Cisco | Networking Academy®
Mind Wide Open™

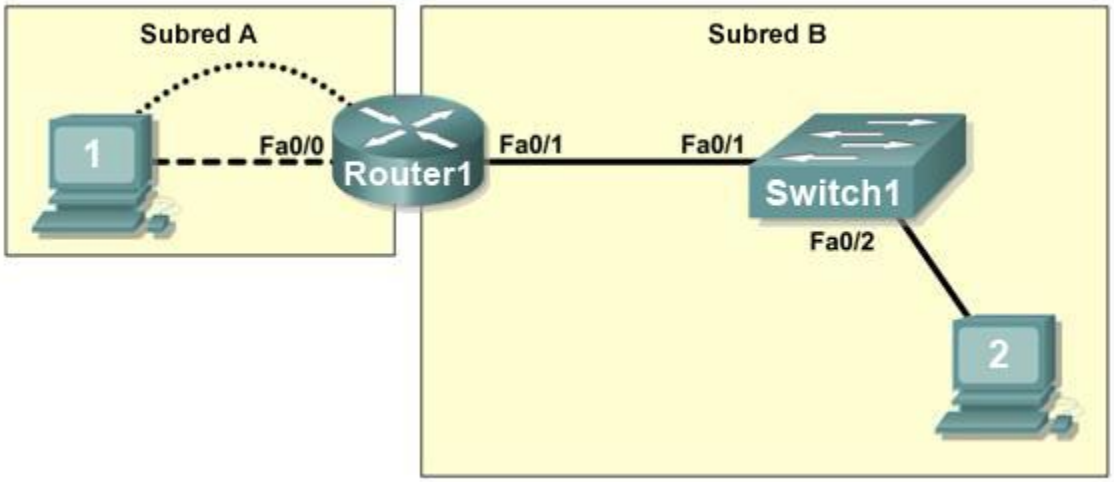
CCNA Exploration 4.0

Conmutación y conexión inalámbrica de LAN

Manual de prácticas de laboratorio para el instructor

Práctica de laboratorio 1.3.1: Revisión de los conceptos de Exploration 1 (Versión para el instructor)

Diagrama de topología



Objetivos de aprendizaje

Al completar esta práctica de laboratorio podrá:

- Crear una topología lógica con los requisitos de red dados
- Crear subredes que cumplan con los requisitos del host
- Configurar la topología física
- Configurar la topología lógica
- Verificar la conectividad de la red
- Configurar y verificar contraseñas

Escenario

En esta práctica de laboratorio diseñará y configurará una pequeña red enrutada y verificará la conectividad a través de múltiples dispositivos de red. Esto requiere la creación y la asignación de dos bloques de subredes, la conexión de hosts y dispositivos de red y la configuración de computadoras hosts y un router Cisco para conectividad de red básica. El switch 1 presenta una configuración predeterminada y no requiere configuración adicional. Utilizará los comandos habituales para evaluar y documentar la red. Se utiliza la subred cero.

El Apéndice 1 contiene una tabla de subred para último octeto de IPv4.

Tarea 1: Diseñar una topología lógica de LAN

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 utiliza la subred 0. No se pueden utilizar calculadoras de subredes. Cree las subredes más pequeñas posible que cumplan los requisitos para los hosts. Asigne la primera subred utilizable a la Subred A.

Subred A	
Especificación	**Entrada del estudiante**
Número de bits en la subred	1
Máscara de IP (binaria)	11111111. 11111111. 11111111.10000000
Nueva máscara de IP (decimal)	255.255.255.128
Cantidad máxima de subredes utilizables (incluyendo la subred 0)	2
Cantidad de hosts utilizables por subred	126
Dirección IP de la subred	192.168.7.0
Primera dirección IP de host	192.168.7.1
Última dirección IP de host	192.168.7.126

Subred B	
Especificación	**Entrada del estudiante**
Número de bits en la subred	2
Máscara de IP (binaria)	11111111. 11111111. 11111111.11000000
Nueva máscara de IP (decimal)	255.255.255.192
Cantidad máxima de subredes utilizables (incluyendo la subred 0)	2
Cantidad de hosts utilizables por subred	62
Dirección IP de red	192.168.7.128
Primera dirección IP de host	192.168.7.129
Última dirección IP de host	192.168.7.190

Los equipos host usan la primera dirección IP utilizable en la subred. El router de la red usa la última dirección IP utilizable en la subred.

Paso 2: Anotar la información de la dirección IP de cada dispositivo.

Dispositivo	Dirección IP	Máscara	Gateway (puerta de salida)
Host1	192.168.7.1	255.255.255.128	192.168.7.126
Router1-Fa0/0	192.168.7.126	255.255.255.128	----------
Host2	192.168.7.129	255.255.255.192	192.168.7.190
Router1-Fa0/1	192.168.7.190	255.255.255.192	----------

Tabla 1. Asignaciones de direcciones IP

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

Tarea 2: Configurar la topología física

Paso 1: Cablear la red.

Consulte la figura y la tabla a continuación para obtener los cables necesarios.

Horizontal	Tipo de cable
Cable LAN entre el Host1 y el Router1 Fa0/0	Interconexión cruzada
Cable LAN entre el Switch1 y el Router1 Fa0/1	De conexión directa
Cable LAN entre el Switch1 y el Host2	De conexión directa
Cable de consola entre el host1 y el Router1	Transpuesto

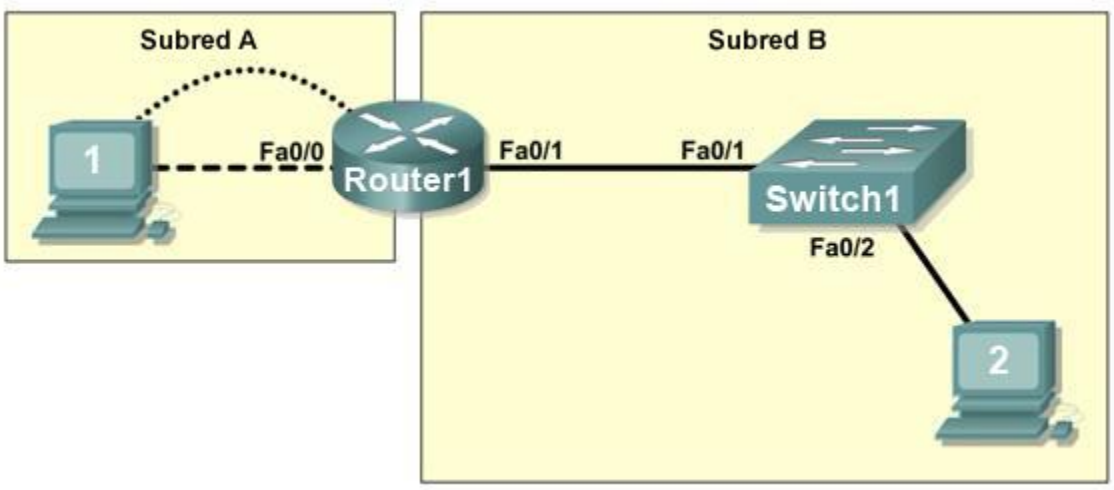


Figura 1. Cableado de la red

Paso 2: Conectar físicamente los dispositivos de la práctica de laboratorio.

Instale el cableado de los dispositivos de la red según se muestra en la Figura 1. Encienda todos los dispositivos, en caso de que no lo estén.

Paso 3: Inspeccionar las conexiones de la red.

Verifique las conexiones visualmente.

Nota para el instructor: Asegúrese de que el switch se encuentre en su configuración predeterminada y de que Fa0/1 y Fa0/2 se encuentren en Vlan1. Asegúrese de que la configuración del router se ha borrado.

Tarea 3: Configurar la topología lógica

Paso 1: Configurar las computadoras host.

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

Nota: Las siguientes instrucciones son para Windows XP. Para configurar hosts utilizando sistemas operativos consulte el manual del sistema operativo.

Para configurar el host vaya a **Inicio > Panel de control > Conexiones de red > Conexión de área local** En la ventana Propiedades de conexión de área local, seleccione **Protocolo de Internet (TCP/IP)** y haga clic en el botón **Propiedades**.

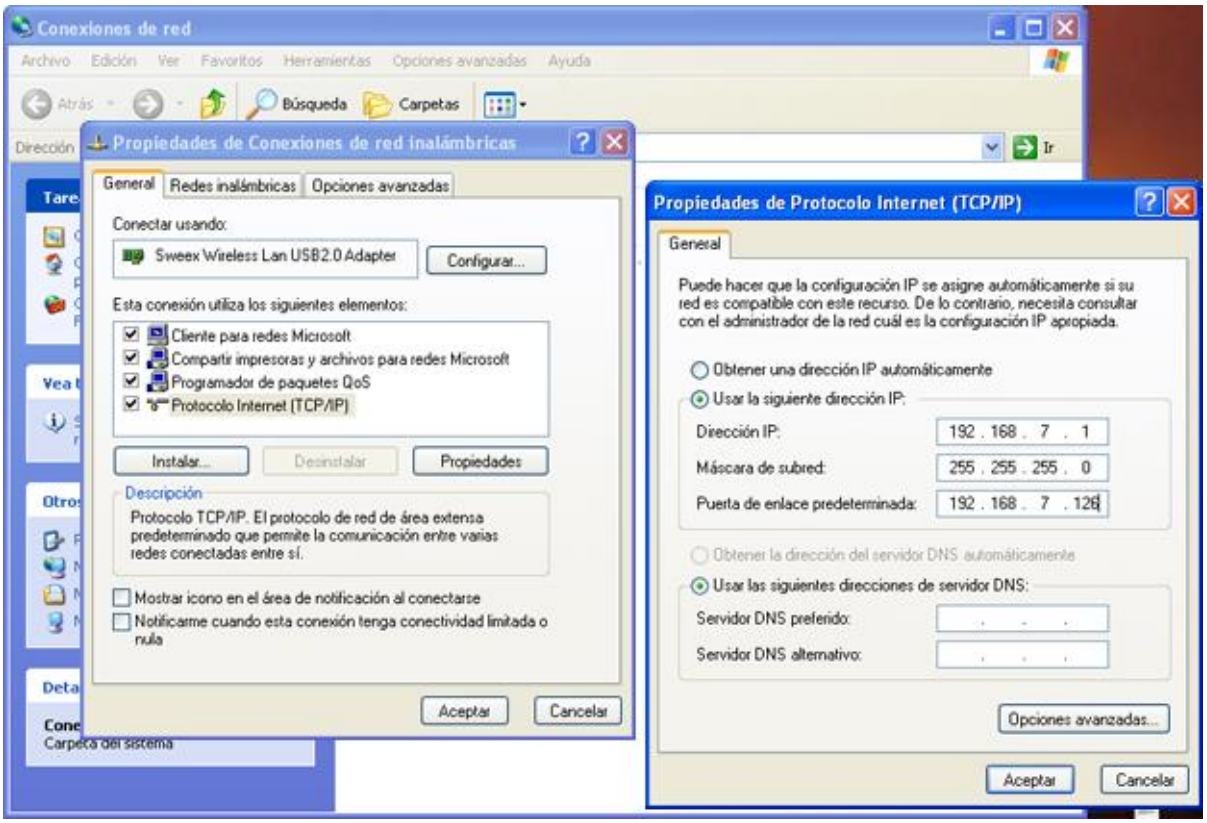


Figura 2. Configuración de propiedades del Protocolo de Internet (TCP/IP)

En el cuadro de diálogo Propiedades de TCP/IP de cada host, ingrese la dirección IP, la máscara de subred y la gateway de la Tabla 1.

Después de configurar cada computadora host, abra una ventana de comandos en el host seleccionando **Inicio > Ejecutar**. Cuando se le solicite que ingrese el nombre de un programa, escriba **cmd** en el cuadro de texto. Desde la ventana de comandos, muestre y verifique las configuraciones de red del host mediante el comando **ipconfig /all**. Las configuraciones deben coincidir con las de las siguientes tablas:

Configuración de red del Host1	
Dirección IP	192.168.7.1
Máscara de subred	255.255.255.128
Gateway predeterminada	192.168.7.126

Configuración de red del Host2	
Dirección IP	192.168.7.129
Máscara de subred	255.255.255.192
Gateway predeterminada	192.168.7.190

¿Coinciden las configuraciones de los hosts con las tablas? _____En caso contrario, reconfigúrelos según sea necesario.

Paso 2: Configurar el Router1.

Desde el Host1, conecte la consola del Router 1 y establezca una sesión de consola. En el Apéndice 2 se encuentran las instrucciones para crear una conexión de consola utilizando HyperTerminal.

Desde la consola del router, configure lo siguiente:

Tarea	Especificación
Nombre del router	Router1
Contraseña encriptada para el modo exec privilegiado	cisco
Contraseña de acceso a la consola	class
Contraseña de acceso Telnet	class
Interfaz Fa0/0 del Router1	Establezca la descripción Establezca la dirección de la Capa 3
Interfaz Fa0/1 del Router1	Establezca la descripción Establezca la dirección de la Capa 3

Introduzca los siguientes comandos en el router:

```
Router>enable
Router#config term
Ingrese los comandos de configuración, uno por línea. Finalice
con 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)# interface fa0/0
Router1(config-if)#ip address 192.168.7.126 255.255.255.128
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 192.168.7.190 255.255.255.192
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 red mediante el comando **ping**.

Nota: Si los pings a los equipos hosts fallan, deshabilite temporalmente el firewall (cortafuegos) de la computadora y vuelva a realizar la verificación. Para deshabilitar un firewall de Windows, **seleccione Inicio > Panel de control > Firewall de Windows**, seleccione **Desactivado** y luego **Aceptar**.

Utilice la siguiente tabla para verificar la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si una prueba falla.

Desde	Hacia	Dirección IP	Resultados de ping
Host1	Dirección IP de la NIC	192.168.7.1	Debe tener éxito
Host1	Router1, Fa0/0	192.168.7.126	Debe tener éxito
Host1	Router1, Fa0/1	192.168.7.190	Debe tener éxito
Host1	Host2	192.168.7.129	Debe tener éxito
Host2	Dirección IP de la NIC	192.168.7.129	Debe tener éxito
Host2	Router1, Fa0/1	192.168.7.190	Debe tener éxito
Host2	Router1, Fa0/0	192.168.7.126	Debe tener éxito
Host2	Host1	192.168.7.1	Debe tener éxito

Además del comando **ping**, ¿Qué otro comando de Windows es útil para mostrar el retardo de red y divisiones en la ruta al destino?_____
tracert

Tarea 5: Verificar contraseñas

Paso 1: Hacer Telnet al router desde el Host2 y verificar la contraseña de Telnet.

Debe poder hacer Telnet a cualquier interfaz Fast Ethernet del router.

En una ventana de comandos del Host2, escriba:

```
telnet 192.168.7.190
```

Cuando se le solicite el ingreso de la contraseña de Telnet, escriba **cisco** y oprima Intro.

¿Telnet fue exitoso? _____

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

Desde la sesión de Telnet, ingrese al modo exec privilegiado y verifique que se encuentre protegido por contraseña:

```
Router>enable
```

¿Se le pidió que introdujera la contraseña secreta de enable? _____

Paso 3: Verificar que la consola se encuentre protegida por contraseña.

Termine y luego reestablezca la conexión de consola desde el Host1 al router para verificar que la consola se encuentra protegida por contraseña.

Dependiendo del cliente Telnet que esté utilizando, la sesión puede terminarse, a menudo, con Ctrl-]. Cuando se reestablece la sesión, se le debe solicitar el ingreso de la contraseña de la consola antes de permitirle acceder a la interfaz de línea de comando.

Tarea 6: Reflexión

¿En qué se diferencian el acceso a la consola y el acceso a Telnet? ¿Cuándo tendría sentido establecer diferentes contraseñas en ambos puertos de acceso? _____

_____

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

_____

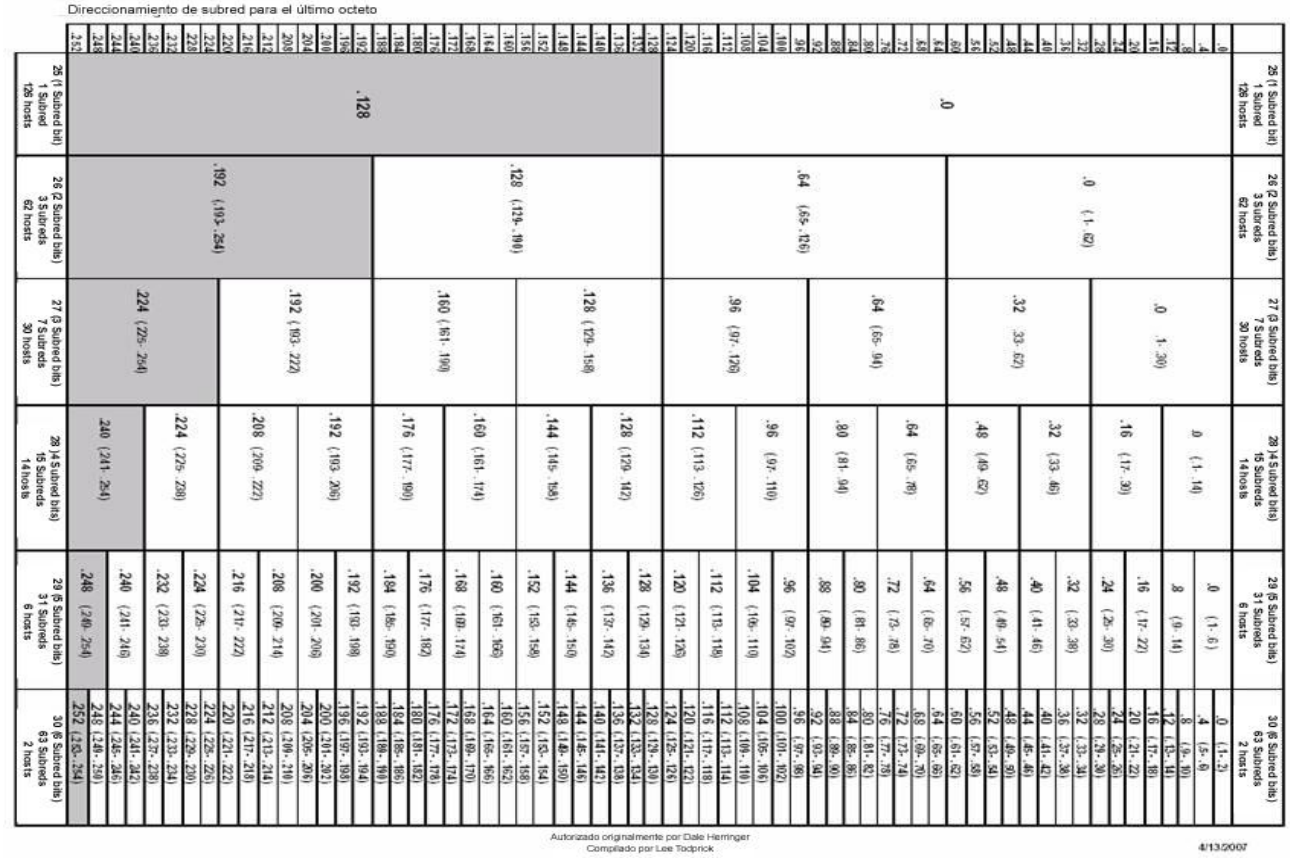
Tarea 7: Limpieza

A menos que su instructor indique lo contrario, borre las configuraciones y cargue nuevamente los switches. Desconecte y guarde el cableado. En caso de PC hosts que están normalmente conectadas a otras redes (tales como la LAN de la escuela o de Internet) vuelva a conectar el cableado apropiado y restaure la configuración de TCP/IP.

Configuración definitiva del Router 1

```
Router1#show run
<selective output omitted>
!
hostname Router1
!
enable secret class
!
!
 interface FastEthernet0/0
 description connection to host1
 ip address 192.168.7.126 255.255.255.128
 no shutdown
!
interface FastEthernet0/1
 description connection to switch1
 ip address 192.168.7.190 255.255.255.192
 no shutdown
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Apéndice 1: Tabla de subred para el último octeto



Apéndice 2: Creación de una sesión de consola del Router utilizando HyperTerminal

Tarea 1: Conectar un router y una computadora con un cable de consola

Paso 1: Establecer una conexión física básica.

Conecte el cable de consola (transpuesto) al puerto de consola del router. Conecte el otro extremo del cable al equipo host con un adaptador
DB-9 o DB-25 al puerto COM 1.

Paso 2: Encender los dispositivos.

Si todavía no están encendidos, encienda la computadora y el router.

Tarea 2: Configurar HyperTerminal para establecer una sesión de consola con el router IOS de Cisco

Paso 1: Iniciar la aplicación de HyperTerminal.

Ejecute el programa HyperTerminal haciendo clic en **Inicio > Programas > Accesorios > Comunicaciones > HyperTerminal**.

Paso 2: Configurar HyperTerminal.

Figura 3. Ventana de configuración de nombre de HyperTerminal

En la ventana Descripción de la conexión introduzca un nombre de sesión en el campo Nombre. Seleccione un ícono adecuado o deje el establecido de manera predeterminada. Haga clic en **Aceptar**.

Figura 4. Tipo de conexión de HyperTerminal

Ingrese COM 1 en el campo Conectar mediante, y luego haga clic en **ACEPTAR**. (Dependiendo de la PC que esté utilizando, podría ser necesario utilizar un puerto COM diferente. Si COM1 no funciona, pruebe sistemáticamente los puertos COM adicionales hasta que tenga éxito).

Figura 5. Configuración del puerto COM1 de HyperTerminal

Como se muestra en la Figura 3, cambie la configuración del puerto con los siguientes valores, y luego haga clic en **ACEPTAR**:

Configuración	**Valor**
Bits por segundo	**9600**
Bits de datos	**8**
Paridad	**Ninguno**
Bits de parada	**1**
Control del flujo	**Ninguno**

Cuando se muestre la ventana de sesión de HyperTerminal, oprima **Intro**. Deberá haber una respuesta del router. Esto significa que la conexión se ha realizado con éxito. Si no hay conexión, haga un diagnóstico de fallas según sea necesario. Por ejemplo: verifique si el router está encendido. Verifique la conexión al puerto COM1 de la PC y el puerto de la consola en el router. Si aún no hay conexión, pida ayuda a su instructor.

Paso 3: Cerrar HyperTerminal.

Cuando termine, cierre la sesión de HyperTerminal seleccionando **Archivo > Salir**. Cuando se le pregunte si desea guardar la sesión, haga clic en **Sí**. Ingrese un nombre para la sesión.

Paso 4: Reconectar la sesión de HyperTerminal.

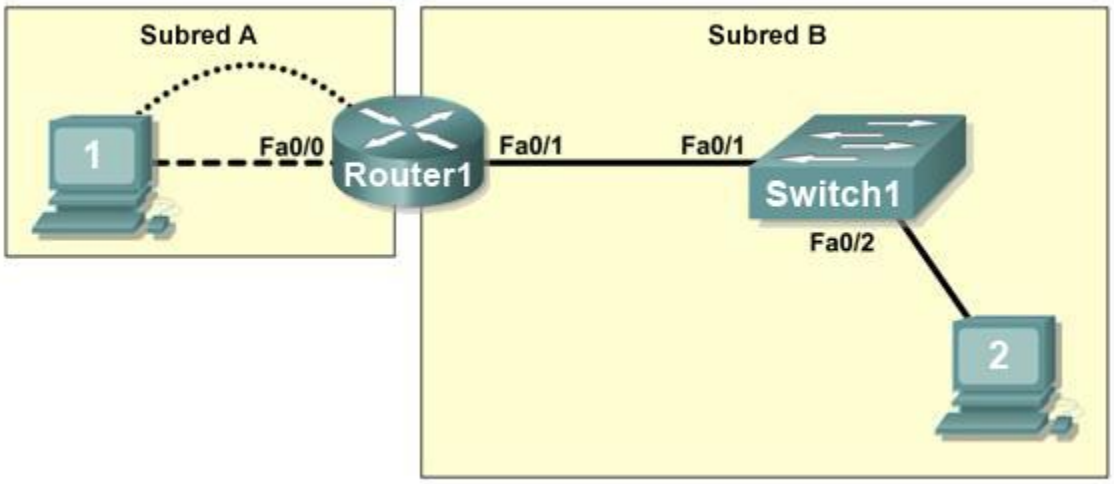
Reabra la sesión HyperTerminal como se describe en la Tarea 2, Paso 1. Esta vez, cuando se abra la ventana de Descripción de la conexión (ver Figura 3), haga clic en **Cancelar**.

Seleccione **Archivo** > **Abrir**. Seleccione la sesión guardada y luego haga clic en **Abrir**. Use este paso para reconectar la sesión de HyperTerminal con un dispositivo Cisco sin reconfigurar una nueva sesión.

Cuando termine, salga de HyperTerminal.

Práctica de laboratorio 1.3.2: Revisión de los conceptos de Exploration 1: Desafío (Versión para el instructor)

Diagrama de topología



Objetivos de aprendizaje

Al completar esta práctica de laboratorio podrá:

- Crear una topología lógica con los requisitos de red dados
- Crear subredes que cumplan con los requisitos del host
- Configurar la topología física
- Configurar la topología lógica
- Verificar la conectividad de la red
- Configurar y verificar contraseñas

Escenario

En esta práctica de laboratorio diseñará y configurará una pequeña red enrutada y verificará la conectividad a través de múltiples dispositivos de red. Esto requiere la creación y la asignación de dos bloques de subredes, la conexión de hosts y dispositivos de red y la configuración de computadoras hosts y un router Cisco para conectividad de red básica. El switch 1 presenta una configuración predeterminada y no requiere configuración adicional. Utilizará los comandos habituales para evaluar y documentar la red. Se utiliza la subred cero.

Tarea 1: Diseñar una topología lógica de LAN

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 utiliza la subred 0. No se pueden utilizar calculadoras de subredes. Cree el número más pequeño de subredes posible que cumplan los requisitos para los hosts. Asigne la primera subred utilizable a la Subred A.

Subred A	
Especificación	**Entrada del estudiante**
Número de bits en la subred	1
Máscara de IP (binaria)	11111111. 11111111. 11111111.11110000
Nueva máscara de IP (decimal)	255.255.255.240
Cantidad máxima de subredes utilizables (incluyendo la subred 0)	2
Cantidad de hosts utilizables por subred	14
Dirección IP de la subred	192.168.30.0
Primera dirección IP de host	192.168.30.1
Última dirección IP de host	192.168.30.14

Subred B	
Especificación	**Entrada del estudiante**
Número de bits en la subred	1
Máscara de IP (binaria)	11111111. 11111111. 11111111.11110000
Nueva máscara de IP (decimal)	255.255.255.240
Cantidad máxima de subredes utilizables (incluyendo la subred 0)	2
Cantidad de hosts utilizables por subred	14
Dirección IP de la subred	192.168.30.16
Primera dirección IP de host	192.168.30.17
Última dirección IP de host	192.168.30.30

Los equipos host utilizan la primera dirección IP en la subred. El router de la red utiliza la última dirección IP en la subred.

Paso 2: Anotar la información de la dirección IP de cada dispositivo.

Dispositivo	Dirección IP	Máscara	Gateway (puerta de salida)
Host1	192.168.30.1	255.255.255.240	192.168.30.14
Router1-Fa0/0	192.168.30.14	255.255.255.240	----------
Host2	192.168.30.17	255.255.255.240	192.168.30.30
Router1-Fa0/1	192.168.30.30	255.255.255.240	----------

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

Tarea 2: Configurar la topología física

Paso 1: Determinar los requisitos de cableado.

En referencia a la Figura 1, identifique cada tipo de cable requerido y documéntelo en la tabla.

Cableado correcto	Tipo de cable
Cable LAN entre el Host1 y el Router1 Fa0/0	Interconexión cruzada
Cable LAN entre el Switch1 y el Router1 Fa0/1	De conexión directa
Cable LAN entre el Switch1 y el Host2	De conexión directa
Cable de consola entre el host1 y el Router1	Transpuesto

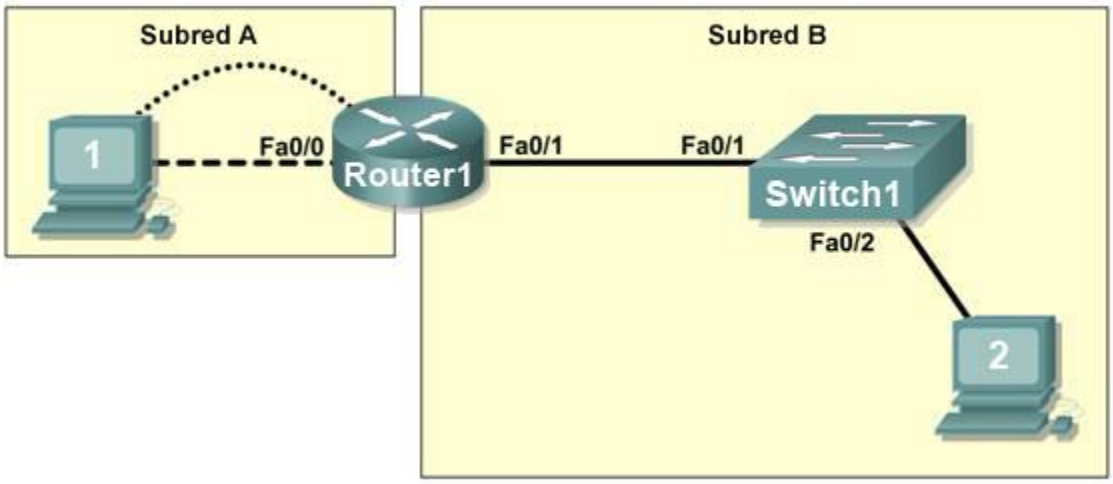


Figura 1. Cableado de la red.

Paso 2. Conectar físicamente los dispositivos de la práctica de laboratorio.

Instale el cableado de los dispositivos de la red según se muestra en la Figura 1. Encienda todos los dispositivos, en caso de que no lo estén.

Paso 3: Inspeccionar las conexiones de la red.

Después de realizar el cableado de los dispositivos de red, verifique las conexiones.

Nota para el instructor: Asegúrese de que el switch se encuentre en su configuración predeterminada y de que Fa0/1 y Fa0/2 se encuentren en VLAN1. Asegúrese de que el router se encuentre configurado de manera predeterminada, sin contraseñas ni interfaces configuradas.

Tarea 3: Configurar la topología lógica

Paso 1: Configurar las computadoras host.

Configure la dirección IP estática, la máscara de subred y la gateway para cada computadora host. Después de configurar cada computadora host, muestre y verifique las configuraciones de red del host mediante el comando **ipconfig /all**.

Configuración de red del Host1	
Dirección física	Las respuestas varían
Dirección IP	192.168.30.1
Máscara de subred	255.255.255.240
Gateway predeterminada	192.168.30.14

Configuración de red del Host2	
Dirección física	Las respuestas varían
Dirección IP	192.168.30.17
Máscara de subred	255.255.255.240
Gateway predeterminada	192.168.30.30

Paso 2: Configurar el Router1.

Desde el Host1, conecte la consola del Router 1 y configure lo siguiente:

Tarea	Especificación
Nombre del router	`Router1`
Contraseña encriptada para el modo exec privilegiado	`class`
Contraseña de acceso a la consola	`cisco`
Contraseña de acceso Telnet	`cisco`
Interfaz Fa0/0 del Router1	Establezca la descripción Establezca la dirección de la Capa 3
Interfaz Fa0/1 del Router1	Establezca la descripción Establezca la dirección de la Capa 3

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 red mediante el comando **ping**.

Nota: Si fallan los pings a las computadoras, verifique si se encuentra en ejecución un programa de firewall en los hosts. Si hay un firewall en ejecución en el host, deshabilítelo en forma temporal y vuelva a realizar la prueba. Para deshabilitar un firewall de Windows, **seleccione Inicio > Panel de control > Firewall de Windows**, seleccione **Desactivado** y luego **Aceptar**.

Utilice la siguiente tabla para verificar la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si una prueba falla.

Desde	Hacia	Dirección IP	Resultados de ping
Host1	Dirección IP de la NIC	192.168.30.1.	Debe tener éxito.
Host1	Router1, Fa0/0	192.168.30.14	Debe tener éxito.
Host1	Router1, Fa0/1	192.168.30.30	Debe tener éxito.
Host1	Host2	192.168.30.17	Debe tener éxito.

Host2	Dirección IP de la NIC	192.168.30.17	Debe tener éxito
Host2	Router1, Fa0/1	192.168.30.30	Debe tener éxito.
Host2	Router1, Fa0/0	192.168.30.14	Debe tener éxito
Host2	Host1	192.168.30.1	Debe tener éxito

Además del comando **ping**, ¿Qué otro comando de Windows es útil para mostrar el retardo de red y divisiones en la ruta al destino?_____
tracert

Tarea 5: Verificar contraseñas

Paso 1: Hacer Telnet al router desde el Host2 y verificar la contraseña de Telnet.

Debe poder hacer Telnet a cualquier interfaz Fast Ethernet del router.

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

Desde la sesión de Telnet, ingrese al modo exec privilegiado y verifique que se encuentre protegido por contraseña.

Paso 3: Verificar que la consola se encuentre protegida por contraseña.

Termine y luego reestablezca la conexión de consola desde el Host1 al router para verificar que la consola se encuentra protegida por contraseña.

Dependiendo del cliente Telnet que esté utilizando, la sesión puede terminarse, a menudo, con Ctrl-].

Tarea 6: Limpieza

A menos que su instructor indique lo contrario, borre las configuraciones y cargue nuevamente los switches. Desconecte y guarde el cableado. En caso de PC hosts que están normalmente conectadas a otras redes (tales como la LAN de la escuela o de Internet) vuelva a conectar el cableado apropiado y restaure la configuración de TCP/IP.

Comandos de configuración del Router

```
Router>en
Router#conf t
Ingrese los comandos de configuración, uno por línea. Finalice con 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 1 4
Router1(config-line)#password cisco
Router1(config-line)#login
Router1(config-line)#interface fa0/0
Router1(config-if)#ip address 192.168.30.14 255.255.255.240
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 192.168.30.30 255.255.255.240
Router1(config-if)#no shutdown
Router1(config-if)#^Z
Router1#
```

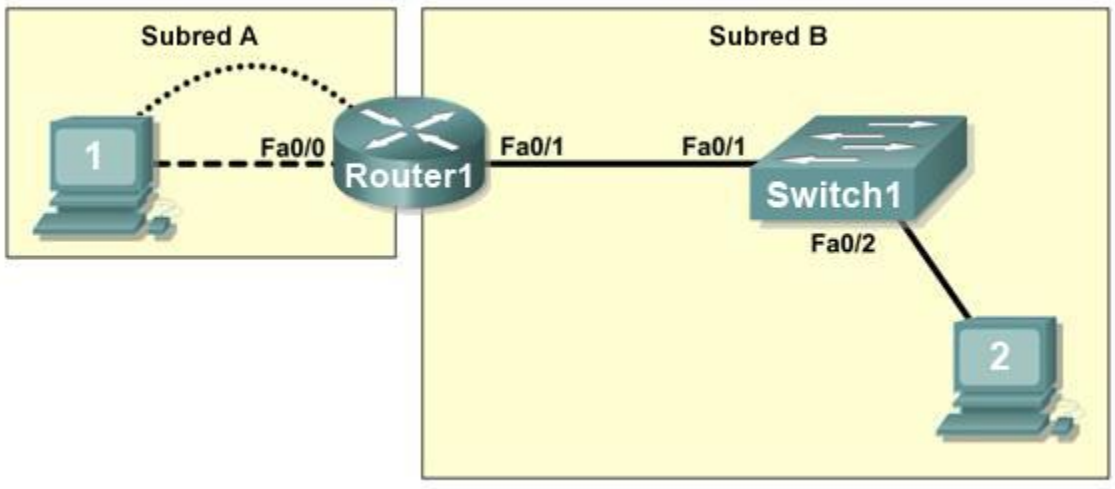
Configuración definitiva del Router 1

```
Router1#show run

<selective output omitted>
!
hostname Router1
!
!
enable secret class
!
interface FastEthernet0/0
 description connection to host1
 ip address 192.168.30.14 255.255.255.240
 no shutdown
!
interface FastEthernet0/1
 description connection to switch1
 ip address 192.168.30.30 255.255.255.240
 no shutdown
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Práctica de laboratorio 1.3.3: Resolución de problemas en una red pequeña (Versión para el instructor)

Diagrama de topología



Objetivos de aprendizaje

Al completar esta práctica de laboratorio podrá:

- Verificar que el diseño en papel cumple con los requisitos de la red
- Cablear una red según el diagrama de topología
- Borrar la configuración inicial y volver a cargar un router al estado predeterminado
- Cargar los routers con las configuraciones provistas
- Descubrir los casos en los que la comunicación no es posible
- Reunir información acerca de la porción de red configurada en forma incorrecta junto con otros errores
- Analizar la información para determinar porqué la comunicación no es posible
- Proponer soluciones a los errores de red
- Implementar soluciones para los errores de red

Escenario

En esta práctica de laboratorio, se le da una configuración completa para una pequeña red enrutada. La configuración incluye errores de diseño y de configuración que están en conflicto con los requerimientos mencionados y evitan la comunicación de extremo a extremo. Examinará el diseño dado e identificará y corregirá cualquier error de diseño. Luego, conectará los cables de la red, configurará los hosts y cargará las configuraciones en el router. Finalmente, resolverá los problemas de conectividad para determinar dónde se producen los errores y los corregirá con el uso de los comandos apropiados. Cuando se hayan corregido todos los errores, cada host debe poder comunicarse con todos los demás elementos configurados de la red y con el otro host.

Tarea 1: Configurar la topología LAN lógica

El bloque de direcciones IP de 172.16.30.3.0/23 se divide en subredes para cumplir con los siguientes requerimientos:

Subred	Cantidad de hosts
Subred A	174
Subred B	60

Requerimientos y especificaciones adicionales:

- Se utiliza la subred 0.
- Se debe utilizar el número más pequeño posible de subredes que satisfagan los requerimientos para los hosts, y mantener el bloque más grande posible en reserva para usos futuros.
- Asigne la primera subred utilizable a la Subred A.
- Los equipos host utilizan la primera dirección IP utilizable en la subred. El router de la red utiliza la última dirección host utilizable de la red.

En base a estos requerimientos, se le ha provisto de la siguiente topología:

Subred A	
Especificación	**Valor**
Máscara de 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	
Especificación	**Valor**
Máscara de IP (decimal)	255.255.255.128 (debe ser 255.255.255.192)
Dirección IP	172.16.31.0
Primera dirección IP de host	172.16.31.1
Última dirección IP de host	172.16.31.126 (debe ser 172.16.31.62 en base a la máscara correcta)

Examine cada uno de los valores en las tablas anteriores y verifique que esta topología cumpla con todos los requerimientos y especificaciones. ¿Alguno de los valores dados es incorrecto? _____

Si su respuesta es afirmativa, corrija los valores en la tabla anterior y escriba los valores corregidos a continuación:

_____

_____

Cree una tabla de configuración similar a la que aparece a continuación utilizando los valores corregidos:

Dispositivo	Dirección IP	Máscara	Gateway (puerta de salida)
Host1	172.16.30.1	255.255.255.0	172.16.30.254
Router1–Fa0/0	172.16.30.254	255.255.255.0	No aplicable
Host2	172.16.31.1	255.255.255.128 (255.255.255.192)	172.16.31.126 (172.16.31.62)
Router1–Fa0/1	172.16.31.126 (172.16.31.62)	255.255.255.128 255.255.255.192	No aplicable

Tarea 2: Cablear, borrar y cargar nuevamente los routers

Paso 1: Cablear la red.

Cablee una red de manera similar al del diagrama de topología.

Paso 2: Borrar la configuración en cada router.

Borre la configuración en el router utilizando el comando **erase startup-config** y luego cargue nuevamente el router. Responda **no** si se le pregunta si desea guardar los cambios.

Tarea 3: Configurar las computadoras host

Paso 1: Configurar las computadoras host.

Configure la dirección IP estática, la máscara de subred y la gateway para cada computadora host en base a la tabla de configuración creada en la tarea 1. Después de configurar cada computadora host, muestre y verifique las configuraciones de red del host con el comando **ipconfig /all**.

Tarea 4: Cargar el router con las configuraciones provistas

(Nota para el instructor: los comandos faltantes o mal configurados se muestran en rojo)

```
enable
!
config term
!
hostname Router1
!
enable secret class
!
no ip domain-lookup
!
 interface FastEthernet0/0
 description connection to host1
 ip address 172.16.30.1 255.255.255.0
(duplicar dirección IP: debe ser 172.16.30.254)
```

```
 duplex auto
 speed auto
 (comando faltante: no shutdown)
!
interface FastEthernet0/1
 description connection to switch1
 ip address 192.16.31.1 255.255.255.192
(dirección IP errónea: debe ser 172.16.31.62)
 duplex auto
 speed auto
(comando faltante: no shutdown)
!
!
line con 0
 password cisco
 login
line vty 0
 login
line vty 1 4
 password cisco
 login
!
end
```

Tarea 5: Identificar problemas de conectividad

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

Utilice la siguiente tabla para probar la conectividad de cada dispositivo de red.

Desde	Hacia	Dirección IP	Resultados de ping
Host1	Dirección IP de la NIC	172.16.30.1	Debe tener éxito.
Host1	Router1, Fa0/0	172.16.30.254	Debe fallar.
Host1	Router1, Fa0/1	172.16.31.126	Debe fallar.
Host1	Host2	172.16.31.1	Debe fallar.
Host2	Dirección IP de la NIC	172.16.30.1	Debe tener éxito
Host2	Router1, Fa0/1	172.16.31.126	Debe fallar.
Host2	Router1, Fa0/0	172.16.30.254	Debe fallar.
Host2	Host1	172.16.30.1	Debe fallar.

Tarea 6: Diagnosticar fallas en las conexiones de red

Paso 1: Comenzar el diagnóstico de fallas en el host conectado al router BRANCH.

Desde el host PC1, ¿es posible hacer ping a PC2? _____ No

Desde el host PC1, ¿es posible hacer ping a la interfaz fa0/1 del router? _____ No

Desde el host PC1, ¿es posible hacer ping a la gateway predeterminada? _____ No

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

¿Cuál es el lugar más lógico para comenzar el diagnóstico de los problemas de conexión en la PC1?

_____

_____

La primera conexión: PC1 a la interfaz fa0/0 del router

Paso 2: **Examinar el router para detectar posibles errores de configuración.**

Comience mediante la visualización del resumen de la información de estado para cada interfaz en el router.

¿Existen problemas con el estado de las interfaces?

_____

_____

Las interfaces fa0/0 and fa0/1 están administrativamente desactivadas

Si existen problemas con el estado de las interfaces, anote los comandos que sean necesarios para corregir los errores de configuración.

_____

_____

config term; interface FastEthernet 0/0; no shutdown; FastEthernet 0/1; no shutdown

Paso 3: **Utilizar los comandos necesarios para corregir la configuración del router.**

Paso 4: **Visualizar un resumen de la información de estado.**

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

¿La información en el resumen de estado de la interfaz indica algún error de configuración en el Router1? _____ no

Si la respuesta es **sí**, realice un diagnóstico de fallas en el estado de la interfaz de las interfaces.

¿Se ha restablecido la conectividad? _____ no

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 la interfaz es consistente con la tabla de configuración? _____ no

Si existen diferencias entre la tabla de configuración y la configuración de la interfaz del router, anote los comandos que sean necesarios para corregir la configuración del router.

_____

_____

config term; interface FastEthernet 0/0; ip address 172.16.30.254 255.255.255.0; interface FastEthernet 0/1; ip address 172.16.31.62 255.255.255.192; end

¿Se ha restablecido la conectividad? _____ sí

¿Por qué es útil para un host hacer ping a su propia dirección?

_____

_____

Verifica la stack de TCP/IP en el host

Tarea 7: Limpieza

A menos que su instructor indique lo contrario, borre las configuraciones y cargue nuevamente los switches. Desconecte y guarde el cableado. En caso de PC hosts que están normalmente conectadas a otras redes (tales como la LAN de la escuela o de Internet) vuelva a conectar el cableado apropiado y restaure la configuración de TCP/IP.

Configuración corregida del Router1

```
Router1#show run
<selective output omitted>
!
hostname Router1
!
enable secret class
!
 interface FastEthernet0/0
 description connection to host1
 ip address 172.16.30.254 255.255.255.0
 no shutdown
!
interface FastEthernet0/1
 description connection to switch1
 ip address 172.16.31.62 255.255.255.192
 no shutdown
!
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Práctica de laboratorio 2.5.1: Configuración básica del switch (Versión para el instructor)

Topología

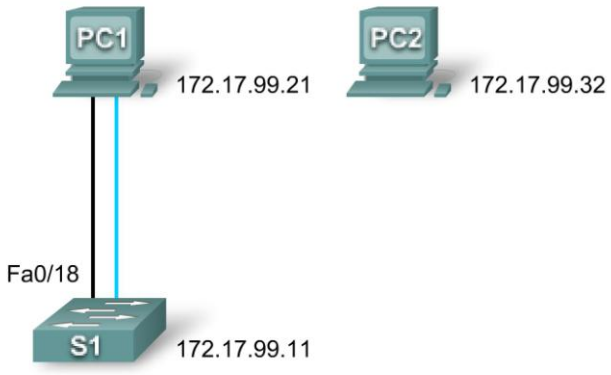


Tabla de direccionamiento

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**	172.17.99.32	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

Al completar esta práctica de laboratorio podrá:

- Cablear una red según el diagrama de topología
- Borrar una configuración existente en un switch
- Examinar y verificar la configuración predeterminada
- Crear una configuración básica de switch, incluyendo un nombre y una dirección IP
- Configurar contraseñas para garantizar que el acceso a la CLI sea seguro
- Configurar la velocidad del puerto de switch y las propiedades dúplex para una interfaz
- Configurar la seguridad básica de puerto del switch
- Administrar la tabla de direcciones MAC
- Asignar direcciones MAC estáticas
- Agregar y mover hosts en un switch

Escenario

En esta práctica de laboratorio, examinará y configurará un switch de LAN independiente. Pese a que el switch realiza funciones básicas en su estado predeterminado de manera no convencional, existe una cantidad de parámetros que un administrador de red debe modificar para garantizar una LAN segura y optimizada. Esta práctica de laboratorio presenta los conceptos básicos de la configuración del switch.

Tarea 1: Cablear, borrar y cargar nuevamente el switch

Paso 1: Cablear una red.

Cablee una red de manera similar al diagrama de topología. Cree una conexión de la consola al switch. De ser necesario, consulte la Práctica de laboratorio 1.3.1 acerca de cómo crear una conexión de consola.

Puede utilizar cualquier switch actual en su práctica de laboratorio siempre y cuando éste tenga las interfaces necesarias que se muestran en la topología. El resultado que se muestra en esta práctica de laboratorio corresponde a un switch 2960. Si utiliza otros switches, el resultado del switch y las descripciones de la interfaz podrían aparecer diferentes.

Nota: PC2 no se encuentra conectada inicialmente al switch. Sólo se utiliza en la tarea 5.

Paso 2: Borrar la configuración en el switch.

Borre la configuración en el switch utilizando el procedimiento del Apéndice 1.

Tarea 2: Verificar la configuración predeterminada de un switch

Paso 1: Entrar al modo privilegiado.

Puede acceder a todos los comandos del switch en modo privilegiado. Sin embargo, debido a que muchos comandos privilegiados configuran parámetros de operación, el acceso privilegiado debe estar protegido por contraseña a fin de evitar el uso no autorizado. Establecerá contraseñas en la Tarea 3.

El conjunto de comandos EXEC privilegiados incluye aquellos comandos del modo EXEC usuario, así como también el comando **configure terminal** a través del cual se obtiene acceso a los modos de comando restantes. Entre al modo EXEC privilegiado introduciendo el comando **enable**.

```
Switch>enable
Switch#
```

Observe que la configuración de la consola de comandos cambia para reflejar el modo EXEC privilegiado.

Paso 2: Examinar la configuración actual del switch.

Examine el archivo de configuración activa actual.

```
Switch#show running-config
```

¿Cuántas interfaces de Fast Ethernet tiene el switch? _____24

¿Cuántas interfaces de Gigabit Ethernet tiene el switch? _____2

¿Cuál es el intervalo de valores que se muestra para las líneas vty? _____0-4; 5-15

Examine el contenido actual de la NVRAM:

```
Switch#show startup-config
startup-config is not present
```

¿Por qué emite esta respuesta el switch?

_____

Todavía no se ha guardado ninguna configuración para NVRAM. Si el switch se ha configurado pero no borrado, se mostrará la configuración inicial. Un switch nuevo no convencional no habría estado preconfigurado.

Examine las características de la interfaz virtual VLAN1:

```
Switch#show interface vlan1
```

¿Tiene el switch una dirección IP establecida? _____no

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

¿Está activada esta interfaz? _____

Los switches de Cisco tienen el comando **no shutdown** configurado de manera predeterminada en VLAN 1 pero VLAN 1 no alcanzará el estado activado/activado hasta que se le asigne un puerto y el mismo también esté activado. Si no hay puerto en estado activado en VLAN 1, la interfaz VLAN 1 estará administrativamente desactivada, protocolo desactivado.

Ahora visualice las propiedades del IP de la interfaz:

```
Switch#show ip interface vlan1
```

¿Qué resultado ve? _____

```
Vlan1 is administratively down, line protocol is down
 Internet protocol processing disabled
```

Paso 3: Mostrar la información de Cisco IOS

Examine la siguiente información acerca de la versión generada por el switch.

```
Switch#show version
```

¿Cuál es la versión de Cisco IOS que ejecuta el switch? _____12.2(25)SEE3 (puede variar)

¿Cuál es el nombre del archivo de imagen del sistema?
_____C2960-LANBASE-M (puede variar)

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

Paso 4: Examinar las interfaces Fast Ethernet.

Examine las propiedades predeterminadas de la interfaz Fast Ethernet que utiliza la PC1.

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

¿Está activada o desactivada la interfaz? _____ Debe estar activado a menos que haya un problema de cableado

¿Qué cosa puede hacer que una interfaz se active? _____ conexión de un host u otro dispositivo

¿Cuál es la dirección MAC de la interfaz? _____varía

¿Cuál es la configuración de velocidad y de dúplex de la interfaz? _____Full-duplex, 100Mb/s

Paso 5: Examinar la información de VLAN.

Examine la configuración VLAN predeterminada del switch.

```
Switch#show vlan
```

¿Cuál es el nombre de la VLAN 1? _____predeterminado

¿Cuáles son los puertos que hay en esta VLAN? _____todos los puertos; Fa0/1 – Fa0/24; Gig1/1, Gig1/2

¿Está activada la VLAN 1? _____sí

¿Qué tipo de VLAN es la VLAN predeterminada? _____(Ethernet)

Paso 6: Examinar la memoria flash.

Ejecute uno de los siguientes comandos para examinar el contenido del directorio flash.

```
Switch#dir flash:
```

o

```
Switch#show flash
```

¿Qué archivos o directorios se encuentran?

_____

c2960-lanbase-mz.122-25.SEE3 (puede variar)

Los archivos tienen una extensión, como .bin, al final de su nombre. Los directorios no tienen una extensión de archivo. Para examinar los archivos en un directorio, ejecute el siguiente comando utilizando el nombre de archivo que se muestra en el resultado del comando anterior:

```
Switch#dir flash:c2960-lanbase-mz.122-25.SEE3
```

El resultado deberá verse de manera similar a lo siguiente:

```
Directory of flash:/c2960-lanbase-mz.122-25.SEE3/
   6 drwx     4480  Mar 1 1993 00:04:42 +00:00 html
 618 -rwx  4671175  Mar 1 1993 00:06:06 +00:00 c2960-lanbase-mz.122-25.SEE3.bin
 619 -rwx      457  Mar 1 1993 00:06:06 +00:00 info
32514048 bytes total (24804864 bytes free)
```

¿Cuál es el nombre del archivo de imagen de Cisco IOS? _____
c2960--lanbase-mz.122-25.SEE3.bin

Paso 7: Examinar el archivo de configuración inicial.

Para ver el contenido del archivo de configuración inicial, ejecute el comando **show startup-config** en el modo EXEC privilegiado:

```
Switch#show startup-config
startup-config is not present
```

¿Por qué aparece este mensaje? _____
Aún no se ha guardado nada en la RAM no volátil (NVRAM).

Haga una modificación a la configuración del switch y guárdela. Escriba los siguientes comandos:

```
Switch#configure terminal
Ingrese los comandos de configuración, uno por línea. Finalice con CNTL/Z.
```

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

Para guardar el contenido del archivo de configuración activo 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]
```

Nota: Es más fácil ingresar este comando mediante la abreviatura **copy run start**.

Ahora muestre los contenidos de la NVRAM usando el comando **show startup-config**.

```
S1#show startup-config
Using 1170 out of 65536 bytes
!
versión 12,2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname S1
!
<resultado omitido>
```

La configuración actual se ha escrito en la NVRAM.

Tarea 3: Crear una configuración básica de switch

Paso 1: Asignar un nombre al switch.

En el último paso de la tarea anterior, configuró el nombre del host. A continuación encontrará un resumen de los comandos utilizados.

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

Paso 2: Establecer las contraseñas de acceso.

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

```
S1#configure terminal
Introduzca los comandos de configuración, uno por cada línea. Al terminar,
regrese al modo de configuración global mediante la ejecución del comando
exit u oprimiendo Ctrl-Z.

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**

¿Por qué se requiere el comando **login**? _____
Sin el comando **login**, el switch no requerira el ingreso de una contraseña.

Paso 3: Configurar las contraseñas de los modos de comando.

Establezca class como contraseña secreta de enable. Esta contraseña protege el acceso al modo EXEC privilegiado.

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

Paso 4: Configurar la dirección de Capa 3 del switch.

Antes de poder administrar la S1 en forma remota desde la PC1, necesita asignar una dirección IP al switch. La configuración predeterminada del switch es que la administración del mismo sea controlada a través de VLAN1. Sin embargo, una optimización para la configuración básica del switch es modificar la administración para que la realice una VLAN que no sea VLAN 1. Las implicancias y razones de esta acción se explican en el próximo capítulo.

A los fines administrativos, utilizaremos VLAN 99. La selección de VLAN 99 es arbitraria y no implica, de modo alguno, que siempre debe utilizarse ésa.

En primer lugar, creará la nueva VLAN 99 en el switch. Luego, configurará la dirección IP del switch en 172.17.99.11 con la máscara de subred 255.255.255.0 en la interfaz virtual interna VLAN 99.

```
S1(config)#vlan 99
S1(config-vlan)#exit
S1(config)#interface vlan99
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down

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

Observe que la interfaz VLAN 99 está en estado desactivado aunque usted ha ingresado el comando **no shutdown**. La interfaz se encuentra desactivada actualmente debido a que no se asignaron puertos del switch a la VLAN 99.

Asigne todos los puertos de usuario a VLAN 99.

```
S1#configure terminal
S1(config)#interface range fa0/1 - 24
S1(config-if-range)#switchport access vlan 99
S1(config-if-range)#exit
S1(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

La exploración completa de las VLAN está fuera del alcance de esta práctica de laboratorio. Este tema se analiza en detalle en el próximo capítulo. Sin embargo, para establecer la conectividad entre el host y el switch, los puertos que utiliza el host deben estar en la misma VLAN que el switch. Observe en el resultado anterior que la interfaz VLAN 1 se desactiva porque no se le asigna ningún puerto. Después de algunos segundos, VLAN 99 se activará porque se le asigna al menos un puerto a esta última.

Paso 5: Establecer la gateway predeterminada del switch.

S1 es un switch de Capa 2, por lo tanto toma decisiones de envío en base al encabezado de la Capa 2. Si hay varias redes conectadas a un switch, necesita especificar el modo en que el switch envía las tramas de internetwork, porque la ruta se debe determinar en la Capa tres. Esto se realiza al especificar una dirección de gateway predeterminada que apunte a un router o un switch de Capa 3. Aunque esta actividad no incluye una gateway de IP externo, tenga en cuenta que eventualmente conectará la LAN a un router para acceso externo. Si suponemos que la interfaz de LAN en el router es 172.17.99.1, establezca la gateway predeterminada para el switch.

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

Paso 6: Verificar la configuración de las LAN de administración.

Verifique la configuración de interfaz de la VLAN 99.

```
S1#show interface vlan 99
Vlan99 is up, line protocol is up
 Hardware is EtherSVI, address is 001b.5302.4ec1 (bia 001b.5302.4ec1)
 Internet address is 172.17.99.11/24
 MTU 1500 bytes, BW 1000000 Kbit, DLY 10 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 00:00:06, output 00:03:23, 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 queue: 0/40 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
    4 packets input, 1368 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    1 packets output, 64 bytes, 0 underruns
    0 output errors, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

¿Cuál es el ancho de banda en esta interfaz? _____ BW 1000000 Kbit

¿Cuáles son los estados de la VLAN?: VLAN99 está _____ activada, el Protocolo de línea está _____activado

¿Cuál es la estrategia de colas? _____fifo

Paso 7: Configurar la dirección IP y la gateway predeterminada para PCI.

Establezca la dirección IP de la PC1 en 172.17.99.21 con una máscara de subred 255.255.255.0. Configure una gateway predeterminada en 172.17.99.11. (De ser necesario, consulte la Práctica de laboratorio 1.3.1 para configurar la NIC de la PC).

Paso 8: Verificar la conectividad.

Para verificar que los hosts y el switch estén configurados correctamente, haga ping a la dirección IP del switch (172.17.99.11) desde la PC1.

¿Fue exitoso el ping? _____debe tener éxito

En caso contrario, realice el diagnóstico de fallas del switch y de la configuración del host. Observe que pueden ser necesarios varios intentos para que los pings tengan éxito.

Paso 9: Configurar la velocidad del puerto y la configuración dúplex para una interfaz Fast Ethernet.

Realice la configuración de velocidad y dúplex en Fast Ethernet 0/18. Utilice 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
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed
state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Protocolo de línea en la interfaz FastEthernet0/18,
estado cambiado a activado
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

El protocolo de línea para la interfaz FastEthernet 0/18 y la interfaz VLAN 99 se desactivará de forma temporal.

El valor predeterminado en la interfaz Ethernet del switch es de detección automática, por lo tanto negocia automáticamente las configuraciones óptimas. Las propiedades dúplex y de velocidad se deben configurar manualmente sólo si un puerto debe funcionar a una cierta velocidad y en modo dúplex. Configurar puertos en forma manual puede conducir a una falta de concordancia en el dúplex, lo cual puede disminuir el rendimiento en forma significativa.

Verifique las nuevas configuraciones de dúplex y de velocidad en la interfaz Fast Ethernet.

```
S1#show interface fastethernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
 Hardware is Fast Ethernet, address is 001b.5302.4e92 (bia 001b.5302.4e92)
 MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Keepalive set (10 sec)
 Full-duplex, 100Mb/s, media type is 10/100BaseTX
 input flow-control is off, output flow-control is unsupported
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input never, output 00:00:01, 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 queue: 0/40 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
    265 packets input, 52078 bytes, 0 no buffer
    Received 265 broadcasts (0 multicast)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 32 multicast, 0 pause input
    0 input packets with dribble condition detected
    4109 packets output, 342112 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
```

```
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier, 0 PAUSE output
 0 output buffer failures, 0 output buffers swapped out
```

Paso 10: Guardar la configuración.

Ha completado la configuración básica del switch. Ahora haga una copia de seguridad del archivo de configuración activo a NVRAM para garantizar que los cambios que se han realizado no se pierdan si el sistema se reinicia o se apaga.

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

Paso 11: Examinar el archivo de configuración inicial.

Para ver la configuración guardada en la NVRAM, ejecute el comando **show startup-config** en el modo EXEC privilegiado.

```
S1#show startup-config
```

¿Todos los cambios realizados están grabados en el archivo? _____sí

Tarea 4: Gestión de la tabla de direcciones MAC

Paso 1: Anotar las direcciones MAC de los hosts.

Determine y anote las direcciones de Capa 2 (físicas) de las tarjetas de interfaz de red de la PC utilizando los siguientes comandos:

Inicio > Ejecutar > cmd > ipconfig /all

PC1: _____

PC2: _____

Paso 2: Determinar las direcciones MAC que el switch ha aprendido.

Muestre las direcciones MAC utilizando el comando **show mac-address-table** en modo EXEC privilegiado.

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

¿Cuántas direcciones dinámicas hay? _____1 (puede variar)

¿Cuántas direcciones MAC hay en total? _____24 (puede variar)

¿Las direcciones MAC dinámicas concuerdan con las direcciones MAC del host? _____sí

Paso 3: Enumerar las opciones show mac-address-table.

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

¿Cuántas opciones hay disponibles para el comando **show mac-address-table**? _____11 (puede variar)

Muestre solamente las direcciones MAC de la tabla que se aprendieron de forma dinámica.

```
S1#show mac-address-table address <PC1 MAC here>
```

¿Cuántas direcciones dinámicas hay? _____1 (puede variar)

Paso 4: Limpiar la tabla de direcciones MAC.

Para eliminar las direcciones MAC existentes, use el comando **clear mac-address-table** en modo EXEC privilegiado.

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

Paso 5: Verificar los resultados.

Verifique que la tabla de direcciones MAC esté en blanco.

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

¿Cuántas direcciones MAC estáticas hay? _____ al menos 20 (otras entradas estáticas podrían haber sido creadas manualmente).

Nota para el instructor: Las primeras 20 direcciones estáticas están incorporadas a la tabla de direcciones MAC.

¿Cuántas direcciones dinámicas hay? _____0 (podría haber 1, dependiendo en lo rápido que las direcciones sean readquiridas por el switch. ¡apúrese!)

Paso 6: Examinar nuevamente la tabla de direcciones MAC.

Hay muchas posibilidades de que una aplicación activa en su PC1 ya haya enviado una trama desde la NIC hacia la S1. Observe nuevamente la tabla de direcciones en modo EXEC privilegiado para ver si S1 ha reaprendido la dirección MAC para la PC1.

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

¿Cuántas direcciones dinámicas hay? _____1

¿Por qué cambió esto desde la última visualización? _____

_____

El switch readquirió dinámicamente las direcciones MAC de la PC.

Si S1 aún no ha reaprendido la dirección MAC para la PC1, haga ping a la dirección de la VLAN 99 del switch desde la PC1 y repita el Paso 6.

Paso 7: Configurar una dirección MAC estática.

Para especificar a qué puertos se puede conectar un host, una posibilidad 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 anotó para PC1 en el paso 1 de esta tarea. La dirección MAC 00e0.2917.1884 se utiliza sólo como ejemplo. Debe utilizar la dirección MAC de su PC1, que es distinta a la del ejemplo.

```
S1(config)#mac-address-table static 00e0.2917.1884 interface fastethernet
0/18 vlan 99
```

Paso 8: Verificar los resultados.

Verifique las entradas de la tabla de direcciones MAC.

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

¿Cuántas direcciones MAC hay en total? _____ 22 (varía)

¿Cuántas direcciones estáticas hay? _____ 22. El total de direcciones MAC y el de direcciones estáticas debe ser el mismo debido a que no hay otros dispositivos conectados actualmente a S1

Paso 10: Eliminar la entrada de MAC estática.

Para completar la siguiente tarea será necesario eliminar la entrada de la tabla de direcciones MAC estáticas. Ingrese al modo de configuración y elimine el comando escribiendo **no** al comienzo de la cadena de comandos.

Nota: La dirección MAC 00e0.2917.1884 se utiliza sólo en el ejemplo. Utilice la dirección MAC para su PC1.

```
S1(config)#no mac-address-table static 00e0.2917.1884 interface fastethernet
0/18 vlan 99
```

Paso 10: Verificar los resultados.

Verifique que la dirección MAC estática se haya borrado.

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

¿Cuántas direcciones MAC estáticas hay en total? _____ 20 (varía)

Tarea 5 Configuración de la seguridad de puerto

Paso 1: Configurar un segundo host.

Para esta tarea es necesario un segundo host. Establezca la dirección IP de la PC2 en 172.17.99.32 con una máscara de subred 255.255.255.0 y una gateway predeterminada en 172.17.99.11. No conecte aún esta PC al switch.

Paso 2: Verificar la conectividad.

Verifique que la PC1 y el switch aún están correctamente configurados haciendo ping a la dirección IP de la VLAN 99 del switch desde el host.

¿Los pings son exitosos? _____sí

Si la respuesta es no, realice el diagnóstico de fallas en la configuración de los hosts y del switch.

Paso 3: Copiar las direcciones MAC del host.

Anote las direcciones MAC de la Tarea 4, Paso 1.

PC1_____

PC2_____

Paso 4: Determinar qué direcciones MAC ha aprendido el switch.

Muestre las direcciones MAC aprendidas utilizando el comando **show mac-address-table** en modo EXEC privilegiado.

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

¿Cuántas direcciones dinámicas hay? _____1

¿Las direcciones MAC concuerdan con las direcciones MAC del host? _____ sí

Paso 5: Enumerar las opciones de seguridad de puerto.

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

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

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

Paso 6: Configurar la seguridad de puerto en un puerto de acceso.

Configure el puerto del switch Fast Ethernet 0/18 para que acepte sólo dos dispositivos, para que aprenda las direcciones MAC de dichos dispositivos dinámicamente y para que bloquee el tráfico de hosts inválidos en caso de violación.

```
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 protect
S1(config-if)#exit
```

Paso 7: Verificar los resultados.

Muestre la configuración de seguridad de puerto.

```
S1#show port-security
```

¿Cuántas direcciones seguras se permiten en Fast Ethernet 0/18?_____2

¿Cuál es la acción de seguridad para este puerto? _____ proteger

Paso 8: Examinar el archivo de configuración activo.

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

¿Hay sentencias enumeradas que reflejan directamente la implementación de seguridad de la configuración activa? _____sí

Paso 9: Modificar la configuración de post seguridad en un puerto.

En la interfaz Fast Ethernet 0/18, establezca la dirección MAC de seguridad máxima del puerto en 1 y que se desactive en caso de violación.

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

Paso 10: Verificar los resultados.

Muestre la configuración de seguridad de puerto.

```
S1#show port-security
```

¿Se ha modificado la configuración de seguridad del puerto para reflejar las modificaciones del Paso 9?
_____ sí

Haga ping a la dirección de la VLAN 99 del switch desde la PC1 para verificar la conectividad y actualizar la tabla de direcciones MAC. En este momento debe ver la dirección MAC para la PC1 “insertada” en la configuración activa.

```
S1#show run
Building configuration...

<resultado omitido>
!
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 00e0.2917.1884
 speed 100
 duplex full
!
<resultado omitido>
```

Paso 11: Introducir un host no autorizado.

Desconecte la PC1 y conecte la PC2 al puerto Fast Ethernet 0/18. Haga ping a la dirección 172.17.99.11 de la VLAN 99 desde el nuevo host. Espere a que la luz de enlace color ámbar se torne verde. Una vez que se torna verde, debe apagarse casi inmediatamente.

Anote cualquier observación: _____
_____

Se envían mensajes de violación a la consola. A continuación presentamos los mensajes a la consola que los estudiantes deben ver con el resultado específico de la seguridad del puerto resaltado:

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed
state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed
state
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
%PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/18, putting Fa0/18
in err-disable state
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by
MAC address 0019.b90a.ab38 on port FastEthernet0/18.
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed
stateto down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
```

Paso 12: Mostrar la información sobre la configuración del puerto.

Para ver la información de configuración sólo para el puerto Fast Ethernet 0/18, ejecute el siguiente comando en modo EXEC privilegiado:

```
S1#show interface fastethernet 0/18
```

¿Cuál es el estado de esta interfaz?

Fast Ethernet0/18 está _____desactivado El protocolo de línea está _____ desactivado (error desactivado)

Paso 13: Reactivar el puerto.

Si se produce una violación de seguridad y el puerto se desconecta, puede utilizar el comando **no shutdown** para reactivarlo. Sin embargo, mientras el host no autorizado se encuentre conectado a Fast Ethernet 0/18, cualquier tráfico desde el host desactivará el puerto. Vuelva a conectar la PC1 a Fast Ethernet 0/18 e ingrese los siguientes comandos en el switch:

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

Nota: Algunas versiones de IOS pueden requerir un comando **shutdown** manual antes de ingresar el comando **no shutdown**.

Paso 14: Limpieza

A menos que se indique lo contrario, borre la configuración en los switches, desconecte el suministro eléctrico a la computadora host y a los switches y retire y guarde los cables.

Configuración final del switch

```
S1#show run
Building configuration...

Configuración actual: 2234 bytes
!
hostname S1
!
enable secret 5 $1$gKdt$bi8UgEDiGotpPSbpRSJ.G1
!
interface FastEthernet0/1
 switchport access vlan 99
!
<resultado omitido>
!
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 0019.b90a.ab38
 speed 100
 duplex full
!
<resultado omitido>
```

```
!
interface Vlan99
 ip address 172.17.99.11 255.255.255.0
 no ip route-cache
!
ip default-gateway 172.17.99.1
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end

S1#
```

Apéndice 1

Borrar y recargar el switch

En la mayoría de las prácticas de laboratorio en Exploration 3, es necesario comenzar con un switch que no esté configurado. El uso de un switch que cuente con una configuración existente puede provocar resultados impredecibles. Estas instrucciones muestran cómo preparar el switch antes de comenzar la práctica de laboratorio. Estas instrucciones son para el switch 2969. Sin embargo, es el mismo procedimiento que para los switches 2900 y 2950.

Paso 1: Ingresar al modo EXEC privilegiado introduciendo el comando enable.

Si pide una contraseña, introduzca **class**. Si esto no funciona, pregunte al instructor.

```
Switch>enable
```

Paso 2: Eliminar el archivo de información de la base de datos de la VLAN.

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

Si no hay ningún archivo VLAN, se muestra el siguiente mensaje:

```
%Error deleting flash:vlan.dat (No such file or directory)
```

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

```
Switch#erase startup-config
```

Como respuesta, aparecerá la siguiente petición de entrada:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Presione **Intro** para confirmar.

La respuesta deberá ser:

```
Erase of nvram: complete
```

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

Verifique que la configuración de la VLAN se haya eliminado en el Paso 2 utilizando el comando **show vlan**.

Si la información de la VLAN se ha eliminado con éxito en el Paso 2, vaya al Paso 5 y reinicie el switch por medio del comando **reload**.

Si la información acerca de la configuración anterior de la VLAN (que no sea la administración predeterminada de la VLAN 1) sigue existiendo, debe apagar y encender el switch (reiniciar el hardware) en lugar de ejecutar el comando **reload**. Para apagar y encender el switch, retire el cable de alimentación de la parte posterior del switch o desenchúfelo y luego vuelva a enchufarlo.

Paso 5: **Reiniciar el software**.

Nota: Este paso no es necesario si el switch se ha reiniciado utilizando el método de apagar y encender.

En el indicador del modo EXEC privilegiado, introduzca el comando **reload**.

```
Switch(config)#reload
```

Como respuesta, aparecerá la siguiente petición de entrada:

```
System configuration has been modified. Save? [yes/no]:
```

Escriba **n** y luego presione **Intro.**

Como respuesta, aparecerá la siguiente petición de entrada:

```
Proceed with reload? [confirm] [Intro]
```

La primera línea de la respuesta será:

```
Reload requested by console.
```

La siguiente petición de entrada aparecerá después de que el switch se recargue:

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

Escriba **n** y luego presione **Intro.**

Como respuesta, aparecerá la siguiente petición de entrada:

```
Press RETURN to get started! [Intro]
```

Práctica de laboratorio 2.5.2: Administración del sistema operativo y de los archivos de configuración del switch (Versión para el instructor)

Diagrama de topología

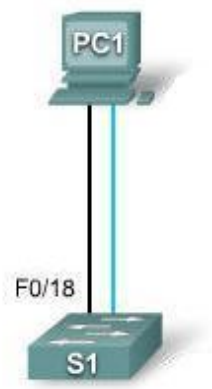


Tabla de direccionamiento

Dispositivo	Nombre del host/Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
PC 1	Host-A	172.17.99.21	255.255.255.0	172.17.99.1
Switch1	VLAN99	172.17.99.11	255.255.255.0	172.17.99.1

Objetivos de aprendizaje

Al completar esta práctica de laboratorio podrá:

- Crear y guardar una configuración de switch básica
- Configurar un servidor TFTP en la red
- Hacer una copia de respaldo del software IOS de Cisco en un servidor TFTP y restaurarlo.
- Hacer una copia de respaldo de la configuración del switch a un servidor TFTP
- Configurar un switch para cargar una configuración desde un servidor TFTP
- Actualizar el software IOS de Cisco desde un servidor TFTP
- Recuperar la contraseña para un switch 2960 (serie 2900)

Escenario

En esta práctica de laboratorio, examinará y configurará un switch de LAN independiente. Pese a que el switch realiza funciones básicas en su estado predeterminado de manera no convencional, existe una cantidad de parámetros que un administrador de red debe modificar para garantizar una LAN segura y optimizada. Esta práctica de laboratorio presenta los conceptos básicos de la configuración del switch.

Tarea 1: Cablear e inicializar la red

Paso 1: Cablear una red.

Cablee una red de manera similar al diagrama de topología. Cree una conexión de la consola al switch. Si es necesario, consulte la Práctica de laboratorio 1.3.1. El resultado que arroja esta práctica de laboratorio es para un switch 2960. Si utiliza otros switches, el resultado del switch y las descripciones de la interfaz podrían aparecer diferentes.

Paso 2: Borrar la configuración en el switch.

Configure una conexión de la consola al switch y borre la configuración existente. De ser necesario, consulte la Práctica de laboratorio 2.5.1, Apéndice 1.

Paso 3: Crear una configuración básica.

Utilice los siguientes comandos para configurar un nombre de host, contraseñas de acceso a la línea, y la contraseña secreta de enable.

```
Switch#configure terminal
Switch(config)#hostname ALSwitch
ALSwitch(config)#exit
ALSwitch(config)#line con 0
ALSwitch(config-line)#password cisco
ALSwitch(config-line)#login
ALSwitch(config-line)#line vty 0 15
ALSwitch(config-line)#password cisco
ALSwitch(config-line)#login
ALSwitch(config-line)#exit
```

Cree VLAN 99 y asigne puertos de usuario a esta VLAN utilizando los siguientes comandos. Vuelva al modo EXEC privilegiado al finalizar.

```
ALSwitch(config)#vlan 99
ALSwitch(config-vlan)#name user
ALSwitch(config-vlan)#exit
ALSwitch(config)#interface vlan 99
ALSwitch(config-if)#ip address 172.17.99.11 255.255.255.0
ALSwitch(config-if)#no shutdown
%LINK-5-CHANGED: Interface Vlan99, changed state to up
ALSwitch(config-if)#exit
ALSwitch(config)#interface fa0/18
ALSwitch(config-if)#switchport access vlan 99
ALSwitch(config-if)#end
ALSwitch#
```

Paso 4: Configurar el host conectado al switch.

Configure el host para utilizar la dirección IP, la máscara y la gateway predeterminada identificada en la tabla de direccionamiento al comienzo de la práctica de laboratorio. En esta práctica de laboratorio este host actuará como el servidor TFTP.

Paso 5: Verificar la conectividad.

Para verificar que el host y el switch estén configurados correctamente, haga ping a la dirección IP del switch que fue configurada para VLAN 99 desde el host.

¿Fue exitoso el ping? _____sí

Si la respuesta es no, realice el diagnóstico de fallas en la configuración de los hosts y del switch.

Tarea 2: Inicio y configuración del servidor TFTP

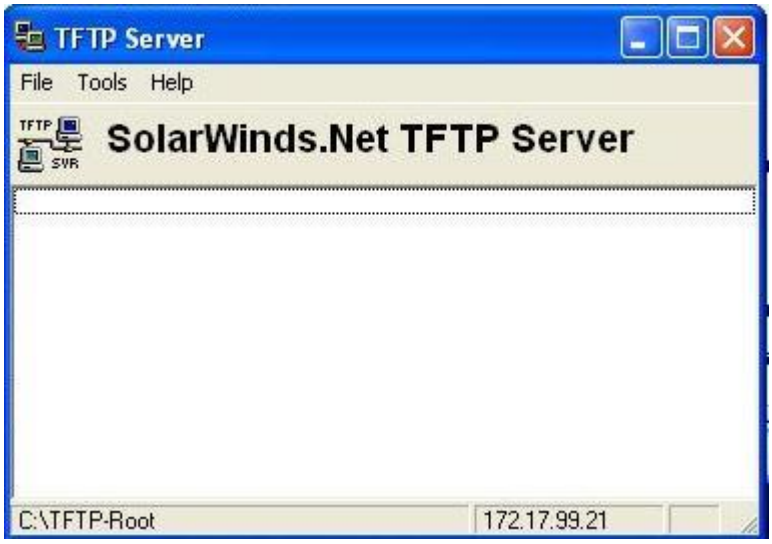
Paso 1: Iniciar y configurar el servidor TFTP.

El servidor TFTP que se presenta en esta práctica de laboratorio es el servidor Solar Winds, disponible en http://www.solarwinds.com/products/freetools/free_tftp_server.aspx. Si esta URL está desactualizada, utilice su motor de búsqueda favorito y busque “descarga del tftp gratuito solar wind”.

Puede no ser igual al utilizado en esta clase. Controle con su instructor las instrucciones operativas para el servidor TFTP que se utilice en lugar del servidor TFTP de Solar Wind.

Inicie el servidor en el host **Inicio > Todos los programas > SolarWinds 2003 Standard Edition > Servidor TFTP**.

El servidor debe iniciarse y adquirir la dirección IP de la interfaz Ethernet y utilizar el directorio C:\TFTP-Root predeterminado.



Cuando el servidor TFTP se está ejecutando y muestra la configuración de dirección correcta en la estación de trabajo, copie el archivo de IOS de Cisco desde el switch al servidor TFTP.

Paso 2: Verificar la conectividad al servidor TFTP.

Verifique que el servidor TFTP está en funcionamiento y que es posible hacer ping al mismo desde el switch.

¿Cuál es la dirección IP del servidor TFTP? _____
172.17.99.21 (Igual al Host A)

```
Switch#ping 172.17.99.21

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.21 , timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1006
ms
Switch#
```

Tarea 3: Guarde el archivo IOS de Cisco en un servidor TFTP

Paso 1: Identificar el nombre de archivo de IOS de Cisco.

Determine el nombre exacto del archivo de imagen que debe guardarse. Desde la sesión de consola, introduzca **show flash**.

```
Switch#show flash
(El resultado varía)
Directory of flash:/
   2  -rwx         556   Mar 8 1993 22:46:45 +00:00  vlan.dat
   5  drwx         192   Mar 1 1993 00:04:53 +00:00  c2960-lanbase-
mz.122-25.FX
32514048 bytes total (26527232 bytes free)
```

¿Cuáles son el nombre y la longitud de la imagen IOS de Cisco almacenados en la memoria flash? ____

_____

Nota: Si el archivo se encuentra en un subdirectorio, como en el resultado anterior, al principio no puede ver el nombre de archivo. Para ver el nombre de archivo de IOS de Cisco, utilice el comando **cd** para cambiar el directorio activo del switch por el directorio IOS de Cisco:

```
Switch#cd flash:/c2960-lanbase-mz.122-25.FX
Switch#show flash
Directory of flash:/c2960-lanbase-mz.122-25.FX/
    6  drwx     4160   Mar 1 1993 00:03:36 +00:00  html
  368  -rwx     4414921   Mar 1 1993 00:04:53 +00:00  c2960-lanbase-
mz.122-25.FX.bin
  369  -rwx      429   Mar 1 1993 00:04:53 +00:00  info

32514048 bytes total (26527232 bytes free)
```

¿Cuáles son el nombre y la longitud de la imagen IOS de Cisco almacenados en la memoria flash? ____

_____

c2960-lanbase-mz.122-25.FX.bin 4414921 bytes

¿Qué atributos se pueden identificar a partir de los códigos en el nombre de archivo IOS de Cisco?_____

_____

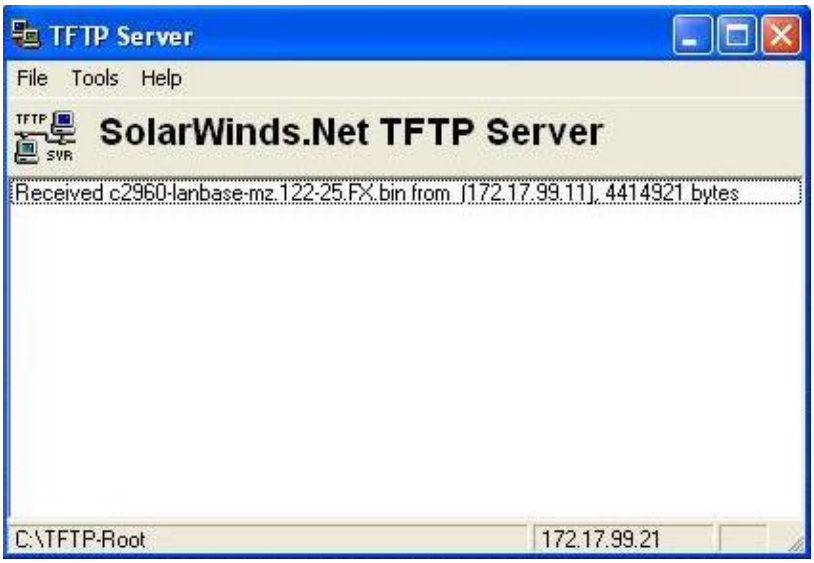
Plataforma, versión, número de lanzamiento, conjunto de funciones

Desde el modo EXEC privilegiado, ingrese el comando **copy flash tftp**. En el indicador, ingrese primero el nombre del archivo de imagen de ISO de Cisco y luego la dirección IP del servidor TFTP. Asegúrese de incluir la ruta completa si el archivo se encuentra en un subdirectorio.

```
Switch#copy flash tftp
Source filename []?c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-
25.FX.bin
Address or name of remote host []? 172.17.99.21
Destination filename [c2960-lanbase-mz.122-25.FX.bin]? [intro]
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
4414921 bytes copied in 10.822 secs (407958 bytes/sec)
Switch#
```

Paso 2: Verificar la transferencia al servidor TFTP.

Verifique la transferencia al servidor TFTP observando el archivo de registro. En el servidor TFTP SolarWind, la transferencia puede verificarse desde la ventana de comandos, según se muestra en la siguiente figura:



Verifique el tamaño de la imagen flash en el directorio raíz del servidor. La ruta del servidor raíz se muestra en la ventana de comandos del servidor —C:\TFTP-root.

Localice este directorio en el servidor utilizando el Administrador de archivos y observe el listado detallado del archivo. La longitud que muestra el comando **show flash** debe ser igual al tamaño del archivo almacenado en el servidor TFTP. Si los tamaños de archivo no son idénticos, consulte con el instructor.

Tarea 4: Restaurar el archivo IOS de Cisco en el Switch desde un Servidor TFTP

Paso 1: Verificar la conectividad.

Verifique que el servidor TFTP esté activo y haga ping a la dirección IP del servidor TFTP desde el switch.

¿Cuál es la dirección IP del servidor TFTP? _____172.17.99.21

```
Switch#ping 172.17.99.21
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.21 , timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1006
ms
Switch#
```

Si no puede hacer ping, realice el diagnóstico de fallas de las configuraciones del switch y del servidor.

Paso 2: Identificar el nombre de archivo IOS de Cisco en el servidor y la ruta completa del destino del switch.

¿Cuál es el nombre del archivo en el directorio raíz del servidor TFTP que se copiará al switch?

_____

(varía) c2960-lanbase-mz.122-25.FX.bin

¿Cuál es el nombre de la ruta de destino para el archivo IOS de Cisco en el switch?

_____

(varía) c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-25.FX.bin

¿Cuál es la dirección IP del servidor TFTP? _____172.17.99.21

Paso 3: Cargar el software IOS de Cisco desde el servidor al switch.

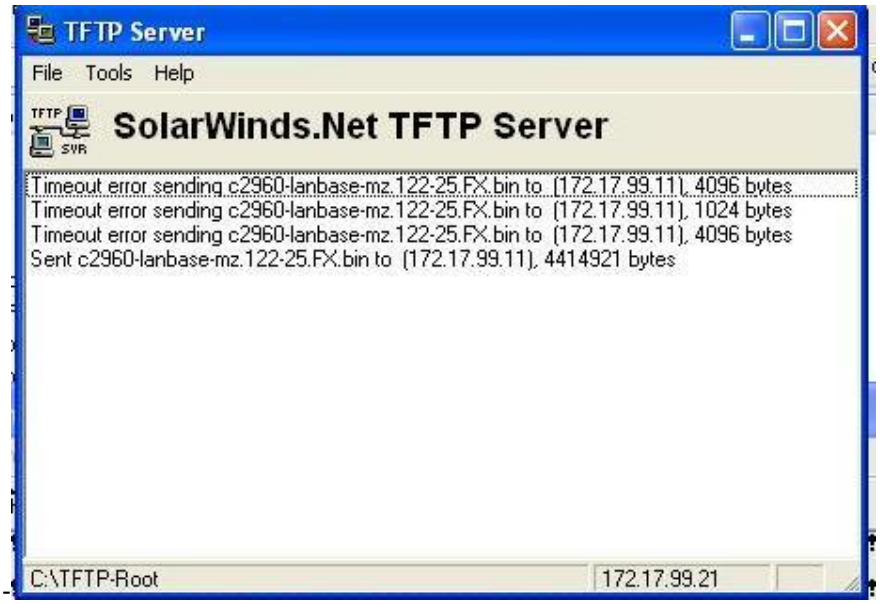
Nota: Es importante que este proceso no se interrumpa.

En modo EXEC privilegiado, copie el archivo desde el servidor TFTP a la memoria flash.

```
Switch#copy tftp flash
Address or name of remote host []? 172.17.99.21
Source filename []? c2960-lanbase-mz.122-25.FX.bin
Destination filename [c2960-lanbase-mz.122-25.FX.bin]? c2960-lanbase-
mz.122-25.F
X/c2960-lanbase-mz.122-25.FX.bin
%Warning:There is a file already existing with this name
Do you want to over write? [confirm] [enter]
Accessing tftp://172.17.99.21 /c2960-lanbase-mz.122-25.FX.bin...
Loading c2960-lanbase-mz.122-25.FX.bin from 172.17.99.21 (via
Vlan1):!!!!!!!!!!!!!!!!!!
<output omitted>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 4414921 bytes]

4414921 bytes copied in 43.964 secs (100421 bytes/sec)
Switch#
```

La pantalla de resultados del servidor debe ser similar a la siguiente:



¿El tamaño del archivo cargado es similar al tamaño del archivo guardado en el directorio raíz del TFTP?
_____sí

Paso 4: Probar la imagen de IOS de Cisco restaurada.

Verifique que la imagen del switch es correcta. Para hacer esto, cargue nuevamente el switch y observe el proceso de inicio para confirmar que no haya errores de flash. Si no hay, entonces el software IOS de Cisco del switch se habrá iniciado correctamente. Para una posterior verificación de la imagen IOS de Cisco en la flash emita el comando **show version** que mostrará un resultado similar a lo siguiente:

```
System image file is "flash:c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-
25.FX.bin"
```

Tarea 5: Hacer una copia de respaldo y restaurar un archivo de configuración desde un servidor TFTP

Paso 1: Copiar el archivo de configuración inicial en el servidor TFTP.

Verifique que el servidor TFTP está en funcionamiento y que es posible hacer ping al mismo desde el switch.

¿Cuál es la dirección IP del servidor TFTP? _____172.17.99.21

En el modo EXEC privilegiado, introduzca el comando **copy running-config startup-config** para asegurarse de que el archivo de configuración activo se guarde en el archivo de configuración de inicio.

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

Haga una copia de respaldo del archivo de configuración guardado en el servidor TFTP mediante el comando **copy startup-config tftp**. En la petición de entrada, introduzca la dirección IP del servidor TFTP:

```
AlSwitch#copy startup-config tftp
Address or name of remote host []? 172.17.99.21
Destination filename [alswitch-confg]? [intro]
!!
1452 bytes copied in 0.445 secs (3263 bytes/sec)#
```

Paso 2: Verificar la transferencia al servidor TFTP.

Verifique la transferencia al servidor TFTP controlando la ventana de comandos del servidor TFTP. El resultado debe ser similar a lo siguiente:

```
Received alswitch-confg from (172.17.99.11), 1452 bytes
```

Verifique que el archivo alswitch-config se encuentre en el directorio C:\TFTP-root del servidor TFTP.

Paso 3: Restaurar el archivo de configuración inicial desde el servidor TFTP.

Para restaurar el archivo de configuración inicial se debe borrar el archivo de configuración inicial existente y se debe volver a cargar el switch.

```
AlSwitch#erase nvram
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
AlSwitch#
AlSwitch#reload
Proceed with reload? [confirm] [enter]
```

Cuando el switch se haya cargado nuevamente, debe volver a establecer la conectividad entre el switch y el servidor TFTP antes de que la configuración pueda restaurarse. Para hacerlo, configure la VLAN 99 con la dirección IP correcta y asigne un puerto Fast Ethernet 0/18 a la VLAN 99. Al terminar, regrese al modo EXEC privilegiado.

```
Switch>enable
Switch#configure terminal
Ingrese los comandos de configuración, uno por línea. Finalice con
CNTL/Z.
Switch(config)#interface vlan 99
Switch(config-if)#ip address 172.17.99.11 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/18
Switch(config-if)#switchport access vlan 99
Switch(config-if)#end
Switch#
```

Después de que la VLAN 99 esté activa, verifique la conectividad haciendo ping al servidor desde el switch.

```
Switch#ping 172.17.99.21
```

Si el ping no tiene éxito, realice el diagnóstico de fallas de las configuraciones del switch y del servidor. Restaure la configuración desde el servidor TFTP mediante el comando **copy tftp startup-config**.

Nota: Es importante que este proceso no se interrumpa.

```
Switch#copy tftp startup-config
Address or name of remote host []? 172.17.99.21
Source filename []? alswitch-confg
Destination filename [startup-config]? [intro]
Accessing tftp://172.17.99.21 /alswitch-confg...
Loading alswitch-confg from 172.17.99.21 (via Vlan99): !
[OK - 1452 bytes]
1452 bytes copied in 9.059 secs (160 bytes/sec)
Switch#
00:21:37: %SYS-5-CONFIG_NV_I: Nonvolatile storage configured from
tftp://172.17.99.21 /alswitch-confg by console
Switch#
```

¿Fue exitosa la operación? _____ sí

Paso 4: Verificar el archivo de configuración inicial restaurado.

En modo EXEC privilegiado, cargue nuevamente el switch. Después de hacerlo, el switch debe mostrar el indicador ALSwitch. Escriba el comando **show startup-config** para verificar que la configuración restaurada se encuentra completa, incluyendo el acceso a la línea y las contraseñas secretas de enable.

Tarea 6: Actualizar el software IOS de Cisco del switch

Nota: Esta práctica de laboratorio requiere una combinación de la imagen IOS de Cisco y del archivo HTML (tar) ubicados de manera predeterminada en el directorio del servidor TFTP por parte del instructor o del estudiante. El instructor debe descargar este archivo del centro de software Cisco Connection online. En esta práctica de laboratorio se hace referencia al archivo c2960-lanbase-mz.122-25.FX.tar para fines de instrucción solamente. Éste tiene la misma raíz de nombre de archivo que la imagen actual. Sin embargo, a los fines de esta práctica de laboratorio, suponga que ésta es una actualización.
La actualización de versión del software IOS de Cisco incluye la imagen binaria y nuevos archivos HTML que admiten cambios en la interfaz de web.

Esta práctica de laboratorio también requiere que haya una copia guardada del archivo de configuración actual como copia de respaldo.

Paso 1: Determinar la secuencia de arranque actual del switch.

Utilice el comando **show boot** para mostrar la configuración de las variables de entorno del arranque.

```
ALSwitch#show boot
BOOT path-list: flash:c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-
25.FX.bin
Config file: flash:/config.text
Private Config file : flash:/private-config.text
Enable Break: no
Manual Boot: no
HELPER path-list:
Auto upgrade        : yes
NVRAM/Config file
      buffer size:   65536
ALSwitch#
```

Determine si hay suficiente memoria para múltiples archivos de imagen:

```
ALSwitch#sh flash
Directory of flash:/
    2  -rwx         616   Mar 1 1993 06:39:02 +00:00  vlan.dat
    4  -rwx           5   Mar 1 1993 10:14:07 +00:00  private-
config.text
    5  drwx         192   Mar 1 1993 00:04:53 +00:00  c2960-lanbase-
mz.122-25.FX
  370  -rwx        1281   Mar 1 1993 10:14:07 +00:00  config.text

32514048 bytes total (26524672 bytes free)
ALSwitch#
```

Observe que en esta plataforma hay sólo 6 MB en uso y aproximadamente 26,5 MB libres, por lo que hay suficiente memoria para varias imágenes. Si no hay espacio suficiente para múltiples imágenes, debe sobreescribir la imagen existente con la nueva; por ese motivo, asegúrese de que haya una copia de respaldo del archivo IOS de Cisco actual en el servidor TFTP antes de comenzar con la actualización.

Paso 2: Preparación para la nueva imagen.

Si el switch cuenta con suficiente memoria disponible como la que se mostró en el último paso, utilice el comando **rename** para renombrar el archivo IOS de Cisco existente con el mismo nombre con la extensión .old:

```
ALSwitch#rename flash:/c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-
25.FX.bin flash:/c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-25.FX.old
```

Verifique que la asignación del nuevo nombre haya sido exitosa:

```
ALSwitch#dir flash:/c2960-lanbase-mz.122-25.FX/
Directory of flash:/c2960-lanbase-mz.122-25.FX/

    6  drwx     4160   Mar 1 1993 00:03:36 +00:00  html
  368  -rwx     4414921   Mar 1 1993 03:26:51 +00:00  c2960-lanbase-
mz.122-25.FX.old
  369  -rwx      429   Mar 1 1993 00:04:53 +00:00  info
32514048 bytes total (26524672 bytes free)
```

Utilice el comando **delete** para eliminar los archivos HTML existentes. La inclusión de un * en el comando en lugar de un nombre de archivo específico borra todos los archivos del directorio.

```
ALSwitch#delete flash:/c2960-lanbase-mz.122-25.FX/html/*
```

Paso 3: Extraer la nueva imagen de IOS de Cisco y los archivos HTML a la memoria flash.

Escriba lo siguiente para ubicar la nueva imagen de IOS de Cisco y los archivos HTML en el directorio destino de la memoria flash:

```
ALSwitch#archive tar /x tftp://172.17.99.21/c2960-lanbase-mz.122-
25.FX.tar flash:/c2960-lanbase-mz.122-25.FX

ALSwitch(config)#ip http server
```

Paso 4: Asociar el nuevo archivo de arranque.

Introduzca el comando **boot** con el nombre de la nueva imagen del nombre de archivo en la petición de entrada del modo de configuración global. Al terminar, regrese al modo EXEC privilegiado y guarde la configuración.

```
ALSwitch(config)#boot system flash:/c2960-lanbase-mz.122-25.FX/c2960-
lanbase-mz.122-25.FX.bin
ALSwitch(config)# end
ALSwitch#copy running-config startup-config
```

Paso 5: Reiniciar el switch.

Reinicie el switch por medio del comando **reload** para ver si el nuevo software IOS de Cisco se ha cargado. Utilice el comando **show version** para ver el nombre de archivo de IOS de Cisco.

¿Cuál es el nombre del archivo de IOS de Cisco desde el cual arrancó el switch? _____

_____ _____

c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-25.FX.bin

¿Es éste el nombre de archivo correcto? _____ sí

Si el nombre de archivo de IOS de Cisco es correcto, elimine el archivo de respaldo de la memoria flash utilizando este comando desde el modo EXEC privilegiado:

```
ALSwitch(config)#delete flash:/c2960-lanbase-mz.122-25.FX/c2960-lanbase-
mz.122-25.FX.old
```

Tarea 7: Recuperar las contraseñas en Catalyst 2960

Paso 1: Reconfigurar la contraseña de consola.

Haga que un compañero cambie las contraseñas de consola y de vty del switch. Guarde los cambios en el archivo startup-config y vuelva a cargar el switch.

Entonces, sin conocer las contraseñas, trate de acceder al switch.

Paso 2: Recuperar el acceso al switch

Asegúrese de que un PC esté conectado al puerto de consola y que haya una ventana de HyperTerminal abierta. Apague el switch. Vuelva a encenderlo mientras presiona el botón **MODE** en la parte delantera del switch al mismo tiempo que se enciende el switch. Suelte el botón **MODE** después de que el LED SYST deja de titilar y queda fijo.

La siguiente información debe aparecer en la pantalla:

```
The system has been interrupted prior to initializing the flash files
system. The following commands will initialize the flash files system,
and finish loading the operating system software:
flash_init
```

```
load_helper
boot
```

Para inicializar el sistema de archivos y terminar de cargar el sistema operativo ingrese los siguientes comandos:

```
switch:flash_init
switch:load_helper
switch:dir flash:
```

Nota: No se olvide de escribir los dos puntos (:) después de **flash** en el comando **dir flash**:

Escriba **rename flash**:**config**.**text flash**:**config**.**old** para cambiar el nombre del archivo de configuración. Este archivo contiene la definición de la contraseña.

Paso 3: Reiniciar el sistema.

Escriba el comando **boot** para arrancar el sistema. Ingrese **n** cuando se le indique que continúe con el dialogo de configuración y cuando se le pregunte si desea terminar la auto instalación.

Para cambiar el nombre al archivo de configuración por su nombre original, escriba el comando **rename flash**:**config**.**old flash**:**config**.**text** en el indicador del modo EXEC privilegiado.

Copie el archivo de configuración a la memoria:

```
Switch#copy flash:config.text system:running-config
Source filename [config.text]?[enter]
Destination filename [running-config][enter]
```

Se ha vuelto a cargar el archivo de configuración. Cambie las contraseñas anteriores que se desconocen como se indica a continuación:

```
ALSwitch#configure terminal
ALSwitch(config)#no enable secret
ALSwitch(config)#enable secret class
ALSwitch(config)#line console 0
ALSwitch(config-line)#password cisco
ALSwitch(config-line)#exit
ALSwitch(config)#line vty 0 15
ALSwitch(config-line)#password cisco
ALSwitch(config-line)#end
ALSwitch#copy running-config startup-config
Destination filename [startup-config]?[enter] Building configuration...
[OK]
ALSwitch#
```

Finalice su conexión de consola y luego vuelva a establecerla para verificar que las nuevas contraseñas se han configurado. De no ser así, repita el procedimiento.

Al completar estos pasos, desconéctese escribiendo **exit** y apague todos los dispositivos. Luego, quite y guarde los cables y el adaptador.

Práctica de laboratorio 2.5.3: Administración de sistema operativo y archivos de configuración del switch (desafío) (Versión para el instructor)

Diagrama de topología

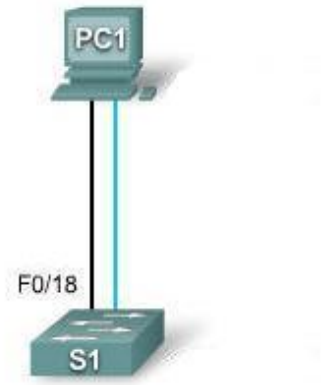


Tabla de direccionamiento

Dispositivo	Nombre del host/Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
PC 1	Host-A	172.17.99.21	255.255.255.0	172.17.99.1
Switch1	VLAN99	172.17.99.11	255.255.255.0	172.17.99.1

Objetivos de aprendizaje

Al completar esta práctica de laboratorio podrá:

- Crear y guardar una configuración de switch básica
- Configurar un servidor TFTP en la red
- Hacer una copia de respaldo del software IOS de Cisco en un servidor TFTP y restaurarlo.
- Hacer una copia de respaldo de la configuración del switch a un servidor TFTP
- Configurar un switch para cargar una configuración desde un servidor TFTP
- Actualizar el software IOS de Cisco desde un servidor TFTP
- Recuperar la contraseña para un switch Cisco 2960 (serie 2900)

Escenario

En esta práctica de laboratorio explorará la administración de archivos y los procedimientos para recuperar contraseñas en un switch Cisco Catalyst.

Tarea 1: Cablear e inicializar la red

Paso 1: Cablear una red.

Cablee una red de manera similar al diagrama de topología. Luego, cree una conexión de consola al switch. Si es necesario, consulte la Práctica de laboratorio 1.3.1. El resultado que arroja esta práctica de laboratorio es para un switch 2960. Si utiliza otros switches, el resultado del switch y las descripciones de la interfaz podrían aparecer diferentes.

Paso 2: Borrar la configuración en cada switch.

Establezca una conexión de la consola al switch. Borre la configuración en el switch.

Paso 3: Crear una configuración básica.

Configure el switch con el siguiente nombre de host y contraseñas de acceso. Luego, cree la contraseña enable secret en el switch.

Nombre de host	Contraseña de la consola	Contraseña Telnet	Contraseña de comando
ALSwitch	cisco	cisco	class

Cree la VLAN 99. Asigne la dirección IP 172.17.99.11 a esta interfaz. Asigne el puerto Fast Ethernet 0/18 a esta VLAN.

```
ALSwitch(config)#vlan 99
ALSwitch(config-vlan)#name user
ALSwitch(config-vlan)#exit
ALSwitch(config)#interface vlan 99
ALSwitch(config-if)#ip address 172.17.99.11 255.255.255.0
ALSwitch(config-if)#no shutdown
%LINK-5-CHANGED: Interface Vlan99, changed state to up
ALSwitch(config-if)#exit
ALSwitch(config)#interface fa0/18
ALSwitch(config-if)#switchport access vlan 99
ALSwitch(config-if)#end
ALSwitch#
```

Paso 4: Configurar el host conectado al switch.

Configure el host para utilizar la dirección IP, la máscara y la gateway predeterminada identificada en la Tabla de direccionamiento. En esta práctica de laboratorio este host actuará como el servidor TFTP.

Paso 5: Verificar la conectividad.

Para verificar que el host y el switch estén configurados correctamente, haga ping a la dirección IP del switch desde el host.

¿Fue exitoso el ping? _____sí

Si la respuesta es no, realice el diagnóstico de fallas en la configuración de los hosts y del switch.

Tarea 2: Inicio y configuración del servidor TFTP

Paso 1: Iniciar y configurar el servidor TFTP.

El servidor TFTP utilizado en el desarrollo de esta práctica de laboratorio es el servidor Solar Wind, disponible en http://www.solarwindssoftware.com/toolsets/tools/tftp-server.aspx

Las prácticas de laboratorio en su aula pueden estar utilizando un servidor TFTP diferente. De ser así, verifique con su instructor las instrucciones de funcionamiento del servidor TFTP en uso.

Inicie el servidor en el host mediante el menú Inicio: **Inicio > Todos los programas> SolarWinds 2003 Standard Edition > TFTP Server**.

El servidor debe iniciarse y obtener la dirección IP de la interfaz Ethernet. El servidor utiliza el directorio C:\TFTP-Root predeterminado.

Paso 2: Verificar la conectividad al servidor TFTP.

Verifique que el servidor TFTP está en funcionamiento y que es posible hacer ping al mismo desde el switch.

```
ALSwitch#ping 172.17.99.21

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.21 , timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1006
ms
ALSwitch#
```

Tarea 3: Guardar el archivo IOS de Cisco en el servidor TFTP

Paso 1: Identificar el nombre de archivo de IOS de Cisco.

Determine el nombre exacto del archivo de imagen que debe guardarse.

```
ALSwitch#show flash
(El resultado varía)
Directory of flash:/
   2  -rwx         556   Mar 8 1993 22:46:45 +00:00  vlan.dat
   5  drwx         192   Mar 1 1993 00:04:53 +00:00  c2960-lanbase-
mz.122-25.FX
32514048 bytes total (26527232 bytes free)
```

Observe que si el archivo se encuentra en un subdirectorio, como en el resultado anterior, al principio no puede ver el nombre de archivo. Para ver el nombre de archivo de IOS de Cisco, primero cambie el directorio activo del switch por el directorio IOS de Cisco.

```
ALSwitch#cd flash:/c2960-lanbase-mz.122-25.FX
ALSwitch#show flash
Directory of flash:/c2960-lanbase-mz.122-25.FX/
    6  drwx     4160   Mar 1 1993 00:03:36 +00:00  html
  368  -rwx     4414921   Mar 1 1993 00:04:53 +00:00  c2960-lanbase-
mz.122-25.FX.bin
  369  -rwx      429   Mar 1 1993 00:04:53 +00:00  info

32514048 bytes total (26527232 bytes free)
ALSwitch#cd
ALSwitch#
```

Examine el resultado desde el switch y responda las siguientes preguntas.

¿Cuáles son el nombre y la longitud de la imagen IOS de Cisco almacenados en la memoria flash?

c2960-lanbase-mz.122-25.FX.bin 4414921 bytes

¿Qué atributos se pueden identificar a partir de los códigos en el nombre de archivo IOS Cisco?

Plataforma, versión, número de lanzamiento, conjunto de funciones

Paso 2: En modo EXEC privilegiado, copiar el archivo de imagen en el servidor TFTP

```
ALSwitch#copy flash tftp
Source filename []?c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-
25.FX.bin
Address or name of remote host []? 172.17.99.21
Destination filename [c2960-lanbase-mz.122-25.FX.bin]? [intro]
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!(output suppressed)
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
4414921 bytes copied in 10.822 secs (407958 bytes/sec)
ALSwitch#
```

Paso 3: Verificar la transferencia al servidor TFTP.

Verifique la transferencia al servidor TFTP observando el archivo de registro. Con el servidor TFTP Solar Wind puede verificar la transferencia desde la ventana de comandos o desde el archivo de registro del servidor en:

C:\Archivos de programas\SolarWinds\2003 Standard Edition\TFTP-Server.log.

Verifique que el tamaño de la imagen flash se encuentre en el directorio raíz del servidor. La ruta del servidor raíz se muestra en la ventana de comandos del servidor:

C:\TFTP-root

Utilice el Administrador de archivos para buscar este directorio en el servidor y observe el listado detallado del archivo. La longitud que muestra el comando **show flash** debe ser igual al tamaño del archivo almacenado en el servidor TFTP. Si los tamaños de archivo no son idénticos, consulte con el instructor.

Tarea 4: Restaurar el archivo IOS de Cisco en el Switch desde un Servidor TFTP

Paso 1: Verificar la conectividad.

Verifique que el servidor TFTP esté activo y haga ping a la dirección IP del servidor TFTP desde el switch.

```
ALSwitch#ping 172.17.99.21
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.21 , timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1006
ms
ALSwitch#
```

Si no puede hacer ping, realice el diagnóstico de fallas de las configuraciones del switch y del servidor.

Paso 2: Identificar el nombre de archivo IOS de Cisco en el servidor y la ruta completa del destino del switch.

¿Cuál es el nombre del archivo en el directorio raíz del servidor TFTP que se copiará al switch?

___

(varía) c2960-lanbase-mz.122-25.FX.bin

¿Cuál es el nombre de ruta del destino para el archivo IOS en el switch?

___

(varía) c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-25.FX.bin

¿Cuál es la dirección IP del servidor TFTP? ___
172.17.99.21

Paso 3: **Cargar el software IOS de Cisco desde el servidor al switch**.

Nota: Es importante que este proceso no se interrumpa.

En modo EXEC privilegiado, copie el archivo desde el servidor TFTP a la memoria flash.

```
ALSwitch#copy tftp flash
Address or name of remote host []? 172.17.99.21
Source filename []? c2960-lanbase-mz.122-25.FX.bin
Destination filename [c2960-lanbase-mz.122-25.FX.bin]? c2960-lanbase-
mz.122-25.FX/c2960-lanbase-mz.122-25.FX.bin
%Warning:There is a file already existing with this name
Do you want to over write? [confirm] [enter]
Accessing tftp://172.17.99.21 /c2960-lanbase-mz.122-25.FX.bin...
Loading c2960-lanbase-mz.122-25.FX.bin from 172.17.99.21 (via
Vlan1):!!!!!!!!!!!!!!!!!
(output suppressed)
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 4414921 bytes]

4414921 bytes copied in 43.964 secs (100421 bytes/sec)
ALSwitch#
```

¿El tamaño del archivo cargado es similar al tamaño del archivo guardado en el directorio raíz del TFTP? ____sí

Paso 4: Probar la imagen de IOS de Cisco restaurada.

Verifique que la imagen del switch es correcta. Para hacer esto, cargue nuevamente la imagen del switch y observe el proceso de inicio. Confirme que no haya errores de flash. Si no hay, entonces el software IOS de Cisco del switch se habrá iniciado correctamente. Para una verificación posterior de la imagen de IOS de Cisco en la flash ejecute el comando que muestra la versión de IOS de Cisco.

```
ALSwitch#show version
<resultado omitido>
System image file is "flash:c2960-lanbase-mz.122-25.FX/c2960-lanbase-
mz.122-25.FX.bin"
```

Tarea 5: Hacer una copia de respaldo y restaurar un archivo de configuración desde un servidor TFTP

Paso 1: Copiar el archivo de configuración inicial en el servidor TFTP.

Verifique que el servidor TFTP está en funcionamiento y que es posible hacer ping al mismo desde el switch. Guarde la configuración activa.

```
ALSwitch#ping 172.17.99.21
ALSwitch#copy running-config startup-config
Destination filename [startup-config]?[enter] Building configuration...
[OK]
```

Haga una copia de respaldo del archivo de configuración en el servidor TFTP.

```
ALSwitch#copy startup-config tftp
Address or name of remote host []? 172.17.99.21
Destination filename [alswitch-confg]? [intro]
!!
1452 bytes copied in 0.445 secs (3263 bytes/sec)
```

Paso 2: Verificar la transferencia al servidor TFTP.

Verifique la transferencia al servidor TFTP observando la ventana de comandos del servidor TFTP. El resultado debe ser similar a lo siguiente:

```
Received alswitch-confg from (172.17.99.11), 1452 bytes
```

Verifique que el archivo alswitch-config se encuentre en el directorio C:\TFTP-root del servidor TFTP.

Paso 3: Restaurar el archivo de configuración inicial desde el servidor TFTP.

Para restaurar el archivo de configuración inicial, primero borre el archivo de configuración inicial existente y luego vuelva a cargar el switch.

```
ALSwitch#erase nvram
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
Switch#reload
Proceed with reload? [confirm] [enter]
```

Cuando el switch se haya cargado nuevamente, debe volver a establecer la conectividad entre el switch y el servidor TFTP antes de que la configuración pueda restaurarse. Para hacerlo, vuelva a configurar la VLAN 99 con la dirección IP correcta y asigne un puerto Fast Ethernet 0/18 a esa VLAN (consulte la Tarea 1).

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. Finalice con CNTL/Z.
Switch(config)#interface vlan 99
Switch(config-if)#ip address 172.17.99.11 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/18
Switch(config-if)#switchport access vlan 99
Switch(config-if)#end
Switch#
```

Después de que la VLAN 99 esté activa, verifique la conectividad haciendo ping al servidor desde el switch.

```
Switch#ping 172.17.99.21
```

Si el ping no tiene éxito, realice el diagnóstico de fallas de las configuraciones del switch y del servidor. Restaure la configuración desde el servidor TFTP copiando el archivo alswitch-confg desde el servidor al switch.

Nota: Es importante que este proceso no se interrumpa.

```
Switch#copy tftp startup-config
      Address or name of remote host []? 172.17.99.21
      Source filename []? alswitch-confg
      Destination filename [startup-config]? [intro]
      Accessing tftp://172.17.99.21 /alswitch-confg...
      Loading alswitch-confg from 172.17.99.21 (via Vlan99): !
      [OK - 1452 bytes]
      1452 bytes copied in 9.059 secs (160 bytes/sec)
      Switch#
      00:21:37: %SYS-5-CONFIG_NV_I: Nonvolatile storage configured from
      tftp://172.17.99.21 /alswitch-confg by console
      Switch#
```

¿Fue exitosa la operación? _____sí

Paso 4: Verificar el archivo de configuración inicial restaurado.

En modo EXEC privilegiado, cargue nuevamente el router. Después de hacerlo, el switch debe mostrar el indicador ALSwitch. Analice la configuración activa para verificar que la configuración restaurada se encuentra completa, incluyendo las contraseñas enable secret y de vty.

Tarea 6: Actualizar el software IOS de Cisco del switch

Nota: Esta práctica de laboratorio requiere una combinación de la imagen IOS de Cisco y del archivo HTML (tar) ubicados de manera predeterminada en el directorio del servidor TFTP por parte del instructor o del estudiante. El instructor debe descargar este archivo del centro de software Cisco Connection online. En esta práctica de laboratorio se hace referencia al archivo c2960-lanbase-mz.122-25.FX.tar para fines de instrucción solamente. Éste tiene la misma raíz de nombre de archivo que la imagen actual. Sin embargo, a los fines de esta práctica de laboratorio, suponga que este archivo es una actualización. La actualización de versión del software IOS de Cisco incluye la imagen binaria y nuevos archivos HTML que admiten cambios en la interfaz de web.

Esta práctica de laboratorio también requiere que haya una copia guardada del archivo de configuración actual como copia de respaldo.

Paso 1: Determinar la secuencia de arranque actual del switch y verificar la disponibilidad de memoria.

```
ALSwitch#show boot
BOOT path-list: flash:c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-
25.FX.bin
(output suppressed)
```

Determine si hay suficiente memoria para múltiples archivos de imagen. Asuma que nos nuevos archivos requieren tanto espacio como los archivos actuales en la memoria flash.

```
ALSwitch#sh flash
      Directory of flash:/
```

```
    2  -rwx         616   Mar 1 1993 06:39:02 +00:00  vlan.dat
    4  -rwx           5   Mar 1 1993 10:14:07 +00:00  private-
config.text
    5  drwx         192   Mar 1 1993 00:04:53 +00:00  c2960-lanbase-
mz.122-25.FX
  370  -rwx        1281   Mar 1 1993 10:14:07 +00:00  config.text

32514048 bytes total (26524672 bytes free)
ALSwitch#
```

Observe que en esta plataforma sólo aproximadamente 6 MB de la memoria flash se encuentran en uso y aproximadamente 26,5 MB libres, por lo que hay suficiente memoria para varias imágenes. Si no hay espacio suficiente para múltiples imágenes, debe sobreescribir la imagen existente con la nueva; por ese motivo, asegúrese de que haya una copia de respaldo del archivo IOS de Cisco actual en el servidor TFTP antes de comenzar con la actualización.

¿Hay suficiente capacidad de memoria para almacenar archivos adicionales de Ios de Cisco y HTML?
_____sí

Paso 2: Preparación para la nueva imagen

Si el switch cuenta con suficiente memoria disponible como la que se describe en el último paso, cambie el nombre del archivo IOS de Cisco para que tenga el mismo nombre con la extensión .old.

```
ALSwitch#rename flash:/c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-
25.FX.bin flash:/c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-25.FX.old
```

Verifique que la asignación del nuevo nombre haya sido exitosa.

```
ALSwitch#dir flash:/c2960-lanbase-mz.122-25.FX/
Directory of flash:/c2960-lanbase-mz.122-25.FX/

    6  drwx        4160   Mar 1 1993 00:03:36 +00:00  html
  368  -rwx     4414921   Mar 1 1993 03:26:51 +00:00  c2960-lanbase-
mz.122-25.FX.old
  369  -rwx         429   Mar 1 1993 00:04:53 +00:00  info
32514048 bytes total (26524672 bytes free)
```

Como medida de precaución, deshabilite el acceso a las páginas HTML del switch y luego elimine los archivos HTML existentes de la memoria flash.

```
ALSwitch(config)#no ip http server
ALSwitch#delete flash:/c2960-lanbase-mz.122-25.FX/html/*
```

Paso 3: Extraer la nueva imagen de IOS de Cisco y los archivos HTML a la memoria flash.

Escriba lo siguiente para ubicar la nueva imagen de IOS de Cisco y los archivos HTML en el directorio destino de la memoria flash:

```
ALSwitch#archive tar /x tftp://172.17.99.21/c2960-lanbase-mz.122-
25.FX.tar flash:/c2960-lanbase-mz.122-25.FX
```

Vuelva a habilitar el servidor HTTP en el switch.

```
ALSwitch(config)#ip http server
```

Paso 4: Asociar el nuevo archivo de arranque.

Introduzca el comando boot system con el nombre de archivo de la nueva imagen en la petición de entrada del modo de configuración y luego guarde la configuración.

```
ALSwitch(config)#boot system flash:/c2960-lanbase-mz.122-25.FX/c2960-
lanbase-mz.122-25.FX.bin
ALSwitch(config)# end
ALSwitch#copy running-config startup-config
```

Nota: En este ejemplo, la secuencia de arranque no se modifica desde la secuencia determinada en el Paso 1 de esta tarea porque utilizamos la misma imagen para simular una actualización del sistema. En una actualización normal, el archivo de la nueva imagen se especificaría en la secuencia de arranque.

Paso 5: Reiniciar el switch.

Reinicie el switch por medio del comando **reload** para ver si el nuevo software IOS de Cisco se ha cargado. Utilice el comando **show version** para ver el nombre del archivo IOS de Cisco.

¿Cuál es el nombre del archivo de IOS de Cisco desde el cual arrancó el switch? _____

_____

¿Es éste el nombre de archivo correcto? _____

Si el nombre de archivo IOS de Cisco es correcto, elimine el archivo de respaldo (con la extensión .old) de la memoria flash.

Tarea 7: Recuperar las contraseñas en Catalyst 2960

Paso 1: Reconfigurar la contraseña de consola.

Haga que un compañero cambie las contraseñas de consola, de vty y enable secret del switch. Guarde los cambios en el archivo startup-config y vuelva a cargar el switch.

Entonces, sin conocer las contraseñas, trate de acceder al modo EXEC privilegiado del switch.

Paso 2: Recuperar el acceso al switch.

Los procedimientos detallados para recuperar contraseñas se encuentran disponibles en la documentación de asistencia en línea de Cisco. En este caso, se pueden encontrar en la sección de diagnóstico de fallas de la Guía de configuración del software del switch Catalyst 2960. Siga los procedimientos para restaurar el acceso al switch.

Nota para el instructor: El procedimiento para recuperar la contraseña de Cisco se encuentra en el Apéndice 1 de esta práctica de laboratorio, en el caso de que no se pueda acceder a Internet en su aula. Sin embargo, parte de este ejercicio consiste en que los estudiantes encuentren y usen la documentación en línea para resolver un problema. Por lo tanto, de ser posible, haga que los estudiantes encuentren el procedimiento por ellos mismos. Los procedimientos se encuentran en http://www.cisco.com/en/US/products/ps6406/products_configuration_guide_chapter09186a00805a7628.html#wp1021182

Al completar estos pasos, desconéctese escribiendo **exit** y apague todos los dispositivos. Luego, quite y guarde los cables y el adaptador.

Apéndice 1: Recuperación de las contraseñas para Catalyst 2960

Recuperación de una contraseña perdida u olvidada

La configuración predeterminada del switch permite que un usuario final con acceso físico al switch recupere una contraseña que ha perdido mediante la interrupción del proceso de arranque durante el encendido y el ingreso de una nueva contraseña. Estos procedimientos de recuperación requieren que usted tenga acceso físico al switch.

Nota: En esos switches, un administrador del sistema puede deshabilitar parte de la funcionalidad de esta función al permitir que un usuario final restablezca una contraseña sólo si accede a regresar a la configuración predeterminada. Si usted es un usuario final que intenta restablecer una nueva contraseña cuando la función de recuperación de contraseña se ha deshabilitado, un mensaje de estado se lo indicará durante el proceso de recuperación.

Estas secciones describen el modo de recuperar una contraseña del switch perdida u olvidada:

- Procedure with Password Recovery Enabled (Procedimiento con la recuperación de contraseña habilitada)
- Procedure with Password Recovery Disabled (Procedimiento con la recuperación de contraseña deshabilitada)

La recuperación de contraseña se habilita o deshabilita mediante el comando de configuración global **service password-recovery**. Siga los pasos en este procedimiento si ha olvidado o perdido la contraseña del switch.

Paso 1 Conecte una terminal o una PC con software de emulación de terminal al puerto de la consola del switch.

Paso 2 Establezca la velocidad de línea en el software de emulación en 9600 baudios.

Paso 3 Desconecte el switch. Vuelva a conectar el cable de alimentación al switch y, dentro de los 15 segundos posteriores, oprima el botón **Modo** mientras el LED del sistema aún parpadea en verde. Continúe oprimiendo el botón **Modo** hasta que el LED del sistema se torne ámbar por un breve instante y luego verde, después suelte el botón **Modo**.

Diversas líneas de información acerca del software aparecen con instrucciones e informan si el procedimiento de recuperación de contraseña se ha deshabilitado o no.

- Si ve un mensaje que comienza de la siguiente manera:

```
El sistema se ha interrumpido antes de inicializar el sistema de
archivos flash. Los
siguientes comandos inicializarán el sistema de archivos flash
```

continúe con la sección "Procedure with Password Recovery Enabled" section y siga los pasos indicados.

- Si ve un mensaje que comienza de la siguiente manera:

```
Se ha activado el mecanismo de recuperación de contraseña pero
está deshabilitado actualmente.
```

continúe con la sección "Procedure with Password Recovery Disabled" section y siga los pasos indicados.

Paso 4 Después de recuperar la contraseña, cargue nuevamente el switch:

```
Switch> reload

Proceed with reload? [confirm] y
```

Procedimiento con la recuperación de contraseña habilitada

Si el mecanismo de recuperación de contraseña se encuentra habilitado, se muestra el siguiente mensaje:

```
El sistema se ha interrumpido antes de inicializar el sistema
de archivos flash. Los siguientes
comandos inicializarán el sistema de archivos flash
y finalizarán la carga del software del
sistema operativo:

flash_init
load_helper
boot
```

Paso 1 Inicialice el sistema de archivos flash:

```
switch: flash_init
```

Paso 2 Si ha configurado la velocidad del puerto de consola en un valor que no sea 9600, ésta se ha restablecido a dicha velocidad. Cambie la velocidad de línea del software de emulación para que coincida con el puerto de la consola del switch.

Paso 3 Cargue cualquier archivo de ayuda:

```
switch: load_helper
```

Paso 4 Muestre el contenido de la memoria flash:

```
switch: dir flash:
```

Se muestra el sistema de archivos del switch:

```
Directory of flash:
   13  drwx         192   Mar 01 1993 22:30:48  c2960-lanbase-
mz.122-25.FX
   11  -rwx        5825   Mar 01 1993 22:31:59  config.text
   18  -rwx         720   Mar 01 1993 02:21:30  vlan.dat

16128000 bytes total (10003456 bytes free)
```

Paso 5 Asigne el nuevo nombre config.text.old al archivo de configuración.

Este archivo contiene la definición de la contraseña.

```
switch: rename flash:config.text flash:config.text.old
```

Paso 6 Arranque el sistema:

```
switch: boot
```

Se le solicitará que inicie el programa de configuración. Introduzca **N** en el indicador:

```
Continue with the configuration dialog? [yes/no]: N
```

Paso 7 En el indicador del switch, ingrese al modo EXEC privilegiado:

```
Switch> enable
```

Paso 8 Vuelva a dar el nombre original al archivo de configuración:

```
Switch# rename flash:config.text.old flash:config.text
```

Paso 9 Copie el archivo de configuración a la memoria:

```
Switch# copy flash:config.text system:running-config
Source filename [config.text]?
Destination filename [running-config]?
```

Oprima **Regresar** en respuesta al indicador de confirmación.

El archivo de configuración está cargado nuevamente y usted puede modificar la contraseña.

Paso 10 Entre al modo de configuración global:

```
Switch# configure terminal
```

Paso 11 Modifique la contraseña:

```
Switch (config)# enable secret password
```

La contraseña secreta puede tener desde 1 hasta 25 caracteres alfanuméricos, puede comenzar con un número, distingue entre mayúsculas y minúsculas y permite espacios pero ignora espacios iniciales.

Paso 12 Vuelva al modo EXEC privilegiado:

```
Switch (config)# exit
Switch#
```

Paso 13 Escriba la configuración activa en el archivo de configuración inicial:

```
Switch# copy running-config startup-config
```

La nueva contraseña es ahora la configuración inicial.

Nota Este procedimiento puede dejar la interfaz virtual del switch en estado desactivado. Puede ver qué interfaz se encuentra en este estado ingresando el comando EXEC privilegiado **show running-config**. Para volver a habilitar la interfaz, ingrese el comando de configuración global **interface vlan** *vlan-id* y especifique el ID de la VLAN de la interfaz desactivada. Con el switch en modo de configuración de interfaz, ingrese el comando **no shutdown**.

Paso 14 Recargue el switch:

```
Switch# reload
```

Procedimiento con la recuperación de contraseña deshabilitada

Si el mecanismo de recuperación de contraseña se encuentra deshabilitado, aparece el siguiente mensaje:

```
Se ha activado el mecanismo de recuperación de contraseña pero
está deshabilitado actualmente. El acceso al indicador de
cargador de arranque mediante el mecanismo de recuperación
de contraseña está deshabilitado. Sin embargo, si accede
a permitir que el sistema vuelva a la configuración de sistema
```

```
predeterminada, el acceso al indicador de cargador de arranque
aún puede permitirse.

¿Desea que el sistema vuelva a la configuración predeterminada?
(s/n)?
```

Precaución Regresar el switch a la configuración predeterminada provoca la pérdida de todas las configuraciones existentes. Recomendamos que se comunique con su administrador de sistema para verificar si hay una copia de respaldo de configuración de VLAN y de switch.

- Si ingresa **n** (no), el proceso de arranque normal continúa como si no se hubiera oprimido el botón **Modo**; no puede acceder al indicador del cargador de arranque y no puede ingresar una nueva contraseña.
Se muestra el mensaje:

```
Presione Intro para continuar........
```

- Si ingresa y (sí), se borran el archivo de configuración en memoria flash y el archivo de la base de datos de la VLAN. Cuando carga la configuración predeterminada puede restablecer la contraseña.

Paso 1 Elija continuar recuperando la contraseña y perdiendo la configuración existente:

```
¿Desea que el sistema vuelva a la configuración predeterminada?
(s/n)? S
```

Paso 2 Cargue cualquier archivo de ayuda:

```
Switch: load_helper
```

Paso 3 Muestre el contenido de la memoria flash:

```
switch: dir flash:
```

Se muestra el sistema de archivos del switch:

```
Directory of flash:
13  drwx         192   Mar 01 1993 22:30:48 c2960-lanbase-
mz.122-25.FX.0

16128000 bytes total (10003456 bytes free)
```

Paso 4 Arranque el sistema:

```
Switch: boot
```

Se le solicitará que inicie el programa de configuración. Para continuar con la recuperación de la contraseña, escriba **N** en el indicador:

```
Continue with the configuration dialog? [yes/no]: N
```

Paso 5 En el indicador del switch, ingrese al modo EXEC privilegiado:

```
Switch> enable
```

Paso 6 Entre al modo de configuración global:

```
Switch# configure terminal
```

Paso 7 Modifique la contraseña:

```
Switch (config)# enable secret password
```

La contraseña secreta puede tener desde 1 hasta 25 caracteres alfanuméricos, puede comenzar con un número, distingue entre mayúsculas y minúsculas y permite espacios pero ignora espacios iniciales.

Paso 8 Vuelva al modo EXEC privilegiado:

```
Switch (config)# exit
Switch#
```

Paso 9 Escriba la configuración activa en el archivo de configuración inicial:

```
Switch# copy running-config startup-config
```

La nueva contraseña es ahora la configuración inicial.

Nota Este procedimiento puede dejar la interfaz virtual del switch en estado desactivado. Puede ver qué interfaz se encuentra en este estado ingresando el comando EXEC privilegiado **show running-config**. Para volver a habilitar la interfaz, ingrese el comando de configuración global **interface vlan** *vlan-id* y especifique el ID de la VLAN de la interfaz desactivada. Con el switch en modo de configuración de interfaz, ingrese el comando **no shutdown**.

Paso 10 Debe volver a configurar el switch. Si el administrador de sistema tiene a su disposición las copias de respaldo del switch y de los archivos de configuración de VLAN, debe utilizarlas.

Práctica de laboratorio 3.5.1: Configuración básica de VLAN (Versión para el instructor)

Diagrama de topología

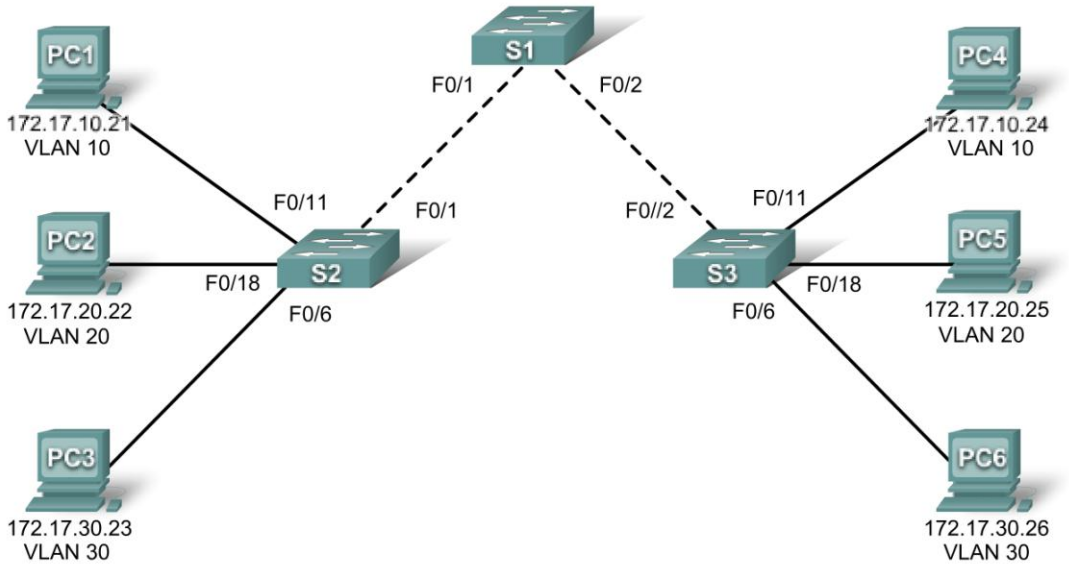


Tabla de direccionamiento

Dispositivo Nombre de host	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 iniciales de puertos (Switches 2 y 3)

Puertos	Asignación	Red
Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN 99 nativa)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30: Guest (predeterminada)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10: Cuerpo docente/personal	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20: Estudiantes	172.17.20.0 /24

Objetivos de aprendizaje

Al completar esta práctica de laboratorio podrá:

- Cablear una red según el diagrama de topología
- Borrar la configuración inicial y volver a cargar un switch al estado predeterminado
- Realizar las tareas de configuración básicas en un switch
- Crear las VLAN
- Asignar puertos de switch a una VLAN
- Agregar, mover y cambiar puertos
- Verificar la configuración de la VLAN
- Habilitar el enlace troncal en conexiones entre switches
- Verificar la configuración de enlace troncal
- Guardar la configuración de la VLAN

Tarea 1: Preparar la red

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

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

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

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

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

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

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

Tarea 2: Realizar las configuraciones básicas del switch

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

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

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

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

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

Tarea 3: Configurar y activar las interfaces Ethernet

Paso 1: Configurar las PC.

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

Tarea 4: Configurar las VLAN en el switch

Paso 1: Crear las VLAN en el switch S1.

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

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

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

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

```
S1#show vlan brief

Nombre de la VLAN                Estado    Puertos
---- ------------------------------ --------- -------------------------------
1    default                        active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                              Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                              Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                              Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                              Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                              Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                              Gi0/2
```

```
10   faculty/staff                    active
20   students                         active
30   guest                            active
99   management                       active
```

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

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

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

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

Consulte la tabla para la asignación de puertos que se encuentra en la página 1. Los puertos se asignan a las VLAN en modo de configuración de interfaces, utilizando el comando **switchport access vlan** *vlan-id*. Puede asignar cada puerto en forma individual o se puede utilizar el comando **interface range** para simplificar la tarea, como se muestra en este ejemplo. Los comandos se muestran sólo para S3, pero S2 y S3 se deben configurar de manera similar. Guarde la configuración al terminar.

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

Paso 4: Determinar qué puertos se han agregado.

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

¿Qué puertos están asignados a la VLAN 10?
_____ Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17

Nota: El comando **show vlan id** *vlan-name* muestra el mismo resultado.

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

Paso 5: Asignar la VLAN de administración.

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

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

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

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

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

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

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

Los enlaces troncales son conexiones entre los switches que permiten a los mismos intercambiar información para todas las VLAN. De manera predeterminada, un puerto troncal pertenece a todas las VLAN, a diferencia del puerto de acceso que sólo puede pertenecer a una sola VLAN. Si el switch admite tanto el encapsulamiento de VLAN ISL como el de 802.1Q, los enlaces troncales deben especificar qué método utilizan. Debido a que el switch 2960 sólo admite el enlace troncal 802.1Q, no se especifica en esta práctica de laboratorio.

Se asigna una VLAN nativa a un puerto troncal 802.1Q. En la topología, la VLAN nativa es VLAN 99. Un enlace troncal 802.1Q admite tráfico de varias VLAN (tráfico etiquetado) así como el tráfico que no proviene de una VLAN (tráfico sin etiquetar). El puerto de enlace troncal 802.1Q coloca el tráfico sin etiquetar en la VLAN nativa. El tráfico sin etiquetar se genera con una computadora conectada a un puerto del switch que se configura con la VLAN nativa. Una de las especificaciones de IEEE 802 1Q para VLAN nativas es mantener la compatibilidad retrospectiva con el tráfico sin etiquetar común en los escenarios de LAN antiguas. A los fines de esta práctica de laboratorio, una VLAN nativa sirve como identificador común en lados opuestos de un enlace troncal. Es una optimización utilizar una VLAN que no sea VLAN 1 como VLAN nativa.

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

```
S1(config)#interface range fa0/1-5
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end

S2(config)# interface range fa0/1-5
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
S2(config-if-range)#end

S3(config)# interface range fa0/1-5
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown
S3(config-if-range)#end
```

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

```
S1#show interface trunk

Puerto      Modo         Estado de encapsulamiento    Vlan nativa
Fa0/1       on           802.1q         trunking      99
Fa0/2       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-4094
Fa0/2       1-4094

Port        VLAN permitidas y activas en el dominio de administración
Fa0/1       1,10,20,30,99
Fa0/2       1,10,20,30,99

Puerto      Vlan en estado de envío de spanning tree y no depuradas
Fa0/1       1,10,20,30,99
Fa0/2       1,10,20,30,99
```

Paso 7: Verificar que los switches se puedan comunicar.

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

```
S1#ping 172.17.99.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.12, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms
```

```
S1#ping 172.17.99.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.13, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Paso 8: Hacer ping a varios hosts desde la PC2.

Haga ping desde el host de PC2 al host de PC1 (172.17.10.21). ¿El intento de hacer ping fue exitoso? _____ no

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

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

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

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

Paso 9: Ubicar la PC1 en la misma VLAN que la PC2.

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

```
S2#configure terminal
Enter configuration commands, one per line. Finalice con CNTL/Z.
S2(config)#interface fastethernet 0/11
S2(config-if)#switchport access vlan 20
S2(config-if)#end
```

Haga ping desde el host PC2 al host PC1. ¿El intento de hacer ping fue exitoso? _____ no

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

Paso 10: Cambiar la drección IP y la red en PC1.

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

¿El intento de hacer ping fue exitoso? _____sí

¿Por qué fue exitoso?

_____

_____

Los hosts deben estar en la misma VLAN y en la misma subred para comunicarse directamente a través de switches.

Tarea 7: Documentar las configuraciones de los switches

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

Tarea 6: Limpieza

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

Configuraciones finales de switch

S1

```
hostname S1
!
enable secret class
no ip domain-lookup
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
```

```
interface FastEthernet0/5
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/6
 shutdown
!
<all remaining FastEthernet and GigabitEthernet interface are shutdown>
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan99
 ip address 172.17.99.11 255.255.255.0
 no ip route-cache
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 5 15
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
!
end
```

S2

```
hostname S2
!
enable secret class
no ip domain-lookup
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
```

```
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/6
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 30
 switchport mode access
 shutdown
!
interface FastEthernet0/8
 switchport access vlan 30
 switchport mode access
 shutdown
!
interface FastEthernet0/9
 switchport access vlan 30
 switchport mode access
 shutdown
!
interface FastEthernet0/10
 switchport access vlan 30
 switchport mode access
 shutdown
!
interface FastEthernet0/11
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 10
 switchport mode access
 shutdown
!
interface FastEthernet0/13
 switchport access vlan 10
 switchport mode access
 shutdown
!
interface FastEthernet0/14
 switchport access vlan 10
 switchport mode access
 shutdown
!
interface FastEthernet0/15
 switchport access vlan 10
 switchport mode access
 shutdown
!
interface FastEthernet0/16
 switchport access vlan 10
```

```
 switchport mode access
 shutdown
!
interface FastEthernet0/17
 switchport access vlan 10
 switchport mode access
 shutdown
!
interface FastEthernet0/18
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 20
 switchport mode access
 shutdown
!
interface FastEthernet0/20
 switchport access vlan 20
 switchport mode access
 shutdown
!
interface FastEthernet0/21
 switchport access vlan 20
 switchport mode access
 shutdown
!
interface FastEthernet0/22
 switchport access vlan 20
 switchport mode access
 shutdown
!
interface FastEthernet0/23
 switchport access vlan 20
 switchport mode access
 shutdown
!
interface FastEthernet0/24
 switchport access vlan 20
 switchport mode access
 shutdown
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
 shutdown
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan99
 ip address 172.17.99.12 255.255.255.0
 no ip route-cache
```

```
!
ip http server
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 5 15
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
!
!
end
```

S3

```
hostname S3
no ip domain-lookup
enable secret class
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/6
switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/7
```

```
 switchport access vlan 30
!
interface FastEthernet0/8
 switchport access vlan 30
!
interface FastEthernet0/9
 switchport access vlan 30
!
interface FastEthernet0/10
 switchport access vlan 30
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 10
!
interface FastEthernet0/13
 switchport access vlan 10
!
interface FastEthernet0/14
 switchport access vlan 10
!
interface FastEthernet0/15
 switchport access vlan 10
!
interface FastEthernet0/16
 switchport access vlan 10
!
interface FastEthernet0/17
 switchport access vlan 10
!
interface FastEthernet0/18
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 20
!
interface FastEthernet0/20
 switchport access vlan 20
!
interface FastEthernet0/21
 switchport access vlan 20
!
interface FastEthernet0/22
 switchport access vlan 20
!
interface FastEthernet0/23
 switchport access vlan 20
!
interface FastEthernet0/24
 switchport access vlan 20
!
interface GigabitEthernet0/1
```

```
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan99
 ip address 172.17.99.13 255.255.255.0
 no ip route-cache
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Práctica de laboratorio 3.5.2: Desafío de configuración de VLAN (Versión para el instructor)

Diagrama de topología

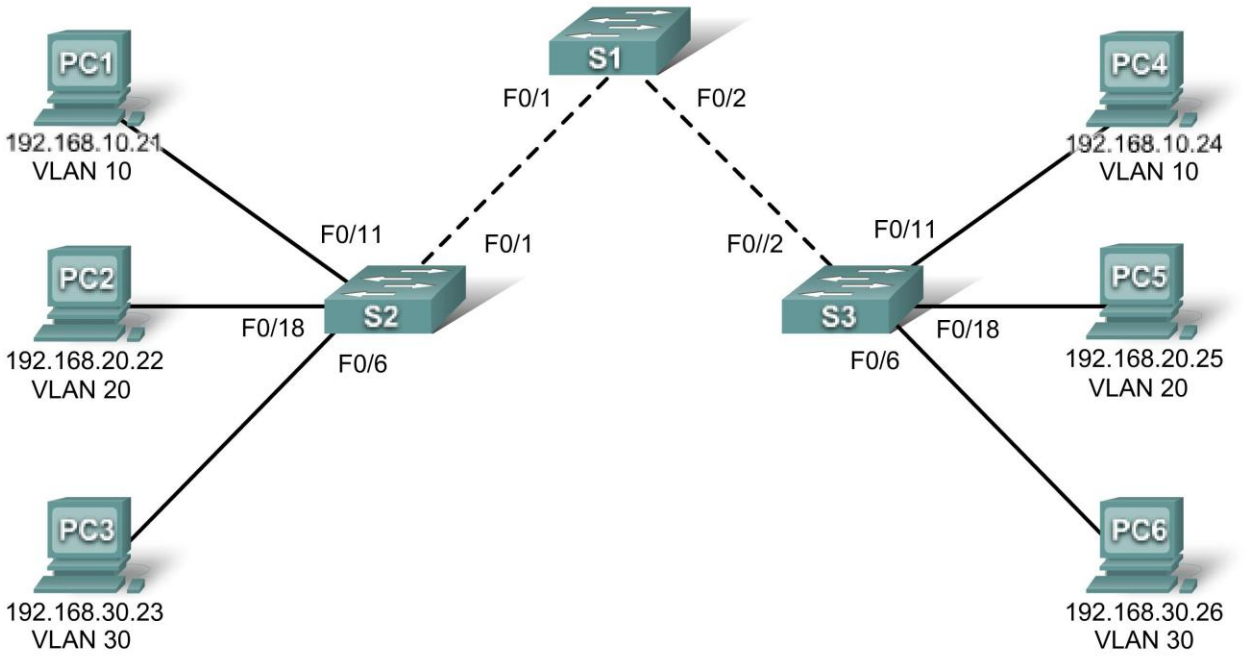


Tabla de direccionamiento

Dispositivo Nombre de host	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**	192.168.30.23	255.255.255.0	192.168.30.1
PC4	**NIC**	192.168.10.24	255.255.255.0	192.168.10.1
PC5	**NIC**	192.168.20.25	255.255.255.0	192.168.20.1
PC6	**NIC**	192.168.30.26	255.255.255.0	192.168.30.1

Asignaciones iniciales de puertos (Switches 2 y 3)

Puertos	Asignación	Red
Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN 56 nativa)	192.168.56.0 /24
Fa0/6 – 0/10	VLAN 30: Guest (predeterminada)	192.168.30.0 /24
Fa0/11 – 0/17	VLAN 10: Cuerpo docente/personal	192.168.10.0 /24
Fa0/18 – 0/24	VLAN 20: Estudiantes	192.168.20.0 /24

Objetivos de aprendizaje

Al completar esta práctica de laboratorio podrá:

- Cablear una red según el diagrama de topología
- Borrar la configuración inicial y volver a cargar un switch al estado predeterminado
- Realizar las tareas de configuración básicas en un switch
- Crear las VLAN
- Asignar puertos de switch a una VLAN
- Agregar, mover y cambiar puertos
- Verificar la configuración de la VLAN
- Habilitar el enlace troncal en conexiones entre switches
- Verificar la configuración de enlace troncal
- Guardar la configuración de la VLAN

Tarea 1: Preparar la red

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

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

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

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

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

Tarea 2: Realizar las configuraciones básicas del switch

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

- Configure el nombre de host del switch.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de modo EXEC: **clase**.

- Configure la contraseña **cisco** para las conexiones de consola.
- Configure la contraseña **cisco** para las conexiones de vty.

```
enable
configure terminal
no ip domain-lookup
enable secret cisco
!
line con 0
 password cisco
 login
!
line vty 0 4
password cisco
login
end
copy running-config starting-config
```

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

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

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

Tarea 3: Configurar y activar las interfaces Ethernet

Paso 1: Configurar las PC.

Configure las interfaces Ethernet de las seis PC con las direcciones IP y las gateways predeterminadas desde la tabla de direccionamiento al comienzo de la práctica de laboratorio.

Tarea 4: Configurar las VLAN en el switch

Paso 1: Crear las VLAN en el switch S1.

```
S1(config)#vlan 56
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
```

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

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

```
S1#show vlan brief

Nombre de VLAN                         Estado    Puertos
---- --------------------------------- --------- -------------------------------
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
56   management                        active
```

Paso 3: Configurar, asignar un nombre y verificar las VLAN en los switches S2 y S3.

Cree y asigne un nombre para las VLAN 10, 20, 30 y 56 en S2 y S3 mediante los comandos del Paso 1. Verifique la configuración correcta mediante el comando **show vlan brief**.

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

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

Paso 5: Determinar qué puertos se han añadido a la VLAN 10 en S2.

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

Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17

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

Una VLAN de administración es cualquier VLAN que se configura para acceder a las capacidades administrativas de un switch. La VLAN 1 funciona como VLAN de administración si no ha definido específicamente otra VLAN. Se asigna a la VLAN de administración una dirección IP y máscara de subred. Un switch puede administrarse mediante HTTP, Telnet, SSH o SNMP. Debido a que la configuración no convencional de un switch Cisco cuenta con la VLAN 1 como VLAN predeterminada, la misma es una mala elección como VLAN de administración. Usted no desea que un usuario arbitrario que se conecta a un switch acceda de manera predeterminada a la VLAN de administración. Recuerde que anteriormente, en esta misma práctica de laboratorio, configuró la VLAN 56 como VLAN de administración.

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

```
S1(config)#interface vlan 56
S1(config-if)#ip address 192.168.56.11 255.255.255.0
S1(config-if)#no shutdown

S2(config)#interface vlan 56
S2(config-if)#ip address 192.168.56.12 255.255.255.0
S2(config-if)#no shutdown

S3(config)#interface vlan 56
S3(config-if)#ip address 192.168.56.13 255.255.255.0
S3(config-if)#no shutdown
```

La asignación de una dirección de administración permite la comunicación IP entre switches y permite también que cualquier host conectado a un puerto asignado a la VLAN 56 se conecte a los switches. Debido a que la VLAN 56 se encuentra configurada como la VLAN de administración, cualquier puerto asignado a esta VLAN se considera puerto de administración y debe contar con seguridad para controlar qué dispositivos pueden conectarse a estos puertos.

Paso 7: Configurar los enlaces troncales y la VLAN nativa para los puertos de enlace troncales en los tres switches. Verificar que los enlaces troncales estén configurados.

Los enlaces troncales son conexiones entre los switches que permiten a los mismos intercambiar información para todas las VLAN. De manera predeterminada, un puerto troncal pertenece a todas las VLAN, a diferencia del puerto de acceso que sólo puede pertenecer a una sola VLAN. Si el switch admite tanto el encapsulamiento de VLAN ISL como el de 802.1Q, los enlaces troncales deben especificar qué método utilizan. Debido a que el switch 2960 sólo admite el enlace troncal 802.1Q, no se especifica en esta práctica de laboratorio.

Se asigna una VLAN nativa a un puerto troncal 802.1Q. En la topología, la VLAN nativa es VLAN 56. Un enlace troncal 802.1Q admite tráfico de varias VLAN (tráfico etiquetado) así como el tráfico que no proviene de una VLAN (tráfico sin etiquetar). El puerto de enlace troncal 802.1Q coloca el tráfico sin etiquetar en la VLAN nativa. El tráfico sin etiquetar se genera con una computadora conectada a un puerto del switch que se configura con la VLAN nativa. Las VLAN nativas se establecen en la especificación IEEE 802 1Q a fin de mantener la compatibilidad retrospectiva con el tráfico sin etiquetar común en los escenarios de la LAN antigua. A los fines de esta práctica de laboratorio, una VLAN nativa sirve como identificador común en lados opuestos de un enlace troncal. Es una optimización utilizar una VLAN que no sea VLAN 1 como VLAN nativa.

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

```
S1(config)#interface range fa0/1-5
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 56
S1(config-if-range)#no shutdown
S1(config-if-range)#end

S2(config)# interface range fa0/1-5
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 56
S2(config-if-range)#no shutdown
S2(config-if-range)#end

S3(config)#interface range fa0/1-5
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 56
S3(config-if-range)#no shutdown
S3(config-if-range)#end
```

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

```
S1#show interface trunk

Puerto      Modo         Estado de encapsulamiento    Vlan nativa
Fa0/1       on           802.1q         trunking      56
Fa0/2       on           802.1q         trunking      56

Port        Vlans allowed on trunk
Fa0/1       1-4094
Fa0/2       1-4094

Port        VLAN permitidas y activas en el dominio de administración
Fa0/1       1,10,20,30,56
Fa0/2       1,10,20,30,56

Puerto      Vlan en estado de envío de spanning tree y no depuradas
Fa0/1       1,10,20,30,56
Fa0/2       1,10,20,30,56
```

Paso 8: Verificar que S1, S2 y S3 se pueden comunicar.

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

```
S1#ping 192.168.56.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.56.12, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms
```

```
S1#ping 192.168.56.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.56.13, 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 la PC2. ¿Cuál es el resultado?

Haga ping desde el host de PC2 a la PC1 (192.168.10.21). ¿El ping es exitoso? No.

Haga ping desde el host PC2 a la dirección IP de la VLAN 56 del switch 192.168.56.12. ¿El ping es exitoso? No.

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

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

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

Paso 10: Ubicar la PC1 en la misma VLAN que la PC2. ¿PC1 puede hacer ping satisfactoriamente a PC2?

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

```
S2#configure terminal
Ingrese los comandos de configuración, uno por línea. End with CNTL/Z.
S2(config)#interface fastethernet 0/11
```

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

Haga ping desde el host PC2 al host PC1. ¿Los intentos de hacer ping fueron exitosos? No.

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

Paso 11: Asignar 192.168.20.22 como dirección IP de PC1. ¿PC1 puede hacer ping satisfactoriamente a PC2?

Asigne 192.168.20.22 como dirección IP de PC1. La máscara de subred y la gateway predeterminada pueden seguir siendo las mismas. Una vez más, haga ping desde el host PC2 al host PC1 utilizando la dirección IP recién asignada. ¿El intento de hacer ping fue exitoso? Sí.

¿Por qué fue exitoso?

Los hosts que se encuentran en la misma VLAN y en la misma subred pueden comunicarse directamente a través de los switches.

Tarea 5: Documentar las configuraciones de los switches

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

Switch 1

```
hostname S1
no ip domain-lookup
enable secret class
!
interface FastEthernet0/1
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/6
 shutdown
!
!<output ommitted - remaining ports on S1 are shutdown>
!
interface Vlan1
```

```
 no ip address
 no ip route-cache
!
interface Vlan56
 ip address 192.168.56.11 255.255.255.0
 no shutdown
!
line con 0
 logging synchronous
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end
```

Switch 2

```
hostname S2
no ip domain-lookup
enable secret class
!
interface FastEthernet0/1
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/6
switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 30
```

```
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 20
```

```
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan56
 ip address 192.168.56.12 255.255.255.0
 no shutdown
!
line con 0
 logging synchronous
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Switch 3

```
hostname S3
no ip domain-lookup
enable secret class
!
interface FastEthernet0/1
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk native vlan 56
```

```
 switchport mode trunk
!
interface FastEthernet0/6
switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 10
switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 20
```

```
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan56
 ip address 192.168.56.13 255.255.255.0
 no ip route-cache
!
line con 0
 logging synchronous
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Tarea 6: Limpieza

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

Práctica de laboratorio 3.5.3: Resolución de problemas de las configuraciones de VLAN (Versión para el instructor)

Diagrama de topología

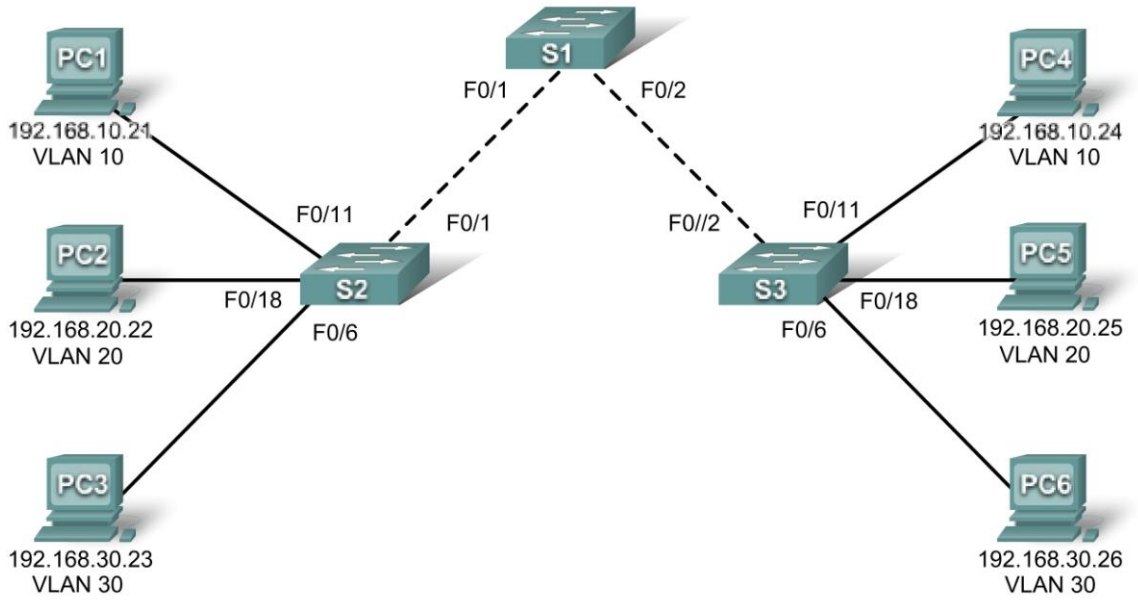


Tabla de direccionamiento

Dispositivo Nombre de host	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**	192.168.30.23	255.255.255.0	192.168.30.1
PC4	**NIC**	192.168.10.24	255.255.255.0	192.168.10.1
PC5	**NIC**	192.168.20.25	255.255.255.0	192.168.20.1
PC6	**NIC**	192.168.30.26	255.255.255.0	192.168.30.1

Asignaciones iniciales de puertos (Switches 2 y 3)

Puertos	Asignación	Red
Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN 56 nativa)	192.168.56.0 /24
Fa0/6 – 0/10	VLAN 30: Guest (predeterminada)	192.168.30.0 /24
Fa0/11 – 0/17	VLAN 10: Cuerpo docente/personal	192.168.10.0 /24
Fa0/18 – 0/24	VLAN 20: Estudiantes	192.168.20.0 /24

Objetivos de aprendizaje

Practicar las capacidades básicas para diagnosticar fallas en VLAN.

Escenario

En esta práctica de laboratorio practicará el diagnóstico de fallas en un entorno de VLAN mal configurada. Cargue o pida a su instructor que cargue las siguientes configuraciones en su equipo de práctica de laboratorio. Su objetivo es localizar y corregir todos los errores en las configuraciones y establecer una conectividad de extremo a extremo. Su configuración final debe coincidir con el diagrama de topología y la tabla de direccionamiento. Todas las contraseñas se establecen como **cisco**, excepto la contraseña de enable secret que se configura como **class**.

Tarea 1: Preparar la red

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

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

Paso 3: Importar las siguientes configuraciones.

Switch 1

```
hostname S1
no ip domain-lookup
enable secret class
!
vlan 10,20,30,56
Es un error habitual olvidar crear las VLAN en todos los switches,
especialmente en un swutch donde no hay puertos en esa VLAN. El comando
show vlan revela este problema.
!
interface range FastEthernet0/1-5
 switchport trunk native vlan 56
 Olvidar este comando provoca la falta de coincidencia de la VLAN nativa.
Se debe haber producido un error en el switch. Esto evita que los datos de
la VLAN 56 pasen adecuadamente desde un switch al otro.
 switchport mode trunk
!
interface range FastEthernet0/6-24
 shutdown
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan56
 ip address 192.168.56.11 255.255.255.0
 no ip route-cache
!
line con 0
 logging synchronous
line vty 0 4
 no login
line vty 5 15
 password cisco
 login
```

```
!
end
```

Switch 2

```
hostname S2
no ip domain-lookup
enable secret class
!
vlan 10,20,30,56
!
interface FastEthernet0/1-5
 switchport trunk native vlan 56
 switchport mode access
 switchport mode trunk
 Configurar erróneamente por accidente estos puertos como puertos de acceso
puede provocar algunas conductas interesantes. El puerto se convierte en
puerto de acceso en VLAN 1 (predeterminada). Esto combinado con que la VLAN
nativa en el enlace troncal es 56, da como resultado que el tráfico en la
VLAN 56 se envíe a la VLAN 1. El comando show interfaces trunk revela este
hecho.
!
interface range FastEthernet0/6-10
 switchport access vlan 30
 switchport mode access
!
interface range FastEthernet0/11-17
 switchport access vlan 10
 switchport mode access
!
interface range FastEthernet0/18-24
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.56.12 255.255.255.0
 no ip address
 La VLAN predeterminada se configuró como VLAN de administración. Se puede
acceder a esta dirección si no se corrige el error cometido en los enlaces
troncales. Esto no es correcto.
 no ip route-cache
 shutdown
!
interface Vlan56
 ip address 192.168.56.12 255.255.255.0
!
La VLAN de administración correcta no se configuró y la dirección IP se puso
en la VLAN predeterminada. El comando show ip interface brief lo revela.
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
```

```
line vty 5 15
 password cisco
 login
!
end
```

Switch 3

```
hostname S3
no ip domain-lookup
enable secret cisco
!
vlan 10,20,30
vlan 56
No se configuró la VLAN de administración. Es un error común asumir que
la VLAN existe si se ha configurado el SVI para esa VLAN.
!
interface range FastEthernet0/1-5
 switchport trunk native vlan 56
 switchport mode trunk
!
interface range FastEthernet0/6-10
 switchport access vlan 30
 switchport mode access
!
interface range FastEthernet0/11-17
 switchport access vlan 10
 switchport mode access
!
interface range FastEthernet0/18-24
 switchport access vlan 20
 switchport mode access
!
Los puertos no se colocaron en sus respectivas VLAN. Esto es evidente porque
todos los hosts conectados a este switch pueden alcanzar a los otros debido
a que todos se encuentran en la VLAN predeterminada. Esto se puede ver
mediante el comando show vlan.
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan56
 ip address 192.168.56.13 255.255.255.0
No se puede llegar a este dispositivo mediante la VLAN de administración sin
una dirección IP. La falta de este comando es evidente a través de un comando
show ip interface brief.
 no ip route-cache
!
line con 0
 password cisco
 login
line vty 0 4
```

```
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Tarea 2: Realizar un diagnóstico de fallas y reparar la configuración de la VLAN

Tarea 3: Documentar las configuraciones de los switches

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

Switch 1

```
hostname S1
no ip domain-lookup
enable secret cisco
!
vlan 10,20,30,56
!
interface FastEthernet0/1
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/6
 shutdown
!
!<output omitted - remaining ports on S1 are shutdown>
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan56
 ip address 192.168.56.11 255.255.255.0
 no ip route-cache
!
line con 0
```

```
 logging synchronous
line vty 0 4
 no login
line vty 5 15
 password cisco
 login
!
end
```

Switch 2

```
hostname S2
no ip domain-lookup
enable secret cisco
!
vlan 10,20,30,56
!
interface FastEthernet0/1
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/6
switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/11
```

```
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet0/1
!
```

```
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan56
 ip address 192.168.56.12 255.255.255.0
 no shutdown
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Switch 3

```
hostname S3
no ip domain-lookup
enable secret class
!
vlan 10,20,30,56
!
interface FastEthernet0/1
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk native vlan 56
 switchport mode trunk
!
interface FastEthernet0/6
 switchport access vlan 30
 switchport mode access
 !
interface FastEthernet0/7
 switchport access vlan 30
 switchport mode access
```

```
!
interface FastEthernet0/8
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 20
 switchport mode access
!
```

```
interface FastEthernet0/22
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan56
 ip address 192.168.56.13 255.255.255.0
 no ip route-cache
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Tarea 4: Limpieza

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

Práctica de laboratorio 4.4.1: Configuración básica del VTP (Versión para el instructor)

Diagrama de topología

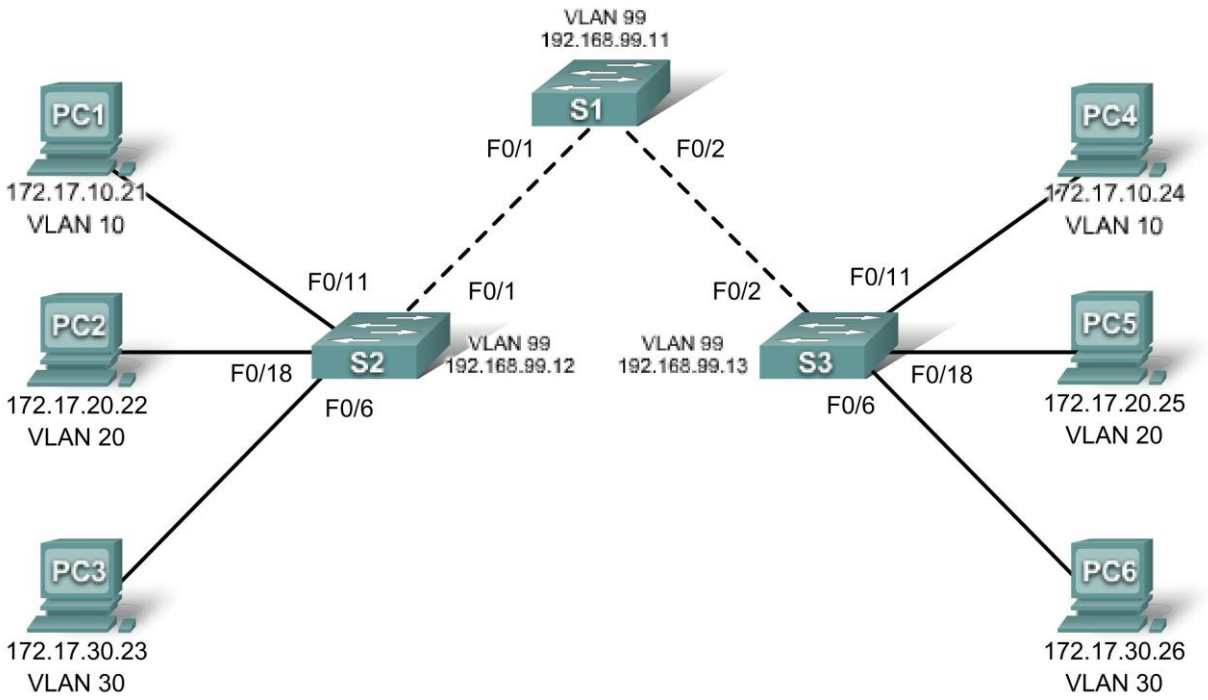


Tabla de direccionamiento

Dispositivo Nombre de host	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 (Switches 2 y 3)

Puertos	Asignación	Red
Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN 99 nativa)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30: Guest (predeterminada)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10: Cuerpo docente/personal	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20: Estudiantes	172.17.20.0 /24

Objetivos de aprendizaje

Al completar esta práctica de laboratorio podrá:

- Cablear una red según el diagrama de topología
- Borrar la configuración inicial y volver a cargar un switch al estado predeterminado
- Realizar las tareas de configuración básicas en un switch
- Configurar las VLAN y el protocolo VLAN Trunking (VTP) en todos los switches
- Habilitar el enlace troncal en conexiones entre switches
- Verificar la configuración de enlace troncal
- Modificar los modos VTP y observar el impacto.
- Crear las VLAN en el servidor VTP y distribuir la información de estas VLAN a los switches en la red.
- Explicar las diferencias en operación entre el modo VTP transparente, el modo servidor y el modo cliente.
- Asignar puertos de switch a las VLAN.
- Guardar la configuración de la VLAN
- Permitir depuraciones de VTP en la red
- Explicar de qué modo la depuración reduce el tráfico de broadcast innecesario en la LAN.

Tarea 1: Preparar la red

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

Puede utilizar cualquier switch actual en su práctica de laboratorio siempre y cuando éste tenga las interfaces necesarias que se muestran en la topología. El resultado que se muestra en esta práctica de laboratorio está basado en los switches 2960. El uso de cualquier otro tipo de switch puede producir resultados distintos. Si va a usar switches más antiguos, algunos comandos pueden ser diferentes o no estar disponibles.

Observe en la Tabla de direccionamiento que las PC se han configurado con una dirección de IP predeterminada de la gateway. Ésta sería la dirección IP del router local que no se incluye en este escenario de práctica de laboratorio. La gateway predeterminada, el router sería necesario para las PC en diferentes VLAN para poder comunicarse. Esto se analiza más adelante, en otro capítulo.

Establezca conexiones de consola en los tres switches.

Paso 2: Borrar toda configuración existente en los switches.

De ser necesario, consulte la Práctica de laboratorio 2.5.1, Apéndice 1 para leer sobre el procedimiento para borrar las configuraciones del switch y las VLAN. Utilice el comando **show vlan** para verificar que solo existan VLAN predeterminadas y que todos los puertos se asignen a la VLAN 1.

```
S1#show vlan

Nombre de la VLAN                     Estado    Puertos
---- -------------------------------- --------- -------------------------------
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
```

Paso 3: Deshabilitar todos los puertos con el comando shutdown.

```
S1(config)#interface range fa0/1-24
S1(config-if-range)#shutdown
S1(config-if-range)#interface range gi0/1-2
S1(config-if-range)#shutdown
```

```
S2(config)#interface range fa0/1-24
S2(config-if-range)#shutdown
S2(config-if-range)#interface range gi0/1-2
S2(config-if-range)#shutdown
```

```
S3(config)#interface range fa0/1-24
S3(config-if-range)#shutdown
S3(config-if-range)#interface range gi0/1-2
S3(config-if-range)#shutdown
```

Paso 4: Volver a habilitar los puertos de usuario en S2 y S3.

Configure los puertos de usuario en modo de acceso. Consulte el diagrama de topología para determinar cuáles puertos están conectados a dispositivos de 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
```

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

Tarea 2: Realizar las configuraciones básicas del switch

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

- Configure el nombre de host del switch según lo indicado en la topología.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de modo EXEC: **class**.
- Configure la contraseña **cisco** para las conexiones de consola.
- Configure la contraseña **cisco** para las conexiones de vty.

(Se muestran los resultados para S1)

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. Finalice con 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: Configurado desde la consola por la consola
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Tarea 3: Configurar las interfaces Ethernet en las PC Host

Configure las interfaces Ethernet de PC1, PC2, PC3, PC4, PC5 y PC6 con las direcciones IP y las gateways predeterminadas indicadas en la tabla de direccionamiento al comienzo de la práctica de laboratorio.

Verifique que la PC1 pueda hacer ping a PC4; que la PC2 pueda hacer ping a la PC5 y que la PC3 pueda hacer ping a la PC6.

Tarea 4: Configurar VTP en los switches

VTP permite al administrador de redes controlar las instancias de las VLAN en la red creando dominios VTP. Dentro de cada dominio VTP se configuran uno o más switches con servidores VTP. Las VLAN se crean en el servidor VTP y se informan a los otros switches en el dominio. Las tareas comunes de configuración VTP son la configuración del modo operativo, del dominio y de la contraseña. En esta práctica de laboratorio se utilizará a S1 como el servidor VTP, con S2 y S3 configurados como clientes o en el modo transparente de VTP.

Paso 1: Verificar las configuraciones VTP actuales en los tres switches.

```
S1#show vtp status

VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Servidor
VTP Domain Name                 :
VTP Pruning Mode                : Deshabilitado
VTP V2 Mode                     : Deshabilitado
VTP Traps Generation            : Deshabilitado
MD5 digest                      : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
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 : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Servidor
VTP Domain Name                 :
VTP Pruning Mode                : Deshabilitado
VTP V2 Mode                     : Deshabilitado
VTP Traps Generation            : Deshabilitado
MD5 digest                      : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
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 : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Servidor
VTP Domain Name                 :
VTP Pruning Mode                : Deshabilitado
VTP V2 Mode                     : Deshabilitado
VTP Traps Generation            : Deshabilitado
MD5 digest                      : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Observe que los tres switches se encuentran en modo servidor. El modo servidor es el modo VTP predeterminado para la mayoría de los switches Catalyst.

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

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

```
S1(config)#vtp mode server
Modo dispositivo ya es SERVIDOR VTP.
S1(config)#vtp domain Lab4
Cambiar el nombre del dominio VTP de NULL a Lab4
S1(config)#vtp password cisco
Configurar la contraseña de la base de datos VLAN del dispositivo en cisco
S1(config)#end

S2(config)#vtp mode client
Configurar el dispositivo en modo CLIENTE VTP
S2(config)#vtp domain Lab4
Cambiar el nombre del dominio VTP de NULL a Lab4
S2(config)#vtp password cisco
Configurar la contraseña de la base de datos VLAN del dispositivo en cisco
S2(config)#end

S3(config)#vtp mode transparent
Configurar el dispositivo en modo TRANPARENT VTP.
S3(config)#vtp domain Lab4
Cambiar el nombre del dominio VTP de NULL a Lab4
S3(config)#vtp password cisco
Configurar la contraseña de la base de datos VLAN del dispositivo en cisco
S3(config)#end
```

Nota: El nombre del dominio VTP puede ser aprendido por un switch de cliente desde un switch de servidor pero solamente si el dominio del switch de cliente se encuentra en estado nulo. No puede aprender un nombre nuevo si un nombre fue establecido anteriormente. Por esta razón, es una buena práctica configurar el nombre de dominio manualmente en todos los switches para asegurar que el nombre del dominio sea configurado correctamente. Los switches en diferentes dominios VTP no intercambian información de VLAN.

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

Simplifique esta tarea con el comando **interface range** en el modo de configuración global.

```
S1(config)#interface range fa0/1-5
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end

S2(config)# interface range fa0/1-5
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
S2(config-if-range)#end

S3(config)# interface range fa0/1-5
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown
S3(config-if-range)#end
```

Paso 4: Configurar la seguridad de Puerto en los switches de capa de acceso S2 y S3.

Configure los puertos fa0/6, fa0/11 y fa0/18 de modo tal que sólo permitan un solo host y aprendan la dirección MAC del host de manera dinámica.

```
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 5: Configurar las VLAN en el servidor VTP.

Hay cuatro VLAN adicionales que se requieren en esta práctica de laboratorio:

- VLAN 99 (administración)
- VLAN 10 (cuerpo docente/personal)
- VLAN 20 (estudiantes)
- VLAN 30 (guest)

Configúrelas en el servidor VTP.

```
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 se hayan creado las VLAN en S1 con el comando **show vlan brief**.

Paso 6: Verificar que las VLAN creadas en S1 se hayan distribuido a S2 y S3.

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

```
S2#show vlan brief

Nombre de VLAN                         Estado    Puerto
---- --------------------------------- --------- -------------------------------
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

Nombre de la VLAN                      Estado    Puertos
---- --------------------------------- --------- -------------------------------
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                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

¿Están configuradas las mismas VLAN en todos los switches? _____ no

Explique por qué S2 y S3 tienen diferentes configuraciones de VLAN en este momento. _____

_____

_____

S2 está en modo cliente y acepta configuraciones de VLAN publicadas por un servidor VTP. S3 está en modo VTP transparente, así que envía publicaciones VTP pero no implementa las VLAN publicadas localmente.

Paso 7: Crear una nueva VLAN en switches 2 y 3.

```
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 le permite crear una nueva VLAN en S2 pero sí en S3? _____

_____

Las VLAN sólo pueden crearse en switches en modo servidor VTP o modo transparente.

Borre la VLAN 88 de S3.

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

Paso 8: Configurar las VLAN en forma manual.

Configure las cuatro VLAN identificadas en el Paso 5 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
```

Aquí se aprecia una de las ventajas del VTP. La configuración manual es tediosa y puede suscitar errores y cualquier error introducido aquí puede evitar la comunicación entre VLAN. Además, puede resultar difícil diagnosticar este tipo de errores.

Paso 9: 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 todos los switches estén correctamente configurados haciendo ping entre ellos. Desde S1, haga ping a la interfaz de administración en S2 y S3. Desde S2, haga ping a la interfaz de administración en S3.

¿Los pings son exitosos? _____sí

En caso contrario, realice el diagnóstico de fallas de las configuraciones de los switches e inténtelo nuevamente.

Paso 10: Asignar puertos de switch a las VLAN.

Consulte la tabla de asignación de puertos al principio de la práctica de laboratorio para asignar puertos a las VLAN. Simplifique esta tarea con el comando **interface range**. Las asignaciones de puertos no se configuran a través del VTP. Las asignaciones de puerto deben ser configurado en cada switch manualmente o dinámicamente utilizando un servidor VMPS. Los comandos se muestran para S3 solamente, pero los switches S2 y S1 deben ser configurados de manera similar. Cuando termine, guarde la configuración.

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

Tarea 5: Configurar la depuración VTP en los switches

La depuración VTP permite a un servidor VTP suprimir tráfico de broadcast IP para VLAN específicas a switches que no tienen ningún puerto en esa VLAN. De manera predeterminada, todos los multicasts y broadcasts en una VLAN se saturan en toda la VLAN. Todos los switches en la red reciben todos los broadcasts, incluso en situaciones en las que unos pocos usuarios están conectados a esa VLAN. La depuración del VTP se utiliza para eliminar o depurar este tráfico innecesario. La depuración ahorra banda ancha LAN porque los broadcasts no tienen que ser enviados a los switches que no los necesitan.

La depuración se configura en el switch del servidor mediante el comando **vtp pruning** en modo de configuración global. La configuración se pulsa a los switches de clientes. Sin embargo, puesto que S3 está en modo transparente, la depuración de VTP debe configurarse localmente en ese switch.

Confirme la configuración de depuración VTP en cada switch utilizando el commando **show vtp status**. El modo de depuración VTP debe estar activado en cada switch.

```
S1#show vtp status
VTP Version                     : 2
Configuration Revision          : 17
Maximum VLANs supported locally : 255
Number of existing VLANs        : 9
VTP Operating Mode              : Servidor
VTP Domain Name                 : Lab4
VTP Pruning Mode                : Habilitado
<resultado omitido>
```

Tarea 6: Limpieza

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

Configuraciones finales

Observe que las configuraciones de S2 y S3 son idénticas, a excepción de la dirección IP asignada a la VLAN de administración (VLAN 99). La configuración del VTP no se guarda en el archivo de configuración. Se guarda en el archivo vlan.dat en la memoria flash.

Configuración de S1

```
hostname S1
enable secret class
no ip domain-lookup
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/6
shutdown
!
<output omitted: FastEthernet 0/7 through 0/24 are the same as FastEthernet
0/6>
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 ip address 172.17.99.11 255.255.255.0
 no shutdown
!
line con 0
 password cisco
 login
line vty 0
 no login
```

```
line vty 1 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

```
S1#show vtp status
VTP Version                     : 2
Configuration Revision          : 17
Maximum VLANs supported locally : 255
Number of existing VLANs        : 9
VTP Operating Mode              : Servidor
VTP Domain Name                 : Lab4
VTP Pruning Mode                : Habilitado
VTP V2 Mode                     : Deshabilitado
VTP Traps Generation            : Deshabilitado
MD5 digest                      : 0xD4 0x02 0x75 0x41 0x70 0x62 0x36 0x3A
Configuration last modified by 172.17.10.11 at 3-1-93 17:52:49
Local updater ID is 172.17.10.11 on interface Vl10 (lowest numbered VLAN
interface found)
```

Configuración de S2

```
hostname S2
enable secret class
no ip domain-lookup
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/6
 switchport access vlan 30
 switchport mode access
 switchport port-security
```

```
 switchport port-security mac-address sticky
!
interface FastEthernet0/7
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/8
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/9
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/10
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/12
 switchport access vlan 10
 shutdown
!
interface FastEthernet0/13
 switchport access vlan 10
 shutdown
!
interface FastEthernet0/14
 switchport access vlan 10
 shutdown
!
interface FastEthernet0/15
 switchport access vlan 10
 shutdown
!
interface FastEthernet0/16
 switchport access vlan 10
 shutdown
!
interface FastEthernet0/17
 switchport access vlan 10
 shutdown
!
interface FastEthernet0/18
 switchport access vlan 20
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/19
 switchport access vlan 20
 shutdown
```

```
!
interface FastEthernet0/20
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/21
switchport access vlan 20
 shutdown
!
interface FastEthernet0/22
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/23
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/24
 switchport access vlan 20
 shutdown
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
 switchport mode trunk
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan99
 ip address 172.17.99.12 255.255.255.0
 no shutdown
!
ip http server
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco

login login
login
line vty 5 15
 password cisco
```

Configuración de S3

```
hostname S3
enable secret class
no ip domain-lookup
```

```
!
vtp domain Lab4
vtp mode transparent
!
vlan 10
 name faculty/staff
!
vlan 20
 name students
!
vlan 30
 name guest
!
vlan 99
 name management
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/6
 switchport access vlan 30
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/7
 switchport access vlan 30
!
interface FastEthernet0/8
 switchport access vlan 30
!
interface FastEthernet0/9
 switchport access vlan 30
!
interface FastEthernet0/10
 switchport access vlan 30
!
interface FastEthernet0/11
 switchport access vlan 20
```

```
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/12
 switchport access vlan 20
!
interface FastEthernet0/13
 switchport access vlan 20
!
interface FastEthernet0/14
 switchport access vlan 20
!
interface FastEthernet0/15
 switchport access vlan 20
!
interface FastEthernet0/16
 switchport access vlan 20
!
interface FastEthernet0/17
 switchport access vlan 20
!
interface FastEthernet0/18
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky

interface FastEthernet0/19
 switchport access vlan 10
!
interface FastEthernet0/20
 switchport access vlan 10
!
interface FastEthernet0/21
 switchport access vlan 10
!
interface FastEthernet0/22
 switchport access vlan 10
!
interface FastEthernet0/23
 switchport access vlan 10
!
interface FastEthernet0/24
 switchport access vlan 10
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan99
```

```
 ip address 172.17.99.13 255.255.255.0
 no shutdown
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
end
```

Práctica de laboratorio 4.4.2 Desafío de configurar un VTP (Versión para el instructor)

Topología

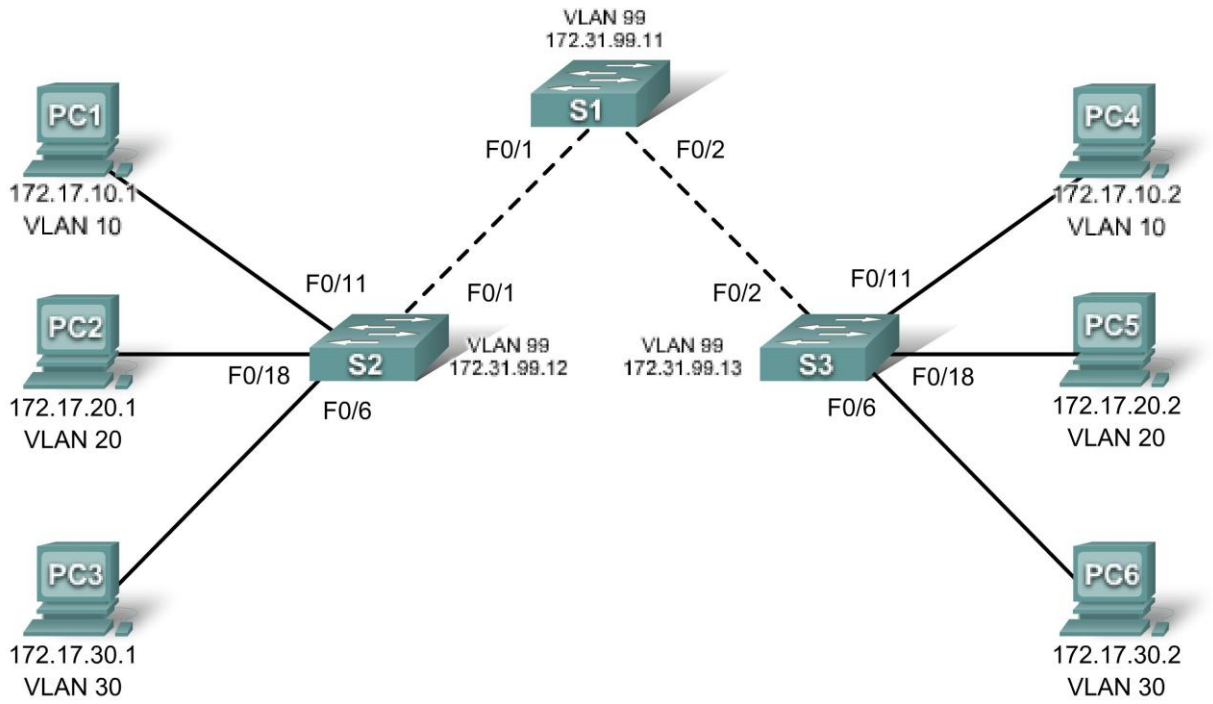


Tabla de direccionamiento

Dispositivo Nombre de host	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
S1	**VLAN 99**	172.31.99.11	255.255.255.0	No aplicable
S2	**VLAN 99**	172.31.99.12	255.255.255.0	No aplicable
S3	**VLAN 99**	172.31.99.13	255.255.255.0	No aplicable
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 (Switches 2 y 3)

Puertos	Asignación	Red
Fa0/1 – 0/5	Enlaces troncales 802.1q	
Fa0/11 – 0/17	VLAN 10: Engineering	172.31.10.0 /24
Fa0/18 – 0/24	VLAN 20: Sales	172.31.20.0 /24
Fa0/6 – 0/10	VLAN 30: Administration	172.31.30.0 /24
Ninguno	VLAN 99: Administración de redes	172.31.99.0 /24

Objetivos de aprendizaje

Al completar esta práctica de laboratorio podrá:

- Cablear una red según el diagrama de topología.
- Borrar la configuración inicial y volver a cargar un switch al estado predeterminado.
- Realizar tareas de configuración básicas en un switch.
- Configurar las VLAN y el protocolo VLAN Trunking (VTP) en todos los switches.
- Habilitar el enlace troncal en conexiones entre switches.
- Verificar la configuración de enlace troncal.
- Modificar los modos VTP y observar el impacto.
- Crear las VLAN en el servidor VTP y distribuir la información de estas VLAN a los switches en la red.
- Explicar las diferencias en operación entre el modo VTP transparente, el modo servidor y el modo cliente.
- Asignar puertos de switch a las VLAN.
- Guardar la configuración de la VLAN.

Tarea 1: Preparar la red

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

Puede utilizar cualquier switch actual en su práctica de laboratorio siempre y cuando éste tenga las interfaces necesarias que se muestran en el diagrama de topología. El resultado que se muestra en esta práctica de laboratorio está basado en los switches 2960. El uso de cualquier otro tipo de switch puede producir resultados distintos. Si va a usar switches más antiguos, algunos comandos pueden ser diferentes o no estar disponibles.

Establezca conexiones de consola en los tres switches.

Paso 2: Borrar toda configuración existente en los switches.

Borre las configuraciones existentes, las VLAN, y vuelva a cargar el switch. Utilice el comando **show vlan** para verificar que solo existan VLAN predeterminadas y que todos los puertos se asignen a la VLAN 1.

```
S1#show vlan

Nombre de la VLAN                      Estado    Puertos
---- --------------------------------- --------- -------------------------------
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
```

Paso 3: Deshabilitar todos los puertos con el comando shutdown.

```
S1(config)#interface range fa0/1-24
S1(config-if-range)#shutdown
S1(config-if-range)#interface range gi0/1-2
S1(config-if-range)#shutdown

S2(config)#interface range fa0/1-24
S1(config-if-range)#shutdown
S2(config-if-range)#interface range gi0/1-2
S1(config-if-range)#shutdown

S3(config)#interface range fa0/1-24
S3(config-if-range)#shutdown
S3(config-if-range)#interface range gi0/1-2
S3(config-if-range)#shutdown
```

Paso 4: Rehabilitar los puertos de usuario en S2 y S3 y poner esos puertos en modo de acceso. Consulte el diagrama de topología para determinar cuáles puertos están conectados a dispositivos de 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

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

Tarea 2: Realizar las configuraciones básicas del switch.

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

- Configure el nombre de host del switch según lo indicado en la topología.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de modo EXEC: **class**.
- Configure la contraseña **cisco** para las conexiones de consola.
- Configure la contraseña **cisco** para las conexiones de vty.

Se muestran los resultados para S1

```
Switch>enable
Switch#configure terminal
Ingrese los comandos de configuración, uno por línea. Finalice con 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: Configurado desde la consola por la consola
S1#copy running-config startup-config
Destination filename [startup-config]?
Creando la configuración...
[OK]
```

Tarea 3: Configurar las interfaces Ethernet en las PC Host

Configure las interfaces Ethernet de PC1 a PC6 con las direcciones IP según la tabla de direccionamiento al comienzo de la práctica de laboratorio.

Tarea 4: Configurar VTP en los switches

VTP permite al administrador de redes controlar las instancias de las VLAN en la red creando dominios VTP. Dentro de cada dominio VTP se configuran uno o más switches con servidores VTP. Las VLAN se crean en el servidor VTP y se pulsan a los otros switches en el dominio. Las tareas comunes de configuración VTP son el modo operativo, el dominio y la contraseña. En esta práctica de laboratorio configurará S1 como servidor VTP, con S2 y S3 configurados como clientes VTP.

Paso 1: Verificar las configuraciones VTP actuales en los tres switches.

```
S1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Servidor
VTP Domain Name                 :
VTP Pruning Mode                : Deshabilitado
VTP V2 Mode                     : Deshabilitado
VTP Traps Generation            : Deshabilitado
MD5 digest                      : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
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 : 255
Number of existing VLANs        : 5
```

```
VTP Operating Mode              : Servidor
VTP Domain Name                 :
VTP Pruning Mode                : Deshabilitado
VTP V2 Mode                     : Deshabilitado
VTP Traps Generation            : Deshabilitado
MD5 digest                      : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
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 : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Servidor
VTP Domain Name                 :
VTP Pruning Mode                : Deshabilitado
VTP V2 Mode                     : Deshabilitado
VTP Traps Generation            : Deshabilitado
MD5 digest                      : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

¿Cuál es el modo operativo VTP (predeterminado) actual en los switches? _____Servidor

¿Cuál es la revisión de configuración en S1 y S2? _____ 0

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

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

```
S1(config)#vtp mode server
Modo dispositivo ya es SERVIDOR VTP.
S1(config)#vtp domain access
Cambiar el nombre del dominio VTP de NULL a access
S1(config)#vtp password lab4
Configurar la contraseña de la base de datos VLAN del dispositivo a lab4
S1(config)#end

S2(config)#vtp mode client
Configurar el dispositivo a modo CLIENTE VTP
S2(config)#vtp domain access
Cambiar el nombre del dominio VTP de NULL a access
S2(config)#vtp password lab4
Configurar la contraseña de la base de datos VLAN del dispositivo a lab4
S2(config)#end

S3(config)#vtp mode transparent
Configurar el dispositivo en modo TRANPARENT VTP.
S3(config)#vtp domain access
Cambiar el nombre del dominio VTP de NULL a access
S3(config)#vtp password lab4
Configurar la contraseña de la base de datos VLAN del dispositivo a lab4
S3(config)#end
```

Nota: El nombre del dominio VTP puede ser aprendido por un switch de cliente desde un switch de servidor pero solamente si el dominio del switch de cliente se encuentra en estado nulo. No puede aprender un nombre nuevo si un nombre fue establecido anteriormente. Por esta razón, es una buena práctica configurar el nombre de dominio manualmente en todos los switches para asegurar que el nombre del dominio sea configurado correctamente. Los switches en diferentes dominios VTP no intercambian información de VLAN. Recuerde que las contraseñas y los nombres de dominios VTP distinguen entre mayúsculas y minúsculas.

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

Configure los puertos Fa0/1 a Fa0/5 en modo de enlace troncal. Configure la VLAN 99 como la VLAN nativa para estos enlaces troncales. Simplifique esta tarea con el comando **interface-range**. No olvide habilitar las interfaces de enlace tronal.

```
S1(config)#interface range fa0/1-5
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end

S2(config)# interface range fa0/1-5
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
S2(config-if-range)#end

S3(config)# interface range fa0/1-5
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown
S3(config-if-range)#end
```

Paso 4: Configurar la seguridad de Puerto en los puertos de acceso S2 y S3.

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

```
S2(config)# interface fa0/6
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 2
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 2
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 2
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 2
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 2
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 2
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#end
```

Paso 5: Configurar las VLAN en el servidor VTP.

Hay cuatro VLAN requeridas en esta práctica de laboratorio:

1. VLAN 99: (Administración de redes)
2. VLAN 10: (engineering)
3. VLAN 20 (sales)
4. VLAN 30 (administración)

Configure estas VLAN en el servidor VTP.

```
S1(config)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#exit
S1(config)#vlan 10
S1(config-vlan)#name engineering
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name sales
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name administration
S1(config-vlan)#exit
```

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

Paso 6: Verificar que las VLAN creadas en S1 se hayan distribuido a S2 y S3.

Utilice el comando **show vlan brief** en S2 y S3 para determinar si el servidor VTP ha pulsado su configuración VLAN a todos estos switches.

```
S2#show vlan brief

Nombre de la VLAN                      Estado    Puertos
---- --------------------------------- --------- -------------------------------
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   engineering                        active
20   sales                              active
30   administration                     active
99   management                         active
```

```
S3#show vlan brief

Nombre de la VLAN                     Estado    Puertos
---- -------------------------------- --------- -------------------------------
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                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

¿Están configuradas las mismas VLAN en todos los switches? _____ no

Explique por qué S2 y S3 tienen diferentes configuraciones de VLAN en este momento. _____

_____

_____

S2 está en modo cliente y acepta configuraciones de VLAN publicadas por un servidor VTP. S3 está en modo VTP transparente, así que envía publicaciones VTP pero no implementa las VLAN publicadas localmente.

Paso 7: Configurar la dirección de la interfaz de administración en los tres switches según la tabla de direccionamiento al comienzo de la práctica de laboratorio.

Asigne estas direcciones a la VLAN de administración de red (VALN 99).

```
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 todos los switches estén correctamente configurados haciendo ping entre ellos. Desde S1, haga ping a la interfaz de administración en S2 y S3. Desde S2, haga ping a la interfaz de administración en S3.

¿Los pings son exitosos? _____sí
En caso contrario, realice el diagnóstico de fallas de las configuraciones de los switch y solucione.

Paso 8: Asignar puertos de switch a las VLAN.

Consulte la tabla de asignación de puertos al principio de la práctica de laboratorio para asignar puertos a las VLAN. Simplifique esta tarea con el comando **interface range**. Observe que las asignaciones de puertos no se configuran a través de VTP. Las asignaciones de puerto deben ser configurado en cada switch manualmente o dinámicamente utilizando un servidor VMPS. Los comandos se muestran para S3 solamente, pero los switches S2 y S1 deben ser configurados de manera similar. Cuando termine, guarde la configuración.

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

Paso 9: Verificar que los enlaces troncales estén operando correctamente.

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

¿Alguno de los pings es exitoso? _____ sí, los pings a PC4 fueron exitosos

¿Por qué algunos de los pings fallaron? _____

_____

Los hosts están en diferentes VLAN.

¿A qué hosts se pudo llegar desde la PC3? _____ PC6 solamente

Tarea 5: Configurar la depuración VTP en los switches

La depuración VTP permite a un servidor VTP suprimir tráfico de broadcast IP para VLAN específicas a switches que no tienen ningún puerto en esa VLAN. De manera predeterminada, todos los multicasts y broadcasts en una VLAN se saturan en toda la VLAN. Todos los switches en la red reciben todos los broadcasts, incluso en situaciones en las que unos pocos usuarios están conectados a esa VLAN. La depuración VTP elimina o depura este tráfico innecesario. La depuración ahorra banda ancha LAN porque los broadcasts no tienen que ser enviados a los switches que no los necesitan.

Configure depuración en el servidir de switches, que será pulsada a los switches de clientes. Sin embargo, puesto que S3 está en modo transparente, la depuración de VTP debe también configurarse localmente en ese switch.

Confirme la configuración de depuración VTP en cada switch utilizando el commando **show vtp status**. El modo de depuración VTP debe mostrar “habilitado” en cada switch.

```
S1#show vtp status
VTP Version                     : 2
Configuration Revision          : 17
Maximum VLANs supported locally : 255
Number of existing VLANs        : 9
VTP Operating Mode              : Servidor
VTP Domain Name                 : acceso
VTP Pruning Mode                : Habilitado
<resultado omitido>
```

Tarea 6: Limpieza

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

Configuraciones finales

Configuración de S1

```
hostname S1
enable secret class
no ip domain-lookup
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/6
shutdown
!
<output omitted: FastEthernet 0/7 through 0/24 are the same as FastEthernet
0/6>
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 ip address 172.17.99.11 255.255.255.0
 no shutdown
!
line con 0
 password cisco
 login
line vty 0
 no login
line vty 1 4
 password cisco
```

```
 login
line vty 5 15
 password cisco
 login
!
end
```

Configuración de S2

```
hostname S2
!
enable secret class
!
no ip domain-lookup
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/6
 switchport access vlan 30
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/7
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/8
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/9
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/10
```

```
 switchport access vlan 30
 shutdown
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
!
interface FastEthernet0/12
 switchport access vlan 10
 shutdown
!
interface FastEthernet0/13
 switchport access vlan 10
 shutdown
!
interface FastEthernet0/14
 switchport access vlan 10
 shutdown
!
interface FastEthernet0/15
 switchport access vlan 10
 shutdown
!
interface FastEthernet0/16
 switchport access vlan 10
 shutdown
!
interface FastEthernet0/17
 switchport access vlan 10
 shutdown
!
interface FastEthernet0/18
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
!
interface FastEthernet0/19
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/20
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/21
switchport access vlan 20
 shutdown
!
interface FastEthernet0/22
 switchport access vlan 20
 shutdown
```

```
!
interface FastEthernet0/23
 switchport access vlan 20
 shutdown
!
interface FastEthernet0/24
 switchport access vlan 20
 shutdown
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
 switchport mode trunk
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan99
 ip address 172.17.99.12 255.255.255.0
 no shutdown
!
ip http server
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
```

Configuración de S3

```
hostname S3
!
enable secret class
!
no ip domain-lookup
!
vtp domain access
vtp mode transparent
!
vlan 10
 name faculty/staff
!
vlan 20
 name students
!
vlan 30
 name guest
```

```
!
vlan 99
 name management
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
switchport trunk native vlan 99
switchport mode trunk
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
interface FastEthernet0/5
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/6
 switchport access vlan 30
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
!
interface FastEthernet0/7
 switchport access vlan 30
interface FastEthernet0/8
 switchport access vlan 30
interface FastEthernet0/9
 switchport access vlan 30
interface FastEthernet0/10
 switchport access vlan 30
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
!
interface FastEthernet0/12
 switchport access vlan 10
interface FastEthernet0/13
 switchport access vlan 10
interface FastEthernet0/14
 switchport access vlan 10
interface FastEthernet0/15
 switchport access vlan 10
interface FastEthernet0/16
 switchport access vlan 10
interface FastEthernet0/17
 switchport access vlan 10
```

```
!
interface FastEthernet0/18
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
!
interface FastEthernet0/19
 switchport access vlan 20
interface FastEthernet0/20
 switchport access vlan 20
interface FastEthernet0/21
 switchport access vlan 20
interface FastEthernet0/22
 switchport access vlan 20
interface FastEthernet0/23
 switchport access vlan 20
interface FastEthernet0/24
 switchport access vlan 20
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan99
 ip address 172.17.99.13 255.255.255.0
 no shutdown
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
end
```

Práctica de laboratorio 4.4.3: Configuración del VTP para solucionar problemas (Versión para el instructor)

Diagrama de topología

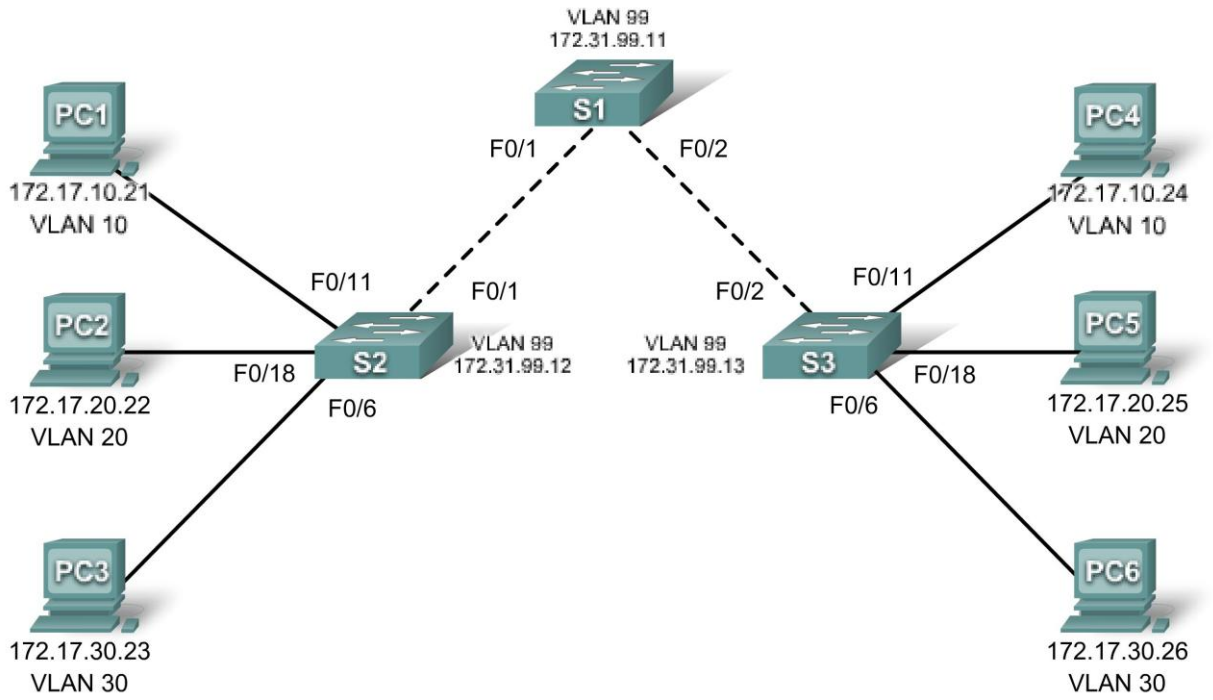


Tabla de direccionamiento

Dispositivo Nombre de host	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 (Switches 2 y 3)

Puertos	Asignación	Red
Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN 99 nativa)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30: Guest (predeterminada)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10: Cuerpo docente/personal	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20: Estudiantes	172.17.20.0 /24

Objetivos

Al completar esta práctica de laboratorio podrá:

- Cablear una red según el diagrama de topología
- Borrar la configuración de inicio y los archivos vlan.dat y volver a cargar un switch al estado predeterminado.
- Cargar los switches con las configuraciones provistas
- Encontrar y corregir todos los errores de configuración
- Documentar la red corregida

Escenario

El protocolo de enlace troncal de VLAN (VTP) ayuda a garantizar configuraciones VLAN uniformes en su red conmutada pero debe estar correctamente configurado. En esta práctica de laboratorio usará las configuraciones suministradas para configurar S1 como servidor VTP, y S2 y S3 como clientes VTP. El nombre de dominio VTP es Lab3_4 y la contraseña es cisco. Sin embargo, existe un número de errores en esta configuración que debe diagnosticar y corregir antes de que se restaure la conectividad extremo a extremo dentro de la VLAN.

Habrá resuelto satisfactoriamente todos los errores cuando las mismas VLAN estén configuradas en los tres switches, y pueda hacer ping entre dos hosts cualesquiera en la misma VLAN o entre dos switches cualesquiera.

Tarea 1: Preparar la red

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

Puede utilizar cualquier switch actual en su práctica de laboratorio siempre y cuando éste tenga las interfaces necesarias que se muestran en el diagrama de topología. El resultado que se muestra en esta práctica de laboratorio está basado en los switches 2960. El uso de cualquier otro tipo de switch puede producir resultados distintos. Si va a usar switches más antiguos, algunos comandos pueden ser diferentes o no estar disponibles.

Establezca conexiones de consola en los tres switches.

Paso 2: Borrar toda configuración existente en los switches.

Borre las configuraciones de switch y las VLAN en los tres switches y vuelva a cargarlos para restaurar el estado predeterminado. Utilice el comando **show vlan** para verificar que solo existan VLAN predeterminadas y que todos los puertos se asignen a la VLAN 1.

Paso 3: Configurar las interfaces Ethernet en las PC host.

Configurar las interfaces Ethernet de PC1, PC2, PC3, PC4, PC5 y PC6 con las direcciones IP indicadas en la tabla de direccionamiento al comienzo de la práctica de laboratorio. No hay necesidad de configurar las gateways predeterminadas para esta práctica de laboratorio.

Tarea 2: Cargar los switches con las configuraciones provistas

Configuración de S1

```
enable
!
config term
hostname S1
enable secret class
no ip domain-lookup
!
vtp mode server
vtp domain lab6_3
vtp password cisco
la contraseña debe ser cisco
!
vlan 99
name management
exit
!
vlan 10
name Faculty/Staff
exit
!
vlan 20
name Students
exit
!
vlan 30
name Guest
exit
!
interface FastEthernet0/1
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode access
! debe ser 'switchport mode trunk'
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode access
! debe ser 'switchport mode trunk'

interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk native vlan 99
 switchport mode trunk
!
interface range FastEthernet0/6-24
shutdown
```

```
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan99
 ip address 179.17.99.11 255.255.255.0
 ! debe ser 172.17.99.11 255.255.255.0
 no shutdown
!
line con 0
 logging synchronous
 password cisco
 login
line vty 0
 no login
line vty 1 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Configuración de S2

```
hostname S2
!
enable secret class
no ip domain-lookup
!
vtp mode client
vtp domain Lab4
! domain name debe ser Lab4_3
! establezca la contraseña vtp a cisco
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode access
modo debe ser enlace troncal
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode access
modo debe ser enlace troncal
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
```

```
!
interface FastEthernet0/5
 switchport trunk native vlan 99
 switchport mode trunk
!
interface range FastEthernet0/6 - 10
 switchport access vlan 10
! este rango debe asignarse a vlan 30
 switchport mode access
!
interface range FastEthernet0/11 - 17
 switchport access vlan 20
este rango debe asignarse a vlan 10
 switchport mode access
!
interface range FastEthernet0/18 - 24
 switchport access vlan 30
! este rango debe asignarse a vlan 20
 switchport mode access
!
interface Vlan99
 ip address 172.17.99.12 255.255.255.0
 no shutdown
!
ip http server
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
```

Configuración de S3

```
hostname S3
!
enable secret class
no ip domain-lookup
!
vtp mode client
vtp domain Lab4
! domain name debe ser Lab4_3
! establezca la contraseña vtp a cisco
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
```

```
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk native vlan 99
 switchport mode trunk
!
interface range FastEthernet0/6 - 10
 switchport access vlan 30
 switchport mode access
!
interface range FastEthernet0/11 - 17
 switchport access vlan 10
 switchport mode access
!
interface range FastEthernet0/18 - 24
 switchport access vlan 20
 switchport mode access
!
interface Vlan99
 ip address 172.17.99.12 255.255.255.0
dirección incorrecta: debe ser 172.17.99.13
 no shutdown
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
end
```

Tarea 3: Diagnosticar y corregir errores de VTP y de configuración

Cuando se hayan corregido todos los errores, debe poder hacer ping a PC4 desde PC1, a PC5 desde PC2 y a PC6 desde PC3. También debe poder hacer ping a las interfaces de administración en S2 y S3 desde S1.

Tarea 4: Documentar la configuración del switch

Cuando haya completado su diagnóstico de fallas, capture el resultado del comando **show run** y guárdelo en un archivo de texto para cada switch.

Tarea 5: Limpieza

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

Práctica de laboratorio 5.5.1: Protocolo spanning tree básico (Versión para el instructor)

Diagrama de topología

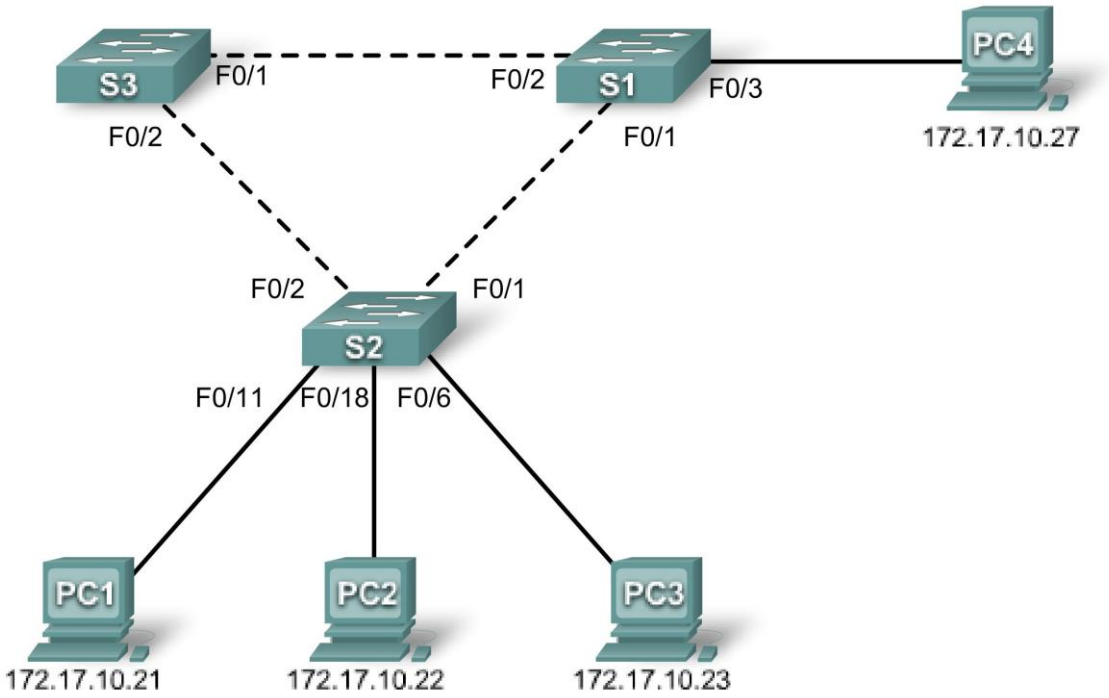


Tabla de direccionamiento

Dispositivo Nombre de host	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
S1	**VLAN 1**	172.17.10.1	255.255.255.0	No aplicable
S2	**VLAN 1**	172.17.10.2	255.255.255.0	No aplicable
S3	**VLAN 1**	172.17.10.3	255.255.255.0	No aplicable
PC1	**NIC**	172.17.10.21	255.255.255.0	172.17.10.254
PC2	**NIC**	172.17.10.22	255.255.255.0	172.17.10.254
PC3	**NIC**	172.17.10.23	255.255.255.0	172.17.10.254
PC4	**NIC**	172.17.10.27	255.255.255.0	172.17.10.254

Objetivos de aprendizaje

Al completar esta práctica de laboratorio podrá:

- Cablear una red según el diagrama de topología
- Borrar la configuración de inicio y volver a cargar la configuración predeterminada, configurando un switch al estado predeterminado
- Realizar las tareas de configuración básicas en un switch
- Observar y explicar el comportamiento predeterminado del Protocolo Spanning Tree (STP, 802.1D)
- Observar la respuesta a un cambio en la topología del spanning tree

Tarea 1: Realizar las configuraciones básicas del switch

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

Puede utilizar cualquier switch actual en su práctica de laboratorio siempre y cuando éste tenga las interfaces necesarias que se muestran en el diagrama de topología. El resultado que se muestra en esta práctica de laboratorio está basado en los switches 2960. El uso de cualquier otro modelo de switch puede producir resultados distintos.

Establezca conexiones de consola en los tres switches.

Paso 2: Borrar toda configuración existente en los switches.

Borre la NVRAM, borre el archivo vlan.dat y reinicie los switches. Consulte la Práctica de laboratorio para el procedimiento. Después de que la recarga se haya completado, utilice el comando privilegiado EXEC **show vlan** para verificar que sólo existan Vlan predeterminadas y que todos los puertos se asignen a VLAN 1.

```
S1#show vlan

Nombre de la VLAN                     Estado    Puertos
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Paso 3: Configurar los parámetros básicos del switch.

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

- Configure el nombre de host del switch.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de modo EXEC: **class**.

- Configure la contraseña **cisco** para las conexiones de consola.
- Configure la contraseña **cisco** para las conexiones de vty.

(Se muestran los resultados para S1)

```
Switch>enable
Switch#configure terminal
Ingrese los comandos de configuración, uno por línea. Finalice con 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: Configurado desde la consola por la consola
S1#copy running-config startup-config
Destination filename [startup-config]?
Creando la configuración...
[OK]
```

Tarea 2: Preparar la red

Paso 1: Deshabilitar todos los puertos con el comando shutdown.

Asegúrese de que los estados del puerto de switch estén inactivos con el comando **shutdown**. Simplifique esta tarea con el comando **interface range** .

```
S1(config)#interface range fa0/1-24
S1(config-if-range)#shutdown
S1(config-if-range)#interface range gi0/1-2
S1(config-if-range)#shutdown

S2(config)#interface range fa0/1-24
S2(config-if-range)#shutdown
S2(config-if-range)#interface range gi0/1-2
S2(config-if-range)#shutdown

S3(config)#interface range fa0/1-24
S3(config-if-range)#shutdown
S3(config-if-range)#interface range gi0/1-2
S3(config-if-range)#shutdown
```

Paso 2: **Volver a habilitar los puertos de usuario en S1 y S2 en modo de acceso**.

Consulte el diagrama de topología para determinar qué puertos de switch en S2 están activados para acceso por el dispositivo de usuario final. Estos tres puertos se configurarán para modo de acceso y se habilitarán con el comando **no shutdown**.

```
S1(config)#interface fa0/3
S1(config-if)#switchport mode access
S1(config-if)#no shutdown

S2(config)#interface range fa0/6, fa0/11, fa0/18
```

```
S2(config-if-range)#switchport mode access
S2(config-if-range)#no shutdown
```

Paso 3: Habilitar los puertos de enlace troncal en S1, S2 y S3

Usaremos solamente una VLAN en esta práctica de laboratorio; no obstante, se ha habilitado enlace troncal en todos los enlaces entre los switches para permitir que otras VLAN puedan agregarse en el futuro.

```
S1(config-if-range)#interface range fa0/1, fa0/2
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#no shutdown

S2(config-if-range)#interface range fa0/1, fa0/2
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#no shutdown

S3(config-if-range)#interface range fa0/1, fa0/2
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#no shutdown
```

Paso 4: Configurar la dirección de la interfaz de administración en los tres switches.

```
S1(config)#interface vlan1
S1(config-if)#ip address 172.17.10.1 255.255.255.0
S1(config-if)#no shutdown

S2(config)#interface vlan1
S2(config-if)#ip address 172.17.10.2 255.255.255.0
S2(config-if)#no shutdown

S3(config)#interface vlan1
S3(config-if)#ip address 172.17.10.3 255.255.255.0
S3(config-if)#no shutdown
```

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

¿Los pings son exitosos? _____sí

En caso contrario, realice el diagnóstico de fallas de las configuraciones de los switches e inténtelo nuevamente.

Tarea 3: Configurar las PC host

Configure las interfaces Ethernet de PC1, PC2 , PC3 y PC4 con la dirección IP, la máscara de subred y la gateway indicadas en la tabla de direccionamiento al comienzo de la práctica de laboratorio.

Tarea 4: Configurar Spanning Tree

Paso 1: Examinar la configuración predeterminada de 802.1D STP.

En cada switch, muestre la tabla de spanning tree con el comando **`show spanning-tree`**. La selección de la raíz varía según el BID de cada switch en su práctica de laboratorio, dando lugar a varios resultados.

```
S1#show spanning-tree


VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0019.068d.6980   Ésta es la dirección MAC del switch raíz

              Este puente es la raíz
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0019.068d.6980
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128,4    P2p
Fa0/3            Desg FWD 19        128,5    P2p

S2#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0019.068d.6980
              Cost        19
              Port        1 (FastEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     001b.0c68.2080
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128,2    P2p
Fa0/6            Desg FWD 19        128.6    P2p
Fa0/11           Desg FWD 19        128.11   P2p
Fa0/18           Desg FWD 19        128.18   P2p


S3#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0019.068d.6980
              Cost        19
              Port        1 (FastEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
  Bridge ID  Priority     32769  (priority 32768 sys-id-ext 1)
             Address      001b.5303.1700
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128,1    P2p
Fa0/2            Altn BLK 19        128.2    P2p
```

Paso 2: Examinar el resultado.

El identificador de Puente (bridge ID) almacenado en el BPDU de spanning tree consiste de la prioridad de puente, de la extensión de ID del sistema y de la dirección MAC. La combinación o adición de la prioridad de puente y la extensión de ID del sistema se conoce como ***bridge id priority*** (prioridad de id de puente). La extension de ID del sistema es siempre el número de la VLAN. Por ejemplo: la extensión de ID del sistema para la VLAN 100 es 100. Utilizando el valor predeterminado de la prioridad de puente de 32 768, la ***prioridad ID de puente*** para la VLAN 100 debe ser 32 868 (32 768 + 100).

El comando **show spanning-tree** muestra el valor de la ***prioridad ID de puente***. Nota: El valor de "prioridad" entre paréntesis representa el valor de prioridad de puente, que es seguido por el valor de la extensión de ID del sistema.

Responda las siguientes preguntas en base al resultado.

1. ¿Cuál es la prioridad ID de puente para los switches S1, S2 y S3 en VLAN 1?
   a. S1 _____32 769 (32 768 + 1)
   b. S2 _____32 769 (32 768 + 1)
   c. S3 _____32 769 (32 768 + 1)
2. ¿Qué switch es la raíz para el spanning tree de VLAN 1? _____S1 (puede variar)
3. En S1, ¿qué puertos del spanning tree están en estado de bloqueo en el switch raíz? _____ninguno
4. En S3, ¿qué puerto del spanning tree está en estado de bloqueo? _____ Fa0/2
5. ¿Cómo elige el STP el switch raíz? _____el ID de puente más bajo
6. Ya que las prioridades de puente son las mismas, ¿qué más usa el switch para determinar la raíz? _____dirección Mac del switch

Tarea 5: Observar la respuesta al cambio de topología en 802.1D STP

Observemos qué pasa cuando simulamos intencionalmente un enlace roto

Paso 1: Poner los switches en modo spanning tree debug utilizando el comando debug spanning-tree events

```
S1#debug spanning-tree events
Spanning Tree event debugging is on

S2#debug spanning-tree events
Spanning Tree event debugging is on

S3#debug spanning-tree events
Spanning Tree event debugging is on
```

Paso 2: Cerrar intencionalmente el puerto Fa0/1 en S1.

```
S1(config)#interface fa0/1
S1(config-if)#shutdown
```

Paso 3: Registrar el resultado de la depuración de S2 y S3

```
S2#
1w2d: STP: VLAN0001 we are the spanning tree root
S2#
1w2d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
1w2d: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
S2#
1w2d: STP: VLAN0001 heard root 32769-0019.068d.6980 on Fa0/2
1w2d:      supersedes 32769-001b.0c68.2080
1w2d: STP: VLAN0001 new root is 32769, 0019.068d.6980 on port Fa0/2, cost 38
1w2d: STP: VLAN0001 sent Topology Change Notice on Fa0/2

S3#
1w2d: STP: VLAN0001 heard root 32769-001b.0c68.2080 on Fa0/2
1w2d: STP: VLAN0001 Fa0/2 -> listening
S3#
1w2d: STP: VLAN0001 Topology Change rcvd on Fa0/2
1w2d: STP: VLAN0001 sent Topology Change Notice on Fa0/1
S3#
1w2d: STP: VLAN0001 Fa0/2 -> learning
S3#
1w2d: STP: VLAN0001 sent Topology Change Notice on Fa0/1
1w2d: STP: VLAN0001 Fa0/2 -> forwarding
```

Cuando el enlace de S2 que está conectado al switch raíz se desconecta, ¿cuál es la coclusión inicial acerca de la raíz del spanning tree)?_____ S2 cree que es la raíz del spanning tree: "we are the spanning tree root".

Una vez que S2 recibe la nueva información en Fa0/2, ¿qué nueva conclusión saca?_____

S2 reconoce una vez más a S1 como la raíz del spanning tree debido al bajo BID de S1.

El puerto Fa0/2 en S3 estaba previamente en estado de bloqueo antes de que el enlace entre S2 y S1 se desconectara. ¿Por qué estados pasa como resultado del cambio en la topología?
_____ escuchar, aprender, enviar

Paso 4: Examinar lo que ha cambiado en la topología del spanning tree utilizando el comando spanning tree

```
S2#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0019.068d.6980
              Cost        38
              Port        2 (FastEthernet0/2)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     001b.0c68.2080
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Root FWD 19        128.2    P2p
Fa0/6            Desg FWD 19        128,6    P2p
Fa0/11           Desg FWD 19        128,11   P2p
Fa0/18           Desg FWD 19        128.18   P2p


S3#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0019.068d.6980
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     001b.5303.1700
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128,2    P2p
```

Responda las siguientes preguntas en base al resultado.

1. ¿Qué ha cambiado en la manera en que S2 envía el tráfico? _____

Puesto que Fa0/1 está físicamente conectado a un puerto que está desconectado, el tráfico se envía y recibe en el puerto Fa0/2.

2. ¿Qué ha cambiado en la manera en que S3 envía el tráfico? _____

Antes Fa0/2 estaba en estado de bloqueo. Ahora está en estado de envío.

Tarea 6: Registrar la configuración de cada switch utilizando el comando show run

```
S1#show run
<resultado omitido>
!
hostname S1
!
!
interface FastEthernet0/1
 switchport mode trunk
!
```

```
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
 switchport mode access
!
! <resultado omitido>
!
interface Vlan1
 ip address 172.17.10.1 255.255.255.0
!
end
```

```
S2#show run
<resultado omitido>
!
hostname S2
!
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
!
! <resultado omitido>
!
interface FastEthernet0/6
 switchport mode access
!
interface FastEthernet0/11
 switchport mode access
!
interface FastEthernet0/18
 switchport mode access
!
!
interface Vlan1
 ip address 172.17.10.2 255.255.255.0
!
end
```

```
S3#show run
<resultado omitido>
!
hostname S3
!
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
!
```

```
!
! <resultado omitido>
!
interface Vlan1
 ip address 172.17.10.3 255.255.255.0
!
end
```

Tarea 7: Limpieza

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

Práctica de laboratorio 5.5.2: Desafío de laboratorio: protocolo spanning tree (Versión del instructor)

Diagrama de topología

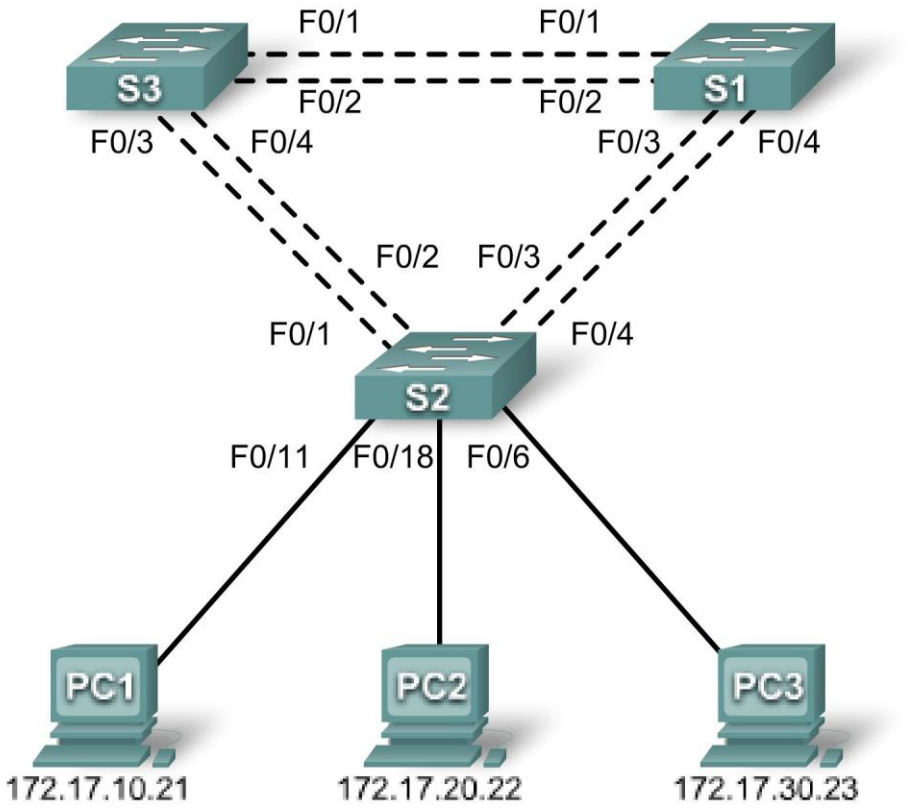


Tabla de direccionamiento

Dispositivo Nombre de host	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 puerto: Switch 2

Puertos	Asignación	Red
Fa0/1 – 0/4	Enlaces troncales 802.1q (VLAN 99 nativa)	172.17.99.0 /24
Fa0/5 – 0/10	VLAN 30: Guest (predeterminada)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10: Cuerpo docente/personal	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20: Estudiantes	172.17.20.0 /24

Objetivos de aprendizaje

Al completar esta práctica de laboratorio podrá:

- Cablear una red según el diagrama de topología
- Borrar la configuración de inicio y volver a cargar la configuración predeterminada, configurando un switch al estado predeterminado
- Realizar las tareas de configuración básicas en un switch
- Configurar las VLAN y el protocolo VLAN Trunking (VTP) en todos los switches
- Observar y explicar el comportamiento predeterminado del Protocolo Spanning Tree (STP, 802.1D)
- Modificar la ubicación de la raíz del spanning tree
- Observar la respuesta a un cambio en la topología del spanning tree
- Explicar las limitaciones de 802.1D STP para soportar la continuidad de servicio
- Configurar Rapid STP (802.1W)
- Observar y explicar las mejoras ofrecidas por Rapad STP

Tarea 1: Preparar la red

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

Puede utilizar cualquier switch actual en su práctica de laboratorio siempre y cuando éste tenga las interfaces necesarias que se muestran en el diagrama de topología. El resultado que se muestra en esta práctica de laboratorio está basado en los switches 2960. El uso de cualquier otro modelo de switch puede producir resultados distintos.

Establezca conexiones de consola en los tres switches.

Paso 2: Borrar toda configuración existente en los switches.

Borre la NVRAM, borre el archivo vlan.dat y reinicie los switches. Consulte la Práctica de laboratorio para el procedimiento. Después de que la recarga se haya completado, utilice el comando privilegiado EXEC **show vlan** para verificar que sólo existan Vlan predeterminadas y que todos los puertos se asignen a VLAN 1.

```
S1#show vlan

Nombre de la VLAN                     Estado   Puertos
---- -------------------------------- --------- -------------------------------
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
```

Paso 3: Deshabilitar todos los puertos con el comando shutdown.

Asegúrese de que los estados del puerto de switch estén inactivos con el comando **shutdown**. Simplifique esta tarea con el comando **interface range**.

```
S1(config)#interface range fa0/1-24
S1(config-if-range)#shutdown
S1(config-if-range)#interface range gi0/1-2
S1(config-if-range)#shutdown

S2(config)#interface range fa0/1-24
S2(config-if-range)#shutdown
S2(config-if-range)#interface range gi0/1-2
S2(config-if-range)#shutdown

S3(config)#interface range fa0/1-24
S3(config-if-range)#shutdown
S3(config-if-range)#interface range gi0/1-2
S3(config-if-range)#shutdown
```

Paso 4: Volver a habilitar los puertos de usuario en S2 en modo de acceso.

Consulte el diagrama de topología para determinar qué puertos de switch en S2 están activados para acceso por el dispositivo de usuario final. Estos tres puertos se configurarán para modo de acceso y se habilitarán con el comando **no shutdown**.

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

Tarea 2: Realizar las configuraciones básicas del switch

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

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

(Se muestran los resultados para S1)

```
Switch>enable
Switch#configure terminal
Ingrese los comandos de configuración, uno por línea. Finalice con 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: Configurado desde la consola por la consola
S1#copy running-config startup-config
Destination filename [startup-config]?
Creando la configuración...
[OK]
```

Tarea 3: Configurar las PC host

Configure las interfaces Ethernet de PC1, PC2 , y PC3 con la dirección IP, la máscara de subred y la gateway indicadas en la tabla de direccionamiento al comienzo de la práctica de laboratorio.

Tarea 4: Configurar las VLAN

Paso 1: Configurar VTP.

Configure VTP en los tres switches utilizando la siguiente tabla. Recuerde que las contraseñas y los nombres de dominios VTP distinguen entre mayúsculas y minúsculas. El modo operativo predeterminado es servidor.

Nombre del switch	Modo de operación VTF	Dominio del VTP	Contraseña de VTP
S1	**Servidor**	**Práctica de Lab5**	**cisco**
S2	**Cliente**	**Práctica de Lab5**	**cisco**
S3	**Cliente**	**Práctica de Lab5**	**cisco**

```
S1(config)#vtp mode server
Modo dispositivo ya es SERVIDOR VTP.
S1(config)#vtp domain Lab5
Cambiar el nombre del dominio VTP de NULL a Lab5
S1(config)#vtp password cisco
Configurar la contraseña de la base de datos VLAN del dispositivo en cisco
S1(config)#end

S2(config)#vtp mode client
Configurar el dispositivo a modo CLIENTE VTP
S2(config)#vtp domain Lab5
Cambiar el nombre del dominio VTP de NULL a Lab5
S2(config)#vtp password cisco
Configurar la contraseña de la base de datos VLAN del dispositivo en cisco
S2(config)#end

S3(config)#vtp mode client
Configurar el dispositivo a modo CLIENTE VTP
S3(config)#vtp domain Lab5
Cambiar el nombre del dominio VTP de NULL a Lab5
S3(config)#vtp password cisco
Configurar la contraseña de la base de datos VLAN del dispositivo en cisco
S3(config)#end
```

Paso 2: Configurar los enlaces troncales y la VLAN nativa

Configure los puertos troncales y la VLAN nativa. Para cada switch, configure los puertos de Fa0/1 a Fa0/4 como puertos de enlace troncal. Designe a VLAN 99 como la VLAN nativa para estos enlaces troncales. Simplifique esta tarea con el comando **interface range** en el modo de configuración global. Recuerde que estos puertos fueron deshabilitados en un paso anterior y deben rehabilitarse con el comando **no shutdown**.

```
S1(config)#interface range fa0/1-4
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end

S2(config)# interface range fa0/1-4
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
S2(config-if-range)#end

S3(config)# interface range fa0/1-4
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown
S3(config-if-range)#end
```

Paso 3: Configurar el servidor VTP con las VLAN.

VTP permite configurar las VLAN en el servidor VTP y poblar dichas VLAN en el VTP clientes en el dominio. Esto asegura la consistencia en la configuración de VLAN en toda la red.

Configure las siguientes VLAN en el servidor VTP:

VLAN	Nombre de la VLAN
VLAN 99	**administración**
VLAN 10	**cuerpo docente-personal**
VLAN 20	**estudiantes**
VLAN 30	**guest**

```
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
```

Paso 4: 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 clientes.

```
S2#show vlan brief

Nombre de la VLAN                     Estado    Puertos
---- -------------------------------- --------- -------------------------------
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

Nombre de la VLAN                     Estado   Puertos
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                Gi0/2
10   faculty/staff                     active
20   students                          active
30   guest                             active
99   management                        active
```

Paso 5: 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
S1(config-if)#no shutdown

S2(config)#interface vlan99
S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#no shutdown

S3(config)#interface vlan99
S3(config-if)#ip address 172.17.99.13 255.255.255.0
S3(config-if)#no shutdown
```

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

¿Los pings son exitosos? _____ sí

En caso contrario, realice el diagnóstico de fallas de las configuraciones de los switches e inténtelo nuevamente.

Paso 6: Asignar puertos de switch a las VLAN.

Asigne puertos a las VLAN en S2. Consulte la tabla de asignaciones de puerto al comienzo de la práctica de laboratorio.

```
S2(config)#interface range fa0/5-10
S2(config-if-range)#switchport access vlan 30
S2(config-if-range)#interface range fa0/11-17
S2(config-if-range)#switchport access vlan 10
S2(config-if-range)#interface range fa0/18-24
S2(config-if-range)#switchport access vlan 20
S2(config-if-range)#end
S2#copy running-config startup-config
Destination filename [startup-config]? [enter]
Creando la configuración...
[OK]
S2#
```

Tarea 5: Configurar Spanning Tree

Paso 1: Examinar la configuración predeterminada de 802.1D STP.

En cada switch, muestre la tabla de spanning tree con el comando **show spanning-tree**. El resultado se muestra para S1 solamente. La selección de la raíz varía según el BID de cada switch en su práctica de laboratorio.

```
S1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0019.068d.6980
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0019.068d.6980
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128,4    P2p
Fa0/3            Desg FWD 19        128,5    P2p
Fa0/4            Desg FWD 19        128,6    P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    32778
              Address     0019.068d.6980
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     0019.068d.6980
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128,4    P2p
Fa0/3            Desg FWD 19        128,5    P2p
Fa0/4            Desg FWD 19        128,6    P2p

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    32788
              Address     0019.068d.6980
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32788  (priority 32768 sys-id-ext 20)
              Address     0019.068d.6980
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128,4    P2p
Fa0/3            Desg FWD 19        128,5    P2p
Fa0/4            Desg FWD 19        128,6    P2p

VLAN0030
  Spanning tree enabled protocol ieee
  Root ID     Priority    32798
              Address     0019.068d.6980
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32798  (priority 32768 sys-id-ext 30)
              Address     0019.068d.6980
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128,4    P2p
Fa0/3            Desg FWD 19        128,5    P2p
Fa0/4            Desg FWD 19        128,6    P2p

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID     Priority    32867
              Address     0019.068d.6980
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32867  (priority 32768 sys-id-ext 99)
              Address     0019.068d.6980
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128,4    P2p
Fa0/3            Desg FWD 19        128,5    P2p
Fa0/4            Desg FWD 19        128,6    P2p
```

Observe que hay cinco instancias del spanning tree en cada switch. La configuración predeterminada del STP en los switches Cisco es Per-VLAN Spanning Tree (PVST+), que crea un spanning tree individual para cada VLAN (VLAN 1 y cualquier VLAN configurada a nivel de usuario).

Examine el spanning tree de VLAN 99 para los tres switches.

```
S1#show spanning-tree vlan 99 priority?

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID     Priority    32867
              Address     0019.068d.6980
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32867  (priority 32768 sys-id-ext 99)
              Address     0019.068d.6980
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128,4    P2p
Fa0/3            Desg FWD 19        128,5    P2p
Fa0/4            Desg FWD 19        128,6    P2p

S2#show spanning-tree vlan 99

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID     Priority    32867
              Address     0019.068d.6980  Ésta es la dirección MAC del switch raíz
(S1 en este caso)
              Cost        19
              Port        3 (FastEthernet0/3)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32867  (priority 32768 sys-id-ext 99)
              Address     001b.0c68.2080
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 15

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128,1    P2p
Fa0/2            Desg FWD 19        128,2    P2p
```

```
Fa0/3            Root FWD 19        128.3    P2p
Fa0/4            Altn BLK 19        128.4    P2p

S3#show spanning-tree vlan 99

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID     Priority    32867
              Address     0019.068d.6980
              Cost        19
              Port        1 (FastEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32867  (priority 32768 sys-id-ext 99)
              Address     001b.5303.1700
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128,1    P2p
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/3            Altn BLK 19        128,3    P2p
Fa0/4            Altn BLK 19        128,4    P2p
```

Ésta es la dirección MAC del switch raíz (S1 en este caso)

Paso 2: Examinar el resultado.

Responda las siguientes preguntas en base al resultado.

1. ¿Cuál es la prioridad ID de puente para los switches S1, S2 y S3 en VLAN 99?
   a. S1 _____32 867 (32 768 + 99)
   b. S2 _____32 867 (32 768 + 99)
   c. S3 _____32 867 (32 768 + 99)
2. ¿Cuál es la prioridad ID de puente para los switches S1, S2 y S3 en las VLAN 10, 20, 30 y 99?
   a. VLAN 10 _____ 32 778 (32 768 +10)
   b. VLAN 20_____32 788 (32 768 +20)
   c. VLAN 30_____32 798 (32 768 +30)
   d. VLAN 99_____32 867 (32 768 +99)
3. ¿Qué switch es la raíz para el spanning tree de VLAN 99? _____S1 (puede variar)
4. En la VLAN 99, ¿qué puertos del spanning tree están en estado de bloqueo en el switch raíz? _____ninguno
5. En la VLAN 99, ¿qué puertos del spanning tree están en estado de bloqueo en los switches que no son raíz? _____varía, pero usando configuraciones predeterminadas, un puerto bloquea en un switch que no es raíz y tres puertos bloquean en los otros switches que no son raíz.
6. ¿Cómo elige el STP el switch raíz? _____ID de puente más bajo
7. Ya que las prioridades de puente son las mismas, ¿qué más usa el switch para determinar la raíz? _____dirección Mac del switch

Tarea 6: Optimizar STP

Dado que hay una instancia separada de spanning tree para cada VLAN activa, se realiza una elección de raíz separada para cada instancia. Como hemos visto, si se usan las prioridades predeterminadas del switch en la selección de raíz, la misma raíz se elige para cada spanning tree. Esto podría llevar a un diseño inferior. Algunas de las razones para controlar la selección del switch raíz incluyen:

- El switch raíz es responsable de generar las BPDU en STP 802.1D y es el punto focal del control de tráfico de spanning tree. El switch raíz debe poder manejar esta carga de procesamiento adicional.
- La ubicación de la raíz define las rutas activas conmutadas en la red. La ubicación aleatoria posiblemente lleve a rutas que no sean las óptimas. Lo ideal es que la raíz se encuentre en la capa de distribución.
- Considere la topología empleada en esta práctica de laboratorio. De los seis enlaces troncales configurados, solamente dos transportan tráfico. Aunque esto evita los bucles, es una pérdida de recursos. Ya que la raíz puede definirse en base a la VLAN, puede haber algunos puertos que bloqueen una VLAN y que envíen a otra. Esto se demuestra debajo.

En este ejemplo, se ha determinado que la selección de raíz utilizando valores predeterminados ha llevado a la subutilización de los enlaces troncales disponibles del switch. Por lo tanto es necesario obligar a otro switch a que se transforme en el switch raíz para la VLAN 99 para imponer compartir algo de la carga en los enlaces troncales.

La selección del switch raíz se logra cambiando la prioridad del spanning tree para la VLAN. Dado que el switch raíz predeterminado puede variar en el entorno de su práctica de laboratorio, configuraremos S1 y S3 para que sean los switches raíz para las VLAN específicas. La prioridad predeterminada, como puede haber observado, es 32 768 más el ID de VLAN. El número más bajo indica una prioridad más alta para la selección de raíz. Establezca la prioridad para la VLAN 99 en S3 en 4096.

```
S3(config)#spanning-tree vlan 99 ?
  forward-time  Establece el retardo de envío para el spanning tree
  forward-time  Establece el intervalo de saludo para el spanning tree
  max-age       Establece el intervalo de antigüedad máxima para el spanning
tree
  priority      Establece la prioridad  de Puente para el spanning tree
  root          Configura el switch como raíz
  <cr>

S3(config)#spanning-tree vlan 99 ?
  <0-61440>  prioridad de Puente en incrementos de 4096

S3(config)#spanning-tree vlan 99 priority 4096
S3(config)#exit
```

Establece la prioridad para las VLAN 1, 10, 20 y 30 en S1 en 4096. Una vez más, el número más bajo indica una prioridad más alta para la selección de raíz.

```
S1(config)#spanning-tree vlan 1 priority 4096
S1(config)#spanning-tree vlan 10 priority 4096
S1(config)#spanning-tree vlan 20 priority 4096
S1(config)#spanning-tree vlan 30 priority 4096
S1(config)#exit
```

Dé un tiempo a los switches para recalcular el spanning tree y luego verifique el árbol para VLAN 99 en el switch S1 y el switch S3.

```
S1#show spanning-tree vlan 99

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID     Priority    4195
              Address     001b.5303.1700
              Cost        19
              Port        3 (FastEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32867  (priority 32768 sys-id-ext 99)
              Address     0019.068d.6980
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.3    P2p
Fa0/2            Altn BLK 19        128.4    P2p
Fa0/3            Desg FWD 19        128,5    P2p
Fa0/4            Desg FWD 19        128,6    P2p
```

Ahora ésta es la dirección MAC de S3 (el nuevo switch raíz)

```
S3#show spanning-tree vlan 99

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID     Priority    4195
              Address     001b.5303.1700
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4195  (priority 4096 sys-id-ext 99)
              Address     001b.5303.1700
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128,1    P2p
Fa0/2            Desg FWD 19        128,2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128,4    P2p
```

¿Qué switch es la raíz para VLAN 99? _____S3

En la VLAN 99, ¿qué puertos del spanning tree están en estado de bloqueo en el nuevo switch raíz? _____ninguno

En la VLAN 99, ¿qué puertos del spanning tree están en estado de bloqueo en el switch raíz antiguo? _____fa0/2 (puede variar)

Compare el spanning tree de la VLAN 99 de S3 arriba con el spanning tree de la VLAN 10 de S3.

```
S3#show spanning-tree vlan 10
```

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    4106
             Address     0019.068d.6980
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     001b.5303.1700
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128,1    P2p
Fa0/2            Altn BLK 19        128,2    P2p
Fa0/3            Altn BLK 19        128,3    P2p
Fa0/4            Altn BLK 19        128.4    P2p
```

Observe que S3 puede ahora usar los cuatro puertos para el tráfico de la VLAN 99 siempre y cuando no estén bloqueados al otro extremo del enlace troncal. No obstante, la topología original del spanning tree, con tres de cuatro puertos de S3 en el modo de bloqueo, todavía está instalada para las otras cuatro VLAN activas. Al configurar grupos de VLAN para usar diversos enlaces troncales como la ruta primaria de envío, mantenemos la redundancia de los enlaces troncales contra fallas, sin tener que dejar enlaces troncales totalmente sin usar.

Tarea 7: Observar la respuesta al cambio de topología en 802.1D STP

Para observar la continuidad a través de la LAN durante un cambio de topología, primero reconfigure PC3, que está conectada al puerto S2 Fa0/6, con la dirección IP 172.17.99.23 255.255.255.0. Luego reasigne el Puerto fa0/6 de S2 a la VLAN 99. Esto le permite hacer ping continuamente a través de la LAN desde el host.

```
S2(config)# interface fa0/6
S2(config-if)#switchport access vlan 99
```

Verifique que los switches puedan hacer ping al host.

```
S2#ping 172.17.99.23
Escriba escape sequence para abortar.

Sending 5, 100-byte ICMP Echos to 172.17.99.23, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1007 ms

S1#ping 172.17.99.23

Escriba escape sequence para abortar.
Sending 5, 100-byte ICMP Echos to 172.17.99.23, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1007 ms
```

Ponga S1 en modo debug de evento del spanning tree para monitorear los cambios durante el cambio de topología.

```
S1#debug spanning-tree events
Spanning Tree event debugging is on
```

Abra una ventana de comandos en PC3 y comience a hacer un ping continuo a la interfaz de administración de S1 con el comando **ping –t 172.17.99.11**. Ahora desconecte los enlaces troncales en S1 Fa0/1 y Fa0/3. Monitoree los pings. Comenzarán a expirar a medida que la conectividad en la LAN se interrumpa. Apenas la conectividad se haya restablecido, finalice los pings presionando Ctrl-C.

Debajo encontrará una versión abreviada del resultado de la depuración que verá en S1 (varios TCN están omitidos para mayor brevedad).

```
S1#debug spanning-tree events
Spanning Tree event debugging is on
S1#
6d08h: STP: VLAN0099 new root port Fa0/2, cost 19
6d08h: STP: VLAN0099 Fa0/2 -> listening
6d08h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
6d08h: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
6d08h: STP: VLAN0099 sent Topology Change Notice on Fa0/2
6d08h: STP: VLAN0030 Topology Change rcvd on Fa0/2
6d08h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to down
6d08h: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to down
6d08h: STP: VLAN0001 Topology Change rcvd on Fa0/4
6d08h: STP: VLAN0099 Fa0/2 -> learning
6d08h: STP: VLAN0099 sent Topology Change Notice on Fa0/2
6d08h: STP: VLAN0099 Fa0/2 -> forwarding
6d08h: STP: VLAN0001 Topology Change rcvd on Fa0/4
```

Recuerde que cuando los puertos están en modo escuchar y aprender, no están enviando tramas, y la LAN está esencialmente desactivada. El recálculo del spanning tree puede tomar hasta 50 segundos para completarse, una interrupción significativa en los servicios de red. El resultado de los ping continuos muestra el tiempo real de interrupción. En este caso fue de aproximadamente 30 segundos. Aunque el STP 802.1D impide la formación de bucles de conmutación, este largo tiempo de restauración es considerado una seria desventaja en las LAN de alta disponibilidad de la actualidad.

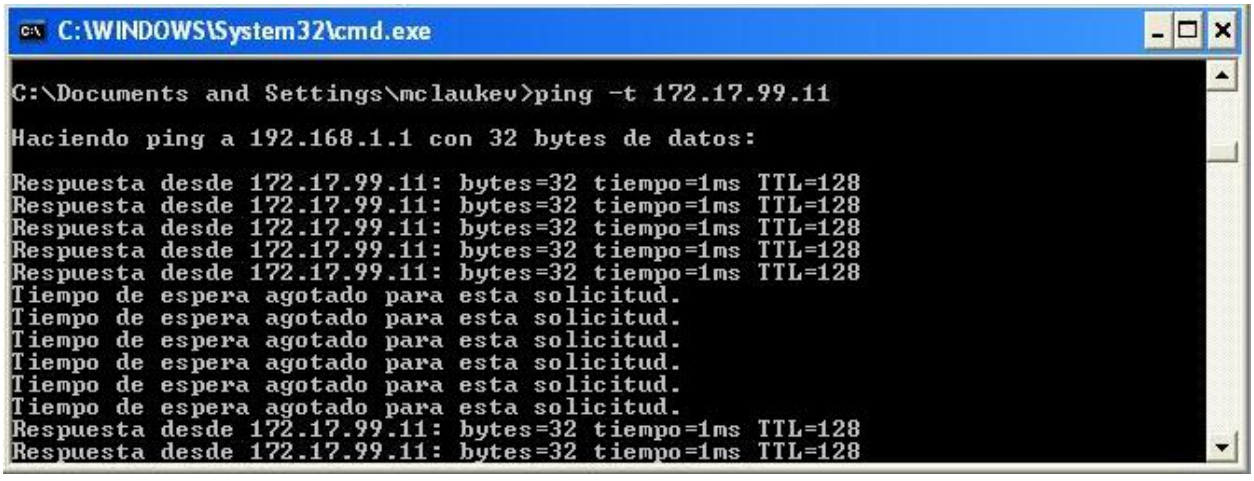


Figura 1. Estos pings muestran un lapso de 30 segundos en la conectividad mientras se recalcula el spanning tree.

Tarea 8: Configurar el protocolo Rapid Spanning Tree PVST

Cisco ha desarrollado varias opciones para tratar los tiempos lentos de convergencia asociados al STP estándar. PortFast, UplinkFast y BackboneFast son opciones que, cuando se configuran correctamente, pueden reducir drásticamente el tiempo requerido para restaurar la conectividad. Incorporar estas características requiere de configuración manual y se debe tener cuidado para hacerlo correctamente. La solución a largo plazo es Rapid STP (RSTP), 802.1w, que incorpora estas características, entre otras. RSTP-PVST está configurado como sigue:

```
S1(config)#spanning-tree mode rapid-pvst
```

Configure los tres switches de esta manera.

Use el comando **show spanning-tree summary** para verificar que RSTP esté habilitado..

Tarea 9: Observar el tiempo de convergencia de RSTP

Comience restaurando los enlaces troncales que desconectó en la Tarea 7, si es que aún no lo ha hecho (puertos Fa0/1 y Fa0/3 en S1). Luego siga estos pasos en la Tarea 7:

- Configure el host PC3 para que haga ping continuamente a toda la red.
- Habilite la depuración de eventos de spanning tree en el switch 1.
- Desconecte los cables a los puertos Fa0/1 y Fa0/3.
- Observe el tiempo requerido para restablecer un spanning tree estable.

A continuación se muestra el resultado parcial de depuración:

```
S1#debug spanning-tree events
Spanning Tree event debugging is on
S1#
6d10h: RSTP(99): updt rolesroot port Fa0/3 is going down
6d10h: RSTP(99): Fa0/2 is now root port Se ha restaurado la conectividad;
interrupción de menos de un segundo
6d10h: RSTP(99): syncing port Fa0/1
6d10h: RSTP(99): syncing port Fa0/4
6d10h: RSTP(99): transmitting a proposal on Fa0/1
6d10h: RSTP(99): transmitting a proposal on Fa0/4
6d10h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to down
6d10h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
```

El tiempo de restauración con RSTP habilitado fue menos de un segundo, y no se descartó ningún ping.

Tarea 10: Limpieza

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

Configuraciones finales

Switch S1

```
hostname S1
!
enable secret class
```

```
!
no ip domain-lookup
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 4096
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 4096
spanning-tree vlan 30 priority 4096
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 shutdown
!
interface FastEthernet0/7
 shutdown
!
(remaining port configuration ommitted - all non-used ports are shutdown)
!
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan1
 ip address 219,170,1000,1 255.255.255.0
 no ip route-cache
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Switch S2

```
hostname S2
!
enable secret class
!
no ip domain-lookup
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 switchport access vlan 30
!
interface FastEthernet0/6
 switchport access vlan 30
!
interface FastEthernet0/7
 switchport access vlan 30
!
interface FastEthernet0/8
 switchport access vlan 30
!
interface FastEthernet0/9
 switchport access vlan 30
!
interface FastEthernet0/10
 switchport access vlan 30
!
interface FastEthernet0/11
 switchport access vlan 10
!
interface FastEthernet0/12
 switchport access vlan 10
!
interface FastEthernet0/13
 switchport access vlan 10
!
interface FastEthernet0/14
 switchport access vlan 10
!
interface FastEthernet0/15
 switchport access vlan 10
```

```
!
interface FastEthernet0/16
 switchport access vlan 10
!
interface FastEthernet0/17
 switchport access vlan 10
!
interface FastEthernet0/18
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 20
!
interface FastEthernet0/20
switchport access vlan 20
!
interface FastEthernet0/21
 switchport access vlan 20
!
interface FastEthernet0/22
 switchport access vlan 20
!
interface FastEthernet0/23
 switchport access vlan 20
!
interface FastEthernet0/24
 switchport access vlan 20
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan1
 ip address 172.17.99.12 255.255.255.0
 no ip route-cache
!
line con 0
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Switch S3

```
hostname S3
!
enable secret class
```

```
!
no ip domain-lookup
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 99 priority 4096
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 shutdown
!
interface FastEthernet0/7
 shutdown
!
(remaining port configuration ommitted - all non-used ports are shutdown)
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan1
 ip address 172.17.99.13 255.255.255.0
 no ip route-cache
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Práctica de laboratorio 5.5.3: Resolución de problemas del protocolo spanning tree (Versión para el instructor)

Diagrama de topología

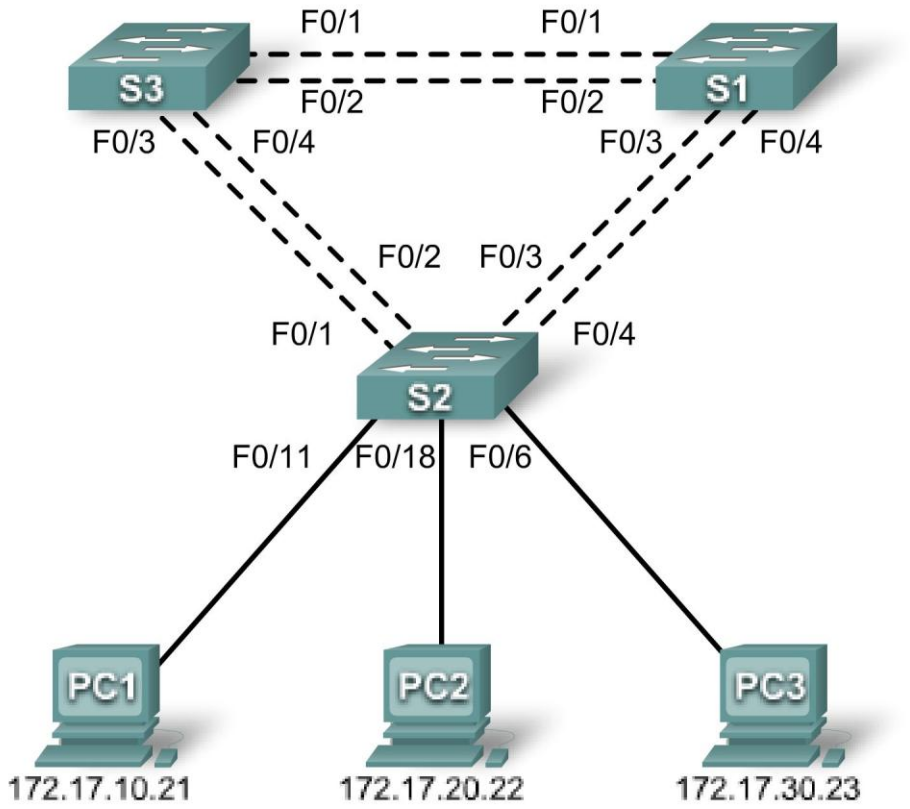


Tabla de direccionamiento

Dispositivo Nombre de host	Interfaz	Dirección IP	Máscara de subred	Gateway 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

Asignaciones de puerto: Switch 2

Puertos	Asignación	Red
Fa0/1 – 0/4	Enlaces troncales 802.1q (LAN 99 nativa)	172.17.99.0 /24
Fa0/5 – 0/10	VLAN 30: Guest (predeterminada)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10: Cuerpo docente/personal	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20: Estudiantes	172.17.20.0 /24

Objetivos de aprendizaje

Al completar esta práctica de laboratorio podrá:

- Analizar un problema de congestión en una red LAN redundante conmutada.
- Reconocer las capacidades para el equilibrio de cargas por VLAN con PVST.
- Modificar la configuración predeterminada de STP para optimizar el ancho de banda disponible.
- Verificar que las modificaciones hayan tenido el efecto deseado.

Escenario

Usted está encargado de la operación de la LAN redundante conmutada que se muestra en el diagrama de topología. Se ha observado una latencia creciente durante las horas pico de uso y el análisis apunta a los enlaces troncales congestionados. Puede reconocer que de los seis enlaces troncales configurados, sólo tres envían paquetes en la configuración predeterminada de STP que se ejecuta actualmente. La solución a este problema requiere un uso más efectivo de los enlaces troncales disponibles. La función PVST+ de los switches de Cisco proporciona la flexibilidad necesaria para distribuir el tráfico entre los switches mediante los seis enlaces troncales.

Esta práctica de laboratorio finaliza cuando todos los enlaces troncales conectados transporten tráfico y los tres switches participen en el balanceo de carga por VLAN para los tres usuarios.

Tarea 1: Preparar la red

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

Puede utilizar cualquier switch actual en su práctica de laboratorio siempre y cuando éste tenga las interfaces necesarias que se muestran en el diagrama de topología. El resultado que se muestra en esta práctica de laboratorio está basado en los switches Cisco 2960. El uso de cualquier otro modelo de switch puede producir resultados distintos.

Establezca conexiones de consola en los tres switches.

Paso 2: Borrar toda configuración existente en los switches.

Borre la NVRAM, borre el archivo vlan.dat y reinicie los switches.

Paso 3: Cargar los switches con la siguiente configuración:

Configuración de S1

```
hostname S1
enable secret class
no ip domain-lookup
!
vtp mode server
vtp domain Lab5
vtp password cisco
!
vlan 99
name Management
exit
!
vlan 10
name Faculty/Staff
exit
!
vlan 20
name Students
exit
!
vlan 30
name Guest
exit
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface range FastEthernet0/5-24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
```

```
shutdown
!
interface Vlan99
 ip address 172.17.99.11 255.255.255.0
 no shutdown
!
line con 0
 logging synchronous
 password cisco
 login
line vty 0
 no login
line vty 1 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Configuración de S2

```
hostname S2
!
enable secret class
no ip domain-lookup
!
vtp mode client
vtp domain Lab5
vtp password cisco
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface range FastEthernet0/5 - 10
 switchport access vlan 30
 switchport mode access
```

```
!
interface range FastEthernet0/11 - 17
 switchport access vlan 10
 switchport mode access
!
interface range FastEthernet0/18 - 24
 switchport access vlan 20
 switchport mode access
!
interface fa0/6
no shutdown
interface fa0/11
no shutdown
interface fa0/18
no shutdown
!
interface Vlan99
 ip address 172.17.99.12 255.255.255.0
 no shutdown
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
```

Configuración de S3

```
hostname S3
!
enable secret class
no ip domain-lookup
!
vtp mode client
vtp domain Lab5
vtp password cisco
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
```

```
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface range FastEthernet0/5 - 10
 switchport access vlan 30
 switchport mode access
!
interface range FastEthernet0/11 - 17
 switchport access vlan 10
 switchport mode access
!
interface range FastEthernet0/18 - 24
 switchport access vlan 20
 switchport mode access
!
interface Vlan99
 ip address 172.17.99.13 255.255.255.0
 no shutdown
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
end
```

Tarea 2: Configurar las PC host

Configure las interfaces Ethernet de PC1, PC2 y PC3 con la dirección IP, la máscara de subred y la gateway indicadas en la tabla de direccionamiento.

Tarea 3: Identificar el estado inicial de todos los enlaces troncales

En cada switch, muestre la tabla de spanning tree con el comando **show spanning-tree**. Observe qué puertos realizan envíos en cada switch e identifique qué enlaces troncales no se están utilizando en la configuración predeterminada. Puede utilizar su diseño de topología de red para documentar el estado inicial de todos los puertos de enlace troncal.

Tarea 4: Modificar spanning tree para lograr el equilibrio de cargas

Modifique la configuración de spanning tree de manera que los seis enlaces troncales estén en uso. Supongamos que las tres LAN de usuario (10, 20 y 30) transportan cantidades iguales de tráfico. Intente encontrar una solución que tenga un conjunto diferente de puertos que hagan envíos para cada una de las tres LAN de usuario. Como mínimo, cada una de las tres VLAN debe tener un switch distinto como raíz del spanning tree.

Tarea 5: Documentar la configuración del switch

Cuando haya completado su solución, capture el resultado del comando **show run** y guárdelo en un archivo de texto para cada switch.

Tarea 6: Limpieza

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

Solución

Hay diversas formas de lograr el equilibrio de cargas. Una de las más directas es la siguiente:

```
S1(config)#spanning-tree vlan 10 priority 4096
S1(config)#spanning-tree vlan 20 priority 16384

S2(config)#spanning-tree vlan 20 priority 4096
S2(config)#spanning-tree vlan 30 priority 16384

S3(config)#spanning-tree vlan 30 priority 4096
S3(config)#spanning-tree vlan 10 priority 16384
```

Práctica de laboratorio 6.4.1: Enrutamiento inter VLAN básico (Versión para el instructor)

Diagrama de topología

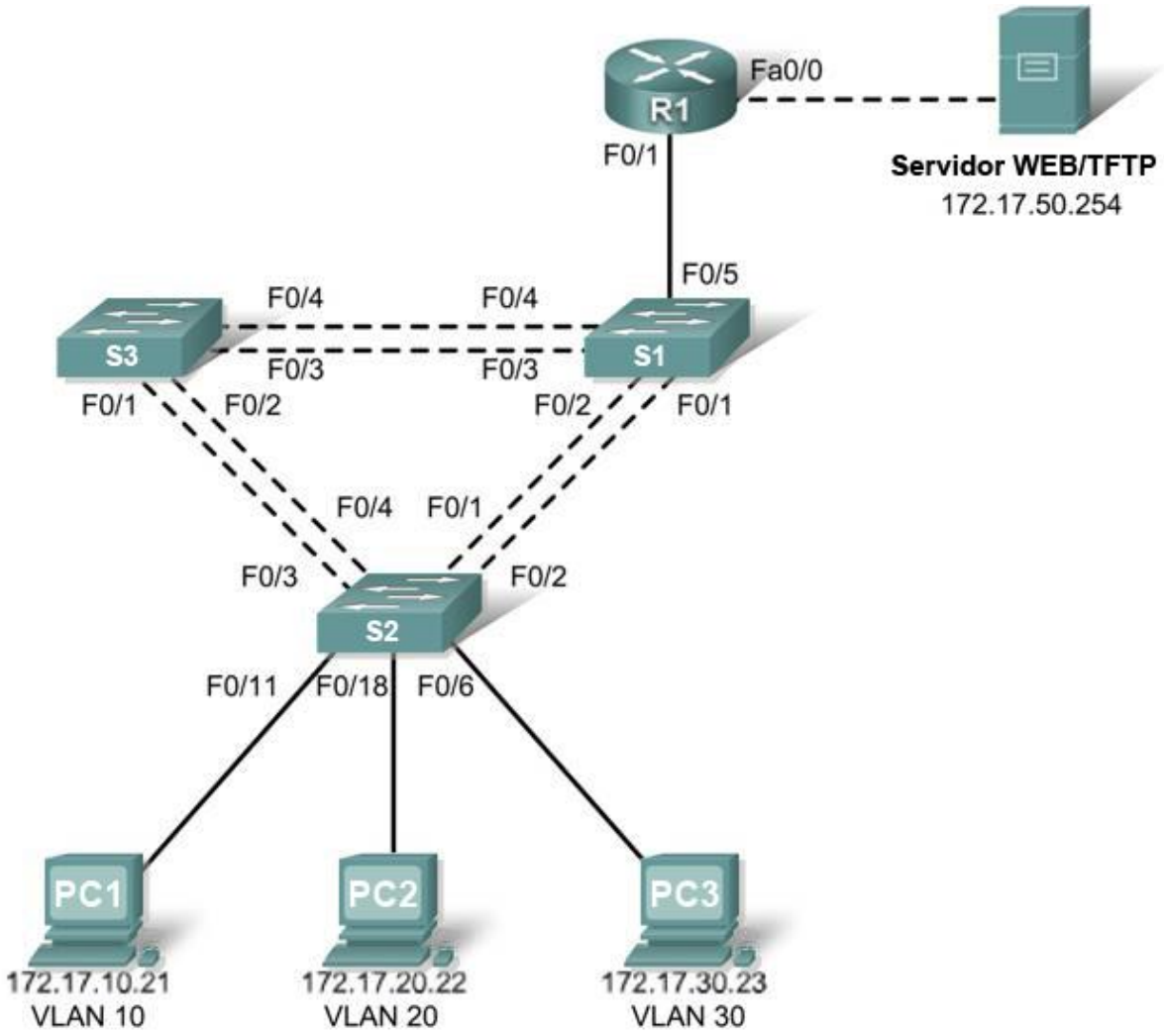


Tabla de direccionamiento

Dispositivo Nombre de host	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	**Fa 0/0**	172.17.50.1	255.255.255.0	No aplicable

R1	**Fa 0/1**	Ver tabla de configuración de interfaz		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
Servidor	**NIC**	172.17.50.254	255.255.255.0	172.17.50.1

Asignaciones de puerto: Switch 2

Puertos	Asignación	Red
Fa0/1 – 0/4	Enlaces troncales 802.1q (LAN 99 nativa)	172.17.99.0 /24
Fa0/5 – 0/10	VLAN 30: Guest (predeterminada)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10: Cuerpo docente/personal	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20: Estudiantes	172.17.20.0 /24

Tabla de configuración de la interfaz: Router 1

Interfaz	Asignación	Dirección IP
Fa0/1,1	VLAN1	172.17.1.1 /24
Fa0/1,10	VLAN 10	172.17.10.1 /24
Fa0/1,20	VLAN 20	172.17.20.1 /24
Fa0/1,30	VLAN 30	172.17.30.1 /24
Fa0/1,99	VLAN 99	172.17.99.1 /24

Objetivos de aprendizaje

Al completar esta práctica de laboratorio podrá:

- Cablear una red según el diagrama de topología
- Borrar las configuraciones y volver a cargar un switch y un router al estado predeterminado
- Realizar las tareas básicas de configuración en una LAN conmutada y un router.
- Configurar las VLAN y el protocolo VLAN Trunking (VTP) en todos los switches
- Demostrar y explicar el impacto de los límites de la Capa 3 impuestas al crear las VLAN.
- Configurar un router para admitir el enlace 802.1q en una interfaz Fast Ethernet
- Configurar un router con subinterfaces que correspondan a las VLAN configuradas
- Demostrar y explicar el enrutamiento entre VLAN

Tarea 1: Preparar la red

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

El resultado que se muestra en esta práctica de laboratorio está basado en los switches 2960 y en un router 1841. Puede utilizar cualquier switch actual en su laboratorio siempre y cuando éste tenga las interfaces necesarias que se muestran en el diagrama de topología. El uso de cualquier otro tipo de dispositivo puede producir resultados distintos. Se debe observar que las interfaces LAN (10Mb) en los routers no admiten enlaces troncales y el software IOS de Cisco anterior a la versión 12.3 puede no admitir enlaces troncales en interfaces de router Fast Ethernet.

Establezca conexiones de consola en los tres switches y en el router.

Paso 2: Borrar toda configuración existente en los switches.

Borre la NVRAM, borre el archivo vlan.dat y reinicie los switches. De ser necesario, consulte la Práctica de laboratorio 2.2.1 para el procedimiento. Después de que la recarga se haya completado, utilice el comando **show vlan** para verificar que solo existan VLAN predeterminadas y que todos los puertos se asignen a la VLAN 1.

```
S1#show vlan

Nombre de la VLAN                     Estado   Puertos
---- -------------------------------- --------- -------------------------------
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
```

Paso 3: Deshabilitar todos los puertos usando el comando shutdown

Asegúrese de que los estados del puerto de switch estén inactivos deshabilitando todos los puertos. Simplifique esta tarea con el comando **interface range**.

```
S1(config)#interface range fa0/1-24
S1(config-if-range)#shutdown
S1(config-if-range)#interface range gi0/1-2
S1(config-if-range)#shutdown

S2(config)#interface range fa0/1-24
S1(config-if-range)#shutdown
S2(config-if-range)#interface range gi0/1-2
S1(config-if-range)#shutdown

S3(config)#interface range fa0/1-24
S3(config-if-range)#shutdown
S3(config-if-range)#interface range gi0/1-2
S3(config-if-range)#shutdown
```

Paso 4: Volver a habilitar los puertos de usuario activos 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
```

Tarea 2: Realizar las configuraciones básicas del switch

Configure los switches S1, S2 y S3 según la tabla de direccionamiento y las siguientes pautas:

- Configure el nombre de host del switch.
- Deshabilite la búsqueda DNS.
- Configure **class** como contraseña de enable secret.
- Configure la contraseña **cisco** para las conexiones de consola.
- Configure la contraseña **cisco** para las conexiones de vty.
- Configure la gateway predeterminada en cada switch.

Se muestran los resultados para S1

```
Switch>enable
Switch#configure terminal
Ingrese los comandos de configuración, uno por línea. Finalice con 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: Configurado desde la consola por la consola
S1#copy running-config startup-config
Destination filename [startup-config]? [enter]
Creando la configuración...
```

Tarea 3: Configurar las interfaces Ethernet en las PC Host

Configure las interfaces Ethernet de PC1, PC2, PC3 y el Servidor TFTP/Web remoto con las direcciones IP de la tabla de direccionamiento.

Tarea 4: Configurar VTP en los switches

Paso 1: Configurar VTP en los tres switches utilizando la siguiente tabla. Recuerde que las contraseñas y los nombres de dominios VTP distinguen entre mayúsculas y minúsculas.

Nombre del switch	Modo de operación VTF	Dominio del VTP	Contraseña de VTP
S1	**Servidor**	**Lab6**	**cisco**
S2	**Cliente**	**Lab6**	**cisco**
S3	**Cliente**	**Lab6**	**cisco**

S1:

```
S1(config)#vtp mode server
Modo dispositivo ya es SERVIDOR VTP.
S1(config)#vtp domain Lab6
Cambiar el nombre del dominio VTP de NULL a Lab6
S1(config)#vtp password cisco
Configurar la contraseña de la base de datos VLAN del dispositivo en cisco
```

```
S1(config)#end
```

S2:

```
S2(config)#vtp mode client
Configurar el dispositivo a modo CLIENTE VTP
S2(config)#vtp domain Lab6
Cambiar el nombre del dominio VTP de NULL a Lab6
S2(config)#vtp password cisco
Configurar la contraseña de la base de datos VLAN del dispositivo en cisco
S2(config)#end
```

S3:

```
S3(config)#vtp mode client
Configurar el dispositivo a modo CLIENTE VTP
S3(config)#vtp domain Lab6
Cambiar el nombre del dominio VTP de NULL a Lab6
S3(config)#vtp password cisco
Configurar la contraseña de la base de datos VLAN del dispositivo en cisco
S3(config)#end
```

Paso 2: Configurar los puertos de enlace troncales y designar la VLAN nativa para los enlaces troncales.

Configure Fa0/1 a Fa0/5 como puertos de enlace y designe la VLAN 99 como la VLAN nativa para estos enlaces troncales. Simplifique esta tarea con el comando **interface range** en el modo de configuración global.

```
S1(config)#interface range fa0/1-4
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end
```

```
S2(config)# interface range fa0/1-4
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
S2(config-if-range)#end
```

```
S3(config)# interface range fa0/1-4
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown
S3(config-if-range)#end
```

Paso 3: Configurar las VLAN en el servidor VTP.

Configure las siguientes VLAN en el servidor VTP:

VLAN	Nombre de la VLAN
VLAN 99	administración
VLAN 10	cuerpo docente-personal
VLAN 20	estudiantes
VLAN 30	guest

```
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 se hayan creado las VLAN en S1 con el comando **show vlan brief**.

Paso 4: Verificar que las VLAN creadas en S1 se hayan 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 clientes.

```
S2#show vlan brief

Nombre de la VLAN                     Estado    Puertos
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                Gi0/2
10   faculty/staff                     active
20   students                          active
30   guest                             active
99   management                        active
```

Paso 5: 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 todos los switches estén correctamente configurados haciendo ping entre ellos. Desde S1, haga ping a la interfaz de administración en S2 y S3. Desde S2, haga ping a la interfaz de administración en S3.

¿Los pings son exitosos? _____

Todos los ping deben tener éxito.

En caso contrario, realice el diagnóstico de fallas de las configuraciones de los switches e inténtelo nuevamente.

Paso 6: Asignar puertos de switch a las VLAN en S2.

Consulte la tabla de asignación de puertos al principio de la práctica de laboratorio para asignar puertos a las VLAN.

```
S2(config)#interface range fa0/5-10
S2(config-if-range)#switchport access vlan 30
S2(config-if-range)#interface range fa0/11-17
S2(config-if-range)#switchport access vlan 10
S2(config-if-range)#interface range fa0/18-24
S2(config-if-range)#switchport access vlan 20
S2(config-if-range)#end
S2#copy running-config startup-config
Destination filename [startup-config]? [enter]
Creando la configuración...
[OK]
```

Paso 7: Verificar la conectividad entre las VLAN.

Abra las ventanas de comandos en los tres hosts conectados a S2. Haga ping desde la PC1 (172.17.10.21) a la PC2 (172.17.20.22). Haga ping desde la PC2 a la PC3 (172.17.30.23).

¿Los pings son exitosos? _____

Estos pings no tienen éxito.

Si no tienen éxito, ¿por qué fallaron?_____

_____

_____

Cada host está en una VLAN diferente. Como cada VLAN está en un dominio de Capa 3 separado, los paquetes deben enrutarse a la Capa 3 entre las VLAN. Aún no hemos configurado los dispositivos con capacidad L3.

Tarea 5: Configurar el Router y la LAN con servidor remoto

Paso 1: Borrar la configuración en el router y volver a cargar.

```
Router#erase nvram:
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
Erase of nvram: complete
Router#reload
System configuration has been modified. Save? [yes/no]: no
```

Paso 2: Crear una configuración básica en el router.

- Configure el router con el nombre de host R1.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de modo EXEC: **cisco**.
- Configure la contraseña **cisco** para las conexiones de consola.
- Configure la contraseña **cisco** para las conexiones de vty.

Paso 3: Configurar la interfaz de enlaces troncales en R1.

Ha demostrado que la conectividad entre las VLAN requiere enrutamiento en la capa de la red, exactamente igual que la conectividad entre dos redes remotas cualesquiera. Hay un par de opciones para configurar el enrutamiento entre las VLAN.

La primera es similar a un enfoque de fuerza bruta. Se conecta un dispositivo L3, ya sea un router o un switch de capa 3, a un switch de LAN con múltiples conexiones: una conexión separada para cada VLAN que requiera conectividad entre las VLAN. Cada uno de los puertos de switch utilizados por el dispositivo L3 se configuran en una VLAN diferente en el switch. Después de que las direcciones IP han sido asignadas a las interfaces en el dispositivo L3, la tabla de enrutamiento ha conectado directamente rutas para todas las VLAN y el enrutamiento entre las VLAN está habilitado. Las limitaciones de este enfoque son la falta de puertos Ethernet suficientes en los routers, subutilización de los puertos en los switches L3 y routers, y cableado excesivo y configuración manual. La topología utilizada en esta práctica de laboratorio no emplea este enfoque.

Un enfoque alternativo 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 el tráfico entre las VLAN sea transportado a y desde el dispositivo de enrutamiento en un solo enlace troncal. Sin embargo, requiere que la interfaz L3 sea configurada con múltiples direcciones IP. Esto puede hacerse creando interfaces ‘virtuales’, llamadas subinterfaces, en uno de los puertos del router Fast Ethernet y configurándolos para que reconozcan la encapsulación dot1q.

Emplear el enfoque de configuración de subinterfaces requiere de los siguientes pasos :

- Ingresar al modo de configuración de subinterfaz
- Establecer encapsulamiento de enlace troncal
- Asociar la VLAN con la subinterfaz
- Asignar una dirección IP desde la VLAN a la subinterfaz

Los comandos son los siguientes:

```
R1(config)#interface fastethernet 0/1
R1(config-if)#no shutdown
R1(config-if)#interface fastethernet 0/1.1
R1(config-subif)#encapsulation dot1q 1
R1(config-subif)#ip address 172.17.1.1 255.255.255.0
R1(config-if)#interface fastethernet 0/1.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0
R1(config-if)#interface fastethernet 0/1.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 172.17.20.1 255.255.255.0
R1(config-if)#interface fastethernet 0/1.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 172.17.30.1 255.255.255.0
R1(config-if)#interface fastethernet 0/1.99
R1(config-subif)#encapsulation dot1q 99 native
R1(config-subif)#ip address 172.17.99.1 255.255.255.0
```

Observe los siguientes puntos en esta configuración:

- La interfaz física se habilita usando el comando **no shutdown** porque las interfaces de los router están inactivas de manera predeterminada. Las interfaces virtuales están activas de manera predeterminada.
- La subinterfaz puede usar cualquier número que pueda describirse con 32 bits, pero es buen ejercicio asignar el número de la VLAN como el número de la interfaz, como se hizo aquí.
- La VLAN nativa está especificada en el dispositivo L3 a fin de que sea consistente con los switches. De lo contrario, la VLAN 1 sería la VLAN nativa predeterminada, y no habría comunicación entre el router y la VLAN de administración en los switches.

Paso 4: Configurar la interfaz de servidor LAN en R1.

```
R1(config)# interface FastEthernet0/0
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. Verifique que pueda enrutar paquetes a las seis redes viendo la tabla de enrutamiento en R1.

```
R1#show ip route
<resultado omitido>

Gateway of last resort is not set

     172.17.0.0/24 is subnetted, 6 subnets
C       172.17.50.0 is directly connected, FastEthernet0/1
C       172.17.30.0 is directly connected, FastEthernet0/0.30
C       172.17.20.0 is directly connected, FastEthernet0/0.20
C       172.17.10.0 is directly connected, FastEthernet0/0.10
C       172.17.1.0 is directly connected, FastEthernet0/0.1
C       172.17.99.0 is directly connected, FastEthernet0/0.99
```

Si su tabla de enrutamiento no muestra las seis redes, realice el diagnóstico de fallas de su configuración y resuelva el problema antes de proceder.

Paso 5: Verificar el enrutamiento entre las VLAN.

Desde la PC1, verifique que pueda hacer ping en el servidor remoto (172.17.50.254) y en los otros dos hosts (172.17.20.22 y 172.17.30.23). Puede que tome un par de pings antes de que se establezca la ruta de extremo a extremo.

¿Los pings son exitosos? _____
Estos pings deben tener éxito.

Si no lo tienen, haga el diagnóstico de fallas de su configuración. Verifique para asegurarse de que las gateways predeterminadas se han establecido en todas las PC y en todos los switches. Si alguno de los hosts ha entrado en hibernación, la interfaz conectada puede desactivarse.

Tarea 6: Reflexión

En la Tarea 5 se recomendó que se configure la VLAN 99 como la VLAN nativa en la configuración de la interfaz del router Fa0/0.99. ¿Por qué fallaron los paquetes del router o de los hosts cuando trataban de llegar a las interfaces de administración del switch si se dejaba la VLAN nativa en su configuración predeterminada?

_____

_____

_____

_____

La VLAN nativa está sin etiquetar. Si el tráfico de la VLAN 99 está sin etiquetar (como lo está, porque es nativa en los switches), el router no puede interpretar los datos porque no hay información de la VLAN en el encabezado, como se espera. a su vez, el router etiqueta todo el tráfico de salida de la VLAN 99 y deja los datos de la VLAN 1 sin etiquetar, por lo tanto los switches tampoco pueden interpretar correctamente. El tráfico de la VLAN a las otras VLAN no debe estar afectado por la asignación de la VLAN nativa.

Tarea 7: Limpieza

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

Configuraciones finales

Router 1

```
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 172.17.50.1 255.255.255.0
 no shutdown
!
interface FastEthernet0/1
```

```
 no shutdown
!
interface FastEthernet0/1,1
 encapsulation dot1Q 1
 ip address 172.17.1.1 255.255.255.0
!
interface FastEthernet0/1,10
 encapsulation dot1Q 10
 ip address 172.17.10.1 255.255.255.0
!
interface FastEthernet0/1,20
 encapsulation dot1Q 20
 ip address 172.17.20.1 255.255.255.0
!
interface FastEthernet0/1,30
 encapsulation dot1Q 30
 ip address 172.17.30.1 255.255.255.0
!
interface FastEthernet0/1,99
 encapsulation dot1Q 99 native
 ip address 172.17.99.1 255.255.255.0
!
<output omitted - serial interfaces not configured>
!
line con 0
line aux 0
line vty 0 4
 login
 password cisco
!
```

Switch 1

```
!
hostname S1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
```

```
interface FastEthernet0/5
 no shutdown
!
<output omitted - all remaining ports in shutdown>
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan1
 ip address 219,170,1000,1 255.255.255.0
 no shutdown
!
ip default-gateway 172.17.99.1
ip http server
!
line con 0
 logging synchronous
line vty 0 4
 login
 password cisco
line vty 5 15
 login
 password cisco
!
end
```

Switch 2

```
!
hostname S2
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 switchport access vlan 30
 switchport mode access
!
```

```
 interface FastEthernet0/6
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 30
!
interface FastEthernet0/8
 switchport access vlan 30
!
interface FastEthernet0/9
 switchport access vlan 30
!
interface FastEthernet0/10
 switchport access vlan 30
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 10
!
 interface FastEthernet0/13
 switchport access vlan 10
!
interface FastEthernet0/14
 switchport access vlan 10
!
interface FastEthernet0/15
 switchport access vlan 10
!
interface FastEthernet0/16
 switchport access vlan 10
!
interface FastEthernet0/17
 switchport access vlan 10
!
interface FastEthernet0/18
 switchport access vlan 20
!
interface FastEthernet0/19
 switchport access vlan 20
!
interface FastEthernet0/20
 switchport access vlan 20
!
interface FastEthernet0/21
 switchport access vlan 20
!
interface FastEthernet0/22
 switchport access vlan 20
!
interface FastEthernet0/23
 switchport access vlan 20
!
```

```
interface FastEthernet0/24
 switchport access vlan 20
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan1
 ip address 172.17.99.12 255.255.255.0
 no shutdown
!
ip default-gateway 172.17.99.1
ip http server
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Switch 3

```
!
hostname S3
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 shutdown
!
<output omitted - all remaining ports in shutdown>
```

```
!
!
interface Vlan1
 ip address 172.17.99.13 255.255.255.0
 no shutdown
!
ip default-gateway 172.17.99.1
ip http server
!
control-plane
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Práctica de laboratorio 6.4.2: Reto al enrutamiento inter VLAN (Versión para el instructor)

Diagrama de topología

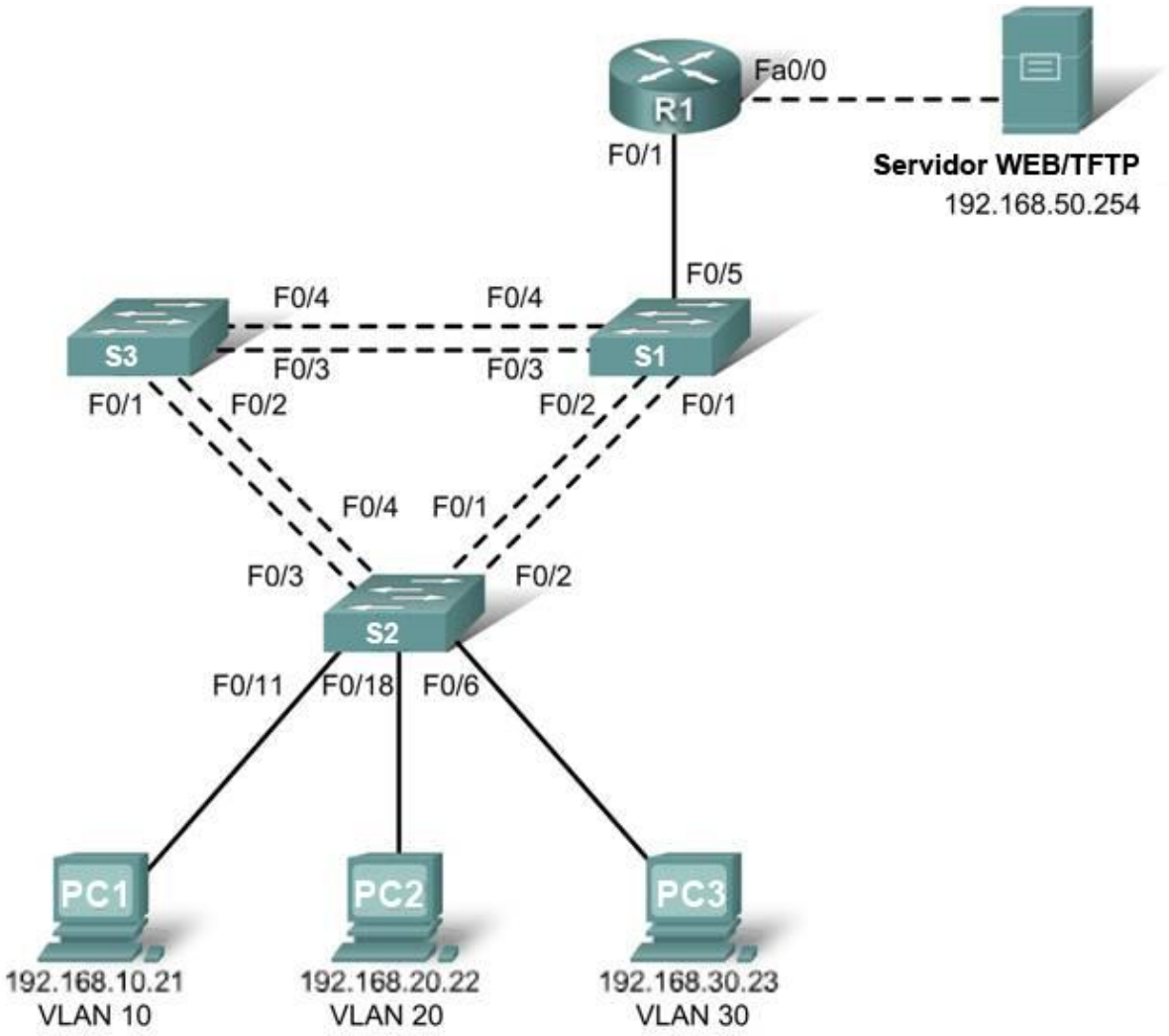


Tabla de direccionamiento

Dispositivo Nombre de host	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	**Fa 0/0**	192.168.50.1	255.255.255.0	No aplicable

R1	**Fa 0/1**	Ver tabla de configuración de subinterfaz		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
Servidor	**NIC**	192.168.50.254	255.255.255.0	192.168.50.1

Asignaciones de puerto: Switch 2

Puertos	Asignación	Red
Fa0/1 – 0/4	Enlaces troncales 802.1q (LAN 99 nativa)	192.168.99.0 /24
Fa0/5 – 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 subintefaz: Router 1

Interfaz del router	Asignación	Dirección IP
Fa0/0,1	VLAN1	192.168.1.1
Fa0/0,10	VLAN 10	192.168.10.1
Fa0/0,20	VLAN 20	192.168.20.1
Fa0/0,30	VLAN 30	192.168.30.1
Fa0/0,99	VLAN 99	192.168.99.1

Objetivos de aprendizaje

Al completar esta práctica de laboratorio podrá:

- Cablear una red según el diagrama de topología
- Borrar las configuraciones y volver a cargar un switch y un router al estado predeterminado
- Realizar las tareas básicas de configuración en una LAN conmutada y un router.
- Configurar las VLAN y el protocolo VLAN Trunking (VTP) en todos los switches
- Configurar un router para admitir el enlace 802.1q en una interfaz Fast Ethernet
- Configurar un router con subinterfaces que correspondan a las VLAN configuradas
- Demostrar el enrutamiento entre las VLAN

Tarea 1: Preparar la red

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

El resultado que se muestra en esta práctica de laboratorio está basado en los switches 2960 y en un router 1841. Puede utilizar cualquier switch actual en su laboratorio siempre y cuando éste tenga las interfaces necesarias que se muestran en el diagrama de topología. El uso de cualquier otro tipo de dispositivo puede producir resultados distintos. Se debe observar que las interfaces LAN (10Mb) en los routers no admiten enlaces troncales y el software IOS de Cisco anterior a la versión 12.3 puede no admitir enlaces troncales en interfaces de router Fast Ethernet.

Establezca conexiones de consola en los tres switches y en el router.

Paso 2: Borrar toda configuración existente en los switches.

Borre la NVRAM, borre el archivo vlan.dat y reinicie los switches. De ser necesario, consulte la Práctica de laboratorio 2.2.1 para el procedimiento. Después de que la recarga se haya completado, utilice el comando **show vlan** para verificar que solo existan VLAN predeterminadas y que todos los puertos se asignen a la VLAN 1.

```
S1#show vlan

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
```

Paso 3: Deshabilitar todos los puertos usando el comando shutdown.

Asegúrese de que los estados del puerto de switch estén inactivos deshabilitando todos los puertos. Simplifique esta tarea con el comando **interface range**.

```
S1(config)#interface range fa0/1-24
S1(config-if-range)#shutdown
S1(config-if-range)#interface range gi0/1-2
S1(config-if-range)#shutdown

S2(config)#interface range fa0/1-24
S2(config-if-range)#shutdown
S2(config-if-range)#interface range gi0/1-2
S2(config-if-range)#shutdown

S3(config)#interface range fa0/1-24
S3(config-if-range)#shutdown
S3(config-if-range)#interface range gi0/1-2
S3(config-if-range)#shutdown
```

Paso 4: Rehabilitar los puertos de usuario activos en S2 en el modo de acceso.

Habilite los puertos Fa0/6, Fa0/11 y Fa0/18 en S2 usando el comando **no shutdown** y configúrelos como puertos 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
```

Tarea 2: Realizar las configuraciones básicas del switch

Configure los switches S1, S2 y S3 según la tabla de direccionamiento y las siguientes pautas:

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

(Se muestran los resultados para S1)

```
Switch>enable
Switch#configure terminal
Ingrese los comandos de configuración, uno por línea.  Finalice con CNTL/Z.
Switch(config)# hostname S1
S1(config)#enable secret class
S1(config)#no ip domain-lookup
S1(config)#ip default-gateway 192.168.99.1
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: Configurado desde la consola por la consola
S1#copy running-config startup-config
Destination filename [startup-config]?
Creando la configuración...
```

Tarea 3: Configurar las interfaces Ethernet en el servidor y las PC Host

Configure las interfaces Ethernet de PC1, PC2, PC3 y el Servidor TFTP/Web remoto con las direcciones IP de la tabla de direccionamiento. Conecte estos dispositivos utilizando los cables e interfaces correctos.

Tarea 4: Configurar VTP en los switches

Paso 1: Configurar VTP en los switches

Ultilice la siguiente tabla para configurar los switches. Recuerde que las contraseñas y los nombres de dominios VTP distinguen entre mayúsculas y minúsculas.

Nombre del switch	Modo de operación VTF	Dominio del VTP	Contraseña de VTP
S1	**Servidor**	**Lab6**	**cisco**
S2	**Cliente**	**Lab6**	**cisco**
S3	**Cliente**	**Lab6**	**cisco**

S1:

```
S1(config)#vtp mode server
Modo dispositivo ya es SERVIDOR VTP.
S1(config)#vtp domain Lab6
Cambiar el nombre del dominio VTP de  NULL a Lab6
S1(config)#vtp password cisco
Configurar la contraseña de la base de datos VLAN del dispositivo en cisco
S1(config)#end
```

S2:

```
S2(config)#vtp mode client
Configurar el dispositivo a modo CLIENTE VTP
S2(config)#vtp domain Lab6
Cambiar el nombre del dominio VTP de  NULL a Lab6
S2(config)#vtp password cisco
Configurar la contraseña de la base de datos VLAN del dispositivo en cisco
S2(config)#end
```

S3:

```
S3(config)#vtp mode client
Configurar el dispositivo a modo CLIENTE VTP
S3(config)#vtp domain Lab6
Cambiar el nombre del dominio VTP de  NULL a Lab6
S3(config)#vtp password cisco
Configurar la contraseña de la base de datos VLAN del dispositivo en cisco
S3(config)#end
```

Paso 2: Configurar los puertos de enlace troncales y designar la VLAN nativa para los enlaces troncales.

Configure Fa0/1 a Fa0/5 como puertos de enlace y designe la VLAN 99 como la VLAN nativa para estos enlaces troncales. Simplifique esta tarea con el comando **interface range** en el modo de configuración global.

```
S1(config)#interface range fa0/1-4
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end
```

```
S2(config)# interface range fa0/1-4
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
S2(config-if-range)#end
```

```
S3(config)# interface range fa0/1-4
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown
S3(config-if-range)#end
```

Paso 3: Configurar las VLAN en el servidor VTP.

Configure las siguientes VLAN en el servidor VTP.

VLAN	Nombre de la VLAN
VLAN 99	Administración
VLAN 10	R&D
VLAN 20	Ingeniería
VLAN 30	Ventas

```
S1(config)#vlan 99
S1(config-vlan)#name Management
S1(config-vlan)#exit
S1(config)#vlan 10
S1(config-vlan)#name R&D
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name Engineering
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name Sales
S1(config-vlan)#exit
```

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

Paso 4: Verificar que las VLAN creadas en S1 se hayan 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 clientes.

```
S2#show vlan brief

Nombre de la VLAN                     Estado    Puertos
---- -------------------------------- --------- -------------------------------
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   R&D                               active
20   Engineering                       active
30   Sales                             active
99   Management                        active
```

Paso 5: Configurar la dirección de la interfaz de administración en los tres switches.

Consulte la tabla de direccionamiento al comienzo de la práctica de laboratorio para asignar la dirección IP de administración en los tres switches.

```
S1(config)#interface vlan 99
S1(config-if)#ip address 192.168.99.11 255.255.255.0
S1(config-if)#no shutdown
```

```
S2(config)#interface vlan 99
S2(config-if)#ip address 192.168.99.12 255.255.255.0
S2(config-if)#no shutdown

S3(config)#interface vlan 99
S3(config-if)#ip address 192.168.99.13 255.255.255.0
S3(config-if)#no shutdown
```

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

¿Los pings son exitosos? _____

Todos los ping deben tener éxito.

En caso contrario, realice el diagnóstico de fallas de las configuraciones de los switch y solucione.

Paso 6: Asignar puertos de switch a las VLAN en S2.

Consulte la tabla de asignación de puertos al principio de la práctica de laboratorio para asignar puertos a las VLAN.

```
S2(config)#interface range fa0/5-10
S2(config-if-range)#switchport access vlan 30
S2(config-if-range)#interface range fa0/11-17
S2(config-if-range)#switchport access vlan 10
S2(config-if-range)#interface range fa0/18-24
S2(config-if-range)#switchport access vlan 20
S2(config-if-range)#end
S2#copy running-config startup-config
Destination filename [startup-config]? [enter]
Creando la configuración...
[OK]
```

Paso 7: Verificar la conectividad entre las VLAN.

Abra las ventanas de comandos en los tres hosts conectados a S2. Haga ping desde la PC1 (192.168.10.21) a la PC2 (192.168.20.22). Haga ping desde la PC2 a la PC3 (192.168.30.23).

¿Los pings son exitosos? _____No

Si no tienen éxito, ¿por qué fallaron?_____

_____

Cada host está en una VLAN diferente. Como cada VLAN está en un dominio de Capa 3 separado, los paquetes deben enrutarse a la Capa 3 entre las VLAN. Aún no hemos configurado los dispositivos con capacidad L3.

Tarea 5: Configurar el router

Paso 1: Borrar la configuración en el router y volver a cargar.

```
Router#erase nvram:
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
Erase of nvram: complete
Router#reload
System configuration has been modified. Save? [yes/no]: n
```

Paso 2: Crear una configuración básica en un router.

- Configure el router con el nombre de host R1.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de modo EXEC: **class**.
- Configure la contraseña **cisco** para las conexiones de consola.
- Configure la contraseña **cisco** para las conexiones de vty.

Paso 3: 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 al comienzo de la práctica de laboratorio. Configure estas subinterfaces con encapsulamiento dot1q y utilice la primera dirección en cada subred de VLAN en la interfaz del router. Especifique la VLAN 99 como la VLAN nativa en su subinterfaz. No asigne una dirección IP a la interfaz física, pero asegúrese de habilitarla. Documente sus subinterfaces y sus respectivas direcciones IP en la tabla de subinterfaces.

```
R1(config)#interface fastethernet 0/1
R1(config-if)#no shutdown
R1(config-if)#interface fastethernet 0/1.1
R1(config-subif)#encapsulation dot1q 1
R1(config-subif)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#interface fastethernet 0/1.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#interface fastethernet 0/1,20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 192.168.20.1 255.255.255.0
R1(config-if)#interface fastethernet 0/1,30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-if)#interface fastethernet 0/1,99
R1(config-subif)#encapsulation dot1q 99 native
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
```

Paso 4: Configurar la interfaz de servidor LAN en R1.

Consulte la tabla de direccionamiento y configure Fa0/0 con la dirección IP y máscara correctas.

```
R1(config)# interface FastEthernet0/0
R1(config-if)#ip address 192.168.50.1 255.255.255.0
R1(config-if)#description server interface
R1(config-if)#no shutdown
R1(config-if)#end
```

Paso 5: Verificar la configuración de enrutamiento.

En este momento debe haber seis redes configuradas en R1. Verifique que pueda enrutar paquetes a las seis redes viendo la tabla de enrutamiento en R1.

```
R1#show ip route
<resultado omitido>

Gateway of last resort is not set

     192.168.0.0/24 is subnetted, 6 subnets
C       192.168.50.0 is directly connected, FastEthernet0/0
```

```
C       192.168.30.0 is directly connected, FastEthernet0/1.30
C       192.168.20.0 is directly connected, FastEthernet0/1.20
C       192.168.10.0 is directly connected, FastEthernet0/1.10
C       192.168.1.0 is directly connected, FastEthernet0/1.1
C       192.168.99.0 is directly connected, FastEthernet0/1.99
```

Si su tabla de enrutamiento no muestra las seis redes, realice el diagnóstico de fallas de su configuración y resuelva el problema antes de proceder.

Paso 6: Verificar el enrutamiento entre las VLAN.

Desde la PC1, verifique que pueda hacer ping en el servidor remoto (192.168.50.254) y en los otros dos hosts (192.168.20.22 and 192.168.30.23). Puede que tome un par de pings antes de que se establezca la ruta de extremo a extremo.

¿Los pings son exitosos? _____
Estos pings deben tener éxito.

Si no lo tienen, haga el diagnóstico de fallas de su configuración. Verifique para asegurarse de que las gateways predeterminadas se han establecido en todas las PC y en todos los switches. Si alguno de los hosts ha entrado en hibernación, la interfaz conectada puede desactivarse.

En este momento usted puede hacer ping a cualquier nodo en cualquiera de las seis redes configuradas en su LAN, incluyendo las interfaces del switch de administración.

Tarea 6: Limpieza

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

Configuraciones finales

Configuración del router 1

```
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 192.168.50.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1,1
 encapsulation dot1Q 1
 ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet0/1,10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
!
interface FastEthernet0/1,20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
!
interface FastEthernet0/1,30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
!
interface FastEthernet0/1,99
 encapsulation dot1Q 99 native
 ip address 192.168.99.1 255.255.255.0
!
 <output omitted - serial interfaces not configured>
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Configuración del switch 1

```
!
hostname S1
!
enable secret class
!
no ip domain lookup
```

```
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 shutdown
!
<output omitted - all remaining ports in shutdown>
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan1
 ip address 192.168.99.11 255.255.255.0
 no shutdown
!
ip default-gateway 192.168.99.1
ip http server
!
line con 0
 logging synchronous
line vty 0 4
 no login
line vty 5 15
 no login
!
end
```

Configuración del switch 2

```
!
hostname S2
!
enable secret class
!
no ip domain lookup
!
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
```

```
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 switchport access vlan 30
 switchport mode access
!
 interface FastEthernet0/6
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 30
!
interface FastEthernet0/8
 switchport access vlan 30
!
interface FastEthernet0/9
 switchport access vlan 30
!
interface FastEthernet0/10
 switchport access vlan 30
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 10
!
 interface FastEthernet0/13
 switchport access vlan 10
!
interface FastEthernet0/14
 switchport access vlan 10
!
interface FastEthernet0/15
 switchport access vlan 10
!
interface FastEthernet0/16
 switchport access vlan 10
!
interface FastEthernet0/17
 switchport access vlan 10
!
interface FastEthernet0/18
 switchport access vlan 20
```

```
!
interface FastEthernet0/19
 switchport access vlan 20
!
interface FastEthernet0/20
 switchport access vlan 20
!
interface FastEthernet0/21
 switchport access vlan 20
!
interface FastEthernet0/22
 switchport access vlan 20
!
interface FastEthernet0/23
 switchport access vlan 100
!
interface FastEthernet0/24
 switchport access vlan 20
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan1
 ip address 192.168.99.12 255.255.255.0
 no shutdown
!
ip default-gateway 192.168.99.1
ip http server
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Configuración del switch 3

```
!
hostname S3
!
enable secret class
!
no ip domain lookup
!
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
```

```
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 shutdown
!
<output omitted - all remaining ports in shutdown>
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan1
 ip address 192.168.99.13 255.255.255.0
 no shutdown
!
ip default-gateway 192.168.99.1
ip http server
!
control-plane
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Práctica de laboratorio 6.4.3: Resolución de problemas del enrutamiento inter VLAN (Versión para el instructor)

Diagrama de topología

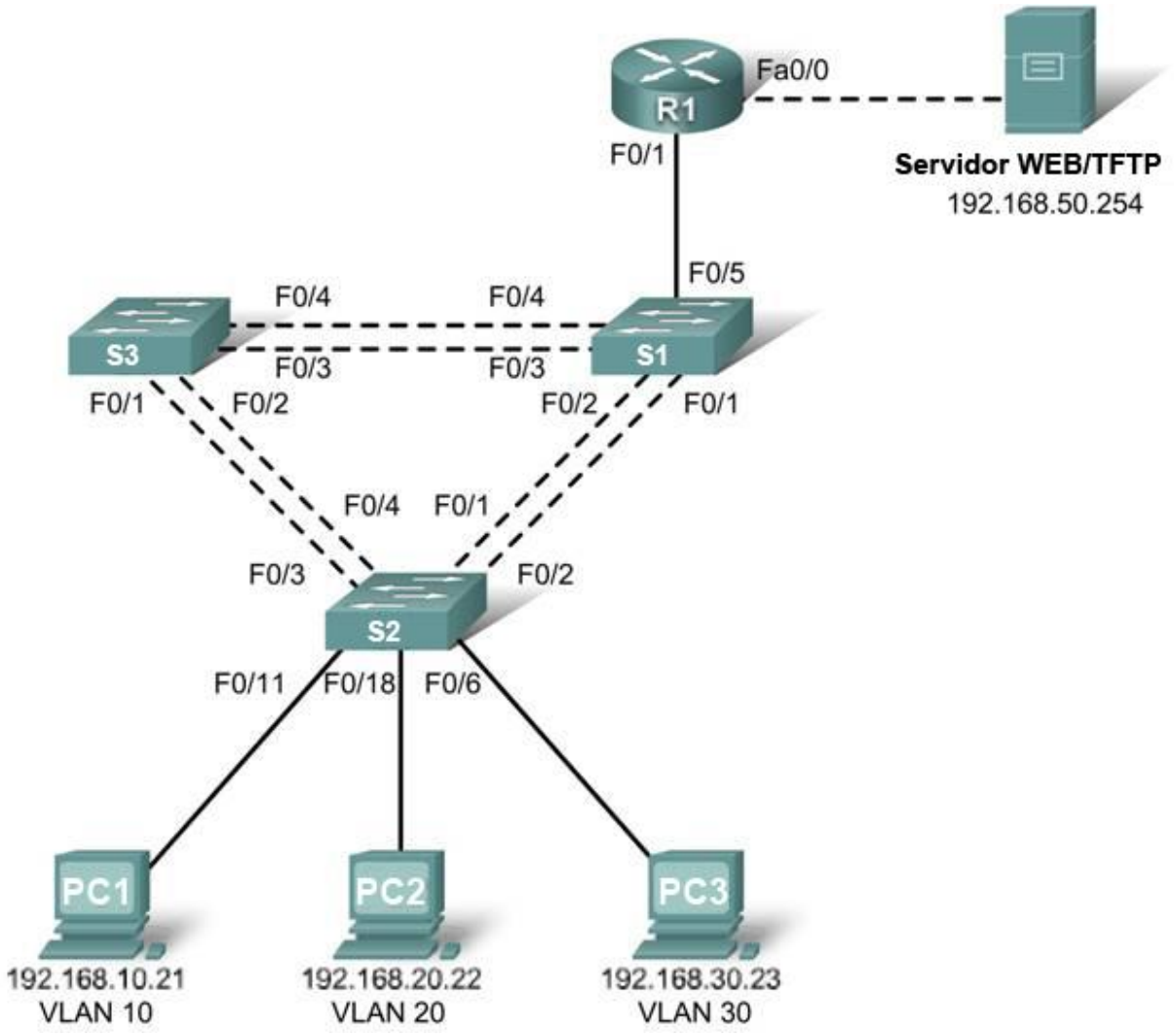


Tabla de direccionamiento

Dispositivo Nombre de host	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	**Fa 0/0**	192.168.50.1	255.255.255.0	No aplicable
R1	**Fa 0/1**	Ver tabla de configuración de subinterfaz		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
Servidor	**NIC**	192.168.50.254	255.255.255.0	192.168.50.1

Asignaciones de puerto – Switch 2

Puertos	Asignación	Red
Fa0/1 – 0/4	Enlaces troncales 802.1q (VLAN 99 nativa)	192.168.99.0 /24
Fa0/5 – 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 subinterfaces – Router 1

Interfaz del router	Asignación	Dirección IP
Fa0/0.1	VLAN1	192.168.1.1
Fa0/0.10	VLAN 10	192.168.10.1
Fa0/0.20	VLAN 20	192.168.20.1
Fa0/0.30	VLAN 30	192.168.30.1
Fa0/0.99	VLAN 99	192.168.99.1

Objetivos de aprendizaje

Para completar esta práctica de laboratorio debe:

- Cablear una red según el diagrama de topología
- Borrar todas las configuraciones y volver a cargar los switches y el router al estado predeterminado.
- Cargar los switches y el router con los guiones suministrados
- Encontrar y corregir todos los errores de configuración
- Documentar la red corregida

Escenario

La red se diseñó y configuró para admitir cinco VLAN y una red de servidor separada. Un router externo en una configuración del router-on-a-stick proporciona el enrutamiento inter VLAN y la red del servidor está enrutada a través de una interfaz Fast Ethernet separada. Sin embargo, no está funcionando como se diseñó, y las quejas de los usuarios no han proporcionado demasiada información sobre el origen de los problemas. Primero debe definir qué es lo que no funciona como se esperó, y luego analizar las configuraciones existentes para determinar y corregir el origen de los problemas.

Este laboratorio está completo cuando puede demostrar la conectividad IP entre cada una de las VLAN del usuario y la red de servidor externa, y entre la VLAN de administración del switch y la red de servidor.

Tarea 1: Preparar la red

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

El resultado que se muestra en esta práctica de laboratorio está basado en los switches 2960 y en un router 1841. Puede utilizar cualquier switch actual en su laboratorio siempre y cuando éste tenga las interfaces necesarias que se muestran en el diagrama de topología. El uso de cualquier otro tipo de dispositivo puede producir resultados distintos. Se debe observar que las interfaces LAN (10Mb) en los routers no admiten enlaces troncales y el software IOS de Cisco anterior a la versión 12.3 puede no admitir enlaces troncales en interfaces de router Fast Ethernet.

Establezca conexiones de consola en los tres switches y en el router.

Paso 2: Borrar toda configuración existente en los switches.

Borre las configuraciones de switch en los tres switches y vuelva a cargar para restaurar el estado predeterminado. Utilice el comando **show vlan** para verificar que solo existan VLAN predeterminadas y que todos los puertos se asignen a la VLAN 1.

Paso 3: Configurar las interfaces Ethernet en las PC Host y el servidor.

Configure las interfaces Ethernet de PC1, PC2, PC3 y el servidor con la dirección IP y las gateways predeterminadas indicados en la tabla de direccionamiento.

Tarea 2: Cargar el router y los switches con los guiones suministrados

Configuración del router 1

```
hostname R1
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 192.168.50.1 255.255.255.192
! no necesita desactivación
!
interface FastEthernet0/1
 no ip address
! no necesita desactivación
!
interface FastEthernet0/1,1
 encapsulation dot1Q 1
 ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet0/1,10
 encapsulation dot1Q 11
 !debe ser encapsulamiento dot1Q 10
 ip address 192.168.10.1 255.255.255.0
!
interface FastEthernet0/1,20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
!
interface FastEthernet0/1,30
 necesita encapsulamiento dot1Q 30
 ip address 192.168.30.1 255.255.255.0
!
interface FastEthernet0/1,99
```

```
 encapsulation dot1Q 99 native
 ip address 192.168.99.1 255.255.255.0
!
line con 0
 logging synchronous
 password cisco
 login
!
line vty 0 4
password cisco
 login
!
end
```

Configuración del switch 1

```
hostname S1
!
vtp mode server
vtp domain lab6_3
vtp password cisco
!
vlan 99
name Management
exit
!
vlan 10
name R&D
exit
!
! vlan 20 Falta configuración(ingeniería)
! nombre ingeniería
! salir
!
vlan 30
name Sales
exit
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
 shutdown
```

```
!no debe haber desactivación
!
!
interface range FastEthernet0/5 - 24
 shutdown
!
interface Vlan1
 ip address 192.168.99.11 255.255.255.0
 no shutdown
!
exit
!
ip default-gateway 192.168.99.1
!
line con 0
 logging synchronous
 password cisco
 login
!
line vty 0 4
password cisco
 login
!
line vty 5 15
 password cisco
 login
!
end
```

Configuración del switch 2

```
!
hostname S2
no ip domain-lookup
enable secret class
!
vtp mode client
vtp domain lab6_3
vtp password cisco
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
 interface range FastEthernet0/5 - 11
```

```
 switchport access vlan 30
 switchport mode access
 ! no debe asignarse el puerto Fa0/11 a la VLAN 10, ni 30
!
interface range FastEthernet0/12 - 17
 switchport access vlan 10
!
interface range FastEthernet0/18-24
 switchport mode access
 switchport access vlan 20
!
interface Vlan1
 ip address 192.168.99.12 255.255.255.0
 no shutdown
exit
!
ip default-gateway 192.168.99.1
ip http server
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Configuración del switch 3

```
!
hostname S3
!
enable secret class
!
vtp mode client
vtp domain lab6_3
vtp password cisco
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
```

```
 no shutdown
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface range FastEthernet0/5 - 24
 shutdown
 exit
!
interfaz Vlan1
 dirección ip 192.168.99.13 255.255.255.0
! Falta asignación de dirección IP de la interfaz VLAN
!
ip default-gateway 192.168.99.1
!
line con 0
 logging synchronous
 password cisco
 login
!
line vty 0 4
password cisco
 login
!
line vty 5 15
 password cisco
 login
!
end
```

Tarea 3: Diagnosticar y corregir los problemas entre las VLAN y los errores de configuración

Comience identificando qué funciona y qué no funciona. ¿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 R1? ¿Qué podría impedir que una red configurada se instale en la tabla de enrutamiento?

Cuando se hayan corregido todos los errores, podrá hacer ping al servidor remoto desde cualquier PC o cualquier switch. Además debe poder hacer ping entre las tres PC y hacer ping a las interfaces de administración en los switches desde cualquier PC.

Tarea 4: Documentar la configuración de la red

Cuando haya terminado con éxito su diagnóstico, capture el resultado del router y los tres switches con el comando **show run** y guárdelo en un archivo de texto.

Tarea 5: Limpieza

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

¿Qué está mal configurado?

Router 1

- la interfaz física fa0/1 no está encendida (No aparecerá ninguna interfaz hasta que se haya habilitado la interfaz física)
- encapsulamiento mal configurado en 0/1.30 (ninguno especificado)
- VLAN incorrecta asociada con 0/1.10 (11 en vez de 10)
- máscara de subred incorrecta en fa0/0 (/26 en vez de /24)

Switch 1

- puerto de enlace troncal fa0/4 no encendido
- La VLAN 20 no se ha creado en el servidor

```
vlan 20
name Engineering
exit
```

Switch 2

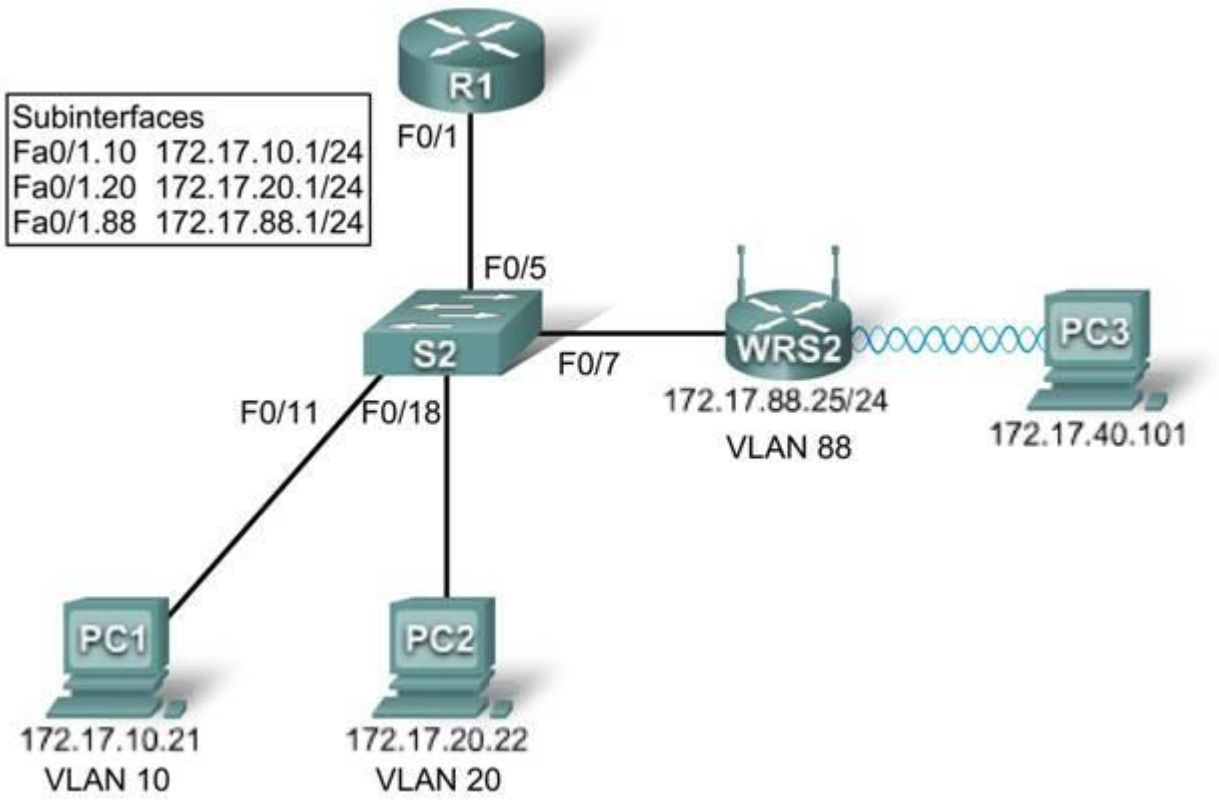
- port fa0/11 asignado a la VLAN incorrecta

Switch 3

- no se asignó dirección IP de administración (debe ser 192.168.99.13)

Práctica de laboratorio 7.5.1: Configuración básica inalámbrica (Versión para el instructor)

Diagrama de topología



Objetivos de aprendizaje

- Configurar opciones en la ficha de configuración Linksys
- Configurar opciones en la ficha inalámbrica Linksys
- Configurar opciones en la ficha de administración Linksys
- Configurar opciones en la ficha de seguridad Linksys
- Agregar conectividad inalámbrica a una PC
- Probar la conectividad

Introducción

En esta actividad configurará el router Linksys inalámbrico, permitiendo el acceso remoto tanto desde PC como de conectividad inalámbrica con seguridad WEP.

Tarea 1: Cargar las configuraciones de inicio.

Paso 1. Cargar las configuraciones de R1.

```
hostname R1
!
interface FastEthernet0/0
 ip address 172.17.50.1 255.255.255.0
 no shutdown
!
interface FastEthernet0/1
 no ip address
 no shutdown
!
interface FastEthernet0/1,10
 encapsulation dot1Q 10
 ip address 172.17.10.1 255.255.255.0
!
interface FastEthernet0/1,20
 encapsulation dot1Q 20
 ip address 172.17.20.1 255.255.255.0
!
interface FastEthernet0/1,88
 encapsulation dot1Q 88
 ip address 172.17.88.1 255.255.255.0
!
```

Paso 2. Cargar las configuraciones de S2.

```
hostname S2
!
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/7
 switchport access vlan 88
 switchport mode access
 no shutdown
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
 no shutdown
!
interface FastEthernet0/18
 switchport access vlan 20
 switchport mode access
 no shutdown
!
```

Tarea 2: Conectar e iniciar sesión en el router inalámbrico.

Para configurar los valores en el router inalámbrico usaremos su utilidad de Web Gui. Puede accederse a la GUI navegando a la dirección IP de LAN/inalámbrica del router con un navegador Web. La dirección predeterminada de la fábrica es 192.168.1.1

Paso 1. Establecer conectividad física.

Conecte un cable de conexión directa desde la PC a uno de los puertos LAN del router inalámbrico. El router inalámbrico proporcionará una dirección IP a la PC utilizando configuraciones DHCP predeterminadas.

Paso 2. Abrir un navegador web.

Paso 3. Navegar a la utilidad web del router inalámbrico.

- Establezca la URL del navegador en http://192.168.1.1.

Las credenciales login predeterminadas son un nombre y contraseña de usuario en blanco de: admin Tenga presente que esto es muy inseguro, ya que es la configuración predeterminada de fábrica y se proporciona públicamente. Estableceremos nuestra propia contraseña más adelante.

Paso 4. Iniciar sesión

- Deje el nombre de usuario en blanco y establezca la contraseña como: admin

Tarea 3: Configurar opciones en la ficha de configuración Linksys.

Paso 1. Establecer el tipo de conexión de Internet a IP estático.

- De manera predeterminada, la página de inicio es la pantalla “Setup”. En los menúes en el aviso de arriba nos encontramos en la sección “Configuración” y debajo de la ficha ‘Configuración básica’.
- En la pantalla Configuración para el router Linksys, ubique la opción **Tipo de conección** a **Internet** en la sección **Configuración de Internet** de esta página. Haga click en el menu desplegable y seleccione **IP Estático** de la lista.

Paso 2. Configurar la dirección IP de VLAN 88, máscara de subred y gateway predeterminada 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: Generalmente en una red doméstica o para una empresa pequeña, esta dirección IP de Internet se asigna por el ISP mediante DHCP o PPPoE (los detalles específicos de PPPoE están fuera del ámbito de este curso).

Paso 3. Configurar los parámetros IP del router.

- Aún en esta página, desplácese hacia abajo a **Configuración de red**. Para los campos **IP de Router** haga los siguiente:

  Establezca la dirección IP en 172.17.40.1 y la máscara subred en 255.255.255.0.
- En **Configuración del servidor DHCP**, asegúrese de que el servidor DHCP esté habilitado.

Paso 4. Guardar las configuraciones.

Haga clic en el botón Guardar configuración en la parte inferior de la pantalla Configuración.

Tenga en cuenta que el rango de la dirección IP para el conjunto DHCP se ajusta a un rango de direcciones para coincidir con los parámetros IP del router. Estas direcciones se usan para clientes inalámbricos y clientes que se conectan al switch interno del router inalámbrico. Los clientes reciben una dirección y máscara IP y se les da la IP del router para que la utilicen como gateway.

Paso 5. Reconectar a WRS2.

Ya que hemos cambiado la dirección IP del router y el conjunto DHCP, tendremos que reconectarnos utilizando la nueva dirección configurada previamente

- Reconéctese al router. Necesitará readquirir una dirección IP del router vía DHCP o establecer su propia dirección manualmente.
- Reconéctese a la configuración GUI del router utilizando una dirección IP de 172.17.88.1 (consulte la Tarea 1 para ayuda).

Tarea 4: Configurar opciones en la ficha inalámbrica Linksys.

Paso 1. Establecer el nombre de la red (SSID).

- Haga clic en la ficha **Inalámbrica**.
- En **Nombre de Red (SSID)**, vuelva a nombrar la red desde **Predeterminada** a **WRS_LAN**.
- Haga clic en **Guardar configuraciones**.

Paso 2. Establecer el modo de seguridad.

- Haga clic en **Seguridad inalámbrica**. Está ubicada junto a **Configuraciones inalámbricas básicas** en la ficha principal **Inalámbrica**.
- Cambie **Modo de seguridad** de **Desactivado** a **WEP**.
- Usando la Encriptación predeterminada de 40/64-Bit, establezca **Clave1** en **1234567890**.
- Haga clic en **Guardar configuraciones**.

Tarea 5: Configurar opciones en la ficha de administración Linksys

Paso 1. Establecer la contraseña del router.

- Haga clic en la ficha **Administración**.
- En **Acceso al router**, cambie la contraseña del router a **cisco 123**. Reingrese la misma contraseña para confirmar.

Paso 2. Habilitar la administración remota.

- En **Acceso remoto**, habilite **administración remota**.
- Haga clic en **Guardar configuraciones**.
- Puede que se le solicite que inicie la sesión otra vez. Utilice la nueva contraseña de **cisco123** y continúe manteniendo el nombre de usuario en blanco.

Tarea 6: Configurar opciones en la ficha de seguridad Linksys

De manera predeterminada, las peticiones a la interfaz LAN/Inalámbrica (172.17.40.1) de WRS2 desde fuentes en su interfaz WAN (por ejemplo PC1 y PC2) se bloquearán por razones de seguridad implementadas por el router inalámbrico. Con el propósito de verificar la conectividad en esta práctica de laboratorio, nos gustaría permitirlas.

Paso 1. Permitir peticiones anónimas de Internet.

- Haga clic en la ficha **Seguridad**.
- En **Filtro de Internet**, desmarque **Filtrar solicitudes anónimas de Internet**.

Tarea 7: Añadir conectividad inalámbrica a una PC

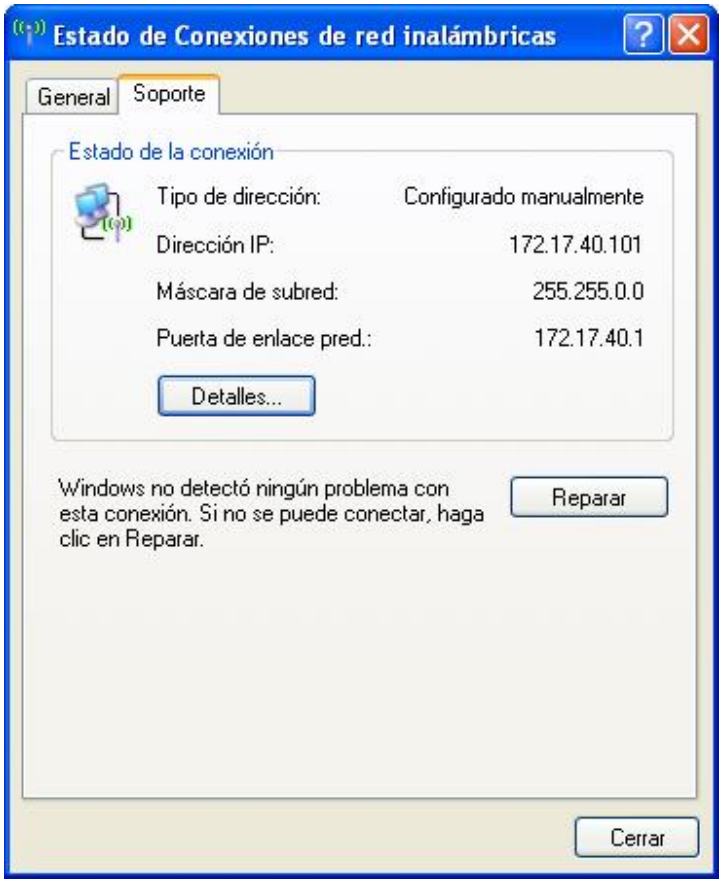
Paso 1. Desconectar la conexión Ethernet desde la Pc3 a WRS2.

Paso 2: Usar Windows XP para conectarse al router inalámbrico.

- Ubique el ícono de Conexión a la red inalámbrica en su barra de tareas o vaya a **Inicio > Panel de control > Conexiones de red**.
- Seleccione **Conexión de red inalámbrica**.
- Navegue al menú **Archivo** y seleccione **Estado**.
- Haga clic en **Ver redes inalámbricas**.
- Localice SSID ‘WRS_LAN’ en la lista de redes disponibles y conéctese a él.
- Cuando se le solicite la clave WEP, ingrésela como en la Tarea 3, **1234567890** y haga clic en **Conectar**.

Paso 3: Verificar la conexión.

- En la ventana **Estado**, seleccione la ficha **Soporte**.
- Verifique que la PC3 haya recibido una dirección IP del conjunto de direcciones DHCP de WRS2 o que haya sido configurada manualmente.



Tarea 8: Probar la conectividad

Paso 1. Haga ping a la interfaz LAN/Inalámbrica de WRS2.

- En la PC3, haga clic en **Inicio->Ejecutar**.
- Escriba **cmd** y seleccione abrir. Esto abrirá la petición de comando.
- En la petición de comando escriba (sin comillas) "**ping 172.17.40.1**".

Paso 2. Hacer ping a la interfaz Fa0/1.88.

- En la petición de comando escriba (sin comillas) "**ping 172.17.88.1**".

Paso 3. Hacer ping a la PC1 y Pc2 desde la PC3.

- En la petición de comando escriba (sin comillas) "**ping 172.17.10.21**" para hacer ping a la PC1.
- Repetir en la dirección de la PC2, 172.17.20.22.

Práctica de laboratorio 7.5.2: Desafío inalámbrico WRT300N (Versión para el instructor)

Diagrama de topología

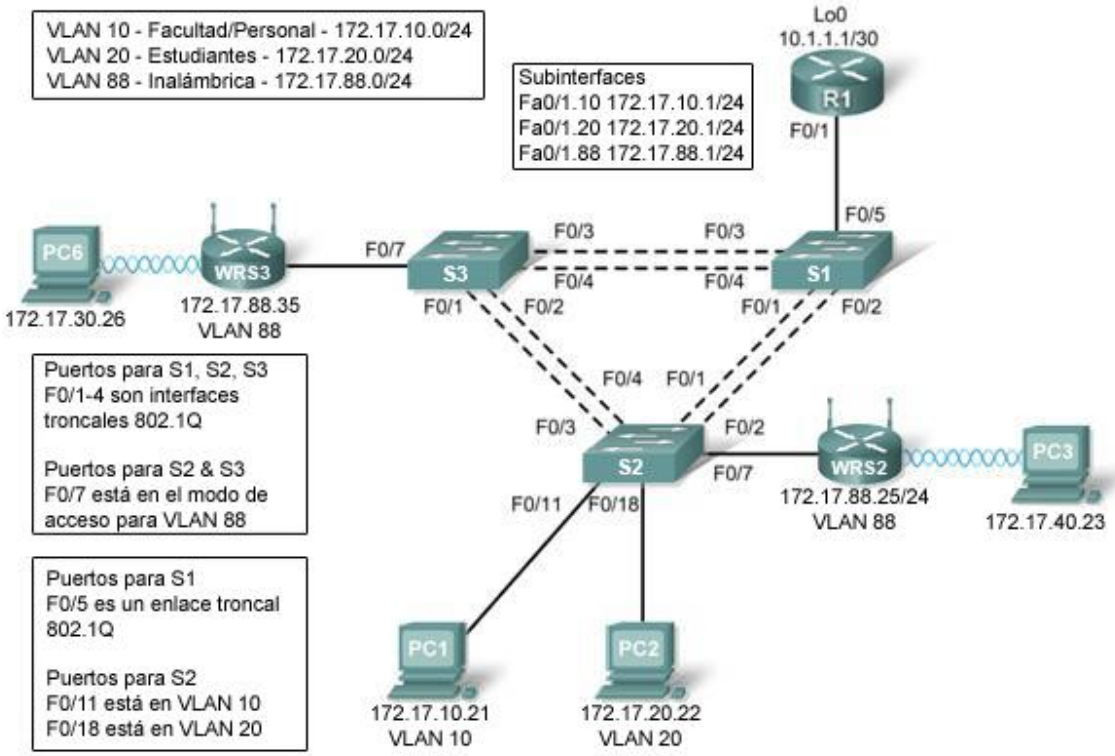


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salia)
R1	**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
	Lo0	10.1.1.1	255.255.255.252	No aplicable
WRS2	**WAN**	172.17.88.25	255.255.255.0	172.17.88.1
	LAN/Inalámbrica	172.17.40.1	255.255.255.0	No aplicable
WRS3	**WAN**	172.17.88.35	255.255.255.0	172.17.88.1
	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

Objetivos de aprendizaje

Al completar esta práctica de laboratorio podrá:

- Configurar información de la VLAN del puerto de switch y seguridad de puerto
- Reiniciar completamente un router Linksys WRT300N
- Conectar y verificar la conectividad a un router inalámbrico
- Navegar a una página de utilidad web Linksys WRT300N
- Establecer las configuraciones IP de un Linksys WRT300N
- Configurar DHCP en un Linksys WRT300N
- Configurar rutas estáticas en routers Cisco estándar y en un WRT300N
- Cambiar el modo de red y el canal de red correspondiente en un WRT300N
- Aprender cómo habilitar la encriptación WEP y deshabilitar la broadcast de SSID
- Habilitar un filtro MAC inalámbrico
- Configurar restricciones de acceso en un WRT300N
- Configurar la contraseña de administración del router en un WRT300N
- Habilitar el inicio de sesión en un WRT300N
- Actualizar el firmware de WRT300N
- Aprender mecanismos de diagnóstico, copias de seguridad, restauración y confirmación en un WRT300N

Escenario

En esta práctica de laboratorio configurará un Linksys WRT300N, un puerto de seguridad en un switch Cisco, y rutas estáticas en múltiples dispositivos. Tome nota de los procedimientos involucrados en la conexión a una red inalámbrica porque algunos de estos cambios involucran la desconexión de clientes, que puede que deban ser reconectados luego de realizar los cambios en la configuración.

Tarea 1: Realizar las configuraciones básicas del router

Configurar R1 según las siguientes pautas:

- Nombre de host del router
- Desactive la búsqueda DNS
- Contraseña de modo EXEC
- Fast Ethernet 0/1 y Fast Ethernet 0/0 y sus subinterfaces
- Loopback0
- Conexión síncrona, exec-timeout y un registro de **cisco** en el puerto de consola

```
enable
configure terminal
no ip domain-lookup
enable secret cisco


interface FastEthernet0/1,1
   encapsulation dot1 1
   ip address 172.17.1.1 255.255.255.0
!
```

```
interface FastEthernet0/1,10
   encapsulation dot1 10
   ip address 172.17.10.1 255.255.255.0
!
interface FastEthernet0/1,20
   encapsulation dot1 20
   ip address 172.17.20.1 255.255.255.0
!
interface FastEthernet0/1,88
   encapsulation dot1 88
   ip address 172.17.88.1 255.255.255.0
!
interface Loopback 0
   ip address 10.1.1.1 255.255.255.252
!
line con 0
 exec-timeout 0 0
 logging synchronous
 password cisco
 login
!
```

Tarea 2: Configurar interfaces de switch

Establezca los switches en transparente, borre la información de la VLAN y cree las VLAN 10, 20 y 88.

<For all three switches>

```
!
vtp mode transparent
no vlan 2-1001
vlan 10,20,88
!
```

Paso 1: Configurar las interfaces de puertos de switch en S1, S2 y S3.

Configure las interfaces en los switches S1, S2 y S3 con las conexiones del diagrama de topología.

Configure enlaces troncales en las conexiones entre dos switches.

En las conexiones a un router inalámbrico, configúrelas en modo de acceso para la vlan 88.

Configure la conexión de S2 a PC1 en la vlan 10 y la conexión a la PC2 en la vlan 20.

Configure la conexión de S1 a R1 como un enlace troncal.

Permita todas las VLAN en las interfaces de enlace troncal.

S1

```
!
interface FastEthernet 0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet 0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
```

```
!
interface FastEthernet 0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet 0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
```

S2

```
!
interface FastEthernet 0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet 0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet 0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet 0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/7
 switchport mode access
 switchport access vlan 88
 no shutdown
!
```

S3

```
!
interface FastEthernet 0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet 0/2
```

```
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet 0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet 0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet 0/7
 switchport mode access
 switchport access vlan 88
 no shutdown
!
interface FastEthernet 0/11
 switchport mode access
 switchport access vlan 11
 no shutdown
!
interface FastEthernet 0/18
 switchport mode access
 switchport access vlan 20
 no shutdown
!
```

Paso 2: Verificar las VLAN y los enlaces troncales.

Use el comando **show ip interface trunk** en S1 y el comando **show vlan** en S2 para verificar que los switches se estén enlazando correctamente y que existan las VLAN correctas.

```
S1#show interface trunk

Puerto      Modo         Estado de encapsulamiento     Vlan nativa
Fa0/1       on           802.1q          trunking      1
Fa0/2       on           802.1q          trunking      1
Fa0/3       on           802.1q          trunking      1
Fa0/4       on           802.1q          trunking      1
Fa0/5       on           802.1q          trunking      1

Port        Vlans allowed on trunk
Fa0/1       1/-4094
Fa0/2       1/-4094
Fa0/3       1/-4094
Fa0/4       1/-4094
Fa0/5       1/-4094

Port        VLAN permitidas y activas en el dominio de administración
Fa0/1       1,10,20,88
Fa0/2       1,10,20,88
Fa0/3       1,10,20,88
Fa0/4       1,10,20,88
Fa0/5       1,10,20,88
```

```
Puerto      Vlan en estado de envío de spanning tree y no depuradas

Puerto      Vlan en estado de envío de spanning tree y no depuradas
Fa0/1       1,10,20,88
Fa0/2       ninguna          ←-- bloqueadas debido al spanning tree
Fa0/3       1,10,20,88
Fa0/4       1,10,20,88
Fa0/5       1,10,20,88>
```

S2#show vlan

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, 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, Gi0/1, Gi0/2
10   VLAN0010                          active    Fa0/11
20   VLAN0020                          active    Fa0/18
88   VLAN0088                          active    Fa0/7
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Cuando haya finalizado, asegúrese de guardar la configuración en ejecución para la NVRAM del router y de los switches.

Paso 3: Configurar las interfaces Ethernet de PC1 y PC2.

Configurar las interfaces Ethernet de PC1 y PC2 con las direcciones IP y las gateways predeterminadas según la tabla de direccionamiento al comienzo de la práctica de laboratorio.

Paso 4: Probar la configuración de la PC.

Haga ping a la gateway predeterminada desde la PC: 172.17.10.1 para la PC1 y 172.17.20.1 para la PC2.

Go to Start->Run->cmd and type ping 172.17.x.x

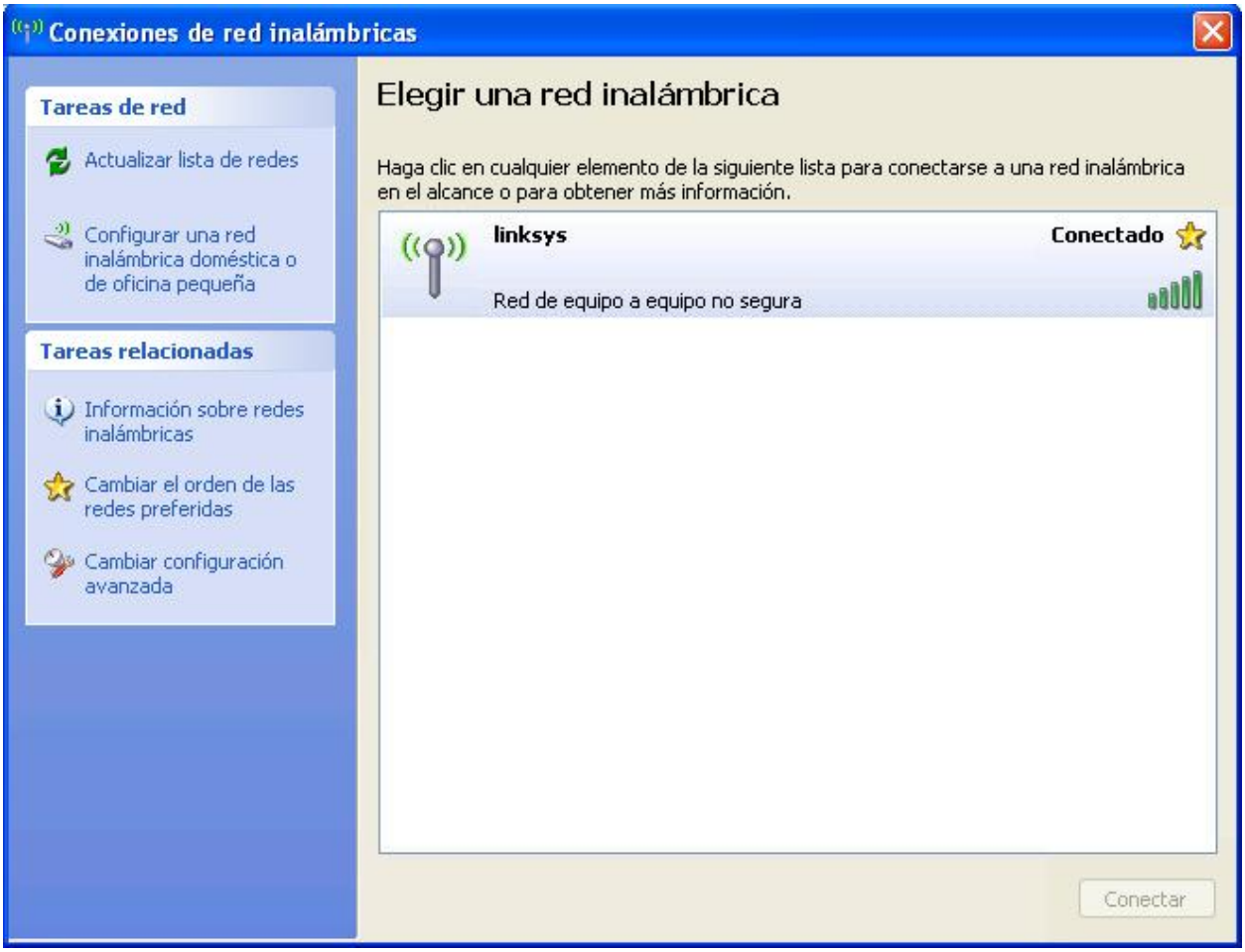
Tarea 3: Conectar al router Linksys WRT300N

Verifique con su instructor que el router inalámbrico tenga sus configuraciones predeterminadas de fábrica. Si no las tiene, debe reiniciar completamente el router. Para hacerlo, encuentre el botón de reinicio en la parte trasera del router. Con un lápiz u otro instrumento delgado, presione el botón de reinicio por 5 segundos. El router debe estar restaurado a sus configuraciones predeterminadas de fábrica.

Paso 1: Usar Windows XP para conectarse al router inalámbrico.

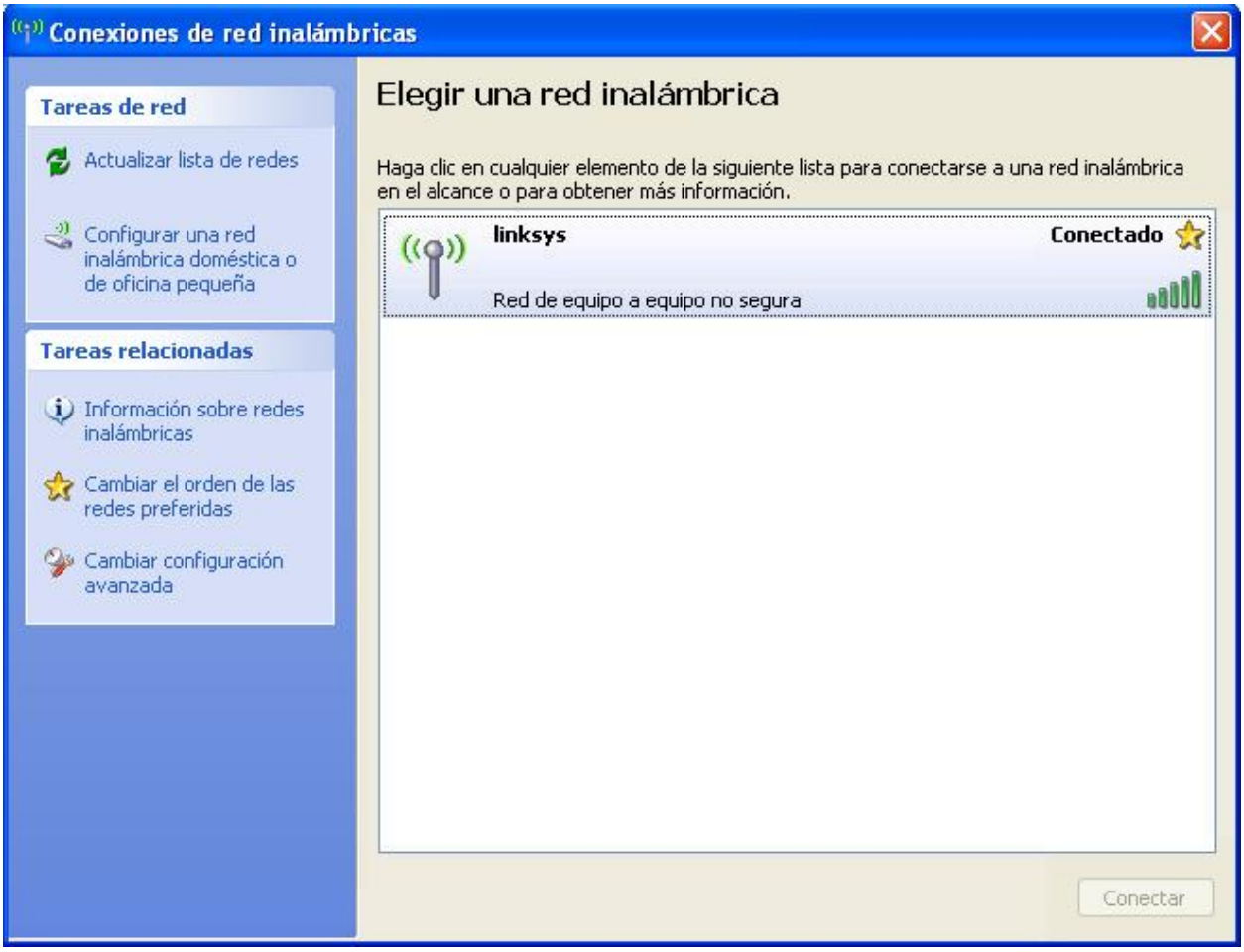
Ubique el ícono de Conexión a la red inalámbrica en su barra de tareas o vaya a **Inicio > Panel de control > Conexiones de red**. Haga click derecho en el ícono y seleccione Ver redes inalámbricas disponibles.

Aparece la siguiente visualización: Observe que el SSID predeterminado de fábrica del router es simplemente “Linksys”.



Seleccione **Linksys** y haga clic en **Conectar**.

En breve, estará conectado.



Paso 2: Verificar las configuraciones de conectividad.

Verifique las configuraciones de conectividad yendo a **Inicio > Ejecutar** y escribiendo **cmd**.
En la petición de entrada de comando, escriba el comando **ipconfig** para ver la información de su dispositivo de red. Fíjese qué dirección IP es la gateway predeterminada. La siguiente es la dirección IP predeterminada de un Linksys WRT300N.

```
Dirección IP. . . . . . . . . . . . : 172.17.30.26
Máscara de subred . . . . . . . . . : 255.255.255.0
Puerta de enlace predeterminada     : 172.17.30.1
```

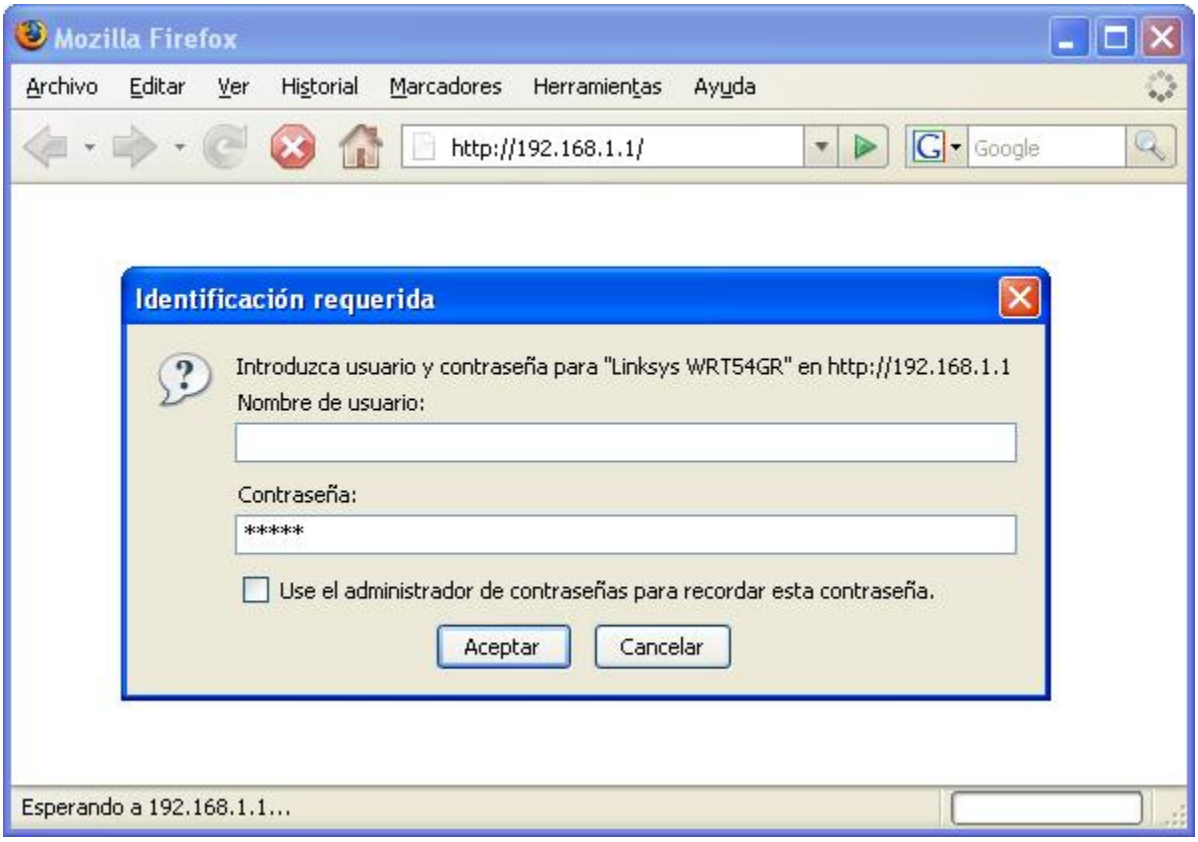
Tarea 4: Configurar WRT300N empleando la utilidad Web

Paso 1: Ir la la URL predeterminada.

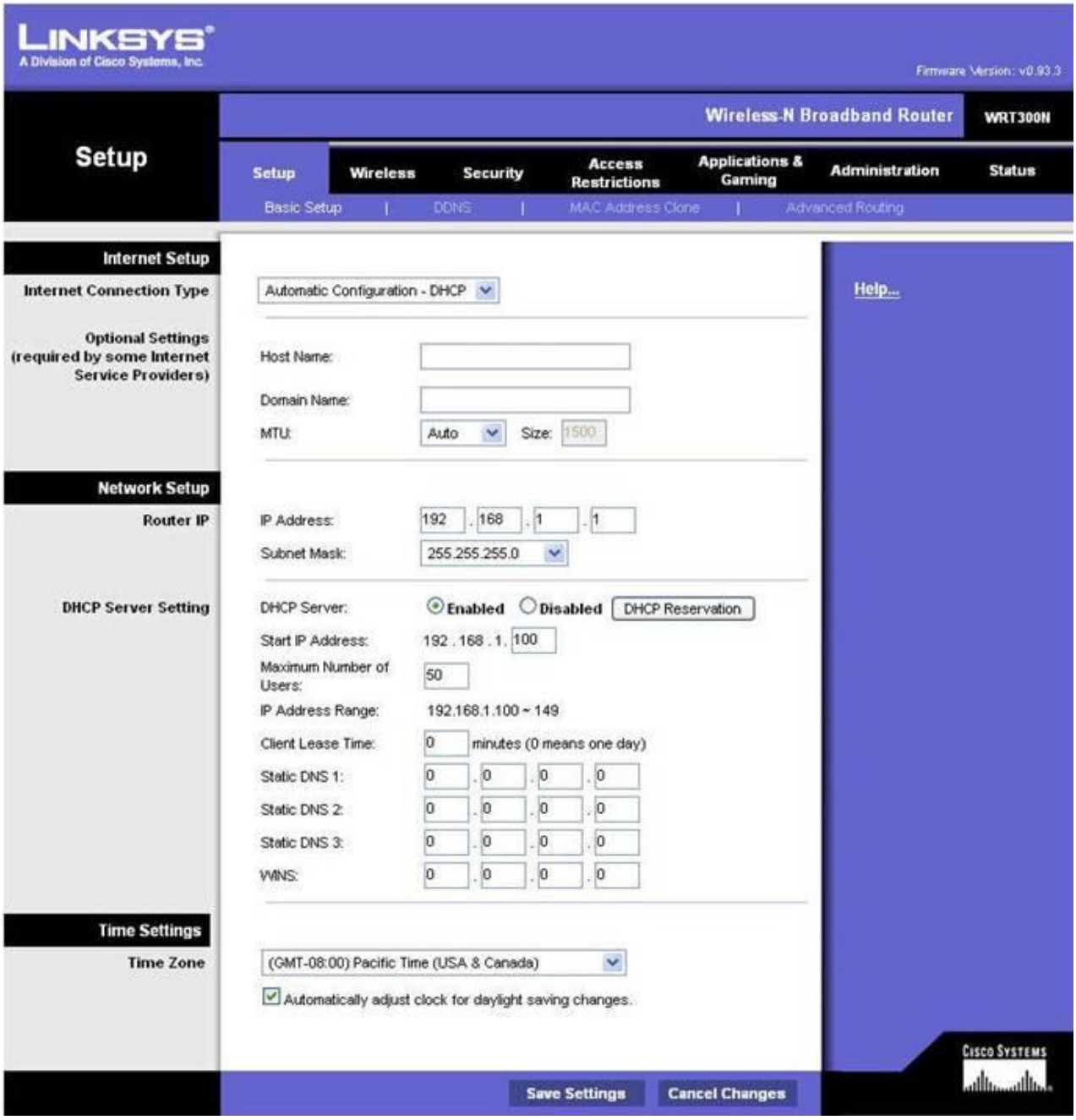
En su navegador web favorito, navegue a **http://192.168.1.1** que es la URL predeterminada del WRT300N.

Paso 2: Ingresar la información de autenticación.

Se le requerirá un nombre de usuario y contraseña. Ingrese la contraseña **admin** predeterminada de fábrica del WRT300N y deje el campo de nombre de usuario en blanco.



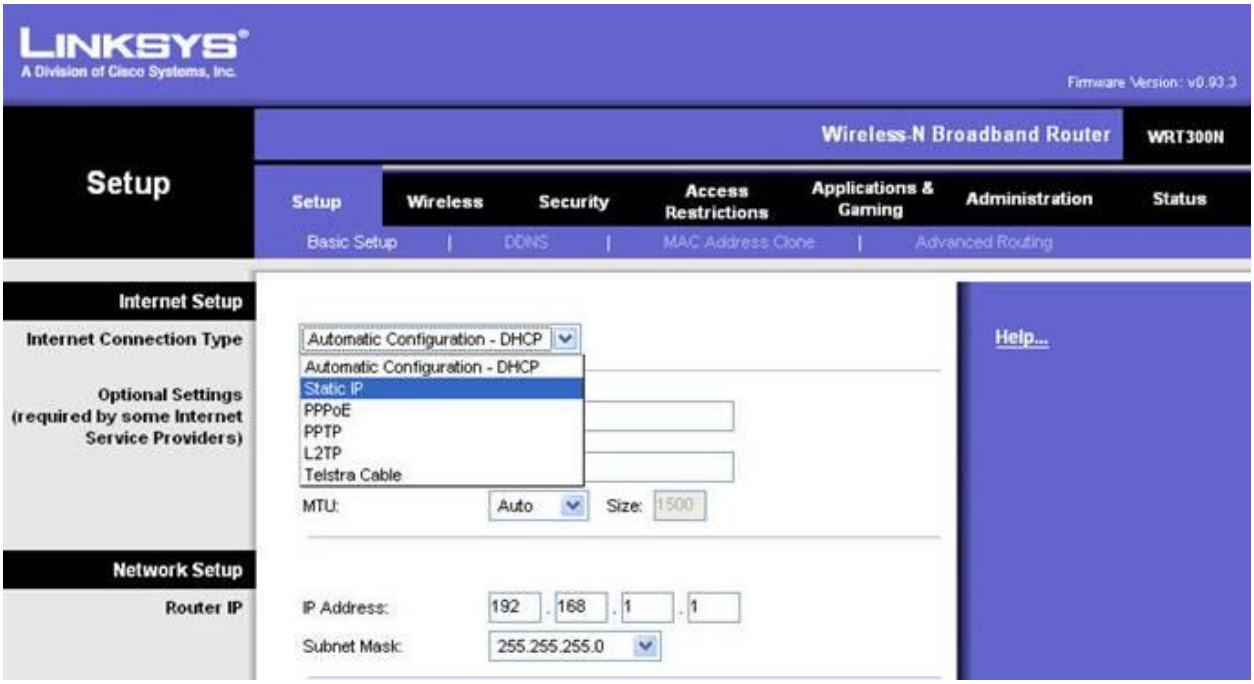
Ahora usted debe estar viendo la página predeterminada de la utilidad web de Linksys WRT300N.

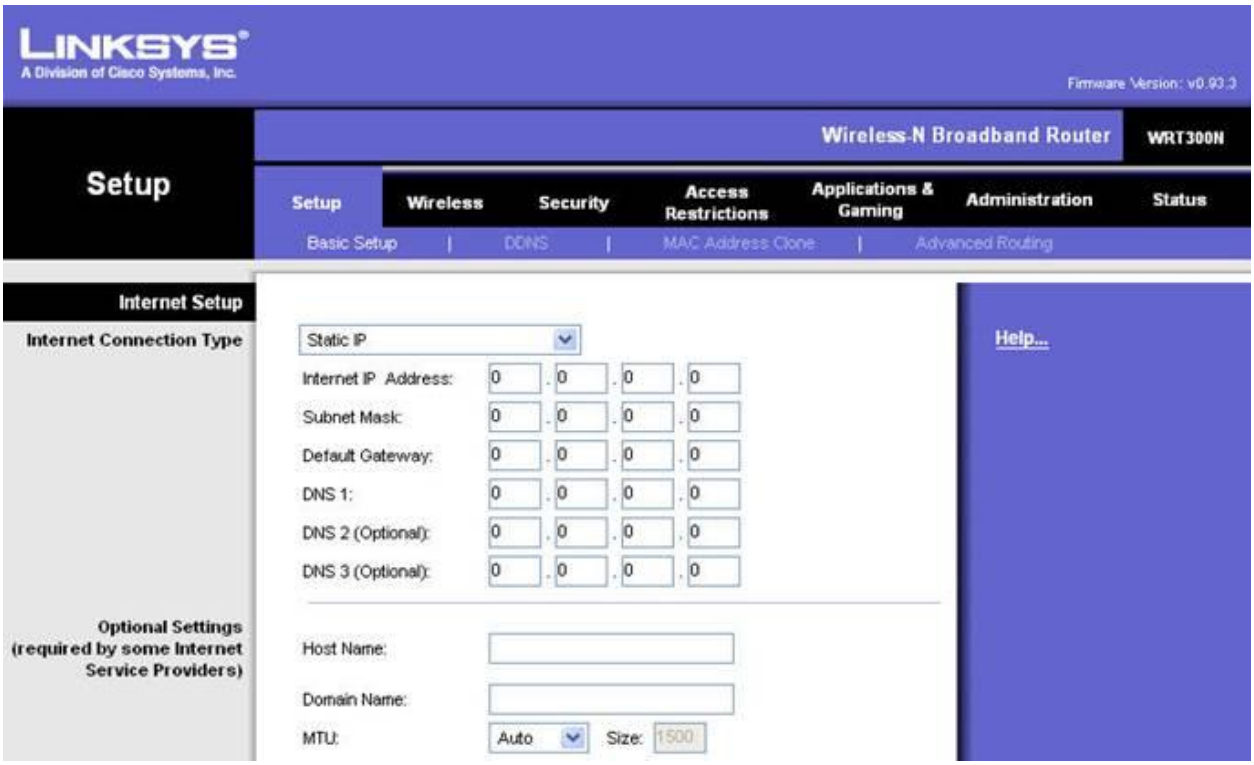


Tarea 5: Establecer las configuraciones IP para el Linksys WRT300N

La mejor manera de entender las siguientes configuraciones es pensar que el WRT300N es similar a un router basado en IOS de Cisco con dos interfaces separadas. Una de las interfaces, la que está configurada en Configuración de Internet, actúa como conexión a los switches y al interior de la red. La otra interfaz, configurada en Configuración de Red, actúa como la interfaz que conecta a los clientes inalámbricos, PC6 y PC3.

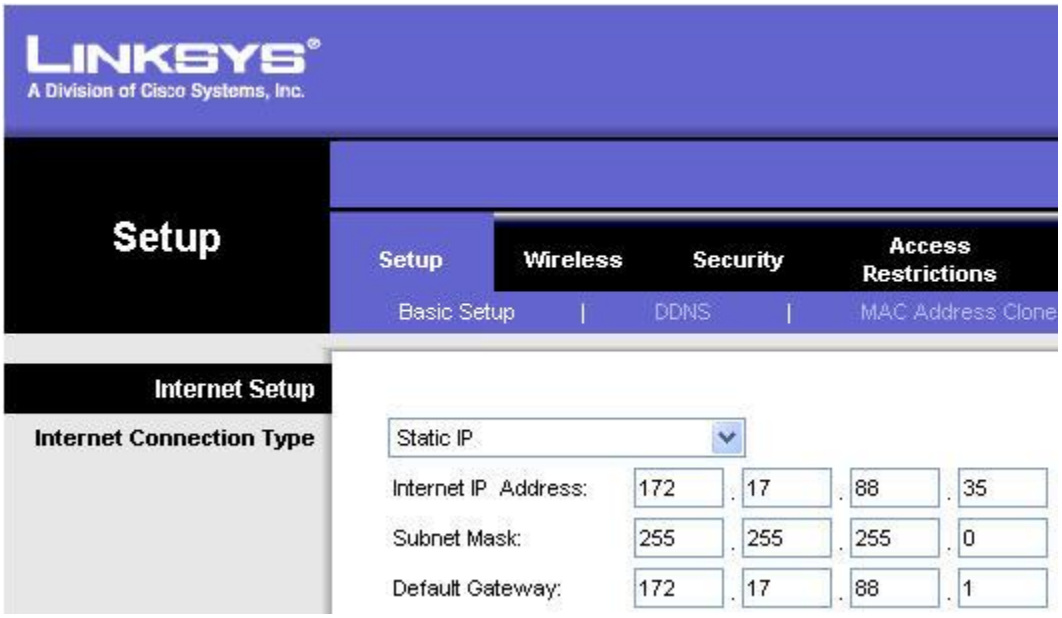
Paso 1: Establecer el tipo de conexión de Internet a IP estático.



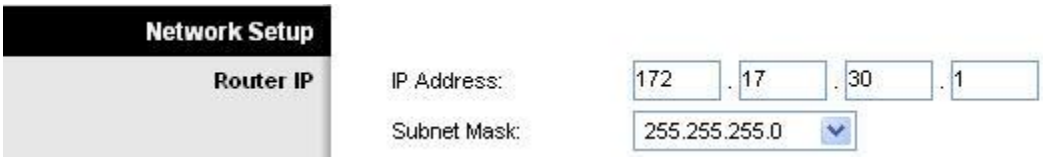


Paso 2: Establecer las configuraciones de las direcciones IP para la Configuración de Internet.

- Establezca la dirección IP de Internet en 172.17.88.35.
- Establezca la máscara de subred en 255.255.255.0.
- Establezca la gateway predeterminada a la dirección IP de la Fa 0/1 VLAN 88 de R1, 172.17.88.1.

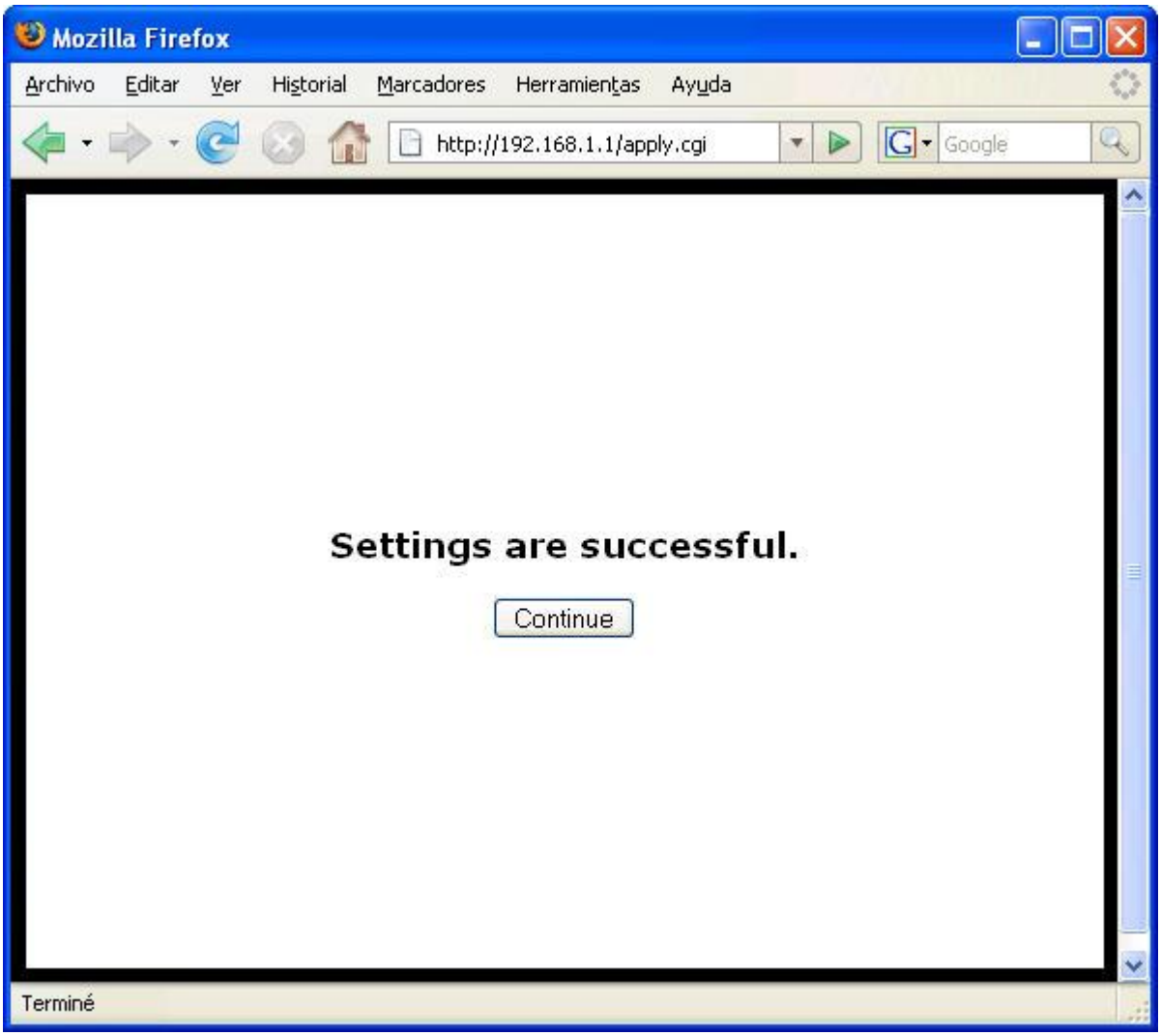


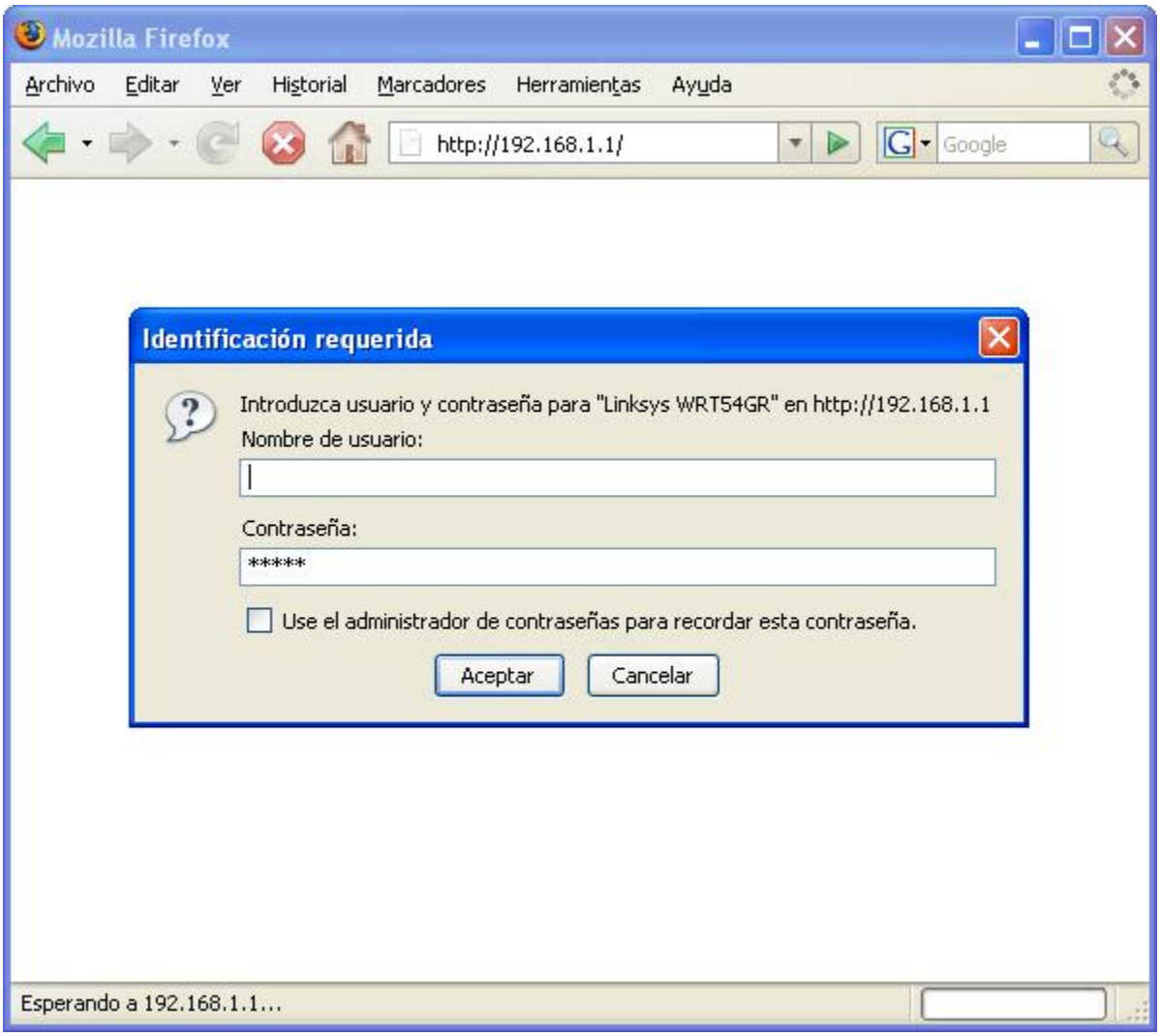
Paso 3: Configurar la dirección IP de configuración de la red en 172.17.30.1.



Paso 4: Guardar las configuraciones.

Haga clic en **Guardar configuraciones**. Aparece la siguiente ventana. Haga clic en **Continuar**. Si no es redireccionado a la nueva URL de la utilidad Web (**http://172.17.30.1**), navegue ahí con su navegador como lo hizo en la Tarea 4, Paso1.





Paso 5: Verificar los cambios en las direcciones IP.

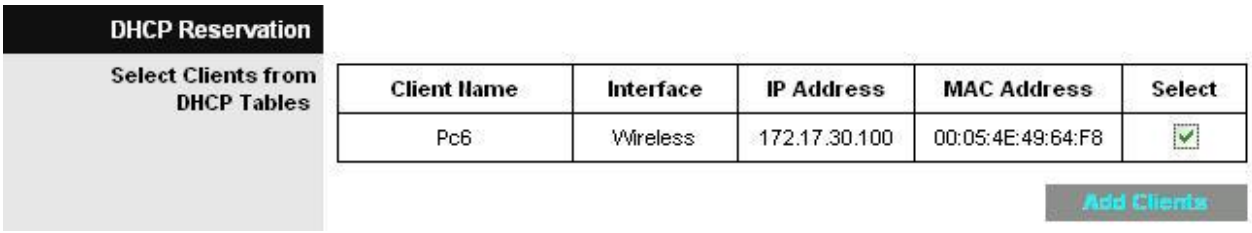
Vuelva a la petición de entrada de comandos y observe las nuevas direcciones IP. Use el comando **ipconfig**.

```
Dirección IP. . . . . . . . . . . . : 172.17.30.26
Máscara de subred . . . . . . . . . : 255.255.255.0
Puerta de enlace predeterminada     : 172.17.30.1
```

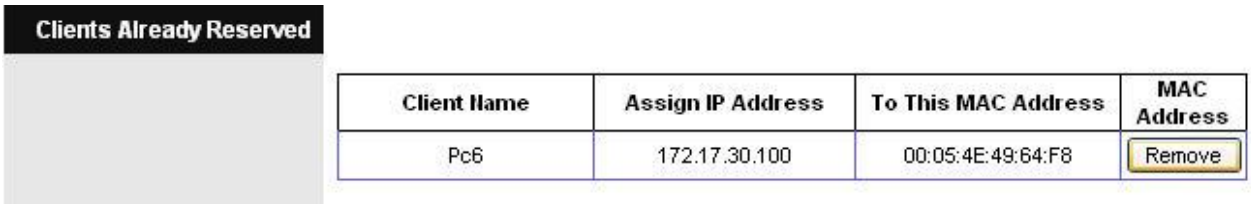
Tarea 6: Establecer las configuraciones DHCP y las configuraciones del huso horario del router

Paso 1: Dar a Pc6 un enlace DHCP estático.

Haga clic en **Reservas DHCP** y busque Pc6 en la lista de clientes DHCP existentes. Haga click en **Agregar Clientes**.

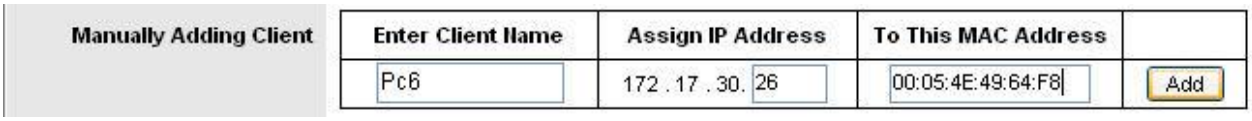


Esto otorga a la Pc6, la computadora con dirección MAC de 00:05:4E:49:64:F8, la misma dirección IP, 172.17.30.100, cuando pide una dirección mediante DHCP. Esto es solo un ejemplo de una forma rápida de unir un cliente permanentemente a la dirección IP dada por DHCP. Ahora asignará a la Pc6 la dirección IP del diagrama de topología, no la que recibió inicialmente. Haga clic en **Eliminar** para asignar una nueva dirección.



Paso 2: Asignar la dirección 172.17.30.26 a la Pc6.

Al ingresar a la dirección de Pc6 en Agregar un cliente manualmente, siempre que la Pc6 se conecte al router inalámbrico, recibirá la dirección IP 172.17.30.26 vía DHCP. Guarde sus cambios.

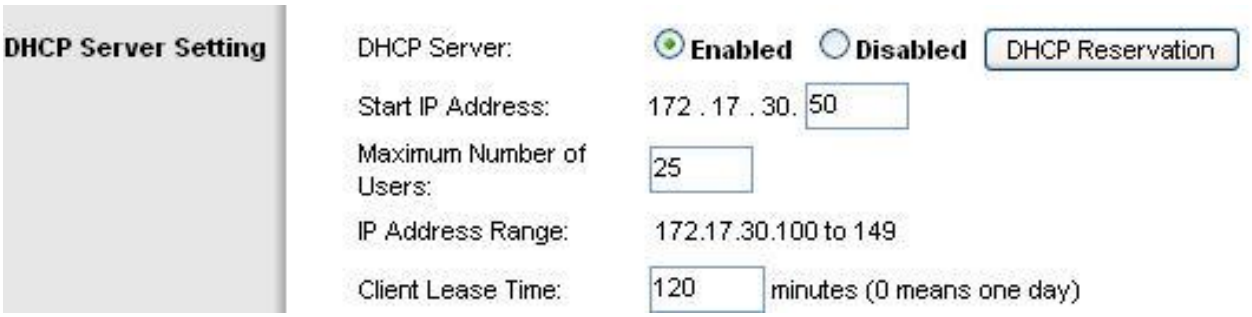


Paso 3: Verificar el cambio de dirección IP estática.

Dado que ya tenemos una dirección IP de DHCP, no vamos a obtener la nueva dirección, 172.17.30.26, hasta que nos reconectemos. Esperaremos, observaremos y verificaremos, más adelante en la Tarea 6, Paso 5, que este cambio se ha hecho.

Paso 4: Configurar el servidor DHCP.

Establezca la dirección de inicio en 50, el número máximo de usuarios en 25, y el tiempo de alquiler en 2 horas (o 120 minutos).

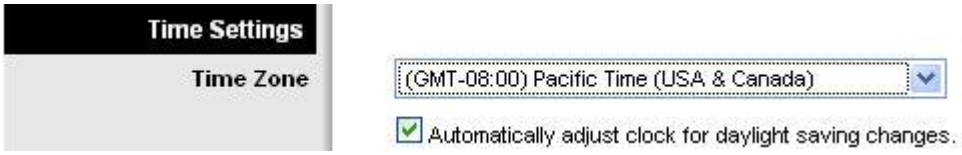


Estas configuraciones dan a cualquier PC que se conecte a este router solicitando inalámbricamente una dirección IP mediante DCHP, una dirección entre 172.17.30.50 y 74. Sólo 25 clientes al mismo tiempo pueden obtener una dirección IP y tener la dirección IP por dos horas, después de las cuales deben solicitar una nueva.

Nota: El rango de direcciones IP no se actualiza hasta que haga clic en **Guardar configuraciones**.

Paso 5: Configurar el router al huso horario apropiado.

En la parte inferior de la página Configuraciones básicas, cambie el huso horario del router para reflejar su ubicación.

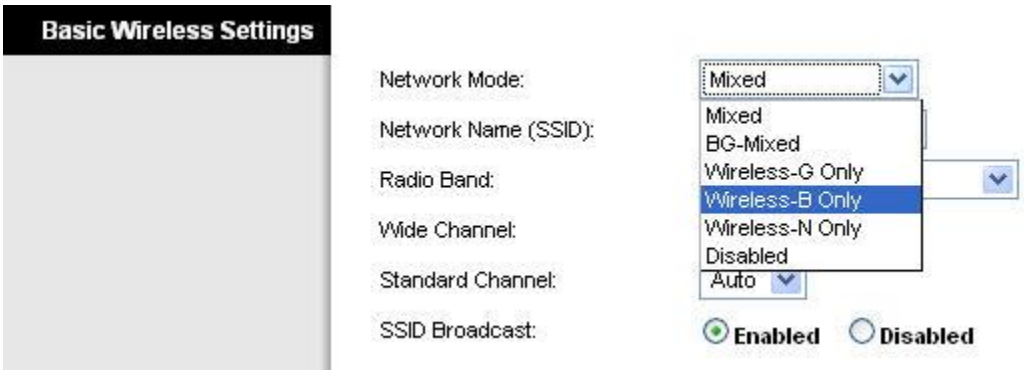


Paso 6: ¡Guarde sus configuraciones!

Tarea 7: Configuraciones inalámbricas básicas

Paso 1: Establecer el modo de red.

Linksys WRT300N permite elegir en qué modo de red operar. Actualmente el modo de red para clientes más utilizado es Wireless-G y para los routers es BG-Mixed. Cuando un router opera en BG-Mixed puede aceptar clientes B y G. Sin embargo, si un cliente B se conecta, el router debe descender al nivel más lento de B. Para esta práctica de laboratorio, se asume que todos los clientes están ejecutando B solamente, por lo tanto debe elegir Sólo inalámbrica-B.



Paso 2: Establecer otras configuracinoes.

Cambie el Nombre de red SSID a WRS3, el Canal estándar a 6 – 2.457 GHZ, y deshabilite el Broadcast de SSID.

¿Por qué es bueno cambiar el canal inalámbrico a uno diferente al predeterminado?

_____

_____

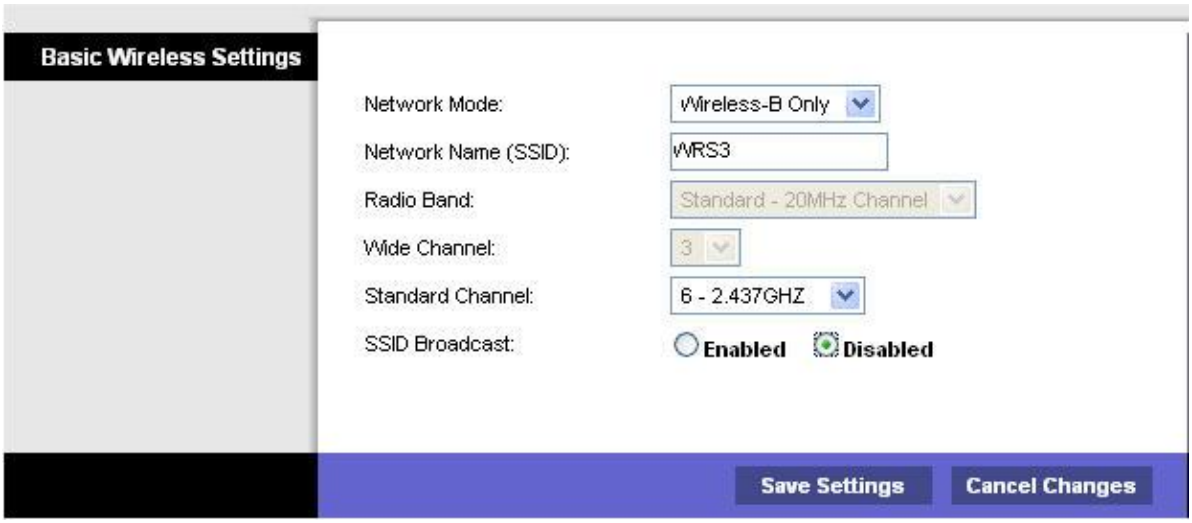
Para ayudar a evitar interferencia de otros routers inalámbricos

¿Por qué se recomienda deshabilitar el broadcast de SSID?

_____

_____

Esto permite una medida de seguridad. Toda persona que quiera conectarse al router necesita como mínimo conocer el SSID antes de poder conectarse.



Paso 3: Haga clic en Guardar configuraciones.

Paso 4: Verificar si el SSID del router ya no está siendo broadcast.

Busque redes inalámbricas, como se hizo en la Tarea 3, Paso 1. ¿Aparece el SSID del router inalámbrico?

_____

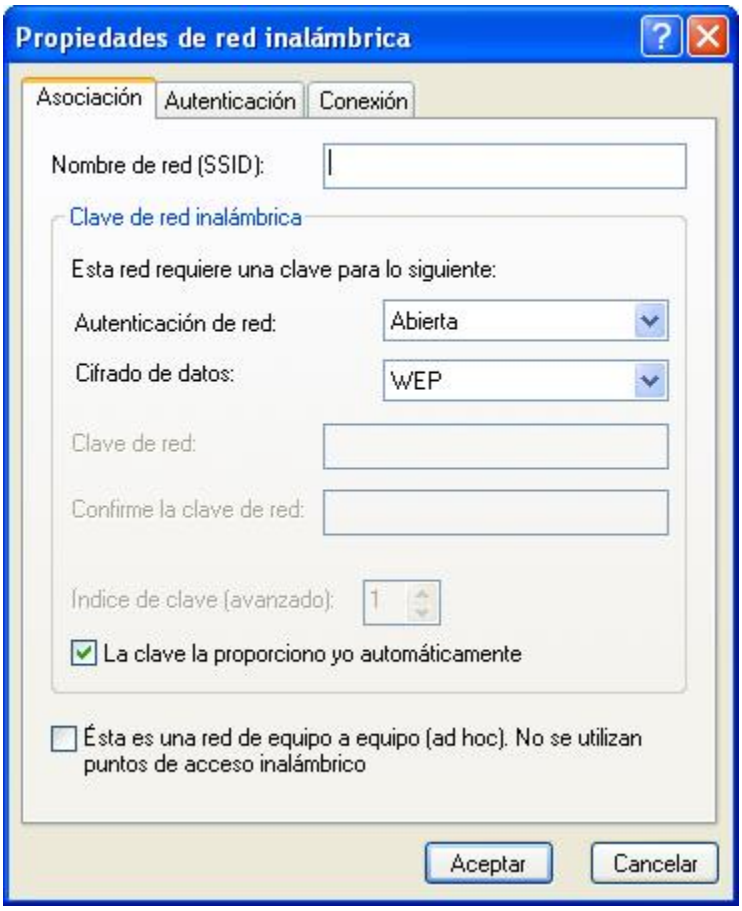
No

Paso 5: Reconectar a la red inalámbrica.

Navegue a **Inicio > Panel de control > Conexiones de red**, haga clic con el botón derecho en el ícono Conexión de red inalámbrica y seleccione Propiedades.

En la ficha Redes inalámbricas seleccione **Agregar**.

En la ficha Asociación, ingrese WR33 como el SSID y establezca la encriptación de datos como Deshabilitada. Seleccione Aceptar, y vuelva a seleccionar Aceptar. Windows intentará ahora reconectarse al router inalámbrico.



Paso 6: Verificar las configuraciones.

Ahora que se ha reconectado a la red, tiene las nuevas configuraciones DHCP que configuró en la Tare 5, Paso 3. Verifique esto en la petición de comandos con el comando **ipconfig**.

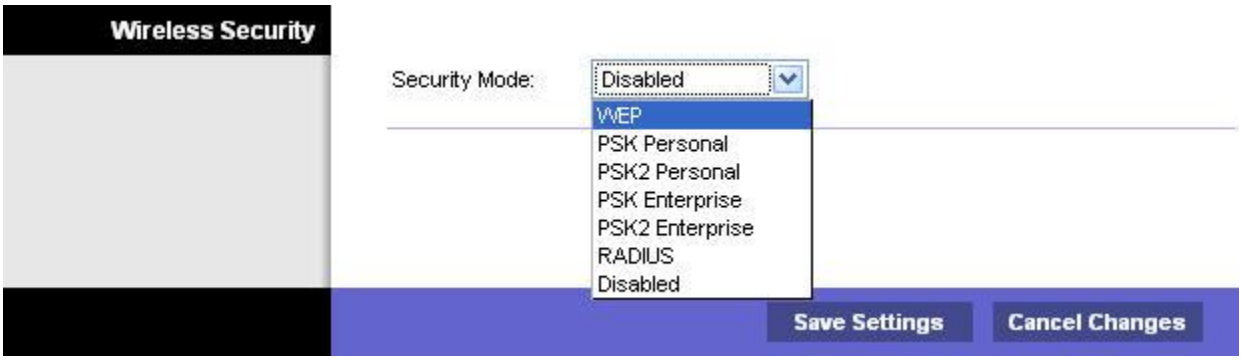
```
Dirección IP. . . . . . . . . . . . : 172.17.30.26
Máscara de subred . . . . . . . . . : 255.255.255.0
Puerta de enlace predeterminada     : 172.17.30.1
```

Tarea 8: Habilitar la seguridad inalámbrica

Paso 1: Reconectarse a la página de configuración del router (http://172.17.30.1).

Paso 2: Navegar a la página Inalámbrica y seleccionar la ficha Seguridad inalámbrica.

Paso 3: Seleccionar WEP en el modo de seguridad.



Paso 4: Ingresar una clave WEP.

Una red es tan segura como su punto más débil, y un router inalámbrico es un lugar muy conveniente para comenzar si alguien quiere dañar su red. Al no difundir el SSID y requerir una clave WEP para conectarse al router, está agregando cierto grado de seguridad.

Desafortunadamente existen herramientas que pueden descubrir redes que ni siquiera están difundiendo sus SSID, e incluso hay herramientas que pueden descifrar la encriptación de clave WEP. Formas más sólidas de seguridad inalámbrica son WPA y WPA-2, que actualmente no están admitidas por este router. Los filtros inalámbricos MAC son más seguros pero a veces un medio poco práctico de proporcionar seguridad a su red. Esto se aborda en la tarea siguiente.

Agregue la clave WEP 1234567890.

Paso 5: Guardar sus configuraciones.

Se desconectará de la red.

Paso 6: Configurar Windows para usar autenticación WEP.

Navegue otra vez a la página Conexiones de redes y haga clic con el botón derecho en el ícono **Conexión inalámbrica de red**. En la ficha Redes inalámbricas, localice la red WRS3 y haga clic en **Propiedades**.

- Establezca la encriptación de datos en WEP.
- Desmarque Me ha sido otorgada esta clave.
- Ingrese la clave de red 1234567890, como se configuró antes en el router.
- Haga clic en Aceptar y en Aceptar.

Windows debe ahora reconectarse a la red.

Tarea 9: Configurar un filtro inalámbrico MAC.

Paso 1: Agregar un filtro MAC.

- Vuelva a navegar en la página de utilidad web del router (http://172.17.30.1).
- Navegue a la sección Inalámbrica y luego a la ficha Filtro inalámbrico de MAC.
- Marque Habilitado.
- Seleccione **No permitir que las PC listadas debajo tengan acceso a la red inalámbrica**.
- Ingrese la dirección MAC 00:05:4E:49:64:87.

Esto evita que cualquier cliente con la dirección MAC 00:05:4E:49:64:87 pueda acceder a la red inalámbrica.

Paso 2: **Hacer clic en Lista de clientes inalámbricos**.

La **Lista de clientes inalámbricos** muestra a todo el que se encuentre actualmente conectado al router mediante una conexión inalámbrica. Tenga también en cuenta la opción **Guardar en la lista de filtros MAC**. Marcar esta opción agrega automáticamente la dirección MAC de ese cliente la la lista de direcciones MAC para evitar o permitir el acceso a la red inalámbrica.

¿Cuál es una manera extremadamente sólida de permitir que se conecten a la red inalámbrica solamente los clientes que usted ha elegido?

_____

_____

Puede establecer la Restricción de acceso en Permitir, que permite solamente a las direcciones MAC listadas en la tabla conectarse inalámbricamente.

¿Por qué esto no es factible en las redes grandes?

_____

_____

Se tiene que ingresar manualmente cada dirección MAC.

¿Cuál es una forma conveniente de agregar direcciones MAC si aquéllos a quienes deseaba permitir el acceso ya están conectados a la red inalámbrica?

_____

_____

Puede simplemente ir a la Lista de clientes inalámbricos y marcar Guardar en la lista de filtro MAC.

Tarea 10: Establecer restricciones de acceso

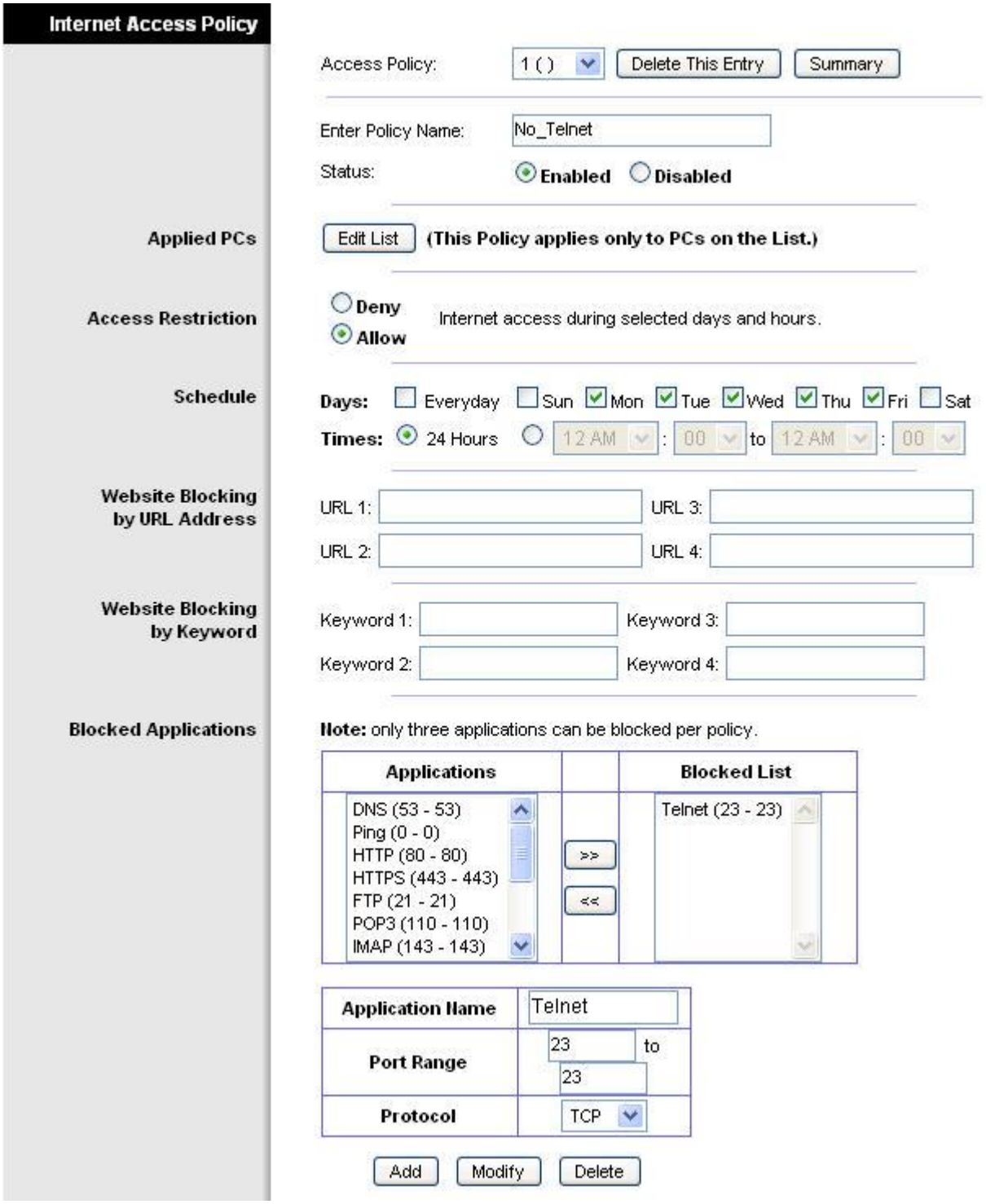
Configure una restricción de acceso que impida acceso Telnet de lunes a viernes a los usuarios que obtengan una dirección DHCP desde el conjunto predeterminado (172.17.30.50 – 74).

Paso 1: Navegar a la ficha Restricciones de acceso.

En la ficha Restricciones de acceso, establezca lo siguiente:

- Nombre de la directiva: No_Telnet
- Estado: Habilitado

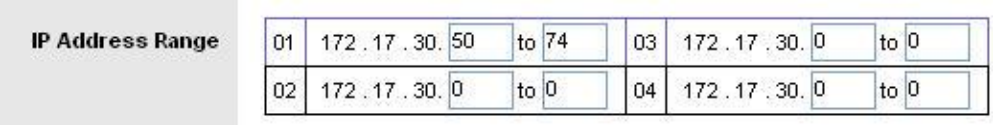
- Acceso a Internet: Permitir
- Días: Marcar lunes a viernes
- Lista bloqueada: Agregar Telnet



Paso 2: Establecer el rango de direcciones IP.

Aplique esta configuración a todos los que usan una dirección DHCP predeterminada en el rango de 172.17.30.50 – 74.172.17.30.50 – 74.

Haga clic en el botón **Editar Lista** en la parte superior de la ventana e ingrese el rango de direcciones IP. Guarde las configuraciones.



Guarde las configuraciones de restricción de acceso

Tarea 11: Administrar y asegurar la utilidad web del router

Paso 1: Configurar el acceso web.

Navegue a la sección **Administración**. Cambie la contraseña del router a **cisco**.

En **Acceso a utilidad web**, seleccione HTTP y HTTPS. Seleccionar acceso HTTPS permite al administrador de red manejar el router mediante https://172.17.30.1 con SSL, una forma más segura de HTTP. Si elige hacer esto en la práctica de laboratorio, tendrá que aceptar certificados.

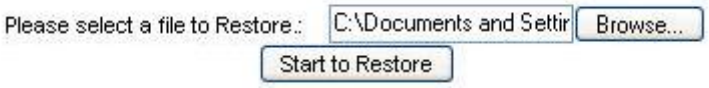
Para **Acceso a la utilidad web por vía inalámbrica,** seleccione Habilitado. Si deshabilita esta opción, la utilidad web no estaría disponible a los clientes conectados inalámbricamente. Deshabilitar el acceso es otra forma de seguridad porque requiere que el usuario esté conectado directamente al router antes de cambiar las configuraciones. Sin embargo, en este escenario de práctica de laboratorio está configurando el router mediante acceso inalámbrico, así que deshabilitar no sería una buena idea.

Haga ahora una copia de respaldo de su configuración haciendo clic en el botón **Configuraciones de copia de respaldo**. Cuando se le requiera, guarde el archive en su escritorio.

Paso 2: Restaurar su configuración.

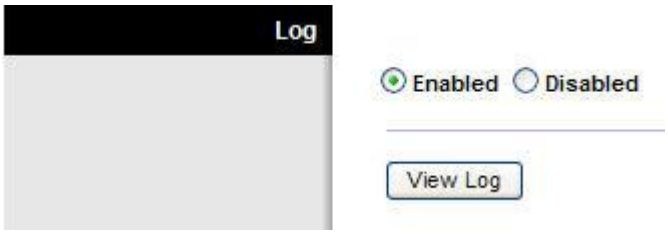
Si sus configuraciones se cambian o borran accidental o intencionalmente, puede restaurarlas de una configuración en uso utilizando la opción **Restaurar configuraciones** que se encuentra en la sección de Realizar una copia de seguridad y restaurar.

Ahora haga clic en el botón **Restaurar Configuración**. En la ventana Restaurar Configuraciones, busque el archivo de configuración que guardó anteriormente. Haga clic en el botón **Comenzar a restaurar**. Sus configuraciones previas deben haberse restaurado con éxito.



Paso 3: Habilitar registro.

Navegue a la ficha **Registro** y habilite el registro. Ahora puede ver el registro del router.



Paso 4: Guardar sus configuraciones y finalizar su conexión inalámbrica al router.

Paso 5: Conectar un cable Ethernet en uno de los puertos inalámbricos LAN del router y conectarse a él.

Paso 6: Navegar a la Web GUI del router.

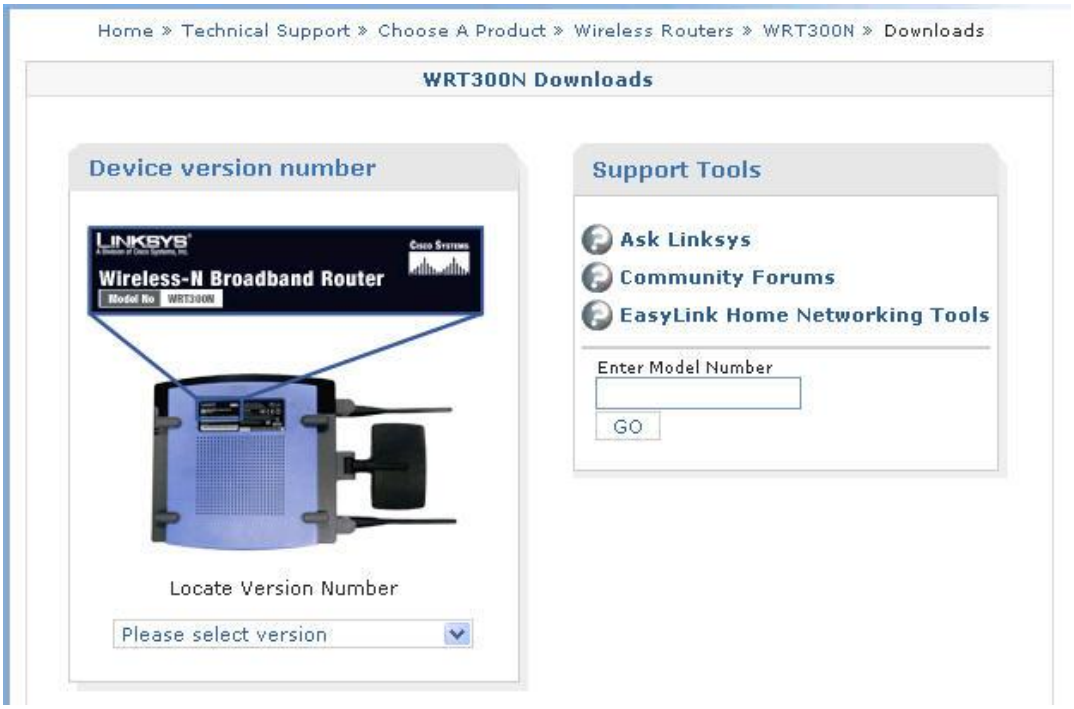
Paso 7: Navegar a la sección Administración.

Paso 8: Actualizar el firmware.

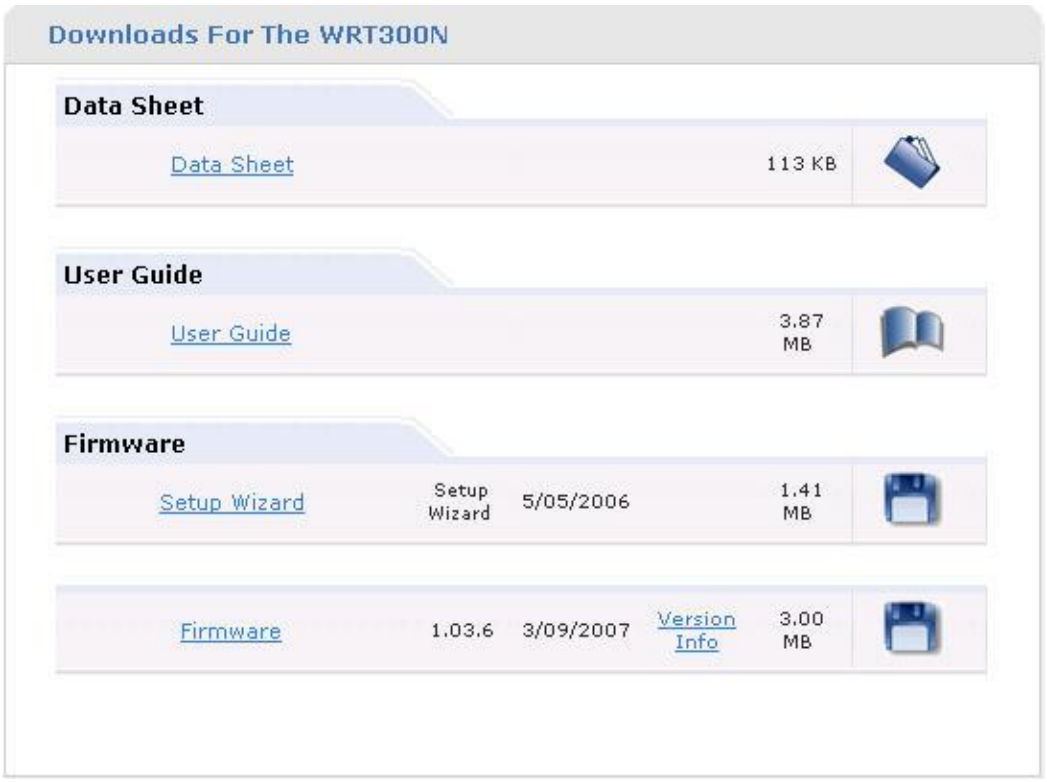
Vaya a

http://www.linksys.com/servlet/Satellite?c=L_CASupport_C2&childpagename=US%2FLayout&cid=1166859841746&pagename=Linksys%2FCommon%2FVisitorWrapper&lid=4174637314B274&displaypage=download

Seleccione la versión de su router. Las instrucciones para identificar la versión se encuentran en el sitio web de Linksys.



Haga clic en **Firmware** o en el ícono guardar. Si se lo solicita, guarde el archivo en el disco.



Antes de realizar la mejora, fíjese en la versión del firmware en la esquina superior derecha.

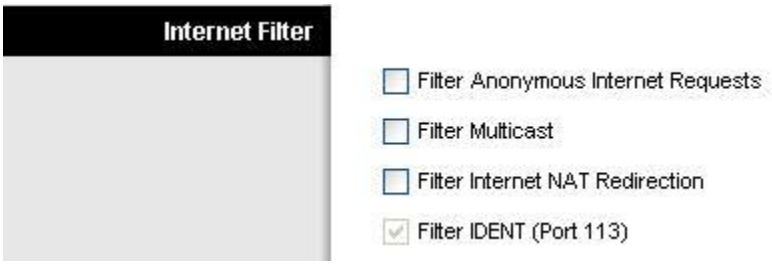
Navegue a la sección **Administración**. Haga clic en **Actualizar firmware**. Busque el archivo que acaba de descargar. Haga clic en **Comenzar a actualizar**. La actualización no debe interrumpirse, por lo tanto asegúrese de no apagar el dispositivo.

Cuando esté completa, verifique la nueva versión del firmware en su dispositivo.

Tarea 12: Crear y verificar conectividad completa

Paso 1: Filtrar las solicitudes anónimas de Internet.

En la sección **Seguridad**, desmarque **Filtrar las solicitudes anónimas de Internet**. Deshabilitar esta opción le permite hacer ping a la dirección IP interna de la LAN/inalámbrica, 172.17.30.1, desde los lugares conectados a su puerto WAN.



Paso 2: Deshabilitar NAT.

En la sección **Configuración**, haga clic en la ficha **Enrutamiento avanzado**. Deshabilite NAT.

Paso 3: Conectar a WRS2.

Establezca las configuraciones de las direcciones IP para la configuración de Internet.

- 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 a la dirección IP de la Fa 0/1 VLAN 88 de R1, 172.17.88.1

Establezca la dirección IP de configuración de la red en 172.17.30.1

Vincule estáticamente la dirección MAC de la PC3 con la dirección DHCP 172.17.40.23 (ayuda: Tarea 6, Paso 2).

Cambie el SSID inalámbrico a WRS2 (ayuda: Tarea 7, Paso 2).

Paso 4: Dar a R1 rutas estáticas a las redes 172.17.30.0 y 172.17.40.0.

```
R1config)#ip route 172.17.30.0 255.255.255.0 172.17.88.35
R1(config)#ip route 172.17.40.0 255.255.255.0 172.17.88.25
```

Paso 5: Repetir los pasos 1 y 2 anteriores para WRS2.

Paso 6: Verificar la conectividad.

Verifique que R1 tenga rutas a las PC3 y PC6 y que pueda hacer ping a las mismas con éxito.

```
R1#sh ip route
<output deleted>

Gateway of last resort is not set

     172.17.0.0/24 is subnetted, 5 subnets
S       172.17.40.0 [1/0] via 172.17.88.25
S       172.17.30.0 [1/0] via 172.17.88.35
C       172.17.20.0 is directly connected, FastEthernet0/1.20
C       172.17.10.0 is directly connected, FastEthernet0/1.10
C       172.17.88.0 is directly connected, FastEthernet0/1.88
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback0
```

```
R1#ping 172.17.30.26

Escriba escape sequence para abortar.
Sending 5, 100-byte ICMP Echos to 172.17.30.26, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

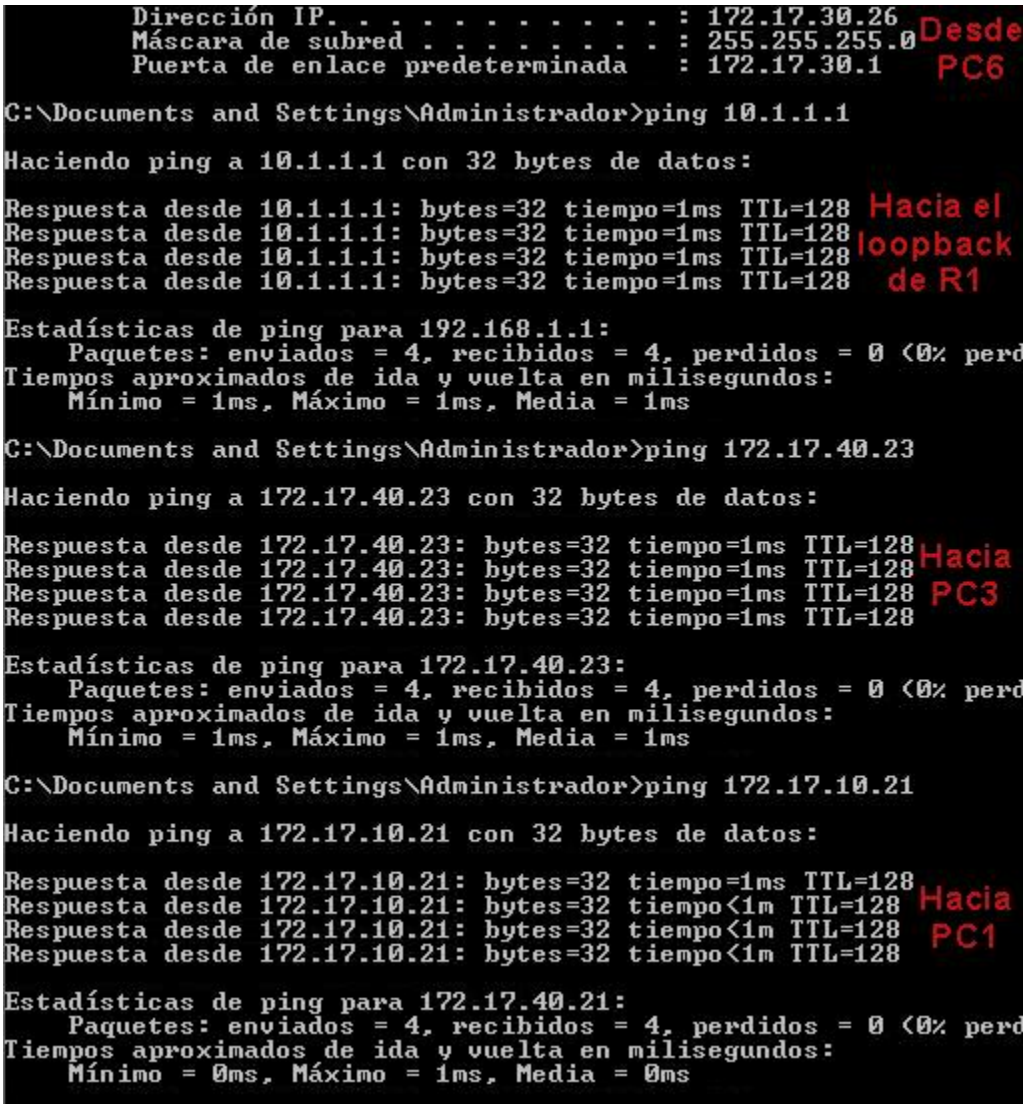
```
R1#ping 172.17.40.23

Escriba escape sequence para abortar.
Sending 5, 100-byte ICMP Echos to 172.17.40.23, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Verifique que la PC3 y la PC6 puedan hacer ping al loopback de R1.

Verifique que la PC3 y la PC6 puedan hacer ping entre sí.

Verifique que la PC3 y la PC6 puedan hacer ping a PC1 y PC2.



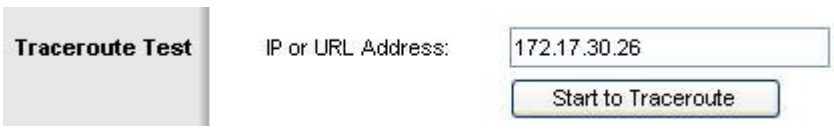
Tarea 13: Configurar la eficiencia del enrutamiento

Paso 1: Utilizar Traceroute para ver la conexión de red.

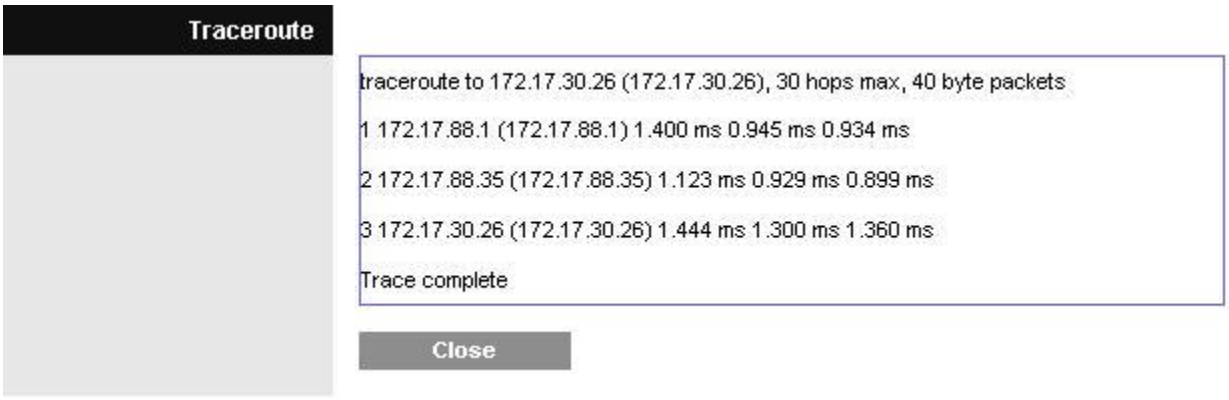
Puesto que R1 es la gateway predeterminada, el router Linksys va a R1 para llegar a una red a la que no sabe cómo llegar, incluyendo los clientes de los otros routers Linksys.

Un paquete de la PC3 alcanza primero su gateway predeterminada de 172.17.40.1, entonces es enviado desde la interfaz WAN WRS2 de 172.17.88.25 hacia la gateway predeterminada de WRS2 (172.17.88.1). Desde allí, R1 envía el paquete a la interfaz WAN WRS3, 172.17.88.35, donde WRS3 lo gestiona.

Puede verificar esto en la ficha **Diagnóstico** en la sección Administración. En el campo Prueba de Traceroute, ingrese la dirección IP de PC6 a PC6, 172.17.30.26



Ahora haga clic en Iniciar Traceroute; aparecerá elemento emergente.

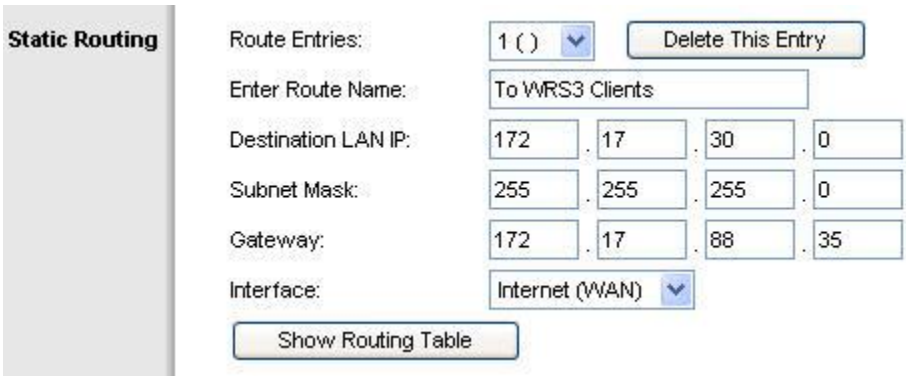


Si WRS2 supiera que puede ir a la red 172.17.30.0 desde la 172.17.88.35, lo enviaría directamente a esa dirección IP. ¡Avisémosle!

Paso 2: Configurar una nueva ruta.

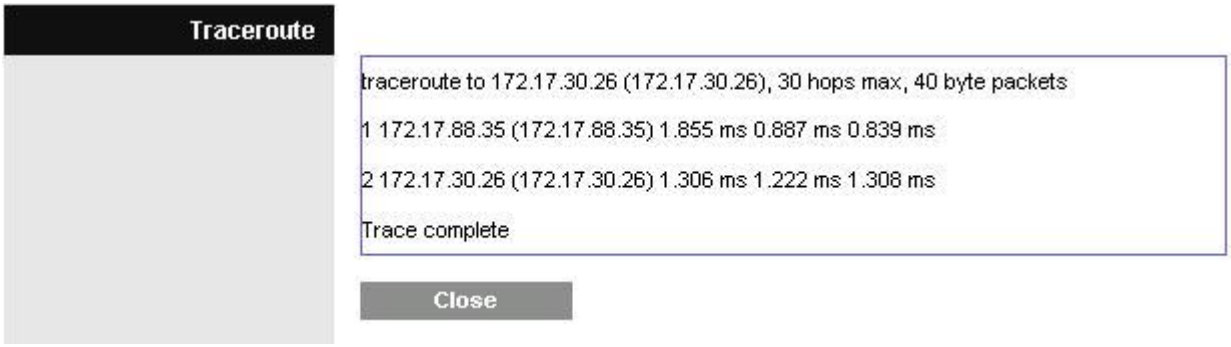
En la sección **Configuración**, haga clic en la ficha **Enrutamiento avanzado**. Para el enrutamiento estático, ingrese las siguientes configuraciones:

- En el campo **Nombre de ruta**, ingrese a **Clientes WRS2**.
- En **IP de LAN de destino**, ingrese la red detrás de WRS2: 172.17.40.0
- Ingrese una máscara de subred de /24
- Ingrese una gateway de 172.17.88.35
- Establezca la interfaz a Internet (WAN)



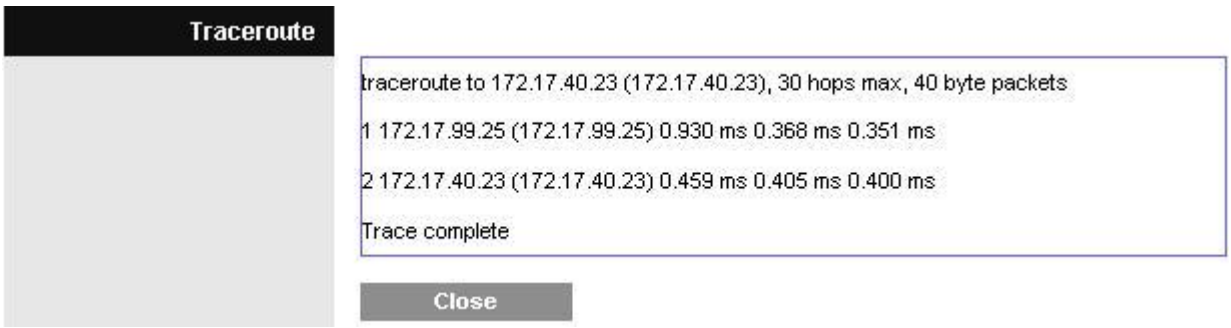
Paso 3: Verificar la nueva ruta.

En la ficha **Diagnóstico** en la sección Administración, reingrese la dirección IP de la PC3 en en campo Verificación de Traceroute. Haga clic en **Iniciar Traceroute** para ver la ruta.



Observe que WRS2 va directamente a WRS3 y nos ahorra el salto extra a R1

Haga lo mismo en WRS3 para la red 172.17.40.0/24, apuntando hacia la interfaz WAN de WRS2, 172.17.88.25.



Tarea 14: Configuración de la seguridad de puerto

Paso 1: Configurar la seguridad de puerto de PC1.

Regístrese en el switch S2. Configure el puerto de switch 11 de la PC1, habilite la seguridad de puerto y habilite las direcciones MAC dinámicas sin modificación.

Paso 2: Configurar la seguridad de puerto de PC2.

Repita el paso 1 para el puerto de switch 18.

S2

```
!
interface FastEthernet 0/11
 switchport mode access
 switchport access vlan 10
 switchport port-security
 switchport port-security mac-address sticky
 no shutdown
!
!
```

```
interface FastEthernet 0/18
 switchport mode access
 switchport access vlan 20
 switchport port-security
 switchport port-security mac-address sticky
 no shutdown
!
```

Paso 3: Generar tráfico en los puertos haciendo ping a PC2 desde PC1.

Paso 4: Verificar la seguridad de puerto.

```
S1#show port-security address
          Secure Mac Address Table
------------------------------------------------------------------------
VLAN    Dirección MAC     Tipo                  Puerto    Tiempo restante
                                                            (mins)
----    -----------       ----                  -----      -------------
  10    0006.5b1e.33fa    SecureSticky          Fa0/11           -
  20    0001.4ac2.22ca    SecureSticky          Fa0/18           -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Total Addresses in System (excluding one mac per port)     : 6272

S1#sh port-security int fa 0/11
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   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0006.5b1e.33fa:10
Security Violation Count   : 0
```

Apéndice

Configuraciones

Nombre de host de R1

```
!
enable secret class
!
no ip domain lookup
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.0
!
interface FastEthernet0/1
 no shutdown
!
interface FastEthernet0/1.10
```

```
 encapsulation dot1Q 10
 ip address 172.17.10.1 255.255.255.0
!
interface FastEthernet0/1.20
 encapsulation dot1Q 20
 ip address 172.17.20.1 255.255.255.0
!
interface FastEthernet0/1.88
 encapsulation dot1Q 88
 ip address 172.17.88.1 255.255.255.0
!
!
ip route 172.17.30.0 255.255.255.0 172.17.88.35
ip route 172.17.40.0 255.255.255.0 172.17.88.25
!
!
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
 password cisco
line aux 0
line vty 0 4
!
!
end
```

Nombre de host del S1

```
!
!
vtp mode transparent
!
!
vlan 10,20,88
!
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```

```
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
end
```

Nombre de host de S2

```
!
!
vtp mode transparent
!
vlan 10,20,88
!
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/7
 switchport mode access
 switchport access vlan 88
!
!
! PC1 and PC2's MAC address will appear after 'sticky' on ports 11
! and 18 respectively, after traffic traverses them
!
!

interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky
!
interface FastEthernet0/18
 switchport access vlan 20
```

```
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
end
```

Nombre de host del S3

```
!
vtp mode transparent
!
vlan 10,20,88
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/7
 switchport mode access
 switchport access vlan 88
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
!
end
```

Práctica de laboratorio 7.5.3: Resolución de problemas de la configuración inalámbrica (Versión para el instructor)

Diagrama de topología

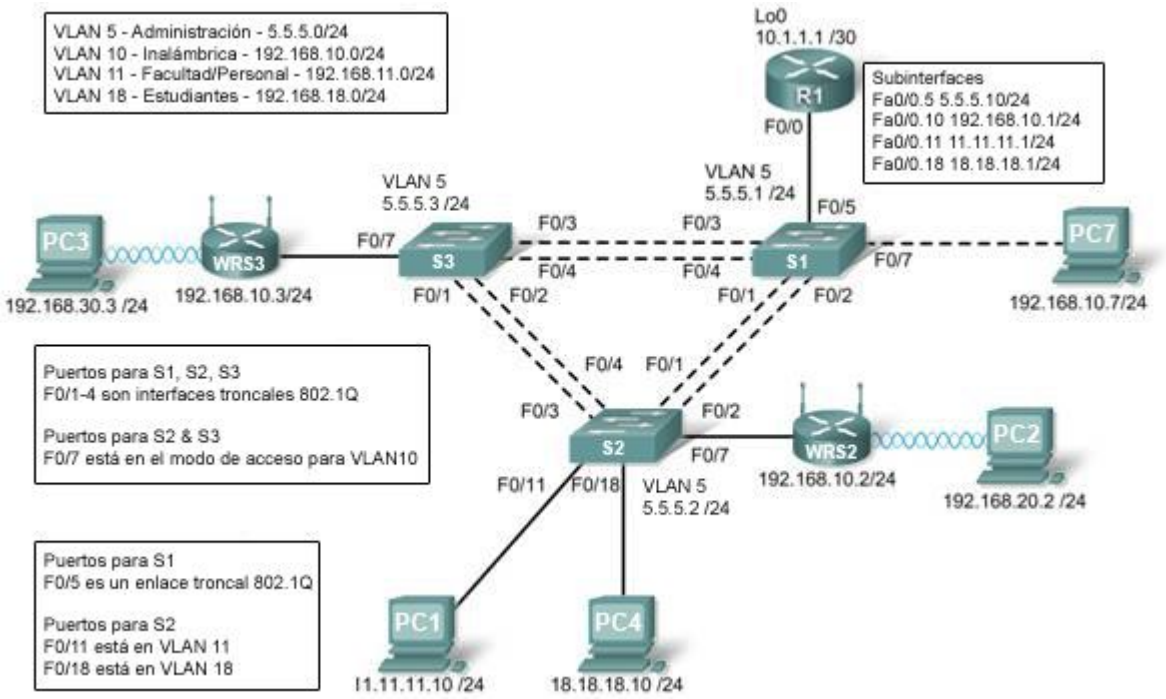


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
R1	**Fa0/1.5**	5.5.5.10	255.255.255.0	No aplicable
	Fa0/1.10	192.168.10.1	255.255.255.0	No aplicable
	Fa0/1.11	11.11.11.1	255.255.255.0	No aplicable
	Fa0/1.18	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

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

Escenario

En esta práctica de laboratorio, una red básica y una red inalámbrica están mal configuradas. Debe encontrar y corregir las configuraciones incorrectas basándose en las especificaciones mínimas de red provistas por su compañía.

Aquí están las configuraciones para que las cargue en su router y switches.

[Nota para el instructor: Las configuraciones que faltan están en rojo y las configuraciones incorrectas están ~~tachadas con rojo~~]

Configuración de R1

```
hostname R1
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.0
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 no shutdown
!
interface FastEthernet0/1,5
 encapsulation dot1Q 5
 ip address 5.5.5.10 255.255.255.0
!
interface FastEthernet0/1,10
 encapsulation dot1Q 10
 ip address 192.168.11.1 255.255.255.0
 ip address 192.168.10.1 255.255.255.0
!
interface FastEthernet0/1,11
 encapsulation dot1Q 11
 ip address 11.11.11.1 255.255.255.0
!
interface FastEthernet0/1,18
 encapsulation dot1Q 18
 ip address 18.18.18.1 255.255.255.0
!
ip route 192.168.20.0 255.255.255.0 192.168.10.2
ip route 192.168.30.0 255.255.255.0 192.168.10.3
ip route 192.168.20.0 255.255.255.0 192.168.10.3
ip route 192.168.30.0 255.255.255.0 192.168.10.2
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
```

```
end
```

Configuración del switch 1

```
hostname S1
!
vtp mode transparent
!
vlan 5,10-11
vlan 18
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11,18
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11,18
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11,18
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11,18
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan5
 ip address 5.5.5.1 255.255.255.0
 no shutdown
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
End
```

Configuración del switch 2

```
hostname S2
!
vtp mode transparent
ip subnet-zero
!
vlan 5,10-11,18
!
```

```
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11,18
 switchport mode access
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11,18
 switchport mode access
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11,18
 switchport mode access
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11,18
 switchport mode access
 switchport mode trunk
!
interface FastEthernet0/7
switchport trunk encapsulation dot1q
 switchport trunk native vlan 10
 switchport mode trunk
!
interface FastEthernet0/11
 switchport access vlan 11
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky
!!! Nota: Aunque esto puede aparecer en la configuración activa después
de haber configurado la seguridad de puerto de direcciones mac fijas, se
negará el acceso a las PC1 y PC4, a menos que tengan esas direcciones.
El estudiante debe borrar esas direcciones fijas predeterminadas
incorrectamente y hacer que el switch descubra adecuada y dinámicamente
las direcciones de PC1 y PC4.
!
interface FastEthernet0/18
 switchport access vlan 18
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 022e.ab13.22fb
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan5
 ip address 5.5.5.2 255.255.255.0
 no shutdown
```

```
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
End
```

Configuración del switch 3

```
hostname S3
!
vtp mode transparent
!
vlan 5,10-11,18
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11,18
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11,18
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11,18
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11,18
 switchport mode trunk
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 11
 switchport mode trunk
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan5
 ip address 6.6.6.3 255.255.255.0
 ip address 5.5.5.3 255.255.255.0
 no shutdown
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
```

```
end
```

Requisitos de la red de router inalámbrico

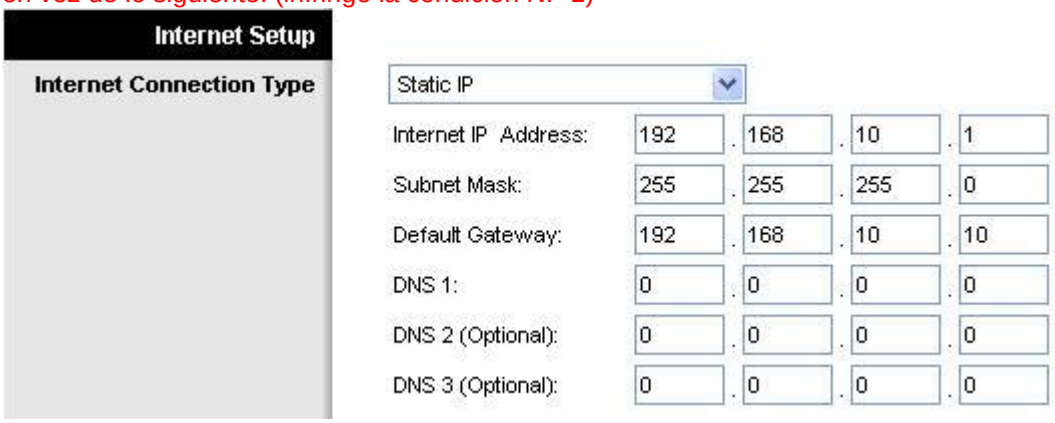
Mientras realiza el diagnóstico de fallas en WRS2 y WRS3, asegúrese que existan al menos las siguientes capacidades:

1. Conexiones a través de direcciones IP indicadas en el diagrama de topología.
2. Más de 30 clientes puedan obtener una dirección IP a través de DHCP al mismo tiempo.
3. Un cliente pueda tener una dirección DHCP por al menos dos horas.
4. Los clientes que estén usando los modos de red inalámbrica B y G puedan conectarse, pero que no puedan los clientes N.
5. Los clientes inalámbricos deben autenticarse utilizando WEP con la clave 5655545251.
6. El tráfico entre PC2 y PC3 debe tomar la ruta más eficiente posible.
7. Las solicitudes de ping que vengan de puertos WAN fuera de los routers Linksys a las direcciones IP internas de LAN/inalámbricas (192.168.30.1) deben tener éxito.
8. DHCP no debe dar direcciones IP en un rango que incluya las direcciones para PC2 y PC3.
9. Las dos redes inalámbricas no deben interferir entre sí.

Solución de red inalámbrica

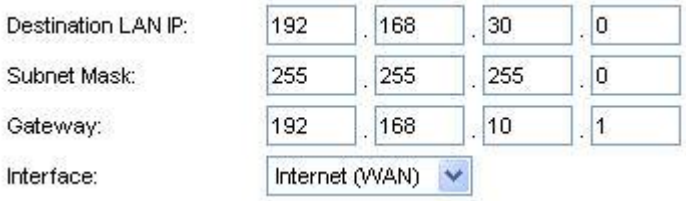
Errores en WRS2

WRS2 debe tener la dirección IP de 192.168.10.2 y una gateway predeterminada de 192.168.10.1, en vez de lo siguiente: (infringe la condición N.º 1)

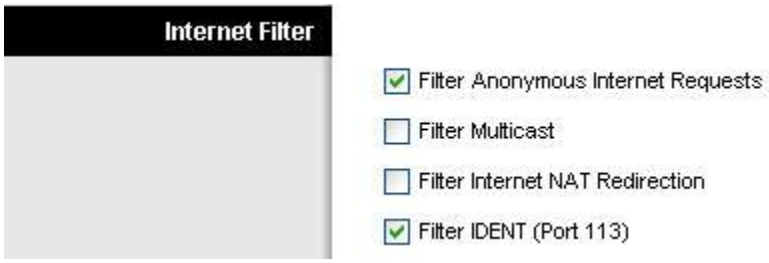


DHCP está configurada para dar direcciones en el rango de 192.168.20.2 – 65. La dirección 20.2 de la PC2 cae dentro de este rango. Aunque DHCP ha reservado la dirección 20.2 y no va a darla vía DHCP a ninguna computadora que no sea PC2, es una optimización dar direcciones solamente en un rango no utilizado. Cambiar la dirección IP de inicio a encima de 20.2 elude este problema. (infringe la condición N.º 8)

En la ficha **Enrutamiento avanzado,** la ruta estática a los clientes WRS3 está configurada incorrectamente. La gateway de 192.168.10.1 es la ruta ineficiente que tratamos de evitar. En lugar de apuntar hacia R1, la ruta estática debe apuntar directamente a WRS3 con la dirección IP 192.168.10.3. Cambie la **Gateway a** esta dirección: (No hacerlo infringe la condición N.º 6)

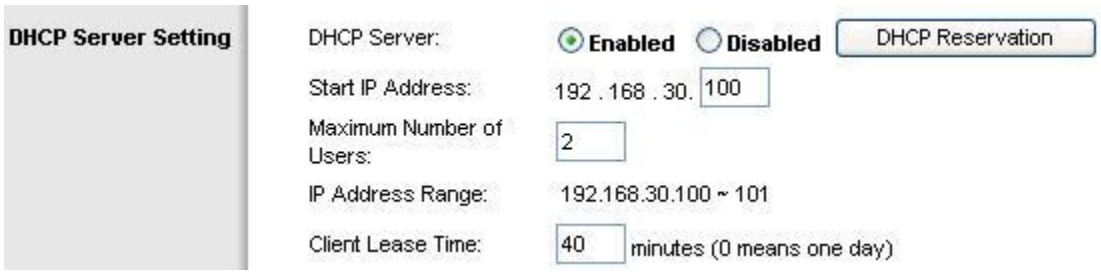


En la ficha **Seguridad,** Filtrar solicitudes anónimas de Internet debe desmarcarse si se quiere que los pings procedentes de fuera de la red LAN/inalámbrica del router a 192.168.20.1 tengan éxito. Asegúrese de que se esté desmarcada. (infringe la condición N.º 7)



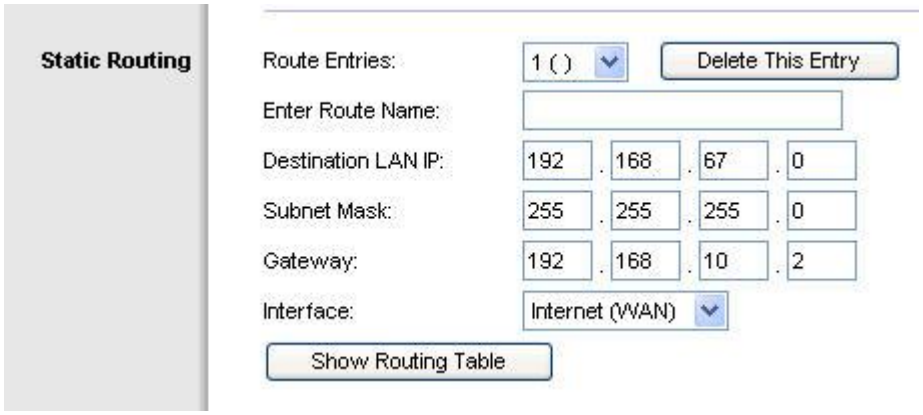
Errores en WRS2

DHCP está configurada para dar solamente dos direcciones IP a la vez y por solamente 40 minutos. (infringe las condiciones N.º 2 y N.º 3)



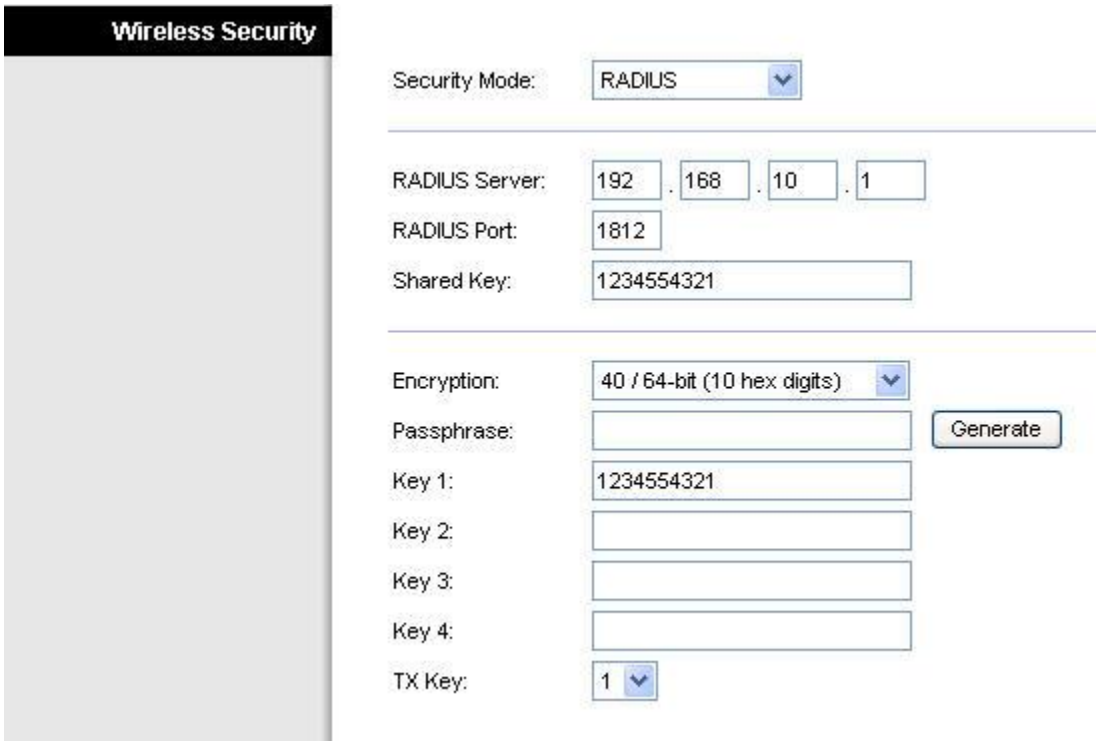
Cambie el **Número máximo de usuarios** a al menos 30 y el **Tiempo de alquiler del cliente** a al menos 120 minutos.

En la ficha **Enrutamiento avanzado,** la ruta estática que está configurada para enrutar eficientemente entre WRS2 y WRS3 es incorrecta. (infringe la condición N.º 6)



En vez de que el destino sea 192.168.67.0, debe ser 192.168.30.0.

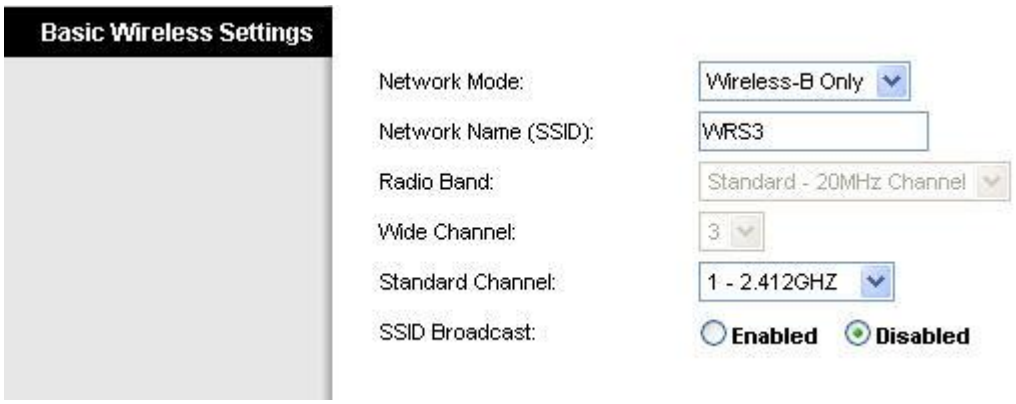
En la ficha **Seguridad inalámbrica**, la autenticación vía RADIUS está configurada, pero se supone que los clientes deben autenticar a través de WEP. (infringe la condición N.º 5)



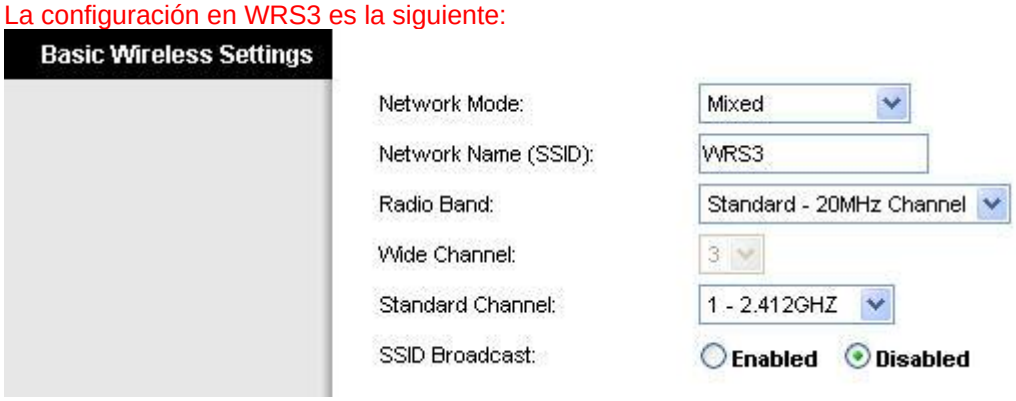
Cambie el **Modo de seguridad** a WEP y utilice la clave 5655545251.

Problemas de conectividad inalámbrica

Las condiciones 4 y 9 requieren el modo de red inalámbrica de B/G en canales sin superposición. La configuración en WRS2 es la siguiente:



La configuración en WRS3 es la siguiente:



Cambie el modo de red en ambos routers a B/G y asegúrese de que los canales no se superpongan, por ejemplo, uno podría estar en el canal 1 y el otro en el canal 6.