

Práctica de laboratorio 3.5.1: Configuración básica de una VLAN

Diagrama de topología

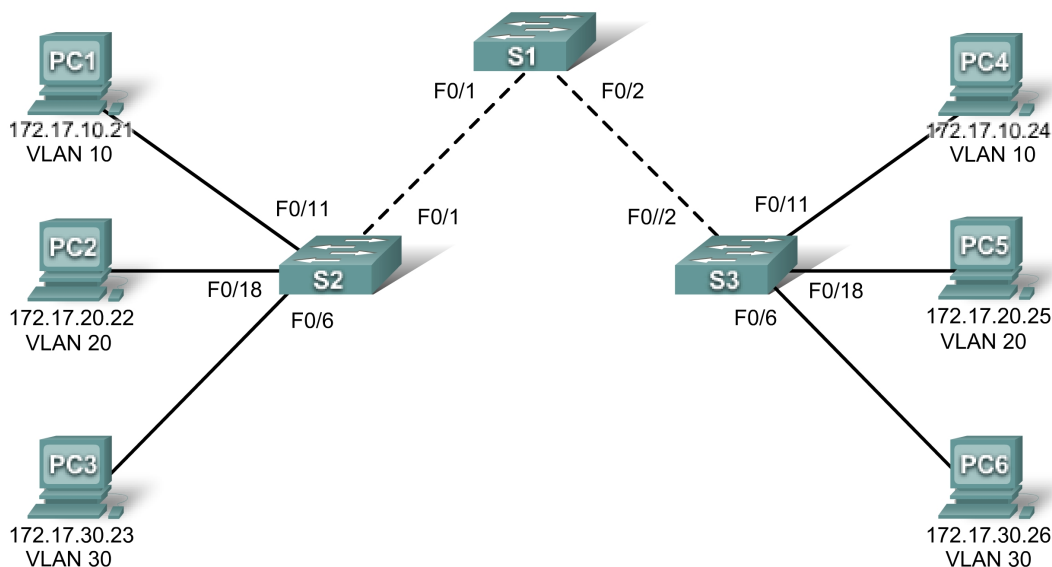


Tabla de direccionamiento

| Dispositivo Nombre de host | Interfaz | Dirección IP | Máscara de subred | Gateway (puerta de salida) 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 iniciales de puertos (Switches 2 y 3)

| Puertos | Asignación | Red |
|---------------|---|-----------------|
| Fa0/1 – 0/5 | Enlaces troncales 802.1q (VLAN 99 nativa) | 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

Al completar esta práctica de laboratorio podrá:

- Cablear una red según el diagrama de topología
- Borrar la configuración inicial y volver a cargar un switch al estado predeterminado
- 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 la VLAN
- Habilitar el enlace troncal en conexiones entre switches
- Verificar la configuración de enlace troncal
- Guardar la configuración de la VLAN

Tarea 1: Preparar la red

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

Puede utilizar cualquier switch actual en su práctica de laboratorio siempre y cuando éste tenga las interfaces necesarias que se muestran en la topología.

Nota: Si utiliza switches 2900 o 2950, los resultados pueden aparecer de manera diferente. Asimismo, ciertos comandos pueden ser diferentes o no encontrarse disponibles.

Paso 2: Borre configuraciones existentes en los switches e inicializar todos los puertos en estado desactivado.

De ser necesario, consulte la Práctica de laboratorio 2.5.1, Apéndice 1, para leer sobre el procedimiento para borrar las configuraciones del switch.

Es una optimización deshabilitar puertos no utilizados en los switches mediante su desactivación. Deshabilite todos los puertos en los switches:

```
Switch#config term
Switch(config)#interface range fa0/1-24
Switch(config-if-range)#shutdown
Switch(config-if-range)#interface range gi0/1-2
Switch(config-if-range)#shutdown
```

Tarea 2: Realizar las configuraciones básicas del switch

Paso 1: Configure los switches de acuerdo con la siguiente guía:

- Configure el nombre de host del switch.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de modo EXEC: **clase**.
- Configure la contraseña **cisco** para las conexiones de consola.
- Configure la contraseña **cisco** para las conexiones de vty.

Paso 2: Vuelva a habilitar los puertos de usuario en S2 y S3.

```

S2(config)#interface range fa0/6, fa0/11, fa0/18
S2(config-if-range)#switchport mode access
S2(config-if-range)#no shutdown

S3(config)#interface range fa0/6, fa0/11, fa0/18
S3(config-if-range)#switchport mode access
S3(config-if-range)#no shutdown

```

Tarea 3: Configurar y activar las interfaces Ethernet**Paso 1: Configure las PC.**

Puede completar esta práctica de laboratorio utilizando sólo dos PC, simplemente modificando las direcciones IP de las dos PC específicas de una prueba que desea llevar a cabo. Por ejemplo: si desea probar la conectividad entre la PC1 y la PC2, configure las direcciones IP para aquellas PC que se refieren a la tabla de direccionamiento al comienzo de la práctica de laboratorio. Alternativamente, puede configurar las seis PC con las direcciones IP y gateways predeterminados.

Tarea 4: 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 añadir una VLAN al switch S1. Hay cuatro VLAN configuradas para esta práctica de laboratorio: VLAN 10 (cuerpo docente/personal); VLAN 20 (estudiantes); VLAN 30 (guest); y VLAN 99 (administración). Después de crear la VLAN, estará en modo de configuración de vlan, donde puede asignar un nombre para la VLAN mediante el comando **name** *nombre de la VLAN*.

```

S1(config)#vlan 10
S1(config-vlan)#name faculty/staff
S1(config-vlan)#vlan 20
S1(config-vlan)#name students
S1(config-vlan)#vlan 30
S1(config-vlan)#name guest
S1(config-vlan)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#end
S1#

```

Paso 2: Verifique que las VLAN estén creadas 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 | active |
| 99 | management | active |

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

Cree y asigne un nombre para las VLAN 10, 20, 30 y 99 en S2 y S3 mediante los comandos del Paso 1. Verifique la configuración correcta mediante el comando **show vlan brief**.

¿Qué puertos se encuentran asignados actualmente a las cuatro VLAN que se han creado?

Ninguno, todos parten con la vlan 1 por defecto y aun estas no son asignadas.

Paso 4: Asigne puertos de 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, utilizando el comando **switchport access vlan id de la VLAN**. Puede asignar cada puerto en forma individual o se puede utilizar el comando **interface range** para simplificar la tarea, como se muestra en este ejemplo. Los comandos se muestran sólo para S3, pero S2 y S3 se deben configurar de manera similar. Guarde la configuración al terminar.

```
S3(config)#interface range fa0/6-10
S3(config-if-range)#switchport access vlan 30
S3(config-if-range)#interface range fa0/11-17
S3(config-if-range)#switchport access vlan 10
S3(config-if-range)#interface range fa0/18-24
S3(config-if-range)#switchport access vlan 20
S3(config-if-range)#end
S3#copy running-config startup-config
Destination filename [startup-config]? [intro]
Building configuration...
[OK]
```

Paso 5: Determine qué puertos se han agregado.

Utilice el comando **show vlan id número de VLAN** en S2 para ver qué puertos se asignan a VLAN 10.

¿Qué puertos están asignados a la VLAN 10?

los puertos [11,17]

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

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

Paso 6: Asigne la VLAN de administración.

Una VLAN de administración es cualquier VLAN que se configura para acceder a las capacidades administrativas de un switch. La VLAN 1 funciona como VLAN de administración si no ha definido específicamente otra VLAN. Se asigna a la VLAN de administración una dirección IP y máscara de subred. Un switch puede administrarse mediante HTTP, Telnet, SSH o SNMP. 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. Usted no desea que un usuario arbitrario que se conecta a un switch acceda de manera predeterminada a la VLAN de administración. Recuerde que anteriormente, en esta misma práctica de laboratorio, configuró la VLAN 99 como VLAN de administración.

Desde el modo de configuración de interfaz, utilice 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 switches y permite también que cualquier host conectado a un puerto asignado a la VLAN 99 se conecte a los switches. Debido a que la VLAN 99 se encuentra configurada como la VLAN de administración, cualquier puerto asignado a esta VLAN se considera puerto de administración y debe contar con seguridad para controlar qué dispositivos pueden conectarse a estos puertos.

Paso 7: Configure 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. De manera predeterminada, un puerto troncal pertenece a todas las VLAN, a diferencia del puerto de acceso que sólo puede pertenecer a una sola VLAN. Si el switch admite tanto el encapsulamiento de VLAN ISL como el de 802.1Q, los enlaces troncales deben especificar qué método utilizan. Debido a que el switch 2960 sólo admite el enlace troncal 802.1Q, no se especifica en esta práctica de laboratorio.

Se asigna una VLAN nativa a un puerto troncal 802.1Q. En la topología, la VLAN nativa es VLAN 99. Un enlace troncal 802.1Q admite tráfico de varias VLAN (tráfico etiquetado) así como el tráfico que no proviene de una VLAN (tráfico sin etiquetar). El puerto de enlace troncal 802.1Q coloca el tráfico sin etiquetar en la VLAN nativa. El tráfico sin etiquetar se genera con una computadora conectada a un puerto del switch que se configura con la VLAN nativa. Una de las especificaciones de IEEE 802.1Q para VLAN nativas es mantener la compatibilidad retrospectiva con el tráfico sin etiquetar común en los escenarios de LAN antiguas. A los fines de esta práctica de laboratorio, una VLAN nativa sirve como identificador común en lados opuestos de un enlace troncal. Es una optimización utilizar una VLAN que no sea VLAN 1 como VLAN nativa.

Simplifique la configuración de enlaces troncales con el comando **interface range** en el modo de configuración global.

```
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
S1(config-if-range)#end

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
S2(config-if-range)#end

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
S3(config-if-range)#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 | 1-4094 |
| Fa0/2 | 1-4094 |

| 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 |

Paso 8: Verifique que los switches se puedan comunicar.

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 la PC2.

Haga ping desde el host de PC2 al host de PC1 (172.17.10.21). ¿El intento de hacer ping fue exitoso?

NO

Haga ping desde el host PC2 a la dirección IP de la VLAN 99 del switch 172.17.99.12. ¿El intento de hacer ping fue exitoso? NO

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.

Haga ping desde el host PC2 al host PC5. ¿El intento de hacer ping fue exitoso? SI

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

Paso 10: Ubique la PC1 en la misma VLAN que la PC2.

El puerto conectado a PC2 (S2 Fa0/18) se asigna a la VLAN 20, y el puerto conectado a la PC1 (S2 Fa0/11) se asigna a la VLAN 10. Reasigne el puerto S2 Fa0/11 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 nueva VLAN, ese puerto se elimina 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 el host PC2 al host PC1. ¿El intento de hacer ping fue exitoso? SI

Aun cuando los puertos utilizados por la PC1 y PC2 se encuentran en la misma VLAN, aún están en subredes diferentes, por lo que no pueden comunicarse directamente.

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

Asigne 172.17.20.21 como dirección IP de PC1. La máscara de subred y el gateway predeterminado pueden seguir siendo los mismos. Una vez más, haga ping desde el host PC2 al host PC1 utilizando la dirección IP recién asignada.

¿El intento de hacer ping fue exitoso? SI

¿Por qué fue exitoso?

No hay enrutador por medio que lo impida. Están todos los equipos conectados contra todos por tanto la IP solo hace de fingerprint.

Tarea 5: Documentar las configuraciones de los switches

En cada switch, capture la configuración activa en un archivo de texto y consérvela para futuras referencias.

Tarea 6: Limpieza

Borre las configuraciones y vuelva a cargar los switches. Desconecte y guarde el cableado. En caso de PC hosts que están normalmente conectadas a otras redes (tales como la LAN de la escuela o de Internet) vuelva a conectar el cableado apropiado y restaure la configuración de TCP/IP.