Module 6. Network security, Maintenance and Troubleshooting procedures

Topic: A SOHO Networks

- Beginner Question

1. What is SOHO network?

   SOHO networks are small LANs (Local Area Networks). Typically, SOHO networks consists of less than 10 computers. Network service servers like DNS server, email server, web server etc., are typically configured outside SOHO network. A SOHO network can be a small wired Ethernet LAN or made of both wired and wireless computers. Below image shows a typical basic SOHO network with internet connectivity.

2. What does SOHO mean networking?

   A SOHO network can be a mixed network of wired and wireless computers. Since these types of networks are meant for businesses, they may also include printers and sometimes voice over IP (VoIP) and fax over IP technology. SOHO is sometimes referred to as a "virtual office" or "single location firm."

- Intermediate Question

1. How does a SOHO network work?

   SOHO is the abbreviation for Small Office/Home Office network. ... SOHO network is meant for use in small businesses. Most cases, SOHO networks are configured for privately owned business or individuals who are self-employed.

2. Issues with Soho Networking?

   Security issues such as authentication, authorization, and access control requirements should be considered when designing services for such networks. As SOHO networks can be either wired or wireless, peculiar vulnerabilities associated with the chosen technology should also be taken into consideration.

- Advance Question

1. How Small is the “S” in SOHO?

   SOHO is an acronym for Small Office Home Office, a term used to distinguish you stay has many advantages, here are a few proâ€™s of owning a SOHO.

2. SOHO Routers vs. Home Routers?

SOHO Routers vs.

   Modern SOHO routers require almost the same functions as home broadband routers, and in fact, small businesses use the same models. ... Another example of a popular SOHO router is the Cisco SOHO 90 Series, which is meant for up to 5 employees and includes firewall protection and VPN encryption.

Topic: NAT & PAT

- Beginner Question

1. What is NAT?

   Network Address Translation (NAT) is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes.

2. What is PAT?

   Process analytical technology (PAT) has been defined by the United States Food and Drug Administration (FDA) as a mechanism to design, analyze, and control pharmaceutical manufacturing processes through the measurement of critical process parameters (CPP) which affect critical quality attributes (CQA).

3. Different between NAT & PAT?

NAT

Translates the private local IP address to the public global IP address.

Superset of PAT.

IPv4 address

Static NATDynamic NAT

PAT

Similar to NAT it also translates the private IP addresses of an internal network to the public IP address with the help of Port numbers.

Variant of NAT (form of a Dynamic NAT).

IPv4 addresses along with the port number.

Static PAT Overloaded PAT

Intermediate Question

1. However, Will Nat work?

   However, it seems as the onmouseout part of it doesn't work, as when my mouse leaves the image, nothing changes and the overlay div is still there. I believe that it is an issue with the onmouseout, not the function, since the function just isn't running.

2. Explain NAT?

Network address translation

Basic NAT. The simplest type of NAT provides a one-to-one translation of IP addresses. RFC 2663 refers to this type of...

One-to-many NAT. The majority of network address translators map multiple private hosts to one publicly exposed IP...

Methods of translation. Network address and port translation may be implemented in several ways. Some applications that...

Type of NAT and NAT traversal, role of port preservation for TCP. The NAT traversal problem arises when peers behind...

External links.

Advance Question

1. What is different between Static & Dynamic NAT?

   Static NAT (Network Address Translation) is useful when a network device inside a private network needs to be accessible from internet. Dynamic NAT (Network Address Translation) - Dynamic NAT can be defined as mapping of a private IP address to a public IP address from a group of public IP addresses called as NAT pool.

2. NAT stand for?

   Network Address Translation (NAT): NAT, in which the Private IP address or local address are translated into the public IP address. NAT is used to slow down the rate of depletion of available IP address by translates the local IP or

Private IP address into global or public ip address. NAT can be a one-to-one relation or many-to-one relation.

3. PAT stand for?

Topic: Authentication and Access Control

- ## Beginner Question

1. What Is Acl?

   Access Control List (ACL) – What are They and How to Configure Them! In the computer networking world, an ACL is one of the most fundamental components of security. An Access Control Lists “ ACL ” is a function that watches incoming and outgoing traffic and compares it with a set of defined statements.

2. What Are Different Types of Acl?

   1 Sequence Number: 2 ACL Name: 3 Remark: 4 Statement: 5 Network Protocol: 6 Source or Destination: 7 Log: Other Criteria: 8

- ## Intermediate Question

1. Explain Standard Access List?

   Standard Access-List. Access-list (ACL) is a set of rules defined for controlling the network traffic and reducing network attacks. ACLs are used to filter traffic based on the set of rules defined for the incoming or out going of the network. These are the Access-list which are made using the source IP address only.

2. Explain Extended Access List?

Extended IP Access Lists

   Although there are times when we only need to filter traffic based on the source address, more often than not we will need to match traffic with a higher level of detail. An option for more precise traffic-filtering control would be an extended IP access list. Here, both the source and destination address are checked. In addition, you also have the ability to specify the protocol and optional TCP or UDP port number to filter more precisely. In the following example, any field represented by is mandatory for the access list, while any field represented by is optional.

- Advance Question

1. What Is Wildcard Mask?

   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.

2. In Which Directions We Can Apply an Access List?

Topic: WAN Technologies

- Beginner Question

1. Fiber-optic communication

   he technique of transmitting data from one location to another by transmitting infrared light pulses using optical fiber is known as fiber optic communication. Here, the light is in the form of a carrier signal that is changed to hold the data. The fiber optic cables replace the electrical cables whenever long distance, high bandwidth, and resistance to electromagnetic interference are necessary.

2. What is Leased Line

   A leased line is a private telecommunications circuit between two or more locations provided according to a commercial contract. It is sometimes also known as a private circuit, and as a data line in the UK. Typically, leased lines are used by businesses to connect geographically distant offices. 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.

3. Explain Circuit switching

Switching techniques

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication.

• Intermediate Question

1. Explain Packet Switching

   n telecommunications, packet switching is a method of grouping data that is transmitted over a digital network into packets. Packets are made of a header and a payload. Data in the header is used by networking hardware to direct the packet to its destination, where the payload is extracted and used by application software. Packet switching is the primary basis for data communications in computer networks worldwide.

2. What is difference between leased line and broadband?

   One general difference between leased lines and broadband connections is that the former tend to be full fibre connections (there are a few exceptions), whereas the latter tend to run over copper wiring for part of their data transmission path.

3. How much is a 100mb Leased Line?

   A 100MB leased line costs about twice as much as 10MB one, which in turn cost just over twice as much as a 2MB connection. As connectivity costs fall, many IT Managers choose to upgrade their company's connection speed by a factor of 5 or 10, rather than stick with the existing speed and take a price cut. For years, 2MB was the standard leased line .

• Advance Question

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

   DIFFERENCE Between leased line service and POTS: ----->POTS is an analog voice transmission phone system built over copper twisted pair wires. It is the phone line technology that most of us grew up with and is exactly what you think it is: copper wires dangling overhead, carrying your voice from one place to another.

2. What is the process of packet switching?

   Packet switching is a digital network transmission process in which data is broken into suitably-sized pieces or blocks for fast and efficient transfer via different network devices. When a computer attempts to send a file to another computer, the file is broken into packets so that it can be sent across the network in the most efficient way. These packets are then routed by network devices to the destination.

3. Difference between circuit switching and packet switching?
   The main difference between circuit switching and packet switching is that Circuit Switching is connection oriented whereas, Packet Switching is connectionless. Let us learn some more differences between Circuit Switching and Packet Switching with the help of comparison chart shown below. Connection oriented. Connectionless.

4. Practice on printer sharing
   Open the Devices and Printers tab. To do that, click on the Start icon, and go to Settings→Devices→Devices and Printers. In the invoked tab, find the printer you want to share, right-click on its name, and pick Printer properties from the pop-up menu. Go to the Sharing tab and tick the box Share this printer.

5. Use of IIS [Via "add and remove" feature from control panel. "appwiz.cpl" command]
   An IIS web server accepts requests from remote client computers and returns the appropriate response. This basic functionality allows web servers to share and deliver information across local area networks (LAN), such as corporate intranets, and wide area networks (WAN), such as the internet.

Topic: Communication technologies Cloud and Virtualization

- ## Beginner Question

1. What is virtualization?
   Creation of a virtual machine over existing operating system and hardware is known as Hardware Virtualization. A Virtual machine provides an environment that is logically separated from the underlying hardware.

2. What are two types of virtualization in cloud?
   A. Server virtualization
   B. Storage virtualization
   C. Operating System virtualization
   D. Software Virtualization

- ## Intermediate Question

1. What are the two types of virtualization?

   1. Desktop Virtualization
   2. Application Virtualization
   3. Server Virtualization
   4. Storage Virtualization
   5. Network Virtualization

2. What is VMware virtualization technology?

   VMware Virtualization is a technology that is used widely in the IT sector and if you are not familiar with it, let’s take a closer look. Any Virtualization that is managed by a program is called a Hypervisor. A Hypervisor is basically a piece of computer software that creates and runs virtual machines.

- ## Advance Question

1. What is the difference between cloud and virtualization?

   Cloud infrastructure cannot be established without the help of virtualization. It is the foundation of cloud networks . In IT infrastructure, cloud computing and virtualization are used together to build a cloud infrastructure.

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

   Virtualization in Cloud Computing is making a virtual platform of server operating system and storage devices. This will help the user by providing multiple machines at the same time it also allows sharing a single physical instance of resource or an application to multiple users. Cloud Virtualizations also manage the workload by transforming traditional computing and make it more scalable, economical and efficient.

Topic: Monitoring Tools

- ## Beginner Question

1. Why are network monitoring tools used?

   Network Monitoring maximizes network availability by monitoring all systems on your network, including servers, workstations and network devices and applications. Whenever a failure is detected, you will immediately be notified via the alerts you configure in the product allowing you to take corrective action in a highly efficient manner.
2. Explain firewalls

   This real time firewall monitoring software provides a high-level overview of all the users that have accessed the internet through the configured firewall devices. It also shows the number of users that are using less than or greater than 20 percent of the bandwidth capacity, along with the protocol used.

- ## Intermediate Question

1. Explain core switches

   Switch monitoring with OpManager. ManageEngine OpManager is a comprehensive network switch monitoring software. With OpManager, you can monitor switch availability, health, and performance. OpManager 's switch monitoring functionality automatically discovers switches in your network and places them on a special switch map .

2. Explain client systems

   Client management tools (previously known as PC configuration life cycle management [PCCLM] tools) manage the configurations of client systems. Specific functionality includes OS deployment, inventory, software distribution, patch management, software usage monitoring and remote control.

Topic: Network Security, Network vulnerabilities

- ## Beginner Question

1. What are network vulnerabilities?
   Network vulnerabilities are known flaws or weaknesses in hardware, software, or other organizational assets, which can be exploited by attackers. When your network security is compromised by a threat, it can lead to a severe security breach.

2. What are the types of network security attacks?

   10 Types of Network Security Attacks

   1) Man-in-the-Middle Attacks
   2) Rootkit
   3) Phishing
   4) Denial-of-Service
   5) SQL Injection Attack
   6) Password Attacks
   7) Computer Viruses
   8) Ransomware
   9) Spyware
   10) Trojan Horse

- ## Intermediate Question

1. What is virus in network security?
   A virus is a computer code or program, which is capable of affecting your computer data badly by corrupting or destroying them. ... A computer virus is actually a malicious software program or "malware" that, when infecting your system, replicates itself by modifying other computer programs and inserting its own code.

2. What is the difference between virus and antivirus?
   Virus is a computer program that has the ability of copying itself and infecting your computer. Antivirus is a computer software used in preventing, detecting and removing malware, like computer viruses, worms, spyware, Trojan horses, adware and spyware.

- ## Advance Question

1. Who is vulnerable in network security?

Substandard back-up and recovery.

Weak authentication management.

Poor network monitoring.

End-user errors and/or misuses.

Inadequate end-point security.

2. How do you assess vulnerability?

Understand your business profile and unique security needs. ...

Planning. ...

Scanning. ...

Scan Report and Analysis. ...

Pen-testing and security audits. ...

Remediation.

3. What are the principles of network security?

   Network security involves three key principles of confidentiality, integrity, and availability. Depending upon the application and context, one of these principles might be more important than the others.