Module 9 CCNA -IP connectivity and IP services

Perimeter, Firewall, and Internal Routers:

* Perimeter Firewall:

A perimeter firewall is an external firewall that serves as the gateway between private networks (such as an organization’s internal network) and other public networks (like the Internet).

Its primary role is to monitor and protect the network from external malicious traffic, harmful programs, and intrusion attacks.

Perimeter firewalls come in various types:

Packet Filtering Firewalls: These inspect the contents of network packets and allow or disallow traffic based on access control lists (ACLs).

Stateful Firewalls: They track the current state of network connections and use this information for access decisions.

Proxy Firewalls: These act as intermediaries for user connections, creating separate connections between users and the firewall to protect privacy.

Next-Generation Firewalls (NGFWs): These combine features of packet filtering, stateful inspection, intrusion detection, and malware protection.

* Internal Firewall:

An internal firewall protects the network from attacks that have bypassed the perimeter.

It controls network traffic between internal devices (such as workstations and servers) within the organization.

Internal firewalls use a Zero Trust Network Access (ZTNA) approach to isolate insider attacks and minimize harm.

Traffic patterns include:

North to South: Traffic between the LAN and the Internet.

East to West: Intra-organization traffic between servers and clients within the organization.

* Internal Routers:

Internal routers enhance security by screening traffic to different parts of the protected corporate network.

They use access lists to control traffic flow.

These routers are strategically placed within the internal network.

Types of Access Lists (ACLs):

Standard ACLs:

Based on source IP addresses only.

Permit or deny the entire protocol suite without distinguishing between specific IP traffic types (e.g., TCP, UDP, HTTPS).

Identified by numbers 1-99 or 1300-1999.

Extended ACLs:

Consider source IP, destination IP, source port, and destination port.

Allow specifying which IP traffic should be allowed or denied.

Numbered range: 100-199 and 2000-2699.

Numbered vs. Named ACLs:

Numbered ACLs cannot be deleted individually; removing a rule deletes the entire ACL.

Named ACLs allow specific rule deletion and can be used with both standard and extended ACLs.

Basic Concept of DHCP (Dynamic Host Configuration Protocol):

DHCP dynamically assigns IP addresses to devices on a network.

Key points:

DHCP Server: Manages IP address allocation.

DHCP Client: Requests an IP address when connecting to the network.

Lease Time: Duration for which an IP address is valid.

IP Pool: Range of available IP addresses.

DHCP Discover, Offer, Request, Acknowledge (DORA) process.

DHCP DORA Process:

Discover: Client broadcasts a DHCP request to discover available servers.

Offer: DHCP server responds with an IP address offer.

Request: Client requests the offered IP address.

Acknowledge: Server acknowledges the request and assigns the IP address.

Basic Operation of NAT (Network Address Translation):

NAT allows private IP addresses within an internal network to communicate with external networks (like the Internet) using a single public IP address.

Types:

Static NAT: One-to-one mapping of private to public IP addresses.

Dynamic NAT: Maps multiple private IPs to a pool of public IPs.

PAT (Port Address Translation): Maps private IPs to different port numbers on a single public IP.

Benefits: IP conservation, security, and network flexibility.

Disadvantages of Using NAT:

Limited IP Pool: NAT restricts the number of available public IP addresses.

Complexity: Managing NAT rules can become intricate.

Application Compatibility: Some applications may not work well with NAT.

Logging Challenges: Tracking individual internal users becomes harder.

Mitigating Security Issues with ACLs:

Access Control Lists (ACLs) are crucial for controlling network traffic and reducing security threats.

Best Practices:

Regularly Review and Update ACLs: Access requirements change over time, so periodic reviews ensure accurate access control.

Least Privilege Principle: Grant minimal permissions required for tasks.

Assign Permissions Based on Need: Use ACLs to tailor access for specific users or groups.

Example Command to Add Permissions for a User:

setfacl -m "u:user:permissions" /path/to/file

Switch Port Security:

Port Security restricts input to an interface by limiting and identifying MAC addresses allowed to access the port.

Types:

Static Secure MAC Addresses: Manually configured and stored in the address table.

Dynamic Secure MAC Addresses: Dynamically learned and stored in the address table.

Sticky Secure MAC Addresses: Dynamically learned or manually configured, added to the running configuration.

Example Command to Set Sticky Secure MAC Address:

setfacl -m u:mandeep:rwx test/declarations.h

ACL with Command:

ACLs control which hosts can access different parts of a network and decide which traffic is forwarded or blocked.

Example Command to Apply an ACL to an Interface:

Router(config-if)# ip access-group ACL\_# in|out

Access Control List Types:

Standard ACLs: These ACLs filter traffic based only on the source IP address.

Extended ACLs: These ACLs provide more granular control by filtering traffic based on source and destination IP addresses, as well as other criteria like port numbers, protocols, etc.

Creating ACLs:

To create a standard ACL, you use a command like this:

Router(config)# access-list {1-99} permit|deny {source-address [source-wildcard]}

Example:

Router(config)# access-list 10 permit 192.168.1.0 0.0.0.255

To create an extended ACL, you use a command like this:

Router(config)# access-list {100-199} permit|deny {protocol source source-wildcard [operator port] destination destination-wildcard [operator port]}

Example:

Router(config)# access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq 80

Applying ACLs:

Once you've created an ACL, you need to apply it to an interface. You do this using the access-group command:

Router(config-if)# ip access-group {acl-number | acl-name} {in | out}

Example:

Router(config-if)# ip access-group 10 in

Verifying ACLs

You can verify the configured ACLs using the show access-lists command:

Router# show access-lists

To view ACLs applied to specific interfaces, you can use the show ip interface command:

go

Router# show ip interface [interface]

Modifying ACLs:

To modify an existing ACL, you can use the ip access-list command followed by the ACL number and then the modification:

Router(config)# ip access-list {extended | standard} {acl-number}

Router(config-ext-nacl)# permit|deny {protocol source source-wildcard [operator port] destination destination-wildcard [operator port]}

Example:

Router(config)# ip access-list extended 101

Router(config-ext-nacl)# permit tcp any host 192.168.1.1 eq 443

DHCP Snooping and ARP Inspection:

DHCP Snooping inspects DHCP traffic and tracks assigned IP addresses.

Dynamic ARP Inspection (DAI) validates ARP packets to prevent spoofing.

Configure DHCP Snooping and DAI:

Switch(config)# ip dhcp snooping

Switch(config)# ip arp inspection vlan 10

DHCP Relay Agent:

A relay agent forwards DHCP requests and replies between clients and servers across different networks.

It adds a gateway address (giaddr) field and Relay Agent Information option (option 82).

Useful in large enterprise networks where DHCP servers are on different segments.

Example Command to Set Up DHCP Relay Agent:

ip helper-address 192.168.2.2

Types of Network Address Translation (NAT):

Static NAT: One-to-one mapping of private to public IP addresses.

Dynamic NAT: Maps multiple private IPs to a pool of public IPs.

PAT (Port Address Translation): Maps private IPs to different port numbers on a single public IP.

Configuring Dynamic NAT:

Dynamic NAT maps internal private IPs to a pool of public IPs.

Example Configuration:

ip nat pool POOL\_NAME start\_ip end\_ip netmask subnet\_mask

ip nat inside source list ACL\_NAME pool POOL\_NAME

Basic Command of Standard Access Lists:

Standard Access Lists (ACLs) filter network traffic based on source IP addresses only.

To create a standard ACL, use the following commands:

Python

# Create a standard ACL with number 10

# Allow traffic from source IP 192.168.1.0/24

# Deny all other traffic

router(config)# access-list 10 permit 192.168.1.0 0.0.0.255

router(config)# access-list 10 deny any

# Apply the ACL to an interface (e.g., FastEthernet0/0)

router(config)# interface FastEthernet0/0

router(config-if)# ip access-group 10 in

AI-generated code. Review and use carefully. More info on FAQ.

Telnet vs. SSH:

Telnet:

Uses port 23.

Designed for local area networks.

Original Internet remote control for managing mainframe computers.

Sends data in plain text (insecure).

SSH (Secure Shell):

Uses port 22 (default, but can be changed).

Provides strong authentication and secure communication over insecure channels.

Encrypts data for confidentiality.

Uses public key authentication.

Replaces Telnet for secure remote access.

How to Configure DHCP:

DHCP (Dynamic Host Configuration Protocol) assigns IP addresses dynamically.

Configuration steps:

Create a DHCP pool:

Python

router(config)# ip dhcp pool VLAN\_10

Specify network and default router (gateway):

router(dhcp-config)# network 172.16.10.0 255.255.255.0

router(dhcp-config)# default-router 172.16.10.1

router(config)# ip dhcp excluded-address 172.16.10.1 172.16.10.20

router(dhcp-config)# dns-server 172.16.2.10

NAT (Network Address Translation) with Command:

NAT allows private IPs to access the Internet using a single public IP.

Types:

Static NAT: One-to-one mapping.

Dynamic NAT: Maps multiple private IPs to a pool of public IPs.

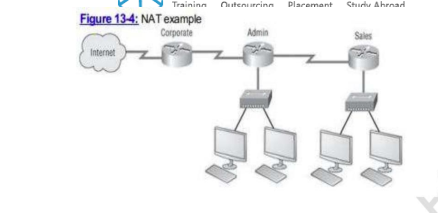
PAT (Port Address Translation): Maps private IPs to different port numbers on a single public IP.

Example configuration:

router(config)# ip nat pool POOL\_NAME start\_ip end\_ip netmask subnet\_mask

router(config)# ip nat inside source list ACL\_NAME pool POOL\_NAME

Explain with commands:



Configure Interface for NAT:

Router(config)# interface <interface>

Router(config-if)# ip nat outside

Explanation:

interface <interface>: Specifies the interface connected to the Internet.

ip nat outside: Marks this interface as the outside interface for NAT, indicating that it's facing the public network.

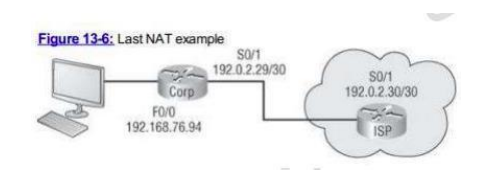
Verify NAT Configuration:

Router# show ip nat translations

Explanation:

show ip nat translations: Displays the active NAT translations on the router, showing the mapping between private and public IP addresses.

Explain with commands:



Network Diagram Description:

The diagram represents a network with the following components:

Router “Corp”:

Has two interfaces:

Serial0/1 (S0/1) with IP address 192.0.2.29/30.

FastEthernet0/0 (Fa0/0) with IP address 192.168.76.94.

Connection between Corp and an external network:

The serial link (S0/1) connects to an external network (not shown in the diagram).

The external network uses the IP address 192.0.2.30/30.

Internal network:

The internal network is connected to the FastEthernet interface (Fa0/0) of the router “Corp”.

Devices within the internal network use private IP addresses (e.g., 192.168.x.x).

Commands to Configure NAT on Router “Corp”:

Let’s assume we want to configure dynamic NAT for the internal network (192.168.76.0/24) to access the external network via the serial link (S0/1).

Dynamic NAT configuration:

# Define an access list to match internal addresses

router(config)# access-list 1 permit 192.168.76.0 0.0.0.255

# Create a NAT pool with public IP addresses

router(config)# ip nat pool NAT\_POOL 192.0.2.31 192.0.2.31 netmask 255.255.255.252

# Apply NAT to the internal interface

router(config)# interface FastEthernet0/0

router(config-if)# ip nat inside

# Apply NAT to the external interface

router(config)# interface Serial0/1

router(config-if)# ip nat outside

# Configure dynamic NAT

router(config)# ip nat inside source list 1 pool NAT\_POOL overload

Explanation:

The access list (ACL 1) permits traffic from the internal network (192.168.76.0/24).

The NAT pool (NAT\_POOL) contains a single public IP address (192.0.2.31).

The ip nat inside command applies NAT to the internal interface (Fa0/0).

The ip nat outside command applies NAT to the external interface (S0/1).

The last command configures dynamic NAT with overload (PAT).