**Tops Technology**

**Q1. What is a SOHO network ?**

Ans. A Small Office Home Office (SOHO) network refers to a type of local area or LAN network connection designed for small businesses or just for a home.

**Q2. What is NAT ?**

Ans. Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more global IP address and vice versa in order to provide internet access to the local hosts. Also this process is also done for the port numbers that means it masks the port number of the host with another port number, in the packet that will be routed to the destination. NAT generally operates on a router or firewall.

**Q3. What is PAT ?**

Ans. Port Address Translation (PAT) is a type of NAT. PAT differs from other forms of NAT because it uses port numbers when mapping private IP addresses to a public IP address, which is the address seen by external systems.

**Q4. Difference between NAT and PAT ?**

Ans.

|  |  |
| --- | --- |
| NAT | PAT |
| Network Address Translation (NAT) | Port Address Translation (PAT) |
| Private IP addresses are translated into the public IP address. | Private IP addresses are translated into the public IP address via Port numbers. |
| NAT can be considered PAT’s superset. | PAT is a dynamic NAT. |
| NAT uses IPv4 address. | PAT is also uses IPv4 address but with port numbers. |

**Q5. What is ACL ?**

Ans. Access List (ACL) is a set of rules defined for controlling network traffic and reducing network attacks. ACL’s are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.

**Q.6 What are different types of ACL? What is Wildcard Mask?**

Ans. There are two types of ACL’s :

1. **Standard Access List :-** These are the Access List that are made using the source IP address only. These ACL’s 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, the router will understand it as a standard ACL and the specified address as the source IP address.
2. **Extended Access List :-** These are the ACL that uses source IP, Destination IP, source port and Destination port. These types of ACL, we can also mention which range from 100-199.

Wildcard Mask allows or denies all the traffic from a network IP address. The wildcard mask tells the router which bits in the IP address need to match the access list and which do not.

**Q7. What is difference between leased line and broadband?**

Ans.

|  |  |
| --- | --- |
| Leased Line | Broadband |
| Quicker connection speeds. | Slower connection speeds. |
| Symmetrical download and upload speeds. | Asymmetrical download and upload speeds. |
| Service level agreements as standard. | Typically no service level agreements. |
| More expensive. | Cheaper. |

**Q8. Difference between a POTS line and a leased line?**

Ans.

|  |  |
| --- | --- |
| POTS (Plain Old Telephone Service) | Leased Line |
| Voice Communication | Dedicated data communication |
| Analog | Digital (copper, fiber optics, wireless) |
| Requires dialing for each call | Permanently connected |
| Limited bandwidth | High bandwidth (1Gbps+) |
| Low, suitable for voice | High, consistent and symmetrical |
| Cheap as in cost wise | Higher cost, fixed monthly and annual fees |
| Used in homes and small businesses | Businesses needing reliable data transfer |
| Dependent on shared network | High reliability due to dedicated line |

**Q8. Use of IIS ?**

Ans. IIS (Internet Information Services) is a flexible, secure web server from Microsoft used for hosting websites, web applications, and services. It supports various frameworks, including ASP.NET and PHP, and can handle static and dynamic content. IIS also provides security features, such as authentication and SSL/TLS encryption, and includes an FTP server for file transfers. It offers extensive logging and diagnostics, supports load balancing for scalability, and allows for application pool management. Integration with Windows technologies, ease of use, and robust performance make IIS a crucial component in many IT infrastructures.

**Q9. Why are network monitoring tools used?**

Ans. Network monitoring tools are essential for ensuring efficient, secure, and reliable IT infrastructure operation. They monitor network performance metrics like bandwidth usage and latency, detect and troubleshoot faults, and identify security threats. These tools assist in capacity planning by analyzing usage trends and support compliance with regulatory requirements through detailed logs. They optimize network configurations, manage network assets, and ensure adherence to Service Level Agreements (SLA’s). Benefits include improved reliability, enhanced security, proactive maintenance, cost efficiency, and better user experience, making them crucial for effective network management. Some example of the above mentioned tools are Splunk, Cacti, Wireshark, etc.

**Q10. What is Ping ?**

Ans. Ping is used to test the reach-ability of a host on an IP network and measure the round-trip time for messages sent to a destination computer. It operates by sending ICMP Echo Request messages and waiting for Echo Replies, measuring the time taken for the round trip and reporting any packet loss. The standard bit size which is echoed is 32 bits.

**Q11. What is Traceroute ?**

Ans. Traceroute is a network diagnostic tool that traces the path of packets from the source to a destination, revealing details about each intermediate router or hop. It works by sending packets with increasing Time to Live (TTL) values and recording ICMP Time Exceeded responses from routers along the route.

**Q12. Explain core switches ?**

Ans. Core switches are powerful devices used in big networks, like in large businesses and data centers, to handle a lot of data traffic. They are very fast, have many ports to connect, and can direct data efficiently. Core switches are reliable, with backup power and parts that can be replaced without shutting down. They help manage data flow securely and are essential for expanding and maintaining high-performance networks, connecting different parts of the network to ensure smooth data transfer.

**Q13. What is network management?**

Ans. Network management involves keeping a computer network running smoothly and securely. It includes monitoring the network to spot any issues, configuring devices like routers and switches, and fixing problems quickly. It also ensures the network performs well by optimizing traffic flow and addressing any slowdowns. Security is a key part, protecting against threats and unauthorized access. Network management tracks resource usage, enforces policies, and generates activity reports, making sure the network is efficient and reliable for all users.

**Q14. Explain Event Viewer ?**

Ans. Event Viewer is a tool in Windows that helps monitor and troubleshoot computer systems and networks. It collects logs of important events like system errors, security issues, and application problems. These logs are categorized into types like Application, Security, and System. Administrators use Event Viewer to find and fix issues quickly and to keep an eye on system and network activity. It also helps track security events, like login attempts and changes to settings. The user-friendly interface makes it easy to browse and manage logs, ensuring the system runs smoothly and securely.

**Q15. What are the types of network security attacks ?**

Ans. Network security attacks come in many forms, targeting different vulnerabilities. Common types include:

1. Malware

2. Phishing

3. DoS/DDoS

4. Man-in-the-Middle

5. SQL Injection

6. Password Attacks

7. Eavesdropping

8. Steganography

9. session hijacking

10. Key loggers.

Having knowledge of these attacks helps a lot in saving a network from getting attacked.

**Q16. What is nslookup?**

Ans. “nslookup” is a command-line tool used to find the IP address of a domain name or the domain name of an IP address. It's useful for checking if a DNS server is working correctly and resolving names properly.

**Q17. What is the difference between cloud and virtualization ?**

Ans. Differences between cloud and virtualization are as follows :

|  |  |
| --- | --- |
| Cloud | Virtualization |
| Delivery of computing services like servers, storage, software over the internet. | Creating virtual version of physical components like server, storage and software. |
| Can be public, private, hybrid, multi-cloud. | Typically deployed within single organization’s data center or cloud infrastructure. |
| Accessible over the internet from anywhere with appropriate permissions. | Accessible within the network where the virtualization is implemented. |
| Managed by cloud service providers, reducing the need for internal IT management. | Managed internally by the organization's IT staff or service providers. |
| Pay-as-you-go or subscription-based pricing models. | Pay-as-you-go or subscription-based pricing models. |
| Ideal for businesses looking for flexible, scalable IT solutions without heavy upfront costs. | Used to maximize resource utilization, run multiple virtual machines on a single physical server. |
| Ex. Amazon Web Services (AWS), Microsoft Azure, Google Cloud. | Ex. VMware, Hyper-V, Oracle VM VirtualBox. |

**Q18. Explain Circuit switching ?**

Ans. Circuit switching is like reserving a special road just for you when you make a phone call. It sets up a dedicated path between two devices for the entire conversation. This ensures a clear connection without interruptions. For example, when you call someone, a circuit is reserved from your phone to theirs until you hang up. While it's reliable, it's not the most efficient because the circuit stays open even when you're not talking. It's great for real-time conversations like phone calls and video chats where a consistent connection is important.

**Q19. Create FTP server.**

Ans. The steps required to create a FTP server through IIS (Internet Information Services) are followed :

1. Open the IIS
2. Click sites in the top left corner
3. Click add FTP site from the drop-down menu
4. Open the new FTP Site Wizard
5. Select IP address for the site
6. Create a username for FTP access to the server
7. Enter the path to the directory you wish the user to have FTP access
8. Set the access permissions, such as read, write, read/write
9. Click finish
10. Restart the FTP server
11. Done.

**Q20. Practice on printer sharing.**

Ans. The steps for turning on printer sharing are as followed :

Control Panel > Network and Sharing Center > Change Advanced Sharing Settings > Private Section > Select and turn on Network Discovery under the Network Discovery > Under File Sharing and Printer Sharing > Turn on File and Printer Sharing > Save Changes.

**Q21. What are network vulnerabilities ?**

Ans. Network vulnerabilities are like old software, easy-to-guess passwords, and settings that aren't safe. Hackers can use these weaknesses to steal information or mess with how the network works. Other vulnerabilities might be mistakes like not setting up security features properly or forgetting to update software. To keep the network safe, it's important to regularly update software, use strong passwords, and make sure security settings are done right.