ECE Paris

Computer Networks

ING 4 – SI (Information Systems, Big Data and Cyber Security)

Rafik ZITOUNI: rafik.zitouni@ece.fr

Takvor MAGADIS: tmagadis@inseec-edu.com

LAB2

Contents

I. Part 1 : IPv6

In this Lab, you will practice configuring IPv6 addresses on a router, servers, and clients. You will also practice verifying your IPv6 addressing implementation (see Figure 1).

1) Configure IPv6 Addressing on the **2811 Router**
2) Configure IPv6 Addressing on Servers
3) Configure IPv6 Addressing on Clients
4) Test and Verify Network Connectivity

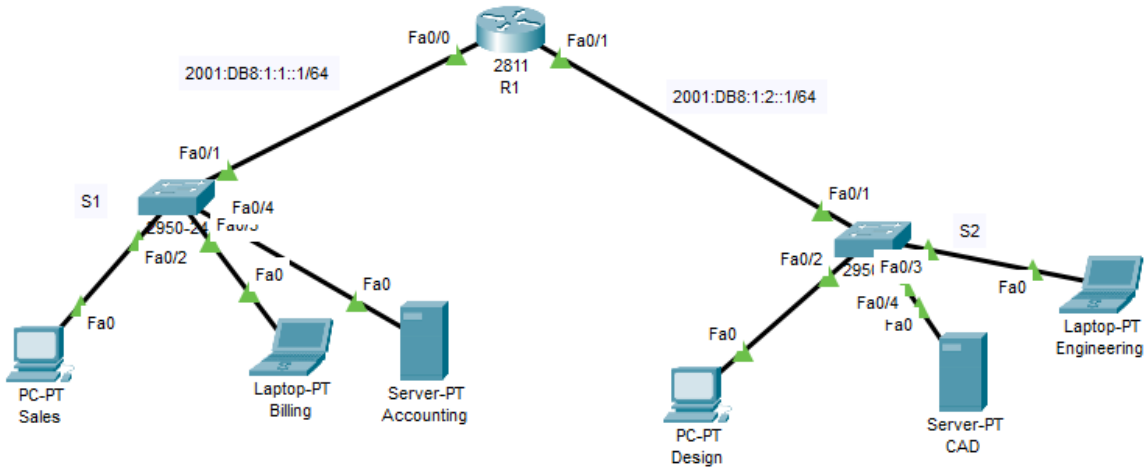

Figure 1 IPv6 topology

Table 1 Addressing Table

Device	Interface	IPv6 Address/Prefix	Default Gateway
R1	F0/0	2001:DB8:1:1::1/64	N/A
	F1/0	2001:DB8:1:2::1/64	N/A
	Link-local	FE80::1	N/A
Accounting	NIC	2001:DB8:1:1::2/64	FE80::1
Computer Aided Design (CAD)	NIC	2001:DB8:1:2::2/64	FE80::1
Design	NIC	2001:DB8:1:2::3/64	FE80::1
Engineering	NIC	2001:DB8:1:2::4/64	FE80::1

1. Autoconfiguration of IPv6 addressing

Autoconfiguration requires the least amount of configuration. It uses the MAC address of the device to create an IPv6 address with the link- local FE80:: prefix.

- **Step 1: Build the IPv6 topology network as shown in Figure 1.**
- **Step 2: Disable DNS lookup.**

```
R(config)#no ip domain-lookup
```

Q1.1 : What is the advantage of disabling DNS lookup ?

- **Step 3: Assign IPv6 auto conf IPv6 addressing**

Carry out the following steps to assign IPv6 addresses using autoconfiguration:

1. Begin by configuring the router, enter the interface configuration mode and enable IPv6 on the interface.

```
Router(config)#ipv6 unicast-routing
Router(config)#interface FastEthernet0/0
Router(config-if)#ipv6 enable
```

2. We will configure a link local address and a global unicast address on this interface. We'll use eui-64 to reduce the configuration.

```
Router(config-if)#ipv6 address autoconfig
Router(config-if)#ipv6 add 2000::/64 eui-64
Router(config-if)#no shutdown
```

3. Verify that the interface is up and has two IPv6 addresses

```
Router#show ipv6 interface brief
```

Q1.2 Why do we obtain two addresses for one interface?

4. Go to the Desktop tab of the PC Sales and Accounting server, open IP Configuration, and under the IPv6 Configuration section, choose Auto Config. The gateway and the PC's IP address will be assigned automatically (copy a screenshot):
5. Use ping to test the connectivity between PC Sales and Accounting. To view the IPv6 address from the command line of PCs and servers, use the **ipv6config** command.

2. Configure static IPv6 Addressing on the Router

Q1.3 For the following steps, show and comment the different modifications

- **Step 1: Reset router configuration**

The objective is to initialize the router with default configuration:

```
Router>enable
Router#write erase
Router#reload
```

- **Step 2: Enable the router to forward IPv6 packets**

Enter the ipv6 unicast-routing global configuration command. This command must be given to enable the router to forward IPv6 packets.

```
R1(config)# ipv6 unicast-routing
```

- **Step 3: Configure IPv6 addressing on FastEthernet0/0**

1. Click R1 and then the CLI tab. Press Enter.
2. Enter privileged EXEC mode.
3. Enter the commands necessary to transition to interface configuration mode for FastEthernet0/0.
4. Configure the IPv6 address with the following command

```
R1(config-if)# ipv6 address 2001:DB8:1:1::1/64
```

5. Configure the link-local IPv6 address with the following command:

```
R1(config-if)# ipv6 address FE80::1 link-local
```

6. Activate the interface.
7. Make **"show ipv6 interface brief"** (copy screenshot and comment the obtained result)

- **Step 4: Configure IPv6 addressing on FastEthernet0/1**

1. Enter the necessary commands to transit to interface configuration mode for FastEthernet0/1.
2. Refer to the Addressing Table to obtain the correct IPv6 address.
3. Configure the IPv6 address, the link-local address and activate the interface.
4. Make **"show ipv6 interface f0/1"** (copy screenshot and compare it to the result of step1)

3. Configure IPv6 Addressing on the Servers

- **Step 1: Configure IPv6 addressing on the Accounting Server. (Copy screenshots)**

1. Click Accounting and click the Desktop tab > IP Configuration.
2. Set the IPv6 Address to 2001:DB8:1:1::2 with a prefix of /64.
3. Set the IPv6 Gateway to the link-local address, FE80::1

- **Step 2: Configure IPv6 addressing on the CAD Server. (Copy screenshots)**

Repeat Steps 1.1 to 1.3 for the CAD server. Refer to the Addressing Table for the IPv6 address.

4. Configure IPv6 Addressing on Clients

- **Step 1: Configure IPv6 addressing on the Sales and Billing Client. (Copy screenshots)**

1. Click Billing and then select the Desktop tab followed by IP Configuration.
2. Configure the IPv6 with Auto Config

Q.1.4 What is the IPv6 address obtained by Auto Config ? the autoconfiguration is it stateless or stateful ?

3. Repeat Steps 1.1 through 1.2 for Sales.

- **Step 2: Configure IPv6 Addressing on the Engineering and Design Clients.** (Copy a screenshots)

1. Click Engineering and then select the Desktop tab followed by IP Configuration.
2. Set the IPv6 Address to 2001:DB8:1:2::4 with a prefix of /64.

3. Set the IPv6 Gateway to the link-local address, FE80::1.
4. Repeat Steps 1.1 through 1.3 for Design. Refer to the Addressing Table for the IPv6 address
5. Test and verify network connectivity

➢ **Step 1: Ping and Traceroute the server from the clients**

1. Click Sales and click the Desktop tab.
2. Click Command Prompt
3. Make Ping and tracert to servers Accounting and CAD (copy a screenshot).

➢ **Step 2: Open the server web pages from the clients.**

1. Click Sales and click the Desktop tab.
2. Click Web Browser. Enter 2001:DB8:1:1::2 in the URL box and click Go. The Accounting website should appear (copy screenshot hereafter).
3. Enter 2001:DB8:1:2::2 in the URL box and click Go. The CAD website should appear. (copy a screenshot)

Q1.5 Compare the two techniques static and autoconfiguration IPv6 addressing, advantages and drawbacks.

II. Part 2: Dynamic Routing (EIGRP)

By contrast to Lab1 (Part2), you will configure the routers using EIGRP dynamic routing protocols. The routes change dynamically related to the state and the topology of the network.
Use the following virtual network topology (see Figure 2).

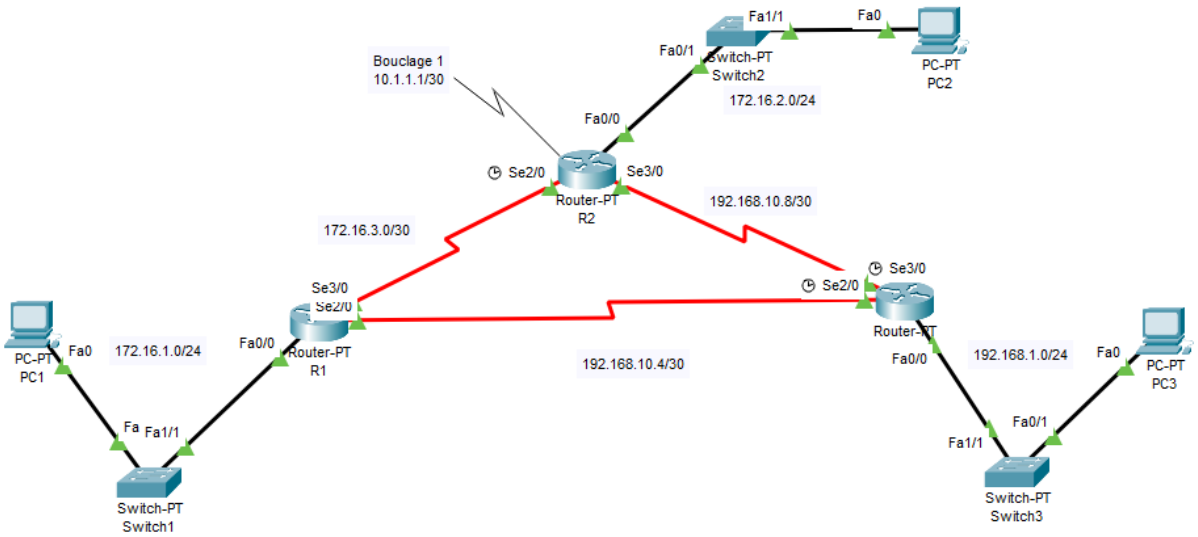

Figure 2 Network topology for EIGRP routing

A loopback address will be used on the R2 router to simulate a connection to an ISP, where all traffic that is not destined for the local network will be sent. Some segments of the network have been subnetted using VLSM (CIDR). EIGRP is a classless routing protocol that can be used to provide subnet mask

information in the routing updates. This will allow VLSM subnet information to be propagated throughout the network.

Table 2 Addressing Table

Device	Interface	IP address	Subnet mask	Default gateway
R1	Fa0/0	172.16.1.1	255.255.255.0	N/A
	Serial 2/0	192.168.10.5	255.255.255.252	N/A
	Serial 3/0	172.16.3.1	255.255.255.252	N/A
R2	Fa0/0	172.16.2.1	255.255.255.0	N/A
	Serial 2/0	172.16.3.2	255.255.255.252	N/A
	Serial 3/0	192.168.10.9	255.255.255.252	N/A
	Lo1	10.1.1.1	255.255.255.252	N/A
R3	Fa0/0	192.168.1.1	255.255.255.0	N/A
	Serial 2/0	192.168.10.6	255.255.255.252	N/A
	Serial 3/0	192.168.10.10	255.255.255.252	N/A
PC1	NIC	172.16.1.10	255.255.255.0	172.16.1.1
PC2	NIC	172.16.2.10	255.255.255.0	172.16.2.1
PC3	NIC	192.168.1.10	255.255.255.0	192.168.1.1

1. Prepare the Network.

- **Step 1: Cable a network that is similar to the one in the Topology Diagram.**

You can use PT-Router since it has the required interfaces shown in the topology.

Q2.1 Explain what the bouclage (loopback) Lo1 would represent for the router R2.

2. Perform Basic Router Configurations

Perform basic configuration of the R1, R2, and R3 routers according to the following guidelines:

1. Configure the router hostname.
2. Configure an EXEC mode password.

3. Configure and Activate Serial and Ethernet Addresses.

- **Step 1: Configure the interfaces on the R1, R2, and R3 routers.**

Configure the interfaces on the R1, R2, and R3 routers with the IP addresses from the Table 2 and Figure 2.

Q2.2: Give the corresponding commands to configure interfaces of one of the three routers.

- **Step 2: Verify IP addressing and interfaces.**

Use the **show ip interface brief** command to verify that the IP addressing is correct and that the interfaces are active. When you have finished, be sure to save the running configuration to the NVRAM of the router.

Q2.3: Bring the screenshot of the ip interfaces of the three routers.

- **Step 3: Configure Ethernet interfaces of PC1, PC2, and PC3.**

Configure the Ethernet interfaces of PC1, PC2, and PC3 with the IP addresses and default gateways from the table under the Topology Diagram.

Q2.4: Try to ping PC2 from PC1, is it possible? if yes or not, please comment.

4. Configure EIGRP on the Routers R1, R2 and R3

- **Step 1: Enable and configure EIGRP on Router R1**

Use the **router eigrp** command in global configuration mode to enable EIGRP on the R1 router. Enter a process ID of 1 for the *autonomous-system* parameter.

```
R1(config)#router eigrp 1
R1(config-router)#
```

Configure classful network 172.16.0.0.

Once you are in the Router EIGRP configuration sub-mode, configure the classful network 172.16.0.0 to be included in the EIGRP updates that are sent out of R1.

```
R1(config-router)#network 172.16.0.0
R1(config-router)#
```

The router will begin to send EIGRP update messages out each interface belonging to the 172.16.0.0 network. EIGRP updates will be sent out of the FastEthernet0/0 and Serial3/0 interfaces because they are both on subnets of the 172.16.0.0 network.

Configure the router to advertise the 192.168.10.4/30 network attached to the Serial2/0 interface.
Use the *wildcard-mask* option with the **network** command to advertise only the subnet and not the entire 192.168.10.0 classful network.
Note: Think of a "*wildcard mask"* as the inverse of a subnet mask. The inverse of the subnet mask 255.255.255.252 is 0.0.0.3. To calculate the inverse of the subnet mask, subtract the subnet mask from 255.255.255.255:

```
     255.255.255.255
-    255.255.255.252      Subtract the subnet mask
------------------
       0.  0.  0.  3      Wildcard mask
```

```
R1(config-router)# network 192.168.10.4 0.0.0.3
R1(config-router)#
```

When you finish with the EIGRP configuration for R1, return to privileged EXEC mode and save the current configuration to NVRAM.

```
R1(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
R1#write memory
```

- **Step 2: Enable and configure EIGRP routing on the R2 router.**

Use a process ID of 1.

```
R2(config)#router eigrp 1
R2(config-router)#
```

Use the classful address 172.16.0.0 to include the network for the FastEthernet0/0 interface.

```
R2(config-router)#network 172.16.0.0
R2(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.16.3.1 (Serial0/0/0) is up:
new adjacency
```

Notice that DUAL sends a notification message to the console stating that a neighbor relationship with another EIGRP router has been established.

Configure the R2 router to advertise the 192.168.10.8/30 network attached to the Serial0/0/1 Interface.

1. Use the *wildcard-mask* option with the **network** command to advertise only the subnet and not the entire 192.168.10.0 classful network.
2. When you are finished, return to privileged EXEC mode.

```
R2(config-router)#network 192.168.10.8 0.0.0.3
R2(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
R2#
```

Q2.5 Which interface on the R2 router is the neighbor adjacent? Use the following command line

```
R2#show ip eigrp neighbors
```

- **Step 3: Enable and configure EIGRP on the R3 router**

Q2.6 Give the corresponding commands for the configuration steps ?

1. Use a process ID of 1.
2. Use the classful network address for the network attached to the FastEthernet0/0 interface.
3. Include the wildcard masks for the subnets attached to the Serial0/0/0 and Serial 0/0/1 interfaces.

Q2.7 After these configurations, bring the screenshot of "`show ip route`" command for the three routers?

Q2.8 Please give the result of the following command : "`show ip protocols`"

Q2.9 Now you are able to ping PC2 and PC3 from PC1. Comment and provide the screenshots. If it doesn't work check the active state of your interfaces.

5. Configure EIGRP Metrics

Use the **show interface serial 3/0** command to view the EIGRP metric information for the interface on values that are shown for the bandwidth, delay, reliability, and load.

```
R1#show interfaces serial 3/0
Serial3/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 172.16.3.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
```

Q2.10: Comment the obtained values.

Q2.11 what is the default bandwidth metric for a serial interface? Modify the bandwidth of the Serial interfaces.

Q2.12 Set the bandwidth to 1024 kbps for the links between R1 ←→R2 R2←→R3 and 64 kbps for the link R1 ←→R3 using "`bandwidth`" command.

The bandwidth needs to be changed so that the EIGRP metric can be calculated correctly.

Q2.13 Check the modification of the bandwidth using "`show interface serial 2/0`"

Q2.14 Examine the successors and feasible distances in the routing table on R1 using the command "`show ip eigrp topology`" and "`show ip route`"

Q2.15 What are the paths to join the network 192.168.1.0? What is the best path resulting from EIGRP protocol? You give the feasible distance.

Q2.16 Simulate the transmission of ICMP messages.

Q2.17 Delete the defined passwords in the second task and report the required commands

III. Part 3: VLAN and Spanning Tree

Virtual LAN (**VLAN**) makes possible breaking the single broadcast domains into multiple ones. On a single switch we can have multiple broadcast domains. Ones we create multiple VLANs on a switch, it is possible to replicate the same configuration on all the other switches. This is where **VLAN Trunking Protocol** (**VTP**) comes in.

Spanning Tree Protocol (STP) provides path redundancy while preventing undesirable loops in the network.

1. Create VLAN

Step 1: Build the following topology using 2950-24 switch

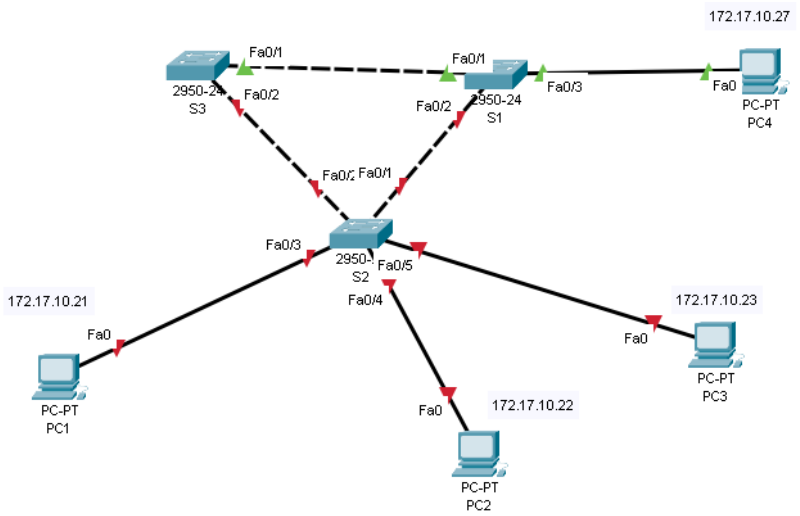

Figure 3 VLAN topology

- **Step 2: Configure Host PCs and verify the switch configuration**

Configure the Ethernet interfaces of PC1, PC2, PC3 and PC4 with the IP address, subnet mask and gateway indicated in the addressing table at the beginning of the lab.

Device	Interface	IP address	Subnet mask	Default gateway
S1	VLAN1	172.17.10.1	255.255.255.0	N/A
S2	VLAN1	172.17.10.2	255.255.255.0	N/A
S3	VLAN1	172.17.10.3	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.10.22	255.255.255.0	172.17.10.1
PC3	NIC	172.17.10.23	255.255.255.0	172.17.10.1
PC4	NIC	172.17.10.27	255.255.255.0	172.17.10.1

Q3.1 How to disable DNS lookup? Give the command line.

Use the **"`show vlan`"** command line to confirm that only default VLANs exist and that all ports are assigned to VLAN 1.

Configure the Ethernet interfaces of PC1, PC2, PC3, and PC4 with the IP address, subnet mask, and gateway indicated in the addressing table at the beginning of the lab.

Q3.2 Comment the obtained result of "`show vlan`" command line. Use "brief" to reduce the given information.

- **Step 3: Enable the user ports on S1 and S2**

Refer to the topology diagram to determine which switch ports on S2 are activated for end-user device access. These three ports will be configured for access mode and enabled with the no shutdown command.

Q3.3 List the possible switchport modes of a Cisco switch. Give the difference between these modes.

Q3.4 Configure the mode access on the interface fa 0/3 of S1 and fa0/3, fa0/4, fa0/5 for S2

For example, to configure the interfaces of the S2 you can use the following commands:

```
S2(config)#interface range fa0/3, fa0/4, fa0/5
S2(config-if-range)#switchport mode access
S2(config-if-range)#no shutdown
```

Check the following mode configuration and bring the screenshot using the command:

```
S1#show interfaces fastEthernet 0/3 switchport
```

- **Step 4: Enable trunk ports on S1, S2, and S3**

We enable a trunking on all links between switches to allow for additional VLANs to be added in the future.

Q3.5 How to enable trunk mode for all interfaces Fa0/1 et Fa0/2 of each switch: S1 S2 and S3 ?

For example, we type the following commands for the switch S1:

```
S1(config)#interface range fa0/1, fa0/2
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#no shutdown
```

You can use **"show interface trunk"** to ensure the good assignment of the interfaces.

- **Step 5: Configure the management interface address on all three switches S1, S2 and S3**

Configure the management interface address on all three switches and check the modification through **"show ip interface brief".**

For example, we use the following commands for S1:

```
S1(config)#interface Vlan1
S1(config-if)#ip address 172.17.10.1 255.255.255.0
S1(config-if)#no shutdown
```

Q3.6 Verify that the switches are correctly configured by pinging between them. From S1, ping the management interface on S2 and S3. From S2, ping the management interface on S3. Comment the obtained result.

- **Step 6: Create a new VLANS on S2 with the id 10, 20 and 30 with names finance, staff and guest, respectively:**

vlan 10 → finance (access mode of the interfaces of Fa0/16 to Fa0/20)
vlan 20 → staff (access mode of the interfaces of Fa0/3)
vlan 30 → guest (access mode of the interfaces from Fa0/4 to Fa0/15)
Example:

```
S2(config)#vlan 30
S2(config-vlan)#name guest
S2(config-vlan)#exit
S2(config)#interface range f0/4-15
S2(config-if-range)#switchport access vlan 30
```

Q3.7 Verify the creation of the VLAN via "`show vlan brief`" command line.

Q3.8 Ping from PC3 the PC1, PC2 and PC4. Comment the obtained result.

2. VTP modes

The objective of this part is to create VLAN Trunking Protocol (VTP) to make easy to share the switches' configuration. VTP has three modes: Server, Client and Transparent2

- **Server:** This is the default mode of VTP; in this mode, switches are allowed to modify their VLANs and send VTP advertisements.
- **Client:** In this mode, switches listen for VTP advertisements from other server switches. Client switches aren't allowed to modify their VLAN database locally.
- **Transparent:** This mode works independent of other switches. In this mode, the switch only forwards the VTP advertisement it receives and does not generate any; neither does it modify its own VLANs on the VTP advertisements.

Q3.9 Use the command "`show vlan status`" on S2. What is the maximum number of supported VLANs?

Q3.10 What is the vtp mode by default on the switches?

Q3.11 Set the name of VTP domain and password of S2

The switch S2 **is on the server mode**. You can define the domain name "My-office" and the password "cisco of the vtp as follow:

```
S2(config)#vtp domain My-office
S2(config)#vtp password cisco
```

Q3.12 change the vtp mode for S1 to client, with the same domain and password of the server, then report the command line.

Use the command line **"show vtp status"** to see the configuration values for each switch.

Q3.13 Try to create a new vlan on the S2. Is it possible? explain.

Step 7: Share the vlan configuration of S2 with the switch S1

The following commands ensure that the trunk mode is set of the interface Fa0/1 of S2.

```
S2(config)#interface fa0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk allowed vlan 1-99
```

Q3.14 Now use the commands "show vtp status" and "show vlan brief" to ensure that the VLAN configuration is the same for S1 and S2. Do the same for the switch S3.

3. Configuration of the Spanning Tree

The Spanning Tree Protocol is an algorithm meant to reduce the overhead in the network. In addition to the STP algorithm allowing information to flow safely between devices, it also stops the potential for loops. STP offers various backups that become active when the main connection experiences technical hiccups.

- **Step 1: Examine the default configuration of 802.1D STP.**

On each switch, display the spanning tree table with the **"show spanning-tree"** command. Root selection varies depending on the Bridge ID of each switch in your lab resulting in varying outputs.

Q3.15 Report the Bridge ID Priority and explain the obtained numbers.

Q3.16 Identify the root bridge switch for each vlan; why a particular switch is selected the root bridge?

To answer this question, please compare the output of the command **"show spanning-tree vlan 20"** for each switch.

Q3.17 Change the root bridge for vlan 20 to be one of the other switches. Give the related command.

Q3.18 Find designated Ports, Root Ports, Blocked Ports on each switch.