



INSTITUT TEKNOLOGI DEL
LAPORAN UJIAN AKHIR SEMESTER GANJIL
SEMESTER GANJIL 2022/2023

Hari/Tanggal	Selasa/13 Desember 2021
Pukul	08.00 – 11.00 WIB
Mata Kuliah	1032101/1042101/Jaringan Komputer
Durasi	180 Menit
Dosen	ESS

Identitas:

Prodi : D4TRPL

Kelompok : 02 Anggota :

No.	NIM	Nama	Kontribusi
1.	11421036	Doli Rajagukguk	Laporan – Configure DTP – Configure IPv4 and IPv6 Static and default routes
2.	11421039	Josep Napitupulu	Laporan – Configure Layer 3 Switching and InterVLAN Routing – Configure IPv4 and IPv6 Static and default routes
3.	11421042	Loeis Lubis	Laporan – Subnet an IPv4 Network– Configure IPv4 and IPv6 Static and default routes
4.	11421058	Melince Yigibalom	Laporan–Configure IPv4 and IPv6 Static and default routes

1. SUBNETTING

Subnet an IPv4 Network

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
CustomerRouter	G0/0	192.168.0.1	255.255.255.192	N/A
	G0/1	192.168.0.65	255.255.255.192	N/A
	S0/1/0	209.165.201.2	255.255.255.252	N/A
LAN-A Switch	VLAN1	192.168.0.2	255.255.255.192	192.168.0.1
LAN-B Switch	VLAN1	192.168.0.66	255.255.255.192	192.168.0.65
PC-A	NIC	192.168.0.62	255.255.255.192	192.168.0.1
PC-B	NIC	192.169.0.126	255.255.255.192	192.168.0.65
ISPRouter	G0/0	209.165.200.225	255.255.255.224	N/A
	S0/1/0	209.165.201.1	255.255.255.252	N/A
ISPSwitch	VLAN1	209.165.200.226	255.255.255.224	209.165.200.225
ISP Workstation	NIC	209.165.200.235	255.255.255.224	209.165.200.225
ISP Server	NIC	209.165.200.240	255.255.255.224	209.165.200.225

Objectives

Part 1: Design an IPv4 Network Subnetting Scheme

Part 2: Configure the Devices

Part 3: Test and Troubleshoot the Network

Background / Scenario

In this activity, you will subnet the Customer network into multiple subnets. The subnet scheme should be based on the number of host computers required in each subnet, as well as other network considerations, like future network host expansion.

After you have created a subnetting scheme and completed the table by filling in the missing host and interface IP addresses, you will configure the host PCs, switches and router interfaces.

After the network devices and host PCs have been configured, you will use the **ping** command to test for network connectivity.

Instructions

Part 1: Subnet the Assigned Network

Step 1: Create a subnetting scheme that meets the required number of subnets and required number of host addresses.

In this scenario, you are a network technician assigned to install a new network for a customer. You must create multiple subnets out of the 192.168.0.0/24 network address space to meet the following requirements:

- The first subnet is the LAN-A network. You need a minimum of 50 host IP addresses.
- The second subnet is the LAN-B network. You need a minimum of 40 host IP addresses.
- You also need at least two additional unused subnets for future network expansion.

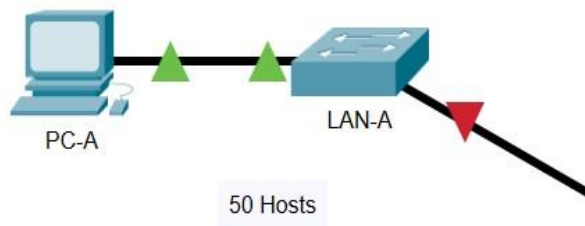
Note: Variable length subnet masks will not be used. All of the device subnet masks should be the same length.

- Answer the following questions to help create a subnetting scheme that meets the stated network requirements:

Questions:

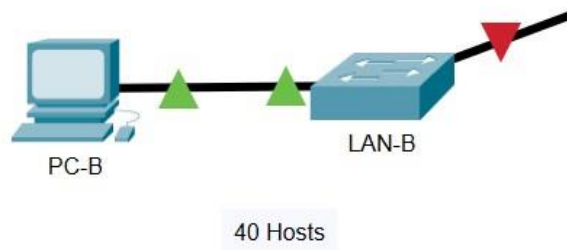
How many host addresses are needed in the largest required subnet?

50 host



What is the minimum number of subnets required?

40 host



The network that you are tasked to subnet is 192.168.0.0/24. What is the /24 subnet mask in binary?

11111111.11111111.11111111.00000000

- e. The subnet mask is made up of two portions, the network portion, and the host portion. This is represented in the binary by the ones and the zeros in the subnet mask.

Questions:

In the network mask, what do the ones represent?

Ones represent the network portion (1 melambangkan network portion)

In the network mask, what do the zeros represent?

Zeros represent the host portion (1 melambangkan host portion)

- f. To subnet a network, bits from the host portion of the original network mask are changed into subnet bits. The number of subnet bits defines the number of subnets.

Questions:

Given each of the possible subnet masks depicted in the following binary format, how many subnets and how many hosts are created in each example?

Hint: Remember that the number of host bits (to the power of 2) defines the number of hosts per subnet (minus 2), and the number of subnet bits (to the power of two) defines the number of subnets. The subnet bits (shown in bold) are the bits that have been borrowed beyond the original network mask of /24. The /24 is the prefix notation and corresponds to a dotted decimal mask of 255.255.255.0.

- 1) (/25) 11111111.11111111.11111111.10000000

Dotted decimal subnet mask equivalent:

255.255.255.128

Number of subnets? Number of hosts?

Subnets = $2^1 = 2$ subnets

Hosts = $(2^7 - 2) = 126$ hosts

- 2) (/26) 11111111.11111111.11111111.11000000

Dotted decimal subnet mask equivalent:

255.255.255.192

Number of subnets? Number of hosts?

Subnets = $2^2 = 4$ subnets

Hosts = $(2^6 - 2) = 62$ hosts

- 3) (/27) 11111111.11111111.11111111.11100000

Dotted decimal subnet mask equivalent:

255.255.255.224

Number of subnets? Number of hosts?

Subnets = $2^3 = 8$ subnets

Hosts = $(2^5 - 2) = 30$ hosts

- 4) (/28) 11111111.11111111.11111111.11110000

Dotted decimal subnet mask equivalent:

255.255.255.240

Number of subnets? Number of hosts?

Subnets = $2^4 = 16$ subnets

Hosts = $(2^4 - 2) = 14$ hosts

- 5) (/29) 11111111.11111111.11111111.11111000

Dotted decimal subnet mask equivalent:

255.255.255.248

Number of subnets? Number of hosts?

Subnets = $2^5 = 32$ subnets

Hosts = $(2^3 - 2) = 6$ hosts

- 6) (/30) 11111111.11111111.11111111.11111100

Dotted decimal subnet mask equivalent:

255.255.255.252

Number of subnets? Number of hosts?

Subnets = $2^6 = 64$ subnets

Hosts = $(2^2 - 2) = 2$ hosts

Considering your answers above, which subnet masks meet the required number of minimum host addresses?

(/25) 11111111.11111111.11111111.10000000 dan

(/26) 11111111.11111111.11111111.11000000

Considering your answers above, which subnet masks meet the minimum number of subnets required?

/26, /27, /28, /29, /30 akan memberikan jumlah subnet yang diperlukan

Considering your answers above, which subnet mask meets both the required minimum number of hosts and the minimum number of subnets required?

/26 berisi 4 subnets dan 62 hosts, yang mana lebih besar dari hosts yang disyaratkan, yaitu 50.

When you have determined which subnet mask meets all of the stated network requirements, derive each of the subnets. List the subnets from first to last in the table. Remember that the first subnet is 192.168.0.0 with the chosen subnet mask.

Subnet Address	Prefix	Subnet Mask
192.168.0.0	/26	255.255.255.192
192.168.0.64	/26	255.255.255.192
192.168.0.128	/26	255.255.255.192

192.168.0.192	/26	255.255.255.192
---------------	-----	-----------------

Step 2: Fill in the missing IP addresses in the Addressing Table

Assign IP addresses based on the following criteria: Use the ISP Network settings as an example.

- a. Assign the first subnet to LAN-A.
 - 1) Use the first host address for the CustomerRouter interface connected to LAN-A switch.
 - 2) Use the second host address for the LAN-A switch. Make sure to assign a default gateway address for the switch.
 - 3) Use the last host address for PC-A. Make sure to assign a default gateway address for the PC.
- b. Assign the second subnet to LAN-B.
 - 1) Use the first host address for the CustomerRouter interface connected to LAN-B switch.
 - 2) Use the second host address for the LAN-B switch. Make sure to assign a default gateway address for the switch.
 - 3) Use the last host address for PC-B. Make sure to assign a default gateway address for the PC.

Part 2: Configure the Devices

Configure basic settings on the PCs, switches, and router. Refer to the Addressing Table for device names and address information.

Step 1: Configure CustomerRouter.

- a. Set the enable secret password on CustomerRouter to **Class123**

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#enable secret Class123
```

- b. Set the console login password to **Cisco123**.

```
Router(config)#line console 0
Router(config-line)#password Cisco123
Router(config-line)#login
Router(config-line)#exit
```

- c. Configure **CustomerRouter** as the hostname for the router.

```
Router(config)#hostname CustomerRouter
CustomerRouter(config)#
```

- d. Configure the G0/0 and G0/1 interfaces with IP addresses and subnet masks, and then enable them.

```
CustomerRouter(config)#interface gigabitEthernet 0/0
CustomerRouter(config-if)#ip address 192.168.0.1 255.255.255.192
CustomerRouter(config-if)#no shutdown

CustomerRouter(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
```

```
CustomerRouter(config-if)#interface g0/1
CustomerRouter(config-if)#ip address 192.168.0.65
% Incomplete command.
CustomerRouter(config-if)#ip address 192.168.0.65 255.255.255.192
CustomerRouter(config-if)#no shutdown

CustomerRouter(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

- e. Save the running configuration to the startup configuration file.\

```
CustomerRouter#
%SYS-5-CONFIG_I: Configured from console by console
copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Step 2: Configure the two customer LAN switches.

Configure the IP addresses on interface VLAN 1 on the two customer LAN switches. Make sure to configure the correct default gateway on each switch.

Step 3: Configure the PC interfaces.

Configure the IP address, subnet mask, and default gateway settings on **PC-A** and **PC-B**.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.0.2
% Incomplete command.
Switch(config-if)#ip address 192.168.0.2 255.255.255.192
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

```
Switch(config)#ip default-gateway 192.168.0.1
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.0.66
% Incomplete command.
Switch(config-if)#ip address 192.168.0.66 255.255.255.192
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

```
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.168.0.65
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

Part 3: Test and Troubleshoot the Network

In Part 3, you will use the **ping** command to test network connectivity.

- Determine if PC-A can communicate with its default gateway. Do you get a reply?

Yes

- Determine if PC-B can communicate with its default gateway. Do you get a reply?

Yes

- Determine if PC-A can communicate with PC-B. Do you get a reply?

Yes

If you answered “no” to any of the preceding questions, then you should go back and check your IP address and subnet mask configurations, and ensure that the default gateways have been correctly configured on PC-A and PC-B.

2. VLAN

Configure DTP

Addressing Table

Device	Interface	IP Address	Subnet Mask
PC1	NIC	192.168.10.1	255.255.255.0
PC2	NIC	192.168.20.1	255.255.255.0
PC3	NIC	192.168.30.1	255.255.255.0
PC4	NIC	192.168.30.2	255.255.255.0
PC5	NIC	192.168.20.2	255.255.255.0
PC6	NIC	192.168.10.2	255.255.255.0
S1	VLAN 99	192.168.99.1	255.255.255.0
S2	VLAN 99	192.168.99.2	255.255.255.0
S3	VLAN 99	192.168.99.3	255.255.255.0

Objectives

- Configure static trunking •

Configure and Verify DTP

Background / Scenario

As the number of switches in a network increases, the administration necessary to manage the VLANs and trunks can be challenging. To ease some of the VLAN and trunking configurations, trunk negotiation between network devices is managed by the Dynamic Trunking Protocol (DTP), and is automatically enabled on Catalyst 2960 and Catalyst 3650 switches.

In this activity, you will configure trunk links between the switches. You will assign ports to VLANs and verify end-to-end connectivity between hosts in the same VLAN. You will configure trunk links between the switches, and you will configure VLAN 999 as the native VLAN.

Instructions

Part 4: Verify VLAN configuration.

Verify the configured VLANs on the switches.

Step 1: On S1, go to privileged EXEC mode and enter the **show vlan brief** command to verify the VLANs that are present.

```
S1# show vlan brief
```

VLAN Name

Status

Ports

```
-----  
1      default                                active    Fa0/1, 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

```

99    Management          active
999   Native              active
      1002    fddi-default    active
      1003    token-ring-default active
      1004    fddinet-default active
      1005    trnet-default   active
  
```

Step 2: Repeat Step 1a on S2

and S3.

```

S2>enable
S2#show vlan brief
  
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, 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
99	Management	active	
999	Native	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```

S3>enable
S3#show vlan brief
  
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, 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
99	Management	active	
999	Native	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Question:

What VLANs are configured on the switches? **Vlan 99 dan 999 dikonfirmasi pada semua switch**

Part 5: Create additional VLANs on S2 and S3.

Step 1: On S2, create VLAN 10 and name it Red.

```
S2(config)# vlan 10
S2(config-vlan)# name Red
```

Step 2: Create VLANs 20 and 30 according to the table below.

VLAN Number	VLAN Name
10	Red
20	Blue
30	Yellow

Step 3: Verify the addition of the new VLANs. Enter **show vlan brief** at the privileged EXEC mode.

```
S2(config-vlan)#name Red
S2(config-vlan)#vlan 20
S2(config-vlan)#name Blue
S2(config-vlan)#vlan 30
S2(config-vlan)#name Yellow
S2(config-vlan)#show vlan brief
^
% Invalid input detected at '^' marker.

S2(config-vlan)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/1, 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
10   Red                    active
20   Blue                   active
30   Yellow                 active
99   Management             active
999  Native                 active
1002 fddi-default           active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active
~^"
```

Question:

In addition to the default VLANs, which VLANs are configured on S2?

VLAN 10 (Red), VLAN 20 (Blue), VLAN 30 (Yellow), VLAN 99 (Management), VLAN 999 (Native)

Step 4: Repeat the previous steps to create the additional VLANs on S3.

```
S3#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, 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
10	Red	active	
20	Blue	active	
30	Yellow	active	
99	Management	active	
999	Native	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Part 6: Assign VLANs to Ports

Use the **switchport mode access** command to set access mode for the access links. Use the **switchport access vlan *vlan-id*** command to assign a VLAN to an access port.

Ports	Assignments	Network
S2 F0/1 – 8 S3 F0/1 – 8	VLAN 10 (Red)	192.168.10.0 /24
S2 F0/9 – 16 S3 F0/9 – 16	VLAN 20 (Blue)	192.168.20.0 /24
S2 F0/17 – 24 S3 F0/17 – 24	VLAN 30 (Yellow)	192.168.30.0 /24

Step 1: Assign VLANs to ports on S2 using assignments from the table above.

```
S2(config-if)# interface range f0/1 - 8
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 10
S2(config-if-range)# interface range f0/9 -16
S2(config-if-range)# switchport mode access
```

```

S2(config-if-range) # switchport access vlan 20
S2(config-if-range) # interface range f0/17 - 24
S2(config-if-range) # switchport mode access
S2(config-if-range) # switchport access vlan 30

```

Step 2: Assign VLANs to ports on S3 using the assignments from the table above.

Now that you have the ports assigned to VLANs, try to ping from **PC1** to **PC6**.

Question:

Was the ping successful? Explain.

```

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.2: bytes=32 time=11ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 3ms

C:\>

```

Tidak, ping akan gagal karena port antara switch berada di VLAN 1 dan PC1 Serta PC6 berada di VLAN 10.

Part 7: Configure Trunks on S1, S2, and S3.

Dynamic trunking protocol (DTP) manages the trunk links between Cisco switches. Currently, all the switchports are in the default trunking mode, which is dynamic auto. In this step, you will change the trunking mode to dynamic desirable for the link between switches S1 and S2. The link between switches S1 and S3 will be set as a static trunk. Use VLAN 999 as the native VLAN in this topology.

Step 1: On switch S1, configure the trunk link to dynamic desirable on the GigabitEthernet 0/1 interface. The configuration of S1 is shown below.

```

S1(config) # interface g0/1
S1(config-if) # switchport mode dynamic desirable

```

Question:

What will be the result of trunk negotiation between S1 and S2?

Link batang sudah ditetapkan di antara S1 dan S2

Step 2: On switch S2, verify that the trunk has been negotiated by entering the **show interfaces trunk** command. Interface GigabitEthernet 0/1 should appear in the output.

```
S2#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Gig0/1	auto	n-802.1q	trunking	1

Port	Vlans allowed on trunk
Gig0/1	1-1005

Port	Vlans allowed and active in management domain
Gig0/1	1,10,20,30,99,999

Port	Vlans in spanning tree forwarding state and not pruned
Gig0/1	1,10,20,30,99,999

Question:

What is the mode and status for this port?

Mode auto, dengan **Status** trunking

Step 3: For the trunk link between S1 and S3, configure interface GigabitEthernet 0/2 as a static trunk link on S1. In addition, disable DTP negotiation on interface G0/2 on S1.

```
S1(config)# interface g0/2
S1(config-if)# switchport mode trunk
S1(config-if)# switchport nonegotiate
```

Step 4: Use the **show dtp** command to verify the status of DTP.

```
S1# show dtp
Global DTP information
  Sending DTP Hello packets every 30 seconds
  Dynamic Trunk timeout is 300 seconds
  1 interfaces using DTP
```

Step 5: Verify trunking is enabled on all the switches using the **show interfaces trunk** command.

```
S1# show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Gig0/1	desirable	n-802.1q	trunking	1
Gig0/2	on	802.1q	trunking	1


```

Port          Vlans allowed on trunk
Gig0/1        1-1005
Gig0/2        1-1005
Port          Vlans allowed and active in management domain
Gig0/1        1,99,999
Gig0/2        1,99,999

Port          Vlans in spanning tree forwarding state and not pruned
Gig0/1        1,99,999
Gig0/2        1,99,999
S1(config-if)#switchport mode trunk
S1(config-if)#switchport nonegotiate
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show dtp
Global DTP information
  Sending DTP Hello packets every 30 seconds
  Dynamic Trunk timeout is 300 seconds
  1 interfaces using DTP
S1#show interfaces trunk
Port          Mode          Encapsulation  Status        Native vlan
Gig0/1        desirable    n-802.1q       trunking      1
Gig0/2        on           802.1q         trunking      1

Port          Vlans allowed on trunk
Gig0/1        1-1005
Gig0/2        1-1005

Port          Vlans allowed and active in management domain
Gig0/1        1,99,999
Gig0/2        1,99,999

Port          Vlans in spanning tree forwarding state and not pruned
Gig0/1        1,99,999
Gig0/2        1,99,999

```

Question:

What is the native VLAN for these trunks currently?

VLAN 1

Step 6: Configure VLAN 999 as the native VLAN for the trunk links on S1.

```

S1(config)# interface range g0/1 - 2
S1(config-if-range)# switchport trunk native vlan 999

```

Question:

What messages did you receive on S1? How would you correct it?


```

S1#show dtp
Global DTP information
    Sending DTP Hello packets every 30 seconds
    Dynamic Trunk timeout is 300 seconds
    1 interfaces using DTP
S1#

```

Step 7: On S2 and S3, configure VLAN 999 as the native VLAN.

```

S2(config)#interface g0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 999
S2(config-if)#show dtp
      ^
% Invalid input detected at '^' marker.

S2(config-if)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#show dtp
Global DTP information
    Sending DTP Hello packets every 30 seconds
    Dynamic Trunk timeout is 300 seconds
    1 interfaces using DTP
S2#

```

Enter configuration commands

```

S3(config)#interface g0/2

```

Enter configuration commands

```

S3(config-if)#switchport mode trunk

S3(config-if)#switchport trunk native vlan 999

S3#show dtp
Global DTP information
    Sending DTP Hello packets every 30 seconds
    Dynamic Trunk timeout is 300 seconds
    1 interfaces using DTP
S3#

```

Step 8: Verify trunking is successfully configured on all the switches. You should be able ping one switch from another switch in the topology using the IP addresses configured on the SVI.

```
S1#ping 192.168.99.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.2, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms

S1#ping 192.168.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.3, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms
```

Step 9: Attempt to ping from PC1 to PC6.

Question:

Why was the ping unsuccessful? (Hint: Look at the '**show vlan brief**' output from all three switches. Compare the outputs from the '**show interface trunk**' on all switches.)

```
S1#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, 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
99 Management	active	
999 Native	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```
S1#
```

```

S1#show int trun
Port      Mode      Encapsulation  Status      Native vlan
Gig0/1    desirable n-802.1q       trunking    999
Gig0/2    on        802.1q         trunking    999

Port      Vlans allowed on trunk
Gig0/1    1-1005
Gig0/2    1-1005

Port      Vlans allowed and active in management domain
Gig0/1    1,99,999
Gig0/2    1,99,999

Port      Vlans in spanning tree forwarding state and not pruned
Gig0/1    1,99,999
Gig0/2    1,99,999

```

Ping tidak berhasil karena VLAN pada S1 tidak terset dengan baik

Step 10: Correct the configuration as necessary

```

S1(config)#vlan 10
S1(config-vlan)#name Red
S1(config-vlan)#vlan 20
S1(config-vlan)#name Blue
S1(config-vlan)#vlan 30
S1(config-vlan)#name Yellow
S1(config-vlan)#exit

```

```

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=1ms TTL=128
Reply from 192.168.10.2: bytes=32 time=1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

Part 8: Reconfigure trunk on S3.

Step 1: Issue the '**show interface trunk**' command on **S3**.

```
S3>enable
S3#show interface trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Gig0/2	on	802.1q	trunking	999


```
Port      Vlans allowed on trunk
Gig0/2    1-1005
```



```
Port      Vlans allowed and active in management domain
Gig0/2    1,10,20,30,99,999
```



```
Port      Vlans in spanning tree forwarding state and not pruned
Gig0/2    1,10,20,30,99,999
```

Question:

What is the mode and encapsulation on G0/2?

Mode on dan Encapsulasi pada G0/2 802.1q

Step 2: Configure **G0/2** to match **G0/2** on **S1**.

```
S3(config)#interface g0/2
S3(config-if)#switchport nonegotiate
S3(config-if)#exit
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#show interface trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Gig0/2	on	802.1q	trunking	999


```
Port      Vlans allowed on trunk
Gig0/2    1-1005
```



```
Port      Vlans allowed and active in management domain
Gig0/2    1,10,20,30,99,999
```



```
Port      Vlans in spanning tree forwarding state and not pruned
Gig0/2    1,10,20,30,99,999
```

Question:

What is the mode and encapsulation on G0/2 after the change?

Mode on dan Encapsulasi 802.1q

Step 3: Issue the command '**show interface G0/2 switchport**' on switch **S3**.


```
S3#show interface G0/2 switchport
Name: Gig0/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 999 (Native)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
--More--
```

Question:

What is the 'Negotiation of Trunking' state displayed?

Off

Part 9: Verify end to end connectivity.

Step 1: From PC1 ping PC6.

```
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Step 2: From PC2 ping PC5.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time=2ms TTL=128
Reply from 192.168.20.2: bytes=32 time<1ms TTL=128
Reply from 192.168.20.2: bytes=32 time<1ms TTL=128
Reply from 192.168.20.2: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

Step 3: From PC3 ping PC4.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.2

Pinging 192.168.30.2 with 32 bytes of data:

Reply from 192.168.30.2: bytes=32 time=2ms TTL=128
Reply from 192.168.30.2: bytes=32 time<1ms TTL=128
Reply from 192.168.30.2: bytes=32 time=1ms TTL=128
Reply from 192.168.30.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

3. INTER-VLAN ROUTING

Configure Layer 3 Switching and Inter-VLAN Routing

Addressing Table

Device	Interface	IP Address / Prefix
MLS	VLAN 10	192.168.10.254 /24
		2001:db8:acad:10::1/64
	VLAN 20	192.168.20.254 /24
		2001:db8:acad:20::1/64
	VLAN 30	192.168.30.254/24
		2001:db8:acad:30::1/64
	VLAN 99	192.168.99.254/24
	G0/2	209.165.200.225
		2001:db8:acad:a::1/64
PC0	NIC	192.168.10.1
PC1	NIC	192.168.20.1
PC2	NIC	192.168.30.1
PC3	NIC	192.168.10.2/24
		2001:db8:acad:10::2/64
PC4	NIC	192.168.20.2/24
		2001:db8:acad:20::2/64
PC5	NIC	192.168.30.2
		2001:db8:acad:10::2/64
S1	VLAN 99	192.168.99.1
S2	VLAN 99	192.168.99.2
S3	VLAN 99	192.168.99.3

Objectives

Part 1: Configure Layer 3 Switching

Part 2: Configure Inter-VLAN Routing

Part 3: Configure IPv6 Inter-VLAN Routing

Background / Scenario

A multilayer switch like the Cisco Catalyst 3650 is capable of both Layer 2 switching and Layer 3 routing. One of the advantages of using a multilayer switch is this dual functionality. A benefit for a small to medium-sized company would be the ability to purchase a single multilayer switch instead of separate switching and routing network devices. Capabilities of a multilayer switch include the ability to route from one VLAN to another using multiple switched virtual interfaces (SVIs), as well as the ability to convert a Layer 2 switchport to a Layer 3 interface.

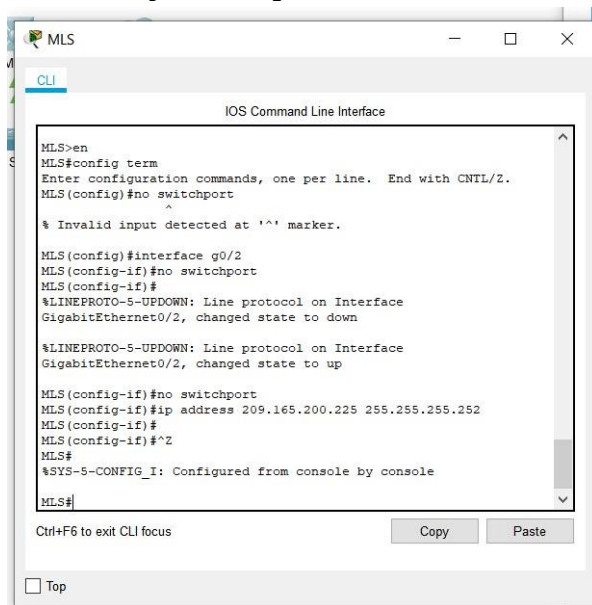
Instructions

Part 1: Configure Layer 3 Switching

In Part 1, you will configure the GigabitEthernet 0/2 port on switch MLS as a routed port and verify that you can ping another Layer 3 address.

- a. On MLS, configure G0/2 as a routed port and assign an IP address according to the Addressing Table.

```
MLS(config)# interface g0/2
MLS(config-if)# no switchport
MLS(config-if)# ip address 209.165.200.225 255.255.255.252
```



- b. Verify connectivity to **Cloud** by pinging 209.165.200.226.

```
MLS# ping 209.165.200.226
```

Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:

!!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

Part 2: Configure Inter-VLAN Routing

Step 1: Add VLANs.

Add VLANs to MLS according to the table below. Packet Tracer scoring is case-sensitive, so type the names exactly as shown.

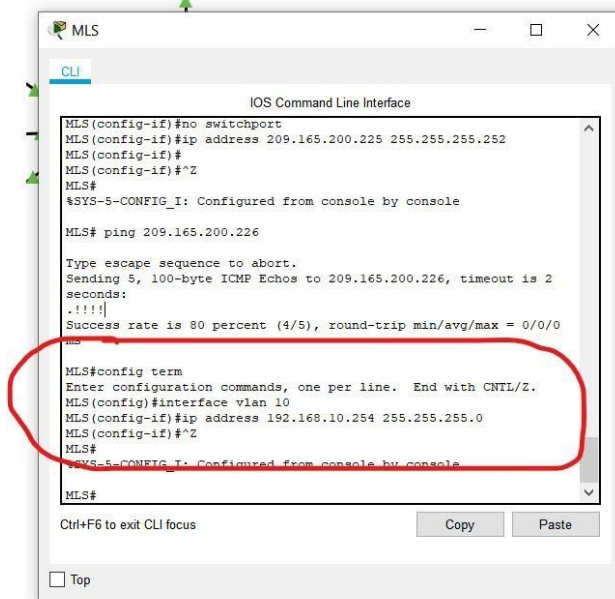
VLAN Number	VLAN Name
10	Staff
20	Student
30	Faculty

Step 2: Configure SVI on MLS.

Configure and activate the SVI interfaces for VLANs 10, 20, 30, and 99 according to the Addressing Table. The configuration for VLAN 10 is shown below as an example.

```
MLS(config)# interface vlan 10
```

```
MLS(config-if)# ip address 192.168.10.254 255.255.255.0
```



Step 3: Configure Trunking on MLS.

Trunk configuration differs slightly on a Layer 3 switch. On the Layer 3 switch, the trunking interface needs to be encapsulated with the dot1q protocol, however it is not necessary to specify VLAN numbers as it is when working with a router and subinterfaces.

- On MLS, configure interface **g0/1**.

- b. Make the interface a static trunk port.

```
MLS(config-if) # switchport mode trunk
```

- c. Specify the native VLAN as 99.

```
MLS(config-if) # switchport trunk native vlan 99
```

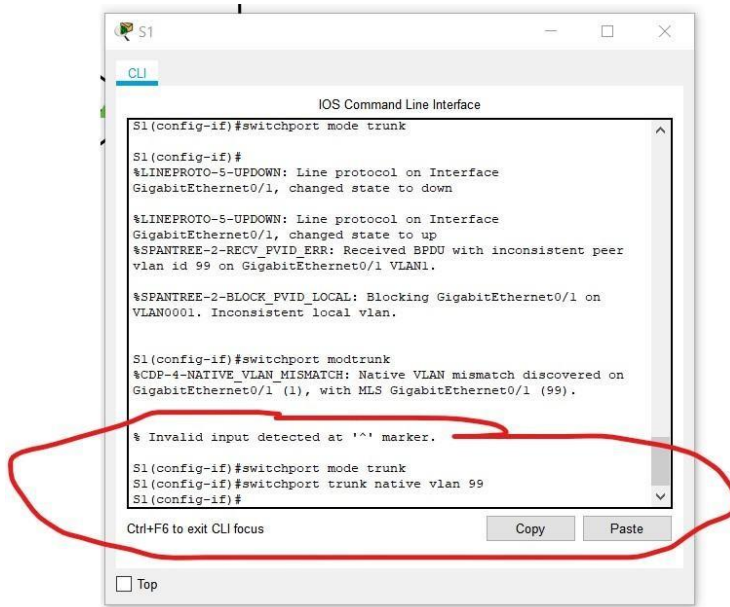
- d. Encapsulate the link with the dot1q protocol.

```
MLS(config-if) # switchport trunk encapsulation dot1q
```

Note: Packet Tracer may not score the trunk encapsulation.excit

Step 4: Configure trunking on S1.

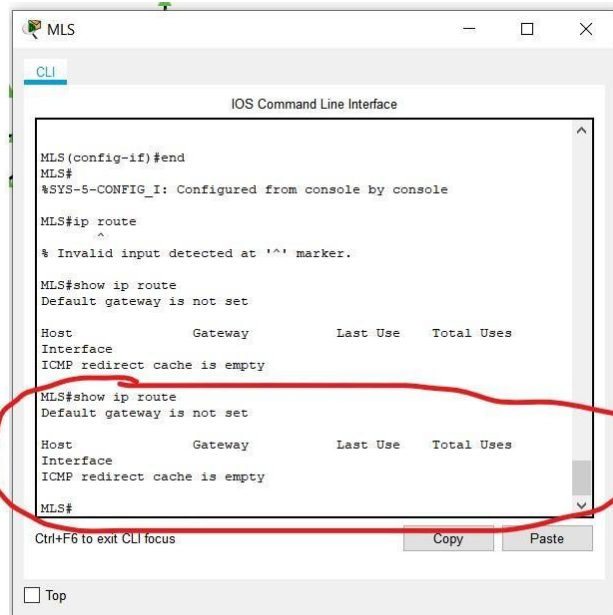
- a. Configure interface **g0/1** of S1 as a static trunk.
b. Configure the native VLAN on the trunk.



Step 5: Enable routing.

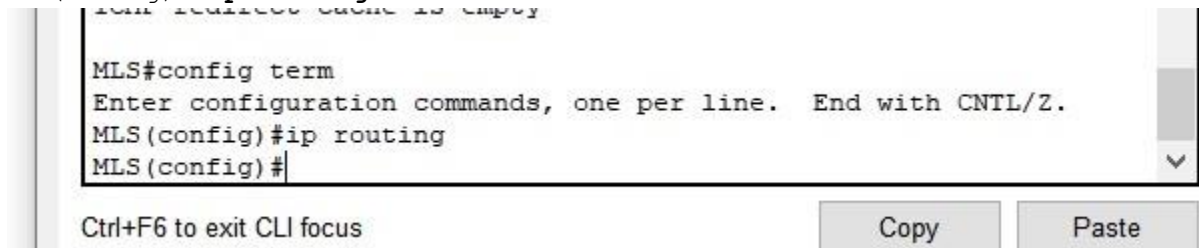
Question:

- a. Use the **show ip route** command. Are there any active routes?



- b. Enter the **ip routing** command to enable routing in global configuration mode.

MLS(config)# **ip routing**



- c. Use the **show ip route** command to verify routing is enabled.

MLS# **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

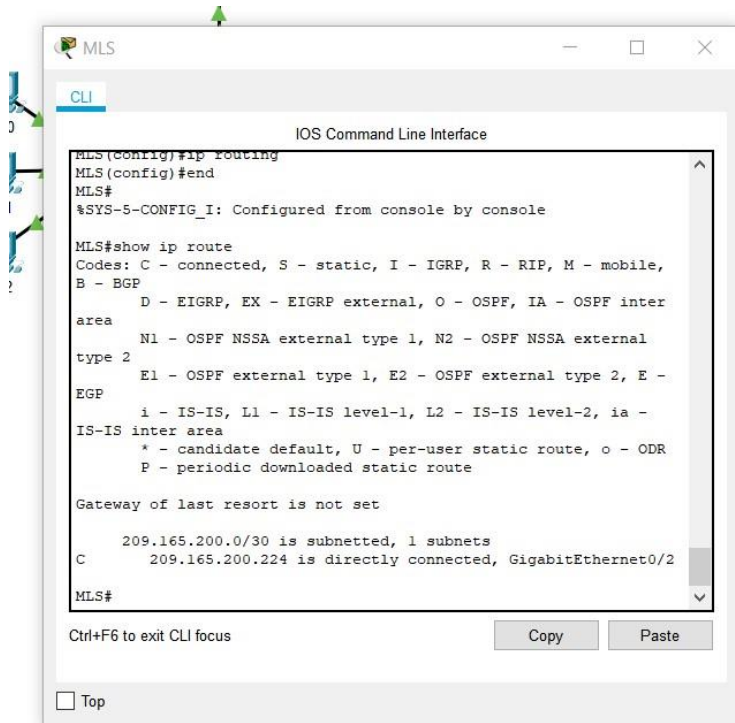
```

Gateway of last resort is not set

```

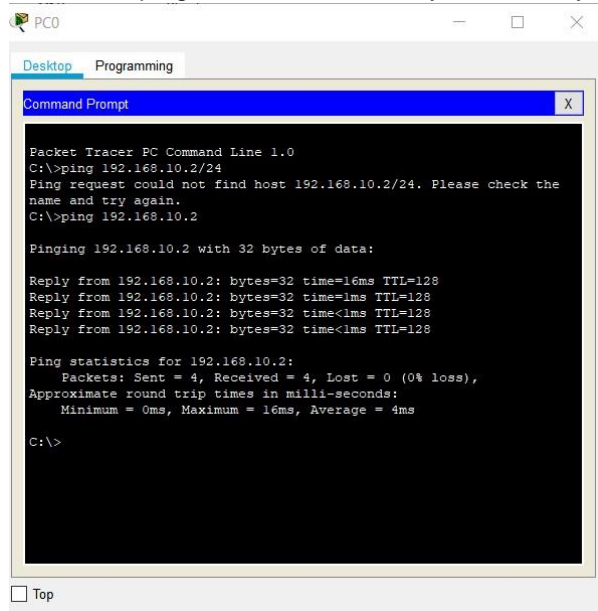
C    192.168.10.0/24 is directly connected, Vlan10
C    192.168.20.0/24 is directly connected, Vlan20
C    192.168.30.0/24 is directly connected, Vlan30
C    192.168.99.0/24 is directly connected, Vlan99
     209.165.200.0/30 is subnetted, 1 subnets
C      209.165.200.224 is directly connected, GigabitEthernet0/2

```

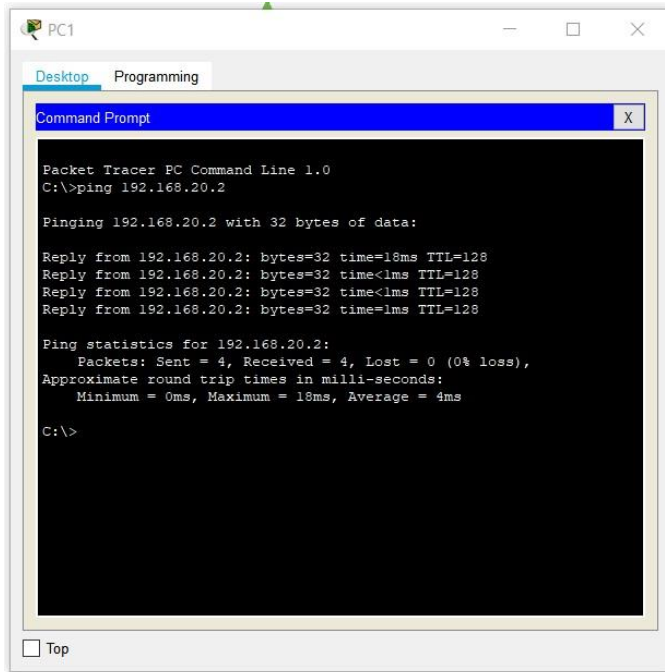


Step 6: Verify end-to-end connectivity.

- From PC0, ping PC3 or MLS to verify connectivity within VLAN 10.



- From PC1, ping PC4 or MLS to verify connectivity within VLAN 20.



PC1

Desktop Programming

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

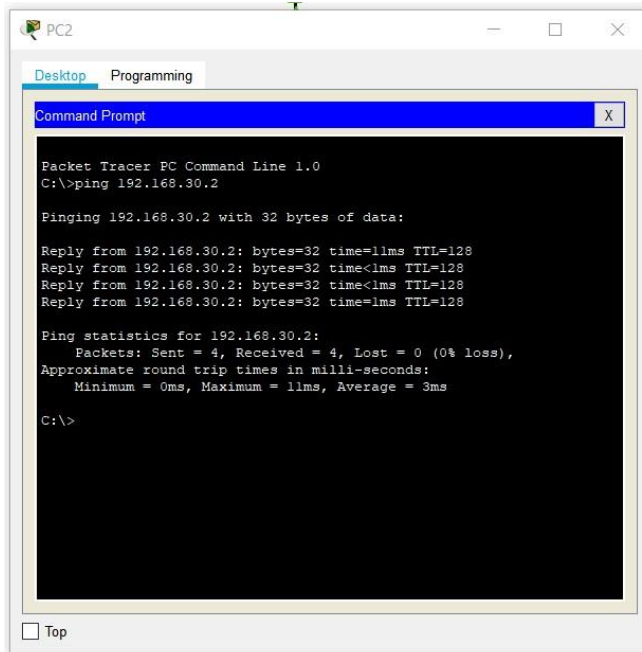
Reply from 192.168.20.2: bytes=32 time=18ms TTL=128
Reply from 192.168.20.2: bytes=32 time<1ms TTL=128
Reply from 192.168.20.2: bytes=32 time<1ms TTL=128
Reply from 192.168.20.2: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 18ms, Average = 4ms

C:\>
```

☐ Top

- c. From PC2, ping PC5 or MLS to verify connectivity within VLAN 30.



PC2

Desktop Programming

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.2

Pinging 192.168.30.2 with 32 bytes of data:

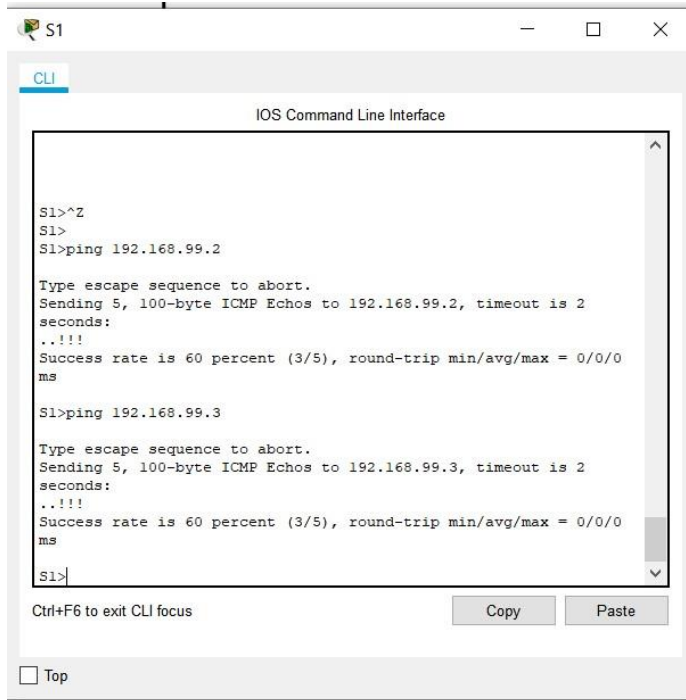
Reply from 192.168.30.2: bytes=32 time=11ms TTL=128
Reply from 192.168.30.2: bytes=32 time<1ms TTL=128
Reply from 192.168.30.2: bytes=32 time<1ms TTL=128
Reply from 192.168.30.2: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 3ms

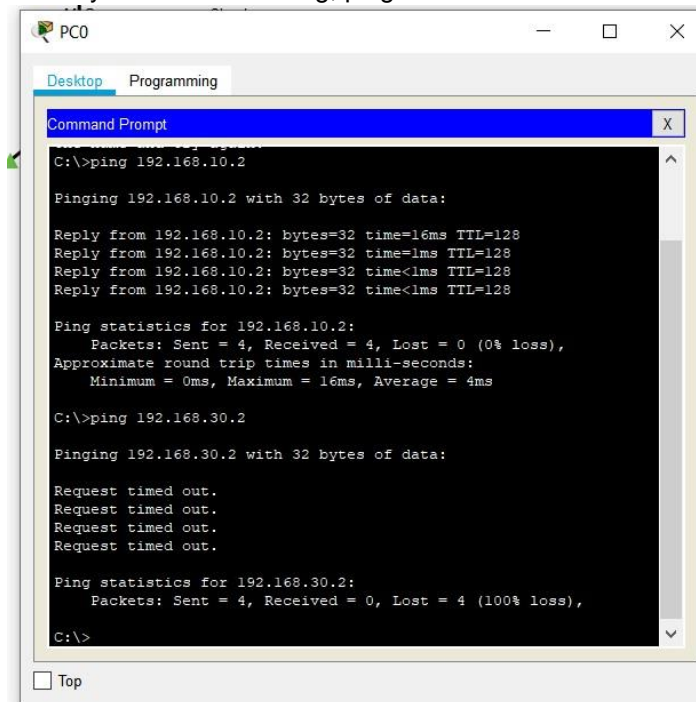
C:\>
```

☐ Top

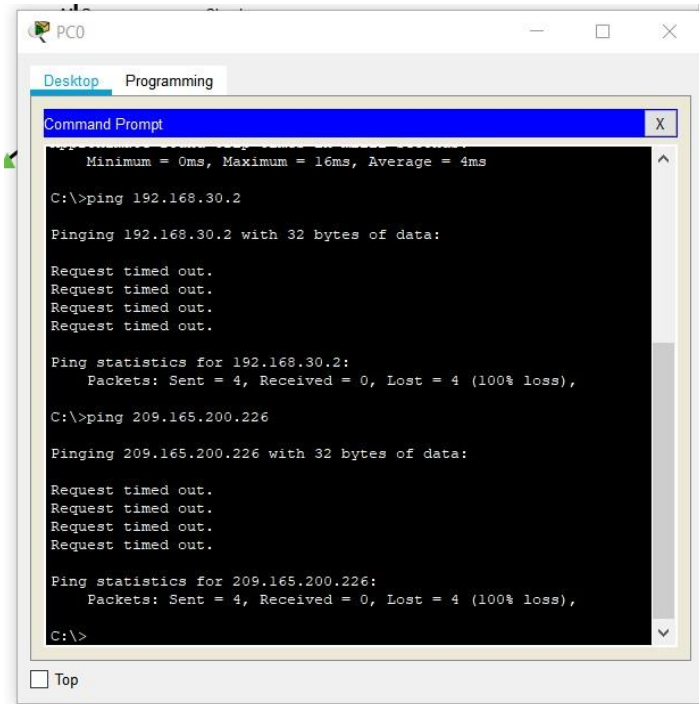
- d. From S1, ping S2, S3, or MLS to verify connectivity with VLAN 99.



- e. To verify inter-VLAN routing, ping devices outside the sender's VLAN.



- f. From any device, ping this address inside **Cloud**, 209.165.200.226.



The Layer 3 switch is now routing between VLANs and providing routed connectivity to the cloud.

Part 3: Configure IPv6 Inter-VLAN Routing

Layer 3 switches also route between IPv6 networks.

Step 1: Enable IPv6 routing.

Enter the **ipv6 unicast-routing** command to enable IPv6 routing in global configuration mode.

```
MLS(config)# ipv6 unicast-routing
MLS>en
MLS#config term
Enter configuration commands, one per line. End with CNTL/Z.
MLS(config)#ipv6 unicast-routing
MLS(config)#
```

Step 2: Configure SVI for IPv6 on MLS.

Configure IPv6 addressing on SVI for VLANs 10, 20, and 30 according to the Addressing Table. The configuration for VLAN 10 is shown below.

```
MLS(config)# interface vlan 10
MLS(config-if)# ipv6 address 2001:db8:acad:10::1/64
em
```

Step 3: Configure G0/2 with IPv6 on MLS.

- Configure IPv6 addressing on G0/2.


```

MLS(config)# interface G0/2
MLS(config-if)# ipv6 address 2001:db8:acad:a::1/64

MLS#config term
Enter configuration commands, one per line. End with CNTL/Z.
MLS(config)# interface G0/2
MLS(config-if)# ipv6 address 2001:db8:acad:a::1/64
MLS(config-if)#^Z
MLS#
%SYS-5-CONFIG_I: Configured from console by console

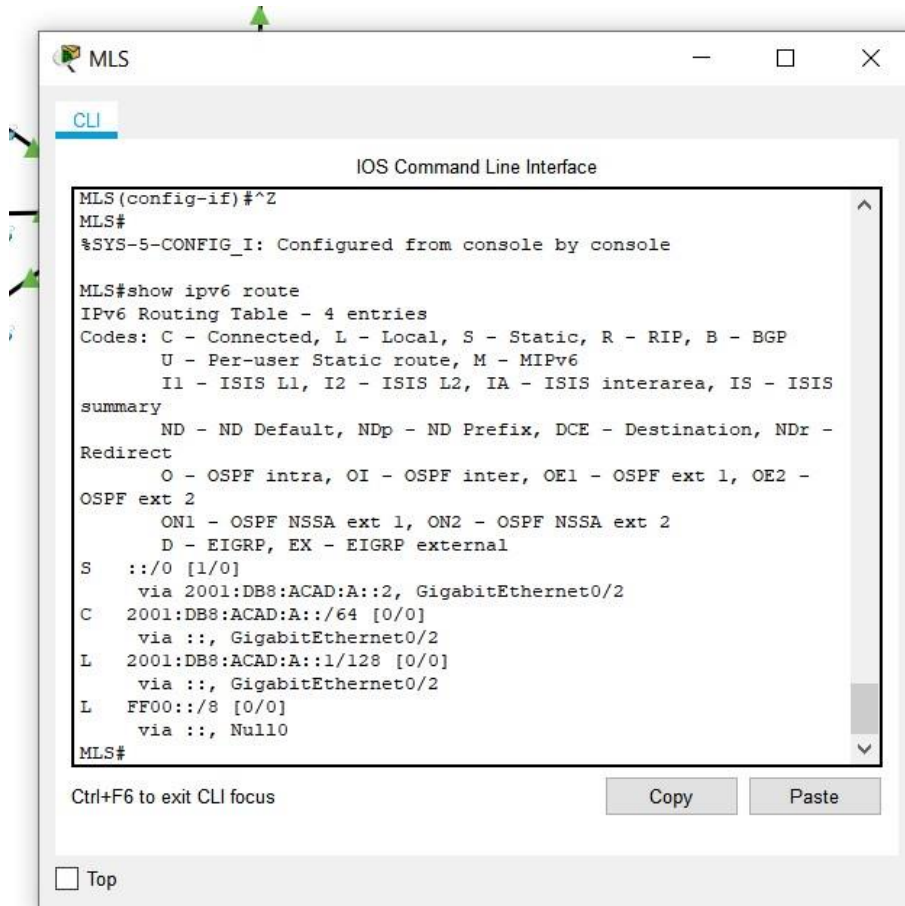
```

- b. Use the **show ipv6 route** command to verify IPv6 connected networks.

```

MLS# show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S  ::/0 [1/0] via 2001:DB8:ACAD:A::2,
   GigabitEthernet0/2
C  2001:DB8:ACAD:A::/64 [0/0]
   via ::, GigabitEthernet0/2
L  2001:DB8:ACAD:A::1/128 [0/0]
   via ::, GigabitEthernet0/2
C  2001:DB8:ACAD:10::/64 [0/0]
   via ::, Vlan10
L  2001:DB8:ACAD:10::1/128 [0/0]
   via ::, Vlan10
C  2001:DB8:ACAD:20::/64 [0/0]
   via ::, Vlan20
L  2001:DB8:ACAD:20::1/128 [0/0]
   via ::, Vlan20
C  2001:DB8:ACAD:30::/64 [0/0]
   via ::, Vlan30
L  2001:DB8:ACAD:30::1/128 [0/0]
   via ::, Vlan30
L  FF00::/8 [0/0]
   via ::, Null0

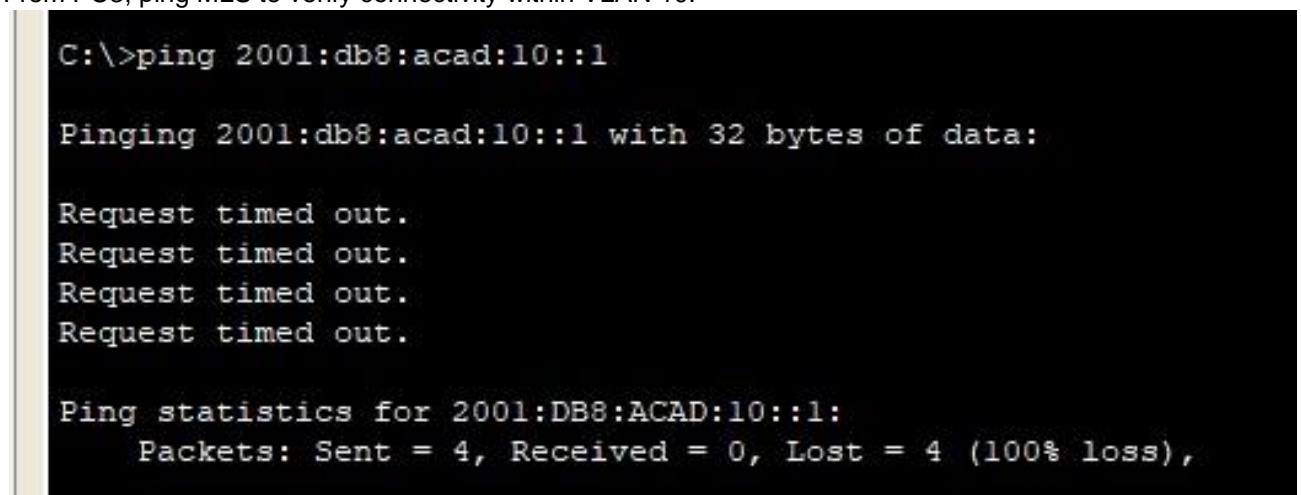
```



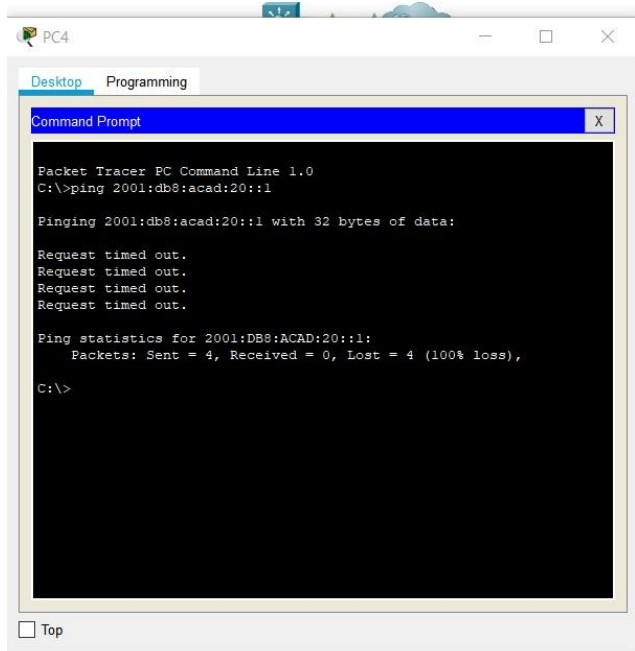
Step 4: Verify IPv6 connectivity.

Devices PC3, PC4, and PC5 have been configured with IPv6 addresses. Verify IPv6 inter-VLAN routing and connectivity to **Cloud**.

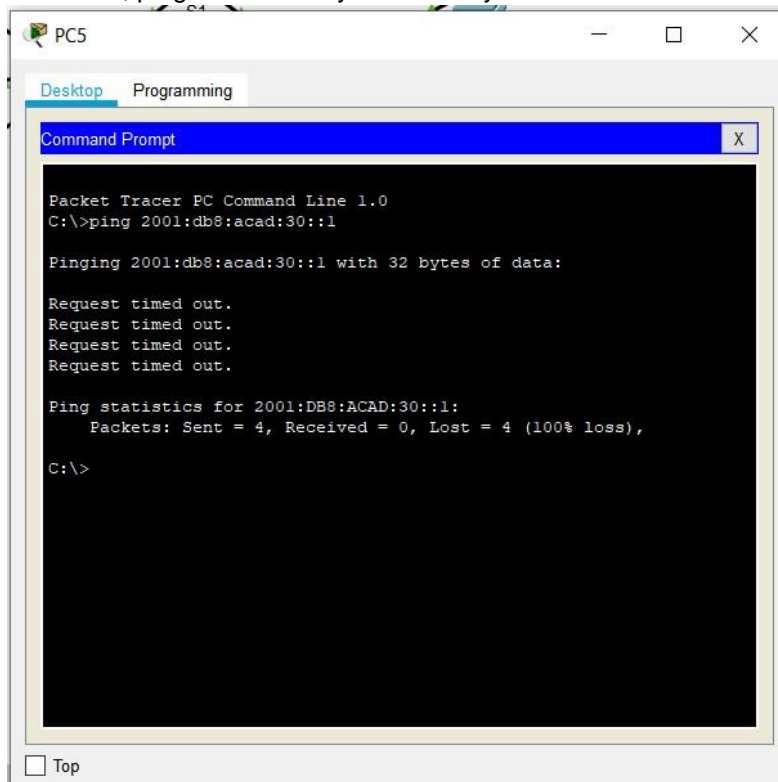
- From PC3, ping MLS to verify connectivity within VLAN 10.



- From PC4, ping MLS to verify connectivity within VLAN 20.



- c. From PC5, ping MLS to verify connectivity within VLAN 30.



- d. To verify inter-VLAN routing, ping between devices PC3, PC4, and PC5.

PC3

Desktop Programming

Command Prompt

```
Invalid Command.

C:\>ping 2001:db8:acad:10::1

Pinging 2001:db8:acad:10::1 with 32 bytes of data:

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

Ping statistics for 2001:DB8:ACAD:10::1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 2001:db8:acad:20::2

Pinging 2001:db8:acad:20::2 with 32 bytes of data:

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

Ping statistics for 2001:DB8:ACAD:20::2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

☐ Top

PC3

Desktop Programming

Command Prompt

```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 2001:db8:acad:20::2

Pinging 2001:db8:acad:20::2 with 32 bytes of data:

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

Ping statistics for 2001:DB8:ACAD:20::2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 2001:db8:acad:30::2

Pinging 2001:db8:acad:30::2 with 32 bytes of data:

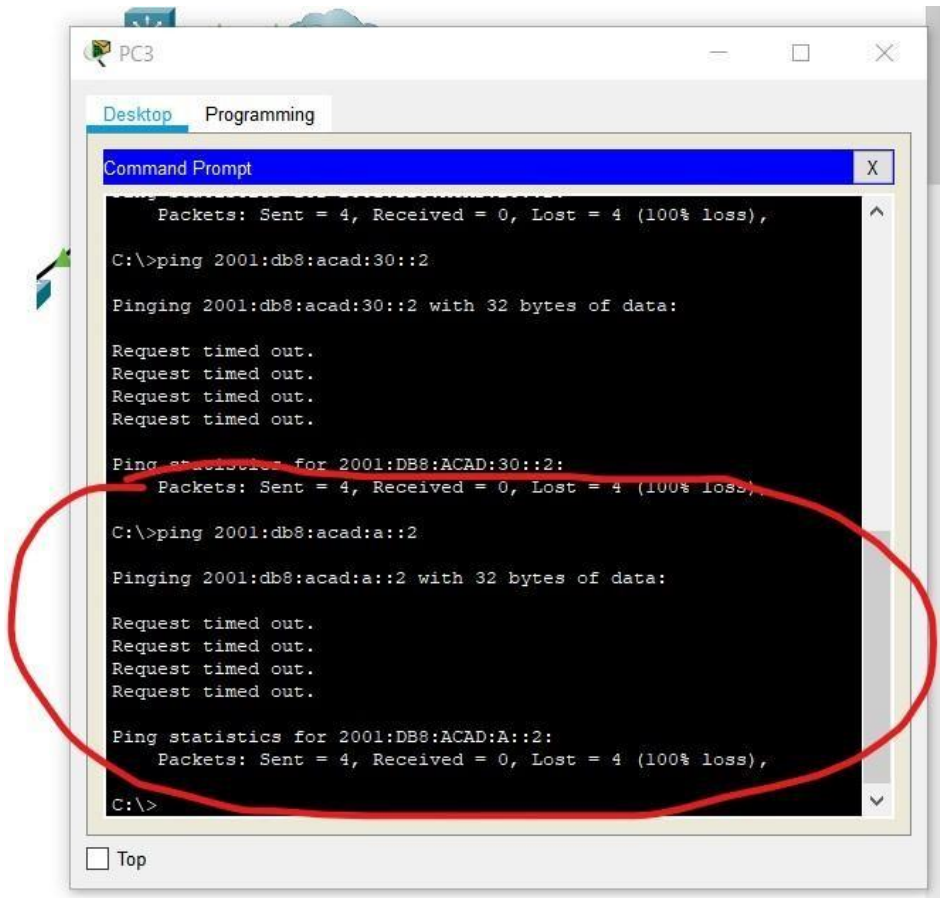
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB8:ACAD:30::2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

☐ Top

- e. From PC3 ping the address inside **Cloud**, 2001:db8:acad:a::2.



4. STATIC-ROUTE

Configure IPv4 and IPv6 Static and Default Routes

Addressing Table

Device	Interface	IP Address / Prefix
Edge_Router	S0/0/0	10.10.10.2/30
		2001:db8:a:1::2/64
	S0/0/1	10.10.10.6/30
		2001:db8:a:2::2/64
	G0/0	192.168.10.17/28
		2001:db8:1:10::1/64
		192.168.11.33/27

	G0/1	2001:db8:1:11::1/64
ISP1	S0/0/0	10.10.10.1/30
		2001:db8:a:1::1/64
	G0/0	198.0.0.1/24
		2001:db8:f:f::1/64
ISP2	S0/0/1	10.10.10.5/30
		2001:db8:a:2::1/64
	G0/0	198.0.0.2/24
		2001:db8:f:f::2/64
PC-A	NIC	192.168.10.19/28
		2001:db8:1:10::19/64
PC-B	NIC	192.168.11.4/27
		2001:db8:1:11::45
Customer Server	NIC	198.0.0.10
		2001:db8:f:f::10

Objectives

In this Packet Tracer summary activity, you will configure static, default, and floating static routes for both the IPv4 and IPv6 protocols.

- Configure IPv4 Static and Floating Static Default Routes.
- Configure IPv6 static and floating static default routes.
- Configure IPv4 static and floating static routes to internal LANs.
- Configure IPv6 static and floating static routes to the internal LANS.
- Configure IPv4 host routes.
- Configure IPv6 host routes.

Background / Scenario

In this activity, you will configure IPv4 and IPv6 default static and floating static routes.

Note: The static routing approach that is used in this lab is used to assess your ability to configure different types of static routes only. This approach may not reflect networking best practices.

Instructions

Part 1: Configure IPv4 Static and Floating Static Default Routes

The PT network requires static routes to provide internet access to the internal LAN users through the ISPs. In addition, the ISP routers require static routes to reach the internal LANs. In this part of the activity, you will configure an IPv4 static default route and a floating default route to add redundancy to the network.

Step 1: Configure an IPv4 static default route.

On Edge_Router, configure a **directly connected** IPv4 default static route. This primary default route should be through router **ISP1**.

```
Edge_Router(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.1
```

Step 2: Configure an IPv4 floating static default route.

On Edge_Router, configure a **directly connected** IPv4 floating static default route. This default route should be through router **ISP2**. It should have an administrative distance of **5**.

```
Edge_Router(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.5 5
```

Part 2: Configure IPv6 Static and Floating Static Default Routes

In this part of the activity, you will configure IPv6 static default and floating static default routes for IPv6.

Step 1: Configure an IPv6 static default route.

On Edge_Router, configure a **next hop** static default route. This primary default route should be through router **ISP1**.

```
Edge_Router(config)#ipv6 route ::/0 2001:db8:a:1::1
```

Step 2: Configure an IPv6 floating static default route.

On Edge_Router, configure a **next hop** IPv6 floating static default route. The route should be via router **ISP2**. Use an administrative distance of **5**.

```
Edge_Router(config)#ipv6 route ::/0 2001:db8:a:2::1 5
```

Part 3: Configure IPv4 Static and Floating Static Routes to the Internal LANs

In this part of the lab you will configure static and floating static routers from the ISP routers to the internal LANs.

Step 1: Configure IPv4 static routes to the internal LANs.

- a. On ISP1, configure a **next hop** IPv4 static route to the **LAN 1** network through Edge_Router.


```
ISP1(config)#ip route 192.168.10.16 255.255.255.240 10.10.10.2
```

- b. On ISP1, configure a **next hop** IPv4 static route to the **LAN 2** network through Edge_Router.

```
ISP1(config)#ip route 192.168.11.32 255.255.255.224 10.10.10.2
```

Step 2: Configure IPv4 floating static routes to the internal LANs.

- a. On ISP1, configure a directly connected floating static route to LAN 1 through the ISP2 router. Use an administrative distance of **5**.

```
ISP1(config)#ip route 192.168.10.16 255.255.255.240 g0/0 5
```

- b. On ISP1, configure a directly connected floating static route to LAN 2 through the ISP2 router. Use an administrative distance of **5**.

```
ISP1(config)#ip route 192.168.11.32 255.255.255.224 g0/0 5
```

Part 4: Configure IPv6 Static and Floating Static Routes to the Internal LANs.

Step 1: Configure IPv6 static routes to the internal LANs.

- c. On ISP1, configure a next hop IPv6 static route to the **LAN 1** network through Edge_Router.

```
ISP1(config)#ipv6 route 2001:db8:1:10::/64 2001:db8:a:1::2
```

- d. On ISP1, configure a next hop IPv6 static route to the **LAN 2** network through Edge_Router.

```
ISP1(config)#ipv6 route 2001:db8:1:11::/64 2001:db8:a:1::2
```

Step 2: Configure IPv6 floating static routes to the internal LANs.

- a. On ISP1, configure a next hop IPv6 floating static route to LAN 1 through the ISP2 router. Use an administrative distance of **5**.

```
ISP1(config)#ipv6 route 2001:db8:1:10::/64 2001:db8:f:f::2 5
```

- b. On ISP1, configure a next hop IPv6 floating static route to LAN 2 through the ISP2 router. Use an administrative distance of **5**.

```
ISP1(config)#ipv6 route 2001:db8:1:11::/64 2001:db8:f:f::2 5
```

If your configuration has been completed correctly, you should be able to ping the Web Server from the hosts on LAN 1 and LAN 2. In addition, if the primary route link is down, connectivity between the LAN hosts and the Web Server should still exist.

Part 5: Configure Host Routes

Users on the corporate network frequently access a server that is owned by an important customer. In this part of the activity, you will configure static host routes to the server. One route will be a floating static route to support the redundant ISP connections.

Step 1: Configure IPv4 host routes.

- a. On Edge Router, configure an IPv4 **directly connected** host route to the customer server.
- b. On Edger Router, configure an IPv4 directly connected floating host route to the customer sever. Use an administrative distance of **5**.

Step 2: Configure IPv6 host routes.

- a. On Edge Router, configure an IPv6 next hop host route to the customer server through the ISP1 router.
- b. On Edger Router, configure an IPv6 directly connected floating host route to the customer sever through the ISP2 router. Use an administrative distance of **5**.