Group 4 - Group A:

1. **P15/141008/2020** - Ibrahim Salim Twaakyondo
2. **P15/145186/2022** - Mubarak Ahmed Mohamud
3. **P15/34499/2014** - Kipngetich Nickson Yegon
4. **P15/144649/2022** - Wambua Solomon Mbithi
5. **P15/139827/2020** - Paul Kimaru Mwangi

SCS3309 LAB 5A

Switched LAN 1

Two **access** layer switches S1 and S2 are connected using **three** fast ethernet links. STP is **disabled** on all switches. There are two PCs: PC1 and PC3 connected to S1. There is one PC: PC2 and a server SVR1 connected to S2. The server hosts a web server. S1and S2 are connected via their Fa0/1, fa0/2 and fa0/3 ports respectively. i.e Fa0/1 on S1 connects to Fa0/1 on S2. Fa0/2 on S1 connects to Fa0/2 on S2. Fa0/3 on S1 connects to Fa0/3 on S2. PC1 and PC3 are connected to ports Fa0/4 and Fa0/5 respectively on S1. PC2 and SVR1 are connected to ports Fa0/4 and Fa0/5 respectively on S2. All the PCs are in Vlan 10 which is mapped to 192.168.10.0. Assume that all devices are well configured and all PCs are able to access the web server. Configure the **display name** for each PC and Server (PC1, PC2, PC3 and SVR 1). Configure the **hostname** for each switch (S1 and S2)

https://drive.google.com/file/d/18Tu1mvQytZtWpmuzg2YVcKQg9StRhX3k/view?usp=sharing

LAB1

As the administrator of the network described above (switched LAN 1), assume that you choose to reorganize the network so that PC1 and PC2 are in Vlan 10 while PC3 and SVR1 are in Vlan 20. Vlan10 is configured to be in network 192.168.10.0. while Vlan 20 is configured to be in network 192.168.20.0.

. Configure the vlans and verify that they are properly configured?Show.(video) Is the transmission of a message from PC1 to Sv1 successful? Explain!

No transmission of message from PC1 to SVR1 it is not successful because PC1 is in VLAN 10 and SVR1 is in VLAN 20 they are in different VLANs and they are connected using a layer 2 switch that is not capable of intervlan routing, so the devices from vlan10 can't communicate with the devices in a vlan20 with the layer 2 switch

Video

https://drive.google.com/file/d/1-rSg3ArBhAbB7hkOb_JK-jdJj4J8cB9V/view?usp=sharing

b. A router is subsequently connected to port Fa0/6 on S2 to enable **inter-vlan** communication using the (i) router on a stick (ROAS) (ii) Multilayer switch method.

- What additional configurations would you need to make on the network to enable inter-vlan communication?show. (video)

- https://drive.google.com/file/d/1iRel5I-S8tdPQgPPHP1m8McKwVkk2bFo/view?usp=sharing

i) Removing the three fast ethernet links and connecting S1 with the router through Fa0/1 on S1 and fastethernet 0/1 on the router, configure the router's fa 0/1 to give default gateway for vlan 10 and also configure the default gateway for vlan20

ii)Changing the default gateway to the gateway we set up in each device of the vlan 10 and 20

- How would you verify that your configuration is correct?show. (video) https://drive.google.com/file/d/1UiTC7p2u7GUtJLHk4waIRm_EeqQxTozi/view?usp=drive_link
-

By trying to send a packet from PC2 to PC3

- Demonstrate that you can have inter vlan communication by transmitting a frame from PC1 to Sv1. Trace the "path" is taken by a message from PC1 to Sv1. show!(video)

- https://drive.google.com/file/d/1wIyjGy-pqxAUUrhOKXioMQUUVtyHxePM/view?usp=sharing
-

c. Virtual LANs: **Network Design Chapter 5: pgs 141 - 146:** In modern networks, how are VLANs typically used in wired LANs? How would the design change/be modified if the network also supports WLANs? Explain!

They divide the physical network into multiple virtual networks with a different broadcast domain

-It helps minimize security breach by separating network traffic into different VLANs
-Reduce network traffic and improves performance, by dividing network manageable domains

How design be modified to supports WLANs

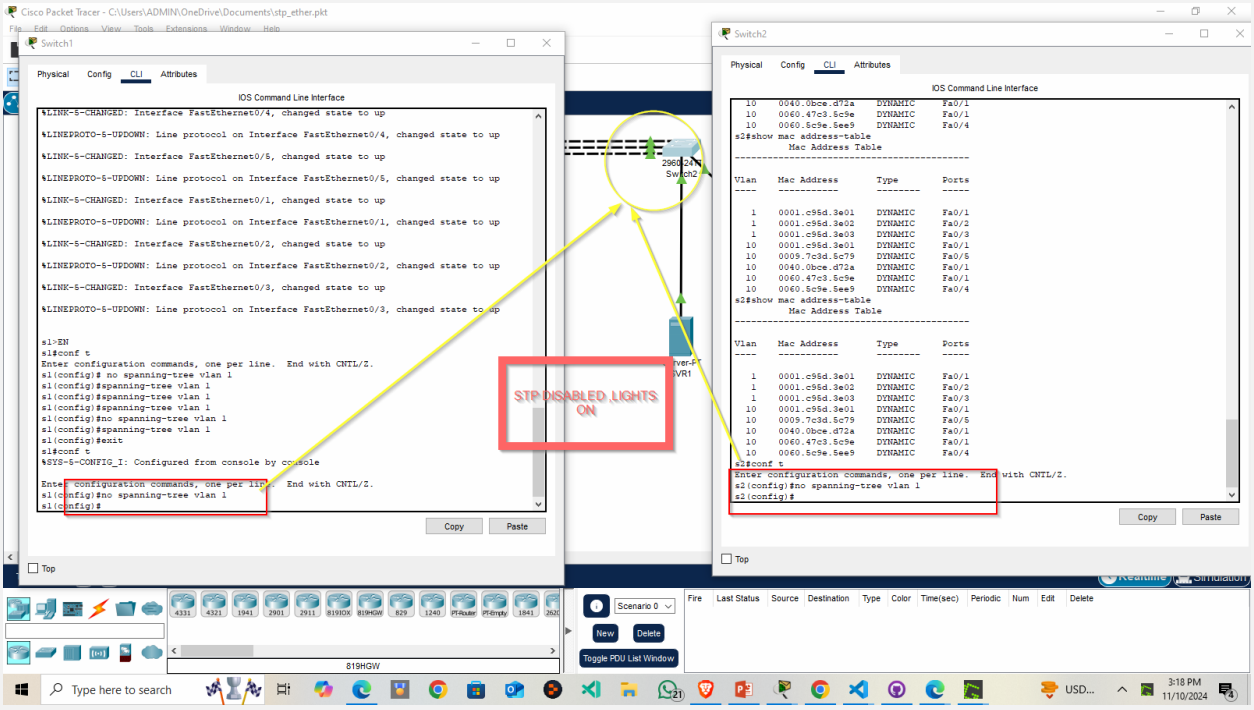
i) Point to point link - Extended over a point WAN link using protocols such as 802.1Q

ii) Extension across VPN tunnels

LAB2 Consider the switched LAN above (switched LAN 1)

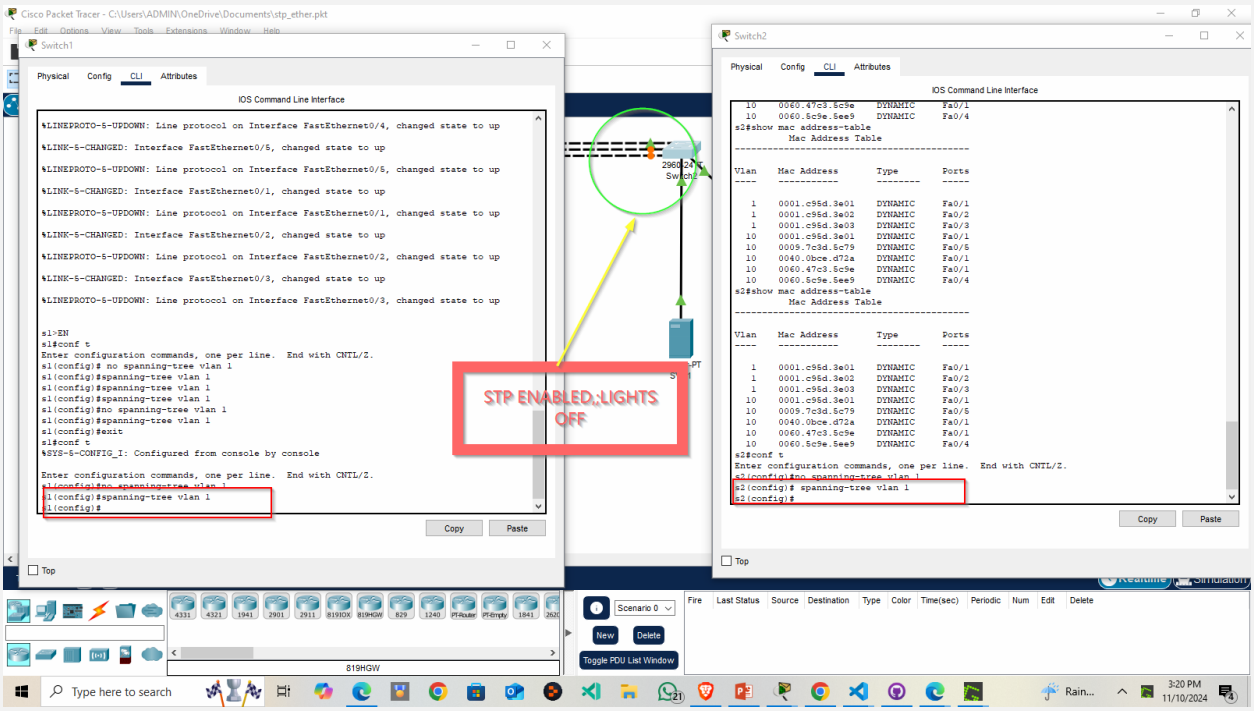
(a) Disable spanning tree on both switches. Observe/record what happens to the Led lights.

- To disable spanning tree: **(en, conf t, no spanning-tree vlan 1**).



(b) Enable spanning tree on both switches. Observe/record what happens to the Led lights.

- To enable spanning tree: **en, conf t, spanning-tree vlan 1**). Observe what happens to the lights.
-



(c) A broadcast frame is transmitted by PC1 on S1. By tracing how the broadcast frame is forwarded explain/show how each of the following undesirable effects manifests in this network.

VIDEO STP DISABLED

https://drive.google.com/file/d/1EunQVHKHhpC-xTcx-4y8keM3hObSGYPM/view?usp=sharing

- Broadcast storm(video)
- Unstable mac address table (video)
- Multiple frame deliveries(video)

VIDEOES ENBLAED

- Broadcast storm(video) noo loops
- Unstable mac address table (video) MACS IS constant across all frames on the same frames with the same devices
- Multiple frame deliveries(video) constant frames in the same broadcasts

- https://drive.google.com/file/d/12i5FtYYlP_A3MaK5bNMvTAGH8fg9yeyd/view?usp=sharing

  packet tracer files activities

  https://drive.google.com/file/d/1KBxygthw_aePTa5-3f9QpGW02QZdFaHz/view?usp=sharing

(d) STP is subsequently enabled in the network described above. By tracing the forwarding of the broadcast frame, has the enabling of STP helped to resolve **each** of the problems highlighted in (a) above. Explain!

STP Disabled (Before Enabling STP):

1. **Broadcast Storm (video):** When STP is disabled, broadcast frames loop endlessly between S1 and S2, causing a broadcast storm. This results in excessive traffic and can overwhelm network devices.
2. **Unstable MAC Address Table (video):** The continuous looping of broadcast frames causes the MAC address tables on S1 and S2 to keep updating, as each switch learns the same MAC addresses from different ports. This creates instability in the MAC tables.
3. **Multiple Frame Deliveries (video):** Due to the looping, the same frame is delivered multiple times to devices, which can lead to confusion and network inefficiency.

STP Enabled (After Enabling STP):

(e) **Broadcast Storm (video):** No loops occur, as STP disables redundant links between S1 and S2. Broadcast frames are sent only once, preventing a broadcast storm.

(f) **Unstable MAC Address Table (video):** With STP enabled, MAC address tables are stable. Each MAC address is associated consistently with the correct port, as frames no longer loop.

(g) **Multiple Frame Deliveries (video):** Only one copy of each broadcast frame is delivered to each device, as STP eliminates redundant paths. This ensures constant, efficient frame delivery.

(h) STP: **Network Design Chapter 5: pgs: 135-140**

LAB3

Consider the switched LAN above (switched LAN 1). The cost of a link is based on the speed of the port as follows: 10 Gbps = 2; 1 Gbps = 4; 100 Mbps = 19; 10 Mbps = 100.

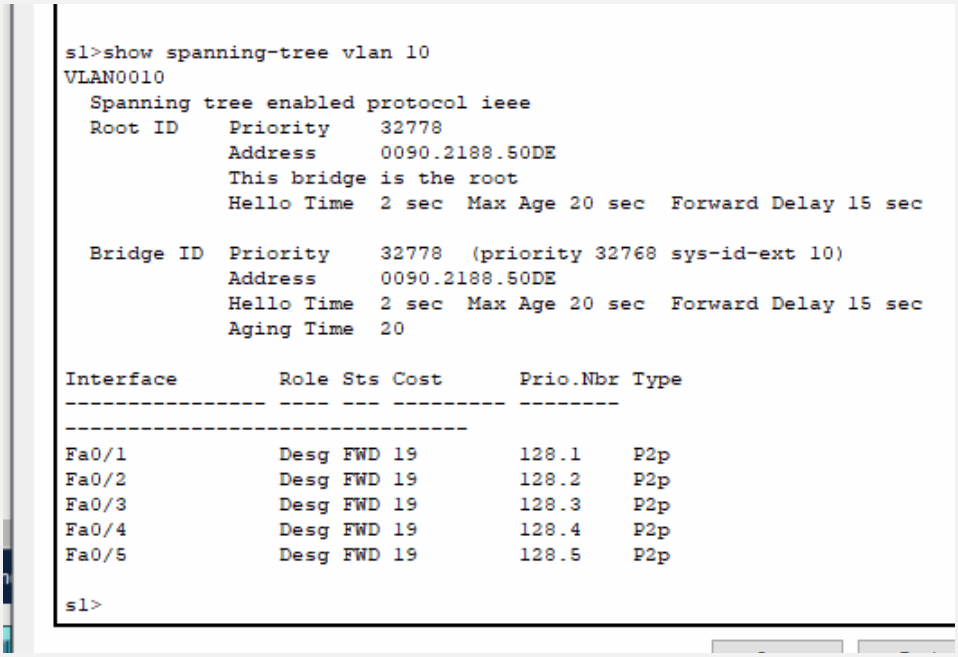
(a) Record the Bridge IDs on the two switches: S1: priority: = xxxxx, system id extension = x, Lowest mac address: = xxxx xxxx xxxx; S2: priority: = xxxxx, system id extension = x, Lowest mac address: = xxxx xxxx xxxx; (video)

VIDEO: https://drive.google.com/file/d/1WutGB0iYN4s78ygj-UrSmgGnMqJVeCbN/view?usp=drive_link

S1: priority: = 32768,system id extension = 10, Lowest mac address: = 0090.2188.50DE;
S2: priority: = 32768,system id extension = 10, Lowest mac address: = 00D0.BCAA.1D9A;

Switch 1

s1>show spanning-tree



```
s1>show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    32778
              Address     0090.2188.50DE
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     0090.2188.50DE
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
--------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p

s1>
```

Switch 2

s2>show spanning-tree vlan 10

```
s2>show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    32778
              Address     0090.2188.50DE
              Cost        19
              Port        1(FastEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     00D0.BCAA.1D9A
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/1            Root FWD 19        128.1    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/3            Altn BLK 19        128.3    P2p

s2>
```

(b) (i) In your network which switch is the (i) root bridge?show. (video) (ii) Explain how STP arrived at this answer.

VIDEO: https://drive.google.com/file/d/1hfb56jQBsmgtx4RfJgbLHr-7Rl0EKCjS/view?usp=drive_link

Switch 1 is the root bridge because:

Since both switches have the same priority for VLAN 10 (32778, 32778 respectively).

STP will then use MAC addresses as election criteria to choose the root bridge. The switch with the lower mac address will be selected.

Switch 1 MAC: **00:90:21:88:50:DE**

Switch 2 MAC: **00:D0:BC:AA:1D:9A**

Both MAC addresses are analyzed by comparing each byte (octet) hexadecimal. First byte for Switch 1 and Switch 2 are 00 and 00 respectively. They are the same, the next byte are 90 and D0 respectively. 90 in hexadecimal is 144 and D0 is 208

Since 90 is lower than 208, STP will choose Switch 1 as the switch with the lower MAC address

Switch S1 is then elected as the root bridge.

```
s1>show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    32778
              Address     0090.2188.50DE
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 se
```

(c) (i) In your network which switch interfaces are (i) root ports (ii) designated ports and (iii) non designated ports? Show (video) (ii) Explain how STP arrived at this answer!

VIDEO:

https://drive.google.com/file/d/1oI4I_vCuHCYQpcULEGW7B7wFvqsaVtQF/view?usp=drive_link

1. Switch S1 (Root Bridge)

Since Switch S1 is the root bridge, STP places all ports on the root bridge in Designated Forwarding (FWD) ports,

Therefore all ports on switch 1: Fa0/1, Fa0/2, Fa0/3, Fa0/4 and Fa0/5: are Designated Ports. that will allow and forward traffic

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
--------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p

s1>
```

2. Switch S2(not root)

Switch S2 is not the root and it knows Switch S1 is the root bridge after the election process. The switch will therefore assign one of its ports with the lowest path cost to the root, or lowest port number, as the Root Port, and block the other two ports as they are redundant.

STP calculates the path cost to reach the root bridge for each link on Switch S2. But In this case all three ports have the same path cost (19) as they are all fastethernet 100Mbps links. STP will then use port number as the criteria to choose the root port.

```
Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/1            Root FWD 19        128.1    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/3            Altn BLK 19        128.3    P2p

s2>
```

So Fa0/1 is the link with the lowest port number and will be assigned as the root port. And the other two ports fa0/2 and fa0/3 are non designated(blocked) to avoid loops. The ports Fa0/4 and Fa0/5 through which PC2 and SVR 1 are connected will be designated ports and will allow and forward traffic

Port designation for switch 1 and switch 2

Switch 1

Switch	Port	Role	State
S1	Fa0/1	Designated	Forwarding
S1	Fa0/2	Designated	Forwarding
S1	Fa0/3	Designated	Forwarding
S1	Fa0/4	Designated	Forwarding
S1	Fa0/5	Designated	Forwarding

Switch 2

S2	Fa0/1	Root Port	Forwarding
S2	Fa0/2	Non-designated	Blocked
S2	Fa0/3	Non-designated	Blocked

S2 Fa0/4 Designated Forwarding

S2 Fa0/5 Designated Forwarding

(d) According to your answers in (b) and (c) above, which path does a message from PC1 to Sv1 take.? Explain!

Initial Transmission from PC1 (assuming MAC address table is empty):

PC1 sends the message destined for SVR1. The message arrives at Switch 1 through port Fa0/4. And then forwarded through all it's outgoing ports. As such the message is forwarded through Fa0/1 on switch 1 towards Switch 2, where the server SVR1 is connected.

The message arrives at switch 2 via Root port Fa0/1 since the other two ports are non-designated(blocked) and no traffic will be received through them.

Switch 2 then forwards the message through its outgoing ports except the one the message comes in and the blocked ports as well. Hence the message is forwarded through port Fa0/5, where SVR1 is connected

SVR1 Receives the Message:

SVR1 receives the message from PC1 via the path PC1 ->S1 Fa0/4-> S1 Fa0/1 -> S2 Fa0/1 -> S2 Fa0/5 -> SVR1.

Once the switches have filled their MAC address table the subsequent transmission from PC1 to SVR1 will be directly forwarded to relevant ports via the path above with no broadcast.

(e) Do the above answers (b,c and d) change if you have an ether channel between s1 and S2 (as in LAB4) instead? Explain!

Yes, If an EtherChannel is configured between S1 and S2, a single Logical Link will be formed between the two switches. EtherChannel protocol will bundle the three physical links (Fa0/1, Fa0/2, and Fa0/3) into a single logical link. And STP will interpret it as a single link as opposed to the previous three links.

Therefore there will be no redundant link between the two switches because there's now only one link(logical) connecting the two.

STP treats this logical link as a single connection between Switch S1 and Switch S2 and will designate the EtherChannel as a Designated Forwarding link on Switch S1 and a Root Port on Switch S2. This will remove the need to block any of the individual links within the EtherChannel.

When PC1 sends a message to SVR1, the message will be distributed across the EtherChannel Since all three links have been bundled into one, and will carry traffic simultaneously as a single logical trunk. It will then be forwarded towards Switch 2 via one logical port, It will arrive on switch two as a single message via one logical port.

With EtherChannel, the path from PC1 to SVR1 could take any of the three physical links in the EtherChannel, depending on load balancing.

Therefore with etherchannel, the message from PC1 to SVR1 will be forwarded like this

PC1 ->S1 Fa0/4-> S1->Etherchannel-> S2 -> S2 Fa0/5 -> SVR1.

(f) Assume that we have the following Bridge IDs on the two switches: S1: priority: = 32678, system id extension = 1, Lowest mac address: = 0009 4368 7908; S2: priority: = 32678, system id extension = 1, Lowest mac address: = 00D0 4368 7908; .

- Which switch would be the (i) root bridge? Explain how STP would arrive at the answer.

- Which switch interfaces would be (i) root ports (ii) designated ports and (iii) non designated ports. Explain how STP would arrive at the answer!

Both Switches have the same priority and system id extension. Therefore STP will use MAC address as criterion for choosing the root bridge.

  - Switch S1 MAC Address: 0009.4368.7908
  - Switch S2 MAC Address: 00D0.4368.7908

Comparing Each Byte of the MAC Addresses

The first byte of Switch S1's MAC (00) and Switch S2's MAC (00) are the same, so we move to the next byte. The second byte of Switch S1's MAC is 09, while Switch S2's MAC is D0. 09 is much lower than D0 because 09 translates to 9 in decimal, while D0 translates to 208 in decimal. Therefore Switch 1 has the lower MAC address and will then be elected as the root bridge.

Port Designation after election:-

Switch 1:

Switch S1 is the root bridge, therefore all ports will be assigned as designated ports that will forward data. Fa0/1, Fa0/2, Fa0/3, Fa0/4 and Fa0/5 on Switch S1 are Designated Ports

Switch 2:

Switch S2 is not the root bridge and it knows Switch 1 is the root bridge after the election process, STP will assign the ports based on the lowest-cost path to reach the root bridge or the lowest port number. Since All links between Switch S1 and Switch S2 are Fast Ethernet with the cost of 19 each, STP will choose the port with the lowest port number as the Root Port.

The Ports Fa0/1-3 have port numbers 128.1 128.2 128.3 respectively. Fa0/1 will therefore be assigned as the root port because it has the lowest port number. The other two ports Fa0/2 and Fa0/2 will be assigned as non designated ports. The ports Fa0/4 and Fa0/5 through which PC2 and SVR 1 are connected will be designated ports and will allow and forward traffic.

Switch	**Port**	**Role**
S1	Fa0/1	Designated
S1	Fa0/2	Designated
S1	Fa0/3	Designated
S1	Fa0/4	Designated
S1	Fa0/5	Designated

S2	Fa0/1	Root Port
S2	Fa0/2	Non-designated
S2	Fa0/3	Non-designated
S2	Fa0/4	Designated
S2	Fa0/5	Designated

LAB4

LAB4

Assume that the three links between the switches in the network (switched Lan 1) above are aggregated/bundled together into an ether channel. Assume that heavy traffic to the server is expected from the PCs on S1 compared to the one on S2.

- How would you configure the ether channel? Show. (video)
- https://drive.google.com/file/d/1tklKxONR8fAUDGqOrJxG-8QjDgDxajKo/view?usp=sharing
-
- How would you verify that the ether channel is properly configured? (video)
- https://drive.google.com/file/d/1xLXj38ttcUSBJFi0M7pC-TFA2Rh-c3cu/view?usp=sharing
-
- Which load balancing method would you consider the **best** if configured on the ether channels in this network traffic scenario? Explain!

  The best load balancing method for this is the source IP (src-ip). In this method, the switch utilizes the Source Ip of each packet to know which physical link in the EtherChannel bundle will be used to forward the packet. It is very effective in situations

where several devices with unique Ips are communicating with a similar destination such as a server/

- How would you go about configuring that in this network? (video)
- How would you verify that Load balancing is properly configured? (video)

https://drive.google.com/file/d/1b86LBHIAZ3AqOMPtJQ4y4DD-REyOci0U/view?usp=sharing

Instructions

- **Group assignment (Groups of 5)**
- **To be submitted by wednesday 30th October 2024: latest by 1:00 p.m.**
- **Remember to save your configurations with wr.**
    - **Router # wr**