Module 3) N+ Network Configuration

TOPIC: Local Area Networking

1. **What is Network?**
   - A network is a group of interconnected devices or computers that can communicate with each other. It can be used to share resources, such as files or printers, or to communicate and collaborate with other people remotely.

   - There are many types of network like LAN, MAN, WAN, PAN.

2. **What is internet & intranet?**
   - Internet :->
     The Internet is a global network of interconnected computer networks that communicate with each other using standardized communication protocols. It is a vast network that allows computers and devices to exchange information and data over long distances, allowing people to connect and communicate with each other from anywhere in the world.

   - Intranet :->
     An intranet is a private network accessible only to authorized users within a specific organization or company. It is similar to the Internet and allows users to access various online services, but only to members of the organization and not to the general public.

Module 3) N+ Network Configuration

1. **How many types of network we used?**
   - There are several types of network that are commonly used:
     - ♦ Local Area Network (LAN): This is a network that covers a small geographic area, such as an office, building, or campus. LANs are often used to connect computers, printers, and other devices so they can share resources and communicate with each other.
       EX: - school/college computer Lab, campus,
     - ♦ Metropolitan Area Network (MAN): This is a network that covers a metropolitan area, such as a large city or urban region.
     - ♦ Wide Area Network (WAN): This is a network that covers a large geographical area, such as a city, state, or country. WANs are used to connect LANs together and also provide connectivity to the Internet.
       EX: - cable TV

2. **Difference between LAN & PAN?**

LAN (Local Area Network)	PAN (Personal Area Network)
LAN cover area up to 10km radius	PAN cover area up to 10m radius
It's mostly used in office and houses	It's mostly used in building and campus
For communication channel use coaxial, STP, UTP, fiber optical.	For communication channel use Intra red waves
It's costlier than PAN	It's cheaper than LAN
LAN is less secure	PAN is secure than LAN

Module 3) N+ Network Configuration

1. **Explain LAN?**
   - LAN stands for Local Area Network, which is a computer network that covers a small geographic area such as a building, office, or campus. It allows devices such as computers, printers, and servers to communicate with each other and share resources such as files, applications, and Internet access.

     Can establish a LAN using a variety of technologies including Ethernet, Wi-Fi and Token Ring. Ethernet, the most popular technology in local area networks, uses wired connections to transfer data between devices. Wi-Fi, on the other hand, uses wireless signals to connect devices to the network.

     Typically owned and managed by a single organization, a LAN offers high data transfer rates and low latency, making it ideal for sharing resources and collaborating among users. It is also more secure than a Wide Area Network (WAN) because it is only accessible to authorized users within the network.

     In general, local area networks are an essential part of modern computer networks, allowing companies and organizations to increase productivity, reduce costs and improve communication between employees.

2. **What are different types of LAN devices?**
   - There are several types of LAN devices that are used to establish and manage local area networks. Here are some of the most common LAN devices:
   - Switch: A switch is the most common LAN device and is used to connect devices on the network. They forward packets between devices based on their MAC add resses, improving network performance and reducing collisions.
   - Router: A router is used to connect multiple LANs or WANs together and provide communication between them. They also allow multiple devices to share a single internet connection.

Module 3) N+ Network Configuration

- Hubs: Hubs are used to connect devices in a network, but they don't filter or forward data like switches and routers do. They are not commonly used in modern LANs because they cause network congestion.

- Network Interface Card (NIC): A network card is used to connect a device to a local area network by providing a physical connection such as Ethernet or Wi-Fi. They are usually built into desktop and laptop computers, but can also be added as expansion cards.

- Access point: An access point is used to extend the range of a wireless LAN. They provide wireless connectivity to devices that do not have built-in wireless capabilities.

- Repeater: Repeaters are used to extend the range of a wired LAN by amplifying the signal and retransmitting it. They are used to overcome signal loss due to distance or interference.

- These are the most common types of LAN devices. Each device plays a vital role in establishing and managing a LAN, and they are essential for ensuring efficient communication and resource sharing among network devices.

Module 3) N+ Network Configuration

Topic: configured Network

1. **What is configured network?**
   - Configuring a network involves creating the rules and protocols that devices on the network will use to communicate. This includes setting up access controls and security measures to prevent unauthorized access or data leakage.

2. **How do we configure network?**
   - Configuring a network involves several steps to set up and customize the network to meet the specific needs of an organization or individual. Here are some general steps for setting up your network:

   - Identify network requirements: Identify network requirements, including the number of devices to be connected to the network, the type of data to be transferred, and the need security.

   - Select Network Devices: Select required network devices such as routers, switches, modems and firewalls. Make sure the device is operational and meets the network requirements.

   - Connect the device: Connect the device to the network device using an appropriate cable such as an Ethernet or fiber optic cable.

   - Configure network settings: Configure network settings, including IP address, subnet mask, and default gateway. You will also need to set up a DNS server and a DHCP server.

   - Establish security measures: Establish security measures to protect the network from unauthorized access, such as installing a firewall, using secure passwords, and securing access.

   - Test the network: Test the network to ensure that all devices can communicate with each other and that data is transferred correctly.

Module 3) N+ Network Configuration

- Monitor and manage the network: Monitor the network regularly to ensure that it is working properly and to identify and resolve problems. Regular maintenance such as software and firmware updates can also help prevent future problems.

- Network configurations may different depending on the size and complexity of the network and the needs and needs of the organization or the individual configuration of the network.

1. **How to check the ip address?**
   - Press win + r button for open run shell
   - Enter command " ncpa.cpl " and click on ok
   - Now open a network connections in control panel
   - Right click on your connected interface and click on status
   - Now showing a status page
   - Click on Details so you show a network connections status
   - And find your ip address

2. **How to check the ip address through cmd?**
   - Firstly open a command prompt as a administrator
   - Enter a command " ipconfig " and press enter
   - Now you can show your ip address

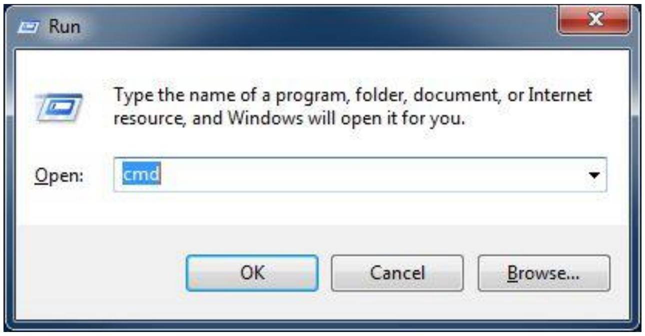
3. **How can we enter static address in network adapter?**
   - Open the Control Panel on your computer.
   - Click on Network and Sharing Center.
   - Click on Change adapter settings.
   - Right-click on the network adapter you want to configure and select Properties.
   - Select Internet Protocol Version 4 (TCP/IPv4) and click on Properties.
   - Select the option "Use the following IP address".

Module 3) N+ Network Configuration

- Enter the IP address, subnet mask, default gateway, and preferred and alternate DNS server addresses in the respective fields.
- Click OK to save the changes.

1. **Do a practical to renew the lease of the ip address.**

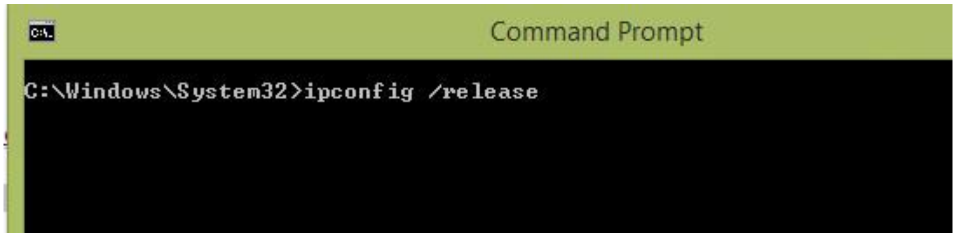
- First step:



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

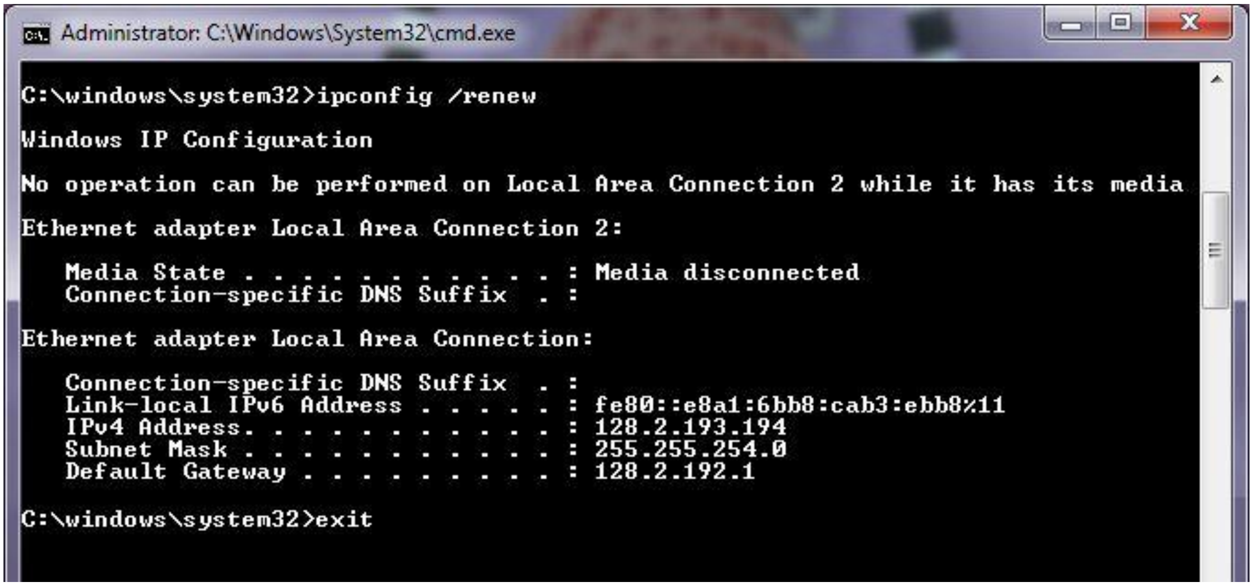
Open: cmd

- Second step:



```
C:\Windows\System32>ipconfig /release
```

- Third step :

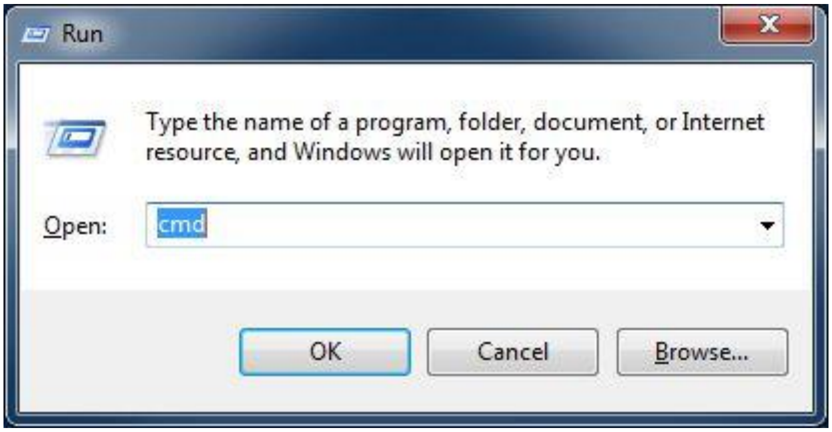


```
C:\windows\system32>ipconfig /renew

Windows IP Configuration

No operation can be performed on Local Area Connection 2 while it has its media

Ethernet adapter Local Area Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e8a1:6bb8:cab3:ebb8%11
   IPv4 Address. . . . . . . . . . . : 128.2.193.194
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 128.2.192.1

C:\windows\system32>exit
```

Module 3) N+ Network Configuration

2. **Do a practical to check the connectivity to the google.**

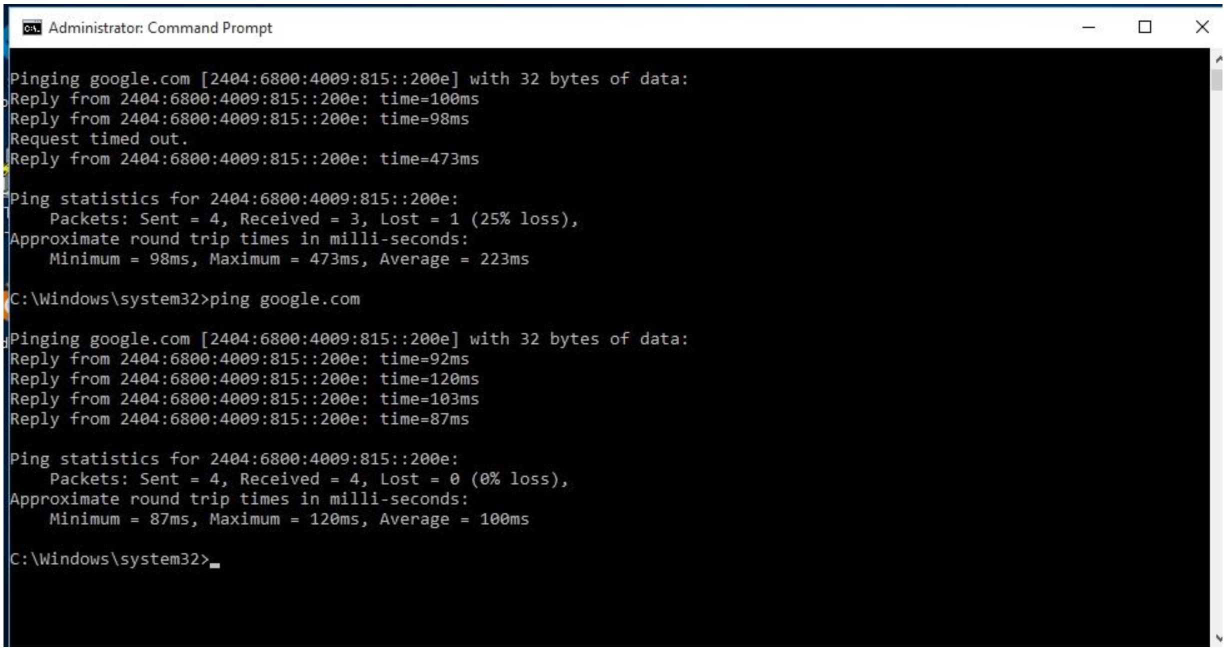
   - First Step:



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

   - Second Step:



```
Pinging google.com [2404:6800:4009:815::200e] with 32 bytes of data:
Reply from 2404:6800:4009:815::200e: time=100ms
Reply from 2404:6800:4009:815::200e: time=98ms
Request timed out.
Reply from 2404:6800:4009:815::200e: time=473ms

Ping statistics for 2404:6800:4009:815::200e:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 98ms, Maximum = 473ms, Average = 223ms

C:\Windows\system32>ping google.com

Pinging google.com [2404:6800:4009:815::200e] with 32 bytes of data:
Reply from 2404:6800:4009:815::200e: time=92ms
Reply from 2404:6800:4009:815::200e: time=120ms
Reply from 2404:6800:4009:815::200e: time=103ms
Reply from 2404:6800:4009:815::200e: time=87ms

Ping statistics for 2404:6800:4009:815::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 87ms, Maximum = 120ms, Average = 100ms

C:\Windows\system32>
```

Module 3) N+ Network Configuration

Topic: Wireless networking

1. **What is the difference between WEP and WPA?**
    - WEP is an older and less secure wireless security protocol that uses weak encryption algorithms, while WPA is a newer and more secure protocol that uses stronger encryption and supports authentication protocols to provide better protection against attacks.

2. **What is Wireless Network?**
    - A wireless network is a computer system that uses wireless data connections to connect devices without physical connections such as cables. Wi-Fi, the most common type of wireless network, allows mobility and easy access to the Internet or network services**.**

1. **What is a wireless network connection?**
    - Wi-Fi is a computer network that uses wireless data connection to communicate between devices without the need for physical connection such as cables.
    - This connection allows devices such as computers, smartphones and tablets To connection allows devices such as computers, smartphones, and tablets to connect to the internet or connect via Wi-Fi or other wireless technologies.
    - A wireless network connection is created by a wireless access point or router that uses radio waves to transfer data between devices.
    - This type of connection is useful as it allows mobility and easy access to network resources without being dependent on a physical connection.

2. **What are the basic concepts of networking?**
    - A network includes the exchange of information or data between various devices or systems. Basic communication concepts include:

    - Protocol: A protocol is a set of rules that govern communication between devices. Some network connections include TCP/IP, HTTP, FTP, and SMTP .

Module 3) N+ Network Configuration

- **IP Address**: An IP address is a unique identifier assigned to each device on the network. It allows devices to communicate with each other in a network Network Topology: Network topology refers to the physical arrangement or arrangement of devices in a network. Common network connections include bus, star, mesh, and ring.

- **Bandwidth:** Bandwidth is the maximum amount of data that can be sent over a network at one time. It is measured in bits per second (bps) or bytes per second (Bps).

- **Cyber Security**: Cybersecurity deals with protecting networks from unauthorized access, hacking and other threats.
  This includes the use of firewalls, antivirus software and security measures.

- **Network equipment**: Network equipment includes routers, switches, hubs, and repeaters. These devices are used to interconnect devices in the network and control the data flow between them.

- **Network Types**: Networks can be of many types, including local area networks (LANs), wide area networks (WANs), and metropolitan areas (MANs).

1. What do you need to know about networking?

- Communication refers to communication between two or more devices, usually via a phone or wireless connection, to exchange information or resources. Here are some important terms and concepts to know when it comes to communication:

- Network Topology: This refers to the physical or logical structure of devices and connections made for the network. Common topologies include bus, star, ring, and mesh.

- Network Protocols: These are the processes and standards that control how devices communicate on a network. Examples of network protocols are TCP/IP, HTTP, FTP, and SMTP.
  Network devices: Hardware devices that facilitate network communication, such as routers, switches, hubs, and modems.

- Network Security: This refers to measures to protect networks and their data from unauthorized access, theft or damage. Examples of network security measures include firewalls, intrusion detection and protection systems, and encryption.

- Network Management: This includes the administration and maintenance of networks, including tasks such as performance monitoring, troubleshooting, and implementing changes or changes.

- Wireless Network: This means that devices are connected to a network using wireless technology such as Wi-Fi or Bluetooth.
  Cloud networking: This includes the use of cloud-based services and resources to support networking and infrastructure.

- Understanding these concepts and techniques is critical to designing, implementing and maintaining effective network solutions.

2. How do you explain computer networking?

- Computer networking is the practice of connecting multiple devices (such as computers, printers, and servers) together to form a network that allows them to share resources and exchange information. This can be done via a phone or wireless connection and is often facilitated by communication devices such as routers, switches and modems.

- The primary purpose of a computer is to enable devices to transmit and share information, which can include files, documents, e-mail, and multimedia content. This is done by rules and standards that control how objects are used in a data exchange network, such as the TCP/IP protocol suite.

- Networking also provides a way for devices to access non-physical devices on the same device or on the same network, for example, accessing the Internet or connecting to a remote control.

- Security is an important part of computer networks because it is necessary to ensure that information and resources are protected from unauthorized access or attack.

- Computer networks in general are an important aspect of modern computing, allowing individuals and organizations to collaborate, share information, and access resources efficiently and effectively.

Module 3) N+ Network Configuration

Topic: THE Internet

1. **What do you mean by the term URL?**
   - The term URL stands for "Uniform Resource Locator". A string of characters that identifies the location of an Internet resource, such as a web page, image, video, document, or other service accessible over the web.

2. **Term which is used to see web pages is called what?**
   - The term used to view web pages is called web browser. A web browser is a software application that allows users to access and view web pages on the Internet. Popular web browsers include Google Chrome, Mozilla Firefox , Apple Safari, Microsoft Edge and Opera.

1. **In the Ethernet which topology is used?**
   - Ethernet technology can support a variety of network connections, but the most commonly used topology for Ethernet networks is the star topology.

   - In a star topology, each network device is connected to a central device, usually a switch or hub. All communication between devices in the network passes through the central device, which helps to control and manage the traffic in the network. This type of topology is widely used because of its advantages of easy scalability, reliability and easy isolation. Additionally, using switches in a star topology allows bidirectional communication between devices, which helps reduce collisions and improve network performance.

2. **Set of rules and regulations while working on internet, which term is used?**
   - The procedures and rules that apply when working on the Internet are often referred to as "Internet etiquette" or "Netetik". These Rules are informal guidelines for conduct and communication in online environments such as chat rooms, forums, social media platforms and email.

- Internet etiquette includes various behaviors such as respecting others, avoiding abusive language or behavior, not sending spam or objectionable messages, and protecting personal and private information. The purpose of Internet etiquette is to create a healthy and productive online community where people can communicate and interact in a respectful and polite manner

1. What do you mean by RAS?

- RAS stands for "Remote Access Service" or "Remote Access Server". RAS is a device used to access a network or computer via a communication method such as telephone, broadband, or the Internet.
  Remote access server is a private server that provides access to a private network or computer system for users on the network. RAS allows remote users to access network services such as files, applications, and databases as if they were physically located on the network.
  Provides remote access using various protocols such as Point-to-Point Protocol (PPP), Virtual Private Network (VPN), and Remote Desktop Protocol (RDP).
  RAS technology is widely used by organizations to provide their employees, customers and partners with secure and convenient access to their networks and resources.

2. What are the main search engines to get more website URL on Internet?

- **Google:** Google is the most popular search engine and uses a complex system to rank websites based on various factors such as relevance, quality, and popularity.
- **Bing:** Bing is a search engine developed by Microsoft, and it provides search results similar to Google.
- **Yahoo:** Yahoo is a search engine that provides search results from its own database as well as from Bing.
- **DuckDuckGo:** DuckDuckGo is a privacy-focused search engine that does not track users' activity or store their personal information.
- These search engines can be used to find website URLs by entering keywords or phrases related to the websites you are looking for in the search bar. The search engine will then return a list of relevant websites and their URLs.

Module 3) N+ Network Configuration

3. **What does the PROTOCOL consist of?**
    - In computer networks, a protocol is a set of rules and standards that define how data is sent over a network. There are many methods, including:

    - Syntax: The syntax of the transaction refers to the format and structure of the data to be sent, including the data type, the size of the data field, and the order in which the data is displayed.

    - Semantics: The semantics of the process are concerned with the meaning and interpretation of the transmitted data. This includes rules about how data is processed and how it is processed.

    - Timing: It refers to the timing of the operation, data transmission time and transmission frequency rules.

    - Error Checking: Error checking protocol refers to the rules for detecting and correcting errors in data transmission to ensure the accuracy and integrity of data.

    - Flow Control: Flow control of the process refers to the rules that control the flow of data between the sender and receiver to prevent data loss or conflict.

    - Session Management: Session management of processes related to connection and termination rules between devices, including authentication and authorization mechanisms.

    - Examples of network protocols include TCP/IP, HTTP, FTP, SMTP, and DNS, each with its own syntax, semantics, timing, error handling, traffic management, and procedures.

Module 3) N+ Network Configuration

Topic: Virtualization

1. **What is Virtualization?**

   - Virtualization is the process of creating a virtual version of something, such as an operating system, server, storage, or network service. Virtualization allows multiple operating systems, applications, and workloads to share a single physical server or computing resource.

2. **What is the Difference between Full Virtualization and Para Virtualization?**

   - Full virtualization and virtualization are two virtualization systems used to create virtual machines (VMs) on physical servers. The main difference between them is how they handle the virtualization of the operating system.

1. **What is Hyper-visor?**

   - A hypervisor, also known as a virtual machine monitor (VMM), is a software layer that allows multiple virtual machines (VMs) to run on a single physical server or computing resource. The hypervisor creates and manages the virtualization environment in which the VMs run, including the allocation of hardware resources and isolation of the VMs.

   - The hypervisor sits between the physical hardware and virtual machines and captures all hardware requests from the VM and forwards them to the physical hardware. It manages the allocation of CPU, memory, storage and network resources to each VM, ensuring efficient and fair use of resources**.**

2. **What are different hypervisors available in Linux?**

   - Many hypervisors are available in Linux, including Type 1 hypervisors like KVM and Xen and Type 2 hypervisors like VirtualBox and QEMU. Each hypervisor has its own strengths and weaknesses, and the choice of hypervisor depends on the specific requirements and use cases. A hypervisor allows multiple virtual machines to run on a single physical server or computing resource, providing efficiency, flexibility, and cost-effectiveness management.

Module 3) N+ Network Configuration

3. . **What is Virtualization and what are its types?**

- Virtualization is the process of creating a virtual version of something that increases service utilization, scalability, and flexibility while reducing cost and complexity. There are many types of virtualization, including server virtualization , storage virtualization, network virtualization, desktop virtualization, application virtualization, and operating system virtualization. Each type of virtualization has its own benefits and uses, and organizations may use one or more depending on their specific needs and goals.

1. **Name the components that are used in VMware infrastructure What is benefits of Virtualization?**

- **Components of VMware infrastructure include:**

- **VMware ESXi Hypervisor:** A virtualization platform that creates and manages virtual machines on physical servers.

- **vCenter Server:** This is the central management platform for VMware infrastructure. It allows administrators to manage, configure and monitor performance of virtual machines.

- **VMware vSphere Client:** This is a graphical user interface for managing and configuring virtual machines and their resources.

- **VMware vMotion:** This allows virtual machines to be moved between physical servers without downtime or application downtime.
  VMware HA (High Availability): This allows the virtual machine running on it to restart on another available server if a physical server fails.

- **VMware DRS (Distributed Resource Scheduler)**: This feature automatically balances the operation of multiple physical servers in a group based on resource usage and availability.

Module 3) N+ Network Configuration

- **The benefits of virtualization include:**

- **Improved resource utilization:** Virtualization improves resource utilization and reduces hardware costs by allowing multiple virtual machines to run on a single physical server.

- **Convenience and scalability:** Virtualization makes it easier and more efficient by making it easier to add or remove virtual machines as needed and move them between physical servers.

- **Improved Disaster Recovery and Business Continuity:** Virtualization extends and shortens business performance by enabling fast and easy backup, replication, and recovery of virtual machines in the event of a disaster

- **Ease of Management:** Virtualization enables centralized management of virtual machines, simplifying management and reducing the time and effort required for routine tasks.

- **Enhanced security and isolation:** Virtual machines are isolated from each other and from underlying devices, increasing security and reducing the risk of malware and other threats.