise, laboratory, a school, college, or university campus. The connectivity is done by means of wires, Ethernet cables, fibre optics, or Wi-Fi. A Local Area Network (LAN) is shown in Figure 1.5.



Figure 1.5: A Local Area Network

LAN is comparatively secure as only authentic users in the network can access other computers or shared resources. Users can print documents using a connected printer, upload/download documents and software to and from the local server. Such LANs provide the short range communication with the high speed data transfer rates. These types of networks can be extended up to 1 km. Data transfer in LAN is quite high, and usually varies from 10 Mbps (called Ethernet) to 1000 Mbps (called Gigabit Ethernet), where Mbps stands for Megabits per second. Ethernet is a set of rules that decides how computers and other devices connect with each other through cables in a local area network or LAN.

1.3.3 Metropolitan Area Network (MAN)

Metropolitan Area Network (MAN) is an extended form of LAN which covers a larger geographical area like a city or a town. Data transfer rate in MAN also ranges in Mbps, but it is considerably less as compared to LAN. Cable TV network or cable based broadband internet services are examples of MAN. This kind of network can be extended up to 30-40 km. Sometimes, many LANs are connected together to form MAN, as shown in Figure 1.6.

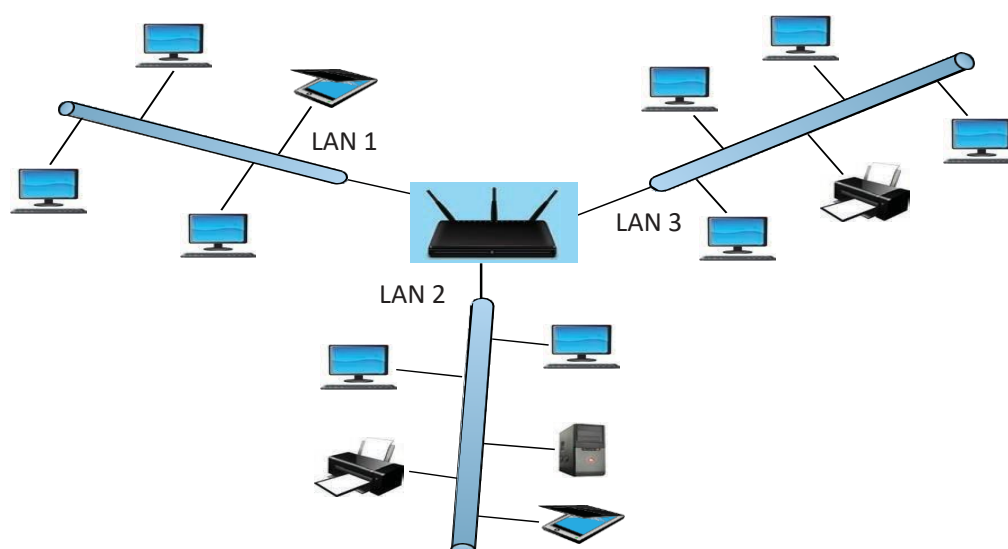


Figure 1.6: A Metropolitan Area Network

1.3.4 Wide Area Network (WAN)

Wide Area Network connects computers and other LANs and MANs, which are spread across different geographical locations of a country or in different countries or continents. A WAN could be formed by connecting a LAN to other LANs (Figure 10.7) via wired/wireless media. Large business, educational and government organisations connect their different branches in different locations across the world through WAN. The Internet is the largest WAN that connects billions of computers, smartphones and millions of LANs from different continents.

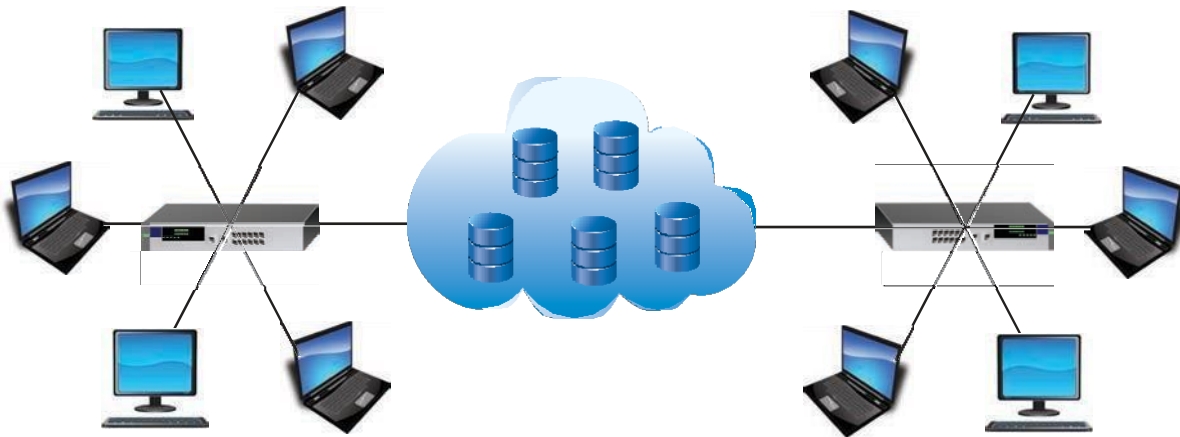


Figure 1.7: A Wide Area Network

1.4 Network Devices

To communicate data through different transmission media and to configure networks with different functionality, we require different devices like Modem, Hub, Switch, Repeater, Router, Gateway, etc. Let us explore them in detail.

1.4.1 Modem

Modem stands for 'MODulator DEModulator'. It refers to a device used for conversion between analog signals and digital bits. We know computers store and process data in terms of 0s and 1s. However, to transmit data from a sender to a receiver, or while browsing the internet, digital data are converted to an analog signal and the medium (be it free-space or a physical media) carries the signal to the receiver. There are modems connected to both the source and destination nodes. The modem at the sender's end acts as a modulator that converts the digital data into analog signals. The modem at the receiver's end acts as a demodulator that converts the analog signals into digital data for the destination node to understand. Figure 1.8 shows connectivity using a modem.

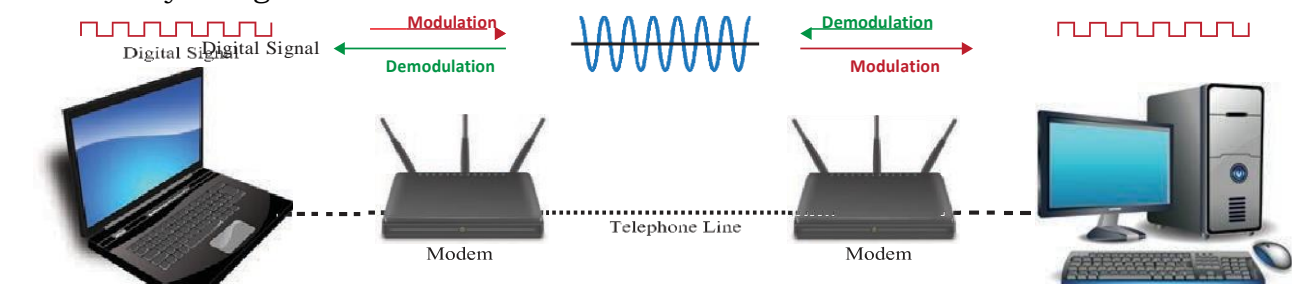


Figure 1.8: Use of modem

1.4.2 Ethernet Card

Ethernet card, also known as Network Interface Card (NIC card in short) is a network adapter used to set up a wired network. It acts as an interface between computer and the network. It is a circuit board mounted on the motherboard of a computer as shown in Figure 1.9. The Ethernet cable connects the computer to the network through NIC. Ethernet cards can support data transfer between 10 Mbps and 1 Gbps (1000 Mbps). Each NIC has a MAC address, which helps in uniquely identifying the computer on the network.

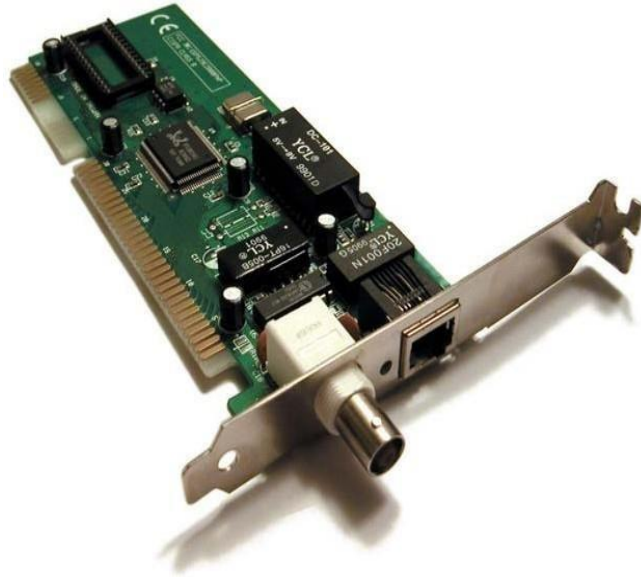


Figure 1.9: A Network Interface Card

1.4.3 RJ45

RJ 45 or Registered Jack-45 is an eight-pin connector (Figure 1.10) that is used exclusively with Ethernet cables for networking. It is a standard networking interface that can be seen at the end of all network cables. Basically, it is a small plastic plug that fits into RJ-45 jacks of the Ethernet cards present in various computing devices.



Figure 1.10: RJ 45

1.4.4 Repeater

Data are carried in the form of signals over the cable. These signals can travel a specified distance (usually about 100 m). Signals lose their strength beyond this limit and become weak. In such conditions, original signals need to be regenerated.

A repeater is an analog device that works with signals on the cables to which it is connected. The weakened signal appearing on the cable is regenerated and put back on the cable by a repeater.

1.4.5 Hub

An Ethernet hub (Figure 1.11) is a network device used to connect different devices through wires. Data arriving on any of the lines are sent out on all the others. The limitation of Hub is that if data from two devices come at the same time, they will collide.



Figure 1.11: A network hub with 8 ports

1.4.5 Switch

A switch is a networking device (Figure 1.12) that plays a central role in a Local Area Network (LAN). Like a hub, a network switch is used to connect multiple computers or communicating devices. When data arrives, the switch extracts the destination address from the data packet and looks it up in a table to see where to send the packet. Thus, it sends signals to only selected devices instead of sending to all. It can forward multiple packets at the same time. A switch does not forward the signals which are noisy or corrupted. It drops such signals and asks the sender to resend it.

Ethernet switches are common in homes/offices to connect multiple devices thus creating LANs or to access the Internet.



Figure 1.12: Cables connected to a network switch

1.4.6 Router

A router (Figure 1.13) is a network device that can receive the data, analyse it and transmit it to other networks. A router connects a local area network to the internet. Compared to a hub or a switch, a router has advanced capabilities as it can analyse the data being carried over a network, decide/alter how it is packaged, and send it to another network of a different

type. For example, data has been divided into packets of a certain size. Suppose these packets are to be carried over a different type of network which cannot handle bigger packets. In such a case, the data is to be repackaged as smaller packets and then sent over the network by a router.



Figure 1.13: A router

A router can be wired or wireless. A wireless router can provide Wi-Fi access to smartphones and other devices. Usually, such routers also contain some ports to provide wired Internet access. These days, home Wi-Fi routers perform the dual task of a router and a modem/ switch. These routers connect to incoming broadband lines, from ISP (Internet Service Provider), and convert them to digital data for computing devices to process.

1.4.7 Gateway

As the term “Gateway” suggests, it is a key access point that acts as a “gate” between an organisation's network and the outside world of the Internet (Figure 1.14). Gateway serves as the entry and exit point of a network, as all data coming in or going out of a network must first pass through the gateway in order to use routing paths. Besides routing data packets, gateways also maintain information about the host network's internal connection paths and the identified paths of other remote networks. If a node from one network wants to communicate with a node of a foreign network, it will pass the data packet to the gateway, which then routes it to the destination using the best possible route.

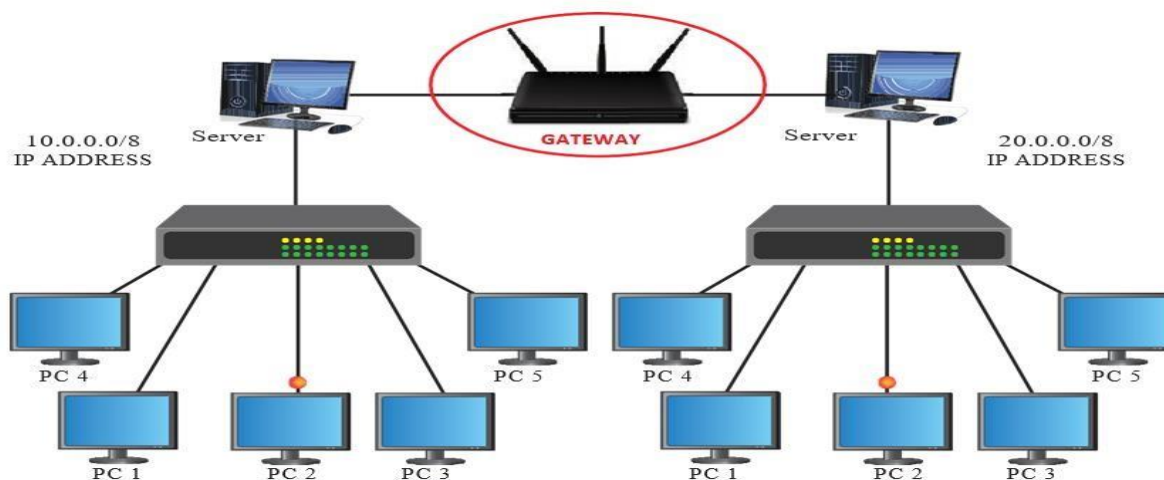


Figure 1.14: A network gateway

For simple Internet connectivity at homes, the gateway is usually the Internet Service Provider that provides access to the entire Internet. Generally, a router is configured to work as a gateway device in computer networks. But a gateway can be implemented completely in software, hardware, or a combination of both. Because a network gateway is placed at the edge of a network, the firewall is usually integrated with it.

1.5 Networking Topologies

We have already discussed that a number of computing devices are connected together to form a Local Area Network (LAN), and interconnections among millions of LANs forms the Internet. The arrangement of computers and other peripherals in a network is called its topology. Common network topologies are Mesh, Ring, Bus, Star and Tree.

1.5.1 Mesh Topology

In this networking topology, each communicating device is connected with every other device in the network as shown in Figure 1.15. Such a network can handle large amounts of traffic since multiple nodes can transmit data simultaneously. Also, such networks are more reliable in the sense that even if a node gets down, it does not cause any break in the transmission of data between other nodes. This topology is also more secure as compared to other topologies because each cable between two nodes carries different data. However, wiring is complex and cabling cost is high in creating such networks and there are many redundant or unutilised connections.

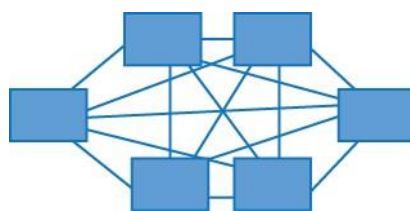


Figure 1.15: A mesh topology

1.5.2 Ring Topology

In ring topology (Figure 1.16), each node is connected to two other devices, one each on either side, as shown in Figure 1.16. The nodes connected with each other thus forms a ring. The link in a ring topology is unidirectional. Thus, data can be transmitted in one direction only (clockwise or counter clockwise).

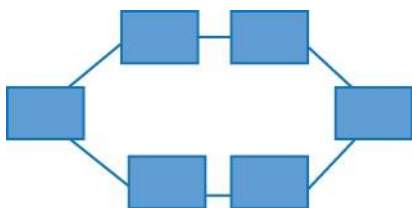


Figure 1.16: A ring topology

1.5.3 Bus Topology

In bus topology (Figure 1.17), each communicating device connects to a transmission medium, known as bus. Data sent from a node are passed on to the bus and hence are transmitted to the length of the bus in both directions. That means, data can be received by any of the nodes connected to the bus.

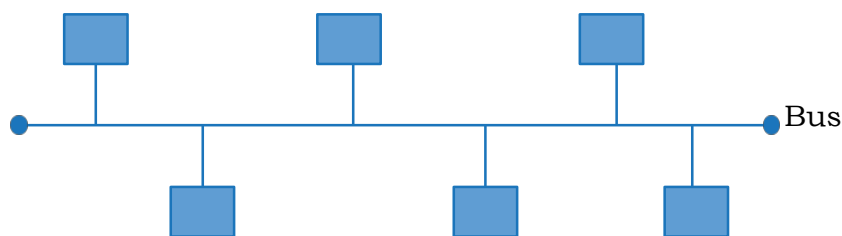


Figure 1.17: A bus topology

In this topology, a single backbone wire called bus is shared among the nodes, which makes it cheaper and easier to maintain. Both ring and bus topologies are considered to be less secure and less reliable.

1.5.4 Star Topology

In star topology (Figure 1.18), each communicating device is connected to a central node, which is a networking device like a hub or a switch, as shown in Figure 1.18.

Star topology is considered very effective, efficient and fast as each device is directly connected with the central device. Although disturbance in one device will not affect the rest of the network, any failure in a central networking device may lead to the failure of complete network.

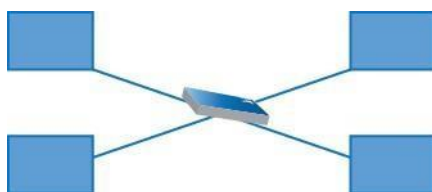


Figure 1.18: A star topology

The central node can be either a broadcasting device means data will be transmitted to all the nodes in the network, or a unicast device means the node can identify the destination and forward data to that node only.

1.5.5 Tree or Hybrid Topology

It is a hierarchical topology, in which there are multiple branches and each branch can have one or more basic topologies like star, ring and bus. Such topologies are usually realised in WANs where multiple LANs are connected. Those LANs may be in the form of a ring, bus or star. In figure 1.19, a hybrid topology is shown connecting 4-star topologies in a bus.

In this type of network, data transmitted from source first reaches the centralised device and from there the data passes through every branch where each branch can have links for more nodes.

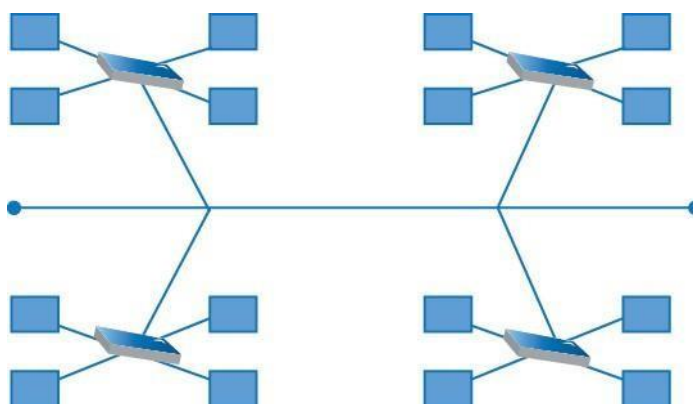


Figure 1.19: A hybrid topology

1.6 OSI Model

There are n numbers of users who use computer network and are located over the world. Therefore, national and worldwide data communication systems must be developed which are compatible to communicate with each other. ISO has developed a standard Model of Network Data Communication. ISO stands for International organization of Standardization. This is called a model for Open System Interconnection (OSI) and is commonly known as OSI model.

The ISO-OSI model is a seven layer architecture. It defines seven layers or levels in a complete communication system. They are:

1. Application Layer
2. Presentation Layer
3. Session Layer
4. Transport Layer
5. Network Layer
6. Datalink Layer
7. Physical Layer

The Important principles to design the model

1. A layer should be created where a different abstraction is needed.
2. Each layer should perform a well-defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the interfaces.

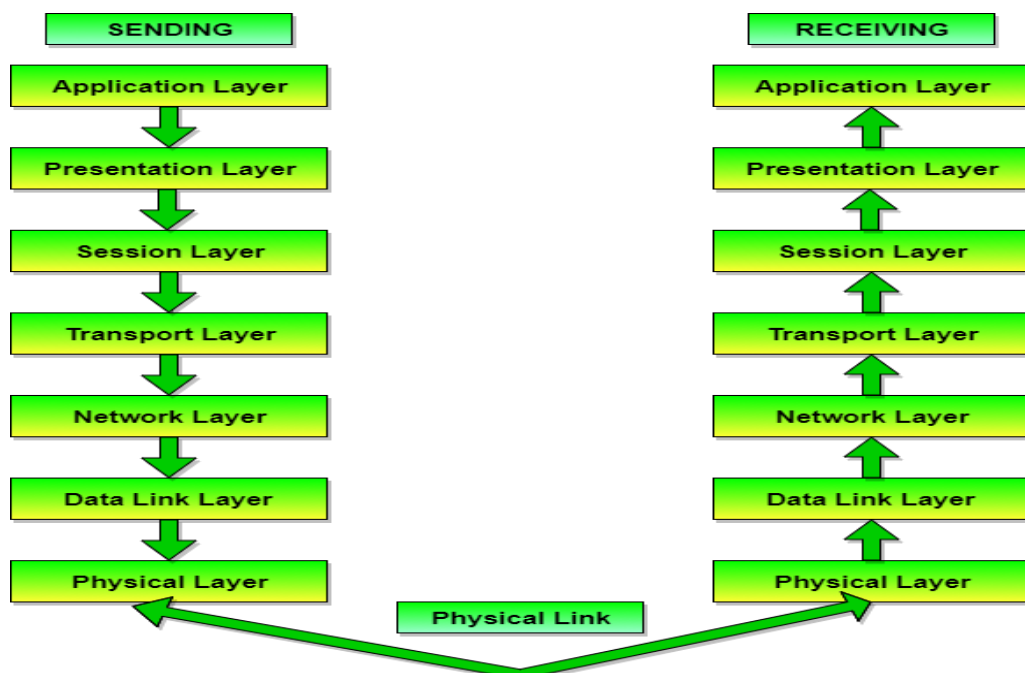


Figure 1.20: Seven layers of the OSI model.

1.6.1 The working principle of different layer in OSI model with their protocol used.

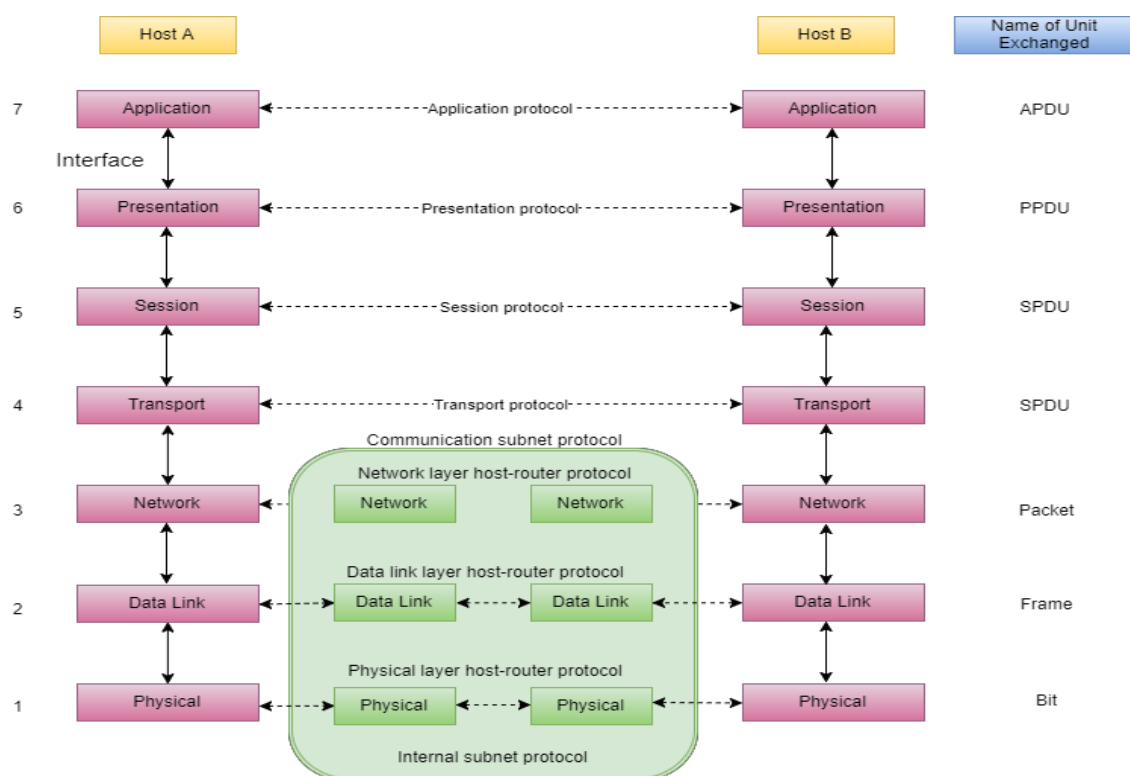


Figure 1.20: The interaction between layers in the OSI model.

Physical Layer

The lowest layer of the OSI Model is concerned with electrically or optically transmitting raw unstructured data bits across the network from the physical layer of the sending device to the physical layer of the receiving device. It can include specifications such as voltages, pin layout, cabling, and radio frequencies. At the physical layer, one might find “physical” resources such as network hubs, cabling, repeaters, network adapters or modems.

Data Link Layer

At the data link layer, directly connected nodes are used to perform node-to-node data transfer where data is packaged into frames. The data link layer also corrects errors that may have occurred at the physical layer.

Network Layer

The network layer is responsible for receiving frames from the data link layer, and delivering them to their intended destinations among based on the addresses contained inside the frame. The network layer finds the destination by using logical addresses, such as IP (internet protocol). At this layer, routers are a crucial component used to quite literally route information where it needs to go between networks.

Transport Layer

The transport layer manages the delivery and error checking of data packets. It regulates the size, sequencing, and ultimately the transfer of data between systems and hosts. One of the most common examples of the transport layer is TCP or the Transmission Control Protocol.

Session Layer

The session layer controls the conversations between different computers. A session or connection between machines is set up, managed, and terminated at layer

5. Session layer services also include authentication and reconnections.

Presentation Layer

The presentation layer formats or translates data for the application layer based on the syntax or semantics that the application accepts. Because of this, it is at times also called the syntax layer. This layer can also handle the encryption and decryption required by the application layer.

1.7 Concept of Protocol.

Protocols are a fundamental aspect of digital communication as they dictate how to format, transmit and receive data. They are a set of rules that determines how the data will be transmitted over the network.

It can also be defined as a communication standard followed by the two key parties (sender and receiver) in a computer network to communicate with each other.

It specifies what type of data can be transmitted, what commands are used to send and receive data, and how data transfers are confirmed.

In simple terms, a protocol is similar to a language. Every language has its own rules and vocabulary. Protocols have their own rules, specifications, and implementations. If two people share the same language, they can communicate very easily and effectively. Similarly, two hosts implementing the same protocol can connect and communicate easily with each other. Hence, protocols provide a common language for network devices participating in data communication.

Protocols are developed by industry-wide organizations. The ARPA (Advanced Research Project Agency) part of the US Defence program was the first organization to introduce the concept of a standardized protocol. Support for network protocols can be built into the software, hardware, or both. All network end-users rely on network protocols for connectivity.

Protocols use a specific model for their implementation like the OSI (Open System Interface) Model, TCP/IP (Transmission Control Protocol / Internet Protocol) Model, etc. There are different layers (for instance, data, network, transport, and application layer, etc.) in these models, where these protocols are implemented.

Combining all these, we can say that protocol is an agreement between a sender and a receiver, which states how communication will be established, and how to maintain & release it. It is the communication between entities in different systems, where entities can be a user application program, file transfer package, DBMS, etc., and systems can be a remote computer, sensor, etc.

1.7.1 Types of Protocol

TCP

Transmission control protocol is used for communication over a network. In TCP data is broken down into small packets and then sent to the destination. However, IP is making sure packets are transmitted to the right address.

Internet Protocol (IP)

IP is also working with TCP. It is an addressing Protocol. IP addresses packets route them and show different nodes and network Unless it reaches its right destination. The IP protocol is developed in 1970.

FTP

File transfer protocol is basically used for transferring files to different networks. There may be a mass of files such as text files, multimedia files, etc. This way of file transfer is quicker than other methods.

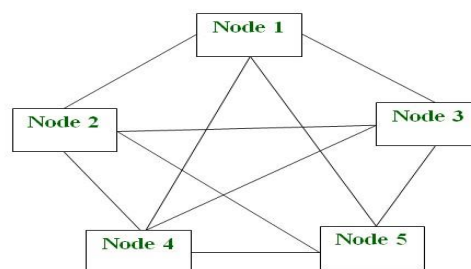
User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) is a lightweight data transport protocol that works on top of IP. UDP provides a mechanism to detect corrupt data in packets, but it does *not* attempt to solve other problems that arise with packets, such as lost or out of order packets. That's why UDP is sometimes known as the *Unreliable* Data Protocol. UDP is simple but fast, at least in comparison to other protocols that work over IP. It's often used for time-sensitive applications (such as real-time video streaming) where speed is more important than accuracy.

1.8 Network Technologies

1.8.1 Peer-to-Peer Network

A peer to peer network is a simple network of computers. It first came into existence in the late 1970s. Here each computer acts as a node for file sharing within the formed network. Here each node acts as a server and thus there is no central server to the network. This allows the sharing of a huge amount of data. The tasks are equally divided amongst the nodes. Each node connected in the network shares an equal workload. For the network to stop working, all the nodes need to individually stop working. This is because each node works independently.



P2P Architecture

1.8.2 Client and Server Network

A client and server networking model is a model in which computers such as servers provide the network services to the other computers such as clients to perform a user based tasks. This model is known as client-server networking model.

Client

A client is a program that runs on the local machine requesting service from the server. A client program is a finite program means that the service started by the user and terminates when the service is completed.

Server

A server is a program that runs on the remote machine providing services to the clients. When the client requests for a service, then the server opens the door for the incoming requests, but it never initiates the service.

A server program is an infinite program means that when it starts, it runs infinitely unless the problem arises. The server waits for the incoming requests from the clients. When the request arrives at the server, then it responds to the request.

The application programs using the client-server model should follow the given below strategies:

- An application program is known as a client program, running on the local machine that requests for a service from an application program known as a server program, running on the remote machine.
- A client program runs only when it requests for a service from the server while the server program runs all time as it does not know when its service is required.
- A server provides a service for many clients not just for a single client. Therefore, we can say that client-server follows the many-to-one relationship. Many clients can use the service of one server.
- Services are required frequently, and many users have a specific client-server application program. For example, the client-server application program allows the user to access the files, send e-mail, and so on. If the services are more customized, then we should have one generic application program that allows the user to access the services available on the remote computer.

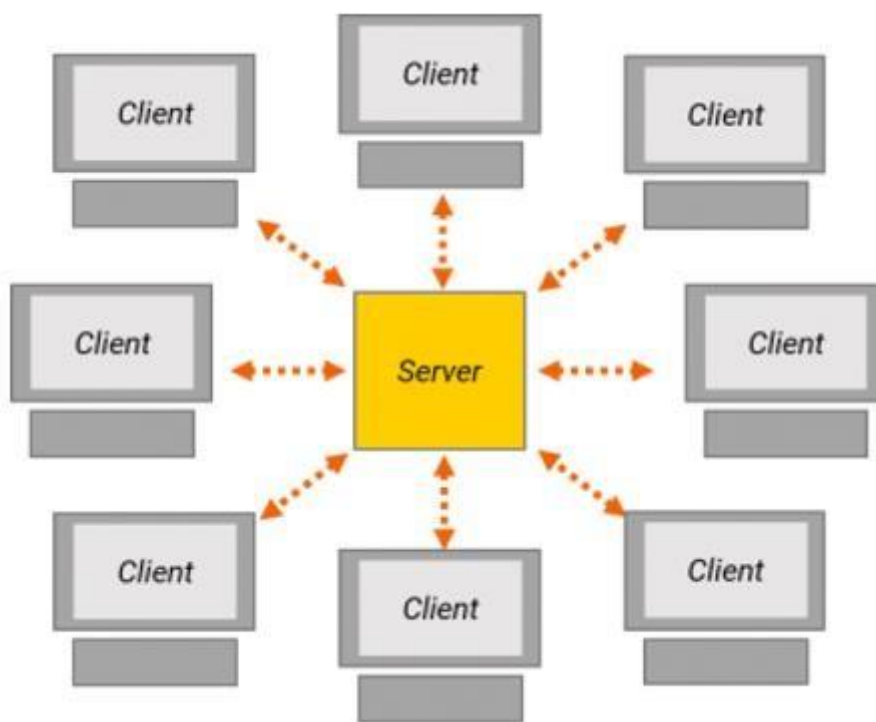


Figure 1.21: Client and Server Network.

1.9 Data Transmission

The way in which data is transmitted from one device to another device is known as Data Transmission mode. The Data transmission mode is also known as the communication mode. Each communication channel has a direction associated with it, and transmission media provide the direction. Therefore, the transmission mode is also known as a directional mode. The Data transmission mode is defined in the physical layer.

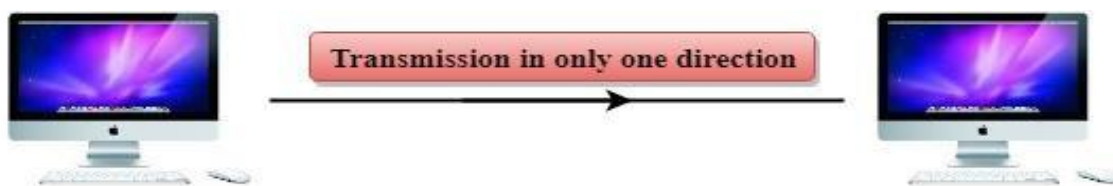
The Data Transmission mode is divided into three categories:

- Simplex mode
- Half-duplex mode
- Full-duplex mode

Simplex mode

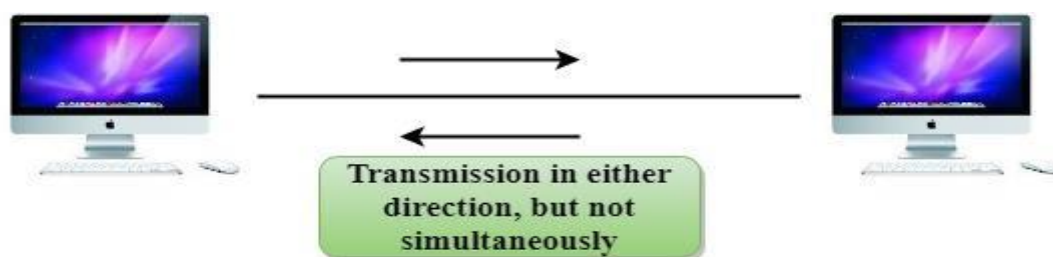
In Simplex mode, the communication is unidirectional, i.e., the data flow in one direction. A device can only send the data but cannot receive it or it can receive the data but cannot send the data. This transmission mode is not very popular as mainly communications require the two-way exchange of data. The simplex mode is used in the business field as in sales that do not require any corresponding reply. The radio station is a simplex channel as it transmits the signal to the listeners but never allows them to transmit back. Keyboard and Monitor are the examples of the simplex mode as a keyboard can only accept the data from the user and monitor can only be used to display the data on the screen. The main advantage of the simplex

mode is that the full capacity of the communication channel can be utilized during transmission.



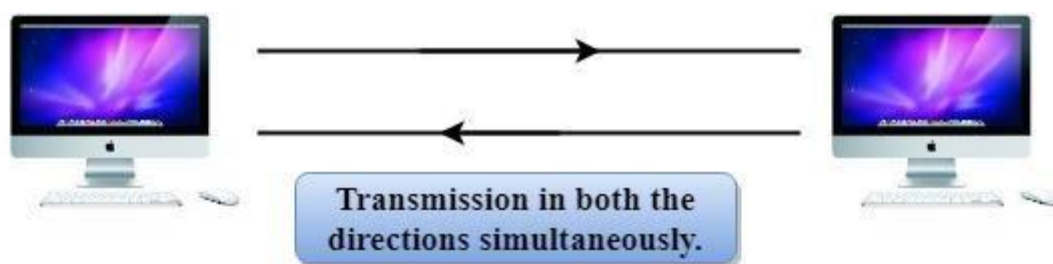
Half-Duplex mode

In a Half-duplex channel, direction can be reversed, i.e., the station can transmit and receive the data as well. Messages flow in both the directions, but not at the same time. The entire bandwidth of the communication channel is utilized in one direction at a time. In half-duplex mode, it is possible to perform the error detection, and if any error occurs, then the receiver requests the sender to retransmit the data. A Walkie-talkie is an example of the Half-duplex mode. In Walkie-talkie, one party speaks, and another party listens. After a pause, the other speaks and first party listens. Speaking simultaneously will create the distorted sound which cannot be understood.



Full-duplex mode

In Full duplex mode, the communication is bi-directional, i.e., the data flow in both the directions. Both the stations can send and receive the message simultaneously. Full-duplex mode has two simplex channels. One channel has traffic moving in one direction, and another channel has traffic flowing in the opposite direction. The Full-duplex mode is the fastest mode of communication between devices. The most common example of the full-duplex mode is a telephone network. When two people are communicating with each other by a telephone line, both can talk and listen at the same time.

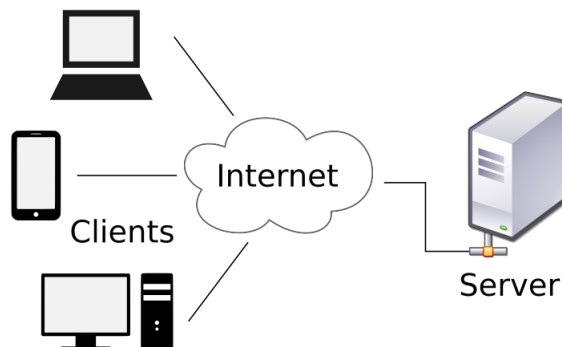


Unit 2: Installation and configuration of Windows Server

Windows Server:

If you're a regular computer user, you may have only come across the consumer-facing editions of Windows. But did you know that Microsoft also publishes an entire Windows Server line of its operating system?

Let's take a look at the differences between Windows Server and regular Windows. We'll see what Windows Server includes, what it leaves out, and why it's so



different.

In case you've never heard of Windows Server, we'll first explain what it is. Essentially, Windows Server is a line of operating systems that Microsoft specifically creates for use on a server. Servers are extremely powerful machines that are designed to run constantly and provide resources for other computers. This means in almost all cases; Windows Server is only used in business settings.

Microsoft has published Windows Server under this name since Windows Server 2003 launched in April 2003. However, even before this, server versions of Windows were available. For instance, Windows NT 4.0 was available in both workstation (for general use) and server flavors.



In almost all cases, normal users don't need to worry about Windows Server. You won't find it on the shelf in stores or accidentally download it from Microsoft when you mean to get the standard version of Windows. But it's still interesting to learn about so you're aware.

Step By Step Installation of Windows Server 2012.

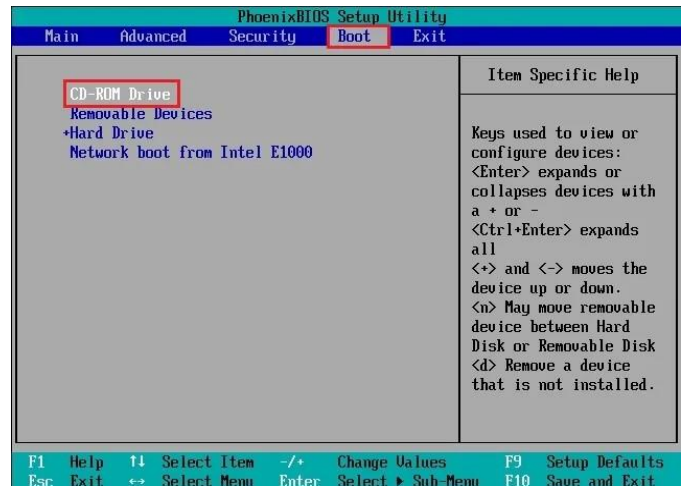
Minimum System Requirements.

Processor – 1.4 GHz 64-bit processor

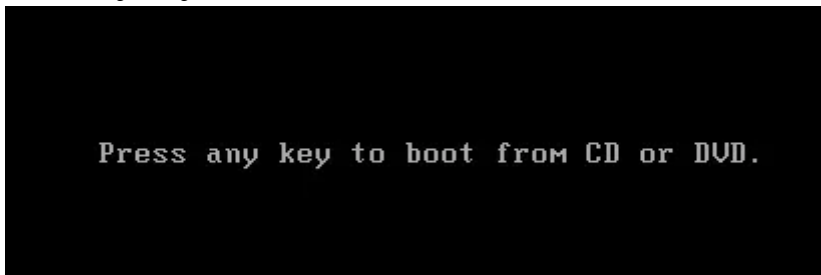
RAM – 512 MB

Disk Space – 32 GB

1. Insert a DVD of Windows Server 2012 into CD/DVD drive or bootable USB and start it set boot option from computer bios to DVD drive or USB.



2. Press any key else from CD or DVD.....



3. Select the language to install, time and currency format, keyboard or input method and click next.



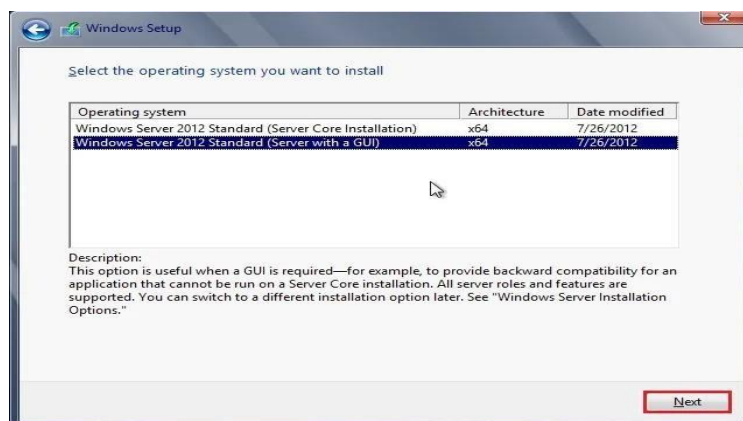
4. Server 2012 setup. click Install Now.



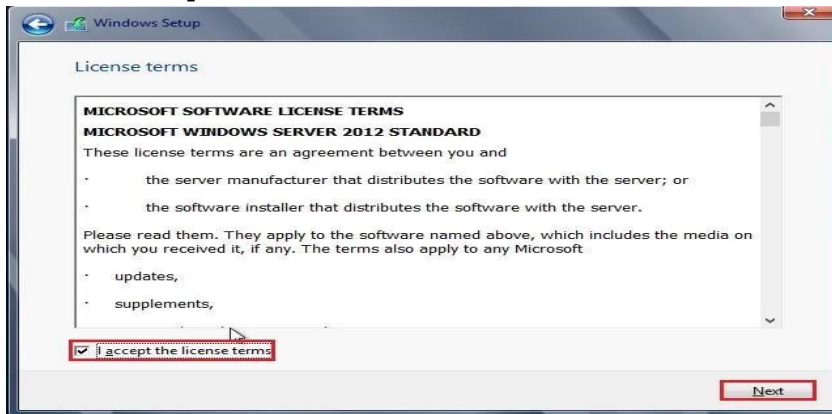
5. Type your 25-digit windows server 2012 key and click next.



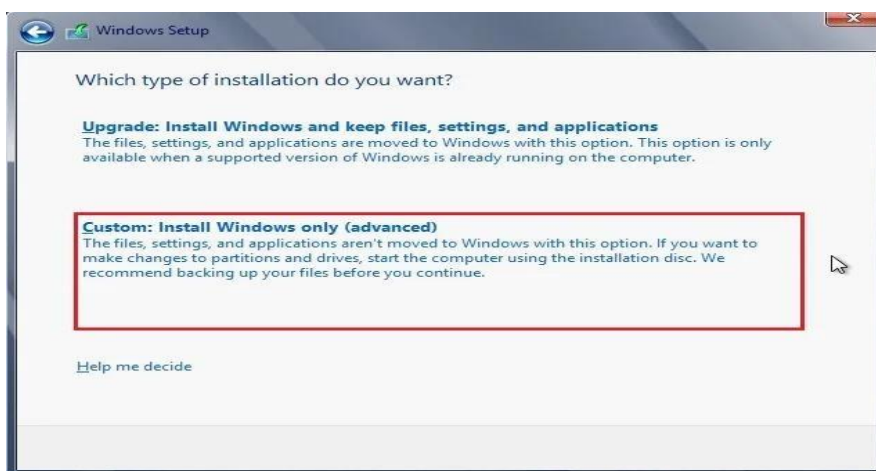
6. Select the operating system you want to install and then click Next.



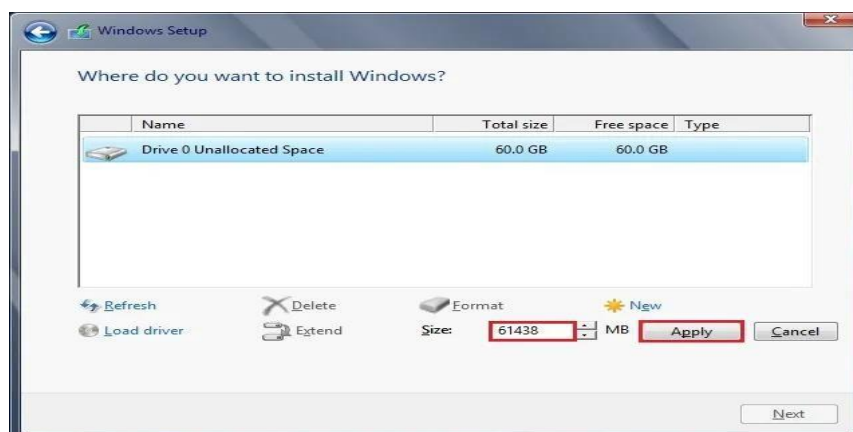
7. Select I accept the license terms and then click Next.



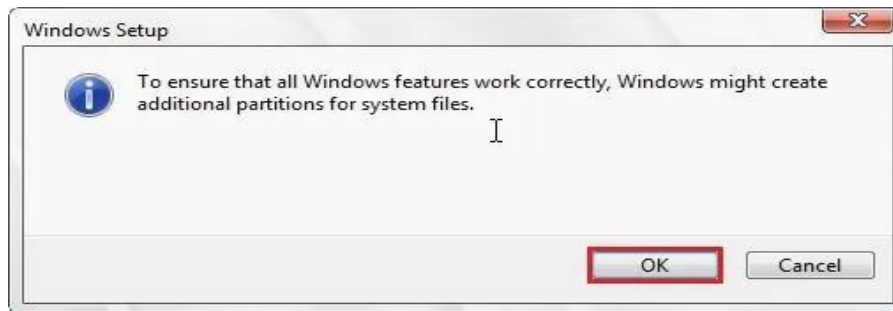
8. Select Custom: Install Windows only (advanced).



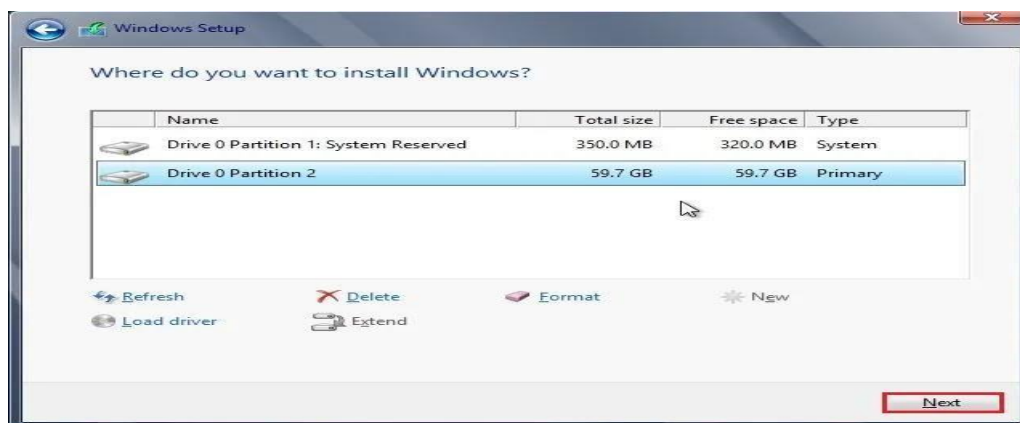
9. Select new to partition the hard disk and Select drive size in MB and then click Apply.



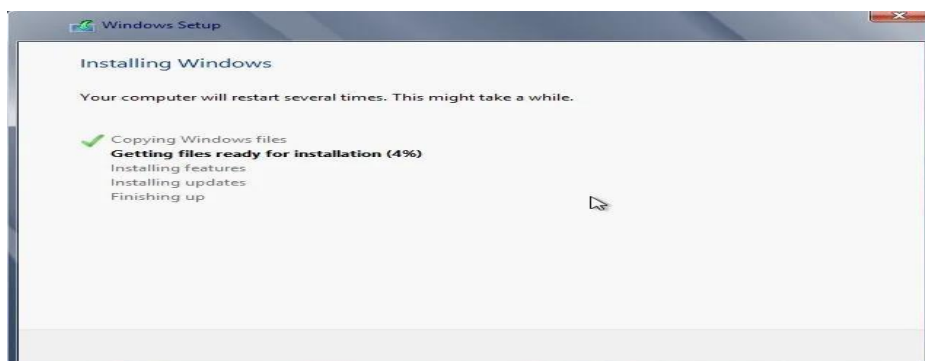
10. Windows might create an additional partition, so click ok.



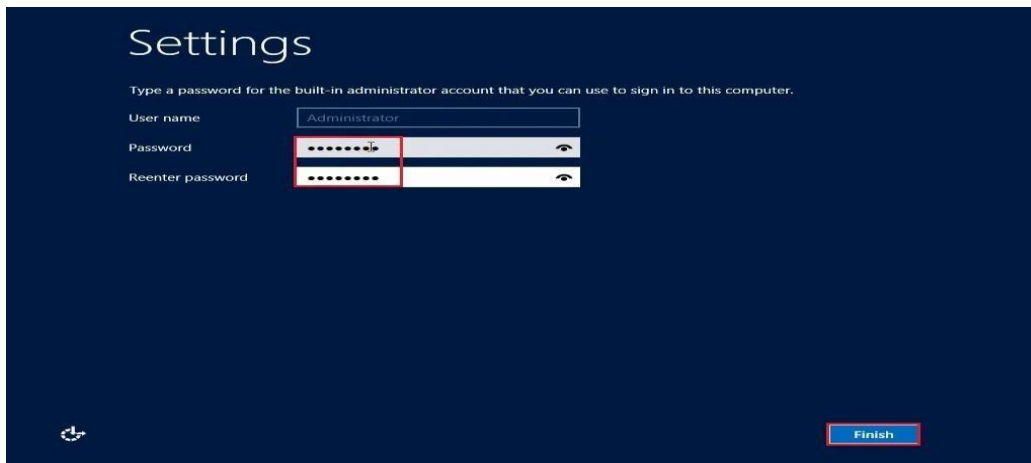
11. Select the drive where you want to install windows server 2012 and then click Next.



12. Copying windows files started > sit back and relax while Installation takes a moment.



13. After rebooting, type an administrative password and then click finish.



14. Login together with your current password to login Windows Server 2012.



15. Now you can change your time, time zone, date, server name and firewall settings.



Performing Post-Installation Tasks on Windows Server:

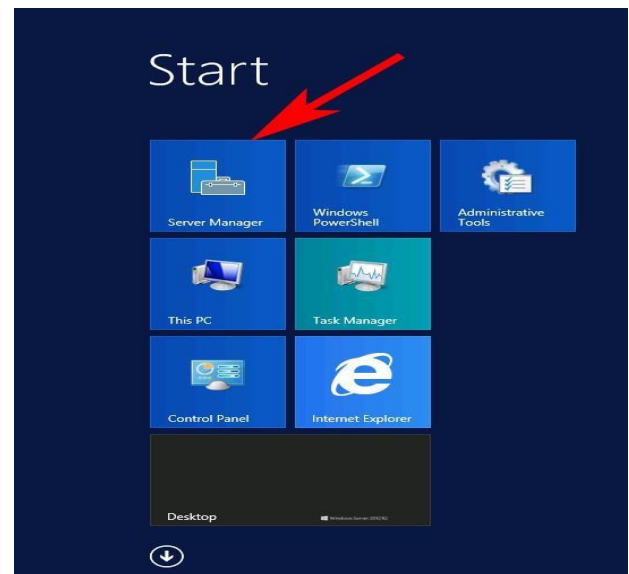
In this lab we will complete the tasks which are necessary after the installation of a freshly installed server. This lab is for the bare metal installation of a new Windows Server 2012 R2.

1. Log in As Administrator:

When installation finishes, log on to the server using Administrator privileges.

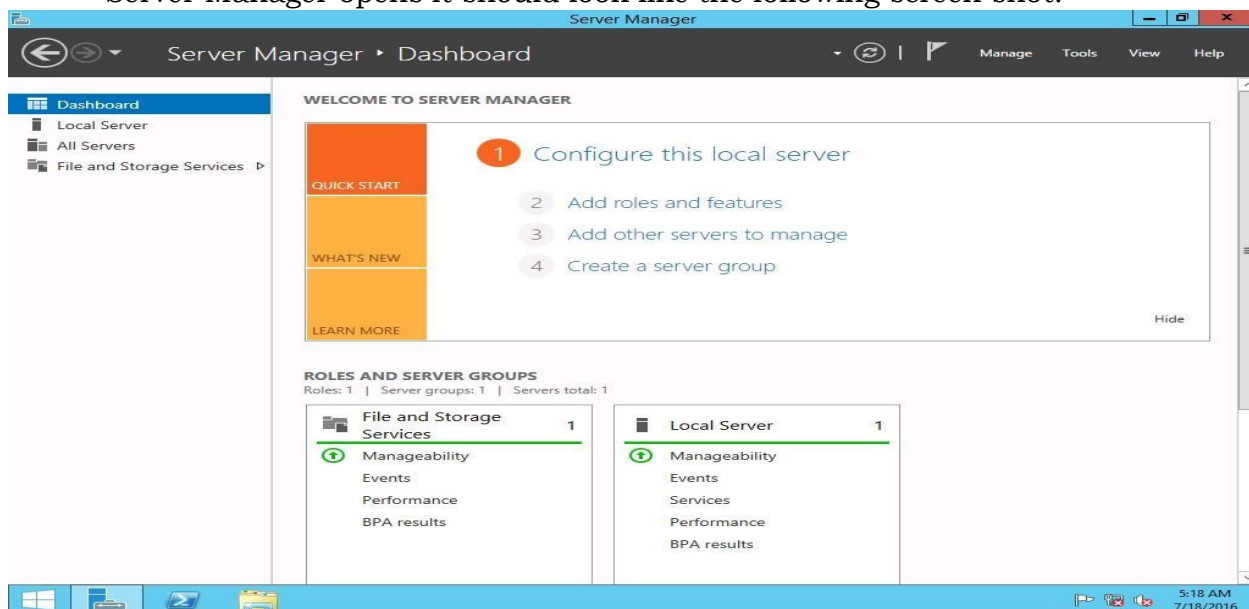
2. Locate Server Manager:

After Logging on as administrator Server Manager Console automatically opens, if it is not loaded automatically, press start button on your keyboard and select Server Manager.



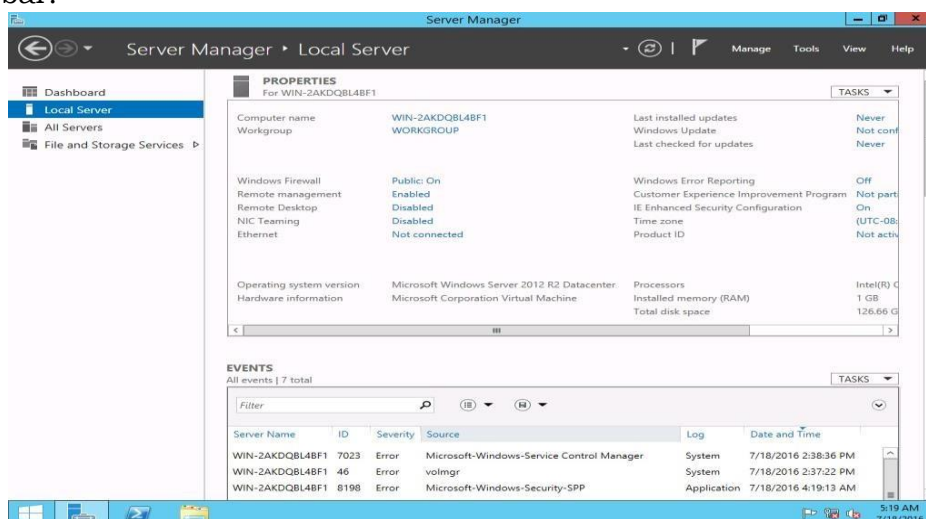
3. Open Server Manager:

Server Manager opens it should look like the following screen shot.



4.

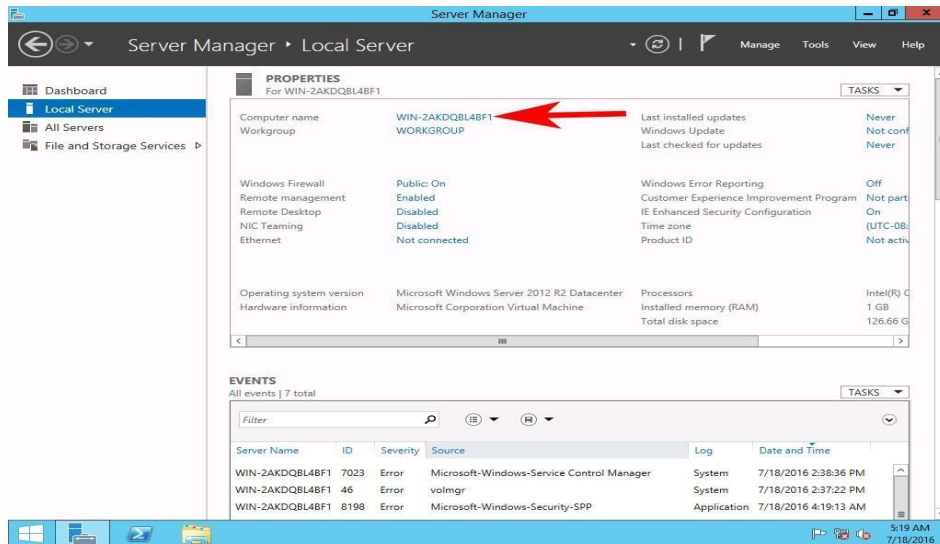
Configure Local Server Properties: In Server Manager window click on the local server in the left sidebar.



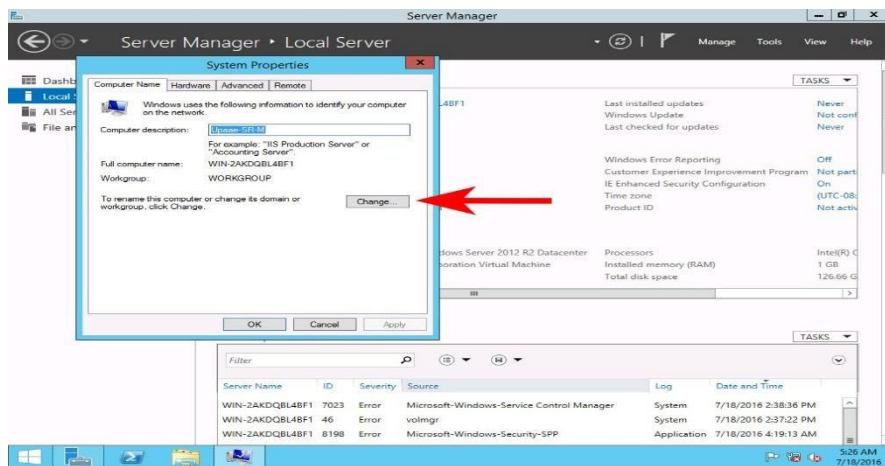
5. Set
Server Name:

24

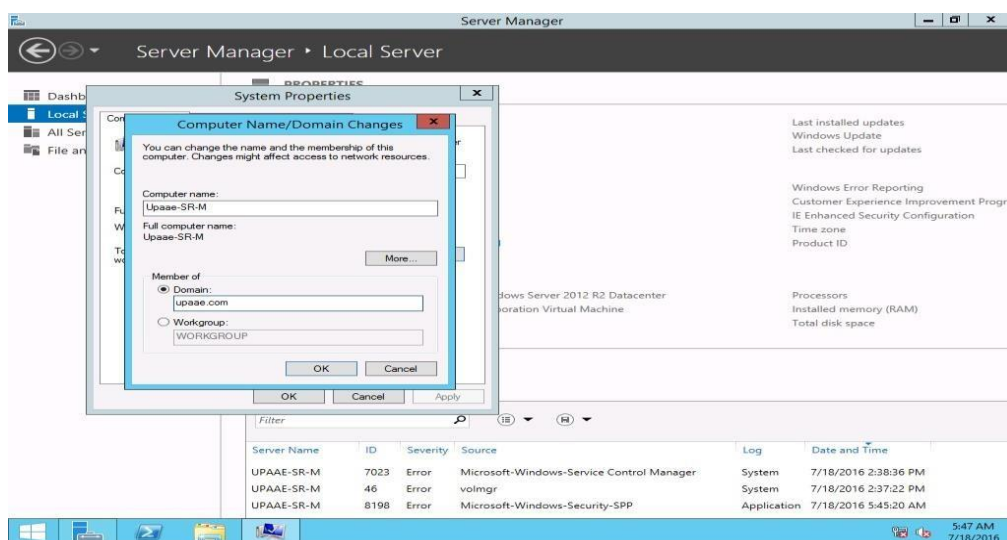
Click on the value of computer name.



A new window will open, type description for this server and then click on the *change* button for specifying the server name.



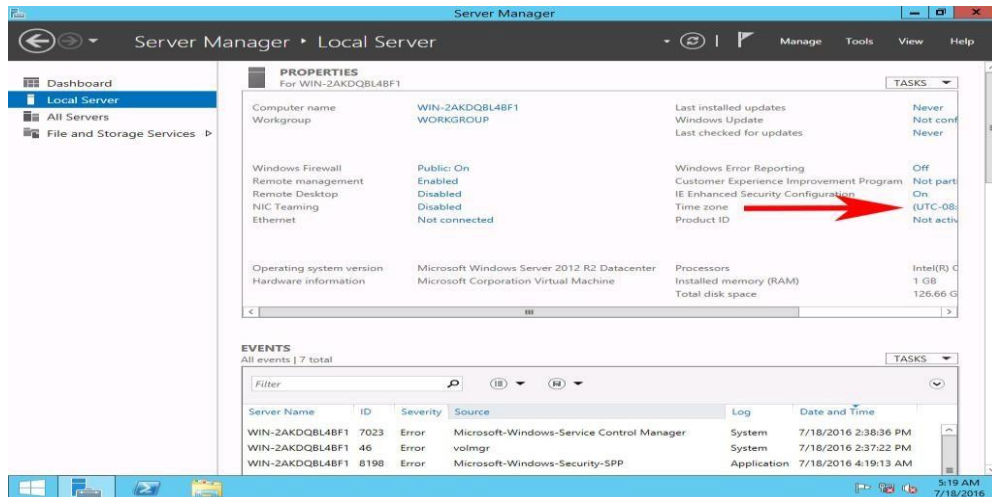
Note: If you already have a domain controller in your network then choose the option Domain and enter your domain name OR if this is your first server in the network then leave the WORKGROUP option selected.



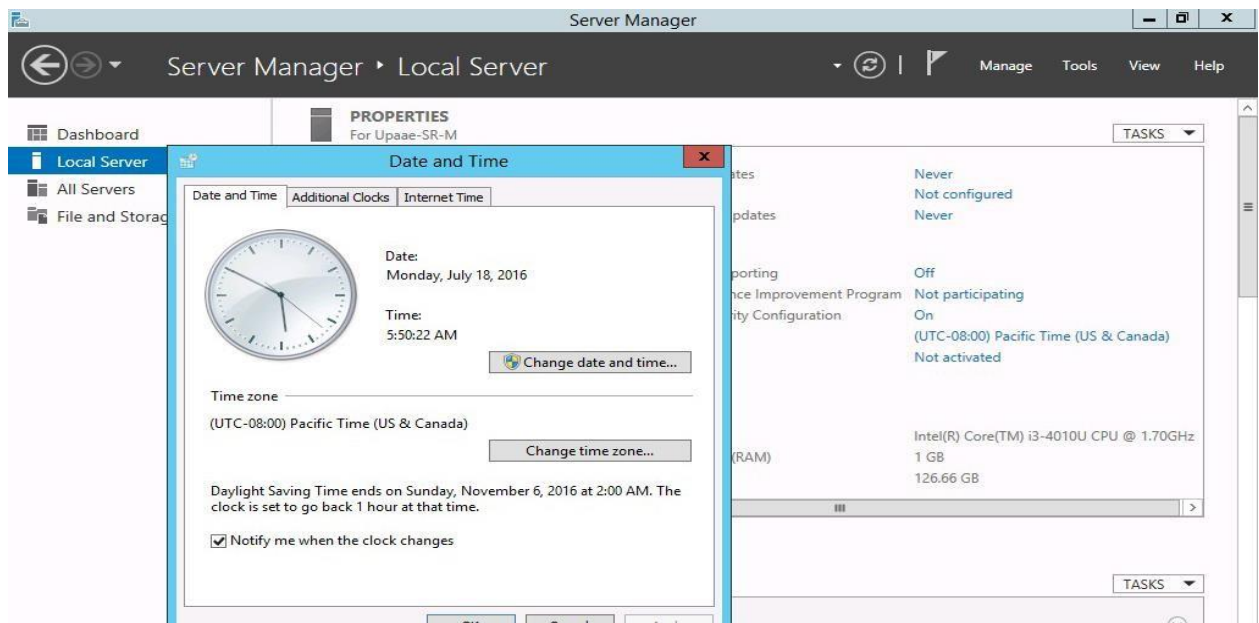
6. Set Time Zone/ Date and Time:

In Servers as well as computers setting the correct time zone is very important, When we are in front of computers we do not look at wrist watches or cell phones to check current time but instead we look at clock in the computer screen. Incorrect time will not just result in missing launch time but will affect scheduled tasks, file information, software and access authorization and will cause other time discrepancies.

Click on the time zone value.

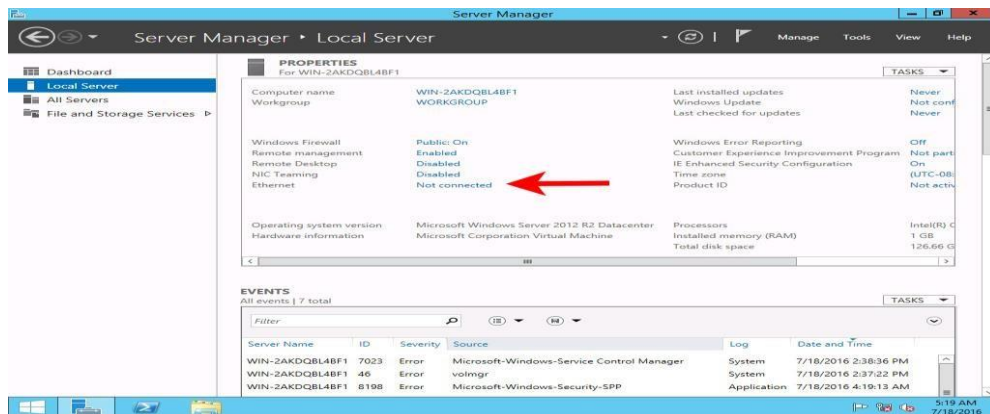


Select your time zone from the “Date and Time” window, set date and time if not already set and click OK button.

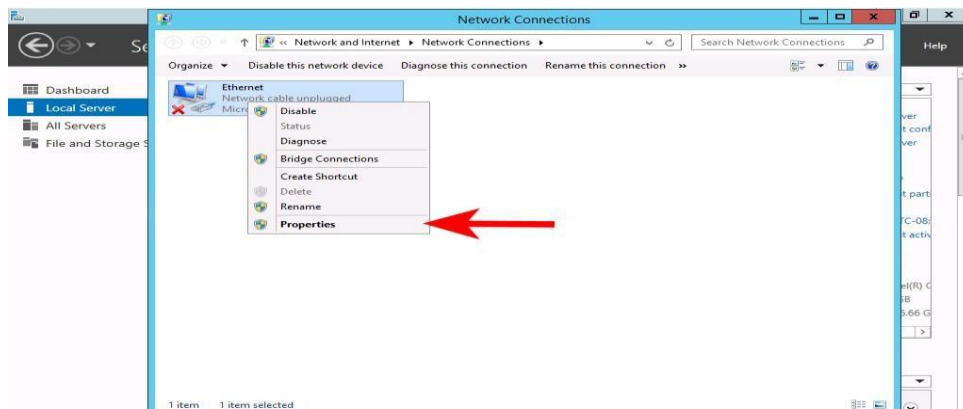


7. Configure Network Details:

Click on the Ethernet value.

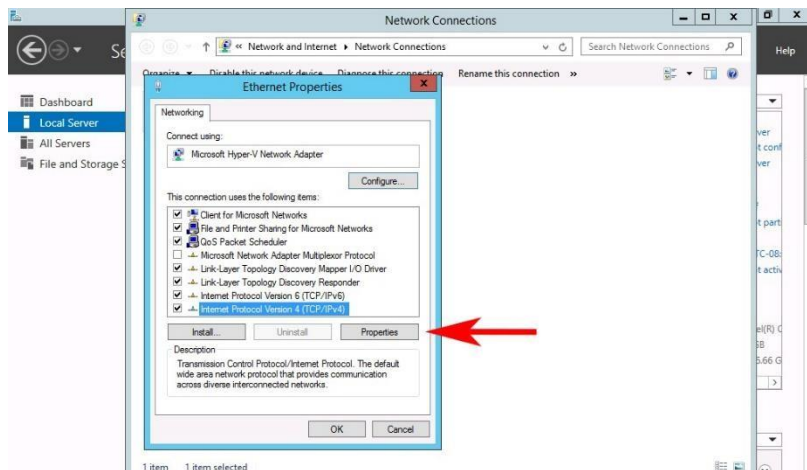


On the network connection window, Right-click the Ethernet connection and from the context menu, select Properties. The Ethernet Properties sheet will appear.

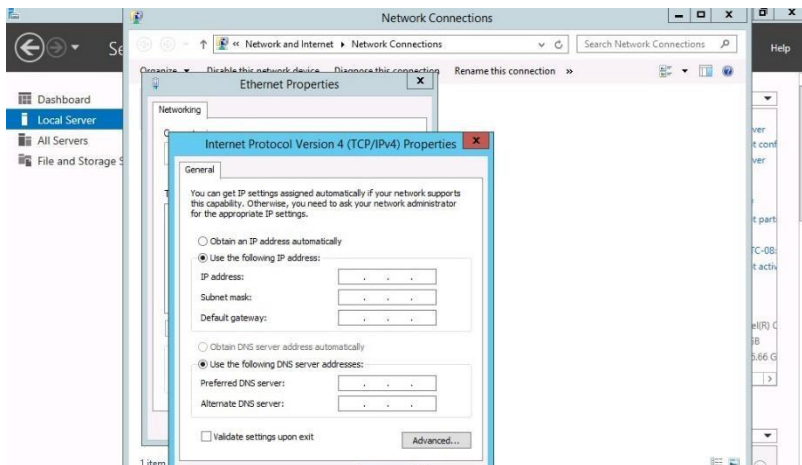


8. Configure TCP/IP:

Double-click Internet Protocol Version 4 (TCP/IPv4) OR select Internet Protocol Version 4 (TCP/IPv4) and click on properties button. This will open Internet Protocol Version 4(TCP/IPv4) Properties sheet.



On the Internet Protocol Version 4(TCP/IPv4) Properties sheet, we will enter network details which are as follows.



Note that servers should be configured with static IP address. Select the *Use the following IP address* option and, in the text boxes, type the following

values:

IP address: 192.168.1.3

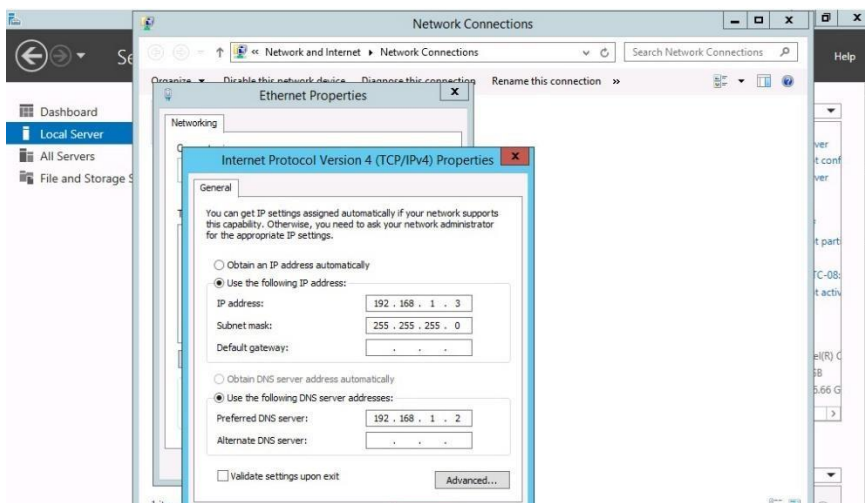
Subnet mask: 255.255.255.0

Default gateway: Leave blank

Select the *Use the following DNS server addresses* option and, in the text boxes, type the following values:

Preferred DNS server: 192.168.1.2

Alternate DNS server: Leave blank



Click OK to close the Internet Protocol Version 4 (TCP/IPv4) Properties sheet.

Click OK to close the Ethernet Properties sheet.

2. Manage Windows Server 2012

2.1. Overview of Windows Server 2012 Management

In Windows Server 2012, Microsoft updated Server Manager to allow it to add features and change server roles over the network. Server Manager could now manage multiple servers simultaneously and by role. Microsoft also increased the number of servers Server Manager can administer to 100. The number of servers that an administrator can manage with a single Server Manager console varies depending on the amount of data requested from the managed servers, as well as network and hardware resources available to the machine running Server Manager.

Windows Server Manager is installed by default on all editions of Windows Server 2012 and Windows Server 2012 R2. The Server Manager console is included with Remote Server Administration Tools for Windows 8 and Windows 8.1. Server Manager cannot manage servers on a machine running a higher version of Windows.

2.2 Introduction to Windows PowerShell.

PowerShell is a cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework. PowerShell runs on Windows, Linux, and macOS.



2.2.1. Command-line Shell

PowerShell is a modern command shell that includes the best features of other popular shells. Unlike most shells that only accept and return text, PowerShell accepts and returns .NET objects. The shell includes the following features:

- ✓ Robust command-line history
- ✓ Tab completion and command prediction
- ✓ Supports command and parameter aliases
- ✓ Pipeline for chaining commands
- ✓ In-console help system, similar to Unix man pages

2.2.2. Scripting language

As a scripting language, PowerShell is commonly used for automating the management of systems. It is also used to build, test, and deploy solutions, often in CI/CD environments. PowerShell is built on the .NET Common Language Runtime (CLR). All inputs and outputs are .NET objects. No need to parse text output to extract information from output. The PowerShell scripting language includes the following features:

- ✓ Extensible through functions, classes, scripts, and modules
- ✓ Extensible formatting system for easy output
- ✓ Extensible type system for creating dynamic types
- ✓ Built-in support for common data formats like CSV, JSON, and XML

```
PS C:\Users\Admin> Get-Help Format-Table

NAME
    Format-Table

SYNTAX
    Format-Table [[-Property] <Object[]>] [-AutoSize] [-HideTable
    [<CommonParameters>]

ALIASES
    ft

REMARKS
    Get-Help cannot find the Help files for this cmdlet on this c
    -- To download and install Help files for the module that
    -- To view the Help topic for this cmdlet online, type: "
    go to https://go.microsoft.com/fwlink/?LinkID=113303.
```

2.2.3. Automation platform

The extensible nature of PowerShell has enabled an ecosystem of PowerShell modules to deploy and manage almost any technology you work with. For example:

Microsoft

- Azure
- Windows
- Exchange
- SQL

Third-party

- ✓ AWS
- ✓ VMWare
- ✓ Google Cloud

Configuration management

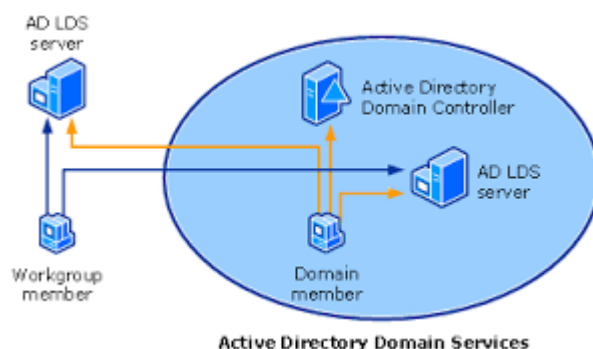
PowerShell Desired State Configuration (DSC) is a management framework in PowerShell that enables you to manage your enterprise infrastructure with configuration as code. With DSC, you can:

- ✓ Create declarative configurations and custom scripts for repeatable deployments
- ✓ Enforce configuration settings and report on configuration drift
- ✓ Deploy configuration using push or pull models

3. Install and configure Active Directory Domain Services

3.1. Overview of AD DS:

A directory is a hierarchical structure that stores information about objects on the network. A directory service, such as Active Directory Domain Services (AD DS), provides the methods for storing directory data and making this data available to network users and administrators. For example, AD DS stores information about user accounts, such as names, passwords, phone numbers, and so on, and enables other authorized users on the same network to access this information.



Active Directory stores information about objects on the network and makes this information easy for administrators and users to find and use. Active Directory uses a structured data store as the basis for a logical, hierarchical organization of directory information.

This data store, also known as the directory, contains information about Active Directory objects. These objects typically include shared resources such as servers, volumes, printers, and the network user and computer accounts. For more information about the Active Directory data store, see [Directory data store](#).

Security is integrated with Active Directory through logon authentication and access control to objects in the directory. With a single network logon, administrators can manage directory data and organization throughout their network, and authorized network users can access resources anywhere on the network. Policy-based administration eases the management of even the most complex network. For more information about Active Directory security, see [Security overview](#).

Active Directory also includes:

- A set of rules, the schema, that defines the classes of objects and attributes contained in the directory, the constraints and limits on instances of these objects, and the format of their names. For more information about the schema, see [Schema](#).
- A global catalog that contains information about every object in the directory. This allows users and administrators to find directory information regardless of which domain in the directory actually contains the data. For more information about the global catalog, see [Global catalog](#).
- A query and index mechanism, so that objects and their properties can be published and found by network users or applications. For more information about querying the directory, see [Searching in Active Directory Domain Services](#).
- A replication service that distributes directory data across a network. All domain controllers in a domain participate in replication and contain a complete copy of all

directory information for their domain. Any change to directory data is replicated to all domain controllers in the domain. For more information about Active Directory replication, see Active Directory Replication Concepts.

3.2. Overview of Domain Controllers

A domain controller is a server that responds to authentication requests and verifies users on computer networks. Domains are a hierarchical way of organizing users and computers that work together on the same network. The domain controller keeps all of that data organized and secured.

The primary responsibility of the DC is to authenticate and validate user access on the network. When users log into their domain, the DC checks their username, password, and other credentials to either allow or deny access for that user.



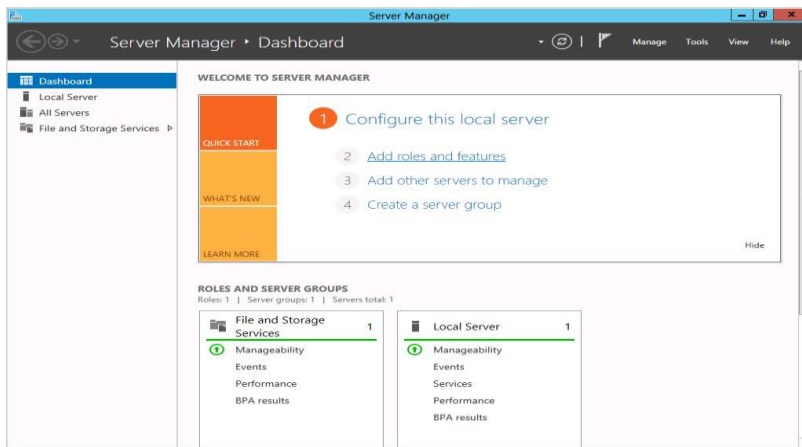
3.3. Installing a domain controller

As the domain controller is vital for the functioning of Active Directory, configuration should be done carefully to avoid any errors. Follow the steps below to make sure your domain controller is set up perfectly.

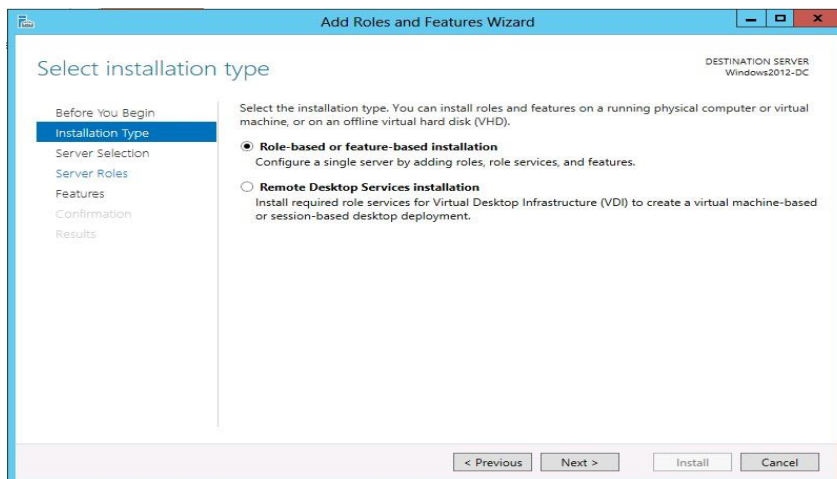
Before you begin, ensure you assign static IP address to your Domain Controller to help Active Directory objects locate the Domain Controller easily.

Step 1: Install Active Directory Domain Services (ADDS)

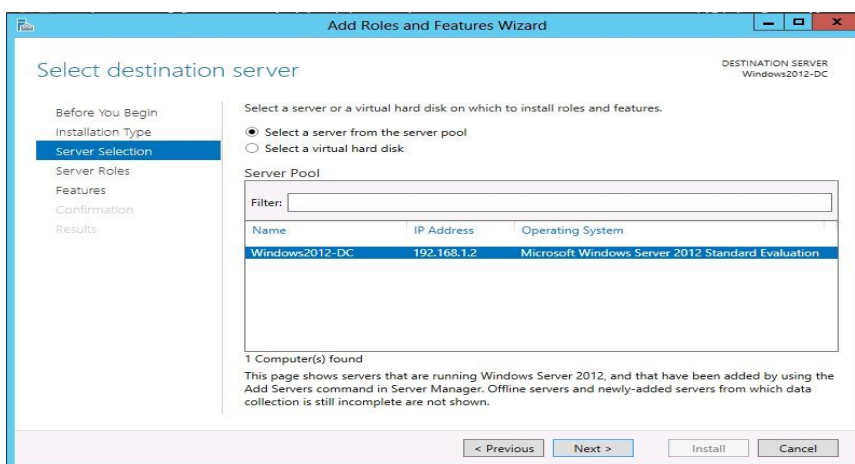
1. Log into your Active Directory Server with administrative credentials.
2. Open Server Manager → Roles Summary → Add roles and features



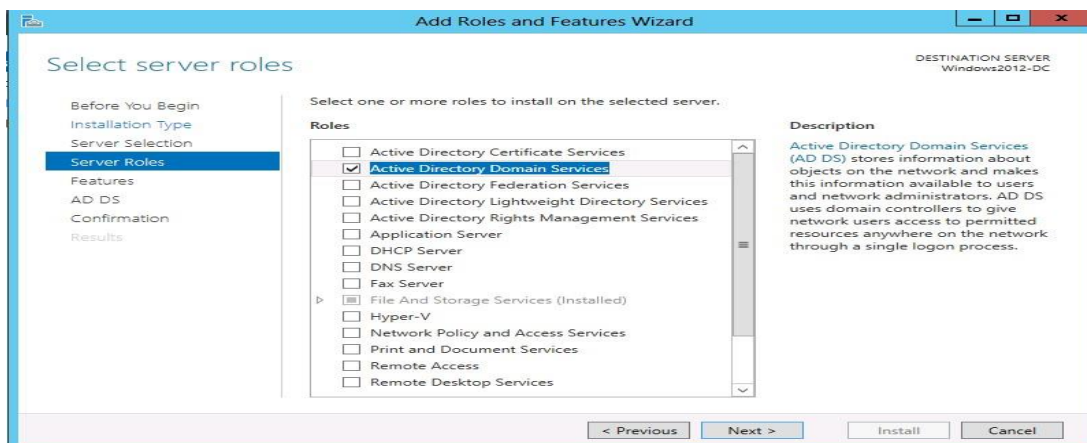
3. The "Before you begin" screen, which pops up next, is purely for an informational purpose. You may read through it and click "next".
4. Select the installation type. If you're going to deploy your DC in a virtual machine, choose Remote Desktop Services installation. Else, choose Role-based or Feature-based installation.



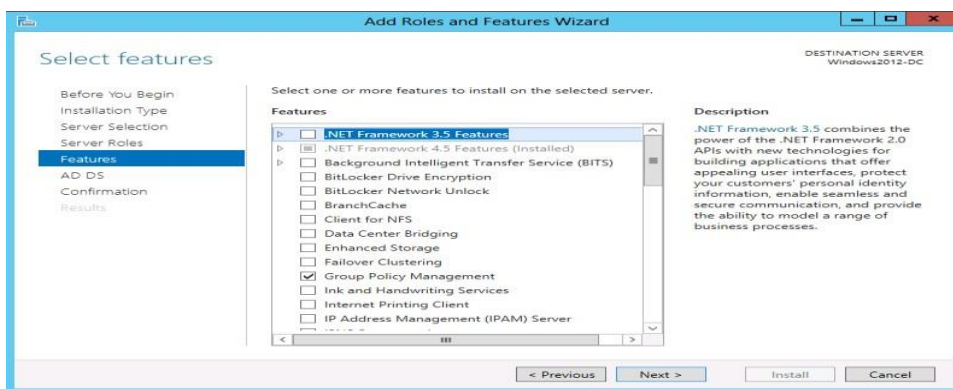
5. Now, select the destination server on which the role will be installed. Make sure the IP address points to the selected server. Else, close the server manager and retry.



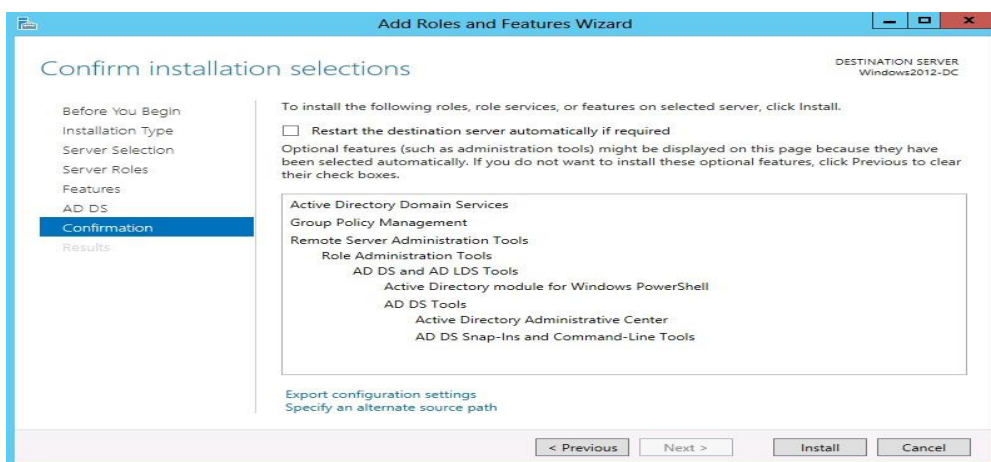
6. Select the roles you want to install on this server. The basic requirements to promote this server into a domain controller is Active Directory Domain Services.



7. The basic features required for proper functioning of this role are selected by default. Click next to install them.

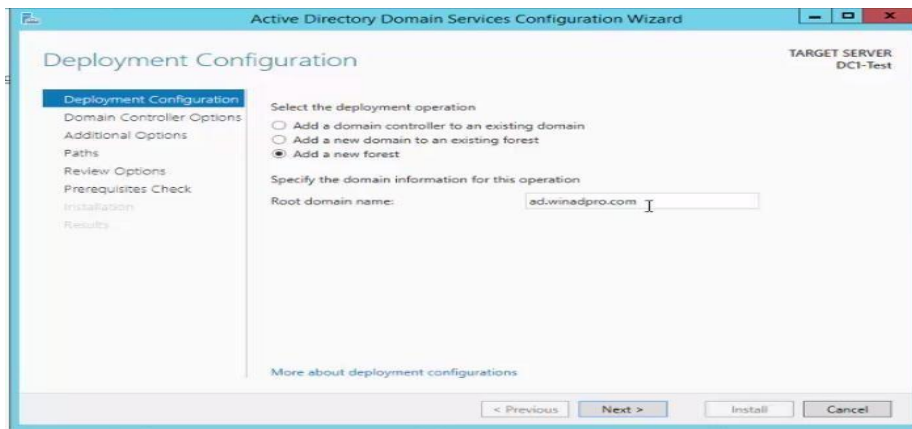


8. Confirm your installation selections. It is recommended to select the "Restart the destination server automatically if required" button. Select "Install" and once installation is complete, close the window.

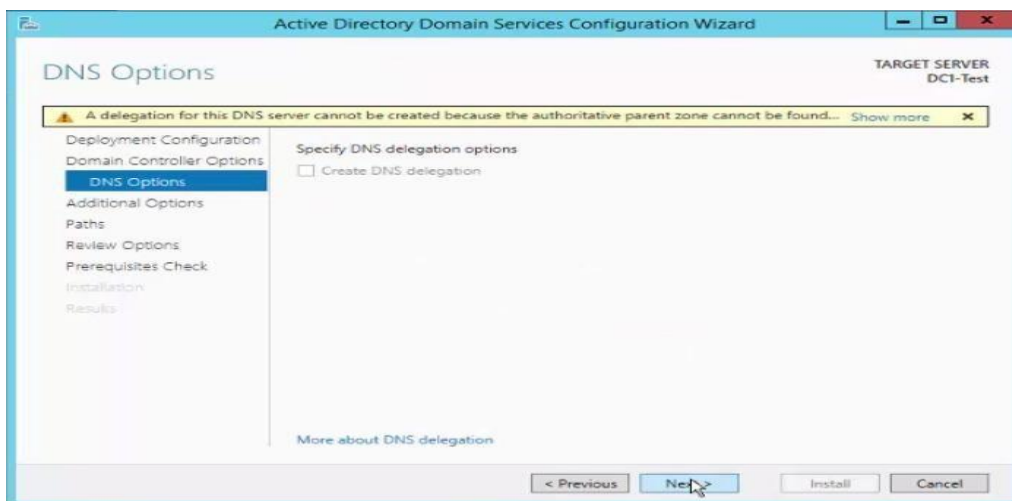


Step 2: Promote the server into a domain controller

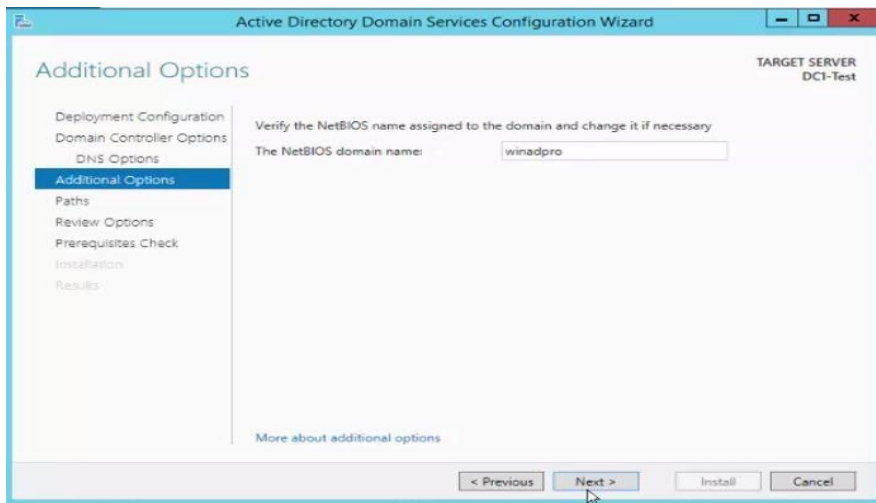
1. Once the ADDS role is installed in this server, you will see a notification flag next to the Manage menu. Select "Promote this server into a domain controller"
2. Select "Add a new forest" and enter Root domain name. This domain name will also be the forest name.



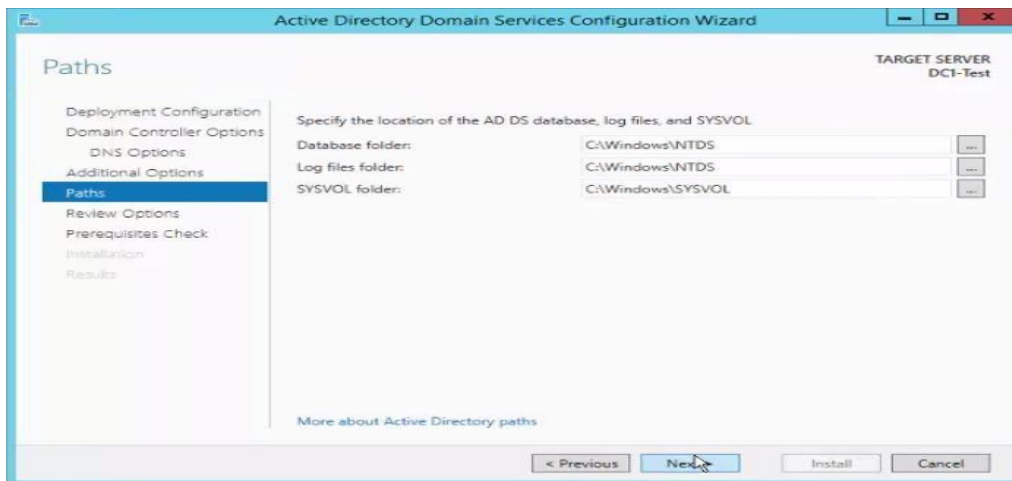
3. Select a forest functional level and a domain functional level of your choice. Ensure that the domain functional level is equal to or higher than the forest functional level. Since this is the first domain controller, it automatically becomes the DNS server and also the Global Catalog (GC). Enter a unique Active Directory Restore Mode password used to retrieve Active Directory data.
4. Since a DNS Server is being configured as part of our efforts, you'll be warned that a delegation for this DNS server cannot be created. This can be safely ignored.



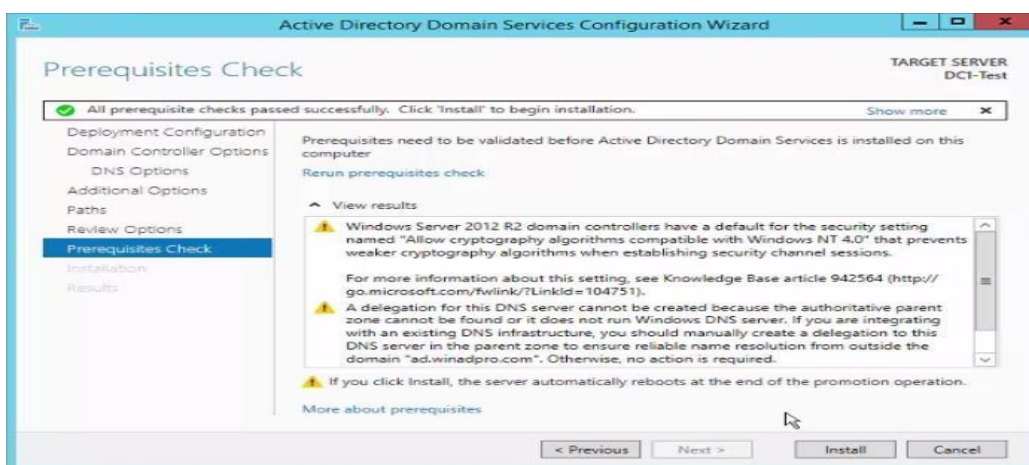
5. Enter a NetBIOS name for your domain. It is preferable to match the NetBIOS name with the root domain name. For more information on NetBIOS name restrictions, see <https://support.microsoft.com/en-us/kb/909264>



6. Select the folder where your database, log files, and SYSVOL will be stored. It is recommended to stick to the default settings.



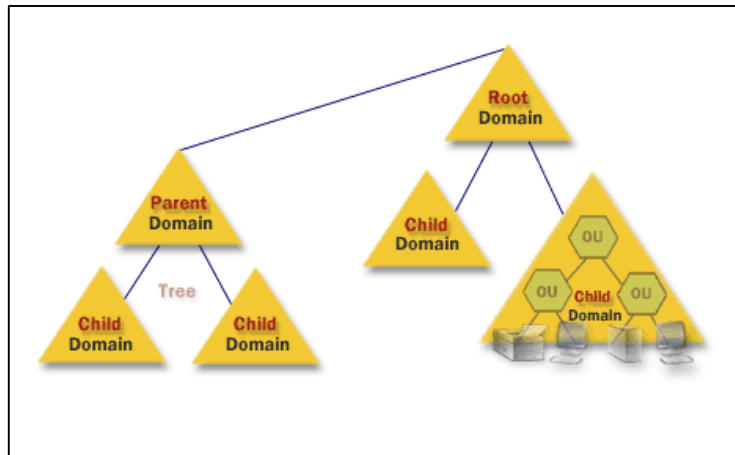
7. Review your options and click Next. A prerequisites check will be done by Active Directory. Once it is completed, click Install.



8. Your system will be rebooted automatically for the changes to take effect. Verify the health of the domain controller by running the command `dcdiag /v` from the command line.

3.4. Structure of AD DS

AD DS organizes data in a hierarchical structure consisting of domains, trees, and forests, as detailed below.



- Domains: A domain represents a group of objects such as users, groups, and devices, which share the same AD database. You can think of a domain as a branch in a tree. A domain has the same structure as standard domains and sub-domains, e.g. yourdomain.com and sales.yourdomain.com.
- Trees: A tree is one or more domains grouped together in a logical hierarchy. Since domains in a tree are related, they are said to “trust” each other.
- Forest: A forest is the highest level of organization within AD and contains a group of trees. The trees in a forest can also trust each other, and will also share directory schemas, catalogs, application information, and domain configurations.
- Organizational Units: An OU is used to organize users, groups, computers, and other organizational units.
- Containers: A container is similar to an OU, however, unlike an OU, it is not possible to link a Group Policy Object (GPO) to a generic Active Directory container.

3.5. Purpose of domain controllers

Domain controllers contain the data that determines and validates access to your network, including any group policies and all computer names. Everything an attacker could possibly need to cause massive damage to your data and network is on the DC, which makes a DC a primary target during a cyberattack.

In general, yes. Any business – no matter the size – that saves customer data on their network needs a domain controller to improve security of their network. There could be exceptions: some businesses, for instance, only use cloud based CRM and payment solutions. In those cases, the cloud service secures and protects customer data.

The key question you need to ask is “where does my customer data live and who can access it?”

The answer determines if you need a domain – and DC – to secure your data.

3.5.1. Benefits of Domain Controller

- 1) Centralized user management
- 2) Enables resource sharing for files and printers
- 3) Federated configuration for redundancy (FSMO)
- 4) Can be distributed and replicated across large networks
- 5) Encryption of user data
- 6) Can be hardened and locked-down for improved security

3.5.2. Limitations of Domain Controller

- 1) Target for cyberattack
- 2) Potential to be hacked
- 3) Users and OS must be maintained to be stable, secure and up-to-date
- 4) Network is dependent on DC uptime
- 5) Hardware/software requirements

4. Manage Active Directory Domain Services Objects

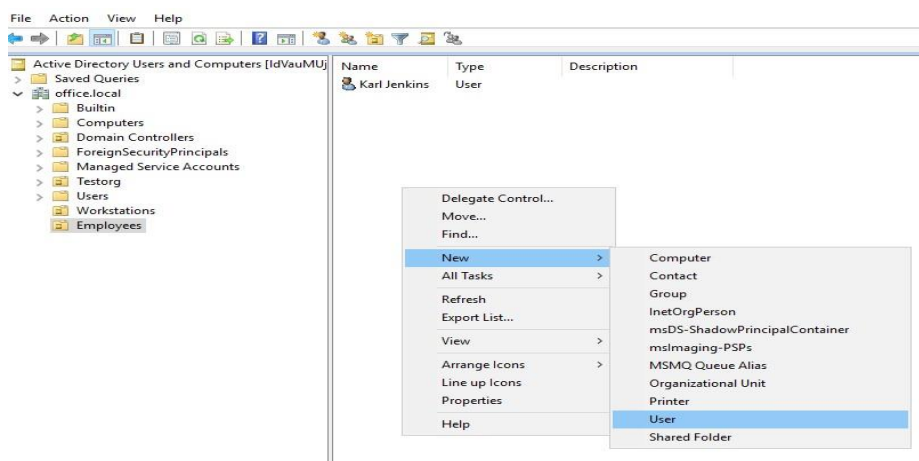
4.1. Managing User Accounts

Users are one of the most popular objects in AD. They are used for authentication and authorization on workstations. Also in many services which are integrated with AD. User management is the main routine for sysadmins and helpdesk specialists. This guide helps to manage such objects in multiple ways. For managing users there is a need to install RSAT tools or manage them from your DC. You have to be signed under domain admin or an Account Operators user or with delegation rights to create objects in the current OU.

Creating User Account Using Active Directory

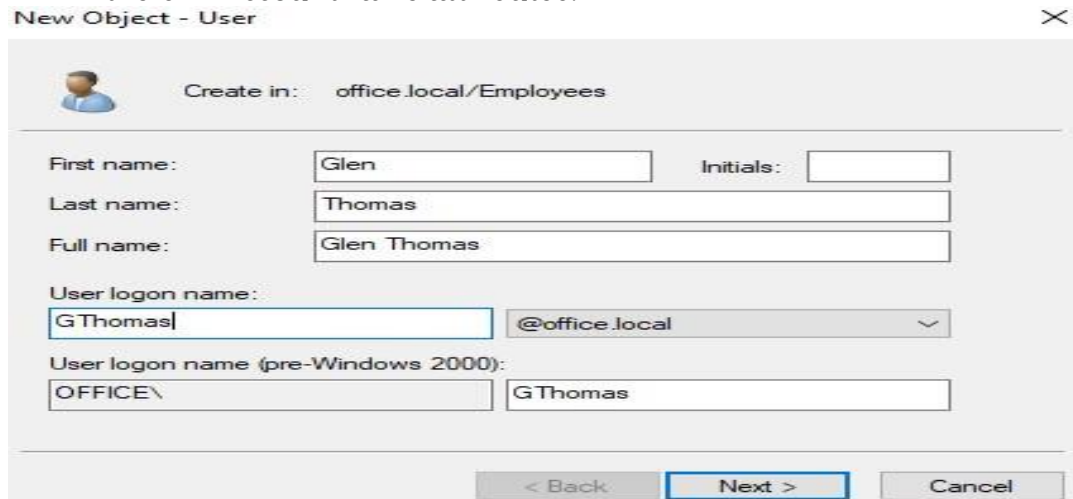
Run ADUC (dsa.msc).

Go to OU where new users should be located. In the taskbar, click the "New User" icon, or right-click on a white space in the main window and then click on "New -> User". Another way is rightclicking the needed Org Unit and select "New -> User".

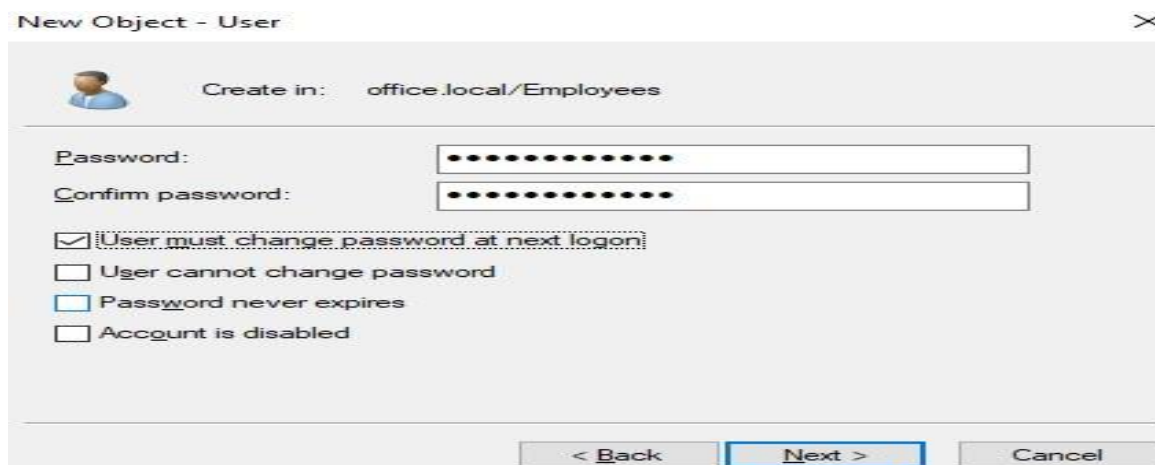


"New Object — User" appears, specify parameters for your user:

- Full name, by either typing the full name into Full Name field or typing it in the First and Last name fields.
- User logon name, this field creates the userPrincipalName and the sAMAccountName attributes.



Click Next and specify strong password and then retype it in the next field and check the needed parameters, usually for regular user you should check “User must change password at next logon”.



Click Next and Finish. Congratulations new user was successfully created!

Creating User Account Using Command Prompt

To make the same thing in cmd we need to use dsadd.exe utility. The following parameters will help to create a user in “Users” container in AD and set default password for it:

```
dsadd.exe user "CN=GSoul,CN=Users,DC=office,DC=local" -upn GSoul@office.local -fn "Gordon" -ln "Soul" -display "Gordon Soul" -pwd "P@&&W0rd"
```

Creating User Account Using Windows PowerShell

Run the following PowerShell code under Administrator privileges:

```
Import-Module ActiveDirectory
New-ADUser -Name FRobinson -Path "CN=Users,DC=office,DC=local"
GivenName "Frank" -Surname "Robinson" -sAMAccountName FRobinson
```

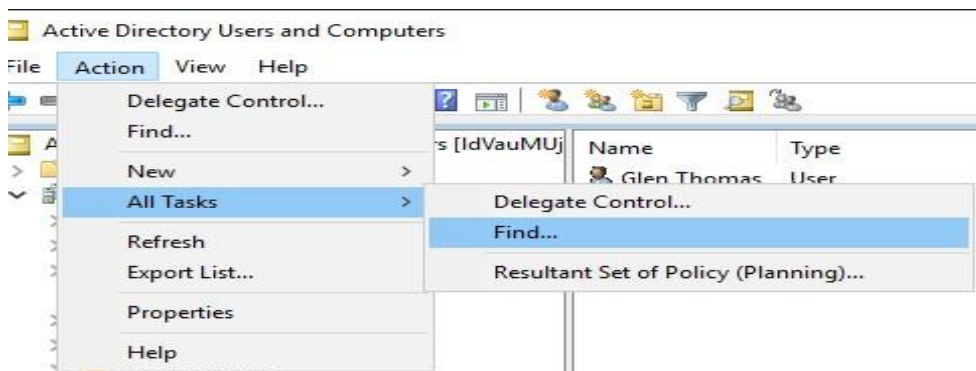
How to Delete a User Account

Lets delete a user from AD environment, follow these easy methods. Note that this action will not completely delete a user account with enabled AD Recycle Bin, it will change its token attributes and move it to deleted objects.

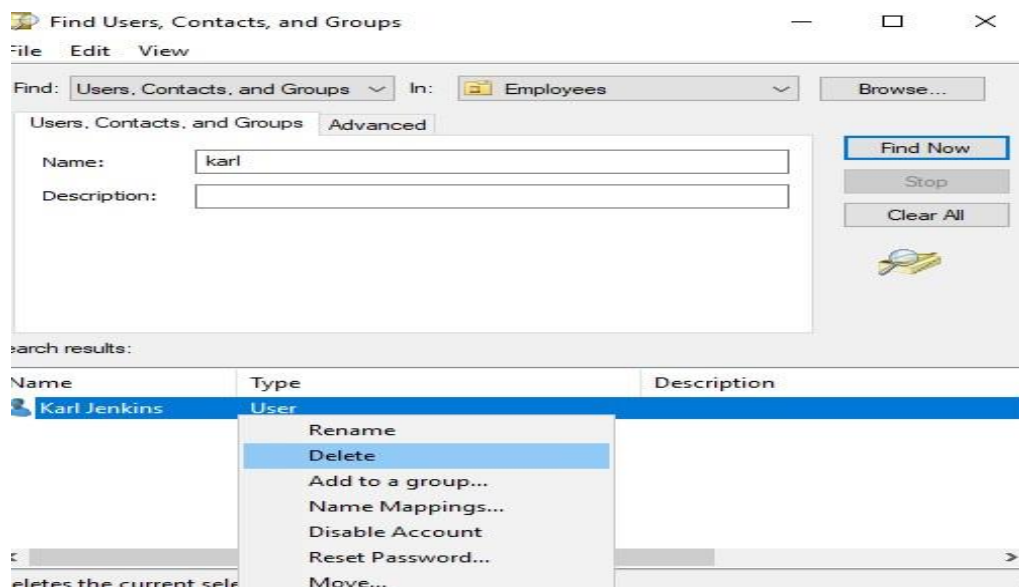
Deleting User Account in Active Directory Users and Computers (ADUC)

Lets delete one user, to achieve that open Active Directory Users and Computers (dsa.msc). Go

to the OU or container where the user that you need to delete resides. Click on the Action menu or right click the OU and select Find.



Type in the name or last name of the user you want to delete into the name field and click "Find Now". The results will be displayed to you, select the object you need to delete, rightclick it and then click on Delete and confirm your decision.



Deleting User Account Using Command Prompt

The following cmd string will delete a user “GSoul” from office.local domain:

```
dsrm.exe user "CN=GSoul,CN=Users,DC=office,DC=local"
```

Deleting User Account Using PowerShell

Execute the following PowerShell code to delete a user GSoul from AD:

```
Import-Module ActiveDirectory
Remove-ADUser -Identity "CN=GSoul,CN=Users,DC=office,DC=local"
```

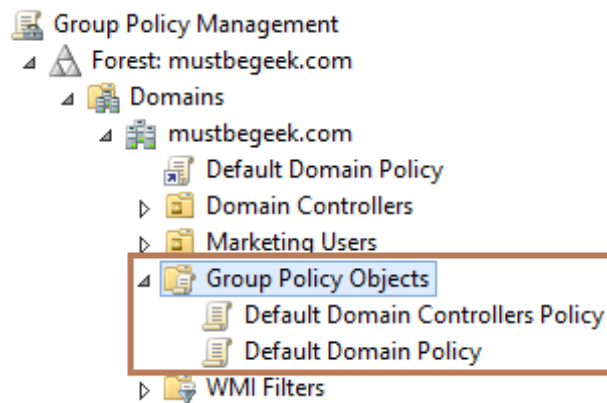
5. Implementing Group Policy

Group Policies are computer or user settings that can be defined to control or secure the Windows server and client infrastructure. Understanding GPO in Windows Server 2012 before actually configuring and applying policy settings is very important. It is easy to understand GPO in Windows Server 2012. There are some new features of GPO in Windows Server 2012.

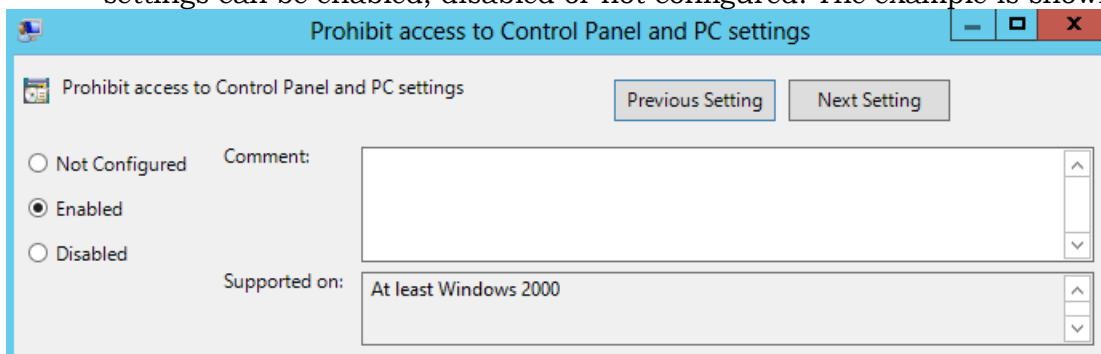
Understanding GPO in Windows Server 2012

Two main components of GPO are, GPO Object and GPO Policy Settings.

- GPO Object: – GPO Object is an active directory object that has various group policy settings. These policy settings can be user settings or computer settings and can be applied to user or computers. GPO objects are stored in GPO container. The GPO object is stored in active directory database and each object has its own unique GUID (Globally Unique Identifier).



- **GPO Policy Settings:** – GPO policy settings are the real settings within GPO object that defines particular action. GPO policy settings comes from GPO templates which are stored in SYSVOL folder of each domain controller. For example, Prohibit Access to Control Panel is a GPO policy setting that will simply disable access to control panel. Most of the GPO settings can be enabled, disabled or not configured. The example is shown below,



When you create a group policy, the GPO object is created and stored in GPO container in active directory and at the same time, GPO template is created and stored in SYSVOL folder. After creating a group policy, it can be linked to Sites, Domains and OUs. Group policy is process in the order of LSDOU: –

1. Local Group Policy
2. Sites
3. Domains
4. Organizational OUs

There are certain things that you should remember while creating and applying GPO settings. As stated earlier there are computer settings and user settings of each GPO object. Computer settings are applied at startup of the client machine. User settings are applied at use logon. Policies refresh can be initiated manually by using, `C:\> gpupdate /force` command or `C:\> Invoke-Gpupdate` PowerShell cmdlet.

In fresh domain controller there are two default group policy settings configured. They are: –

1. **Default Domain Policy:** – This policy is linked to the entire domain and has policies like password policies, account lockout policies and kerberos protocol policies. It is recommended that not to edit this policy. If you want to link new group policy then create new GPO and link to the domain.
2. **Default Domain Controller Policy:** – This policy setting is applied to domain controllers and is linked to domain controllers OU. This policy affects domain controllers only.

Unit 3:- Installation and configuration of Linux server

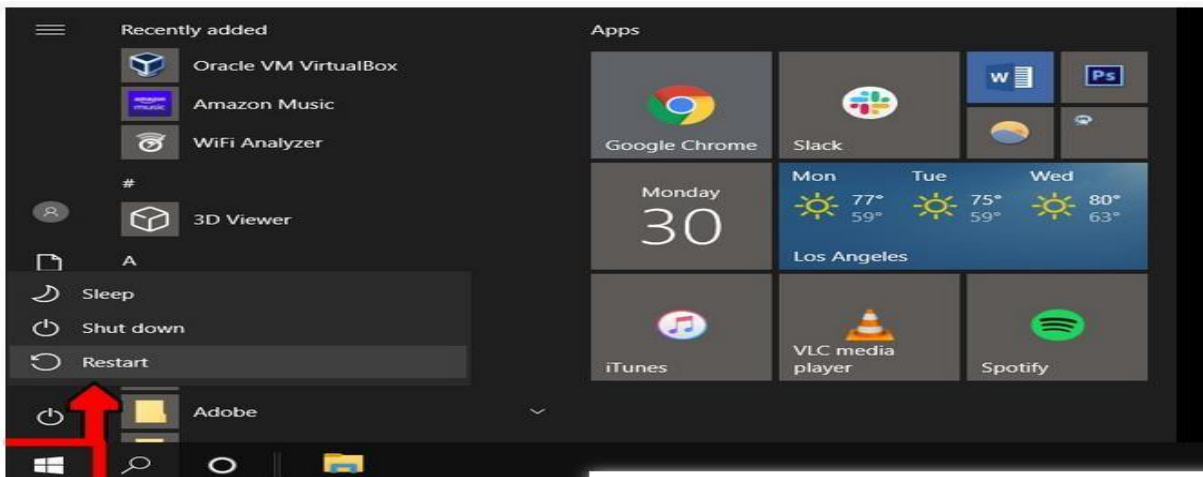
13.1 Linux server overview

A Linux server is a server built on the Linux open-source operating system. It offers businesses a low-cost option for delivering content, apps and services to their clients. Because Linux is open-source, users also benefit from a strong community of resources and advocates.

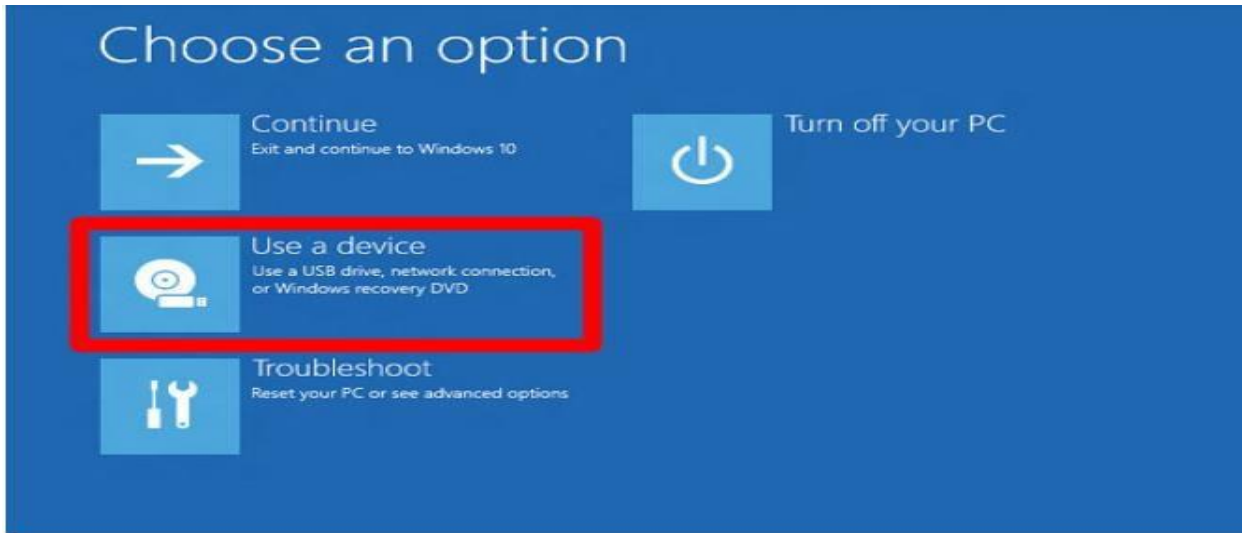


Installation process of linux server

1. Insert a bootable Linux USB drive.
2. Click the start menu. This is the button in the lower-left corner of your screen that looks like the Windows logo.
3. Then hold down the SHIFT key while clicking Restart. This will take you into the Windows Recovery Environment.



4. Then select Use a Device.



5. Find your device in the list. If you don't see your drive, choose EFI USB Device, then pick your drive from the next screen.



6. Your computer will now boot Linux. If your computer reboots Windows, there was either an issue with your drive, or you might have to change settings in your BIOS.

Warning: Changing BIOS settings can damage your computer if you don't know what you're doing.

13.2 Overview of linux server management

Linux server management is an integration of cyber security and business objectives. Linux server management at scale is a vastly different activity from interacting with a terminal on one machine. The best Linux server management tools universally offer a server management GUI within a web browser. Implementation details matter, especially in a pay-for-compute

world. System admin tools that don't have a lightweight footprint increase overall compute costs.

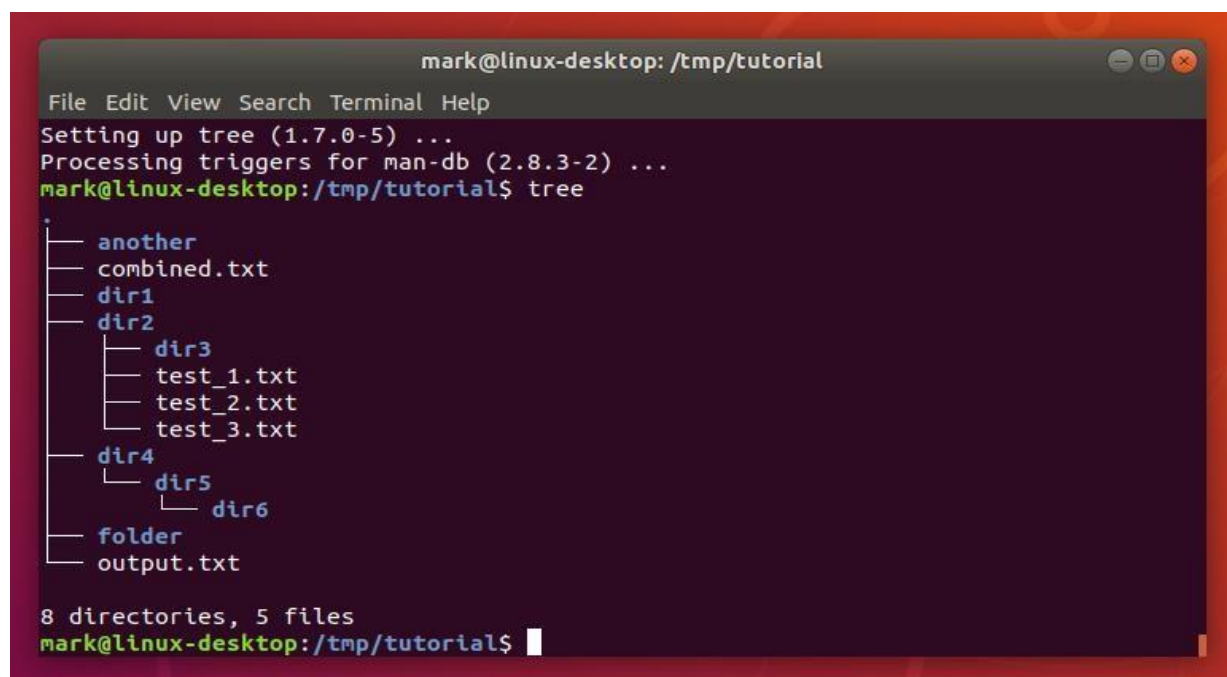
In short, the two most desirable attributes for your Linux server management tools are:

1. Lightweight: the Linux server management software should not compete with your workload for memory, disk, and processor resources
2. Scalable: the server dashboard should allow you to manage a large fleet as easily as one machine

linux terminal and concept of super user

linux terminal:- The Linux terminal is a text-based interface used to control a Linux computer. It's just one of the many tools provided to Linux users for accomplishing any given task, but it's widely considered the most efficient method available.

superuser:- In Linux and Unix-like systems, the superuser account, called 'root', is virtually omnipotent, with unrestricted access to all commands, files, directories, and resources. Root can also grant and remove any permissions for other users. Mac OS X, is Unix-like, but unlike Unix and Linux, is rarely deployed as a server.



```
mark@linux-desktop: /tmp/tutorial
File Edit View Search Terminal Help
Setting up tree (1.7.0-5) ...
Processing triggers for man-db (2.8.3-2) ...
mark@linux-desktop:/tmp/tutorial$ tree
.
├── another
├── combined.txt
├── dir1
├── dir2
│   ├── dir3
│   │   ├── test_1.txt
│   │   ├── test_2.txt
│   │   └── test_3.txt
│   ├── dir4
│   │   └── dir5
│   │       └── dir6
├── folder
└── output.txt

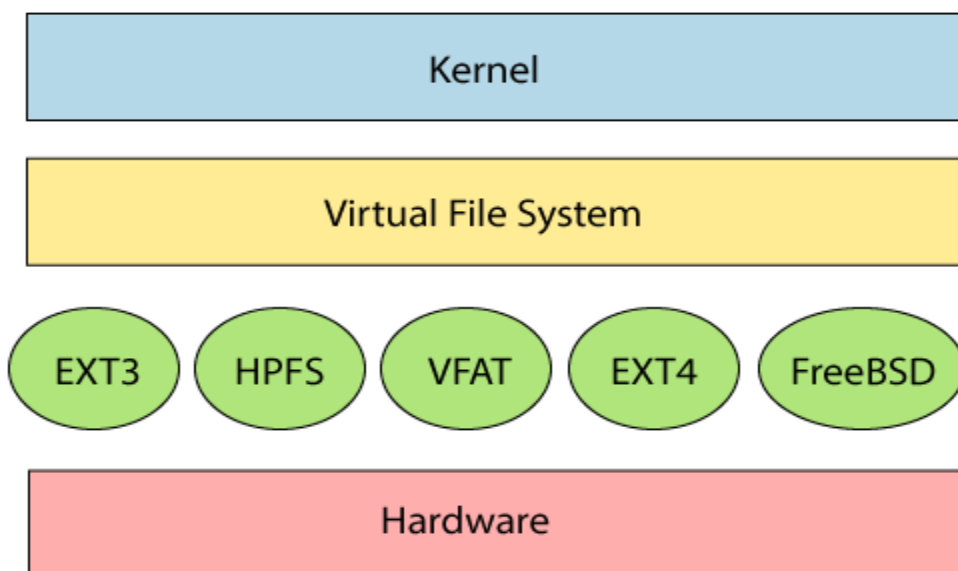
8 directories, 5 files
mark@linux-desktop:/tmp/tutorial$
```

linux terminal and command

13.3 Understand the file structure of linux

overview of linux file structure

A Linux file system is a structured collection of files on a disk drive or a partition. A partition is a segment of memory and contains some specific data. In our machine, there can be various partitions of the memory. Generally, every partition contains a file system.



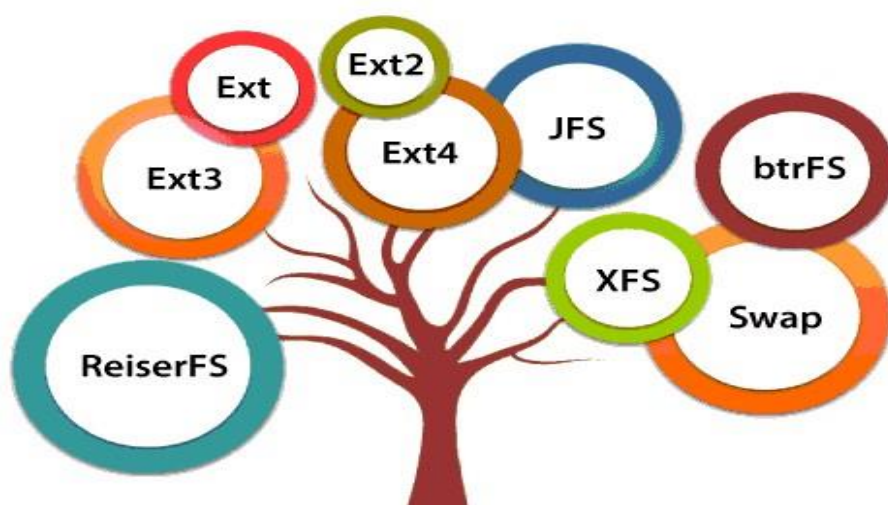
The general-purpose computer system needs to store data systematically so that we can easily access the files in less time. It stores the data on hard disks (HDD) or some equivalent storage type. There may be below reasons for maintaining the file system:

- Primarily the computer saves data to the RAM storage; it may lose the data if it gets turned off. However, there is non-volatile RAM (Flash RAM and SSD) that is available to maintain the data after the power interruption.
- Data storage is preferred on hard drives as compared to standard RAM as RAM costs more than disk space. The hard disks costs are dropping gradually comparatively the RAM.

Linux File System Structure

- Linux file system has a hierarchal file structure as it contains a root directory and its subdirectories. All other directories can be accessed from the root directory. A partition usually has only one file system, but it may have more than one file system.
- A file system is designed in a way so that it can manage and provide space for non-volatile storage data. All file systems required a namespace that is a naming and organizational methodology. The namespace defines the naming process, length of the file name, or a subset of characters that can be used for the file name. It also defines the logical structure of files on a memory segment, such as the use of directories for organizing the specific files. Once a namespace is described, a Metadata description must be defined for that particular file.

Types of Linux File System



Linux File System Features

In Linux, the file system creates a tree structure. All the files are arranged as a tree and its branches. The topmost directory called the root (/) directory. All other directories in Linux can be accessed from the root directory.

Some key features of Linux file system are as following:

- Specifying paths: Linux does not use the backslash (\) to separate the components; it uses forward slash (/) as an alternative. For example, as in Windows, the data may be stored in C:\ My Documents\ Work, whereas, in Linux, it would be stored in /home/ My Document/ Work.
- Partition, Directories, and Drives: Linux does not use drive letters to organize the drive as Windows does. In Linux, we cannot tell whether we are addressing a partition, a network device, or an "ordinary" directory and a Drive.
- Case Sensitivity: Linux file system is case sensitive. It distinguishes between lowercase and uppercase file names. Such as, there is a difference between test.txt and Test.txt in Linux. This rule is also applied for directories and Linux commands.
- File Extensions: In Linux, a file may have the extension '.txt,' but it is not necessary that a file should have a file extension. While working with Shell, it creates some problems for the beginners to differentiate between files and directories. If we use the graphical file manager, it symbolizes the files and folders.
- Hidden files: Linux distinguishes between standard files and hidden files, mostly the configuration files are hidden in Linux OS. Usually, we don't need to access or read the hidden files. The hidden files in Linux are represented by a dot (.) before the file name (e.g., .ignore). To access the files, we need to change the view in the file manager or need to use a specific command in the shell.

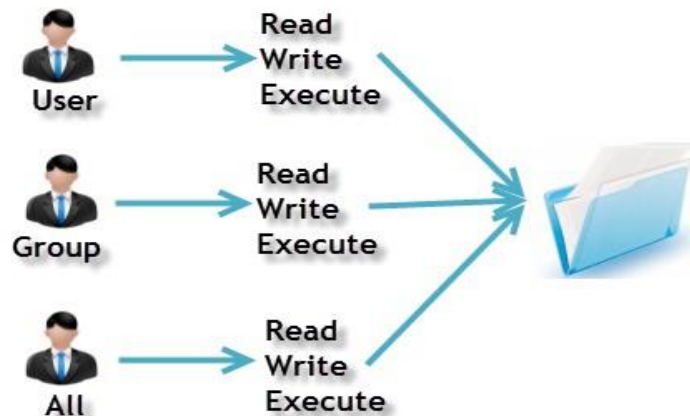
User permission read , write and execute

Every file and directory in your UNIX/Linux system has following 3 permissions defined for all the 3 owners discussed above.

- Read: This permission give you the authority to open and read a file. Read permission on a directory gives you the ability to lists its content.

- **Write:** The write permission gives you the authority to modify the contents of a file. The write permission on a directory gives you the authority to add, remove and rename files stored in the directory. Consider a scenario where you have to write permission on file but do not have write permission on the directory where the file is stored. You will be able to modify the file contents. But you will not be able to rename, move or remove the file from the directory.
- **Execute:** In Windows, an executable program usually has an extension “.exe” and which you can easily run. In Unix/Linux, you cannot run a program unless the execute permission is set. If the execute permission is not set, you might still be able to see/modify the program code(provided read & write permissions are set), but not run it.

Owners assigned Permission On Every File and Directory



File Permissions in Linux/Unix

The table below gives numbers for all for permissions types.

Number	Permission Type	Symbol
0	No Permission	—
1	Execute	-x
2	Write	-w-
3	Execute + Write	-wx
4	Read	r-
5	Read + Execute	r-x
6	Read +Write	rw-
7	Read + Write +Execute	rw-x

Permissions

Every file, directory, and other system objects in Linux are assigned an owner and a group. This is the most basic, yet essential, part of system security that protects users from each other. Owners, users belonging to a group, and all others may be granted different types of access to read from, write to, or execute files. This is generally referred to as *file permissions* in Linux.

To set permissions and manage ownership, we will use the following commands:

- `chmod`: change file permissions
- `chown`: change file owner
- `chgrp`: change group ownership
- `id`: print user and group IDs

Special Permissions

Besides the standard `rwx` file permissions, there are three others that are worth mentioning: `setuid`, `setgid`, and the sticky bit. Let's examine each of them.

- When the `setuid` bit is set on an executable file, any user can execute it using the permissions of the owner of such file.
- When the `setgid` bit is set on an executable file, any user can execute it using the permissions of the group of such file

13.4 Install and remove packages for services

What is the command to install packages in Linux? Debian, Ubuntu, Mint, and other Debian-based distributions all use `.deb` files and the `dpkg` package management system. There are two ways to install apps via this system. You can use the `apt` application to install from a repository, or you can use the `dpkg` app to install apps from

Linux Commands To Update All Packages

1. Debian / Ubuntu / Mint Linux and friends try the [apt-get command/apt command](#).
2. CentOS / RHEL / Red Hat / Fedora Linux and friends try [yum command](#).
3. Suse / OpenSUSE Linux use the `zypper` command. We can also use graphical tool called YaST online update.
4. Slackware Linux user try the `slackpkg` command.
5. Arch Linux user try the `pacman` command.
6. Gentoo Linux user try `emerge` command.
7. Alpine Linux user must use [apk command](#).

Unit 4:- IT security fundamentals

14.1 Appreciate IT security

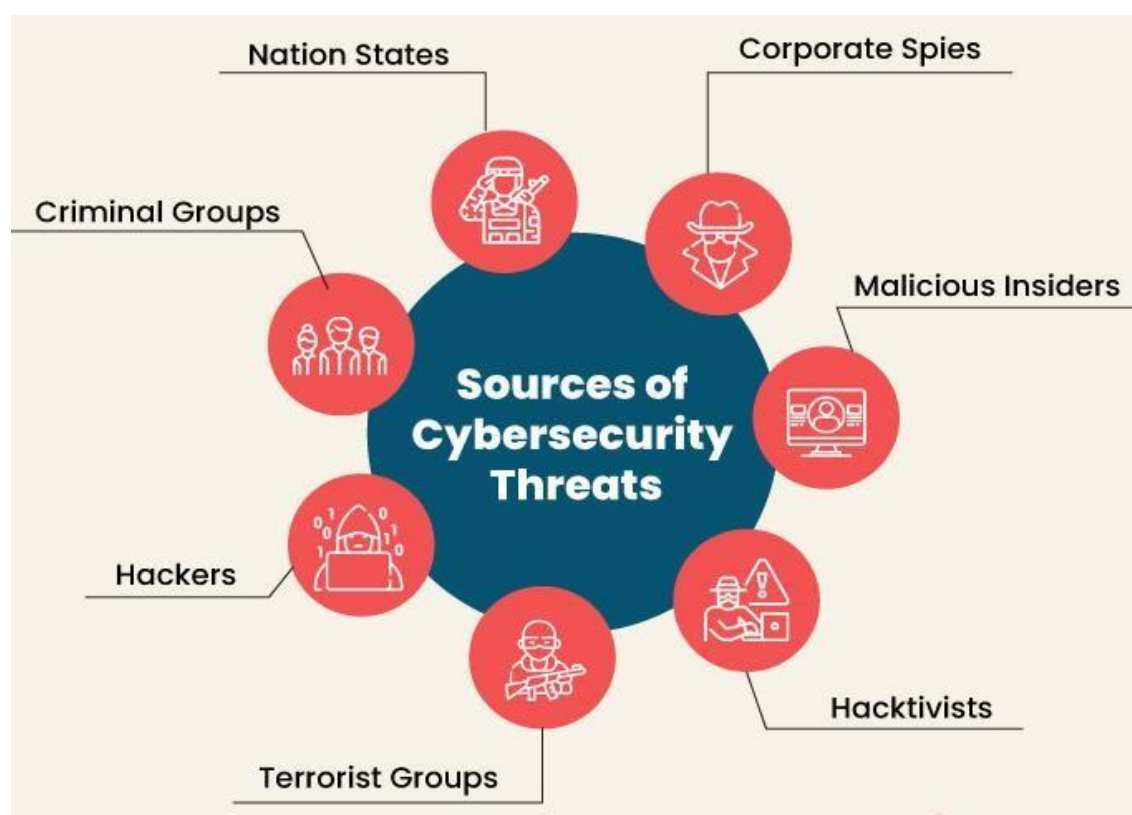
concept of IT security

IT security is a set of cyber security strategies that prevents unauthorized access to organizational assets such as computers, networks, and data. It maintains the integrity and confidentiality of sensitive information, blocking the access of sophisticated hackers.

What is the need for IT security?

As hackers get smarter, the need to protect your digital assets and network devices is even greater. While providing IT security can be expensive, a significant breach costs an organization far more.

Some Types of Data Threads



virus:- A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk.

Malware:- Malware known as malicious software is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behaviour an attacker wants. And because malware comes in so many variants, there are numerous methods to infect computer systems.

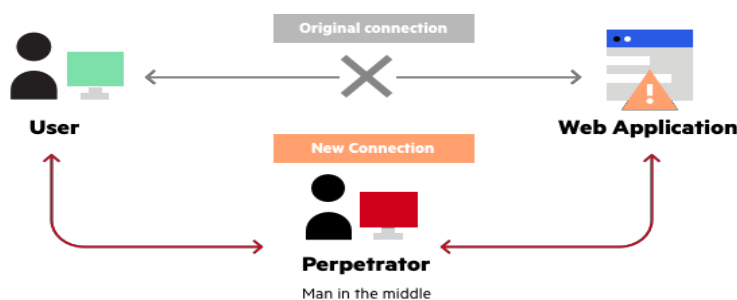
Types of malware



Dos attack:- A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

Phishing attack:- Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

Man in the middle attack:- . A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.



File security and personnel security

File security:- File security is all about safeguarding your business-critical information from prying eyes by implementing stringent access control measures and flawless permission hygiene. Apart from enabling and monitoring security access controls data storage also plays an important role in securing files. Regularly optimize file storage by purging old, stale, and other junk files to focus on business-critical files. Tackle data security threats and storage inefficiencies with periodic reviews and enhancements to your file security strategy.

Personnel security:- Create a Difficult Mobile Passcode – Not Your Birth date or Bank PIN. Install Apps from Trusted Sources. Keep Your Device Updated – Hackers Use Vulnerabilities in Unpatched Older Operating Systems. Avoid sending PII or sensitive information over text message or email.

14.2 Use antivirus software

Anti virus:- Antivirus is a kind of software used to prevent, scan, detect and delete viruses from a computer. Once installed, most antivirus software runs automatically in the background to provide real-time protection against virus attacks.



some example of anti virus

- ☐ Bitdefender Internet Security.
- ☐ Norton Security.
- ☐ McAfee.
- ☐ Comodo Internet Security.
- ☐ Malwarebytes

Anti malware

Antimalware is a type of software program created to protect information technology (IT) systems and individual computers from malicious software, or malware. Antimalware programs scan a computer system to prevent, detect and remove malware.

What is an example of anti-malware?

Types of malware that anti-malware software typically protect systems from include viruses, Trojan horses, worms, spyware and keylogger programs, ransomware, rootkits, bootkits and even adware etc.

Antivirus installation process

To install an antivirus program on your computer, follow the steps below.

1.If you purchased the antivirus program from a retail store, insert the [CD](#) or [DVD](#) into the computer's disc drive. The installation process should start automatically, with a window opening to help guide you through the install process.

2. If you downloaded the antivirus program on the Internet, find the downloaded file on your computer. If the downloaded file is a zip file,
3. In the installation process window, follow the steps provided to install the antivirus program. The install process provides recommended options so the antivirus program will function properly, which in most cases can be accepted as is.
4. When the install process is complete, close out of the install window.
5. If used, remove the CD or DVD from the computer's disc drive.

The antivirus program is now installed and ready to use. While it may not be required, we recommend restarting your computer so that any modified settings in the operating system can take effect correctly.

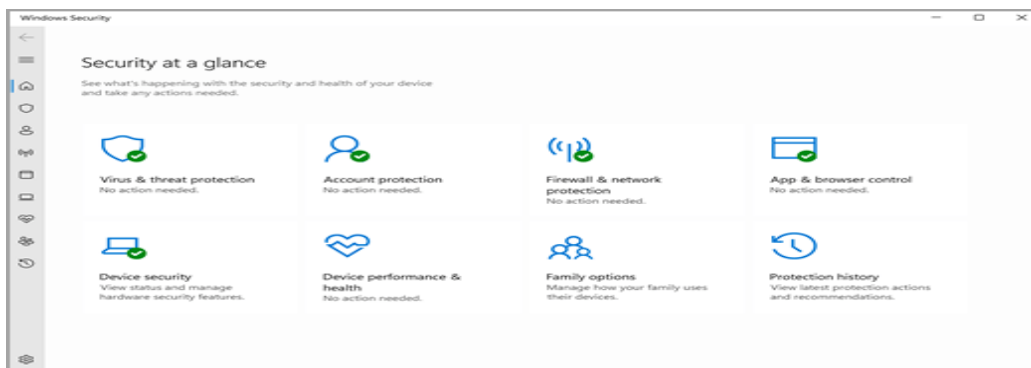
Update the antivirus program after installation

Out of the box, antivirus programs are not up-to-date and are missing the latest virus and spyware definitions. Without the latest definitions, the antivirus program will not know about the most recently created viruses and spyware, making your computer vulnerable to an infection.

After installing the antivirus program, we highly recommend you update it with the latest virus and spyware definitions. The updates allow the antivirus program to protect your computer from all viruses and spyware.

In many cases, the antivirus program automatically checks for and installs the latest updates. If prompted to do so, select Yes to update the antivirus program. If it does not prompt you to update immediately.

setting of antivirus software



1. Virus and threat protection:- Monitor threats to your device, run scans, and get updates to help detect the latest threats. (Some of these options are unavailable if you're running Windows 10 in S mode.)
2. Account protection:- Access sign-in options and account settings, including Windows Hello and dynamic lock.
3. Firewall and network protection:- Manage firewall settings and monitor what's happening with your networks and internet connections.

4. App and browser control:- Update settings for Microsoft Defender SmartScreen to help protect your device against potentially dangerous apps, files, sites, and downloads. You'll have exploit protection and you can customize protection settings for your devices.

5. Device security:- Review built-in security options to help protect your device from attacks by malicious software.

6. Device performance and health:- View status info about your device's performance health, and keep your device clean and up to date with the latest version of Windows.

14.3 Describe vulnerabilities

Port service:-

The process of scanning a computer's port is called port scanning. It provides information on whether a device's ports are open, closed or filtered. It is mainly performed to identify if a port is sending or receiving any information.

Port scanning also involves the sending of data to specific ports and analyzing the responses to identify vulnerabilities.

It is also one of the techniques used by attackers to discover devices/services they can break into.

Ports and Port Numbers

Ports are communication endpoints that connect network devices. Each port is identified with a 16-bit unsigned port number. The various types of port numbers are as follows:

Port Number	Description
1	TCP Port Service Multiplexer (TCPMUX)
5	Remote Job Entry (RJE)
7	ECHO
18	Message Send Protocol (MSP)
20	FTP — Data
21	FTP — Control
22	SSH Remote Login Protocol

14.4 Describe security procedures

security policy

An information security policy (ISP) sets forth rules and processes for workforce members, creating a standard around the acceptable use of the organization's information technology, including networks and applications to protect data confidentiality, integrity, and availability.

When writing your ISP, you want to consider the following:

- How to control access to information
- How to prevent “snooping”
- How to prevent a data breach
- How to prevent data leakage

securing the network

Network Security involves access control, virus and antivirus software, application security, network analytics, types of network-related security (endpoint, web, wireless), firewalls, VPN encryption and more.

5 steps to secure networking

1. Use a layered defence.
2. Incorporate people and processes in the network security planning.
3. Clearly define security tools and network zones.
4. Maintain the integrity of network.
5. Control device network admission through endpoint compliance.

OS updates

Operating system updates contain new software that helps keep your computer current. Examples of updates include service packs, version upgrades, security updates, drivers, or other types of updates. Important and high-priority updates are critical to the security and reliability of your computer

It's important to install new security updates as soon as they become available.

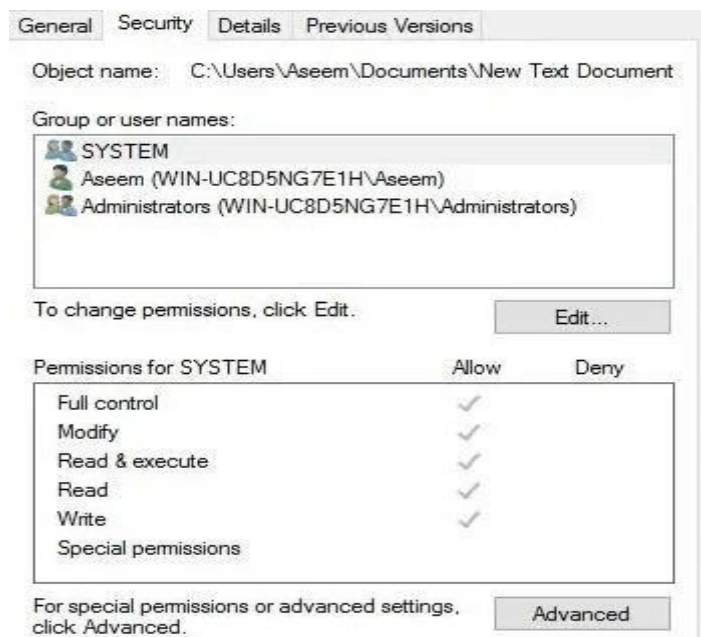
The easiest way to do this is to turn on automating and use the recommended setting, which downloads recommended updates and installs them on a schedule you set.

In Windows Vista, you control the automatic updating settings through the Windows Update Control Panel. For more information, Turn automating updating ON or OFF.

14.5 Protected data

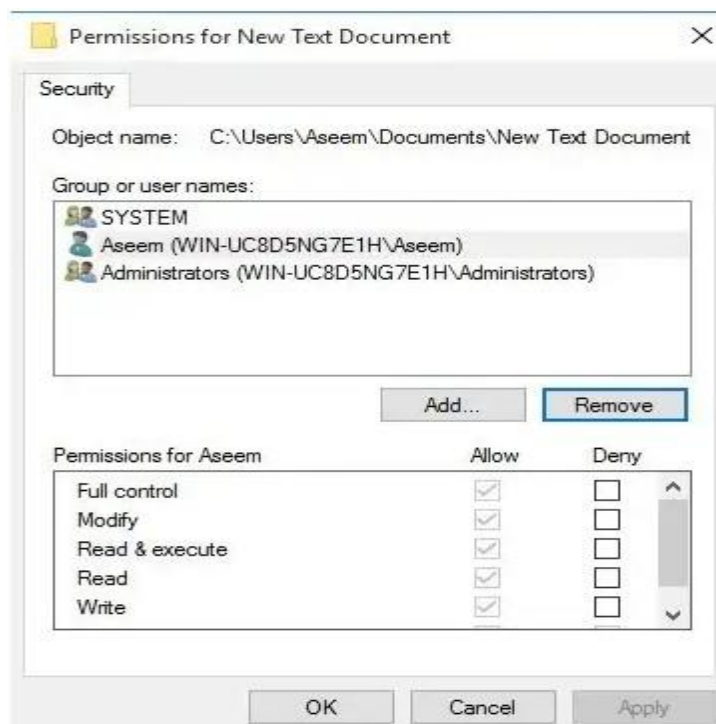
File and folder permission

Now that we got all of that out of the way, let's talk about permissions in Windows. Every file and every folder in Windows has its own set of permissions. Permissions can be broken down into Access Control Lists with users and their corresponding rights. Here is an example with the user list at the top and the rights at the bottom:



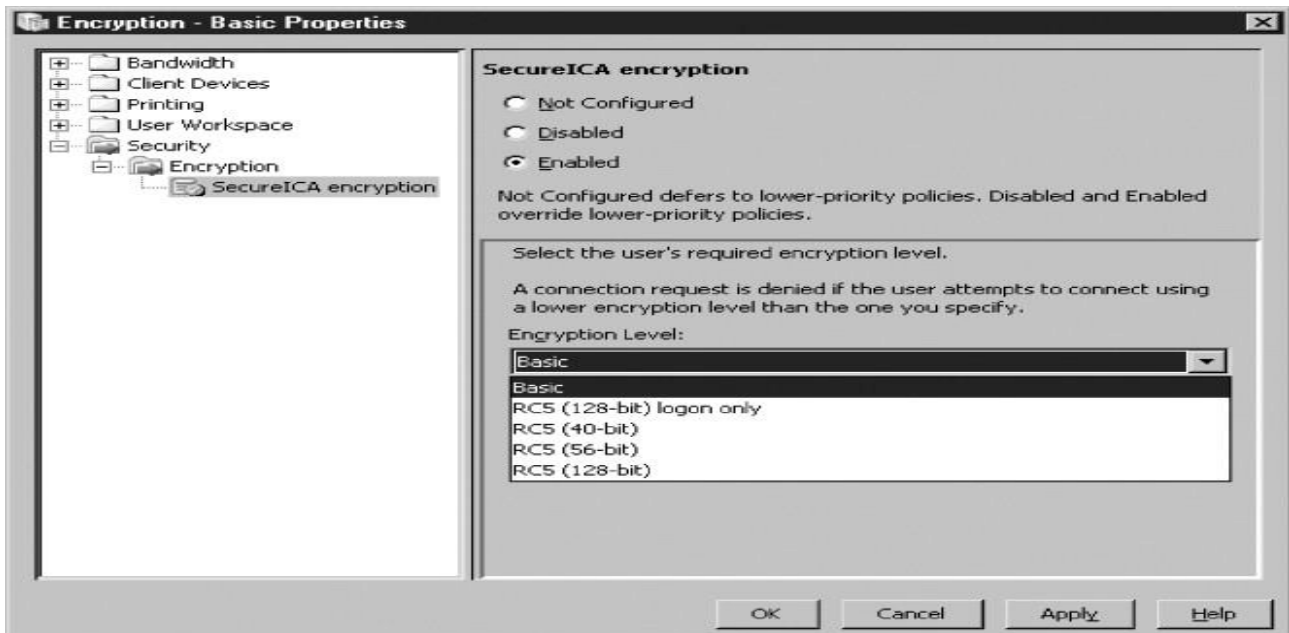
Permissions are also either inherited or not. Normally in Windows, every file or folder gets their permissions from the parent folder. This hierarchy keeps going all the way up to the root of the hard drive. The simplest permissions have at least three users: SYSTEM, currently logged in user account and the Administrators group.

These permissions usually come from the C:\Users\Username folder on your hard drive. You can access these permissions by right-clicking on a file or folder, choosing Properties and then clicking on the Security tab. To edit permissions for a particular user, click on that user and then click the Edit button.



Encryption and group policy

Encryption policies define when encryption should or shouldn't be used and the encryption technologies or algorithms that are acceptable. For example, a policy might mandate that specific proven algorithms such as 3DES, RSA, or IDEA be used and prohibit use of proprietary or nonstandard algorithms.



Group Policy is a hierarchical infrastructure that allows a network administrator in charge of Microsoft's Active Directory to implement specific configurations for users and computers. Group Policy is primarily a security tool, and can be used to apply security settings to users and computer.



14.6 Appreciate the use of firewalls

Windows Firewall is a application that filters information coming to your system from the Internet and blocking potentially harmful programs. The software blocks most programs from communicating through the. Users simply add a program to the list of allowed programs to allow it to communicate through the firewall. When using a public, Windows Firewall can also secure the system by blocking all unsolicited attempts to connect to your computer.

What does Windows Firewall do?

Known as Internet connection firewall (ICF) before the introduction of Windows XP Service Pack 2 in 2004, Windows Firewall is Windows' built-in security feature that guards against unauthorized traffic on a user's. It helps protect a user's computer from intrusions and harmful attacks by controlling incoming and outgoing network.

The native acts as a barrier between the user's computer and, monitoring all inbound and outbound connections that travel across users' network connections. This protects users against, and other malicious software. A firewall can also be used to regulate or restrict access to certain internet services, such as online games or peer-to-peer file-sharing networks.

In addition to being integrated into Microsoft Windows XP Service Pack 2, previous versions of Microsoft operating systems also had Firewall installed by default.

Software Firewalls

Software firewalls are installed separately on individual devices. They provide more granular control to allow access to one application or feature while blocking others. But they can be expensive in terms of resources since they utilize the CPU and RAM of the devices they are installed on, and administrators must configure and manage them individually for each device. Additionally, all devices within an intranet may not be compatible with a single software firewall, and several different firewalls may be required.

Hardware Firewalls

On the other hand, hardware firewalls are physical devices, each with its computing resources. They act as gateways between internal networks and the internet, keeping data packets and traffic requests from untrusted sources outside the private network. Physical firewalls are convenient for organizations with many devices on the same network. While they block malicious traffic well before it reaches any endpoints, they do not provide security against insider attacks. Therefore, a combination of software and hardware firewalls can provide optimal protection to your organization's network.

Software and Hardware Firewalls

- Software Firewalls. Software firewalls are installed separately on individual devices.
- Hardware Firewalls.
- Packet Filtering Firewalls.
- Circuit-Level Gateways.
- State full Inspection Firewalls.
- Application-Level Gateways (Proxy Firewalls)

Packet Filtering Firewalls

Packet filtering firewalls are the oldest, most basic type of firewalls. Operating at the network layer, they check a data packet for its source IP and destination IP, the protocol, source port, and destination port against predefined rules to determine whether to pass or discard the packet. Packet filtering firewalls are essentially stateless, monitoring each packet independently without any track of the established connection or the packets that have passed through that connection previously. This makes these firewalls very limited in their capacity to protect against advanced threats and attacks.

Packet filtering firewalls are fast, cheap, and effective. But the security they provide is very basic. Since these firewalls cannot examine the content of the data packets, they are incapable of protecting against malicious data packets coming from trusted source IPs. Being stateless, they are also vulnerable to source routing attacks and tiny fragment attacks. But despite their minimal functionality, packet filtering firewalls paved the way for modern firewalls that offer stronger and deeper security.

Stateful Inspection Firewalls

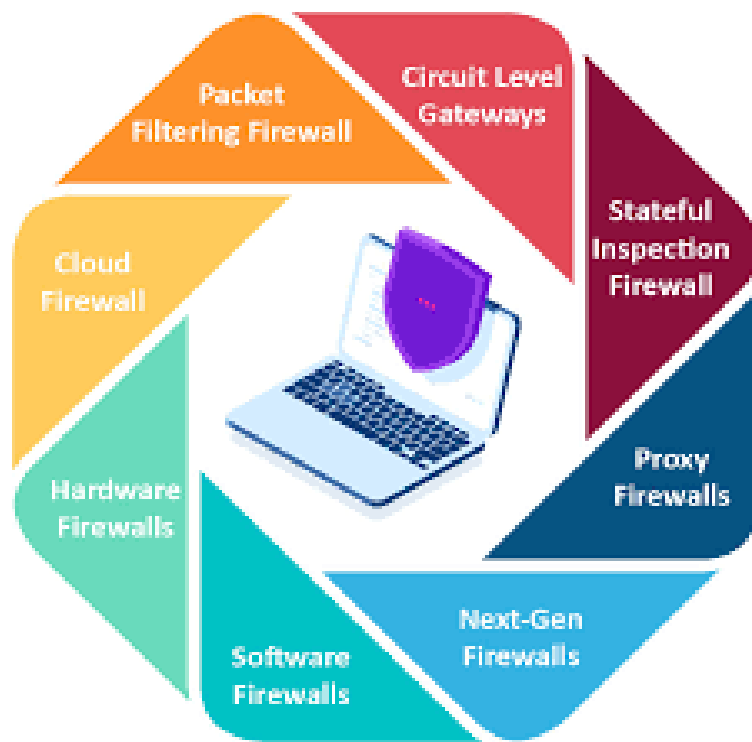
A step ahead of circuit-level gateways, stateful inspection firewalls, and verifying and keeping track of established connections also perform packet inspection to provide better, more comprehensive security. They work by creating a state table with source IP, destination IP, source port, and destination port once a connection is established. They create their own rules dynamically to allow expected incoming network traffic instead of relying on a hardcoded set of rules based on this information. They conveniently drop data packets that do not belong to a verified active connection.

Stateful inspection firewalls check for legitimate connections and source and destination IPs to determine which data packets can pass through. Although these extra checks provide advanced security, they consume a lot of system resources and can slow down traffic considerably. Hence, they are prone to DDoS (distributed denial-of-service attacks).

Application-Level Gateways (Proxy Firewalls)

Application-level gateways, also known as proxy firewalls, are implemented at the application layer via a proxy device. Instead of an outsider accessing your internal network directly, the connection is established through the proxy firewall. The external client sends a request to the proxy firewall. After verifying the authenticity of the request, the proxy firewall forwards it to one of the internal devices or servers on the client's behalf. Alternatively, an internal device may request access to a webpage, and the proxy device will forward the request while hiding the identity and location of the internal devices and network.

Unlike packet filtering firewalls, proxy firewalls perform stateful and deep packet inspection to analyze the context and content of data packets against a set of user-defined rules. Based on the outcome, they either permit or discard a packet. They protect the identity and location of your sensitive resources by preventing a direct connection between internal systems and external networks. However, configuring them to achieve optimal network protection can be tricky. You must also keep in mind the tradeoff—a proxy firewall is essentially an extra barrier between the host and the client, causing considerable slowdowns.



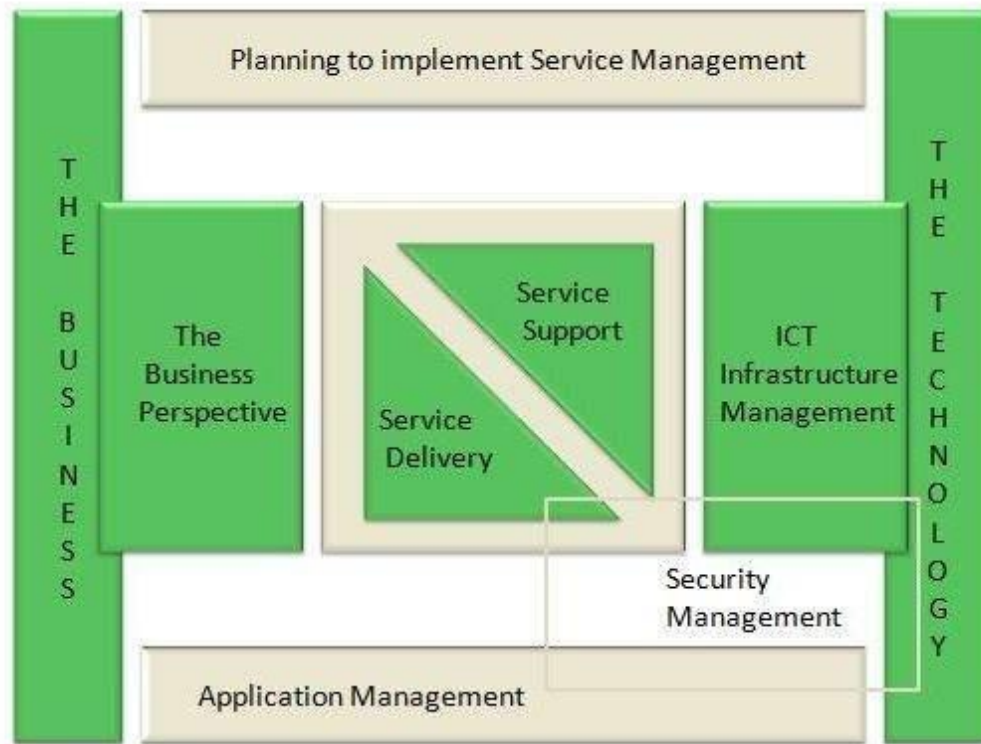
Describe the structure of the ITIL service lifecycle

. In the best practices of, services lifecycles are defined to describe the process of how services are initiated and maintained. Without these ITIL lifecycles, services can not be implemented and managed with optimal efficiency and efficacy. It is important to adhere to the principles of the ITIL lifecycles for IT services to run smoothly. The ITIL lifecycle for services is designed into five stages. These stages are interlinked. The reason behind this is to ensure that the end-goal is always kept in mind during all the stages of the ITIL lifecycle for services. This interlinked system is designed to enable consistent IT services.

Unit 5: Basics of ITIL v3

ITIL is a framework providing best practice guidelines on all aspects of end to end service management. It covers complete spectrum of people, processes, products and use of partners.

Now a day's ITIL is being practiced by almost every company providing IT services to the customers.



ITIL Framework

The processes, tasks and checklists described in ITIL are not organization-specific, but can be implemented by any organization. It gives organization a framework to plan, implement and measure IT services.

ITIL was published in 1989 by Her Majesty's Stationery Office (HMSO) in UK on behalf of the Central Communications and Telecommunications Agency (CCTA), now subsumed within the Office of Government Commerce (OGC).

Requirement of ITIL

ITIL helps business managers and IT managers to deliver services to the customers in effective manner and hence gaining the customer's confidence and satisfaction. Here are the areas where ITIL plays an effective role –

- IT and business strategic planning
- Integrating and aligning IT and business goals
- Implementing continuous improvement
- Acquiring and retaining the right resources and skill sets
- Reducing costs and the Total Cost of Ownership

- Demonstrating the business value to IT
- Achieving and demonstrating Value for Money and Return on Investment.
- Measuring IT organization effectiveness and efficiency
- Developing business and IT partnerships and relationships
- Improving project delivery success
- Managing constant business and IT change

ITIL Versions

ITIL was originated as collection of books. These books of ITIL cover all aspects of IT service management. Since its origin, it has undergone many changes which lead to the following versions of ITIL –

- ITIL V1 was the initial version of ITIL consisting of 31 books
- From 2000 to 2004, ITIL V1 was revised and replaced by 7 books (ITIL V2). This version became globally accepted and is now used in many countries by thousands of organizations
- In 2007, ITIL v2 was modified and consolidated with 3rd version of ITIL, consisting of five core books covering the service lifecycle. ITIL V3 included 26 processes and 4 functions
- In 2011, the 2011 edition of V3 was published. It was an updated version released in 2007.

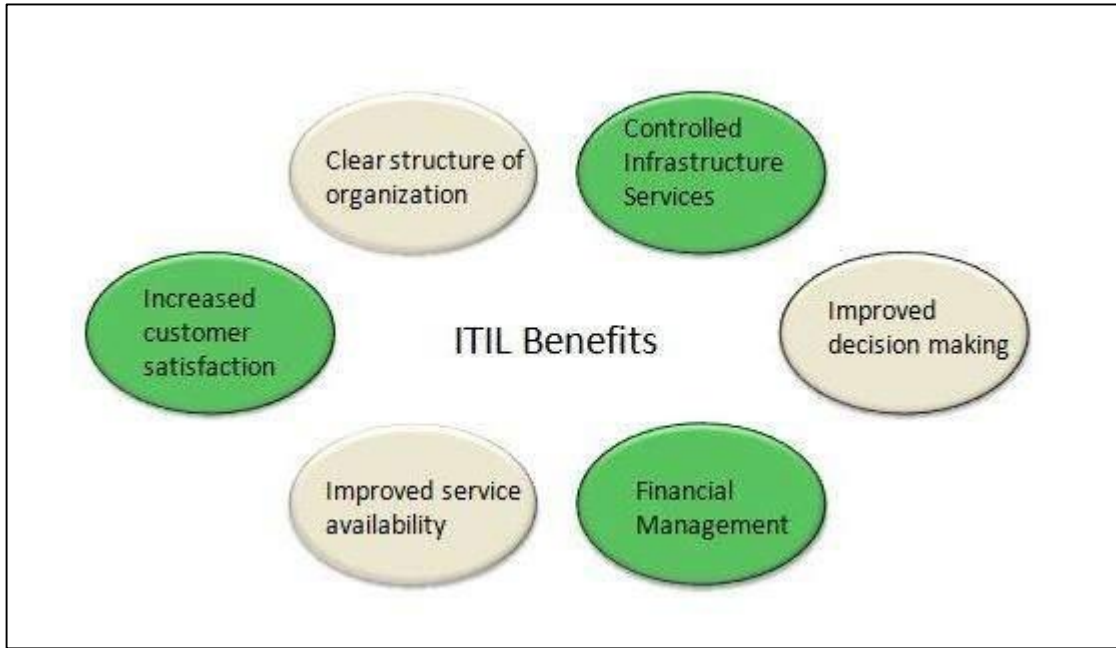
ITIL Publications

ITIL core publications include a set of five manuals –Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Management.



Benefits of ITIL

Following diagram shows several benefits of ITIL –



ITIL V2 vs ITIL V3

ITIL V2	ITIL V3
Focused on product, process and people.	Focused on product, process, people and partner.
Process oriented approach	Lifecycle based approach.
Security management is part of evaluation	Security management is a separate process
Emphasizes on service design and service strategy	Equal attention to all processes
Have 10 processes and 2 functions	Have 26 processes and 4 functions.

2. Describe the concepts of Service

2.1. Internal Customer

Internal customer is a division, individual or unit employee who purchases or is the receiver of products, materials, services or information from other units in the same company (internal supplier). This is practiced by a number of companies in order to train the workers on how to deal and treat external customers effectively. In this way, they are consciously aware of how they work and they help in the enhancement of the quality.

2.2. External Customer

External customers are customers who don't belong to the organization. In different terms, they are purchasers of the products' (service) of that business but in no way affiliated with the company. These may also pertain to customers who purchase or rent products that are not of the same company, but they are affiliated in the same industry. Those who drop by and check the products are still considered one.



2.3. Difference between Internal and External Customers

Internal customers are people who are connected with the company. They are purchasing the products right from inside the business while external customers are in no way affiliated with the company. Internal customers know the sellers pretty well so they know how to make bargains and get it at a reasonable price while external customers are not personally familiar with the sellers, it would be hard for some to get them at nice prices. Internal customers, even if they don't get to bargain the products, can avail of bigger discounts unlike the external customers who get the usual price.

Internal and external customers always want to get good products when buying something. No matter what their position in the company is, clients treat them the same way and still maintain good customer service.

3. IT service management

IT service management -- often referred to as ITSM -- is simply how IT teams manage the end-to-end delivery of IT services to customers. This includes all the processes and activities to design, create, deliver, and support IT services.

The core concept of ITSM is the belief that IT should be delivered as a service. A typical ITSM scenario could involve asking for new hardware like a laptop. You would submit your request through a portal, filling out a ticket with all relevant information, and kicking off a repeatable workflow. Then, the ticket would land in the IT team's queue, where incoming requests are sorted and addressed according to importance.

Due to their day-to-day interactions with IT, people often misconstrue ITSM as basic IT support. On the contrary, ITSM teams oversee all kinds of workplace technology, ranging from laptops, to servers, to business-critical software applications.

There is a common line of thinking in the IT industry that posits that a proper approach to ITSM should follow three steps in this order: 1) Build and implement IT technology. 2) Bring in and enforce the right process. 3) People can learn the technology and abide by the process. Atlassian flips that paradigm.

3.1. The importance of ITSM

ITSM benefits your IT team, and service management principles can improve your entire organization. ITSM leads to efficiency and productivity gains. A structured approach to service management also brings IT into alignment with business goals, standardizing the delivery of services based on budgets, resources, and results. It reduces costs and risks, and ultimately improves the customer experience.

We've found some of the most common benefits of ITSM to include:

- Aligning IT teams with business priorities tracked through success metrics
- Enabling cross-department collaboration
- Bringing IT teams and development teams together through streamlined project management approaches
- Empowering IT teams to share knowledge and continuously improve
- Improving request coordination for more efficient service
- Promoting customer-centricity with self-service and better processes
- Responding more quickly to major incidents, and preventing future ones

All of which decrease costs and lead to better service.

3.2. Stakeholders in service

management

IT services (and, consequently, ITSM) deal with stakeholders in almost every process and throughout the ITSM organization. Stakeholders of an IT service are employees of the ITSM organization and the organization's management, other employees of the company, management of the company, users and customers, vendors, suppliers, regulators, partners, etc. They all have interest in IT services.

Stakeholders can be divided into two categories:

Internal – these are teams, groups, and employees who work in the same organization. In case of internal IT providers, this also means internal customers.

External – these are all parties who are not part of the same organization: typically, external customers or suppliers.

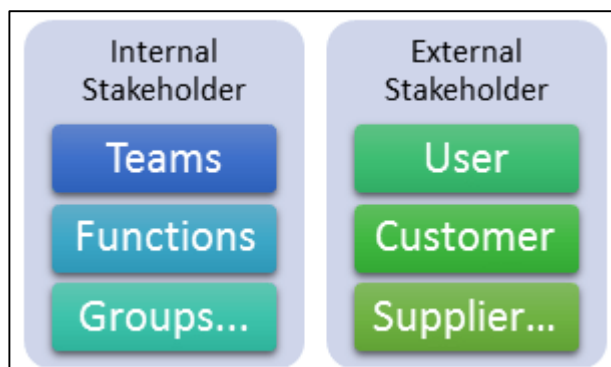


Figure: Internal and external stakeholders

5. Problem management

A problem is the cause or potential cause of multiple incidents. Problems can arise from major incidents affecting many users, or from recurring incidents. Further, problems can be identified in infrastructure diagnostic systems before users are affected.

Incidents hinder business productivity, and providing quick solutions helps ensure seamless continuity of business operations. However, when multiple incidents occur at once or the same incident occurs multiple times, it's not feasible to move forward by providing patchwork solutions, or offering the same resolutions over and over again.

ITIL® problem management is a procedural way to ensure minimal incidents emerge from IT infrastructure operations by delving deep into incidents to find the root causes and fixes, and also reduce the severity of the incidents through suitable documentation of existing issues and providing workarounds.

Problem management is a methodical approach to identify the cause of an incident and manage the life cycle of all problems. The goal of ITIL® problem management process is to minimize the impact of incidents and eliminate recurring ones. While ITIL® doesn't state any specific technique to perform problem management, it recommends three phases to follow:



Problem identification



Problem control



Error control

These phases will be discussed in detail later in the guide.

Reactive management deals with incidents that are currently affecting users, whereas proactive problem management addresses issues that could potentially surface as incidents in the future should they be left alone.

A sound problem management process has the potential to significantly reduce the influx of incident tickets, saving IT service desk staff significant time and effort. This advantage ripples into other benefits such as reduction in mean time to repair (MTTR), higher customer satisfaction, a robust known error database, and reduced cost of IT services and issues. Moreover, an organization that practices proactive problem management is likely to find tremendous value from identifying and eliminating issues before they disrupt business processes.

Problem management as an ITIL® practice is most useful when used with other ITIL® practices in the overall service value chain. Information is exchanged between the various ITIL® practices, namely incident management, change management, IT asset management, knowledge management, and continual service improvement. This information exchanged between parties accumulates value as it moves through each ITIL® practice, in turn building an ideal IT service management process.

Before going further, the following definitions will be useful in understanding the context of this guide.

- **Workaround:** Temporary solutions that restore services and ensure business continuity. A workaround reduces the impact of an incident or problem.
- **Root cause analysis (RCA):** The root cause is the problem's underlying issue. RCA is the investigation techniques that help discover the root cause of a problem.
- **Known error:** Problems that have occurred before and have a workaround or known root causes.
- **Known error database (KEDB):** A database created by documenting the known errors using incident management and problem management.

In this guide, we'll examine each facet of problem management in detail, providing all the knowledge you need to get up to speed on how to implement problem management in your enterprise.

Benefits of IT problem management:

There are a few hurdles organizations might encounter in the process of establishing problem management. The organization might not have the resources to allocate for a problem management team, or it may already have an unorthodox way of managing problems and is reluctant to change. Sometimes, it could just be a cost-related denial of request.

Consequently, it's vital to include all stakeholders in the problem management process, and



express how it provides value to different facets of the organization. These benefits include:

- Eliminates the faults in an organization's services through suitable documentation.
- Refines the service design by identifying and solving weak points, ensuring the most effective and efficient path for service delivery.
- Increases the first time fix rate on service failures by providing permanent solutions to incidents rather than stopping at workarounds.
- Diminishes the impact of incidents affecting multiple users, or a single user at a crucial time.
- Prevents most of the incidents and problems plaguing an organization over time, boosting user productivity.
- Strengthens the confidence users have in the organization's IT services.
- Decreases the time it takes to recover from failures through systematic maintenance of a KEDB.
- Prevents recurring incidents through one-time fixes, sparing valuable service desk efforts in resolving them.

- Encourages IT services to mature as the organization develops by the learning from the resolved problems.
 - Develops IT talent within the organization through technical awareness and valuable insights.
-