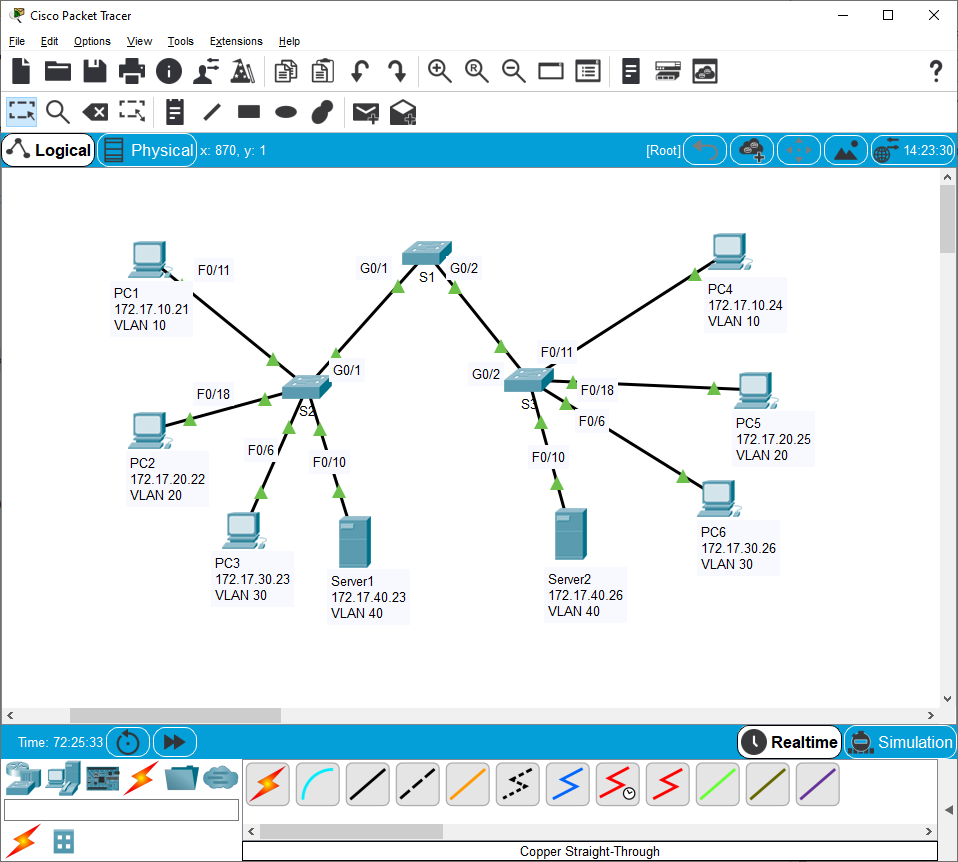
**Practice 12 – Configuring VLANs**

**Topology**



**Addressing Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **VLAN** |
| PC1 | NIC | 172.17.10.21 | 255.255.255.0 | 10 |
| PC2 | NIC | 172.17.20.22 | 255.255.255.0 | 20 |
| PC3 | NIC | 172.17.30.23 | 255.255.255.0 | 30 |
| PC4 | NIC | 172.17.10.24 | 255.255.255.0 | 10 |
| PC5 | NIC | 172.17.20.25 | 255.255.255.0 | 20 |
| PC6 | NIC | 172.17.30.26 | 255.255.255.0 | 30 |
| Server1 | NIC | 172.17.40.23 | 255.255.255.0 | 40 |
| Server2 | NIC | 172.17.40.26 | 255.255.255.0 | 40 |

1. **Objectives**

**Part 1: Verify the Default VLAN Configuration**

**Part 2: Configure VLANs**

**Part 3: Assign VLANs to Ports**

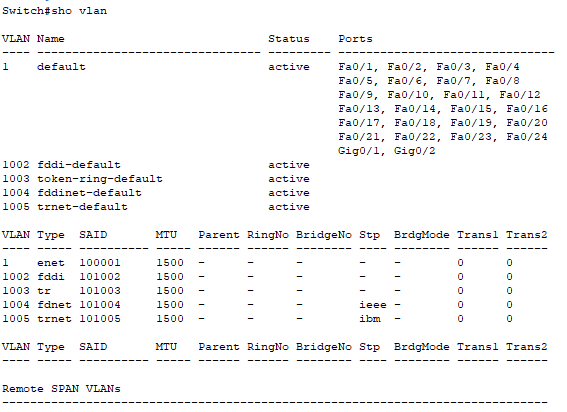
**Background**

VLANs are helpful in the administration of logical groups, allowing members of a group to be easily moved, changed, or added. This activity focuses on creating and naming VLANs, and assigning access ports to specific VLANs.

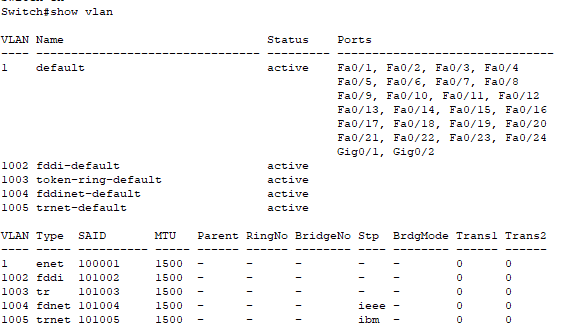
1. **View the Default VLAN Configuration**
   1. **Display the current VLANs.**

On S1, issue the command that displays all VLANs configured. By default, all interfaces are assigned to VLAN 1.

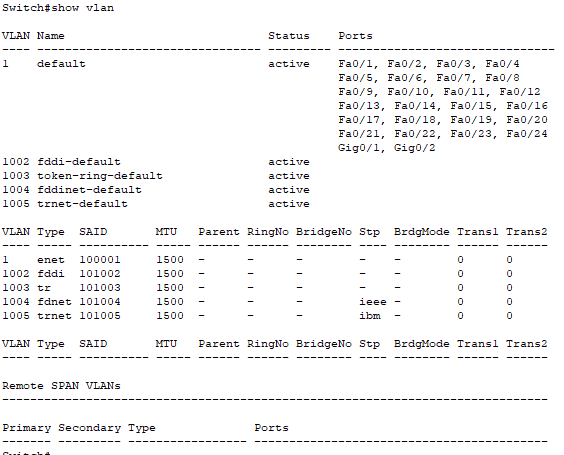
**Switch 1**

****

**Switch 2**

****

**Switch 3**

****

* 1. **Verify connectivity between PCs on the same network.**

Notice that each PC can ping the other PC that shares the same network.

* PC1 can ping PC4
* PC2 can ping PC5
* PC3 can ping PC6
* Server1 can ping Server2

Pings to PCs and Servers in other networks fail.





What benefit will configuring VLANs provide to the current configuration?

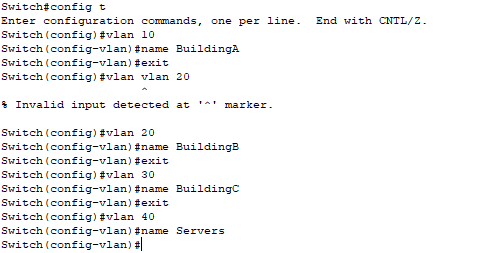
**Cuando configuramos las VLANs la topología actual obtendremos seguridad, mayor rendimiento, aplicaciones más simples, entre otros.**

**Configure VLANs**

* 1. **Create and name VLANs on S1.**

Create the following VLANs. Names are case-sensitive:

* VLAN 10: BuildingA
* VLAN 20: BuildingB
* VLAN 30: BuildingC
* VLAN 40: Servers
* VLAN 99: Management&Native



* 1. **Verify the VLAN configuration.**

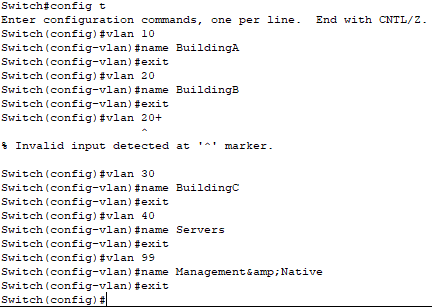
Which command will only display the VLAN name, status, and associated ports on a switch?

**# show vlan brief**

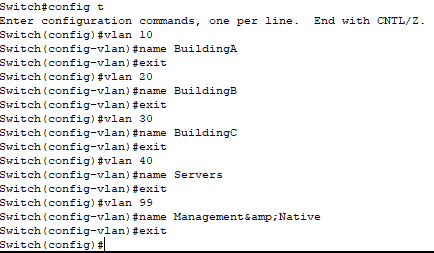
* 1. **Create the VLANs on S2 and S3.**

Using the same commands from Step 1, create and name the same VLANs on S2 and S3.

**S2**



**S3**

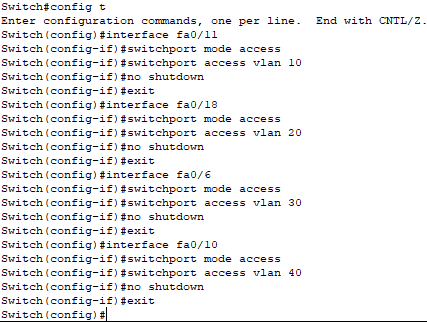
****

* 1. **Verify the VLAN configuration.**

1. **Assign VLANs to Ports**
   1. **Assign VLANs to the active ports on S2.**

Configure the interfaces as access ports and assign the VLANs as follows:

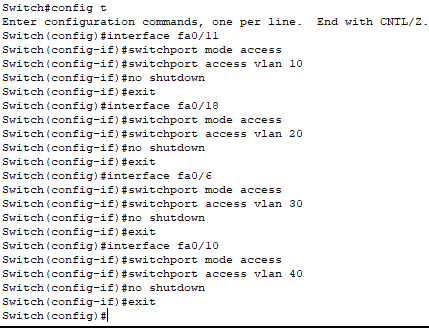
* VLAN 10: FastEthernet 0/11
* VLAN 20: FastEthernet 0/18
* VLAN 30: FastEthernet 0/6
* VLAN 40: FastEthernet 0/10



* 1. **Assign VLANs to the active ports on S3.**

S3 uses the same VLAN access port assignments as S2. Configure the interfaces as access ports and assign the VLANs as follows:

* VLAN 10: FastEthernet 0/11
* VLAN 20: FastEthernet 0/18
* VLAN 30: FastEthernet 0/6
* VLAN 40: FastEthernet 0/10



* 1. **Verify loss of connectivity.**

Previously, PCs that shared the same network could ping each other successfully.



Try pinging between PC1 and PC4. Although the access ports are assigned to the appropriate VLANs, were the pings successful? Why?

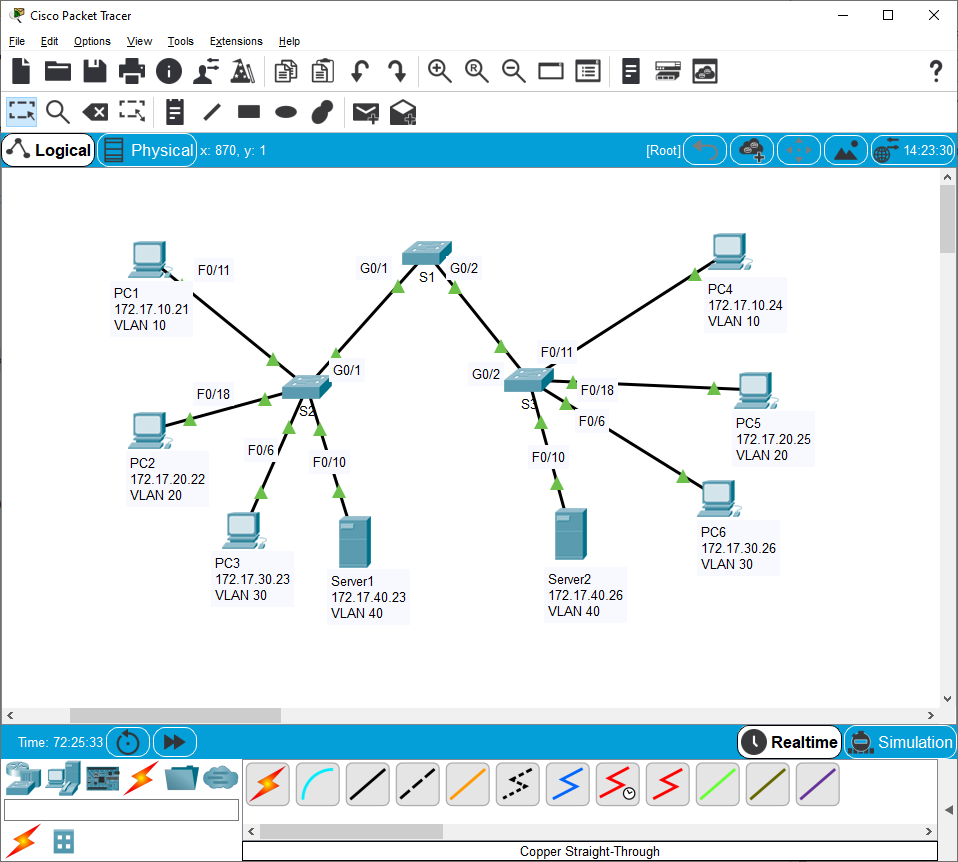
**No, todos los pings que se habían realizado al principio fallaron porque los puertos contienen las VLAN que se configuraron anteriormente.**

What could be done to resolve this issue?

**Configurar los puertos de los switch como trunk**

**Practice 13 – Configuring Trunks**

**Topology**



1. **Addressing Table**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Switch Port** | **VLAN** |
| PC1 | NIC | 172.17.10.21 | 255.255.255.0 | S2 F0/11 | 10 |
| PC2 | NIC | 172.17.20.22 | 255.255.255.0 | S2 F0/18 | 20 |
| PC3 | NIC | 172.17.30.23 | 255.255.255.0 | S2 F0/6 | 30 |
| PC4 | NIC | 172.17.10.24 | 255.255.255.0 | S3 F0/11 | 10 |
| PC5 | NIC | 172.17.20.25 | 255.255.255.0 | S3 F0/18 | 20 |
| PC6 | NIC | 172.17.30.26 | 255.255.255.0 | S3 F0/6 | 30 |
| Server1 | NIC | 172.17.40.23 | 255.255.255.0 | S2 F0/10 | 40 |
| Server2 | NIC | 172.17.40.26 | 255.255.255.0 | S3 F0/10 | 40 |

1. **Objectives**

**Part 1: Verify VLANs**

**Part 2: Configure Trunks**

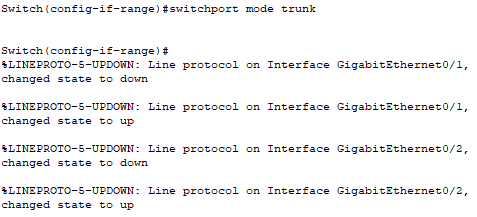
1. **Background**

Trunks are required to pass VLAN information between switches. A port on a switch is either an access port or a trunk port. Access ports carry traffic from a specific VLAN assigned to the port. A trunk port by default is a member of all VLANs; therefore, it carries traffic for all VLANs. This activity focuses on creating trunk ports, and assigning them to a native VLAN other than the default.

1. **Verify VLANs**
   1. **Display the current VLANs.**
      1. On **S1**, issue the command that will display all VLANs configured. There should be ten VLANs in total. Notice how all 24 access ports on the switch are assigned to VLAN 1.
      2. On **S2** and **S3**, display and verify all the VLANs are configured and assigned to the correct switch ports according to the **Addressing Table**.
   2. **Verify loss of connectivity between PCs on the same network.**

Although **PC1** and **PC4** are on the same network, they cannot ping one another. This is because the ports connecting the switches are assigned to VLAN 1 by default. In order to provide connectivity between the PCs on the same network and VLAN, trunks must be configured.

1. **Configure Trunks**
   1. **Configure trunking on S1 and use VLAN 99 as the native VLAN.**
      1. Configure G0/1 and G0/2 interfaces on S1 for trunking.



* + 1. Configure VLAN 99 as the native VLAN for G0/1 and G0/2 interfaces on **S1**.

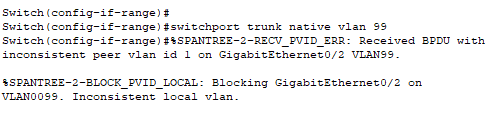
S1(config-if)# **switchport trunk native vlan 99**

The trunk port takes about a minute to become active due to Spanning Tree. Click **Fast Forward Time** to speed the process. After the ports become active, you will periodically receive the following syslog messages:

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (99), with S3 GigabitEthernet0/2 (1).

%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (99), with S2 GigabitEthernet0/1 (1).

You configured VLAN 99 as the native VLAN on S1. However, S2 and S3 are using VLAN 1 as the default native VLAN as indicated by the syslog message.



Although you have a native VLAN mismatch, pings between PCs on the same VLAN are now successful. Why?

**Por que se habilitaron los puertos, ya que configuramos en modo trunk, entonces automáticamente se habilita el otro lado de los enlaces.**

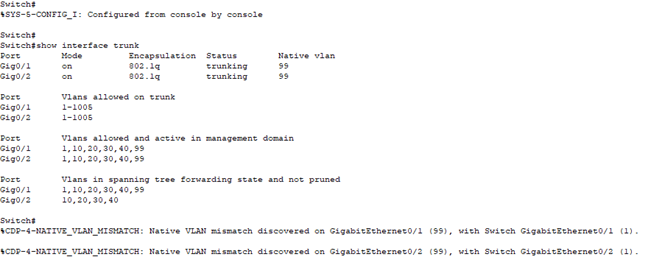
* 1. **Verify trunking is enabled on S2 and S3.**

On **S2** and **S3**, issue the **show interface trunk** command to confirm that DTP has successfully negotiated trunking with S1 on S2 and S3. The output also displays information about the trunk interfaces on S2 and S3.

Which active VLANs are allowed to cross the trunk?

**1, 10, 20, 30, and 99.**

* 1. **Correct the native VLAN mismatch on S2 and S3.**
     1. Configure VLAN 99 as the native VLAN for the appropriate interfaces on S2 and S3.
     2. Issue **show interface trunk** command to verify the correct native VLAN configuration.
  2. **Verify configurations on S2 and S3.**
     1. Issue the **show interface** *interface* **switchport** command to verify that the native VLAN is now 99.



* + 1. Use the **show vlan** command to display information regarding configured VLANs. Why is port G0/1 on S2 no longer assigned to VLAN 1?

**Porque configuramos el puerto G0/1 cómo trunk y con ese comando no se muestran los puertos cuando están en modo trunk**