Network Infrastructure Portfolio: Protocols and Configurations in Packet Tracer

By: Dalal Arafeh

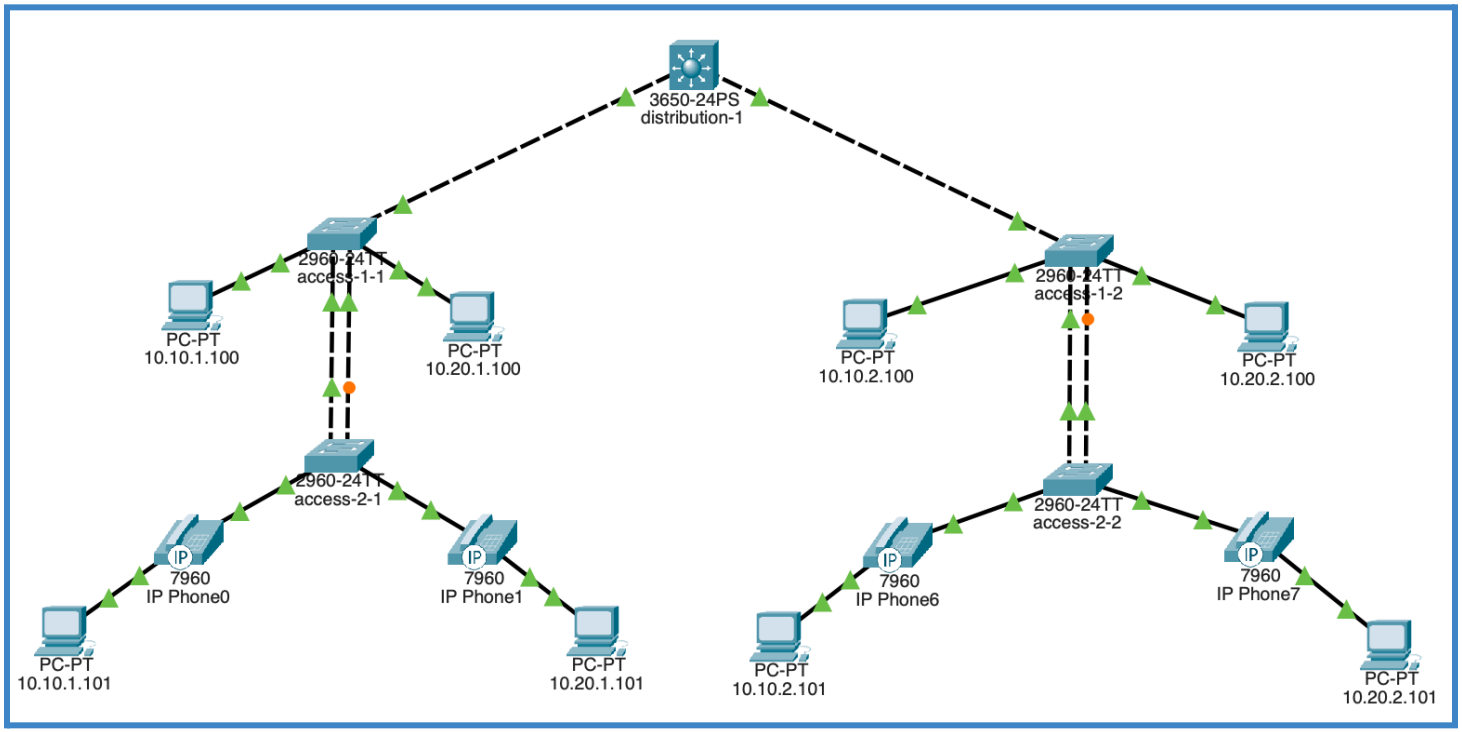
2024-2025

Table of Contents

Purpose

I configured enterprise-level networks, focusing on VLANs for security and traffic management, and trunk links for VLAN communication. I used EtherChannel with LACP, set up routed ports and static routes for network connectivity, and configured DHCPv4 for dynamic IP addressing. I also established management VLANs, enabled PortFast and BPDU Guard for quick and secure port transitions, and implemented HSRP. I used STP for primary and secondary root bridges to ensure network stability and prevent loops.

Lab1: VLANs



a. Basic Access Configurations

I set up foundational connectivity for network devices to ensure proper communication. This establishes the base configuration for all devices and prepares the devices for configurations for VLANs and trunking.

```
hostname <access-name>
no ip domain-lookup
banner motd <banner-title>
enable secret class
line console 0
password cisco
logging synchronous
exec-timeout 0 0
line vty 0 4
password cisco
login
transport input ssh
```

b. VLAN configuration

I configured VLANs to segment the network for better security and manage traffic. By isolating different network segments, this manages the network traffic efficiently and applies specific network policies to different segments by reducing the risk of broadcast storms.

```
vlan <vlan-id>
name <vlan-name>
```

c. Default Port and Active Access Port Configurations

I configured default settings for all switch ports to ensure all ports are in a known state. I set up ports actively used by devices to allow devices connected to these ports to communicate within their assigned VLAN.

```
interface range fa0/1-24, gi0/1-2
switchport mode access
switchport access vlan 255
shutdown
```

```
interface fa0/10
switchport mode access
switchport access vlan 10
no shutdown

interface fa0/20
switchport mode access
switchport access vlan 20
no shutdown
```

d. Trunking Configuration

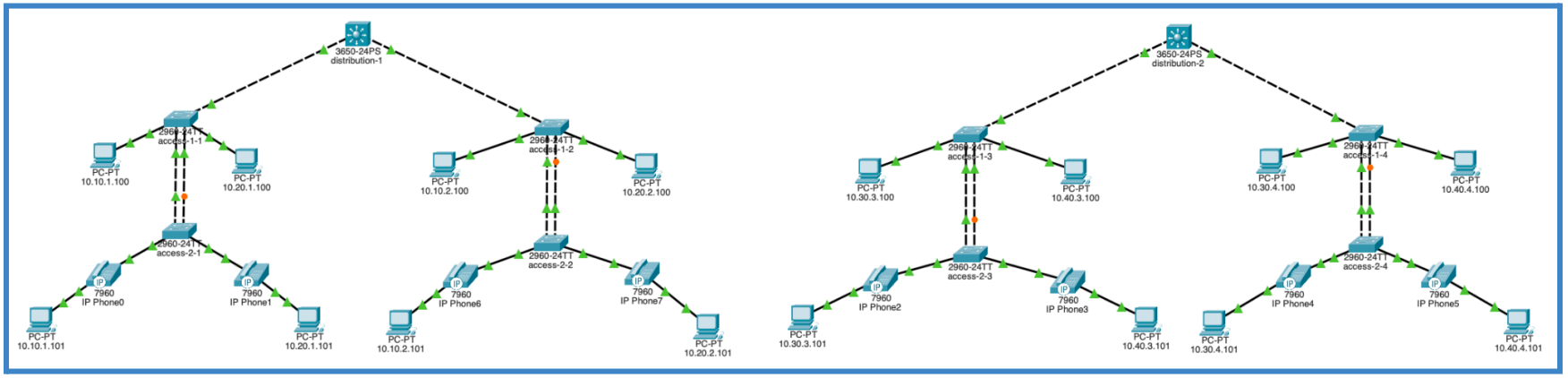
I configured trunk links to carry multiple VLANs through a single physical interface. This reduces the number of physical links required and keeps the VLANs isolated, simplifying the network topology.

```
interface range fa0/1-2
switchport mode trunk
switchport trunk allowed vlan <vlan-ids>
switchport trunk native vlan 254
no shutdown
```

e. End Device Configurations

To finalize the network setup, I ensured that end devices are correctly configured to utilize VLAN and trunking settings. I configured the default gateway and interface Fa 0 for each PC to ensure efficient communication within the network and proper routing to external networks.

Lab 2: Distribution Switches



a. Distribution Switch Configurations

The distribution switches serve as intermediaries between access switches and the core switch. Distribution switches gather traffic from multiple access switches and perform routing between VLANs. Without enabling routing on the distribution switches, there is no communication between VLANs.

distribution-1:

```
interface range g1/0/1-24, g1/1/1-4
switchport mode access
switchport access vlan 255
shutdown
```

```
interface range g1/0/1-2
no switchport access vlan 255
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 1,10,20,30,40,90,100,180,254
switchport trunk native vlan 254
no shutdown

interface vlan 10
ip address 10.10.0.1 255.255.255.0
no shutdown

interface vlan 20
ip address 10.20.0.1 255.255.255.0
no shutdown
```

b. Configuring the Distribution as the Default Gateway

I configured Switched Virtual Interfaces (SVIs) on a Layer 3 distribution switch to act as default gateways for VLANs. An SVI is a virtual interface with an IP address associated with a specific VLAN. SVIs allow the switch to perform routing functions between VLANs without needing an outside router. This ensures that SVIs are reachable by end devices within their respective VLANs. Trunk links carrying all VLANs ensure proper connectivity between switches.

SVIs for VLAN 10 and VLAN 20 on distribution-1:

```
interface vlan 10
ip address 10.10.0.1 255.255.255.0
no shutdown

interface vlan 20
ip address 10.20.0.1 255.255.255.0
no shutdown
```

SVIs for VLAN 30 and VLAN 40 on distribution-2:

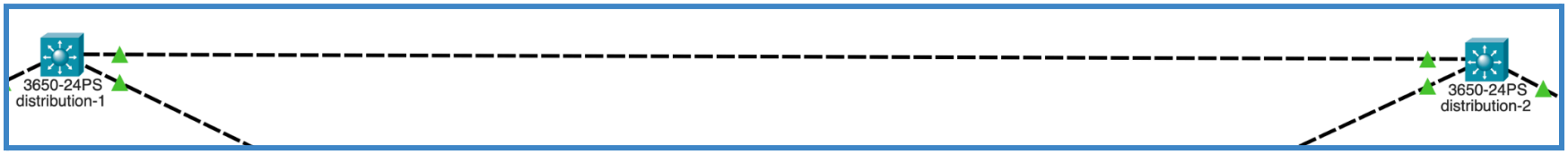
```
interface vlan 30
ip address 10.30.0.1 255.255.255.0
no shutdown

interface vlan 40
ip address 10.40.0.1 255.255.255.0
no shutdown
```

c. Enable Routing on Layer 3 Distribution Switches

A Layer 3 switch needs to have IPv4 routing enabled to forward packets between different VLANs. Once enabled, the switch will route between directly connected networks and any remote networks it learns via static or dynamic routing protocols.

```
ip routing
exit
```

Lab 3: Routed Ports



a. Physically Connecting Inter-Router Links

I set up distribution switches and enabled them to communicate with each other. This includes configuring routed ports and verifying they are functional, as well as setting up static routes to remote networks. We connected an Ethernet cross-over cable on the GigabitEthernet 1/0/24 ports between Distribution-1 and Distribution-2. Routed ports are typically used for router-to-router or router-to-Layer2 switch connections.

distribution-1:

```
interface g1/0/24
no switchport access vlan 255
no switchport
ip address 10.111.1.1 255.255.255.0
no shutdown
```

b. Configure Static Routes to Remote Networks

I configured static routes on Distribution-1 to enable connectivity to remote networks via Distribution-2. Distribution-1 has IPv4 addresses associated with its SVIs on VLAN 10 and VLAN 20, along with the IPv4 address configured on the routed port g1/0/24. We configured static routes (S) to remote networks via the next-hop IPv4 address of Distribution-2 (10.111.1.2). The command `show ip route` verifies this by showing us the routing table.

distribution-1:

```
ip route 10.30.0.0 255.255.0.0 10.111.1.2
ip route 10.40.0.0 255.255.0.0 10.111.1.2
```

distribution-2:

```
ip route 10.10.0.0 255.255.0.0 10.111.1.1
ip route 10.20.0.0 255.255.0.0 10.111.1.1
```

To verify, we use ping or traceroute commands to verify connectivity between VLANs and remote networks.

Lab 4: Management VLANs

This lab involves setting up management VLANs on Distribution-1 and Distribution-2, and then on all access switches. The process includes configuring the VLAN interface, assigning IP addresses, and verifying the configuration.

a. Configure Management VLAN on Distribution Switches

Each distribution switch and its own connected access switches will use VLAN 180 for management purposes. The IP address 10.180.1.1/24 is assigned to the management VLAN on distribution-1. The IP address 10.180.1.2/24 is assigned to the management VLAN on distribution-2. These IPs will serve as the default gateway for other devices in the same management VLAN for each distribution.

distribution-1:

```
interface vlan 180
ip address 10.180.1.1 255.255.255.0
no shutdown
```

b. Configure Management VLAN on Access Layer Switches

Access switches need a default gateway to forward packets to a Layer 3 device for remote management. For example, access switches connected to distribution-1 will use 10.180.1.1 as the default gateway. Each access switch is assigned an IP address within the 10.180.1.0/24 network.

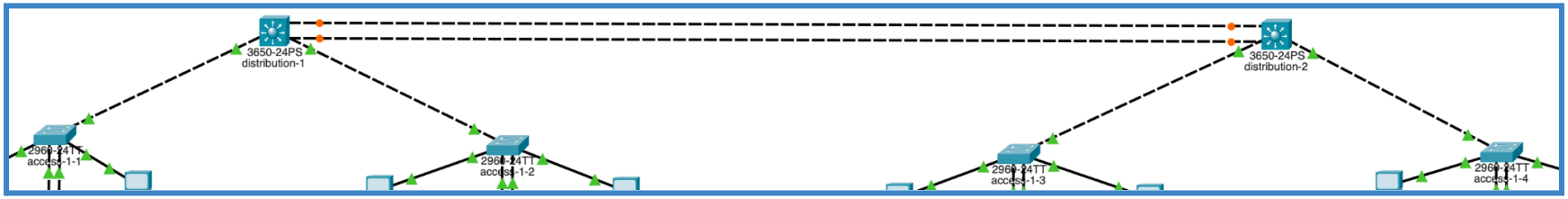
distribution-1
Default gateway: 10.180.1.1/24
access-1-1: 10.180.1.10/24
access-2-1: 10.180.1.20/24
access-1-2: 10.180.1.30/24
access-2-2: 10.180.1.40/24

distribution-2
Default gateway: 10.180.2.1/24
access-1-3: 10.180.2.10/24
access-2-3: 10.180.2.10/24
access-1-4: 10.180.2.10/24
access-1-4: 10.180.2.10/24

access switches on distribution-1:

```
interface vlan 180
ip address 10.180.1.10 255.255.255.0
no shutdown

ip default-gateway 10.180.1.1
```

Lab 6: Etherchannel



I configured EtherChannel using Link Aggregation Control Protocol (LACP) on both Layer 2 and Layer 3 switches. This setup is preferred for its ability to dynamically manage link aggregation and its standardized and widely supported implementation. It simplifies management by ensuring compatibility across different networks by combining multiple physical links into one.

a. LACP

Both ends of the EtherChannel need to be consistently configured to ensure proper negotiation and load balancing. Starting with the access switches on the first column, I shut down the interfaces before configuring EtherChannel to avoid inconsistencies. I repeated the EtherChannel configuration on the other remaining 8 access switches.

access-x-y:

```
port-channel load-balance src-dst-ip
```

```
interface range fa 0/1-2
shutdown
channel-protocol lacp
channel-group 1 mode active

interface port-channel 1
switchport trunk allowed vlan 1,10,20,30,40,90,100,180,254

interface range fa 0/1-2
  no shutdown
```

b. Second Routed Port between Distribution Switches

I added another physical connection between distribution switches with cross-over cable using GigabitEthernet 1/0/23 ports. Adding a second routed port provides redundancy and load balancing.

c. Configuring Layer 3 EtherChannel using LACP

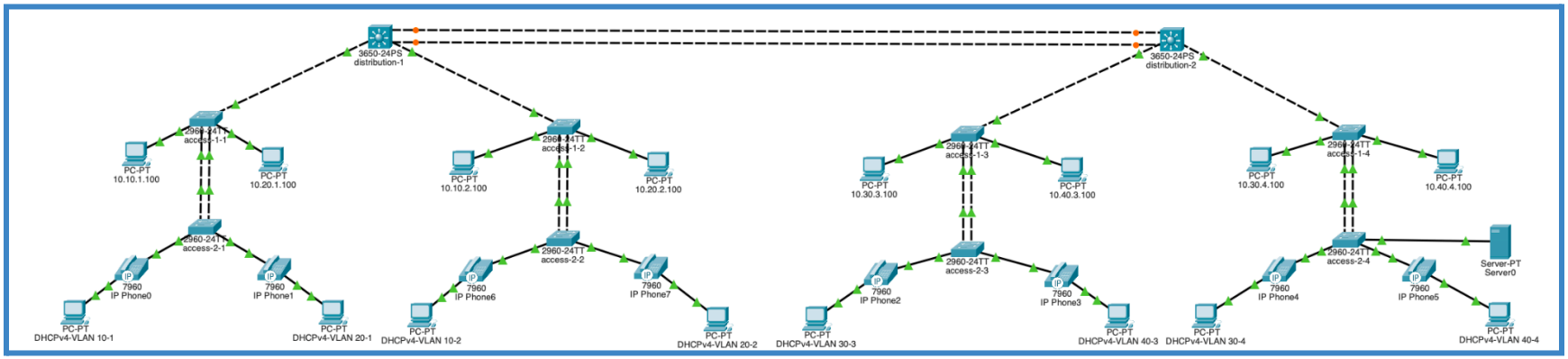
Setting up a Layer 3 EtherChannel on a distribution switch using LACP involves setting up routed ports and channel groups to ensure the IP addresses and channel protocols are correctly configured. To enable it to route packets, I assign 10.111.1.1 255.255.255.0 to distribution-1 and 10.111.1.2 255.255.255.0 on distribution-2.

distribution-1:

```
interface g 1/0/24
no ip address

interface Port-channel2
no switchport
ip address 10.111.1.1 255.255.255.0
no shutdown

interface range g 1/0/23-24
shutdown
```

```
no switchport
channel-protocol lacp
channel-group 2 mode active
no shutdown
```

Lab 7: DHCPv4



Dynamic Host Configuration Protocol (DHCPv4) is a network protocol used to automatically assign IP addresses and other network configuration parameters to devices on a network. It allows devices to request and receive an IP address automatically from a DHCP server. This ensures devices can seamlessly connect and communicate over the network without manually setting up an IP.

a. Preparing DHCPv4 Clients

For the PCs connected to the access layer switches on Layer 2, I changed the configuration for DHCPv4 by selecting DHCP from the settings. This ensures PCs are configured to request IP addresses from the DHCP server.

b. Adding the DHCPv4 Server

I centralized IP address distribution for VLAN 40 by integrating the DHCP server into the network. I added a DHCPv4 server to the 10.40.0.0/16 network (VLAN 40) and configured it with an IP address of 10.40.0.99/16 and a default gateway of 10.40.0.1.

ip dhcp pool VLAN10
network 10.10.0.0 255.255.0.0
default-router 10.10.0.1
dns-server 10.88.88.88

ip dhcp pool VLAN20
network 10.20.0.0 255.255.0.0
default-router 10.20.0.1
dns-server 10.88.88.88

ip dhcp pool VLAN30
network 10.30.0.0 255.255.0.0
default-router 10.30.0.1
dns-server 10.88.88.88

ip dhcp pool VLAN40
network 10.40.0.0 255.255.0.0
default-router 10.40.0.1
dns-server 10.88.88.88

c. Connecting the DHCPv4 Server to the Network

I physically connected the DHCPv4 server to the network using the GigabitEthernet 0/1 port on the access layer switch, allowing it to communicate with client devices.

```
interface GigabitEthernet0/1
switchport mode access
switchport access vlan 40
no shutdown
```

d. Configuring the Switchport for DHCPv4

To ensure it can handle DHCP traffic, I configured the switchport for VLAN 40, ensuring it is enabled and active. I also changed the port from VLAN 255 (parking lot VLAN) to VLAN 40.

```
interface GigabitEthernet0/1
switchport access vlan 40
no shutdown
```

e. Configuring ip helper-address

I want to be able to forward DHCP requests to the DHCP server. For example, I configured the ip helper-address command on the Distribution-2 switch for VLAN 30. This allows devices in VLAN 30 to obtain IP addresses from the DHCP server on a different VLAN, ensuring they can communicate with the DHCP server, even if they are on different subnets.

distribution-2:

```
interface vlan 30
ip helper-address 10.40.0.99
```

For distribution-1, I extended DHCP relay functionality to VLANs 10 and 20, allowing devices in these VLANs to obtain IP addresses.

distribution-1:

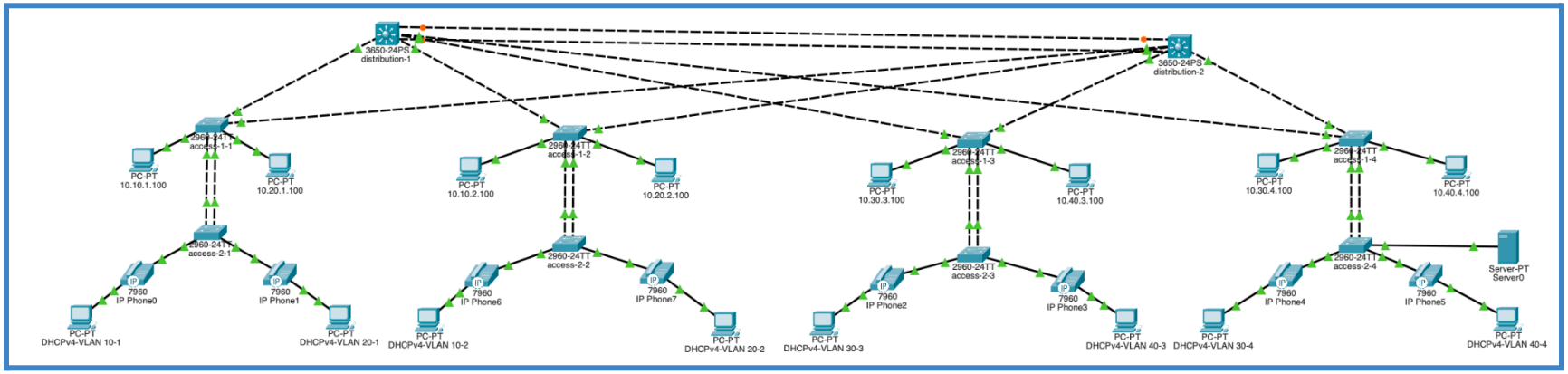
```
interface vlan 10
ip helper-address 10.40.0.99

interface vlan 20
ip helper-address 10.40.0.99
```

f. Enabling PortFast and BPDU Guard

I enabled PortFast and BPDU Guard on the switchport to allow it to transition immediately to the forwarding state. This reduces the time it takes for ports to become operational by preventing loops in spanning tree topologies.

```
interface fa0/21
spanning-tree portfast
spanning-tree bpduguard enable
```

Lab 8: FHRP



a. Modify SVI IP Addresses

Changing the SVIs for VLAN 10 and VLAN 20 ensures these IP addresses are not used as the default gateway addresses for end devices. I added SVIs for VLAN 30 and VLAN 40 to ensure that these VLANs have dedicated IP addresses (which are not default gateway addresses). I do the same for distribution-2 by changing the SVIs for VLAN 30 and VLAN 40 and adding SVI's for VLAN10 and VLAN20.

distribution-1:

```
interface vlan 10
no ip address
ip address 10.10.0.5 255.255.0.0
exit

interface vlan 20
no ip address
ip address 10.20.0.5 255.255.0.0
exit

interface vlan 30
ip address 10.30.0.5 255.255.0.0
no shutdown
exit

interface vlan 40
ip address 10.40.0.5 255.255.0.0
no shutdown
exit
```

b. Adding New Trunk Links

I connected each level 1 access layer switch to the other distribution switch. Configuring trunk links allows multiple VLANs to be carried over a single physical link, improving network efficiency and scalability. Trunking is essential for passing VLAN information between switches and maintaining VLAN isolation across the network.

c. Configuring Distributions as Virtual Active Router for VLANs

A Cisco protocol called HSRP (Hot Standby Router Protocol) acts as a router failover mechanism to guarantee high network availability. Configuring HSRP ensures that there is always an active router ready to take over if the primary router fails by ensuring availability of routing paths. Configuring distribution-1 as the active router for VLANs 10 and 20 ensures that it will handle traffic for these VLANs unless it fails, at

which point the standby router will take over. Setting distribution-1 as the standby router for VLANs 30 and 40 provides a backup in case distribution-2 (the primary router) fails.

distribution-1:

```
interface vlan 10
standby 1 ip 10.10.0.1
standby 1 priority 200
standby 1 preempt
exit

interface vlan 20
standby 1 ip 10.20.0.1
standby 1 priority 200
standby 1 preempt
exit

interface vlan 30
standby 1 ip 10.30.0.1
standby 1 priority 100
standby 1 preempt
exit

interface vlan 40
standby 1 ip 10.40.0.1
standby 1 priority 100
standby 1 preempt
exit
```

By configuring distribution-2 as the active router for VLANs 30 and 40, we ensure that it will manage traffic for these VLANs, with distribution-1 as the standby. This setup provides a balanced load. Setting distribution-2 as the standby router for VLANs 10 and 20 ensures that it will take over if distribution-1 fails

d. Configuring Primary and Secondary Root Bridge on Distributions

The Spanning Tree Protocol (STP) prevents network loops in a Layer 2 Ethernet. By configuring distribution-1 as the primary root bridge for VLANs 10 and 20, I set it as the central point. Making it the secondary root bridge for VLANs 30 and 40 provides a backup if the primary root bridge (distribution-2) fails. Configuring distribution-2 as the primary root bridge for VLANs 30 and 40 and the secondary root bridge for VLANs 10 and 20 ensures a balanced distribution of STP roles. This setup helps in maintaining a stable network by having clear primary and secondary bridges for each VLAN.

distribution-2:

```
spanning-tree vlan 30 root primary
spanning-tree vlan 40 root primary

spanning-tree vlan 10 root secondary
spanning-tree vlan 20 root secondary
```