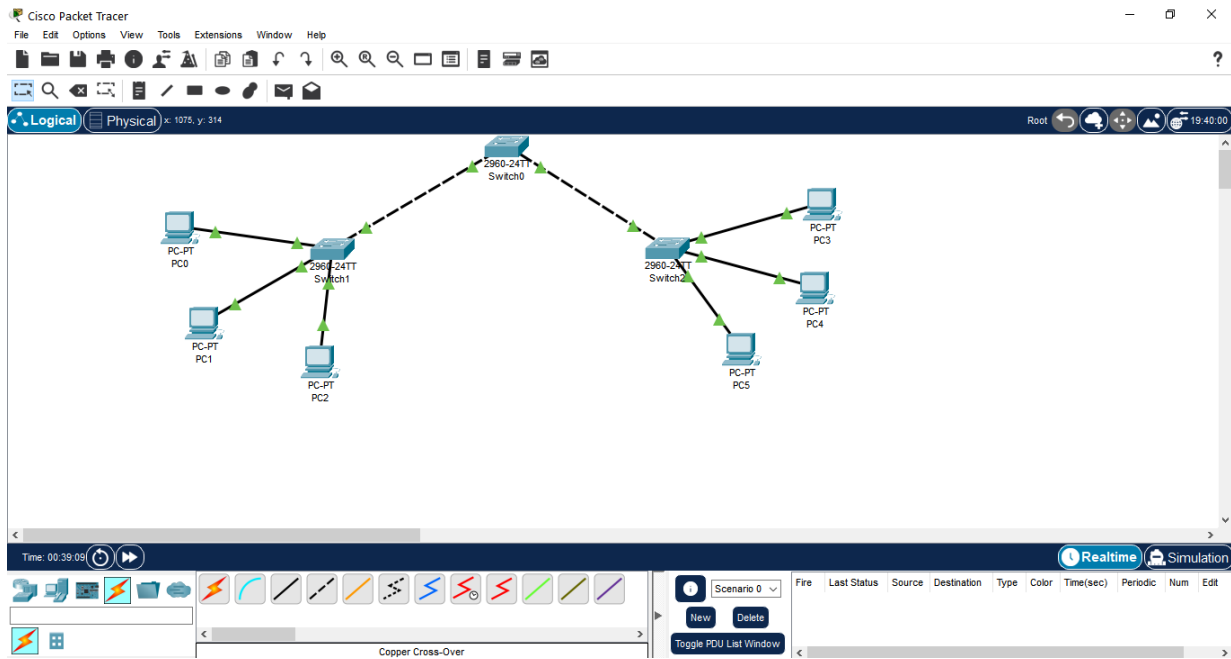


# Basic VLAN Configuration (ESP)

Cisco Packet Tracer 8.1.1

## 1: Preparar la red

### Paso 1: Cablear una red de manera similar al diagrama de topología.



Para poder realizar la practica se necesitan 6 PC y 3 Switch (los switches son de modelo 2960-24TT).

El switch 1 (S1) será el troncal, mientras que el Switch S2 y S3 son de acceso.

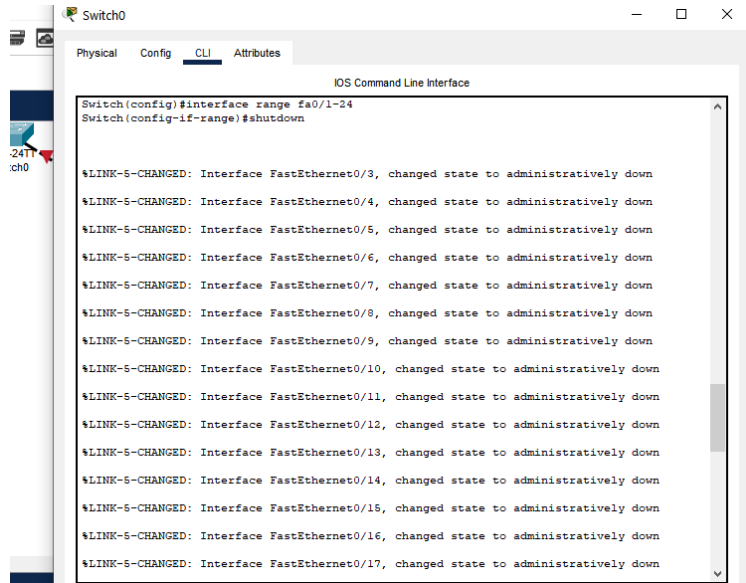
Conexiones de los hosts:

- En los switches se utilizarán cables Cooper Cross-Over e irán direccionados del S2 al S1, en donde las entradas de ambos serán fastEthernet0/1 y para S3 y S1 las entradas en ambos son fastEthernet0/2 en ambos.
- En las PC los cables que se utilizan son Cooper Straight-Through, donde los puertos que se utilizaran en los switches son:
  - ✓ PC0 puerto fastEthernet 0/11
  - ✓ PC1 puerto fastEthernet 0/18
  - ✓ PC2 puerto fastEthernet 0/6
  - ✓ PC3 puerto fastEthernet 0/11
  - ✓ PC4 puerto fastEthernet 0/18
  - ✓ PC5 puerto fastEthernet 0/6

### Paso 2: Deshabilitación y habilitación de puertos de acceso.

En este paso se deshabilitarán los puertos que no se utilizaran dentro de los switches y será mediante su desactivación. Esto se deberá de aplicar en los 3 switches y se tendrán que deshabilitar los puertos tanto fastEthernet como los GigabitEthernet.

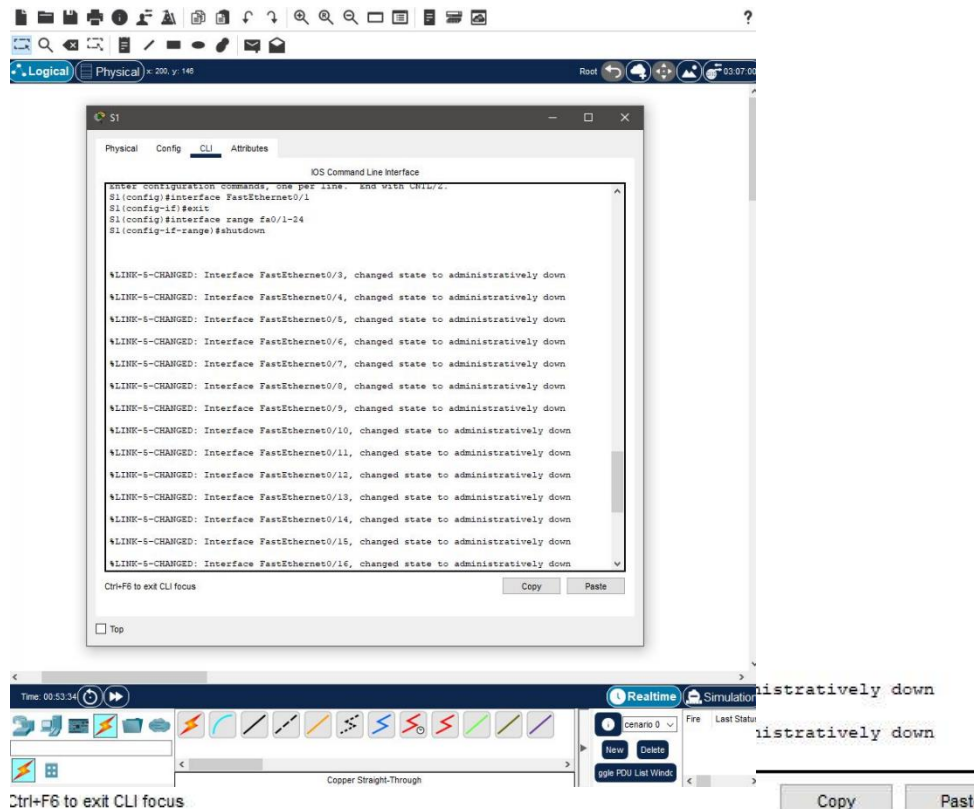
S1

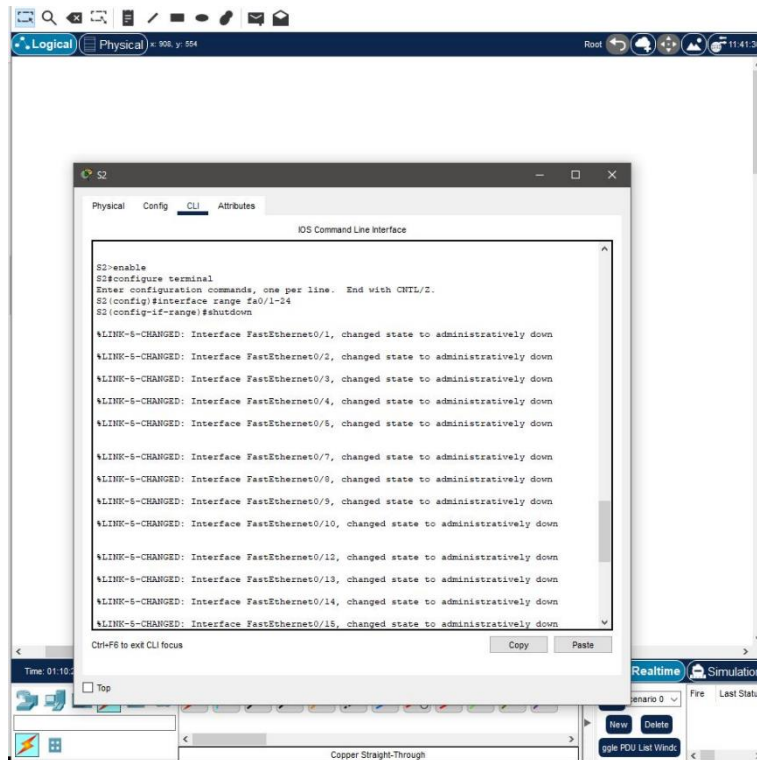


S2

```
Switch(config-if-range)#interface range gi0/1-2
Switch(config-if-range)#shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
Switch(config-if-range)#
```



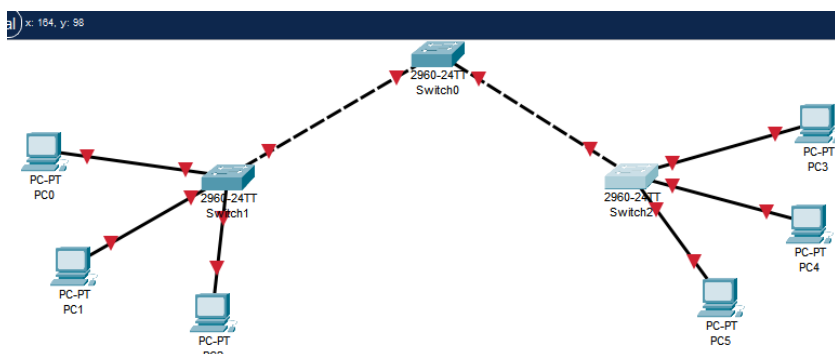


```

S2(config-if-range)#shutdown
S2(config-if-range)#interface range gi0/1-2
S2(config-if-range)#shutdown
  
```

```

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
S2(config-if-range)#
  
```



En la imagen anterior se puede apreciar que los puertos quedaron deshabilitados.

## 2: Realizar las configuraciones básicas del switch.

### Paso 1: Configurar los switches de acuerdo con la guía:

#### S1

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#enable password clase1
S1(config)#enable secret clase
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

#### Nombre del host y contraseña modo EXEC

```
S1>enable
Password:
Password:
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#line console 0
S1(config-line)#login
% Login disabled on line 0, until 'password' is set
S1(config-line)#password clase1
S1(config-line)#exit
S1(config)#exit
S1#
```

#### Contraseña para conexiones de consola

```
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#line vty 0 4
S1(config-line)#login
% Login disabled on line 1, until 'password' is set
% Login disabled on line 2, until 'password' is set
% Login disabled on line 3, until 'password' is set
% Login disabled on line 4, until 'password' is set
% Login disabled on line 5, until 'password' is set
S1(config-line)#password clase1
S1(config-line)#
```

Ctrl+F6 to exit CLI focus

Copy

Paste

#### Contraseña para conexiones vty

#### S2

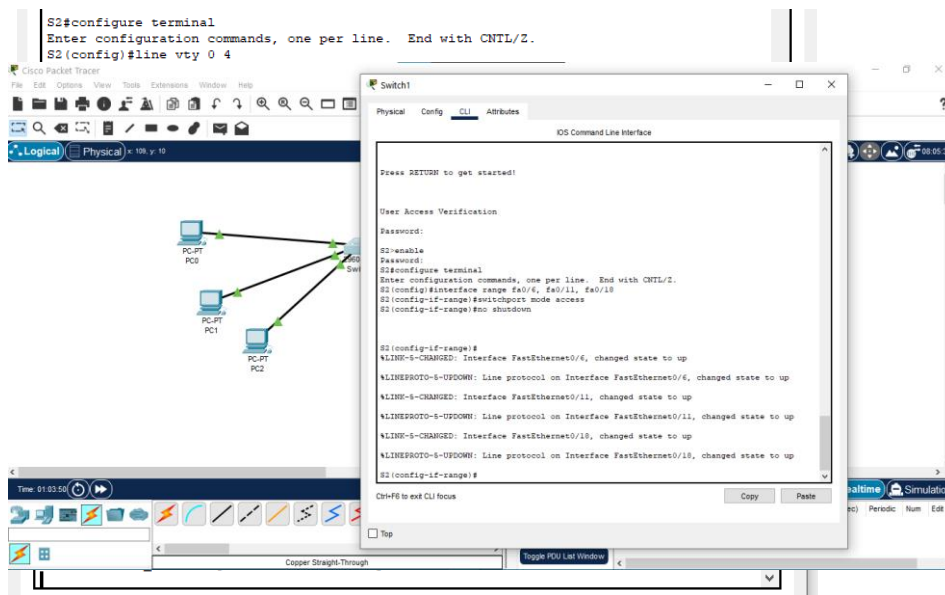
```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#enable password clase2
S2(config)#enable secret clase
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
```

#### Nombre del host y contraseña modo EXEC

```
S2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#line console 0
S2(config-line)#login
% Login disabled on line 0, until 'password' is set
S2(config-line)#password clase2
S2(config-line)#exit
..
```

#### Contraseña para conexiones de consola



## Nombre del host y contraseña modo EXEC

```
S3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#line console 0
S3(config-line)#login
% Login disabled on line 0, until 'password' is set
S3(config-line)#password clase3
S3(config-line)#exit
S3(config)#
```

Ctrl+F8 to exit CLI focus

Copy

Paste

## Contraseña para conexiones de consola

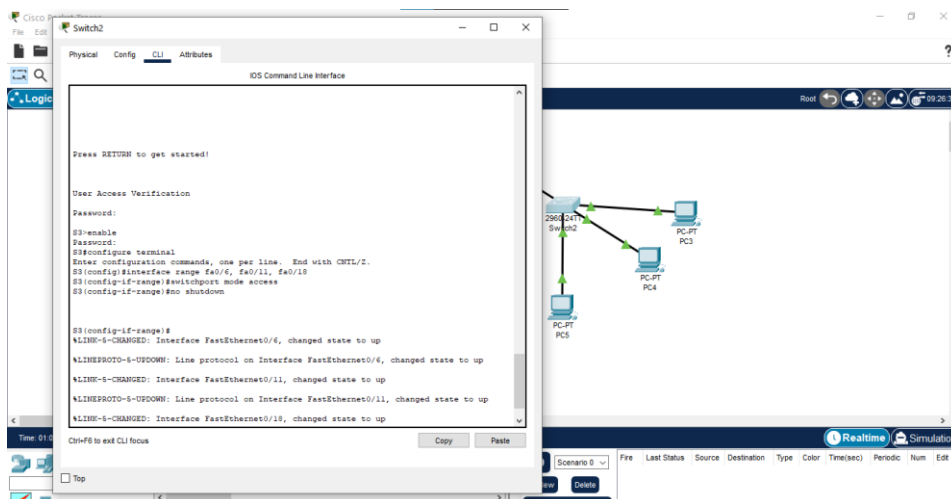
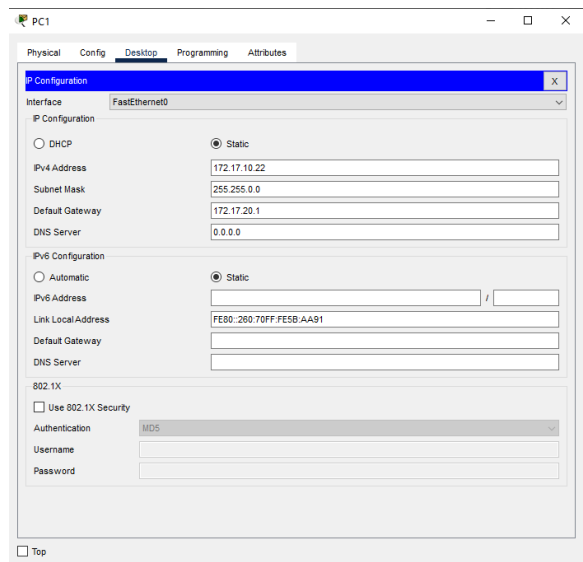
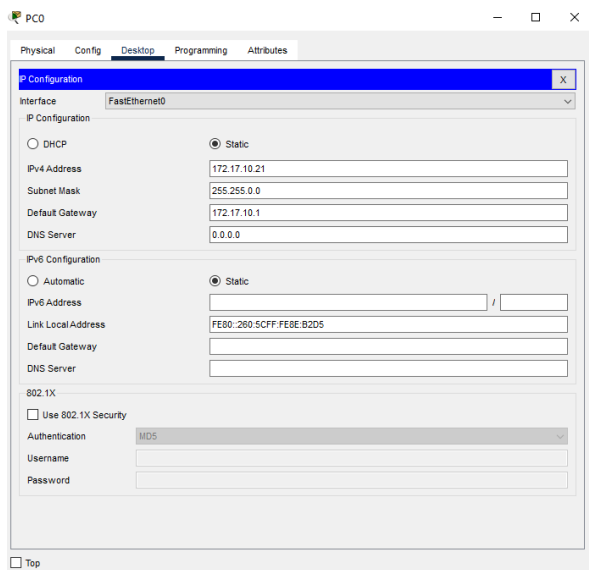
```
S3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#line vty 0 4
S3(config-line)#login
% Login disabled on line 1, until 'password' is set
% Login disabled on line 2, until 'password' is set
% Login disabled on line 3, until 'password' is set
% Login disabled on line 4, until 'password' is set
% Login disabled on line 5, until 'password' is set
S3(config-line)#password clase3
S3(config-line)#exit
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

## Contraseña para conexiones vty

### **Paso 2: Volver a habilitar los puertos de usuario en S2 y S3**

Para poder tener acceso a los puertos, es necesario volverlos a activar. Pero solo los puertos que se están ocupando en los switches, que en este caso son fa0/11, fa0/18 y fa0/6 (esto en el S2 y S3).

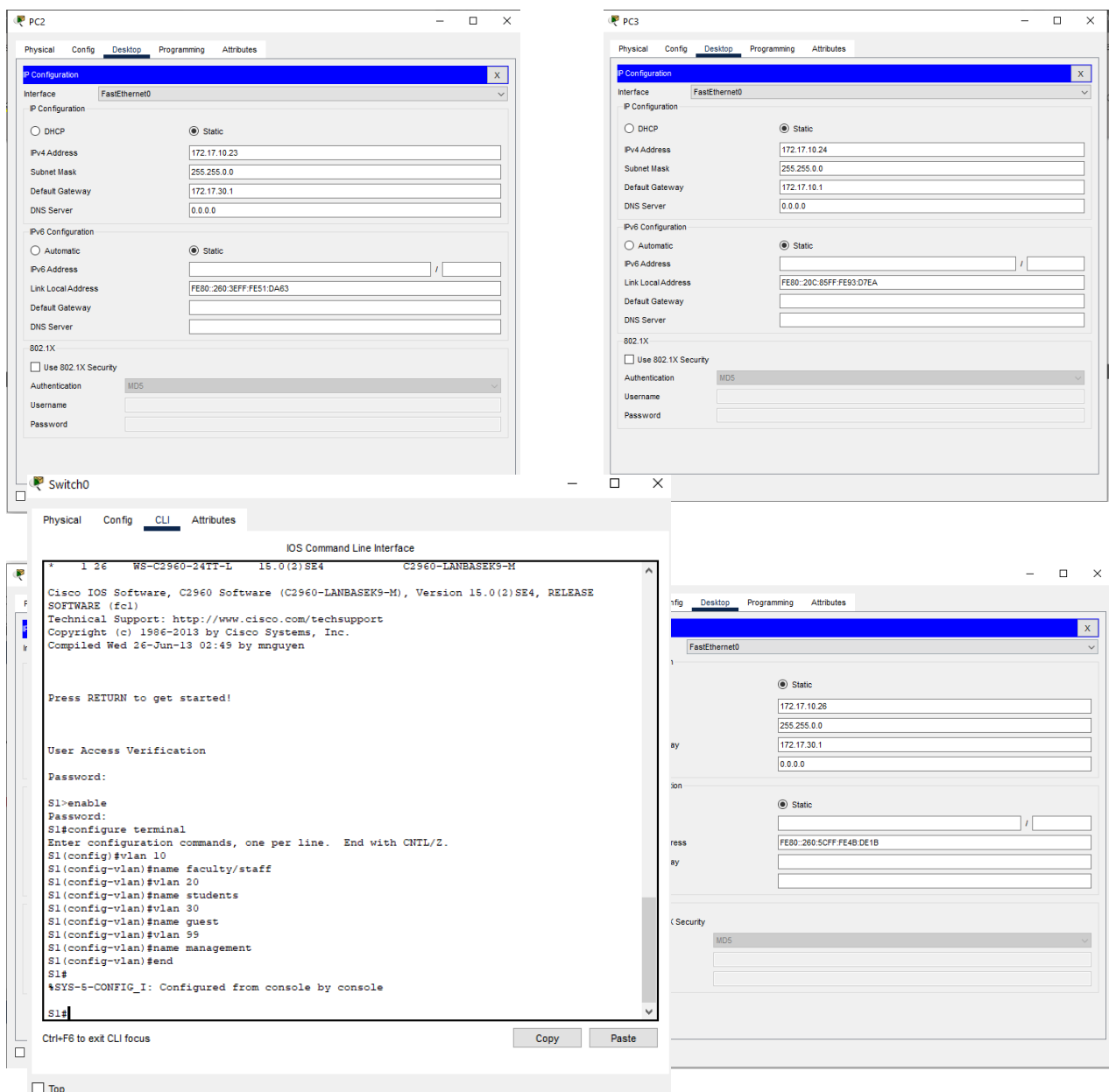
**S2**



## **Paso 1: Configurar las PC**

Las PC serán configuradas como se muestran a continuación:

Dispositivo Nombre de host	Interfaz	Dirección IP	Máscara de subred	Gateway (Puerta de salida predeterminada)
PC0	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC1	NIC	172.17.10.22	255.255.255.0	172.17.20.1
PC2	NIC	172.17.10.23	255.255.255.0	172.17.30.1
PC3	NIC	172.17.10.24	255.255.255.0	172.17.10.1
PC4	NIC	172.17.10.25	255.255.255.0	172.17.20.1
PC5	NIC	172.17.10.26	255.255.255.0	172.17.30.1

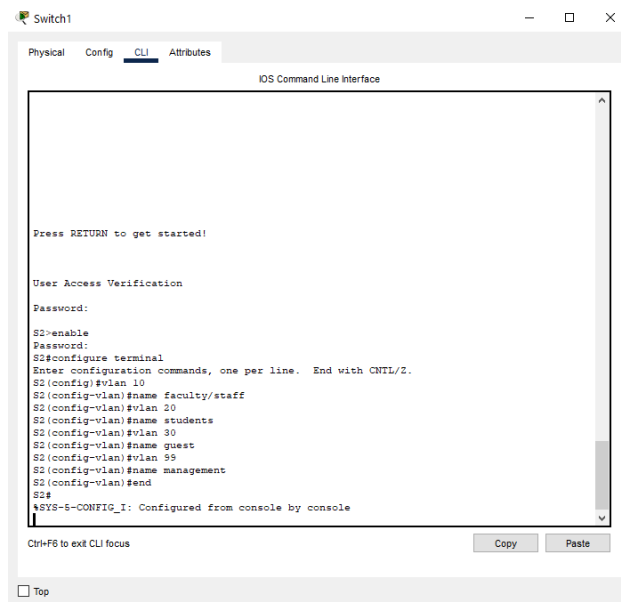


## 4: Configurar las VLAN en el switch

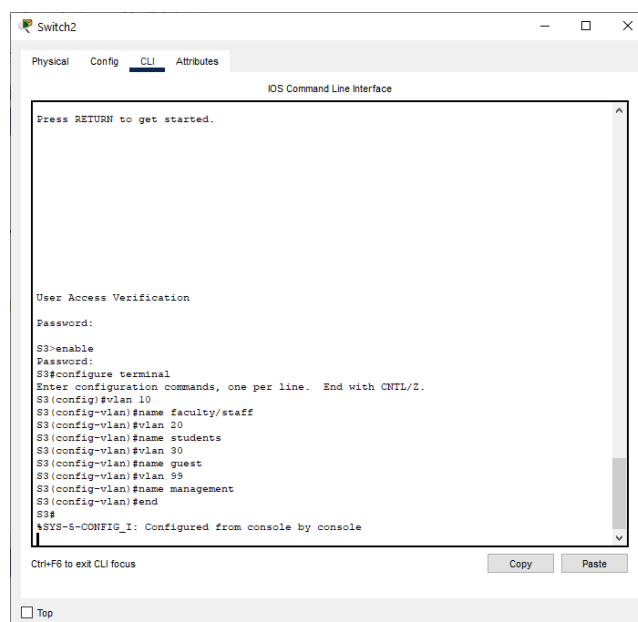
### Paso1: Crear las VLAN en el switch S1.

En este paso se tendrán que configurar 4 VLAN con respectivos nombres diferentes

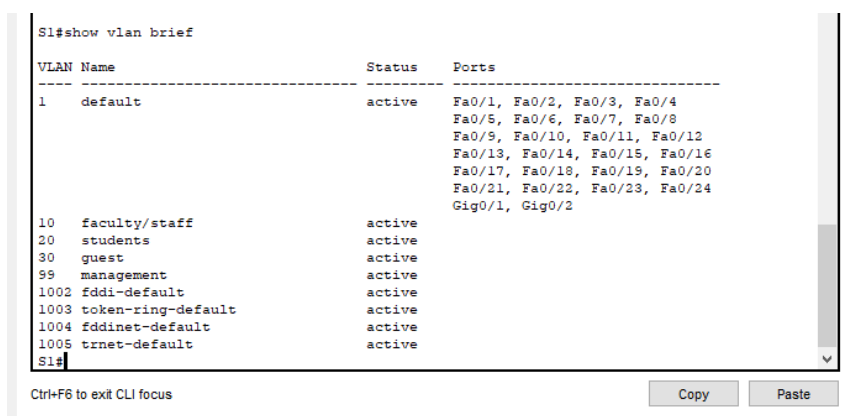
VLAN	Nombre
VLAN 10	Docente/personal
VLAN 20	Estudiantes
VLAN30	Guest
VLAN 99	Administración



## **Paso 2: Verificar que las VLAN estén creadas en S1.**



En este paso se verifica que las VLAN han sido creadas correctamente.





```
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   faculty/staff           active
20   students                active
30   guest                   active
99   management              active
1002 fddi-default             active
1003 token-ring-default       active
1004 fddinet-default          active
1005 trnet-default            active
S3#
```

Ctrl+F6 to exit CLI focus

Copy Paste

### Paso 3: Configurar y asignar un nombre a las VLAN en los switches S2 y S3

S2

S3

### Verificación de VLAN

S2

```
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   faculty/staff           active
20   students                active
30   guest                   active
99   management              active
1002 fddi-default             active
1003 token-ring-default       active
1004 fddinet-default          active
1005 trnet-default            active
S2#
```

Ctrl+F6 to exit CLI focus

Copy Paste

S3

```
S2#
S2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface range fa0/6-10
S2(config-if-range)#switchport access vlan 30
S2(config-if-range)#interface range fa0/11-17
S2(config-if-range)#switchport access vlan 10
S2(config-if-range)#interface range fa0/18-24
S2(config-if-range)#switchport access vlan 20
S2(config-if-range)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console
copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
```

Ctrl+F6 to exit CLI focus

Copy Paste

### Paso 4: Asignar puertos de switch a las VLAN en S2 y S3.

Los puertos se asignan a las VLAN en modo de configuración de interfaces.

La asignación corresponde a la siguiente (será para S2 y S3).

Puertos	Asignación
Fa0/6-0/10	VLAN 30
Fa0/11-0/17	VLAN 10
Fa0/18-0/24	VLAN 20

S2

```
S2#
S2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface range fa0/6-10
S2(config-if-range)#switchport access vlan 30
S2(config-if-range)#interface range fa0/11-17
S2(config-if-range)#switchport access vlan 10
S2(config-if-range)#interface range fa0/18-24
S2(config-if-range)#switchport access vlan 20
S2(config-if-range)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console
copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
```

Ctrl+F6 to exit CLI focus

Copy

Paste

S3

```
S2#show vlan id 10
```

VLAN Name	Status	Ports
10 faculty/staff	active	Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
10	enet	100010	1500	-	-	-	-	-	0	0

```
S2#
```

Ctrl+F6 to exit CLI focus

Copy

Paste

#### Paso 4: Determinar qué puertos se han agregado

S2

- Los puertos de switch 2 dentro de la VLAN 10 son: Fa0/11 a la Fa0/17

#### Paso 5: Asignar la VLAN de administración

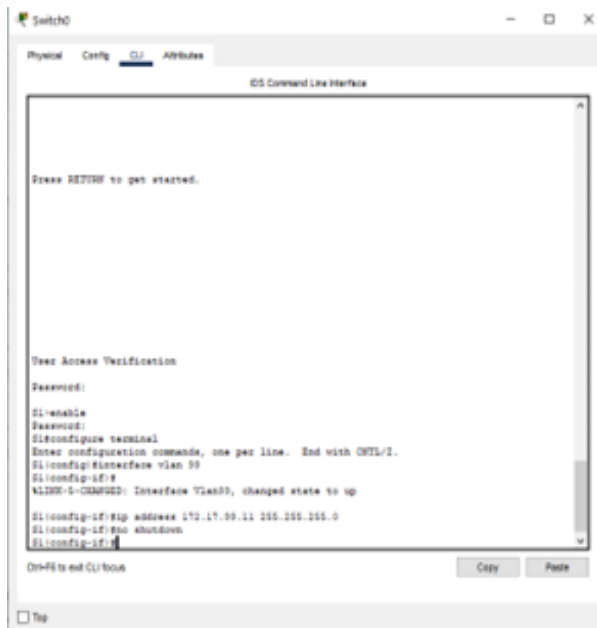
Una VLAN de administración se configura para acceder a las capacidades administrativas de un switch.

La VLAN 1 funciona como VLAN de administración si no se ha definido específicamente otra VLAN. Para ello la VLAN de administración necesita una dirección IP y máscara de subred. Debido a que la configuración no convencional de un switch Cisco cuenta con la VLAN 1 como VLAN predeterminada, la misma es una

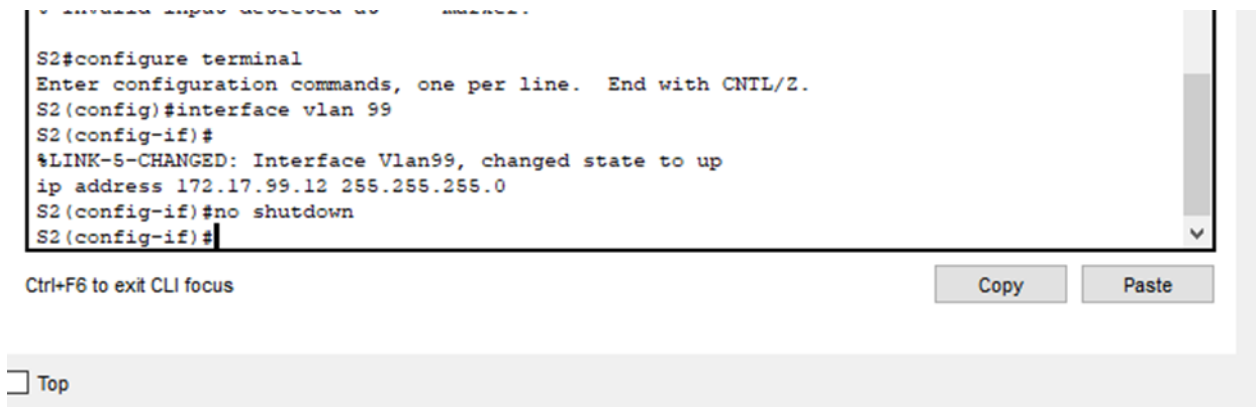
mala elección como VLAN de administración, esto se debe a que no se desea que cualquier usuario pueda acceder al switch de manera determinada.

Y para ello se tiene que mencionar que la VLAN 99 se ha configurado como VLAN de administración.

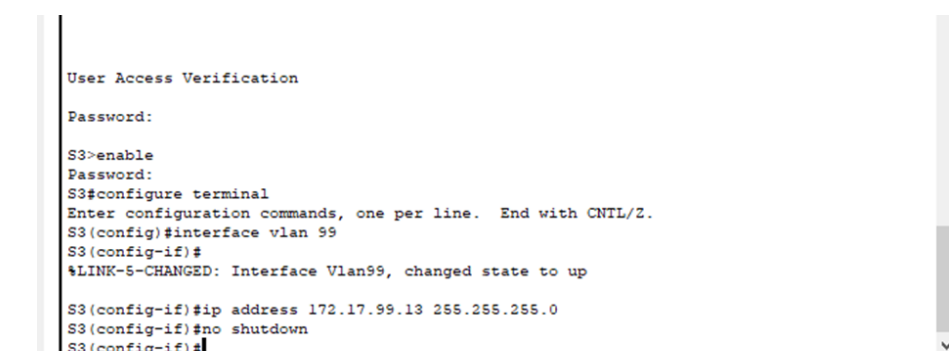
## S1



## S2



## S3



Cuando se asigna una dirección de administración, permite la comunicación IP entre switches y que cualquier host conectado a un puerto asignado a la VLAN 99 se conecte a los switches. Esto es gracias a que la VLAN 99 se encuentra configurada como VLAN de administración y cualquier puerto asignado a esta VLAN se considera puerto de administración. También se debe contar con seguridad para controlar qué dispositivos pueden conectarse a estos puertos.

### **Paso 6: Configurar los enlaces troncales y la VLAN nativa para los puertos de enlace troncales en todos los switches.**

Los enlaces troncales son conexiones entre los switches que permiten a los mismos intercambiar información para todas las VLAN. En la topología, la VLAN nativa es VLAN 99. Es por ello por lo que en los siguientes comandos se implementará la configuración de enlaces troncales (esto será en S1, S2 Y S3).

#### **S1**

```
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface range fa0/1-5
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown

%LINK-S-CHANGED: Interface FastEthernet0/1, changed state to down

%LINK-S-CHANGED: Interface FastEthernet0/2, changed state to down

%LINK-S-CHANGED: Interface FastEthernet0/3, changed state to down

%LINK-S-CHANGED: Interface FastEthernet0/4, changed state to down

%LINK-S-CHANGED: Interface FastEthernet0/5, changed state to down
S1(config-if-range)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Ctrl+F6 to exit CLI focus

Copy

Paste

#### **S2**

```
S2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface range fa0/1-5
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown

%LINK-S-CHANGED: Interface FastEthernet0/2, changed state to down

%LINK-S-CHANGED: Interface FastEthernet0/3, changed state to down

%LINK-S-CHANGED: Interface FastEthernet0/4, changed state to down

%LINK-S-CHANGED: Interface FastEthernet0/5, changed state to down
S2(config-if-range)#
%LINK-S-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-S-UPDOWN: Line protocol on Interface Vlan99, changed state to up

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

Ctrl+F6 to exit CLI focus

Copy

Paste

#### **S3**

```

S3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#interface range fa0/1-5
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to down
S3(config-if-range)#
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S3(config-if-range)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console

```

Ctrl+F6 to exit CLI focus

Copy

Paste

**Verificación de enlaces troncales:**—Donde nos muestra que Fa0/1 y Fa0/2 están encendidos. Y funcionan con el estándar IEEE 802.1Q.

**S1**

```

S1#show interface trunk

```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	99
Fa0/2	on	802.1q	trunking	99

```

Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa0/2     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1,10,20,30,99
Fa0/2     1,10,20,30,99

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1,10,20,30,99
Fa0/2     1,10,20,30,99

```

Ctrl+F6 to exit CLI focus

Copy

Paste

**Paso 7: Verificar que los switches se pueden comunicar**

```
Sl#ping 172.17.99.12

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.12, timeout is 2 seconds:
...!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms

Sl#ping 172.17.99.13

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.13, timeout is 2 seconds:
...!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms

Sl#
```

Ctrl+F6 to exit CLI focus

Copy Paste

### **Paso 8: Hacer ping a varios hosts desde la pc2**

PC1

Physical Config **Desktop** Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>l72.17.10.21
Invalid Command.

C:\>ping 172.17.10.21

Pinging 172.17.10.21 with 32 bytes of data:

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

Ping statistics for 172.17.10.21:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.17.10.12

Pinging 172.17.10.12 with 32 bytes of data:

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

Ping statistics for 172.17.10.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Debido a que estos hosts se encuentran en diferentes subredes y diferentes VLAN, no pueden comunicarse sin un dispositivo de Capa 3 que sirva de ruta entre las subredes separadas.

```

C:\>ping 172.17.10.25

Pinging 172.17.10.25 with 32 bytes of data:

Reply from 172.17.10.25: bytes=32 time<1ms TTL=128
Reply from 172.17.10.25: bytes=32 time<1ms TTL=128
Reply from 172.17.10.25: bytes=32 time=1ms TTL=128
Reply from 172.17.10.25: bytes=32 time<1ms TTL=128

Ping statistics for 172.17.10.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>

```

### **Paso 9: Ubicar la PC1 en la misma VLAN que la PC2**

```

User Access Verification

Password:
Password:

S2>enable
Password:
S2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface fastEthernet 0/11
S2(config-if)#switchport access vlan 20
S2(config-if)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#

```

Ctrl+F6 to exit CLI focus

Copy

Paste

El puerto conectado a la PC2 (S2 Fa0/18) estaba asignado a la VLAN 20, y el puerto conectado a la PC1 (S2 Fa0/11) estaba asignado a la VLAN 10. Reasignamos el puerto S2 Fa0/11 de la PC1 VLAN 20 en la que forma parte de la PC2, esto a través de la siguiente configuración:

S2# configure terminal

Enter configuration commands, one per line. Finalice con CNTL/Z.

S2(config) #interface fasthernet 0/11

S2(config-if) #switchport access vlan 20

S2(config-if) #end

**Ping desde el host PC2 al host PC1**



```

C:\>ping 172.17.10.21

Pinging 172.17.10.21 with 32 bytes of data:

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

Ping statistics for 172.17.10.21:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

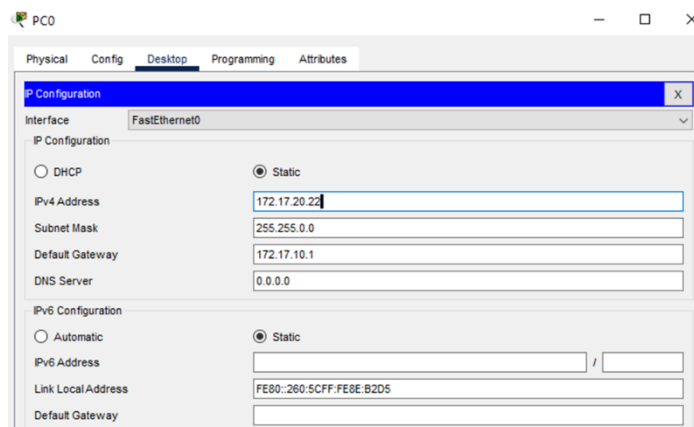
C:\>

```

- No es posible su conexión por que se encuentran en subredes distintas a pesar de estar en la VLAN.

### **Paso 10: Cambiar la dirección IP y la red en PC1**

Asigne 172.17.20.22 como dirección IP de PC1. La máscara de subred y la gateway predeterminada pueden seguir siendo las mismas. Una vez más, haga ping desde el host PC2 al host PC1 utilizando la dirección IP recién asignada.



```

C:\>ping 172.17.10.22

Pinging 172.17.10.22 with 32 bytes of data:

Reply from 172.17.10.22: bytes=32 time<1ms TTL=128
Reply from 172.17.10.22: bytes=32 time=14ms TTL=128
Reply from 172.17.10.22: bytes=32 time=13ms TTL=128
Reply from 172.17.10.22: bytes=32 time=13ms TTL=128

Ping statistics for 172.17.10.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 10ms

C:\>

```

### **5: switch config.txt**



## Tabla de Términos

NOMBRE DEL COMANDO, CONFIGURACIÓN O PROTOCOLO	DEFINICIÓN
VLAN	Son redes de área local virtuales, pueden considerarse como dominios de difusión lógica, ésta divide los grupos de usuarios de la red de una red física real en segmentos de redes lógicas. (IBM, 2021)
CABLE COOPER STRAIGHT-TROUGH	Se utiliza en las redes de área local para conectar un ordenador a un concentrador de red, como un router. El cable de conexión directa hace coincidir las clavijas de los cables. Ambos extremos utilizan el estándar de cableado T568A o bien el estándar de cableado T568B. (Tugurium, (s.f).)
CABLE COOPER CROSS OVER	Se utiliza para las conexiones de Hub con Hub, de un ordenador a otro, de Switch a Switch, o entre el equipo de la misma capa de acuerdo con el modelo OSI. (CCNA, (s.f).)
VLAN BRIEF	Muestra todas las listas de todas las VLAN configuradas. (CCNA, (s.f).)
SWITCHPORT ACCESS	El comando es optativo, pero se aconseja como práctica recomendada de seguridad. Con este comando, la interfaz cambia al modo de acceso permanente. (Sapalomera, (s.f).)
INTERFACE RANGE	Con este comando la interfaz cambia al modo de acceso permanente. (Sapalomera, (s.f).)
SWITCH TRONCAL	El termino switch troncal se refiere a los que se utilizan en el núcleo central (core) de las grandes redes. Es decir, a estos switches están conectados otros de jerarquía inferior, además de servidores, routers WAN, etc. (MS.Gonzalez, 2012)
SUBRED	Subred es la división de una red grande en pequeños grupos de direcciones IP

	<p>contiguas más pequeños. Si una red estuviera formada por 200 direcciones IP y quisiéramos agrupar 50 de ellas en un segmento independiente, podríamos crear una subred para esas 50 IPs</p> <p>(Harold, 2022)</p>
<b>HOSTNAME</b>	<p>El hostname es un nombre único para un ordenador o conexión de red en una red. Los nombres de host son nombres o cadenas de caracteres específicos que hacen referencia a un host y lo hacen utilizable para la red y las personas.</p> <p>(Ryte Wiki, 2021)</p>
<b>SWITCHPORT MODE TRUNK</b>	<p>Coloca la interfaz en modo de enlace troncal permanente y negocia para convertir el enlace en un enlace troncal. La interfaz se convierte en una interfaz de enlace troncal.</p> <p>(Sapalomera, (s.f).)</p>
<b>ENABLE PASSWORD</b>	<p>Activa una contraseña (sin encriptar) para acceder al modo privilegiado.</p> <p>(CISCO,2017)</p>
<b>ENABLE SECRET</b>	<p>Proporciona mayor seguridad al almacenar la contraseña enable secret usando una función criptográfica no reversible. La capa adicional de encriptación de seguridad resulta útil en entornos donde la contraseña cruza la red.</p> <p>(Anónimo, 2022)</p>
<b>NO SHUTDOWN</b>	<p>Este es el comando que habilita una interfaz.</p> <p>(CISCO. (s.f).)</p>
<b>SHUTDOWN</b>	<p>Es decir, para apagar el ordenador. Se trata de un parámetro que permitirá reiniciar o apagar el ordenador en el momento que queramos.</p> <p>(Editorial nobbot, 2020)</p>
<b>COPY RUNNING-CONFIG STARTUP-CONFIG</b>	<p>Sirve para guardar la configuración del router recién creada</p> <p>(anónimo, 2017)</p>
<b>TELNET</b>	<p>Telnet es un protocolo de capa de aplicaciones utilizado en Internet o en redes de área local (LAN) para proporcionar una instalación de comunicación bidireccional interactiva orientada al texto mediante una conexión de terminal virtual.</p> <p>(CISCO, 2017)</p>

<b>FAST ETHERNET</b>	<p>Conjunto de estándares de red para velocidades de transferencia de datos que excede la velocidad Ethernet original de 10 megabits.</p> <p>(Anonimo, 2020)</p>
<b>CONFIGURACION IP</b>	<p>La configuración de una dirección IP estática es una función de red avanzada, y se necesita un conocimiento básico y fundamental de TCP/IP. Se usa para los dispositivos fuera del rango de su grupo DHCP, que en la mayoría de las redes domésticas es su router.</p> <p>(TRENDnet. (s.f))</p>
<b>FA0/1</b>	<p>Es un parámetro en el que 0 es el número de modulo y 1 el número de puerto</p> <p>(Cisco, 28)</p>
<b>FA0/6</b>	<p>Es un parámetro en el que 0 es el número de modulo y 6 el número de puerto</p> <p>(Cisco, 28)</p>
<b>FA0/11</b>	<p>Es un parámetro en el que 0 es el número de modulo y 11 el número de puerto</p> <p>(Cisco, 28)</p>
<b>FA0/18</b>	<p>Es un parámetro en el que 0 es el número de modulo y 18 el número de puerto</p> <p>(Cisco, 28)</p>
<b>ENLACE TRONCAL</b>	<p>Es un enlace punto a punto entre dos dispositivos de red que lleva más de una VLAN. El enlace troncal de VLAN amplia las VLAN a través de todas las redes.</p> <p>(Paloma, 2018)</p>
<b>PUERTOS DE ACCESO</b>	<p>Se utiliza para conectar dispositivos como ordenadores de escritorio, portátiles, impresoras, etc. que solo se encuentran disponibles en el enlace de acceso.</p> <p>(John, 2022)</p>
<b>SHOW VLAN ID</b>	<p>Este comando muestra la lista de todas las VLAN configuradas</p> <p>(Walton,2020)</p>
<b>SSH</b>	<p>Es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros</p>

	<p>protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.</p> <p>(giret. (s.f).)</p>
<b>SNMP</b>	<p>El Protocolo Simple de Administración de Redes es un protocolo de capa de aplicación definido por la junta de arquitectura de Internet (IAB) en RFC1157 para intercambiar información de administración entre dispositivos de red.</p> <p>(OpManager, (s.f).)</p>
<b>HTTP</b>	<p>De sus siglas en inglés “Hypertext Transfer Protocol”, es el nombre de un protocolo el cual nos permite realizar una petición de datos y recursos.</p> <p>(Mdn web docs, (s.f).)</p>
<b>SWITCHPORT TRUNK NATIVE</b>	<p>Este comando se utiliza para añadir o borrar VLANs de un enlace troncal.</p> <p>(Cisco, 2012)</p>
<b>VLAN ISL</b>	<p>Este protocolo encapsula cada trama añadiendo otra cabecera de 26 bytes y un nuevo CRC de 4 bytes al final, Se encapsulan y etiquetan todas las tramas.</p> <p>(Anónimo, 2018)</p>
<b>TRAFICO ETIQUETADO</b>	<p>Son un método para identificar el tráfico de red del ordenador y canalizar el tráfico hacia el destino correcto. Redes de área local no necesitan etiquetas, pero VLAN - Virtual Local Área Networks - cambian con frecuencia sus segmentos de arquitectura y de red. Las direcciones en las redes no son consistentes con el tiempo, pero el tráfico etiquetado permite a los paquetes de datos para encontrar a su destinatario correcto.</p> <p>(Anonimo,2022)</p>
<b>TRAFICO SIN ETIQUETAR</b>	<p>Cuando un puerto de enlace troncal de un switch Cisco recibe tramas sin etiquetar, envía esas tramas a la VLAN nativa. Si no hay dispositivos asociados a la VLAN nativa (lo que no es poco usual) y no existen otros puertos de enlace troncal (lo que no es poco usual), se descarta la trama.</p> <p>(Pérez, 2017)</p>

<b>IEEE 802.1 Q</b>	802.1Q es encapsulación que se utilizan para transportar datos de varias VLAN a través de links troncales. (Cisco, 2022)
---------------------	---

## Conclusion

En esta red se tiene formado una **topología de árbol**, ya que cuentas con switches de acceso y un switch troncal, esto con la finalidad de que el switch troncal sea el principal host de comunicación en las dos redes plasmadas.

El switch troncal es importante, ya que este logra controlar los broadcasts (es la difusión masiva de información o paquete de datos) de la red, para que este transmita el trafico de las VLANS de las redes.

Los switches de acceso, que irán conectados a las PCs su cable será Cooper Straight-Through y el switch troncal ira conectado a los switches de ambas redes por medio del cable Cooper Cross-Over.

Se debe de tomar en cuenta que cuando se termina de preparar la red, se necesita implementar la deshabilitación de puertos, por medio del comando `interface range fa0/1-24` este desactivara los puertos de fastEthernet y el comando `interface range gi0/1-2` desactivara los puestos de Gigabit Ethernet. En este caso solo se habilitarán solo los puertos que se usaran en los switches que en este caso son los fa0/1 y los fa0/2 y será por medio del comando `interface range`, el cual permitirá la activación de los puertos y el comando `switchport mode access` que este influye en que la interfaz la cambia al modo de acceso permanente.

La configuración de las PCs irá conforme a la tabla que esta dentro de la práctica, donde podemos ver que son de **clase B** ya que están entre el numero 128 al 191, esto se clasifica por su primer octeto.

Para poder crear las VLAN se implementó el comando `vlan-id` que sirve para mostrar información sobre el número de ID de la VLAN identificado y para verificar que las VLAN son creadas, para ello se implementó el comando `show vlan brief` este comando sirve para mostrar el nombre de la VLAN, el estado y sus puertos una VLAN por línea. También para poder generar la conexión se realiza la asignación de los puertos, donde estos irán asignados a las VLAN en modo de configuración de interfaces y para ello se necesita el comando `witchport access vlan` que sirve para establecer el puerto en modo de acceso y por ultimo necesitamos el comando `copy running-config startup-config` ya que este es importante para guardar las configuraciones que se han realizado dentro del switch.

Y para verificar que los puertos se han agregado de manera correcta, se implementara el código `show vlan id` para poder verificar que se han creado de manera correcta, ya que este comando te ayuda a visualizar las VLAN que se han creado. El comando `interface range fa0/1-5` configura todas las interfaces para poder usar `switchport mode trunk`.

Trunk native vlan 99 va a funcionar como la VLAN nativa la cual se debe habilitar, mediante el comando `no shutdown`, ya que la VLAN 99 se encuentra configurada como VLAN de administración y cualquier puerto asignado a esta VLAN se considera puerto de administración.

Al utilizar el comando `show interface trunk` en el switch se puede verificar que cada uno de los enlaces troncales han sido configurados y así poder hacer uso del comando `ping`, el cual funciona para probar la comunicación con el switch, y así poder mandar paquetes de información a las diferentes direcciones especificadas, y a su vez estos regresen.

## References

- Alegre, J. M. H. (s. f.). *switchport trunk native vlan* —. El BLOG de Juan Miguel Huertas Alegre. <https://juanmhalegre.wordpress.com/tag/switchport-trunk-native-vlan/>
- Como configurar una dirección IP estática. (s. f.). <https://www.trendnet.com/langsp/press/resource-library/how-to-set-static-ip-address>
- Configurar el acceso de Telnet o SSH al dispositivo con VRF. (2022, 12 marzo). Cisco. [https://www.cisco.com/c/es\\_mx/support/docs/ip/telnet/200718-Configure-Telnet-SSH-Access-to-Device-wi.html](https://www.cisco.com/c/es_mx/support/docs/ip/telnet/200718-Configure-Telnet-SSH-Access-to-Device-wi.html)
- Descripción general de diferentes tipos de puertos en los switches Ethernet |Comunidad FS. (s. f.). Knowledge. <https://community.fs.com/es/blog/ethernet-switch-port-types-overview.html>
- Editorial Nobbot. (2020, 14 octubre). *Comando shutdown: qué es y cómo ejecutar en Windows, MAC y Linux*. Nobbot. <https://www.nobbot.com/tecnologia/guia-y-trucos/comando-shutdown-que-es-windows-mac-linux/>
- *Enable secret - Cisco Secure*. Cisco Certified Expert. <https://www.ccexpert.us/cisco-secure/enable-secret.html>

- Esquivel, P. (2019). *Redes VLAN en un entorno conmutado múltiple*. sapalomera. <https://www.sapalomera.cat/moodlecf/RS/2/course/module3/3.1.2.1/3.1.2.1.html#:~:text=Un%20enlace%20troncal%20es%20un,Ethernet%20y%2010%2DGigabit%20Ethernet>.
- *Generalidades del protocolo HTTP - HTTP | MDN*. (2022, 3 octubre). <https://developer.mozilla.org/es/docs/Web/HTTP/Overview>
- *Información básica / Preparación*. (2018). Cisco. [http://www.utez.edu.mx/curriculas/ccna2\\_ES/pdf/knet-1076521143041/CCNA2\\_lab\\_3\\_2\\_9\\_es.pdf](http://www.utez.edu.mx/curriculas/ccna2_ES/pdf/knet-1076521143041/CCNA2_lab_3_2_9_es.pdf)
- *ISL (Inter Switch Link). | PAR05.- Configuración de redes virtuales*. (s. f.). [https://ikastaroak.birt.eus/edu/argitalpen/backupa/20200331/1920k/es/ASIR/PAR/PAR05/es\\_ASIR\\_PAR05\\_Contenidos/website\\_42\\_isl\\_inter\\_switch\\_link.html](https://ikastaroak.birt.eus/edu/argitalpen/backupa/20200331/1920k/es/ASIR/PAR/PAR05/es_ASIR_PAR05_Contenidos/website_42_isl_inter_switch_link.html)
- *¿Qué es la etiqueta de tráfico? / Seabrookewindows.com*. (s. f.). <https://www.seabrookewindows.com/N0PjALGW9/>
- *¿Qué es FastEthernet? QueSignificado.org*. <https://quesignificado.org/que-es-fastethernet/>
- *¿Qué es el Hostname? - Ryte Digital Marketing Wiki*. (s. f.). <https://es.ryte.com/wiki/Hostname>
- *Redes de área local virtuales (VLAN)*. (s. f.). <https://www.ibm.com/docs/es/aix/7.1?topic=cards-virtual-local-area-networks>
- *Redes VLAN en un entorno conmutado múltiple*. (s. f.). sapalomera. Recuperado 23 de noviembre de 2022, de <https://www.sapalomera.cat/moodlecf/RS/2/course/module3/3.1.2.4/3.1.2.4.html>
- (s. f.). *¿Qué es SNMP? | Protocolo SNMP – Monitorización – Puerto SNMP - ManageEngine OpManager*. <https://www.manageengine.com/es/network-monitoring/what-is-snmp.html>
- Madrid, J. E. L. P. /. (s. f.). *straight through cable - GTI - Glosario Terminología Informática*. <http://www.tugurium.com/gti/termino.php?Tr=straight+through+cable>
- Walton, A. (2020, 10 junio). ▷ *Configuración de VLAN [Comandos]*». CCNA desde Cero. <https://ccnadesdecero.es/configuracion-vlan/>