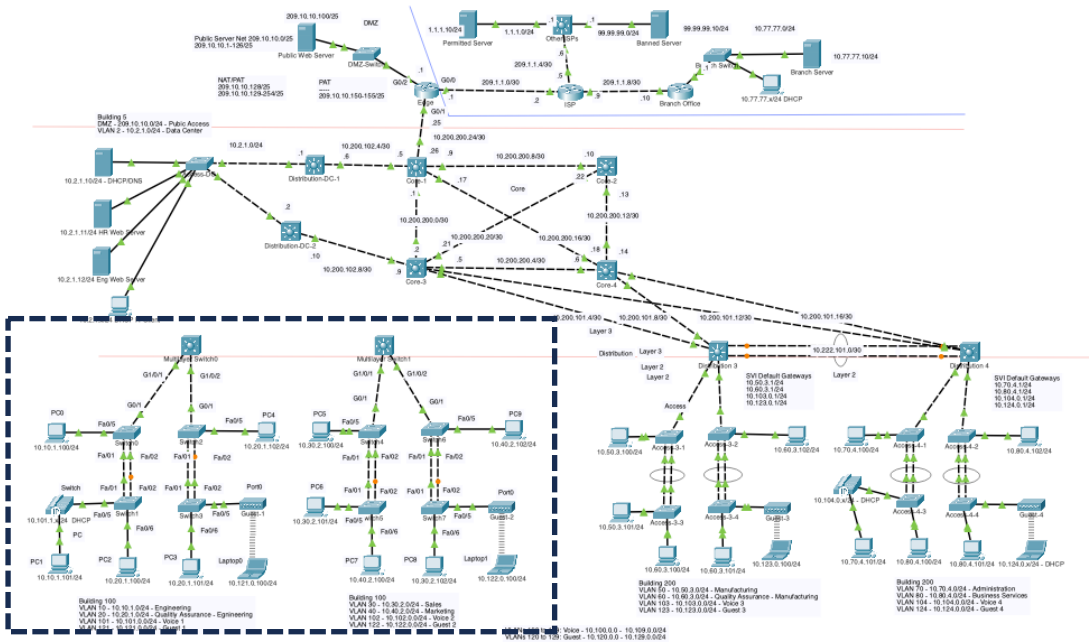
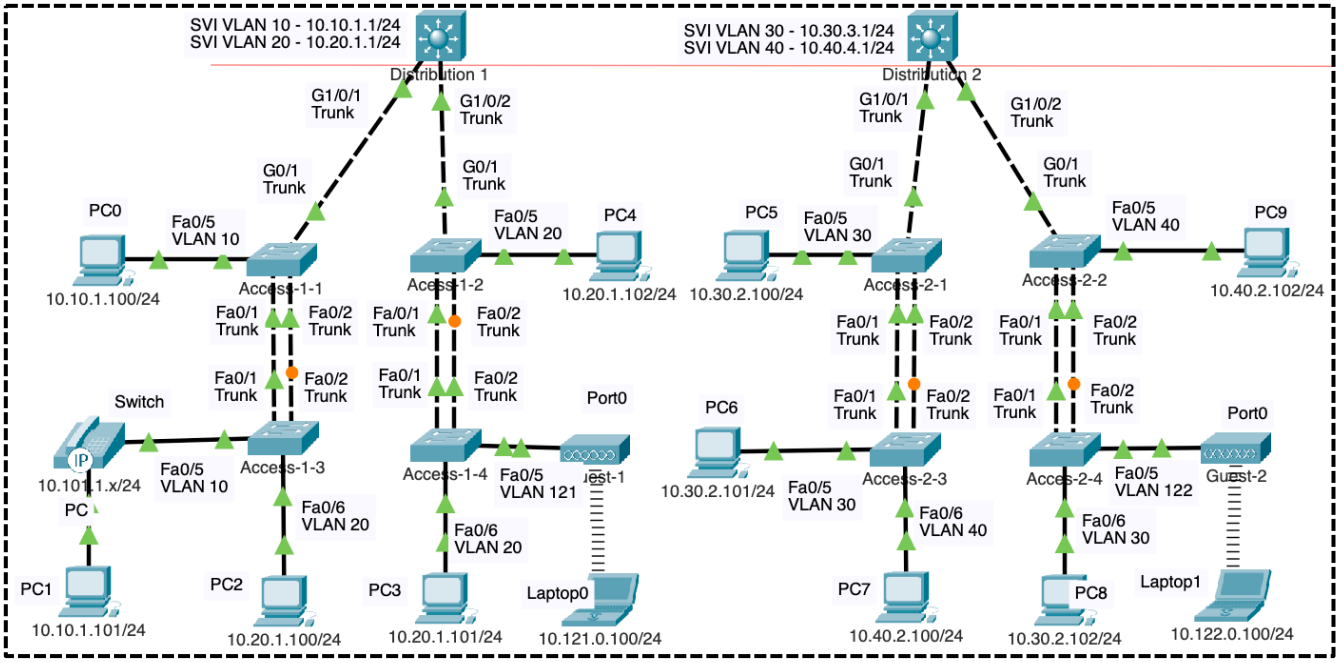
Enterprise Network
Lab 4 – Routed Ports and Routing





Note: SVIs are configured and routing is occurring within Distribution switches because all interfaces are directly connected and Distribution switches have had routing enabled.

Current Topology and Objectives

In the previous lab you configured the SVIs and enabled for the above topology.

The list of objectives covered in this lab:

1. **Review Layer 3 Switch Configuration**:
   - Verify previously configured SVIs and routing on Layer 3 switches.
2. **Configure Routed Ports**:
   - Convert switch interfaces from Layer 2 to Layer 3 using the no switchport command.
   - Assign IP addresses to routed ports using a /30 network for efficient IP address usage.
3. **Verify Routed Ports**:
   - Use commands like show interface switchport and show ip route to confirm routed port configurations.
4. **Understand VLAN, Trunking, and Routing Integration**:
   - Trace the flow of traffic from one VLAN and network to another through routed ports and Layer 3 routing.
5. **Configure Static Routes**:
   - Add static routes on Distribution-1 and Distribution-2 to enable communication between networks not directly connected to each switch.
6. **Verify Connectivity**:
   - Use ping to test reachability between devices on different VLANs and networks.
   - Use tracert to examine the path packets take through the Layer 3 network.
7. **Explore Routing Protocol Transition**:
   - Understand the limitations of static routes and introduce the concept of replacing them with OSPF in a future lab for scalability and dynamic routing.
8. **Develop Deeper Understanding**:
   - Emphasize the importance of comprehending how VLANs, trunking, routing, ARP, and MAC address tables interact to provide end-to-end connectivity.

Review: SVIs and Routing Configured on a Layer 3 Switches

In the previous lab we configured SVIs and enabled routing on both Distribution switches using the **ip routing** command.

```
distribution-1# conf t

distribution-1(config)# interface vlan 10
distribution-1(config-if)# ip address 10.10.1.1 255.255.255.0
distribution-1(config-if)# exit

distribution-1(config)# interface vlan 20
distribution-1(config-if)# ip address 10.20.1.1 255.255.255.0
distribution-1(config-if)# exit

distribution-1(config)# ip routing
distribution-1(config)# end

distribution-1# 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

     10.0.0.0/24 is subnetted, 2 subnets
C       10.10.1.0 is directly connected, Vlan10
C       10.20.1.0 is directly connected, Vlan20

distribution-1#
```

On Distribution-1. the IP network addresses **10.10.1.0/24** and **10.20.1.0/24** appear in the routing table as **directly connected** routes because the SVIs for VLAN 10 and VLAN 20 have been configured with IP addresses and are in an "up" state. This means that any devices connected to ports assigned to VLAN 10 or VLAN 20 can communicate with the switch, and since routing has been enabled with the **ip routing** command, the switch can also route traffic between these two VLANs.

Note: This is New! Routing can now occur between the two networks because **Distribution-1** is directly connected to both the **10.10.1.0/24** and **10.20.1.0/24** networks via the SVIs for VLAN 10 and VLAN 20. The exit interface in the routing table specifies the VLAN (e.g., VLAN 10 or VLAN 20) instead of a physical interface. For example, Distribution-1 can reach any device on its 10.10.1.0/24 network through any of its VLAN 10 interface including access ports on VLAN 10 and trunk links that carry VLAN 10. The same applies for VLAN 20.

For end devices to reach their default gateway (SVI) on the distribution switch, the switch must have either an access port or a trunk link carrying the appropriate VLAN. The access layer switch can connect to the distribution switch in one of two ways:

1. Through separate access ports for each VLAN corresponding to an SVI.
2. Through a trunk link carrying all VLANs needed to reach the SVIs.

```
distribution-2# conf t

distribution-2(config)# interface vlan 30
distribution-2(config-if)# ip address 10.30.2.1 255.255.255.0
distribution-2(config-if)# exit

distribution-2(config)# interface vlan 40
distribution-2(config-if)# ip address 10.40.2.1 255.255.255.0
distribution-2(config-if)# exit

distribution-2(config)# ip routing
distribution-2(config)# end

distribution-2# 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

     10.0.0.0/24 is subnetted, 2 subnets
C       10.30.2.0 is directly connected, Vlan30
C       10.40.2.0 is directly connected, Vlan40

distribution-2#
```

What applies to Distribution-1 also applies to Distribution-2. Since Distribution-2 is directly connected to the **10.30.2.0/24** and **10.40.2.0/24** networks through SVIs for VLAN 30 and VLAN 40, it can route traffic between these networks. Similarly, the exit interfaces in the routing table specify VLANs instead of physical interfaces, meaning Distribution-2 can reach any devices on these IP networks as long as it has either an access port in the VLAN or a trunk link carrying the VLAN.

Verifying the Default Gateway

For end devices to reach their default gateway (SVI) on the distribution switch, the switch must have either an access port or a trunk link carrying the appropriate VLAN. The access layer switch can connect to the distribution switch in one of two ways:

1. Through separate access ports for each VLAN corresponding to an SVI.
2. Through a trunk link carrying all VLANs needed to reach the SVIs.

From PC0, 10.10.1.100/24 attempt to ping PC4, 10.20.1.102/24.

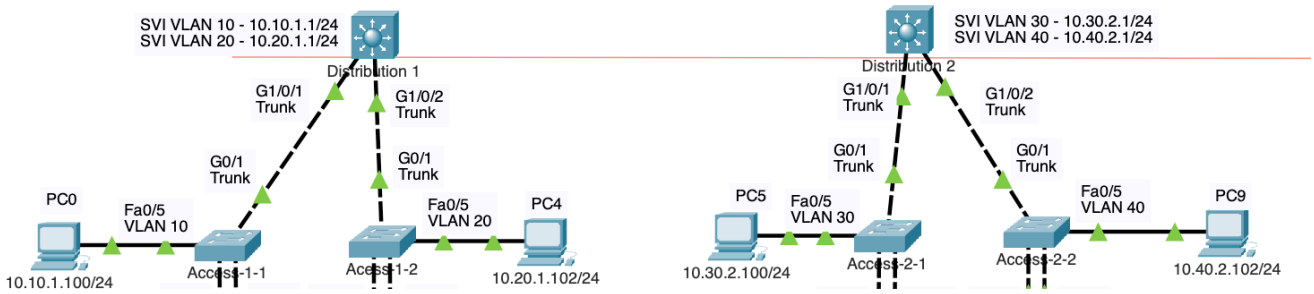
```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::201:63FF:FE0A:83B0
   IPv6 Address....................: ::
   IPv4 Address....................: 10.10.1.100
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     10.10.1.1

C:\>ping 10.20.1.102

Pinging 10.20.1.102 with 32 bytes of data:

Request timed out.
Reply from 10.20.1.102: bytes=32 time<1ms TTL=127
Reply from 10.20.1.102: bytes=32 time<1ms TTL=127
Reply from 10.20.1.102: bytes=32 time<1ms TTL=127

Ping statistics for 10.20.1.102:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>tracert 10.20.1.102

Tracing route to 10.20.1.102 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      10.10.1.1
  2    0 ms      0 ms      0 ms      10.20.1.102

Trace complete.

C:\>
```

Notice that this time, the ping is successful (after the first time out due to an ARP Request).

The traceroute from **10.10.1.100/24** to **10.20.1.102/24** is successful because the traffic is routed via the default gateway **10.10.1.1** on VLAN 10, and the response follows the return path via the default gateway **10.20.1.1** on VLAN 20. This demonstrates successful inter-VLAN routing on the distribution switch.

All devices on both VLANs/IP networks with Distribution-1 as their default gateway, across all access switches, should now be able to reach (ping).

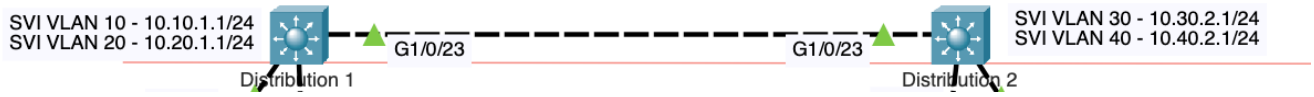
Still No Reachability Between Distribution-1 and Distribution-2



Obviously, there is no routing between devices connected to Distribution-1 and Distribution-2. We will need to connect a physical link between these two Layer 3 switches and additional IP addressing.

We will do this here!

Connecting Distribution-1 and Distribution-2



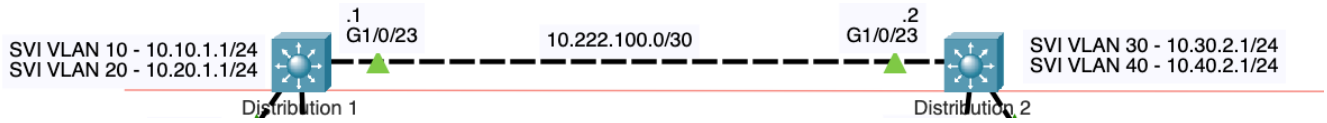
We have used a crossover cable to connect the G1/0/23 interfaces on both Distribution-1 and Distribution-2 switches for this lab. Note: With MDIX enabled on either switch, a straight-through cable can also be used instead of a crossover cable.

VTP Note:

If VTP (VLAN Trunking Protocol) were enabled on both Distribution-1 and Distribution-2 switches, and they had the correct VTP status, the link between G1/0/23 interfaces might automatically negotiate to become a trunk link. This is because VTP can propagate VLAN information across trunk links. To prevent unintended trunking, many network administrators prefer to use the **switchport nonegotiate** option on switchports. This ensures the port remains in its manually configured mode, avoiding unexpected behavior and improving network stability.

In our case, we do not want a trunk link. We will be configuring these ports not as Layer 2 trunk ports, but as Layer 3 routed ports.

Routed Port



There are multiple ways to configure a network to forward data within the same VLAN (IP network) or between VLANs (different IP networks). Following our campus architecture model and best practices, we will add a link between the two distribution switches and configure this link as a separate Layer 3 network. This approach utilizes a **routed port**.

A **routed port** on a Layer 3 switch is a physical interface configured to function like a port on a router. It is not associated with any VLAN and is instead assigned an IP address and subnet mask to enable routing between different networks.

To configure a routed port, the **no switchport** command is used to disable Layer 2 switching on the interface, enabling it to operate in Layer 3 mode. This configuration is ideal for interconnecting distribution switches, as it avoids Spanning Tree Protocol, enhances scalability, and supports dynamic routing protocols, improving network reliability and performance.

Routed ports on a Layer 3 switch share several similarities with physical ports on a router:

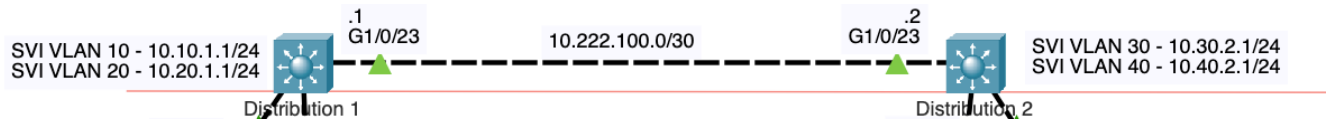
- **IP Addressing:** Both require an IP address configuration to enable routing functionality.
- **Network Segmentation:** Both connect and route traffic between different IP networks, ensuring logical separation.
- **Routing Protocols:** Both support dynamic routing protocols such as OSPF, EIGRP, and BGP to exchange routing information and optimize routing decisions.

Benefits of Routed Ports over Trunk Links

While using a Layer 3 link with routed ports is a common approach, another option is to use a Layer 2 trunk link to connect switches. However, Layer 3 links are often preferred for their advantages in redundancy and flexibility. Layer 3 connections allow for active redundant links and load balancing, whereas Layer 2 links with Spanning Tree Protocol (STP) block redundant paths to prevent network loops.

By eliminating spanning tree dependencies, Layer 3 links reduce the risk of loops and minimize convergence delays. They also enhance scalability, as routing protocols can efficiently manage larger networks and dynamically adapt to changes in topology. Furthermore, they offer granular control over traffic flow, improving overall network performance, reliability, and ease of troubleshooting.

Configuring Routed Ports



Many Layer 3 switches have ports configured as Layer 2 by default, as indicated by the command output showing **"Switchport: Enabled"**. This means these ports function as standard Layer 2 switchports unless explicitly configured as Layer 3 routed ports.

```
distribution-1# show interface g 1/0/23 switchport
Name: Gig1/0/23
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
<output omitted for brevity>
```

These following commands are used to configure a routed port on interface g1/0/23 with a specific IP address and enable it for network traffic. To conserve IPv4 addresses, we are using a /30 prefix length (255.255.255.252 subnet mask) since this network only requires two "host" devices, Distribution-1 and Distribution-2 IP addresses.

```
distribution-1(config)#interface g 1/0/23
distribution-1(config-if)# ip address 10.222.100.1 255.255.255.252
                                   ^
% Invalid input detected at '^' marker.

distribution-1(config-if)# no switchport

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/23, changed
state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/23, changed
state to up

distribution-1(config-if)# ip address 10.222.100.1 255.255.255.252
distribution-1(config-if)# no shutdown
```

To configure routed ports, we purposely assigned an IP address to the interfaces before applying the **no switchport** command to demonstrate the error that occurs when attempting to configure an IP address on a port still in Layer 2 mode. This step highlights an important distinction: on some Layer 3 switches, ports may default to Layer 2 mode, requiring the **no switchport** command to enable Layer 3 functionality, whereas other switches may default to Layer 3 mode. This variability emphasizes the need to understand the default behavior of your specific switch model during configuration.

Here is a brief description of the commands:

1. **interface g1/0/23**
    - **Description**: This command selects the interface GigabitEthernet 1/0/23 for configuration.
2. **no switchport**
    - **Description**: This command changes the mode of the interface from a Layer 2 switch port to a Layer 3 routed port. By executing this, the interface no longer deals with VLAN tags and behaves more like a port on a router, capable of making routing decisions based on IP addresses.
3. **ip address 10.222.100.1 255.255.255.252**
    - **Description**: Assigns the IP address 10.222.100.1 with a subnet mask of 255.255.255.252 to the interface. The IP address must be unique within its network segment to avoid conflicts.
4. **no shutdown**
    - **Description**: This command brings the interface up, making it active and operational. By default, Cisco interfaces are administratively down, meaning they need to be explicitly enabled before they can transmit data.

To configure Distribution-2, assign the other host address available within the /30 network range.

```
distribution-2(config)# interface g 1/0/23
distribution-2(config-if)# no switchport
distribution-2(config-if)# ip address 10.222.100.2 255.255.255.252
distribution-2(config-if)# no shutdown
```

It is also a good practice to verify your configuration by examining the running configuration to ensure accuracy. Always check for any leftover commands, such as a default 'parking lot' configuration like **switchport access vlan 255**, which could cause conflicts if not properly removed before applying the new settings. If needed, use the **no** parameter prior to a command to remove it.

```
distribution-1# show run | begin interface GigabitEthernet1/0/23
interface GigabitEthernet1/0/23
 no switchport
 ip address 10.222.100.1 255.255.255.252
 duplex auto
 speed auto
!
```

```
distribution-2# show run | begin interface GigabitEthernet1/0/23
interface GigabitEthernet1/0/23
 no switchport
 ip address 10.222.100.2 255.255.255.252
 duplex auto
 speed auto
!
```

Verify Routed Port Configuration

The routed port can be used by using the **show interface <interface> switchport** command. The switchport shows as "**Disabled**", which indicates that this port is no longer a layer 2 switch port, but is not a layer 3 routed port. "**Enabled**" would indicate that the port is a layer 2 switch port.

```
distribution-1# show interface g 1/0/23 switchport
Name: Gig1/0/23
Switchport: Disabled

distribution-1#
```

Examine the routing table on Distribution-1.

```
distribution-1# 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

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.10.1.0/24 is directly connected, Vlan10
C       10.20.1.0/24 is directly connected, Vlan20
C       10.222.100.0/30 is directly connected, GigabitEthernet1/0/23

distribution-1# ping 10.222.100.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.222.100.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

distribution-1#
```

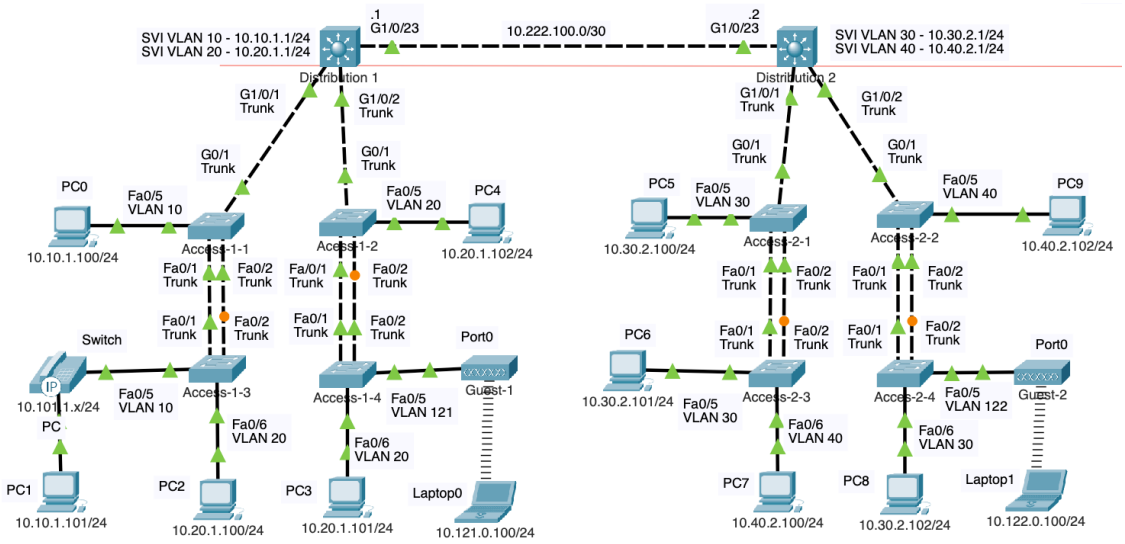
The routed port on G1/0/23 is now visible in the routing table as a directly connected route, associated with the physical interface. This configuration allows the switches to route traffic across the newly created Layer 3 link using the G1/0/23 interface. With this setup, we can now successfully ping between the two switches over this interface, verifying connectivity. It is important to note that the first ping may fail due to the ARP request process, which resolves the MAC address of the destination device. Subsequent pings should succeed as the ARP table is updated.

From Distribution-1 attempt to ping a device on a one of Distribution-2's directly connected networks (VLANs).

```
distribution-1# ping 10.30.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.30.2.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

distribution-1#
```

Pings to devices on Distribution-2's networks will fail because Distribution-1 only has routing information for its own directly connected networks: 10.10.1.0/24, 10.20.1.0/24, and 10.222.100.0/30, as shown in the previous routing table. Without additional routing configurations, such as static routes or a dynamic routing protocol, Distribution-1 is unaware of the networks connected to Distribution-2 and cannot route traffic to them.

Configure Static Routes to Remote Networks



In this section, we will configure static routes so that Distribution-1 and Distribution-2 can communicate with each other's IP networks. This is essential for ensuring connectivity between devices in different VLANs across the two switches. It's important to remember that these distribution switches act as the default gateways for their respective networks. By adding static routes, we will enable these switches to forward traffic to the appropriate destination networks that are not directly connected to them.

Static Routes for now but Dynamic Routing Protocol OSPF Later

While static routes are suitable for small or simple networks, they can become cumbersome to manage as networks grow in size and complexity. In this lab, static routes are used to establish connectivity between Distribution-1 and Distribution-2, providing a straightforward way to route traffic between their networks. However, static routing requires manual configuration and updating, which makes it impractical for larger networks where changes, such as the addition of new subnets or links, occur frequently.

In a later lab, we will expand on this setup by connecting these distribution switches to core routers and replacing the static routes with the dynamic routing protocol OSPF (Open Shortest Path First). OSPF will enable the distribution switches to automatically discover and adapt to network changes, ensuring scalability, redundancy, and efficient traffic routing in the larger network environment.

Configure static routes on Distribution-1 to reach remote networks on Distribution-2

```
distribution-1(config)# ip route 10.30.2.0 255.255.255.0 10.222.100.2
distribution-1(config)# ip route 10.40.2.0 255.255.255.0 10.222.100.2
```

On Distribution-1, the static routes direct traffic destined for Distribution-2's networks (10.30.2.0/24 and 10.40.2.0/24) via the next-hop IP address on the routed port link (10.222.100.2).

Configure static routes on Distribution-2 to reach remote networks on Distribution-1

```
distribution-2(config)# ip route 10.10.1.0 255.255.255.0 10.222.100.1
distribution-2(config)# ip route 10.20.1.0 255.255.255.0 10.222.100.1
```

Similarly, on Distribution-2, the static routes are configured to send traffic destined for Distribution-1's networks (10.10.1.0/24 and 10.20.1.0/24) through the next-hop IP address on the same routed link (10.222.100.1).

Verify the Static Routes in the IP Routing Table

We can use the show ip route command on both Distribution-1 and Distribution-2 switches to verify the static routes have been correctly added to the routing tables. This command displays the routing table, including the static routes marked with an '**S**' to indicate their manually configured status. On Distribution-1, the static routes should show that traffic destined for 10.30.2.0/24 and 10.40.2.0/24 is routed via 10.222.100.2.

```
distribution-1# 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
       <output omitted for brevity>

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.10.1.0/24 is directly connected, Vlan10
C       10.20.1.0/24 is directly connected, Vlan20
S       10.30.2.0/24 [1/0] via 10.222.100.2
S       10.40.2.0/24 [1/0] via 10.222.100.2
C       10.222.100.0/30 is directly connected, GigabitEthernet1/0/23

distribution-1#
```

Similarly, on Distribution-2, the routing table should display static routes pointing to 10.10.1.0/24 and 10.20.1.0/24 via 10.222.100.1. Verifying these entries ensures that each switch knows how to route traffic to networks on the other switch, confirming the static route configuration is correct.

```
distribution-2# 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

     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
S       10.10.1.0/24 [1/0] via 10.222.100.1
S       10.20.1.0/24 [1/0] via 10.222.100.1
C       10.30.2.0/24 is directly connected, Vlan30
C       10.40.2.0/24 is directly connected, Vlan40
C       10.222.100.0/30 is directly connected, GigabitEthernet1/0/23

distribution-2#
```

Verify Reachability using Ping and Traceroute

From PC2 (10.20.1.100/24) use **ping** to test reachability to PC7 (10.40.2.100).

```
C:\> ping 10.40.2.100

Pinging 10.40.2.100 with 32 bytes of data:

Request timed out.
Reply from 10.40.2.100: bytes=32 time<1ms TTL=126
Reply from 10.40.2.100: bytes=32 time<1ms TTL=126
Reply from 10.40.2.100: bytes=32 time<1ms TTL=126

Ping statistics for 10.40.2.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Using the ping command, we can verify reachability from the 10.2.1.0/24 network to the 10.40.2.0/24 network and confirm that traffic can flow in both directions. A successful ping indicates that the static routes on Distribution-1 and Distribution-2 are correctly configured, allowing traffic to traverse the routed link and reach its destination. Additionally, it verifies that responses from the destination network are able to return to the source, confirming end-to-end connectivity.

From PC2 (10.20.1.100/24), use **tracert** (traceroute) to examine the path to PC7 (10.40.2.100).

```
C:\> tracert 10.40.2.100

Tracing route to 10.40.2.100 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      10.20.1.1
  2    0 ms      0 ms      0 ms      10.222.100.2
  3    0 ms      0 ms      0 ms      10.40.2.100

Trace complete.

C:\>
```

Using the **tracert** command, we can observe the path that packets take to reach the remote network, showing that the traffic passes through both Layer 3 switches.

The first hop (10.20.1.1) in the output represents the default gateway of the device initiating the trace (PC2), which directs the packet towards the destination network. The subsequent hop is the routed port on the opposite distribution switch, confirming that the static routes are functioning correctly and traffic is being forwarded as expected. This verification ensures that the path between the source and destination is properly configured across the Layer 3 infrastructure.

A Step-by-Step Explanation of VLANs, Trunking and Routing

Here's a step-by-step explanation of how the packet travels from PC2 at 10.20.1.100/24 to PC7 at 10.40.2.100/24:

1. **PC2 Sends the Packet:**
    - PC2, with IP address 10.20.1.100/24, needs to send a packet to PC7 at 10.40.2.100/24.
    - Since PC7 is in a different network, PC2 forwards the packet to its default gateway, Distribution-1's SVI at 10.20.1.1.
    - PC2 encapsulates the packet in a frame with the destination MAC address of Distribution-1's SVI (10.20.1.1). If PC2 does not already know the MAC address, it sends an ARP request to resolve it.

2. **Packet Reaches Access-1-3:**
    - The frame is sent to Access-1-3 on a VLAN 20 access port (untagged).
    - Access-1-3 examines its MAC address table, finds that the destination MAC Address is reachable through its trunk port, and forwards the frame out the trunk port with an 802.1Q VLAN 20 tag.

3. **Access-1-1 Receives the Frame:**
    - Access-1-1 receives the frame on its trunk port.
    - It removes the VLAN 20 tag but still notes the frame belongs to VLAN 20.
    - After searching its MAC address table for the destination MAC address, Access-1-1 forwards the frame out its trunk port to Distribution-1, adding back the VLAN 20 tag.

4. **Distribution-1 Processes the Frame:**
    - Distribution-1 receives the frame on its trunk port and sees the destination MAC address matches its VLAN 20 SVI.
    - Distribution-1 removes the VLAN 20 tag and processes the packet at Layer 3 because it is also a router, not to mention the default gateway for PC2.
    - Distribution-1 checks its routing table, determines the next hop is Distribution-2, and forwards the packet out its routed port G1/0/23.
    - The destination MAC address is that of Distribution-2's next-hop IP address 10.222.100.2.

5. **Packet Travels to Distribution-2:**
    - Distribution-2 receives the packet on its routed port G1/0/23, after de-encapsulating the packet from the frame.
    - It checks the destination IP address (10.40.2.100) and consults its routing table to determine the next hop.
    - Distribution-2 encapsulates the packet in a frame with the destination MAC address of PC7. If it does not already know PC7's MAC address, it sends an ARP request to resolve it.
    - Since the connected interface belongs to VLAN 40, Distribution-2 adds an 802.1Q VLAN 40 tag and forwards the frame out its G1/0/1 trunk port.

6. **Access-2-1 Processes the Frame:**
    - Access-2-1 receives the frame on its trunk port with the VLAN 40 tag, and removes the tag.
    - It examines the destination MAC address and consults its MAC address table then determines the frame should be forwarded to Access-2-3.
    - Access-2-1 forwards the frame out its trunk port with a new VLAN 40 tag.

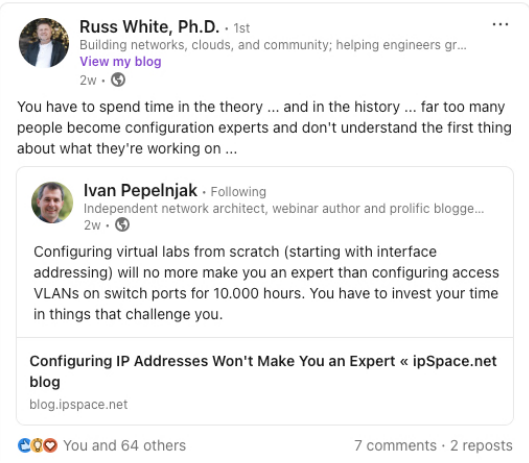
7. **Access-2-3 Forwards the Frame:**
    - Access-2-3 receives the frame on its trunk port, removes the VLAN 40 tag.
    - It examines the destination MAC address and determines that PC7 is reachable through its access port Fa0/6, which belongs to VLAN 40.
    - Access-2-3 forwards the frame out Fa0/6.

8. **PC7 Receives the Packet:**
    - PC7 receives the frame on its access port (untagged for VLAN 40).
    - The destination MAC address matches PC7's MAC address, and the packet is processed at Layer 3. The destination IP address also matches PC7's IP address (10.40.2.100).

Key Points:

- **VLAN Tagging and Trunking:** VLAN tags (802.1Q) are added and removed as the frame traverses the network, ensuring it is correctly handled within its VLAN.
- **Routing Between Networks:** Distribution-1 and Distribution-2 perform Layer 3 routing to forward packets between VLAN 20 and VLAN 40.
- **MAC Address Resolution:** ARP requests may occur at various points to resolve unknown MAC addresses.
- **Layer 2 and Layer 3 Integration:** This process demonstrates how VLANs, trunking, and routing work together to provide end-to-end connectivity.

Important Note



Although many people can follow the steps to configure a network and may have a general understanding of what is happening, it often takes someone with experience to fully comprehend the intricate processes at play. Knowing each individual part—VLANs, trunking, routing, ARP, MAC address tables, and other protocols—is important, but putting them together seamlessly requires a deeper level of understanding that comes with time and practice.

Once you begin to grasp how these parts interact and influence one another, it sets you apart from others, even those who might hold certifications you do not yet have. The key is not just in performing configurations but in truly understanding the underlying protocols and mechanisms that make the network function. No matter how many times you configure a feature, it is this deeper knowledge of how the parts fit together that will distinguish you as a skilled and capable network professional.