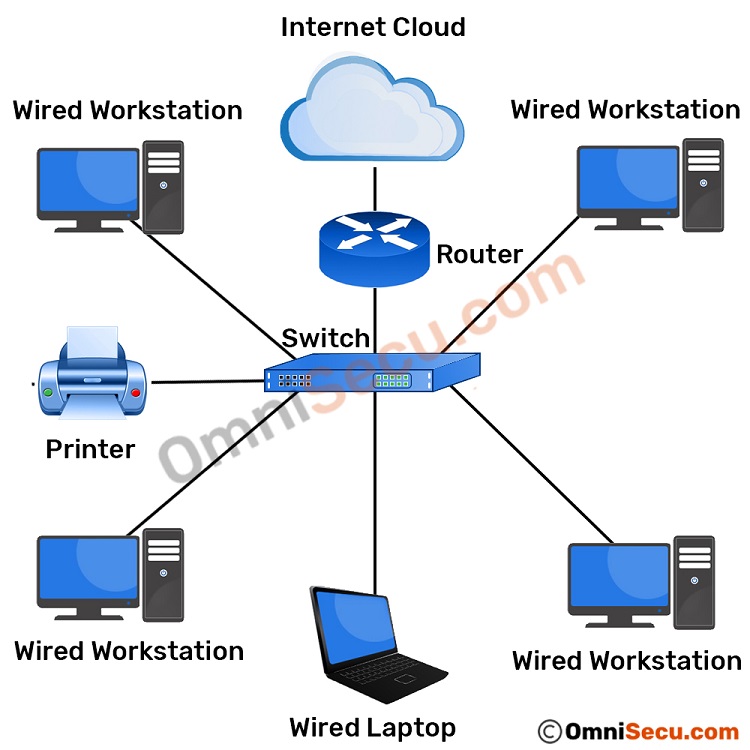
***Module 6. Network security, Maintenance and Troubleshooting procedures***

* ***Topic: A SOHO Networks.Beginner Question***

1. ***What is SOHO network?***

***Ans.*** *SOHO network is a small office/home office network.*

1. ***What does SOHO mean networking?***

***Ans.*** *The term small office/home office (SOHO) refers to a small business that is often run out of small office spaces, homes, or even virtually.*

* ***Intermediate Question***

1. ***How does a SOHO network work?***

***Ans.*** *SOHO network or also termed as single or small office/home office network is mainly referred to a business category involving a small number of workers usually from 1 to 10. It is a type of local area or LAN network connection meant to be used in small businesses.*

1. ***Issues with Soho Networking?***

***Ans.*** *Small office/home office (SOHO) routers are a staple networking appliance for millions of consumers.*  
*Universal Issues Realized*

* *misconfiguration of network services,*
* *the assumption of security on the LAN,*
* *insecure default configurations, and.*
* *poor security design and implementation*
* ***Advance Question***

1. ***How Small is the “S” in SOHO?***

***Ans.*** *The standard definition limits SOHO networks to those that support between 1 and 10 people, but there isn't any magic that happens when the 11th person or device joins the network. The term SOHO is used only to identify a small network, so the number isn't as relevant. In practice, SOHO routers can support somewhat larger networks than this.*

1. ***SOHO Routers vs. Home Routers?***

***Ans.***

***Topic: NAT & PAT***

* ***Beginner Question***

1. ***What is NAT?***

***Ans.*** *NAT stands for network address translation. It's a way to map multiple local private addresses to a public one before transferring the information.*

1. ***What is PAT?***

***Ans.*** *Port Address Translation (PAT) is an extension of Network Address Translation (NAT) that permits multiple devices on a LAN to be mapped to a single public IP address to conserve IP addresses.*

1. ***Different between NAT & PAT?***

***Ans.*** *NAT translates the inside local addresses into inside global addresses; similarly, PAT translates the private unregistered IP addresses into public registered IP addresses. However, unlike NAT, PAT also uses source port numbers, allowing multiple hosts to share a single IP address while using different port numbers.*

* ***Intermediate Question***

1. ***However, Will Nat work?***

***Ans.*** *there is a laptop connected to a home router. Someone uses the laptop to search for directions to their favorite restaurant. The laptop sends this request in a packet to the router, which passes it along to the web. But first, the router changes the outgoing IP address from a private local address to a public address.*

1. ***Explain NAT?***

***Ans.*** *NAT stands for network address translation. It's a way to map multiple local private addresses to a public one before transferring the information. Organizations that want multiple devices to employ a single IP address use NAT, as do most home routers.*

* ***Advance Question***

1. ***What is different between Static & Dynamic NAT?***

***Ans.*** *While static NAT is a constant mapping between inside local and global addresses, dynamic network address translation allows you to automatically map inside local and global addresses (which are usually public IP addresses). Dynamic NAT uses a group or pool of public IPv4 addresses for translation.*

1. ***NAT stand for?***

***Ans.*** *NAT stands for network address translation.*

1. ***PAT stand for?***

*Ans. PAT stand for Port Address Translation.*

***Topic: Authentication and Access Control***

* ***Beginner Question***

1. ***What Is Acl?***

***Ans.*** *Acl is a access control list.*

1. ***What Are Different Types of Acl?***

***Ans.*** *There are two types of ACLs: 1) Standard ACLs 2) Extended ACLs.*

* ***Intermediate Question***

1. ***Explain Standard Access List?***

***Ans.*** *These are the Access-list which are made using the source IP address only. These ACLs permit or deny the entire protocol suite. They don’t distinguish between the IP traffic such as TCP, UDP, HTTPS, etc. By using numbers 1-99 or 1300-1999, the router will understand it as a standard ACL and the specified address as the source IP address.*

1. ***Explain Extended Access List?***

***Ans.*** *It is one of the types of Access-list which is mostly used as it can distinguish IP traffic therefore the whole traffic will not be permitted or denied like in standard access-list. These are the ACL that uses both source and destination IP addresses and also the port numbers to distinguish IP traffic. In this type of ACL, we can also mention which IP traffic should be allowed or denied.*

* ***Advance Question***

1. ***What Is Wildcard Mask?***

***Ans.*** *A wildcard mask is a* [*mask*](https://en.wikipedia.org/wiki/Mask_(computing)) *of* [*bits*](https://en.wikipedia.org/wiki/Bit) *that indicates which parts of an* [*IP address*](https://en.wikipedia.org/wiki/IP_address) *are available for examination.*

1. ***In Which Directions We Can Apply an Access List?***

***Ans.*** *The ACLs apply to the source and destination addresses in the packet's IP header. 3- You could apply it in the out direction and just reverse the source and destinations in the ACL.*

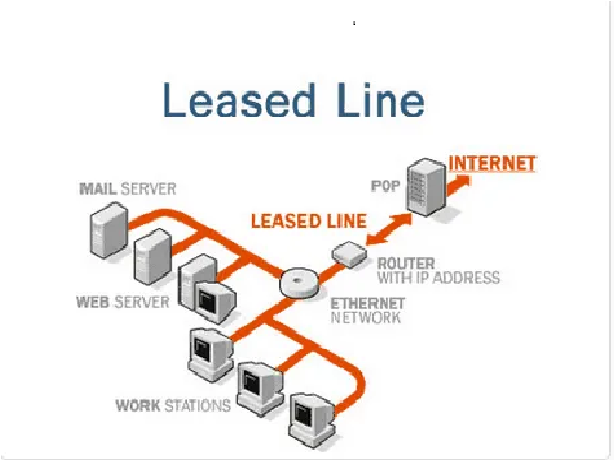
***Topic: WAN Technologies***

* ***Beginner Question***

1. ***Fiber-optic communication***

***Ans.*** *Fiber-optic communication is a method of transmitting information from one place to another by sending pulses of infrared light through an optical fiber.*

1. ***What is Leased Line***

***Ans.*** *A leased line is a dedicated data connection with a fixed bandwidth. It enables small, medium, and large businesses to connect to the internet in a secure, reliable, and highly efficient manner, with maximum download capacity, resilience, and uptime.*

1. ***Explain Circuit switching***

***Ans.*** *In circuit switching network resources (bandwidth) are divided into pieces and bit delay is constant during a connection. The dedicated path/circuit established between sender and receiver provides a guaranteed data rate. Data can be transmitted without any delays once the circuit is established.*

* ***Intermediate Question***

1. ***Explain Packet Switching***

***Ans.*** *Packet switching is a method of transferring the data to a network in form of packets. In order to transfer the file fast and efficiently manner over the network and minimize the transmission latency, the data is broken into small pieces of variable length, called Packet. At the destination, all these small parts (packets) have to be reassembled, belonging to the same file. A packet composes of payload and various control information. No pre-setup or reservation of resources is needed.*

1. ***What is difference between leased line and broadband?***

***Ans.*** *A regular broadband connection, compared with a leased line, is more likely to provide faster and stable connection speed. While download and upload speeds are symmetric on leased lines, download speed is faster than upload speed, i.e. symmetric on broadband. In a corporate environment, faster upload speed is crucial, especially for backups and cloud storage.*

*Because fibre broadband is not a dedicated connection, it is shared with other users. A leased line contract guarantees businesses uninterruptible download and upload speeds, unlike broadband that competes for* [*internet speed*](https://www.airtel.in/speedtest/) *and bandwidth with other users. Furthermore, broadband allows users to manage upload and download speeds as required by the business. Furthermore, the leased line allows users to operate seamlessly with* [*video and voice-based applications*](https://www.airtel.in/business/b2b/airtel-iq)*.*

1. ***How much is a 100mb Leased Line?***

***Ans.*** *as it stands right now the cheapest you will find a 100Mb Leased line for is about £195 per month.*

* ***Advance Question***

1. ***Difference between a POTS line and a leased line?***

***Ans.***

1. ***What is the process of packet switching?***

***Ans.*** *Packet switching is the transfer of small pieces of data across various networks. These data chunks or “packets” allow for faster, more efficient data transfer.*

*Often, when a user sends a file across a network, it gets transferred in smaller data packets, not in one piece. For example, a 3MB file will be divided into packets, each with a packet header that includes the origin IP address, the destination IP address, the number of packets in the entire data file, and the sequence number.*

1. ***Difference between circuit switching and packet switching?***

***Ans.*** *Packet switching and circuit switching are the primary models for facilitating enterprise network connections. Each mode has its place, depending on the facts and user needs.*

*Circuit switching is most often used for voice and video calling systems—communications systems that require that users establish a dedicated circuit or channel before they can connect. A circuit switching channel is always reserved, and is in use only when the users are communicating.*

*Circuit switching connections might allocate one or two channels for communications. Those with one channel are called half duplex. Those with two channels are full duplex.*

*Circuit switching is different from packet switching because it creates a physical path between the destination and source. There is no physical path in packet switching, which instead sends packets over a variety of routes.*

1. ***Practice on printer sharing***

***Ans.***

1. ***Use of IIS [ Via "add and remove" feature from control panel. "appwiz.cpl" command]***

***Ans.***

***Topic: Communication technologies Cloud and Virtualization***

* ***Beginner Question***

1. ***What is virtualization?***

***Ans.*** [*Virtualization*](https://www.redhat.com/en/topics/virtualization) *is technology that lets you create useful IT services using resources that are traditionally bound to hardware. It allows you to use a physical machine’s full capacity by distributing its capabilities among many users or environments.*

1. ***What are two types of virtualization in cloud?***

***Ans. Types Of Virtualization In Cloud Computing***

* *Server Virtualization.*
* *Application Virtualization.*
* *Network Virtualization.*
* *Desktop Virtualization.*
* *Storage Virtualization.*
* ***Intermediate Question***

1. ***What are the two types of virtualization?***

***Ans.***

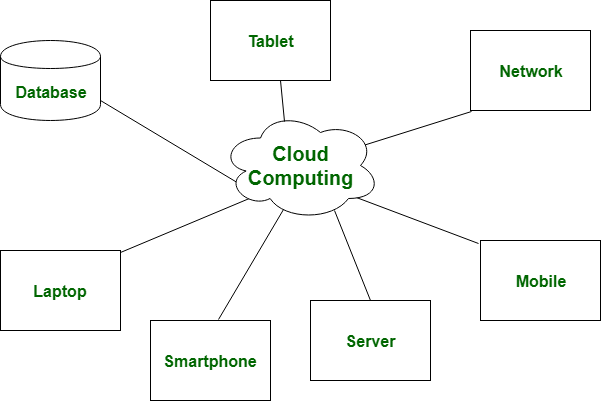
1. ***What is VMware virtualization technology?***

***Ans.*** *Virtualization relies on software to simulate hardware functionality and create a virtual computer system. This enables IT organizations to run more than one virtual system – and multiple operating systems and applications – on a single server. The resulting benefits include economies of scale and greater efficiency.*

* ***Advance Question***

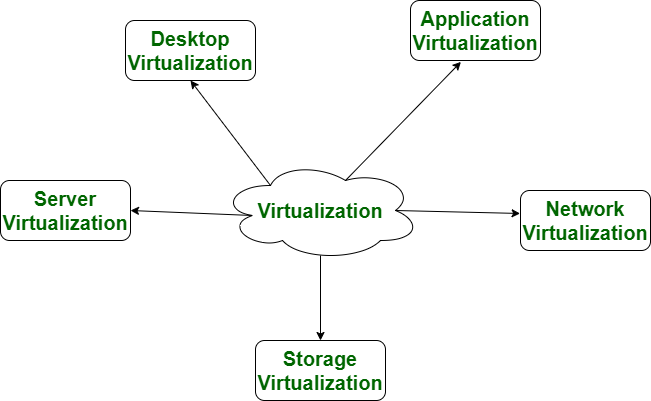
1. ***What is the difference between cloud and virtualization?***

***Ans. 1. Cloud Computing :***

*Cloud computing is a client-server computing architecture. In cloud computing, resources are used in centralized pattern and cloud computing is a high accessible service. Cloud computing is a payment and useful business tool, users pay for usage.*

***2. Virtualization:***

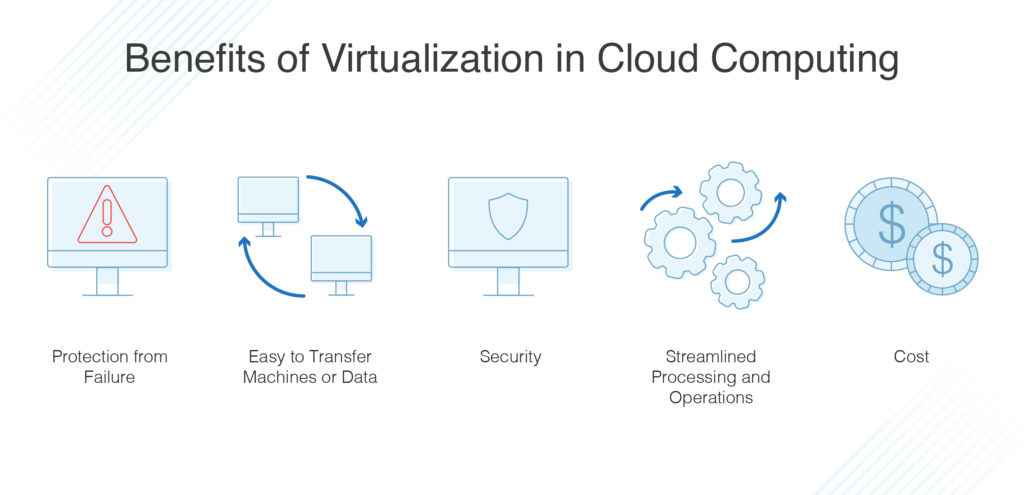
*Virtualization is the establishment of cloud computing. It is this novelty that empowers a continuous asset age from certain eccentric conditions or a singular physical device framework. Here the job of hypervisor is essential, which is legitimately associated with the equipment to make a few virtual machines from it. These virtual machines working is unmistakable, independent and doesn’t meddle with one another.In the condition of disaster recovery, it relies on single peripheral device as single dedicated hardware do a great job in it.*

*Virtualization exists in different classes which are:-*

1. ***What are the benefits of implementing virtualization in cloud computing?***

***Ans. the benefits of implementing virtualization in cloud computing:-***

* *Security*
* *Server and OS flexibility*
* *Improved workflow*



***Topic: Monitoring Tools***

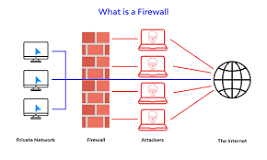
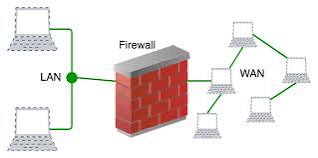
* ***Beginner Question***

1. ***Why are network monitoring tools used?***

***Ans.*** *Network monitoring tools collect data from the network devices present in the environment through network protocols and keep the network immune to any threats. They help track various performance metrics like traffic, bandwidth utilization, availability, packet loss and much more.*

1. ***Explain firewalls***

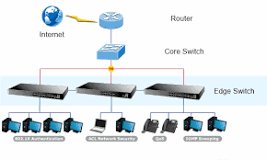
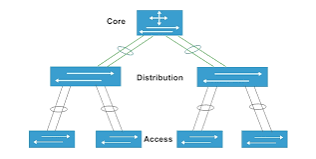
***Ans.*** *A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.*



* ***Intermediate Question***

1. ***Explain core switches***

***Ans.*** *A core switch is a high-capacity switch generally positioned within the backbone or physical core of a network. Core switches serve as the gateway to a wide area network (WAN) or the Internet - they provide the final aggregation point for the network and allow multiple aggregation modules to work together.*



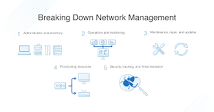
1. ***Explain client systems***

***Ans.*** *Client Systems means any communication line, modem connection or other facilities, software, hardware, Mobile Devices or equipment provided and used by You to transmit or receive any information.*

* ***Advance Question***

1. ***What is network management?***

***Ans.*** *Network management is the process of administering and managing computer networks. Services provided by this discipline include fault analysis, performance management, provisioning of networks and maintaining quality of service.*



1. ***Explain Event Viewer***

***Ans.*** *Microsoft Windows Server Event Viewer is a monitoring tool that shows a log of events that can be used to troubleshoot issues on a Windows-based system. The Event Viewer displays information about application, security-related, system and setup events.*

1. ***Practice "parental control" or "family safety" option in control panel***

***Ans.*** *Done in lab.*

***Topic: Network Security, Network vulnerabilities***

* ***Beginner Question***

1. ***What are network vulnerabilities?***

***Ans.*** *Network security vulnerabilities are weaknesses or flaws within the system's software, hardware, or organizational processes. Network vulnerabilities can be either non-physical or physical. Non-Physical: This weakness refers to anything related to data and software.*

1. ***What are the types of network security attacks?***

***Ans.*** *the Common Types of Network Attacks?*

* *Unauthorized access. Unauthorized access refers to attackers accessing a network without receiving permission.*
* *Distributed Denial of Service (DDoS) attacks.*
* *Man in the middle attacks.*
* *Code and SQL injection attacks.*
* *Privilege escalation.*
* *Insider threats.*
* ***Intermediate Question***

1. ***What is virus in network security?***

***Ans.*** *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. See malicious code.*

1. ***What is the difference between virus and antivirus?***

***Ans.*** *Antivirus software or anti-virus software is a computer program used to prevent, detect, and remove the virus. Whereas, Virus is a kind of malware that infects files and then spreads through a device whenever the file or program is run.*

* ***Advance Question***

1. ***Who is vulnerable in network security?***

***Ans.***  *‍If software or a website assumes that all input is safe, it may run unintended SQL injection. People – Social engineering is the biggest threat to the majority of organizations. So, humans can be one of the biggest causes of vulnerability.*

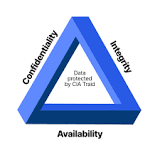
1. ***How do you assess vulnerability?***

***Ans.*** *Steps To Conduct A Vulnerability Assessment*

* *Asset discovery. First, you need to decide what you want to scan, which isn't always as simple as it sounds. ...*
* *Prioritisation.*
* *Vulnerability scanning.*
* *Result analysis & remediation.*
* *Continuous cyber security.*

1. ***What are the principles of network security?***

***Ans.*** *The basic tenets of information security are confidentiality, integrity and availability. Every element of the information security program must be designed to implement one or more of these principles. Together they are called the CIA Triad.*



1. ***What is a firewall to use for?***

***Ans.*** *Firewalls provide protection against outside cyber attackers by shielding your computer or network from malicious or unnecessary network traffic. Firewalls can also prevent malicious software from accessing a computer or network via the internet.*

1. ***configure advanced firewall setting?***

***Ans.*** *Done in lab.*

1. ***configure "date and time" opti***

***Ans.*** *Done in lab.*