Efficient Network Setup for Small and Large Enterprises

Group member

1. Ahmed Mohamed Goumaa
2. Mahmed Alaa
3. Ahmed Diab
4. Ahmed Mahmoud
5. Mariam

supervisor

Eng : Mina Essam

Contents

Introduction to the Network Topology

This network topology represents a scalable and secure infrastructure designed to support a wide range of networking services and devices. It features a hierarchical architecture that integrates multiple routers, switches, servers, and endpoints to efficiently manage data traffic, provide network security, and ensure high availability. The topology is structured to meet the needs of both internal users and external connections, with distinct segments for data, management, and backup services.

Key Objectives of the Topology:

1. **Efficient Traffic Management**: The topology employs a hierarchical structure, allowing for the efficient flow of data between different network segments. Routers interconnect various subnetworks, ensuring data packets are appropriately routed based on predefined policies. Switches handle local area network (LAN) traffic, managing communications within each subnet through VLANs, reducing broadcast domains and enhancing security.
2. **Scalability and Flexibility**: Designed to be modular, this topology allows for easy expansion as network demands grow. New devices or network segments can be added without disrupting the existing infrastructure. The use of VLANs and routing protocols such as OSPF enables the network to scale efficiently, whether for a growing number of users, devices, or servers.
3. **Redundancy and High Availability**: To ensure minimal downtime, this topology incorporates redundancy at both the

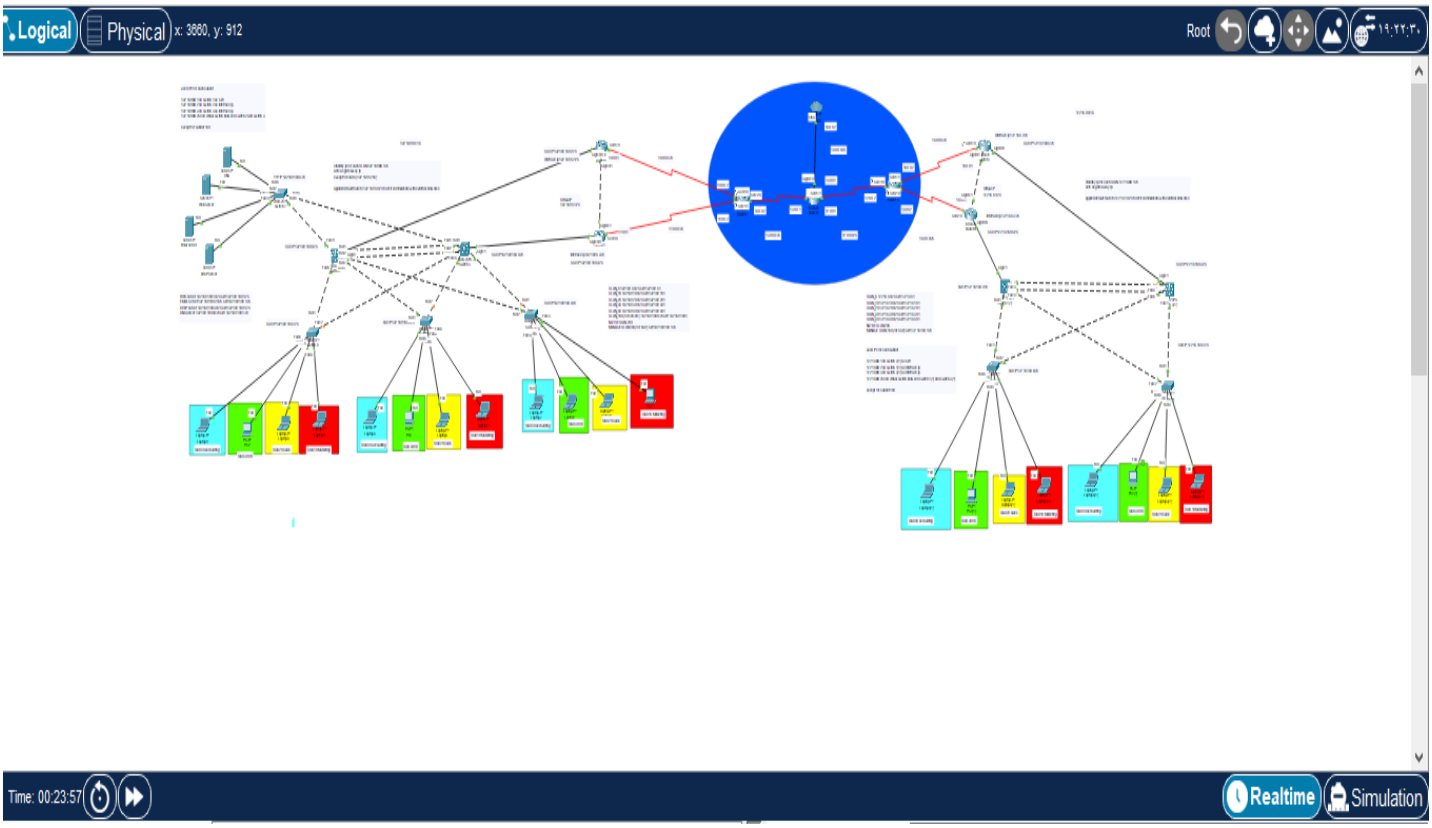
routing and switching levels. Protocols like HSRP (Hot Standby Router Protocol) ensure router failover, while link aggregation is implemented to provide redundancy on the switch-to-switch connections. These mechanisms reduce the risk of a single point of failure, ensuring business continuity and reliable network performance.

4. **Security and Traffic Segmentation**: Security is embedded into the topology with the deployment of firewalls that protect the boundary between the internal network and external connections. Firewalls are configured with access control lists (ACLs) and Network Address Translation (NAT) to monitor and regulate incoming and outgoing traffic. The use of VLANs helps in segmenting network traffic, providing an additional layer of security by isolating different departments or user groups, and preventing unauthorized access.
5. **Dynamic IP Management**: The topology includes dedicated DHCP servers that dynamically assign IP addresses to devices within the network. This reduces the administrative overhead of manual IP assignment and ensures efficient management of IP resources across the network.
6. **Monitoring and Management**: Network management protocols like SNMP (Simple Network Management Protocol) and Syslog are integrated into the topology to allow for real-time monitoring, logging, and management of network devices. This ensures that network administrators have visibility into network performance, can detect issues early, and quickly respond to any anomalies or security threats.

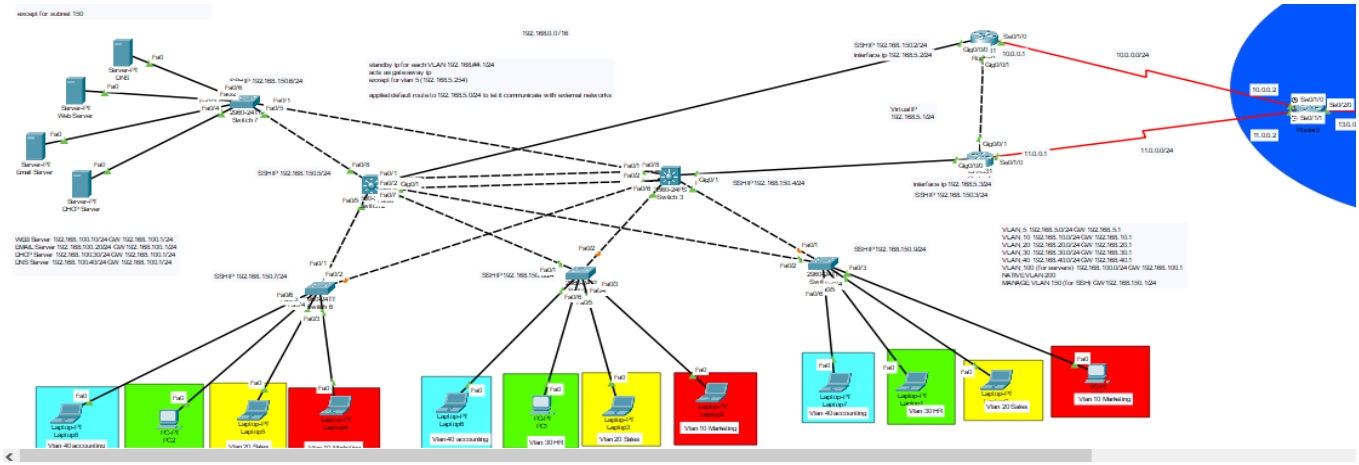
Core Components in the Topology:

1. **Routers**: Serve as gateways between different subnets and external networks, running dynamic routing protocols to ensure that data traffic is efficiently directed across the network.
2. **Switches**: Layer 2 and Layer 3 switches are used for traffic handling within local network segments, with VLANs configured to isolate and manage different types of traffic for better performance and security.
3. **Firewalls**: Protect the network perimeter and ensure that only authorized traffic is allowed through, using advanced filtering techniques such as ACLs, NAT, and stateful inspection.
4. **Servers**: Provide essential services, such as DNS for domain name resolution and DHCP for dynamic IP address assignment, ensuring smooth network operations.
5. **End Devices**: Includes user computers, printers, and other networked devices, which are connected through the switches and routers to access network resources.
6. **Backup and Failover Systems**: Built-in redundancy at key points in the network (routers, links, and switches) ensures that if any component fails, the network will automatically reroute traffic, minimizing downtime.
7. This network topology not only addresses the need for connectivity but also focuses on robust security, scalability, and high availability. Whether for small to medium

enterprises or large-scale organizations, this design can be tailored to support increasing network demands while ensuring data integrity and smooth communication.



1.Basic configuration of branch Cairo



1.1 Switch2 Configuration

Initially, the switch is accessed via the console and placed into privileged EXEC mode, followed by entering global configuration mode. The hostname is set to "Switch2," and the domain name is configured as "Depi.com" to enable SSH functionality. A password is established for console access, enhancing security, along with an enable secret for privileged EXEC mode. VLAN 150 is assigned the IP address 192.168.150.5 with a subnet mask of 255.255.255.0, and the interface is enabled. A local user account with administrative privileges is created for SSH access, while the VTY lines are configured to allow remote access. SSH version 2 is enabled to secure remote connections, and a default gateway of 192.168.5.1 is set to ensure external connectivity. Finally, the configuration is saved to retain all settings after a reboot, ensuring that Switch2 is properly configured for efficient network operations and management.

```
!
hostname switch2
!
!
enable secret 5 $1$mERr$3HhIgMGBA/9qNmgzccuxv0
!
!
!
!
!
ip routing
!
!
!
!
username admin privilege 15 secret 5 $1$mERr$3HhIgMGBA/9qNmgzccuxv0
!
!
!
!
!
!
!
!
!
!
ip ssh version 2
ip domain-name Depi.com
```

1.3 Switch3 Configuration

The setup for Switch3 emphasizes secure network management and connectivity. Following console access and entry into privileged EXEC mode, the hostname is defined as "Switch3," and the domain name "Depi.com" is established for SSH access. A console password and an enable secret are configured for security enhancement. VLAN 150 receives the IP address 192.168.150.4 with a subnet mask of 255.255.255.0, and the interface is enabled. A local admin user account is created for SSH, and remote access is allowed on the VTY lines. SSH version 2 is enabled for secure communication, while the default gateway of 192.168.5.1 facilitates external connectivity. The configuration is saved to ensure persistence after a reboot.

1.4 Switch4 Configuration

Switch4 is configured to support secure management and efficient network access. After entering privileged EXEC mode

through the console, the hostname is assigned as "Switch4," with the domain name "Depi.com" set for SSH functionality. A console password and an enable secret are created to bolster security. VLAN 150 is configured with the IP address 192.168.150.9 and a subnet mask of 255.255.255.0, and the interface is activated. An administrative user account is established for SSH access, and VTY lines are set to permit remote connections. SSH version 2 is enabled for encrypted access, and the default gateway of 192.168.5.1 ensures connectivity outside the local network. The configuration is saved to retain settings post-reboot.

1.5 Switch5 Configuration

The configuration of Switch5 prioritizes secure network management. After accessing the console and entering privileged EXEC mode, the hostname is designated as "Switch5," and the domain name "Depi.com" is set for SSH use. A password for the console and an enable secret are established for enhanced security. VLAN 150 is given the IP address 192.168.150.8 with a subnet mask of 255.255.255.0, and the interface is activated. A local user account with admin privileges is created for SSH, while remote access on the VTY lines is enabled. SSH version 2 is enabled for secure remote access, and a default gateway of 192.168.5.1 is configured for external connectivity. The configuration is saved to maintain settings after reboot.

1.6 Switch6 Configuration

For Switch6, the configuration is focused on secure management and connectivity. After entering privileged EXEC mode from the

console, the hostname is set to "Switch6," and the domain name "Depi.com" is configured for SSH support. A console password and an enable secret enhance security measures. VLAN 20 is assigned the IP address 192.168.150.7 with a subnet mask of 255.255.255.0, and the interface is enabled. An admin user account is created for SSH access, and VTY lines are set up for remote connections. SSH version 2 is activated to secure communications, with a default gateway of 192.168.5.1 allowing external access. The configuration is saved to ensure persistence after a reboot.

1.7 Switch7 Configuration

Switch7 is configured to ensure secure network management and connectivity. Accessing the console leads to privileged EXEC mode, where the hostname is set to "Switch7" and the domain name "Depi.com" is configured for SSH capabilities. A console password and an enable secret are established to improve security. VLAN 150 is assigned the IP address 192.168.150.6 with a subnet mask of 255.255.255.0, and the interface is activated. A local administrative account is created for SSH access, while VTY lines are configured to allow remote connections. SSH version 2 is enabled for secure access, and a default gateway of 192.168.5.1 is set for external connectivity. The configuration is saved to maintain settings after reboot.

2. What Is VLAN?

A virtual local area network (VLAN) is a virtualized connection that connects multiple devices and network nodes from different LANs into one logical network.

2.1 What are the types of VLAN?

VLANs are virtual local area networks (LANs) that enable multiple devices to communicate via wireless internet, allowing organizations to scale, segment, increase security measures, and decrease latency. These networks are essential for complex networking systems, allowing devices to communicate securely and efficiently.

- **Management VLAN**: A smaller network that manages traffic from devices, application logging, and monitoring, enhancing network security by minimizing broadcast radiation and restricting access.
- **Voice VLAN**: Configured for voice traffic, it preserves bandwidth and improves VoIP quality by prioritizing transmission for VoIP devices like IP phones.
- **Native VLAN**: Used for devices that don't support VLANs, this network carries untagged traffic on trunk links, serving as a common identifier.
- **Default VLAN**: A default network for all access ports until reassigned, allowing device connectivity. It cannot be renamed or deleted.
- **Data VLAN**: Segments the network into user and device groups, carrying only user-generated data and allowing administrators to group users across different switches.

2.2 Advantages of VLAN

- **Cost Savings:** VLANs allow devices to communicate through switches, reducing reliance on routers for external data exchange. This setup minimizes bottlenecks and enhances security, cutting costs and lowering latency.

- **Greater Flexibility:** VLANs can be easily configured based on port, subnet, or protocol, independent of physical connections. This flexibility facilitates collaboration and data sharing.

- **Simplified Administration and Enhanced Security:** VLANs require minimal monitoring and allow easy management of access controls. They enable segmentation for security without reconfiguration when users or devices change, saving time and resources.

2.3 configuration on switch4 and the same on switch5and switch6

2.3.1 Create VLANs and we name them so they can be more recognizable

```
Switch(config)#vlan 10
Switch(config-vlan)#name Marketing
Switch(config-vlan)#ex
Switch(config)#vlan 100
Switch(config-vlan)#name Servers
Switch(config-vlan)#ex
Switch(config)#vlan 150
Switch(config-vlan)#name Management
Switch(config-vlan)#ex
Switch(config)#vlan 200
Switch(config-vlan)#name Native
Switch(config-vlan)#ex
```

As you can see in the opposite configuration, we created VLANs 10,100,150,200
and named each one of them as VLAN 10 is called Marketing VLAN.

2.3.2 Decide which ports will be access or trunk ports

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#ex
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#ex
```

On an interface we can use switchport mode command that we can choose between different modes as there are four modes.

- **Access mode** is used to assign ports to specific VLAN.
- **Trunk mode** is used between ports that connect switches to tag each VLAN's traffic.
- **Dynamic Auto and Dynamic desirable** these two modes are used while DTP (Dynamic Trunk Protocol) is enabled, it gives the switches the ability to assign port automatically to operate as trunk port if there at least one port is Dynamic desirable from any side of the connection link.

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
5    VLAN0005                         active
10   Marketing                        active    Fa0/1
100  Servers                          active
150  Management                       active
200  Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

2.3.2 Apply security configuration on ports

1. Shut down unused ports by using shutdown command on interface

```
Switch(config)#interface range fastEthernet 0/3-24, gigabitEthernet 0/1-2
Switch(config-if-range)#shutdown
```

```
Switch#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual down                  down
FastEthernet0/2        unassigned      YES manual down                  down
FastEthernet0/3        unassigned      YES manual administratively down down
FastEthernet0/4        unassigned      YES manual administratively down down
FastEthernet0/5        unassigned      YES manual administratively down down
FastEthernet0/6        unassigned      YES manual administratively down down
FastEthernet0/7        unassigned      YES manual administratively down down
FastEthernet0/8        unassigned      YES manual administratively down down
FastEthernet0/9        unassigned      YES manual administratively down down
FastEthernet0/10       unassigned      YES manual administratively down down
FastEthernet0/11       unassigned      YES manual administratively down down
FastEthernet0/12       unassigned      YES manual administratively down down
FastEthernet0/13       unassigned      YES manual administratively down down
FastEthernet0/14       unassigned      YES manual administratively down down
FastEthernet0/15       unassigned      YES manual administratively down down
FastEthernet0/16       unassigned      YES manual administratively down down
FastEthernet0/17       unassigned      YES manual administratively down down
FastEthernet0/18       unassigned      YES manual administratively down down
FastEthernet0/19       unassigned      YES manual administratively down down
FastEthernet0/20       unassigned      YES manual administratively down down
FastEthernet0/21       unassigned      YES manual administratively down down
FastEthernet0/22       unassigned      YES manual administratively down down
FastEthernet0/23       unassigned      YES manual administratively down down
FastEthernet0/24       unassigned      YES manual administratively down down
GigabitEthernet0/1     unassigned      YES manual administratively down down
GigabitEthernet0/2     unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
```

2.Disable DTP on every used port and change the native VLAN on trunk ports to unused VLAN

```
Switch(config)#interface range fastEthernet 0/2
Switch(config-if-range)#switchport nonegotiate
Switch(config-if-range)#switchport trunk native vlan 200
Switch(config-if-range)#ex
Switch(config)#
```

i. Due to the default mode on switches is dynamic auto we need to disable DTP to ensure that the port won't operate automatically as trunk port, so we use the command switchport nonegotiate
ii. Due to switches assign all the ports to the native VLAN as default (VLAN 1), and the native VLAN is the only VLAN that its traffic isn't tagged, so we need to change the native VLAN number to prevent any possible attacks.

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/2       on           802.1q         trunking      200

Port        Vlans allowed on trunk
Fa0/2       1-1005

Port        Vlans allowed and active in management domain
Fa0/2       1,5,10,100,150,200

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/2       none
```

DTP configuration options are as follows:

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited connectivity
Access	Access	Access	Limited connectivity	Access

3.Apply port-security on access ports

iii. Enable port-security on an interface by using switchport port-security command
iv. The command switchport port-security maximum 4 is used to set the maximum number of MAC addresses allowed on a port.
v. If the MAC address of a device attached to a port differs from the list of secure addresses, then a port violation occurs and the port enters the error-disabled state, there are three modes of violation
    1. Shutdown mode the port transitions to the error-disabled state immediately, an administrator must re-enable it by entering the shutdown and no shutdown commands.
    2. Restrict mode the port drops packets with unknown source addresses, this mode causes the Security Violation counter to increment and generates a syslog message, until you delete a sufficient number of secured MAC addresses to drop below the maximum value or increase the maximum value.
    3. Protect mode This is the least secure of the security violation modes. The port drops packets with unknown MAC source addresses, until you delete a sufficient number of secured MAC addresses to drop

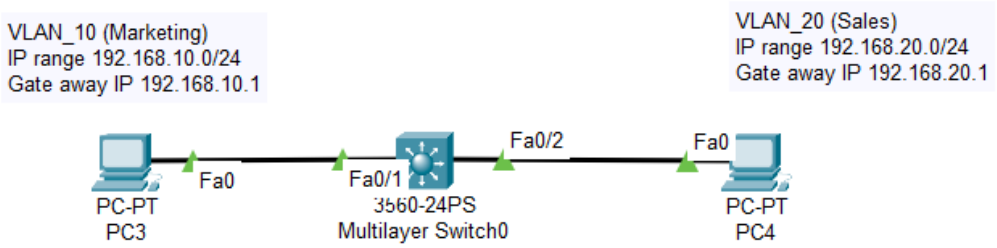
below the maximum value or increase the maximum value.

vi. Use aging to remove secure MAC addresses on a secure port without manually deleting the existing secure MAC addresses, and it can be used by setting the aging time for static and dynamic secure addresses on a port and two types of aging are supported per port

1. Absolute The secure addresses on the port are deleted after the specified aging time.
2. Inactivity the secure addresses on the port are deleted if they are inactive for a specified time.

2.3.3 Inter VLAN Routing

To do Inter VLAN Routing we need to do a couple of things first on an end device and a Layer 3 switch from this topology



2.4 Create VLANs on the switch.

```
Switch(config)#vlan 10
Switch(config-vlan)#name Marketing
Switch(config-vlan)#ex
Switch(config)#vlan 20
Switch(config-vlan)#name Sales
Switch(config-vlan)#ex
```

2.5 Assign VLANs to the appropriate interfaces.

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#ex
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#ex
```

2.6 Adjust an IP for each SVI (Switch Virtual Interfaces) to be the gateaway for end devices

```
Switch(config)#interface vlan 10
Switch(config-if)#ip address 192.168.10.1 255.255.255.0
Switch(config-if)#ex
Switch(config)#interface vlan 20
Switch(config-if)#ip address 192.168.20.1 255.255.255.0
Switch(config-if)#ex
```

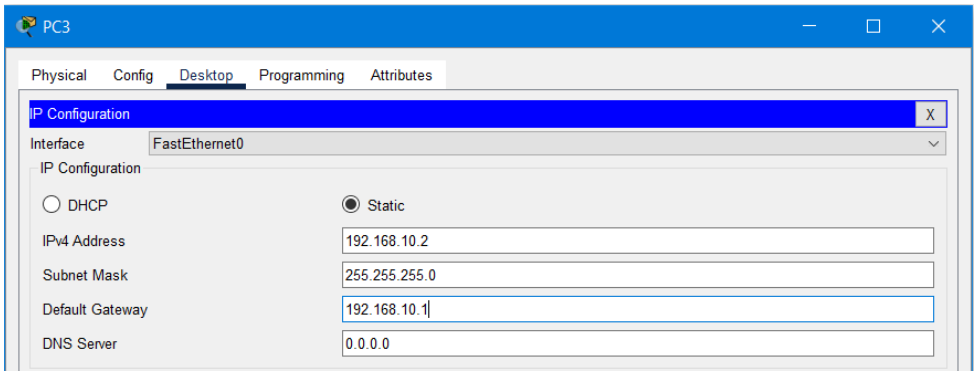
2.7 Verify (VLANs creation, Access port, SVI's IP) by using show vlan brief and show ip interface brief commands.

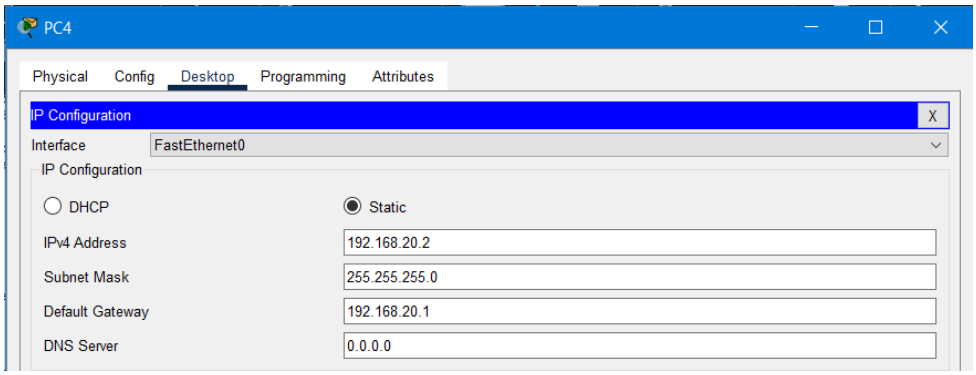
```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   Marketing                        active    Fa0/1
20   Sales                            active    Fa0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES unset  up                    up
FastEthernet0/2        unassigned      YES unset  up                    up
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  down                  down
FastEthernet0/6        unassigned      YES unset  down                  down
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
Vlan1                  unassigned      YES unset  administratively down down
Vlan10                 192.168.10.1    YES manual up                    up
Vlan20                 192.168.20.1    YES manual up                    up
```

2.8 Apply the command ip routing on global configuration mode to allow the routing between the two VLANs and verify the networks that the layer 3 switch can deal with.

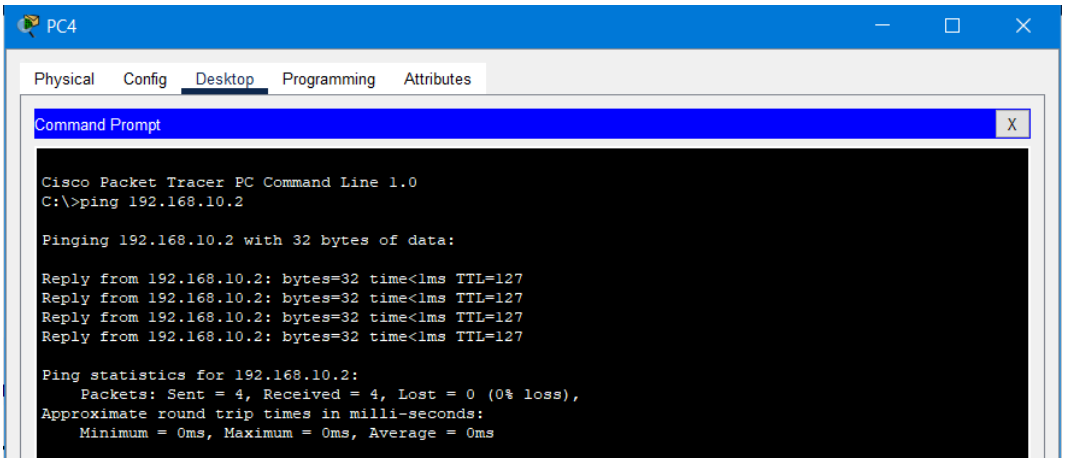
```
Switch(config)#ip routing
Switch(config)#
Switch(config)#
Switch(config)#ip routing
Switch(config)#ex
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.10.0/24 is directly connected, Vlan10
C    192.168.20.0/24 is directly connected, Vlan20
```

2.9 configure an IP and Gate away statically for End Devices





2.10 Test the Connectivity between the End Devices



3.What is STP and how does it work?

Spanning Tree Protocol (STP) is a Layer 2 network protocol used to prevent looping within a network topology. STP was created to avoid the problems that arise when computers exchange data on a local area network () that contains redundant paths. If the flow of traffic is not carefully monitored and controlled, the data can be caught in a loop that circles around network segments, affecting performance and bringing traffic to a near halt

3.2 What are STP port states?

When STP is enabled on a network bridge, each port is set to one of five states to control frame forwarding:

1. **Disabled.** The port does not participate in frame forwarding or STP operations.

2. **Blocking.** The port does not participate in frame forwarding and discards frames received from the attached network segment. However, the port continues to listen for and process BPDUs.
3. **Listening.** From the blocking state, the port transitions to the listening state. The port discards frames from the attached network segment or forwarded from another port. However, it receives BPDUs and redirects them to the switch module for processing.
4. **Learning.** The port moves from the listening state to the learning state. It listens for and processes BPDUs but discards frames from the attached network segment or forwarded from another port. It also starts updating the address table with the information it's learned. In addition, it processes user frames but does not forward those frames.
5. **Forwarding.** The port moves from the learning state to the forwarding state and starts forwarding frames across the network segments. This includes frames from the attached network segment and those forwarded from another port. The port also continues to receive and process BPDUs, and the address table continues to be updated.

3.3 What are STP modes?

To understand STP modes, it helps to go back to STP's beginnings. The original spanning tree protocol and algorithm were invented in 1985 by Radia Perlman when she was working at Digital Equipment Corporation. Spanning tree protocols were later standardized by the Institute of Electrical and Electronics Engineers (IEEE). Since

then, the protocol has evolved in a number of ways, and new variations have been introduced.

The most common spanning tree protocols

PROTOCOL	IEEE STANDARD	SWITCH	DESCRIPTION
Spanning Tree Protocol (STP)	IEEE 802.1D	stp	The original STP version
Rapid STP (RSTP)	IEEE 802.1w	rstp	An evolution of STP 802.1D that addresses the STP convergence time gap issue with enhanced BPDU exchange
Multiple STP (MSTP)	IEEE 802.1s	mstp	A format for mapping multiple VLANs into the same spanning tree to reduce processing on the switch
Per-VLAN Spanning Tree (PVST+)	Cisco protocol based on 802.1D	pvst	An 802.1D enhancement that provides a separate STP instance for each VLAN configured in the network
Rapid PVST+	Cisco protocol based on 802.1w	rapid-pvst	An 802.1w enhancement that provides a separate STP instance for each VLAN, enabling faster convergence times

3.4 configuration on switch 2 and switch 3

The switch is configured to use Rapid PVST for faster network convergence and improved VLAN management. VLANs 1-4094 are prioritized to 4096, ensuring the switch acts as the root bridge for these VLANs. Portfast and BPDU guard are enabled to accelerate port transitions and prevent network loops. Additionally, IP routing is activated, allowing the switch to forward packets between different IP networks.

```
switch2(config)#spanning-tree mode rapid-pvst
switch2(config)#spanning-tree vlan 1-4094 priority 4096
switch2(config)#spanning-tree portfast default
switch2(config)#spanning-tree portfast bpduguard default
switch2(config)#
switch2(config)#
switch2(config)#ip routing
```

4.1 What is EtherChannel?

EtherChannel is a port-channel architecture or port-link aggregation technology that is predominantly utilized on Cisco switches. For the aim of providing fault-tolerance and fast connectivity between switches, routers, and servers, it enables the grouping of numerous physical Ethernet links into one logical Ethernet link.

4.2 Purpose of EtherChannel in Networking

EtherChannel's primary function is to provide redundant, high-speed connections between network devices. Key benefits include:

1. **Increased Bandwidth**: Aggregates multiple links into one logical connection. For example, four 100 Mbps links become a single 400 Mbps link.
2. **Improved Redundancy**: Ensures fault tolerance by switching traffic to active links if one fails, maintaining connectivity without dropping data.
3. **Enhanced Load Balancing**: Distributes traffic across multiple links based on criteria like MAC or IP addresses, reducing bottlenecks and improving performance.

4.3 How EtherChannel Works

EtherChannel uses two main protocols:

1. **PAgP (Port Aggregation Protocol)**: Cisco-proprietary protocol with two modes—Desirable (actively requests EtherChannel) and Auto (waits passively for a request).

2. **LACP (Link Aggregation Control Protocol)**: IEEE standard used across different vendor devices. It has three modes—Active (actively requests), Passive (waits), and On (assumes EtherChannel without negotiation).

4.4 configuration on switch 2 and switch 3

"There are two EtherChannel groups defined, each consisting of two physical ports. Group 1, named "Po1," is in a suspended state, while Group 2, named "Po2," is active and in use. Both groups are configured using the Port Aggregation Protocol (PAgP) in symmetric mode.

```
switch2#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)           -      Fa0/1(P) Fa0/2(P)
2      Po2(SD)           -      Fa0/3(D) Fa0/4(D)
switch2#
```

5.1 What is HSRP?

HSRP (Hot Standby Router Protocol) is a Cisco proprietary protocol used in networks to provide high availability and redundancy for IP routing. Its primary function is to ensure continuous network service in case the primary router (or gateway) fails by automatically switching to a backup router.

5.2 Key Features of HSRP:

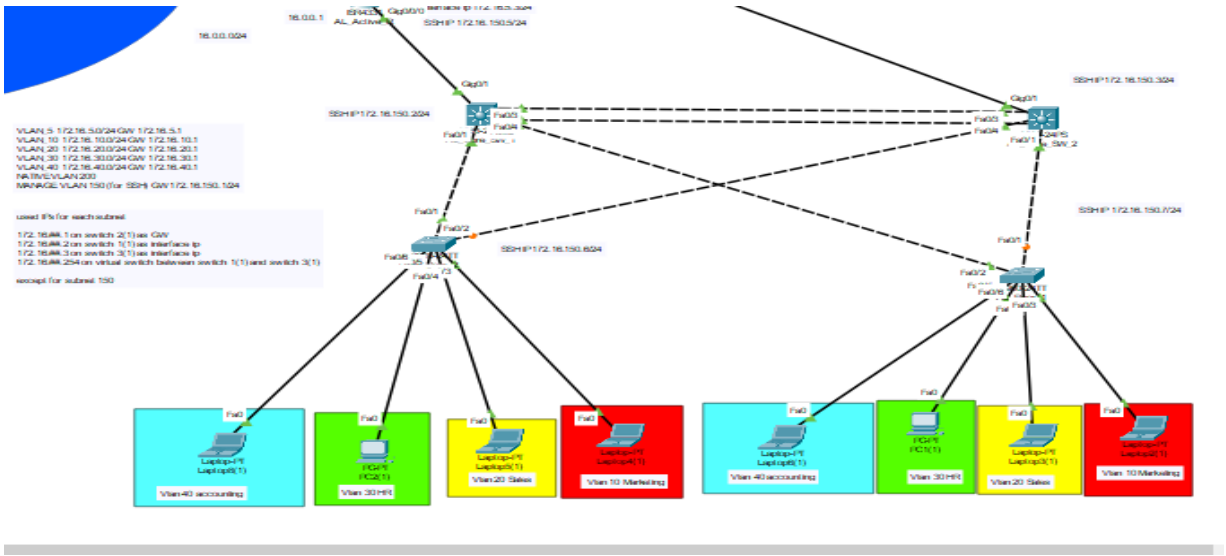
1. **Redundancy**: HSRP enables the configuration of a group of routers to act as a single virtual router (gateway) for devices on a local network. One router is elected as the **active router**, while another is designated as the **standby router**.
2. **Failover**: If the active router fails or becomes unreachable, the standby router takes over without any noticeable disruption to the end-users. This provides seamless network availability.
3. **Virtual IP and MAC Address**: HSRP assigns a **virtual IP address** that acts as the default gateway for network hosts. The active router responds to ARP requests using a **virtual MAC address**, ensuring that devices don't need to change their configurations if a failover occurs.
4. **Priority and Preemption**: Routers in the HSRP group are assigned **priority values**. The router with the highest priority becomes the active router. Preemption allows a router with a higher priority to take over as the active router if it becomes available again after a failure.

5.3 HSRP configuration

```
switch2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl5         5    110 P Active   local           192.168.5.4     192.168.5.254
Vl10        10   110 P Active   local           192.168.10.3    192.168.10.1
Vl20        20   110 P Active   local           192.168.20.3    192.168.20.1
Vl30        30   100 P Standby  192.168.30.3    local           192.168.30.1
Vl40        40   100 P Standby  192.168.40.3    local           192.168.40.1
Vl100       100  110 P Active   local           192.168.100.3   192.168.100.1
Vl150       150  100 P Listen   192.168.150.5   192.168.150.4   192.168.150.1
switch2#
```

```
Router0#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0/0    1    110 P Active   local           192.168.5.2     192.168.5.1
Router0#
```

6. configuration of switching on branch ALX



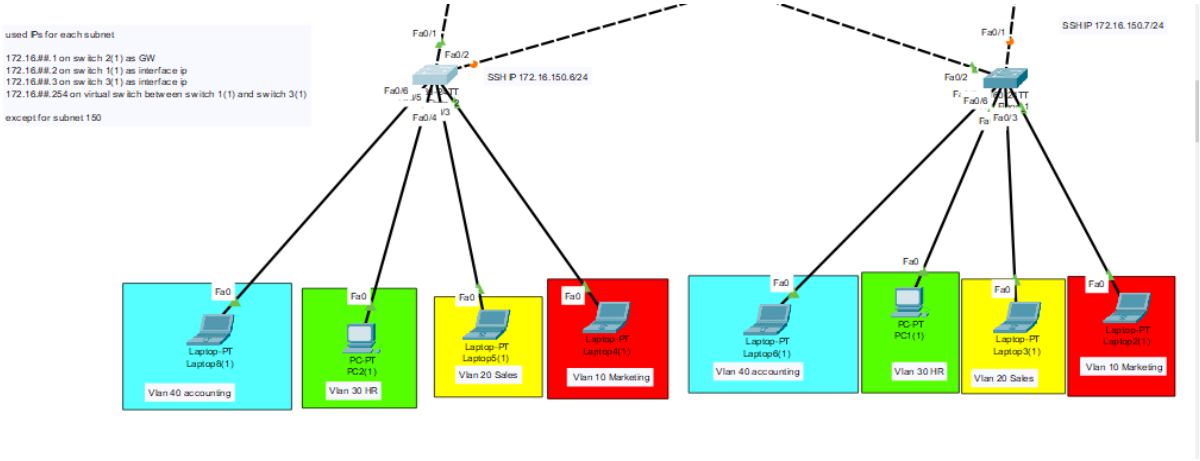
In this network topology, we will configure the four switches to support VLANs, inter-VLAN routing, and establish a Port Channel (EtherChannel) for link aggregation between two of the switches.

Basic Configuration for Each Switch

The device's hostname is set to "Floor_1", indicating the floor or location where the switch might be deployed. Security measures are implemented, including an enable secret password that is encrypted with an algorithm to ensure the integrity and confidentiality of the device's privileged access.
SSH (Secure Shell) is enabled with SSH version 2 for secure remote management of the device, which is configured with the domain name Alex.com. Additionally, a local user account with the username "admin" is created, secured by an encrypted password. This configuration emphasizes security best practices by using encrypted passwords and SSH instead of less secure options like Telnet, making the switch management more secure from external attacks.

```
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Floor_1
!
enable secret 5 $1$mERr$3HhIgMGBA/9qNmgzccuxv0
!
!
!
ip ssh version 2
ip domain-name Alex.com
!
username admin secret 5 $1$mERr$3HhIgMGBA/9qNmgzccuxv0
!
!
.
hostname Floor_2
!
enable secret 5 $1$mERr$3HhIgMGBA/9qNmgzccuxv0
!
!
!
ip ssh version 2
ip domain-name Alex.com
!
username admin secret 5 $1$mERr$3HhIgMGBA/9qNmgzccuxv0
'
```

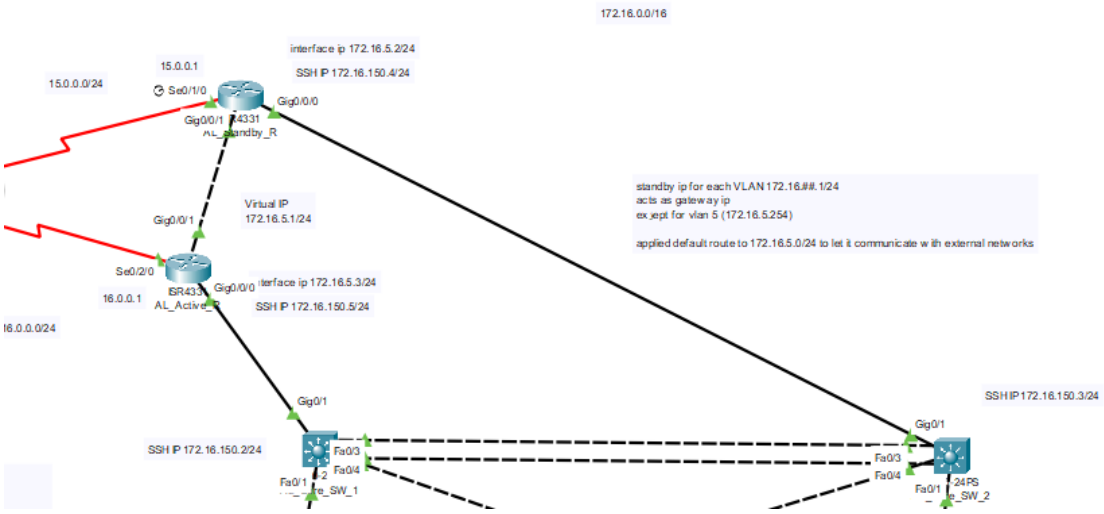
6.1 vlan configuration



a network setup using VLANs (Virtual Local Area Networks) to segregate traffic within a switch-based architecture. Various devices, such as laptops and PCs, are assigned to different VLANs based on their department or function. VLAN 40 is assigned to **Accounting**, VLAN 30 to **HR**, VLAN 20 to **Sales**, and VLAN 10 to **Marketing**. Each VLAN has a designated subnet to maintain logical separation.

For instance, VLAN 40 (Accounting) uses the subnet **172.16.40.0/24**, while VLAN 10 (Marketing) uses **172.16.10.0/24**. The switches are configured with appropriate VLAN interfaces (SVIs) to route traffic between VLANs, using different gateway addresses for each subnet. SSH access is enabled via the **172.16.150.6/24** IP address, allowing remote management of the device. The network setup efficiently manages traffic and ensures separation between different departments, promoting better network organization, security, and resource management.

6.2 HSRP and Etherchannel configuration



EtherChannel is used to bundle multiple physical links into a single logical link, increasing bandwidth and providing redundancy. In this setup, we'll configure EtherChannel between Switch 1 (SW1) and Switch 2 (SW2) using two interfaces.

Steps for Port Channel Configuration on SW1 and SW2

1. Configure Port Channel on SW1

Switch1(config)# interface range gigabitEthernet 0/1 - 2

Switch1(config-if-range)# channel-group 1 mode active

Switch1(config-if-range)# exit

Switch1(config)# interface port-channel 1

Switch1(config-if)# switchport mode trunk

Switch1(config-if)# switchport trunk allowed vlan 5,10,20,30,50

2. Configure Port Channel on SW2

```
Switch2(config)# interface range gigabitEthernet 0/1 - 2
Switch2(config-if-range)# channel-group 1 mode active
Switch2(config-if-range)# exit
Switch2(config)# interface port-channel 1
Switch2(config-if)# switchport mode trunk
Switch2(config-if)# switchport trunk allowed vlan 5,10,20,30,50
```

Explanation:

- Channel-group 1 mode active: This command enables LACP (Link Aggregation Control Protocol) on both interfaces to form an EtherChannel.
- Port-channel 1: The virtual logical interface created after bundling the two physical links.
- Trunk Mode: Configured on the Port Channel to allow multiple VLANs over the link between SW1 and SW2.

HSRP is used for providing network redundancy. In this diagram, HSRP ensures that if the primary router (R1) fails, a secondary router (R2 or R3) will take over, allowing uninterrupted network services.

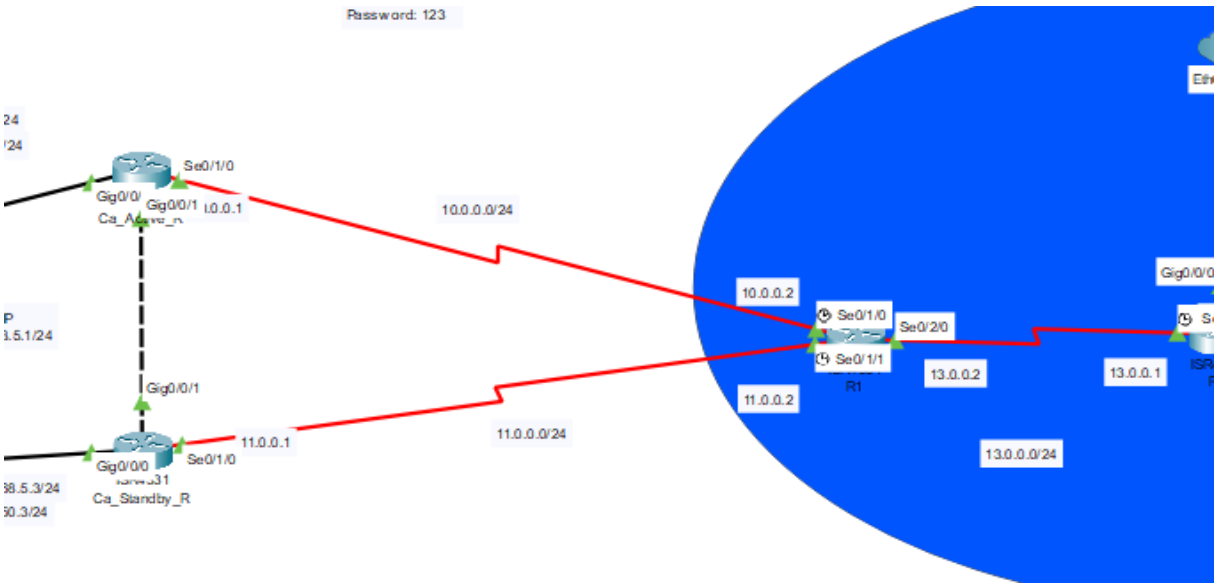
How HSRP Works:

- **Virtual IP Address**: HSRP assigns a virtual IP address shared between multiple routers. End devices use this virtual IP as their gateway, unaware of which physical router is actively routing traffic.

- **Priority**: Each router is assigned a priority. The router with the highest priority becomes the active router. If the active router fails, the router with the next highest priority takes over.
- **HSRP Groups**: Routers are configured in HSRP groups, where they communicate with each other to decide which one should be active or standby.

---

1. Ospf protocol and configuration



OSPF (Open Shortest Path First) is a dynamic, link-state routing protocol used in IP networks to determine the most efficient path for data to travel between devices. OSPF operates within an Autonomous System (AS) and is based on the Dijkstra algorithm, which calculates the shortest path to each network node. It uses the concept of areas to limit the propagation of routing updates

and reduce network congestion. The OSPF protocol ensures that routers maintain a synchronized view of the network's topology through regular exchanges of link-state advertisements (LSAs).

more information

Benefits of OSPF:

- Scalability: OSPF supports large, complex networks by organizing them into hierarchical areas, reducing the routing table size and update overhead.
- Fast Convergence: OSPF quickly detects changes in the network and recalculates routes to ensure minimal downtime, making it ideal for networks requiring high availability.
- Load Balancing: OSPF can support equal-cost multi-path (ECMP) routing, allowing traffic to be distributed over multiple best paths, improving bandwidth utilization.
- VLSM and CIDR Support: It allows the use of Variable Length Subnet Masking (VLSM) and Classless Inter-Domain Routing (CIDR), optimizing IP address usage.
- Security: OSPF supports authentication to secure routing updates between routers, preventing unauthorized routing changes.

Using OSPF:

OSPF is typically configured on routers in environments where there are multiple networks or complex topologies. To use OSPF, network administrators define OSPF areas and assign networks or interfaces to these areas. OSPF routers exchange LSAs with each

other, build a link-state database, and use the Dijkstra algorithm to compute the shortest path to each destination. For example, an administrator may configure OSPF with the command router ospf <process-id>, followed by specifying the network ranges with network commands and defining OSPF area boundaries to control traffic flow and optimize network performance.

By using OSPF, businesses can ensure that their networks adapt dynamically to changes while maintaining efficient, loop-free routing across multiple interconnected devices.

OSPF Configuration

- **On layer 3 switches**

switch2(config)#	ip routing
switch2(config)#	router ospf 1
switch2(config-router)#	network 192.168.5.0 0.0.0.255 area 0
switch2(config-router)#	network 192.168.5.0 0.0.0.255 area 0
switch2(config-router)#	network 192.168.10.0 0.0.0.255 area 0
switch2(config-router)#	network 192.168.20.0 0.0.0.255 area 0
switch2(config-router)#	network 192.168.30.0 0.0.0.255 area 0
switch2(config-router)#	network 192.168.40.0 0.0.0.255 area 0
switch2(config-router)#	network 192.168.100.0 0.0.0.255 area 0
switch2(config-router)#	network 192.168.150.0 0.0.0.255 area 0

- **On routers**

Router0

```
Router0(config-router)#router ospf 1
Router0(config-router)#network 192.168.5.0 0.0.0.255 area 0
Router0(config-router)#network 10.0.0.0 0.0.0.255 area 0
Router0(config-router)#network 192.168.150.0 0.0.0.255 area 0
Router0(config-router)#exit
```

Router 1

```
Router1(config)#router ospf 1
Router1(config-router)#network 192.168.5.0 0.0.0.255 area 0
Router1(config-router)#network 11.0.0.0 0.0.0.255 area 0
Router1(config-router)#network 192.168.150.0 0.0.0.255 area 0
Router1(config-router)#exit
```

Router 2

```
Router2(config)#router ospf 1
Router2(config-router)#network 10.0.0.0 0.0.0.255 area 0
Router2(config-router)#network 11.0.0.0 0.0.0.255 area 0
Router2(config-router)#network 13.0.0.0 0.0.0.255 area 0
Router2(config-router)#exit
```

Router 3

```
Router3#show ip route o
     10.0.0.0/24 is subnetted, 1 subnets
O       10.0.0.0 [110/128] via 13.0.0.2, 01:55:50, Serial0/1/0
     11.0.0.0/24 is subnetted, 1 subnets
O       11.0.0.0 [110/128] via 13.0.0.2, 01:55:50, Serial0/1/0
O    192.168.5.0 [110/129] via 13.0.0.2, 01:55:10, Serial0/1/0
O    192.168.10.0 [110/130] via 13.0.0.2, 01:28:45, Serial0/1/0
O    192.168.20.0 [110/130] via 13.0.0.2, 01:31:45, Serial0/1/0
O    192.168.30.0 [110/130] via 13.0.0.2, 01:55:10, Serial0/1/0
O    192.168.40.0 [110/130] via 13.0.0.2, 01:55:10, Serial0/1/0
O    192.168.100.0 [110/130] via 13.0.0.2, 01:55:10, Serial0/1/0
O    192.168.150.0 [110/130] via 13.0.0.2, 01:55:10, Serial0/1/0
     200.200.200.0/32 is subnetted, 1 subnets
O       200.200.200.1 [110/65] via 13.0.0.2, 01:55:50, Serial0/1/0
```

6)Access list

- To allow VLANS 10 and 20 in both networks to communicate with each other only.

- VLANS 30 and 40 are not allowed to communicate with VLANS 10 and 20.
- VLANS 10 and 20 communicate with other Vlans in the network.

ACL deny between VLANs in LAN 2

deny ip 172.16.10.0 0.0.0.255 172.16.30.0 0.0.0.255

deny ip 172.16.10.0 0.0.0.255 172.16.40.0 0.0.0.255

deny ip 172.16.20.0 0.0.0.255 172.16.30.0 0.0.0.255

deny ip 172.16.20.0 0.0.0.255 172.16.40.0 0.0.0.255

deny ip 172.16.30.0 0.0.0.255 172.16.10.0 0.0.0.255

deny ip 172.16.30.0 0.0.0.255 172.16.20.0 0.0.0.255

deny ip 172.16.40.0 0.0.0.255 172.16.10.0 0.0.0.255

deny ip 172.16.40.0 0.0.0.255 172.16.20.0 0.0.0.255

ACL deny between VLANs in LAN 1

deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255

deny ip 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255

deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255

deny ip 192.168.20.0 0.0.0.255 192.168.40.0 0.0.0.255

deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255

deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255

deny ip 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.255

deny ip 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255

ACL VLAN isolation between the two LANs

deny ip 192.168.10.0 0.0.0.255 172.16.30.0 0.0.0.255

deny ip 192.168.10.0 0.0.0.255 172.16.40.0 0.0.0.255

deny ip 192.168.20.0 0.0.0.255 172.16.30.0 0.0.0.255

deny ip 192.168.20.0 0.0.0.255 172.16.40.0 0.0.0.255

deny ip 172.16.10.0 0.0.0.255 192.168.30.0 0.0.0.255

deny ip 172.16.10.0 0.0.0.255 192.168.40.0 0.0.0.255

deny ip 172.16.20.0 0.0.0.255 192.168.30.0 0.0.0.255

deny ip 172.16.20.0 0.0.0.255 192.168.40.0 0.0.0.255

deny ip 192.168.30.0 0.0.0.255 172.16.10.0 0.0.0.255

deny ip 192.168.30.0 0.0.0.255 172.16.20.0 0.0.0.255

deny ip 192.168.40.0 0.0.0.255 172.16.10.0 0.0.0.255

deny ip 192.168.40.0 0.0.0.255 172.16.20.0 0.0.0.255

deny ip 172.16.30.0 0.0.0.255 192.168.10.0 0.0.0.255

deny ip 172.16.30.0 0.0.0.255 192.168.20.0 0.0.0.255

deny ip 172.16.40.0 0.0.0.255 192.168.10.0 0.0.0.255

deny ip 172.16.40.0 0.0.0.255 192.168.20.0 0.0.0.255

---

permit other subnets to communicate with each other

LAN 1

permit ip any 192.168.10.0 0.0.0.255

permit ip 192.168.10.0 0.0.0.255 any

permit ip any 192.168.20.0 0.0.0.255

permit ip 192.168.20.0 0.0.0.255 any

permit ip any 192.168.30.0 0.0.0.255

permit ip 192.168.30.0 0.0.0.255 any

permit ip any 192.168.40.0 0.0.0.255

permit ip 192.168.40.0 0.0.0.255 any

LAN 2

permit ip any 172.16.10.0 0.0.0.255

permit ip 172.16.10.0 0.0.0.255 any

permit ip any 172.16.20.0 0.0.0.255

permit ip 172.16.20.0 0.0.0.255 any

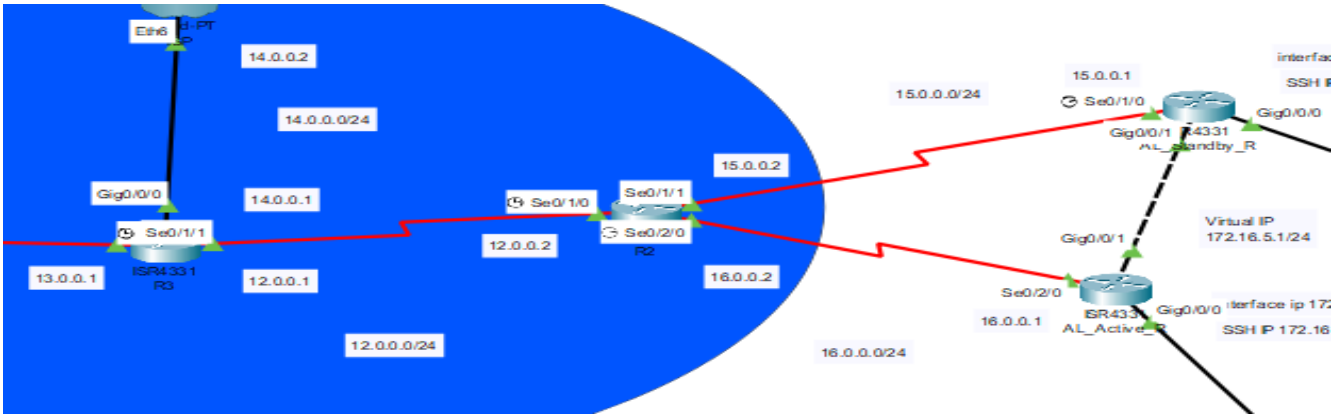
permit ip any 172.16.30.0 0.0.0.255

permit ip 172.16.30.0 0.0.0.255 any

permit ip any 172.16.40.0 0.0.0.255

permit ip 172.16.40.0 0.0.0.255 any

2.EIGRP Protocol



EIGRP (Enhanced Interior Gateway Routing Protocol) is an advanced hybrid routing protocol developed by Cisco that combines features of both distance-vector and link-state protocols. It is designed to efficiently manage the routing of IP traffic across a network by utilizing the Diffusing Update Algorithm (DUAL). This algorithm allows routers to rapidly identify the best path for traffic while maintaining a backup route in case the primary path fails, ensuring fast network convergence.

One of EIGRP's unique characteristics is its classless routing capability, which enables the use of Variable Length Subnet Masks (VLSM) and Classless Inter-Domain Routing (CIDR). EIGRP only exchanges updates when necessary and sends only the changes, rather than entire routing tables, making it highly efficient in terms of bandwidth usage.

Key Benefits of EIGRP

- Fast Convergence: One of the primary benefits of EIGRP is its fast convergence time. The protocol can quickly recalculate

routes when there's a network topology change, ensuring minimal disruption in network communication. The use of the DUAL algorithm allows for the immediate use of a backup route if the primary route fails, ensuring minimal downtime.

- Low Bandwidth Usage: EIGRP minimizes bandwidth consumption by sending incremental updates only when a topology change occurs, rather than broadcasting full routing tables at regular intervals. This makes it more efficient than traditional distance-vector protocols, which periodically send full updates.
- Scalability: EIGRP can scale to support large networks with many routers and thousands of routes. It allows network administrators to divide the network into multiple autonomous systems (AS), enabling more efficient routing management. It also works well in both LAN and WAN environments.
- Support for Multiple Network Protocols: Although primarily used with IP networks, EIGRP can also route other protocols like IPv6, IPX, and AppleTalk, making it versatile in mixed network environments.
- Load Balancing: EIGRP supports both equal-cost and unequal-cost load balancing, which means it can distribute traffic across multiple paths, even when the paths have different bandwidths. This feature helps optimize network traffic and prevent bottlenecks by utilizing available resources more effectively.
- Flexible Metric Calculation: EIGRP uses a composite metric based on bandwidth, delay, reliability, and load.

Administrators can adjust these metric parameters to influence path selection, offering better control over how traffic flows through the network.

- Reliable Transport Protocol (RTP): EIGRP uses RTP to ensure reliable delivery of routing updates, adding a layer of dependability to the protocol's operation. RTP ensures that updates are either acknowledged by neighboring routers or retransmitted if necessary.
- Feasible Successor and Backup Routes: EIGRP maintains a list of backup routes called feasible successors. If the primary route fails, it can immediately switch to a feasible successor route without needing to recalculate, which reduces downtime.

How EIGRP is Used

To use EIGRP, network administrators configure the protocol on Cisco routers with a few simple commands. The process typically involves specifying the Autonomous System (AS) number and defining which networks to include in the EIGRP process. The router then starts exchanging Hello packets with neighboring routers, forming adjacencies and exchanging routing information.

Once the EIGRP process is enabled, administrators can specify the networks involved in routing by using the network command:

EIGRP then calculates the best path using its composite metric, considering factors like bandwidth, delay, load, and reliability. If multiple paths to a destination are available, EIGRP can be configured to perform unequal-cost load balancing using the

variance command, which allows traffic to be distributed over different paths with varying metric values.

Overall, EIGRP is used in both small and large-scale enterprise networks where efficient routing, fast convergence, and dynamic path optimization are critical. It's a go-to protocol in Cisco-based environments because of its ease of configuration, robust features, and flexibility in supporting various network topologies and sizes.

EIGRP configuration

On Al-core-sw1

router eigrp 1

network 172.16.5.4 0.0.0.0

network 172.16.10.2 0.0.0.0

network 172.16.20.2 0.0.0.0

network 172.16.30.2 0.0.0.0

network 172.16.40.2 0.0.0.0

network 172.16.150.0 0.0.0.255

no auto-summ

On Al-core-sw2

router eigrp 1

network 172.16.5.5 0.0.0.0

network 172.16.10.3 0.0.0.0

network 172.16.20.3 0.0.0.0

network 172.16.30.3 0.0.0.0

network 172.16.40.3 0.0.0.0

network 172.16.150.0 0.0.0.255

no auto-summ

On AL-Active-R

enable

config ter

router eigrp 1

network 172.16.5.2 0.0.0.0

network 172.150.50.4 0.0.0.0

no auto-summ

On AL-Standby-R

enable

config ter

router eigrp 1

network 172.16.5.3 0.0.0.0

network 16.0.0.1 0.0.0.0

network 172.150.50.5 0.0.0.0

no auto-summ

On R2

enable

config ter

router eigrp 1

network 12.0.0.2 0.0.0.0

network 15.0.0.2 0.0.0.0

network 16.0.0.2 0.0.0.0

no auto-summ

On R3

enable

config ter

router eigrp 1

network 12.0.0.1 0.0.0.0

no auto-summ

redistribute ospf 1 metric 100 100 50 20 1500

router ospf 1

network 13.0.0.1 0.0.0.0 area 0

redistribute eigrp 1 subnets

exit

NAT Protocol

On Ca-Sandby-R

config ter

int s0/1/0

ip nat outside

exit

int g0/0/0

ip nat inside

exit

access-list 25 permit 192.168.0.0 0.0.255.255

ip nat pool WAN2 200.200.200.130 200.200.200.150 netmask 255.255.255.128

ip nat inside source list 25 pool WAN2

ip route 200.200.200.128 255.255.255.128 null 0

router ospf 1

network 200.200.200.128 0.0.0.127 area 0

exit

On Ca-Active-R

config terminal

int s0/1/0

ip nat outside

exit

int g0/0/0

ip nat inside

exit

access-list 25 permit 192.168.0.0 0.0.255.255

ip nat pool WAN1 200.200.200.1 200.200.200.20 netmask 255.255.255.128

ip nat inside source list 25 pool WAN1

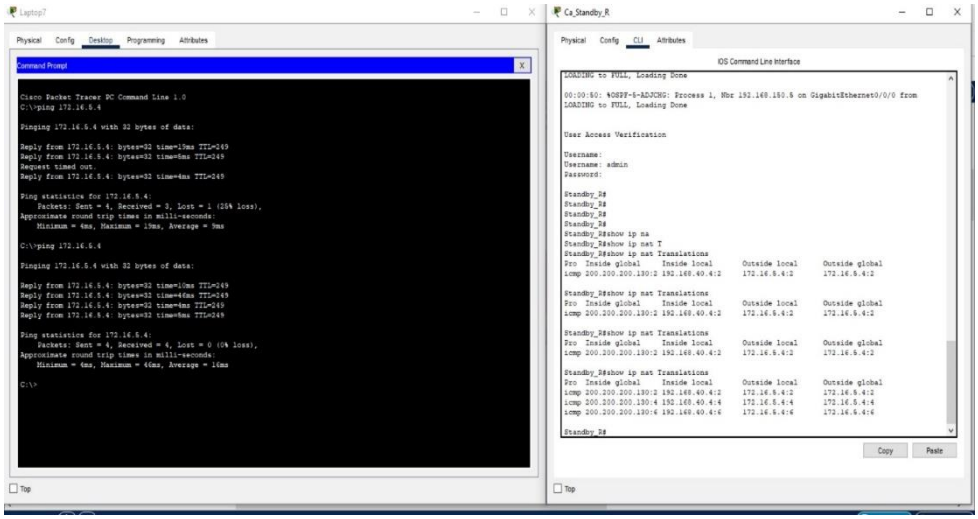
ip route 200.200.200.0 255.255.255.128 null 0

router ospf 1

network 200.200.200.0 0.0.0.127 area 0

exit

On AL-Standby-R



interface GigabitEthernet0/0/0

ip nat inside

exit

interface Serial0/2/0

ip nat outside

exit

access-list 15 permit 172.16.0.0 0.0.255.255

ip nat pool LAN2 100.100.100.130 100.100.100.150 netmask 255.255.255.128

ip nat inside source list 15 pool LAN2

ip route 100.100.100.128 255.255.255.128 null 0

router eigrp 1

network 100.100.100.128 0.0.0.127

no auto-summary

exit

DHCP Snooping & Arp Security

sw 6

ip dhcp snooping

ip dhcp snooping vlan 10,20,30,40,5,50,150,200

ip arp inspection vlan 10,20,30,40,5,50,150,200

int rang f0/1-2

ip dhcp snooping trust

ip arp inspection trust

int rang f0/3-6

ip dhcp snooping limit rate 20

sw 5

ip dhcp snooping

ip dhcp snooping vlan 10,20,30,40,5,50,150,200

ip arp inspection vlan 10,20,30,40,5,50,150,200

int rang f0/1-2

ip dhcp snooping trust

ip arp inspection trust

int rang f0/3-6

ip dhcp snooping limit rate 20

sw 4

ip dhcp snooping

ip dhcp snooping vlan 10,20,30,40,5,50,150,200

ip arp inspection vlan 10,20,30,40,5,50,150,200

int rang f0/1-2

ip dhcp snooping trust

ip arp inspection trust

int rang f0/3-6

ip dhcp snooping limit rate 20

sw 3

ip dhcp snooping

ip dhcp snooping vlan 10,20,30,40,5,50,150,200

ip arp inspection vlan 10,20,30,40,5,50,150,200

int rang f0/1-2

ip dhcp snooping trust

ip arp inspection trust

int rang f0/3-6

ip dhcp snooping limit rate 20

sw 2

ip dhcp snooping

ip dhcp snooping vlan 10,20,30,40,5,50,150,200

ip arp inspection vlan 10,20,30,40,5,50,150,200

int rang f0/1-2

ip dhcp snooping trust

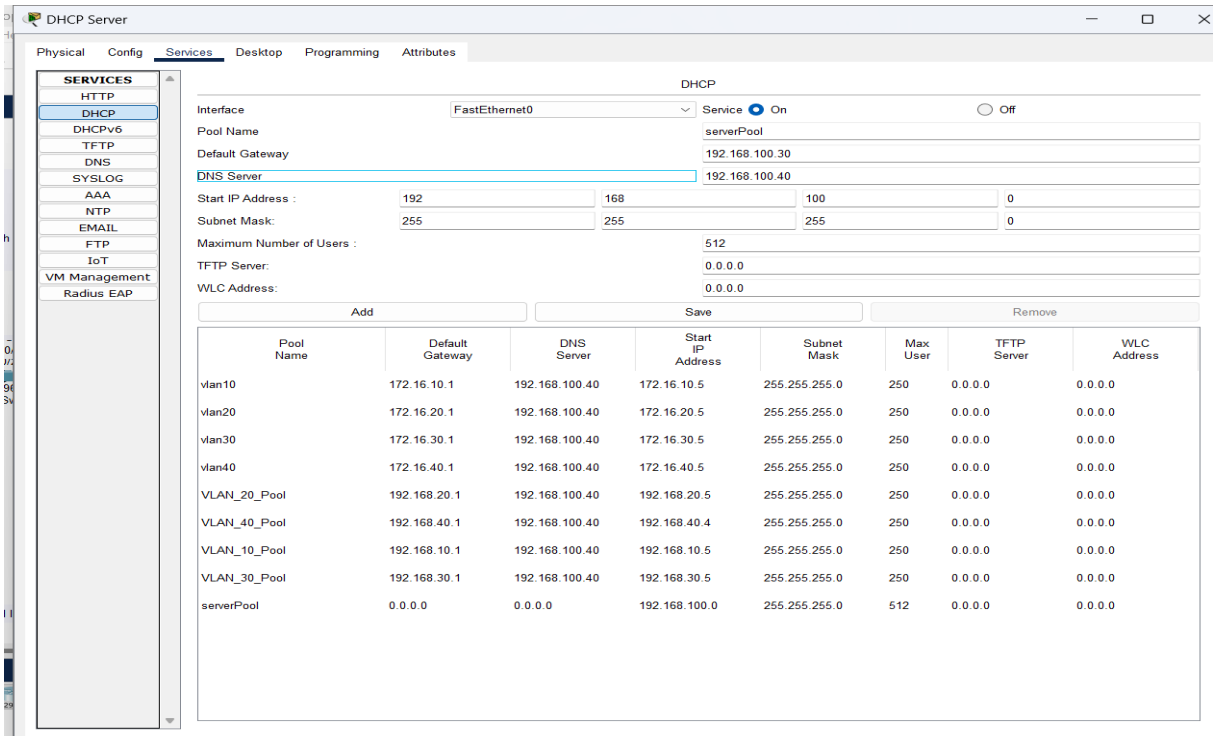
ip arp inspection trust

int rang f0/3-6

ip dhcp snooping limit rate 20

1. DHCP

- Adjusting the pools for VLANS 10,20,30,40 for both networks
- Editing the default gateway for each VLAN,DNS server,start ip,subnet mask,max number of users.

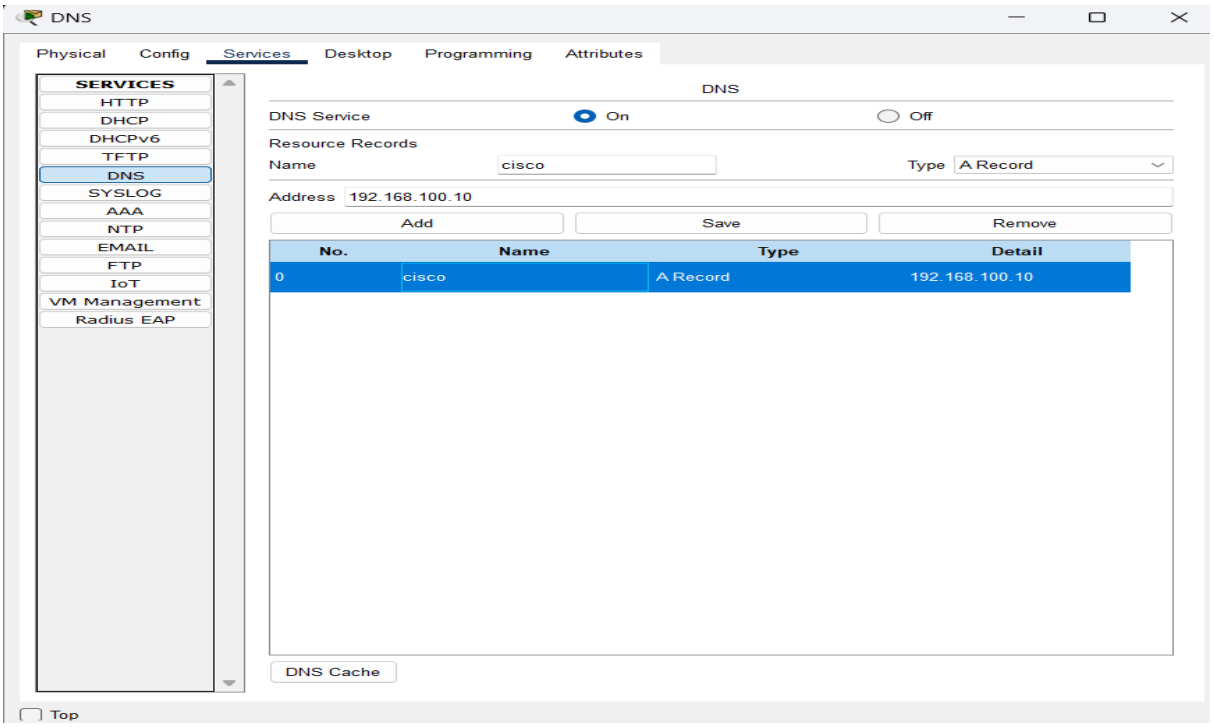


- Using the “IP helper address” command on each layer 3 switch in both LANS

```
switch2(config-if)#int vlan 10
switch2(config-if)#ip helper-address 192.168.100.30
switch2(config-if)#int vlan 20
switch2(config-if)#ip helper-address 192.168.100.30
switch2(config-if)#int vlan 30
switch2(config-if)#ip helper-address 192.168.100.30
switch2(config-if)#int vlan 40
switch2(config-if)#ip helper-address 192.168.100.30
```

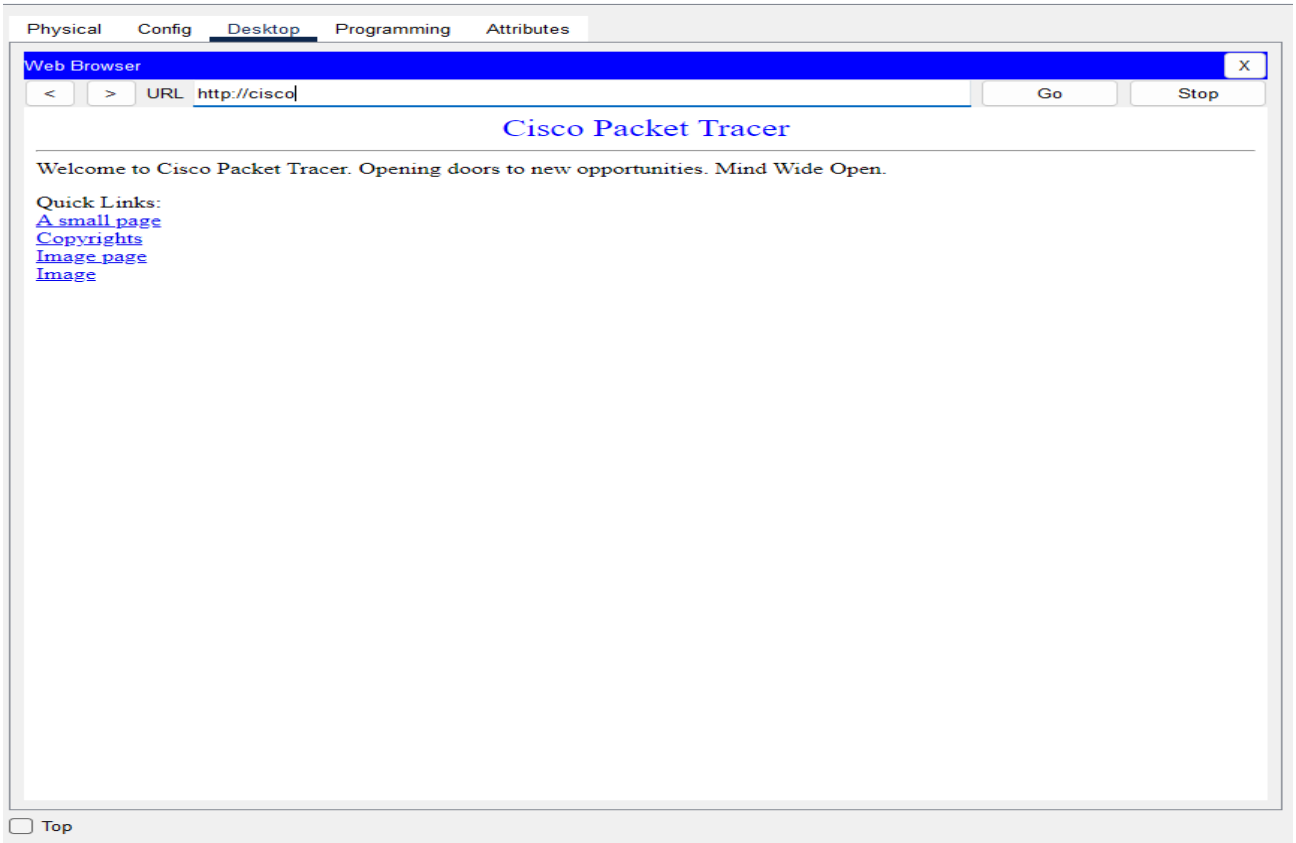
2.DNS SERVER

- Editing the DNS Server's IP address, default gateway, subnet mask,DNS server IP(same as IP address)
- Adding the DNS server IP address in the address log and naming the website



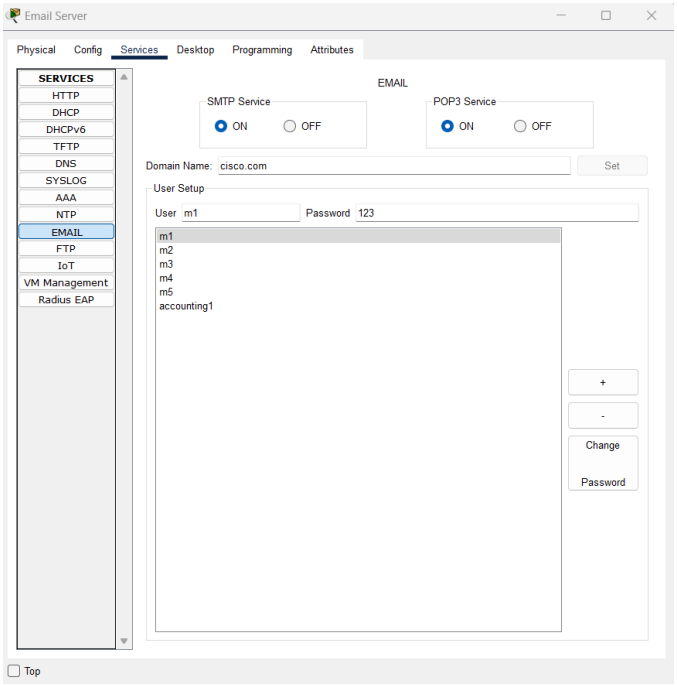
3.Web server

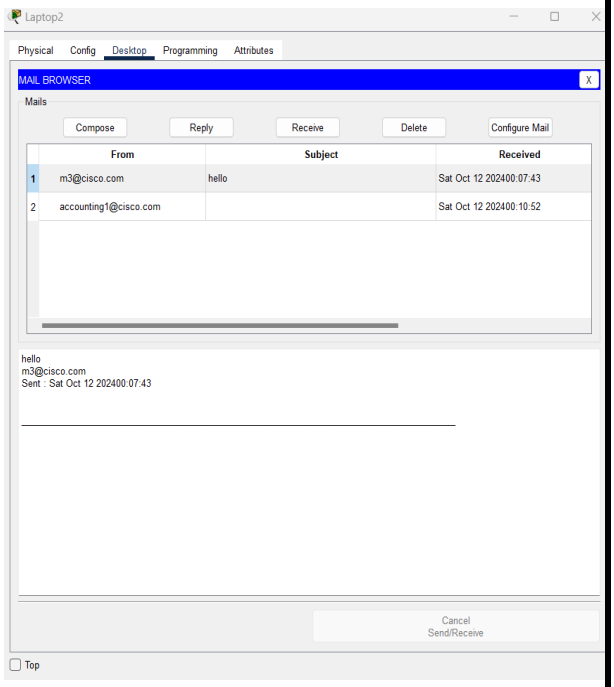
- Editing IP address, subnet mask, default gateway, and DNS server IP address.
- Making sure all VLANS access the html page



4.Mail server

- Adding Individual emails for marketing pcs and left accounting pc so that they could all contact each other.





- Going to each pc and configuring its email address,mail server ip,username and password.