Module 9 CCNA -IP connectivity and IP services

1.Explain Perimeter, Firewall, and Internal Routers

- Perimeter: Also known as a network perimeter or security zone, perimeter refers to the area where a network is connected to other networks, such as the Internet. It is the first line of defense against intrusions and potential threats. The purpose of perimeters is to establish a clear boundary and control the flow of traffic entering and leaving the network. Acting as a filter, it only allows traffic to pass while blocking or scanning for bad or illegal traffic.

- **Firewall:** A firewall is a security device or software used around the network or in an internal network to monitor and control network traffic.It acts as a barrier between trust in networks and distrust outside, such as the Internet. Firewalls enforce security policies by examining packets entering and leaving the network and deciding whether to allow them based on defined rules. These rules can be based on location and criteria such as IP address, port, protocol and packet content. Firewalls can also provide additional security, such as network address translation (NAT) and virtual private network (VPN) capabilities.

- **Internal Router:** An internal router, also known as an internal router or distribution router, is a device used to interconnect different networks in an organization's internal network.They are responsible for managing network traffic between different subnets or internal network segments. Unlike perimeter firewalls, which focus primarily on controlling traffic around the network, internal routers facilitate internal network communication. Based on the network topology and routing protocols, they determine the most efficient path for packets to travel from one part of the network to another. Internal routers can also provide additional security, such as access control lists (ACLs) to control traffic between different network segments and enforce security policies.

Module 9 CCNA -IP connectivity and IP services

---

2. Explain types of Access Lists

- Standard ACL: Standard ACL is the simplest form of ACL and is used to filter traffic based on IP addresses only. These ACLs usually allow or deny traffic based on the IP address specified in the policy. Standard ACLs are often used at network boundaries to block or allow traffic from specific IP addresses or networks.

- Extended ACL: Extended ACLs provide better control over network connections than standard ACLs. They allow filtering based on many parameters including location and IP address, protocol, port number and other parameters.Extended ACLs are often used to control security policies, such as allowing or denying the types of traffic to and from specific owners or organizations.

- VLAN ACL: A VLAN ACL, also known as VLAN access map or VLAN access control list, is used to filter traffic within a particular LAN (VLAN). They can be used for Layer 2 switches to control traffic between different VLANs or within specific VLANs. VLAN ACLs work by assigning rules based on source and address MAC address, IP address, or other layer 2 and layer 3.

- Revolving ACLs: Revolving ACLs, also known as IP communication Fixed ACLs or dynamic ACLs are designed to allow traffic dynamically returned in response to the initial request.They work by monitoring the status of network connections and have created temporary rules so that access can be effective. Revolving ACLs can increase **security** by only allowing traffic that is part of a legitimate conversation over the internal network.

- Context-Based ACL: Context-Based ACL (CBAC) is a Cisco IOS Firewall feature that provides further filtering. CBAC examines application-level traffic and dynamically allows traffic to be rotated by session. It allows granular control of traffic based on application-specific features and dynamic creation of ad-hoc ACL rules.
- Time-based ACL: A time-based ACL is used to define a specific time range that is allowed or denied. This type of ACL allows administrators to restrict or allow certain types of traffic on a specific schedule. For example, an organization may choose to block certain websites or processes during business hours, but allow access outside of business hours.

Module 9 CCNA -IP connectivity and IP services

---

3. Explain Basic Concept of DHCP

- The main concept of DHCP (Dynamic Host Configuration Protocol) is the process of assigning IP addresses and other network settings to network devices. DHCP simplifies network management and reduces the need for manual configuration by assigning IP addresses. This is how

- **DHCP works:**
- DHCP Server: A DHCP server is a network device (usually a router or server) that manages and assigns IP addresses and other parameters to devices on the network. A DHCP server manages the pool of IP addresses that can be assigned to devices.

- DHCP Discovery: When a device such as a computer or smartphone is connected to a network, it sends a DHCP discovery message, usually a broadcast message.This message looks at the DHCP server to get the proper network configuration.

- DHCP Offer: After receiving a DHCP Discover message, the DHCP server checks the pool of IP addresses and other parameters. If an IP address is available, the DHCP server sends DHCP messages back to the requesting device. This message contains the IP address that the server wants to assign to the device, as well as other configuration details such as subnet mask, default gateway, DNS servers, and home rental period.

- DHCP Request: A device that receives a DHCP request can receive multiple requests from multiple DHCP servers on the network.It then chooses one of the offers and sends a DHCP request to the selected DHCP server, confirming that it accepts the IP address.

- DHCP Ack: After receiving a DHCP request, the DHCP server sends a DHCP Ack message to the device, accepting the requested IP address and providing a configuration recommendation. This message also includes the lease term, which specifies how long the device can use an IP address before the lease needs to be renewed.
- Configure and Refresh: The device configures the network configuration according to the information received in the DHCP receipt. It now has a valid IP address and can

communicate on the network.The tool monitors the rental period and restarts the rental process when the rental period expires. Renewal allows the device to continue using the same IP address or request a new IP address if necessary.

4. Explain DHCP DORA Process

- The DHCP DORA process, also known as the four-step DHCP process, describes the exchange of messages between a client and a DHCP server to obtain an IP address and other network settings. DORA stands for Discover, Offer, Claim and Recognize. Here is a breakdown of each step:

- Discovery: During the discovery step, the client (DHCP client) broadcasts DHCP discovery messages on the local network. A discover message is a request to a DHCP server to provide an IP address and other network configuration information. Broadcast messages are sent to a non-broadcast address (255th.
- Subnet broadcast address such as 255.255.255 or 192.168.1.255 depends on the network configuration.

- Provided: When the DHCP server receives a Discover message, it checks the IP address and other settings. If the server finds an IP address to assign, it sends a DHCP Offer message to the client.
- The message includes the IP address, subnet mask, lease period, default gateway, DNS server address, and other configuration details. Delivery messages are usually sent directly to the client's MAC address as unicast messages.

- Request: After receiving one or more Offer messages from different DHCP devices, the client selects a request and sends the DHCP Request message to the selected DHCP server. The request is a valid request for an IP address and the configuration is incorrect. It contains the IP address of the selected DHCP server and the details of the selection.
- Confirmation: When the DHCP server receives the request, it checks if the IP address still exists. If the address is available, the DHCP server sends a DHCP acknowledgment message to the client. The confirmation message confirms the IP address and provides the recommended settings. It includes the lease period, which shows how long the user can use the IP address.

Module 9 CCNA -IP connectivity and IP services

---

5. **Explain the basic operation of NAT**
   - NAT (Network Address Translation) is a technique for translating IP addresses and port numbers between different networks. It allows multiple devices on a private network to share a public IP address while communicating with other devices on the internet. NAT plays an important role in storing IPv4 addresses and facilitating communication between private and public networks. A simple explanation of how
   - NAT works:
   - Private IP address: On a local network, devices are usually connected to devices such as those specified in RFC 1918.
   - These private IP addresses cannot be used on the public internet and are for internal use only.

   - Public IP address: A public IP address is assigned to the network that connects your local network to the internet. This public IP address is unique worldwide and can be accessed by devices outside the local network.

   - Outbound Connections: When a device from the local network initiates an outbound connection to a device on the Internet, NAT translates the device's source IP address into the network's public IP address. It also provides a unique port number for the connection.This translation allows the device to communicate with external devices without revealing its IP address.

   - Translations: NAT maintains a translation table that tracks the mapping between IP addresses, port numbers, and its translators' IP addresses and port numbers. This table is used as address and port translation for network input and output.

   - Inbound Connection: NAT identifies the IP address and port number of incoming packets when a device outside the Internet sends a response to the network's public IP address or initiates a connection. It then consults the dictionary to determine the appropriate private IP address and port number of the target device on the local network.
   - NAT performs reverse translation by replacing the public IP address and port number with the IP address and port number before forwarding the packet to the appropriate device.

Module 9 CCNA -IP connectivity and IP services

- Port Multiplexing: NAT uses a technique called port multiplexing or Port Translation (PAT) to allow multiple devices in a shared IP address space. It does this by assigning a different port number to each connection. The combination of public IP addresses and unique port numbers allows NAT to distinguish between different connections and effectively translate traffic.

6.. Explain disadvantages of using NAT

- First, NAT can be problematic for some apps and services that require direct peer-to-peer connections, such as social networking apps, time, and some VPNs. Compatibility issues may arise due to the translation process and the mapping of IP addresses in the application payload.

- Additionally, NATs can make it difficult to trace network traffic back to its original destination on the local network, hindering troubleshooting and investigation. Relying on public IP addresses for external connections also limits network growth and requires additional addresses as the network grows.

- Indicates a remote access issue that requires special techniques such as NAT, VPN, or port forwarding.Especially in large networks, the maintenance burden increases with the management of NAT settings and translations.

- In general, while NAT benefits many areas of the network, the disadvantages of IP should be carefully considered where directly connected, efficient, end-to-end traceability or scalability is important. Organizations should evaluate their specific needs and consider alternative solutions or migrate to IPv6, which has a larger address space and easier address allocation and is another way to reduce restrictions on NAT.

Module 9 CCNA -IP connectivity and IP services

---

7. How to solved Mitigating Security Issues with ACLs

- Review and evaluate current ACL configuration: Start with a complete review of the current ACL configuration. Identify any vulnerabilities, misconfigurations, or inconsistencies that could cause security issues.
- Policy of Least Privilege (PoLP): Apply the policy of least privilege to your ACLs. This policy ensures that each user or organization is granted minimal access to perform required functions. Do not allow excessive access or access to individuals or groups as this will increase the risk of unauthorized access.
- Update and maintain the ACL regularly: The ACL should be reviewed and updated to reflect changes in organization, personnel, and needs. When employees change roles or leave the organization, their access rights should be removed immediately or updated as necessary.
- Use strong authentication tools: Enhance the security of ACLs by using strong authentication mechanisms such as multi-factor authentication (MFA). MFA adds an extra layer of protection by requiring users to provide different credentials before allowing access.
- Monitor ACL Activity and Logs: Enable monitoring and logging to monitor ACL activity and detect suspicious or unauthorized access.
- Periodically review the log to identify patterns or anomalies that may indicate a security breach or attempt to compromise the ACL. Periodic Testing and Analysis of
- ACL Configurations: Periodically perform security checks and access tests to identify weaknesses in ACL configurations. These tests help identify potential security or configuration errors that may have been overlooked during the initial setup.
- Educate Users and Administrators: Provide education and awareness to users and administrators about the importance of ACL security and best practices. This can include topics such as password preferences, avoiding sharing credentials, and reporting suspicious activity.
- Regular network updates and system security: Keep your network infrastructure and systems up to date with the latest security updates and updates. This includes the underlying devices and platforms that use ACLs because vulnerabilities in these components could affect the effectiveness of ACLs.
- Use network segmentation: Split your network into separate lanes or zones and use ACLs to control traffic between them. This helps reduce the risk of security breaches and reduce the attack surface.

Module 9 CCNA -IP connectivity and IP services

---

8. Explain Switch Port Security

- The main points and features of port forwarding security are as follows:
- MAC Address Based Management: Port forwarding security usually relies on the MAC (Media Access Control) address as control. A MAC address is a unique identifier assigned to a device's network interface card (NIC). By configuring port forwarding security, you can specify which MAC addresses are allowed or denied access to certain forwarding ports. This helps ensure that only authorized devices with specific MAC addresses can connect to the network.
- Port type: Port transfer security supports different types that determine how the port transfer port is configured
- Protection Mode: This mode blocks access to the switch port and stops traffic from illegal MAC addresses. It can also create logs or send notifications to network administrators.
- Restricted mode: In this mode, the switch monitors traffic and sends alerts for violations, but not immediately. It provides a graceful transition from a more permissive type to a more strict type.
- Shutdown Mode: This mode disables port switching if the device is not allowed to attempt to connect. The port will remain active until manually re-enabled by the network administrator.
- MAC Address Learning: The switch learns and stores the MAC addresses of the devices connected to its ports. When switch port security is enabled, the switch compares incoming MAC addresses with the configured list of MAC addresses.If the MAC address matches, the device is allowed access; otherwise it will be rejected or restricted depending on the type of setting.
- MAC Address Limit: Switch Security allows the administrator to set a limit for the number of MAC addresses allowed on the port. This helps prevent unauthorized devices from connecting via MAC address spoofing techniques.
  The Clear MAC Address feature allows the switch to dynamically learn and store the MAC address of the devices connected to the port. The change turns the dynamically learned address into a sticky address that persists even after the device is terminated.
- Crime and Logging: In the event of a crime, Switch Security can do many things, such as sending SNMP (Simple Network Management Protocol) traps, creating log entries or filling the port. These actions allow network administrators to be notified of security breaches and take appropriate action.

Module 9 CCNA -IP connectivity and IP services

- Simple Configuration: Switch port security is configurable on a per port basis, allowing administrators to define different security policies for each switch port based on specific requirements and device type.

9. Explain ACL with command

- Access Control Lists (ACLs) are an essential tool used to manage network connections and provide security in routers, switches, and firewalls. ACLs work by filtering packets based on specific criteria such as source/address IP address, protocol, port, or other attributes. Allows network administrators to allow or deny traffic from the device based on defined rules.
- ACLs can be used by various commands depending on the network device and operating system. Below is an overview of the commonly used ACL commands on Cisco IOS devices:

```
access-list 10 permit 192.168.0.0 0.0.255.255
interface GigabitEthernet0/1
permit tcp any host 192.168.1.10 eq 80
deny icmp any any
permit tcp 10.0.0.0 0.0.255.255 any eq 22
deny ip any host 192.168.1.100
no access-list 10
```

10.Explain DHCP Snooping and ARP Inspection

- **1. DHCP Snooping:**
- DHCP (Dynamic Host Configuration Protocol) snooping is a security method that prevents unauthorized or malicious DHCP servers from assigning IP addresses on the network. It works by choosing to trust only DHCP messages while losing or mitigating the effects of unscrupulous DHCP servers.
- Trusted Ports: DHCP Snooping selects some switch ports as trusted ports to connect to a legitimate DHCP server. These ports are usually set by network administrators.
- Untrusted Ports: By default, all other switches are considered untrusted ports.
- DHCP Snooping examines DHCP messages over untrusted ports and applies filtering rules.
- DHCP binding table: DHCP Snooping maintains a DHCP binding table that records the DHCP client's MAC address, IP address, lease information, and transport information. This binding information is learned by listening for the DHCP server's response.

- Filtering and Rate Limiting: DHCP snooping filters DHCP messages and rejects all DHCP, DHCPACK, or DHCPNAK requests from untrusted ports. It also uses rate limiting to prevent DHCP-based attacks involving flooding of multiple DHCP messages.
- **2. ARP inspection:**
- ARP (Address Resolution Protocol) inspection is a security system that can use ARP packets to prevent ARP spoofing attacks. ARP is used to map IP addresses to MAC addresses on the local network.
- ARP Authentication: ARP Inspection checks the consistency of ARP packets by verifying the mapping of the sender's IP and MAC address data and the binding data in the DHCP Snooping binding table.
- Trusted ports: Similar to DHCP snooping, ARP control identifies trusted ports that should run legitimate ARP traffic, such as ports attached to routers or switches.
- Untrusted ports: All other ports are considered untrusted ports using ARP inspection.
- ARP packets passing through these untrusted ports will be examined and authenticated.
- ARP Rate Limiting: ARP Control controls the speed of ARP packets by limiting the rate to reduce ARP flooding attacks.
- ARP packet filtering: ARP inspection drops or lists ARP packets that violate established information, such as ARP responses from unauthorized sources or multiple ARP responses from multiple sources for the same IP address.

11. Explain DHCP Relay Agent

- A DHCP relay agent is a network link that enables communication between DHCP clients and servers in different segments or subnets. When the DHCP client is not in the same session as the DHCP server, it cannot obtain network configuration information directly from the server. A DHCP relay agent acts as an intermediary by sending DHCP messages between clients and servers.
- When a DHCP client sends a request for an IP address, the DHCP agent captures the message and forwards it to the appropriate DHCP server. It listens for DHCP broadcasts in one network segment and unicasts to servers configured in other segments.
- The relay agent adds its own IP or network address as the destination IP to the message to let the server know the client's original session.

- A DHCP relay agent can be implemented in the form of hardware, the operating system on a router, or software on a network device. They are usually installed on routers or Layer 3 switches in the network area of subnets.
- DHCP Relay Agent allows network administrators to manage DHCP servers, reduce the number of servers required, and simplify IP address management in complex networks with multiple subnets. It eliminates the need for a DHCP server on each subnet and provides efficient network-wide IP address allocation and configuration.
- Overall, the DHCP Relay Agent is an essential component for facilitating DHCP communication on a network with segmented subnets.

12. Types of Network Address Translation

- There are many different types of Network Address Translation (NAT), a technique used to assign IP addresses between different sites. The most common types of NAT are:
- Static NAT: Static NAT is a one-to-one mapping technique in which a public IP address is permanently associated with a private IP address. It allows you to define a private IP address to a public IP address and vice versa. Static NAT is often used when certain resources need to be exposed to the public internet.
- Dynamic NAT: Dynamic NAT allows multiple IP addresses to be translated into a pool of IP addresses.It dynamically picks a public IP address from the pool and assigns it to the IP address. Dynamic NAT is useful for keeping IP addresses public, as it allows some public addresses to be shared with multiple internal devices.
- Overloaded NAT (or Port Address Translation - PAT): Also known as Port Address Translation (PAT), Overloaded NAT is a type of NAT that allows multiple IP addresses to be assigned to one IP address. It uses different ports to distinguish connections. PAT allows multiple devices to share a single IP address by monitoring a unique port on each internal connection.
- Source NAT (SNAT): Source NAT changes the IP address of the outgoing message to a different IP address. It is often used to enable multiple devices on a private network to share a public IP address when communicating with other networks.
- Destination NAT (DNAT): Destination NAT changes the IP address of an incoming packet to another IP address. It is often used to forward requests from public IP addresses to specific IP addresses or servers on the network.

Module 9 CCNA -IP connectivity and IP services

---

13. Configuring Dynamic NAT

- Dynamic NAT is a method of dynamically mapping private IP addresses to public IP addresses. It allows multiple devices on a private network to share a certain number of public IP addresses. To set up dynamic NAT, follow these general steps: verify private IP address, verify public IP address, define translation policy, enter network, go to EXEC mode, configure access lists, configure NAT pools with public IP addresses, enable NAT overloading (PAT) , apply the NAT configuration to the appropriate interface, save the configuration and test the connection. Be sure to consult your own network's documentation or user manual for detailed instructions, as commands and procedures may vary depending on the device and functionality used.

14.

- Standard Access Lists are used in network devices, such as routers, to filter traffic based on source IP addresses. They are numbered from 1 to 99 and allow or deny traffic based on the source IP address only. Here are some basic commands for configuring Standard Access Lists:

```
configure terminal
access-list <number> {permit | deny}
<source-ip> [wildcard-mask]
interface <interface-name>
 ip access-group <number> {in | out}
show access-lists
```

15.Explain Telnet/SSH

- Telnet and SSH are network protocols used to control and manage network devices such as routers, switches, and servers. They provide a way to create a secure command line interface with remote devices over the network.
- **Telnet:**
- Telnet is an older and less secure protocol. It allows users to log in and access the device using the command line interface (CLI) to execute commands. Telnet segments send information, including login credentials, in plain text, making them vulnerable to unauthorized access.

- **SSH (Secure Shell):**
- SSH is a more secure alternative to Telnet. It provides encryption and authentication methods to protect the confidentiality and integrity of data transmitted between clients and remote devices. SSH provides secure connections and remote devices using public key information to authenticate servers and clients.

16.Explain How to Configure DHCP

- Access the DHCP server.
- Configures a DHCP pool with an IP address range, subnet mask, default gateway, and DNS server address.
- Set the lease duration of the current IP address.
- A specific IP address is excluded from DHCP assignment.
- DNS server, domain name etc. Enhanced other DHCP options such as
- Enable the DHCP service.
- Save the settings.
- Test DHCP by connecting client device and verify successful IP address

17.NAT Explain with Command

- **enable**
  configure terminal
  interface <interface-name>
  ip nat outside
  exit
  interface <interface-name>
  ip nat inside
  exit
  ip nat inside source list <access-list-number> interface <interface-name> overload
  ip nat inside source static <local-ip> <global-ip>
  ip nat pool <pool-name> <start-ip> <end-ip> netmask <subnet-mask>
  access-list <access-list-number> permit <source-ip> <wildcard-mask>
  interface <interface-name>
  ip nat inside/outside
  write memory

Module 9 CCNA -IP connectivity and IP services