Module 9 CCNA -IP connectivity and IP services

* ***Beginner Question***

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

***Ans.*** *Perimeter :- A network perimeter may include: Border Routers serve as a final router from outside untrusted networks and direct traffic into, out of, and throughout networks.*

*Firewall :- Firewalls act as gatekeepers, following specific rules to allow or deny specific traffic to pass through into the internal network.*

*Internal routers :- internal router An internal router has all the interfaces connect to the same area. All internal routers have same link-state databases. Backbone router A backbone router has at least one interface connected to area 0.*

1. ***Explain types of Access Lists***

***Ans.***

* **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. They don’t distinguish between the IP traffic such as TCP, UDP, HTTPS, etc. By using numbers 1-99 or 1300-1999, the router will understand it as a standard ACL and the specified address as the source IP address.
* **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 IP traffic should be allowed or denied. These use range 100-199 and 2000-2699.

1. ***Explain Basic Concept of DHCP***

***Ans.*** *Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.*

1. ***Explain DHCP DORA Process***

***Ans.*** *Broadcast-based DORA (Discover, Offer, Request, Acknowledgement). This process consists of the following steps: The DHCP client sends a DHCP Discover broadcast request to all available DHCP servers within range. A DHCP Offer broadcast response is received from the DHCP server, offering an available IP address lease.*

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

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

1. ***Explain disadvantages of using NAT***

***Ans.*** *NAT cannot support applications where the initiator lies on the “outside”. Because the local addresses behind the NAT are private they can't be routed across the internet. Therefore it's impossible for the external device to direct any packet to that device behind the NAT in order to initiate a session.*

* ***Intermediate Question***

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

***Ans.*** *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***

***Ans.*** *The switchport security feature (Port Security) is an important piece of the network switch security puzzle; it provides the ability to limit what addresses will be allowed to send traffic on individual switchports within the switched network.*

1. ***Explain ACL with command***

***Ans.*** *An access control list (ACL) consists of one or more access control entries (ACEs) that collectively define the network traffic profile. This profile can then be referenced by Cisco IOS XR Software software features such as traffic filtering, priority or custom queueing, and dynamic access control.*

***Command :-***

*Enable*

*Conf t*

*Access-list 10 deny host (ip add )*

*Access-list 10 permit any*

*exit*

*Int (interface id )*

*Ip access-group 10 out*

*exit*

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

***Ans.*** *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***

***Ans.*** *DHCP is a client server protocol that automatically provides IP hosts with IP addresses and other related configuration information. A DHCP relay (agent) is a host that forwards DHCP packets between clients and servers that are not on the same physical subnet.*

1. ***Types of Network Address Translation***

***Ans.* *Static NAT:*** *Static NAT maps an internal IP address to an external one on a one-to-one basis. This doesn’t help with the scalability of IPv4 but does make a system reachable from outside of the network without disrupting internal addressing schemes.*

***Dynamic NAT:*** *With Dynamic NAT, a firewall has a pool of external IP addresses that it assigns to internal computers as needed. Like Static NAT, this creates a one-to-one mapping between internal and external IP addresses; however, these mappings are not permanent.*

1. ***Configuring Dynamic NAT***

***Ans.*** *Enable*

*Conf t*

*Access-list 10 permit (source ip add) (wide card mask)*

*Ip net pool (pool name) (starting ip add to last ip add )(net mask )*

*Ip net inside source list (list nu.) pool (pool name)*

*exit*

* ***Advance question***

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

***Ans.*** *Enable*

*Conf t*

*Access-list 10 deny host (ip add )*

*Access-list 10 permit any*

*exit*

*Int (interface id )*

*Ip access-group 10 out*

*exit*

1. ***Explain Telnet/SSH***

***Ans.*** *SSH is more secure compared to Telnet. 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***

***Ans.*** *Enable*

*Conf t*

*Ip dhcp pool (pool name)*

*Network (network ip* *add )*

*Default-router (getway ip* *add )*

*exit*

1. ***NAT Explain with Command***

***Ans.***  *Enable*

*Conf t*

*Access-list 10 permit (source ip add) (wide card mask)*

*Ip net pool (pool name) (starting ip add to last ip add )(net mask )*

*Ip net inside source list (list nu.) pool (pool name)*

*exit*

1. ***Explain with Command***

***Ans.*** *Done in lab.*

1. ***Explain with Command***

***Ans.*** *Done in lab.*