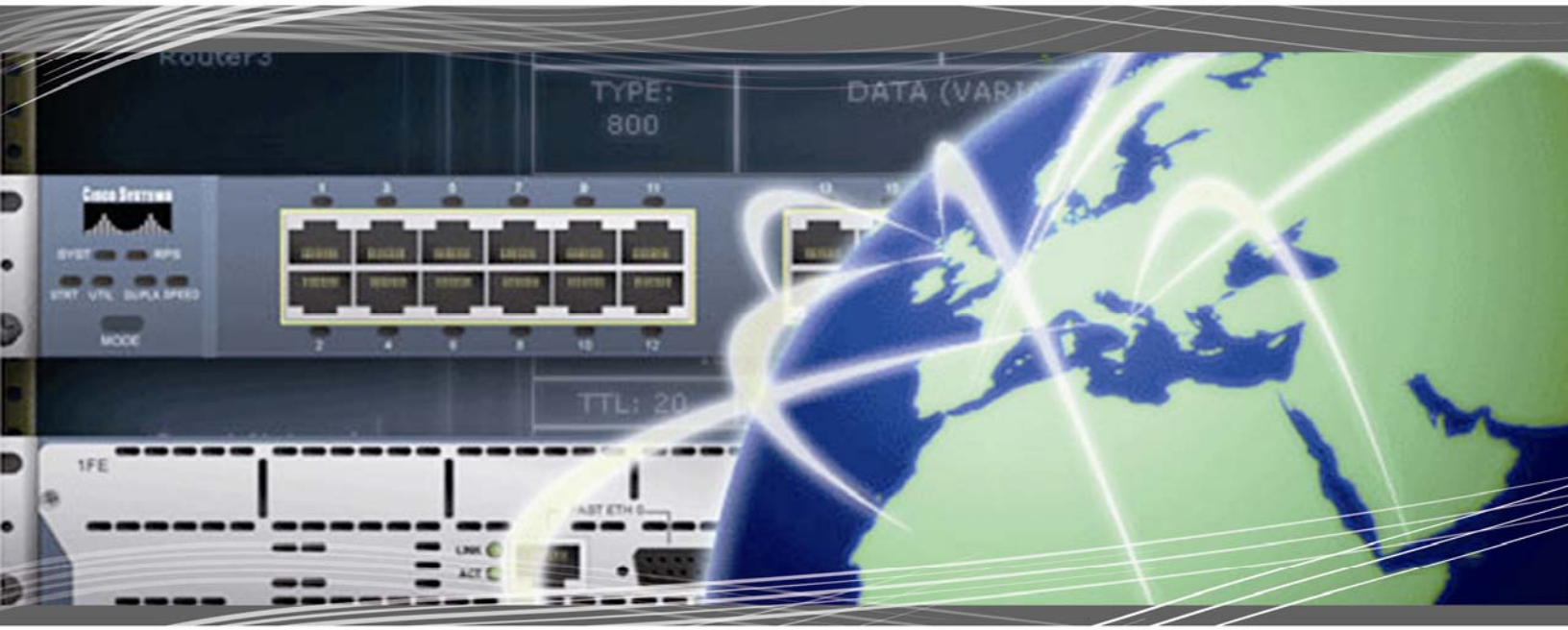
Cisco | Networking Academy®
Mind Wide Open™



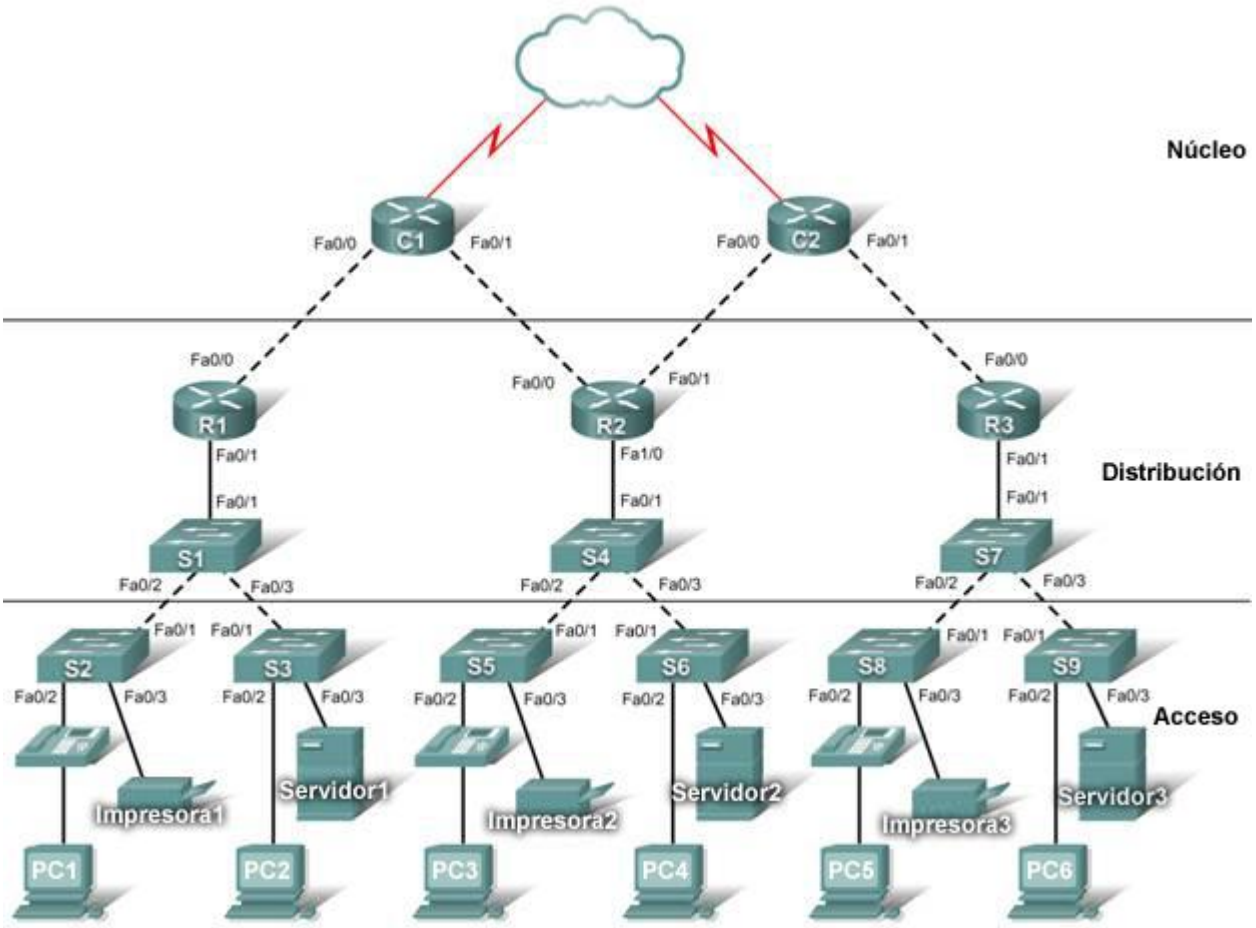
CCNA Exploration 4.0

Conmutación y conexión inalámbrica de LAN

Manual de prácticas de laboratorio del Packet Tracer para el estudiante

Actividad PT 1.2.4: Generar una topología jerárquica

Diagrama de topología



Objetivos de aprendizaje

- Agregar dispositivos a una topología
- Conectar los dispositivos

Introducción

Packet Tracer está integrado a lo largo de este curso. El usuario debe saber cómo navegar en el entorno de Packet Tracer para completar este curso. Use los tutoriales si necesita revisar los principios fundamentales de Packet Tracer. Los tutoriales se encuentran en el menú **Help** de Packet Tracer.

Esta actividad se centra en la creación de una topología jerárquica, desde el núcleo hasta las capas de distribución y acceso.

Tarea 1: Agregar dispositivos a la topología

Paso 1. Agregar los routers y switches de la capa de distribución faltantes.

- Los routers necesarios se encuentran en la ubicación de dispositivos personalizados Custom Made Devices. R1 y R3 son routers 1841. Presione Ctrl y haga clic en el router 1841 para agregar más de uno. Presione Esc para cancelar. R2 es un router 2811.
- Ahora agregue los switches S1, S2 y S3 de la capa de distribución utilizando el modelo 2960-24TT.

Paso 2. Agregar los switches de la capa de acceso restantes.

Siguiendo el diagrama de topología, agregue los switches 2690-24TT para completar el resto de la capa de acceso. Recuerde que si presiona Ctrl y hace clic, puede agregar varios dispositivos del mismo tipo.

Paso 3. Cambiar el nombre para mostrar de cada dispositivo nuevo.

- Haga clic en un dispositivo para abrir su ventana de configuración.
- Seleccione la ficha **Config** para acceder a las opciones básicas de configuración.
- En Global Settings, debajo de Display Name y Hostname, escriba el nombre del dispositivo que se muestra en el diagrama de topología.
- Repita el proceso para todos los dispositivos nuevos que haya agregado.

Si bien Packet Tracer no califica la adición de nombres para mostrar, este paso debe llevarse a cabo para completar correctamente la actividad.

Paso 4. Verificar los resultados.

El porcentaje final del usuario debe ser del 14%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 2: Conectar los dispositivos

Preste especial atención al diagrama de topología y a las interfaces con etiquetas al conectar los dispositivos. Recibirá calificaciones por las conexiones. Por ejemplo, en el diagrama de topología, el switch S1 está conectado a R1 a través de la interfaz Fa0/1 en ambos lados. Esta conexión recibe calificación en relación con el tipo de cable y la designación de la interfaz. No use la utilidad Smart Connection para efectuar estas conexiones, ya que no tiene control sobre la interfaz que se selecciona.

Paso 1. Conectar el cable de los routers de capa núcleo a los routers de capa de distribución.

- Usando cables de conexión de cobre, conecte los routers de capa núcleo, C1 y C2, a los routers de capa de distribución, R1, R2 y R3.
- C1 se conecta a R1 y R2; y C2 se conecta a R2 y R3.
- Al igual que con los dispositivos, puede presionar Ctrl y hacer clic en el tipo de cable para efectuar varias conexiones sin tener que volver a seleccionar el cable.
- Recuerde consultar el diagrama de topología para determinar qué interfaces se deben usar para estas conexiones.

Paso 2. Conectar el cable de los routers de capa de distribución a los switches de capa de acceso.

Conecte los routers de capa de distribución a los switches de capa de acceso mediante cables de cobre de conexión directa. R1 se conecta a S1, R2 se conecta a S4 y R3 se conecta a S7.

Paso 3. Conectar los switches de capa de acceso.

Conecte los switches de capa de acceso con cables de cobre de conexión cruzada. Siga el diagrama de topología para obtener las conexiones correctas.

Paso 4. Conectar los dispositivos finales.

Conecte los dispositivos finales restantes (teléfonos IP, impresoras, PC y servidores) al switch correcto mediante cables de cobre de conexión directa. Al conectar un switch a un equipo PC, recuerde conectarlo al puerto Fast Ethernet del equipo PC.

Paso 5. Verificar los resultados.

El porcentaje final del usuario debe ser del 100%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Nota: Un error en Packet Tracer puede hacer que el porcentaje sólo se muestre como 99% aunque se hayan completado todos los componentes obligatorios. Si espera lo suficiente, Packet Tracer finalmente actualizará el porcentaje y mostrará el 100% completo.

Paso 6. Reflexión.

Observe que los colores de las luces de enlace de los puertos entre los switches, y entre un switch y un dispositivo final eventualmente cambiarán de ámbar a verde. ¿Por qué las luces de enlace de los puertos entre los routers y de los puertos entre los routers y los switches están de color rojo?

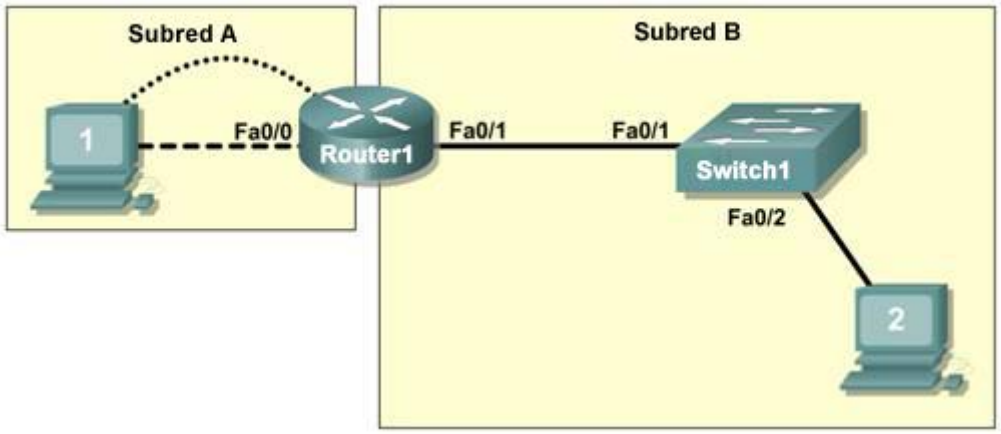
_____

_____

_____

Actividad PT 1.3.1: Revisión de los conceptos de Exploration 1

Diagrama de topología



Objetivos de aprendizaje

- Diseñar la topología LAN lógica
- Configurar la topología física
- Configurar la topología lógica
- Verificar la conectividad de la red
- Verificar las contraseñas

Introducción

En esta actividad, se podrá diseñar y configurar una red pequeña enrutada y verificar la conectividad entre varios dispositivos de red. Esto requiere la creación y asignación de dos bloques de subred, la conexión de hosts y dispositivos de red y la configuración de equipos host y un router Cisco para la conectividad básica de la red. El Switch1 tiene una configuración por defecto y no requiere configuraciones adicionales. Se usarán comandos comunes para probar y documentar la red. Se utilizará la subred cero.

Tarea 1: Diseñar una topología LAN lógica

Paso 1. Diseñar un esquema de direccionamiento IP.

Dado un bloque de direcciones IP de 192.168.7.0 /24, diseñe un esquema de direccionamiento IP que cumpla con los siguientes requisitos:

Subred	Cantidad de hosts
Subred A	**110**
Subred B	**54**

Se utilizará la subred 0. No se permite el uso de calculadoras de subred. Cree las subredes más pequeñas posibles que cumplan con los requisitos para los hosts. Asigne la primera subred utilizable a la Subred A.

Los equipos host utilizarán la primera dirección IP en la subred. El router de red usará la última dirección IP en la subred.

Paso 2. Tomar nota de la información de la dirección IP de cada dispositivo.

Antes de continuar, verifique las direcciones IP con el instructor.

Tarea 2: Configurar la topología física

Paso 1. Establecer el cableado de la red.

- Conecte Host1 a la interfaz Fa0/0 en el Router1.
- Conecte un cable de consola entre Host1 y Router1.
- Conecte la interfaz Fa0/1 en el Switch1 a la interfaz Fa0/1 en el Router1.
- Conecte Host2 a la interfaz Fa0/2 en el Switch1.

Paso 2. Inspeccionar las conexiones de red.

Verifique las conexiones visualmente.

Tarea 3: Configurar la topología lógica

Paso 1. Configurar los equipos host.

Configure la dirección IP estática, la máscara de subred y la gateway para cada equipo host.

Paso 2. Configurar el Router1.

Conecte el Router1 a través de la conexión de terminal en el Host1. Introduzca los siguientes comandos en el router:

Recuerde: Packet Tracer distingue entre mayúsculas y minúsculas al calificar el comando **description**.

```
Router>enable
Router#config term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Router1
Router1(config)#enable secret class
Router1(config)#line console 0
Router1(config-line)#password cisco
Router1(config-line)#login
Router1(config-line)#line vty 0 4
Router1(config-line)#password cisco
Router1(config-line)#login
Router1(config-line)#int fa0/0
Router1(config-if)#ip address addr sub_mask Obtenga la respuesta de la Tarea 1
Router1(config-if)#no shutdown
Router1(config-if)#description connection to host1
Router1(config-if)#interface fa0/1
Router1(config-if)#description connection to switch1
Router1(config-if)#ip address addr sub_mask Obtenga la respuesta de la Tarea 1
Router1(config-if)#no shutdown
Router1(config-if)#end
Router1#
```

Tarea 4: Verificar la conectividad de la red

Paso 1. Usar el comando ping para verificar la conectividad de la red.

Puede verificar la conectividad de la red con el comando **ping**.

Tarea 5: Verificar las contraseñas

Paso 1. Establecer una conexión Telnet al router desde Host2 y verificar la contraseña de Telnet.

Debe poder establecer una conexión telnet a cualquier interfaz Fast Ethernet del router.

En una ventana de comando en el Host2, escriba:

```
Packet Tracer PC Command Line 1.0
PC>telnet 192.168.7.190
Trying 192.168.7.190 ...

User Access Verification

Password:
```

Cuando se solicite la contraseña de Telnet, escriba **cisco** y presione Intro.

Paso 2. Verificar que se haya configurado la contraseña secreta de enable.

Desde la sesión de Telnet, ingrese al Modo exec privilegiado y verifique que esté protegido por contraseñas.

```
Router1>enable
```

¿Se solicitó la contraseña secreta de enable?

Tarea 6: Reflexión

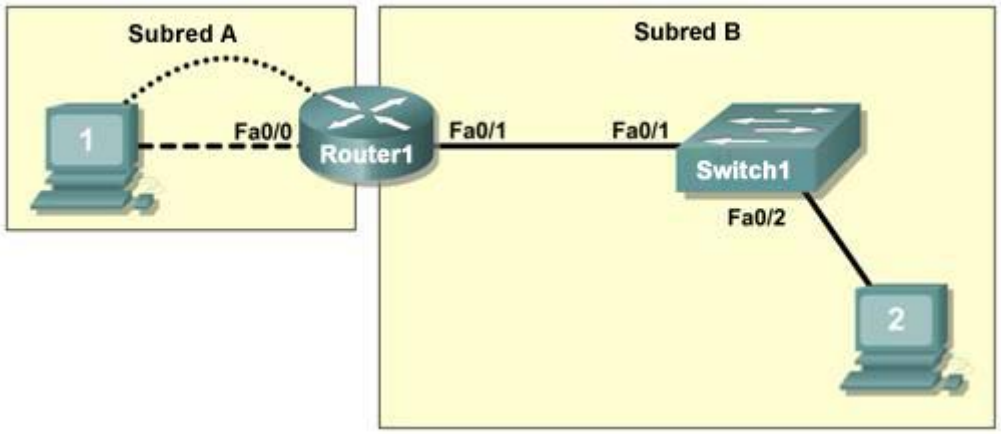
¿En qué se diferencian el acceso Telnet y el acceso de consola?

¿Cuándo puede ser necesario definir diferentes contraseñas para estos dos puertos de acceso?

¿Por qué el switch entre Host2 y el router no requiere configuración con una dirección IP para reenviar paquetes?

Actividad PT 1.3.2: Revisión de los conceptos de Exploration 1: Reto

Diagrama de topología



Objetivos de aprendizaje

- Diseñar la topología LAN lógica
- Configurar la topología física
- Configurar la topología lógica
- Verificar la conectividad de la red
- Verificar las contraseñas

Introducción

En esta actividad, se podrá diseñar y configurar una red pequeña enrutada y verificar la conectividad entre varios dispositivos de red. Esto requiere la creación y asignación de dos bloques de subred, la conexión de hosts y dispositivos de red y la configuración de equipos host y un router Cisco para la conectividad básica de la red. El Switch1 tiene una configuración por defecto y no requiere configuraciones adicionales. Se usarán comandos comunes para probar y documentar la red. Se utilizará la subred cero.

Tarea 1: Diseñar una topología LAN lógica

Paso 1. Diseñar un esquema de direccionamiento IP.

Dado un bloque de direcciones IP de **192.168.30.0 /27**, diseñe un esquema de direccionamiento IP que cumpla con los siguientes requisitos:

Subred	Cantidad de hosts
Subred A	**7**
Subred B	**14**

Se utilizará la subred 0. No se permite el uso de calculadoras de subred. Cree las subredes más pequeñas posibles que cumplan con los requisitos para los hosts. Asigne la primera subred utilizable a la Subred A.

Los equipos host utilizarán la primera dirección IP en la subred. El router de red usará la última dirección IP en la subred.

Paso 2. Tomar nota de la información de la dirección IP de cada dispositivo.

Antes de continuar, verifique las direcciones IP con el instructor.

Tarea 2: Configurar la topología física

Paso 1. Establecer el cableado de la red.

Paso 2. Inspeccionar las conexiones de red.

Tarea 3: Configurar la topología lógica

Paso 1. Configurar los equipos host.

Paso 2. Configurar el Router1.

Introduzca los siguientes comandos en el router:

- Nombre de router **Router1**
- Contraseña secreta **class**
- Establezca las contraseñas de las líneas de consola y VTY en **cisco**
- Direcciones de interfaz
- Descripción de las interfaces
    - Texto en Fa0/0: conexión con Host1
    - Texto en Fa0/1: conexión con Switch1

Tarea 4: Verificar la conectividad de la red

Paso 1. Usar el comando ping para verificar la conectividad de la red.

Puede verificar la conectividad de la red con el comando **ping**.

Tarea 5: Verificar las contraseñas

Paso 1. Establecer una conexión Telnet al router desde Host2 y verificar la contraseña de Telnet.

Paso 2. Verificar que se haya configurado la contraseña secreta de enable.

Tarea 6: Reflexión

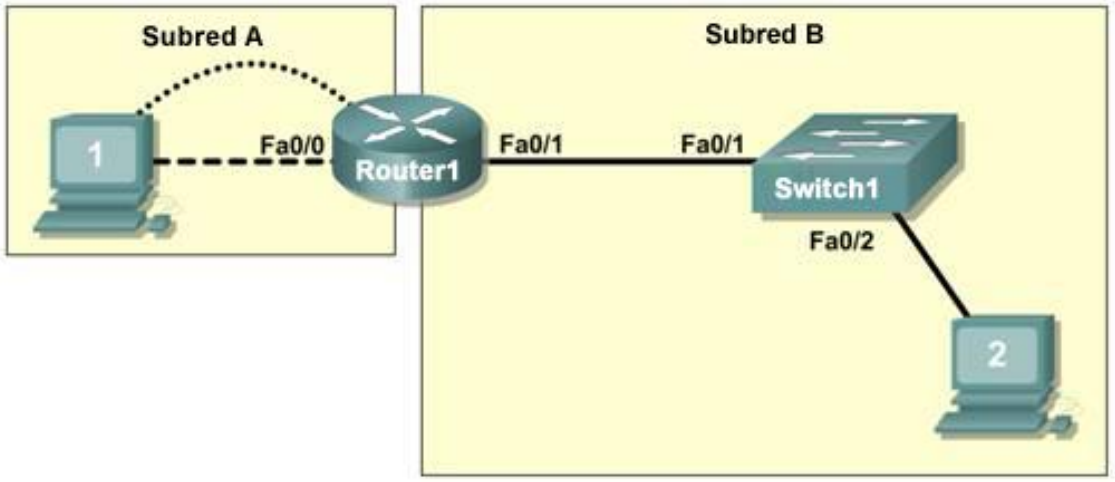
¿En qué se diferencian el acceso Telnet y el acceso de consola?

¿Cuándo puede ser necesario definir diferentes contraseñas para estos dos puertos de acceso?

¿Por qué el switch entre Host2 y el router no requiere configuración con una dirección IP para reenviar paquetes?

Actividad PT 1.3.3: Resolución de problemas en una red pequeña

Diagrama de topología



Objetivos de aprendizaje

- Examinar la topología LAN lógica
- Realizar la resolución de problemas de conexiones de red

Introducción

La configuración incluye errores de diseño y configuración que entran en conflicto con los requisitos manifestados e impiden la comunicación de extremo a extremo. Realizará la resolución de problemas de conectividad a fin de determinar dónde ocurren los errores y corregirlos usando los comandos adecuados. Una vez que se hayan corregido todos los errores, cada host debe poder comunicarse con todos los demás elementos de red configurados y con el otro host.

Tarea 1: Examinar la topología LAN lógica

Paso 1. Diseñar un esquema de direccionamiento IP.

El bloque de dirección IP de **172.16.30.0 /23** está dividido en subredes para cumplir con los siguientes requisitos:

Subred	Cantidad de hosts
Subred A	**174**
Subred B	**60**

Requisitos y especificaciones adicionales:

- Se utilizará la subred 0.
- Se debe usar la menor cantidad posible de subredes que satisfaga los requisitos de los hosts, reservando el bloque más grande posible para utilizarlo más adelante.
- Asigne la primera subred utilizable a la Subred A.
- Los equipos host usan la primera dirección IP en la subred.
- El router de la red usa la última dirección de host de la red.

Según estos requisitos, se ha proporcionado el siguientes esquema de direccionamiento:

Subred A	
Máscara IP (decimal)	**255.255.255.0**
Dirección IP	**172.16.30.0**
Primera dirección IP de host	**172.16.30.1**
Última dirección IP de host	**172.16.30.254**
Subred B	
Máscara IP (decimal)	**255.255.255.128**
Dirección IP	**172.16.31.0**
Primera dirección IP de host	**172.16.31.1**
Última dirección IP de host	**172.16.31.126**

Examine cada uno de los valores de las tablas anteriores y verifique que esta topología cumpla con todos los requisitos y las especificaciones. ¿Alguno de los valores no es correcto?

De ser así, tome nota de los valores corregidos.

Tarea 2: Realizar la resolución de problemas de conexiones de red

Paso 1. Comenzar la resolución de problemas en el host conectado al router BRANCH.

Desde el host PC1, ¿es posible hacer ping a PC2?

Desde el host PC1, ¿es posible hacer ping a la interfaz fa0/1 del router?

Desde el host PC1, ¿es posible hacer ping a la gateway predeterminada?

Desde el host PC1, ¿es posible hacer ping a él mismo?

¿Cuál es el lugar más lógico para comenzar a realizar la resolución de problemas de conexión de PC1?

Paso 2. Examinar el router para buscar posibles errores de configuración.

Comience por consultar el resumen de la información de estado para cada interfaz del router.

¿Hay algún problema con el estado de las interfaces?

Si hay problemas con el estado de las interfaces, registre los comandos necesarios para corregir los errores de configuración.

Paso 3. Usar los comandos necesarios para corregir la configuración del router.

Paso 4. Ver un resumen de la información de estado.

Si se efectuaron cambios en la configuración durante el paso anterior, consulte el resumen de información de estado correspondiente a las interfaces del router.

¿La información en el resumen de estado de las interfaces indica errores en la configuración del Router1?

Si la respuesta es sí, realice la resolución de problemas del estado de interfaz de las interfaces.

¿Se ha restaurado la conectividad?

Paso 5. Verificar la configuración lógica.

Examine el estado completo de Fa0/0 y 0/1. ¿Las direcciones IP y la información de la máscara de subred en el estado de interfaz son coherentes con la tabla de configuración?

Si hay diferencias entre la tabla de configuración y la configuración de interfaz del router, registre los comandos necesarios para corregir la configuración del router.

¿Se ha restaurado la conectividad?

¿Por qué resulta útil que un host haga ping a su propia dirección?

Actividad PT 1.4.1: Reto de habilidades de Integración de Packet Tracer

Diagrama de topología

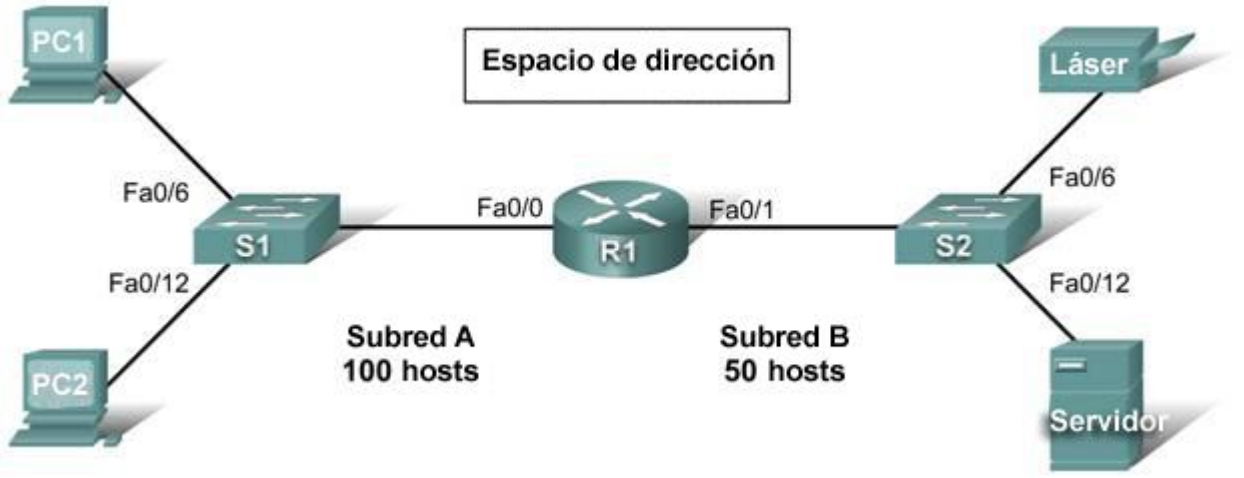


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de enlace) predeterminada
R1	**Fa0/0**			No aplicable
	Fa0/1			No aplicable
PC1	**NIC**			
PC2	**NIC**			
Láser	**NIC**			
Servidor	**NIC**			

Objetivos de aprendizaje

- Diseñar la red
- Crear la red
- Aplicar una configuración básica
- Probar la conectividad

Introducción

En esta actividad se repasan las habilidades adquiridas en el curso Exploration: Principios básicos de networking. Entre las habilidades se incluyen la creación de subredes, la creación de una red, la aplicación de un esquema de direccionamiento y la prueba de la conectividad. El usuario debe revisar estas habilidades antes de continuar. Además, en esta actividad se repasan los principios básicos del uso del programa Packet Tracer. Packet Tracer está integrado a lo largo de este curso. El usuario debe saber cómo navegar en el entorno de Packet Tracer para completar este curso. Use los tutoriales si necesita revisar los principios fundamentales de Packet Tracer. Los tutoriales se encuentran en el menú **Help** de Packet Tracer.

Tarea 1: Diseñar y documentar un esquema de direccionamiento

Paso 1. Diseñar un esquema de direccionamiento.

Utilizando el espacio de dirección 192.168.1.0/24, diseñe un esquema de direccionamiento según los siguientes requisitos:

Subred A

- Cree una subred en el espacio de dirección para 100 hosts.
- Asigne la primera dirección IP utilizable a la interfaz Fa0/0.
- Asigne la segunda dirección IP utilizable a PC1.
- Asigne la última dirección IP utilizable en la subred a PC2.

Subred B

- Cree una subred en el espacio de dirección restante para 50 hosts.
- Asigne la primera dirección IP utilizable a la interfaz Fa0/1.
- Asigne la segunda dirección IP utilizable a la impresora láser.
- Asigne la última dirección IP utilizable en la subred al servidor.

Paso 2. Documentar el esquema de direccionamiento.

Complete una tabla de direccionamiento para el router y para cada dispositivo final de la red.

Tarea 2: Agregar y conectar los dispositivos

Paso 1. Agregar el equipo necesario.

Agregue los siguientes dispositivos a la red. Para colocar estos dispositivos, consulte el diagrama de topología.

- Dos switches 2690-24TT
- Un router 1841
- Dos equipos PC genéricos
- Un servidor genérico
- Una impresora genérica

Paso 2. Asignar nombres a los dispositivos.

Cambie el nombre para mostrar y el nombre de host de modo que coincidan con los nombres de los dispositivos que se muestran en el diagrama de topología. Los nombres de los dispositivos distinguen entre mayúsculas y minúsculas.

Paso 3. Conectar los dispositivos.

Use las siguientes especificaciones para las conexiones entre los dispositivos:

- S1 Fa0/1 a R1 Fa0/0
- S1 Fa0/6 a PC1
- S1 Fa0/12 a PC2
- S2 Fa0/1 a R1 Fa0/1
- S2 Fa0/6 a láser
- S2 Fa0/12 a servidor

Paso 4. Verificar los resultados.

El porcentaje final del usuario debe ser del 46%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 3: Aplicar configuraciones básicas

Paso 1. Configurar el router.

- La contraseña secreta de EXEC privilegiado es **class**.
- El mensaje es **Authorized Access Only.**
- La contraseña de línea es **cisco** para la consola y para telnet.
- Configure las interfaces correspondientes. Utilice las siguientes descripciones:
  - **Link to PC LAN**
  - **Link to Server & Printer**

Nota: Recuerde que el mensaje y las descripciones distinguen entre mayúsculas y minúsculas. No olvide activar las interfaces.

Paso 2. Configurar los dispositivos finales.

Paso 3. Verificar los resultados.

El porcentaje final del usuario debe ser del 100%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 4: Probar la conectividad y examinar la configuración

Ahora se debe contar con conectividad de extremo a extremo, lo que significa que se debe poder acceder a todos los dispositivos finales desde cualquier otro dispositivo final. Desde PC1 y PC2, haga ping a todos los dispositivos finales de la red. Si recibe un error, intente hacer ping nuevamente para asegurarse de que las tablas ARP estén actualizadas. Si aún recibe un error, compruebe la división de subredes, los cables y las direcciones IP. Aísle los problemas e implemente soluciones.

Actividad PT 2.3.8: Configuración de la administración básica del switch

Diagrama de topología

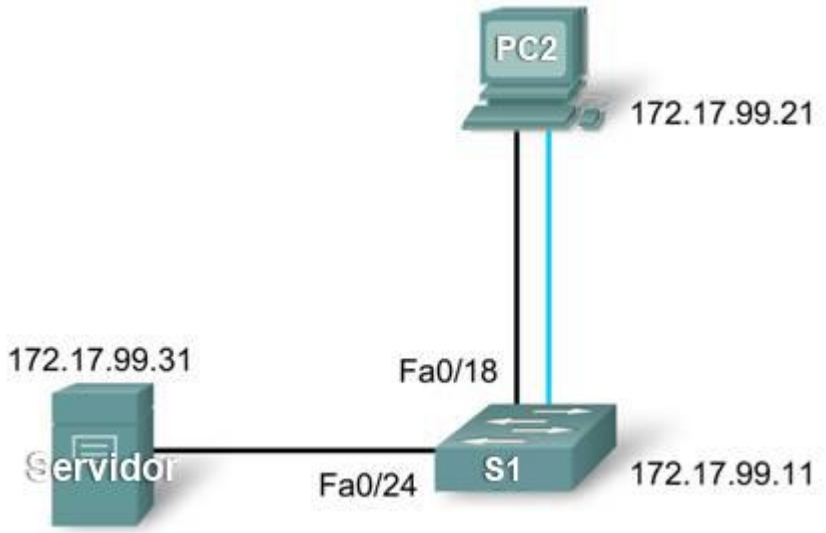


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
S1	**VLAN99**	172.17.99.11	255.255.255.0
PC1	**NIC**	172.17.99.21	255.255.255.0
Servidor	**NIC**	172.17.99.31	255.255.255.0

Objetivos de aprendizaje

- Conectarse al switch usando una conexión de consola
- Navegar por diversos modos CLI
- Usar el servicio de ayuda para configurar el reloj
- Acceder al historial de comandos y configurarlo
- Configurar la secuencia de arranque
- Configurar un equipo PC y conectarlo a un switch
- Configurar full duplex
- Administrar la tabla de direcciones MAC
- Administrar el archivo de configuración del switch

Introducción

La administración básica del switch es la base de la configuración de los switches. Esta actividad se centra en la navegación entre los modos de interfaz de la línea de comandos, el uso de las funciones de ayuda, el acceso al historial de comandos, la configuración de parámetros de la secuencia de arranque, la definición de la configuración de velocidad y duplex; además de la administración de la tabla de direcciones MAC y el archivo de configuración de switch. Las habilidades adquiridas en esta actividad son necesarias para la configuración de la seguridad básica del switch incluida en capítulos posteriores.

Tarea 1: Conectarse al switch

Paso 1: Conectar S1 y PC1.

- Utilice un cable de consola y conecte la interfaz RS 232 de PC1 a la interfaz de la consola del switch S1.
- Haga clic en **PC1** y luego en la ficha **Desktop**. Seleccione **Terminal** de la ficha Desktop.
- Conserve la configuración por defecto para la configuración del terminal y, luego, haga clic en **OK**.

  Bits Per Second = 9600
  Data Bits = 8
  Parity = None
  Stop Bits = 1
  Flow Control = None
- El usuario está conectado a la consola en S1. Presione **Intro** para ver el indicador Switch.

Paso 2: Verificar los resultados.

El porcentaje final del usuario debe ser del 6%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 2: Navegar por los modos CLI

Paso 1: En el Modo EXEC del usuario, escriba ? Tenga en cuenta la lista de comandos disponibles.

Mientras está en el Modo EXEC del usuario, los comandos disponibles son sólo los comandos básicos de monitorización.

Paso 2: Use el comando enable para ir al Modo EXEC privilegiado.

```
Switch>enable
Switch#
```

El indicador cambia de **>** a **#**.

Paso 3: En el Modo EXEC privilegiado, escriba ?. Tenga en cuenta la lista de comandos disponibles.

Ahora hay más comandos disponibles que en el Modo EXEC del usuario. Además de los comandos básicos de monitorización, ahora se puede obtener acceso a los comandos de configuración y administración.

Paso 4: Cambiar al modo de configuración global.

```
Switch#configure terminal
Switch(config)#
```

Paso 5: En el modo de configuración global, escriba ?. Tenga en cuenta la lista de comandos disponibles.

Paso 6: Configurar S1 como el nombre de host.

```
Switch(config)#hostname S1
S1(config)#
```

Paso 7: Cambiar al modo de configuración de interfaz para VLAN99.

El comando **interface vlan 99** crea la interfaz y cambia al modo de configuración de interfaz para VLAN99.

```
S1(config)#interface vlan 99
S1(config-if)#
```

Paso 8: Configurar VLAN99 con 172.17.99.11/24 y activar la interfaz.

Use los comandos **ip address** y **no shutdown** para asignar la dirección IP y la máscara de subred correctas y activar la interfaz.

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

Paso 9: Cambiar al modo de configuración de interfaz para Fa0/18.

```
S1(config-if)#interface fa0/18
S1(config-if)#
```

Paso 10: Definir el modo de puerto al que se debe acceder.

Para permitir el envío y la recepción de tramas desde la interfaz, cambie al modo de conmutación al que se debe acceder mediante el comando **switchport mode access**.

```
S1(config-if)#switchport mode access
```

Paso 11: Asignar VLAN99 al puerto.

Para permitir que la interfaz Fa0/18 actúe como miembro de VLAN 99, ejecute el comando **switchport access vlan 99**.

```
S1(config-if)#switchport access vlan 99
```

Paso 12: Salir del modo de configuración de interfaz.

Ejecute el comando **exit** para abandonar el modo de configuración de interfaz y entrar al modo de configuración global.

Paso 13: Entrar al modo de configuración de línea para la consola.

```
S1(config)#line console 0
S1(config-line)#
```

Paso 14: En el modo de configuración de línea, escriba ? Tenga en cuenta la lista de comandos disponibles.

Paso 15: Escribir cisco como la contraseña e introducir el comando login.

```
S1(config-line)#password cisco
S1(config-line)#login
```

Paso 16: Regresar el Modo EXEC privilegiado mediante el comando end.

```
S1(config-line)#end
S1#
```

Paso 17: Verificar los resultados.

El porcentaje final del usuario debe ser del 31%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 3: Usar el servicio de ayuda para configurar el reloj

Paso 1: En la petición de entrada del Modo EXEC privilegiado, escriba clock ?.

```
S1#clock ?
```

La única opción es **set**.

Paso 2: Usar la ayuda para facilitar la configuración del reloj según la hora actual.

```
S1#clock ?
  set  Set the time and date

S1#clock set ?
  hh:mm:ss Current Time

S1#clock set 12:12:12 ?
  <1-31>  Day of the month
  MONTH   Month of the year
```

Continúe con la ejecución del comando **?** hasta haber completado la configuración del reloj. Recibirá el mensaje de advertencia **% Incomplete command message** si el comando **clock** no se ha introducido completamente con todos los argumentos requeridos.

Paso 3: Verificar que el reloj esté configurado.

Para verificar que el reloj esté configurado, ejecute el comando **show clock.**

Nota: Packet Tracer no siempre muestra la hora correcta configurada.

El porcentaje final será del 31% al final de esta tarea.

Tarea 4: Acceder al historial de comandos y configurarlo

Paso 1: Ver los comandos introducidos más recientemente.

Ejecute el comando **show history**. Recuerde la cantidad de comandos incluidos en la lista.

```
S1#show history
```

Paso 2: Cambiar la cantidad de comandos almacenada en el búfer del historial.

Entre al modo de configuración de línea para la consola y para Telnet. Defina la cantidad de comandos retenidos en el búfer del historial en 35.

```
S1(config)#line console 0
S1(config-line)#history size 35
S1(config-line)#line vty 0 4
S1(config-line)#history size 35
```

Paso 3: Verificar que el tamaño del búfer del historial se haya modificado.

Regrese al Modo EXEC privilegiado y ejecute el comando **show history** nuevamente. Se deben mostrar más comandos que antes.

Paso 4: Verificar los resultados.

El porcentaje final del usuario debe ser del 50%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 5: Configurar la secuencia de arranque

Paso 1: Comprobar la versión de software IOS de Cisco cargada.

```
S1#show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX,
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team
<output omitted>
```

La versión se indica en la primera línea.

Paso 2: Comprobar las imágenes de IOS de Cisco cargadas en la memoria flash.

```
S1#show flash
Directory of flash:/

    3  -rw-     4414921          <no date>  c2960-lanbase-mz.122-25.FX.bin
    2  -rw-     4670455          <no date>  c2960-lanbase-mz.122-25.SEE1.bin
    6  -rw-         616          <no date>  vlan.dat

32514048 bytes total (23428056 bytes free)
S1#
```

Tenga en cuenta que hay dos versiones en la memoria flash. La versión cargada es **c2960-lanbase-mz.122-25.FX.bin**.

Paso 3: Configurar el sistema para que arranque mediante una imagen de IOS de Cisco diferente.

En el modo de configuración global, ejecute este comando.

```
S1(config)#boot system flash:/c2960-lanbase-mz.122-25.SEE1.bin
```

Nota: Si bien puede introducir este comando en Packet Tracer, el switch aún carga la primera imagen que se indica en la memoria flash.

Packet Tracer no califica el comando **boot system** en los switches, de modo que el porcentaje final continúa en 50% al completar esta tarea.

Tarea 6: Configurar un equipo PC y conectarlo a un switch

Paso 1: Configurar PC1 con la dirección IP y la máscara de subred 172.17.99.21/24.

- Salga de la terminal para regresar a la ficha **Desktop**.
- Haga clic en **IP Configuration** y establezca la dirección IP en 172.17.99.21 y la máscara de subred en 255.255.255.0.

Paso 2: Conectar PC1 a Fa0/18 en el switch.

Utilice el cable de cobre de conexión directa, para conectar el puerto FastEthernet del equipo PC al puerto Fa0/18 del switch.

Paso 3: Probar la conectividad entre S1 y PC1.

Haga ping entre S1 y PC1. Es posible que deba intentarlo varias veces, pero normalmente, debería realizarse correctamente.

Paso 4: Verificar los resultados.

El porcentaje final del usuario debe ser del 69%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 7: Configurar el duplex y la velocidad

Paso 1: Usar la ficha Config para cambiar la configuración.

En PC1, seleccione la ficha **Config**. Establezca el ancho de banda de la interfaz FastEthernet en 100 Mbps y Full Duplex.

Paso 2: Usar los comandos de IOS de Cisco para configurar Fa0/18.

Regrese al escritorio y seleccione **Terminal**; luego, configure la interfaz.

```
S1(config)#interface fa0/18
S1(config-if)#duplex full
S1(config-if)#speed 100
```

Paso 3: Probar la conectividad entre S1 y PC1.

Ejecute un ping desde S1 a PC1. Es posible que deba intentarlo varias veces, pero normalmente, debería realizarse correctamente.

Paso 4: Verificar los resultados.

El porcentaje final del usuario debe ser del 81%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 8: Administrar la tabla de direcciones MAC

Paso 1: Comprobar la dirección MAC del servidor.

Haga clic en **Server**, luego en la ficha **Config** y en **FastEthernet**. La dirección MAC es 0060.3EDD.19A3.

Paso 2: Configurar MAC estática para el servidor TFTP.

Al configurar una MAC estática para el servidor TFTP, el switch siempre sabe qué puerto usar para enviar tráfico destinado al servidor. En el modo de configuración global en S1, agregue la dirección MAC a la tabla de direccionamiento del switch.

```
S1(config)#mac-address-table static 0060.3EDD.19A3 vlan 99 int fa0/24
```

Paso 3: Verificar que la dirección MAC estática esté ahora en la tabla de direcciones MAC.

```
S1#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  99    0060.3edd.19a3    STATIC      Fa0/24
  99    0060.5c5b.cd23    DYNAMIC     Fa0/18
S1#
```

Tenga en cuenta cómo la dirección MAC de PC1 se agregó dinámicamente. Esta entrada puede estar o no en la tabla según el tiempo transcurrido desde que se hizo ping desde PC1 a S1.

Paso 4: Probar la conectividad entre S1 y PC1.

Ejecute un ping desde S1 a PC1. Es posible que deba intentarlo varias veces, pero normalmente, debería realizarse correctamente.

Packet Tracer no califica este comando. Este comando es necesario para permitir que el switch conozca el lugar al que debe enviar el tráfico destinado para el servidor. El porcentaje final será del 81% al final de esta tarea.

Tarea 9: Administrar el archivo de configuración del switch

Utilice el cable de cobre de conexión directa para conectar el puerto FastEthernet del servidor al puerto Fa0/24 del switch.

Paso 1: Entrar al modo de configuración de interfaz para Fa0/24.

```
S1#configure terminal
S1(config)#interface fa0/24
S1(config-if)#
```

Paso 2: Definir el modo de puerto al que se debe acceder.

Configurar el modo de puerto al que se debe acceder permite el envío y la recepción de tramas desde la interfaz.

```
S1(config-if)#switchport mode access
```

Nota: Packet Tracer no califica el comando **`switchport mode access`**. No obstante, el comando es necesario para cambiar la interfaz del modo por defecto al modo de acceso.

Paso 3: Asignar VLAN99 al puerto.

La asignación de VLAN99 al puerto permite que la interfaz Fa0/24 actúe como miembro de VLAN 99.

```
S1(config-if)#switchport access vlan 99
```

Paso 4: Verificar que S1 pueda hacer ping al servidor.

Haga ping al servidor desde S1. Es posible que deba intentarlo varias veces, pero normalmente, debería realizarse correctamente.

Paso 5: Hacer una copia de respaldo de la configuración de inicio en el servidor.

En el Modo EXEC privilegiado, copie la configuración de inicio en el servidor. Cuando se solicite la dirección del host remoto, introduzca la dirección IP del servidor, 172.17.99.31. Para conocer el nombre del archivo destino, use el nombre de archivo por defecto presionando **Intro**.

```
S1#copy startup-config tftp:
Address or name of remote host []? 172.17.99.31
Destination filename [S1-confg]? [Enter]
```

Paso 6: Verificar que el servidor tenga la configuración de inicio.

Para determinar si la configuración de inicio se transfirió correctamente al servidor, haga clic en el servidor y, luego, en la ficha **Config**. El archivo S1-confg debe mostrarse bajo Services y TFTP.

Nota: La restauración del inicio desde el servidor no se simula completamente en Packet Tracer.

Paso 7: Verificar los resultados.

El porcentaje final del usuario debe ser del 100%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Actividad PT 2.4.7: Configurar la seguridad del switch

Diagrama de topología

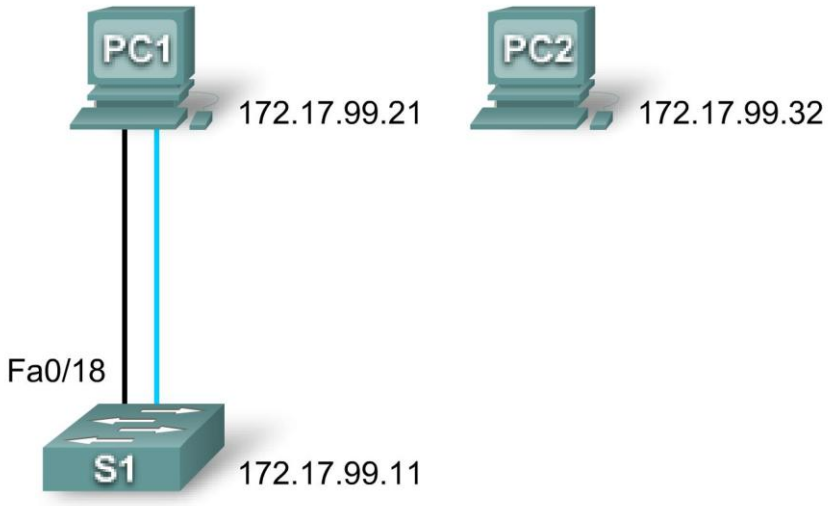


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
S1	**VLAN99**	172.17.99.11	255.255.255.0
PC1	**NIC**	172.17.99.21	255.255.255.0
PC2	**NIC**	172.17.99.32	255.255.255.0

Objetivos de aprendizaje

- Configurar la administración básica del switch
- Configurar la seguridad de los puertos dinámicos
- Probar la seguridad de los puertos dinámicos
- Proteger los puertos sin utilizar

Tarea 1: Configurar la administración básica del switch

Paso 1: Desde PC1, acceda a la conexión de consola a S1.

- Haga clic en PC1 y luego en la ficha Desktop. Seleccione Terminal de la ficha Desktop.
- Conserve la configuración por defecto para la configuración del terminal y, luego, haga clic en OK:

  Bits Per Second = 9600
  Data Bits = 8
  Parity = None
  Stop Bits = 1
  Flow Control = None
- El usuario está conectado a la consola en S1. Presione Intro para ver el indicador Switch.

Paso 2: Cambiar al Modo EXEC privilegiado.

Para acceder al Modo EXEC privilegiado, escriba el comando **enable**. El indicador cambia de **>** a **#**.

```
S1>enable
S1#
```

Observe que se pudo entrar al Modo EXEC privilegiado sin proporcionar una contraseña. ¿Por qué la ausencia de una contraseña para el Modo EXEC privilegiado constituye una amenaza de seguridad?

_____

_____

_____

Paso 3: Cambiar al modo de configuración global y configurar la contraseña EXEC privilegiado.

- Mientras está en el Modo EXEC privilegiado, puede acceder al modo de configuración global mediante el comando **configure terminal**.
- Use el comando **enable secret** para establecer la contraseña. Para esta actividad, establezca **class** como contraseña.

```
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#enable secret class
S1(config)#
```

Nota: PT no calificará el comando **enable secret**.

Paso 4: Configurar contraseñas de terminal virtual y de consola e introducir el comando login.

Se debe exigir una contraseña para acceder a la línea de consola. Incluso el Modo EXEC del usuario básico puede proporcionar información importante a un usuario malintencionado. Además, las líneas vty deben tener una contraseña antes de que los usuarios puedan acceder al switch de manera remota.

- Acceda al indicador de consola mediante el comando **line console 0**.
- Use el comando **password** para configurar las líneas de consola y vty con **cisco** como contraseña. Nota: PT no calificará el comando **password cisco** en este caso.
- A continuación, introduzca el comando **login**, que requiere que los usuarios escriban una contraseña antes de poder acceder al Modo EXEC del usuario.
- Repita el proceso con las líneas vty. Use el comando **line vty 0 15** para acceder al indicador correcto.
- Escriba el comando **exit** para regresar al indicador de configuración global.

```
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```

Paso 5: Configurar la encriptación de contraseñas.

La contraseña de EXEC privilegiado ya está encriptada. Para encriptar las contraseñas de la línea recién configurada, escriba el comando **service password-encryption** en el modo de configuración global.

```
S1(config)#service password-encryption
S1(config)#
```

Paso 6: Configurar y probar el mensaje MOTD.

Configure el mensaje del día (MOTD, *message of the day*) con el texto **Authorized Access Only**. El texto del mensaje distingue entre mayúsculas y minúsculas. Asegúrese de no agregar espacios antes o después del texto del mensaje. Use un carácter delimitante antes y después del texto del mensaje para indicar dónde comienza y finaliza el texto. El carácter delimitante que se utiliza en el ejemplo a continuación es **&,** pero se puede usar cualquier carácter que no se use en el texto del mensaje. Después de haber configurado el MOTD, desconéctese del switch para verificar que el mensaje se muestra al volver a iniciar sesión.

```
S1(config)#banner motd &Authorized Access Only&
S1(config)#end [or exit]
S1#exit

S1 con0 is now available

Press RETURN to get started.

[Enter]

Authorized Access Only

User Access Verification

Password:
```

- El indicador de contraseña ahora requiere una contraseña para entrar al modo EXEC del usuario. Introduzca la contraseña **cisco**.
- Entre al Modo EXEC privilegiado con la contraseña **class** y regrese al modo de configuración global con el comando **configure terminal**.

```
Password: [cisco] !Nota: la contraseña no se muestra al escribirla.

S1>enable
Password: [class] !Nota: la contraseña no se muestra al escribirla.
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#
```

Paso 7: Verificar los resultados.

El porcentaje final del usuario debe ser del 40%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 2: Configurar la seguridad de los puertos dinámicos

Paso 1: Habilitar VLAN99.

Packet Tracer se abre con la interfaz VLAN 99 en el estado inactivo, que no es como funciona un switch real. Se debe habilitar VLAN 99 con el comando **no shutdown** antes de que la interfaz se active en Packet Tracer.

```
S1(config)#interface vlan 99
S1(config-if)#no shutdown
```

Paso 2: Entrar al modo de configuración de interfaz para FastEthernet 0/18 y habilitar la seguridad de puertos.

Antes de poder configurar otros comandos de seguridad de puertos en la interfaz, se debe habilitar la seguridad de puertos.

```
S1(config-if)#interface fa0/18
S1(config-if)#switchport port-security
```

Observe que no tiene que salir nuevamente del modo de configuración global antes de entrar al modo de configuración de interfaz para fa0/18.

Paso 3: Configurar la cantidad máxima de direcciones MAC.

Para configurar el puerto de modo que obtenga sólo una dirección MAC, establezca el parámetro **maximum** en **1**:

```
S1(config-if)#switchport port-security maximum 1
```

Nota: PT no califica el comando **switchport port-security maximum 1**; no obstante, este comando es fundamental en la configuración de la seguridad de puertos.

Paso 4: Configurar el puerto para agregar la dirección MAC a la configuración en ejecución.

La dirección MAC obtenida en el puerto puede agregarse (“adherirse”) a la configuración en ejecución de ese puerto.

```
S1(config-if)#switchport port-security mac-address sticky
```

Nota: PT no califica el comando **switchport port-security mac-address sticky**; no obstante, este comando es fundamental en la configuración de la seguridad de puertos.

Paso 5: Configurar el puerto para que se desactive automáticamente si se infringe la seguridad del puerto.

Si no se configura el siguiente comando, S1 sólo registrará la infracción en las estadísticas de seguridad del puerto pero no lo desactiva.

```
S1(config-if)#switchport port-security violation shutdown
```

Nota: PT no califica el comando **switchport port-security violation shutdown**; no obstante, este comando es fundamental en la configuración de la seguridad de puertos.

Paso 6: Confirmar que S1 ha obtenido la dirección MAC para PC1.

Haga ping desde PC1 a S1.

Confirme que S1 ahora tiene una entrada de dirección MAC estática para PC1 en la tabla MAC:

```
S1#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  99    0060.5c5b.cd23    STATIC      Fa0/18
```

La dirección MAC está ahora “adherida” a la configuración en ejecución.

```
S1#show running-config
<output omitted>
interface FastEthernet0/18
 switchport access vlan 99
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0060.5C5B.CD23
<output omitted>
S1#
```

Paso 7: Verificar los resultados.

El porcentaje final del usuario debe ser del 70%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 3: Probar la seguridad de los puertos dinámicos

Paso 1: Quitar la conexión entre PC1 y S1 y conectar PC2 a S1.

- Para probar la seguridad de los puertos, elimine la conexión Ethernet entre PC1 y S1. Si se elimina accidentalmente la conexión del cable de consola, simplemente vuelva a conectarlo.
- Conecte PC2 a Fa0/18 en S1. Espere a que la luz de enlace de color ámbar se encienda de color verde y, luego, haga ping de PC2 a S1. El puerto debe desactivarse automáticamente.

Paso 2: Verificar que la seguridad del puerto es el motivo por el que se desactiva el puerto.

Para verificar que la seguridad del puerto haya desactivado el puerto, introduzca el comando **show interface fa0/18**.

```
S1#show interface fa0/18
FastEthernet0/18 is down, line protocol is down (err-disabled)
  Hardware is Lance, address is 0090.213e.5712 (bia 0090.213e.5712)
<output omitted>
```

El protocolo de línea está desactivado a causa de un error (**err**) al aceptar una trama con una dirección MAC diferente que la dirección MAC obtenida, de modo que el software de IOS de Cisco desactivó (**disabled**) el puerto.

También puede verificar una infracción de seguridad mediante el comando **show port-security interface fa0/18**.

```
S1#show port-security interface fa0/18
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
```

```
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 00E0.F7B0.086E:99
Security Violation Count   : 1
```

Observe que el estado de puerto es **secure-shutdown** y el conteo de infracciones de seguridad es **1**.

Paso 3: Restaurar la conexión entre PC1 y S1 y restablecer la seguridad del puerto.

Quite la conexión entre PC2 y S1. Vuelva a conectar PC1 al puerto Fa0/18 en S1.

Observe que el puerto aún está desactivado incluso a pesar de haber vuelto a conectar el equipo PC permitido en el puerto. Un puerto que está desactivado a causa de una infracción de seguridad debe volver a activarse manualmente. Desactive el puerto y luego actívelo con **no shutdown**.

```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface fa0/18
S1(config-if)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to
administratively down
S1(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
S1(config-if)#exit
S1(config)#
```

Paso 4: Probar la conectividad mediante un ping a S1 desde PC1.

El ping desde PC1 a S1 debe ejecutarse correctamente.

El porcentaje final del usuario aún debería ser del 70% al finalizar esta tarea.

Tarea 4: Proteger los puertos sin utilizar

Un método simple que muchos administradores usan para ayudar a garantizar la seguridad de su red ante accesos no autorizados es deshabilitar todos los puertos que no se utilizan en el switch de una red.

Paso 1: Deshabilitar la interfaz Fa0/17 en S1.

Entre al modo de configuración de interfaz para FastEthernet 0/17 y desactive el puerto.

```
S1(config)#interface fa0/17
S1(config-if)#shutdown
```

Paso 2: Probar el puerto mediante la conexión de PC2 a Fa0/17 en S1.

Conecte PC2 a la interfaz Fa0/17 en S1. Observe que las luces de enlace son de color rojo. PC2 no tiene acceso a la red.

Paso 3: Verificar los resultados.

El porcentaje final del usuario debe ser del 100%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Actividad PT 2.5.1: Configuración básica del switch

Topología

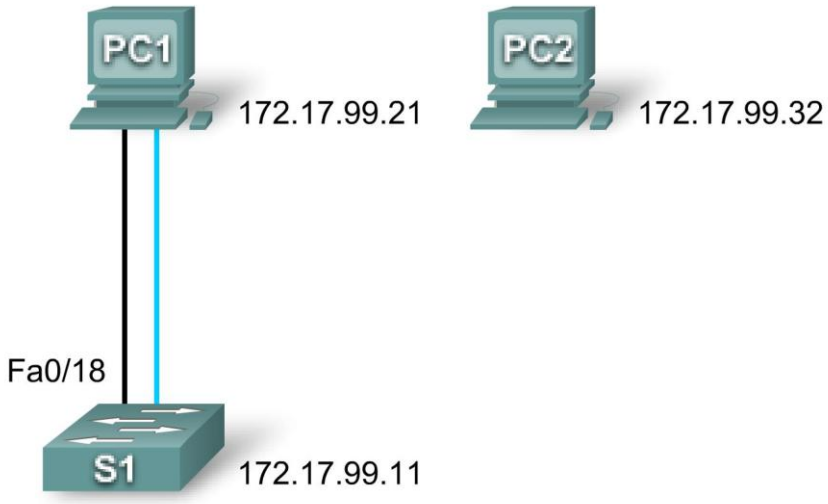


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
PC1	**NIC**	172.17.99.21	255.255.255.0	172.17.99.11
PC2	**NIC**	172.17.99.22	255.255.255.0	172.17.99.11
S1	**VLAN99**	172.17.99.11	255.255.255.0	172.17.99.1

Objetivos de aprendizaje

- Borrar una configuración existente en un switch
- Verificar la configuración por defecto del switch
- Crear una configuración básica de switch
- Administrar la tabla de direcciones MAC
- Configurar la seguridad de puerto

Introducción

En esta actividad, se examinará y configurará un switch LAN independiente. Si bien un switch realiza funciones básicas en su estado por defecto de fábrica, hay una cantidad de parámetros que un administrador de red debe modificar para garantizar una LAN segura y optimizada. En esta actividad se presentan los principios básicos de la configuración de switches.

Tarea 1: Borrar una configuración existente de un switch

Paso 1. Entrar al Modo EXEC privilegiado mediante el comando enable.

Haga clic en S1 y luego en la ficha CLI. Ejecute el comando **enable** para entrar al Modo EXEC privilegiado.

```
Switch>enable
Switch#
```

Paso 2. Quitar el archivo de información de la base de datos de la VLAN.

La información de la base de datos de la VLAN se almacena por separado de los archivos de configuración en vlan.dat de la memoria flash. Para quitar el archivo VLAN, ejecute el comando **delete flash:vlan.dat**

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]? [Enter]
Delete flash:vlan.dat? [confirm] [Enter]
```

Paso 3. Quitar el archivo de configuración de inicio del switch de la NVRAM.

```
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm] [Enter]
[OK]
Erase of nvram: complete
```

Paso 4. Verificar que la información de la VLAN se haya eliminado.

Verifique con el comando **show vlan** que la configuración de la VLAN se haya eliminado.

```
Switch#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
10   VLAN10                            active
30   VLAN30                            active
1002 fddi-default                      active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

La información de la VLAN aún está en el switch. Siga el paso a continuación para borrarla.

Paso 5. Volver a cargar el switch.

En el indicador del Modo EXEC privilegiado, introduzca el comando **reload** para comenzar el proceso.

```
Switch#reload
Proceed with reload? [confirm] [Enter]
```

```
%SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.

<output omitted>

Press RETURN to get started! [Enter]

Switch>
```

Tarea 2: Verificar la configuración por defecto del switch

Paso 1. Entrar al modo privilegiado.

Es posible acceder a todos los comandos del switch en el modo privilegiado. No obstante, dado que muchos de los comandos privilegiados configuran parámetros de funcionamiento, el acceso privilegiado debe estar protegido mediante contraseñas para evitar el uso no autorizado. El conjunto de comandos privilegiados incluye aquellos comandos del Modo EXEC del usuario, así como el comando **configure** a través del cual se obtiene acceso a los modos de comando restantes.

```
Switch>enable
Switch#
```

Observe que el indicador cambió en la configuración para mostrar el Modo EXEC privilegiado.

Paso 2. Examinar la configuración actual del switch.

Examine la configuración en ejecución actual mediante el comando **show running-config**.

¿Cuántas interfaces Fast Ethernet tiene este switch? _____

¿Cuántas interfaces Gigabit Ethernet tiene este switch? _____

¿Cuál es el intervalo de valores que se muestra para las líneas vty? _____

Examine el contenido actual de la NVRAM ejecutando el comando **show startup-config**.

¿Por qué emite esta respuesta el switch?

_____

Analice las características de la interfaz virtual VLAN1 ejecutando el comando **show interface vlan1**.

¿Tiene el switch una dirección IP establecida? _____

¿Cuál es la dirección MAC de esta interfaz de switch virtual? _____

¿Está activada esta interfaz? _____

Ahora consulte las propiedades IP de la interfaz mediante **show ip interface vlan1**.

¿Cuál es el resultado observado? _____

Paso 3. Mostrar información de IOS de Cisco.

Visualice la información de IOS de Cisco mediante el comando **show version**.

¿Cuál es la versión de IOS de Cisco que ejecuta el switch? _____

¿Cuál es el nombre del archivo de imagen del sistema? _____

¿Cuál es la dirección MAC base de este switch? _____

Paso 4. Examinar las interfaces Fast Ethernet.

Examine las propiedades por defecto de la interfaz Fast Ethernet que utiliza PC1 mediante el comando **show interface fastethernet 0/18**.

```
Switch#show interface fastethernet 0/18
```

¿Está activada o desactivada la interfaz? _____

¿Qué puede provocar que se active una interfaz? _____

¿Cuál es la dirección MAC de la interfaz? _____

¿Cuál es la configuración de velocidad y duplex de la interfaz? _____

Paso 5. Examinar la información de la VLAN.

Examine la configuración por defecto de la VLAN del switch mediante el comando **show vlan**.

¿Cuál es el nombre de la VLAN 1? _____

¿Cuáles son los puertos que hay en esta VLAN? _____

¿Está activa la VLAN 1? _____

¿Qué tipo de VLAN es la VLAN por defecto? _____

Paso 6. Analizar la memoria flash.

Hay dos comandos para analizar la memoria flash: **dir flash:** o **show flash**. Ejecute uno de los dos comandos para examinar el contenido del directorio flash.

¿Qué archivos o directorios se encuentran?

_____

Paso 7. Analizar y guardar el archivo de configuración de inicio.

Anteriormente en el paso 2, se observó que el archivo de configuración de inicio no existía. Efectúe un cambio en la configuración del switch y luego guárdelo. Escriba los siguientes comandos:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#exit
S1#
```

Para guardar el contenido del archivo de configuración en ejecución en la RAM no volátil (NVRAM), ejecute el comando **copy running-config startup-config.**

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

Ahora consulte el contenido de la NVRAM. La configuración actual se ha escrito en la NVRAM.

Tarea 3: Crear una configuración básica de switch

Paso 1. Asignar un nombre al switch.

Entre al modo de configuración global. El modo de configuración permite administrar el switch. Introduzca los comandos de configuración, uno en cada línea. Observe que el indicador de línea de comando cambia para mostrar el indicador actual y el nombre del switch. En el último paso de la tarea anterior, se configuró el nombre de host. a continuación se incluye un repaso de los comandos usados.

```
S1#configure terminal
S1(config)#hostname S1
S1(config)#exit
```

Paso 2. Configurar las contraseñas de acceso.

Entre al modo de configuración de línea para la consola. Establezca **cisco** como la contraseña de inicio de sesión. También configure las líneas vty 0 a 15 con la contraseña **cisco**.

```
S1#configure terminal
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```

¿Por qué se requiere el comando **login**? _____

Paso 3. Configurar las contraseñas de modo de comando.

Establezca class como la contraseña secreta de enable.

```
S1(config)#enable secret class
```

Paso 4. Configurar la dirección de capa 3 del switch.

Establezca la dirección IP del switch en 172.17.99.11 con una máscara de subred de 255.255.255.0 en la interfaz virtual interna VLAN 99. La VLAN debe primero crearse en el switch antes de que pueda asignarse la dirección.

```
S1(config)#vlan 99
S1(config-vlan)#exit
S1(config)#interface vlan99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
```

Paso 5. Asignar puertos a la VLAN del switch.

Asigne Fastethernet 0/1, 0/8, y 0/18 a puertos a la VLAN 99.

```
S1(config)#interface fa0/1
S1(config-if)#switchport access vlan 99
S1(config-if)#exit
```

Paso 6. Establecer la gateway por defecto del switch.

S1 es un switch de capa 2, de modo que toma las decisiones de reenvío en función del encabezado de capa 2. Si hay varias redes conectadas a un switch, se debe especificar el modo en que el switch

reenviará las tramas internetwork, dado que la ruta debe determinarse en la capa tres. Para ello, se especifica una dirección de gateway por defecto que apunta a un router o switch de capa 3. Si bien esta actividad no incluye una gateway IP externa, se deben suponer que tarde o temprano la LAN se conectará a un router para acceso externo. Suponiendo que la interfaz LAN en el router es 172.17.99.1, defina la gateway por defecto para el switch.

```
S1(config)#ip default-gateway 172.17.99.1
S1(config)#exit
```

Paso 7. Verificar la configuración de administración de las LAN.

Verifique la configuración de interfaz de la VLAN 99 mediante el comando **show interface vlan 99**.

```
S1#show interface vlan 99
Vlan99 is up, line protocol is up
  Hardware is CPU Interface, address is 0060.47ac.1eb8 (bia 0060.47ac.1eb8)
  Internet address is 172.17.99.11/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
<Output Omitted>
```

¿Cuál es el ancho de banda en esta interfaz? _____

¿Cuál es la estrategia de colas? _____

Paso 8. Configurar la dirección IP y la gateway por defecto para PC1.

Establezca la dirección IP de PC1 en 172.17.99.21, con una máscara de subred de 255.255.255.0. Configure una gateway por defecto de 172.17.99.11. Haga clic en PC1 y en su ficha Desktop, luego, en IP Configuration para introducir los parámetros de direccionamiento.

Paso 9. Verificar la conectividad.

Para verificar que los hosts y los switches estén configurados correctamente, haga ping al switch desde PC1.

Si el ping no tuviera éxito, realice la resolución de problemas en la configuración del switch y del host. Observe que quizás será necesario hacer varios intentos hasta que los pings se realicen correctamente.

Paso 10. Configurar la velocidad y duplex del puerto para una interfaz Fast Ethernet.

Establezca la configuración de duplex y velocidad en Fast Ethernet 0/18. Use el comando **end** para regresar al Modo EXEC privilegiado al finalizar.

```
S1#configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#speed 100
S1(config-if)#duplex full
S1(config-if)#end
```

La configuración por defecto de la interfaz Ethernet del switch es de auto-detección, de modo que negocia automáticamente la configuración óptima. El duplex y la velocidad se deben establecer manualmente únicamente si un puerto debe funcionar a una velocidad y un modo duplex en particular. La configuración manual de los puertos puede dar lugar a incoherencias de duplex, lo que puede disminuir considerablemente el rendimiento.

Observe cómo el enlace entre PC1 y S1 se desactivó. Quite los comandos **speed 100** y **duplex full**. Ahora verifique la configuración de la interfaz Fast Ethernet mediante el comando **show interface fa0/18**.

```
S1#show interface fastethernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Lance, address is 0060.5c36.4412 (bia 0060.5c36.4412)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
<Output omitted>
```

Paso 11. Guardar la configuración.

Se ha finalizado la configuración básica del switch. Ahora se debe crear una copia de seguridad de la configuración en ejecución en la NVRAM para garantizar que los cambios realizados no se perderán si el sistema se reinicia o se produce una interrupción eléctrica.

```
S1#copy running-config startup-config

Destination filename [startup-config]?[Enter]
Building configuration...
[OK]
S1#
```

Paso 12. Examinar el archivo de configuración de inicio.

Para ver la configuración que se guarda en la NVRAM, ejecute el comando **show startup-config** en el Modo EXEC privilegiado (modo enable).

¿Todos los cambios realizados están grabados en el archivo?

Tarea 4: Administrar la tabla de direcciones MAC

Paso 1. Tomar nota de las direcciones MAC de los hosts.

Determine y anote las direcciones de capa 2 (físicas) de las tarjetas de interfaz de red del equipo PC mediante los siguientes pasos:

- Haga clic en el equipo PC.
- Seleccione la ficha Desktop.
- Haga clic en Command Prompt.
- Escriba **ipconfig /all**.

Paso 2. Determinar las direcciones MAC que ha obtenido el switch.

Muestre las direcciones MAC mediante el comando **show mac-address-table** en el Modo EXEC privilegiado. Si no hay direcciones MAC; haga ping desde PC1 a S1, y luego verifique nuevamente.

```
S1#show mac-address-table
```

Paso 3. Borrar la tabla de direcciones MAC.

Para quitar las direcciones MAC existentes, use el comando **clear mac-address-table dynamic** desde el Modo EXEC privilegiado.

```
S1#clear mac-address-table dynamic
```

Paso 4. Verificar los resultados.

Verifique que la tabla de direcciones MAC se haya borrado.

```
S1#show mac-address-table
```

Paso 5. Examinar nuevamente la tabla de direcciones MAC.
Observe la tabla de direcciones MAC nuevamente en el Modo EXEC privilegiado. La tabla no se ha modificado, haga ping a S1 desde PC1 y verifique nuevamente.

Paso 6. Configurar una dirección MAC estática.

Para especificar los puertos a los que se puede conectar un host, una opción es crear una asignación estática de la dirección MAC del host a un puerto.

Configure una dirección MAC estática en la interfaz Fast Ethernet 0/18 utilizando la dirección que se registró para PC1 en el paso 1 de esta tarea, 0002.16E8.C285.

```
S1(config)#mac-address-table static 0002.16E8.C285 vlan 99 interface
fastethernet 0/18
```

Paso 7. Verificar los resultados.

Verifique las entradas de la tabla de direcciones MAC.

```
S1#show mac-address-table
```

Paso 8. Quitar la entrada MAC estática.

Entre al modo de configuración y quite la MAC estática colocando un **no** al principio de la cadena de comandos.

```
S1(config)#no mac-address-table static 0002.16E8.C285 vlan 99 interface
fastethernet 0/18
```

Paso 9. Verificar los resultados.

Verifique que la dirección MAC estática se haya borrado mediante el comando **show mac-address-table static**.

Tarea 5: Configuración de la seguridad de puertos

Paso 1. Configurar un segundo host.

Se necesita un segundo host para esta tarea. Establezca la dirección IP de PC2 en 172.17.99.22, con una máscara de subred de 255.255.255.0 y una gateway por defecto de 172.17.99.11. No conecte aún este equipo PC al switch.

Paso 2. Verificar la conectividad.

Verifique que PC1 y el switch aún estén configurados correctamente. Para ello, haga ping a la dirección IP de la VLAN 99 del switch desde el host. Si los pings no tuvieran éxito, realice la resolución de problemas en la configuración del switch y del host.

Paso 3. Determinar las direcciones MAC que ha obtenido el switch.

Muestre las direcciones MAC obtenidas mediante el comando **show mac-address-table** en el Modo EXEC privilegiado.

Paso 4. Enumerar las opciones de seguridad de puerto.

Explore las opciones para configurar la seguridad del puerto en la interfaz Fast Ethernet 0/18.

```
S1# configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#switchport port-security ?
  mac-address  Secure mac address
  maximum      Max secure addresses
  violation    Security violation mode
  <cr>
```

Paso 5. Configurar la seguridad del puerto en un puerto de acceso.

Configure el puerto Fast Ethernet 0/18 del switch para que acepte sólo dos dispositivos, para que aprenda las direcciones MAC de esos dispositivos de forma dinámica y para que desactive el puerto si se detecta una infracción.

```
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 2
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#switchport port-security violation shutdown
S1(config-if)#exit
```

Paso 6. Verificar los resultados.

Muestre la configuración de seguridad del puerto mediante el comando **show port-security interface fa0/18**.

¿Cuántas direcciones seguras están permitidas en Fast Ethernet 0/18?
¿Cuál es la acción de seguridad para este puerto?

Paso 7. Examinar el archivo de configuración en ejecución.

```
S1#show running-config
```

¿Hay sentencias en el listado que reflejan directamente la implementación de seguridad de la configuración en ejecución?

Paso 8. Modificar la configuración de seguridad del puerto en un puerto.

En la interfaz Fast Ethernet 0/18, cambie el conteo máximo de direcciones MAC de seguridad del puerto a 1.

```
S1(config-if)#switchport port-security maximum 1
```

Paso 9. Verificar los resultados.

Muestre la configuración de seguridad del puerto mediante el comando **show port-security interface fa0/18**.

¿Ha cambiado la configuración de seguridad del puerto para reflejar las modificaciones del paso 8?

Haga ping a la dirección de la VLAN 99 del switch desde PC1 para verificar la conectividad y actualizar la tabla de direcciones MAC.

Paso 10. Introducir un host no autorizado ni permitido.

Desconecte el equipo PC conectado a Fast Ethernet 0/18 desde el switch. Conecte PC2, que tiene asignado la dirección IP 172.17.99.22, al puerto Fast Ethernet 0/18. Haga ping a la dirección 172.17.99.11 de la VLAN 99 desde el nuevo host.

¿Qué sucedió al intentar hacer ping a S1?

Nota: La convergencia puede demorar hasta un minuto. Alterne entre los modos de simulación y tiempo real para acelerar la convergencia.

Paso 11. Reactivar el puerto.

Siempre y cuando el host no autorizado ni permitido esté conectado a Fast Ethernet 0/18, no pasará ningún tráfico entre el host y el switch. Vuelva a conectar PC1 a Fast Ethernet 0/18 e introduzca los siguientes comandos en el switch para reactivar el puerto.

```
S1#configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#no shutdown
S1(config-if)#exit
```

Paso 12. Verificar la conectividad.

Después de la convergencia, PC1 debe poder hacer ping nuevamente a S1.

Actividad PT 2.6.1: Reto de habilidades de Integración de Packet Tracer

Diagrama de topología

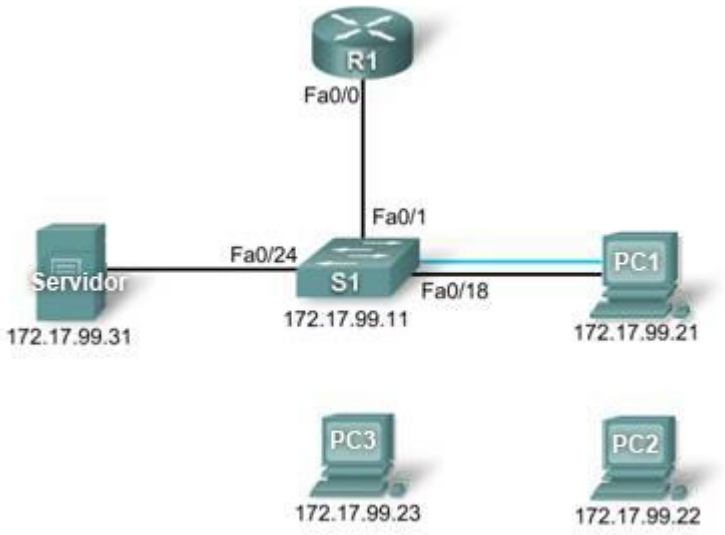


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	**Fa0/0**	172.17.99.1	255.255.255.0
S1	**Fa0/1**	172.17.99.11	255.255.255.0
PC1	**NIC**	172.17.99.21	255.255.255.0
PC2	**NIC**	172.17.99.22	255.255.255.0
Server	**NIC**	172.17.99.31	255.255.255.0

Objetivos

- Establecer una conexión de consola a un switch
- Configurar el nombre de host y la VLAN99
- Configurar el reloj
- Modificar el búfer del historial
- Configurar las contraseñas y el acceso de consola/Telnet
- Configurar los mensajes de inicio de sesión
- Configurar el router
- Configurar la secuencia de arranque

- Solucionar la falta de concordancia de duplex y velocidad
- Administrar la tabla de direcciones MAC
- Configurar la seguridad de puerto
- Proteger los puertos sin utilizar
- Administrar el archivo de configuración del switch

Introducción

En esta actividad, Reto de habilidades de Integración de Packet Tracer, se configurará la administración básica del switch, incluidos los comandos de mantenimiento general, las contraseñas y la seguridad del puerto. En esta actividad se proporciona una oportunidad de revisar las habilidades adquiridas anteriormente.

Tarea 1: Establecer una conexión de consola a un switch

Paso 1: Conectar un cable de consola a S1.

Para esta actividad, el acceso directo a las fichas S1 Config y CLI está deshabilitado. Se debe establecer una sesión de consola a través de PC1. Conecte un cable de consola desde PC1 a S1.

Paso 2: Establecer una sesión de terminal.

Desde PC1, abra una ventana de terminal y use la configuración de terminal por defecto. Ahora se debe poder acceder a la CLI para S1.

Paso 3: Verificar los resultados.

El porcentaje final del usuario debe ser del 6%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 2: Configurar el nombre de host y la VLAN 99

Paso 1: Configurar el nombre de host del switch como S1.

Paso 2: Configurar el puerto Fa0/1 y la interfaz VLAN 99.

Asigne VLAN 99 a FastEthernet 0/1 y establezca el modo en modo de acceso. Estos comandos se explican más adelante en el próximo capítulo.

```
S1(config)#interface fastethernet 0/1
S1(config-if)#switchport access vlan 99
S1(config-if)#switchport mode access
```

Configure la conectividad IP en S1 usando VLAN 99.

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

Paso 3: Configurar la gateway predeterminada para S1.

Configure la gateway predeterminada y luego pruebe la conectividad. S1 debe poder hacer ping a R1.

Paso 4: Verificar los resultados.

El porcentaje final del usuario debe ser del 26%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron. Además, asegúrese de que la interfaz VLAN 99 está activa.

Tarea 3: Configurar el reloj usando la ayuda

Paso 1: Configurar el reloj según la hora actual.

En el indicador EXEC privilegiado, escriba **clock ?** Use la ayuda para descubrir cada paso adicional necesario para configurar la hora actual. Packet Tracer no califica este comando, de modo que el porcentaje final no se modifica.

Paso 2: Verificar que el reloj esté configurado según la hora actual.

Use el comando **show clock** para verificar que el reloj esté ahora configurado según la hora actual. Puede que Packet Tracer no simule correctamente la hora introducida.

Tarea 4: Modificar el búfer del historial

Paso 1: Establecer el búfer del historial en 50 para la línea de consola.

Paso 2: Establecer el búfer del historial en 50 para las líneas vty.

Paso 3: Verificar los resultados.

El porcentaje final del usuario debe ser del 32%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 5: Configurar las contraseñas y el acceso de consola/Telnet

Paso 1: Configurar la contraseña de EXEC privilegiado.

Use la forma encriptada de la contraseña del Modo EXEC privilegiado y establezca **class** como contraseña.

Paso 2: Configurar las contraseñas para la consola y para Telnet.

Establezca **cisco** como contraseña para la consola y vty, y solicite a los usuarios que inicien sesión.

Paso 3: Encriptar contraseñas.

Consulte la configuración actual en S1. Observe que las contraseñas de línea se muestran en texto sin encriptar. Introduzca el comando para encriptar estas contraseñas.

Paso 4: Verificar los resultados.

El porcentaje final del usuario debe ser del 41%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 6: Configurar el mensaje de inicio de sesión

Si no se introduce el texto del mensaje exactamente según se especifica, Packet Tracer no calificará el comando correctamente. Estos comandos distinguen entre mayúsculas y minúsculas. Además, asegúrese de no agregar espacios antes o después del texto.

Paso 1: Configurar el título de mensaje del día en S1.

Configure el mensaje del día como **Authorized Access Only**.

Paso 2: Verificar los resultados.

El porcentaje final del usuario debe ser del 44%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 7: Configurar el router

Paso 1: Configurar el router con los mismos comandos básicos que se usaron en S1.

Los routers y switches comparten muchos de los mismos comandos. Acceda a la CLI para R1 haciendo clic en el dispositivo. En R1, haga lo siguiente:

- Configure el nombre de host.
- Establezca el búfer del historial en 50 para la consola y vty.
- Configure la forma encriptada de la contraseña del Modo EXEC privilegiado y establezca **class** como contraseña.
- Establezca **cisco** como contraseña para la consola y vty, y solicite a los usuarios que inicien sesión.
- Encripte las contraseñas de la consola y vty.
- Configure el mensaje del día como **Authorized Access Only**.

Paso 2: Verificar los resultados.

El porcentaje final del usuario debe ser del 65%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 8: Configurar la secuencia de arranque

Paso 1: Ver los archivos actuales almacenados en flash.

En S1, introduzca el comando **show flash**. Se deberían ver los siguientes archivos en la lista:

```
S1#show flash
Directory of flash:/

    1  -rw-     4414921          <no date>  c2960-lanbase-mz.122-25.FX.bin
    3  -rw-     4670455          <no date>  c2960-lanbase-mz.122-25.SEE1.bin
    2  -rw-         616          <no date>  vlan.dat

32514048 bytes total (23428056 bytes free)
```

Paso 2: Configurar S1 para que se arranque mediante la segunda imagen de la lista.

Asegúrese de que el comando incluya el sistema de archivos, que es **flash.**

Nota: Packet Tracer no muestra este comando en la configuración en ejecución. Además, si se vuelve a cargar el switch, Packet Tracer no carga la imagen especificada.

Paso 3: Verificar los resultados.

El porcentaje final del usuario debe ser del 68%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 9: Solucionar una falta de concordancia entre duplex y velocidad

Paso 1: Cambiar el duplex y la velocidad en S1.

PC1 y Servidor no tienen actualmente acceso a través de S1 debido a una falta de concordancia entre duplex y velocidad. Introduzca los comandos en S1 para solucionar este problema.

Paso 2: Verificar la conectividad.

PC1 y Servidor deben ahora poder hacer ping a S1, R1 y entre sí.

Paso 3: Verificar los resultados.

El porcentaje final del usuario debe ser del 74%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 10: Administrar la tabla de direcciones MAC

Paso 1: Ver la tabla de direcciones MAC actual.

¿Qué comando se usa para mostrar la tabla de direcciones MAC?

```
S1#_____________________________________
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  99    0001.637b.b267    DYNAMIC     Fa0/24
  99    0004.9a32.8e01    DYNAMIC     Fa0/1
  99    0060.3ee6.1659    DYNAMIC     Fa0/18
```

La lista de direcciones MAC que se muestra puede ser diferente según el tiempo transcurrido desde que se enviaron los paquetes a través del switch.

Paso 2: Configurar una dirección MAC estática.

La política de red puede indicar que todas las direcciones de los servidores se configuren de manera estática. Introduzca el comando para configurar de manera estática la dirección MAC del servidor.

Paso 3: Verificar los resultados.

El porcentaje final del usuario debe ser del 76%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 11: Configurar la seguridad de puerto

Paso 1: Configurar la seguridad de puerto para PC1.

Use la siguiente política para establecer la seguridad de puerto en el puerto que usa PC1.

- Habilitar la seguridad del puerto
- Permitir sólo una dirección MAC
- Configurar la primera dirección MAC aprendida para “adherirla” a la configuración
- Configurar el puerto para que se desconecte si se produce una infracción de seguridad.

Nota: Sólo el paso en que se habilita la seguridad del puerto es calificado por Packet Tracer e incorporado en el porcentaje final. No obstante, todas las tareas relativas a la seguridad de puertos anteriores son obligatorias para completar esta actividad correctamente.

Paso 2: Verificar la seguridad del puerto.

Verifique que la seguridad del puerto esté habilitada para Fa0/18. La información que se obtiene debe asemejarse a la siguiente. Observe que S1 aún no ha aprendido una dirección MAC para esta interfaz.

¿Qué comando generó la siguiente información?

```
S1#_____________________________________
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Paso 3: Hacer que S1 aprenda la dirección MAC para PC1.

Envíe un ping de PC1 a S1. a continuación, verifique que S1 ha agregado la dirección MAC para PC1 a la configuración en ejecución.

```
!
interface FastEthernet0/18
 <output omitted>
 switchport port-security mac-address sticky 0060.3EE6.1659
 <output omitted>
!
```

Paso 4: Probar la seguridad del puerto.

Quite la conexión FastEthernet entre S1 y PC1. Conecte PC2 a Fa0/18. Espere hasta que las luces de enlace se enciendan en color verde. Si fuera necesario, envíe un ping de PC1 a S1 para desactivar el puerto. La seguridad del puerto debe mostrar los siguientes resultados:

```
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 00D0.BAD6.5193:99
Security Violation Count   : 1
```

La visualización de la interfaz Fa0/18 muestra **line protocol is down (err-disabled)**, lo que también indica una infracción de seguridad.

```
S1#show interface fa0/18
FastEthernet0/18 is down, line protocol is down (err-disabled)
<output omitted>
```

Paso 5: Volver a conectar PC1 y volver a habilitar el puerto.

Para volver a habilitar el puerto, desconecte PC2 de Fa0/18 y vuelva a conectar PC1. La interfaz Fa0/18 debe configurarse manualmente antes de regresar al estado activo.

Paso 6: Verificar los resultados.

El porcentaje final del usuario debe ser del 82%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 12: Proteger los puertos sin utilizar

Paso 1: Deshabilitar todos los puertos sin utilizar en S1.

Deshabilite todos los puertos que no se usan actualmente en S1. Packet Tracer califica el estado de los siguientes puertos. Fa0/2, Fa0/3, Fa0/4, Gig 1/1 y Gig 1/2.

Paso 2: Verificar los resultados.

El porcentaje final del usuario debe ser del 97%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 13: Administrar el archivo de configuración del switch

Paso 1: Guardar la configuración actual en la NVRAM para R1.

Paso 2: Realizar una copia de respaldo de los archivos de configuración de inicio para S1 y R1 en el servidor.

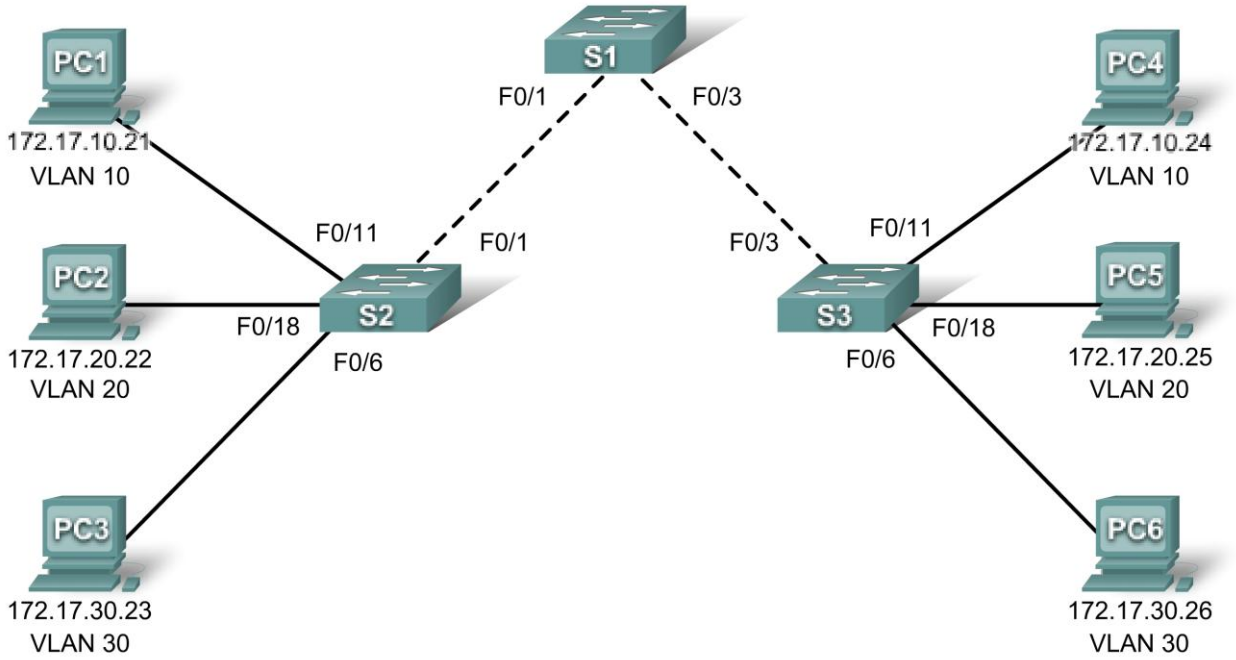
Realice una copia de respaldo de los archivos de configuración de inicio en S1 y R1 subiéndolos al servidor. Una vez finalizado, verifique que el servidor tenga los archivos **R1-confg** y **S1-confg**.

Paso 3: Verificar los resultados.

El porcentaje final del usuario debe ser del 100%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Actividad PT 3.1.4: Investigación de la implementación de una VLAN

Diagrama de topología



Objetivos de aprendizaje

- Observar el tráfico de broadcast en una implementación de VLAN
- Observar el tráfico de broadcast sin VLAN

Introducción

Esta actividad se abre con un porcentaje final del 100%. El objetivo de esta actividad es observar cómo los switches envían el tráfico de broadcast cuando las VLAN están configuradas y cuando no lo están.

Tarea 1: Observar el tráfico de broadcast en una implementación de VLAN

Paso 1: Hacer ping de PC1 a PC6.

Espere hasta que todas las luces de enlace se enciendan en verde. Para acelerar este proceso, alterne una y otra vez entre los modos de simulación y de tiempo real.

Use la herramienta **Add Simple PDU**. Haga clic en PC1 y luego en PC6. Haga clic en el botón **Capture/Forward** para continuar con el proceso. Observe las solicitudes de ARP a medida que atraviesan la red.

En condiciones de funcionamiento normales, cuando un switch recibe una trama de broadcast en uno de sus puertos, reenvía la trama desde todos los otros puertos. Tenga en cuenta que S2 sólo envía la solicitud de ARP de Fa0/1 a S1. Además, observe que S3 sólo envía la solicitud de ARP de Fa0/11 a PC4. PC1 y PC4 pertenecen a VLAN 10. PC6 pertenece a VLAN 30. Dado que el tráfico de broadcast

está dentro de la VLAN, PC6 nunca recibe la solicitud de ARP desde PC1. Asimismo, debido a que PC4 no es el destino, descarta la solicitud de ARP. El ping desde PC1 no se realiza correctamente, ya que PC1 nunca recibe una respuesta ARP.

Paso 2. Hacer ping de PC1 a PC4.

Use la herramienta **Add Simple PDU**. Haga clic en PC1 y luego en PC4. Observe las solicitudes de ARP a medida que atraviesan la red. PC1 y PC4 pertenecen a VLAN 10, de modo que la ruta de la solicitud de ARP es la misma que antes. Dado que PC4 es el destino, responde a la solicitud de ARP. PC1 puede entonces enviar el ping con la dirección MAC destino para PC4.

Tarea 2: Observar el tráfico de broadcast sin VLAN

Paso 1. Borrar las configuraciones de los tres switches y eliminar la base de datos de la VLAN.

En los tres switches, entre al Modo EXEC del usuario con la contraseña **cisco**. a continuación, entre al Modo EXEC privilegiado con la contraseña **class**.

Para observar el tráfico de broadcast sin VLAN, borre la configuración y elimine la base de datos de la VLAN en cada switch. Los comandos para S1 se muestran a continuación.

```
S1#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
S1#delete vlan.dat
Delete filename [vlan.dat]? Enter
Delete flash:/vlan.dat? [confirm]Enter
```

Paso 2. Volver a cargar los switches.

```
S1#reload
Proceed with reload? [confirm]Enter
```

Espere hasta que todas las luces de enlace vuelvan a encenderse en verde. Para acelerar este proceso, alterne una y otra vez entre los modos de simulación y de tiempo real.

Paso 3. Haga clic en Capture/Forward para enviar la solicitud de ARP y pings.

Después de que se vuelvan a cargar los switches y de que las luces de enlace vuelvan a encenderse en verde, la red estará lista para reenviar el tráfico ARP y ping. Haga clic en el botón **Capture/Forward** para continuar con el proceso. Observe que los switches ahora reenvían las solicitudes de ARP a todos los puertos, excepto al puerto en el que se recibió la solicitud de ARP. Esta acción por defecto de los switches es el motivo por el que las VLAN pueden mejorar el rendimiento de la red. El tráfico de broadcast está dentro de cada VLAN.

Tenga en cuenta que el ping de PC1 a PC6 aún falla. ¿Por qué? ¿Qué se requiere para que este ping se realice correctamente?

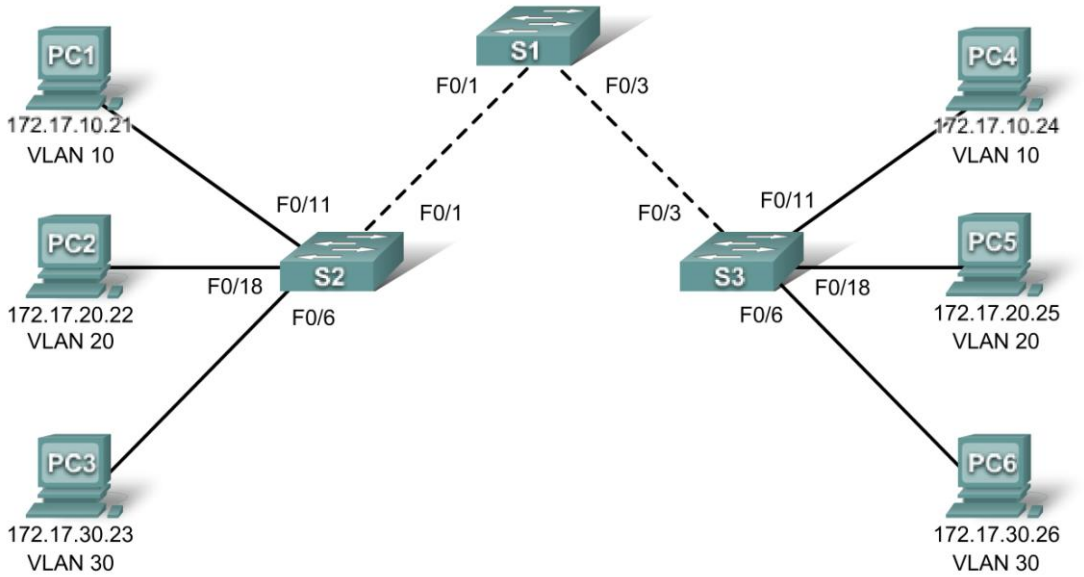
_____

_____

_____

Actividad PT 3.2.3: Investigación de los enlaces troncales de la VLAN

Diagrama de topología



Objetivos de aprendizaje

- Activar la interfaz VLAN 99
- Visualizar la configuración del switch
- Investigar la etiqueta de la VLAN en el encabezado de la trama.

Introducción

Los enlaces troncales transmiten el tráfico de varias VLAN a través de un único enlace, lo que los convierte en un elemento fundamental de la comunicación entre los switches y las VLAN. Esta actividad se abre con un porcentaje final de 100% y se centra en la visualización de la configuración del switch, la configuración del enlace troncal y la información del etiquetado de la VLAN.

Tarea 1: Visualizar la configuración del switch

En S1, entre al Modo EXEC del usuario con la contraseña **cisco**. a continuación, entre al Modo EXEC privilegiado con la contraseña **class**. En el indicador EXEC privilegiado, ejecute el comando **show running-config.**

```
S1#show running-config
```

Al visualizar la configuración en ejecución, observe qué interfaces están configuradas en el enlace troncal. Se verá el comando **switchport mode trunk** en esas interfaces.

¿Qué interfaces están configuradas actualmente en el enlace troncal?

_____

_____

El comando **switchport trunk native vlan 99** también se indica debajo de varias interfaces. Este comando se usa para configurar la VLAN nativa para el enlace troncal. En este caso, VLAN 99 es la VLAN nativa.

Tarea 2: Investigar la etiqueta de la VLAN en el encabezado de la trama

Paso 1. Hacer ping de PC1 a PC4.

Si las luces de enlace aún están de color ámbar, alterne una y otra vez entre los modos de tiempo real y simulación hasta que las luces de enlace se enciendan en verde.

Use la herramienta **Add Simple PDU**. Haga clic en PC1 y luego en PC4.

Paso 2. Hacer clic en Capture/Forward para observar el ping.

Dado que PC1 y PC4 están en la misma VLAN y red de capa 3, PC4 envía una respuesta de ARP a PC1. PC1 luego envía un ping a PC4. Por último, PC4 responde al ping. Haga clic en **View Previous Events** cuando se le solicite.

Paso 3. Investigar los detalles de PDU en uno de los switches.

Desplácese hasta la parte superior de la lista de eventos. En la columna **Info**, haga clic en el cuadro de color para el evento de S2 a S1. a continuación, haga clic en la ficha **Inbound PDU Details**. Observe los dos campos debajo de la dirección MAC de origen. ¿Cuáles son los objetivos de estos dos campos?

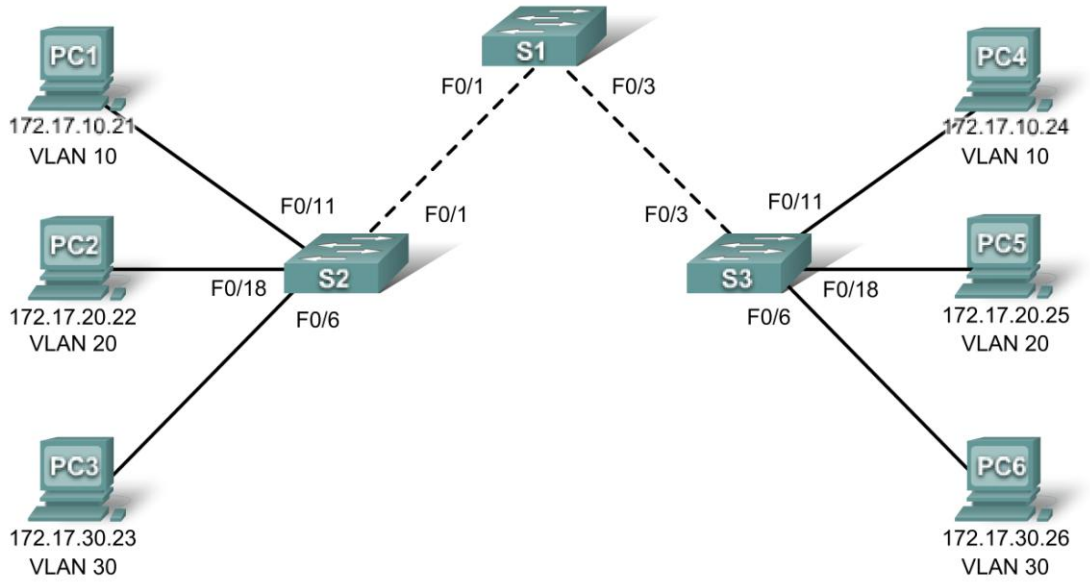
_____

_____

_____

Actividad PT 3.3.4: Configuración de las VLAN y de los enlaces troncales

Diagrama de topología



Objetivos de aprendizaje

- Visualizar la configuración predeterminada de la VLAN
- Configurar las VLAN
- Asignar VLAN a puertos
- Configurar enlaces troncales

Introducción

Las VLAN son útiles en la administración de grupos lógicos, ya que permiten agregar miembros a un grupo, moverlos o cambiarlos de grupo con facilidad. Esta actividad se centra en la creación y asignación de nombres de VLAN, la asignación de puertos de acceso a VLAN específicas, el cambio de la VLAN nativa y la configuración de enlaces troncales.

Tarea 1: Visualizar la configuración por defecto de la VLAN

Paso 1. Verificar la configuración en ejecución actual de los switches.

En los tres switches, entre al Modo EXEC del usuario con la contraseña **cisco**. a continuación, entre al Modo EXEC privilegiado con la contraseña **class**.

Desde el Modo EXEC privilegiado en los tres switches, ejecute el comando **show running-config** para verificar la configuración en ejecución actual. Las configuraciones básicas ya están establecidas, pero no hay asignaciones de VLAN.

Paso 2. Mostrar las VLAN actuales.

En S1, ejecute el comando **show vlan**. Las únicas VLAN presentes son las configuradas por defecto. Por defecto, todas las interfaces están asignadas a VLAN 1.

Paso 3. Verificar la conectividad entre los equipos PC de una misma red.

Observe que cada equipo PC puede hacer ping al otro equipo PC que comparte la misma red:

- PC1 puede hacer ping a PC4
- PC2 puede hacer ping a PC5
- PC3 puede hacer ping a PC6

Los pings a los equipos PC de otras redes fallan.

¿Qué ventajas ofrece la configuración de las VLAN a la configuración actual?

_____

_____

_____

Tarea 2: Configurar las VLAN

Paso 1. Crear VLAN en S1.

El comando **vlan** *vlan-id* crea una VLAN. Use el comando **name** *vlan-name* para asignar un nombre a una VLAN.

En S1, cree cuatro VLAN usando los *vlan-ids* y los nombres que se muestran a continuación:

```
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(Default)
S1(config-vlan)#vlan 99
S1(config-vlan)#name Management&Native
```

Paso 2. Verificar la configuración de la VLAN.

Después de crear las VLAN, regrese a EXEC privilegiado y ejecute el comando **show vlan brief** para verificar la creación de las nuevas VLAN.

```
S1#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
                                                 Gig1/1, Gig1/2
10   Faculty/Staff                     active
20   Students                          active
30   Guest(Default)                    active
99   Management&Native                 active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S1#
```

Paso 3. Cree las VLAN en S2 y S3.

En S2 y S3, use los mismos comandos que usó en S1 para crear las VLAN y asignarles nombres.

Paso 4. Verificar la configuración de la VLAN.

Use el comando **show vlan brief** para verificar que todas las VLAN están configuradas y tienen nombre.

Paso 5. Verificar los resultados.

El porcentaje final del usuario debe ser del 38%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 3: Asignar VLAN a puertos

El comando **range** reduce en gran medida la cantidad de comandos repetitivos que se deben introducir al configurar los mismos comandos en varios puertos. No obstante, Packet Tracer no admite el comando **range**. Por lo tanto, sólo se califican las interfaces activas para el comando **switchport mode access**.

Paso 1. Asignar VLAN a los puertos activos en S2.

El comando **switchport mode access** configura la interfaz como un puerto de acceso. El comando **switchport access vlan** *vlan-id* asigna una VLAN al puerto. Se puede asignar sólo una VLAN de acceso a cada puerto de acceso. Introduzca los siguientes comandos en S2.

```
S2(config)#interface fastEthernet 0/6
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 30
S2(config-if)#interface fastEthernet 0/11
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#interface fastEthernet 0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20
```

Paso 2. Asignar VLAN a los puertos activos en S3.

Asigne VLAN a los puertos activos en S3. S3 usa las mismas asignaciones de puerto de acceso VLAN que se configuraron en S2.

Paso 3. Verificar la pérdida de conectividad.

Anteriormente, los equipos PC que compartían la misma red podían hacer ping entre sí correctamente. Intente hacer ping entre PC1 y PC4. Si bien los puertos de acceso están asignados a las VLAN adecuadas, el ping falla. ¿Por qué?

_____

_____

_____

Paso 4. Verificar los resultados.

El porcentaje final del usuario debe ser del 75%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 4: Configurar enlaces troncales

Paso 1. Configurar S1 Fa0/1 y Fa0/3 para enlaces troncales y para usar VLAN 99 como la VLAN nativa.

```
S1(config)#interface FastEthernet 0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#interface FastEthernet 0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
```

El puerto de enlace troncal demora aproximadamente un minuto para activarse nuevamente. Puede alternar entre los modos de tiempo real y de simulación tres o cuatro veces para activar rápidamente el puerto otra vez.

A continuación, los puertos en S2 y S3 que se conectan a S1 se vuelven inactivos. Nuevamente, puede alternar entre los modos de tiempo real y de simulación tres o cuatro veces para activar rápidamente los puertos otra vez.

Una vez que los puertos estén activos, recibirá periódicamente los siguientes mensajes syslog:

```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/1 (99), with S2 FastEthernet0/1 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/3 (99), with S3 FastEthernet0/3 (1).
```

Se ha configurado la VLAN nativa en S1 como VLAN 99. No obstante, la VLAN nativa en S2 y S3 está configurada en la VLAN 1 por defecto.

Paso 2. Verificar la conectividad entre los dispositivos de la misma VLAN.

Si bien actualmente hay una falta de concordancia de VLAN nativa, los pings entre los equipos PC de la misma VLAN ahora se realizan correctamente. ¿Por qué?

_____

_____

_____

Paso 3. Verificar que los enlaces troncales estén habilitados en S2 y configurar VLAN 99 como la VLAN nativa.

El Protocolo de enlace troncal dinámico (DTP, *Dynamic Trunking Protocol*) ha habilitado automáticamente el puerto Fast Ethernet 0/1 en S2 para los enlaces troncales. Una vez que configure el modo de enlaces troncales en S1, los mensajes de DTP enviados de S1 a S2 indicarán automáticamente a S1 que cambie el estado de Fa0/1 a enlaces troncales. Esto puede verificarse con el siguiente comando en S1:

```
S2#show interface fastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
<output omitted>
S2#
```

Observe que el modo administrativo está establecido en **dynamic auto**. Éste es el estado por defecto de todos los puertos en los switches IOS de Cisco. No obstante, DTP ha negociado los enlaces troncales, por lo que el modo de funcionamiento es **trunk**. Esto dará como resultado una falta de concordancia de VLAN nativa.

Como práctica recomendada, el modo administrativo de la interfaz de enlaces troncales se debe configurar en modo de enlace troncal. De este modo, se garantiza que la interfaz estará configurada de manera estática como un puerto de enlace troncal y nunca negociará un modo diferente.

```
S2(config)#interface FastEthernet 0/1
S2(config-if)#switchport mode trunk
```

Para corregir la falta de concordancia de VLAN nativa, configure el puerto de enlace troncal mediante el comando **switchport trunk native vlan 99**.

```
S2(config-if)#switchport trunk native vlan 99
```

Paso 4. Verificar que los enlaces troncales estén habilitados en S3 y configurar VLAN 99 como la VLAN nativa.

DTP también ha negociado correctamente un enlace troncal entre S1 y S3.

```
S3#show interfaces fastEthernet 0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
<output omitted>
S3#
```

Configure el modo administrativo de la interfaz de enlaces troncales en modo de enlace troncal y corrija la falta de concordancia de VLAN nativa con el comando **switchport trunk native vlan 99**.

Paso 5. Verificar los resultados.

El porcentaje final del usuario debe ser del 100%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Actividad PT 3.4.2: Resolución de problemas en la implementación de una VLAN

Diagrama de topología

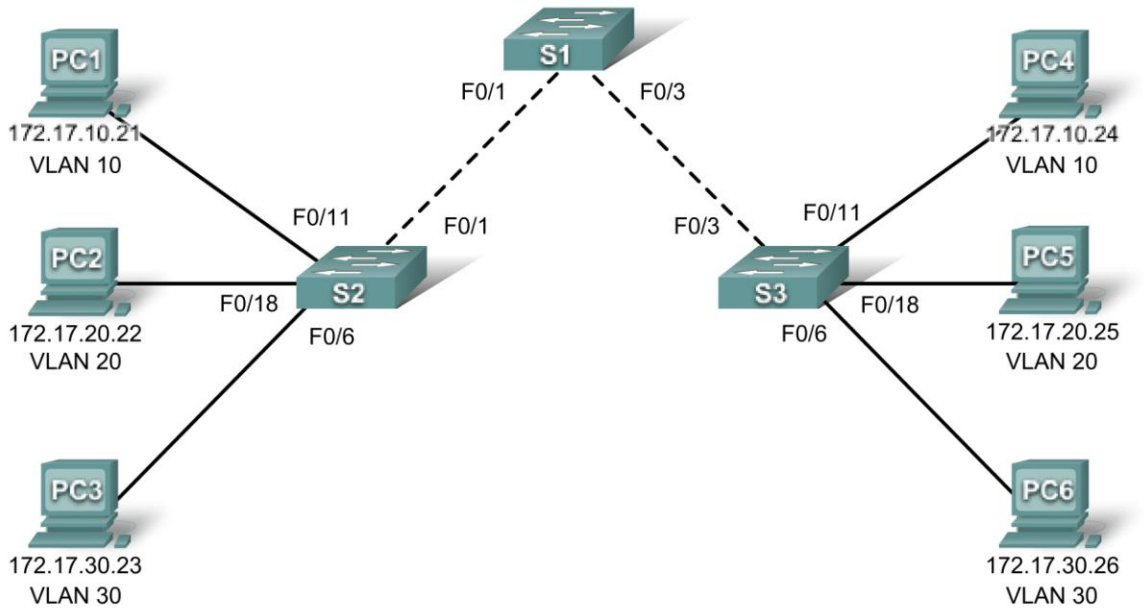


Tabla de direccionamiento

Dispositivo	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
PC1	172.17.10.21	255.255.255.0	172.17.10.1
PC2	172.17.20.22	255.255.255.0	172.17.20.1
PC3	172.17.30.23	255.255.255.0	172.17.30.1
PC4	172.17.10.24	255.255.255.0	172.17.10.1
PC5	172.17.20.25	255.255.255.0	172.17.20.1
PC6	172.17.30.26	255.255.255.0	172.17.30.1

Objetivos de aprendizaje

- Probar la conectividad
- Investigar los problemas de conectividad mediante la recopilación de datos
- Implementar la solución y probar la conectividad

Introducción

En esta actividad, se realizará la resolución de problemas de conectividad entre los equipos PC de la misma VLAN. La actividad estará completa cuando se alcance un porcentaje del 100% y los equipos PC puedan hacer ping a otros equipos PC de la misma VLAN. Cualquier solución que implemente deberá ajustarse al diagrama de topología.

Tarea 1: Probar la conectividad entre equipos PC de la misma VLAN

Use la herramienta **Add Simple PDU** para hacer ping entre dos equipos PC de la misma VLAN. Las siguientes pruebas deben realizarse correctamente al finalizar esta actividad. No obstante, estas pruebas generarán errores en este punto.

- PC1 no puede hacer ping a PC4
- PC2 no puede hacer ping a PC5
- PC3 no puede hacer ping a PC6

Tarea 2: Recopilar datos sobre el problema

Paso 1. Verificar la configuración en los equipos PC.

¿Son correctas las siguientes configuraciones para cada equipo PC?

- Dirección IP
- Máscara de subred
- Gateway predeterminada

Paso 2. Verificar la configuración en los switches.

¿Son correctas las configuraciones en los switches? Asegúrese de verificar lo siguiente:

- Los puertos están asignados a las VLAN correctas
- Los puertos se ha configurado para el modo correcto
- Los puertos están conectados al dispositivo correcto

Paso 3: Documentar el problema y sugerir soluciones.

¿Por qué falló la conectividad entre los equipos PC? ¿Cuáles son las soluciones? Es probable que haya más de un problema y más de una solución. Todas las soluciones deberán ajustarse al diagrama de topología.

PC1 a PC4

Problema: _____

Solución: _____

PC2 a PC5

Problema: _____

Solución: _____

PC3 a PC6

Problema: _____

Solución: _____

Tarea 3: Implementar la solución y probar la conectividad

Paso 1: Hacer cambios de acuerdo con las soluciones sugeridas en la Tarea 2.

Paso 2: Probar la conectividad entre los equipos PC de la misma VLAN.

Si se modifican las configuraciones IP, se deben crear nuevos pings, dado que los pings anteriores usan la antigua dirección IP.

- PC1 debe poder hacer ping a PC4
- PC2 debe poder hacer ping a PC5
- PC3 debe poder hacer ping a PC6

¿Puede PC1 hacer ping a PC4? _____

¿Puede PC2 hacer ping a PC5? _____

¿Puede PC3 hacer ping a PC6? _____

Si algunos pings no se realizan correctamente, regrese a la Tarea 2 para continuar con la resolución de problemas.

Paso 3. Verificar el porcentaje final.

El porcentaje final del usuario debe ser del 100%. De lo contrario, regrese al Paso 1 y continúe con la implementación de las soluciones sugeridas. No podrá hacer clic en **Check Results** y ver qué componentes obligatorios aún no se completaron.

Actividad PT 3.5.1: Configuración básica de la VLAN

Diagrama de topología

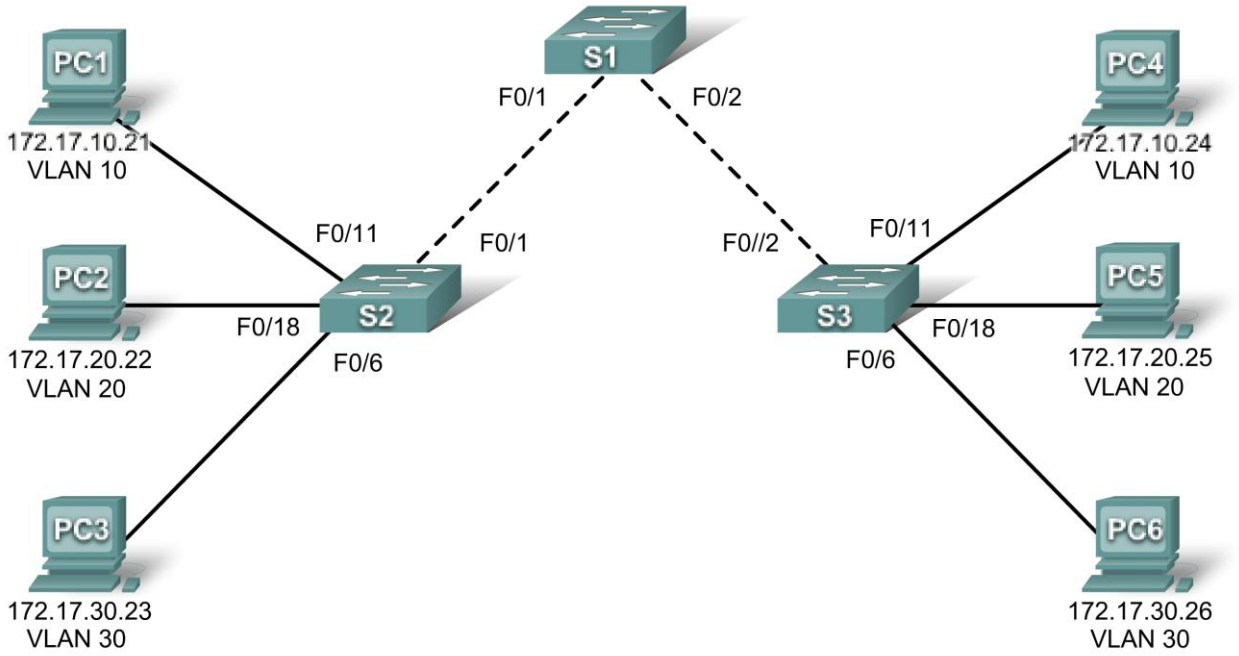


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de enlace) predeterminada
S1	**VLAN 99**	172.17.99.11	255.255.255.0	No aplicable
S2	**VLAN 99**	172.17.99.12	255.255.255.0	No aplicable
S3	**VLAN 99**	172.17.99.13	255.255.255.0	No aplicable
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 las configuraciones de switch básicas. Packet Tracer sólo calificará los nombres de host del switch.

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

Tarea 2: Configurar y activar interfaces Ethernet

Configure las interfaces Ethernet de los seis equipos PC con las direcciones IP y gateways por defecto que se indican en la tabla de direccionamiento.

Nota: La dirección IP para PC1 estará marcada como equivocada por ahora. Cambiará la dirección IP de PC1 más adelante.

Tarea 3: Configurar las VLAN en el switch

Paso 1. Crear VLAN en el switch S1.

Use el comando **vlan** *vlan-id* 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** *name*.

```
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. Verificar 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. Configurar 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. Asignar 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** *vlan-id*. 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 access vlan 30
S2(config-if)#interface fastEthernet0/11
S2(config-if)#switchport access vlan 10
S2(config-if)#interface fastEthernet0/18
S2(config-if)#switchport access vlan 20
S2(config-if)#end
S2#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
```

Nota: La VLAN de acceso Fa0/11 estará marcada como incorrecta por ahora. Esta situación se corregirá más adelante en la actividad.

Repita los mismos comandos en S3.

Paso 5. Determinar qué puertos se han agregado.

Use el comando **show vlan id** *vlan-number* 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** *vlan-name* muestra la misma información.

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

Paso 6. Asignar 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. Configurar 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. Verificar 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. Hacer 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. Mover 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. Cambiar la dirección IP y la red en PC1.

Cambie la dirección IP en PC1 a 172.17.20.21. La máscara de subred y la gateway por defecto 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?

_____

_____

Actividad PT 3.5.2: Desafío de configuración de VLAN

Diagrama de topología

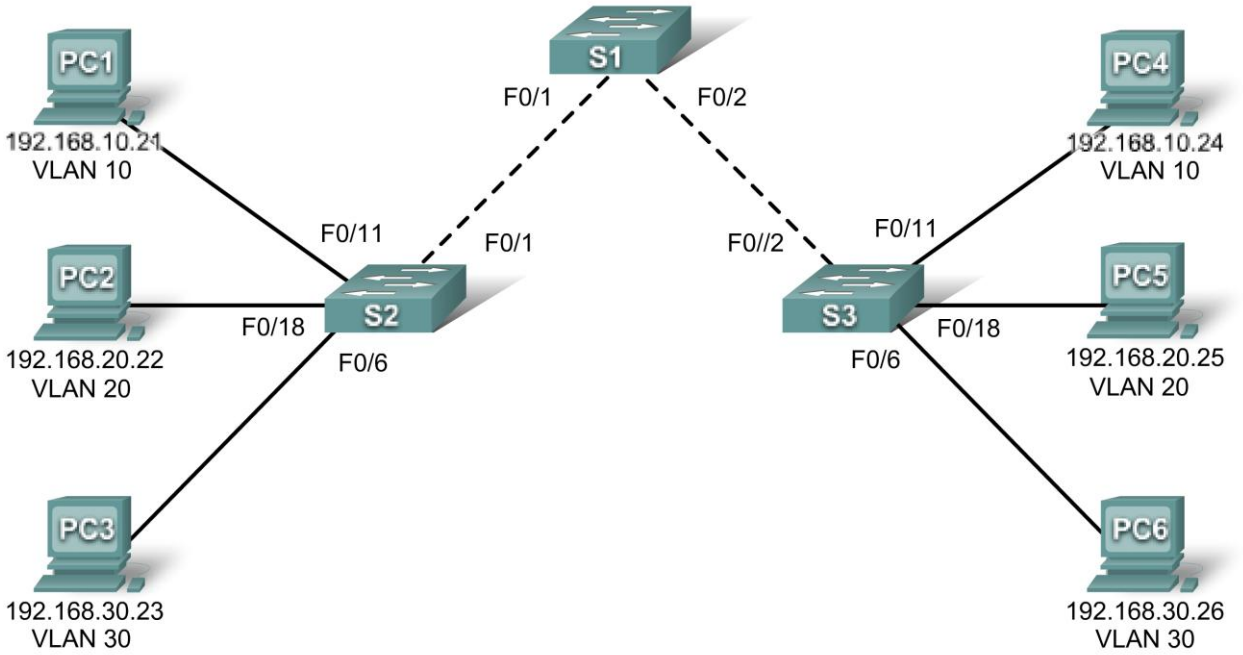


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
S1	**VLAN 56**	192.168.56.11	255.255.255.0	No aplicable
S2	**VLAN 56**	192.168.56.12	255.255.255.0	No aplicable
S3	**VLAN 56**	192.168.56.13	255.255.255.0	No aplicable
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**	192.168.20.23	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	Red
Fa0/1 – 0/5	VLAN 99 – Management&Native	192.168.56.0/24
Fa0/6 – 0/10	VLAN 30 – Guest(Default)	192.168.30.0/24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	192.168.10.0/24
Fa0/18 – 0/24	VLAN 20 – Students	192.168.20.0/24

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

Configure los switches de acuerdo con las siguientes pautas. Packet Tracer sólo calificará los nombres de host.

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

Tarea 2: Configurar y activar interfaces Ethernet

Paso 1. Configurar los equipos PC.

Configure las interfaces Ethernet de los seis equipos PC con las direcciones IP y las gateways predeterminadas de la tabla de direccionamiento que aparece al comienzo de la actividad. La dirección IP para PC1 será calificada como incorrecta por ahora. La dirección de PC1 se cambiará más adelante en la actividad.

Paso 2. Habilitar los puertos del usuario para el acceso en S2 y S3.

Tarea 3: Configurar las VLAN en el switch

Paso 1. Crear VLAN en el switch S1.

Los ID y nombres de la VLAN se enumeran en la tabla de asignaciones de puertos al comienzo de esta actividad.

Paso 2. Verificar que las VLAN se hayan creado en S1.

Paso 3. Configurar, asignar nombres y verificar las VLAN en los switches S2 y S3.

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

Nota: El puerto S2 Fa0/11 se calificará como incorrecto por ahora y Packet Tracer sólo calificará la primera asignación de puertos para cada VLAN.

Paso 5. Determinar los puertos que se han agregado a la VLAN 10 en S2.

Paso 6. Configurar la VLAN 56 de administración en cada uno de los switches.

Paso 7. Configurar los enlaces troncales y la VLAN nativa para los puertos de enlaces troncales en los tres switches. Verificar que los enlaces troncales se hayan configurado.

Paso 8. Verificar que S1, S2 y S3 puedan comunicarse.

Paso 9. Hacer ping a varios hosts desde PC2. ¿Cuál es el resultado?

Paso 10. Mover PC1 a la misma VLAN que PC2. ¿Se puede hacer ping correctamente de PC1 a PC2?

Paso 11. Cambiar la dirección IP en PC1 a 192.168.20.21. ¿Se puede hacer ping correctamente de PC1 a PC2?

Actividad PT 3.5.3: Resolución de problemas de configuraciones de VLAN

Diagrama de topología

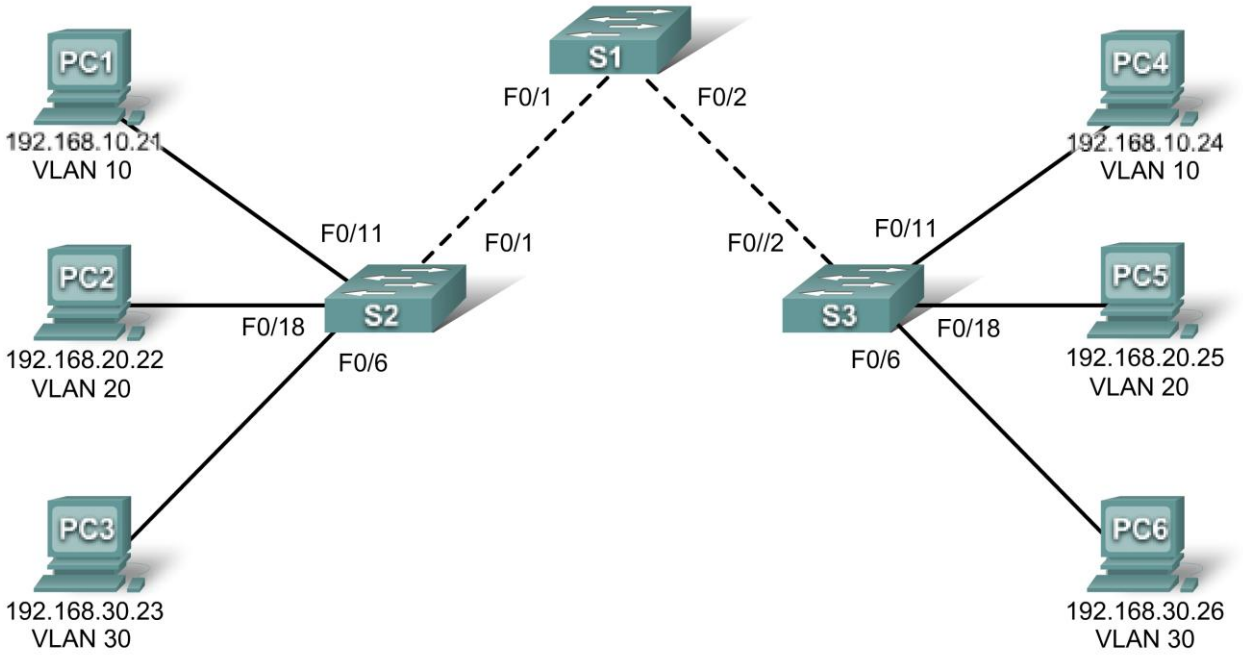


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
S1	**VLAN 56**	192.168.56.11	255.255.255.0	No aplicable
S2	**VLAN 56**	192.168.56.12	255.255.255.0	No aplicable
S3	**VLAN 56**	192.168.56.13	255.255.255.0	No aplicable
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**	192.168.20.23	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	Red
Fa0/1 – 0/5	VLAN 56 – Management&Native	192.168.56.0/24
Fa0/6 – 0/10	VLAN 30 – Guest(Default)	192.168.30.0/24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	192.168.10.0/24
Fa0/18 – 0/24	VLAN 20 – Students	192.168.20.0/24

Objetivos de aprendizaje

- Buscar y corregir errores de red
- Documentar la red corregida

Introducción

En esta actividad, se practicará la resolución de problemas de un entorno de VLAN configurado erróneamente. La red inicial tiene errores. El objetivo es ubicar y corregir todos los errores en las configuraciones y establecer la conectividad de extremo a extremo. La configuración final debe coincidir con el diagrama de topología y la tabla de direccionamiento. Todas las contraseñas están configuradas como **cisco**, excepto la contraseña **enable secret**, que es **class**.

Tarea 1: Buscar y corregir errores de red

Una vez corregidos todos los errores, los equipos PC que pertenecen a la misma VLAN deben poder hacer ping entre sí. Además, S1, S2 y S3 deben poder hacer ping entre sí.

Tarea 2: Documentar la red corregida

Actividad PT 3.6.1: Desafío de habilidades de Integración de Packet Tracer

Diagrama de topología

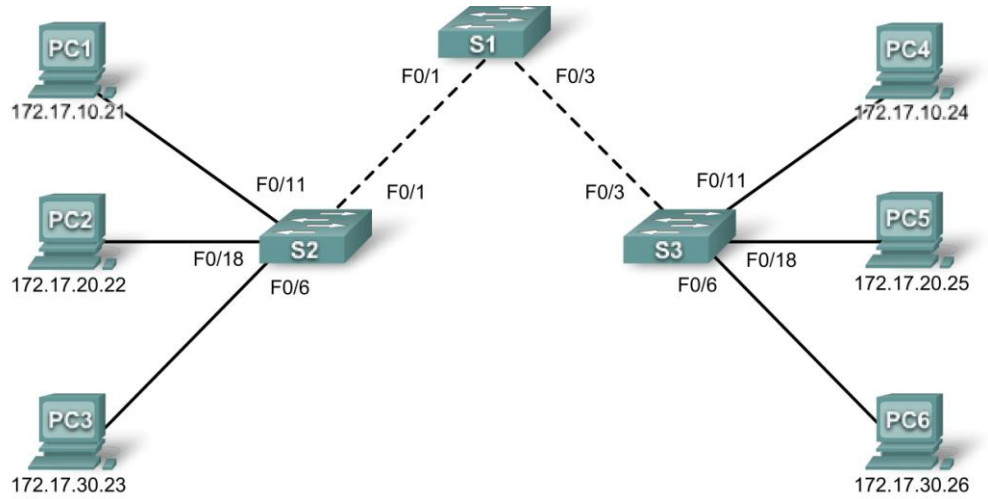


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
S1	**VLAN 99**	172.17.99.31	255.255.255.0	172.17.99.1
S2	**VLAN 99**	172.17.99.32	255.255.255.0	172.17.99.1
S3	**VLAN 99**	172.17.99.33	255.255.255.0	172.17.99.1
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

Objetivos de aprendizaje

- Agregar y conectar switches
- Agregar y conectar equipos PC
- Verificar la configuración básica del dispositivo y la conectividad
- Configurar y verificar la seguridad del puerto
- Configurar las VLAN en los switches
- Configurar enlaces troncales en los switches
- Verificar la conectividad de extremo a extremo

Introducción

En esta actividad, se conectará y configurará por completo la topología del Capítulo 3, incluida la adición y la conexión de dispositivos, así como la configuración de seguridad y de las VLAN.

Tarea 1: Agregar y conectar los switches

Paso 1. Agregar el switch S2.

S2 debe ser un switch de la serie 2960. Cambie el nombre para mostrar y el nombre de host a S2. Los nombres distinguen entre mayúsculas y minúsculas.

Paso 2. Conectar S2 a S1.

Conecte S2 Fa0/1 a S1 Fa0/1.

Paso 3. Agregar el switch S3.

S3 debe ser un switch de la serie 2960. Cambie el nombre para mostrar y el nombre de host a S3. Los nombres distinguen entre mayúsculas y minúsculas.

Paso 4. Conectar S3 a S1.

Conecte S3 Fa0/3 a S1 Fa0/3.

Paso 5. Verificar los resultados.

El porcentaje final del usuario debe ser del 9%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 2: Agregar y conectar los equipos PC

Paso 1. Agregar PC1, PC2, PC3, PC4, PC5 y PC6.

- Agregue los seis equipos PC según la topología del capítulo.
- Si fuera necesario, cambie el nombre para mostrar de modo que coincida con los nombres en la tabla de direccionamiento. Los nombres para mostrar distinguen entre mayúsculas y minúsculas.

Paso 2. Conectar PC1, PC2 y PC3 a S2.

- Conecte PC1 a Fa0/11 en S2.
- Conecte PC2 a Fa0/18 en S2.
- Conecte PC3 a Fa0/6 en S2.

Paso 3. Conectar PC4, PC5 y PC6 con S3.

- Conecte PC4 a Fa0/11 en S3.
- Conecte PC5 a Fa0/18 en S3.
- Conecte PC6 a Fa0/6 en S3.

Paso 4. Verificar los resultados.

El porcentaje final del usuario debe ser del 29%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 3: Configurar los dispositivos y verificar la conectividad

Paso 1. Configurar los switches con los comandos básicos.

Configure cada switch con las siguientes configuraciones básicas. Packet Tracer sólo califica el comando **hostname**.

- Nombre de host en S1.
- Mensaje
- Contraseña secreta de enable
- Configuraciones de la línea
- Encriptación del servicio

Paso 2. Configurar la interfaz VLAN de administración en S1, S2 y S3.

Configure VLAN 99 como la interfaz VLAN de administración en S1, S2 y S3. Esta interfaz no estará activa hasta después de haber configurado los enlaces troncales más adelante en esta actividad. No obstante, active la interfaz en este momento con el comando adecuado.

Paso 3. Configurar el direccionamiento IP del equipo PC.

Configure los equipos PC con el direccionamiento IP de acuerdo con la tabla de direccionamiento.

Paso 4. Verificar que los equipos PC en la misma subred puedan hacer ping entre sí.

Use la herramienta **Add Simple PDU** para crear pings entre los equipos PC en una misma VLAN. Verifique que los siguientes equipos PC puedan hacer ping entre sí:

- PC1 a PC4
- PC2 a PC5
- PC3 a PC6

Paso 5. En el modo de simulación, observe el tráfico de broadcast.

- Borre las direcciones MAC obtenidas de modo que los switches deban enviar mediante broadcast los paquetes de ping.
- En el modo de simulación, observe el tráfico de broadcast que se propaga a través de la LAN hasta que los switches obtengan los puertos de cada PC.

Paso 6. Verificar los resultados.

El porcentaje final del usuario debe ser del 53%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 4: Configurar y verificar la seguridad del puerto

Paso 1. Configurar enlaces de acceso con la seguridad del puerto.

Normalmente, el usuario configura la seguridad del puerto en todos los puertos de acceso o deshabilita el puerto si no está en uso. Use la siguiente política para establecer la seguridad del puerto sólo en los puertos usados por los equipos PC.

- Establezca el puerto en el modo de acceso.
- Habilite la seguridad del puerto.
- Permita sólo una dirección MAC.
- Configure la primera dirección MAC obtenida para “adherirla” a la configuración.
- Configure el puerto para que se desconecte si se produce una infracción de seguridad.

Haga que los switches obtengan las direcciones MAC enviando pings entre los tres switches.

Nota: Packet Tracer sólo califica la habilitación de la seguridad del puerto. No obstante, todas las tareas relativas a la seguridad de puertos anteriores son obligatorias para completar esta actividad.

Paso 2. Verificar que la seguridad del puerto esté activa para las interfaces conectadas a los equipos PC.

¿Qué comando usaría para verificar que la seguridad del puerto está activa en una interfaz?

_____

```
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0050.0F00.6668:1
Security Violation Count   : 0
```

Nota: La información **Last Source Address:Vlan** debe mostrar una dirección MAC. Es posible que la dirección MAC del usuario sea diferente a la que se muestra aquí. Si la dirección MAC en este campo es 0000.0000.0000, envíe tráfico al puerto mediante un ping entre el switch y el otro equipo PC en la misma subred.

Paso 3. Probar la seguridad del puerto.

- Conecte PC2 al puerto de PC3, y conecte PC3 al puerto de PC2.
- Envíe pings entre los equipos PC en la misma subred.
- Los puertos para PC2 y PC3 deben desactivarse.

Paso 4. Verificar que los puertos estén en el modo “err-disabled” y que no se haya registrado una infracción de seguridad.

¿Qué comando muestra la siguiente información?

_____

```
FastEthernet0/6 is down, line protocol is down (err-disabled)
  Hardware is Lance, address is 000a.41e8.c906 (bia 000a.41e8.c906)
<output omitted>
```

¿Qué comando muestra la siguiente información?

_____

```
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
```

```
Last Source Address:Vlan    : 0050.0F00.6668:1
Security Violation Count    : 1
```

Paso 5. Volver a conectar los equipos PC al puerto correcto y borrar las infracciones de seguridad del puerto.

- Conecte PC2 y PC3 nuevamente al puerto correcto.
- Borre la infracción de seguridad del puerto.
- Verifique que PC2 y PC3 puedan enviar pings a través de S2.

Paso 6. Verificar los resultados.

El porcentaje final del usuario debe ser del 75%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 5: Configurar las VLAN en los switches

Paso 1. Crear y asignar nombres a las VLAN.

Cree y asigne nombres a las siguientes VLAN en los switches S1, S2 y S3:

- VLAN 10, nombre = **Faculty/Staff**
- VLAN 20, nombre = **Students**
- VLAN 30, nombre = **Guest(Default)**
- VLAN 99, nombre = **Management&Native**

Paso 2. Asignar puertos de acceso a las VLAN.

Asigne los siguientes puertos de acceso de PC a las VLAN:

- VLAN 10: PC1 y PC4
- VLAN 20: PC2 y PC5
- VLAN 30: PC3 y PC6

Paso 3. Verificar la implementación de VLAN.

¿Qué comando verifica la configuración de VLAN, incluidas las asignaciones de puertos?

_____

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig1/1, Gig1/2
10   Faculty/Staff                     active    Fa0/11
20   Students                          active    Fa0/18
30   Guest(Default)                    active    Fa0/6
99   Management&Native                 active
<output omitted>
```

Paso 4. Verificar los resultados.

El porcentaje final del usuario debe ser del 92%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 6: Configurar enlaces troncales en los switches

Paso 1. Configurar enlaces troncales en las interfaces correspondientes.

- Configure enlaces troncales en las interfaces correspondientes del switch S1.
- Verifique que los switches S2 y S3 están ahora en el modo de enlace troncal.
- Configure manualmente las interfaces correspondientes en S2 y S3 para enlaces troncales.
- Configure VLAN 99 como la VLAN nativa para todos los enlaces troncales.

Paso 2. Probar la conectividad

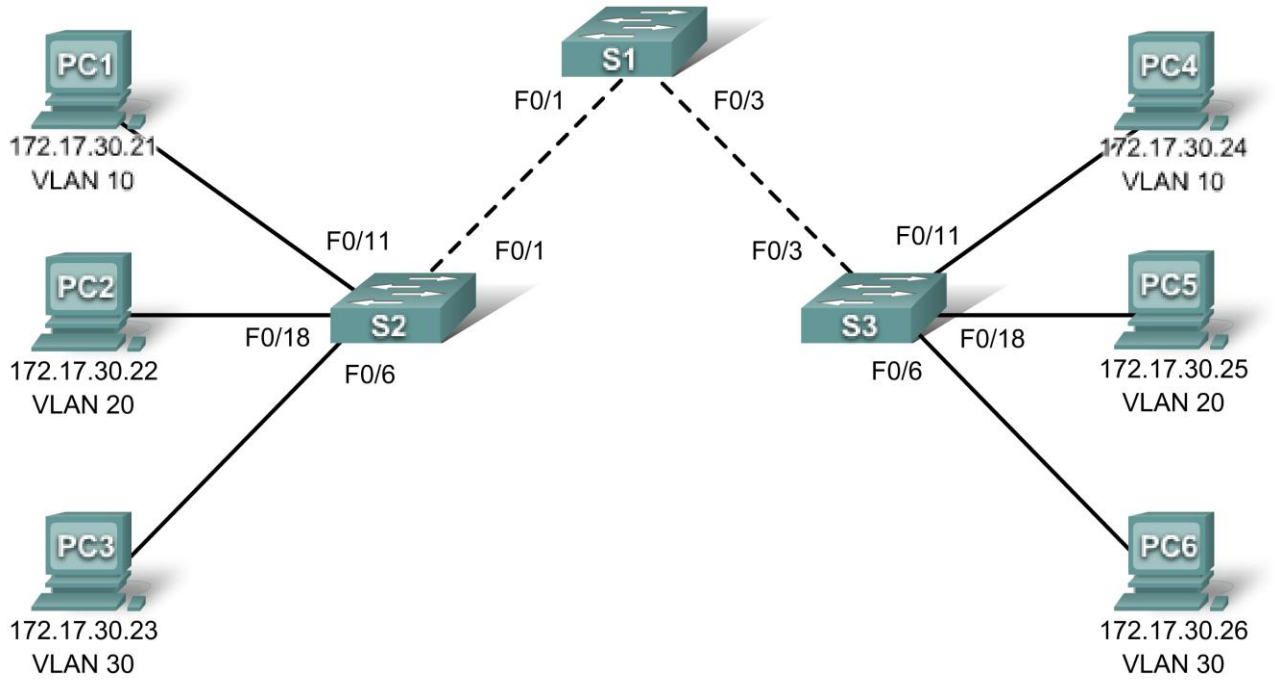
Después de que los puertos de enlaces troncales del switch cambien al estado de envío (luces de enlace de color verde), debería poder hacer ping correctamente entre los equipos PC de una misma VLAN.

Paso 3. Verificar los resultados.

El porcentaje final del usuario debe ser del 100%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Actividad PT 4.3.3: Configurar VTP

Diagrama de topología



Objetivos de aprendizaje

- Investigar la configuración actual
- Configurar S1 como servidor VTP
- Configurar S2 y S3 como clientes VTP
- Configurar las VLAN en S1
- Configurar enlaces troncales en S1, S2 y S3
- Verificar el estado del VTP en S1, S2 y S3
- Asignar VLAN a puertos en S2 y S3
- Verificar la implementación de VLAN y probar la conectividad

Introducción

En esta actividad, se podrá practicar la configuración de VTP. Cuando Packet Tracer se abre por primera vez, los switches ya incluyen una configuración parcial. La contraseña EXEC del usuario es **cisco** y la contraseña EXEC privilegiado es **class**.

Tarea 1: Investigar la configuración actual

Paso 1. Verificar la configuración en ejecución actual de los switches.

¿Qué configuraciones ya están presentes en los switches?

_____

_____

_____

Paso 2. Mostrar las VLAN actuales en cada switch.

¿Hay VLAN presentes? ¿Las VLAN presentes son VLAN por defecto o creadas por el usuario?

_____

```
S1#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
                                                Gig1/1, Gig1/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

El porcentaje final debe ser de 0% al finalizar esta tarea.

Tarea 2: Configurar S1 como servidor VTP

Paso 1. Configurar el comando del modo VTP.

S1 será el servidor para VTP. Establezca S1 en el modo de servidor.

```
S1(config)#vtp mode server
Device mode already VTP SERVER.
S1(config)#
```

Observe que el switch ya está establecido en el modo de servidor por defecto. No obstante, es importante que configure explícitamente este comando para asegurarse de que el switch esté en el modo de servidor.

Paso 2. Configurar el nombre de dominio VTP.

Configure S1 con **CCNA** como el nombre de dominio VTP. Recuerde que los nombres de dominio VTP distinguen entre mayúsculas y minúsculas.

```
S1(config)#vtp domain CCNA
Changing VTP domain name from NULL to CCNA
S1(config)#
```

Paso 3. Configurar la contraseña de dominio VTP.

Configure S1 con **cisco** como la contraseña de dominio VTP. Recuerde que las contraseñas de dominio VTP distinguen entre mayúsculas y minúsculas.

```
S1(config)#vtp password cisco
Setting device VLAN database password to cisco
S1(config)#
```

Paso 4. Confirmar los cambios en la configuración.

Use el comando **show vtp status** en S1 para confirmar que el modo VTP y el dominio están configurados correctamente.

```
S1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x8C 0x29 0x40 0xDD 0x7F 0x7A 0x63
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Para verificar la contraseña de VTP, use el comando **show vtp password**.

```
S1#show vtp password
VTP Password: cisco
S1#
```

Paso 5. Verificar los resultados.

El porcentaje final del usuario debe ser del 8%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 3: Configurar S2 y S3 como clientes VTP

Paso 1. Configurar el comando del modo VTP.

S2 y S3 serán clientes VTP. Establezca estos dos switches en modo de cliente.

Paso 2. Configurar el nombre de dominio VTP.

Antes de que S2 y S3 acepten publicaciones VTP de S1, deben pertenecer al mismo dominio VTP. Configure S2 y S3 con **CCNA** como el nombre de dominio VTP. Recuerde que los nombres de dominio VTP distinguen entre mayúsculas y minúsculas.

Paso 3. Configurar la contraseña de dominio VTP.

S2 y S3 también deben usar la misma contraseña antes de aceptar publicaciones VTP del servidor VTP. Configure S2 y S3 con **cisco** como la contraseña de dominio VTP. Recuerde que las contraseñas de dominio VTP distinguen entre mayúsculas y minúsculas.

Paso 4. Confirmar los cambios en la configuración.

Use el comando **show vtp status** en cada switch para confirmar que el modo VTP y el dominio están configurados correctamente. a continuación se muestra la información para S3.

```
S3#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x8C 0x29 0x40 0xDD 0x7F 0x7A 0x63
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Observe que el número de revisión de la configuración es 0 en los tres switches. ¿Por qué?

_____

_____

_____

Para verificar la contraseña de VTP, use el comando **show vtp password**.

```
S3#show vtp password
VTP Password: cisco
S3#
```

Paso 5. Verificar los resultados.

El porcentaje final del usuario debe ser del 31%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 4: Configurar las VLAN en S1

Las VLAN se pueden crear en el servidor VTP y distribuir a otros switches en el dominio VTP. En esta tarea se crearán cuatro VLAN nuevas en el servidor VTP, S1. Estas VLAN se distribuirán a S1 y S3 a través de VTP.

Paso 1. Crear las VLAN.

A los fines de la calificación de Packet Tracer, los nombres de las VLAN distinguen entre mayúsculas y minúsculas.

- VLAN 10 con el nombre **Faculty/Staff**
- VLAN 20 con el nombre **Students**
- VLAN 30 con el nombre **Guest(Default)**
- VLAN 99 con el nombre **Management&Native**

Paso 2. Verificar las VLAN.

Use el comando **show vlan brief** para verificar las VLAN y sus nombres.

```
S1#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
                                            Gig1/1, Gig1/2
10   Faculty/Staff                active
20   Students                     active
30   Guest(Default)               active
99   Management&Native            active
1002 fddi-default                 active
1003 token-ring-default           active
1004 fddinet-default              active
1005 trnet-default                active
```

Si se introduce el mismo comando en S2 y S3, se observa que las VLAN no están en su base de datos de VLAN. ¿Por qué?

_____

_____

Paso 3. Verificar los resultados.

El porcentaje final del usuario debe ser del 46%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 5: Configurar enlaces troncales en S1, S2 y S3.

Use el comando **switchport mode trunk** para establecer el modo de enlace troncal para cada uno de los enlaces troncales. Use el comando **switchport trunk native vlan 99** para establecer la VLAN 99 como la VLAN nativa.

Paso 1. Configurar FastEthernet 0/1 y FastEthernet 0/3 en S1 para enlaces troncales.

Introduzca los comandos correspondientes para configurar enlaces troncales y definir la VLAN 99 como la VLAN nativa.

Una vez configurada, el protocolo de enlace troncal dinámico (DTP) activará los enlaces troncales. Puede verificar que S2 y S3 sean ahora enlaces troncales si introduce el comando **show interface fa0/1 switchport** en S2 y el comando **show interface fa0/3 switchport** en S3.

Si espera algunos minutos a que Packet Tracer simule todos los procesos, S1 publicará la configuración de VLAN a S2 y S3. Esta verificación puede ejecutarse en S2 o S3 mediante los comandos **show vlan brief** o **show vtp status**.

No obstante, se recomienda configurar ambos extremos de los enlaces troncales en el modo **on**.

Paso 2. Configurar Fast Ethernet 0/1 en S2 para enlaces troncales.

Introduzca los comandos correspondientes para configurar enlaces troncales y definir la VLAN 99 como la VLAN nativa.

Paso 3. Configurar Fast Ethernet 0/3 en S3 para enlaces troncales.

Introduzca los comandos correspondientes para configurar enlaces troncales y definir la VLAN 99 como la VLAN nativa.

Paso 4. Verificar los resultados.

El porcentaje final del usuario debe ser del 77%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 6: Verificar el estado del VTP

Use los comandos **show vtp status** y **show vlan brief** para verificar lo siguiente.

- S1 debe mostrar el estado del servidor
- S2 y S3 deben mostrar el estado de cliente
- S2 y S3 deben tener VLAN de S1

Nota: Las publicaciones de VTP se envían a través del dominio de administración cada cinco minutos o siempre que se efectúe una modificación en las configuraciones de la VLAN. Para acelerar este proceso, se puede cambiar entre el modo de tiempo real y el modo de simulación hasta la siguiente ronda de actualizaciones. No obstante, es probable que sea necesario intentarlo varias veces dado que sólo se adelantará al reloj de Packet Tracer 10 segundos cada vez. Otra opción es cambiar uno de los switches cliente al modo transparente y luego volverlo al modo de cliente.

¿Cuál es el número de revisión de la configuración? _____

¿Por qué el número de revisión de la configuración es más alto que el número de VLAN creadas?

_____

_____

¿Cuál es el número actual de VLAN existentes? _____

¿Por qué hay más VLAN existentes que las cuatro que se han creado?

_____

El porcentaje final debe ser del 77% al final de esta tarea.

Tarea 7: Asignar VLAN a puertos

Use el comando **switchport mode access** para establecer el modo de acceso de los enlaces de acceso. Use el comando **switchport access vlan** *vlan-id* para asignar una VLAN a un puerto de acceso.

Paso 1. Asignar VLAN a los puertos en S2.

- Fa0/11 en VLAN 10
- Fa0/18 en VLAN 20
- Fa0/6 en VLAN 30

Paso 2. Asignar VLAN a los puertos en S3.

- Fa0/11 en VLAN 10
- Fa0/18 en VLAN 20
- Fa0/6 en VLAN 30

Paso 3. Verificar los resultados.

El porcentaje final del usuario debe ser del 100%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 8: Verificar la implementación de VLAN y probar la conectividad

Paso 1. Verificar la configuración de la VLAN y las asignaciones de puertos.

Use el comando **show vlan brief** para verificar la configuración de la VLAN y las asignaciones de puertos en cada switch. Compare la información obtenida con la topología.

Paso 2. Probar la conectividad entre PC.

Los pings entre los equipos PC de una misma VLAN deben realizarse correctamente, mientras que los pings entre los equipos PC en diferentes VLAN deben provocar errores.

Desde PC1, haga ping a PC4.

Desde PC2, haga ping a PC5.

Desde PC3, haga ping a PC6.

Actividad PT 4.4.1: Configuración básica del VTP

Diagrama de topología

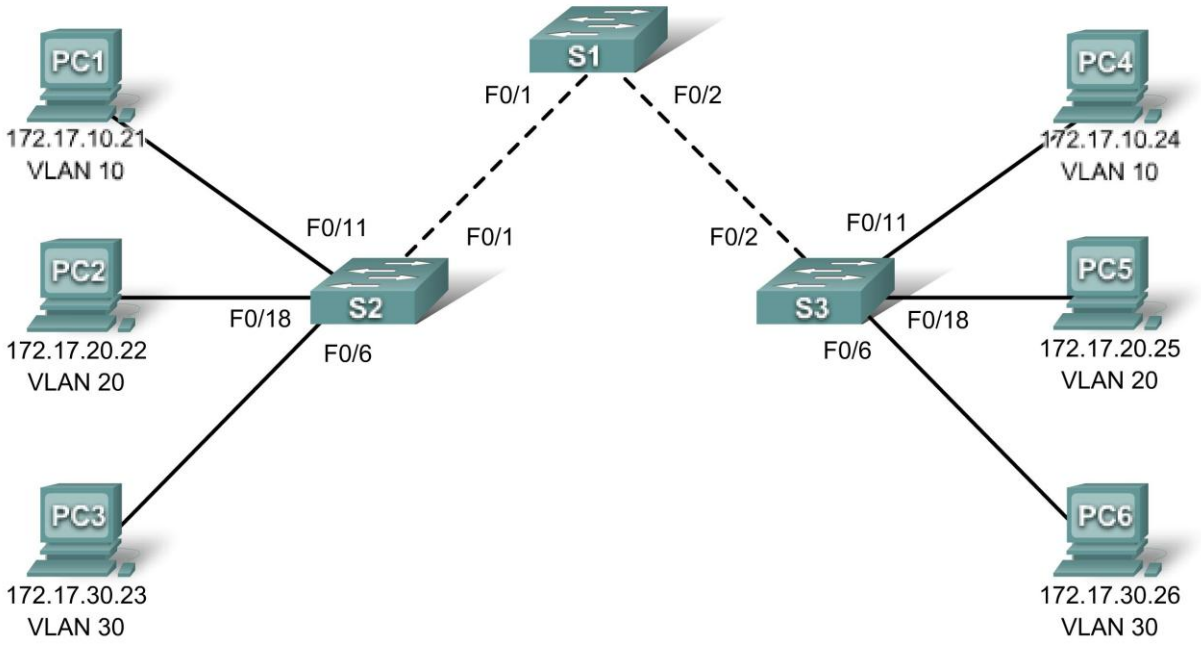


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
S1	**VLAN 99**	172.17.99.11	255.255.255.0	No aplicable
S2	**VLAN 99**	172.17.99.12	255.255.255.0	No aplicable
S3	**VLAN 99**	172.17.99.13	255.255.255.0	No aplicable
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 (S2 y S3)

Puertos	Asignaciones	Red
Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN nativa 99)	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 configuraciones básicas del switch
- Configurar las interfaces Ethernet en los equipos PC host
- Configurar VTP y seguridad en los switches

Introducción

En esta actividad, se efectuarán las configuraciones básicas del switch, se configurará el VTP, se establecerán los enlaces troncales, se aprenderá sobre los modos de VTP, se creará y distribuirá información VLAN y se asignarán puertos a la VLAN. La red inicial se abre en un estado seguro con todos los puertos desactivados administrativamente.

Tarea 1: Realizar configuraciones de switches básicas

Configure los switches S1, S2 y S3 según las siguientes pautas y guarde todas las configuraciones:

- Configure el nombre de host del switch, según se indica en la topología.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de **class** en el Modo EXEC.
- Configure una contraseña de **cisco** para las conexiones de consola.
- Configure una contraseña de **cisco** para las conexiones vty.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#no ip domain-lookup
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Tarea 2: Configurar las interfaces Ethernet en los equipos PC host

Configure las interfaces Ethernet de PC1, PC2, PC3, PC4, PC5 y PC6 con las direcciones IP y las gateways por defecto indicadas en la tabla de direccionamiento.

Tarea 3: Configurar VTP y seguridad en los switches

Paso 1. Habilitar los puertos del usuario en S2 y S3.

Configure los puertos del usuario en el modo de acceso. Consulte el diagrama de topología para determinar los puertos que están conectados a los dispositivos del usuario final.

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

Paso 2. Comprobar la configuración VTP actual en los tres switches.

Use el comando show vtp status para determinar el modo de funcionamiento VTP para los tres switches.

```
S1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

S2#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

S3#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
```

```
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

VTP permite que el administrador de red controle las instancias de VLAN en la red mediante la creación de dominios de VTP. Dentro de cada dominio VTP, se configuran uno o más switches como servidores VTP. Las VLAN pueden crearse en el servidor VTP y distribuirse a otros switches en el dominio de VTP. Las tareas comunes de configuración de VTP son la configuración del modo de funcionamiento, el dominio y la contraseña. Tenga en cuenta que los tres switches están en el modo de servidor. El modo de servidor es el modo de VTP por defecto para la mayoría de los switches Catalyst. En esta actividad, se usará S1 como el servidor VTP, con S2 y S3 configurados como clientes VTP o en el modo transparente VTP.

Paso 3. Configurar el modo de funcionamiento, el nombre de dominio y la contraseña de VTP en los tres switches.

Establezca el nombre de dominio de VTP en Lab4 y la contraseña de VTP en cisco en los tres switches. Configure S1 en el modo de servidor, S2 en el modo cliente y S3 en el modo transparente.

```
S1(config)#vtp mode server
Device mode already VTP SERVER.
S1(config)#vtp domain Lab4
Changing VTP domain name from NULL to Lab4
S1(config)#vtp password cisco
Setting device VLAN database password to cisco
S1(config)#end

S2(config)#vtp mode client
Setting device to VTP CLIENT mode
S2(config)#vtp domain Lab4
Changing VTP domain name from NULL to Lab4
S2(config)#vtp password cisco
Setting device VLAN database password to cisco
S2(config)#end

S3(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
S3(config)#vtp domain Lab4
Changing VTP domain name from NULL to Lab4
S3(config)#vtp password cisco
Setting device VLAN database password to cisco
S3(config)#end
```

Nota: Un switch cliente puede obtener el nombre de dominio de VTP desde un switch servidor, pero sólo si el dominio del switch cliente está en el estado nulo. No obtiene un nuevo nombre si se ha configurado uno anteriormente. Por este motivo, se recomienda configurar manualmente el nombre de dominio en todos los switches para garantizar que el nombre de dominio se configuró correctamente. Los switches de los diferentes dominios de VTP no intercambian la información de la VLAN.

Paso 4. Configurar los enlaces troncales y la VLAN nativa para los puertos de enlaces troncales en los tres switches.

En todos los switches, configure los enlaces troncales y la VLAN nativa para las interfaces FastEthernet 0/1-5. Sólo los comandos para fa0/1 en cada switch se muestran a continuación.

```
S1(config)#interface fa0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#no shutdown
S1(config-if)#interface fa0/2
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#no shutdown
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)#no shutdown
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)#no shutdown
S3(config-if)#end
```

Paso 5. Configurar la seguridad del puerto en los switches de la capa de acceso S2 y S3.

Configure los puertos fa0/6, fa0/11 y fa0/18 de modo que permitan sólo un host y obtengan la dirección MAC del host dinámicamente.

```
S2(config)#interface fa0/6
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#interface fa0/11
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#interface fa0/18
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#end

S3(config)#interface fa0/6
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#interface fa0/11
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#interface fa0/18
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#end
```

Paso 6. Configurar las VLAN en el servidor VTP.

En esta práctica de laboratorio se requieren cuatro VLAN:

- VLAN 99 (management)
- VLAN 10 (faculty/staff)
- VLAN 20 (students)
- VLAN 30 (guest)

Configure las VLAN en el servidor VTP. La calificación de Packet Tracer distingue entre mayúsculas y minúsculas.

```
S1(config)#vlan 99
S1(config-vlan)#name management
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
S1(config-vlan)#exit
```

Verifique que las VLAN se hayan creado en S1 mediante el comando show vlan brief.

Paso 7. Comprobar si las VLAN creadas en S1 se han distribuido a S2 y S3.

Use el comando show vlan brief en S2 y S3 para determinar si el servidor VTP ha enviado su configuración VLAN a todos los switches.

```
S2#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

S3#show vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, 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, Gig1/1
                                                 Gig1/2
1002 fddi-default                      active
1003 token-ring-default                active
```

```
1004 fddinet-default                active
1005 trnet-default                  active
```

¿Están configuradas las mismas VLAN en todos los switches? _____

¿Por qué S2 y S3 tienen diferentes configuraciones VLAN en este punto?

_____

Paso 8. Crear una nueva VLAN en S2 y S3.

```
S2(config)#vlan 88
%VTP VLAN configuration not allowed when device is in CLIENT mode.

S3(config)#vlan 88
S3(config-vlan)#name test
S3(config-vlan)#
```

¿Por qué no se puede crear una nueva VLAN en S2 pero sí puede en S3?

_____

Elimine la VLAN 88 de S3.

```
S3(config)#no vlan 88
```

Paso 9. Configurar manualmente las VLAN.

Configure las cuatro VLAN identificadas en el paso 6 en el switch S3.

```
S3(config)#vlan 99
S3(config-vlan)#name management
S3(config-vlan)#exit
S3(config)#vlan 10
S3(config-vlan)#name faculty/staff
S3(config-vlan)#exit
S3(config)#vlan 20
S3(config-vlan)#name students
S3(config-vlan)#exit
S3(config)#vlan 30
S3(config-vlan)#name guest
S3(config-vlan)#exit
```

A continuación, puede ver una de las ventajas de VTP. La configuración manual es tediosa y propensa a errores y, cualquier error que se produzca aquí podría impedir la comunicación entre las VLAN. Además, estos tipos de errores pueden ser difíciles de solucionar.

Paso 10. Configurar la dirección de la interfaz de administración en los tres 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
```

Verifique que los switches estén configurados correctamente haciendo ping entre ellos. En S1, haga ping a la interfaz de administración de S2 y S3. En S2, haga ping a la interfaz de administración de S3.

¿Los pings se realizaron correctamente? En caso contrario, realice la resolución de problemas de configuración del switch y vuelva a intentarlo.

Paso 11. Asignar puertos del switch a las VLAN.

Consulte la tabla de asignación de puertos al comienzo de la actividad para asignar puertos a las VLAN. Dado que Packet Tracer 4.11 no usa el comando de intervalo de la interfaz, sólo configure la primera interfaz para cada VLAN. Las asignaciones de puertos no se configuran a través de VTP. Las asignaciones de puertos deben configurarse en cada switch de forma manual o dinámica mediante un servidor VMPS. Los comandos se muestran para S3 solamente, pero los switches S2 y S3 deben configurarse de manera similar. Guarde la configuración cuando haya terminado.

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

Actividad PT 4.4.2: Desafío de la configuración del VTP

Diagrama de topología

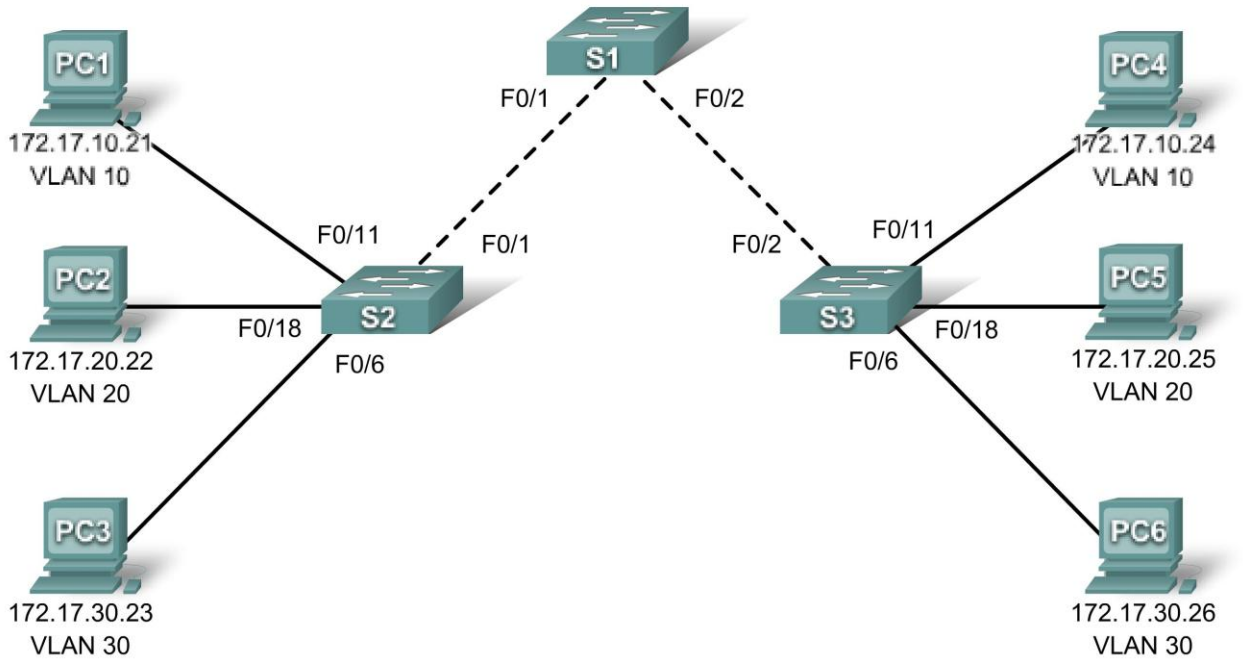


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
S1	**VLAN 99**	172.31.99.11	255.255.255.0
S2	**VLAN 99**	172.31.99.12	255.255.255.0
S3	**VLAN 99**	172.31.99.13	255.255.255.0
PC1	**NIC**	172.31.10.1	255.255.255.0
PC2	**NIC**	172.31.20.1	255.255.255.0
PC3	**NIC**	172.31.30.1	255.255.255.0
PC4	**NIC**	172.31.10.2	255.255.255.0
PC5	**NIC**	172.31.20.2	255.255.255.0
PC6	**NIC**	172.31.30.2	255.255.255.0

Asignaciones de puertos (S2 y S3)

Puertos	Asignaciones	Red
Fa0/1 – 0/5	Enlaces troncales 802.1q	
Fa0/6 – 0/10	VLAN 30 – Administration	172.31.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Engineering	172.31.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Sales	172.31.20.0 /24
Ninguno	VLAN 99 – Network Mgmt	172.31.99.0 /24

Objetivos de aprendizaje

- Realizar las configuraciones básicas del switch
- Configurar las interfaces Ethernet en los equipos PC host
- Configurar VTP en los swtiches

Introducción

En esta actividad, se efectuarán las configuraciones básicas del switch, se configurará el VTP, se establecerán los enlaces troncales, se aprenderá sobre los modos de VTP, se creará y distribuirá información VLAN y se asignarán puertos a la VLAN.

Tarea 1: Realizar configuraciones de switches básicas

Configure los switches S1, S2 y S3 según las siguientes pautas y guarde todas las configuraciones:

- Configure el nombre de host del switch, según se indica en la topología.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de class en el Modo EXEC.
- Configure una contraseña de cisco para las conexiones de consola.

Tarea 2: Configurar las interfaces Ethernet en los equipos PC host

Configure las interfaces Ethernet de PC1, PC2, PC3, PC4, PC5 y PC6 con las direcciones IP indicadas en la tabla de direccionamiento. Las configuraciones de gateway predeterminada no son necesarias para esta actividad.

Tarea 3: Configurar VTP en los switches

VTP permite que el administrador de red controle las instancias de VLAN en la red mediante la creación de dominios de VTP. Dentro de cada dominio de VTP, se configuran uno o más switches como servidores VTP. Las VLAN pueden crearse en el servidor VTP y distribuirse a otros switches en el dominio de VTP. Las tareas comunes de configuración de VTP son la configuración del modo de funcionamiento, el dominio y la contraseña. En esta práctica de laboratorio, se configurará S1 como un servidor VTP, con S2 y S3 configurados como clientes VTP.

Paso 1. Comprobar la configuración VTP actual en los tres switches.

Paso 2. Configurar el modo de funcionamiento, el nombre de dominio y la contraseña de VTP en los tres switches.

Establezca el nombre de dominio de VTP en **access** y la contraseña de VTP en **lab4** en los tres switches. Configure S1 en el modo de servidor, S2 en el modo cliente y S3 en el modo transparente.

Packet Tracer calificará inicialmente el modo para S3 como incorrecto. Esta situación se corregirá más adelante en la actividad.

Nota: Un switch de cliente puede obtener el nombre de dominio de VTP desde un switch servidor, pero sólo si el dominio del switch cliente está en el estado nulo. No obtiene un nuevo nombre si se ha configurado uno anteriormente. Por este motivo, se recomienda configurar manualmente el nombre de dominio en todos los switches para garantizar que el nombre de dominio se configuró correctamente. Los switches de los diferentes dominios de VTP no intercambian la información de la VLAN.

Paso 3. Configurar los enlaces troncales y la VLAN nativa para los puertos de enlaces troncales en los tres switches.

En todos los switches, configure los enlaces troncales y la VLAN nativa para las interfaces FastEthernet 0/1-5.

Paso 4. Configurar la seguridad del puerto en los switches de la capa de acceso S2 y S3.

Configure los puertos Fa0/6, Fa0/11 y Fa0/18 en S2 y S3 de modo que permitan un máximo de dos hosts para conectar estos puertos y obtener las direcciones MAC de los hosts dinámicamente.

Paso 5. Configurar las VLAN en el servidor VTP.

En esta práctica de laboratorio se requieren cuatro VLAN:

- VLAN 99 (management)
- VLAN 10 (engineering)
- VLAN 20 (sales)
- VLAN 30 (administration)

Configure las VLAN en el servidor VTP.

Cuando termine, verifique que se hayan creado las cuatro VLAN en S1.

Paso 6. Comprobar si las VLAN creadas en S1 se han distribuido a S2 y S3.

Use el comando **show vlan brief** en S2 y S3 para determinar si el servidor VTP ha enviado su configuración VLAN a todos los switches.

¿Están configuradas las mismas VLAN en todos los switches? _____

¿Por qué S2 y S3 tienen diferentes configuraciones VLAN en este punto? _____

_____

_____

Paso 7. Configurar la dirección de la interfaz de administración en los tres switches.

Antes de continuar, cambie el modo VTP en S3 a cliente. a continuación, verifique que S3 reciba las configuraciones VLAN de S1 a través de VTP.

Configure los tres switches con las direcciones IP identificadas en la tabla de direccionamiento al comienzo de la práctica de laboratorio. Asigne estas direcciones a la VLAN de administración de red (VLAN 99).

Verifique que los switches estén configurados correctamente haciendo ping entre ellos. En S1, haga ping a la interfaz de administración de S2 y S3. En S2, haga ping a la interfaz de administración de S3.

¿Los pings se realizaron correctamente? _____

En caso contrario, realice la resolución de problemas de configuración del switch y corrija los errores.

Paso 8. Asignar puertos del switch a las VLAN.

Consulte la tabla de asignación de puertos al comienzo de la práctica de laboratorio para asignar puertos a las VLAN. Tenga en cuenta que las asignaciones de puertos no se configuran a través de VTP. Recuerde que los switches S2 y S3 deben configurarse en forma similar. Guarde la configuración cuando haya terminado.

Paso 9. Verificar que los enlaces troncales funcionen correctamente.

Desde PC1, intente hacer ping a PC4, PC5 y PC6.

¿Alguno de los pings se realizó correctamente? _____

¿Por qué algunos de los pings generaron errores?

_____

_____

¿Qué hosts pueden alcanzarse desde PC3? _____

Actividad PT 4.4.3: Resolución de problemas de configuración del VTP

Diagrama de topología

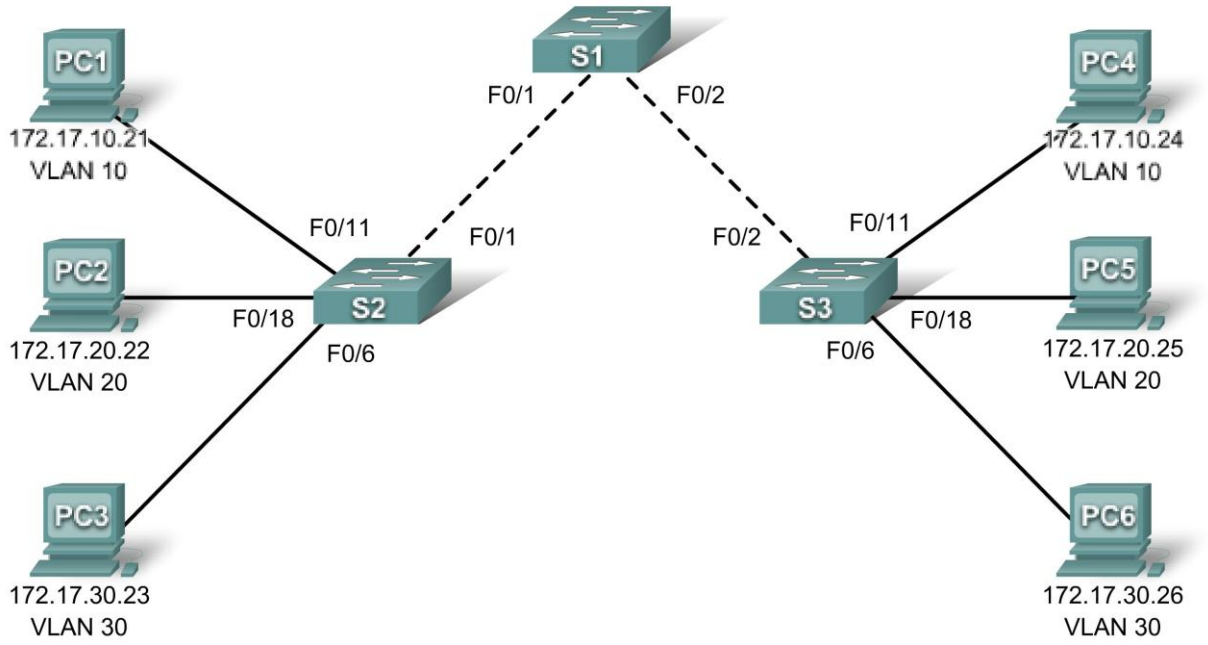


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
S1	**VLAN 99**	172.17.99.11	255.255.255.0
S2	**VLAN 99**	172.17.99.12	255.255.255.0
S3	**VLAN 99**	172.17.99.13	255.255.255.0
PC1	**NIC**	172.17.10.21	255.255.255.0
PC2	**NIC**	172.17.20.22	255.255.255.0
PC3	**NIC**	172.17.30.23	255.255.255.0
PC4	**NIC**	172.17.10.24	255.255.255.0
PC5	**NIC**	172.17.20.25	255.255.255.0
PC6	**NIC**	172.17.30.26	255.255.255.0

Asignaciones de puertos (S2 y S3)

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

- Buscar y corregir todos los errores de configuración
- Documentar la red corregida

Introducción

El protocolo de enlace troncal de la VLAN (VTP) contribuye a garantizar la uniformidad de las configuraciones de VLAN en la red conmutada, pero debe configurarse correctamente. En esta actividad, el nombre de dominio VTP es **Lab3_4** y la contraseña VTP es **cisco**. No obstante, hay numerosos errores en esta configuración que se deben solucionar y corregir antes de que se pueda restaurar la conectividad de extremo a extremo en la VLAN. Los errores se habrán resuelto correctamente cuando las mismas VLAN estén configuradas en los tres switches y se pueda hacer ping entre los dos hosts en la misma VLAN o entre dos switches.

Tarea 1: Realizar la resolución de problemas y corregir errores de VTP y de configuración

Una vez corregidos todos los errores, se debería poder hacer ping a PC4 desde PC1, a PC5 desde PC2 y a PC6 desde PC3. También se debería poder hacer ping a las interfaces de administración en S2 y S3 desde S1.

Tarea 2: Documentar la configuración del switch

Cuando haya finalizado la resolución de problemas, capture los resultados del comando **show run** y guárdelos como un documento de texto para cada switch.

Actividad PT 4.5.1: Desafío de habilidades de integración de Packet Tracer

Diagrama de topología

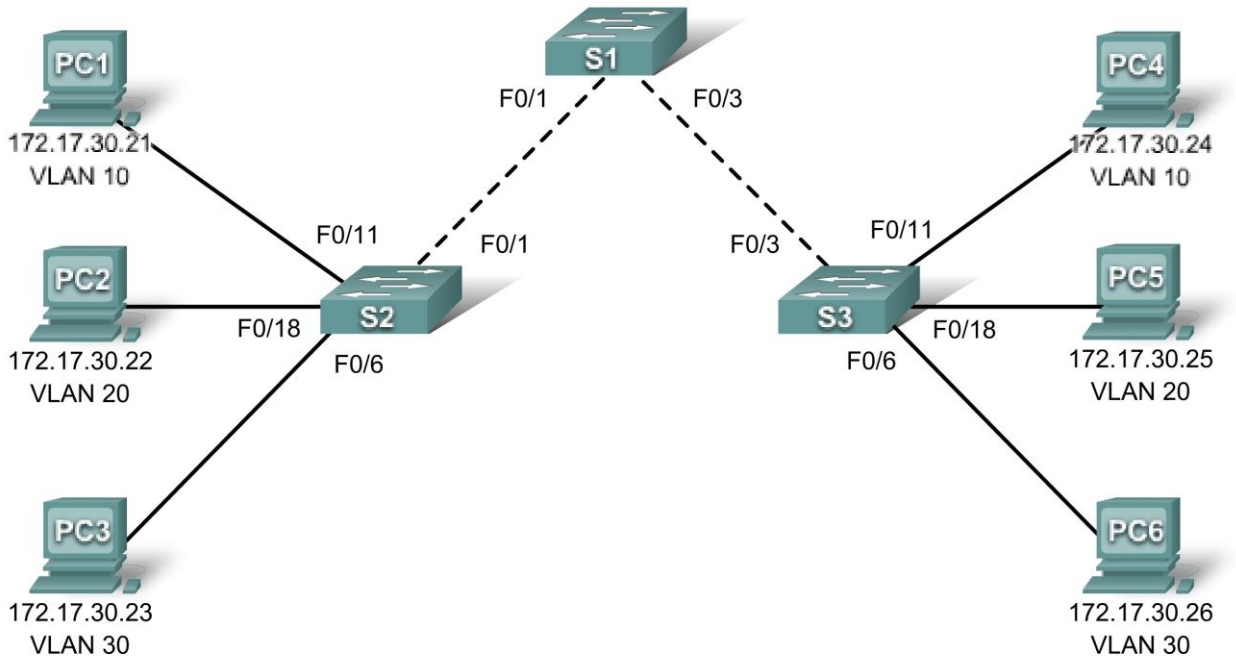


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
S1	**VLAN 99**	172.17.99.31	255.255.255.0	172.17.99.1
S2	**VLAN 99**	172.17.99.32	255.255.255.0	172.17.99.1
S3	**VLAN 99**	172.17.99.33	255.255.255.0	172.17.99.1
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

Objetivos de aprendizaje:

- Configurar y verificar las configuraciones básicas del dispositivo
- Configurar y verificar la seguridad del puerto

- Configurar VTP
- Configurar enlaces troncales
- Configurar las VLAN
- Asignar VLAN a puertos
- Verificar la conectividad de extremo a extremo

Introducción

En esta actividad, se configurarán los switches, incluidos la configuración básica, la seguridad del puerto, los enlaces troncales y las VLAN. Se usará VTP para publicar las configuraciones VLAN a otros switches.

Tarea 1: Configurar y verificar las configuraciones básicas del dispositivo

Paso 1. Configurar los comandos básicos.

Configure cada switch con los siguientes comandos básicos. Packet Tracer sólo calificará el comando **hostname**.

- Nombre de host en S1.
- Mensaje
- Contraseña secreta de enable
- Configuraciones de la línea
- Encriptación del servicio

Paso 2. Configurar la interfaz VLAN de administración en S1, S2 y S3.

Cree y habilite la interfaz VLAN 99 en cada switch. Use la tabla de direccionamiento para la configuración de las direcciones.

Paso 3. Verificar que los equipos PC en la misma subred puedan hacer ping entre sí.

Los equipos PC ya están configurados con el direccionamiento correcto. Cree PDU simples para probar la conectividad entre los dispositivos de la misma subred:

Paso 4. Verificar los resultados.

El porcentaje final del usuario debe ser del 15%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 2: Configurar y verificar la seguridad del puerto

Paso 1. Configurar todos los enlaces de acceso con la seguridad del puerto.

Normalmente, el usuario configura la seguridad del puerto en todos los puertos de acceso o deshabilita el puerto, si no lo va a utilizar. Use la siguiente política para establecer la seguridad del puerto sólo en los puertos usados por los equipos PC.

- Establezca el puerto en el modo de acceso.
- Habilite la seguridad del puerto.
- Permita sólo una dirección MAC.
- Configure la primera dirección MAC aprendida para “adherirla” a la configuración.
- Configure el puerto para que se desconecte si se produce una infracción de seguridad.
- Haga que los switches obtengan las direcciones MAC enviando pings entre los tres switches.

NOTA: Packet Tracer sólo califica la habilitación de la seguridad del puerto. No obstante, todas las tareas relativas a la seguridad de puertos anteriores son obligatorias para completar esta actividad.

Paso 2. Probar la seguridad del puerto.

- Conecte PC2 al puerto PC3 y conecte PC3 al puerto PC2.
- Envíe pings entre los equipos PC en la misma subred.
- Los puertos para PC2 y PC3 deben desactivarse.

Paso 3. Verificar que los puertos estén en el modo "err-disabled" y que no se haya registrado una infracción de seguridad.

Paso 4. Volver a conectar los equipos PC al puerto correcto y borrar las infracciones de seguridad del puerto.

- Conecte PC2 y PC3 nuevamente al puerto correcto.
- Borre la infracción de seguridad del puerto.
- Verifique que PC2 y PC3 puedan enviar pings a través de S2.

Paso 5. Verificar los resultados.

El porcentaje final del usuario debe ser del 55%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 3: Configurar VTP

Paso 1. Configurar el modo VTP en los tres switches.

Configure S1 como el servidor. Configure S2 y S3 como clientes.

Paso 2. Configurar el nombre de dominio VTP en los tres switches.

Use **CCNA** como el nombre de dominio de VTP.

Paso 3. Configurar la contraseña de dominio de VTP en los tres switches.

Use **cisco** como la contraseña de dominio de VTP.

Paso 4. Verificar los resultados.

El porcentaje final del usuario debe ser del 70%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 4: Configurar enlaces troncales

Paso 1. Configurar enlaces troncales en S1, S2 y S3.

Configure las interfaces correspondientes en el modo de enlace troncal y asigne VLAN 99 como la VLAN nativa.

Paso 2. Verificar los resultados.

El porcentaje final del usuario debe ser del 83%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 5: Configurar las VLAN

Paso 1. Crear las VLAN en S1.

Cree las siguientes VLAN en S1 solamente y asígneles nombre. VTP publicará las nuevas VLAN en S1 y S2.

- VLAN 10 **Faculty/Staff**
- VLAN 20 **Students**
- VLAN 30 **Guest(Default)**
- VLAN 99 **Management&Native**

Paso 2. Verificar que las VLAN se hayan enviado a S2 y S3.

Use los comandos adecuados para verificar que S2 y S3 ahora tienen las VLAN creadas en S1. Es probable que demore algunos minutos hasta que Packet Tracer simule las publicaciones de VTP.

Paso 3. Verificar los resultados.

El porcentaje final del usuario debe ser del 90%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 6: Asignar VLAN a puertos

Paso 1. Asignar VLAN a puertos de acceso en S2 y S3.

Asigne los puertos de acceso de PC a VLAN:

- VLAN 10: PC1 y PC4
- VLAN 20: PC2 y PC5
- VLAN 30: PC3 y PC6

Paso 2. Verificar la implementación de VLAN.

Use el comando correspondiente para verificar la implementación de VLAN.

Paso 3. Verificar los resultados.

El porcentaje final del usuario debe ser del 100%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 7: Verificar la conectividad de extremo a extremo

Paso 1. Verificar que PC1 y PC4 puedan hacer ping entre sí.

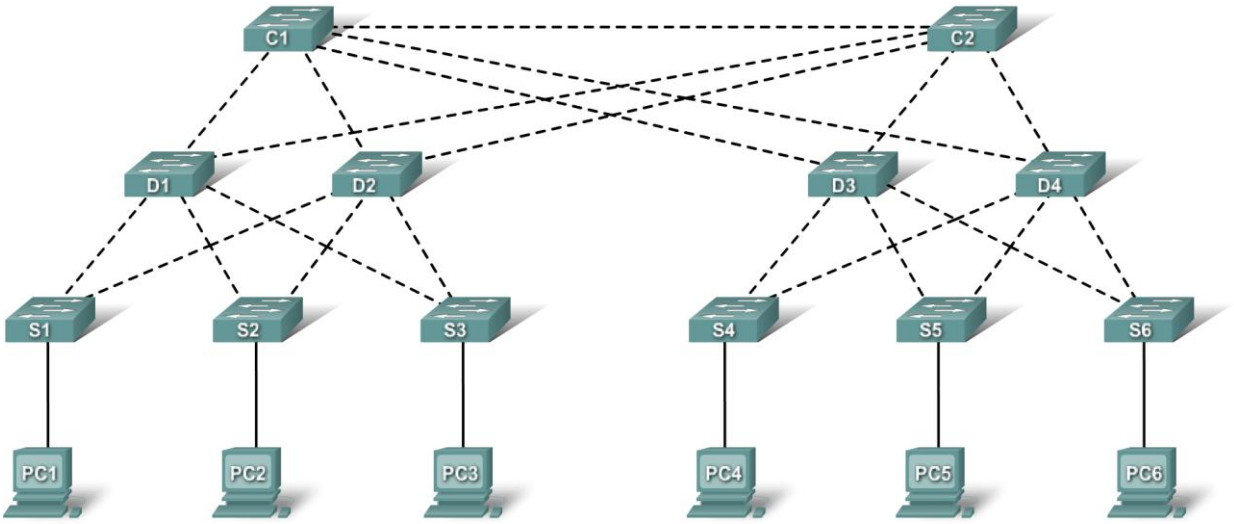
Paso 2. Verificar que PC2 y PC5 puedan hacer ping entre sí.

Paso 3. Verificar que PC3 y PC6 puedan hacer ping entre sí.

Paso 4. Los equipos PC de diferentes VLAN no deben poder hacer ping entre sí.

Actividad PT 5.1.3: Análisis de un diseño redundante

Diagrama de topología



Objetivos de aprendizaje

- Comprobar la convergencia de STP
- Examinar el proceso de ARP
- Probar la redundancia en una red conmutada

Introducción

En esta actividad, se examinará cómo STP funciona por defecto. Los switches se han agregado a la red “de fábrica”. Los switches de Cisco pueden enchufarse y conectarse a una red sin ninguna acción adicional de parte del administrador de red. Por lo tanto, estos switches funcionarán de acuerdo con la configuración por defecto.

Tarea 1: Comprobar la convergencia de STP

Cuando STP sea completamente convergente, existirán las siguientes condiciones:

- Todos los equipos PC tienen luces de enlace de color verde en los puertos con switch.
- Los switches de la capa de acceso tienen un enlace de reenvío (verde) a un switch de la capa de distribución y un enlace de bloqueo (ámbar) a un segundo switch de la capa de distribución.
- Los switches de la capa de distribución tienen un enlace de reenvío (verde) a un switch de la capa núcleo y un enlace de bloqueo (ámbar) a un segundo switch de la capa núcleo.

Tarea 2: Examinar el proceso de ARP

Paso 1. Cambiar al modo de simulación.

Paso 2. Hacer ping desde PC1 a PC6.

Use la herramienta Add Simple PDU para crear una PDU desde PC1 a PC6. Asegúrese de que ICMP esté seleccionado en **Event List Filters**. Haga clic en **Capture/Forward** para examinar el proceso de ARP a medida que la red conmutada obtiene las direcciones MAC de PC1 y PC6. Observe que los puertos de bloqueo detienen todos los bucles posibles. Por ejemplo, la solicitud ARP de PC1 viaja desde S1 a D2 a C1 a D1 y luego vuelve a S1. No obstante, dado que STP bloquea el enlace entre S1 y D1, no se produce ningún bucle.

Observe que la respuesta de ARP de PC6 viaja de vuelta en una ruta. ¿Por qué?

_____

_____

_____

Registre la ruta sin bucles entre PC1 y PC6.

_____

_____

Paso 3. Examinar el proceso de ARP nuevamente.

Haga ping entre dos PC diferentes para examinar el proceso de ARP nuevamente.

¿Qué parte de la ruta se modificó desde el último conjunto de pings?

_____

_____

Tarea 3: Probar la redundancia en una red conmutada

Paso 1. Eliminar el enlace entre S1 y D2.

Cambie al modo de tiempo real. Elimine el enlace entre S1 y D2. Demora algo de tiempo para hacer que STP sea convergente y establecer una nueva ruta sin bucles. Dado que sólo S1 se ve afectada, observe cómo la luz ámbar del enlace entre S1 y D1 cambia a verde.

Paso 2. Hacer ping entre PC1 y PC6.

Una vez que el enlace entre S1 y D1 esté activo (indicado a través de una luz verde), cambie al modo de simulación y haga ping entre PC1 y PC6 otra vez.

Registre la nueva ruta sin bucles.

_____

_____

Paso 3. Eliminar el enlace entre C1 y D3.

Cambie al modo de tiempo real. Observe que los enlaces entre D3 y D4 a C2 son de color ámbar. Elimine el enlace entre C1 y D3. Demora algo de tiempo para hacer que STP sea convergente y establecer una nueva ruta sin bucles. Observe los enlaces de color ámbar en D3 y D4. Puede alternar entre los modos de simulación y tiempo real para acelerar el proceso.

¿Qué enlace es ahora el enlace activo en C2?

_____

_____

Paso 4. Hacer ping entre PC1 y PC6.

Cambie al modo de simulación y haga ping entre PC1 y PC6.

Registre la nueva ruta sin bucles.

_____

_____

Paso 5. Eliminar D4.

Cambie al modo de tiempo real. Tenga en cuenta que S4, S5 y S6 envían el tráfico hacia D4. Elimine D4. Demora algo de tiempo para hacer que STP sea convergente y establecer una nueva ruta sin bucles. Observe que los enlaces entre S4, S5 y S6 a D3 cambian a envío (verde). Los tres switches deben ahora enviar el tráfico a D3.

Paso 6. Hacer ping entre PC1 y PC6.

Cambie al modo de simulación y haga ping entre PC1 y PC6.

Registre la nueva ruta sin bucles.

_____

_____

¿Qué característica exclusiva tiene la nueva ruta que no ha visto antes?

_____

_____

_____

Paso 7. Eliminar C1.

Cambie al modo de tiempo real. Tenga en cuenta que D1 y D2 envían el tráfico hacia C1. Elimine C1. Demora algo de tiempo para hacer que STP sea convergente y establecer una nueva ruta sin bucles. Observe que los enlaces entre D1 y D2 a C2 cambian a envío (verde). Una vez convergentes, los switches deben ahora enviar el tráfico a C2.

Paso 8. Hacer ping entre PC1 y PC6.

Cambie al modo de simulación y haga ping entre PC1 y PC6.

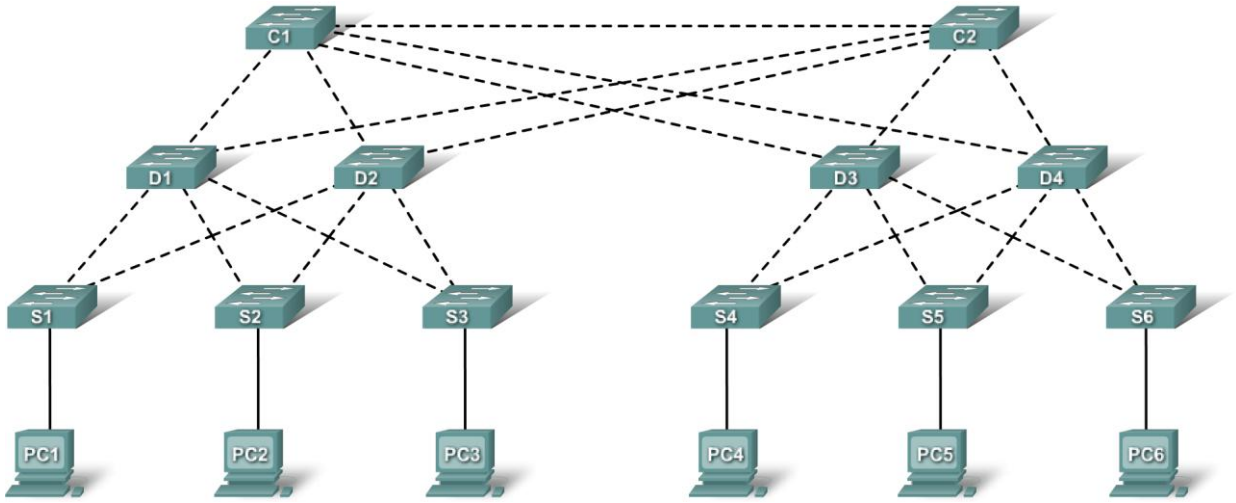
Registre la nueva ruta sin bucles.

_____

_____

Actividad PT 5.2.5: Configuración de STP

Diagrama de topología



Objetivos de aprendizaje

- Examinar el estado por defecto de STP
- Configurar el puente raíz
- Configurar el puente raíz de respaldo
- Finalizar la configuración de STP

Introducción

En esta actividad, los switches son “de fábrica” y no tienen configuraciones. Se manipulará la elección del puente raíz de modo que se seleccionen los switches núcleo antes que los switches de la capa de acceso o de distribución.

Tarea 1: Examinar el estado por defecto de STP

Paso 1. Examinar las luces de enlace.

Cuando STP sea completamente convergente, existirán las siguientes condiciones:

- Todos los equipos PC tienen luces de enlace de color verde en los puertos con switch.
- Los switches de la capa de acceso tienen un enlace de reenvío (verde) a un switch de la capa de distribución y un enlace de bloqueo (ámbar) al switch de la capa de núcleo.
- Los switches de la capa de distribución tienen un enlace de reenvío (verde) a un switch de la capa núcleo y un enlace de bloqueo (ámbar) a un segundo switch de la capa núcleo.

Paso 2. Cambiar al modo de simulación.

Paso 3. Determinar el puente raíz.

Haga clic en **Capture/Forward**. Sin observar los detalles BPDU, las direcciones MAC o el comando **show spanning-tree**, ¿puede indicar qué switch está en el puente raíz?

_____

_____

¿Cuál puede ser el motivo por el que este switch no es una buena opción como raíz?

_____

_____

Tarea 2: Configurar el puente raíz

Paso 1. Configurar el puente raíz.

Uno de los switches núcleo debe ser la raíz; el otro debe ser la raíz de respaldo. Cambie al modo de tiempo real y configure C1 con una prioridad de **4096**.

Paso 2. Cambiar entre los modos de tiempo real y simulación.

Cambie entre el modo de tiempo real y simulación varias veces hasta que todos los puertos en C1 estén de color verde.

Paso 3. Cambiar al modo de simulación.

Paso 4. Asegúrese de que C1 sea el puente raíz.

Haga clic en **Capture/Forward** varias veces para observar las BPDU de configuración. C1 debe iniciar la propagación de BPDU.

Paso 5. Verificar los resultados.

El porcentaje final del usuario debe ser del 17%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 3: Configurar el puente raíz de respaldo

Paso 1. Configurar el puente raíz de respaldo.

El otro switch núcleo sirve como un puente raíz de respaldo. Cambie al modo de tiempo real y configure C2 con una prioridad de **8192**.

Paso 2. Cambiar entre los modos de tiempo real y simulación.

Cambie entre el modo de tiempo real y simulación varias veces hasta que todos los puertos en C2 estén de color verde.

Paso 3. Examinar los enlaces conectados a C2.

¿Cuál es la característica exclusiva de los enlaces C2 a los switches de la capa de distribución que no está presente en los enlaces C1?

_____

_____

Paso 4. Verificar los resultados.

El porcentaje final del usuario debe ser del 33%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 4: Finalizar la configuración de STP

Es recomendable que un switch de capa de acceso nunca se convierta en raíz. Para garantizar esto, todos los switches de capa de acceso se deben configurar con una prioridad más alta que la configurada por defecto. No obstante, dado que hay menos switches de distribución, resulta más eficaz configurar estos switches con una prioridad levemente más alta que el switch raíz de respaldo.

Paso 1. Configurar los switches de distribución.

Configure D1, D2, D3 y D4 con una prioridad de **12288**.

Paso 2. Verificar los resultados.

El porcentaje final del usuario debe ser del 100%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Actividad PT 5.5.2: Desafío de protocolo spanning tree

Diagrama de topología

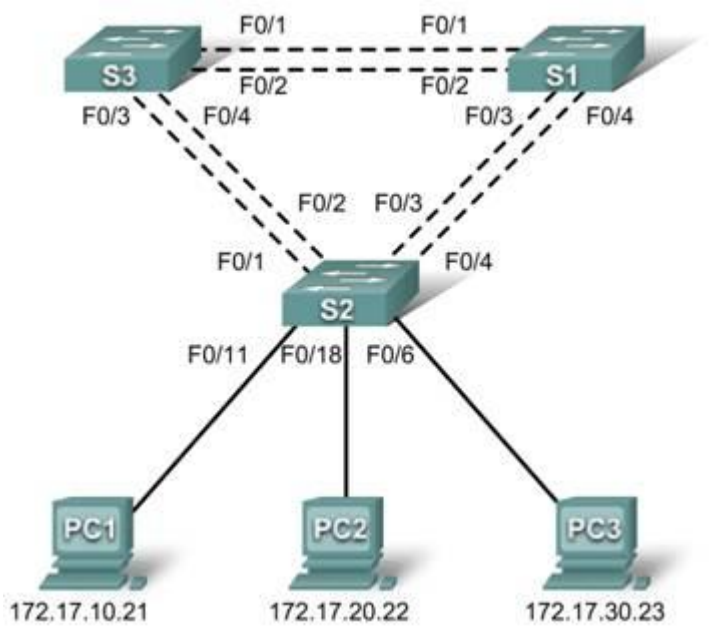


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
S1	**VLAN 99**	172.17.99.11	255.255.255.0	No aplicable
S2	**VLAN 99**	172.17.99.12	255.255.255.0	No aplicable
S3	**VLAN 99**	172.17.99.13	255.255.255.0	No aplicable
PC1	**NIC**	172.17.10.21	255.255.255.0	172.17.10.12
PC2	**NIC**	172.17.20.22	255.255.255.0	172.17.20.12
PC3	**NIC**	172.17.30.23	255.255.255.0	172.17.30.12

Asignaciones de puertos: S2

Puertos	Asignaciones	Red
Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN nativa 99)	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 configuraciones básicas del switch
- Configurar las interfaces Ethernet en los equipos PC host
- Configurar las VLAN
- Configurar spanning-tree
- Optimizar STP

Introducción

En esta actividad, se realizarán las configuraciones básicas del switch, se configurará el direccionamiento en los equipos PC, se configurará las VLAN, se examinará el protocolo de spanning-tree y se aprenderá cómo optimizarlo.

Tarea 1: Realizar configuraciones de switches básicas

Configure los switches S1, S2 y S3 según las siguientes pautas y guarde todas las configuraciones:

Configure el nombre de host del switch, según se indica en la topología.

- Deshabilite la búsqueda DNS.
- Configure una contraseña de **class** en el Modo EXEC.
- Configure una contraseña de **cisco** para las conexiones de consola.
- Configure una contraseña de **cisco** para las conexiones vty.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#no ip domain-lookup
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Tarea 2: Configurar las interfaces Ethernet en los equipos PC host

Configure las interfaces Ethernet de PC1, PC2 y PC3 con la dirección IP, la máscara de subred y la gateway que se indican en la tabla de direccionamiento.

Tarea 3: Configurar las VLAN

Paso 1. Habilitar los puertos del usuario en S2 en el modo de acceso.

Consulte el diagrama de topología para determinar los puertos del switch en S2 que están activados para el acceso del dispositivo del usuario final. Estos tres puertos estarán configurados para el modo de acceso y habilitados con el comando no shutdown.

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

Paso 2. Configurar VTP.

Configure VTP en los tres switches según la siguiente tabla. Recuerde que los nombres y las contraseñas de dominio VTP distinguen entre mayúsculas y minúsculas. El modo de funcionamiento por defecto es servidor.

Nombre del switch	Modo de funcionamiento VTP	Dominio VTP	Contraseña de VTP
S1	Server	Lab5	cisco
S2	Client	Lab5	cisco
S3	Client	Lab5	cisco

```
S1(config)#vtp mode server
Device mode already VTP SERVER.
S1(config)#vtp domain Lab5
Changing VTP domain name from NULL to Lab5
S1(config)#vtp password cisco
Setting device VLAN database password to cisco
S1(config)#end

S2(config)#vtp mode client
Setting device to VTP CLIENT mode
S2(config)#vtp domain Lab5
Changing VTP domain name from NULL to Lab5
S2(config)#vtp password cisco
Setting device VLAN database password to cisco
S2(config)#end

S3(config)#vtp mode client
Setting device to VTP CLIENT mode
S3(config)#vtp domain Lab5
Changing VTP domain name from NULL to Lab5
S3(config)#vtp password cisco
Setting device VLAN database password to cisco
S3(config)#end
```

Paso 3. Configurar enlaces troncales y VLAN nativa.

Configure los puertos de enlace troncal y VLAN nativa. Para cada switch, configure los puertos de Fa0/1 a Fa0/5 como puertos de enlace troncal. Designe VLAN 99 como la VLAN nativa para estos enlaces troncales. Cuando se comenzó esta actividad, estos puertos estaban deshabilitados y deben volver a habilitarse mediante el comando **no shutdown**.

Sólo se muestran los comandos para la interfaz FastEthernet0/1 en cada switch, pero los comandos deben aplicarse hasta la interfaz FastEthernet0/5.

```
S1(config)#interface fa0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#no shutdown
S1(config)#end

S2(config)#interface fa0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 99
S2(config-if)#no shutdown
S2(config-if)#end

S3(config)#interface fa0/1
S3(config-if#switchport mode trunk
S3(config-if)#switchport trunk native vlan 99
S3(config-if)#no shutdown
S3(config-if)#end
```

Paso 4. Configurar el servidor VTP con las VLAN.

VTP permite configurar las VLAN en el servidor VTP y completarlas con los clientes VTP del dominio. De esta forma, se garantiza la coherencia en la configuración VLAN en toda la red.

Configure las siguientes VLAN en el servidor VTP.

VLAN	Nombre de VLAN
VLAN 99	management
VLAN 10	faculty-staff
VLAN 20	students
VLAN 30	guest

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

Paso 5. Verificar las VLAN.

Use el comando **show vlan brief** en S2 y S3 para verificar que las cuatro VLAN se hayan distribuido a los switches cliente.

```
S2#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

S3#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
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Paso 6. Configurar la dirección de la interfaz de administración en los tres switches.

```
S1(config)#interface vlan99
S1(config-if)#ip address 172.17.99.11 255.255.255.0

S2(config)#interface vlan99
S2(config-if)#ip address 172.17.99.12 255.255.255.0

S3(config)#interface vlan99
S3(config-if)#ip address 172.17.99.13 255.255.255.0
```

Verifique que los switches estén configurados correctamente haciendo ping entre ellos. En S1, haga ping a la interfaz de administración de S2 y S3. En S2, haga ping a la interfaz de administración de S3.

¿Los pings se realizaron correctamente? En caso contrario, realice la resolución de problemas de configuración del switch y vuelva a intentarlo.

Paso 7. Asignar puertos del switch a las VLAN.

Las asignaciones del puerto se indican en la tabla del comienzo de la actividad. No obstante, dado que Packet Tracer 4.11 no admite el comando **interface range**, sólo se debe asignar el primer puerto de cada intervalo.

```
S2(config)#interface fa0/6
S2(config-if)#switchport access vlan 30
S2(config-if)#interface fa0/11
S2(config-if)#switchport access vlan 10
S2(config-if)#interface fa0/18
S2(config-if)#switchport access vlan 20
S2(config-if)#end
S2#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
S2#
```

Tarea 4: Configurar spanning-tree

Paso 1. Examinar la configuración por defecto del protocolo de spanning-tree (STP) 802.1D.

En cada switch, muestre la tabla del spanning-tree mediante el comando **show spanning-tree**. Se muestran los resultados para S1 solamente. La selección de la raíz varía en función del BID por defecto de cada switch. En esta actividad, S3 es actualmente la raíz.

```
S1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0030.F20D.D6B1
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0050.0F68.146E
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.3    Shr
Fa0/2            Altn BLK 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/4            Desg FWD 19        128.3    Shr


VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     0030.F20D.D6B1
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     0050.0F68.146E
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.3    Shr
```

```
Fa0/2            Altn BLK 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/4            Desg FWD 19        128.3    Shr


VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    32788
             Address     0030.F20D.D6B1
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
             Address     0050.0F68.146E
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.3    Shr
Fa0/2            Altn BLK 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/4            Desg FWD 19        128.3    Shr


VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority    32798
             Address     0030.F20D.D6B1
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32798  (priority 32768 sys-id-ext 30)
             Address     0050.0F68.146E
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.3    Shr
Fa0/2            Altn BLK 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/4            Desg FWD 19        128.3    Shr


VLAN0099
  Spanning tree enabled protocol ieee
  Root ID    Priority    32867
             Address     0030.F20D.D6B1
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32867  (priority 32768 sys-id-ext 99)
             Address     0050.0F68.146E
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.3    Shr
Fa0/2            Altn BLK 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/4            Desg FWD 19        128.3    Shr
```

Tenga en cuenta que hay cinco instancias de STP en cada switch.

Examine el spanning-tree de la VLAN 99 de los tres switches.

```
S1#show spanning-tree vlan 99

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID    Priority    32867
             Address     0030.F20D.D6B1
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32867  (priority 32966 sys-id-ext 99)
             Address     0050.0F68.146E
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.3    Shr
Fa0/2            Altn BLK 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/4            Desg FWD 19        128.3    Shr

S2#show spanning-tree vlan 99

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID    Priority    32867
             Address     0030.F20D.D6B1
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32867  (priority 32966 sys-id-ext 99)
             Address     00E0.F7AE.7258
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.3    Shr
Fa0/2            Altn BLK 19        128.3    Shr
Fa0/3            Altn BLK 19        128.3    Shr
Fa0/4            Altn BLK 19        128.3    Shr

S3#show spanning-tree vlan 99

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID    Priority    32867
             Address     0030.F20D.D6B1
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32867  (priority 32966 sys-id-ext 99)
             Address     0030.F20D.D6B1
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.3    Shr
Fa0/2            Desg FWD 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/4            Desg FWD 19        128.3    Shr
```

Paso 2. Examinar los resultados.

Responda a las siguientes preguntas en función de los resultados.

¿Cuál es la prioridad de los switches S1, S2 y S3 en VLAN 99?

_____

¿Cuál es la prioridad de S1 en las VLAN 10, 20, 30 y 99?

_____

¿Qué puertos están bloqueando VLAN 99 en el switch raíz?

_____

¿Qué puertos están bloqueando VLAN 99 en los switches no raíz?

_____

¿Cómo selecciona STP la raíz?

_____

Dado que las prioridades del puente son las mismas, ¿qué otra cosa usa el switch para determinar la raíz?

_____

Tarea 5: Optimizar STP

Dado que hay una instancia separada del spanning-tree para cada VLAN activa, se efectúa una elección de raíz separada para cada instancia. Si las prioridades del switch por defecto se usan en la selección de la raíz, la misma raíz se elige para cada spanning-tree de la manera que se ha descrito. Esto pueda dar lugar a un diseño inferior. Entre algunos de los motivos para controlar la selección del switch raíz se incluye:

- El switch raíz es responsable de generar BPDU en STP 802.1D y es el punto de enfoque para el tráfico de control de spanning-tree. El switch raíz debe poder controlar esta carga adicional.
- La ubicación de la raíz define las rutas conmutadas activas en la red. Es probable que una ubicación aleatoria dé lugar a rutas subóptimas. Idealmente, la raíz se encuentra en la capa de distribución.
- Considere la topología que se utiliza en esta actividad. De los seis enlaces troncales configurados, sólo dos transportan tráfico. Si bien esto evita los bucles, representa un uso ineficaz de los recursos. Dado que la raíz puede definirse en función de la VLAN, es posible que algunos puertos estén bloqueando elementos para una VLAN y reenviando elementos a otra. Esto se demuestra a continuación.

En este ejemplo, se ha determinado que la selección de la raíz mediante valores por defecto resultó en una utilización ineficaz de los enlaces troncales disponibles del switch. Por lo tanto, es necesario obligar a otro switch a convertirse en el switch raíz para VLAN 99, a fin de imponer el uso compartido de cargas en los enlaces troncales.

En los resultados de ejemplo que se indican a continuación, el switch raíz por defecto para todas las VLAN es S3.

La selección del switch raíz se logra al cambiar la prioridad del spanning-tree para la VLAN. Como se ha observado, la prioridad por defecto es 32768 más el ID de la VLAN. El número menor indica una prioridad más alta para la selección de la raíz. Establezca la prioridad para VLAN 99 de S3 en 4096.

```
S1(config)#spanning-tree vlan 99 priority 4096
S1(config)#exit
```

Permita que los switches vuelvan a calcular el spanning-tree y, a continuación, compruebe el árbol de la VLAN 99 del switch S3 (la raíz de VLAN 99 original) y del switch 1 (el switch no raíz seleccionado para convertirse en la raíz nueva de VLAN 99).

```
S3#show spanning-tree vlan 99

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID    Priority    4195
             Address     0050.0F68.146E
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32867  (priority 32966 sys-id-ext 99)
             Address     0030.F20D.D6B1
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Desg FWD 19        128.3    Shr
Fa0/1            Root FWD 19        128.3    Shr
Fa0/2            Altn BLK 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr

S1#show spanning-tree vlan 99

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID    Priority    4195
             Address     0050.0F68.146E
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4195  (priority 4294 sys-id-ext 99)
             Address     0050.0F68.146E
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Desg FWD 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/2            Desg FWD 19        128.3    Shr
Fa0/1            Desg FWD 19        128.3    Shr
```

¿Qué switch es la raíz para VLAN 99?

_____

¿Qué puertos están bloqueando el tráfico VLAN 99 en la nueva raíz?

_____

¿Qué puertos están bloqueando ahora el tráfico VLAN 99 en la raíz anterior?

_____

Compare el spanning-tree de VLAN 99 de S1 anterior con el spanning-tree de VLAN 10 de S1.

```
S1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     0030.F20D.D6B1
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
  Bridge ID  Priority    32778  (priority 32788 sys-id-ext 10)
             Address     0050.0F68.146E
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Desg FWD 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/2            Altn BLK 19        128.3    Shr
Fa0/1            Root FWD 19        128.3    Shr
```

Tenga en cuenta que S1 ahora puede usar los cuatro puertos para el tráfico de VLAN 99, siempre y cuando no estén bloqueados en el otro extremo del enlace troncal. No obstante, la topología del spanning-tree original, con uno de los cuatro puertos S1 en el modo de bloqueo, aún está se aplica a las otras cuatro VLAN activas. Al configurar grupos de VLAN para que usen enlaces troncales diferentes como su ruta de envío primaria, se conserva la redundancia de enlaces troncales de migración tras error, sin tener que dejar enlaces troncales sin utilizar.

Actividad PT 5.5.3: Resolución de problemas del protocolo spanning tree

Diagrama de topología

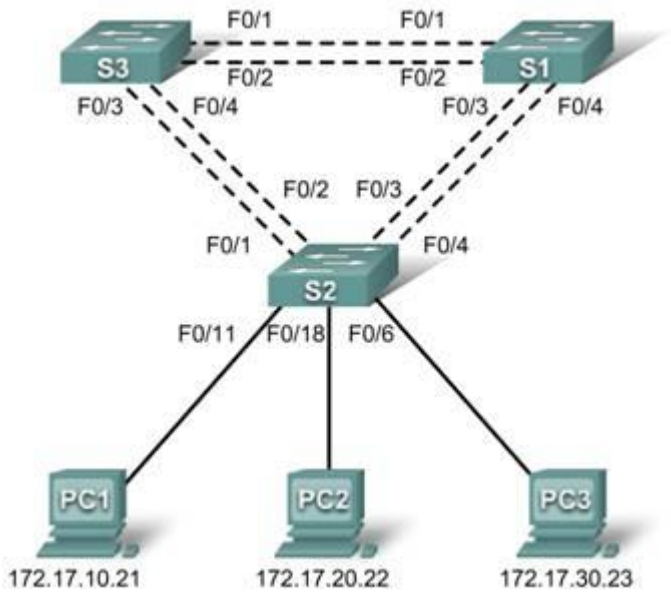


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
S1	**VLAN 99**	172.17.99.11	255.255.255.0	No aplicable
S2	**VLAN 99**	172.17.99.12	255.255.255.0	No aplicable
S3	**VLAN 99**	172.17.99.13	255.255.255.0	No aplicable
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

Asignaciones de puertos: S2

Puertos	Asignaciones	Red
Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN nativa 99)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Guests(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

- Identificar el estado inicial de todos los enlaces troncales
- Corregir el origen del problema
- Documentar la configuración del switch

Escenario

El usuario es el responsable del funcionamiento de la LAN conmutada redundante que se muestra en el diagrama de topología. Se ha observado una mayor latencia durante los momentos de uso pico y un análisis se concentra en los enlaces troncales congestionados. Se reconoce que, de los seis enlaces troncales configurados, sólo dos reenvían paquetes en la configuración STP por defecto actualmente en ejecución. La solución para este problema requiere un uso más eficaz de los enlaces troncales disponibles.

Esta actividad se completa cuando todos los enlaces troncales con cable transportan tráfico y los tres switches participan en el balanceo de carga por VLAN para las tres VLAN del usuario.

Tarea 1: Identificar el estado inicial de todos los enlaces troncales

En cada uno de los switches, muestre la tabla del spanning-tree mediante el comando **show spanning-tree**. Observe los puertos que reenvían elementos en cada switch e identifique los enlaces troncales que no se usan en la configuración por defecto. Se puede usar el diagrama de topología de red para documentar el estado inicial de todos los puertos de enlace troncal.

Tarea 2: Corregir el origen del problema

Modifique la configuración del spanning-tree de modo que los tres enlaces troncales estén en uso. Se debe suponer que las tres LAN de usuario (10, 20 y 30) transportan una cantidad igual de tráfico. Busque una solución que tenga un conjunto diferente de puertos que reenvían elementos a cada una de las tres VLAN de usuario.

Para que esta actividad sea calificada correctamente, se debe cumplir con las siguientes pautas:

- S1 es la raíz para VLAN 10 (prioridad 4096) y la raíz de respaldo para VLAN 20 (prioridad 16384)
- S2 es la raíz para VLAN 20 (prioridad 4096) y la raíz de respaldo para VLAN 30 (prioridad 16384)
- S3 es la raíz para VLAN 30 (prioridad 4096) y la raíz de respaldo para VLAN 10 (prioridad 16384)

Tarea 3: Documentar la configuración del switch

Cuando haya finalizado la solución, capture los resultados del comando **show run** y guárdelos en un archivo de texto para cada switch.

Actividad PT 5.6.1: Desafío de habilidades de Integración de Packet Tracer

Diagrama de topología

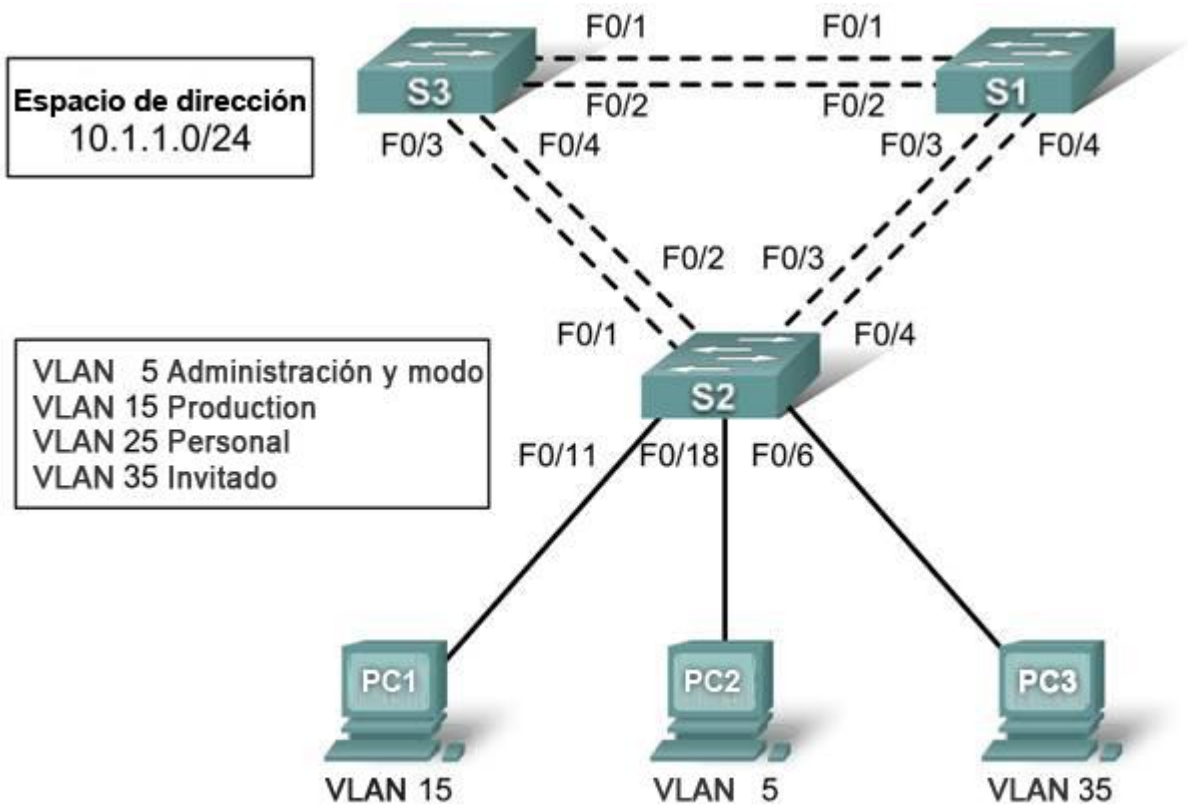


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
S1	VLAN 5			
S2	VLAN 5			
S3	VLAN 5			
PC1	NIC			
PC2	NIC			
PC3	NIC			

Objetivos de aprendizaje

- Diseñar y documentar un esquema de direccionamiento
- Configurar y verificar las configuraciones básicas del dispositivo
- Configurar VTP
- Configurar enlaces troncales
- Configurar las VLAN
- Asignar VLAN a puertos
- Configurar STP
- Configure los equipos PC host

Introducción

En esta actividad, se configurará una red redundante con VTP, VLAN y STP. Además, se diseñará un esquema de direccionamiento en función de los requisitos de usuario. Las VLAN de esta actividad son diferentes de las que se han observado en los capítulos anteriores. Es importante saber que la VLAN de administración y por defecto no tiene que ser 99. Puede ser cualquier número seleccionado por el usuario. Por lo tanto, en esta actividad se usará la VLAN 5.

Tarea 1: Diseñar y documentar un esquema de direccionamiento

El esquema de direccionamiento debe cumplir con los siguientes requisitos:

- La VLAN Production necesita 100 direcciones de host
- La VLAN Staff necesita 50 direcciones de host
- VLAN Guest necesita 20 direcciones de host
- La VLAN Management&Native necesita 10 direcciones de host

Tarea 2: Configurar y verificar las configuraciones básicas del dispositivo

Paso 1. Configurar los comandos básicos.

Configure cada switch con los siguientes comandos básicos. Packet Tracer sólo califica los nombres de host y las gateways predeterminadas.

- Nombres de host
- Mensaje
- Contraseña secreta de enable
- Configuraciones de la línea
- Encriptación del servicio
- Gateways predeterminadas

Paso 2. Configurar la interfaz VLAN de administración en S1, S2 y S3.

Cree y habilite VLAN 5 de la interfaz en cada switch. Use el esquema de direccionamiento para obtener la configuración de direcciones.

Paso 3. Verificar los resultados.

El porcentaje final del usuario debe ser del 18%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 3: Configurar VTP

Paso 1. Configurar el modo VTP en los tres switches.

Configure S1 como el servidor. Configure S2 y S3 como clientes.

Paso 2. Configurar el nombre de dominio VTP en los tres switches.

Use **XYZCORP** como el nombre de dominio de VTP.

Paso 3. Configurar la contraseña de dominio de VTP en los tres switches.

Use **westbranch** como la contraseña de dominio de VTP.

Paso 4. Verificar los resultados.

El porcentaje final del usuario debe ser del 30%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 4: Configurar enlaces troncales

Paso 1. Configurar enlaces troncales en S1, S2 y S3.

Configure las interfaces correspondientes en el modo de enlace troncal y asigne VLAN 5 como la VLAN nativa.

Paso 2. Verificar los resultados.

El porcentaje final del usuario debe ser del 66%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 5: Configurar las VLAN

Paso 1. Crear las VLAN en S1.

Cree las siguientes VLAN en S1 solamente y asígneles nombre. VTP publicará las nuevas VLAN en S1 y S2.

- VLAN 15 **Production**
- VLAN 25 **Staff**
- VLAN 35 **Guest(Default)**
- VLAN 5 **Management&Native**

Paso 2. Verificar que las VLAN se hayan enviado a S2 y S3.

Use los comandos adecuados para verificar que S2 y S3 ahora tienen las VLAN creadas en S1. Es probable que demore algunos minutos hasta que Packet Tracer simule las publicaciones de VTP.

Paso 3. Verificar los resultados.

El porcentaje final del usuario debe ser del 72%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 6: Asignar VLAN a puertos

Paso 1. Asignar VLAN a los puertos de acceso en S2.

Asigne los puertos de acceso de PC a VLAN:

- VLAN 15: PC1 conectado a Fa0/11
- VLAN 25: PC2 conectado a Fa0/18
- VLAN 35: PC3 conectado a Fa0/6

Paso 2. Verificar la implementación de VLAN.

Use el comando correspondiente para verificar la implementación de VLAN.

Paso 3. Verificar los resultados.

El porcentaje final del usuario debe ser del 81%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 7: Configurar STP

Paso 1. Asegúrese de que S1 sea el puente raíz.

Defina el nivel de prioridad en S1 de modo que siempre sea el puente raíz para todas las VLAN.

Paso 2. Asegúrese de que S1 sea el puente raíz.

Paso 3. Verificar los resultados.

El porcentaje final del usuario debe ser del 87%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 8: Configurar los equipos PC host

Paso 1. Configurar los equipos PC host.

Use el esquema de direccionamiento para configurar la interfaz Fast Ethernet y la gateway predeterminada de los equipos PC.

Paso 2. Verificar los resultados.

El porcentaje final del usuario debe ser del 100%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Actividad PT 6.2.2.4: Configuración de enrutamiento tradicional entre VLAN

Diagrama de topología

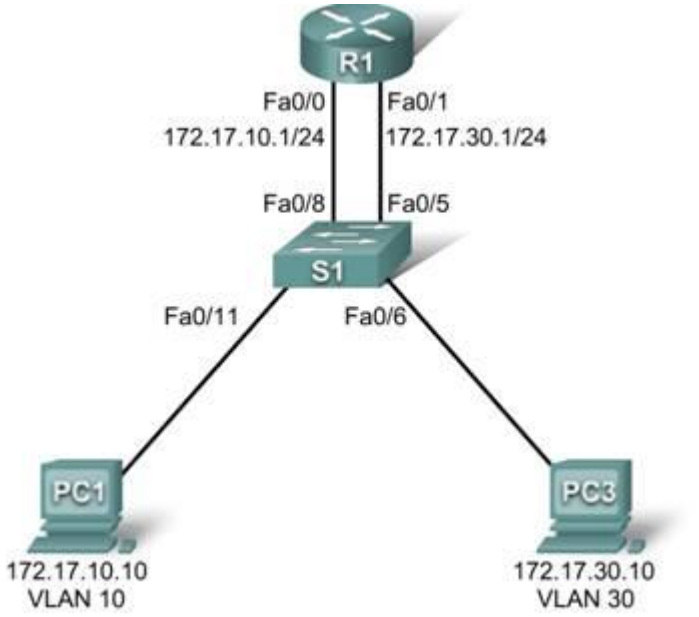


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
R1	**Fa0/0**	172.17.10.1	255.255.255.0	No aplicable
	Fa0/1	172.17.30.1	255.255.255.0	No aplicable
PC1	**NIC**	172.17.10.10	255.255.255.0	172.17.10.1
PC3	**NIC**	172.17.30.10	255.255.255.0	172.17.30.1

Objetivos de aprendizaje

- Probar la conectividad sin enrutamiento entre VLAN
- Agregar VLAN a un switch
- Configurar el direccionamiento IP en un router
- Probar la conectividad con enrutamiento entre VLAN

Introducción

En esta actividad, se configurará el enrutamiento tradicional entre VLAN mediante la configuración de dos interfaces Fast Ethernet en un router. R1 tiene dos conexiones a S1, una para cada VLAN. S1 y R1 ya tienen las configuraciones básicas. La contraseña EXEC del usuario es **cisco** y la contraseña EXEC privilegiado es **class**. La configuración se completará mediante la adición de VLAN a S1 y la asignación de VLAN a los puertos correctos. Luego, se deberá configurar R1 con direccionamiento IP. En el enrutamiento tradicional entre VLAN, no es necesario efectuar configuraciones adicionales de VLAN en R1.

Tarea 1: Probar la conectividad sin enrutamiento entre VLAN

Paso 1. Hacer ping entre PC1 y PC3.

Espere la convergencia del switch. Las luces de enlace del switch que conecta PC1 y PC3 cambian de color ámbar a verde. Cuando las luces de enlace estén de color verde, haga ping entre PC1 y PC3. Dado que los dos equipos PC están en redes separadas y el router no está configurado, no pueden comunicarse entre sí, de modo que el ping falla.

Paso 2. Cambiar al modo de simulación para monitorizar los pings.

- Para cambiar al modo de simulación, haga clic en la ficha **Simulation** o presione **Mayús+S**.
- Haga clic en **Capture/Forward** para conocer los pasos que recorre el ping entre PC1 y PC3.
- Tenga en cuenta que el ping no puede atravesar el switch.

El porcentaje final del usuario debe ser del 0%.

Tarea 2: Agregar VLAN

Paso 1. Crear VLAN en S1.

Cree dos VLAN en S1, una para PC1 y otra para PC3. PC1 pertenece a la VLAN 10 y PC3 pertenece a la VLAN 30. Para crear las VLAN, ejecute los comandos **vlan 10** y **vlan 30** en el modo de configuración global.

```
S2#configure terminal
S2(config)#vlan 10
S2(config-vlan)#vlan 30
```

Para comprobar si se crearon las VLAN, ejecute el comando **show vlan brief** desde el indicador de EXEC privilegiado.

```
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
                                                Gig1/1, Gig1/2
10   VLAN0010                         active
30   VLAN0030                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Paso 2. Asignar las VLAN a puertos.

Cada puerto del switch se asigna a una VLAN para permitir la comunicación entre VLAN.

Asigne los puertos del switch de la siguiente manera:

- Asigne las interfaces Fa0/5 y Fa0/6 a la VLAN 30.
- Asigne las interfaces Fa0/8 y Fa0/11 a la VLAN 10.

Para asignar una VLAN a un puerto, entre en la configuración de la interfaz. Para Fa0/8, el comando es **interface fa0/8**. El comando **switchport access vlan 10** asigna la VLAN 10 a ese puerto. El comando **switchport mode access** define el puerto en modo de acceso.

```
S2(config)#interface fa0/8
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
```

Repita los pasos anteriores para Fa0/5, Fa0/6 y Fa0/11 y asigne las VLAN correctas a cada interfaz.

Paso 3. Probar la conectividad entre PC1 y PC3.

Ejecute un ping entre PC1 y PC3. El ping debe provocar errores.

Paso 4. Verificar los resultados.

El porcentaje final del usuario debe ser del 45%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 3: Configurar el direccionamiento IP

Paso 1. Configurar el direccionamiento IP en R1.

Configure la interfaz Fa0/0 de R1 con la dirección IP 172.17.10.1 y la máscara de subred 255.255.255.0.

Configure la interfaz Fa0/1 con la dirección IP 172.17.30.1 y la máscara de subred 255.255.255.0.

Ejecute el comando **no shutdown** en ambas interfaces para activarlas.

```
R1(config)#interface fa0/0
R1(config-if)#ip address 172.17.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#interface fa0/1
R1(config-if)#ip address 172.17.30.1 255.255.255.0
R1(config-if)#no shutdown
```

Paso 2. Verificar los resultados.

El porcentaje final del usuario debe ser del 100%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 4: Probar la conectividad nuevamente

Paso 1. Hacer ping entre PC1 y PC3.

Espere la convergencia de STP. Luego haga ping desde PC1 a PC3. El ping debe realizarse correctamente.

Paso 2. Cambiar al modo de simulación para monitorizar los pings.

- Para cambiar al modo de simulación, haga clic en la ficha **Simulation** o presione **Mayús+S**.
- Haga clic en **Capture/Forward** para conocer los pasos que recorre el ping entre PC1 y PC3.
- Espere mientras el ping viaja desde PC1 hasta S1, y luego hasta R1 y regresa a S1 y, por último, hasta PC3.

Actividad PT 6.2.2.5: Configuración del enrutamiento del router único entre VLAN

Diagrama de topología

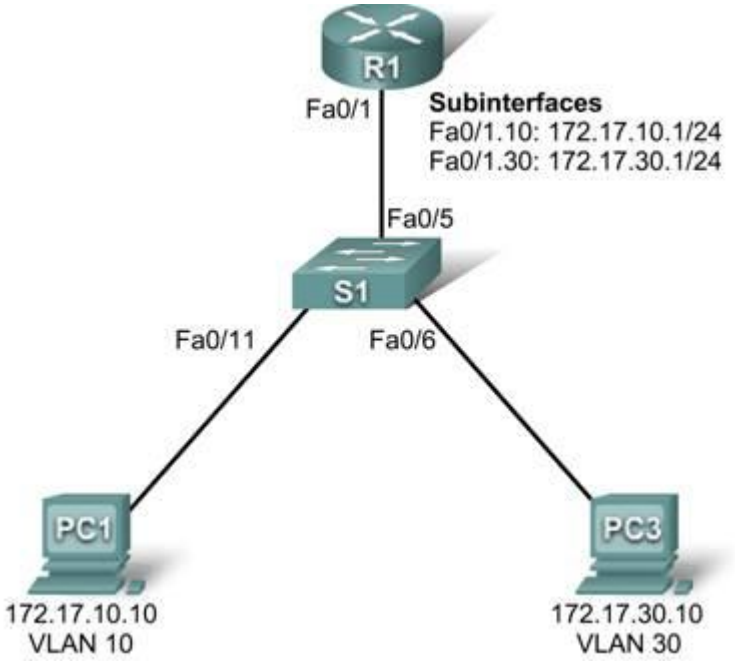


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
R1	**Fa0/1.10**	172.17.10.1	255.255.255.0	No aplicable
	Fa0/1.30	172.17.30.1	255.255.255.0	No aplicable
PC1	**NIC**	172.17.10.10	255.255.255.0	172.17.10.1
PC3	**NIC**	172.17.30.10	255.255.255.0	172.17.30.1

Objetivos de aprendizaje

- Probar la conectividad sin enrutamiento entre VLAN
- Agregar VLAN a un switch
- Configurar el direccionamiento IP en un router
- Probar la conectividad con enrutamiento entre VLAN

Introducción

En esta actividad, se configurará el enrutamiento entre VLAN con router-on-a-stick. R1 tiene una conexión a S1. S1 y R1 ya tienen las configuraciones básicas. La contraseña EXEC del usuario es **cisco** y la contraseña EXEC privilegiado es **class**. La configuración se completará mediante la adición de VLAN a S1 y la asignación de VLAN a los puertos correctos. a continuación, se configurará R1 con subinterfaces, encapsulación 802.1Q y direccionamiento IP.

Tarea 1: Probar la conectividad sin enrutamiento entre VLAN

Paso 1. Hacer ping entre PC1 y PC3.

Espere la convergencia del switch. Las luces de enlace del switch que conecta PC1 y PC3 cambian de color ámbar a verde. Cuando las luces de enlace estén de color verde, haga ping entre PC1 y PC3. Dado que los dos equipos PC están en redes separadas y no se ha configurado el enrutamiento entre VLAN, no pueden comunicarse entre sí, de modo que el ping falla.

Paso 2. Cambiar al modo de simulación para monitorizar los pings.

- Para cambiar al modo de simulación, seleccione la ficha **Simulation** o presione **Mayús+S**.
- Haga clic en **Capture/Forward** para conocer los pasos que recorre el ping entre PC1 y PC3.
- Tenga en cuenta que el ping no puede atravesar el switch.

El porcentaje final del usuario debe ser del 0%.

Tarea 2: Agregar VLAN

Paso 1. Crear VLAN en S1.

Cree la VLAN 10 y la VLAN 30 en S1. PC1 pertenece a la VLAN 10 y PC2 pertenece a la VLAN 30. Para crear las VLAN, ejecute los comandos **vlan 10** y **vlan 30** en el modo de configuración global.

```
S1#configure terminal
S1(config)#vlan 10
S1(config-vlan)#vlan 30
```

Para comprobar si se crearon las VLAN, ejecute el comando **show vlan brief** desde el indicador de EXEC privilegiado.

```
S1#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
                                                 Gig1/1, Gig1/2
10   VLAN0010                          active
30   VLAN0030                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Paso 2. Asignar las VLAN a puertos.

Cada puerto se asigna a una VLAN para permitir la comunicación entre VLAN. La interfaz Fa0/11 pertenece a la VLAN 10 y la interfaz Fa0/6 pertenece a la VLAN 30.

Para asignar una VLAN a un puerto, entre al modo de configuración de la interfaz. Para Fa0/11, el comando es **interface fa0/11**. Ejecute el comando **switchport mode access** para establecer el puerto en modo de acceso. El comando **switchport access vlan 10** asigna la VLAN 10 a ese puerto.

```
S1(config-if)#interface fa0/11
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
```

Repita los pasos de la interfaz Fa0/6 para la VLAN 30.

```
S1(config)#interface fa0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
```

El puerto Fa0/5 en S1 está definido en enlace troncal, lo que le permite transmitir información desde las VLAN 10 y 30. Desde la interfaz Fa0/5, ejecute el comando **switchport mode trunk** para establecer el puerto en enlace troncal. Packet Tracer no califica este comando, pero es necesario para configurar el enrutamiento entre VLAN.

```
S1(config-if)#interface fa0/5
S1(config-if)#switchport mode trunk
```

Paso 3. Probar la conectividad entre PC1 y PC3.

Ejecute un ping entre PC1 y PC3. El ping debe provocar errores.

Paso 4. Verificar los resultados.

El porcentaje final del usuario debe ser del 27%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 3: Configurar el direccionamiento IP

Paso 1. Configurar subinterfaces con encapsulación 802.1Q.

Cree dos subinterfaces en R1: Fa0/1.10 y Fa0/1.30. Estas subinterfaces se asignan a las VLAN. Para crear la primera subinterfaz, entre al modo de configuración de interfaz para Fa0/1.10 ejecutando el comando **interface fa0/1.10**. Tenga en cuenta que el indicador del router cambia.

Mientras se encuentra en el modo de configuración de subinterfaz, ejecute el comando **encapsulation dot1Q 10** para establecer el tipo de encapsulación en 802.1Q y asignar la VLAN 10 a la interfaz virtual.

Asigne la dirección IP correcta al puerto. Para Fa0/1.10, es 172.17.10.1 con una máscara de subred de 255.255.255.0.

Repita estos pasos para la interfaz Fa0/1.30 usando la dirección IP y el ID de VLAN correctos.

```
R1(config)#interface fa0/1,10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0
R1(config-subif)#interface fa0/1.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 172.17.30.1 255.255.255.0
```

Paso 2. Verificar los resultados.

El porcentaje final del usuario debe ser del 100%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 4: Probar la conectividad nuevamente

Paso 1. Hacer ping entre PC1 y PC3.

Haga ping desde PC1 a PC3. El ping debe realizarse correctamente.

Paso 2. Cambiar al modo de simulación para monitorizar los pings.

- Para cambiar al modo de simulación, seleccione la ficha **Simulation** o presione **Mayús+S**.
- Haga clic en **Capture/Forward** para conocer los pasos que recorre el ping entre PC1 y PC3.
- Observe cómo el ping viaja desde PC1 hasta S1, y luego hasta R1 y regresa a S1 y, por último, hasta PC3.

Actividad PT 6.3.3: Resolución de problemas de enrutamiento entre VLAN

Diagrama de topología

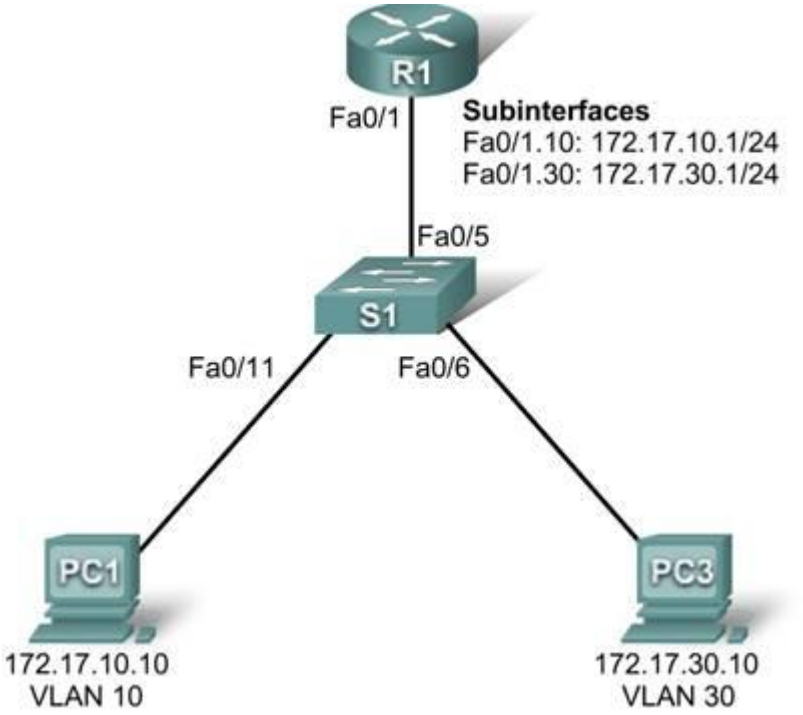


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
R1	**Fa0/1.10**	172.17.10.1	255.255.255.0	No aplicable
	Fa0/1.30	172.17.30.1	255.255.255.0	No aplicable
PC1	**NIC**	172.17.10.10	255.255.255.0	172.17.10.1
PC3	**NIC**	172.17.30.10	255.255.255.0	172.17.30.1

Objetivos de aprendizaje

- Probar la conectividad entre los equipos PC y un router
- Recopilar datos sobre el problema
- Implementar la solución y probar la conectividad

Introducción

En esta actividad, se realizará la resolución de problemas de conectividad entre PC1 y PC3. La actividad finaliza cuando se alcance el 100% y los dos equipos PC puedan hacer ping entre sí. Cualquier solución que implemente deberá ajustarse al diagrama de topología.

Tarea 1: Probar la conectividad entre los equipos PC y un router

Use la herramienta **Add Simple PDU** para hacer ping entre dos equipos PC de la misma VLAN. Las siguientes pruebas deben realizarse correctamente al finalizar esta actividad:

- PC1 puede hacer ping a R1
- PC3 puede hacer ping a R1
- PC1 puede hacer ping a PC3

¿PC1 puede hacer ping a R1? _____

¿PC3 puede hacer ping a R1? _____

¿PC1 puede hacer ping a PC3? _____

Tarea 2: Recopilar datos sobre el problema

Paso 1. Verificar la configuración en los equipos PC.

¿Son correctas las siguientes configuraciones para cada equipo PC?

- Dirección IP
- Máscara de subred
- Gateway predeterminada

Paso 2. Verificar la configuración en S1.

¿Son correctas las configuraciones en el switch? Asegúrese de verificar lo siguiente:

- Los puertos están asignados a las VLAN correctas
- Los puertos se ha configurado para el modo correcto
- Los puertos están conectados al dispositivo correcto

Paso 3. Verificar la configuración en R1.

¿Son correctas las configuraciones en el router? Asegúrese de verificar lo siguiente:

- Direcciones IP
- Estado de la interfaz
- Encapsulación y asignación de la VLAN

Paso 4. Documentar el problema y sugerir soluciones.

¿Por qué falló la conectividad entre los equipos PC? ¿Cuáles son las soluciones? Es probable que haya más de un problema y más de una solución. Todas las soluciones deberán ajustarse al diagrama de topología.

PC1 y/o PC3

Problema: _____

Solución: _____

S1

Problema: _____

Solución: _____

R1

Problema: _____

Solución: _____

Tarea 3: Implementar la solución y probar la conectividad

Paso 1. Hacer cambios de acuerdo con las soluciones sugeridas en la Tarea 2.

Nota: Si se realizan cambios en la configuración del switch, éstos se deben hacer en el modo de tiempo real en lugar de en el modo de simulación. Esto es necesario de modo que el puerto del switch proceda al estado de reenvío.

Paso 2. Probar la conectividad entre los equipos PC y R1.

Si se modifican las configuraciones IP, se deben crear nuevos pings, dado que los pings anteriores usan la antigua dirección IP.

- PC1 debe poder hacer ping a R1
- PC3 debe poder hacer ping a R1
- PC1 debe poder hacer ping a PC3

¿PC1 puede hacer ping a R1? _____

¿PC3 puede hacer ping a R1? _____

¿PC1 puede hacer ping a PC3? _____

Si algunos pings no se realizan correctamente, regrese a la Tarea 2 para continuar con la resolución de problemas.

Paso 3. Verificar el porcentaje final.

El porcentaje final del usuario debe ser del 100%. De lo contrario, regrese al Paso 1 y continúe con la implementación de las soluciones sugeridas. No podrá hacer clic en **Check Results** y ver qué componentes obligatorios aún no se completaron.

Actividad PT 6.4.1: Enrutamiento básico entre VLAN

Diagrama de topología

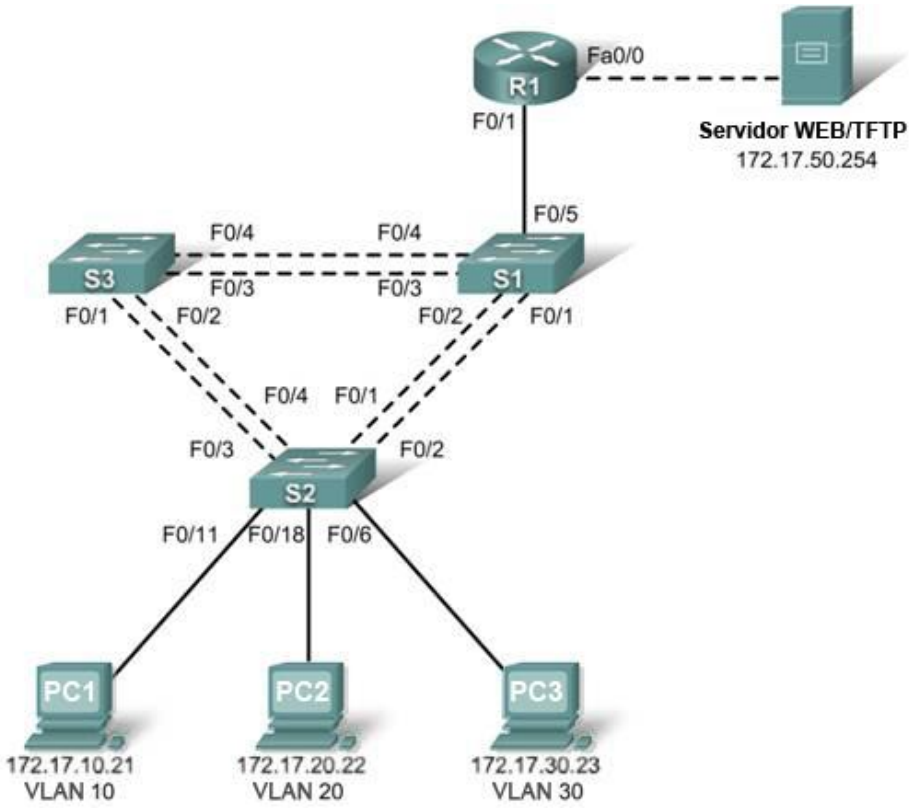


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
S1	**VLAN 99**	172.17.99.11	255.255.255.0	172.17.99.1
S2	**VLAN 99**	172.17.99.12	255.255.255.0	172.17.99.1
S3	**VLAN 99**	172.17.99.13	255.255.255.0	172.17.99.1
R1	**Fa0/0**	Consulte la tabla de configuración de interfaces		No aplicable
	Fa0/1	172.17.50.1	255.255.255.0	No aplicable
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
Server	**NIC**	172.17.50.254	255.255.255.0	172.17.50.1

Asignaciones de puertos: S2

Puertos	Asignaciones	Red
Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN nativa 99)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Guests(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

Tabla de configuración de subinterfaces: R1

Interfaz	Asignaciones	Dirección IP
Fa0/0.1	VLAN 1	172.17.1.1 /24
Fa0/0.10	VLAN 10	172.17.10.1 /24
Fa0/0.20	VLAN 20	172.17.20.1 /24
Fa0/0.30	VLAN 30	172.17.30.1 /24
Fa0/0.99	VLAN 99	172.17.99.1 /24

Objetivos de aprendizaje

- Realizar las configuraciones básicas del switch
- Configurar las interfaces Ethernet en los equipos PC host
- Configurar VTP en los switches
- Configurar el router y la LAN de servidor remoto

Introducción

En esta actividad, se realizarán las configuraciones básicas del switch, se configurará el direccionamiento en los equipos PC, se configurará VTP y se establecerá el enrutamiento entre VLAN.

Tarea 1: Realizar configuraciones de switches básicas

Configure los switches S1, S2 y S3 según la tabla de direccionamiento y las siguientes pautas:

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

```
Switch>enable
Switch#config term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#no ip domain-lookup
S1(config)#ip default-gateway 172.17.99.1
```

```
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
```

Tarea 2: Configurar las interfaces Ethernet en los equipos PC host

Configure las interfaces Ethernet de PC1, PC2 y PC3 con las direcciones IP de la tabla de direccionamiento.

Tarea 3: Configurar VTP en los switches

Paso 1. Habilitar los puertos del usuario en S2 en el modo de acceso.

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

Paso 2. Configurar VTP.

Configure VTP en los tres switches según la siguiente tabla. Recuerde que los nombres y las contraseñas de dominio VTP distinguen entre mayúsculas y minúsculas.

Nombre del switch	Modo de funcionamiento VTP	Dominio VTP	Contraseña de VTP
S1	Server	Lab5	cisco
S2	Client	Lab5	cisco
S3	Client	Lab5	cisco

```
S1(config)#vtp mode server
Device mode already VTP SERVER.
S1(config)#vtp domain Lab6
Changing VTP domain name from NULL to Lab6
S1(config)#vtp password cisco
Setting device VLAN database password to cisco
S1(config)#end
```

```
S2(config)#vtp mode client
Setting device to VTP CLIENT mode
S2(config)#vtp domain Lab6
Changing VTP domain name from NULL to Lab6
S2(config)#vtp password cisco
Setting device VLAN database password to cisco
S2(config)#end
```

```
S3(config)#vtp mode client
Setting device to VTP CLIENT mode
S3(config)#vtp domain Lab6
Changing VTP domain name from NULL to Lab6
S3(config)#vtp password cisco
Setting device VLAN database password to cisco
S3(config)#end
```

Paso 3. Configurar puertos de enlaces troncales y diseñar la VLAN nativa para los enlaces troncales.

Configure de Fa0/1 a Fa0/5 como puertos de enlaces troncales y designe a la VLAN 99 como la VLAN nativa para estos enlaces troncales. Cuando se comenzó esta actividad, estos puertos estaban deshabilitados y deben volver a habilitarse mediante el comando **no shutdown**.

Sólo se muestran los comandos para la interfaz FastEthernet0/1 en cada switch, pero los comandos deben aplicarse hasta la interfaz FastEthernet0/5.

```
S1(config)#interface fa0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#no shutdown
S1(config)#end

S2(config)#interface fa0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 99
S2(config-if)#no shutdown
S2(config-if)#end

S3(config)#interface fa0/1
S3(config-if#switchport mode trunk
S3(config-if)#switchport trunk native vlan 99
S3(config-if)#no shutdown
S3(config-if)#end
```

Paso 4. Configurar el servidor VTP con las VLAN.

Configure las siguientes VLAN en el servidor VTP.

VLAN	Nombre de VLAN
VLAN 99	management
VLAN 10	faculty-staff
VLAN 20	students
VLAN 30	guest

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

Verifique que las VLAN se hayan creado en S1 mediante el comando show vlan brief.

Paso 5. Comprobar si las VLAN creadas en S1 se han distribuido a S2 y S3.

Use el comando **show vlan brief** en S2 y S3 para verificar que las cuatro VLAN se hayan distribuido a los switches cliente.

```
S2#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

S3#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    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
                                                 Gig1/1, Gig1/2
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
```

Paso 6. Configurar la dirección de la interfaz de administración en los tres switches.

```
S1(config)#interface vlan99
S1(config-if)#ip address 172.17.99.11 255.255.255.0

S2(config)#interface vlan99
S2(config-if)#ip address 172.17.99.12 255.255.255.0

S3(config)#interface vlan99
S3(config-if)#ip address 172.17.99.13 255.255.255.0
```

Verifique que los switches estén configurados correctamente haciendo ping entre ellos. En S1, haga ping a la interfaz de administración de S2 y S3. En S2, haga ping a la interfaz de administración de S3.

¿Los pings se realizaron correctamente? _____

En caso contrario, realice la resolución de problemas de configuración del switch y vuelva a intentarlo.

Paso 7. Asignar puertos del switch a las VLAN en S2.

Las asignaciones del puerto se indican en la tabla del comienzo de la actividad. No obstante, dado que Packet Tracer 4.11 no admite el comando **interface range**, sólo se debe asignar el primer puerto de cada intervalo.

```
S2(config)#interface fa0/6
S2(config-if)#switchport access vlan 30
S2(config-if)#interface fa0/11
S2(config-if)#switchport access vlan 10
S2(config-if)#interface fa0/18
S2(config-if)#switchport access vlan 20
S2(config-if)#end
S2#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
S2#
```

Paso 8. Verificar la conectividad entre VLAN.

Abra el indicador de comandos en los tres equipos PC.

- Haga ping desde PC1 a PC2 (172.17.20.22).
- Haga ping desde PC2 a PC3 (172.17.30.23).
- Haga ping desde PC3 a PC1 (172.17.30.21).

¿Los pings se realizaron correctamente? _____

De no ser así, ¿por qué fallan estos pings no se realizaron correctamente?

Tarea 4: Configurar el router y la LAN de servidor remoto

Paso 1. Crear una configuración básica en el router.

- Configure el router con el nombre de host R1.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de **class** en el Modo EXEC.
- Configure una contraseña de **cisco** para las conexiones de consola.
- Configure una contraseña de **cisco** para las conexiones vty.

Paso 2. Configurar la interfaz de enlaces troncales en R1.

Se ha demostrado que la conectividad entre VLAN requiere el enrutamiento en la capa de red, exactamente igual a la conectividad entre dos redes remotas. Hay numerosas opciones para la configuración del enrutamiento entre VLAN.

La primera es similar a un método de fuerza bruta. Un dispositivo L3 (un router o un switch compatible con la capa 3) se conecta a un switch de LAN con varias conexiones; una conexión independiente para cada VLAN que requiere conectividad entre VLAN. Cada uno de los puertos del switch que el dispositivo L3 utiliza se configura en una VLAN diferente en el switch. Después de que las direcciones IP se asignen a la interfaz del dispositivo L3, la tabla de enrutamiento tiene rutas conectadas directamente para todas las VLAN y se habilita el enrutamiento entre VLAN. Los límites de este método son la falta de suficientes puertos Fast Ethernet en los routers, la utilización ineficaz de los puertos en los switches y routers L3 y la excesiva conexión con cables y configuración manual. La topología que se utiliza en esta práctica de laboratorio no usa este método.

Otra opción es crear una o más conexiones Fast Ethernet entre el dispositivo L3 (el router) y el switch de capa de distribución, y configurar estas conexiones como enlaces troncales **dot1q**. Esto permite que todo el tráfico entre VLAN se transporte hacia el dispositivo de enrutamiento y desde éste, en un único enlace troncal. No obstante, la interfaz L3 se debe configurar con varias direcciones IP. Para ello, se crean interfaces virtuales denominadas subinterfaces en uno de los puertos Fast Ethernet del router y éstas se configuran de modo que sean conscientes de **dot1q**.

Para utilizar el método de configuración de subinterfaces, es necesario seguir estos pasos:

- Entre al modo de configuración de subinterfaces.
- Establezca la encapsulación de enlaces troncales.
- Asocie una VLAN con la subinterfaz.
- Asigne una dirección IP desde la VLAN a la subinterfaz.

Los comandos son los siguientes:

```
R1(config)#interface fastethernet 0/0
R1(config-if)#no shutdown
R1(config-if)#interface fastethernet 0/0.1
R1(config-subif)#encapsulation dot1q 1
R1(config-subif)#ip address 172.17.1.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/0.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 172.17.20.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/0.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 172.17.30.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/0.99
R1(config-subif)#encapsulation dot1q 99 native
R1(config-subif)#ip address 172.17.99.1 255.255.255.0
```

Tenga en cuenta los siguientes puntos en esta configuración:

- La interfaz física se habilita mediante el comando **no shutdown**, dado que las interfaces del router están desactivadas por defecto. La subinterfaz estará activada por defecto.
- La subinterfaz puede usar cualquier número que pueda describirse con 32 bits, pero se recomienda asignar el número de la VLAN como el número de interfaz; de la misma forma que se hizo aquí.
- La VLAN nativa se especifica en el dispositivo L3 de modo que será coherente con los switches. De lo contrario, la VLAN 1 es la nativa por defecto y no hay comunicación entre el router y la VLAN de administración de los switches.

Paso 3. Configurar la interfaz de LAN servidor en R1.

```
R1(config)#interface FastEthernet0/1
R1(config-if)#ip address 172.17.50.1 255.255.255.0
R1(config-if)#description server interface
R1(config-if)#no shutdown
R1(config-if)#end
```

Ahora hay seis redes configuradas. Consulte la tabla de enrutamiento en R1 para verificar que se pueden enrutar paquetes a las seis.

```
R1#show ip route
<output omitted>
```

```
Gateway of last resort is not set

     172.17.0.0/24 is subnetted, 6 subnets
C       172.17.1.0 is directly connected, FastEthernet0/0.1
C       172.17.10.0 is directly connected, FastEthernet0/0.10
C       172.17.20.0 is directly connected, FastEthernet0/0.20
C       172.17.30.0 is directly connected, FastEthernet0/0.30
C       172.17.50.0 is directly connected, FastEthernet0/1
C       172.17.99.0 is directly connected, FastEthernet0/0.99
```

Si la tabla de enrutamiento no muestra las seis redes, realice la resolución de problemas de configuración y corrija los problemas antes de continuar.

Paso 4. Verificar el enrutamiento entre distintas VLAN.

Desde PC1, compruebe que puede hacer ping al servidor remoto (172.17.50.254) y a los otros dos hosts (172.17.20.22 y 172.17.30.23). Es posible que deba hacer ping varias veces hasta que se establezca la ruta de extremo a extremo.

Los pings deberían realizarse correctamente. De lo contrario, realice la resolución de problemas de la configuración. Asegúrese de que las gateways por defecto se hayan configurado en todos los switches y equipos PC.

Tarea 5: Reflexión

En la Tarea 4, la VLAN 99 se configuró como VLAN nativa en la configuración de la interfaz Fa0/0.99 del router. ¿Por qué los paquetes del router o los hosts provocarían errores al intentar llegar a las interfaces de administración del switch, si la VLAN nativa sigue siendo la VLAN por defecto?

Actividad PT 6.4.2: Desafío de enrutamiento entre VLAN

Diagrama de topología

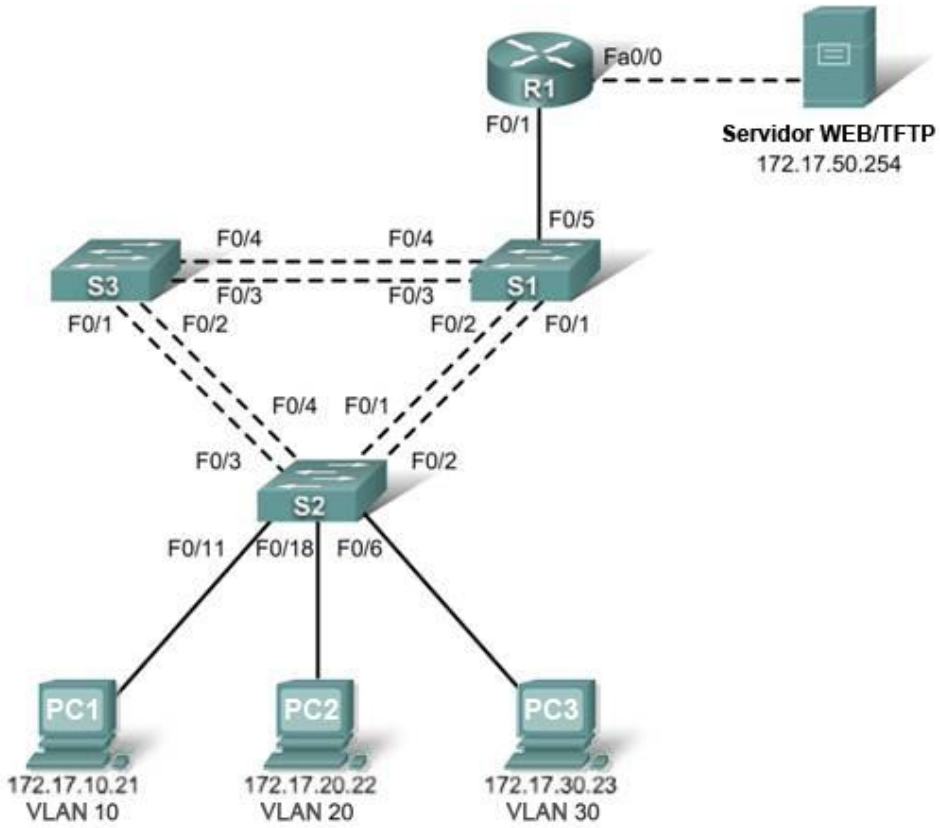


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
S1	**VLAN 99**	192.168.99.11	255.255.255.0	192.168.99.1
S2	**VLAN 99**	192.168.99.12	255.255.255.0	192.168.99.1
S3	**VLAN 99**	192.168.99.13	255.255.255.0	192.168.99.1
R1	**Fa0/0**	192.168.50.1	255.255.255.0	No aplicable
	Fa0/1	Consulte la tabla de configuración de interfaces		No aplicable
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
Server	**NIC**	192.168.50.254	255.255.255.0	192.168.50.1

Asignaciones de puertos: S2

Puertos	Asignaciones	Red
Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN nativa 99)	192.168.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Sales	192.168.30.0 /24
Fa0/11 – 0/17	VLAN 10 – R&D	192.168.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Engineering	192.168.20.0 /24

Tabla de configuración de interfaces: R1

Interfaz	Asignaciones	Dirección IP
Fa0/0.1	VLAN 1	192.168.1.1 /24
Fa0/0.10	VLAN 10	192.168.10.1 /24
Fa0/0.20	VLAN 20	192.168.20.1 /24
Fa0/0.30	VLAN 30	192.168.30.1 /24
Fa0/0.99	VLAN 99	192.168.99.1 /24

Objetivos de aprendizaje

- Realizar las configuraciones básicas del switch
- Configurar las interfaces Ethernet en el servidor y en los equipos PC host
- Configurar VTP en los switches
- Configurar el router

Introducción

En esta actividad, se realizarán las configuraciones básicas del switch, se configurará el VTP, se establecerán los enlaces troncales y las subinterfaces y se demostrará el enrutamiento entre VLAN.

Tarea 1: Realizar configuraciones de switches básicas

Configure los switches S1, S2 y S3 según las siguientes pautas y guarde todas las configuraciones:

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

Tarea 2: Configurar las interfaces Ethernet en el servidor y en los equipos PC host

Configure las interfaces Ethernet de PC1, PC2 y PC3 y el servidor TFTP/Web remoto con las direcciones IP de la tabla de direccionamiento. Conecte estos dispositivos usando los cables y las interfaces correctos.

Tarea 3: Configurar VTP en los switches

Paso 1. Configurar VTP en los tres switches.

Use la siguiente tabla para configurar los switches. Recuerde que los nombres y las contraseñas de dominio VTP distinguen entre mayúsculas y minúsculas.

Nombre del switch	Modo de funcionamiento VTP	Dominio VTP	Contraseña de VTP
S1	Server	Lab5	cisco
S2	Client	Lab5	cisco
S3	Client	Lab5	cisco

Paso 2. Configurar puertos de enlaces troncales y diseñar la VLAN nativa para los enlaces troncales.

Configure de Fa0/1 a Fa0/5 como puertos de enlaces troncales y designe a la VLAN 99 como la VLAN nativa para estos enlaces troncales.

Paso 3. Configurar las VLAN en el servidor VTP.

Configure las siguientes VLAN en el servidor VTP.

VLAN	Nombre de VLAN
VLAN 99	Management
VLAN 10	R&D
VLAN 20	Engineering
VLAN 30	Sales

Verifique que las VLAN se hayan creado en S1 mediante el comando **show vlan brief**.

Paso 4. Comprobar si las VLAN creadas en S1 se han distribuido a S2 y S3.

Use el comando **show vlan brief** en S2 y S3 para verificar que las cuatro VLAN se hayan distribuido a los switches cliente.

Paso 5. Configurar la dirección de la interfaz de administración en los tres switches.

Consulte la tabla de direccionamiento y asigne el direccionamiento IP a los tres switches.

Verifique que los switches estén configurados correctamente haciendo ping entre ellos. En S1, haga ping a la interfaz de administración de S2 y S3. En S2, haga ping a la interfaz de administración de S3.

¿Los pings se realizaron correctamente? _____

En caso contrario, realice la resolución de problemas de configuración del switch y corrija los errores.

Paso 6. Asignar puertos del switch a las VLAN en S2.

Consulte la tabla de asignaciones de puertos para asignar puertos a la VLAN en S2.

Paso 7. Verificar la conectividad entre VLAN.

Abra las ventanas de comandos en los tres host conectados a S2. Haga ping desde PC1 (192.168.10.21) a PC2 (192.168.20.22). Haga ping desde PC2 a PC3 (192.168.30.23).

¿Los pings se realizaron correctamente? _____

De no ser así, ¿por qué estos pings no se realizaron correctamente?

_____

Tarea 4: Configurar el router

Paso 1. Crear una configuración básica en el router.

- Configure el router con el nombre de host R1.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de **class** en el Modo EXEC secreto.
- Configure una contraseña de **cisco** para las conexiones de consola.
- Configure una contraseña de **cisco** para las conexiones vty.

Paso 2. Configurar la interfaz de enlaces troncales en R1.

Configure la interfaz Fa0/1 en R1 con cinco subinterfaces, una para cada VLAN identificada en la tabla de configuración de subinterfaces del comienzo de la actividad. Configure estas subinterfaces con encapsulación dot1q y use la primera dirección de cada subred de la VLAN en la subinterfaz del router. Especifique la VLAN 99 como la VLAN nativa en su subinterfaz. No asigne ninguna dirección IP a la interfaz física, pero asegúrese de habilitarla. Documente las subinterfaces y sus respectivas direcciones IP en la tabla de subinterfaces.

Paso 3. Configurar la interfaz de LAN servidor en R1.

Consulte la tabla de direccionamiento y configure Fa0/0 con la dirección IP y máscara correctas. Describa la interfaz como **server interface**.

Paso 4. Verificar la configuración de enrutamiento.

En este momento, debe haber seis redes configuradas en R1. Consulte la tabla de enrutamiento en R1 para verificar que se pueden enrutar paquetes a las seis.

Si la tabla de enrutamiento no muestra las seis redes, realice la resolución de problemas de configuración y corrija los problemas antes de continuar.

Paso 5. Verificar el enrutamiento entre distintas VLAN.

Desde PC1, compruebe que puede hacer ping al servidor remoto (192.168.50.254) y a los otros dos hosts (192.168.20.22 y192.168.30.23). Es posible que deba hacer ping varias veces hasta que se establezca la ruta de extremo a extremo.

¿Los pings se realizaron correctamente? _____

De lo contrario, realice la resolución de problemas de la configuración. Asegúrese de que las gateways predetrminadas se hayan configurado en todos los switches y equipos PC. Si alguno los hosts pasaron al modo de hibernación, es probable que la interfaz conectada se deshabilite.

En este momento, debe poder hacer ping a cualquier nodo de cualquiera de las seis redes configuradas en la LAN, incluidas las interfaces de administración del switch.

Actividad PT 6.4.3: Resolución de problemas de enrutamiento entre VLAN

Diagrama de topología

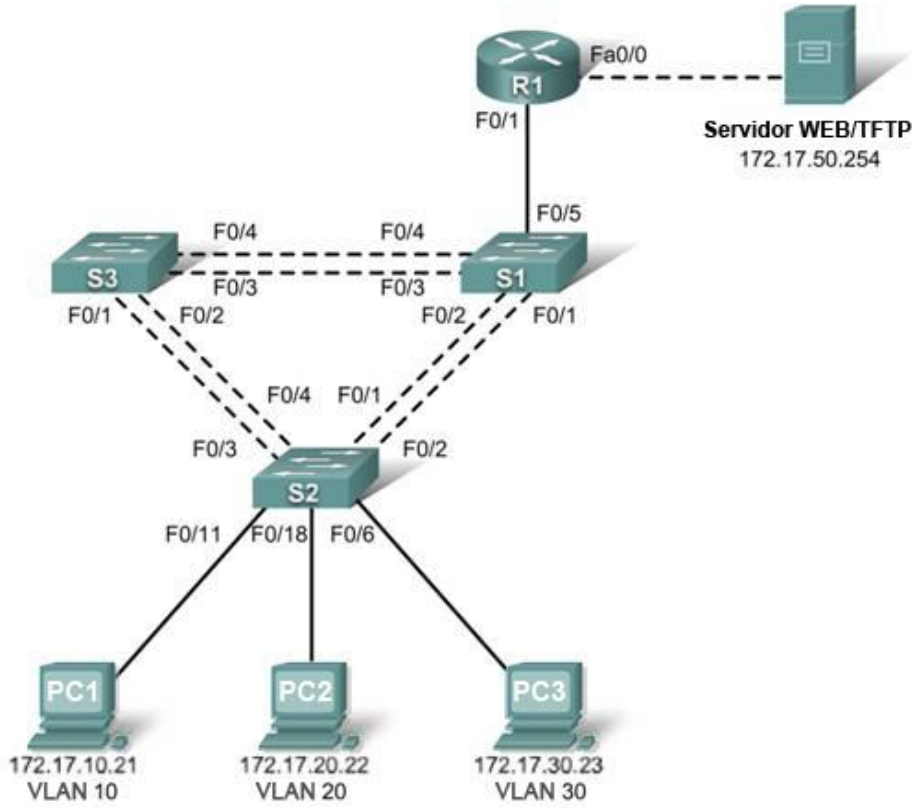


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
S1	**VLAN 99**	192.168.99.11	255.255.255.0	192.168.99.1
S2	**VLAN 99**	192.168.99.12	255.255.255.0	192.168.99.1
S3	**VLAN 99**	192.168.99.13	255.255.255.0	192.168.99.1
R1	**Fa0/0**	192.168.50.1	255.255.255.0	No aplicable
	Fa0/1	Consulte la tabla de configuración de interfaces		No aplicable
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
Server	**NIC**	192.168.50.254	255.255.255.0	192.168.50.1

Asignaciones de puertos: S2

Puertos	Asignaciones	Red
Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN nativa 99)	192.168.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Sales	192.168.30.0 /24
Fa0/11 – 0/17	VLAN 10 – R&D	192.168.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Engineering	192.168.20.0 /24

Tabla de configuración de interfaces: R1

Interfaz	Asignaciones	Dirección IP
Fa0/0.1	VLAN 1	192.168.1.1 /24
Fa0/0.10	VLAN 10	192.168.10.1 /24
Fa0/0.20	VLAN 20	192.168.20.1 /24
Fa0/0.30	VLAN 30	192.168.30.1 /24
Fa0/0.99	VLAN 99	192.168.99.1 /24

Objetivos de aprendizaje

- Solucionar y corregir los problemas entre VLAN y los errores de configuración
- Documentar la configuración de la red

Introducción

En esta actividad, se realizará la resolución de problemas de la red, se buscarán y corregirán los errores de configuración y se documentará la red corregida.

Tarea 1: Solucionar y corregir los problemas entre VLAN y los errores de configuración

Comience por identificar qué funciona bien y qué no:

¿Cuál es el estado de las interfaces?

_____

¿Qué hosts pueden hacer ping a otros hosts?

_____

¿Qué hosts pueden hacer ping al servidor?

_____

¿Qué rutas deben estar en la tabla de enrutamiento de R1?

_____

Cuando se corrijan todos los errores, se debería poder hacer ping al servidor remoto desde cualquier equipo PC o switch. Además, se debería poder hacer ping entre los tres equipos PC y a las interfaces de administración de los switches desde cualquier equipo PC.

Tarea 2: Documentar la configuración de la red

Cuando haya finalizado correctamente la resolución de problemas, capture los resultados del router y de los tres switches mediante el comando **show run** y guárdelos en un archivo de texto.

Actividad PT 6.5.1: Desafío de habilidades de Integración de Packet Tracer

Diagrama de topología

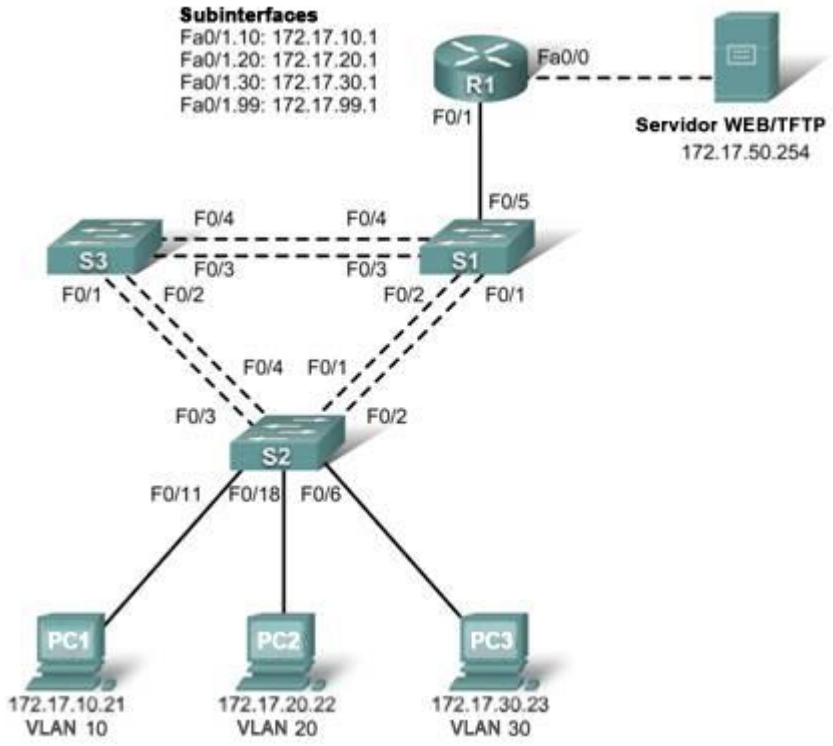


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
R1	**Fa0/0**	172.17.50.1	255.255.255.0	No aplicable
	Fa0/1.10	172.17.10.1	255.255.255.0	No aplicable
	Fa0/1.20	172.17.20.1	255.255.255.0	No aplicable
	Fa0/1.30	172.17.30.1	255.255.255.0	No aplicable
	Fa0/1.99	172.17.99.1	255.255.255.0	No aplicable
S1	**VLAN 99**	172.17.99.31	255.255.255.0	172.17.99.1
S2	**VLAN 99**	172.17.99.32	255.255.255.0	172.17.99.1
S3	**VLAN 99**	172.17.99.33	255.255.255.0	172.17.99.1
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

Objetivos de aprendizaje

- Configurar y verificar las configuraciones básicas del dispositivo
- Configurar VTP
- Configurar enlaces troncales
- Configurar las VLAN
- Asignar VLAN a puertos
- Configurar STP
- Configurar el enrutamiento entre VLAN con router-on-a-stick
- Verificar la conectividad de extremo a extremo

Introducción

En esta actividad, se demostrará y reforzará la habilidad del usuario para configurar switches y routers para la comunicación entre VLAN. Entre las capacidades que demostrará el usuario se incluye la configuración de VLAN, VTP y enlaces troncales en los switches. También se administrará STP en los switches y se configurará un router-on-a-stick usando subinterfaces.

Tarea 1: Configurar y verificar las configuraciones básicas del dispositivo

Paso 1: Configurar comandos básicos.

Configure el router y cada switch con los siguientes comandos básicos. Packet Tracer sólo califica los nombres de host y las gateways predeterminadas.

- Nombres de host
- Mensaje
- Contraseña secreta de enable
- Configuraciones de la línea
- Encriptación del servicio
- Gateways predeterminadas del switch

Paso 2: Configurar la interfaz de la VLAN de administración en S1, S2 y S3.

Cree y habilite VLAN 99 de la interfaz en cada switch. Use la tabla de direccionamiento para la configuración de las direcciones.

Paso 3: Verificar los resultados.

El porcentaje final del usuario debe ser del 17%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 2: Configurar VTP

Paso 1: Configurar el modo VTP en los tres switches.

Configure S1 como el servidor. Configure S2 y S3 como clientes.

Paso 2: Configurar el nombre de dominio de VTP en los tres switches.

Use **CCNA** como el nombre de dominio de VTP.

Paso 3: Configurar la contraseña de dominio de VTP en los tres switches.

Use **cisco** como la contraseña de dominio de VTP.

Paso 4: Verificar los resultados.

El porcentaje final del usuario debe ser del 28%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 3: Configurar enlaces troncales

Paso 1: Configurar enlaces troncales en S1, S2 y S3.

Configure las interfaces correspondientes en el modo de enlace troncal y asigne VLAN 99 como la VLAN nativa.

Paso 2: Verificar los resultados.

El porcentaje final del usuario debe ser del 62%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 4: Configurar las VLAN

Paso 1: Crear las VLAN en S1.

Cree las siguientes VLAN en S1 solamente y asígneles nombre. VTP publica las nuevas VLAN en S1 y S2.

- VLAN 10 **Faculty/Staff**
- VLAN 20 **Students**
- VLAN 30 **Guest(Default)**
- VLAN 99 **Management&Native**

Paso 2: Verificar que las VLAN se hayan enviado a S2 y S3.

Use los comandos adecuados para verificar que S2 y S3 ahora tienen las VLAN creadas en S1. Es probable que demore algunos minutos hasta que Packet Tracer simule las publicaciones de VTP.

Paso 3: Verificar los resultados.

El porcentaje final del usuario debe ser del 67%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 5: Asignar VLAN a puertos

Paso 1: Asignar VLAN a los puertos de acceso en S2.

Asigne los puertos de acceso de PC a VLAN:

- VLAN 10: PC1 conectado a Fa0/11
- VLAN 20: PC2 conectado a Fa0/18
- VLAN 30: PC3 conectado a Fa0/6

Paso 2: Verificar la implementación de la VLAN.

Use los comandos correspondientes para verificar la implementación de VLAN.

Paso 3: Verificar los resultados.

El porcentaje final del usuario debe ser del 75%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 6: Configurar STP

Paso 1: Asegurarse de que S1 sea el puente raíz.

Establezca las prioridades en 4096.

Paso 2: Verificar que S1 sea el puente raíz.

Paso 3: Verificar los resultados.

El porcentaje final del usuario debe ser del 82%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 7: Configurar el enrutamiento entre VLAN con router-on-a-stick

Paso 1: Configurar las interfaces.

Configure las subinterfaces Fa0/1 en R1 usando la información de la tabla de direccionamiento.

Paso 2: Verificar los resultados.

El porcentaje final del usuario debe ser del 100%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 8: Verificar la conectividad de extremo a extremo

Paso 1: Verificar que PC1 y el servidor Web/TFTP puedan hacer ping entre sí.

Paso 2: Verificar que PC1 y PC2 puedan hacer ping entre sí.

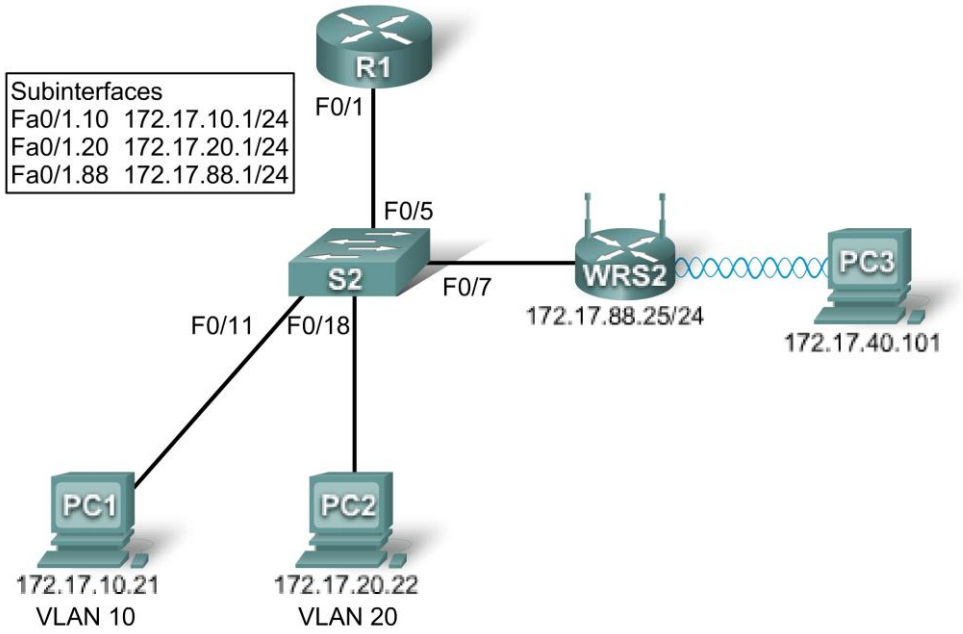
Paso 3: Verificar que PC3 y PC1 puedan hacer ping entre sí.

Paso 4: Verificar que PC2 y PC3 puedan hacer ping entre sí.

Paso 5: Verificar que los switches puedan hacer ping a R1.

Actividad PT 7.3.2: Configuración del acceso a LAN inalámbrica

Diagrama de topología



Objetivos de aprendizaje

- Agregar un router inalámbrico a la red
- Configurar las opciones en la ficha Linksys Setup
- Configurar las opciones en la ficha Linksys Wireless
- Configurar las opciones en la ficha Linksys Administration
- Agregar conectividad inalámbrica a un equipo PC
- Probar la conectividad

Introducción

En esta actividad, se configurará un router inalámbrico Linksys de manera que permita el acceso remoto desde equipos PC, además de la conectividad inalámbrica con seguridad WEP.

Tarea 1: Agregar un router inalámbrico a la red

Paso 1. Agregar un Linksys WRT300N a la red.

En el administrador de dispositivos, haga clic en **Wireless Devices** y seleccione Linksys-WRT300N. Agregue el dispositivo entre el switch y PC3, tal como se muestra en el diagrama de topología.

Paso 2. Configurar el nombre para mostrar.

Haga clic en el router Linksys para abrir la interfaz gráfica de usuario de configuración. Seleccione la ficha Config y establezca WRS2 como nombre para mostrar.

Paso 3. Conectar la interfaz Internet a S1.

Con un cable de conexión directa, conecte la interfaz Internet del router Linksys a la interfaz Fa0/7 del switch.

Paso 4. Verificar los resultados.

El porcentaje final del usuario debe ser del 19%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 2: Configurar las opciones en la ficha Linksys Setup

Paso 1. Establecer el tipo de conexión Internet en IP estática.

- Haga clic en el router Linksys y seleccione la ficha GUI.
- En la pantalla Setup para el router Linksys, ubique la opción Internet Connection Type bajo Internet Setup. Haga clic en el menú desplegable y seleccione Static IP de la lista.

Paso 2. Configurar la dirección IP, la máscara de subred y la gateway predeterminada de la VLAN 88 para WRS2.

- Establezca la dirección IP de Internet en 172.17.88.25.
- Establezca la máscara de subred en 255.255.255.0.
- Establezca la gateway predeterminada en 172.17.88.1.

Nota: En general, en una red doméstica o de empresa pequeña, esta dirección IP la asigna el ISP a través de DHCP.

Paso 3. Configurar los parámetros IP del router.

- En la pantalla **Setup**, desplácese hasta **Network Setup**. Para la opción **Router IP**, establezca la dirección IP 172.17.40.1 y la máscara de subred en 255.255.255.0.
- En **DHCP Server Setting,** asegúrese de que esté habilitado el servidor DHCP.

Paso 4. Guardar configuración.

Haga clic en el botón **Save Settings** en la parte inferior de la pantalla **Setup**.

Tenga en cuenta que el intervalo de direcciones IP para el pool de DHCP se ajusta a un intervalo de direcciones que coincide con los parámetros IP del router. Estas direcciones se usan para los clientes inalámbricos. Los clientes reciben una dirección IP y una máscara; y reciben la dirección IP del router para usar como gateway.

Paso 5. Verificar los resultados.

El porcentaje final del usuario debe ser del 50%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 3: Configurar las opciones en la ficha Linksys Wireless

Paso 1. Definir el nombre de red (SSID).

- Haga clic en la ficha **Wireless**.
- En **Network Name (SSID)**, cambie el nombre de la red de Default a WRS_LAN.
- Haga clic en **Save Settings**.

Paso 2. Establecer el modo de seguridad.

- Haga clic en **Wireless Security**. Esta opción se encuentra junto a Basic Wireless Settings en la ficha Wireless.
- Cambie la opción **Security Mode** de Disabled a WEP.
- Utilice la encriptación por defecto de 40/64 bite y establezca **Key1** en 0123456789
- Haga clic en **Save Settings**.

Paso 3. Verificar los resultados.

El porcentaje final del usuario debe ser del 69%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 4: Configurar las opciones en la ficha Linksys Administration

Paso 1. Configurar la contraseña del router.

- Haga clic en la ficha **Administration**.
- En **Router Access**, cambie la contraseña del router a cisco123. Vuelva a introducir la misma contraseña para confirmar.

Paso 2. Habilitar la administración remota.

- En **Remote Access**, habilite la administración remota.
- Haga clic en **Save Settings**.

Nota: PC1 y PC2 pueden hacer ping a WRS2, pero no podrán administrarlo en forma remota a través de la interfaz Internet. Por defecto, WRT300N bloquea todos los intentos para acceder a la interfaz Web desde el mundo exterior. Actualmente, Packet Tracer no admite la inhabilitación de esta función de seguridad. La administración remota se probará una vez establecida la conectividad inalámbrica de PC3.

Paso 3. Verificar los resultados.

El porcentaje final del usuario debe ser del 75%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Cierre el explorador Web del equipo PC.

Tarea 5: Agregar conectividad inalámbrica a un equipo PC

Paso 1. Quitar la NIC Fast Ethernet de PC3.

- Haga clic en **PC3** y luego en la ficha **Physical**.
- En la vista de dispositivos físicos se muestra una imagen del equipo PC. Haga clic en el botón de encendido para apagar el equipo PC.
- Quite la NIC Fast Ethernet. Para ello, arrástrela hacia la esquina inferior derecha de la ventana. La NIC se encuentra en la parte inferior de la máquina.

Paso 2. Instalar la NIC inalámbrica en PC3.

- En **Modules**, busque Linksys-WMP300N y arrástrelo y colóquelo donde se encuentra la NIC Fast Ethernet.
- Vuelva a encender la alimentación.

Paso 3. Configurar PC3 con una clave WEP.

- En la GUI de configuración para PC3, haga clic en la ficha **Desktop**.
- Haga clic en PC Wireless para comenzar a configurar la clave WEP para PC3. Se muestra una pantalla de Linksys. Debe ver que el equipo PC no está asociado a ningún punto de acceso.
- Haga clic en la ficha **Connect**.
- Debe aparecer WRS_LAN en la lista de redes inalámbricas disponibles. Asegúrese de que esté seleccionado y haga clic en **Connect**.
- En **WEP Key 1**, escriba la clave WEP (ciscoccna1) y haga clic en **Connect**.
- Vaya a la ficha **Link Information**. Los indicadores de intensidad de la señal y de calidad del enlace deben mostrar que tiene una señal intensa.
- Haga clic en el botón **More Information** para ver los detalles de la conexión. Verá la dirección IP que el equipo PC recibió del pool de DHCP.
- Cierre la ventana de configuración PC Wireless.

Paso 4. Verificar los resultados.

El porcentaje final del usuario debe ser del 100%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 6: Probar la conectividad

Todos los equipos PC deben disponer de conectividad entre sí. Haga clic en **Check Results** y, luego, en la ficha **Connectivity Tests** para comprobarlo. Si el porcentaje final es del 100%, pero las pruebas de conectividad demostraron errores, intente apagar PC3 y encenderlo nuevamente.

Actividad PT 7.5.2: Desafío inalámbrico WRT300N

Diagrama de topología

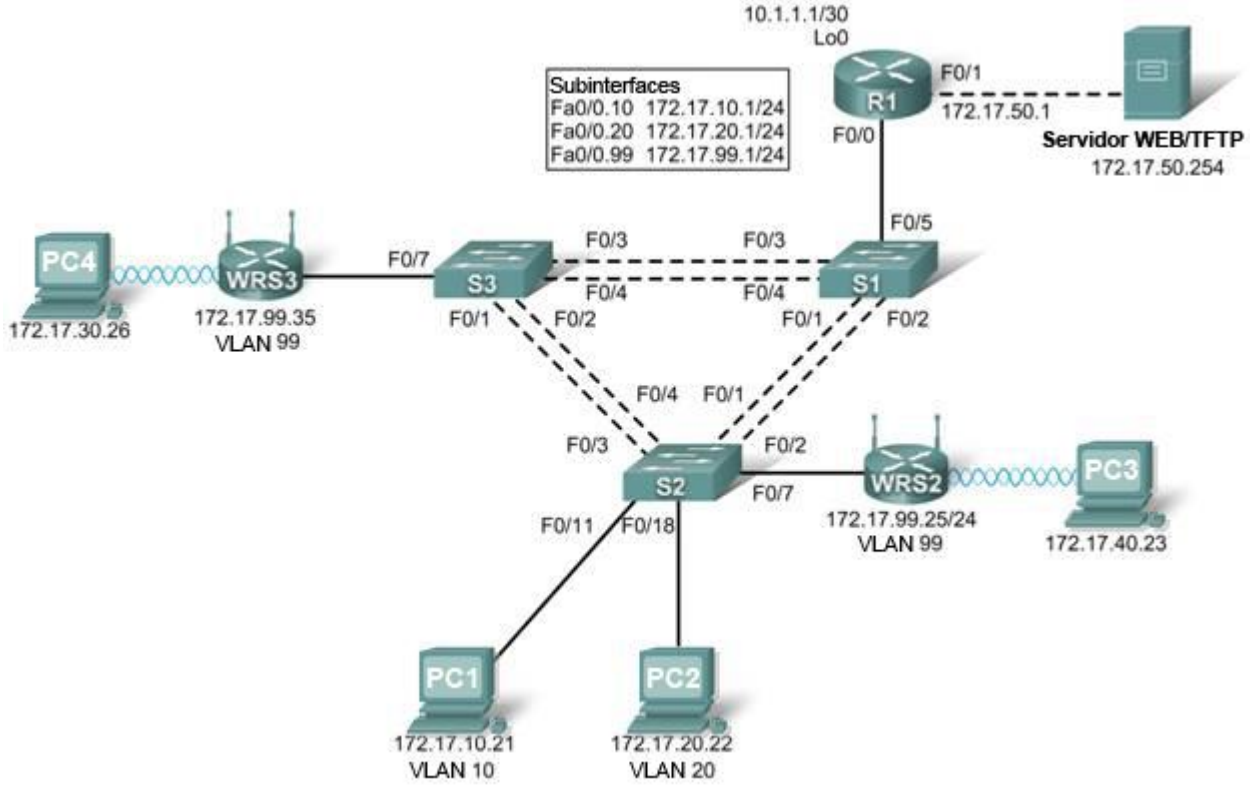


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
R1	Fa0/1	172.17.50.1	255.255.255.0	No aplicable
	Fa0/0.10	172.17.10.1	255.255.255.0	No aplicable
	Fa0/0.20	172.17.20.1	255.255.255.0	No aplicable
	Fa0/0.99	172.17.99.1	255.255.255.0	No aplicable
	Lo0	10.1.1.1	255.255.255.252	No aplicable
WRS2	WAN	172.17.99.25	255.255.255.0	172.17.99.1
	LAN inalámbrica	172.17.40.1	255.255.255.0	No aplicable
WRS3	WAN	172.17.99.35	255.255.255.0	172.17.99.1
	LAN inalámbrica	172.17.30.1	255.255.255.0	No aplicable
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

Tabla de VLAN

ID de VLAN	Nombre de VLAN	Red
VLAN 10	Faculty/Staff	172.17.10.0 /24
VLAN 20	Students	172.17.20.0 /24
VLAN 99	Wireless(Guest)	172.17.99.0 /24

Objetivos de aprendizaje

- Realizar las configuraciones básicas del router
- Realizar las configuraciones del switch
- Conectarse al router Linksys WRT300N
- Acceder a WRT300N
- Establecer la configuración IP para Linksys WRT300N
- Establecer la configuración DHCP
- Establecer la configuración básica de acceso inalámbrico
- Habilitar la seguridad de acceso inalámbrico
- Administrar y fijar la seguridad de la utilidad Web del router
- Configurar WRS2
- Crear y verificar la conectividad completa
- Configurar la seguridad de puerto

Introducción

En esta actividad, se configurará un Linksys WRT300N, se establecerá la seguridad del puerto en un switch Cisco y se definirán las rutas estáticas en varios dispositivos. Anote los procedimientos implicados en la conexión de una red inalámbrica, dado que algunos cambios implican la desconexión de clientes, que pueden tener que volver a conectarse después de realizar cambios en la configuración.

Tarea 1: Realizar las configuraciones básicas del router

Paso 1. Realizar las configuraciones básicas del router.

Configure R1 según las siguientes pautas:

- Nombre de host del router.
- Desactive la búsqueda DNS.
- Configure una contraseña de **class** en el Modo EXEC.
- Configure una contraseña de **cisco** para las conexiones de consola.
- Configure una contraseña de **cisco** para las conexiones vty.

Paso 2. Configurar las interfaces del router.

Configure Loopback0, FastEthernet 0/0, 0/1 y cualquier subinterfaz mencionada en la tabla de direccionamiento. Antes de configurar las direcciones IP en las subinterfaces, la encapsulación debe establecerse en 802.1Q. El ID de VLAN se identifica mediante el número de subinterfaz.

Verifique que las interfaces estén activas y que sus direcciones IP sean correctas mediante el comando **show ip interfaces brief**.

Tarea 2: Realizar las configuraciones del switch

Paso 1. Realizar las configuraciones básicas del switch.

Configure los tres switches de acuerdo a lo siguiente:

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

Paso 2. Configurar el modo VTP y crear VLAN.

Para todos los switches, establezca el modo VTP en **transparent** y cree las VLAN según la tabla del inicio de esta actividad.

Verifique la creación de las VLAN mediante el comando **show vlan brief**.

Paso 3. Configurar las interfaces del puerto del switch en S1, S2 y S3.

Configure las interfaces en los switches S1, S2 y S3 de acuerdo a lo siguiente:

- Fa0/7 en S2 y S3 están en VLAN 99
- Fa0/5 en S1 es un enlace troncal 802.1Q
- Fa0/11 en S2 está en la VLAN 10
- Fa0/18 en S2 está en la VLAN 20
- Los puertos conectados restantes son interfaces de enlaces troncales
- Permitir todas las VLAN en las interfaces de enlaces troncales

Paso 4. Verificar las VLAN y los enlaces troncales.

Use el comando **show interfaces trunk** en S1 y el comando **show vlan brief** en S2 para verificar que los switches contengan los enlaces troncales correctos y que existan las VLAN adecuadas.

Paso 5. Configurar las interfaces Ethernet de PC1 y PC2.

Configure las interfaces Ethernet de PC1 y PC2 con las direcciones IP y las gateways predeterminadas según la tabla de direccionamiento que se indica al principio de la actividad.

Paso 6. Probar la configuración del equipo PC.

Acceda al símbolo del sistema en cada equipo PC y haga ping a su gateway predeterminadas. Los pings deben realizarse correctamente. De lo contrario, realice la resolución de problemas.

Tarea 3: Conectarse al router Linksys WRT300N

Paso 1. Conectarse a un router inalámbrico.

Desde PC6, acceda al escritorio y, luego, a la PC Wireless. Desde aquí, seleccione la ficha Connect y conéctese con la red por defecto.

Paso 2. Verificar la configuración de conectividad.

En el escritorio del equipo PC, cierre la ventana de la GUI de Linksys y luego verifique la configuración de conectividad. Para ello, acceda al símbolo del sistema y escriba el comando **ipconfig**.

```
PC>ipconfig

IP Address.....................: 192.168.1.101
Subnet Mask....................: 255.255.255.0
Default Gateway................: 192.168.1.1

PC>
```

Tarea 4: Acceder a WRT300N

Paso 1. Acceder a WRS3 a través del navegador Web.

En PC6, cierre el símbolo del sistema y haga clic en el explorador Web. Introduzca el URL 192.168.1.1, la gateway predeterminada del equipo PC.

Paso 2. Introducir la información de autenticación.

Se solicitará un nombre de usuario y contraseña. El nombre de usuario y contraseña por defecto son **admin**. Una vez introducida la información de inicio de sesión, se debería ver la página por defecto de la utilidad Web de Linksys WRT300N.

Tarea 5: Establecer la configuración IP para Linksys WRT300N

La mejor forma de comprender la siguiente configuración es considerar que WRT300N es similar a un router Cisco basado en IOS con dos interfaces independientes. Una de las interfaces (la configurada en Internet Setup) actúa como la conexión a los switches y el interior de la red. La otra interfaz (configurada en Network Setup) actúa como la interfaz que se conecta a los clientes inalámbricos PC6 y PC3.

Paso 1. Establecer el tipo de conexión Internet en IP estática.

Debe ir a la página Setup del router Linksys. En Internet Setup se encuentra la opción Internet Connection Type. Seleccione Static IP.

Paso 2. Definir la configuración de dirección IP para la configuración de Internet.

- Establezca la dirección IP de Internet en **172.17.99.35**.
- Establezca la máscara de subred en **255.255.255.0**.
- Establezca la gateway predeterminada en la dirección IP de la VLAN 99 Fa0/1 de R1, **172.17.99.1**.

Paso 3. Configurar la dirección IP de la configuración de red en 172.17.30.1 /24.

Paso 4. Guardar la configuración.

Haga clic en **Save Settings**. Aparecerá una ventana indicando que la configuración se estableció correctamente. Haga clic en Continue. Dado que se ha modificado la gateway predeterminada, PC6 no podrá acceder a la utilidad Web hasta que se actualicen su dirección IP y gateway.

Paso 5. Renovar la configuración IP en PC6.

Cierre el explorador Web y vuelva al escritorio de PC6. Nuevamente, acceda al símbolo del sistema. Escriba el comando **ipconfig /renew** para actualizar la dirección IP y la gateway predeterminada de PC6.

Nota: En Packet Tracer, se debe dejar un espacio entre **ipconfig y /renew**.

```
PC>ipconfig /renew

IP Address.....................: 172.17.30.101
Subnet Mask....................: 255.255.255.0
```

```
Default Gateway.................: 172.17.30.1
DNS Server......................: 0.0.0.0

PC>
```

Tarea 6: Establecer la configuración DHCP

Ahora vuelva a acceder al router inalámbrico a través del explorador Web, pero esta vez en el URL 172.17.30.1.

En DHCP Server Settings, establezca la dirección de inicio en 25 y el número máximo de usuarios en 25.

Estas configuraciones asignan una dirección entre 172.17.30.25-49 a cualquier equipo PC que se conecta a este router de manera inalámbrica para solicitar una dirección IP a través de DHCP. Sólo 25 clientes a la vez pueden obtener una dirección IP.

Haga clic en **Save Settings** para aplicar los cambios.

Tarea 7: Establecer la configuración básica de acceso inalámbrico

Paso 1. Configurar el SSID.

Acceda a la página Wireless y cambie el SSID del nombre de la red de **Default** a **WRS3**.

Paso 2. Guardar la configuración.

Paso 3. Volver a conectarse a la red inalámbrica.

Dado que el SSID ha cambiado, PC6 no puede en este momento acceder a la red WRS3.
En el escritorio, vuelva a PC Wireless y seleccione la ficha Connect. Conéctese a la red WRS3.

Paso 4. Verificar la configuración.

Ahora que se ha vuelto a conectar a la red, tiene la nueva configuración DHCP que configuró en la Tarea 6. Verifique esto en el símbolo del sistema mediante el comando **ipconfig**.

```
PC>ipconfig

IP Address......................: 172.17.30.26
Subnet Mask.....................: 255.255.255.0
Default Gateway.................: 172.17.30.1
DNS Server......................: 0.0.0.0

PC>
```

Nota: Es probable que Packet Tracer necesite ayuda para actualizar la configuración IP. Si la dirección IP no es 172.17.30.26 o la gateway predeterminada es errónea, intente con el comando **ipconfig /renew**. Si esto no funciona, vuelva al escritorio y seleccione IP Configuration. Desde aquí, cambie a Static y luego vuelva a DHCP. La configuración debe coincidir con aquélla mencionada.

Tarea 8: Habilitar la seguridad de acceso inalámbrico

Paso 1. Volver a conectarse a la página de configuración del router (http://172.17.30.1).

Paso 2. Desplazarse a la página Wireless y seleccionar la ficha Wireless Security.

Paso 3. En el Security Mode, seleccionar WEP.

Paso 4. Introducir una clave WEP.

Una red es sólo tan segura como su punto más débil, y un router inalámbrico es un punto de inicio muy conveniente si alguien desea dañar la red. Al solicitar una clave WEP para conectarse al router, agregará un nivel de seguridad.

Desafortunadamente, hay herramientas que pueden descifrar la encriptación de la clave WEP. Una forma más eficaz para la seguridad de inalámbrico es WPA y WPA-2, actualmente no compatibles con Packet Tracer.

Agregue la clave WEP **1234567890**.

Paso 5. Guardar la configuración.

Se desconectará de la red nuevamente después de guardar la configuración.

Paso 6. Configurar PC6 para usar autenticación WEP.

- Vuelva al escritorio y haga clic en PC Wireless.
- Haga clic en la ficha **Connect**.
- En la lista de redes inalámbricas disponibles, seleccione **WRS3** y conéctese.
- Aparecerá una ventana que le solicitará la clave WEP. En WEP Key 1, escriba la clave **1234567890**.
- Haga clic en Link Information para verificar la conectividad al punto de acceso.

Tarea 9: Administrar y fijar la seguridad de la utilidad Web del router

Paso 1. Configurar la contraseña de acceso Web.

Vuelva a la página de la utilidad Web del router (http://172.17.30.1) y navegue a la sección Administration. Cambie la contraseña del router a **cisco**. Observe que la opción Acceso a la utilidad Web HTTP ya está seleccionada por defecto. Déjelo así.

Paso 2. Guardar la configuración.

Tarea 10: Configurar WRS2

Paso 1. Conectar WRS2 desde PC3.

Consulte la Tarea 3 si necesita ayuda.

Paso 2. Conectarse a la utilidad Web a través del explorador Web.

Acceda a WRS2 a través de la gateway predeterminada, 192.168.2.1.

Paso 3. Completar la configuración de Internet y de la red.

- Asigne una IP estática a la interfaz Internet. Use el direccionamiento de la tabla del inicio de la actividad.
- Configure la dirección IP del router con el direccionamiento LAN de la tabla del inicio de la actividad.
- Para la configuración del servidor DHCP, comience asignando las direcciones IP en 172.17.40.22, para hasta 25 usuarios.
- Guarde la configuración.

Paso 4. Renovar la configuración IP de PC3.

El comando **ipconfig /renew** no renueva correctamente la dirección IP del nuevo intervalo DHCP. Vaya a IP Configuration del escritorio, cambie a Static y luego, nuevamente a DHCP. Verifique el nuevo direccionamiento mediante el comando **ipconfig**.

```
PC>ipconfig

IP Address.....................: 172.17.40.23
Subnet Mask....................: 255.255.255.0
Default Gateway................: 172.17.40.1

PC>
```

Paso 5. Cambiar SSID a WRS2.

Vuelva a la utilidad Web y en la página Wireless cambie el SSID a WRS2. Asegúrese de hacer clic en Save Settings.

Vuelva a conectar PC3 a WRS2. Consulte el paso 3 de la Tarea 7 para obtener ayuda.

Paso 6. Configurar WEP en WRS2 desde la utilidad Web.

Configure la clave WEP en **1234567890** y configure PC3 para que use esa clave. Consulte la Tarea 8 para obtener ayuda.

Paso 7. Configurar la contraseña de acceso Web en cisco.

Consulte la Tarea 9 para obtener ayuda.

Tarea 11: Crear y verificar la conectividad completa.

Paso 1. Asignar a R1 rutas estáticas a las redes 172.17.30.0 y 172.17.40.0.

Estas rutas permitirán que R1 haga ping a la dirección IP inalámbrica/LAN interna de los routers inalámbricos.

```
!
ip route 172.17.30.0 255.255.255.0 172.17.99.35
ip route 172.17.40.0 255.255.255.0 172.17.99.25
!
```

Paso 2. Verificar la conectividad.

Verifique que R1 tenga rutas a PC3 y PC6 mediante el comando **show ip route**, y que R1 pueda hacer ping a la dirección IP inalámbrica/LAN interna de cada router inalámbrico.

Debido a un error de Packet Tracer, PC3 y PC6 no podrán hacer ping entre sí.

Tarea 12: Configuración de la seguridad de puertos

Paso 1. Configurar la seguridad de los puertos de PC1 y PC2.

Habilite la seguridad de los puertos y direcciones MAC dinámicas sin modificación.

Paso 2. Generar tráfico entre los puertos con pings a PC2 desde PC1.

Paso 3. Verificar la seguridad de los puertos.

Actividad PT 7.5.3: Resolución de problemas de WRT300N inalámbrico

Diagrama de topología

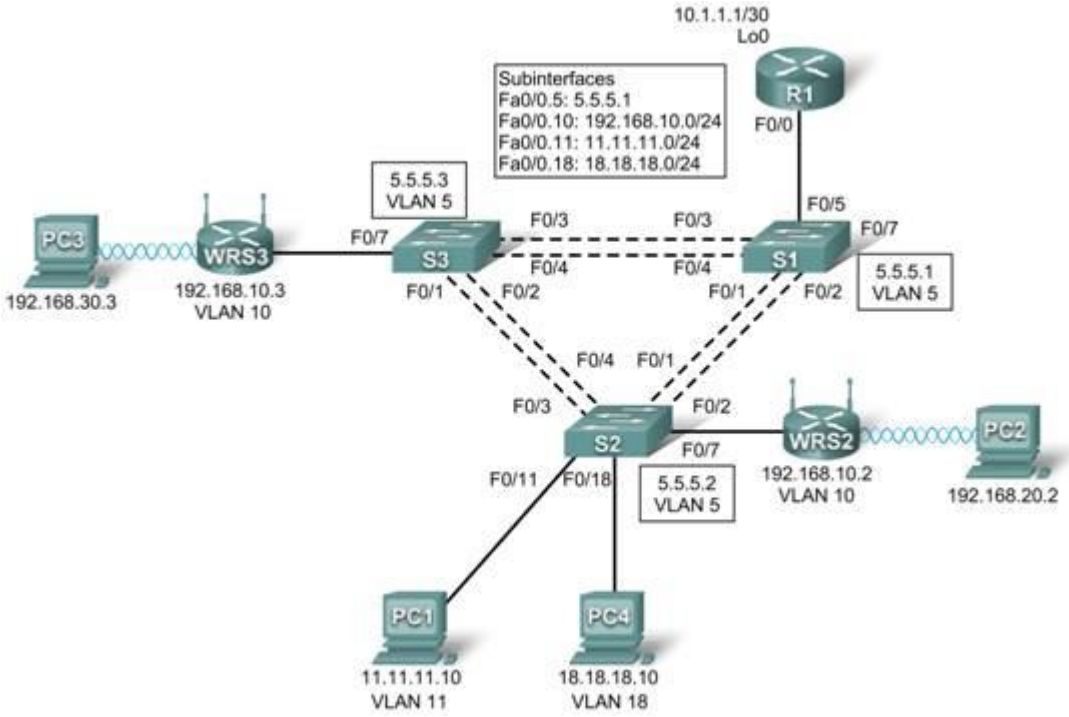


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
R1	**Fa0/0.5**	5.5.5.10	255.255.255.0	No aplicable
	Fa0/0.10	192.168.10.1	255.255.255.0	No aplicable
	Fa0/0.11	11.11.11.1	255.255.255.0	No aplicable
	Fa0/0.18	18.18.18.1	255.255.255.0	No aplicable
	Lo0	10.1.1.1	255.255.255.252	No aplicable
WRS2	**WAN**	192.168.10.2	255.255.255.0	192.168.10.1
	LAN inalámbrica	192.168.20.1	255.255.255.0	No aplicable
WRS3	**WAN**	192.168.10.3	255.255.255.0	192.168.10.1
	LAN inalámbrica	192.168.30.1	255.255.255.0	No aplicable
PC1	**NIC**	11.11.11.10	255.255.255.0	11.11.11.1
PC4	**NIC**	18.18.18.10	255.255.255.0	18.18.18.1

La tabla de direccionamiento continúa en la siguiente página

Continuación de la tabla de direccionamiento

S1	**VLAN 5**	5.5.5.1	255.255.255.0	No aplicable
S2	**VLAN 5**	5.5.5.2	255.255.255.0	No aplicable
S3	**VLAN 5**	5.5.5.3	255.255.255.0	No aplicable

Objetivos de aprendizaje

- Solucionar problemas de la red
- Verificar la conectividad

Escenario

Para esta actividad, se configuraron incorrectamente una red básica y una red inalámbrica. Se deben buscar y corregir las configuraciones erróneas en función de las especificaciones mínimas de la red proporcionadas por la empresa.

Tarea 1: Solucionar problemas de la red

Examine los routers y los switches, determine los errores de la red.

Nota: Packet Tracer no calificará las VLAN permitidas para el modo de enlace troncal.

Los requisitos de enrutamiento inalámbrico son los siguientes:

- Conexiones a través de las direcciones IP que se muestran en el diagrama de topología.
- Treinta clientes pueden obtener una dirección IP a través de DHCP a la vez.
- Los clientes inalámbricos deben autenticarse mediante WEP con **5655545251** como clave.
- Las solicitudes de pings provenientes desde fuera de los puertos WAN de los routers Linksys a sus direcciones IP LAN/inalámbricas (192.168.30.1) deben realizarse correctamente.
- DHCP debe asignar a PC2 y PC3 sus propias direcciones IP.

Tarea 2: Verificar la conectividad

Si se produce un error, Packet Tracer no permite que PC2 y PC3 hagan ping entre sí. No obstante, debe haber conectividad en todas las demás condiciones. Todos los equipos PC deben poder hacer ping entre sí y a R1. Si no lo hacen, continúe con la resolución de problemas.

Actividad PT 7.6.1: Desafío de habilidades de Integración de Packet Tracer

Diagrama de topología

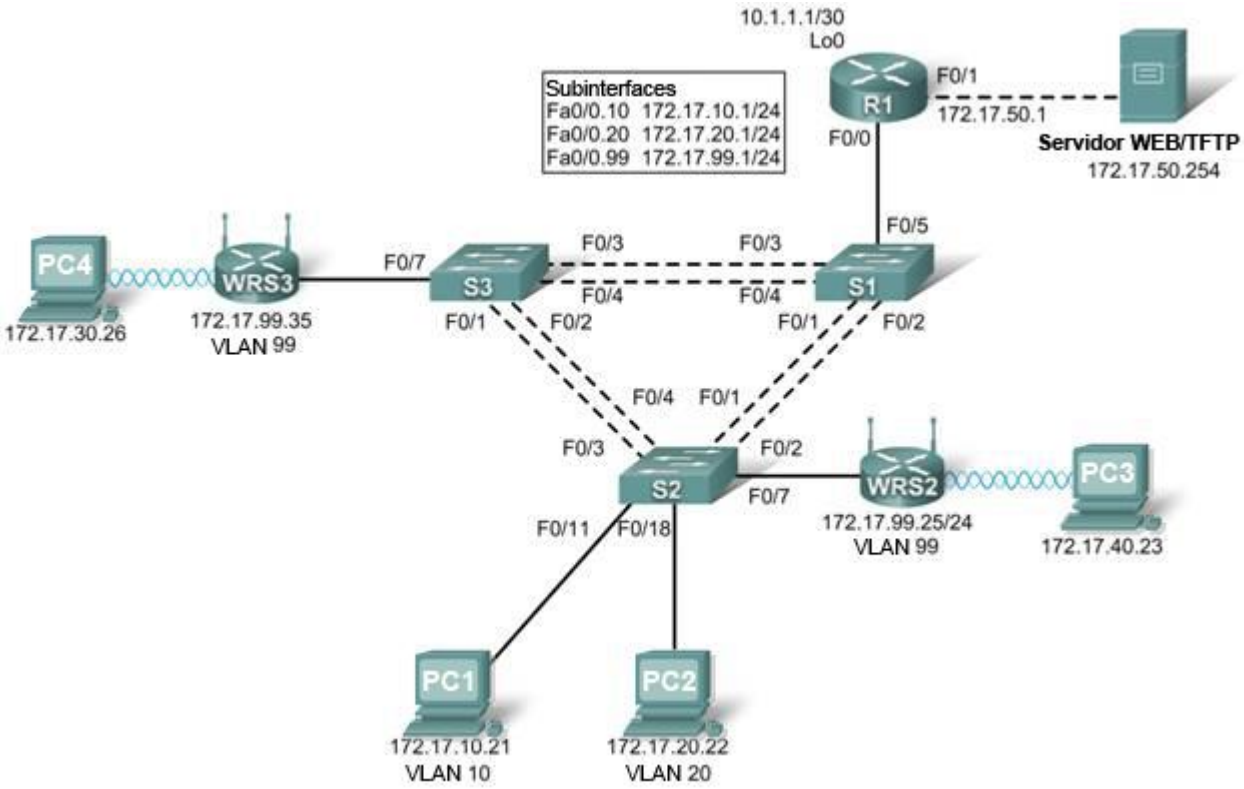


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
R1	**Fa0/0**	172.17.50.1	255.255.255.0	No aplicable
	Fa0/1.10	172.17.10.1	255.255.255.0	No aplicable
	Fa0/1.20	172.17.20.1	255.255.255.0	No aplicable
	Fa0/1.88	172.17.88.1	255.255.255.0	No aplicable
	Fa0/1.99	172.17.99.1	255.255.255.0	No aplicable
WRS2	**Internet**	172.17.88.25	255.255.255.0	172.17.88.1
	LAN	172.17.40.1	255.255.255.0	No aplicable
WRS3	**Internet**	172.17.88.35	255.255.255.0	172.17.88.1
	LAN	172.17.30.1	255.255.255.0	No aplicable

La tabla de direccionamiento continúa en la siguiente página

Continuación de la tabla de direccionamiento

S1	**VLAN 99**	172.17.99.31	255.255.255.0	172.17.99.1
S2	**VLAN 99**	172.17.99.32	255.255.255.0	172.17.99.1
S3	**VLAN 99**	172.17.99.33	255.255.255.0	172.17.99.1
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

Objetivos de aprendizaje

- Configurar y verificar las configuraciones básicas del dispositivo
- Configurar VTP
- Configurar enlaces troncales
- Configurar las VLAN
- Asignar VLAN a puertos
- Configurar STP
- Configurar el enrutamiento entre VLAN con router-on-a-stick.
- Configurar la conectividad inalámbrica
- Verificar la conectividad de extremo a extremo

Introducción

Esta es la actividad final del Reto de habilidades de Integración de Packet Tracer para Exploration. En el curso Conmutación y conexión inalámbrica de LAN, aplicará todas las habilidades aprendidas, incluidas la configuración de VLAN y VTP, la optimización de STP, la habilitación del enrutamiento entre VLAN y la integración de la conectividad inalámbrica.

Tarea 1: Configurar y verificar las configuraciones básicas del dispositivo

Paso 1. Configurar los comandos básicos.

Configure cada switch con los siguientes comandos básicos. Packet Tracer sólo califica los nombres de host y las gateways predeterminadas.

- Nombres de host
- Mensaje
- Contraseña secreta de enable
- Configuraciones de la línea
- Encriptación del servicio
- Gateways predeterminadas del switch

Paso 2. Configurar la interfaz VLAN de administración en S1, S2 y S3.

Cree y habilite VLAN 99 de la interfaz en cada switch. Use la tabla de direccionamiento para la configuración de las direcciones.

Paso 3. Verificar los resultados.

El porcentaje final del usuario debe ser del 13%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 2: Configurar VTP

Paso 1. Configurar el modo VTP en los tres switches.

Configure S1 como el servidor. Configure S2 y S3 como clientes.

Paso 2. Configurar el nombre de dominio VTP en los tres switches.

Use **CCNA** como el nombre de dominio de VTP.

Paso 3. Configurar la contraseña de dominio de VTP en los tres switches.

Use **cisco** como la contraseña de dominio de VTP.

Paso 4. Verificar los resultados.

El porcentaje final del usuario debe ser del 21%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 3: Configurar enlaces troncales

Paso 1. Configurar enlaces troncales en S1, S2 y S3.

Configure las interfaces correspondientes en el modo de enlace troncal y asigne VLAN 99 como la VLAN nativa.

Paso 2. Verificar los resultados.

El porcentaje final del usuario debe ser del 44%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 4: Configurar las VLAN

Paso 1. Crear las VLAN en S1.

Cree las siguientes VLAN en S1 solamente y asígneles nombre. VTP publica las nuevas VLAN en S2 y S3.

- VLAN 10 **Faculty/Staff**
- VLAN 20 **Students**
- VLAN 88 **Wireless(Guest)**
- VLAN 99 **Management&Default**

Paso 2. Verificar que las VLAN se hayan enviado a S2 y S3.

Use los comandos adecuados para verificar que S2 y S3 ahora tienen las VLAN creadas en S1. Es probable que demore algunos minutos hasta que Packet Tracer simule las publicaciones de VTP.

Paso 3. Verificar los resultados.

El porcentaje final del usuario debe ser del 54%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 5: Asignar VLAN a puertos

Paso 1. Asignar VLAN a puertos de acceso en S2 y S3.

Asigne los puertos de acceso de PC a VLAN:

- VLAN 10: PC1
- VLAN 20: PC2

Asigne los puertos de acceso del router inalámbrico a VLAN 88.

Paso 2. Verificar la implementación de VLAN.

Use los comandos correspondientes para verificar la implementación de VLAN.

Paso 3. Verificar los resultados.

El porcentaje final del usuario debe ser del 61%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 6: Configurar STP

Paso 1. Asegúrese de que S1 sea el puente raíz para todas las instancias de spanning-tree.

Use la prioridad 4096.

Paso 2. Asegúrese de que S1 sea el puente raíz.

Paso 3. Verificar los resultados.

El porcentaje final del usuario debe ser del 66%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 7: Configurar el enrutamiento entre VLAN con router-on-a-stick

Paso 1. Configurar la subinterfaces.

Configure las subinterfaces Fa0/1 en R1 usando la información de la tabla de direccionamiento.

Paso 2. Verificar los resultados.

El porcentaje final del usuario debe ser del 79%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 8: Configurar la conectividad inalámbrica

Paso 1. Configurar el direccionamiento IP para WRS2 y WRS3.

Establezca la configuración LAN y, luego, el direccionamiento estático de las interfaces de Internet para WRS2 y WRS3 usando las direcciones de la topología.

Nota: Un error de Packet Tracer puede impedir la asignación de la dirección IP estática en primer lugar. Una solución para este problema es establecer primero la configuración LAN en Network Setup. Guarde la configuración. Luego, configure la información de IP estática en Internet Connection Type y vuelva a guardar la configuración.

Paso 2. Establecer la configuración de red inalámbrica.

- Las SSID para los routers son WRS2_LAN y WRS3_LAN, respectivamente.
- La WEP para ambas es 12345ABCDE.

Paso 3. Configurar los routers inalámbricos para el acceso remoto.

Configure cisco123 como contraseña de administración.

Paso 4. Configurar PC3 y PC4 para que accedan a la red usando DHCP.

PC3 se conecta a WRS2_LAN, y PC4 se conecta a WRS3_LAN.

Paso 5. Verificar la capacidad de acceso remoto.

Paso 6. Verificar los resultados.

El porcentaje final del usuario debe ser del 100%. De lo contrario, haga clic en **Check Results** para consultar qué componentes obligatorios aún no se completaron.

Tarea 9: Verificar la conectividad de extremo a extremo

Paso 1. Verificar que PC1 y el servidor Web/TFTP puedan hacer ping entre sí.

Paso 2. Verificar que PC1 y PC2 puedan hacer ping entre sí.

Paso 3. Verificar que PC3 y PC1 puedan hacer ping entre sí.

Paso 4. Verificar que PC2 y PC3 puedan hacer ping entre sí.