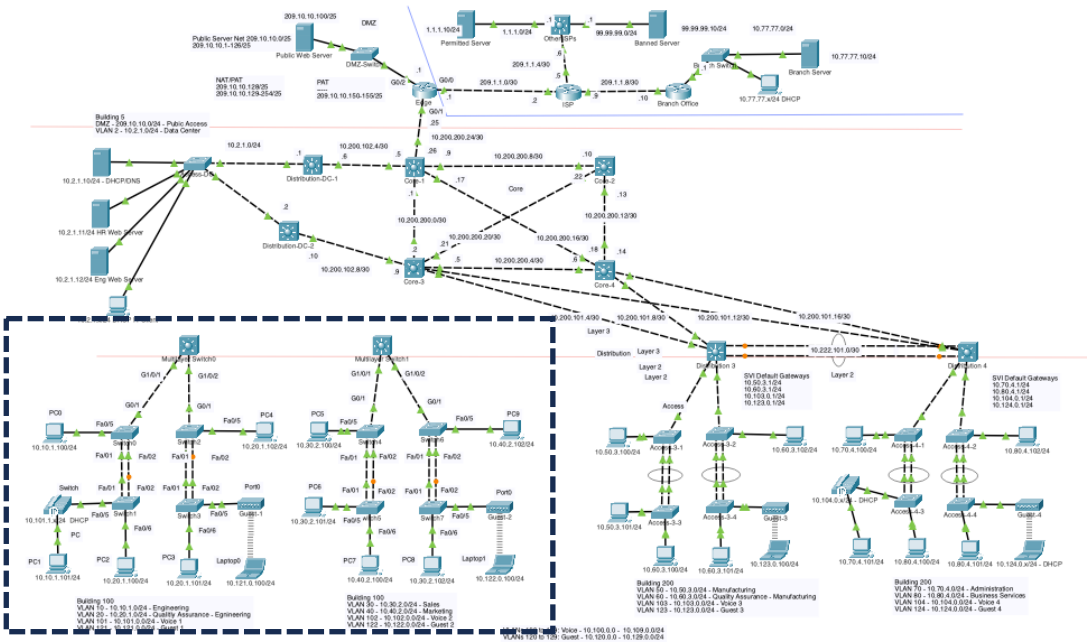
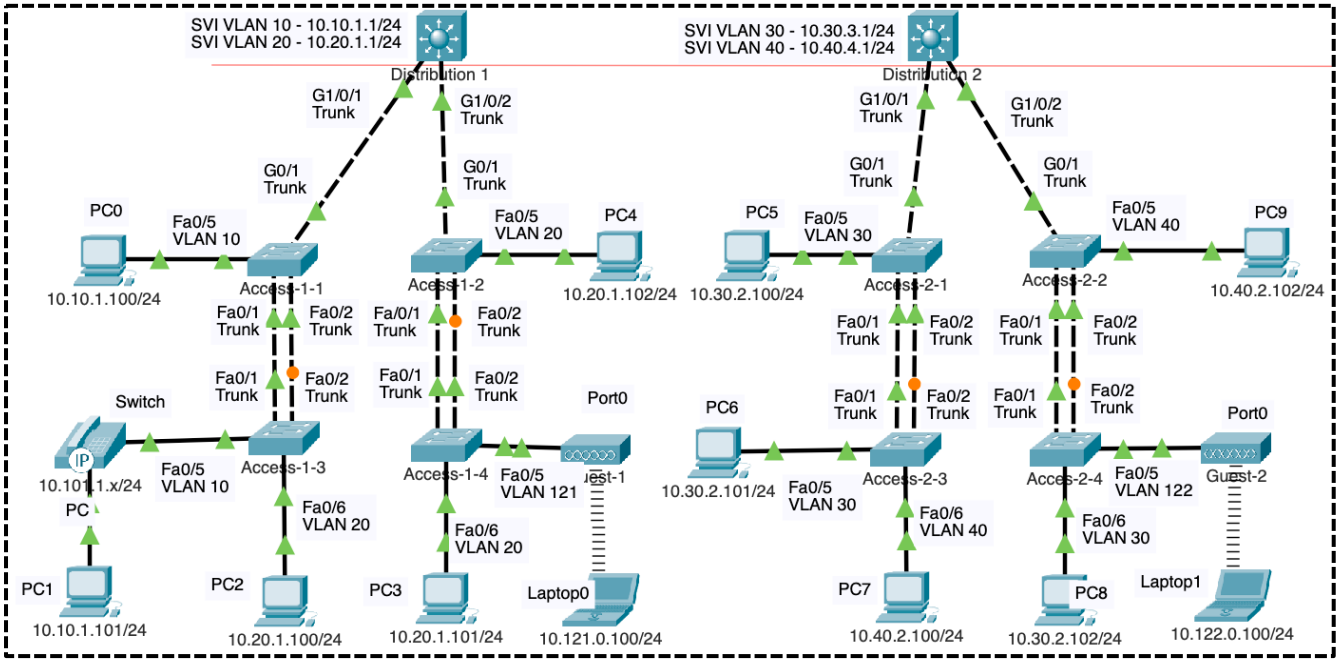
Enterprise Network
Lab 3 – Switched Virtual Interface (SVI)





Note: The SVI addressing on the Distribution switches will be configured later in this lab.

Current Topology and Objectives

In the previous lab you configured the access VLANs and trunk links for the above topology. The topology has been updated to indicate the VLANs and trunk links.

The list of objectives covered in this lab:

1. **Understand the Role of SVIs**: Learn how Switched Virtual Interfaces (SVIs) enable remote management and inter-VLAN routing on switches.
2. **Configure SVIs**: Configure SVIs on both Layer 2 and Layer 3 switches to provide IP addresses for VLANs.
3. **Enable Routing**: Enable routing on Layer 3 switches to allow inter-VLAN communication.
4. **Verify Connectivity**: Test connectivity between devices in the same VLAN and across different VLANs using tools like ping and traceroute.
5. **Examine Routing Tables**: Analyze the routing tables on switches to understand the role of directly connected routes.
6. **Management VLAN Setup**: Discuss best practices for configuring a dedicated management VLAN to access switches securely.
7. **Practical Troubleshooting**: Verify and troubleshoot SVI configurations and connectivity issues.

Switched Virtual Interfaces (SVIs)

An **SVI (Switched Virtual Interface)** is a virtual interface assigned to a VLAN on a switch. It allows the switch to have an IP address for that VLAN, which can be used for remote management, such as accessing the switch via SSH or Telnet.

An SVI is similar to a computer connected to a switch because both are assigned an IP address and associated with a specific VLAN. Just as a computer needs an IP address to communicate on a network, an SVI provides an IP address for the switch itself, allowing it to communicate within the VLAN.

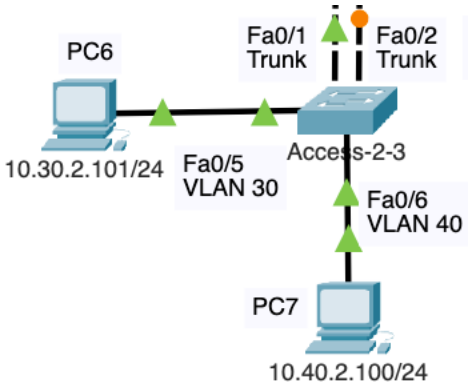
We will see in a moment that the SVI also plays a role in multilayer switches, enabling Layer 3 functionality, allowing the switch to route traffic between VLANs/IP networks.

SVIs on Layer 2 Switches

To enable remote management on a Layer 2 switch, you can configure a Switched Virtual Interface (SVI) by assigning an IP address to a specific VLAN. This allows the switch to be accessed remotely using protocols like SSH or Telnet, providing a convenient way to manage the switch without being physically present.

Configuring SVIs on Layer 2 Switches

Only devices in the same VLAN and IP network as the switch's SVI can communicate with the switch's IP address. Devices on a different VLAN and IP network than the switch's SVI will not be able to remotely access the switch unless routing has been configured.



If the Access-2-3 switch is configured with an SVI on the 10.30.2.0/24 network for VLAN 30 (e.g., IP address 10.30.2.8/24), only devices within the same IP network and VLAN, such as PC6 (10.30.2.101/24 on VLAN 30), will be able to directly communicate with the switch's IP address. Devices in a different VLAN or IP network, like PC7 (10.40.2.100/24 on VLAN 40), will not be able to communicate with the switch's SVI unless routing is enabled somewhere on the network.

```
access-2-3(config)# interface vlan 30

%LINK-5-CHANGED: Interface Vlan30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up

access-2-3(config-if)# ip address 10.30.2.8 255.255.255.0
access-2-3(config-if)# end

access-2-3# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual up                    up
<output omitted for brevity>
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  unassigned      YES manual administratively down down
Vlan30                 10.30.2.8       YES manual up                    up
access-2-3#
```

In the example above, access-2-3 is configured with the SVI 10.30.2.8/24 on VLAN 30.

- **interface vlan 30** - This command creates or selects the VLAN 30 SVI (Switched Virtual Interface) for configuration. When the command is entered, the switch automatically activates the interface, as indicated by the %LINK-5-CHANGED and %LINEPROTO-5-UPDOWN messages. Unlike physical interfaces, an SVI comes up without the no shutdown command if the VLAN is active and there are operational switch ports in the VLAN.
- **ip address 10.30.2.8 255.255.255.0** - This assigns the IP address 10.30.2.8 with a subnet mask of 255.255.255.0 to the VLAN 30 SVI. This IP address allows the switch to communicate on the 10.30.2.0/24 subnet for management purposes.

The **show ip interface brief** command can be used to verify the IP address of the SVI and that it is operational.

- **show ip interface brief** - This command provides a summary of all interfaces, showing their IP addresses, operational status (Status), and protocol status (Protocol).
- **VLAN 30 (10.30.2.8)**: The Status and Protocol columns both show up, indicating the interface is active and operational. This confirms that the VLAN 30 SVI is functional.

Key Point: The SVI (VLAN 30) interface comes up automatically without using the no shutdown command because VLAN 30 has active member ports (e.g., FastEthernet 0/5) in the VLAN, and the VLAN itself is active in the VLAN database. ***For an SVI to remain up, the VLAN must have at least one operational switch port, either an access port or a trunk port. Otherwise, it is an SVI to nowhere.***

Verify Reachability to SVI

From PC6, 10.30.2.101/24 ping the switch's SVI 10.30.2.8

```
C:\>ping 10.30.2.8

Pinging 10.30.2.8 with 32 bytes of data:

Request timed out.
Reply from 10.30.2.8: bytes=32 time<1ms TTL=255
Reply from 10.30.2.8: bytes=32 time<1ms TTL=255
Reply from 10.30.2.8: bytes=32 time<1ms TTL=255

Ping statistics for 10.30.2.8:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>arp -a
  Internet Address      Physical Address      Type
  10.30.2.8             00e0.f753.b601        dynamic

C:\>
```

PC6 can now ping the SVI on the switch (IP address 10.30.2.8) because both PC6 and the SVI are on the same IP network (10.30.2.0/24) and VLAN (VLAN 30). This allows direct communication without requiring routing.

The ARP table on PC6 shows that it has learned the MAC address associated with the switch's SVI IP address (10.30.2.8). The physical address **00e0.f753.b601** corresponds to the MAC address of VLAN 30 on the Access-2-3 switch, confirming successful Layer 2 communication between PC6 and the switch, as shown with the **show interface vlan 30** command on the switch.

```
access-2-3# show interface vlan 30
Vlan30 is up, line protocol is up
  Hardware is CPU Interface, address is 00e0.f753.b601 (bia 00e0.f753.b601)
  Internet address is 10.30.2.8/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1682 packets input, 530955 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     563859 packets output, 0 bytes, 0 underruns
     0 output errors, 23 interface resets
     0 output buffer failures, 0 output buffers swapped out

access-2-3#
```

Verify that PC6, 10.30.2.101/24 can now remotely log into this switch using ssh.

```
C:\>ssh -l admin 10.30.2.8

Password: sshadmin

access-2-3>show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.9726.8c01    DYNAMIC     Fa0/1
  10    0001.9726.8c01    DYNAMIC     Fa0/1
  20    0001.9726.8c01    DYNAMIC     Fa0/1
  30    0001.9726.8c01    DYNAMIC     Fa0/1
  30    0002.1781.8345    DYNAMIC     Fa0/5
  40    0001.9726.8c01    DYNAMIC     Fa0/1
 101    0001.9726.8c01    DYNAMIC     Fa0/1
 102    0001.9726.8c01    DYNAMIC     Fa0/1
 121    0001.9726.8c01    DYNAMIC     Fa0/1
 122    0001.9726.8c01    DYNAMIC     Fa0/1
 180    0001.9726.8c01    DYNAMIC     Fa0/1
 254    0001.9726.8c01    DYNAMIC     Fa0/1
access-2-3>exit

[Connection to 10.30.2.8 closed by foreign host]
C:\>
```

Note: If ssh is not working, verify that the switch has been configured with the necessary commands:

```
access-2-3(config)#username admin secret sshadmin
access-2-3(config)#ip domain-name SSH-KEY.com

access-2-3(config)#crypto key generate rsa general-keys modulus 1024

access-2-3(config)#line vty 0 15
access-2-3(config-line)# login local
access-2-3(config-line)# transport input ssh
access-2-3(config-line)# exit
```

From PC7, 10.40.2.100/24, attempt to ping the switch's IP address 10.30.2.8.

```
C:\>ping 10.30.2.8

Pinging 10.30.2.8 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.30.2.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.30.2.101

Pinging 10.30.2.101 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.30.2.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Of course, without routing enable, PC7 cannot ping any device on a different IP network (VLAN), including access-2-3 switch (10.30.2.8) and PC6 (10.30.2.101). Once we have routing enabled, this will no longer be an issue.

The Management VLAN

It is considered best practice to use a dedicated **management VLAN** for accessing Layer 2 and Layer 3 switches. A management VLAN is a separate network, isolated from user data traffic, designed specifically for accessing the switch's SVIs and performing administrative tasks. This VLAN does not have any access ports assigned to it, as it is not intended for end-user devices; instead, it is reserved solely for management purposes. However, trunk ports on the switch must be configured to carry the management VLAN to ensure connectivity between devices in the management network. Additionally, routing must be enabled to allow administrators to reach the management VLAN from other networks, ensuring secure and efficient access to network devices without mixing management traffic with regular user data traffic.

For example, in our scenario VLAN 180, 10.180.x.x network has been reserved for the Management VLAN.

Note: The management VLAN will be discussed in a separate lab.

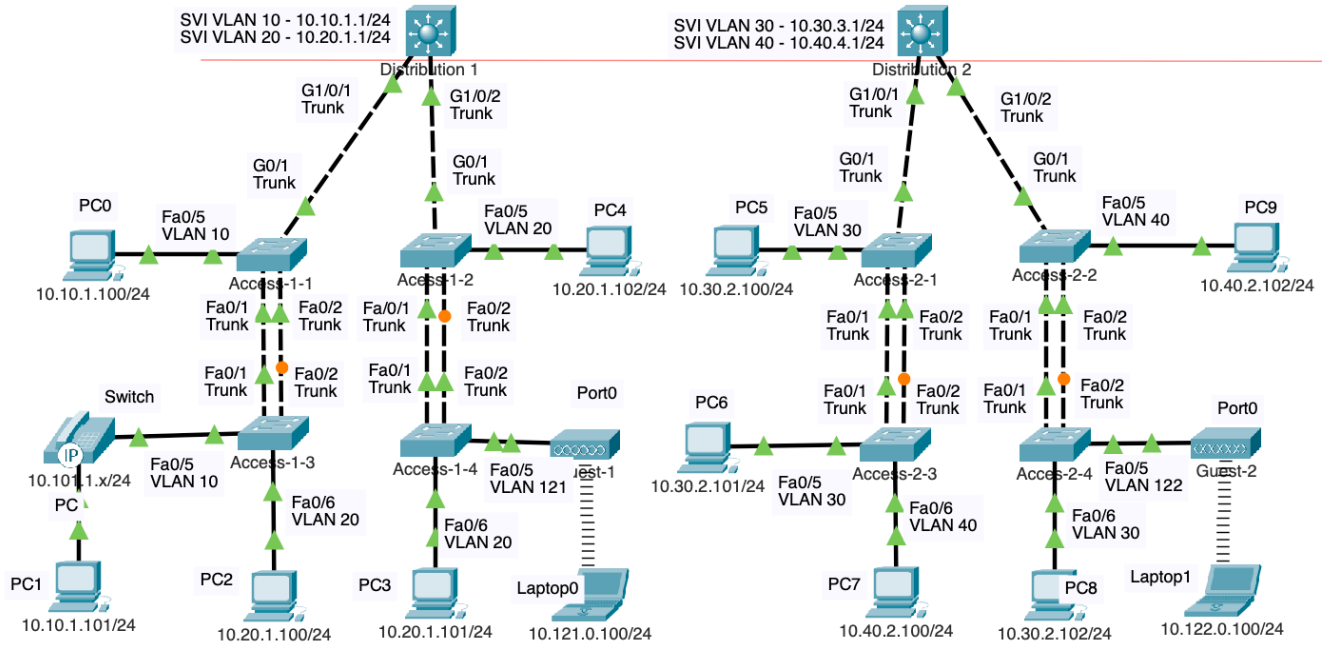
Configuring SVIs on Access-x-x Switches

You have the option of configuring an SVI on the other seven Access-x-x switches, but this is not necessary as we will see how to use a management VLAN in a later lab. If you choose to configure an SVI on each of these switches, be sure to choose a VLAN/IP network that is reachable from one of the PCs. Once again, only a PC on the same VLAN/IP network as the switch SVI will be able to ping/ssh the switch until we enable routing.

SVIs on Layer 3 Switches

As we have seen previously, there is no reachability between devices in different VLANs/IP networks.

In this section, we will configure the Distribution-1 and Distribution-2 multilayer (Layer 3) switches, with SVI IP addresses that will be used as the default gateway addresses for devices on those networks. We will also need to enable routing these Layer 3 switches.



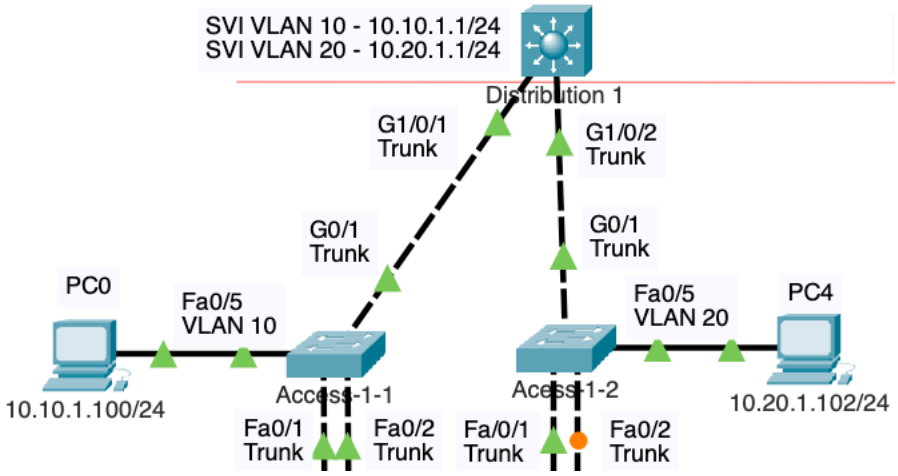
Switched Virtual Interfaces (SVIs) play an important role within the context of Layer 3 distribution layer switches. Similar to an SVI on a Layer 2 switch, an SVI is a virtual interface with an IP address that is associated with a specific VLAN and allows remote access to the switch using SSH or telnet.

An SVI on a Layer 3 switch also enables it to perform routing functions between VLANs, IP networks, without the need for an external router. Therefore, the SVI typically is the default gateway for end-devices on the same VLAN, the same IP network.

These are the default gateways on the PCs.

- Via Distribution-1 switch:
    - Devices on a VLAN 10 port, 10.10.1.0/24 network have the default gateway 10.10.1.1
    - Devices on a VLAN 20 port, 10.20.1.0/24 network have the default gateway 10.20.1.1
- Via Distribution-2 switch:
    - Devices on a VLAN 30 port, 10.30.2.0/24 network have the default gateway 10.30.2.1
    - Devices on a VLAN 40 port, 10.40.2.0/24 network have the default gateway 10.40.2.1

Configure the SVI on the Layer 3 Switch



Configure the SVIs on Distribution-1 switch that will used as the default gateway for devices on the VLAN/IP network.

```
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
```

Verify that both SVI are functional, up.

```
distribution-1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1/0/1   unassigned      YES unset  up                    up
GigabitEthernet1/0/2   unassigned      YES unset  up                    up
GigabitEthernet1/0/3   unassigned      YES unset  down                  down
GigabitEthernet1/0/4   unassigned      YES unset  down                  down
<output omitted>
GigabitEthernet1/1/4   unassigned      YES unset  down                  down
Vlan1                  unassigned      YES unset  administratively down down
Vlan10                 10.10.1.1       YES manual up                    up
Vlan20                 10.20.1.1       YES manual up                    up
distribution-1#
```

Verify that that the PCs on the VLAN/IP network can reach the SVI to be used as their default gateway. Below is the example from PC0, 10.10.1.100/24.

```
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 10.10.1.100

Pinging 10.10.1.100 with 32 bytes of data:

Reply from 10.10.1.100: bytes=32 time=3ms TTL=128
Reply from 10.10.1.100: bytes=32 time=1ms TTL=128
Reply from 10.10.1.100: bytes=32 time=3ms TTL=128
Reply from 10.10.1.100: bytes=32 time=7ms TTL=128

Ping statistics for 10.10.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 7ms, Average = 3ms

C:\>
```

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

```
C:\>ping 10.20.1.102

Pinging 10.20.1.102 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.20.1.102:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Notice that PC0, 10.10.1.100/24 is unable to reach PC4, 10.20.1.102/24 which is on different network. This is because we still have not enabled routing the Distribution-1 switch.

Enable Routing on a Layer 3 Switch

Examine the routing table on Distribution-1.

```
distribution-1# show ip route
Default gateway is not set

Host               Gateway           Last Use    Total Uses  Interface
ICMP redirect cache is empty

distribution-1#
```

Notice that the routing table not similar to a router's routing table but more that of a end device.

To enable routing, we must use the **ip routing** command.

```
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#
```

The IP network addresses **10.10.1.0/24** and **10.20.1.0/24** now 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.

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, meaning Distribution-1 can reach any devices on these IP networks. For this to work, Distribution-1 must have either an access port belonging to the VLAN or a trunk link carrying that VLAN to ensure connectivity to devices in the respective network.

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.

Once again, from PC0, 10.10.1.100/24 attempt to ping PC4, 10.20.1.102/24.

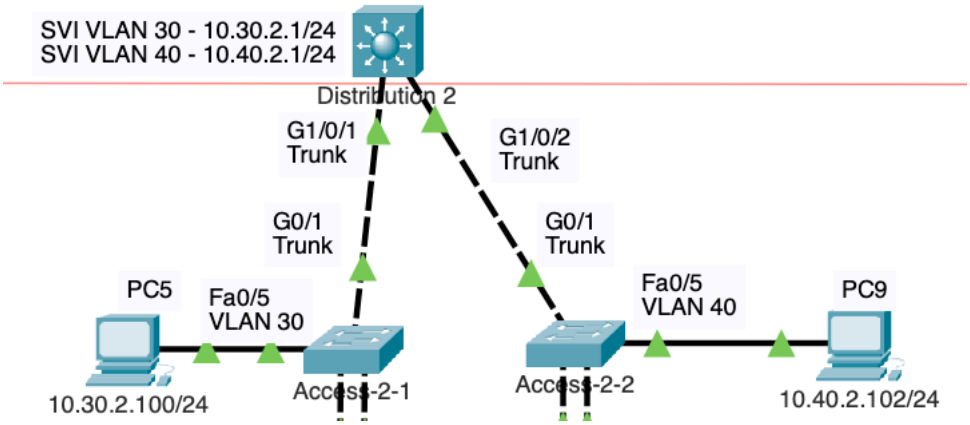
```
C:\>ping 10.20.1.102

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).

Configure and Verify Similar Functionality on Distribution-2



Perform similar configuration on Distribution-2.

```
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#
```

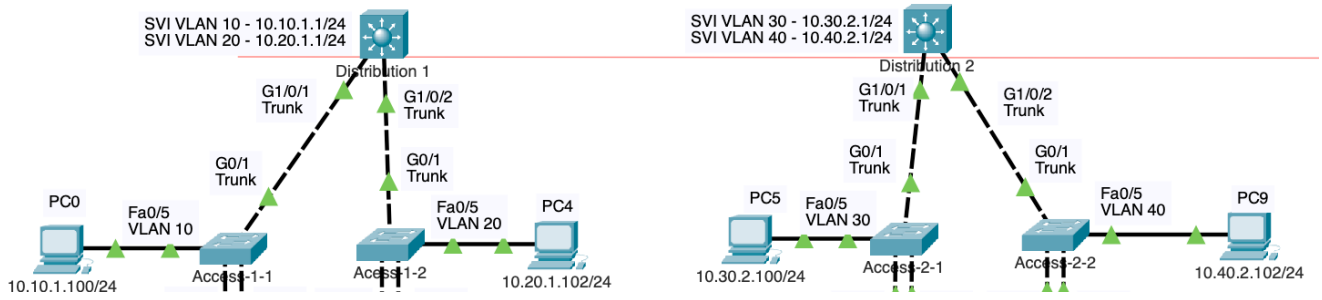
Similar to Distribution-1, routing can now occur between the two networks because **Distribution-2** is directly connected to both the **10.30.2.0/24** and **10.40.2.0/24** networks via the SVIs for VLAN 30 and VLAN 40. Once again, the exit interface in the routing table specifies the VLAN (e.g., VLAN 30 or VLAN 40) instead of a physical interface, meaning Distribution-2 can reach any devices on these IP networks. For this to work, Distribution-2 must have either an access port belonging to the VLAN or a trunk link carrying that VLAN to ensure connectivity to devices in the respective network.

Verify that there is reachability between devices on different VLAN/IP networks. From PC5, 10.30.2.100/24 attempt to ping PC9, 10.40.2.102/24.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::2D0:BAFF:FE28:2A96
   IPv6 Address.....: ::
   IPv4 Address.....: 10.30.2.100
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 10.30.2.1
C:\>ping 10.40.2.102

Pinging 10.40.2.102 with 32 bytes of data:

Request timed out.
Reply from 10.40.2.102: bytes=32 time<1ms TTL=127
Reply from 10.40.2.102: bytes=32 time<1ms TTL=127
Reply from 10.40.2.102: bytes=32 time<1ms TTL=127

Ping statistics for 10.40.2.102:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Similar to the Distribution-1, we have reachability between devices on different VLANs/IP networks connected to Distribution-2. Also similar to Distribution-1, all devices on both VLANs/IP networks with Distribution-2 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.

This will be done in the next lab!