

OBJETIVOS DE APRENDIZAJE:

- Realizar tareas de configuración básicas en un switch.
- Crear las VLAN.
- Asignar puertos de switch a una VLAN.
- Agregar, mover y cambiar puertos.
- Verificar la configuración de la VLAN.
- Habilitar el enlace troncal en conexiones entre switches.
- Verificar la configuración de enlace troncal.
- Guardar la configuración de la VLAN.

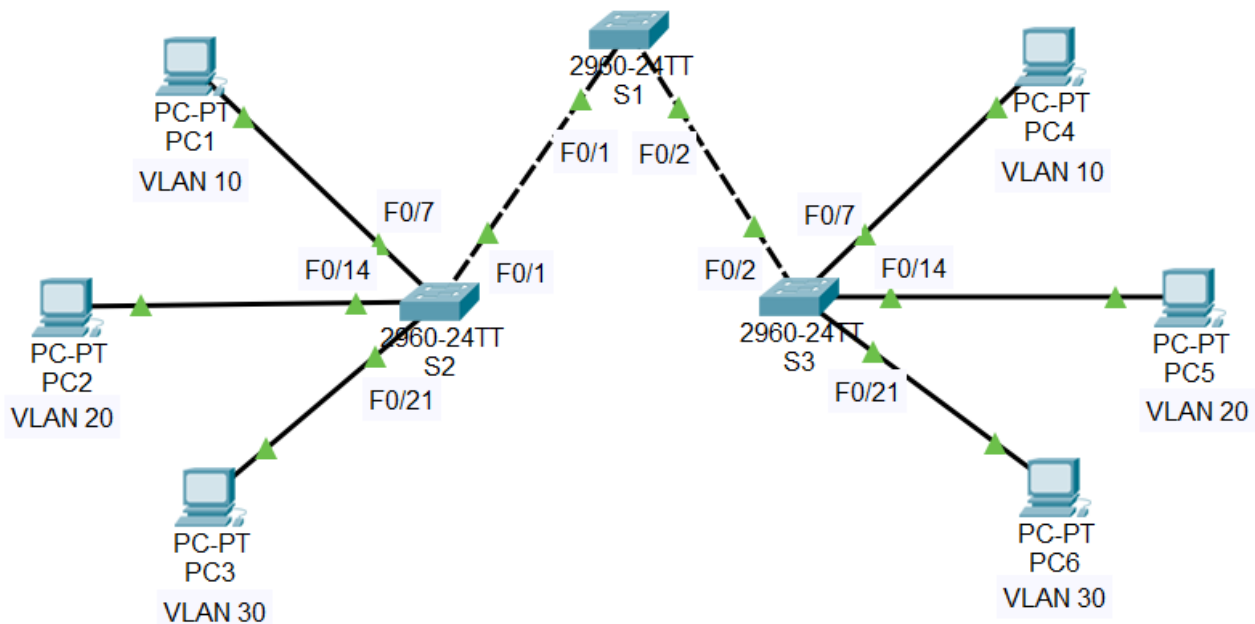
DIAGRAMA DE TOPOLOGÍA:

Figura 1 Diagrama de Topología

TABLA DE DIRECCIONAMIENTO:

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway Predeterminado
S1	VLAN 150	192.168.150.11	255.255.255.0	NA
S2	VLAN 150	192.168.150.12	255.255.255.0	NA
S3	VLAN 150	192.168.150.13	255.255.255.0	NA
PC1	NIC	192.168.10.21	255.255.255.0	192.168.10.1
PC2	NIC	192.168.20.22	255.255.255.0	192.168.20.1
PC3	NIC	192.168.30.23	255.255.255.0	192.168.30.1
PC4	NIC	192.168.10.24	255.255.255.0	192.168.10.1
PC5	NIC	192.168.20.25	255.255.255.0	192.168.20.1
PC6	NIC	192.168.30.26	255.255.255.0	192.168.30.1

ASIGNACIONES DE PUERTOS (Switches 2 y 3):

Puertos	Asignaciones	Dirección IP
Fa0/1 a Fa0/5	VLAN 150 – Administrativa&Nativa	192.168.150.0/24
Fa0/6 a Fa0/12	VLAN 10 – Profesores	192.168.10.0/24
Fa0/13 a Fa0/19	VLAN 20 – Estudiantes	192.168.20.0/24
Fa0/20 a Fa0/24	VLAN 30 – Invitados	192.168.30.0/24

TAREA 1: Realizar configuraciones básicas del switch

Realice la configuración básica en los tres switches.

- Configure los nombres de host del switch.
- Deshabilite la búsqueda del DNS así:
Switch(config) # **No ip domain lookup**
- Configure una contraseña del modo EXEC privilegiado encriptado en **clase**.
- Configure la contraseña **redes** para las conexiones de consola.
- Configure la contraseña **redes** para las conexiones vty.

TAREA 2: Configurar y activar las interfaces Ethernet

Desde la pestaña **Desktop**, seleccione **IP Configuration** para configurar las interfaces Ethernet de las seis PC con las direcciones IP y los gateways predeterminados que se indican en la tabla de direccionamiento.

TAREA 3: Configurar las VLAN en el switch**Paso 1. Cree las VLAN en el switch S1.**

Utilice el comando **vlan id de la VLAN** en modo de configuración global para agregar las VLAN al switch S1. Hay que configurar cuatro VLAN para esta actividad. Después de crear la VLAN, se encontrará en el modo de configuración de vlan, donde puede asignar un nombre a la vlan con el comando **vlan name**.

```
S1(config)#vlan 150
S1(config-vlan)#name Administrativa&Nativa
S1(config-vlan)#exit
S1(config)#vlan 10
S1(config-vlan)#name Profesores
```

```
S1 (config-vlan) #exit
S1 (config) #vlan 20
S1 (config-vlan) #name Estudiantes
S1 (config-vlan) #exit
S1 (config) #vlan 30
S1 (config-vlan) #name Invitados
S1 (config-vlan) #exit
```

Paso 2. Verifique que las VLAN se creen en el S1.

Utilice el Comando **show vlan brief** para verificar que las VLAN se crearon correctamente.

```
S1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, 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, Gi0/1 Gi0/2
10	Profesores	active	
20	Estudiantes	active	
30	Invitados	active	
150	Administrativa&Native	active	

Paso 3. Configure y asigne un nombre a las VLAN en los switches S2 y S3.

Cree y asigne un nombre a las VLAN 10, 20, 30 y 150 en S2 y S3 con los comandos del Paso 1. Verifique la configuración correcta con el comando **show vlan brief**.

¿Qué puertos están asignados actualmente a las cuatro VLAN que creó?

Paso 4. Asigne los puertos del switch a las VLAN en S2 y S3.

Consulte la tabla para la asignación de puertos que se encuentra en la página 1. Los puertos se asignan a las VLAN en modo de configuración de interfaces con el comando **switchport access vlan id de la VLAN**. Es posible utilizar el comando **interface range**, pero dependiendo la versión de Packet Tracer puede que no sea admitido.

```
S2 (config) #interface fastEthernet0/7
S2 (config-if) #switchport mode access
S2 (config-if) #switchport access vlan 10
S2 (config-if) #interface fastEthernet0/14
S2 (config-if) #switchport mode access
S2 (config-if) #switchport access vlan 20
S2 (config-if) #interface fastEthernet0/21
S2 (config-if) #switchport mode access
S2 (config-if) #switchport access vlan 30
S2 (config-if) #end

S2#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
```

Nota: Por el momento, las VLAN de acceso se marcan como incorrectas. Usted lo corrige más adelante en la actividad.

Repita los mismos comandos en S3.

Paso 5. Determine qué puertos se agregaron.

Utilice el comando **show vlan id número de VLAN** en S2 para ver qué puertos están asignados a la VLAN 10.

¿Qué puertos están asignados a la VLAN 10?

Nota: El comando **show vlan name nombre de la VLAN** muestra el mismo resultado.

También puede ver la información sobre la asignación de VLAN con el comando **show interfaces switchport**.

Paso 6. Asigne la VLAN de administración.

Una VLAN administrativa es cualquier VLAN que configure para acceder a las habilidades administrativas de un switch. VLAN 1 sirve como la VLAN administrativa si no se definió de forma específica otra VLAN. Se le asigna a la VLAN administrativa una dirección IP y una máscara de subred. Se puede administrar un switch mediante HTTP, Telnet, SSH o SNMP. Porque la configuración de fábrica de un switch Cisco tiene a VLAN 1 como la VLAN predeterminada, VLAN 1 es una mala elección para ser la VLAN administrativa. No es necesario un usuario arbitrario que se conecta a un switch para ser la VLAN predeterminada. Recuerde que configuró la VLAN de administración como VLAN 150 anteriormente en este laboratorio.

Desde el modo de configuración de interfaz, utilice el comando **ip address** para asignar la dirección IP administrativa a los switches.

```
S1(config)#interface vlan 150
S1(config-if)#ip address 192.168.150.11 255.255.255.0
S1(config-if)#no shutdown

S2(config)#interface vlan 150
S2(config-if)#ip address 192.168.150.12 255.255.255.0
S2(config-if)#no shutdown

S3(config)#interface vlan 150
S3(config-if)#ip address 192.168.150.13 255.255.255.0
S3(config-if)#no shutdown
```

La asignación de una dirección administrativa permite la comunicación IP entre los switches, y, además, permite que cualquier host conectado a un puerto asignado a la VLAN 150 se conecte a los switches. Ya que la VLAN 150 se configura como la VLAN administrativa, los puertos que se asignen a esta VLAN se consideran puertos administrativos y se deben asegurar para controlar qué dispositivos se pueden conectar a estos puertos.

Paso 7. Configure la VLAN troncal y nativa para los puertos troncales de todos los switches.

Los enlaces troncales son conexiones entre los switches que permiten el intercambio de información para todas las VLAN. De forma predeterminada, un puerto de enlace troncal pertenece a todas las VLAN, contrario a un puerto de acceso, que sólo puede pertenecer a una sola VLAN. Si el switch soporta la encapsulación de VLAN ISL y 802.1Q, los enlaces troncales deben especificar qué método se utilizará. Dado que el switch 2960 sólo admite los enlaces troncales 802.1Q, no se especificará en esta actividad.

Una VLAN nativa está asignada a un puerto troncal 802.1Q. En la topología, la VLAN nativa es la VLAN 150. Un puerto de enlace troncal 802.1Q admite el tráfico que llega de muchas VLAN (tráfico etiquetado) como también el tráfico que no llega de una VLAN (tráfico no etiquetado). El puerto troncal 802.1Q coloca el tráfico no etiquetado en la VLAN nativa. El tráfico no etiquetado lo genera una computadora conectada a un puerto de switch que se configura con la VLAN nativa. Una de las especificaciones IEEE 802.1Q para las VLAN nativas es mantener la compatibilidad retrospectiva con el tráfico no etiquetado común para las situaciones de herencia de LAN. Para fines de esta actividad, una VLAN nativa sirve como un identificador común en los extremos opuestos de un enlace troncal. Es mejor utilizar una VLAN, que no sea la VLAN 1, como VLAN nativa.

```
S1(config)#interface fa0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 150
S1(config-if)#interface fa0/2
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 150
S1(config-if)#end
```

```
S2(config)#interface fa0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 150
S2(config-if)#end
```

```
S3(config)#interface fa0/2
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 150
S3(config-if)#end
```

Verifique que los enlaces troncales se configuren con el comando `show interface trunk`.

```
S1#show interface trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	150
Fa0/2	on	802.1q	trunking	150

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

Port	Vlans allowed and active in management domain
Fa0/1	1,10,20,30,150,1002,1003,1004,1005
Fa0/2	1,10,20,30,150,1002,1003,1004,1005

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	1,10,20,30,150,1002,1003,1004,1005
Fa0/2	1,10,20,30,150,1002,1003,1004,1005

Paso 8. Verifique que los switches se puedan comunicar.

Desde el S1, haga ping en la dirección de administración tanto en S2 como en S3.

```
S1#ping 192.168.150.12
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.150.12, timeout is 2 seconds:

..!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms

```
S1#ping 192.168.150.13
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.150.13, timeout is 2 seconds:
```

```
..!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Paso 9. Haga ping en varios hosts desde la PC2.

Haga ping desde la PC2 host hasta la PC1 host (192.168.10.21). ¿El intento de ping tuvo éxito?

Haga ping desde la PC2 host a la dirección IP de VLAN 150 del switch 192.168.150.12. ¿El intento de ping tuvo éxito?

Debido a que estos hosts se encuentran en subredes y en VLAN diferentes, no pueden comunicarse sin un dispositivo de capa 3 que realice el enrutamiento entre las subredes independientes.

Haga ping del host PC2 al host PC5 (192.168.20.25). ¿El intento de ping tuvo éxito?

Debido a que la PC2 se encuentra en la misma VLAN y en la misma subred que la PC5, el ping es exitoso.

Paso 10. Traslade la PC1 a la misma VLAN que la PC2.

El puerto conectado a PC2 (S2 Fa0/14) se asigna a la VLAN 20, y el puerto conectado a la PC1 (S2 Fa0/7) se asigna a la VLAN 10. Reasigne el puerto S2 Fa0/7 a la VLAN 20. No es necesario eliminar primero un puerto de una VLAN para cambiar su pertenencia de VLAN. Después de reasignar un puerto a una VLAN nueva, dicho puerto se elimina de forma automática de su VLAN anterior.

```
S2#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
S2(config)#interface fastethernet 0/7
```

```
S2(config-if)#switchport access vlan 20
```

```
S2(config-if)#end
```

Haga ping de la PC2 host a la PC1 host. ¿El intento de ping tuvo éxito?

Paso 11. Cambie la dirección IP y la red de la PC1.

Cambie la dirección IP de la PC1 a 192.168.20.21. La máscara de subred y el gateway predeterminado pueden permanecer iguales. Una vez más, haga ping desde la PC2 host hasta la PC1 host, utilizando la dirección IP que se acaba de asignar.

¿El intento de ping tuvo éxito?

¿Por qué tuvo éxito este intento?

PRÁCTICA FINALIZADA. GUARDE LA SIMULACIÓN.

NOTA: Práctica basada en CCNA EXPLORATION, 2010