**Module : - 2**

**Network**

1. A Small Office Home Office (SOHO) network refers to a type of local area or LAN network connection designed for small businesses.
2. NAT stands for network address translation. It's a way to map multiple private addresses inside a local network to a public IP address before transferring the information onto the internet.
3. A Personal Access Token (PAT) is a security credential used to authenticate a user when accessing a service, often in place of a password. PATs are commonly used in APIs or when automating tasks and can provide specific permissions based on the token.
4. NET :- NAT is a method used to translate one set of IP addresses to another set. It is commonly used to allow multiple devices on a private network to share a single public IP address.

* With NAT, each device on the private network is assigned a private IP address. When a device sends data to the internet, the router translates the private IP address to a public IP address.
* This helps in conserving IP addresses and adds a layer of security by hiding the internal network structure from the outside world.
* PAT : - PAT, also known as "NAT overload" or "NAT with Port Mapping," is a more advanced form of NAT.
* PAT extends NAT by using port numbers to allow multiple devices on a private network to share the same public IP address. It does this by keeping track of unique combinations of private IP addresses and port numbers.

1. A network access control list (ACL) is made up of rules that either allow access to a computer environment or deny it.
2. Types of ACLs :- standard ACL

* Extended ACL
* Named ACL
* Reflexive ACL
* Time-based ACL
* Mac ACL
* The wildcard mask is a technique for matching specific IP address or range of IP addresses. Cisco access control lists (ACL) filter based on the IP address range configured from a wildcard mask.

1. Circuit switching is a type of network configuration in which a physical path is obtained and dedicated to a single connection between two endpoints in the network for the duration of a dedicated connection.
2. leased line:- Dedicated Connection: A leased line is a dedicated connection between two locations, providing a fixed, continuous link.

* Symmetrical Speeds: Leased lines typically offer symmetrical upload and download speeds, which means the speed in both directions is the same.
* High Reliability: Leased lines are known for their reliability and stability because they are less susceptible to congestion or interference from other users.
* Guaranteed Bandwidth: Leased lines come with a guaranteed level of bandwidth, which ensures consistent performance and availability.
* Broadband:- Shared Connection: Broadband is a shared connection, meaning the Select the Start button, then select Settings > Network & Internet > Wi-Fi.
* Under Related settings, select Change advanced sharing options.
* In the Advanced sharing settings dialog box, expand the Private section. ...
* Under File and printer sharing, select Turn on file and printer sharingAsymmetrical Speeds: Broadband connections typically offer asymmetrical speeds, with faster download speeds and slower upload speeds.
* Variable Performance: Broadband performance can vary depending on network congestion and the number of users sharing the connection.
* No Guaranteed Bandwidth: Broadband typically does not guarantee a specific bandwidth level, which means speeds can fluctuate.

1. Post line:- Analog Voice Communication: POTS lines are traditional analog telephone lines designed primarily for voice communication.

* Limited Data Speeds: While POTS lines can carry data, they are limited to low data speeds (e.g., modem speeds up to 56 kbps).
* Dedicated for Voice: POTS lines are mainly used for voice calls, although they can also support fax machines and dial-up internet connections.
* Leased line:- Digital Data Communication: Leased lines are dedicated digital data connections designed to carry data, voice, or other types of traffic.
* High Data Speeds: Leased lines offer high data speeds and can support modern internet and data transfer requirements.
* Dedicated Connection: Leased lines provide a dedicated connection between two locations, ensuring a fixed and continuous link.

1. Select the Start button, then select Settings > Network & Internet > Wi-Fi.

* Under Related settings, select Change advanced sharing options.
* In the Advanced sharing settings dialog box, expand the Private section.
* Under File and printer sharing, select Turn on file and printer sharing.

1. Internet Information Services, also known as IIS, is a Microsoft web server that runs on Windows operating system and is used to exchange static and dynamic web content with internet users.
2. Navigate to Start > Control Panel > Administrative Tools > Server Manager. In the Windows Server Manager, go to Roles node, and expand Web Server (IIS) . Right-click on Web Server (IIS) , and click on Add Role Services . In the Add Role Services window, go to Roles Services , and check FTP Server.
3. Virtualization :- Definition: Virtualization is the process of creating virtual versions of physical hardware components such as servers, storage, networks, and operating systems.

* Purpose: It allows you to run multiple virtual environments on a single physical hardware system, thereby maximizing resource utilization and efficiency.
* Types: There are different types of virtualization, including server virtualization, storage virtualization, and network virtualization.
* Cloud:- Definition: Cloud computing is the delivery of computing resources such as servers, storage, databases, networking, and software over the internet (the "cloud").
* Purpose: It enables users to access and use resources on-demand without the need to own or maintain physical infrastructure.
* Service Models: Cloud computing offers different service models, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

1. 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.
2. A ping (Packet Internet or Inter-Network Groper) is a basic Internet program that allows a user to test and verify if a particular destination IP address exists and can accept requests in computer network administration.
3. A traceroute provides a map of how data on the internet travels from its source to its destination. When you connect with a website, the data you get must travel across multiple devices and networks along the way, particularly routers.
4. Nslookup is an abbreviation of name server lookup and allows you to query your DNS service. The tool is typically used to obtain a domain name via your command line interface (CLI), receive IP address mapping details, and lookup DNS records.
5. A core switch is the primary switch in a network, built to transfer data fast. A core switch sits at the top of a network's structure.
6. Network management is the sum total of applications, tools and processes used to provision, operate, maintain, administer and secure network infrastructure.
7. The Event Viewer is a tool in Windows that displays detailed information about significant events on your computer. Examples of these are programs that don't start as expected, or automatically downloaded updates. Event Viewer is especially useful for troubleshooting Windows and application errors.
8. Parental control, also known as family safety, is a feature available in many operating systems, applications, and routers that allows parents to manage and monitor their children's online activities. This can include setting limits on screen time, restricting access to certain websites, and monitoring what children are doing on their devices.

* Network vulnerabilities refer to weaknesses or gaps in a computer network or system that could be exploited by attackers. These vulnerabilities can be in hardware, software, or configurations and can lead to unauthorized access, data breaches, or other security incidents.

1. Types of network security 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.