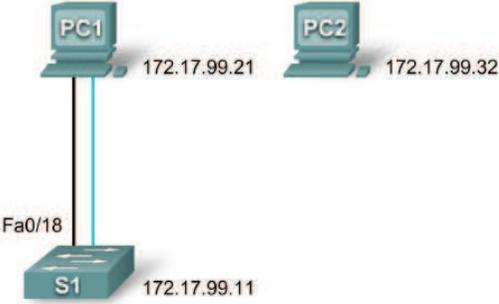


Unidad de aprendizaje:	Administración de redes de área local virtuales.	Número:	3
Práctica	Configuración básica de un switch y Administra el Sistema Operativo (IOS) del switch siguiendo procedimiento.	Número:	9
Propósito de la práctica	Crear una configuración básica de switch, que incluya un nombre y una dirección IP siguiendo procedimiento, para su operación.		
Escenario	Laboratorio de informática	Duración	2 hrs.
Materiales, Herramientas, Instrumental, Maquinaria y Equipo.		Desempeños	
2 Estaciones de trabajo 1 switch. 1 cables directo. 1 cable de consola.		<ul style="list-style-type: none"> • Aplica las siguientes medidas de seguridad e higiene en el desarrollo de la práctica: <ul style="list-style-type: none"> - Evita la manipulación de comida o líquidos cerca del equipo de cómputo - No introduce objetos extraños en las entradas físicas de dispositivos de la computadora - No utiliza imanes cerca de discos compactos, memorias extraíbles ó de la computadora - Limpia el área de trabajo, prepara herramientas y los materiales a utilizar ↳ Utilizar las hojas por ambas caras y colocar las de desecho las en el recipiente destinado para su posterior envío a reciclaje <p>NOTA El docente deberá adecuar la práctica al equipo y recursos de software con el que se cuenta.</p> <p>Topología</p> 	

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños																				
	<p>Tabla de direccionamiento</p> <table border="1" data-bbox="981 363 1854 571"> <thead> <tr> <th>Dispositivo</th> <th>Interfaz</th> <th>Dirección IP</th> <th>Máscara de subred</th> <th>Gateway predeterminado</th> </tr> </thead> <tbody> <tr> <td>PC1</td> <td>NIC</td> <td>172.17.99.21</td> <td>255.255.255.0</td> <td>172.17.99.1</td> </tr> <tr> <td>PC2</td> <td>NIC</td> <td>172.17.99.32</td> <td>255.255.255.0</td> <td>172.17.99.1</td> </tr> <tr> <td>S1</td> <td>VLAN99</td> <td>172.17.99.11</td> <td>255.255.255.0</td> <td>172.17.99.1</td> </tr> </tbody> </table> <p>Situación</p> <p>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.</p> <p>Tarea 1: Cablear, borrar y cargar nuevamente el switch</p> <p>Paso 1: Conecte una red.</p> <p>Conectar una red que sea similar a la del 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.</p> <p>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.</p> <p>Nota: PC2 no se encuentra conectada inicialmente al switch. Sólo se utiliza en la tarea 5.</p> <p>Paso 2: Borre la configuración en cada switch.</p> <p>Borre la configuración en el switch utilizando el procedimiento del Apéndice 1.</p>	Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado	PC1	NIC	172.17.99.21	255.255.255.0	172.17.99.1	PC2	NIC	172.17.99.32	255.255.255.0	172.17.99.1	S1	VLAN99	172.17.99.11	255.255.255.0	172.17.99.1
Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado																	
PC1	NIC	172.17.99.21	255.255.255.0	172.17.99.1																	
PC2	NIC	172.17.99.32	255.255.255.0	172.17.99.1																	
S1	VLAN99	172.17.99.11	255.255.255.0	172.17.99.1																	

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Tarea 2: Verificar la configuración predeterminada de un switch</p> <p>Paso 1: Entre al modo privilegiado.</p> <p>Puede acceder a todos los comandos del switch en modo privilegiado. Sin embargo, debido a que muchos de los comandos privilegiados configuran parámetros operativos, el acceso privilegiado se debe proteger con una contraseña para evitar el uso no autorizado. Establecerá contraseñas en la Tarea 3.</p> <p>El conjunto de comandos EXEC privilegiados incluye aquellos comandos del modo EXEC del usuario, así como también el comando <code>configure</code> a través del cual se obtiene acceso a los modos de comando restantes. Entre al modo EXEC privilegiado introduciendo el comando <code>enable</code>.</p> <pre>Switch>enable Switch#</pre> <p>Observe que el indicador cambia en la configuración para reflejar el modo EXEC privilegiado.</p> <p>Paso 2: Examine la configuración actual del switch.</p> <p>Examine el archivo de configuración activa actual.</p> <pre>Switch#show running-config</pre> <p>¿Cuántas interfaces FastEthernet tiene el switch? _____</p> <p>¿Cuántas interfaces Gigabit Ethernet tiene el switch? _____</p> <p>¿Cuál es el rango de valores que se muestra para las líneas vty? _____</p> <p>Examine el contenido actual de la NVRAM:</p> <pre>Switch#show startup-config startup-config is not present</pre> <p>¿Por qué el switch emite esta respuesta?</p> <p>_____</p> <p>Examine las características de la interfaz virtual VLAN1:</p> <pre>Switch#show interface vlan1</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>¿Hay una dirección IP establecida en el switch? _____</p> <p>¿Cuál es la dirección MAC de esta interfaz virtual del switch? _____</p> <p>¿Está activa esta interfaz? _____</p> <p>Ahora visualice las propiedades del IP de la interfaz:</p> <p>Switch#show ip interface vlan1</p> <p>¿Qué resultado ve? _____</p> <p>Paso 3: Muestre la información de Cisco IOS</p> <p>Examine la siguiente información acerca de la versión generada por el switch.</p> <p>Switch#show version</p> <p>¿Cuál es la versión de IOS de Cisco que está ejecutando el switch? _____</p> <p>¿Cuál es el nombre del archivo de imagen del sistema? _____</p> <p>¿Cuál es la dirección MAC base de este switch? _____</p> <p>Paso 4: Examine las interfaces de FastEthernet.</p> <p>Examine las propiedades predeterminadas de la interfaz FastEthernet que utiliza la PC1.</p> <p>Switch#show interface fastethernet 0/18</p> <p>¿La interfaz está activa o desactivada? _____</p> <p>¿Qué haría que una interfaz se active? _____</p> <p>¿Cuál es la dirección MAC de la interfaz? _____</p> <p>¿Cuál es la configuración de velocidad y de dúplex de la interfaz? _____</p> <p>Paso 5: Examine la información de VLAN.</p> <p>Examine la configuración VLAN predeterminada del switch.</p> <p>Switch#show vlan</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>¿Cuál es el nombre de la VLAN 1? _____</p> <p>¿Qué puertos hay en esta VLAN? _____</p> <p>¿La VLAN 1 está activa? _____</p> <p>¿Qué tipo de VLAN es la VLAN predeterminada? _____</p> <p>Paso 6: Examine la memoria flash.</p> <p>Ejecute uno de los siguientes comandos para examinar el contenido del directorio flash. Switch#dir flash:</p> <pre> o Switch#show flash </pre> <p>¿Qué archivos o directorios se encuentran?</p> <p>_____</p> <p>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:</p> <pre> Switch#dir flash:c2960-lanbase-mz.122-25.SEE3 </pre> <p>El resultado deberá verse de manera similar a lo siguiente:</p> <pre> 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) </pre> <p>¿Cuál es el nombre del archivo de imagen de IOS de Cisco? _____</p> <p>Paso 7: Examine el archivo de configuración de inicio.</p> <p>Para ver el contenido del archivo de configuración de inicio, ejecute el comando <code>show startup-config</code> en el modo EXEC privilegiado:</p> <pre> Switch#show startup-config startup-config is not present </pre> <p>¿Por qué aparece este mensaje? _____</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Haga una modificación a la configuración del switch y guárdela. Escriba los siguientes comandos:</p> <pre>Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# hostname S1 S1(config)#exit S1#</pre> <p>Para guardar el contenido del archivo de configuración en ejecución en la RAM no volátil (NVRAM), ejecute el comando <code>copy running-config startup-config</code>.</p> <pre>Switch#copy running-config startup-config Destination filename [startup-config]? (Intro) Building configuration... [OK]</pre> <p>Nota: Es más fácil ingresar este comando mediante la abreviatura <code>copy run start</code>.</p> <p>Ahora muestre los contenidos de la NVRAM usando el comando <code>show startup-config</code>.</p> <pre>S1#show startup-config Using 1170 out of 68836 bytes ! version 12.2 no service pad service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname S1 !</pre> <p><se omite el resultado></p> <p>La configuración actual se ha escrito en la NVRAM.</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Tarea 3: Crear una configuración básica de switch</p> <p>Paso 1: Asigne un nombre al switch.</p> <p>En el último paso de la tarea anterior, usted configuró el nombre de host. A continuación encontrará un resumen de los comandos utilizados.</p> <pre>S1#configure terminal S1 (config)#hostname S1 S1 (config)#exit</pre> <p>Paso 2: Establezca las contraseñas de acceso.</p> <p>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.</p> <pre>S1#configure terminal Enter the configuration commands, one for each line. When you are finished, return to global configuration mode by entering the exit command or pressing Ctrl-Z.</pre> <pre>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</pre> <p>¿Por qué se requiere el comando login? _____</p> <p>Paso 3: Configure las contraseñas del modo de comando.</p> <p>Establezca la contraseña secreta de enable como class. Esta contraseña protege el acceso al modo EXEC privilegiado.</p> <pre>S1 (config)#enable secret class</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Paso 4: Configure la dirección de la capa 3 del switch.</p> <p>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 de éste 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.</p> <p>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.</p> <p>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.</p> <pre>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)#</pre> <p>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.</p> <p>Asigne todos los puertos de usuario a VLAN 99.</p> <pre>S1 (config)#interface range fa0/1 - 24 S1 (config-if-range)#switchport access vlan 99 S1 (config-if-range)#exit S1 (config)# %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up</pre> <p>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.</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Paso 5: Establezca el gateway predeterminado del switch.</p> <p>S1 es un switch de Capa 2, por lo tanto toma decisiones de envío en base al encabezado de la Capa 2. Si se conectan múltiples redes a un switch, es necesario que especifique cómo el switch envía las tramas de internetwork, ya que la ruta se debe determinar en la Capa 3. Esto se lleva a cabo al especificar una dirección de gateway predeterminado hacia un router o al switch de la Capa 3. Aunque esta actividad no incluye un gateway IP externo, se debe tener en cuenta que finalmente conectará la LAN a un router para tener acceso externo. Si suponemos que la interfaz de LAN en el router es 172.17.99.1, establezca el gateway predeterminado para el switch.</p> <pre>S1(config)#ip default-gateway 172.17.99.1 S1(config)#exit</pre> <p>Paso 6: Verifique la configuración de las LAN de administración.</p> <p>Verifique la configuración de interfaz de la VLAN 99.</p> <pre>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</pre> <p>¿Cuál es el ancho de banda en esta interfaz? _____</p> <p>¿Cuáles son los estados de la VLAN?: VLAN99 está _____, el Protocolo de línea está _____</p> <p>¿Cuál es la estrategia para formar las colas? _____</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Paso 7: Configure la dirección IP y el gateway predeterminado para PC1.</p> <p>Establezca la dirección IP de la PC1 en 172.17.99.21 con una máscara de subred 255.255.255.0. Configure un gateway predeterminado de 172.17.99.1. (De ser necesario, consulte la Práctica de laboratorio 1.3.1 para configurar la NIC de la PC).</p> <p>Paso 8: Verifique la conectividad.</p> <p>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.</p> <p>¿Tuvo éxito el ping? _____</p> <p>En caso contrario, resuelva los problemas del switch y de la configuración del host. Observe que pueden ser necesarios varios intentos para que los pings tengan éxito.</p> <p>Paso 9: Configure la velocidad del puerto y la configuración dúplex para una interfaz FastEthernet.</p> <p>Realice la configuración de velocidad y dúplex en FastEthernet 0/18. Utilice el comando end para regresar al modo EXEC privilegiado al finalizar.</p> <pre>S1#configure terminal S1 (config)#interface fastethernet 0/18 S1 (config-if)#speed 100 S1 (config-if)#duplex full S1 (config-if)#end</pre> <p>%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 to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up</p> <p>El protocolo de línea para la interfaz FastEthernet 0/18 y la interfaz VLAN 99 se desactivará de forma temporal.</p> <p>El valor predeterminado en la interfaz Ethernet del switch es de detección automática, por lo tanto negocia automáticamente las configuraciones óptimas. Usted debe establecer el modo dúplex y la velocidad 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.</p> <p>Verifique las nuevas configuraciones de dúplex y de velocidad en la interfaz FastEthernet.</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> S1#show interface fastethernet 0/18 FastEthernet0/18 is up, line protocol is up (connected) Hardware is FastEthernet, 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 </pre> <p>Paso 10: Guarde la configuración.</p> <p>Ha completado la configuración básica del switch. Ahora haga una copia de seguridad del archivo de configuración en ejecución a NVRAM para garantizar que los cambios que se han realizado no se pierdan si el sistema se reinicia o se apaga.</p> <pre> S1#copy running-config startup-config Destination filename [startup-config]?[Intro] Building configuration... [OK] S1# </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Paso 11: Examine el archivo de configuración de inicio.</p> <p>Para ver la configuración guardada en la NVRAM, ejecute el comando <code>show startup-config</code> en el modo EXEC privilegiado.</p> <pre>S1#show startup-config</pre> <p>¿Todos los cambios realizados están grabados en el archivo? _____</p> <p>Tarea 4: Administrar la tabla de direcciones MAC</p> <p>Paso 1: Anote las direcciones MAC de los hosts.</p> <p>Determine y anote las direcciones de Capa 2 (físicas) de las tarjetas de interfaz de red de la PC utilizando los siguientes comandos:</p> <p>Inicio > Ejecutar > cmd > ipconfig /all</p> <p>PC1: _____</p> <p>PC2: _____</p> <p>Paso 2: Determine las direcciones MAC que el switch ha aprendido.</p> <p>Muestre las direcciones MAC utilizando el comando <code>show mac-address-table</code> en modo EXEC privilegiado.</p> <pre>S1#show mac-address-table</pre> <p>¿Cuántas direcciones dinámicas hay? _____</p> <p>¿Cuántas direcciones MAC hay en total? _____</p> <p>¿La dirección MAC dinámica concuerda con la dirección MAC de la PC1? _____</p> <p>Paso 3: Enumere las opciones show mac-address-table.</p> <pre>S1#show mac-address-table ?</pre> <p>¿Cuántas opciones hay disponibles para el comando <code>show mac-address-table</code>? _____</p> <p>Muestre solamente las direcciones MAC de la tabla que se aprendieron de forma dinámica.</p> <pre>S1#show mac-address-table address dynamic</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>¿Cuántas direcciones dinámicas hay? _____</p> <p>Visualice la entrada de la dirección MAC para la PC1.</p> <p><code>S1#show mac-address-table address <MAC de la PC1 aquí></code></p> <p>Paso 4: Limpie la tabla de direcciones MAC.</p> <p>Para eliminar las direcciones MAC existentes, use el comando <code>clear mac-address-table</code> en modo EXEC privilegiado.</p> <p><code>S1#clear mac-address-table dynamic</code></p> <p>Paso 5: Verifique los resultados.</p> <p>Verifique que la tabla de direcciones MAC esté en blanco.</p> <p><code>S1#show mac-address-table</code></p> <p>¿Cuántas direcciones MAC estáticas hay? _____</p> <p>¿Cuántas direcciones dinámicas hay? _____</p> <p>Paso 6: Examine nuevamente la tabla de direcciones MAC</p> <p>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.</p> <p><code>S1#show mac-address-table</code></p> <p>¿Cuántas direcciones dinámicas hay? _____</p> <p>¿Por qué cambió esto desde la última visualización? _____</p> <p>_____</p> <p>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.</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Paso 7: Configure una dirección MAC estática.</p> <p>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.</p> <p>Configure una dirección MAC estática en la interfaz FastEthernet 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.</p> <pre>S1 (config)#mac-address-table static 00e0.2917.1884 vlan 99 interface fastethernet 0/18</pre> <p>Paso 8: Verifique los resultados.</p> <p>Verifique las entradas de la tabla de direcciones MAC.</p> <pre>S1#show mac-address-table</pre> <p>¿Cuántas direcciones MAC hay en total? _____</p> <p>¿Cuántas direcciones estáticas hay? _____</p> <p>Paso 9: Elimine la entrada de MAC estática.</p> <p>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.</p> <p>Nota: La dirección MAC 00e0.2917.1884 se utiliza sólo en el ejemplo. Utilice la dirección MAC para su PC1.</p> <pre>S1 (config)#no mac-address-table static 00e0.2917.1884 vlan 99 interface fastethernet 0/18</pre> <p>Paso 10: Verifique los resultados.</p> <p>Verifique que la dirección MAC estática se haya borrado.</p> <pre>S1#show mac-address-table</pre> <p>¿Cuántas direcciones MAC estáticas hay en total? _____</p>

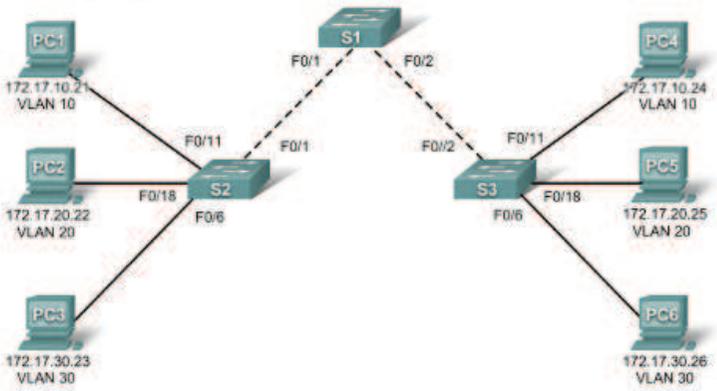
Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Tarea 5: Configurar la seguridad de puerto</p> <p>Paso 1: Configure un segundo host. Para esta tarea es necesario un segundo host. Establezca la dirección IP de la PC2 en 172.17.99.32 con una máscara de subred 255.255.255.0 y un gateway predeterminado en 172.17.99.1. No conecte aún esta PC al switch.</p> <p>Paso 2: Verifique 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 tuvieron éxito? _____ Si la respuesta es no, resuelva los problemas en la configuración de los hosts y del switch.</p> <p>Paso 3: Copie las direcciones MAC del host. Anote las direcciones MAC de la Tarea 4, Paso 1. PC1 _____ PC2 _____</p> <p>Paso 4: Determine qué direcciones MAC ha aprendido el switch. Muestre las direcciones MAC aprendidas utilizando el comando <code>show mac-address-table</code> en modo EXEC privilegiado. S1#show mac-address-table ¿Cuántas direcciones dinámicas hay? _____ ¿La entrada de la dirección MAC concuerda con la dirección MAC de la PC1? _____</p> <p>Paso 5: Enumere las opciones de seguridad de puerto. Explore cuáles son las opciones para configurar la seguridad de puerto en la interfaz FastEthernet 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</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre>violation Security violation mode <cr></pre> <p>S1 (config-if)#switchport port-security</p> <p>Paso 6: Configure la seguridad de puerto en un puerto de acceso.</p> <p>Configure el puerto del switch FastEthernet 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.</p> <pre>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)#end</pre> <p>Paso 7: Verifique los resultados.</p> <p>Muestre la configuración de seguridad de puerto.</p> <pre>S1#show port-security</pre> <p>¿Cuántas direcciones seguras se permiten en FastEthernet 0/18? _____</p> <p>¿Qué medida de seguridad debe tomarse para este puerto? _____</p> <p>Paso 8: Examine el archivo de configuración activo.</p> <pre>S1#show running-config</pre> <p>¿Hay afirmaciones enumeradas que reflejan directamente la implementación de seguridad de la configuración en ejecución? _____</p> <p>Paso 9: Modifique la configuración de seguridad de puerto en un puerto.</p> <p>En la interfaz FastEthernet 0/18, establezca la dirección MAC de seguridad máxima del puerto en 1 y que se desactive en caso de violación.</p> <pre>S1 (config-if)#switchport port-security maximum 1 S1 (config-if)#switchport port-security violation shutdown</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Paso 10: Verifique los resultados.</p> <p>Muestre la configuración de seguridad de puerto.</p> <pre> S1#show port-security </pre> <p>¿Las configuraciones de seguridad de los puertos reflejan las modificaciones del Paso 9? _____</p> <p>Haga ping en la dirección VLAN99 del switch desde 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 en ejecución.</p> <pre> S1#show run Building configuration... <se omite el resultado> ! 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 ! <se omite el resultado> </pre> <p>Paso 11: Introduzca un host no autorizado.</p> <p>Desconecte la PC1 y conecte la PC2 al puerto FastEthernet 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.</p> <p>Anote cualquier observación: _____</p> <p>_____</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Paso 12: Muestre la información sobre la configuración del puerto.</p> <p>Para ver la información de configuración sólo para el puerto FastEthernet 0/18, ejecute el siguiente comando en modo EXEC privilegiado:</p> <pre>S1#show interface fastethernet 0/18</pre> <p>¿Cuál es el estado de esta interfaz? FastEthernet0/18 está _____ El protocolo de línea está _____</p> <p>Paso 13: Reactive el puerto.</p> <p>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 FastEthernet 0/18, cualquier tráfico desde el host desactivará el puerto. Vuelva a conectar la PC1 a FastEthernet 0/18 e ingrese los siguientes comandos en el switch:</p> <pre>S1# configure terminal S1 (config)#interface fastethernet 0/18 S1 (config-if)#no shutdown S1 (config-if)#exit</pre> <p>Nota: Algunas versiones de IOS pueden requerir un comando shutdown manual antes de ingresar el comando no shutdown.</p> <p>Paso 14: Limpieza</p> <p>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.</p> <p><i>Tomado del Material de Cisco CCNA para efectos educativos: Cisco Networking Academy 1992-2007</i></p> <p>Entrega un informe de las actividades realizadas en la práctica, formando el portafolio de evidencias.</p> <p> ADVERTENCIA DE RIESGO ELÉCTRICO</p>

Unidad de aprendizaje:	Administración de redes de área local virtuales.	Número:	3
Práctica	Configuración básica de una VLAN VLAN siguiendo procedimiento.	Número:	10
Propósito de la práctica	Crear VLANs en un switch, de acuerdo a las características solicitadas VLAN, para su operación.		
Escenario	Laboratorio de informática	Duración	2 hrs.
Materiales, Herramientas, Instrumental, Maquinaria y Equipo.		Desempeños	
6 Estaciones de trabajo 3 switches. 6 cables directo. 2 cables cruzados.		<ul style="list-style-type: none"> • Aplica las siguientes medidas de seguridad e higiene en el desarrollo de la práctica: <ul style="list-style-type: none"> - Evita la manipulación de comida o líquidos cerca del equipo de cómputo - No introduce objetos extraños en las entradas físicas de dispositivos de la computadora - No utiliza imanes cerca de discos compactos, memorias extraíbles ó de la computadora - Limpia el área de trabajo, prepara herramientas y los materiales a utilizar ↻ Utilizar las hojas por ambas caras y colocar las de desecho las en el recipiente destinado para su posterior envié a reciclaje <p>NOTA El docente deberá adecuar la práctica al equipo y recursos de software con el que se cuenta.</p>	

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p data-bbox="965 288 1205 316">Diagrama de topología</p>  <p>The diagram illustrates a network topology with three switches (S1, S2, S3) and six PCs (PC1-PC6). - Switch S1 is connected to S2 via F0/1 and F0/11. - Switch S1 is connected to S3 via F0/2 and F0/11. - Switch S2 is connected to S3 via F0/6 and F0/18. - PC1 (172.17.10.21, VLAN 10) is connected to S2 via F0/11. - PC2 (172.17.20.22, VLAN 20) is connected to S2 via F0/18. - PC3 (172.17.30.23, VLAN 30) is connected to S2 via F0/6. - PC4 (172.17.10.24, VLAN 10) is connected to S3 via F0/11. - PC5 (172.17.20.25, VLAN 20) is connected to S3 via F0/18. - PC6 (172.17.30.26, VLAN 30) is connected to S3 via F0/6.</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños																																																																	
	<p>Tabla de direccionamiento</p> <table border="1" data-bbox="920 328 1955 767"> <thead> <tr> <th>Dispositivo Nombre de host</th> <th>Interfaz</th> <th>Dirección IP</th> <th>Máscara de subred</th> <th>Gateway (puerta de salida) predeterminado</th> </tr> </thead> <tbody> <tr> <td>S1</td> <td>VLAN 99</td> <td>172.17.99.11</td> <td>255.255.255.0</td> <td>N/C</td> </tr> <tr> <td>S2</td> <td>VLAN 99</td> <td>172.17.99.12</td> <td>255.255.255.0</td> <td>N/C</td> </tr> <tr> <td>S3</td> <td>VLAN 99</td> <td>172.17.99.13</td> <td>255.255.255.0</td> <td>N/C</td> </tr> <tr> <td>PC1</td> <td>NIC</td> <td>172.17.10.21</td> <td>255.255.255.0</td> <td>172.17.10.1</td> </tr> <tr> <td>PC2</td> <td>NIC</td> <td>172.17.20.22</td> <td>255.255.255.0</td> <td>172.17.20.1</td> </tr> <tr> <td>PC3</td> <td>NIC</td> <td>172.17.30.23</td> <td>255.255.255.0</td> <td>172.17.30.1</td> </tr> <tr> <td>PC4</td> <td>NIC</td> <td>172.17.10.24</td> <td>255.255.255.0</td> <td>172.17.10.1</td> </tr> <tr> <td>PC5</td> <td>NIC</td> <td>172.17.20.25</td> <td>255.255.255.0</td> <td>172.17.20.1</td> </tr> <tr> <td>PC6</td> <td>NIC</td> <td>172.17.30.26</td> <td>255.255.255.0</td> <td>172.17.30.1</td> </tr> </tbody> </table> <p>Asignaciones iniciales de puertos (Switches 2 y 3)</p> <table border="1" data-bbox="994 839 1883 978"> <thead> <tr> <th>Puertos</th> <th>Asignación</th> <th>Red</th> </tr> </thead> <tbody> <tr> <td>Fa0/1 – 0/5</td> <td>Enlaces troncales 802.1q (VLAN 99 nativa)</td> <td>172.17.99.0 /24</td> </tr> <tr> <td>Fa0/6 – 0/10</td> <td>VLAN 30 – Guest (Default)</td> <td>172.17.30.0 /24</td> </tr> <tr> <td>Fa0/11 – 0/17</td> <td>VLAN 10 – Faculty/Staff</td> <td>172.17.10.0 /24</td> </tr> <tr> <td>Fa0/18 – 0/24</td> <td>VLAN 20 – Students</td> <td>172.17.20.0 /24</td> </tr> </tbody> </table> <p>Tarea 1: Preparar la red</p> <p>Paso 1: Cablee una red de manera similar al diagrama de topología.</p> <p>Puede utilizar cualquier switch actual en su práctica de laboratorio siempre y cuando éste tenga las interfaces necesarias que se muestran en la topología.</p> <p>Nota: Si utiliza switches 2900 o 2950, los resultados pueden aparecer de manera diferente. Asimismo, ciertos comandos pueden ser diferentes o no encontrarse disponibles.</p>	Dispositivo Nombre de host	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminado	S1	VLAN 99	172.17.99.11	255.255.255.0	N/C	S2	VLAN 99	172.17.99.12	255.255.255.0	N/C	S3	VLAN 99	172.17.99.13	255.255.255.0	N/C	PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1	PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1	PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1	PC4	NIC	172.17.10.24	255.255.255.0	172.17.10.1	PC5	NIC	172.17.20.25	255.255.255.0	172.17.20.1	PC6	NIC	172.17.30.26	255.255.255.0	172.17.30.1	Puertos	Asignación	Red	Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN 99 nativa)	172.17.99.0 /24	Fa0/6 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24	Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24	Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24
Dispositivo Nombre de host	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminado																																																														
S1	VLAN 99	172.17.99.11	255.255.255.0	N/C																																																														
S2	VLAN 99	172.17.99.12	255.255.255.0	N/C																																																														
S3	VLAN 99	172.17.99.13	255.255.255.0	N/C																																																														
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1																																																														
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1																																																														
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1																																																														
PC4	NIC	172.17.10.24	255.255.255.0	172.17.10.1																																																														
PC5	NIC	172.17.20.25	255.255.255.0	172.17.20.1																																																														
PC6	NIC	172.17.30.26	255.255.255.0	172.17.30.1																																																														
Puertos	Asignación	Red																																																																
Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN 99 nativa)	172.17.99.0 /24																																																																
Fa0/6 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24																																																																
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24																																																																
Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24																																																																

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Paso 2: Borre configuraciones existentes en los switches e inicializar todos los puertos en estado desactivado.</p> <p>De ser necesario, consulte la Práctica de laboratorio 2.5.1, Apéndice 1, para leer sobre el procedimiento para borrar las configuraciones del switch.</p> <p>Es una optimización deshabilitar puertos no utilizados en los switches mediante su desactivación. Deshabilite todos los puertos en los switches:</p> <pre>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</pre> <p>Tarea 2: Realizar las configuraciones básicas del switch</p> <p>Paso 1: Configure los switches de acuerdo con la siguiente guía:</p> <ul style="list-style-type: none"> • 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. <p>Paso 2: Vuelva a habilitar los puertos de usuario en S2 y S3.</p> <pre>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</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños						
	<p>Tarea 3: Configurar y activar las interfaces Ethernet</p> <p>Paso 1: Configure las PC.</p> <p>Puede completar esta práctica de laboratorio utilizando sólo dos PC, simplemente modificando las direcciones IP de las dos PC específicas de una prueba que desea llevar a cabo. Por ejemplo: si desea probar la conectividad entre la PC1 y la PC2, configure las direcciones IP para aquellas PC que se refieren a la tabla de direccionamiento al comienzo de la práctica de laboratorio. Alternativamente, puede configurar las seis PC con las direcciones IP y gateways predeterminados.</p> <p>Tarea 4: Configurar las VLAN en el switch</p> <p>Paso 1: Cree las VLAN en el switch S1.</p> <p>Utilice el comando <code>vlan</code> <i>id de la VLAN</i> 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 <code>vlan</code>, donde puede asignar un nombre para la VLAN mediante el comando <code>name</code> <i>nombre de la VLAN</i>.</p> <pre>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#</pre> <p>Paso 2: Verifique que las VLAN estén creadas en S1.</p> <p>Use el comando <code>show vlan brief</code> para verificar que las VLAN se hayan creado.</p> <pre>S1#show vlan brief</pre> <table border="1"> <thead> <tr> <th>VLAN Name</th> <th>Status</th> <th>Ports</th> </tr> </thead> <tbody> <tr> <td>1 default</td> <td>active</td> <td>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</td> </tr> </tbody> </table>	VLAN Name	Status	Ports	1 default	active	Fa0/1, Fa0/2, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2
VLAN Name	Status	Ports					
1 default	active	Fa0/1, Fa0/2, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2					

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> 10 faculty/staff active 20 students active 30 guest active 99 management active </pre> <p>Paso 3: Configure y asigne un nombre a las VLAN en los switches S2 y S3.</p> <p>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 <code>show vlan brief</code>.</p> <p>¿Qué puertos se encuentran asignados actualmente a las cuatro VLAN que se han creado?</p> <hr/> <p>Paso 4: Asigne puertos de switch a las VLAN en S2 y S3.</p> <p>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 <code>switchport access vlan id de la VLAN</code>. Puede asignar cada puerto en forma individual o se puede utilizar el comando <code>interface range</code> 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.</p> <pre> 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] </pre> <p>Paso 5: Determine qué puertos se han agregado.</p> <p>Utilice el comando <code>show vlan id número de VLAN</code> en S2 para ver qué puertos se asignan a VLAN 10.</p> <p>¿Qué puertos están asignados a la VLAN 10?</p> <hr/> <p>Nota: El comando <code>show vlan name nombre de la VLAN</code> muestra el mismo resultado.</p> <p>También puede ver la información sobre la asignación de VLAN utilizando el comando <code>show interfaces interface switchport</code>.</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Paso 6: Asigne la VLAN de administración.</p> <p>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.</p> <p>Desde el modo de configuración de interfaz, utilice el comando <code>ip address</code> para asignar la dirección IP de administración a los switches.</p> <pre>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</pre> <p>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.</p> <p>Paso 7: Configure los enlaces troncales y la VLAN nativa para los puertos de enlace troncales en todos los switches.</p> <p>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.</p>

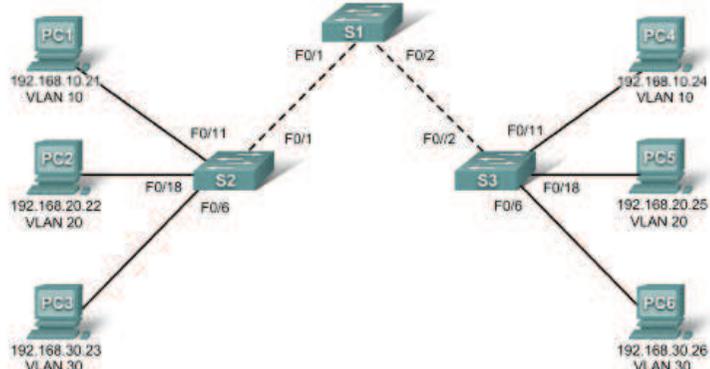
Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Se asigna una VLAN nativa a un puerto troncal 802.1Q. En la topología, la VLAN nativa es VLAN 99. Un enlace troncal 802.1Q admite tráfico de varias VLAN (tráfico etiquetado) así como el tráfico que no proviene de una VLAN (tráfico 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.</p> <p>Simplifique la configuración de enlaces troncales con el comando <code>interface range</code> en el modo de configuración global.</p> <pre>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</pre> <p>Verifique que los enlaces troncales se hayan configurado mediante el comando <code>show interface trunk</code>.</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> S1#show interface trunk Port Mode Encapsulation Status Native vlan Fa0/1 on 802.1q trunking 99 Fa0/2 on 802.1q trunking 99 Port Vlans allowed on trunk Fa0/1 1-4094 Fa0/2 1-4094 Port Vlans allowed and active in management domain Fa0/1 1,10,20,30,99 Fa0/2 1,10,20,30,99 Port Vlans in spanning tree forwarding state and not pruned Fa0/1 1,10,20,30,99 Fa0/2 1,10,20,30,99 </pre> <p>Paso 8: Verifique que los switches se puedan comunicar.</p> <p>Desde S1, haga ping a la dirección de administración en S2 y S3.</p> <pre> 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 </pre> <p>Paso 9: Haga ping a varios hosts desde la PC2.</p> <p>Haga ping desde el host de PC2 al host de PC1 (172.17.10.21). ¿El intento de hacer ping fue exitoso? _____</p> <p>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? _____</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>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.</p> <p>Haga ping desde el host PC2 al host PC5. ¿El intento de hacer ping fue exitoso? _____</p> <p>Debido a que la PC2 se encuentra en la misma VLAN y la misma subred que la PC5, el ping fue exitoso.</p> <p>Paso 10: Ubique la PC1 en la misma VLAN que la PC2.</p> <p>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.</p> <pre>S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2 (config)#interface fastethernet 0/11 S2 (config-if)#switchport access vlan 20 S2 (config-if)#end</pre> <p>Haga ping desde el host PC2 al host PC1. ¿El intento de hacer ping fue exitoso? _____</p> <p>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.</p> <p>Paso 11: Cambie la dirección IP y la red en PC1.</p> <p>Asigne 172.17.20.21 como dirección IP de PC1. La máscara de subred y el gateway predeterminado pueden seguir siendo los mismos. Una vez más, haga ping desde el host PC2 al host PC1 utilizando la dirección IP recién asignada.</p> <p>¿El intento de hacer ping fue exitoso? _____</p> <p>¿Por qué fue exitoso?</p> <p>_____</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Tarea 5: Documentar las configuraciones de los switches</p> <p>En cada switch, capture la configuración activa en un archivo de texto y consérvela para futuras referencias.</p> <p>Tarea 6: Limpieza</p> <p>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.</p> <p><i>Tomado del Material de Cisco CCNA para efectos educativos: Cisco Networking Academy 1992-2007</i></p> <p>Entrega un informe de las actividades realizadas en la práctica, formando el portafolio de evidencias.</p> <p> ADVERTENCIA DE RIESGO ELÉCTRICO</p>

Unidad de aprendizaje:	Administración de redes de área local virtuales.	Número:	3
Práctica	Resolución de problemas en la configuración de una VLAN siguiendo procedimiento.	Número:	11
Propósito de la práctica	Detecta problemas que impiden que funcione correctamente la configuración de una VLAN común VLAN siguiendo procedimiento, para su análisis y resolución.		
Escenario	Laboratorio de informática	Duración	2 hrs.

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
<p>6 Estaciones de trabajo 3 switches. 6 cables directo. 2 cable cruzados.</p>	<ul style="list-style-type: none"> • Aplica las siguientes medidas de seguridad e higiene en el desarrollo de la práctica: <ul style="list-style-type: none"> - Evita la manipulación de comida o líquidos cerca del equipo de cómputo - No introduce objetos extraños en las entradas físicas de dispositivos de la computadora - No utiliza imanes cerca de discos compactos, memorias extraíbles ó de la computadora - Limpia el área de trabajo, prepara herramientas y los materiales a utilizar ∪ Utilizar las hojas por ambas caras y colocar las de desecho las en el recipiente destinado para su posterior envió a reciclaje <p>NOTA El docente deberá adecuar la práctica al equipo y recursos de software con el que se cuenta.</p> <p>Diagrama de topología</p> 

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños																																																																	
	<p>Tabla de direccionamiento</p> <table border="1" data-bbox="907 331 1982 794"> <thead> <tr> <th>Dispositivo Nombre de host</th> <th>Interfaz</th> <th>Dirección IP</th> <th>Máscara de subred</th> <th>Gateway (puerta de salida) predeterminado</th> </tr> </thead> <tbody> <tr><td>S1</td><td>VLAN 56</td><td>192.168.56.11</td><td>255.255.255.0</td><td>N/C</td></tr> <tr><td>S2</td><td>VLAN 56</td><td>192.168.56.12</td><td>255.255.255.0</td><td>N/C</td></tr> <tr><td>S3</td><td>VLAN 56</td><td>192.168.56.13</td><td>255.255.255.0</td><td>N/C</td></tr> <tr><td>PC1</td><td>NIC</td><td>192.168.10.21</td><td>255.255.255.0</td><td>192.168.10.1</td></tr> <tr><td>PC2</td><td>NIC</td><td>192.168.20.22</td><td>255.255.255.0</td><td>192.168.20.1</td></tr> <tr><td>PC3</td><td>NIC</td><td>192.168.30.23</td><td>255.255.255.0</td><td>192.168.30.1</td></tr> <tr><td>PC4</td><td>NIC</td><td>192.168.10.24</td><td>255.255.255.0</td><td>192.168.10.1</td></tr> <tr><td>PC5</td><td>NIC</td><td>192.168.20.25</td><td>255.255.255.0</td><td>192.168.20.1</td></tr> <tr><td>PC6</td><td>NIC</td><td>192.168.30.26</td><td>255.255.255.0</td><td>192.168.30.1</td></tr> </tbody> </table> <p>Asignaciones iniciales de puertos (Switches 2 y 3)</p> <table border="1" data-bbox="990 869 1899 1010"> <thead> <tr> <th>Puertos</th> <th>Asignación</th> <th>Red</th> </tr> </thead> <tbody> <tr><td>Fa0/1 – 0/5</td><td>Enlaces troncales 802.1q (VLAN 56 nativa)</td><td>192.168.56.0 /24</td></tr> <tr><td>Fa0/6 – 0/10</td><td>VLAN 30 – Guest (Default)</td><td>192.168.30.0 /24</td></tr> <tr><td>Fa0/11 – 0/17</td><td>VLAN 10 – Faculty/Staff</td><td>192.168.10.0 /24</td></tr> <tr><td>Fa0/18 – 0/24</td><td>VLAN 20 – Students</td><td>192.168.20.0 /24</td></tr> </tbody> </table> <p>Situación</p> <p>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.</p>	Dispositivo Nombre de host	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminado	S1	VLAN 56	192.168.56.11	255.255.255.0	N/C	S2	VLAN 56	192.168.56.12	255.255.255.0	N/C	S3	VLAN 56	192.168.56.13	255.255.255.0	N/C	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	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 (Default)	192.168.30.0 /24	Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	192.168.10.0 /24	Fa0/18 – 0/24	VLAN 20 – Students	192.168.20.0 /24
Dispositivo Nombre de host	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminado																																																														
S1	VLAN 56	192.168.56.11	255.255.255.0	N/C																																																														
S2	VLAN 56	192.168.56.12	255.255.255.0	N/C																																																														
S3	VLAN 56	192.168.56.13	255.255.255.0	N/C																																																														
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																																																														
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 (Default)	192.168.30.0 /24																																																																
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	192.168.10.0 /24																																																																
Fa0/18 – 0/24	VLAN 20 – Students	192.168.20.0 /24																																																																

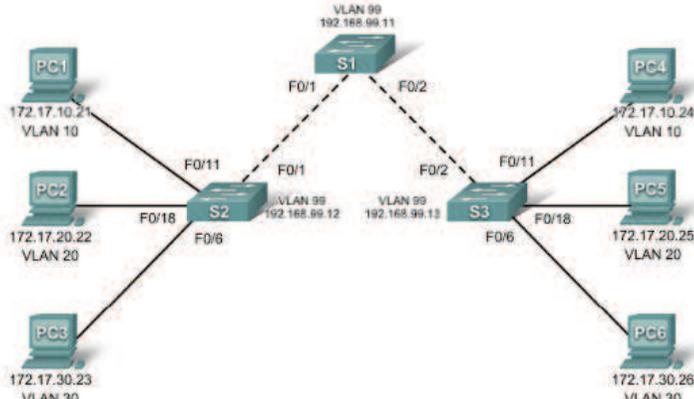
Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Tarea 1: Preparar la red</p> <p>Paso 1: Cablee una red de manera similar al diagrama de topología.</p> <p>Paso 2: Borre configuraciones existentes en los switches e inicializar todos los puertos en estado desactivado.</p> <p>Paso 3: Importe las siguientes configuraciones.</p> <p>Switch 1</p> <pre>hostname S1 no ip domain-lookup enable secret class ! ! interface range FastEthernet0/1-5 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</pre> <p>Switch 2</p> <pre>hostname S2 no ip domain-lookup enable secret class</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> ! vlan 10,20,30,56 ! interface range FastEthernet0/1-5 switchport trunk native vlan 56 ! 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 route-cache shutdown ! line con 0 password cisco login line vty 0 4 password cisco login line vty 5 15 password cisco login ! end </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> Switch 3 hostname S3 no ip domain-lookup enable secret class ! vlan 10,20,30 ! interface range FastEthernet0/1-5 switchport trunk native vlan 56 switchport mode trunk ! interface range FastEthernet0/6-10 switchport mode access ! interface range FastEthernet0/11-17 switchport mode access ! interface range FastEthernet0/18-24 switchport mode access ! interface GigabitEthernet0/1 ! interface GigabitEthernet0/2 ! interface Vlan1 no ip address no ip route-cache shutdown ! interface Vlan56 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 </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Tarea 2: Realizar un diagnóstico de fallas y reparar la configuración de la VLAN</p> <p>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.</p> <p>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.</p> <p><i>Tomado del Material de Cisco CCNA para efectos educativos: Cisco Networking Academy 1992-2007</i></p> <p>Entrega un informe de las actividades realizadas en la práctica, formando el portafolio de evidencias.</p> <p> ADVERTENCIA DE RIESGO ELÉCTRICO</p>

Unidad de aprendizaje:	Administración de redes de área local virtuales.	Número:	3
Práctica	Configuración básica de la función VTP bajo procedimiento.	Número:	12
Propósito de la práctica	Configurar las VLAN y el protocolo de enlaces troncales (VTP) en todos los switches por procedimiento, para su uso.		
Escenario	Laboratorio de informática	Duración	2 hrs.

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
<p>2 Estaciones de trabajo 1 switch. 1 cables directo. 1 cable de consola.</p>	<ul style="list-style-type: none"> • Aplica las siguientes medidas de seguridad e higiene en el desarrollo de la práctica: <ul style="list-style-type: none"> - Evita la manipulación de comida o líquidos cerca del equipo de cómputo - No introduce objetos extraños en las entradas físicas de dispositivos de la computadora - No utiliza imanes cerca de discos compactos, memorias extraíbles ó de la computadora - Limpia el área de trabajo, prepara herramientas y los materiales a utilizar ☺ Utilizar las hojas por ambas caras y colocar las de desecho las en el recipiente destinado para su posterior envío a reciclaje <p>NOTA El docente deberá adecuar la práctica al equipo y recursos de software con el que se cuenta.</p> <p>Diagrama de topología</p>  <p>The diagram shows a network topology with three switches: S1, S2, and S3. S1 is at the top, S2 is at the bottom left, and S3 is at the bottom right. S1 and S2 are connected via F0/11 on S1 and F0/1 on S2. S1 and S3 are connected via F0/2 on S1 and F0/2 on S3. S2 and S3 are connected via F0/6 on both. PC1 (172.17.10.21, VLAN 10) is connected to S1 (F0/1). PC2 (172.17.20.22, VLAN 20) is connected to S2 (F0/18). PC3 (172.17.30.23, VLAN 30) is connected to S2 (F0/6). PC4 (172.17.10.24, VLAN 10) is connected to S3 (F0/11). PC5 (172.17.20.25, VLAN 20) is connected to S3 (F0/18). PC6 (172.17.30.26, VLAN 30) is connected to S3 (F0/6). S1 has a management IP of 192.168.99.11 (VLAN 99). S2 has a management IP of 192.168.99.12 (VLAN 99). S3 has a management IP of 192.168.99.13 (VLAN 99).</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños																																																																	
	<p>Tabla de direccionamiento</p> <table border="1" data-bbox="904 325 1890 748"> <thead> <tr> <th>Dispositivo Nombre de host</th> <th>Interfaz</th> <th>Dirección IP</th> <th>Máscara de subred</th> <th>Gateway predeterminada</th> </tr> </thead> <tbody> <tr><td>S1</td><td>VLAN 99</td><td>172.17.99.11</td><td>255.255.255.0</td><td>N/C</td></tr> <tr><td>S2</td><td>VLAN 99</td><td>172.17.99.12</td><td>255.255.255.0</td><td>N/C</td></tr> <tr><td>S3</td><td>VLAN 99</td><td>172.17.99.13</td><td>255.255.255.0</td><td>N/C</td></tr> <tr><td>PC1</td><td>NIC</td><td>172.17.10.21</td><td>255.255.255.0</td><td>172.17.10.1</td></tr> <tr><td>PC2</td><td>NIC</td><td>172.17.20.22</td><td>255.255.255.0</td><td>172.17.20.1</td></tr> <tr><td>PC3</td><td>NIC</td><td>172.17.30.23</td><td>255.255.255.0</td><td>172.17.30.1</td></tr> <tr><td>PC4</td><td>NIC</td><td>172.17.10.24</td><td>255.255.255.0</td><td>172.17.10.1</td></tr> <tr><td>PC5</td><td>NIC</td><td>172.17.20.25</td><td>255.255.255.0</td><td>172.17.20.1</td></tr> <tr><td>PC6</td><td>NIC</td><td>172.17.30.26</td><td>255.255.255.0</td><td>172.17.30.1</td></tr> </tbody> </table> <p>Asignaciones de puertos (Switches 2 y 3)</p> <table border="1" data-bbox="1010 844 1901 987"> <thead> <tr> <th>Puertos</th> <th>Asignación</th> <th>Red</th> </tr> </thead> <tbody> <tr><td>Fa0/1 – 0/5</td><td>Enlaces troncales 802.1q (VLAN 99 nativa)</td><td>172.17.99.0 /24</td></tr> <tr><td>Fa0/6 – 0/10</td><td>VLAN 30 – Guest (Default)</td><td>172.17.30.0 /24</td></tr> <tr><td>Fa0/11 – 0/17</td><td>VLAN 10 – Faculty/Staff</td><td>172.17.10.0 /24</td></tr> <tr><td>Fa0/18 – 0/24</td><td>VLAN 20 – Students</td><td>172.17.20.0 /24</td></tr> </tbody> </table> <p>Tarea 1: Preparar la red</p> <p>Paso 1: Cablee una red de manera similar al diagrama de topología.</p> <p>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.</p>	Dispositivo Nombre de host	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminada	S1	VLAN 99	172.17.99.11	255.255.255.0	N/C	S2	VLAN 99	172.17.99.12	255.255.255.0	N/C	S3	VLAN 99	172.17.99.13	255.255.255.0	N/C	PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1	PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1	PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1	PC4	NIC	172.17.10.24	255.255.255.0	172.17.10.1	PC5	NIC	172.17.20.25	255.255.255.0	172.17.20.1	PC6	NIC	172.17.30.26	255.255.255.0	172.17.30.1	Puertos	Asignación	Red	Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN 99 nativa)	172.17.99.0 /24	Fa0/6 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24	Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24	Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24
Dispositivo Nombre de host	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminada																																																														
S1	VLAN 99	172.17.99.11	255.255.255.0	N/C																																																														
S2	VLAN 99	172.17.99.12	255.255.255.0	N/C																																																														
S3	VLAN 99	172.17.99.13	255.255.255.0	N/C																																																														
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1																																																														
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1																																																														
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1																																																														
PC4	NIC	172.17.10.24	255.255.255.0	172.17.10.1																																																														
PC5	NIC	172.17.20.25	255.255.255.0	172.17.20.1																																																														
PC6	NIC	172.17.30.26	255.255.255.0	172.17.30.1																																																														
Puertos	Asignación	Red																																																																
Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN 99 nativa)	172.17.99.0 /24																																																																
Fa0/6 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24																																																																
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24																																																																
Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24																																																																

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños																		
	<p>Observe en la Tabla de direccionamiento que las PC se han configurado con una dirección de IP predeterminada de gateway. Ésta sería la dirección IP del router local que no se incluye en este escenario de práctica de laboratorio. El gateway predeterminado, el router sería necesario para las PC en diferentes VLAN para poder comunicarse. Esto se analiza más adelante, en otro capítulo.</p> <p>Establezca conexiones de consola en los tres switches.</p> <p>Paso 2: Borre toda configuración existente en los switches.</p> <p>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 <code>show vlan</code> para verificar que sólo existan VLAN predeterminadas y que todos los puertos se asignen a la VLAN 1.</p> <pre>Switch#show vlan</pre> <table border="1"> <thead> <tr> <th>VLAN Name</th> <th>Status</th> <th>Ports</th> </tr> </thead> <tbody> <tr> <td>1 default</td> <td>active</td> <td>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</td> </tr> <tr> <td>1002 fddi-default</td> <td>active</td> <td></td> </tr> <tr> <td>1003 token-ring-default</td> <td>active</td> <td></td> </tr> <tr> <td>1004 fddinet-default</td> <td>active</td> <td></td> </tr> <tr> <td>1005 trnet-default</td> <td>active</td> <td></td> </tr> </tbody> </table> <p>Paso 3: Deshabilitar todos los puertos con el comando shutdown. Repita estos comandos para cada switch de la topología.</p> <pre>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</pre>	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	
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																		

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Tarea 2: Realizar las configuraciones básicas del switch</p> <p>Paso 1: Complete la configuración básica de los switches S1, S2 y S3.</p> <p>Configure los switches S1, S2 y S3 según las siguientes pautas y guarde todas sus configuraciones:</p> <ul style="list-style-type: none"> • 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. <p>(Se muestran los resultados para S1)</p> <pre>Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#hostname S1 S1(config)#enable secret class S1(config)#no ip domain-lookup S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#end %SYS-5-CONFIG_I: Configured from console by console S1#copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK]</pre> <p>Paso 2: Vuelva a habilitar los puertos de usuario en S2 y S3.</p> <p>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.</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> 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 Step 3: Re-enable the trunk ports on S1, S2 and S3 S1(config)#interface fa0/1 S1(config-if)#no shutdown S1(config)#interface fa0/2 S1(config-if)#no shutdown S2(config)#interface fa0/1 S2(config-if)#no shutdown S3(config)#interface fa0/2 S3(config-if)#no shutdown </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Tarea 3: Configurar las interfaces Ethernet en las PC Host</p> <p>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.</p> <p>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.</p> <p>Tarea 4: Configurar VTP en los switches</p> <p>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 VTP o en el modo transparente de VTP.</p> <p>Paso 1: Verifique las configuraciones VTP actuales en los tres switches.</p> <pre> S1#show vtp status VTP Version : 2 Configuration Revision : 0 Maximum VLANs supported locally : 255 Number of existing VLANs : 5 VTP Operating Mode : Server VTP Domain Name : VTP Pruning Mode : Disabled VTP V2 Mode : Disabled VTP Traps Generation : Disabled MD5 digest : 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 : Server VTP Domain Name : VTP Pruning Mode : Disabled VTP V2 Mode : Disabled VTP Traps Generation : Disabled 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) </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre>S3#show vtp status VTP Version : 2 Configuration Revision : 0 Maximum VLANs supported locally : 255 Number of existing VLANs : 5 VTP Operating Mode : Server VTP Domain Name : VTP Pruning Mode : Disabled VTP V2 Mode : Disabled VTP Traps Generation : Disabled MD5 digest : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00</pre> <p>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.</p> <p>Paso 2: Configure el modo operativo, el nombre de dominio y la contraseña de VTP en los tres switches.</p> <p>Establezca Lab4 como nombre de dominio VTP y cisco como contraseña de VTP en los tres switches. Configure S1 en modo servidor, S2 en modo cliente, y S3 en modo transparente.</p> <pre>S1(config)#vtp mode server Device mode already VTP SERVER. S1(config)#vtp domain Lab4 Changing VTP domain name from NULL to Lab4 S1(config)#vtp password cisco Setting device VLAN database password to cisco S1(config)#end S2(config)#vtp mode client Setting device to VTP CLIENT mode S2(config)#vtp domain Lab4 Changing VTP domain name from NULL to Lab4 S2(config)#vtp password cisco Setting device VLAN database password to cisco S2(config)#end</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre>S3(config)#vtp mode transparent Setting device to VTP TRANSPARENT mode. S3(config)#vtp domain Lab4 Changing VTP domain name from NULL to Lab4 S3(config)#vtp password cisco Setting device VLAN database password to cisco S3(config)#end</pre> <p>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.</p> <p>Paso 3: Configure los enlaces troncales y la VLAN nativa para los puertos de enlace troncales en los tres switches.</p> <p>Simplifique esta tarea con el comando <code>interface range</code> en el modo de configuración global.</p> <pre>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</pre> <p>Paso 4: Configure la seguridad de Puerto en los switches de capa de acceso S2 y S3.</p> <p>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.</p> <pre>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</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre>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</pre> <p>Paso 5: Configure las VLAN en el servidor VTP.</p> <p>Hay cuatro VLAN adicionales que se requieren en esta práctica de laboratorio:</p> <ul style="list-style-type: none"> • VLAN 99 (management) • VLAN 10 (faculty/staff) • VLAN 20 (students) • VLAN 30 (guest)

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños																		
	<p>Configúrelas en el servidor VTP.</p> <pre>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</pre> <p>Verifique que se hayan creado las VLAN en S1 con el comando <code>show vlan brief</code>.</p> <p>Paso 6: Verifique que las VLAN creadas en S1 se hayan distribuido a S2 y S3.</p> <p>Utilice el comando <code>show vlan brief</code> en S2 y S3 para determinar si el servidor VTP ha enviado su configuración VLAN a todos los switches.</p> <pre>S2#show vlan brief</pre> <table border="1"> <thead> <tr> <th>VLAN Name</th> <th>Status</th> <th>Ports</th> </tr> </thead> <tbody> <tr> <td>1 default</td> <td>active</td> <td>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</td> </tr> <tr> <td>10 faculty/staff</td> <td>active</td> <td></td> </tr> <tr> <td>20 students</td> <td>active</td> <td></td> </tr> <tr> <td>30 guest</td> <td>active</td> <td></td> </tr> <tr> <td>99 management</td> <td>active</td> <td></td> </tr> </tbody> </table>	VLAN Name	Status	Ports	1 default	active	Fa0/1, Fa0/2, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2	10 faculty/staff	active		20 students	active		30 guest	active		99 management	active	
VLAN Name	Status	Ports																	
1 default	active	Fa0/1, Fa0/2, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2																	
10 faculty/staff	active																		
20 students	active																		
30 guest	active																		
99 management	active																		

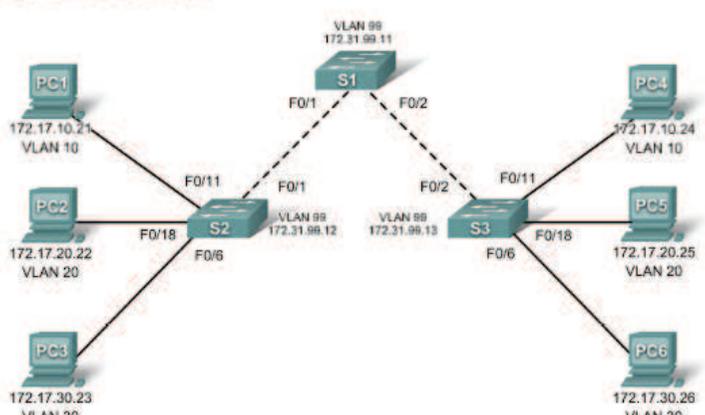
Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños																		
	<pre>S3#show vlan brief</pre> <table border="1"> <thead> <tr> <th>VLAN Name</th> <th>Status</th> <th>Ports</th> </tr> </thead> <tbody> <tr> <td>1 default</td> <td>active</td> <td>Fa0/1, Fa0/2, Fa0/4, Fa0/5 Fa0/6, 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</td> </tr> <tr> <td>1002 fddi-default</td> <td>act/unsup</td> <td></td> </tr> <tr> <td>1003 token-ring-default</td> <td>act/unsup</td> <td></td> </tr> <tr> <td>1004 fddinet-default</td> <td>act/unsup</td> <td></td> </tr> <tr> <td>1005 trnet-default</td> <td>act/unsup</td> <td></td> </tr> </tbody> </table> <p>¿Están configuradas las mismas VLAN en todos los switches? _____</p> <p>Explique por qué S2 y S3 tienen diferentes configuraciones de VLAN en este momento. _____</p> <p>_____</p> <p>_____</p> <p>Paso 7: Cree una nueva VLAN en switches 2 y 3.</p> <pre>S2(config)#vlan 88 %VTP VLAN configuration not allowed when device is in CLIENT mode.</pre> <pre>S3(config)#vlan 88 S3(config-vlan)#name test S3(config-vlan)#</pre> <p>¿Por qué no se le permite crear una nueva VLAN en S2 pero sí en S3? _____</p> <p>_____</p> <p>Borre la VLAN 88 de S3.</p> <pre>S3(config)#no vlan 88</pre>	VLAN Name	Status	Ports	1 default	active	Fa0/1, Fa0/2, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2	1002 fddi-default	act/unsup		1003 token-ring-default	act/unsup		1004 fddinet-default	act/unsup		1005 trnet-default	act/unsup	
VLAN Name	Status	Ports																	
1 default	active	Fa0/1, Fa0/2, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2																	
1002 fddi-default	act/unsup																		
1003 token-ring-default	act/unsup																		
1004 fddinet-default	act/unsup																		
1005 trnet-default	act/unsup																		

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Paso 8: Configure las VLAN en forma manual.</p> <p>Configure las cuatro VLAN identificadas en el Paso 5 en el switch S3.</p> <pre>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</pre> <p>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.</p> <p>Paso 9: Configure la dirección de la interfaz de administración en los tres switches.</p> <pre>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</pre> <p>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.</p> <p>¿Los pings son exitosos? _____</p> <p>En caso contrario, realice el diagnóstico de fallas de las configuraciones de los switches e inténtelo nuevamente.</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Paso 10: Asigne puertos de switch a las VLAN.</p> <p>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 <code>interface range</code>. Las asignaciones de puertos no se configuran a través del VTP. Las asignaciones de puerto deben ser configuradas en cada switch manualmente o dinámicamente con 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.</p> <pre>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#</pre> <p>Tarea 5: Configurar la depuración VTP en los switches</p> <p>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.</p> <p>La depuración se configura en el switch del servidor mediante el comando <code>vtp pruning</code> en modo de configuración global. La configuración se envía a los switches de clientes.</p> <p>Confirme la configuración de depuración VTP en cada switch con el comando <code>show vtp status</code>. El modo de depuración VTP debe estar activado en cada switch.</p> <pre>S1#show vtp status VTP Version : 2 Configuration Revision : 17 Maximum VLANs supported locally : 255 Number of existing VLANs : 9 VTP Operating Mode : Server VTP Domain Name : Lab4 VTP Pruning Mode : Enabled <resultado omitido></pre> <p>Tarea 6: Limpieza</p> <p>Borre las configuraciones y vuelva a cargar los switches. Desconecte y guarde el cableado. En caso de los equipos 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.</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p><i>Tomado del Material de Cisco CCNA para efectos educativos: Cisco Networking Academy 1992-2007</i></p> <p>Entrega un informe de las actividades realizadas en la práctica, formando el portafolio de evidencias.</p> <p> ADVERTENCIA DE RIESGO ELÉCTRICO</p>

Unidad de aprendizaje:	Administración de redes de área local virtuales.	Número:	3
Práctica	Resolución de problemas en la configuración de la función VTP bajo procedimiento.	Número:	13
Propósito de la práctica	Encontrar y corregir todos los errores de configuración de switches bajo procedimiento, para el funcionamiento de la función VTP.		
Escenario	Laboratorio de informática	Duración	2 hrs.

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
<p>6 Estaciones de trabajo 3 switches. 6 cables directo. 2 cables de cruzados.</p>	<ul style="list-style-type: none"> • Aplica las siguientes medidas de seguridad e higiene en el desarrollo de la práctica: <ul style="list-style-type: none"> - Evita la manipulación de comida o líquidos cerca del equipo de cómputo - No introduce objetos extraños en las entradas físicas de dispositivos de la computadora - No utiliza imanes cerca de discos compactos, memorias extraíbles ó de la computadora - Limpia el área de trabajo, prepara herramientas y los materiales a utilizar ↳ Utilizar las hojas por ambas caras y colocar las de desecho las en el recipiente destinado para su posterior envío a reciclaje <p>NOTA El docente deberá adecuar la práctica al equipo y recursos de software con el que se cuenta.</p> <p>Diagrama de topología</p>  <p>The diagram shows a network topology with three switches: S1, S2, and S3. S1 is at the top, S2 is at the bottom left, and S3 is at the bottom right. S1 and S2 are connected via a dashed line (F0/1 on S1, F0/18 on S2). S1 and S3 are connected via a dashed line (F0/2 on S1, F0/18 on S3). S2 and S3 are connected via a solid line (F0/6 on S2, F0/6 on S3). There are six PCs connected to the switches: PC1 (172.17.10.21, VLAN 10) to S2 (F0/11); PC2 (172.17.20.22, VLAN 20) to S2 (F0/18); PC3 (172.17.30.23, VLAN 30) to S2 (F0/6); PC4 (172.17.10.24, VLAN 10) to S3 (F0/11); PC5 (172.17.20.25, VLAN 20) to S3 (F0/18); PC6 (172.17.30.26, VLAN 30) to S3 (F0/6). S1 has a management IP of 172.31.99.11 (VLAN 99). S2 has a management IP of 172.31.99.12 (VLAN 99). S3 has a management IP of 172.31.99.13 (VLAN 99).</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños																																																							
	<p>Tabla de direccionamiento</p> <table border="1" data-bbox="976 336 1930 809"> <thead> <tr> <th>Dispositivo Nombre de host</th> <th>Interfaz</th> <th>Dirección IP</th> <th>Máscara de subred</th> </tr> </thead> <tbody> <tr> <td>S1</td> <td>VLAN 99</td> <td>172.17.99.11</td> <td>255.255.255.0</td> </tr> <tr> <td>S2</td> <td>VLAN 99</td> <td>172.17.99.12</td> <td>255.255.255.0</td> </tr> <tr> <td>S3</td> <td>VLAN 99</td> <td>172.17.99.13</td> <td>255.255.255.0</td> </tr> <tr> <td>PC1</td> <td>NIC</td> <td>172.17.10.21</td> <td>255.255.255.0</td> </tr> <tr> <td>PC2</td> <td>NIC</td> <td>172.17.20.22</td> <td>255.255.255.0</td> </tr> <tr> <td>PC3</td> <td>NIC</td> <td>172.17.30.23</td> <td>255.255.255.0</td> </tr> <tr> <td>PC4</td> <td>NIC</td> <td>172.17.10.24</td> <td>255.255.255.0</td> </tr> <tr> <td>PC5</td> <td>NIC</td> <td>172.17.20.25</td> <td>255.255.255.0</td> </tr> <tr> <td>PC6</td> <td>NIC</td> <td>172.17.30.26</td> <td>255.255.255.0</td> </tr> </tbody> </table> <p>Asignaciones de puertos (Switches 2 y 3)</p> <table border="1" data-bbox="990 906 1930 1059"> <thead> <tr> <th>Puertos</th> <th>Asignación</th> <th>Red</th> </tr> </thead> <tbody> <tr> <td>Fa0/1 – 0/5</td> <td>Enlaces troncales 802.1q (VLAN 99 nativa)</td> <td>172.17.99.0 /24</td> </tr> <tr> <td>Fa0/6 – 0/10</td> <td>VLAN 30 – Guest (Default)</td> <td>172.17.30.0 /24</td> </tr> <tr> <td>Fa0/11 – 0/17</td> <td>VLAN 10 – Faculty/Staff</td> <td>172.17.10.0 /24</td> </tr> <tr> <td>Fa0/18 – 0/24</td> <td>VLAN 20 – Students</td> <td>172.17.20.0 /24</td> </tr> </tbody> </table>	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	Puertos	Asignación	Red	Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN 99 nativa)	172.17.99.0 /24	Fa0/6 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24	Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24	Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24
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																																																					
Puertos	Asignación	Red																																																						
Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN 99 nativa)	172.17.99.0 /24																																																						
Fa0/6 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24																																																						
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24																																																						
Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24																																																						

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Situación</p> <p>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 Lab4_3 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.</p> <p>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.</p> <p>Tarea 1: Preparar la red</p> <p>Paso 1: Cablee una red de manera similar al diagrama de topología.</p> <p>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.</p> <p>Establezca conexiones de consola en los tres switches.</p> <p>Paso 2: Borre toda configuración existente en los switches.</p> <p>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.</p> <p>Paso 3: Configure las interfaces Ethernet en las PC host.</p> <p>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.</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Tarea 2: Cargar los switches con las configuraciones provistas</p> <p>Configuración de S1</p> <pre> enable ! config term hostname S1 enable secret class no ip domain-lookup ! vtp mode server vtp domain lab6_3 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 ! interface FastEthernet0/2 switchport trunk native vlan 99 switchport mode access ! interface FastEthernet0/3 switchport trunk native vlan 99 switchport mode access </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> 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 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 </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Configuración de S2</p> <pre> hostname S2 ! enable secret class no ip domain-lookup ! vtp mode client vtp domain Lab4 ! ! interface FastEthernet0/1 switchport trunk native vlan 99 switchport mode access ! interface FastEthernet0/2 switchport trunk native vlan 99 switchport mode access ! 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 </pre>

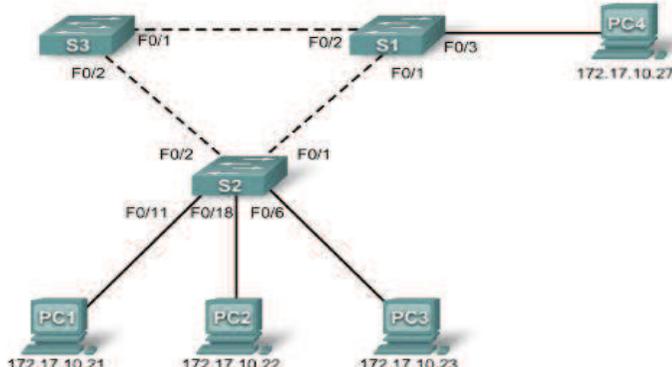
Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> switchport mode access ! interface range FastEthernet0/11 - 17 switchport access vlan 20 switchport mode access ! interface range FastEthernet0/18 - 24 switchport access vlan 30 switchport mode access ! interface Vlan99 ip 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 </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre>! ! 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</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre>! 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 no shutdown ! line con 0 password cisco login line vty 0 4 password cisco login line vty 5 15 password cisco login end</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Tarea 3: Diagnosticar y corregir errores de VTP y de configuración</p> <p>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.</p> <p>Tarea 4: Documentar la configuración del switch</p> <p>Cuando haya completado su diagnóstico de fallas, capture el resultado del comando show run y guárdelo en un archivo de texto para cada switch.</p> <p>Tarea 5: Limpieza</p> <p>Borre las configuraciones y vuelva a cargar los switches. Desconecte y guarde el cableado. En caso de los equipos 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.</p> <p><i>Tomado del Material de Cisco CCNA para efectos educativos: Cisco Networking Academy 1992-2007</i></p> <p>Entrega un informe de las actividades realizadas en la práctica, formando el portafolio de evidencias.</p> <p> ADVERTENCIA DE RIESGO ELÉCTRICO</p>

Unidad de aprendizaje:	Administración de redes de área local virtuales.	Número:	3
Práctica	Configuración básica del protocolo Spaning Tree de acuerdo a topología.	Número:	14
Propósito de la práctica	Llevar a cabo las tareas de configuración básica del Protocolo Spaning Tree de acuerdo a una topología o diseño específico, para su uso.		
Escenario	Laboratorio de informática	Duración	2 hrs.

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
<p>4 Estaciones de trabajo 3 switches. 4 cables directo. 3 cables de cruzados.</p>	<ul style="list-style-type: none"> • Aplica las siguientes medidas de seguridad e higiene en el desarrollo de la práctica: <ul style="list-style-type: none"> - Evita la manipulación de comida o líquidos cerca del equipo de cómputo - No introduce objetos extraños en las entradas físicas de dispositivos de la computadora - No utiliza imanes cerca de discos compactos, memorias extraíbles ó de la computadora - Limpia el área de trabajo, prepara herramientas y los materiales a utilizar ☺ Utilizar las hojas por ambas caras y colocar las de desecho las en el recipiente destinado para su posterior envío a reciclaje <p>NOTA El docente deberá adecuar la práctica al equipo y recursos de software con el que se cuenta.</p> <p>Diagrama de topología</p> 

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños																																								
	<p>Tabla de direccionamiento</p> <table border="1" data-bbox="898 331 1912 692"> <thead> <tr> <th>Dispositivo Nombre de host</th> <th>Interfaz</th> <th>Dirección IP</th> <th>Máscara de subred</th> <th>Gateway predeterminada</th> </tr> </thead> <tbody> <tr> <td>S1</td> <td>VLAN 1</td> <td>172.17.10.1</td> <td>255.255.255.0</td> <td>N/C</td> </tr> <tr> <td>S2</td> <td>VLAN 1</td> <td>172.17.10.2</td> <td>255.255.255.0</td> <td>N/C</td> </tr> <tr> <td>S3</td> <td>VLAN 1</td> <td>172.17.10.3</td> <td>255.255.255.0</td> <td>N/C</td> </tr> <tr> <td>PC1</td> <td>NIC</td> <td>172.17.10.21</td> <td>255.255.255.0</td> <td>172.17.10.254</td> </tr> <tr> <td>PC2</td> <td>NIC</td> <td>172.17.10.22</td> <td>255.255.255.0</td> <td>172.17.10.254</td> </tr> <tr> <td>PC3</td> <td>NIC</td> <td>172.17.10.23</td> <td>255.255.255.0</td> <td>172.17.10.254</td> </tr> <tr> <td>PC4</td> <td>NIC</td> <td>172.17.10.27</td> <td>255.255.255.0</td> <td>172.17.10.254</td> </tr> </tbody> </table> <p>Tarea 1: Realizar las configuraciones básicas del switch</p> <p>Paso 1: Cablee una red de manera similar al diagrama de topología.</p> <p>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.</p> <p>Establezca conexiones de consola en los tres switches.</p> <p>Paso 2: Borre toda configuración existente en los switches.</p> <p>Borre la NVRAM, borre el archivo vlan.dat y reinicie los switches. Consulte la Práctica de laboratorio 2.5.1 para el procedimiento. Después de que la recarga se haya completado, utilice el comando privilegiado EXEC <code>show vlan</code> para verificar que sólo existan Vlan predeterminadas y que todos los puertos se asignen a VLAN 1.</p>	Dispositivo Nombre de host	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminada	S1	VLAN 1	172.17.10.1	255.255.255.0	N/C	S2	VLAN 1	172.17.10.2	255.255.255.0	N/C	S3	VLAN 1	172.17.10.3	255.255.255.0	N/C	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
Dispositivo Nombre de host	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminada																																					
S1	VLAN 1	172.17.10.1	255.255.255.0	N/C																																					
S2	VLAN 1	172.17.10.2	255.255.255.0	N/C																																					
S3	VLAN 1	172.17.10.3	255.255.255.0	N/C																																					
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																																					

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> 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 Gig0/1, Gig0/2 1002 fddi-default active 1003 token-ring-default active 1004 fddinet-default active 1005 trnet-default active </pre> <p>Paso 3: Configure los parámetros básicos del switch.</p> <p>Configure los switches S1, S2 y S3 según las siguientes pautas:</p> <ul style="list-style-type: none"> • 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.

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre>(Se muestran los resultados para S1) Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# hostname S1 S1(config)#enable secret class S1(config)#no ip domain-lookup S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#end %SYS-5-CONFIG_I: Configured from console by console S1#copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK]</pre> <p>Tarea 2: Preparar la red</p> <p>Paso 1: Deshabilite todos los puertos con el comando shutdown.</p> <p>Asegúrese de que los estados del puerto de switch estén inactivos con el comando shutdown. Simplifique esta tarea con el comando interface range.</p> <pre>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</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Paso 2: Vuelva a habilitar los puertos de usuario en S1 y S2 en modo de acceso.</p> <p>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.</p> <pre>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</pre> <p>Paso 3: Habilite los puertos de enlace troncal en S1, S2 y S3.</p> <p>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.</p> <pre>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</pre> <p>Paso 4: Configure la dirección de la interfaz de administración en los tres switches.</p> <pre>S1(config)#interface vlan1 S1(config-if)#ip address 172.17.10.1 255.255.255.0 S1(config-if)#no shutdown</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre>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</pre> <p>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.</p> <p>¿Los pings son exitosos? _____</p> <p>En caso contrario, realice el diagnóstico de fallas de las configuraciones de los switches e inténtelo nuevamente.</p> <p>Tarea 3: Configurar las PC host</p> <p>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.</p> <p>Tarea 4: Configurar Spanning Tree</p> <p>Paso 1: Examine la configuración predeterminada de 802.1D STP.</p> <p>En cada switch, muestre la tabla de spanning tree con el comando <code>show spanning-tree</code>. La selección de la raíz varía según el BID de cada switch en su práctica de laboratorio, dando lugar a varios resultados.</p> <pre>S1#show spanning-tree VLAN0001 Spanning tree enabled protocol ieee Root ID Priority 32769 Address 0019.068d.6980</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> 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 </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> 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 ELK 19 128.2 P2p </pre> <p>Paso 2: Examine el resultado.</p> <p>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 <i>bridge ID priority</i> (prioridad de id de puente). La extensión 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. Con el valor predeterminado de la prioridad de puente de 32 768, la <i>bridge ID priority</i> para la VLAN 100 debe ser 32 868 (32 768 + 100).</p> <p>El comando <code>show spanning-tree</code> muestra el valor de la <i>bridge ID priority</i>. 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.</p> <p>Responda las siguientes preguntas en base al resultado.</p> <ol style="list-style-type: none"> ¿Cuál es la prioridad ID de puente para los switches S1, S2 y S3 en VLAN 1? <ol style="list-style-type: none"> S1 _____ S2 _____ S3 _____

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>2. ¿Qué switch es la raíz para el spanning tree de VLAN 1? _____</p> <p>3. ¿Qué puertos del spanning tree están en estado de bloqueo en el switch raíz? _____</p> <p>4. ¿Alguno de los switches que no son raíz tiene un puerto de bloqueo? _____ ¿Qué switch y qué puerto están en el estado de bloqueo? _____</p> <p>5. ¿Cómo elige el STP el switch raíz? _____</p> <p>6. Ya que las prioridades de puente son las mismas, ¿qué más usa el switch para determinar la raíz? _____</p> <p>Tarea 5: Observar la respuesta al cambio de topología en 802.1D STP</p> <p>Observemos qué pasa cuando simulamos intencionalmente un enlace roto</p> <p>Paso 1: Ponga los switches en modo spanning tree debug con el comando debug spanning-tree events.</p> <pre>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</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Paso 2: Desactive de forma intencional un puerto en el switch raíz. Este ejemplo utiliza a S1, ya que es la raíz. Su switch raíz puede variar.</p> <pre>S1(config)#interface fa0/1 S1(config-if)#shutdown</pre> <p>Paso 3: Registre el resultado de depuración de los switches que no son raíz. En este ejemplo registramos el resultado de S2 y S3, pues son los switches que no son raíz.</p> <pre>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 32769-0019.0c68d.6980 on Fa0/2 1w2d: supersedes 32769-001b.0c68.2080 1w2d: STP: VLAN0001 new root is 32769, 0019.0c68d.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</pre>

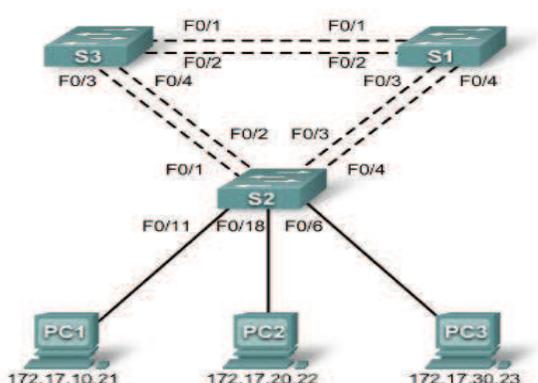
Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>De acuerdo al resultado de este ejemplo, cuando el enlace de S2 que está conectado al switch raíz se desactiva, ¿cuál es la conclusión inicial sobre la raíz spanning tree?_____</p> <p>Una vez que S2 recibe la nueva información en Fa0/2, ¿qué nueva conclusión saca?_____</p> <p>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? _____</p> <p>Paso 4: Examine lo que ha cambiado en la topología del spanning tree con el comando spanning tree.</p> <p>S2#show spanning-tree</p> <pre>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</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre>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</pre> <p>Responda las siguientes preguntas en base al resultado.</p> <ol style="list-style-type: none"> 1. ¿Qué ha cambiado en la manera en que S2 envía el tráfico? _____ 2. ¿Qué ha cambiado en la manera en que S3 envía el tráfico? _____ <p>Tarea 6: Registrar la configuración de cada switch con el comando show run</p> <pre>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 !</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> ! <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 </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> 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 </pre> <p>Tarea 7: Limpieza</p> <p>Borre las configuraciones y recargue las configuraciones predeterminadas de los switches. Desconecte y guarde el cableado. En caso de los equipos hosts que están normalmente conectados 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.</p> <p>Tomado del Material de Cisco CCNA para efectos educativos: Cisco Networking Academy 1992-2007 Entrega un informe de las actividades realizadas en la práctica, formando el portafolio de evidencias.</p> <p> ADVERTENCIA DE RIESGO ELÉCTRICO</p>

Unidad de aprendizaje:	Administración de redes de área local virtuales.	Número:	3
Práctica	Resolución de problemas en la configuración del Protocolo Spanning Tree siguiendo procedimiento.	Número:	15
Propósito de la práctica	Encontrar y corregir todos los errores de configuración de switches, siguiendo procedimiento, para el funcionamiento del Protocolo Spanning Tree.		
Escenario	Laboratorio de informática	Duración	2 hrs.

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
<p>3 Estaciones de trabajo 3 switches. 3 cables directo. 6 cables de cruzados.</p>	<ul style="list-style-type: none"> • Aplica las siguientes medidas de seguridad e higiene en el desarrollo de la práctica: <ul style="list-style-type: none"> - Evita la manipulación de comida o líquidos cerca del equipo de cómputo - No introduce objetos extraños en las entradas físicas de dispositivos de la computadora - No utiliza imanes cerca de discos compactos, memorias extraíbles ó de la computadora - Limpia el área de trabajo, prepara herramientas y los materiales a utilizar ☺ Utilizar las hojas por ambas caras y colocar las de desecho las en el recipiente destinado para su posterior envío a reciclaje <p>NOTA El docente deberá adecuar la práctica al equipo y recursos de software con el que se cuenta.</p> <p>Diagrama de topología</p>  <pre> graph TD S3 --- F0/1 S1 S3 --- F0/2 S1 S3 --- F0/3 S1 S3 --- F0/4 S1 S1 --- F0/1 S2 S1 --- F0/2 S2 S1 --- F0/3 S2 S1 --- F0/4 S2 S2 --- F0/1 PC1 S2 --- F0/18 PC2 S2 --- F0/6 PC3 </pre> <p>IP addresses: PC1 (172.17.10.21), PC2 (172.17.20.22), PC3 (172.17.30.23)</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños																																																		
	<p data-bbox="1010 323 1305 347">Tabla de direccionamiento</p> <table border="1" data-bbox="1016 360 1935 627"> <thead> <tr> <th>Dispositivo Nombre de host</th> <th>Interfaz</th> <th>Dirección IP</th> <th>Máscara de subred</th> <th>Gateway predeterminado</th> </tr> </thead> <tbody> <tr> <td>S1</td> <td>VLAN 99</td> <td>172.17.99.11</td> <td>255.255.255.0</td> <td>N/C</td> </tr> <tr> <td>S2</td> <td>VLAN 99</td> <td>172.17.99.12</td> <td>255.255.255.0</td> <td>N/C</td> </tr> <tr> <td>S3</td> <td>VLAN 99</td> <td>172.17.99.13</td> <td>255.255.255.0</td> <td>N/C</td> </tr> <tr> <td>PC1</td> <td>NIC</td> <td>172.17.10.21</td> <td>255.255.255.0</td> <td>172.17.10.1</td> </tr> <tr> <td>PC2</td> <td>NIC</td> <td>172.17.20.22</td> <td>255.255.255.0</td> <td>172.17.20.1</td> </tr> <tr> <td>PC3</td> <td>NIC</td> <td>172.17.30.23</td> <td>255.255.255.0</td> <td>172.17.30.1</td> </tr> </tbody> </table> <p data-bbox="965 683 1406 707">Asignaciones de puerto – Switch 2</p> <table border="1" data-bbox="1066 783 1928 986"> <thead> <tr> <th>Puertos</th> <th>Asignaciones</th> <th>Red</th> </tr> </thead> <tbody> <tr> <td>Fa0/1 – 0/4</td> <td>Enlaces troncales 802.1q (VLAN nativa 99)</td> <td>172.17.99.0 /24</td> </tr> <tr> <td>Fa0/5 – 0/10</td> <td>VLAN 30 – Guest (Default)</td> <td>172.17.30.0 /24</td> </tr> <tr> <td>Fa0/11 – 0/17</td> <td>VLAN 10 – Faculty/Staff</td> <td>172.17.10.0 /24</td> </tr> <tr> <td>Fa0/18 – 0/24</td> <td>VLAN 20 – Students</td> <td>172.17.20.0 /24</td> </tr> </tbody> </table> <p data-bbox="889 1034 1008 1058">Situación</p> <p data-bbox="902 1082 1995 1265">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. Reconoce que de los seis enlaces troncales configurados, únicamente dos envían paquetes en la configuración predeterminada actualmente en ejecución del STP. 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.</p> <p data-bbox="902 1286 1980 1334">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.</p>	Dispositivo Nombre de host	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado	S1	VLAN 99	172.17.99.11	255.255.255.0	N/C	S2	VLAN 99	172.17.99.12	255.255.255.0	N/C	S3	VLAN 99	172.17.99.13	255.255.255.0	N/C	PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1	PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1	PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1	Puertos	Asignaciones	Red	Fa0/1 – 0/4	Enlaces troncales 802.1q (VLAN nativa 99)	172.17.99.0 /24	Fa0/5 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24	Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24	Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24
Dispositivo Nombre de host	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado																																															
S1	VLAN 99	172.17.99.11	255.255.255.0	N/C																																															
S2	VLAN 99	172.17.99.12	255.255.255.0	N/C																																															
S3	VLAN 99	172.17.99.13	255.255.255.0	N/C																																															
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1																																															
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1																																															
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1																																															
Puertos	Asignaciones	Red																																																	
Fa0/1 – 0/4	Enlaces troncales 802.1q (VLAN nativa 99)	172.17.99.0 /24																																																	
Fa0/5 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24																																																	
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24																																																	
Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24																																																	

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Tarea 1: Preparar la red</p> <p>Paso 1: Conecte una red que sea similar a la del diagrama de topología.</p> <p>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.</p> <p>Establezca conexiones de consola en los tres switches.</p> <p>Paso 2: Borre toda configuración existente en los switches.</p> <p>Borre la NVRAM, borre el archivo vlan.dat y reinicie los switches.</p> <p>Paso 3: Cargue los switches con la siguiente configuración:</p> <p>Configuración de S1</p> <pre>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</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> ! 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 ! </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> 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 </pre>

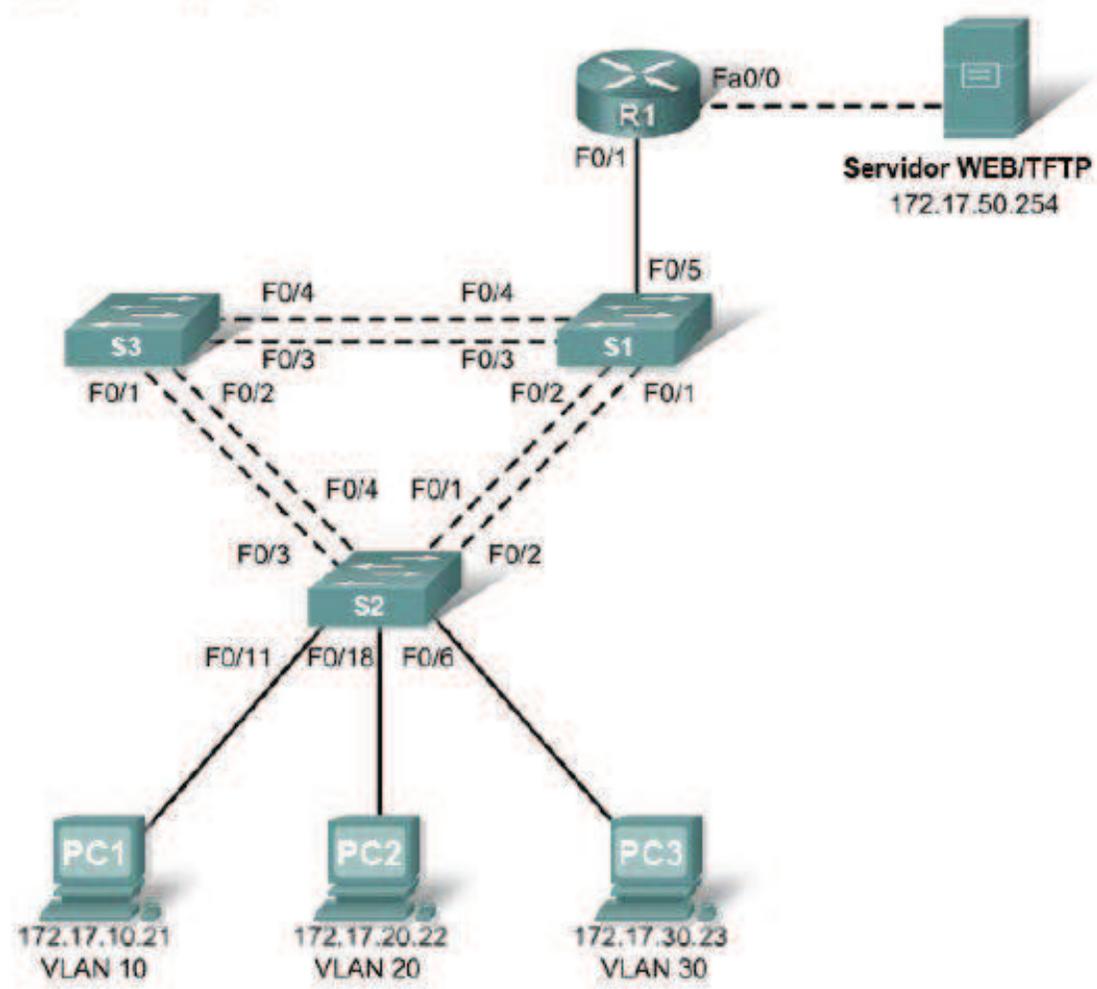
Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> ! interface FastEthernet0/2 switchport trunk native vlan 99 switchport mode trunk no shutdown ! interface FastEthernet0/3 switchport trunk native vlan 99 switchport mode trunk no shutdown ! interface FastEthernet0/4 switchport 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 ! interfaz fa0/6 no shutdown interfaz fa0/11 no shutdown interfaz fa0/18 no shutdown ! </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> 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 </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> 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 </pre> <p>Tarea 2: Configurar las PC host</p> <p>Configure las interfaces Ethernet de PC1, PC2 y PC3 con la dirección IP, la máscara de subred y el gateway que se indican en la tabla de direccionamiento.</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Tarea 3: Identificar el estado inicial de todos los enlaces troncales</p> <p>En cada switch, muestre la tabla de spanning tree con el comando <code>show spanning-tree</code>. 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.</p> <p>Tarea 4: Modificar spanning tree para lograr el balanceo de cargas</p> <p>Modifique la configuración de spanning tree de manera que los seis enlaces troncales estén en uso. Asuma que las tres LAN del usuario (10, 20 y 30) transportan la misma cantidad 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.</p> <p>Tarea 5: Documentar la configuración del switch</p> <p>Cuando haya completado su solución, capture el resultado del comando <code>show run</code> y guárdelo en un archivo de texto para cada switch.</p> <p>Tarea 6: Limpiar</p> <p>Borre las configuraciones y vuelva a cargar los switches. Desconecte y guarde los cables. Para las computadoras host que normalmente se conectan a otras redes (tales como la LAN de la escuela o Internet), reconecte los cables correspondientes y restablezca las configuraciones TCP/IP.</p> <p><i>Tomado del Material de Cisco CCNA para efectos educativos: Cisco Networking Academy 1992-2007</i></p> <p>Entrega un informe de las actividades realizadas en la práctica, formando el portafolio de evidencias.</p> <p> ADVERTENCIA DE RIESGO ELÉCTRICO</p>

Unidad de aprendizaje:	Administración de redes de área local virtuales.	Número:	3
Práctica	Realiza la configuración del enrutamiento básico entre VLANs siguiendo procedimiento.	Número:	16
Propósito de la práctica	Realizar las tareas básicas de configuración en una LAN conmutada y un router, siguiendo procedimiento, para su operación.		
Escenario	Laboratorio de informática	Duración	2 hrs.
Materiales, Herramientas, Instrumental, Maquinaria y Equipo.		Desempeños	
3 Estaciones de trabajo 3 switches. 1 Router 1 Servidor Web/FTP 3 cables directo. 6 cables de cruzados.		<ul style="list-style-type: none"> • Aplica las siguientes medidas de seguridad e higiene en el desarrollo de la práctica: <ul style="list-style-type: none"> - Evita la manipulación de comida o líquidos cerca del equipo de cómputo - No introduce objetos extraños en las entradas físicas de dispositivos de la computadora - No utiliza imanes cerca de discos compactos, memorias extraíbles ó de la computadora - Limpia el área de trabajo, prepara herramientas y los materiales a utilizar ↻ Utilizar las hojas por ambas caras y colocar las de desecho las en el recipiente destinado para su posterior envío a reciclaje <p>NOTA El docente deberá adecuar la práctica al equipo y recursos de software con el que se cuenta.</p>	

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Diagrama de topología</p>  <p>The diagram illustrates a network topology with the following components and connections:</p> <ul style="list-style-type: none"> Switches: S1, S2, and S3. S1 and S2 are connected to S3 via dashed lines (F0/4 to F0/4, F0/3 to F0/3, F0/2 to F0/2). Router: R1 is connected to S1 (F0/1 to F0/5) and S2 (F0/1 to F0/4). Server: Servidor WEB/TFTP (172.17.50.254) is connected to R1 (Fa0/0). PCs: PC1 (172.17.10.21, VLAN 10) is connected to S2 (F0/11 to F0/6). PC2 (172.17.20.22, VLAN 20) is connected to S2 (F0/18 to F0/6). PC3 (172.17.30.23, VLAN 30) is connected to S2 (F0/6 to F0/6).

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños																																																																																			
	<p>Tabla de direccionamiento</p> <table border="1"> <thead> <tr> <th>Dispositivo Nombre de host</th> <th>Interfaz</th> <th>Dirección IP</th> <th>Máscara de subred</th> <th>Gateway predeterminado</th> </tr> </thead> <tbody> <tr> <td>S1</td> <td>VLAN 99</td> <td>172.17.99.11</td> <td>255.255.255.0</td> <td>172.17.99.1</td> </tr> <tr> <td>S2</td> <td>VLAN 99</td> <td>172.17.99.12</td> <td>255.255.255.0</td> <td>172.17.99.1</td> </tr> <tr> <td>S3</td> <td>VLAN 99</td> <td>172.17.99.13</td> <td>255.255.255.0</td> <td>172.17.99.1</td> </tr> <tr> <td>R1</td> <td>Fa 0/0</td> <td>172.17.50.1</td> <td>255.255.255.0</td> <td>N/C</td> </tr> <tr> <td>R1</td> <td>Fa 0/1</td> <td colspan="2">Ver tabla de configuración de interfaz</td> <td>N/C</td> </tr> <tr> <td>PC1</td> <td>NIC</td> <td>172.17.10.21</td> <td>255.255.255.0</td> <td>172.17.10.1</td> </tr> <tr> <td>PC2</td> <td>NIC</td> <td>172.17.20.22</td> <td>255.255.255.0</td> <td>172.17.20.1</td> </tr> <tr> <td>PC3</td> <td>NIC</td> <td>172.17.30.23</td> <td>255.255.255.0</td> <td>172.17.30.1</td> </tr> <tr> <td>Server</td> <td>NIC</td> <td>172.17.50.254</td> <td>255.255.255.0</td> <td>172.17.50.1</td> </tr> </tbody> </table> <p>Asignaciones de puerto – Switch 2</p> <table border="1"> <thead> <tr> <th>Puertos</th> <th>Asignaciones</th> <th>Red</th> </tr> </thead> <tbody> <tr> <td>Fa0/1 – 0/5</td> <td>Enlaces troncales 802.1q (VLAN nativa 99)</td> <td>172.17.99.0 /24</td> </tr> <tr> <td>Fa0/6 – 0/10</td> <td>VLAN 30 – Guest (Default)</td> <td>172.17.30.0 /24</td> </tr> <tr> <td>Fa0/11 – 0/17</td> <td>VLAN 10 – Faculty/Staff</td> <td>172.17.10.0 /24</td> </tr> <tr> <td>Fa0/18 – 0/24</td> <td>VLAN 20 – Students</td> <td>172.17.20.0 /24</td> </tr> </tbody> </table> <p>Tabla de configuración de la interfaz – Router 1</p> <table border="1"> <thead> <tr> <th>Interfaz</th> <th>Asignaciones</th> <th>Dirección IP</th> </tr> </thead> <tbody> <tr> <td>Fa0/1.1</td> <td>Dirección de</td> <td>172.17.1.1 /24</td> </tr> <tr> <td>Fa0/1.10</td> <td>VLAN 10</td> <td>172.17.10.1 /24</td> </tr> <tr> <td>Fa0/1.20</td> <td>VLAN 20</td> <td>172.17.20.1 /24</td> </tr> <tr> <td>Fa0/1.30</td> <td>VLAN 30</td> <td>172.17.30.1 /24</td> </tr> <tr> <td>Fa0/1.99</td> <td>VLAN 99</td> <td>172.17.99.1 /24</td> </tr> </tbody> </table>	Dispositivo Nombre de host	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado	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	N/C	R1	Fa 0/1	Ver tabla de configuración de interfaz		N/C	PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1	PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1	PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1	Server	NIC	172.17.50.254	255.255.255.0	172.17.50.1	Puertos	Asignaciones	Red	Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN nativa 99)	172.17.99.0 /24	Fa0/6 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24	Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24	Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24	Interfaz	Asignaciones	Dirección IP	Fa0/1.1	Dirección de	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
Dispositivo Nombre de host	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado																																																																																
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	N/C																																																																																
R1	Fa 0/1	Ver tabla de configuración de interfaz		N/C																																																																																
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1																																																																																
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1																																																																																
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1																																																																																
Server	NIC	172.17.50.254	255.255.255.0	172.17.50.1																																																																																
Puertos	Asignaciones	Red																																																																																		
Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN nativa 99)	172.17.99.0 /24																																																																																		
Fa0/6 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24																																																																																		
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24																																																																																		
Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24																																																																																		
Interfaz	Asignaciones	Dirección IP																																																																																		
Fa0/1.1	Dirección de	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																																																																																		

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños																		
	<p>Tarea 1: Preparar la red</p> <p>Paso 1: Conecte una red que sea similar a la del diagrama de topología.</p> <p>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.</p> <p>Establezca conexiones de consola en los tres switches y en el router.</p> <p>Paso 2: Borre toda configuración existente en los switches.</p> <p>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 <code>show vlan</code> para verificar que solo existan VLAN predeterminadas y que todos los puertos se asignen a la VLAN 1.</p> <pre>Switch#show vlan</pre> <table border="1" data-bbox="891 836 1957 1177"> <thead> <tr> <th>VLAN Name</th> <th>Status</th> <th>Ports</th> </tr> </thead> <tbody> <tr> <td>1 default</td> <td>active</td> <td>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</td> </tr> <tr> <td>1002 fddi-default</td> <td>active</td> <td></td> </tr> <tr> <td>1003 token-ring-default</td> <td>active</td> <td></td> </tr> <tr> <td>1004 fddinet-default</td> <td>active</td> <td></td> </tr> <tr> <td>1005 trnet-default</td> <td>active</td> <td></td> </tr> </tbody> </table> <p>Paso 3: Deshabilite todos los puertos usando el comando shutdown.</p> <p>Asegúrese de que los estados del puerto de switch estén inactivos deshabilitando todos los puertos. Simplifique esta tarea con el comando <code>interface range</code>. Repita estos comandos para cada switch de la topología.</p>	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 Gig0/1, Gig0/2	1002 fddi-default	active		1003 token-ring-default	active		1004 fddinet-default	active		1005 trnet-default	active	
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 Gig0/1, Gig0/2																	
1002 fddi-default	active																		
1003 token-ring-default	active																		
1004 fddinet-default	active																		
1005 trnet-default	active																		

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre>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</pre> <p>Tarea 2: Realizar las configuraciones básicas del switch</p> <p>Paso 1: Configurar los switches S1, S2 y S3.</p> <p>Utilice la tabla de direccionamiento y las siguientes pautas:</p> <ul style="list-style-type: none"> • 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 vty. • Configure el gateway predeterminado en cada switch. <p>Se muestran los resultados para S1</p> <pre>Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#hostname S1 S1(config)#enable secret class S1(config)#no ip domain-lookup S1(config)#ip default-gateway 172.17.99.1 S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#end %SYS-5-CONFIG_I: Configured from console by console S1#copy running-config startup-config Destination filename [startup-config]? [Intro] Building configuration...</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños																
	<p>Paso 2: Vuelva a habilitar los puertos de usuario activos en S2 en el modo de acceso.</p> <pre>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</pre> <p>Tarea 3: Configurar las interfaces Ethernet en las computadoras Host</p> <p>Configure las interfaces Ethernet de PC1, PC2, PC3 y el Servidor TFTP/Web remoto con las direcciones IP de la tabla de direccionamiento.</p> <p>Tarea 4: Configurar VTP en los switches</p> <p>Paso 1: Configure VTP en los tres switches utilizando la siguiente tabla. Recuerde que los nombres de dominio VTP y las contraseñas distinguen mayúsculas de minúsculas.</p> <table border="1" data-bbox="904 900 1973 1070"> <thead> <tr> <th>Nombre del switch</th> <th>Modo de operación VTP</th> <th>Dominio VTP</th> <th>Contraseña de VTP</th> </tr> </thead> <tbody> <tr> <td>S1</td> <td>Servidor</td> <td>Lab6</td> <td>cisco</td> </tr> <tr> <td>S2</td> <td>Cliente</td> <td>Lab6</td> <td>cisco</td> </tr> <tr> <td>S3</td> <td>Cliente</td> <td>Lab6</td> <td>cisco</td> </tr> </tbody> </table>	Nombre del switch	Modo de operación VTP	Dominio VTP	Contraseña de VTP	S1	Servidor	Lab6	cisco	S2	Cliente	Lab6	cisco	S3	Cliente	Lab6	cisco
Nombre del switch	Modo de operación VTP	Dominio VTP	Contraseña de VTP														
S1	Servidor	Lab6	cisco														
S2	Cliente	Lab6	cisco														
S3	Cliente	Lab6	cisco														

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>S1:</p> <pre>S1(config)#vtp mode server Device mode already VTP SERVER. S1(config)#vtp domain Lab6 Changing VTP domain name from NULL to Lab6 S1(config)#vtp password cisco Setting device VLAN database password to cisco S1(config)#end</pre> <p>S2:</p> <pre>S2(config)#vtp mode client Setting device to VTP CLIENT mode S2(config)#vtp domain Lab6 Changing VTP domain name from NULL to Lab6 S2(config)#vtp password cisco Setting device VLAN database password to cisco S2(config)#end</pre> <p>S3:</p> <pre>S3(config)#vtp mode client Setting device to VTP CLIENT mode S3(config)#vtp domain Lab6 Changing VTP domain name from NULL to Lab6 S3(config)#vtp password cisco Setting device VLAN database password to cisco S3(config)#end</pre> <p>Paso 2: Configure los puertos de enlace troncales y designe la VLAN nativa para los enlaces troncales.</p> <p>Configure desde Fa0/1 hasta Fa0/5 como puertos de enlace troncal y designe la VLAN 99 como VLAN nativa para estos enlaces troncales. Simplifique esta tarea con el comando <code>interface range</code> en el modo de configuración global.</p> <pre>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</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños										
	<pre>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</pre> <p>Paso 3: Configure las VLAN en el servidor VTP. Configure las siguientes VLAN en el servidor VTP:</p> <table border="1" data-bbox="1124 778 1789 949"> <thead> <tr> <th>VLAN</th> <th>Nombre de VLAN</th> </tr> </thead> <tbody> <tr> <td>VLAN 99</td> <td>management</td> </tr> <tr> <td>VLAN 10</td> <td>faculty-staff</td> </tr> <tr> <td>VLAN 20</td> <td>students</td> </tr> <tr> <td>VLAN 30</td> <td>guest</td> </tr> </tbody> </table> <pre>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)#end</pre> <p>Verifique que las VLAN se creen en S1 con el comando <code>show vlan brief</code>.</p>	VLAN	Nombre de VLAN	VLAN 99	management	VLAN 10	faculty-staff	VLAN 20	students	VLAN 30	guest
VLAN	Nombre de VLAN										
VLAN 99	management										
VLAN 10	faculty-staff										
VLAN 20	students										
VLAN 30	guest										

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Paso 4: Verificar que las VLAN creadas en S1 se hayan distribuido a S2 y S3.</p> <p>Use el comando <code>show vlan brief</code> en S2 y S3 para verificar que las cuatro VLAN se hayan distribuido a los switches clientes.</p> <p>S2#show vlan brief</p> <pre> VLAN Name Status Ports ----- 1 default active Fa0/1, Fa0/2, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2 10 faculty-staff active 20 students active 30 guest active 99 management active </pre> <p>Paso 5: Configure la dirección de la interfaz de administración en los tres switches.</p> <pre> S1(config)#interface vlan 99 S1(config-if)#ip address 172.17.99.11 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#end S2(config)#interface vlan 99 S2(config-if)#ip address 172.17.99.12 255.255.255.0 S2(config-if)#no shutdown S2(config-if)#end S3(config)#interface vlan 99 S3(config-if)#ip address 172.17.99.13 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#end </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Verifique que todos los switches estén correctamente configurados haciendo ping entre ellos. Desde S1, haga ping en la interfaz de administración de S2 y S3. Desde S2, haga ping a la interfaz de administración en S3.</p> <p>¿Los pings tuvieron éxito? _____</p> <p>En caso contrario, resuelva los problemas de las configuraciones de los switches e inténtelo nuevamente.</p> <p>Paso 6: Asigne puertos de switch a las VLAN en S2.</p> <p>Consulte la tabla de asignación de puertos al principio de la práctica de laboratorio para asignar puertos a las VLAN.</p> <pre>S2(config)#interface range fa0/6-10 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]? [Intro] Building configuration... [OK]</pre> <p>Paso 7: Verifique la conectividad entre las VLAN.</p> <p>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).</p> <p>¿Los pings son satisfactorios? _____</p> <p>En caso contrario ¿por qué fallan? _____</p> <p>_____</p> <p>_____</p> <p>Tarea 5: Configurar el Router y la LAN con servidor remoto</p> <p>Paso 1: Borre la configuración en el router y vuelva a cargar.</p> <pre>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</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Paso 2: Cree una configuración básica en el router.</p> <ul style="list-style-type: none"> • 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 vty. <p>Paso 3: Configure la interfaz de enlaces troncales en R1.</p> <p>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.</p> <p>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 que utiliza el dispositivo L3 se configura 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 para este enfoque son la falta de puertos suficientes de Fast Ethernet en los routers, la utilización insuficiente de los puertos en los switches de L3 y los routers, el cableado excesivo y la configuración manual. La topología utilizada en esta práctica de laboratorio no emplea este enfoque.</p> <p>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 todo el tráfico entre las VLAN entre y salga del dispositivo de enrutamiento por un enlace troncal único. Sin embargo, requiere que la interfaz de L3 se configure 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.</p> <p>La utilización del enfoque de configuración de subinterfaces requiere estos pasos:</p> <ul style="list-style-type: none"> • Ingresar al modo de configuración de subinterfaz • Establecer encapsulación de enlace troncal • Asociar la VLAN con la subinterfaz • Asignar una dirección IP desde la VLAN a la subinterfaz <p>Los comandos son los siguientes:</p> <pre>R1 (config)#interface fastethernet 0/1 R1 (config-if)#no shutdown</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre>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</pre> <p>Observe los siguientes puntos en esta configuración:</p> <ul style="list-style-type: none"> • La interfaz física se habilita usando el comando <code>no shutdown</code> porque las interfaces de los router están inactivas de manera predeterminada. Las interfaces virtuales están activas de manera predeterminada. • La subinterfaz puede utilizar cualquier número que se pueda describir con 32 bits, pero se aconseja asignar el número de la VLAN como número de la interfaz, como se ha hecho 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. <p>Confirme la creación y el estado de las subinterfaces con el comando <code>show ip interface brief</code>:</p> <pre>R1#show ip interface brief Interface IP-Address OK? Method Status Protocol FastEthernet0/0 unassigned YES unset administratively down down FastEthernet0/1 unassigned YES unset up up FastEthernet0/1.1 172.17.1.1 YES manual up up FastEthernet0/1.10 172.17.10.1 YES manual up up FastEthernet0/1.20 172.17.20.1 YES manual up up FastEthernet0/1.30 172.17.30.1 YES manual up up FastEthernet0/1.99 172.17.99.1 YES manual up up</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Si su tabla de enrutamiento no muestra las seis redes, lleve a cabo la resolución de problemas de su configuración y arregle el problema antes de continuar.</p> <p>Paso 5: Verifique el enrutamiento entre VLAN.</p> <p>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 ser necesario hacer un par de pings antes de que se establezca la ruta de extremo a extremo.</p> <p>¿Los pings son satisfactorios? _____</p> <p>En caso contrario, lleve a cabo la resolución de problemas de su configuración. Verifique para asegurarse de que los gateways predeterminados se han establecido en todas las PC y en todos los switches. Si alguno de los hosts ha pasado a hibernación, la interfaz conectada se puede desactivar.</p> <p>Paso 4: Configure la interfaz de servidor LAN en R1.</p> <pre>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</pre> <p>Ahora hay seis redes configuradas. Verifique que pueda enrutar paquetes a las seis mediante la verificación en la tabla de enrutamiento en R1.</p> <pre>R1#show ip route <se omite el resultado></pre> <pre>Gateway of last resort is not set</pre> <pre> 172.17.0.0/24 is subnetted, 6 subnets C 172.17.50.0 is directly connected, FastEthernet0/0 C 172.17.30.0 is directly connected, FastEthernet0/1.30 C 172.17.20.0 is directly connected, FastEthernet0/1.20 C 172.17.10.0 is directly connected, FastEthernet0/1.10 C 172.17.1.0 is directly connected, FastEthernet0/1.1 C 172.17.99.0 is directly connected, FastEthernet0/1.99</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Tarea 6: Reflexionar</p> <p>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?</p> <hr/> <hr/> <hr/> <hr/> <p>Tarea 7: Limpiar</p> <p>Borre las configuraciones y vuelva a cargar los switches. Desconecte y guarde los cables. Para las computadoras host que normalmente se conectan a otras redes (tales como la LAN de la escuela o Internet), reconecte los cables correspondientes y restablezca las configuraciones TCP/IP.</p> <p>Configuraciones finales</p> <p>Router 1</p> <pre>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</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> 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 ! <se omite el resultado - las interfaces seriales no están configuradas> ! 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 ! </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> 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 ! <se omite el resultado - las interfaces seriales no están configuradas> ! interface Vlan1 no ip address no ip route-cache ! interface Vlan99 ip address 172.17.99.11 255.255.255.0 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 </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> 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 trunk native vlan 99 switchport mode trunk ! interface FastEthernet0/6 switchport access vlan 30 switchport mode access ! interface FastEthernet0/7 </pre>

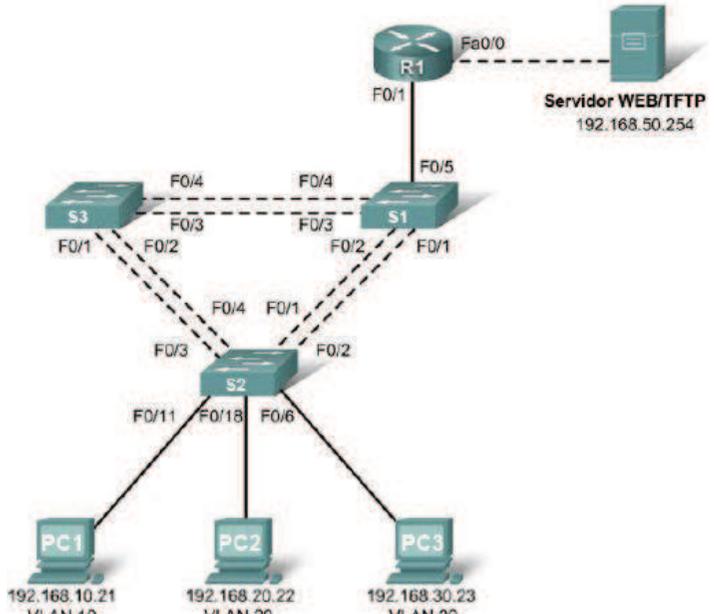
Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> switchport access vlan 30 ! interface FastEthernet0/8 switchport access vlan 30 ! interface FastEthernet0/9 switchport access vlan 30 ! interface FastEthernet0/10 switchport access vlan 30 ! interface FastEthernet0/11 switchport 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 </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> ! 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 Vlan99 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 </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> 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 switchport trunk native vlan 99 switchport mode trunk ! <se omite el resultado - las interfaces seriales no están configuradas> ! interface Vlan99 </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> 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 </pre> <p><i>Tomado del Material de Cisco CCNA para efectos educativos: Cisco Networking Academy 1992-2007</i></p> <p>Entrega un informe de las actividades realizadas en la práctica, formando el portafolio de evidencias.</p> <p> ADVERTENCIA DE RIESGO ELÉCTRICO</p>

Unidad de aprendizaje:	Administración de redes de área local virtuales.	Número:	3
Práctica	Resuelve problemas en la configuración del enrutamiento básico entre VLANs siguiendo procedimiento.	Número:	17
Propósito de la práctica	Encontrar y corregir todos los errores de configuración en el enrutamiento básicos de switches entre VLANs siguiendo procedimiento, para su funcionamiento adecuado.		
Escenario	Laboratorio de informática	Duración	2 hrs.

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
<p>3 Estaciones de trabajo 3 switches. 1 Router 1 Servidor Web/FTP 3 cables directo. 6 cables de cruzados.</p>	<ul style="list-style-type: none"> • Aplica las siguientes medidas de seguridad e higiene en el desarrollo de la práctica: <ul style="list-style-type: none"> - Evita la manipulación de comida o líquidos cerca del equipo de cómputo - No introduce objetos extraños en las entradas físicas de dispositivos de la computadora - No utiliza imanes cerca de discos compactos, memorias extraíbles ó de la computadora - Limpia el área de trabajo, prepara herramientas y los materiales a utiliza • Utilizar las hojas por ambas caras y colocar las de desecho las en el recipiente destinado para su posterior envió a reciclaje <p>NOTA El docente deberá adecuar la práctica al equipo y recursos de software con el que se cuenta.</p> <p>Diagrama de topología</p> 

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños																																																																																			
	<p>Tabla de direccionamiento</p> <table border="1"> <thead> <tr> <th>Dispositivo Nombre de host</th> <th>Interfaz</th> <th>Dirección IP</th> <th>Máscara de subred</th> <th>Gateway (puerta de salida) predeterminado</th> </tr> </thead> <tbody> <tr> <td>S1</td> <td>VLAN 99</td> <td>192.168.99.11</td> <td>255.255.255.0</td> <td>192.168.99.1</td> </tr> <tr> <td>S2</td> <td>VLAN 99</td> <td>192.168.99.12</td> <td>255.255.255.0</td> <td>192.168.99.1</td> </tr> <tr> <td>S3</td> <td>VLAN 99</td> <td>192.168.99.13</td> <td>255.255.255.0</td> <td>192.168.99.1</td> </tr> <tr> <td>R1</td> <td>Fa 0/0</td> <td>192.168.50.1</td> <td>255.255.255.0</td> <td>N/C</td> </tr> <tr> <td>R1</td> <td>Fa 0/1</td> <td colspan="2">Ver tabla de configuración de subinterfaz</td> <td>N/C</td> </tr> <tr> <td>PC1</td> <td>NIC</td> <td>192.168.10.21</td> <td>255.255.255.0</td> <td>192.168.10.1</td> </tr> <tr> <td>PC2</td> <td>NIC</td> <td>192.168.20.22</td> <td>255.255.255.0</td> <td>192.168.20.1</td> </tr> <tr> <td>PC3</td> <td>NIC</td> <td>192.168.30.23</td> <td>255.255.255.0</td> <td>192.168.30.1</td> </tr> <tr> <td>Server</td> <td>NIC</td> <td>192.168.50.254</td> <td>255.255.255.0</td> <td>192.168.50.1</td> </tr> </tbody> </table> <p>Asignaciones de puerto – Switch 2</p> <table border="1"> <thead> <tr> <th>Puertos</th> <th>Asignación</th> <th>Red</th> </tr> </thead> <tbody> <tr> <td>Fa0/1 – 0/5</td> <td>Enlaces troncales 802.1q (VLAN 99 nativa)</td> <td>192.168.99.0 /24</td> </tr> <tr> <td>Fa0/6 – 0/10</td> <td>VLAN 30 – Sales</td> <td>192.168.30.0 /24</td> </tr> <tr> <td>Fa0/11 – 0/17</td> <td>VLAN 10 – R&D</td> <td>192.168.10.0 /24</td> </tr> <tr> <td>Fa0/18 – 0/24</td> <td>VLAN 20 – Engineering</td> <td>192.168.20.0 /24</td> </tr> </tbody> </table> <p>Tabla de configuración de subinterfaces – Router 1</p> <table border="1"> <thead> <tr> <th>Interfaz del router</th> <th>Asignación</th> <th>Dirección IP</th> </tr> </thead> <tbody> <tr> <td>Fa0/1.1</td> <td>VLAN1</td> <td>192.168.1.1</td> </tr> <tr> <td>Fa0/1.10</td> <td>VLAN 10</td> <td>192.168.10.1</td> </tr> <tr> <td>Fa0/1.20</td> <td>VLAN 20</td> <td>192.168.20.1</td> </tr> <tr> <td>Fa0/1.30</td> <td>VLAN 30</td> <td>192.168.30.1</td> </tr> <tr> <td>Fa0/1.99</td> <td>VLAN 99</td> <td>192.168.99.1</td> </tr> </tbody> </table>	Dispositivo Nombre de host	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminado	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	N/C	R1	Fa 0/1	Ver tabla de configuración de subinterfaz		N/C	PC1	NIC	192.168.10.21	255.255.255.0	192.168.10.1	PC2	NIC	192.168.20.22	255.255.255.0	192.168.20.1	PC3	NIC	192.168.30.23	255.255.255.0	192.168.30.1	Server	NIC	192.168.50.254	255.255.255.0	192.168.50.1	Puertos	Asignación	Red	Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN 99 nativa)	192.168.99.0 /24	Fa0/6 – 0/10	VLAN 30 – Sales	192.168.30.0 /24	Fa0/11 – 0/17	VLAN 10 – R&D	192.168.10.0 /24	Fa0/18 – 0/24	VLAN 20 – Engineering	192.168.20.0 /24	Interfaz del router	Asignación	Dirección IP	Fa0/1.1	VLAN1	192.168.1.1	Fa0/1.10	VLAN 10	192.168.10.1	Fa0/1.20	VLAN 20	192.168.20.1	Fa0/1.30	VLAN 30	192.168.30.1	Fa0/1.99	VLAN 99	192.168.99.1
Dispositivo Nombre de host	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminado																																																																																
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	N/C																																																																																
R1	Fa 0/1	Ver tabla de configuración de subinterfaz		N/C																																																																																
PC1	NIC	192.168.10.21	255.255.255.0	192.168.10.1																																																																																
PC2	NIC	192.168.20.22	255.255.255.0	192.168.20.1																																																																																
PC3	NIC	192.168.30.23	255.255.255.0	192.168.30.1																																																																																
Server	NIC	192.168.50.254	255.255.255.0	192.168.50.1																																																																																
Puertos	Asignación	Red																																																																																		
Fa0/1 – 0/5	Enlaces troncales 802.1q (VLAN 99 nativa)	192.168.99.0 /24																																																																																		
Fa0/6 – 0/10	VLAN 30 – Sales	192.168.30.0 /24																																																																																		
Fa0/11 – 0/17	VLAN 10 – R&D	192.168.10.0 /24																																																																																		
Fa0/18 – 0/24	VLAN 20 – Engineering	192.168.20.0 /24																																																																																		
Interfaz del router	Asignación	Dirección IP																																																																																		
Fa0/1.1	VLAN1	192.168.1.1																																																																																		
Fa0/1.10	VLAN 10	192.168.10.1																																																																																		
Fa0/1.20	VLAN 20	192.168.20.1																																																																																		
Fa0/1.30	VLAN 30	192.168.30.1																																																																																		
Fa0/1.99	VLAN 99	192.168.99.1																																																																																		

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Situación</p> <p>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.</p> <p>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.</p> <p>Tarea 1: Preparar la red</p> <p>Paso 1: Cablee una red de manera similar al diagrama de topología.</p> <p>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.</p> <p>Establezca conexiones de consola en los tres switches y en el router.</p> <p>Paso 2: Borre toda configuración existente en los switches.</p> <p>Borre las configuraciones de switch en los tres switches y vuelva a cargar para restaurar el estado predeterminado. Utilice el comando <code>show vlan</code> para verificar que solo existan VLAN predeterminadas y que todos los puertos se asignen a la VLAN 1.</p> <p>Paso 3: Configure las interfaces Ethernet en las PC Host y el servidor.</p> <p>Configure las interfaces Ethernet de PC1, PC2, PC3 y el servidor con la dirección IP y los gateways predeterminados indicados en la tabla de direccionamiento.</p>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Tarea 2: Cargar el router y los switches con los guiones suministrados</p> <p>Configuración del router 1</p> <pre> hostname R1 ! no ip domain lookup ! interface FastEthernet0/0 ip address 192.168.80.1 255.255.255.192 ! interface FastEthernet0/1 no ip address ! interface FastEthernet0/1.1 encapsulation dot1Q 1 ip address 192.168.1.1 255.255.255.0 ! interface FastEthernet0/1.10 encapsulation dot1Q 11 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 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 </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre>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 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 !</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> interface FastEthernet0/4 switchport trunk native vlan 99 switchport mode trunk shutdown ! interface FastEthernet0/5 switchport trunk native vlan 99 switchport mode trunk ! interface range FastEthernet0/6 - 24 shutdown ! interface Vlan99 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 </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre>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 FastEthernet0/5 switchport trunk native vlan 99 switchport mode trunk ! interface range FastEthernet0/6 - 11 switchport access vlan 30 switchport mode access ! interface range FastEthernet0/12 - 17 switchport access vlan 10 ! interface range FastEthernet0/18 - 24 switchport mode access switchport access vlan 20 !</pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> interface Vlan99 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 </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<pre> ! 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 FastEthernet0/5 switchport trunk native vlan 99 switchport mode trunk ! interface range FastEthernet0/6 - 24 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 </pre>

Materiales, Herramientas, Instrumental, Maquinaria y Equipo.	Desempeños
	<p>Tarea 3: Diagnosticar y corregir los problemas entre las VLAN y los errores de configuración</p> <p>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?</p> <p>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.</p> <p>Tarea 4: Documentar la configuración de la red</p> <p>Cuando haya terminado con éxito su diagnóstico, capture el resultado del router y los tres switches con el comando <code>show run</code> y guárdelo en un archivo de texto.</p> <p>Tarea 5: Limpieza</p> <p>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.</p> <p><i>Tomado del Material de Cisco CCNA para efectos educativos: Cisco Networking Academy 1992-2007</i></p> <p>Entrega un informe de las actividades realizadas en la práctica, formando el portafolio de evidencias.</p> <p> ADVERTENCIA DE RIESGO ELÉCTRICO</p>