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

**• Beginner Question**

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

* It is the last router under an organization's control and is physically connected to both the internal and external networks. Perimeter Firewall: The perimeter firewall sits behind the border router and is an organization's first line of defense against external threats.

1. **Explain types of Access Lists**

* There are two main different types of Access-list namely:

1. Standard Access-list – These are the Access-list that are made using the source IP address only. These ACLs permit or deny the entire protocol suite.
2. Extended Access-list – These are the ACL that uses source IP, Destination IP, source port, and Destination port.
3. **Explain Basic Concept of DHCP**

* Dynamic Host Configuration Protocol (DHCP) is a standard protocol defined by RFC 1541 (which is superseded by RFC 2131) that allows a server to dynamically distribute IP addressing and configuration information to clients. Normally the DHCP server provides the client with at least this basic information: IP Address.

1. **Explain DHCP DORA Process**

* The DORA process is a technique used by DHCP to dynamically assign IP addresses to any device, node or client machine over the Internet, which facilitates communication and exchange of information with other devices.

1. **Explain the basic operation of NAT**

* NAT stands for network address translation. It's a way to map multiple private addresses inside a local network to a public IP address before transferring the information onto the internet. Organizations that want multiple devices to employ a single IP address use NAT, as do most home routers.

1. **Explain disadvantages of using NAT**

* Disadvantages

1. Increased Network Complexity − NAT adds a layer of complexity to network design. ...
2. Limited Connectivity − NAT can limit the ability of devices on a private network to establish certain types of connections. ...
3. Performance issues − Another problem is NAT can introduce performance issues.

**• Intermediate Question**

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

* Using ACLs on the perimeter routers can mitigate some common security threats. Threat mitigation starts by disabling unused services running on the router. You can also mitigate threats on the network by limiting the number of users and services on the router.

1. **Explain Switch Port Security**

* Switches learn MAC addresses when the frame is forwarded through a switch port. By using port security, users can limit the number of MAC addresses that can be learned to a port, set static MAC addresses, and set penalties for that port if it is used by an unauthorized user.

1. **Explain ACL with command**

* The command syntax format of a standard ACL is access-list access-list-number {permit|deny} {host|source source-wildcard|any}. Standard ACLs compare the source address of the IP packets to the addresses configured in the ACL in order to control traffic.

1. **Explain DHCP Snooping and ARP Inspection**

* DHCP snooping listens to DHCP message exchanges and builds a bindings database of valid tuples (MAC address, IP address, VLAN interface). When DAI is enabled, the switch drops ARP packet if the sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database.

1. **Explain DHCP Relay Agent**

* A DHCP relay agent is a host or router that forwards DHCP packets between clients and servers. Network administrators can use the DHCP Relay service of the SD-WAN appliances to relay requests and replies between local DHCP Clients and a remote DHCP Server.

1. **Types of Network Address Translation**

* There are three different types of NAT: static, dynamic, and port address translation.

1. **Configuring Dynamic NAT**

* Done.

**• Advance question**

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

* The command syntax of a standard ACL is as follows: router(config)#access-list access-list-number {permit | deny} {source [source-wildcard] | host hostname | any}

1. **Explain Telnet/SSH**

* SSH encrypts the data while Telnet sends data in plain text. SSH uses a public key for authentication while Telnet does not use any authentication. SSH adds a bit more overhead to the bandwidth compared to Telnet. Telnet has been all but replaced by SSH in almost all uses.

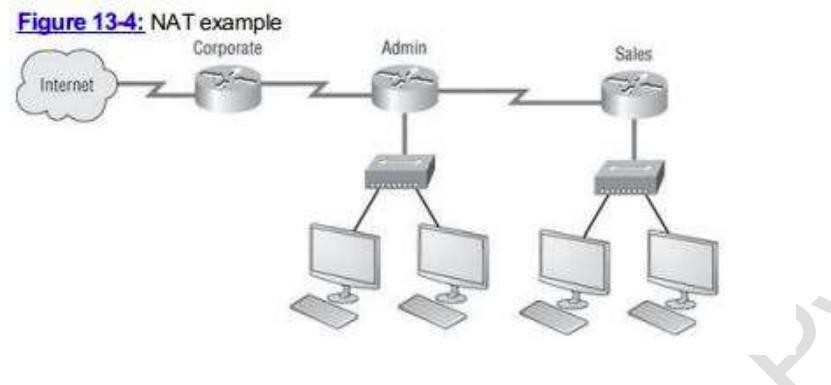
1. **Explain How to Configure DHCP**

* To add DHCP using Server Manager, select Add Roles and Features, and then select DHCP in the Roles list. Install the DHCP role by using Windows PowerShell. The installation takes about one minute to complete. Once admins install the DHCP service, they can manage it by selecting Tools > DHCP.

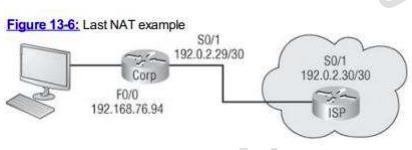
1. **NAT Explain with Command**

* Identifying the inside interface and the outside global interface by using the command “ip nat <inside/outside>” on the appropriate interfaces. The inside interface in this case is the fa0/0 interface connected to the HTTP server, while the outside global address is the s0/0/0 interface on R1.

**5. Explain with Command**



* Identifying the inside interface and the outside global interface by using the command “ip nat <inside/outside>” on the appropriate interfaces. The inside interface in this case is the fa0/0 interface connected to the HTTP server, while the outside global address is the s0/0/0 interface on R1.

1. **Explain with Command**

* ISP(config)#access-list 1 permit 192.168.76.0 0.0.0.255

ISP(config)#ip nat pool tops 192.168.2.30 192.168.2.29 netmask 255.0.0.0

ISP(config)#ip nat inside source list 1 pool tops

ISP(config)#in

ISP(config)#interface se

ISP(config)#interface serial 0/0/1

ISP(config-if)#ip nat inside

ISP(config-if)#exit

ISP(config)#in

ISP(config)#interface fa

ISP(config)#interface fastEthernet 0/0

ISP(config-if)#ip nat outside

ISP(config-if)#exit

ISP(config)#do wr

Building configuration...

[OK]