Module 9 CCNA -IP connectivity and IP services

• Beginner Question

1. Explain Perimeter, Firewall, and Internal Routers

ANS: **Perimeter:**

- The perimeter in network security refers to the outer boundary of a network.

It serves as the first line of defense against unauthorized access and potential threats from external sources.

- Perimeter security measures include firewalls, intrusion detection/prevention systems, and access controls to protect the network from external attacks.

Firewall:

- A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- It acts as a barrier between a trusted internal network and entrusted external networks (such as the internet), allowing or blocking data packets based on established security policies.
- Firewalls can be hardware-based, software-based, or a combination of both.

Internal Routers:

- Internal routers are devices within a network that manage the flow of data between different segments of the internal network.
- They are responsible for routing data packets between devices within the same network and facilitating communication between various subnets.
- Internal routers help maintain efficient and organized data traffic within the internal network, enhancing overall network performance.

2. Explain types of Access Lists

ANS**:**

✚ **Standard Access Control Lists (Standard ACLs):**

- Standard ACLs filter traffic based on the source IP address.

They are simple and used primarily to permit or deny traffic from specific source IP addresses.

- Standard ACLs are numbered from 1 to 99 and 1300 to 1999. For example, you might configure an ACL to permit or deny traffic from a particular range of source IP addresses.

Example:

Access-list 1 permits 192.168.1.0 0.0.0.255

✚ **Extended Access Control Lists (Extended ACLs):**

- Extended ACLs offer more granularities by allowing you to filter traffic based on source and destination IP addresses, protocols, ports, and other criteria.
- They provide more control and are commonly used for complex network traffic filtering.
- Extended ACLs are numbered from 100 to 199 and 2000 to 2699.

Example:

Access-list 101 permit tcp 192.168.1.0 0.0.0.255 host 10.1.1.1 eq 80

3. Explain Basic Concept of DHCP

ANS: Dynamic Host Configuration Protocol (DHCP) is a network protocol used to automatically assign and manage IP addresses and other network configuration information to devices on a network. Here's a brief explanation of the basic concepts of DHCP:

IP Address Assignment:

- DHCP enables automatic assignment of IP addresses to devices (such as computers, printers, or smartphones) on a network.
- When a device joins a network, it can request an IP address from the DHCP server.

Lease Duration:

- DHCP assigns IP addresses for a specific lease duration, which is the period for which a device is allowed to use the assigned IP address.
- Before the lease expires, the device may renew the lease to continue using the same IP address.

Dynamic Configuration:

- DHCP dynamically provides configuration information to devices, including IP addresses, subnet masks, default gateways, DNS server addresses, and other settings.
- This dynamic configuration eliminates the need for manual configuration on each device.

DHCP Server:

- The DHCP server is a network device that manages and distributes IP addresses and configuration information.
- It responds to DHCP requests from client devices, assigns IP addresses, and provides the necessary configuration parameters.

DHCP Client:

- A DHCP client is a device (such as a computer or smartphone) that needs an IP address and other network configuration details.
- The client sends a DHCP request to the DHCP server to obtain this information.

DHCP Discover, Offer, Request, and Acknowledge (DORA) Process:

- **Discover:** The client broadcasts a DHCP Discover message to find available DHCP servers.
- **Offer:** DHCP servers respond with DHCP Offer messages, proposing IP addresses and configuration details.
- **Request:** The client selects one DHCP server and sends a DHCP Request message, indicating its acceptance of the offered configuration.
- **Acknowledge:** The selected DHCP server sends a DHCP Acknowledge message, confirming the IP address assignment to the client.

4. Explain DHCP DORA Process

ANS: **DHCP Discover, Offer, Request, and Acknowledge (DORA) Process:**

- **Discover:** The client broadcasts a DHCP Discover message to find available DHCP servers.
- **Offer:** DHCP servers respond with DHCP Offer messages, proposing IP addresses and configuration details.
- **Request:** The client selects one DHCP server and sends a DHCP Request message, indicating its acceptance of the offered configuration.
- **Acknowledge:** The selected DHCP server sends a DHCP Acknowledge message, confirming the IP address assignment to the client.

5. Explain the basic operation of NAT

ANS: Network Address Translation (NAT) is a technique used to map private IP addresses within an internal network to a single public IP address when accessing resources on the Internet.

Private and Public IP Addresses:

- Internal devices use private IP addresses (e.g., within the ranges 192.168.x.x, 10.x.x.x, or 172.16.x.x to 172.31.x.x).
- The NAT device, often a router or firewall, has both a private and a public IP address.

Translation Process:

- When an internal device initiates a connection to the Internet, NAT translates its private IP address to the public IP address of the NAT device.
- This allows the internal device to communicate with external servers using the NAT device's public IP address.

Port Mapping:

- NAT also assigns unique port numbers to each internal connection to distinguish between multiple simultaneous connections from different internal devices.
- This combination of public IP address and unique port number is used to identify and track each translation.

Outbound and Inbound Traffic:

- For outbound traffic (internal to external), NAT maps internal private IP addresses to the public IP address and assigns unique port numbers.
- For inbound traffic (external to internal), NAT uses the port number to determine which internal device to forward the incoming data to.

Conservation of Public IP Addresses:

- NAT helps conserve public IP addresses because multiple devices within the internal network can share a single public IP address.

6. Explain disadvantages of using NAT

ANS:

- Limited Peer-to-Peer Connectivity
- Complex Configuration for Services
- Potential for Overloaded Public IP
- Complicates Network Troubleshooting
- Application Layer Gateways (ALG) Issues
- Dependency on IPv4

• Intermediate Question

1. How to solved Mitigating Security Issues with ACLs

ANS: **Explicit Deny Rule:**

```
Access-list 100 deny ip any any
```

Sequence Order

Regular Review and Updates

Use Named ACLs:

```
ip access-list extended MY_ACL
```

Logging:

```
Access-list 100 deny ip any any log
```

Apply ACLs Strategically

Document ACL Rules

Least Privilege Principle

Regular Security Audits

Secure Management Access

2. Explain Switch Port Security

1. ANS: **Address Limiting**:

Switch Port Security restricts the number of devices (MAC addresses) allowed to connect to a specific switch port.

2. **MAC Address Filtering**:

Administrators can configure the switch to allow only specific MAC addresses to access a particular switch port. Any unauthorized MAC addresses attempting to connect will be blocked.

3. **Violation Modes:**

Switches can be configured with violation modes to determine the action taken when a violation occurs (e.g., more MAC addresses detected than allowed). Common modes include shutting down the port, sending an alert, or restricting additional MAC addresses.

4. **Sticky MAC Addresses:**

Sticky MAC addresses allow the switch to dynamically learn and store the MAC addresses of connected devices. This reduces the need for manual configuration and helps in automatically securing authorized devices.

5. **Protects Against MAC Spoofing:**

Switch Port Security helps protect against MAC address spoofing, where an unauthorized device attempts to impersonate an authorized device by using its MAC address.

Configuration Example:

```
Interface FastEthernet0/1
Switch port mode access
Switch port port-security
switch port port-security maximum 2
switch port port-security violation restrict
switchport port-security mac-address sticky
```

In this example, the switch port is configured to allow a maximum of 2 MAC addresses, take restrictive action on violation, and use sticky MAC addresses.

3. Explain ACL with command

ANS: **Access Control Lists (ACLs):**

ACLs are sets of rules that define what types of traffic are allowed or denied through a network device based on criteria such as source/destination IP addresses, protocols, and port numbers.

Example Command for Standard IPv4 ACL:

```
Access-list 1 permits 192.168.1.0 0.0.0.255
```

Applying ACL to Interface:

```
interface GigabitEthernet0/0
ip access-group 1 in
```

Example Command for Extended IPv4 ACL:

```
access-list 100 permit tcp 192.168.1.0 0.0.0.255 host 10.1.1.1 eq 80
```

Applying Extended ACL:

```
interface GigabitEthernet0/0
ip access-group 100 in
```

4. Explain DHCP Snooping and ARP Inspection

ANS: **DHCP Snooping:**

- Functionality: Prevents rogue DHCP servers by monitoring and verifying DHCP messages.
- Operation: Switch maintains a DHCP Snooping binding table; entrusted ports are restricted for DHCP traffic.

Configuration Example:

```
ip dhcp snooping
Interface GigabitEthernet0/1
ip dhcp snooping trust
```

ARP Inspection (Dynamic ARP Inspection):

- Functionality: Mitigates ARP spoofing by validating ARP packets before forwarding.
- Operation: Builds a mapping table of IP-MAC bindings; drops ARP packets with mismatches.

Configuration Example:

```
ip arp inspection vlan 1-10
interface GigabitEthernet0/1
ip arp inspection trust
```

5. Explain DHCP Relay Agent

ANS: A DHCP Relay Agent is a network device or software feature that assists in the communication between DHCP clients and DHCP servers in different subnets. It forwards DHCP broadcast messages from clients to DHCP servers and relays the server's responses back to the clients, enabling centralized IP address assignment in networks with multiple subnets. Configuration typically involves specifying the IP address of the DHCP server on the relay agent

6. Types of Network Address Translation

ANS: Static NAT (SNAT)
Dynamic NAT (DNAT)

7. Configuring Dynamic NAT

ANS: Private IP Range: 192.168.1.0/24 (internal network)
Public IP Range: 203.0.113.1 to 203.0.113.10 (available pool of public IP addresses)

```
enable
configure terminal
ip nat pool PUBLIC_POOL 203.0.113.1 203.0.113.10 netmask 255.255.255.0
access-list 1 permit 192.168.1.0 0.0.0.255
```

```
ip nat inside source list 1 pool PUBLIC_POOL
interface GigabitEthernet0/0   # Replace with the appropriate interface
ip nat inside
interface GigabitEthernet0/1   # Replace with the appropriate interface
ip nat outside
show ip nat translations
write memory
```

• Advance question

1. Write basic command of Standard Access Lists

```
ANS: access-list 1 permits 192.168.1.0 0.0.0.255
Interface GigabitEthernet0/0
ip access-group 1 in
```

2. Explain Telnet/SSH

Telnet (Telecommunication Network):

Functionality: Telnet is a network protocol used for remote terminal access. It allows a user to log into a remote system and interact with its command-line interface as if they were physically present.

Security Concerns: Telnet transmits data, including passwords, in plain text, making it vulnerable to interception. Due to security risks, it is recommended to use more secure alternatives like SSH.

SSH (Secure Shell):

Functionality: SSH is a cryptographic network protocol that provides secure, encrypted communication over a potentially unsecured network. It allows secure access to a remote system's command-line interface, similar to Telnet.

Security Features: SSH encrypts the data exchanged between the client and server, providing a secure and confidential communication channel. It also supports public-key authentication, further enhancing security.

Port: SSH typically operates on port 22.

Comparison:

- Telnet is less secure as it transmits data in plain text, while SSH encrypts data, ensuring confidentiality.
- SSH is the preferred choice for remote access due to its enhanced security features, making it resistant to eavesdropping and man-in-the-middle attacks.
- When possible, it is recommended to use SSH instead of Telnet for secure remote access to network devices and servers.

3. Explain How to Configure DHCP

```
    ANS: # Install DHCP Server Role
    Install-WindowsFeature -Name DHCP -IncludeManagementTools
# Authorize DHCP Server
    Add-DhcpServerInDC
# Create DHCP Scope
    Add-DhcpServerv4Scope -Name "MyScope" -StartRange 192.168.1.10 -EndRange
    192.168.1.100 -SubnetMask 255.255.255.0 -LeaseDuration 8.00:00:00
```

4. NAT Explain with Command

ANS: Static NAT:

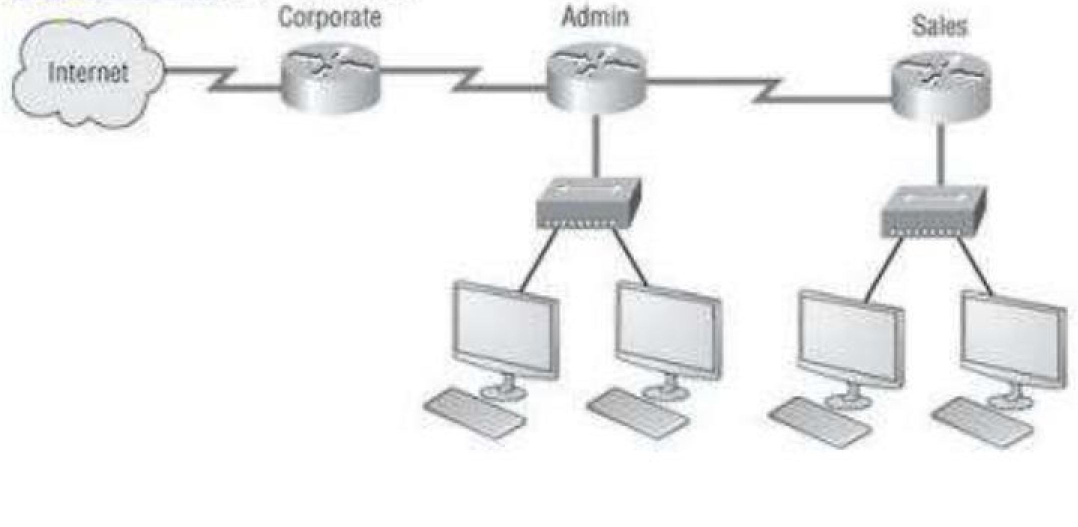
```
# Define a static NAT mapping
ip nat inside source static 192.168.1.2 203.0.113.2
# Apply NAT to the interface (inside interface)
interface GigabitEthernet0/0
ip nat inside
# Apply NAT to the interface (outside interface)
interface GigabitEthernet0/1
ip nat outside
```

Dynamic NAT:

```
# Define a pool of public IP addresses
ip nat pool PUBLIC_POOL 203.0.113.1 203.0.113.10 netmask 255.255.255.0
# Create an access list to identify internal traffic
access-list 1 permit 192.168.1.0 0.0.0.255
# Apply dynamic NAT using the access list and pool
ip nat inside source list 1 pool PUBLIC_POOL
# Apply NAT to the interface (inside interface)
interface GigabitEthernet0/0
ip nat inside
# Apply NAT to the interface (outside interface)
interface GigabitEthernet0/1
ip nat outside
```

5. Explain with Command

Figure 13-4: NAT example



ANS: Admin network: 192.168.1.0/24

Sales network: 192.168.2.0/24

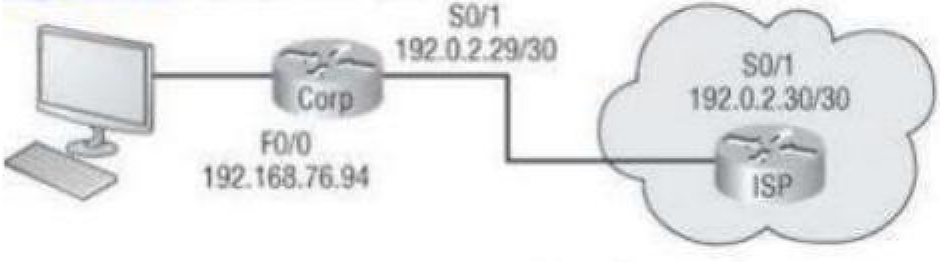
Internet-facing interface: GigabitEthernet0/0 with IP 203.0.113.1/24

```
# Enable NAT
```

```
enable
configure terminal

# Define a static NAT mapping for admin server
ip nat inside source static 192.168.1.10 203.0.113.2

# Define a pool of public IP addresses for sales dynamic NAT
ip nat pool SALES_POOL 203.0.113.3 203.0.113.10 netmask 255.255.255.0

# Create an access list to identify sales traffic
access-list 2 permit 192.168.2.0 0.0.0.255

# Apply dynamic NAT using the access list and pool for sales
ip nat inside source list 2 pool SALES_POOL

# Apply PAT for internet access
ip nat inside source list 2 interface GigabitEthernet0/0 overload

# Apply NAT to the inside interfaces
interface GigabitEthernet0/1
ip nat inside

# Apply NAT to the outside interface
interface GigabitEthernet0/0
ip nat outside

# Save the configuration
write memory
```

6.Explain with Command

Figure 13-6: Last NAT example



ANS:

```
# Enable NAT
Enable
configure terminal
# Define an access list to identify internal traffic
access-list 1 permit 192.168.76.0 0.0.0.255
# Define the PAT translation
ip nat inside source list 1 interface Serial0/1 overload
# Apply NAT to the inside interface
interface FastEthernet0/0
ip nat inside
# Apply NAT to the outside interface
interface Serial0/1
ip nat outside
# Verify the NAT translations
show ip nat translations
# Save the configuration
write memory
```