**Ch-13**

**1. Network Access Control (NAC):** Network Access Control (NAC) is a method of securing network hosts before they’re allowed to access the network.

**2. Challenge Handshake Authentication Protocol (CHAP):** CHAP (Challenge-Handshake Authentication Protocol) is a more secure procedure for connecting to a system than the Password Authentication Procedure (PAP).

**3. Extensible Authentication Protocol (EAP):** Extensible Authentication Protocol (EAP) is an extension to PPP that provides a host of additional authentication methods for remote-access clients.

**4. Minimum Length?**

Ans: Strong passwords should be at least eight characters (the more, the merrier), but they shouldn’t be any longer than 15 characters to make them easier to remember.

“The Weak List” for passwords—never uses them:

* The word *password* (not kidding—people actually do this!)  
  Proper names  
  Your pet’s name  
  Your spouse’s name  
  Your children’s names  
  Any word in the dictionary  
  A license plate number  
  Birth dates  
  Anniversary dates  
  Your username  
  The word *server*  
  Any text or label on the PC or monitor  
  Your company’s name  
  Your occupation  
  Your favorite color

**4. Know two ways you can filter traffic using an access control list?**

Ans: Access control lists can filter traffic by IP address or MAC address.

**5. Know which protocols can be used for tunneling and encryption of data?**

Ans: Tunneling and encryption protocols include SSL, VPN, L2TP, PPTP, and IPSec.

**6. Know which services allow you to remotely access computers across a network?**

Ans: RAS, RDP, PPP, PPPoE, and ICA are remote-access services and protocols.

**7. Port filtering?**

Ans: Port filtering allowing or blocking network packets into or out of a device or the network based on their application (port number).

**8. What is Tunneling?**

Ans: Tunneling is a protocol that allows for the secure movement of data from one network to another.

**Ch-15**

**1. What is firewall?**

Ans: A firewall is a system designed to prevent unauthorized access to or from a private network.

**2. Network-based firewall.**

Ans: A network-based firewall is a hardware device on the network or on a router that protects a group of computers.

**3. Host-based firewall.**

Ans: A host-based firewall is software installed on one individual machine, and it protects only that machine.

**4. How a firewall determines which traffic can pass through it.**

Ans: Firewalls use access control lists (ACLs), which are sets of rules, to determine which traffic is allowed to pass through.

**5. Where a DMZ can be placed.**

Ans: A demilitarized zone (DMZ) can be located outside a firewall, connected directly to the Internet. However, it can also be placed after the firewall.

**6. Dynamic Packet Filtering?**

Ans: Packet filtering refers to the ability of a router or a fiewall to discard packets that don’t meet the right criteria.

**7. What a proxy server is and what types of proxying are common.**

Ans: A proxy server is a computer that makes and fulfills requests on behalf of another computer. Many firewalls can act as proxies. Common proxy services include IP proxy, web proxy, FTP proxy, and mail (SMTP) proxy.

**8. Which levels of the OSI model various security devices operate?**

Ans: Firewalls work at the Application Layer or the Network layer. Port security on switches operates at the Data Link layer.

**9. The difference between stateful and stateless firewalls.**

Ans: A stateful firewall keeps track of the established connections passing through it. When another packet is received that’s part of an existing connection (part of a current state), the packet is passed without checking the ACLs.

A stateless firewall examines each packet individually and does not track existing states. This makes it a bit slower and more susceptible to network attacks.

**10. What types of services firewalls can provide.**

Ans: Most firewalls provide scanning services, content filtering, signature identification, and the ability to segregate network segments into separate security zones.

**11. VPN Concentrators.**

Ans: A VPN concentrator is a device that creates remote access for virtual private networks (VPNs)

**Ch-17**

**1. Describe some of the GUI tools available to assist in testing and troubleshooting.**

Ans: These include protocol analyzers, throughput testers, and connectivity software.

**2. Protocol Analyzers.**

Ans: Protocol analyzers, also called sniffers or network monitors, are used to capture packets in their raw format as they cross the network.

**Ch-18**

**1. Network Scanners Tools?**

Ans:

* Packet sniffers
* Intrusion detection system / intrusion prevention system (IDS/IPS) software
* Port scanners

These devices can help you both troubleshoot and fix your network as well as find and stop hackers in their tracks.

**2. The basic purpose of a packet sniffer.**

Ans: The basic purpose of packet sniffers or network analyzers is to collect and analyze each individual packet that is captured on a specific network segment to determine if problems are happening.

**3. The main purpose of IDS/IPS software.**

Ans: The IDS detects unwanted attempts to manipulate network systems and/or environment,

and the IPS is a computer security device that monitors network and/or system activities for malicious behavior and can react in real time to stop attacks.

**4. Port Scanners.**

Ans: A port scanner is a software tool designed to search a host for open ports.

**5. Identifying Hardware Tools.**

Ans: Cable Testers, Loopback Plug, Wire-Map Testers, Continuity Testers, Certifiers, Time-Domain Reflectometer, Optical Time-Domain Reflectometer, Multimeter, Toner Probe, Butt Set, Cable Stripper/Snips, Voltage Event Recorder

**6. Time-Domain Reflectometer.**

Ans: A time-domain reflctometer (TDR) is a tool that fids and describes faults in metallic cables like twisted wire pairs and coaxial cables.

**7. Optical Time-Domain Reflectometer.**

Ans: An optical time-domain reflectometer (OTDR) is an optoelectronic instrument used to give you the skinny on optical fibers.

**8. The difference between cable testers and certifiers.**

Ans: Cable testers simply tell you if the cable will function. Cable certifiers run much more sophisticated tests that determine if the cable performs according to specifications called for in the standard.

**9. The value of temperature and humidity monitors.**

Ans: These devices can monitor environmental conditions and alert you if either the temperature or the humidity in a server room or area falls below or rises above the prescribed range of safe values.

**Ch-19**

**1. The seven troubleshooting steps.**

Ans:

1. Identify the problem.

2. Establish a theory of probable cause.

3. Test the theory to determine cause.

4. Establish a plan of action to resolve the problem and identify potential effects.

5. Implement the solution or escalate as necessary.

6. Verify full system functionality, and if applicable, implement preventative measures.

7. Document findings, actions, and outcomes.

**Ch-20**

**1. The difference between a physical network diagram and a logical network diagram**.

Ans: A physical diagram shows all of the physical connections and devices and in many cases the cables or connections between the devices. It’s a very detail-oriented view of the hardware on your network.

A logical network diagram takes a higher-level view, such as your subnets and which protocols those subnets use to communicate with each other.

**2. The difference between policies, procedures, and regulations**.

Ans: A policy is created to give users guidance as to what is acceptable behavior on the network.

Procedures are steps to be taken when an event occurs on the network, such as what to do when a user is fired or how to respond to a natural disaster.

Regulations are imposed on your organization; you are required to follow them, and if you don’t, you may be subject to punitive actions.

**3. How your servers and network devices can help you monitor your network.**

Ans: Most servers and network devices have monitoring tools built in that are capable of tracking data and events on your network. These include graphical tools as well as log files.

**4. Understand several theories of performance optimization.**

Ans: There are several ways to manage traffic on your network to speed up access and in some cases guarantee available bandwidth to applications. These include QoS, traffi shaping, load balancing, high availability, and using caching servers.

**5. Know some examples of bandwidth-intensive applications**.

Ans: Two examples of high-bandwidth applications are Voice over IP (VoIP) and real-time video streaming.

**6. Quality of Service.**

Ans: Quality of service (QoS) refers to the way the resources are controlled so that the quality of services is maintained.

QoS methods focus on one of five problems that can affect data as it traverses network cable:

Delay, Dropped packets, Jittert, Out-of-Order delivery.