**Name : Darshak kandoriya**

**Module 9 CCNA -IP connectivity and IP services**

* Beginner Question
  1. Explain Perimeter, Firewall, and Internal Routers

Ans: - Perimeter: The outer boundary of a network, acting as a security barrier bet ween the internal network and external threats

Firewall: A security system that controls and filters network traffic based on predetermined rules to protect against unauthorized access and potential threats

Internal Routers: Network devices that manage data flow within a network, directing traffic between different subnets to optimize communication

* 1. Explain types of Access Lists

Ans: Extended Access Lists: Filter traffic based on source and destination IP addresses, protocols, and ports

* 1. Explain Basic Concept of DHCP

Ans: -Dynamic Host Configuration Protocol (DHCP): Automatically assigns IP addresses and network configuration information to devices on a network

* 1. Explain DHCP DORA Process

Ans: -DHCP DORA Process: Discovery, Offer, Request, and Acknowledgment - the four steps involved in dynamically assigning IP addresses to devices on a network

* 1. Explain the basic operation of NAT

Ans: -Network Address Translation (NAT): Modifies network address information in packet headers to allow multiple devices on a local network to share a single public IP address for internet access

* 1. Explain disadvantages of using NAT

Ans: Disadvantages of NAT: Complicates end-to-end communication, hinders certain applications, and may pose challenges for peer-to-peer networking due to address translation

* Intermediate Question
  1. How to solved Mitigating Security Issues with ACLs

Ans: Mitigating security issues with ACLs: Regularly review and update Access Control Lists to restrict unnecessary access, prevent unauthorized traffic, and enhance network security

* 1. Explain Switch Port Security
  2. Explain ACL with command

Ans: Creating an ACL in Cisco routers: Example command - "access-list 1 permit 192.168.1.0 0.0.0.255," permitting traffic from the specified IP range

* 1. Explain DHCP Snooping and ARP Inspection

Ans: DHCP Snooping: Prevents unauthorized DHCP servers by monitoring and filtering DHCP messages

ARP Inspection: Mitigates ARP spoofing attacks by validating ARP packets against DHCP snooping bindings

* 1. Explain DHCP Relay Agent

Ans: -DHCP Relay Agent: Forwards DHCP requests from clients in one subnet to a DHCP server in another, facilitating dynamic IP address assignment across different network segments

* 1. Types of Network Address Translation

Ans: Network Address Translation (NAT) Types: Static NAT assigns a fixed public IP to a private address and PAT (Port Address Translation) maps multiple private IPs to a single public IP using unique port numbers

* 1. Configuring Dynamic NAT

Ans: -Configuring Dynamic NAT: Example command - "ip nat inside source list ACL pool POOL\_NAME" to dynamically map private IP addresses to available public IP addresses from a pool

* Advance question
  1. Write basic command of Standard Access Lists

Ans: Basic command for Standard Access Listsaccess-list access-list-number {permit | deny} {source}

* 1. Explain Telnet/SSH

Ans: Telnet is a network protocol that enables text-based communication between devices over a network including login credentials, in plaintext / SSH (Secure Shell) is a secure network protocol that allows encrypted communication and secure access to remote devices, ensuring confidentiality and integrity of data during transmission

* 1. Explain How to Configure DHCP

Ans: To configure DHCP, set up the DHCP server by specifying IP address ranges, lease durations, and network settings to dynamically assign IP addresses to devices on the network

* 1. NAT Explain with Command

Ans: Enable NAT on a router with the command "ip nat inside source list [ACL] interface [interface] overload" to dynamically translate private IP addresses to a single public IP address for outbound traffic e