Small Office Network

By:

- Abdelrhman Mamdouh
- Aya Abdelaty
- Lugyn Mahmoud
- Osama Mosdak
- Sagy Abdalaziz
- Yasmin Hassan

List of contents

Introduction

In today's interconnected world, small businesses require robust and efficient networks to support their operations. The need for seamless communication, secure data transmission, and reliable access to the internet is crucial for even the smallest offices. This project, "Design and Implement a Small Office Network," aims to address these needs by creating a scalable and well-structured network for a small office environment.

The objective of this project is to design, configure, and implement a network that supports a defined number of users and devices while ensuring efficient connectivity and network management. The project is divided into three key phases: Planning and Design, Configuration of Basic Devices, and Advanced Configuration and Testing. Each phase plays a critical role in ensuring the successful deployment of the office network.

A trading floor Support centre employs 600 staff. They have recently expanded and as a result, need to move to a new building. A building has been identified but has no network. This means that before they can make to move out, new network service needs to be designed and implemented in the new building. Existing Network comprises of the following elements: The new building is expected to have three floors with two departments in each for example;

1. **First floor-** (Sales and Marketing Department-120 users expected, Human Resource and Logistics Department-120 users expected).
2. **Second floor-** (Finance and Accounts Department-120 users expected, Administrator and Public Relations Department-120 users expected).
3. **Third floor-** (ICT-120 users expected, server Room-12 devices expected).

Phase 1: Planning and Design.

In this topology, all devices are connected to a central hub (the router) and communicate through it. This provides a simple and manageable structure for a small networks.

VLAN

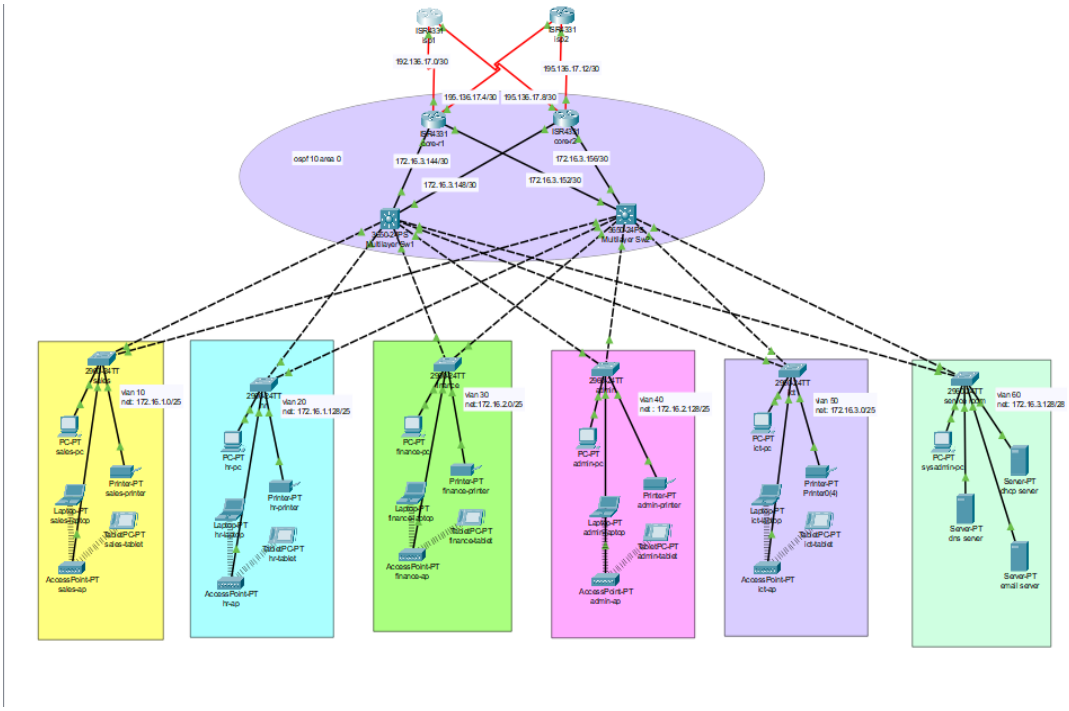
Each department should be in a different VLAN and in different subnetwork and wireless network

- **VLAN 10**
- **VLAN 20**
- **VLAN 30**
- **VLAN 40**
- **VLAN 50**
- **VLAN 60**

IP Addressing

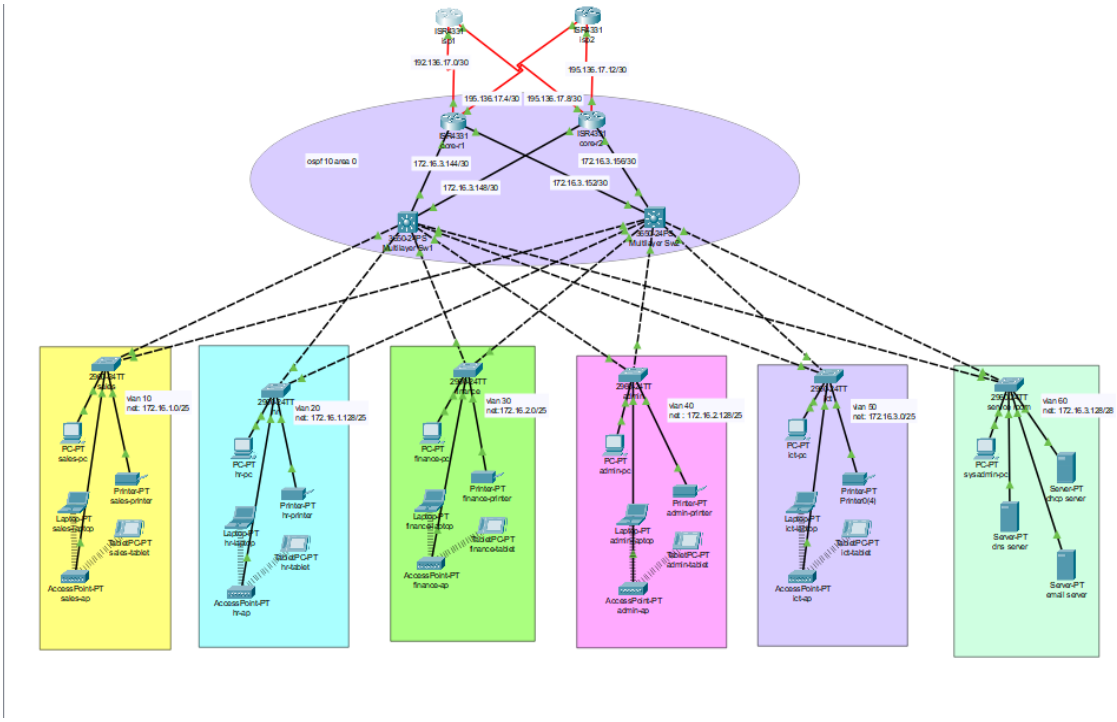
Provided a base network of 172.16.1.0, carry out subnetting to allocate the correct number of IP addresses to each department

The company network is connected to the static, public IP addresses (Internet Protocol) 195.136.17.0/30, 195.136.17.4/30, 195.136.17.8/30 and 195.136.17.12/30 connected to the two Internet providers



Phase 2: Configuration of Basic Devices

- Configure basic device settings such as hostnames, console password, enable password, banner messages, disable IP domain lookup.
- Devices in all the departments are required to communicate with each other with the respective multilayer switch configured for inter-VLAN routing.
- The Multilayer switches are expected to carry out both routing and switching functionalities thus will be assigned IP addresses.
- All devices in the network are expected to obtain an IP address dynamically from the dedicated DHCP servers located at the server room.
- The Multilayer switches are expected to carry out both routing and switching functionalities thus will be assigned IP addresses and All devices in the network are expected to obtain an IP address dynamically from the dedicated DHCP servers located at the server room.
- Configure SSH in all the routers and layer three switches for remote login.
- Configure port-security for the Finance and Accounts department to allow only one device to connect to a switchport, use sticky method to obtain mac-address and violation mode shutdown.
- Configure PAT to use the respective outbound router interface IPv4 address, implement the necessary ACL rule



ISP1 ROUTER	ISP2 ROUTER
hostname Router1 no ip cef no ipv6 cef spanning-tree mode pvst interface GigabitEthernet0/0/0 no ip address duplex auto speed auto interface GigabitEthernet0/0/1 no ip address duplex auto speed auto interface GigabitEthernet0/0/2 no ip address duplex auto speed auto interface Serial0/1/0 ip address 192.136.17.2 255.255.255.252 interface Serial0/1/1 ip address 192.136.17.10 255.255.255.252 interface Vlan1 no ip address router ospf 10 router-id 5.5.5.5 log-adjacency-changes network 195.136.17.8 0.0.0.3 area 0 network 195.136.17.0 0.0.0.3 area 0 ip classless ip flow-export version 9 line con 0 line aux 0 Line vty 0 4 login end	hostname Router2 no ip cef no ipv6 cef spanning-tree mode pvst interface GigabitEthernet0/0/0 no ip address duplex auto speed auto interface GigabitEthernet0/0/1 no ip address duplex auto speed auto interface GigabitEthernet0/0/2 no ip address duplex auto speed auto interface Serial0/1/0 ip address 192.136.17.6 255.255.255.252 interface Serial0/1/1 ip address 192.136.17.14 255.255.255.252 interface Vlan1 no ip address router ospf 10 router-id 6.6.6.6 log-adjacency-changes network 195.136.17.4 0.0.0.3 area 0 network 195.136.17.12 0.0.0.3 area 0 ip classless ip flow-export version 9 line con 0 line aux 0 line vty 0 4 login end

ROUTER OSPF1	ROUTER OSPF2
hostname core-r1 enable password 7 0822455D0A16 no ip cef no ipv6 cef username admin password 7 0822455D0A16 ip ssh version 2 no ip domain-lookup ip domain-name cisco.com spanning-tree mode pvst interface GigabitEthernet0/0/0 ip address 172.16.3.146 255.255.255.252 ip nat inside duplex auto speed auto interface GigabitEthernet0/0/1 ip address 172.16.3.154 255.255.255.252 ip nat inside duplex auto speed auto interface GigabitEthernet0/0/2 no ip address duplex auto speed auto interface Serial0/1/0 ip address 192.136.17.1 255.255.255.252 ip nat outside clock rate 2400 interface Serial0/1/1 ip address 192.136.17.5 255.255.255.252 ip nat outside clock rate 2400 interface Vlan1 no ip address shutdown router ospf 10 router-id 3.3.3.3 log-adjacency-changes network 172.16.3.144 0.0.0.3 area 0 network 172.16.3.152 0.0.0.3 area 0 network 195.136.17.0 0.0.0.3 area 0 network 195.136.17.4 0.0.0.3 area 0 ip nat inside source list 1 interface Serial0/1/1 overload ip classless ip route 0.0.0.0 0.0.0.0 Serial0/1/0 ip route 0.0.0.0 0.0.0.0 Serial0/1/1 80 ip flow-export version 9 access-list 1 permit 172.16.1.0 0.0.0.127 access-list 1 permit 172.16.1.128 0.0.0.127 access-list 1 permit 172.16.2.0 0.0.0.127 access-list 1 permit 172.16.2.128 0.0.0.127 access-list 1 permit 172.16.3.0 0.0.0.127 access-list 1 permit 172.16.3.128 0.0.0.15 banner motd $no unauthorized access$ line con 0 password 7 0822455D0A16 login line aux 0 line vty 0 4 login local transport input ssh end	hostname core-r2 enable password 7 0822455D0A16 no ip cef no ipv6 cef username admin password 7 0822455D0A16 ip ssh version 2 no ip domain-lookup ip domain-name cisco.com spanning-tree mode pvst interface GigabitEthernet0/0/0 ip address 172.16.3.150 255.255.255.252 ip nat inside duplex auto speed auto interface GigabitEthernet0/0/1 ip address 172.16.3.158 255.255.255.252 ip nat inside duplex auto speed auto interface GigabitEthernet0/0/2 no ip address duplex auto speed auto interface Serial0/1/0 ip address 195.136.17.9 255.255.255.252 ip nat outside clock rate 2400 interface Serial0/1/1 ip address 195.136.17.13 255.255.255.252 ip nat outside clock rate 2400 interface Vlan1 no ip address shutdown router ospf 10 router-id 4.4.4.4 log-adjacency-changes network 172.16.3.148 0.0.0.3 area 0 network 172.16.3.156 0.0.0.3 area 0 network 195.136.17.8 0.0.0.3 area 0 network 195.136.17.12 0.0.0.3 area 0 ip nat inside source list 1 interface Serial0/1/1 overload ip classless ip route 0.0.0.0 0.0.0.0 Serial0/1/0 ip route 0.0.0.0 0.0.0.0 Serial0/1/1 80 ip flow-export version 9 access-list 1 permit 172.16.1.0 0.0.0.127 access-list 1 permit 172.16.1.128 0.0.0.127 access-list 1 permit 172.16.2.0 0.0.0.127 access-list 1 permit 172.16.2.128 0.0.0.127 access-list 1 permit 172.16.3.0 0.0.0.127 access-list 1 permit 172.16.3.128 0.0.0.15 banner motd $no unauthorized access$ line con 0 password 7 0822455D0A16 login line aux 0 line vty 0 4 login local transport input ssh end

MultiLayer SWITCH1	MultiLayer SWITCH2
hostname mlt-sw1	hostname mlt-sw2
enable password 7 0822455D0A16	enable password 7 0822455D0A16
no ip cef	no ip cef
ip routing	ip routing
no ipv6 cef	no ipv6 cef
username admin password 7 0822455D0A16	username admin password 7 0822455D0A16
ip ssh version 2	ip ssh version 2
no ip domain-lookup	no ip domain-lookup
ip domain-name cisco.com	ip domain-name cisco
spanning-tree mode pvst	spanning-tree mode pvst
interface GigabitEthernet1/0/1	interface GigabitEthernet1/0/1
no switchport	no switchport
ip address 172.16.3.145 255.255.255.252	ip address 172.16.3.153 255.255.255.252
duplex auto	duplex auto
speed auto	speed auto
interface GigabitEthernet1/0/2	interface GigabitEthernet1/0/2
no switchport	no switchport
ip address 172.16.3.149 255.255.255.252	ip address 172.16.3.157 255.255.255.252
duplex auto	duplex auto
speed auto	speed auto
interface GigabitEthernet1/0/3	interface GigabitEthernet1/0/3
switchport mode trunk	switchport mode trunk
interface GigabitEthernet1/0/4	interface GigabitEthernet1/0/4
switchport mode trunk	switchport mode trunk
interface GigabitEthernet1/0/5	interface GigabitEthernet1/0/5
switchport mode trunk	switchport mode trunk
interface GigabitEthernet1/0/6	interface GigabitEthernet1/0/6
switchport mode trunk	switchport mode trunk
interface GigabitEthernet1/0/7	interface GigabitEthernet1/0/7
switchport mode trunk	switchport mode trunk
interface GigabitEthernet1/0/8	interface GigabitEthernet1/0/8
switchport mode trunk	switchport mode trunk
interface Vlan1	interface Vlan1
no ip address	no ip address
shutdown	shutdown
interface Vlan10	interface Vlan10
mac-address 0060.3ed9.7001	mac-address 00e0.f9d1.c101
ip address 172.16.1.1 255.255.255.128	ip address 172.16.1.1 255.255.255.128
ip helper-address 172.16.3.130	ip helper-address 172.16.3.130
interface Vlan20	interface Vlan20
mac-address 0060.3ed9.7002	mac-address 00e0.f9d1.c102
ip address 172.16.1.129 255.255.255.128	ip address 172.16.1.129 255.255.255.128
ip helper-address 172.16.3.130	ip helper-address 172.16.3.130
interface Vlan30	interface Vlan30
mac-address 0060.3ed9.7003	mac-address 00e0.f9d1.c103

ip address 172.16.2.1 255.255.255.128 ip helper-address 172.16.3.130 interface Vlan40 mac-address 0060.3ed9.7004 ip address 172.16.2.129 255.255.255.128 ip helper-address 172.16.3.130 interface Vlan50 mac-address 0060.3ed9.7005 ip address 172.16.3.1 255.255.255.128 ip helper-address 172.16.3.130 interface Vlan60 mac-address 0060.3ed9.7006 ip address 172.16.3.129 255.255.255.240 ip helper-address 172.16.3.130 router ospf 10 router-id 1.1.1.1 log-adjacency-changes network 172.16.1.0 0.0.0.127 area 0 network 172.16.1.128 0.0.0.127 area 0 network 172.16.2.0 0.0.0.127 area 0 network 172.16.2.128 0.0.0.127 area 0 network 172.16.3.0 0.0.0.127 area 0 network 172.16.3.128 0.0.0.15 area 0 network 172.16.3.144 0.0.0.3 area 0 network 172.16.3.148 0.0.0.3 area 0 ip classless ip route 0.0.0.0 0.0.0.0 GigabitEthernet1/0/1 ip route 0.0.0.0 0.0.0.0 GigabitEthernet1/0/2 80 ip flow-export version 9 banner motd $no unauthorized access$ line con 0 password 7 0822455D0A16 login line aux 0 line vty 0 4 login local transport input ssh end	ip address 172.16.2.1 255.255.255.128 ip helper-address 172.16.3.130 interface Vlan40 mac-address 00e0.f9d1.c104 ip address 172.16.2.129 255.255.255.128 ip helper-address 172.16.3.130 interface Vlan50 mac-address 00e0.f9d1.c105 ip address 172.16.3.1 255.255.255.128 ip helper-address 172.16.3.130 interface Vlan60 mac-address 00e0.f9d1.c106 ip address 172.16.3.129 255.255.255.240 ip helper-address 172.16.3.130 router ospf 10 router-id 2.2.2.2 log-adjacency-changes network 172.16.1.0 0.0.0.127 area 0 network 172.16.1.128 0.0.0.127 area 0 network 172.16.2.0 0.0.0.127 area 0 network 172.16.2.128 0.0.0.127 area 0 network 172.16.3.0 0.0.0.127 area 0 network 172.16.3.128 0.0.0.15 area 0 network 172.16.3.152 0.0.0.3 area 0 network 172.16.3.156 0.0.0.3 area 0 ip classless ip route 0.0.0.0 0.0.0.0 GigabitEthernet1/0/1 ip route 0.0.0.0 0.0.0.0 GigabitEthernet1/0/2 80 ip flow-export version 9 banner motd $no unauthorized access$ line con 0 password 7 0822455D0A16 login line aux 0 line vty 0 4 login local transport input ssh end

Sales Switch	Hr Switch
hostname sales-sw enable password 7 0822455D0A16 no ip domain-lookup spanning-tree mode pvst spanning-tree extend system-id interface FastEthernet0/1 switchport mode trunk interface FastEthernet0/2 switchport mode trunk interface FastEthernet0/3 switchport access vlan 10 switchport mode access switchport port-security switchport port-security mac-address sticky switchport port-security mac-address sticky 0090.0CE4.7EC4 interface FastEthernet0/4 switchport access vlan 10 switchport mode access switchport port-security switchport port-security mac-address sticky switchport port-security mac-address sticky 00D0.FFE9.D47E interface FastEthernet0/5 switchport access vlan 10 switchport mode access interface range fa0/6- 24 switchport access vlan 10 switchport mode access switchport port-security switchport port-security mac-address sticky interface GigabitEthernet0/1 switchport access vlan 100 switchport mode access shutdown interface GigabitEthernet0/2 switchport access vlan 100 switchport mode access shutdown interface Vlan1 no ip address shutdown banner motd $no unauthorized access$ line con 0 password 7 0822455D0A16 login line vty 0 4 login line vty 5 15 login end	hostname hr-sw enable password 7 0822455D0A16 no ip domain-lookup spanning-tree mode pvst spanning-tree extend system-id interface FastEthernet0/1 switchport mode trunk interface FastEthernet0/2 switchport mode trunk interface range fa0/3- 24 switchport access vlan 20 switchport mode access interface GigabitEthernet0/1 switchport access vlan 100 switchport mode access shutdown interface GigabitEthernet0/2 switchport access vlan 100 switchport mode access shutdown interface Vlan1 no ip address shutdown banner motd $no unauthorized access$ line con 0 password 7 0822455D0A16 login line vty 0 4 login line vty 5 15 login end

Finance Switch	Admin Switch
hostname finance-sw enable password 7 0822455D0A16 no ip domain-lookup spanning-tree mode pvst spanning-tree extend system-id interface FastEthernet0/1 switchport mode trunk interface FastEthernet0/2 switchport mode trunk interface range fa0/3- 24 switchport access vlan 30 switchport mode access interface GigabitEthernet0/1 switchport access vlan 100 switchport mode access shutdown interface GigabitEthernet0/2 switchport access vlan 100 switchport mode access shutdown interface Vlan1 no ip address shutdown banner motd $no unauthorized access$ line con 0 password 7 0822455D0A16 login line vty 0 4 login line vty 5 15 login end	hostname admin-sw enable password 7 0822455D0A16 no ip domain-lookup spanning-tree mode pvst spanning-tree extend system-id interface FastEthernet0/1 switchport mode trunk interface FastEthernet0/2 switchport mode trunk interface range fa0/3- 24 switchport access vlan 40 switchport mode access interface GigabitEthernet0/1 switchport access vlan 100 switchport mode access shutdown interface GigabitEthernet0/2 switchport access vlan 100 switchport mode access shutdown interface Vlan1 no ip address shutdown banner motd $no unauthorized access$ line con 0 password 7 0822455D0A16 login line vty 0 4 login line vty 5 15 login end

Ict Switch	ServiceRoom Switch
hostname ict-sw enable password 7 0822455D0A16 no ip domain-lookup spanning-tree mode pvst spanning-tree extend system-id interface FastEthernet0/1 switchport mode trunk interface FastEthernet0/2 switchport mode trunk interface range fa0/3 -24 switchport access vlan 50 switchport mode access interface GigabitEthernet0/1 switchport access vlan 100 switchport mode access shutdown interface GigabitEthernet0/2 switchport access vlan 100 switchport mode access shutdown interface Vlan1 no ip address shutdown banner motd $no unauthorized access$ line con 0 password 7 0822455D0A16 login line vty 0 4 login line vty 5 15 login end	hostname sys-sw enable password 7 0822455D0A16 no ip domain-lookup spanning-tree mode pvst spanning-tree extend system-id interface FastEthernet0/1 switchport mode trunk interface FastEthernet0/2 switchport mode trunk interface range fa0/3 switchport access vlan 60 switchport mode access interface GigabitEthernet0/1 switchport access vlan 100 switchport mode access shutdown interface GigabitEthernet0/2 switchport access vlan 100 switchport mode access shutdown interface Vlan1 no ip address shutdown banner motd $no unauthorized access$ line con 0 password 7 0822455D0A16 login line vty 0 4 login line vty 5 15 login end

Brief

First we make intro configuration such as change hostname and enable the password to get access , then we create VLANs (10,20,30,40,50,60) after that we Assign VLANs to Switch Ports , finally Configure the Trunk Port and ssh

---

Port security

Port security is a feature on network switches that limits and controls the devices that can connect to a switch port. It is primarily used to prevent unauthorized access to a network by restricting which MAC addresses are allowed to communicate through specific switch ports.

Key Functions of Port Security :-

1. **MAC Address Limiting**: Limits the number of unique MAC addresses that can be learned on a port. This prevents network attacks like MAC flooding.
2. **MAC Address Static Assignment**: Administrators can manually specify which MAC addresses are allowed on a port, ensuring only known devices can access the network.
3. **Violation Actions**: When port security detects an unauthorized MAC address, different actions can be configured:
    - **Protect**: Ignores unauthorized MAC addresses but does not log or block them.
    - **Restrict**: Blocks unauthorized MAC addresses and logs the violation, but the port remains active for legitimate devices.
    - **Shutdown**: Disables the port entirely upon detecting a violation, requiring administrative action to bring the port back online.
4. **Dynamic Learning**: The switch can dynamically learn MAC addresses up to a configured limit, which helps in environments where devices may change but the number of connected devices remains consistent.

OSPF Concept

Open Shortest Path First (OSPF) is a link-state routing protocol developed as an alternative to the distance vector Routing Information Protocol (RIP). OSPF offers faster convergence and scales to larger network implementations, using the concept of areas for scalability. Links are interfaces on routers, network segments connecting two routers, or stub networks connected to a single router. All link-state information includes network prefix, prefix length, and cost. Routers exchange messages to convey routing information using five types of packets: the Hello packet, the database description packet, the link-state request packet, the link-state update packet, and the link-state acknowledgment packet. OSPF messages are used to create and maintain three OSPF databases: the adjacency database creates the neighbor table, the link-state database (LSDB) creates the topology table, and the forwarding database creates the routing table. The topology table is built using the Dijkstra SPF algorithm, which is based on the cumulative cost of reaching a destination. To maintain routing information, OSPF routers complete a generic link-state routing process to reach a state of convergence. Single-area OSPF is useful in smaller networks with few routers, while multi-area OSPF divides a large

routing domain into smaller areas for hierarchical routing. OSPFv3 is the OSPFv2 equivalent for exchanging IPv6 prefixes**.**

DNS Concept

DNS (Domain Name System) is a system that converts human-readable domain names into machine-readable IP addresses, enabling computers to locate and connect on a network. It works by initiating a domain name query, which is then sent to a recursive DNS resolver. If the resolver doesn't have the IP address cached, it queries a root DNS server, which directs the resolver to the appropriate Top-Level Domain (TLD) server. The authoritative name server for the domain stores the actual IP address, which the resolver retrieves. The recursive resolver returns the IP address to the user, allowing the browser to establish a connection to the web server hosting the website. DNS is crucial for making the internet user-friendly, supporting load balancing, email delivery, and content delivery networks. However, DNS is vulnerable to attacks such as DNS spoofing, DDoS attacks, and DNS hijacking.

NAT Concept

Private IPv4 addresses cannot be routed over the internet due to insufficient public IPv4 addresses. To allow a device with a private IPv4 address to access devices and resources outside of the local network, it must first be translated to a public address. NAT provides the translation of private addresses to public addresses, primarily used to conserve public IPv4 addresses. It allows networks to use private IPv4 addresses internally and provides translation to a public address only when needed. When an internal device sends traffic out of the network, the NAT-enabled router translates the internal IPv4 address of the device to a public address from the NAT pool.

NAT terminology is always applied from the perspective of the device with the translated address, with inside (the device being translated) and outside (the destination device). Local or global addresses are also used to addresses. There are two types of NAT: static NAT, which uses a one-to-one mapping of local and

global addresses, and dynamic NAT, which uses a pool of public addresses and assigns them on a first-come, first-served basis. Port Address Translation (PAT), also known as NAT overload, maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses, ensuring that devices use a different TCP port number for each session with a server on the internet. PAT translates most common protocols carried by IPv4 that do not use TCP or UDP as a transport layer protocol, such as ICMPv4.

ACL Concept

Several tasks performed by routers require the use of ACLs to identify traffic. An ACL is a series of IOS commands that are used to filter packets based on information found in the packet header. A router does not have any ACLs configured by default. However, when an ACL is applied to an interface, the router performs the additional task of evaluating all network packets as they pass through the interface to determine if the packet can be forwarded. An ACL uses a sequential list of permit or deny statements, known as ACEs. Cisco routers support two types of ACLs: standard ACLs and extended ACLs. An inbound ACL filters packets before they are routed to the outbound interface. If the packet is permitted by the ACL, it is then processed for routing. An outbound ACL filters packets after being routed, regardless of the inbound interface. When an ACL is applied to an interface, it follows a specific operating procedure:

1. The router extracts the source IPv4 address from the packet header.
2. The router starts at the top of the ACL and compares the source IPv4 address to each ACE in a sequential order.
3. When a match is made, the router carries out the instruction, either permitting or denying the packet, and the remaining ACEs in the ACL, if any, are not analyzed.
4. If the source IPv4 address does not match any ACEs in the ACL, the packet is discarded because there is an implicit deny ACE automatically applied to all ACLs.
