ASSIGNMENT 2

Q.1 What is SOHO network?

ANS. SOHO stands for Small Office and Home Office Networks. It allows computers in a home office or remote office to connect to a corporate network, or access centralized, shared resources. It is a LAN (local area network) mainly referred to as a business category involving a small number of workers usually from 01 to 10.

Q.2 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. Organizations that want multiple devices to employ a single IP address use NAT, as do most home routers.

Q.3 What is PAT?

ANS. Port Address Translation (PAT), is an extension to network address translation (NAT) that permits multiple devices on a local area network (LAN) to be mapped to a single public IP address. The goal of PAT is to conserve IP addresses.

Q.4 Different between NAT & PAT?

ANS.

Basic for Comparison	Network Address Translation (NAT)	Port Address Translation (PAT)
Basic	It converts the private local IP address to the public global IP address.	It is similar to NAT; it also uses port numbers to transform private IP addresses from an internal network to public IP addresses.
Full-Form	The full-form of NAT is ***Network Address Translation.***	The full-form of PAT is ***Port Address Translation.***
Uses	NAT uses an **IPv4 address.**	PAT uses **IPv4** addresses along with the **port number.**
Relationship	Superset of **PAT.**	A variant of **NAT** (a form of a **Dynamic NAT)**
Types	There are three types of NAT: **Static NAT, Dynamic NAT** and **PAT/NAT** Overloading/IP masquerading.	There are two types of PAT: **Static PAT** and **overloaded PAT**.

Q.5 What Is Acl?

ANS. An access control list (ACL) contains rules that grant or deny access to certain digital environments. There are two types of ACLs: Filesystem ACLs—filter access to files and/or directories. Filesystem ACLs tell operating systems which users can access the system, and what privileges the users are allowed.

Q.6 What Are Different Types of Acl?

ANS. Standard ACL

An access-list that is developed solely using the source IP address. These access control lists allow or block the entire protocol suite. They don't differentiate between IP traffic such as UDP, TCP, and HTTPS. They use numbers 1-99 or 1300-1999 so the router can recognize the address as the source IP address.

Extended ACL

An access-list that is widely used as it can differentiate IP traffic. It uses both source and destination IP addresses and port numbers to make sense of IP traffic. You can also specify which IP traffic should be allowed or denied. They use the numbers 100-199 and 2000-2699.

Q.7 What Is Wildcard Mask?

ANS. A wildcard mask is a mask of bits that indicates which parts of an IP address are available for examination. In the Cisco IOS, they are used in several places, for example: To indicate the size of a network or subnet for some routing protocols, such as OSPF.

Q.8 Explain Circuit switching?

ANS. 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. Ordinary voice phone service uses circuit switching. This reserved circuit is used for the duration of a call.

Q.9 What is difference between leased line and broadband?

ANS.

PARAMETER	BROADBAND	LEASED LINE
Customer connectivity	Shared connection between customer premises and provider local exchange	Dedicated connection between customer premises and provider local exchange
Upload and Download Speed	Asymmetric speed i.e. higher download speed than upload speed	Symmetric speed i.e. same download speed than upload speed.
Availability and performance SLA	Very less cases where SLA guarantee is provided by Service provider	SLA guarantee is provided by Service provider for Leased links
Performance	Lower than Leased Line	High performance
Bandwidth Sharing	Bandwidth is shared across multiple customer	Bandwidth is dedicated to a customer
Reliability	Low	High
Bandwidth	Broadband speed on ADSL upto 8 Mbps and ADSL+ upto 24 Mbps	Greater speed up to multiples of 10 Mbps
Plan Types	Very few options of unlimited usage	Option of Unlimited usage Plans
QOS	Limited or no QoS	Better QoS than Broadband
Public IP Block	Generally Public IP is not provided for using customer own Web facing applications like web server etc.	Public IP are generally provided for using customer own Web facing applications like web server etc.

Voice and Video traffic	Less preferred for voice and video traffic	leased Link is preferred choice for Voice and Video applications
Cost	Cheaper than Leased Line	Costlier than Broadband connection
Security	A Broadband connection is shared across multiple customers. Hence there is quite a probability of data breach and security issues	A leased line is dedicated to a customer. Hence there is a very less chance of data breach or any other security issues

Q.10 Difference between a POTS line and a leased line?

ANS. Unlike traditional telephone lines in the public switched telephone network (PSTN) leased lines are generally not switched circuits, and therefore do not have an associated telephone number. Each side of the line is permanently connected, always active and dedicated to the other.

Q.11 Practice on printer sharing

ANS. 1>In the search box on the taskbar, type control panel and then select Control Panel.

2>Under Hardware and Sound, select View devices and printers.

3>Select and hold (or right-click) the printer you want to share, select Printer properties, and then choose the Sharing tab.

4>On the Sharing tab, select Share this printer.

Q.12 Use of IIS

ANS. 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. IIS can be used to host, deploy, and manage web applications using technologies such as ASP.NET and PHP.

Q.13 Create FTP server

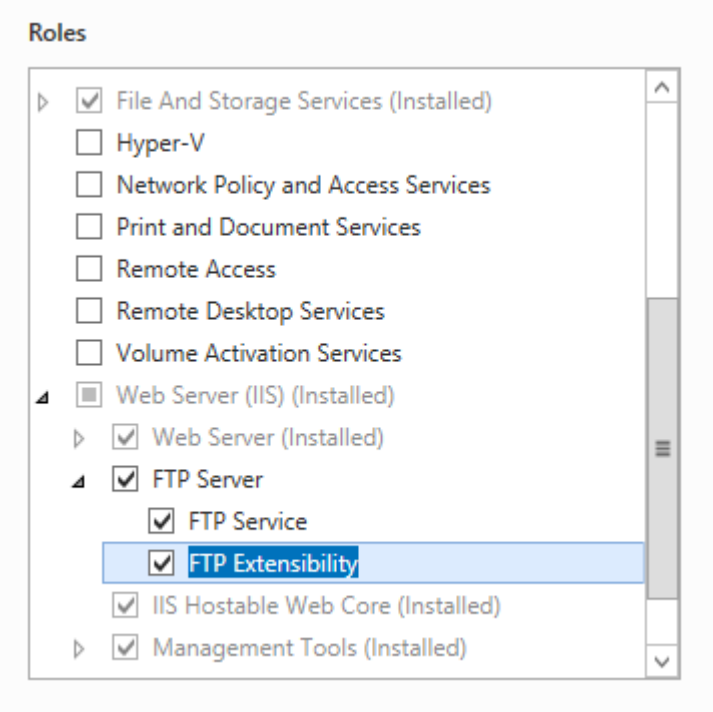
ANS. 1.On the taskbar, click **Server Manager**.

1. In **Server Manager**, click the **Manage** menu, and then click **Add Roles and Features**.
2. In the **Add Roles and Features** wizard, click **Next**. Select the installation type and click **Next**. Select the destination server and click **Next**.
3. On the **Server Roles** page, expand **Web Server (IIS)**, and then select **FTP Server**.

Note

To support ASP.Membership authentication or IIS Manager authentication for the FTP service, you will need to select **FTP**

Extensibility, in addition to **FTP Service**.



4. Click **Next**, and then on the **Select features** page, click **Next** again.
5. On the **Confirm installation selections** page, click **Install**.
6. On the **Results** page, click **Close**.

Q.14 What is the difference between cloud and virtualization?

ANS.

Definition	Technology	Methodology
Purpose	Create multiple simulated environments from 1 physical hardware system	Pool and automate virtual resources for on-demand use
Use	Deliver packaged resources to specific users for a specific purpose	Deliver variable resources to groups of users for a variety of purposes

Configuration	Image-based	Template-based
Lifespan	Years (long-term)	Hours to months (short-term)
Cost	High capital expenditures (CAPEX), low operating expenses (OPEX)	Private cloud: High CAPEX, low OPEX Public cloud: Low CAPEX, high OPEX
Scalability	Scale up	Scale out
Workload	Stateful	Stateless
Tenancy	Single tenant	Multiple tenants

Q.15 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.

Q.16 What is ping ?

ANS. Ping (latency is the technically more correct term) means the time it takes for a small data set to be transmitted from your device to a server on the Internet and back to your device again. The ping time is measured in milliseconds (ms).

Q.17 What is traceroute ?

ANS. Traceroute is a network diagnostic tool used to track in real-time the pathway taken by a packet on an IP network from

source to destination, reporting the IP addresses of all the routers it pinged in between.

Q.18 What is nslookup?

ANS. The nslookup command queries internet domain name servers in two modes. Interactive mode allows you to query name servers for information about various hosts and domains, or to print a list of the hosts in a domain. In noninteractive mode, the names and requested information are printed for a specified host or domain.

Q.19 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.

Q.20 What is network management?

ANS. Network management is the sum total of applications, tools and processes used to provision, operate, maintain, administer and secure network infrastructure. The overarching role of network management is ensuring network resources are made available to users efficiently, effectively and quickly.

Q.21 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.

Q.22 Practice "parental control" or "family safety" option in control pane What are network vulnerabilities?

ANS. **FAMILY SAFETY**

1. Select Start > Settings > Accounts > Family & Other People, and then choose Manage Family Settings Online.

2. Log in if prompted, and then locate the child account from the list of accounts included with your family. Select Screen Time below your child's name to open the Screen Time tab.

3. Make changes to the default Screen Time Settings using the drop-down lists and daily timelines.

4. Select More Options under your child's name and choose Content Restrictions.

5. Activate Block Inappropriate Apps And Games and Block Inappropriate Websites. Add any apps or websites you wish to block or allow and select an appropriate age rating.

6. Select the Activity tab and expand Manage. Select Turn On Activity Reporting and Email weekly reports to me to get weekly reports of your child’s activities while online.

7. Continue to explore other settings as desired.

PARENTAL CONTROLS

1.Open Control Panel. You can search for it from the Start screen or from the Desktop.

2.Select User Accounts And Family Safety, then choose Set Up Parental Controls For Any User.

3.Select the child's account.

4.Under Parental Controls, choose Enforce Current Settings.

5.Under Activity Reporting, choose Collect Information About PC Usage.

6.Select the links provided for the following options and configure as desired:

->Web Filtering to block certain websites and prevent downloads

->Time Limits to choose when and on what days your child can access the PC

->Windows Store and Game Restrictions to set age, title, and rating limits on the apps your child can use

->App Restrictions to set the apps that your child can use

7.You'll receive an email that includes information about the Microsoft Family Safety login page and what's available there. If you use a Microsoft Account for your child you'll be able to view activity reports and make changes online, from any computer.

Q.23 What are the types of network security attacks?

ANS. 1.Malware Attack. This is one of the most common types of cyberattacks.

2.Phishing Attack.

3.Password Attack.

4.Man-in-the-Middle Attack.

5.SQL Injection Attack.

6.Denial-of-Service Attack.

7.nsider Threat.

8.ryptojacking.