Actividad de Packet Tracer 3.5.1: Configuración básica de una VLAN

Diagrama de topología

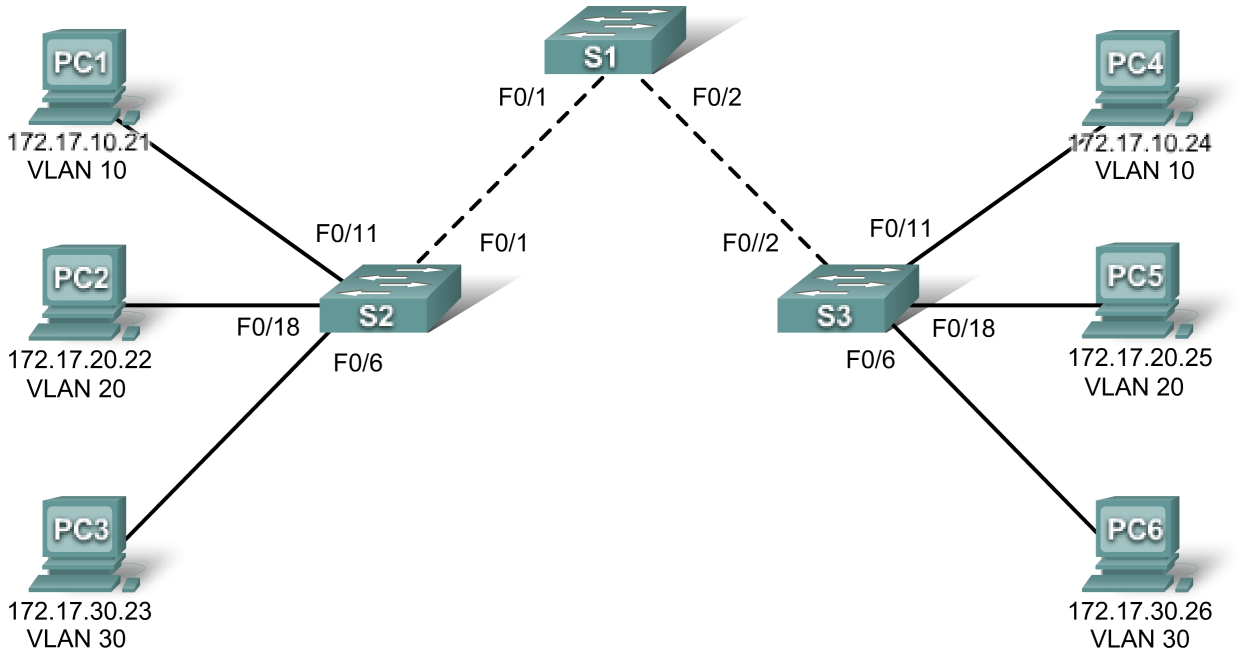

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de enlace) predeterminado
S1	**VLAN 99**	172.17.99.11	255.255.255.0	N/C
S2	**VLAN 99**	172.17.99.12	255.255.255.0	N/C
S3	**VLAN 99**	172.17.99.13	255.255.255.0	N/C
PC1	**NIC**	172.17.10.21	255.255.255.0	172.17.10.1
PC2	**NIC**	172.17.20.22	255.255.255.0	172.17.20.1
PC3	**NIC**	172.17.30.23	255.255.255.0	172.17.30.1
PC4	**NIC**	172.17.10.24	255.255.255.0	172.17.10.1
PC5	**NIC**	172.17.20.25	255.255.255.0	172.17.20.1
PC6	**NIC**	172.17.30.26	255.255.255.0	172.17.30.1

Asignaciones de puertos (switches 2 y 3)

Puertos	Asignaciones	Red
Fa0/1 – 0/5	VLAN 99 – Management&Native	172.17.99.0/24
Fa0/6 – 0/10	VLAN 30 – Guest(Default)	172.17.30.0/24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0/24
Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0/24

Objetivos de aprendizaje

- Realizar las 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 VLAN.
- Habilitar los enlaces troncales en las conexiones entre los switches.
- Verificar la configuración del enlace troncal.
- Guardar la configuración de VLAN.

Tarea 1: Realizar configuraciones de switches básicas

Realice la configuración básica en los tres switches.

- Configure los nombres de host del switch.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de **class** en el Modo EXEC privilegiado encriptado.
- Configure una contraseña de **cisco** para las conexiones de consola.
- Configure una contraseña de **cisco** para las conexiones vty.

Su porcentaje de finalización debe ser del 25%. Si no es así, efectúe la resolución de problemas para detectar cualquier error.

Tarea 2: Configurar y activar interfaces Ethernet

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

Nota: Por el momento, la dirección IP para la PC1 se califica como incorrecta. Cambiará la dirección IP de PC1 más adelante.

Su porcentaje de finalización debe ser del 51%. Si no es así, efectúe la resolución de problemas para detectar cualquier error.

Tarea 3: Configurar las VLAN en el switch

Paso 1: Cree VLAN en el switch S1.

Use el comando **vlan** *id de la VLAN* en el modo de configuración global para agregar VLAN al switch S1. Hay cuatro VLAN para configurar en esta actividad. Después de crear la VLAN, estará en modo de configuración vlan, que permite asignar un nombre a la vlan mediante el comando **vlan** *nombre*.

```
S1(config)#vlan 99
S1(config-vlan)#name Management&Native
S1(config-vlan)#exit
S1(config)#vlan 10
S1(config-vlan)#name Faculty/Staff
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name Students
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name Guest(Default)
S1(config-vlan)#exit
```

Paso 2: Verifique que las VLAN se hayan creado en S1.

Use el comando **show vlan brief** para verificar que las VLAN se hayan creado.

```
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   Faculty/Staff                     active
20   Students                          active
30   Guest(Default)                    active
99   Management&Native                 active
```

Paso 3: Configure y asignar nombres a las VLAN en los switches S2 y S3.

Cree y asigne nombres a las VLAN 10, 20, 30 y 99 en S2 y S3 usando los comandos del paso 1. Verifique la configuración correcta mediante el comando **show vlan brief**.

¿Qué puertos están actualmente asignados a las cuatro VLAN creadas?

_____

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

Consulte la tabla de asignación de puertos. Los puertos se asignan a las VLAN en el modo de configuración de interfaz, mediante el comando **switchport access vlan** *id de la VLAN*. Packet Tracer sólo calificará la primera interfaz de cada rango (la interfaz a la que está conectado el equipo PC). Normalmente, se usaría el comando **interface range**, pero Packet Tracer no admite este comando.

```
S2(config)#interface fastEthernet0/6
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 30
```



```
S2(config-if)#interface fastEthernet0/11
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#interface fastEthernet0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20
S2(config-if)#end
S2#copy running-config startup-config
Destination filename [startup-config]? [Intro]
Building configuration...
[OK]
```

Nota: Por el momento, la VLAN de acceso Fa0/11 se marca como incorrecta. Esta situación se corregirá más adelante en la actividad.

Repita los mismos comandos en S3.

Paso 5: Determine qué puertos se han agregado.

Use el comando **show vlan id** *número de VLAN* en S2 para ver los puertos que están asignados a VLAN 10.

¿Qué puertos están asignados a VLAN 10? _____

Nota: El comando **show vlan name** *nombre de la VLAN* muestra la misma información.

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

Paso 6: Asigne la VLAN de administración.

Una VLAN de administración es cualquier VLAN configurada para acceder a las capacidades de administración de un switch. VLAN 1 sirve como la VLAN de administración si no definió específicamente otra VLAN. El usuario asigna una dirección IP y una máscara de subred a la VLAN de administración. Un switch puede administrarse a través de HTTP, Telnet, SSH o SNMP. Dado que la configuración de fábrica de un switch Cisco tiene VLAN 1 como VLAN por defecto, VLAN 1 no es una elección adecuada para la VLAN de administración. No sería deseable que un usuario que se conecte a un switch acceda por defecto a la VLAN de administración. Recuerde que anteriormente en esta práctica de laboratorio configuró la VLAN de administración como VLAN 99.

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

```
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown

S2(config)#interface vlan 99
S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#no shutdown

S3(config)#interface vlan 99
S3(config-if)#ip address 172.17.99.13 255.255.255.0
S3(config-if)#no shutdown
```

La asignación de una dirección de administración permite la comunicación IP entre los switches. Además permite que cualquier host conectado a un puerto asignado a VLAN 99 se conecte con los switches. Dado que la VLAN 99 está configurada como la VLAN de administración, los puertos asignados a esta VLAN se consideran puertos de administración y se debe garantizar su seguridad para controlar los dispositivos que pueden conectarse a ellos.

Paso 7: Configure los enlaces troncales y la VLAN nativa para los puertos de enlaces troncales en todos los switches.

Los enlaces troncales son conexiones entre los switches que permiten que los switches intercambien información para todas las VLAN. Por defecto, un puerto de enlace troncal pertenece a todas las VLAN, a diferencia de un puerto de acceso, que sólo puede pertenecer a una única VLAN. Si el switch admite encapsulación de VLAN ISL y 802.1Q, los enlaces troncales deben especificar el método que se usa. Dado que el switch 2960 sólo admite los enlaces troncales 802.1Q, no se explicará en esta actividad.

Una VLAN nativa se asigna a un puerto de enlace troncal 802.1Q. En la topología, la VLAN nativa es la VLAN 99. Un puerto de enlace troncal 802.1Q admite el tráfico proveniente de muchas VLAN (tráfico etiquetado) así como el tráfico que no proviene de una VLAN (tráfico no etiquetado). El puerto de enlace troncal 802.1Q coloca el tráfico no etiquetado en la VLAN nativa. El tráfico no etiquetado lo genera un equipo PC conectado a un puerto del switch configurado 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 que suele verse en a las situaciones de LAN heredadas. Para los fines de esta actividad, una VLAN nativa sirve como un identificador común en los extremos opuestos de un enlace troncal. Una práctica recomendada consiste en usar una VLAN diferente de la VLAN 1 como la VLAN nativa.

```
S1(config)#interface fa0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#interface fa0/2
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#end

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

S3(config)#interface fa0/2
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 99
S3(config-if)#end
```

Verifique que los enlaces troncales se hayan configurado mediante el comando show interface trunk.

```
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       1,10,20,30,99,1002,1003,1004,1005
Fa0/2       1,10,20,30,99,1002,1003,1004,1005

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,30,99,1002,1003,1004,1005
Fa0/2       1,10,20,30,99,1002,1003,1004,1005
```


Paso 8: Verifique que los switches puedan comunicarse.

Desde S1, haga ping a la dirección de administración en S2 y S3.

```
S1#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 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms

S1#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 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Paso 9: Haga ping a varios hosts desde PC2.

Haga ping desde PC2 a PC1 (172.17.10.21). ¿El intento de ping se realizó correctamente? _____

Haga ping desde PC2 host a la dirección IP 172.17.99.12 de la VLAN 99 del switch. ¿El intento de ping se realizó correctamente? _____

Dado que estos hosts están en subredes diferentes y en VLAN diferentes, no pueden comunicarse sin un dispositivo de capa 3 que funcione como ruta entre las diferentes subredes.

Haga ping desde PC2 host a PC5 host. ¿El intento de ping se realizó correctamente? _____

Dado que PC2 está en la misma VLAN y la misma subred que PC5, el ping se realiza correctamente.

Paso 10: Mueva PC1 a la misma VLAN que PC2.

El puerto conectado a PC2 (S2 Fa0/18) está asignado a la VLAN 20, y el puerto conectado a PC1 (S2 Fa0/11) está asignado a la VLAN 10. Reasigne el puerto S2 Fa0/11 a la VLAN 20. No es necesario que primero quite un puerto de una VLAN para cambiar su pertenencia de VLAN. Después de reasignar un puerto a una nueva VLAN, ese puerto se quita automáticamente de su VLAN anterior.

```
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
```

Haga ping desde PC2 host a PC1 host. ¿El intento de ping se realizó correctamente? _____

Paso 11: Cambie la dirección IP y la red en PC1.

Cambie la dirección IP en PC1 a 172.17.20.21. La máscara de subred y el gateway predeterminado pueden permanecer sin cambios. Una vez más, haga ping desde PC2 host a PC1 host, usando la dirección IP recientemente asignada.

¿El intento de ping se realizó correctamente? _____

¿Por qué este intento se realizó correctamente?

_____

_____

Su porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Check Results** para ver qué componentes requeridos aún no se han completado.

