DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

YINA MARCELA MONTILLA YUCUMÁ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
PROGRAMA: INGENIERÍA DE SISTEMAS
LA PLATA - HUILA
2015

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

YINA MARCELA MONTILLA YUCUMÁ

DIPLOMADO PRESENTADO PARA OBTENER EL TÍTULO DE
INGENIERÍA DE SISTEMAS

DOCENTE ASOCIADO
INVESTIGADOR JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
PROGRAMA: INGENIERÍA DE SISTEMAS
LA PLATA - HUILA
2015

TABLA DE CONTENIDO

LISTA DE TABLAS

Pág.

TABLA DE IMÁGENES

INTRODUCCIÓN

En este trabajo se puede observar el desarrollo de los laboratorios correspondientes donde se trabaja las temáticas relacionadas con los routers dinámicos, los portocolos de enrutamiento y la tabla de routing. Además se estudia el protocolo OSPF y su configuración. Cabe resaltar que las redes dinámicas cada vez se vuelven más complejas y aun para las cuestiones más simples es necesario contar con los conocimientos básicos sobre direcciones IP, esquemas de direccionamientos y clases de direcciones. Ahora no solamente tenemos computadores conectados entre sí, sino además un sistema de dispositivos cableados e inalámbricos, como equipos móviles, smarphone, tablets, cámaras de vigilancia, etc. Todos estos dispositivos necesitan su dirección IP para conectare entre sí.

Se trabajara la misma dinámica planteada en el módulo CCNA1, en el cual se seguirá las instrucciones asignadas en cada documento de laboratorio y posteriormente se realiza el procedimiento dejando las evidencias correspondientes con la ayuda del material didáctico elaborado por CISCO basado en las más modernas técnicas de la metodología de aprendizaje práctico, con posibilidad de acceder al material desde casa a través de Internet prácticas reales con equipos comerciales, tutorías telemáticas a través de Internet y foros de discusión. Haciendo prácticas a través de Packet Tracer proporcionado por Cisco dentro de la plataforma de NETACAD.

OBJETIVOS

OBJETIVO GENERAL

Afianzar y desarrollar las temáticas vistas en la unidad 3

OBJETIVOS ESPECÍFICOS

- Analizar los dispositivos utilizados de las comunicaciones en las redes de datos e Internet.
- Describir la función de capas de protocolo en redes de datos.
- Conocer la importancia de las capas de redes de datos en entornos IPv4 e IPv6
- Conocer los conceptos de Ethernet fundamentales
- Analizar la utilidad de las redes más comunes

1 INFORME: 2.1.1.6 LABORATORIO - CONFIGURING BASIC SWITCH SETTINGS

1.1 PRÁCTICA DE LABORATORIO: CONFIGURACIÓN DE LOS PARÁMETROS BÁSICOS DE UN SWITCH

1.1.1 PARTE 1.- TENDER EL CABLEADO DE RED Y VERIFICAR LA CONFIGURACIÓN PREDETERMINADA DEL SWITCH

1.1.2 PASO 1.- REALIZAR EL CABLEADO DE RED TAL COMO SE MUESTRA EN LA TOPOLOGÍA

a. Con Tera Term u otro programa de emulación de terminal, cree una conexión de consola de la PC-A al switch.

¿Por qué debe usar una conexión de consola para configurar inicialmente el switch? ¿Por qué no es posible conectarse al switch a través de Telnet o SSH?

Rta: Porque no hay una configuración inicial en la IOS del Switch que me permita acceder por Telnet o SSH

b. Examine el archivo de configuración activa actual.

Switch#**show running-config.**

¿Cuántas interfaces FastEthernet tiene un switch 2960? **Rta: 24**
¿Cuántas interfaces Gigabit Ethernet tiene un switch 2960? **Rta: 2**
¿Cuál es el rango de valores que se muestra para las líneas vty? **Rta: 0 - 15**

c. Examine el archivo de configuración de inicio en la NVRAM.

Switch# **show startup-config.**

Startup-config is not present.

¿Por qué aparece este mensaje?
Rta: Porque no hay configuración cargada en la NVRAM

d. Examine las características de la SVI para la VLAN 1.

Switch# **show interface vlan1**

¿Hay alguna dirección IP asignada a la VLAN 1?
Rta: Ninguna

¿Cuál es la dirección MAC de esta SVI?
Rta: 00e0.b0e5.8d16 (bia 00e0.b0e5.8d16)

¿Está activa esta interfaz?
Rta: NO

e. Examine las propiedades IP de la VLAN 1 SVI.

Switch#**show ip interface vlan1**

¿Qué resultado ve?
Rta: Vlan1 isadministrativelydown, line protocolisdown Internet protocol processing disabled.

Conecte el cable Ethernet de la PC-A al puerto 6 en el switch y examine las propiedades IP de la VLAN 1 SVI. Aguarde un momento para que el switch y la computadora negocien los parámetros de dúplex y velocidad.

Nota: si utiliza Netlab, habilite la interfaz F0/6 en el S1.

Switch# **show ip interface vlan1**

¿Qué resultado ve?
Rta: Vlan1 isadministrativelydown, line protocolisdownInternet protocolprocessingdisabled

Examine la información de la versión del IOS de Cisco del switch.

Switch#**show versión.**

¿Cuál es la versión del IOS de Cisco que está ejecutando el switch?
Rta: 12.2

¿Cuál es el nombre del archivo de imagen del sistema?
Rta: C2960-LANBASE-M

¿Cuál es la dirección MAC base de este switch?
Rta: Las respuestas varían. 00E0.B0E5.8D16

Examine las propiedades predeterminadas de la interfaz FastEthernet que usa la PC-A.

Switch#**show interface f0/6.**

¿La interfaz está activa o desactivada? **Rta: Activada**

¿Qué haría que una interfaz se active?
Rta: Que haya conectividad con otro dispositivo de red que este activo

¿Cuál es la dirección MAC de la interfaz?
Rta: 0001.6374.cb06 (bia 0001.6374.cb06)

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

Examine la configuración VLAN predeterminada del switch.

Switch#**show vlan**

¿Cuál es el nombre predeterminado de la VLAN 1?
Rta: default

¿Qué puertos hay en esta VLAN?
Rta:
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

¿La VLAN 1 está activa? **Rta: SI**

¿Qué tipo de VLAN es la VLAN predeterminada? **Rta: 1**

Examine la memoria flash.

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

Switch#**show flash**
Switch#**dir flash:**

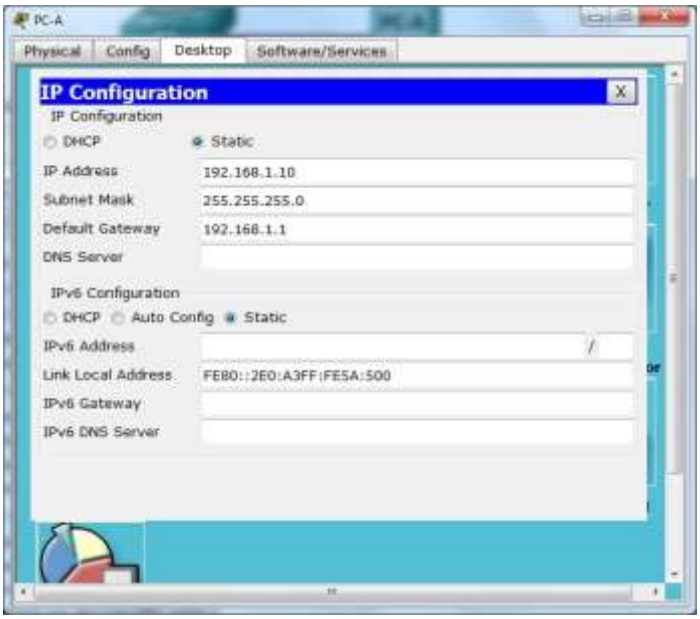
Los archivos poseen una extensión, tal como .bin, al final del nombre del archivo. Los directorios no tienen una extensión de archivo.

¿Cuál es el nombre de archivo de la imagen de IOS de Cisco?
Rta: c2960-lanbase-mz.122-25.FX.bin

2.- configurar los parámetros básicos de los dispositivos de red

¿Por qué se requiere el comando **login**?
Rta: para que active el password de acceso

Paso 2. configurar una dirección IP en la PC-A.
Asigne a la computadora la dirección IP y la máscara de subred que se muestran en la tabla de



Paso 3. mostrar la configuración del switch.

a. Verifique la configuración de la VLAN 99 de administración.

¿Cuál es el ancho de banda en esta interfaz?
Rta: BW 100000 Kbit

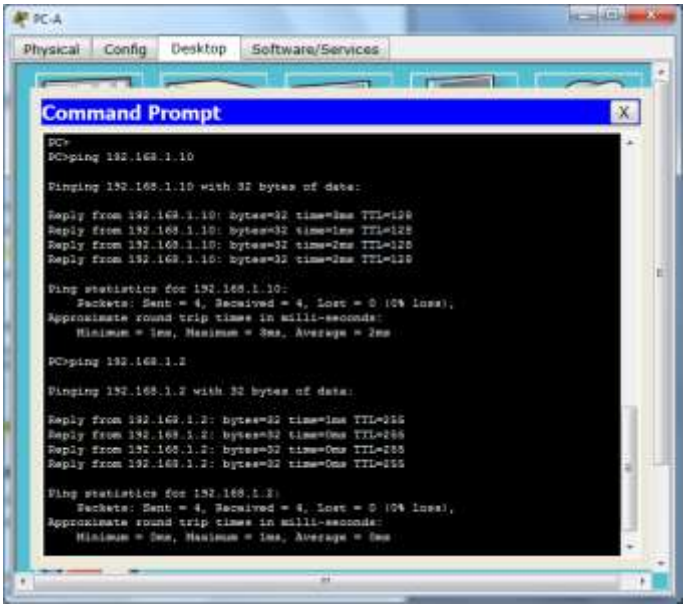
¿Cuál es el estado de la VLAN 99?
Rta: Vlan99 is up

¿Cuál es el estado del protocolo de línea?
Rta: line protocol is up.

Paso 4. probar la conectividad de extremo a extremo con ping.
a. En el símbolo del sistema de la PC-A, haga ping a la dirección de la propia PC-A primero.
C:\Users\User1>**ping 192.168.1.10 - pantallazos**

b. En el símbolo del sistema de la PC-A, haga ping a la dirección de administración de SVI del S1.

C:\Users\User1>**ping 192.168.1.2**

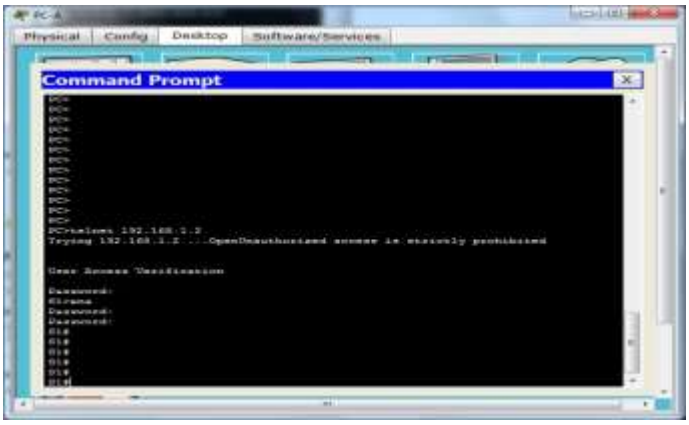


Paso 5. probar y verificar la administración remota del S1.

a. Con la ventana cmd abierta en la PC-A, emita un comando de Telnet para conectarse al S1 a través de la dirección de administración de SVI. La contraseña es **cisco**.

C:\Users\User1>**telnet 192.168.1.2 – Pantallazo Telnet**

b. Después de introducir la contraseña **cisco**, quedará en la petición de entrada del modo EXEC del usuario. Acceda al modo EXEC privilegiado.



Parte 2. Administrar la tabla de direcciones MAC.

En la parte 4, determinará la dirección MAC que detectó el switch, configurará una dirección MAC estática en una interfaz del switch y, a continuación, eliminará la dirección MAC estática de esa interfaz.

Paso 1. registrar la dirección MAC del host.

En el símbolo del sistema de la PC-A, emita el comando **ipconfig /all** para determinar y registrar las direcciones (físicas) de capa 2 de la NIC de la computadora.
PhysicalAddress. 00E0.A35A.0500

Paso 2. Determine las direcciones MAC que el switch ha aprendido.

Muestre las direcciones MAC con el comando **show mac address-table**.
S1# **show mac address-table**

¿Cuántas direcciones dinámicas hay? **Rta: 1**
¿Cuántas direcciones MAC hay en total? **Rta: 1**
¿La dirección MAC dinámica coincide con la dirección MAC de la PC-A? **Rta: SI**

Paso 3. enumerar las opciones del comando show mac address-table.

a. Muestre las opciones de la tabla de direcciones MAC.

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

¿Cuántas opciones se encuentran disponibles para el comando **show mac address-table**?
Rta: 1address-table

b. Emita el comando **show mac address-table dynamic** para mostrar solo las direcciones MAC que se detectaron dinámicamente.

S1# **show mac address-table dynamic**

¿Cuántas direcciones dinámicas hay? **Rta: Ninguna**

Paso 4. Configure una dirección MAC estática.

a. limpie la tabla de direcciones MAC.

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

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

b. Verifique que la tabla de direcciones MAC se haya eliminado.
c.
S1# **show mac address-table.**

¿Cuántas direcciones MAC estáticas hay? **Rta: Ninguna**

¿Cuántas direcciones dinámicas hay? **Rta: Ninguna**

d. Examine nuevamente la tabla de direcciones MAC. Es muy probable que una aplicación en ejecución en la computadora ya haya enviado una trama por la NIC hacia el S1. Observe nuevamente la tabla de direcciones MAC en el modo EXEC privilegiado para ver si el S1 volvió a detectar la dirección MAC para la PC-A.
S1# **show mac address-table**

¿Cuántas direcciones dinámicas hay? **Rta: 1**

¿Por qué cambió esto desde la última visualización?
Rta: porque se limpió la tabla de direcciones MAC

Si el S1 aún no volvió a detectar la dirección MAC de la PC-A, haga ping a la dirección IP de la VLAN 99 del switch desde la PC-A y, a continuación, repita el comando **show mac address-table**.

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

Configure una dirección MAC estática en F0/6 con la dirección que se registró para la PC-A en la parte 4, paso 1. La dirección MAC 0050.56BE.6C89 se usa solo como ejemplo. Debe usar la dirección MAC de su PC-A, que es distinta de la del ejemplo.

S1(config)# **mac address-table static 0050.56BE.6C89 vlan 99 interface fastethernet 0/6**

f. Verifique las entradas de la tabla de direcciones MAC.
S1# **show mac address-table**

¿Cuántas direcciones MAC hay en total? **Rta: 1**

¿Cuántas direcciones estáticas hay? **Rta: 1**

Elimine la entrada de MAC estática. Ingrese al modo de configuración global y elimine el comando escribiendo **no** delante de la cadena de comandos.

Nota: la dirección MAC 0050.56BE.6C89 se usa solo en el ejemplo. Use la dirección MAC de su PC-A.

S1 (config)# **no mac address-table static 0050.56BE.6C89 vlan 99 interface fastethernet 0/6**

g. Verifique que la dirección MAC estática se haya borrado.
S1# **show mac address-table**

¿Cuántas direcciones MAC estáticas hay en total? **Rta: Ninguna**

Reflexión

1. ¿Por qué debe configurar las líneas vty para el switch?
Rta: para tener acceso remoto mediante Telnet y SSH

2. ¿Para qué se debe cambiar la VLAN 1 predeterminada a un número de VLAN diferente?
Rta: El switch está configurado de manera predeterminada para que la administración de este se realice a través de VLAN 1. Sin embargo, la práctica recomendada para la configuración básica del switch es cambiar la VLAN de administración a otra VLAN distinta de la VLAN 1

3. ¿Cómo puede evitar que las contraseñas se envíen como texto no cifrado?
Rta: Encriptándolas

4. ¿Para qué se debe configurar una dirección MAC estática en una interfaz de puerto?
Rta: Para especificar a qué puertos se puede conectar un host, una opción es crear una asignación estática de la dirección MAC del host a un puerto

1.1.3 INFORME - CONCLUSIONES

Esta práctica me permitió aprender a configurar un enlace como troncal (Trunk) o también llamado punto a punto, el cual se usa básicamente para comunicar varios dispositivos Switch en la misma red (multiplexar), varias Vlan en un solo enlace, es decir no usan una Vlan específica, sino que se asimila a un solo tubo o conducto, por donde se va a pasar la información, allí las Vlan entregaran la información a un puerto asignado.

A lo anterior, se le suma que se aprendió conceptos nuevos como Vlan nativa y el protocolo IEEE 802.1Q. La Vlan nativa es la Vlan a la que pertenece un puerto en un switch antes de ser configurado como trunk. Hay que tener en cuenta que sólo se puede tener una VLAN nativa por puerto. El protocolo IEEE 802.1Q o dot1Q, nos define la encapsulación necesaria para enlaces troncales en redes Ethernet.

Con la ayuda de comandos básicos de configuración, visualización y verificación a través del CLI en los Switch Cisco, como: show Vlan, que nos muestra la información detallada acerca de todas las VLAN, el comando show Vlan Brief, que nos permite observar la asignación de VLAN para todos los puertos del switch, el Switchport mode trunk que nos permite realizar la configuración del puerto o Interfaz elegida como un enlace troncal permanente 802.1Q y el comando sh interfaces switchport, que nos sirve para verificar cual es la Vlan nativa habilitada.

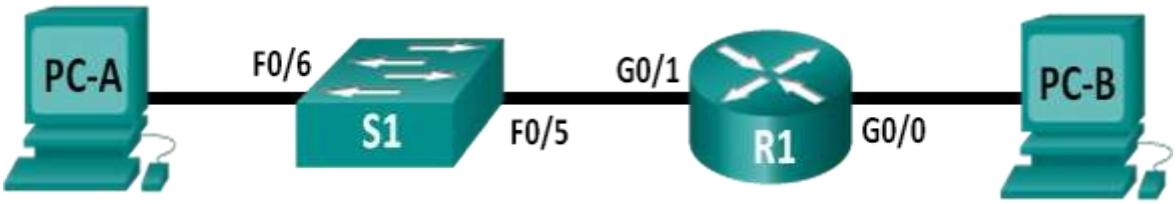
Este tipo de prácticas, nos ayudara a adquirir la experiencia necesaria para enfrentarnos a una situación real como posibles administradores de una red, lo cual nos exigirá en determinado momento usar todos los conocimientos adquiridos de una manera práctica.

2 INFORME: 4.1.4.6 LAB - CONFIGURING BASIC ROUTER SETTINGS WITH IOS CLI

2.1 PRÁCTICA DE LABORATORIO: CONFIGURACIÓN DE LOS PARÁMETROS BÁSICOS DEL ROUTER CON LA CLI DEL IOS

2.1.1 TOPOLOGÍA

Imagen 1. Topología Informe 4.1.4.6



Fuente: Datos del Informe

Tabla de direccionamiento

Tabla 1. Tabla de Direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Fuente: Datos del Informe

Objetivos

Parte 1: establecer la topología e inicializar los dispositivos

- Realizar el cableado de los equipos para que coincidan con la topología de la red.
- Inicializar y reiniciar el router y el switch.

Parte 2: configurar los dispositivos y verificar la conectividad

- Asignar información de IPv4 estática a las interfaces de la computadora.
- Configurar los parámetros básicos del router.
- Verificar la conectividad de la red

Configurar el router para el acceso por SSH.

Parte 3: mostrar la información del router

- Recuperar información del hardware y del software del router.

- Interpretar el resultado de la configuración de inicio.
- Interpretar el resultado de la tabla de routing.
- Verificar el estado de las interfaces.

Parte 4: configurar IPv6 y verificar la conectividad
Información básica/situación

Esta es una práctica de laboratorio integral para revisar comandos de router de IOS que se abarcaron anteriormente. En las partes 1 y 2, realizará el cableado de los equipos y completará las configuraciones básicas y las configuraciones de las interfaces IPv4 en el router.

En la parte 3, utilizará SSH para conectarse de manera remota al router y usará comandos de IOS para recuperar la información del dispositivo para responder preguntas sobre el router. En la parte 4, configurará IPv6 en el router de modo que la PC-B pueda adquirir una dirección IP y luego verificará la conectividad.

Para fines de revisión, esta práctica de laboratorio proporciona los comandos necesarios para las configuraciones de router específicas.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960 con IOS de Cisco, versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio.

Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que el router y el switch se hayan borrado y no tengan configuraciones de inicio. Consulte el apéndice A para conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios
- 1 router (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola

- Cables Ethernet, como se muestra en la topología

Nota: las interfaces Gigabit Ethernet en los ISR Cisco 1941 cuentan con detección automática, y se puede utilizar un cable directo de Ethernet entre el router y la PC-B. Si utiliza otro modelo de router Cisco, puede ser necesario usar un cable cruzado Ethernet.

Parte 1: establecer la topología e inicializar los dispositivos

Paso 1. realizar el cableado de red tal como se muestra en la topología.

h. Conecte los dispositivos tal como se muestra en el diagrama de la topología y realice el cableado según sea necesario.

Imagen 2. Topología de Cableado de Red

Fuente: Datos del Informe

i. Encienda todos los dispositivos de la topología.

j.

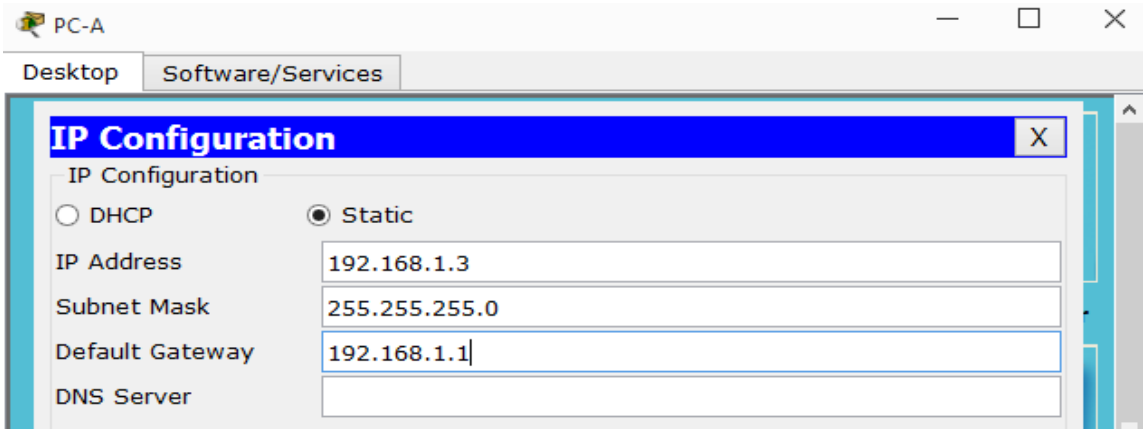
Paso 2. inicializar y volver a cargar el router y el switch.

Nota: en el apéndice A, se detallan los pasos para inicializar y volver a cargar los dispositivos.

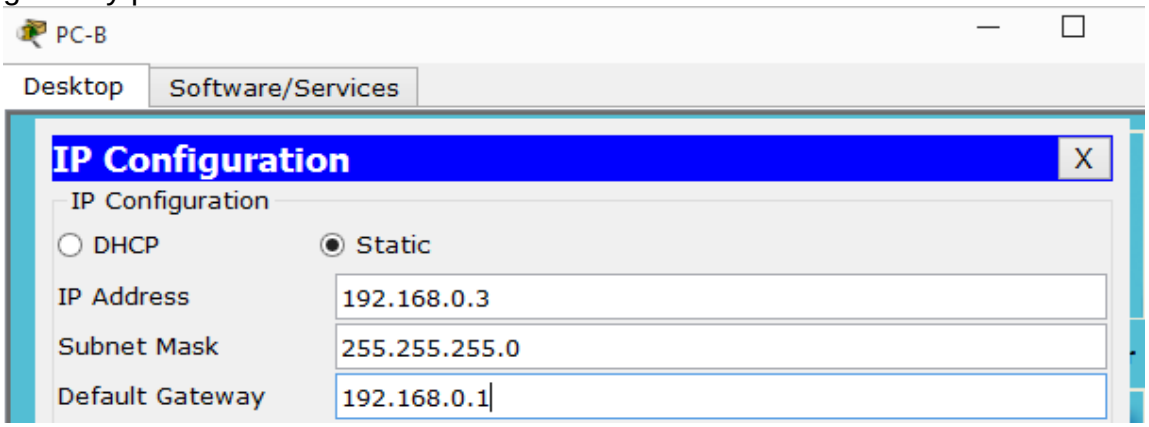
Parte 2: Configurar dispositivos y verificar la conectividad

Paso 1. Configure las interfaces de la PC.

a. Configure la dirección IP, la máscara de subred y la configuración del gateway predeterminado en la PC-A.



b. Configure la dirección IP, la máscara de subred y la configuración del gateway predeterminado en la PC-B.



Paso 2. Configurar el router.

a. Acceda al router mediante el puerto de consola y habilite el modo EXEC privilegiado.

```
Router>enable
Router#
```

b. Ingrese al modo de configuración global.

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

c. Asigne un nombre de dispositivo al router.

```
Router(config)#hostname R1
R1(config)#
```

d. Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.

```
R1(config)#no ip domain-lookup
R1(config)#
```

e. Establezca el requisito de que todas las contraseñas tengan como mínimo 10 caracteres.

```
R1(config)#security passwords min-length 10
R1(config)#
```

Además de configurar una longitud mínima, enumere otras formas de aportar seguridad a las contraseñas.

USAR CONTRASEÑAS SECRETAS Y ENCRIPTACION DE CONTRASEÑAS

f. Asigne **cisco12345** como la contraseña cifrada del modo EXEC privilegiado.

```
R1(config)#enable secret cisco12345
R1(config)#
```

g. Asigne **ciscoconpass** como la contraseña de consola, establezca un tiempo de espera, habilite el inicio de sesión y agregue el comando **logging synchronous**. El comando **logging synchronous** sincroniza la depuración y el resultado del software IOS de Cisco, y evita que estos mensajes interrumpan la entrada del teclado.

```
R1(config)#line con 0
R1(config-line)#password ciscoconpass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#
```

Para el comando **exec-timeout**, ¿qué representan el **5** y el **0**?

QUE LA SESION SE DESCONECTARA SI NO HAY USO EN 5 MINUTOS Y 0 SEGUNDOS

Asigne **ciscovtypass** como la contraseña de vty, establezca un tiempo de espera, habilite el inicio de sesión y agregue el comando **logging synchronous**

```
R1(config)#line vty 0 4
R1(config-line)#password ciscovtypass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#
```

h. Cifre las contraseñas de texto no cifrado.

```
R1(config)#service password-encryption
R1(config)#
```

i. Cree un aviso que advierta a todo aquel que acceda al dispositivo que el acceso no autorizado está prohibido.

```
R1(config)#banner motd "Prohibido el acceso no autorizado"
R1(config)#
```

j. Configure una dirección IP y una descripción de interfaz. Active las dos interfaces en el router.

```
R1(config)#interface g0/0
R1(config-if)#description Conexion a PC-B
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R1(config-if)#interface g0/1
R1(config-if)#description Conexion a S1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to up

R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

k. Configure el reloj en el router, por ejemplo:

```
R1#
R1#clock set 09:08:00 21 April 2015
R1#show clock
*9:8:6.847 UTC Tue Apr 21 2015
R1#
```

l. Guarde la configuración en ejecución en el archivo de configuración de inicio.

```
R1#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

¿Qué resultado obtendría al volver a cargar el router antes de completar el comando **copy running-config startup-config**?
Rta: se pierden las configuraciones hechas

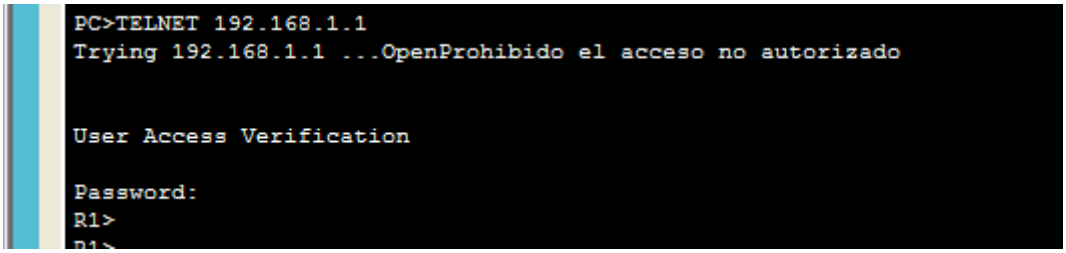
Paso 3. Verificar la conectividad de la red

m. Haga ping a la PC-B en un símbolo del sistema en la PC-A.
Nota: quizá sea necesario deshabilitar el firewall de las computadoras.

¿Tuvieron éxito los pings? **Rta: SI**
Después de completar esta serie de comandos, ¿qué tipo de acceso remoto podría usarse para acceder al R1?
Rta: por TELNET desde el PC-A

n. Acceda de forma remota al R1 desde la PC-A mediante el cliente de Telnet de Tera Term.

Abra Tera Term e introduzca la dirección IP de la interfaz G0/1 del R1 en el campo Host: de la ventana Tera Term: New Connection (Tera Term: nueva conexión). Asegúrese de que el botón de opción **Telnet** esté seleccionado y después haga clic en **OK** (Aceptar) para conectarse al router.



¿Pudo conectarse remotamente? **Rta: SI**

¿Por qué el protocolo Telnet es considerado un riesgo de seguridad?
Rta: porque cualquier usuario que conozca la contraseña se puede conectar desde cualquier PC que este en la misma subred.

Paso 4. configurar el router para el acceso por SSH.
o. Habilite las conexiones SSH y cree un usuario en la base de datos local del router.
Imagen 3. Configuración Router Acceso por SSH

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip domain-name CCNA-lab.com
R1(config)#username admin privilege 15 secret adminpass1
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#crypto key generate rsa modulus
                                    ^
% Invalid input detected at '^' marker.

R1(config)#crypto key generate rsa
The name for the keys will be: R1.CCNA-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#exit
*abr. 21 9:21:24.970:  %SSH-5-ENABLED: SSH 1.99 has been enabled
R1#
```

Acceda remotamente al R1 desde la PC-A con el cliente SSH de Tera Term.
Abra Tera Term e introduzca la dirección IP de la interfaz G0/1 del R1 en el campo Host: de la ventana Tera Term: New Connection (Tera Term: nueva conexión). Asegúrese de que el botón de opción **SSH** esté seleccionado y después haga clic en **OK** para conectarse al router.

```
PC>ssh -l admin 192.168.1.1
Open
Password:

Prohibido el acceso no autorizado

R1#
R1#
```

¿Pudo conectarse remotamente? **Rta: SI**

Parte 3: mostrar la información del router
En la parte 3, utilizará comandos **show** en una sesión SSH para recuperar información del router.

Paso 5. establecer una sesión SSH para el R1.
Mediante Tera Term en la PC-B, abra una sesión SSH para el R1 en la dirección IP 192.168.0.1 e inicie sesión como **admin** y use la contraseña **adminpass1**.

Paso 6. recuperar información importante del hardware y el software.
p. Use el comando **show version** para responder preguntas sobre el router.

¿Cuál es el nombre de la imagen de IOS que el router está ejecutando?
Rta: flash0:c1900-universalk9-mz.SPA.151-1.M4.bin

¿Cuánta memoria de acceso aleatorio no volátil (NVRAM) tiene el router?
Rta: 255 Kilobytes
¿Cuánta memoria flash tiene el router?
Rta: 249,856 Megabytes

q. Con frecuencia, los comandos **show** proporcionan varias pantallas de resultados. Filtrar el resultado permite que un usuario visualice determinadas secciones del resultado. Para habilitar el comando de filtrado, introduzca una barra vertical (**|**) después de un comando **show**, seguido de un parámetro de filtrado y una expresión de filtrado. Para que el resultado coincida con la instrucción de filtrado, puede usar la palabra clave **include** para ver todas las líneas del resultado que contienen la expresión de filtrado. Filtre el comando **show version** mediante **show version | include register** para responder la siguiente pregunta.

¿Cuál es el proceso de arranque para el router en la siguiente recarga?
Rta: en el packet tracer no se visualizan resultados porque no soporta el carácter |

Paso 7. mostrar la configuración de inicio.
Use el comando **show startup-config** en el router para responder las siguientes preguntas.

¿De qué forma figuran las contraseñas en el resultado?
Rta: estan cifradas, entonces solo aparecen números y letras sin sentido

Use el comando **show startup-config | begin vty**.
¿Qué resultado se obtiene al usar este comando?
Rta: en el packet tracer no se visualizan resultados porque no soporta el carácter |

Paso 8. mostrar la tabla de routing en el router.

Use el comando **show ip route** en el router para responder las siguientes preguntas.

```
R1#SHOw IP ROUTE
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.0.0/24 is directly connected, GigabitEthernet0/0
L       192.168.0.1/32 is directly connected, GigabitEthernet0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
R1#
```

¿Qué código se utiliza en la tabla de routing para indicar una red conectada directamente?
Rta: la letra C

¿Cuántas entradas de ruta están cifradas con un código C en la tabla de routing?
Rta: 2

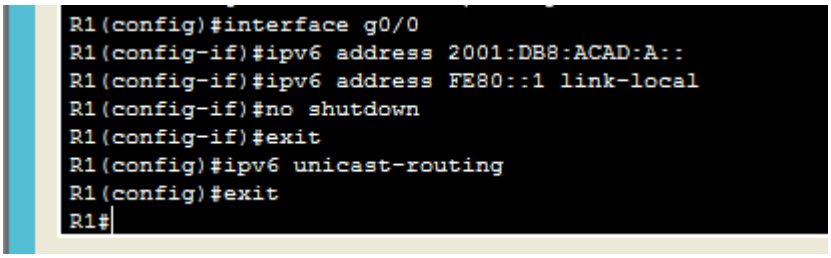
Paso 9. mostrar una lista de resumen de las interfaces del router.
Use el comando **show ip interface brief** en el router para responder la siguiente pregunta.

¿Qué comando cambió el estado de los puertos Gigabit Ethernet de administrativamente inactivo a activo?
Rta: NO SHUTDOWN

Parte 4: configurar IPv6 y verificar la conectividad

Paso 10. asignar direcciones IPv6 a la G0/0 del R1 y habilitar el routing IPv6.

Nota: la asignación de una dirección IPv6, además de una dirección IPv4, en una interfaz se conoce como “dual stacking”, debido a que las pilas de protocolos IPv4 e IPv6 están activas. Al habilitar el routing de unidifusión IPv6 en el R1, la PC-B recibe el prefijo de red IPv6 de G0/0 del R1 y puede configurar automáticamente la dirección IPv6 y el gateway predeterminado.
r. Asigne una dirección de unidifusión global IPv6 a la interfaz G0/0; asigne la dirección link-local en la interfaz, además de la dirección de unidifusión; y habilite el routing IPv6.



b. Use el comando **show ipv6 int brief** para verificar la configuración de IPv6 en el R1.
Si no se asignó una dirección IPv6 a la G0/1, ¿por qué se indica como [up/up]?

Rta: porque solo muestra que está activa o sea en capa 2, pero no quiere decir que tiene dirección IP, ósea en capa 3

Emita el comando **ipconfig** en la PC-B para examinar la configuración de IPv6.

¿Cuál es la dirección IPv6 asignada a la PC-B?
Rta: 2001:DB8: ACAD: A:: 1

¿Cuál es el gateway predeterminado asignado a la PC-B?
Rta: 192.168.0.1

En la PC-B, haga ping a la dirección link-local del gateway predeterminado del R1. ¿Tuvo éxito?
Rta: SI

En la PC-B, haga ping a la dirección IPv6 de unidifusión del R1 2001:db8:acad:a:: 1. ¿Tuvo éxito?
Rta: SI

2.1.2 REFLEXIÓN

1. Durante la investigación de un problema de conectividad de red, un técnico sospecha que no se habilitó una interfaz. ¿Qué comando **show** podría usar el técnico para resolver este problema?
Rta: Show ip interface brief

2. Durante la investigación de un problema de conectividad de red, un técnico sospecha que se asignó una máscara de subred incorrecta a una interfaz. ¿Qué comando **show** podría usar el técnico para resolver este problema?
Rta: Show startup-config

3. Después de configurar IPv6 en la LAN de la PC-B en la interfaz G0/0 del R1, si hiciera ping de la PC-A a la dirección IPv6 de la PC-B, ¿el ping sería correcto? ¿Por qué o por qué no?

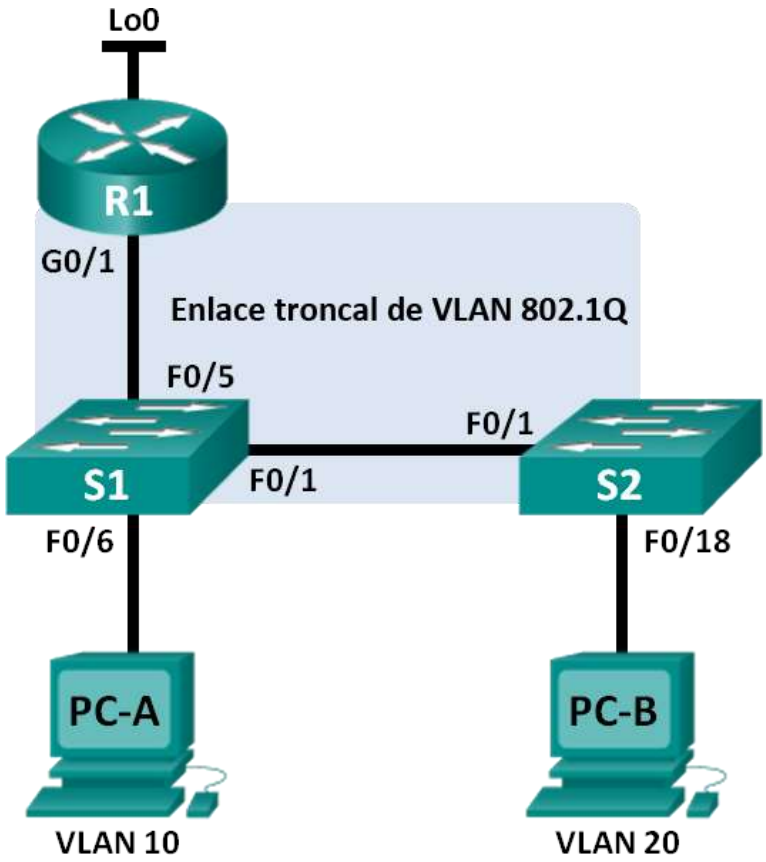
Rta: No sería correcto porque pc-a no fue configurado con ipv6 y porque la interfaz (g0/1) tampoco tiene activo el direccionamiento ipv6

3 INFORME: 5.1.3.7 LAB - CONFIGURING 802.1Q TRUNK-BASED INTER-VLAN ROUTING

3.1 PRÁCTICA DE LABORATORIO: CONFIGURACIÓN DE ROUTING ENTRE VLAN BASADO EN ENLACES TRONCALES 802.1Q

3.1.1 TOPOLOGÍA

Imagen 4. Topología Informe 5.1.3.7



Fuente: Datos del Informe

Tabla de direccionamiento

Tabla 2. Tabla de Direccionamiento Informe 5.1.3.7

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1.1	192.168.1.1	255.255.255.0	N/A
	G0/1.10	192.168.10.1	255.255.255.0	N/A
	G0/1.20	192.168.20.1	255.255.255.0	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Fuente: Datos del Informe

Especificaciones de la asignación de puertos de switch

Tabla 3. Tabla de Asignación de Puertos Switch

Puertos	Asignaciones	Red
S1 F0/1	Enlace troncal de 802.1Q	N/A
S2 F0/1	Enlace troncal de 802.1Q	N/A
S1 F0/5	Enlace troncal de 802.1Q	N/A
S1 F0/6	VLAN 10: Estudiantes	192.168.10.0/24
S2 F0/18	VLAN 20: Cuerpo docente	192.168.20.0/24

Fuente: Datos del Informe

Objetivos

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
Parte 2: configurar switches con VLAN y enlaces troncales
Parte 3: configurar routing entre VLAN basado en enlaces troncales
Información básica/situación

Un segundo método para proporcionar routing y conectividad a varias VLAN es mediante el uso de un enlace troncal 802.1Q entre uno o más switches y una única interfaz del router. Este método también se conoce como “routing entre VLAN con router-on-a-stick”. En este método, se divide la interfaz física del router en varias subinterfaces que proporcionan rutas lógicas a todas las VLAN conectadas.

En esta práctica de laboratorio, configurará el routing entre VLAN basado en enlaces troncales y verificará la conectividad a los hosts en diferentes VLAN y con un loopback en el router.

Nota: en esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar el routing entre VLAN basado en enlaces troncales. Sin embargo, los comandos requeridos para la configuración se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar los dispositivos sin consultar el apéndice.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de la práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

- 1 router (Cisco 1941 con IOS de Cisco, versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco, versión 15.0(2), imagen lanbasek9 o similar)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, configurará la topología de la red y configurará los parámetros básicos en los equipos host, los switches y el router.

Paso 1. realizar el cableado de red tal como se muestra en la topología.
Paso 2. configurar los equipos host.
Paso 3. inicializar y volver a cargar los routers y switches, según sea necesario.
Paso 4. configurar los parámetros básicos para cada switch.

c. Desactive la búsqueda del DNS.
d. Configure los nombres de los dispositivos como se muestra en la topología.
e. Asigne **class** como la contraseña del modo EXEC privilegiado.
f. Asigne **cisco** como la contraseña de consola y la contraseña de vty.
g. Configure **logging synchronous** para la línea de consola.
h. Configure la dirección IP que se indica en la tabla de direccionamiento para la VLAN 1 en ambos switches.
i. Configure el gateway predeterminado en los dos switches.
j. Desactive administrativamente todos los puertos que no se usen en el switch.
k. Copie la configuración en ejecución en la configuración de inicio

Paso 5. configurar los parámetros básicos para el router.
a. Desactive la búsqueda del DNS.
b. Configure los nombres de los dispositivos como se muestra en la topología.
c. Configure la dirección IP Lo0, como se muestra en la tabla de direccionamiento. No configure las subinterfaces en esta instancia; esto lo hará en la parte 3.
d. Asigne **cisco** como la contraseña de consola y la contraseña de vty.
e. Asigne **class** como la contraseña del modo EXEC privilegiado.
f. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada de comandos.
g. Copie la configuración en ejecución en la configuración de inicio

Parte 2: configurar los switches con las VLAN y los enlaces troncales

En la parte 2, configurará los switches con las VLAN y los enlaces troncales.

Nota: los comandos requeridos para la parte 2 se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar el S1 y el S2 sin consultar el apéndice.

Paso 1. Configurar las VLAN en S1.

a. En el S1, configure las VLAN y los nombres que se indican en la tabla Especificaciones de la asignación de puertos de switch. En el espacio proporcionado, escriba los comandos que utilizó.

```
S1(config)#vlan 10
S1(config-vlan)#name Student
S1(config-vlan)#vlan 20
S1(config-vlan)#name Faculty
S1(config-vlan)#
```

b. En el S1, configure la interfaz conectada al R1 como enlace troncal. También configure la interfaz conectada al S2 como enlace troncal. En el espacio proporcionado, escriba los comandos que utilizó.

```
S1(config)#interface f0/5
S1(config-if)#switc?
switchport
S1(config-if)#switc
S1(config-if)#switchport mode trunk
S1(config-if)#interface f0/1
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state t
o down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state t
o up

S1(config-if)#
```

c. En el S1, asigne el puerto de acceso para la PC-A a la VLAN 10. En el espacio proporcionado, escriba los comandos que utilizó.

```
S1(config)#interface f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
S1(config-if)#
```

Paso 2. configurar las VLAN en el switch 2.

d. En el S2, configure las VLAN y los nombres que se indican en la tabla Especificaciones de la asignación de puertos de switch.

```
S2(config)#vlan 10
S2(config-vlan)#name Student
S2(config-vlan)#vlan 20
S2(config-vlan)#name Faculty
S2(config-vlan)#
```

e. En el S2, verifique que los nombres y números de las VLAN coincidan con los del S1. En el espacio proporcionado, escriba el comando que utilizó.

```
S2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                                Gig1/2
10   Student                          active
20   Faculty                          active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S2#
```

```
S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig1/1, Gig1/2
10   Student                          active    Fa0/6
20   Faculty                          active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S1#
```

f. En el S2, asigne el puerto de acceso para la PC-B a la VLAN 20.

```
S2(config)#inter f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20
S2(config-if)#
```

g. En el S2, configure la interfaz conectada al S1 como enlace troncal.

```
S2(config)#interface f0/1
S2(config-if)#switchport mode trunk
S2(config-if)#
```

configurar routing entre VLAN basado en enlaces troncales

En la parte 3, configurará el R1 para enrutar a varias VLAN mediante la creación de subinterfaces para cada VLAN. Este método de routing entre VLAN se denomina “router-on-a-stick”.

Nota: los comandos requeridos para la parte 3 se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar el routing entre VLAN basado en enlaces troncales o con router-on-a-stick sin consultar el apéndice.

Paso 3. configurar una subinterfaz para la VLAN 1.

h. Cree una subinterfaz en la interfaz G0/1 del R1 para la VLAN 1 y use el 1 como ID de la subinterfaz. En el espacio proporcionado, escriba el comando que utilizó.

```
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface g0/1.1
R1(config-subif)#
```

i. Configure la subinterfaz para que opere en la VLAN 1. En el espacio proporcionado, escriba el comando que utilizó.

```
R1(config-subif)#
R1(config-subif)#encapsulation dot1Q 1
R1(config-subif)#
```

j. Configure la subinterfaz con la dirección IP de la tabla de direccionamiento. En el espacio proporcionado, escriba el comando que utilizó.

```
R1(config-subif)#
R1(config-subif)#ip addres 192.168.1.1 255.255.255.0
R1(config-subif)#
```

Paso 4. configurar una subinterfaz para la VLAN 10.

k. Cree una subinterfaz en la interfaz G0/1 del R1 para la VLAN 10 y use el 10 como ID de la subinterfaz.

```
R1(config)#interface g0/1.10
```

l. Configure la subinterfaz para que opere en la VLAN 10.

```
R1(config-subif)#encapsulation d
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#
```

m. Configure la subinterfaz con la dirección de la tabla de direccionamiento.

```
R1(config-subif)#
R1(config-subif)#ip address 192.168.10.1 255.255.255.0
R1(config-subif)#
```

Paso 5. configurar una subinterfaz para la VLAN 20.

n. Cree una subinterfaz en la interfaz G0/1 del R1 para la VLAN 20 y use el 20 como ID de la subinterfaz.

```
R1(config)#
R1(config)#interface g0/1.20
```

o. Configure la subinterfaz para que opere en la VLAN 20.

```
R1(config-subif)#encapsulation dot1q 20
```

Configure la subinterfaz con la dirección de la tabla de direccionamiento

```
R1(config-subif)#ip addres 192.168.20.1 255.255.255.0
R1(config-subif)#
```

Paso 6. habilitar la interfaz G0/1.

Habilite la interfaz G0/1. En el espacio proporcionado, escriba los comandos que utilizó.

```
R1(config)#interface g0/1
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed stat
e to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.1, changed st
ate to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.10, changed s
tate to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.20, changed s
tate to up

R1(config-if)#
```

Paso 7. Verifique la conectividad.

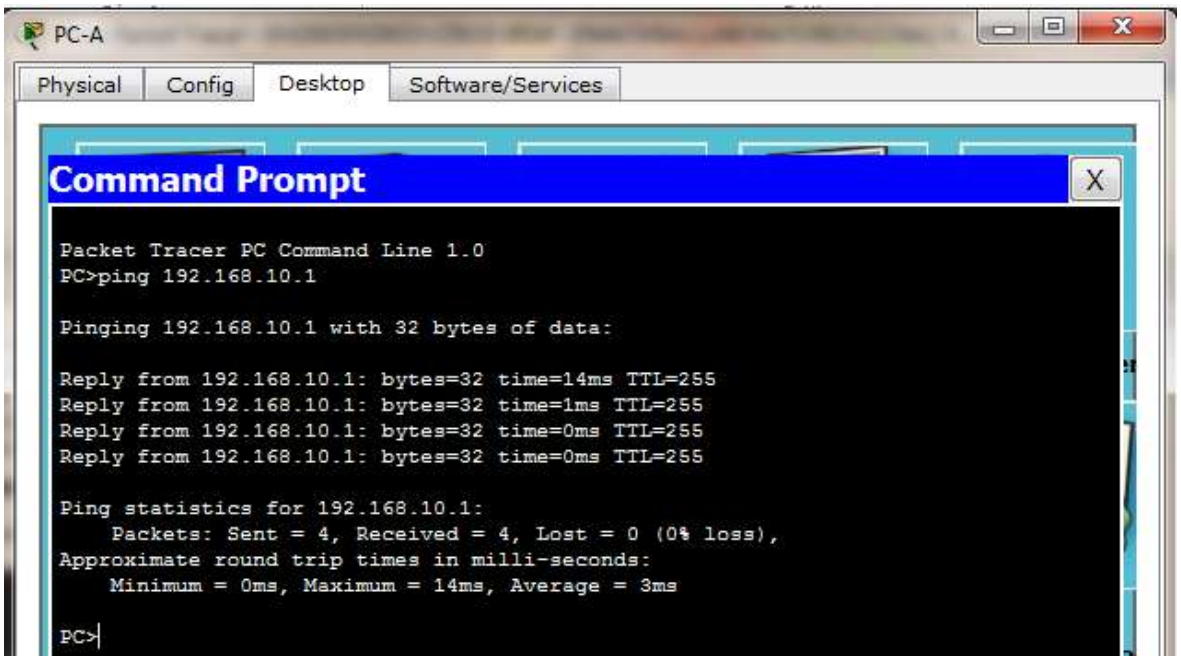
Introduzca el comando para ver la tabla de routing en el R1. ¿Qué redes se enumeran?

Rta:

- ✓ ***192.168.1.0***
- ✓ ***192.168.10.0***
- ✓ ***192.168.20.0***
- ✓ ***209.165.200.224***

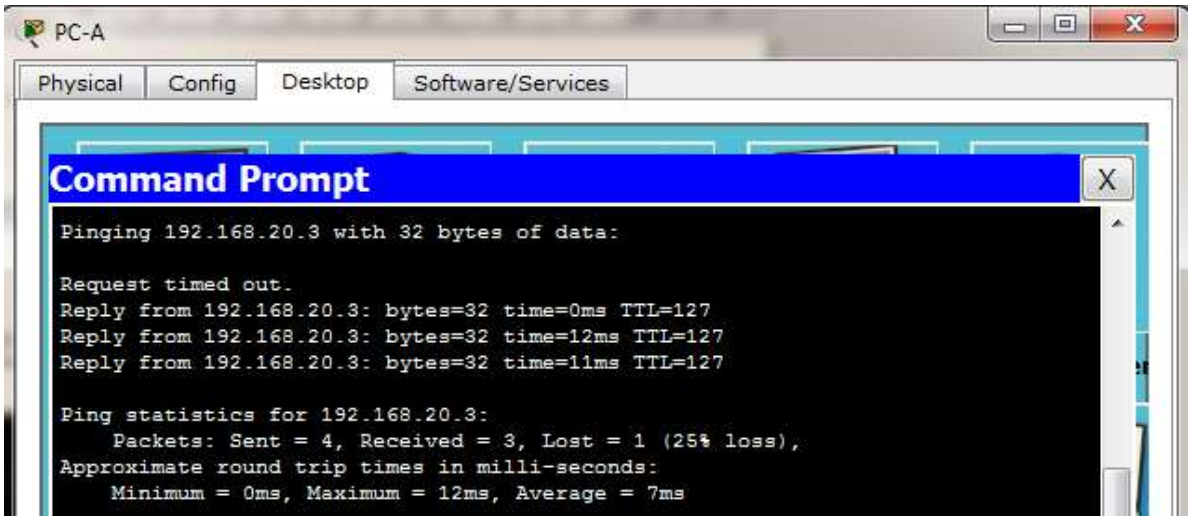
```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1.1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1.1
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/1.10
L       192.168.10.1/32 is directly connected, GigabitEthernet0/1.10
     192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, GigabitEthernet0/1.20
L       192.168.20.1/32 is directly connected, GigabitEthernet0/1.20
     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.224/27 is directly connected, Loopback0
L       209.165.200.225/32 is directly connected, Loopback0
R1#
```

¿Es posible hacer ping de la PC-A al gateway predeterminado de la VLAN 10?
Rta: SI

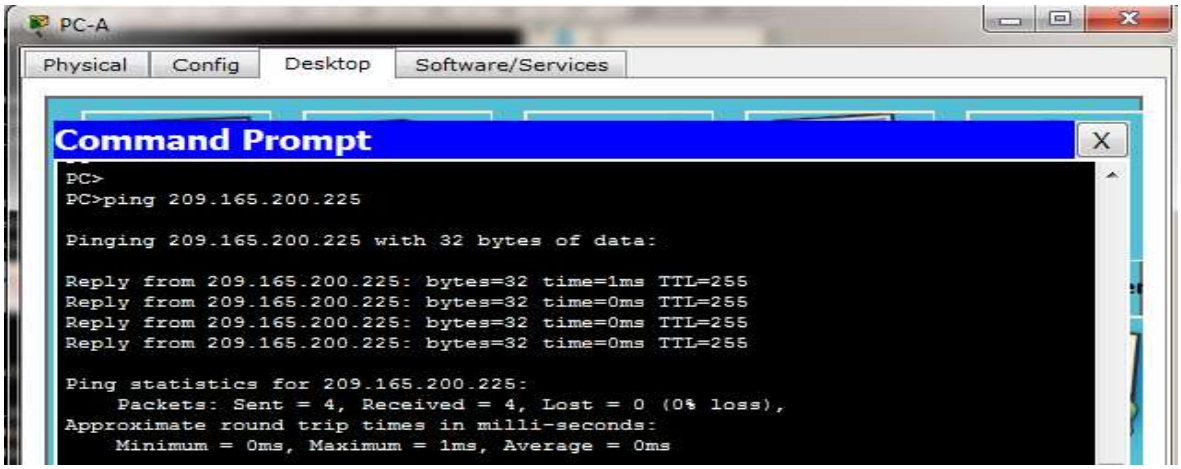


¿Es posible hacer ping de la PC-A a la PC-B?
Rta: SI

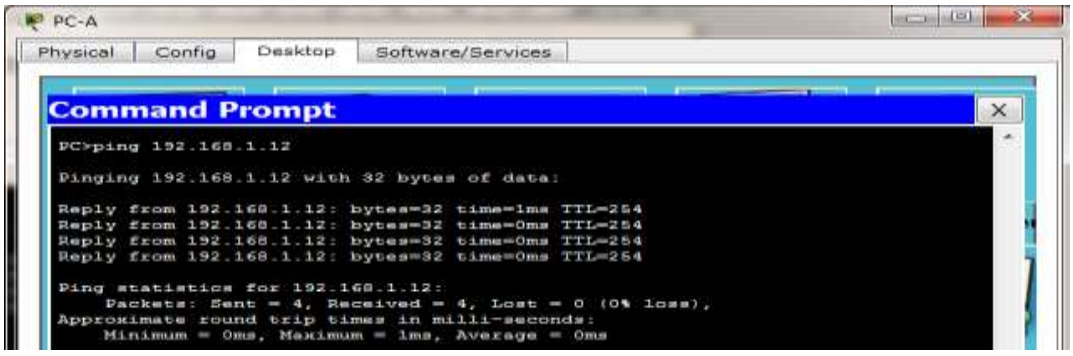
Imagen 5. Comando Prompt Informe 5.1.3.7



¿Es posible hacer ping de la PC-A a la interfaz Lo0?
Rta: SI



¿Es posible hacer ping de la PC-A al S2?
Rta: SI



Si la respuesta a cualquiera de estas preguntas es **no**, resuelva los problemas de configuración y corrija los errores.

3.1.2 REFLEXIÓN

¿Cuáles son las ventajas del routing entre VLAN basado en enlaces troncales comparado con el routing entre VLAN con router-on-a-stick?

Rta: El primero solo necesita una interfaz para enrutar varias VLAN, mientras que la última necesita una interfaz por VLAN.

Tabla de resumen de interfaces del router

Tabla 4. Tabla de Resumen de Interfaces Router Informe 5.1.3.7

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.				

Fuente: Datos del Informe

Apéndice A: comandos de configuración

Switch S1

S1(config)# **vlan 10**
S1(config-vlan)# **name Students**
S1(config-vlan)# **vlan 20**
S1(config-vlan)# **name Faculty**
S1(config-vlan)# **exit**
S1(config)# **interface f0/1**
S1(config-if)# **switchport mode trunk**

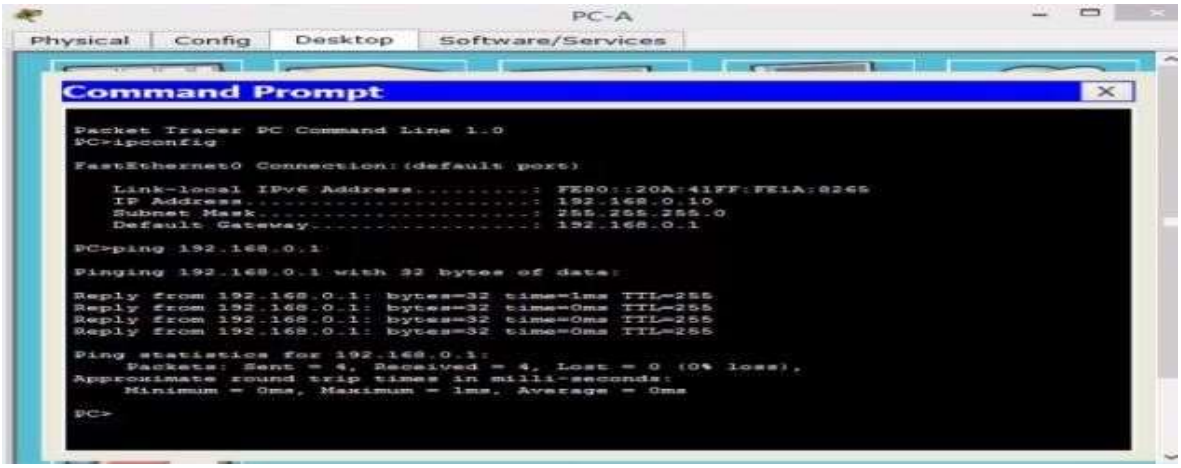
S1(config-if)# **interface f0/5**
S1(config-if)# **switchport mode trunk**
S1(config-if)# **interface f0/6**
S1(config-if)# **switchport mode access**
S1(config-if)# **switchport access vlan 10**
Switch S2
S2(config)# **vlan 10**
S2(config-vlan)# **name Students**
S2(config-vlan)# **vlan 20**
S2(config-vlan)# **name Faculty**
S2(config)# **interface f0/1**
S2(config-if)# **switchport mode trunk**
S2(config-if)# **interface f0/18**
S2(config-if)# **switchport mode access**
S2(config-if)# **switchport access vlan 20**
Router R1
R1(config)# **interface g0/1.1**
R1(config-subif)# **encapsulation dot1Q 1**
R1(config-subif)# **ip address 192.168.1.1 255.255.255.0**
R1(config-subif)# **interface g0/1.10**
R1(config-subif)# **encapsulation dot1Q 10**
R1(config-subif)# **ip address 192.168.10.1 255.255.255.0**
R1(config-subif)# **interface g0/1.20**
R1(config-subif)# **encapsulation dot1Q 20**
R1(config-subif)# **ip address 192.168.20.1 255.255.255.0**
R1(config-subif)# **exit**
R1(config)# **interface g0/1**
R1(config-if)# **no shutdown**

4 INFORME: 6.2.2.5 LAB - CONFIGURING IPV4 STATIC AND DEFAULT ROUTES

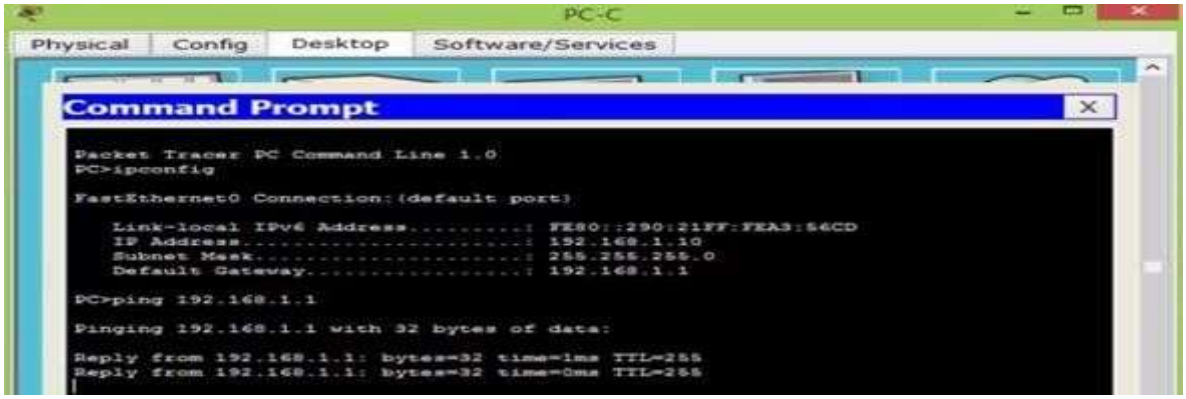
Paso 1. verificar la conectividad de las LAN.

a. Para probar la conectividad, haga ping de cada computadora al gateway predeterminado que se configuró para ese host.

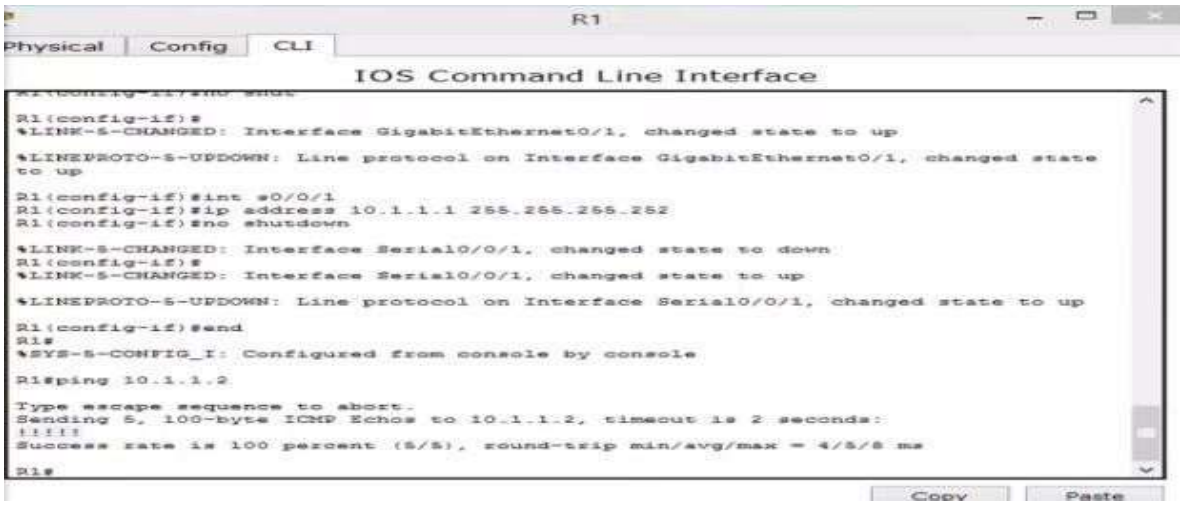
¿Es posible hacer ping de la PC-A al gateway predeterminado?
Rta: Si



¿Es posible hacer ping de la PC-C al gateway predeterminado?
Rta: Si

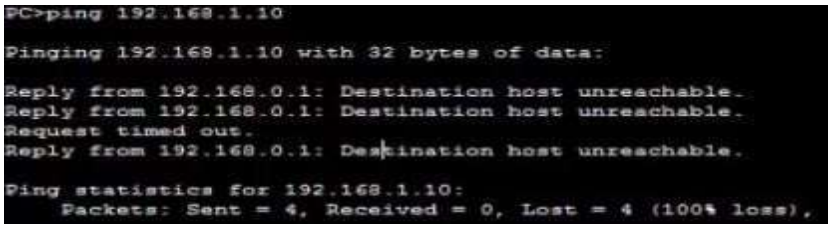


b. Para probar la conectividad, haga ping entre los routers conectados directamente.
¿Es posible hacer ping del R1 a la interfaz S0/0/0 del R3?
Rta: Si

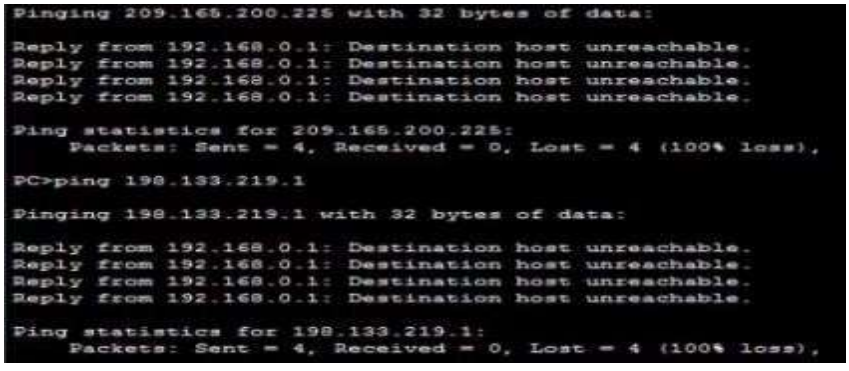


Si la respuesta a cualquiera de estas preguntas es **no**, resuelva los problemas de configuración y corrija el error.

c. Pruebe la conectividad entre los dispositivos que no están conectados directamente.
¿Es posible hacer ping de la PC-A a la PC-C?
Rta: No



¿Es posible hacer ping de la PC-A a la interfaz Lo0? **Rta: No**
¿Es posible hacer ping de la PC-A a la interfaz Lo1? **Rta: No**



¿Los pings eran correctos? ¿Por qué o por qué no?

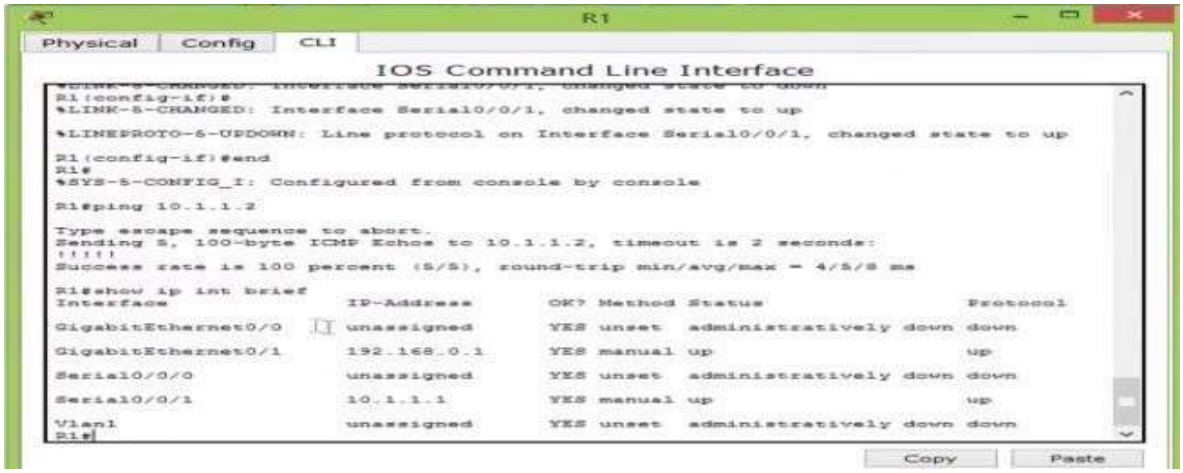
Rta: No fueron satisfactorios porque el router no tiene rutas hacia redes distantes.

Nota: puede ser necesario desactivar el firewall de las computadoras para hacer ping entre ellas.

Paso 2. Reunir información.

Revise el estado de las interfaces en el R1 con el comando **show ip interface brief**

¿Cuántas interfaces están activadas en el R1? **Rta: 2**



d. Revise el estado de las interfaces en el R3.

¿Cuántas interfaces están activadas en el R3? **Rta: 4**

e. Vea la información de la tabla de routing del R1 con el comando **show ip route**.
¿Qué redes están presentes en la tabla de direccionamiento de esta práctica de laboratorio, pero no en la tabla de routing del R1?

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.0.1	255.255.255.0	N/A
	S0/0/1	10.1.1.1	255.255.255.252	N/A
R3	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
	Lo1	198.133.219.1	255.255.255.0	N/A
PC-A	NIC	192.168.0.10	255.255.255.0	192.168.0.1
PC-C	NIC	192.168.1.10	255.255.255.0	192.168.1.1

f. Vea la información de la tabla de routing para el R3.
¿Qué redes están presentes en la tabla de direccionamiento de esta práctica de laboratorio, pero no en la tabla de routing del R3?

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.0.1	255.255.255.0	N/A

¿Por qué ninguna de las redes está presente en las tablas de enrutamiento para cada uno de los routers?
Rta: Los routers no están configurados con un protocolo de ruteo estático y dinámico, y solo conoce sus redes directamente conectadas.

Parte 3. Configure las rutas estáticas.
En la parte 3, empleará varias formas de implementar rutas estáticas y predeterminadas, confirmará si las rutas se agregaron a las tablas de routing del R1 y el R3, y verificará la conectividad sobre la base de las rutas introducidas.

Nota: en esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar el routing estático. Sin embargo, los comandos requeridos se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar los dispositivos sin consultar el apéndice.

Paso 1. Configure una ruta estática recursiva.
Con una ruta estática recursiva, se especifica la dirección IP del siguiente salto. Debido a que solo se especifica la IP de siguiente salto, el router tiene que hacer varias búsquedas en la tabla de routing antes de reenviar paquetes. Para configurar rutas estáticas recursivas, utilice la siguiente sintaxis:
Router(config)# **ip route** *dirección-red máscara-subred dirección-ip*

a. En el router R1, configure una ruta estática a la red 192.168.1.0 utilizando la dirección IP de la interfaz serial 0/0/0 del R3 como la dirección de siguiente salto. En el espacio proporcionado, escriba el comando que utilizó.

```
R1(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.2
```

b. Observe la tabla de enrutamiento para verificar la entrada de la nueva ruta estática.
¿Cómo se indica esta ruta nueva en la tabla de routing?

```
Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/1
L       10.1.1.1/32 is directly connected, Serial0/0/1
     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.0.0/24 is directly connected, GigabitEthernet0/1
L       192.168.0.1/32 is directly connected, GigabitEthernet0/1
S    192.168.1.0/24 [1/0] via 10.1.1.2
R1#
```

Posible hacer ping del host PC-A host a al host PC-C? **Rta: Falla**

```
PC>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Estos pings deben fallar. Si la ruta estática recursiva se configuró correctamente, el ping llega a la PC-C. La PC-C envía un ping de respuesta a la PC-A. Sin embargo, este ping se descarta en el R3, porque el R3 no tiene una ruta de retorno a la red 192.168.0.0 en la tabla de routing.

Paso 2. configurar una ruta estática conectada directamente.
Con una ruta estática conectada directamente, se especifica el parámetro *interfaz-salida*, que permite que el router resuelva una decisión de reenvío con una sola búsqueda. En general, una ruta estática conectada directamente se utiliza con una interfaz serial punto a punto. Para configurar rutas estáticas conectadas directamente con una interfaz de salida especificada, utilice la siguiente sintaxis:
Router(config)# **ip route** *dirección-red máscara-subred interfaz-salida.*

c. En el router R3, configure una ruta estática a la red 192.168.0.0 con la interfaz S0/0/0 como la interfaz de salida. En el espacio proporcionado, escriba el comando que utilizó.

```
R3(config)#ip route 192.168.0.0 255.255.255.0 s0/0/0
```

d. Observe la tabla de enrutamiento para verificar la entrada de la nueva ruta estática.
¿Cómo se indica esta ruta nueva en la tabla de routing?

```
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.2/32 is directly connected, Serial0/0/0
S     192.168.0.0/24 is directly connected, Serial0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/1
L        192.168.1.1/32 is directly connected, GigabitEthernet0/1
      198.133.219.0/24 is variably subnetted, 2 subnets, 2 masks
C        198.133.219.0/24 is directly connected, Loopback1
L        198.133.219.1/32 is directly connected, Loopback1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/27 is directly connected, Loopback0
L        209.165.200.225/32 is directly connected, Loopback0
```

e. ¿Es posible hacer ping del host PC-A host a al host PC-C? **Rta: Si**

```
Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Este ping debe tener éxito.

Nota: puede ser necesario desactivar el firewall de las computadoras para hacer ping entre ellas.

Paso 3. configurar una ruta estática.

f. En el router R1, configure una ruta estática a la red 198.133.219.0 utilizando una de las opciones de configuración de ruta estática de los pasos anteriores. En el espacio proporcionado, escriba el comando que utilizó.

```
R1(config)#ip route 198.133.219.0 255.255.255.0 10.1.1.2
```

g. En el router R1, configure una ruta estática a la red 209.165.200.224 en el R3 utilizando la otra opción de configuración de ruta estática de los pasos anteriores. En el espacio proporcionado, escriba el comando que utilizó.

```
R1(config)#ip route 209.165.200.224 255.255.255.224 s0/0/1
```

h. Observe la tabla de enrutamiento para verificar la entrada de la nueva ruta estática.
¿Cómo se indica esta ruta nueva en la tabla de routing?

```
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/1
L        10.1.1.1/32 is directly connected, Serial0/0/1
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet0/1
L        192.168.0.1/32 is directly connected, GigabitEthernet0/1
S     192.168.1.0/24 [1/0] via 10.1.1.2
S     198.133.219.0/24 [1/0] via 10.1.1.2
      209.165.200.0/27 is subnetted, 1 subnets
S        209.165.200.224/27 is directly connected, Serial0/0/1
```

i. ¿Es posible hacer ping del host PC-A a la dirección 198.133.219.1 del R1? **Rta: Si**

```
PC>ping 198.133.219.1

Pinging 198.133.219.1 with 32 bytes of data:

Reply from 198.133.219.1: bytes=32 time=2ms TTL=254
Reply from 198.133.219.1: bytes=32 time=1ms TTL=254
Reply from 198.133.219.1: bytes=32 time=1ms TTL=254
Reply from 198.133.219.1: bytes=32 time=1ms TTL=254

Ping statistics for 198.133.219.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Este ping debe tener éxito.

Paso 4. Elimine las rutas estáticas de las direcciones de loopback.

j. En el R1, utilice el comando **no** para eliminar las rutas estáticas de las dos direcciones de loopback de la tabla de routing. En el espacio proporcionado, escriba los comandos que utilizó.

```
R1(config)#no ip route 209.165.200.224 255.255.255.224 s0/0/1
R1(config)#no ip route 198.133.219.0 255.255.255.0 10.1.1.2
```

k. Observe la tabla de routing para verificar si se eliminaron las rutas.
¿Cuántas rutas de red se indican en la tabla de routing del R1? 3 redes

```
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/1
L        10.1.1.1/32 is directly connected, Serial0/0/1
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet0/1
L        192.168.0.1/32 is directly connected, GigabitEthernet0/1
S     192.168.1.0/24 [1/0] via 10.1.1.2
R1#
```

¿El gateway de último recurso está establecido? **Rta: Es una ruta por defecto.**

Parte 4. configurar y verificar una ruta predeterminada

En la parte 4, implementará una ruta predeterminada, confirmará si la ruta se agregó a la tabla de routing y verificará la conectividad sobre la base de la ruta introducida.

Una ruta predeterminada identifica el gateway al cual el router envía todos los paquetes IP para los que no tiene una ruta descubierta o estática. Una ruta estática predeterminada es una ruta estática con 0.0.0.0 como dirección IP y máscara de subred de destino. Comúnmente, esta ruta se denomina “ruta de cuádruple cero”.

En una ruta predeterminada, se puede especificar la dirección IP del siguiente salto o la interfaz de salida. Para configurar una ruta estática predeterminada, utilice la siguiente sintaxis:

Router(config)# **ip route 0.0.0.0 0.0.0.0** {*ip-address or exit-intf*}

a. Configure el router R1 con una ruta predeterminada que utilice la interfaz de salida S0/0/1. En el espacio proporcionado, escriba el comando que utilizó.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
```

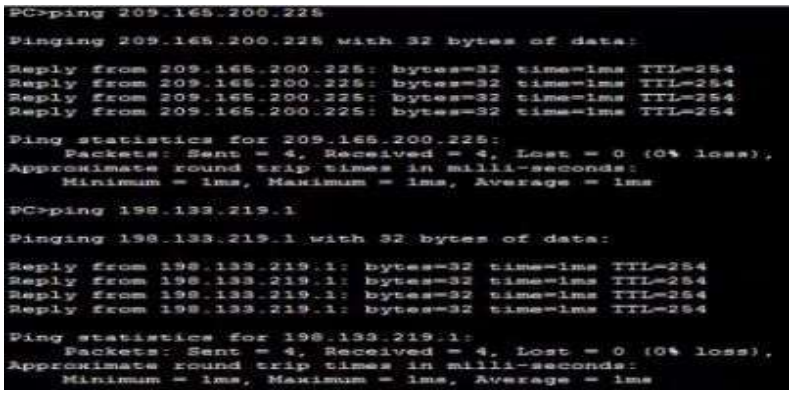
b. Observe la tabla de enrutamiento para verificar la entrada de la nueva ruta estática.
¿Cómo se indica esta ruta nueva en la tabla de routing?

```
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/1
L        10.1.1.1/32 is directly connected, Serial0/0/1
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet0/1
L        192.168.0.1/32 is directly connected, GigabitEthernet0/1
S     192.168.1.0/24 [1/0] via 10.1.1.2
S*    0.0.0.0/0 is directly connected, Serial0/0/1
R1#
```

¿Cuál es el gateway de último recurso?

```
S     192.168.1.0/24 [1/0] via 10.1.1.2
S*    0.0.0.0/0 is directly connected, Serial0/0/1
```

c. ¿Es posible hacer ping del host PC-A a 209.165.200.225? **Rta: Si**
d. ¿Es posible hacer ping del host PC-A a 198.133.219.1? **Rta: Si**
Estos pings deben tener éxito.



4.1.1 REFLEXIÓN

1. Una nueva red 192.168.3.0/24 está conectada a la interfaz G0/0 del R1. ¿Qué comandos podrían utilizarse para configurar una ruta estática a esa red desde el R3?
Rta:
Ip route 192.168.3.0 255.255.255.0 10.1.1.1
Ip route 192.168.3.0 255.255.255.0 s0/0/0
Or ip route 0.0.0.0.0.0.0.0 s0/0/0

2. ¿Ofrece alguna ventaja configurar una ruta estática conectada directamente, en vez de una ruta estática?

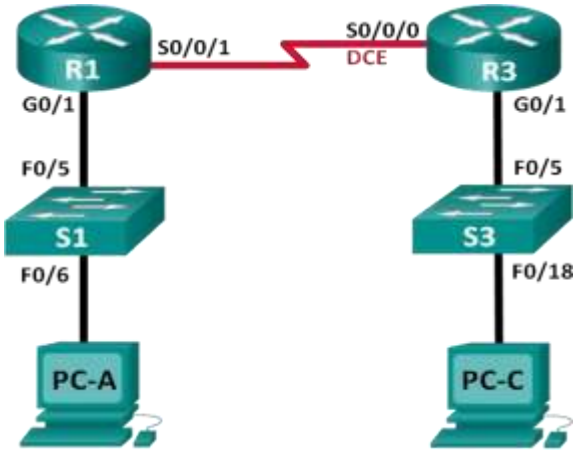
Rta: El beneficio es que cuando se usa una ruta estática directamente conectada la interface de salida se resuelve en una sola búsqueda, mientras que una ruta estática recursiva se necesita 2 búsquedas para resolver la interface de salida.

3. ¿Por qué es importante configurar una ruta predeterminada en un router?
Rta: Ayuda a enviar paquetes hacia rutas desconocidas.

5 INFORME: 6.2.4.5 LAB - CONFIGURING IPV6 STATIC AND DEFAULT ROUTES

5.1 TOPOLOGÍA

Imagen 6. Topología Informe 6.2.4.5



Fuente: Datos del Informe

Tabla de direccionamiento

Tabla 5. Tabla de Direccionamiento Informe 6.2.4.5

Dispositivo	Interfaz	Dirección IPv6/longitud de prefijo	Gateway predeterminado
R1	G0/1	2001:DB8:ACAD:A::/64 eui-64	N/A
	S0/0/1	FC00::1/64	N/A
R3	G0/1	2001:DB8:ACAD:B::/64 eui-64	N/A
	S0/0/0	FC00::2/64	N/A
PC-A	NIC	SLAAC	SLAAC
PC-C	NIC	SLAAC	SLAAC

Fuente: Datos del Informe

Objetivos

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

- Habilitar el routing de unidifusión IPv6 y configurar el direccionamiento IPv6 en los routers.
- Deshabilitar el direccionamiento IPv4 y habilitar SLAAC de IPv6 para las interfaces de red de las computadoras.
- Usar **ipconfig** y **ping** para verificar la conectividad LAN.
- Usar los comandos **show** para verificar la configuración de IPv6.

Parte 2: configurar rutas estáticas y predeterminadas IPv6

- Configurar una ruta estática IPv6 conectada directamente.
- Configurar una ruta estática IPv6 recursiva.
- Configurar una ruta estática predeterminada IPv6.

Información básica/situación

En esta práctica de laboratorio, configurará toda la red para establecer la comunicación solo con direccionamiento IPv6. Esto incluye la configuración de los routers y las computadoras. Usará la configuración automática de dirección sin estado (SLAAC) para configurar las direcciones IPv6 para los hosts. También configurará rutas estáticas y predeterminadas IPv6 en los routers para habilitar la comunicación con redes remotas que no están conectadas directamente.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

- 2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

Parte 5. armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, realizará el cableado de la red y la configurará para que establezca la comunicación utilizando direccionamiento IPv6.

Paso 1. Realice el cableado de red tal como se muestra en el diagrama de topología.
Paso 2. inicializar y volver a cargar los routers y los switches.
Paso 3. habilitar el routing de unidifusión IPv6 y configurar el direccionamiento IPv6 en los routers.

a. Mediante Tera Term, acceda al router etiquetado R1 en el diagrama de la topología mediante el puerto de consola y asígnele el nombre R1.
b. En el modo de configuración global, habilite el routing IPv6 en el R1.
R1(config)# **ipv6 unicast-routing**
c. Configure las interfaces de red en el R1 con direcciones IPv6. Observe que IPv6 está habilitado en cada interfaz. La interfaz G0/1 tiene una dirección de unidifusión enrutable globalmente, y se utiliza EUI-64 para crear la porción del identificador de la interfaz de la dirección. La interfaz S0/0/1 tiene una dirección local única y enrutable de forma privada, que se recomienda para las conexiones seriales punto a punto.

R1(config)# **interface g0/1**
R1(config-if)# **ipv6 address 2001:DB8:ACAD:A::/64 eui-64**
R1(config-if)# **no shutdown**
R1(config-if)# **interface serial 0/0/1**
R1(config-if)# **ipv6 address FC00::1/64**
R1(config-if)# **no shutdown**
R1(config-if)# exit

```
Router(config)#hostname R1
R1(config)#ipv6 unicast-routing
R1(config)#interface g0/1
R1(config-if)#ipv6 address 2001:db8:acad:a::/64 eui-64
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to up

R1(config-if)#interface s0/0/1
R1(config-if)#ipv6 address fc00::1/64
R1(config-if)#no shutdown
```

d. Asigne un nombre de dispositivo al router R3.
e. En el modo de configuración global, habilite el routing IPv6 en el R3.
R3(config)# **ipv6 unicast-routing**
f. Configure las interfaces de red en el R3 con direcciones IPv6. Observe que IPv6 está habilitado en cada interfaz. La interfaz G0/1 tiene una dirección de

unidifusión enrutable globalmente, y se utiliza EUI-64 para crear la porción del identificador de la interfaz de la dirección. La interfaz S0/0/0 tiene una dirección local única y enrutable de forma privada, que se recomienda para las conexiones seriales punto a punto. La frecuencia de reloj está establecida, porque es el extremo del DCE del cable serial.

R3(config)# **interface gigabit 0/1**
R3(config-if)# **ipv6 address 2001:DB8:ACAD:B::/64 eui-64**
R3(config-if)# **no shutdown**
R3(config-if)# **interface serial 0/0/0**
R3(config-if)# **ipv6 address FC00::2/64**
R3(config-if)# **clock rate 128000**
R3(config-if)# **no shutdown**
R3(config-if)# **exit**

```
Router(config)#hostname R3
R3(config)#ipv6 unicast-routing
R3(config)#interface g0/1
R3(config-if)#ipv6 address 2001:DB8:ACAD:B::/64 eui-64
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to up

R3(config-if)#interface s0/0/0
R3(config-if)#ipv6 address FC00::2/64
R3(config-if)#clock rate 128000
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R3(config-if)#exit
```

Paso 4. deshabilitar el direccionamiento IPv4 y habilitar SLAAC de IPv6 para las interfaces de red de las computadoras.

g. En la PC-A y la PC-C, navegue hasta el menú **Inicio** > **Panel de control**. Haga clic en el enlace **Centro de redes y recursos compartidos** en la vista por íconos. En la ventana Centro de redes y recursos compartidos, haga clic en el enlace **Cambiar configuración del adaptador**, que se encuentra en el lado izquierdo de la ventana, para abrir la ventana Conexiones de red.

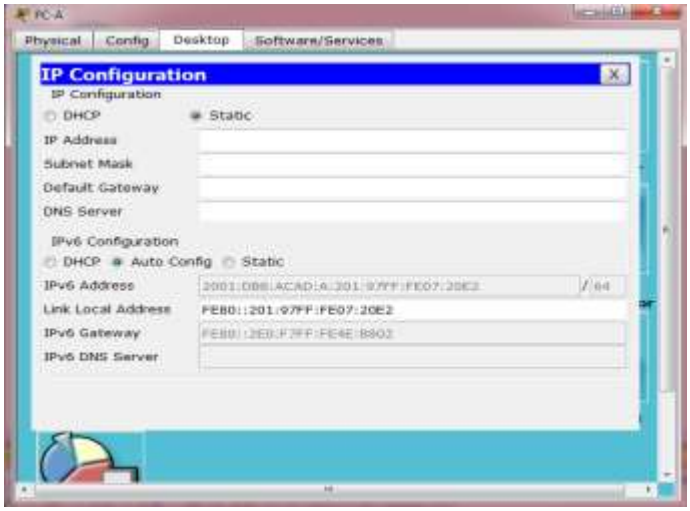
h. En la ventana Conexiones de red, verá los íconos de los adaptadores de interfaz de red. Haga doble clic en el ícono de Conexión de área local de la interfaz de red de la computadora que está conectada al switch. Haga clic en **Propiedades** para abrir la ventana de diálogo Propiedades de conexión de área local.

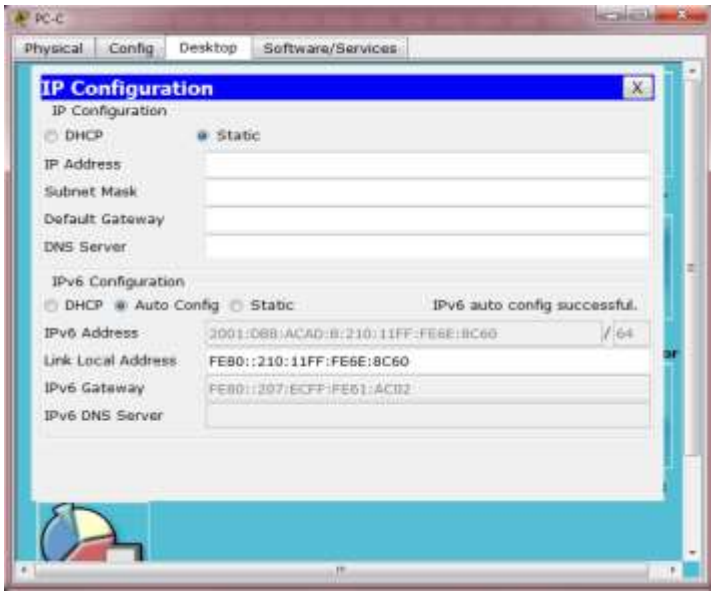
i. Con la ventana Propiedades de conexión de área local abierta, desplácese hacia abajo por los elementos y desactive la casilla de verificación del elemento **Protocolo de Internet versión 4 (TCP/IPv4)** para deshabilitar el protocolo IPv4 en la interfaz de red.

j. Con la ventana Propiedades de conexión de área local todavía abierta, haga clic en la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y luego en **Propiedades**.

k. Con la ventana Propiedades > Protocolo de Internet versión 6 (TCP/IPv6) abierta, verifique que los botones de opción **Obtener una dirección IPv6 automáticamente** y **Obtener la dirección del servidor DNS automáticamente** estén seleccionados. Si no lo están, selecciónelos.

l. Si las computadoras están configuradas para obtener una dirección IPv6 automáticamente, se comunicarán con los routers para obtener la información del gateway y de la subred de la red y configurarán automáticamente la información de la dirección IPv6. En el siguiente paso, verificará la configuración.





Paso 5. usar ipconfig y ping para verificar la conectividad LAN.

m. En la PC-A, abra un símbolo del sistema, escriba **ipconfig /all** y presione Enter. El resultado debe ser similar al que se muestra a continuación. En el resultado, debería ver que la computadora ahora tiene una dirección IPv6 de unidifusión global, una dirección IPv6 link-local y una dirección IPv6 link-local de gateway predeterminado. Es posible que también vea una dirección IPv6 temporal y, en direcciones del servidor DNS, tres direcciones locales de sitio que empiezan con FEC0. Las direcciones locales de sitio son direcciones privadas que tienen compatibilidad retrospectiva con NAT. Sin embargo, no son compatibles con IPv6, y se reemplazaron con direcciones locales únicas.

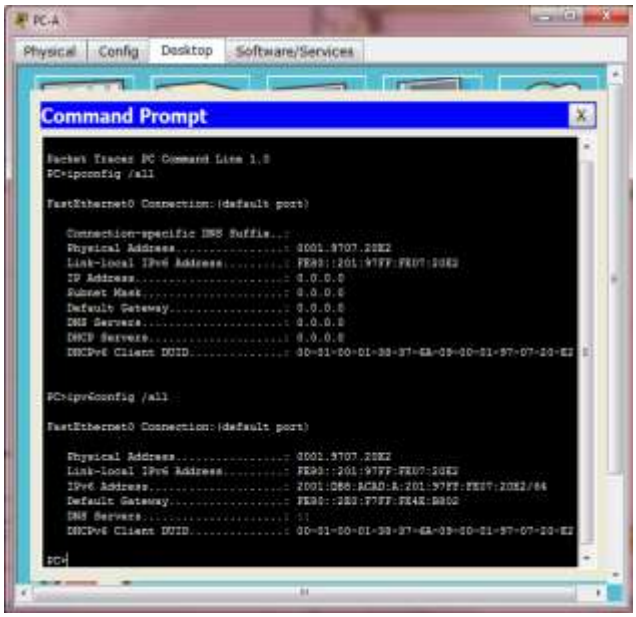
C:\Users\User1> **ipconfig /all**

Windows IP Configuration

<Output Omitted>

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) 82577LC Gigabit Network Connection
Physical Address. . . . . : 1C-C1-DE-91-C3-5D
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:db8:acad:a:7c0c:7493:218d:2f6c(Preferred)
Temporary IPv6 Address. . . . . .
2001:db8:acad:a:bc40:133a:54e7:d497(Preferred)
Link-local IPv6 Address . . . . . : fe80::7c0c:7493:218d:2f6c%13(Preferred)
Default Gateway . . . . . : fe80::6273:5cff:fe0d:1a61%13
DNS Servers . . . . . : fec0:0:0:ffff::1%1
fec0:0:0:ffff::2%1
fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Disabled



Sobre la base de la implementación de la red y el resultado del comando **ipconfig /all**, ¿la PC-A recibió información de direccionamiento IPv6 del R1?

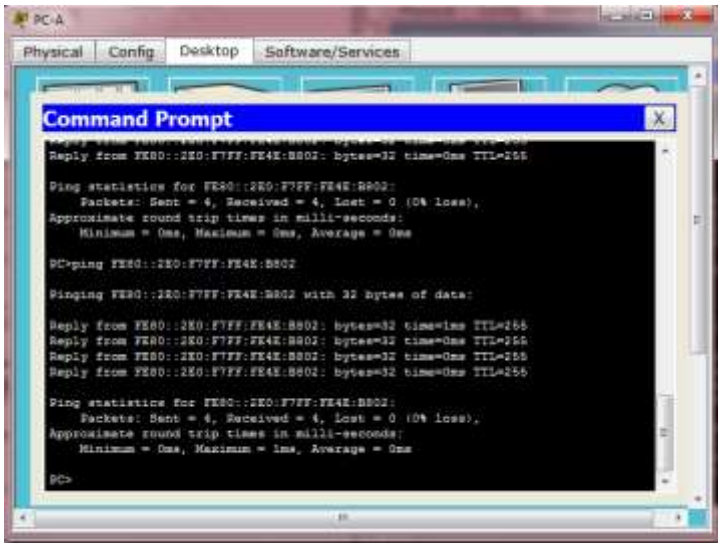
Rta: Si, la Ipv6 de esta PC fue negociada con la interface del router R1, esta cuenta con información de los dos dispositivos.

n. ¿Cuál es la dirección IPv6 de unidifusión global de la PC-A?
Rta: 2001:db8:acad:a:201:97ff:fe07:20e2/64

o. ¿Cuál es la dirección IPv6 link-local de la PC-A?
Rta: fe80::201:97ff:fe07:20e2

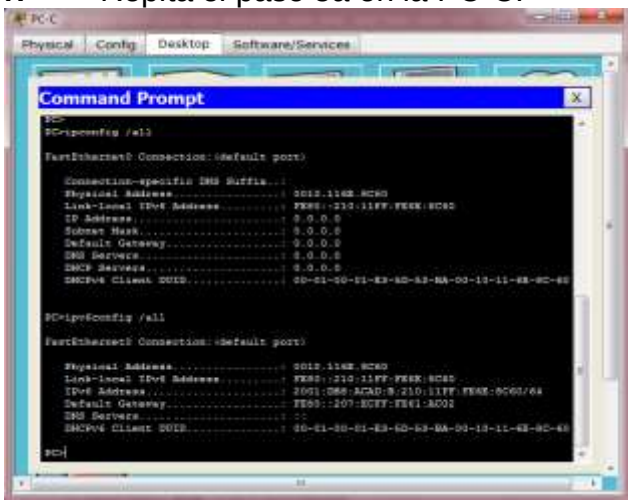
p. ¿Cuál es la dirección IPv6 de gateway predeterminado de la PC-A?
Rta: fe80::2e0:f7ff:fe4e:b802

q. En la PC-A, use el comando **ping -6** para emitir un ping IPv6 a la dirección link-local de gateway predeterminado. Debería ver respuestas del router R1.



C:\Users\User1> **ping -6 <default-gateway-address>**
¿La PC-A recibió respuestas al ping hizo que al R1?
Rta: SI

r. Repita el paso 5a en la PC-C.



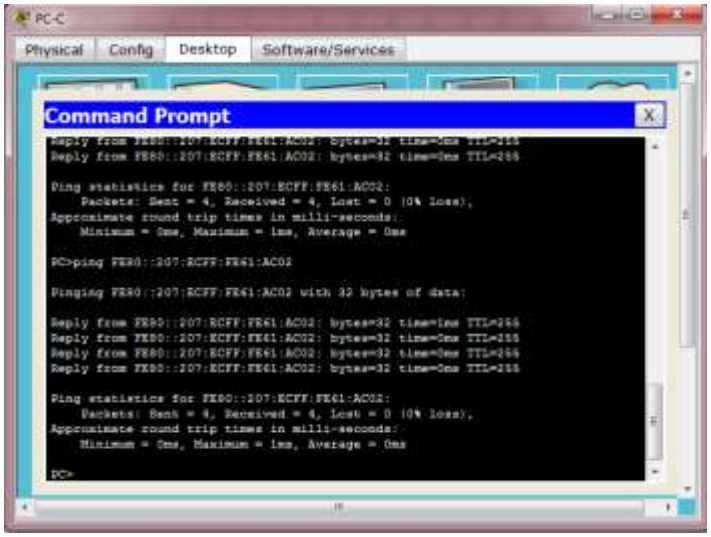
¿La PC-C recibió información de direccionamiento IPv6 del R3?
Rta: SI

s. ¿Cuál es la dirección IPv6 de unidifusión global de la PC-C?
Rta: 2001:db8:acad:b:210:11ff:fe6e:8c60/64

t. ¿Cuál es la dirección IPv6 link-local de la PC-C?
Rta: fe80::210:11ff:fe6e:8c60

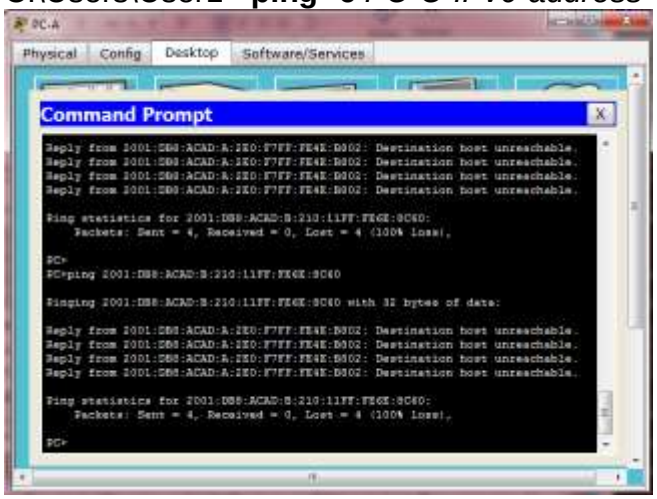
u. ¿Cuál es la dirección IPv6 de gateway predeterminado de la PC-C?
Rta: fe80::207:ecff:fe61:ac02

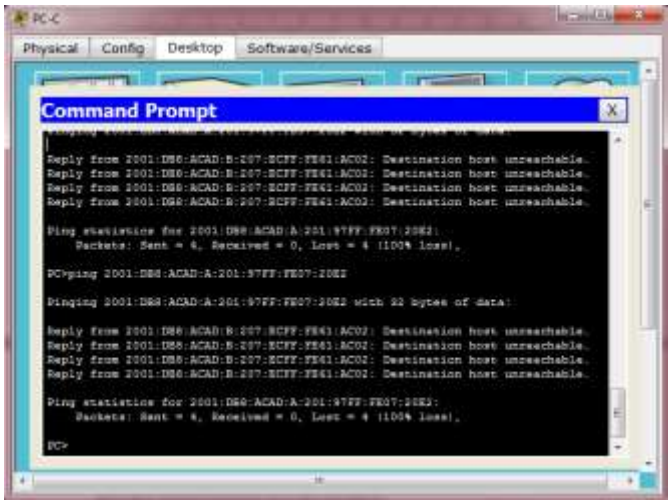
v. En la PC-C, use el comando **ping -6** para hacer ping al gateway predeterminado de la PC-C.



¿La PC-C recibió respuestas a los pings que hizo al R3?
Rta: SI

w. Intente hacer **ping -6** IPv6 de la PC-A a la dirección IPv6 de la PC-C.
C:\Users\User1> **ping -6** *PC-C-IPv6-address*





¿El ping se realizó correctamente? ¿Por qué o por qué no?
Rta: No, estos fallaron puesto que los routers no cuentan con rutas configuradas para estas redes.

Paso 6. Use los comandos show para verificar la configuración de IPv6.

x. Revise el estado de las interfaces en el R1 con el comando **show ipv6 interface brief**.

```
R1>enable
R1#show ipv6 interface brief
GigabitEthernet0/0         [administratively down/down]
GigabitEthernet0/1         [up/up]
    FE80::2E0:F7FF:FE4E:B802
    2001:DB8:ACAD:A:2E0:F7FF:FE4E:B802
Serial0/0/0                [administratively down/down]
Serial0/0/1                [up/up]
    FE80::2E0:F7FF:FE4E:B801
    FC00::1
Vlan1                      [administratively down/down]
R1#
```

¿Cuáles son las dos direcciones IPv6 de la interfaz G0/1 y qué tipo de direcciones IPv6 son?
Rta:

- **fe80::2e0:f7ff:fe4e:b802 - link-local:**
- **2001:db8:acad:a:2e0:f7ff:fe4e:b802 - global-unicast:**

¿Cuáles son las dos direcciones IPv6 de la interfaz S0/0/1 y qué tipo de direcciones IPv6 son?
Rta:

- **fe80::2e0:f7ff:fe4e:b801 - link.local**
- **fc00::1 - global-unicast.**

y. Para ver información más detallada sobre las interfaces IPv6, escriba el comando **show ipv6 interface** en el R1 y presione Enter.
¿Cuáles son las direcciones del grupo de multidifusión de la interfaz Gigabit Ethernet 0/1?
Rta:

- **ff02::1**
- **ff02::2**
- **ff02::1:ff4e:b802**

¿Cuáles son las direcciones del grupo de multidifusión de la interfaz S0/0/1?
Rta:

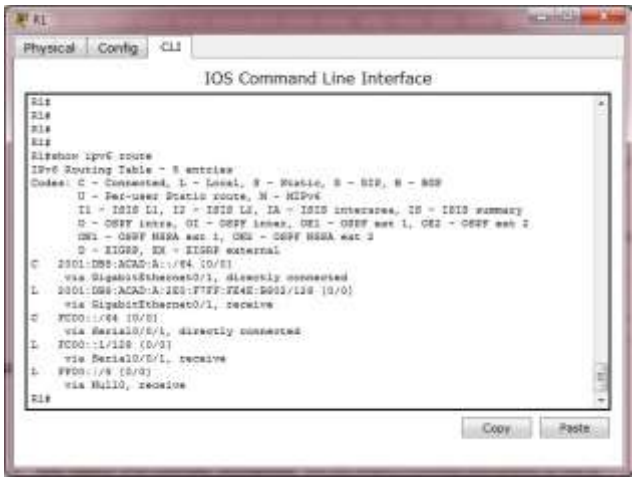
- **ff02::1:ff00:1**
- **ff02::1:ff4e:b801**

¿Para qué se usa la dirección de multidifusión FF02::1?
Rta: Para hacer llegar algún tipo de información a todos los nodos o con el fin de conocer los vecinos.

¿Para qué se usa la dirección de multidifusión FF02::2?
Rta: Estas los utilizan los routers para conocer información de los vecinos.

¿Qué tipo de direcciones de multidifusión son FF02::1:FF00:1 y FF02::1:FF0D:1A60 y para qué se usan?
Rta: Estas las utilizan los dispositivos poder resolver las direcciones de los vecinos del enlace local.

z. Vea la información de la tabla de routing IPv6 del R1 con el comando **show ipv6 route**. La tabla de routing IPv6 debe tener dos rutas conectadas, una para cada interfaz, y tres rutas locales, una para cada interfaz y otra para el tráfico de multidifusión a una interfaz Null0.



¿De qué forma el resultado de la tabla de routing del R1 revela el motivo por el que no pudo hacer ping de la PC-A a la PC-C?
Rta: Si observamos la tabla de enrutamiento para R1 observamos claramente que esta no conoce la red a la cual está conectado el PC3, esta es el motivo por el cual el paquete es descartado.

Parte 6. configurar rutas estáticas y predeterminadas IPv6
En la parte 2, configurará rutas estáticas y predeterminadas IPv6 de tres maneras distintas. Confirmará que las rutas se agreguen a las tablas de routing y verificará que la conectividad entre la PC-A y la PC-C sea correcta.
Configurará tres tipos de rutas estáticas IPv6:

- **Ruta estática IPv6 conectada directamente**: una ruta estática conectada directamente se crea al especificar la interfaz de salida.

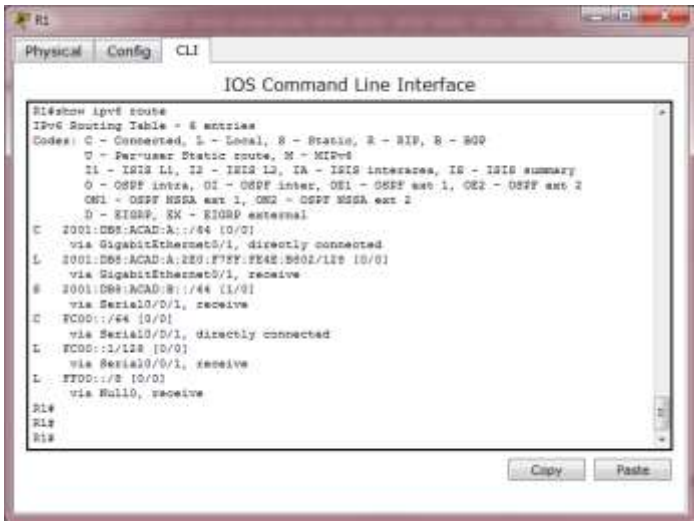
- **Ruta estática IPv6 recursiva**: una ruta estática recursiva se crea al especificar la dirección IP del siguiente salto. Este método requiere que el router ejecute una búsqueda recursiva en la tabla de routing para identificar la interfaz de salida.
- **Ruta estática predeterminada IPv6**: similar a una ruta IPv4 de cuádruple cero, una ruta estática predeterminada IPv6 se crea al hacer que el prefijo IPv6 de destino y la longitud de prefijo sean todos ceros, :: /0.

Paso 1. configurar una ruta estática IPv6 conectada directamente.
En una ruta estática IPv6 conectada directamente, la entrada de ruta especifica la interfaz de salida del router. En general, una ruta estática conectada directamente se utiliza con una interfaz serial punto a punto. Para configurar una ruta estática IPv6 conectada directamente, utilice el siguiente formato de comando:
Router(config)# **ipv6 route** *<ipv6-prefix/prefix-length> <outgoing-interface-type> <outgoing-interface-number>*

a. En el router R1, configure una ruta estática IPv6 a la red 2001:DB8:ACAD:B::/64 en el R3 mediante la interfaz de salida S0/0/1 del R1.
R1(config)# **ipv6 route 2001:DB8:ACAD:B::/64 serial 0/0/1**
R1(config)#

```
R1>enable
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ipv6 route 2001:db8:acad:b::/64 s0/0/1
R1(config)#
```

b. Consulte la tabla de routing IPv6 para verificar la entrada de la ruta estática nueva.



¿Cuáll es la letra de código y la entrada de la tabla de routing de la ruta que se agregó recientemente a la tabla de routing?
Rta: S 2001:DB8:ACAD:B::/64 [1/0] - via Serial0/0/1, receive

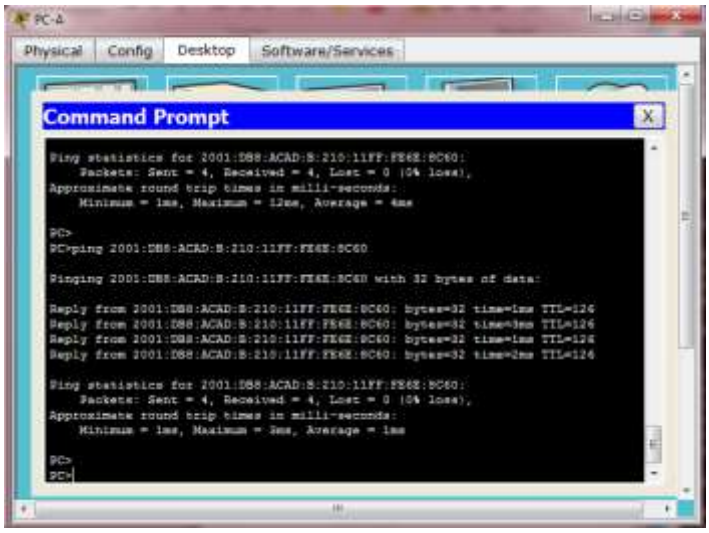
c. Ahora que la ruta estática se configuró en el R1, ¿es posible hacer ping de la PC-A al host PC-C?
Rta: R1 tiene una ruta para llegar a las PC3, pero el R3 no tiene un ruta de retorno para llegar a PC1.

Estos pings deben fallar. Si la ruta estática recursiva se configuró correctamente, el ping llega a la PC-C. La PC-C envía un ping de respuesta a la PC-A. Sin embargo, ese ping se descarta en el R3, porque el R3 no tiene una ruta de retorno a la red 2001:DB8:ACAD:A::/64 en la tabla de routing. Para hacer ping correctamente a través de la red, también debe crear una ruta estática en el R3.

d. En el router R3, configure una ruta estática IPv6 a la red 2001:DB8:ACAD:A::/64, mediante la interfaz de salida S0/0/0 del R3.
R3(config)# **ipv6 route 2001:DB8:ACAD:A::/64 serial 0/0/0**
R3(config)#

```
R3#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ipv6 route 2001:DB8:ACAD:A::/64 serial 0/0/0
R3(config)#
```

e. Ahora que ambos routers tienen rutas estáticas, intente hacer **ping -6** de IPv6 desde la PC-A hasta la dirección IPv6 de unidifusión global de la PC-C.



¿El ping se realizo correctamente? ¿Por qué?
Rta: Si, las rutas creadas funcionan bien, cada router tiene una ruta para la red distante, y esa red cuenta con una ruta de respuesta.
Paso 2. configurar una ruta estática IPv6 recursiva.
En una ruta estática IPv6 recursiva, la entrada de ruta tiene la dirección IPv6 del router del siguiente salto. Para configurar una ruta estática IPv6 recursiva, utilice el siguiente formato de comando:

Router (config)# **ipv6 route** *<ipv6-prefix/prefix-length> <next-hop-ipv6-address>*

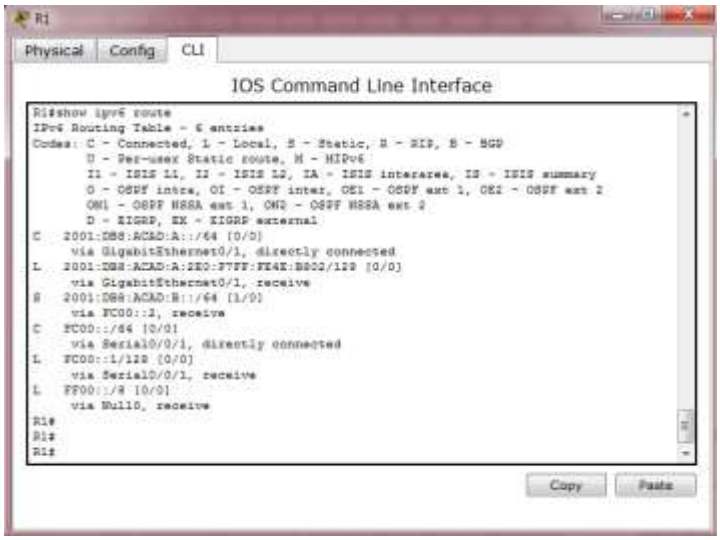
f. En el router R1, elimine la ruta estática conectada directamente y agregue una ruta estática recursiva.
R1(config)# **no ipv6 route 2001:DB8:ACAD:B::/64 serial 0/0/1**
R1(config)# **ipv6 route 2001:DB8:ACAD:B::/64 FC00::2**
R1(config)# **exit**

```
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#no ipv6 route 2001:DB8:ACAD:B::/64 serial 0/0/1
R1(config)#ipv6 route 2001:DB8:ACAD:B::/64 FC00::2
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

g. En el router R3, elimine la ruta estática conectada directamente y agregue una ruta estática recursiva.
R3(config)# **no ipv6 route 2001:DB8:ACAD:A::/64 serial 0/0/0**
R3(config)# **ipv6 route 2001:DB8:ACAD:A::/64 FC00::1**
R3(config)# **exit**

```
R3(config)#no ipv6 route 2001:DB8:ACAD:A::/64 serial 0/0/0
R3(config)#ipv6 route 2001:DB8:ACAD:A::/64 FC00::1
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#
```

h. Consulte la tabla de routing IPv6 del R1 para verificar la entrada de la ruta estática nueva.



¿Cuáll es la letra de código y la entrada de la tabla de routing de la ruta que se agregó recientemente a la tabla de routing?
Rta: S 2001:DB8:ACAD:B::/64 [1/0] - via FC00::2, receive

i. Para verificar la conectividad, emita un comando **ping -6** de la PC-A a la PC-C.
¿El ping se realizó correctamente?
Rta: SI

Nota: puede ser necesario desactivar el firewall de las computadoras para hacer ping entre ellas.

Paso 3. configurar una ruta estática predeterminada IPv6.
En una ruta estática predeterminada, el prefijo IPv6 de destino y la longitud de prefijo son todos ceros.

Router(config)# **ipv6 route ::/0** *<outgoing-interface-type> <outgoing-interface-number> {and/or} <next-hop-ipv6-address>*

j. En el router R1, elimine la ruta estática recursiva y agregue una ruta estática predeterminada.

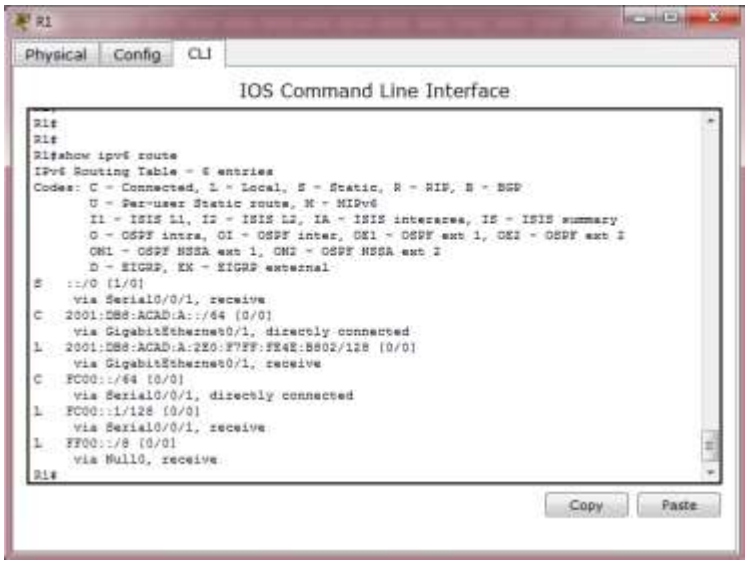
R1(config)# **no ipv6 route 2001:DB8:ACAD:B::/64 FC00::2**
R1(config)# **ipv6 route ::/0 serial 0/0/1**
R1(config)#

```
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#no ipv6 route 2001:DB8:ACAD:B::/64 FC00::2
R1(config)#ipv6 route ::/0 serial 0/0/1
R1(config)#exit
R1#
```

k. En el R3, elimine la ruta estática recursiva y agregue una ruta estática predeterminada.

```
R3(config)#
R3(config)#no ipv6 route 2001:DB8:ACAD:A::/64 FC00::1
R3(config)#ipv6 route ::/0 serial 0/0/0
R3(config)#exit
R3#
```

Consulte la tabla de routing IPv6 del R1 para verificar la entrada de la ruta estática nueva.



¿Cuál es la letra de código y la entrada de la tabla de routing de la ruta predeterminada que se agregó recientemente a la tabla de routing?
Rta: S ::/0 [1/0] - via Serial0/0/1, receive

l. Para verificar la conectividad, emita un comando **ping -6** de la PC-A a la PC-C.
Rta: ¿El ping se realizó correctamente?
SI
Nota: quizás sea necesario inhabilitar el firewall de las computadoras para hacer ping entre estas.

5.1.1 REFLEXIÓN

1. Esta práctica de laboratorio se centra en la configuración de rutas estáticas y predeterminadas IPv6. ¿Puede pensar en una situación en la que tendría que configurar rutas estáticas y predeterminadas IPv6 e IPv4 en un router?
Rta: Pienso que esto es posible, pues IPV6 ya está funcionando en internet, pero IPV4 no ha salido, esto quiere decir que las dos tecnologías conviven.

2. En la práctica, la configuración de rutas estáticas y predeterminadas IPv6 es muy similar a la configuración de rutas estáticas y predeterminadas IPv4. Independientemente de las diferencias obvias entre el direccionamiento IPv6 e IPv4, ¿cuáles son algunas otras diferencias que se observan al configurar y verificar una ruta estática IPv6 en comparación con una ruta estática IPv4?
Rta: La forma en que se crean esta rutas es muy similar, lo que si cambia es algo los comandos empleados para crearlas.

Tabla de resumen de interfaces del router

Tabla 6. Tabla de Resumen de Interfaces del Router Informe 6.2.4.5

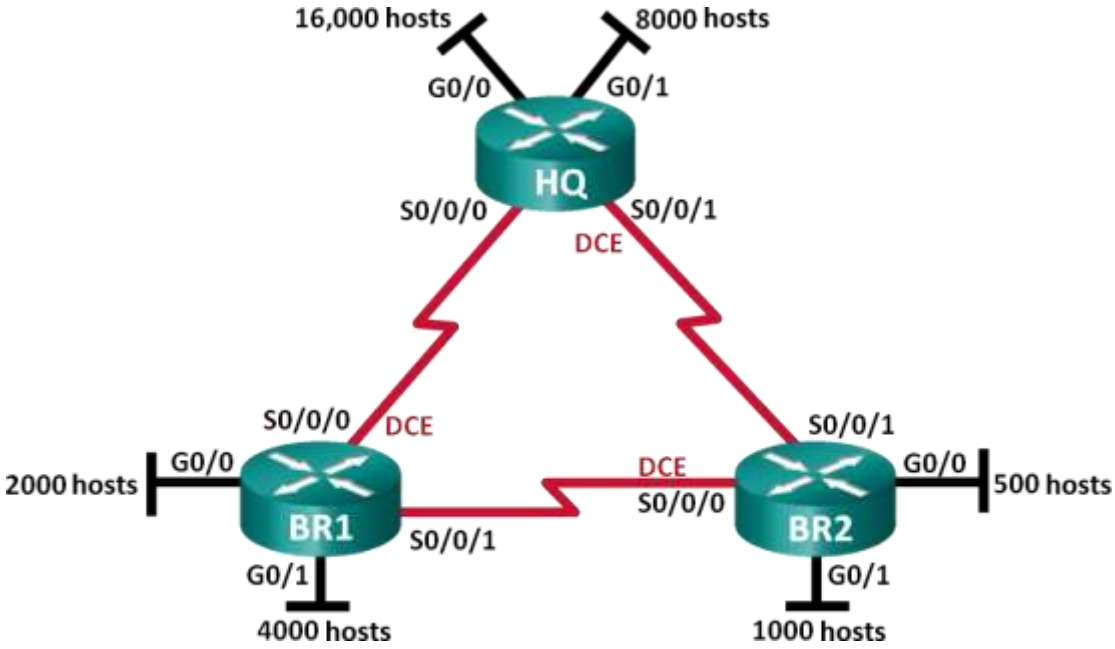
Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.				

Fuente: Datos del Informe

6 INFORME: 6.3.3.7 LAB - DESIGNING AND IMPLEMENTING IPV4 ADDRESSING WITH VLSM

6.1 TOPOLOGÍA

Imagen 7. Topología Informe 6.3.3.7



Fuente: Datos del Informe

Objetivos

Parte 1: examinar los requisitos de la red

Parte 2: diseñar el esquema de direcciones VLSM

Parte 3: realizar el cableado y configurar la red IPv4

Información básica/situación

La máscara de subred de longitud variable (VLSM) se diseñó para conservar direcciones IP. Con VLSM, una red se divide en subredes, que luego se subdividen nuevamente. Este proceso se puede repetir varias veces para crear subredes de distintos tamaños, según el número de hosts requerido en cada subred. El uso eficaz de VLSM requiere la planificación de direcciones.

En esta práctica de laboratorio, se le asigna la dirección de red 172.16.128.0/17 para que desarrolle un esquema de direcciones para la red que se muestra en el diagrama de la topología. Se usará VLSM para que se pueda cumplir con los requisitos de direccionamiento. Después de diseñar el esquema de direcciones VLSM, configurará las interfaces en los routers con la información de dirección IP adecuada.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Pueden utilizarse otros routers y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 computadora (con un programa de emulación de terminal, como Tera Term, para configurar los routers)
- Cable de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet (optativo) y seriales, como se muestra en la topología
- Calculadora de Windows (optativo)

Parte 1: examinar los requisitos de la red

En la parte 1, examinará los requisitos de la red y utilizará la dirección de red 172.16.128.0/17 para desarrollar un esquema de direcciones VLSM para la red que se muestra en el diagrama de la topología.

Nota: puede utilizar la aplicación Calculadora de Windows y la calculadora de subredes IP de www.ipcalc.org como ayuda para sus cálculos.

Paso 1. determinar la cantidad de direcciones host disponibles y la cantidad de subredes que se necesitan.

¿Cuántas direcciones host se encuentran disponibles en una red /17?
Rta: 32766

¿Cuál es la cantidad total de direcciones host que se necesitan en el diagrama de la topología?
Rta: 31506

¿Cuántas subredes se necesitan en la topología de la red?
Rta: 9

Paso 2. determinar la subred más grande que se necesita.

Descripción de la subred (p. ej., enlace BR1 G0/1 LAN o BR1-HQ WAN)
Rta: HQ G0/0 LAN

¿Cuántas direcciones IP se necesitan en la subred más grande?
Rta: 16 000

¿Cuál es la subred más pequeña que admite esa cantidad de direcciones?
Rta: /18 - 255.255.192.0

¿Cuántas direcciones host admite esa subred?
Rta: 16 382

¿Se puede dividir la red 172.16.128.0/17 en subredes para admitir esta subred?
Rta: Sí.

¿Cuáles son las dos direcciones de red que se obtendrían de esta división en subredes?
Rta:

- **172.16.128.0/18**
- **172.16.192.0/18**

Utilice la primera dirección de red para esta subred.

Paso 3. determinar la segunda subred más grande que se necesita.
Descripción de la subred
Rta: HQ G0/1 LAN

¿Cuántas direcciones IP se necesitan para la segunda subred más grande?
Rta: 8000

¿Cuál es la subred más pequeña que admite esa cantidad de hosts?
Rta: /19 - 255.255.224.0

¿Cuántas direcciones host admite esa subred?
Rta: 8190

¿Se puede volver a dividir la subred restante en subredes sin que deje de admitir esta subred?
Rta: Sí.

¿Cuáles son las dos direcciones de red que se obtendrían de esta división en subredes?
Rta:

- **172.16.192.0/19**
- **172.16.224.0/19**

Utilice la primera dirección de red para esta subred.

Paso 4. determinar la siguiente subred más grande que se necesita.
Descripción de la subred
Rta: BR1 G0/1 LAN

¿Cuántas direcciones IP se necesitan para la siguiente subred más grande?
Rta: 4000

¿Cuál es la subred más pequeña que admite esa cantidad de hosts?
Rta: 172.16.224.0/20

¿Cuántas direcciones host admite esa subred?
Rta: 4094

¿Se puede volver a dividir la subred restante en subredes sin que deje de admitir esta subred?
Rta: Sí.

¿Cuáles son las dos direcciones de red que se obtendrían de esta división en subredes?
Rta:

- **172.16.224.0/20**
- **172.16.240.0/20**

Utilice la primera dirección de red para esta subred.

Paso 5. determinar la siguiente subred más grande que se necesita.
Descripción de la subred
Rta: BR1 G0/0 LAN

¿Cuántas direcciones IP se necesitan para la siguiente subred más grande?
Rta: 2000

¿Cuál es la subred más pequeña que admite esa cantidad de hosts?
Rta: 21 - 255.255.248.0

¿Cuántas direcciones host admite esa subred?
Rta: 2046

¿Se puede volver a dividir la subred restante en subredes sin que deje de admitir esta subred?
Rta: Sí.

¿Cuáles son las dos direcciones de red que se obtendrían de esta división en subredes?
Rta:

- **172.16.240.0/21**
- **172.16.248.0/21**

Utilice la primera dirección de red para esta subred.

Paso 6. determinar la siguiente subred más grande que se necesita.
Descripción de la subred
Rta: BR2 G0/1 LAN

¿Cuántas direcciones IP se necesitan para la siguiente subred más grande?
Rta: 1000

¿Cuál es la subred más pequeña que admite esa cantidad de hosts?
Rta: /22 - 255.255.252.0

¿Cuántas direcciones host admite esa subred?
Rta: 1022

¿Se puede volver a dividir la subred restante en subredes sin que deje de admitir esta subred?
Rta: Sí.

¿Cuáles son las dos direcciones de red que se obtendrían de esta división en subredes?
Rta:

- **172.16.248.0/22**
- **172.16.252.0/22**

Utilice la primera dirección de red para esta subred.

Paso 7. determinar la siguiente subred más grande que se necesita.
Descripción de la subred
Rta: BR2 G0/0 LAN

¿Cuántas direcciones IP se necesitan para la siguiente subred más grande?
Rta: 500

¿Cuál es la subred más pequeña que admite esa cantidad de hosts?
Rta: /23 o 255.255.254.0

¿Cuántas direcciones host admite esa subred?
Rta: 510
¿Se puede volver a dividir la subred restante en subredes sin que deje de admitir esta subred?

Rta: Sí.
¿Cuáles son las dos direcciones de red que se obtendrían de esta división en subredes?
Rta:

- **172.16.252.0/23**
- **172.16.254.0/23**

Utilice la primera dirección de red para esta subred.

Paso 8. determinar las subredes que se necesitan para admitir los enlaces seriales.

¿Cuántas direcciones host se necesitan para cada enlace de subred serial?
Rta: 2

¿Cuál es la subred más pequeña que admite esa cantidad de direcciones host?
Rta: /30 - 255.255.255.252

m. Divida la subred restante en subredes y, a continuación, escriba las direcciones de red que se obtienen de esta división.
Rta:

- **172.16.254.0/24**
- **172.16.255.0/24**

n. Siga dividiendo en subredes la primera subred de cada subred nueva hasta obtener cuatro subredes /30. Escriba las primeras tres direcciones de red de estas subredes /30 a continuación.
Rta:

- **172.16.254.0/30**
- **172.16.254.4/30**
- **172.16.254.8/30**

o. Introduzca las descripciones de las subredes de estas tres subredes a continuación.
Rta:

- **HQ - BR1**
- **HQ - BR2**
- **BR1 - BR2**

Parte 2: diseñar el esquema de direcciones VLSM
Paso 1. calcular la información de subred.

Utilice la información que obtuvo en la parte 1 para completar la siguiente tabla.

Tabla 7. Tabla de Resultados Informe 6.3.3.7

Descripción de la subred	Cantidad de hosts necesarios	Dirección de red/CIDR	Primera dirección de host	Dirección de broadcast
HQ G0/0	16 000	172.16.128.0/18	172.16.128.1	172.16.191.255
HQ G0/1	8 000	172.16.192.0/19	172.16.192.1	172.16.223.255
BR1 G0/1	4 000	172.16.224.0/20	172.16.224.1	172.16.239.255
BR1 G0/0	2 000	172.16.240.0/21	172.16.240.1	172.16.247.255
BR2 G0/1	1.000	172.16.248.0/22	172.16.248.1	172.16.251.255
BR2 G0/0	500	172.16.252.0/23	172.16.252.1	172.16.253.255
HQ S0/0/0-BR1 S0/0/0	2	172.16.254.0/30	172.16.254.1	172.16.254.3
HQ S0/0/1-BR2 S0/0/1	2	172.16.254.4/30	172.16.254.5	172.16.254.7
BR1 S0/0/1-BR2 S0/0/0	2	172.16.254.8/30	172.16.254.9	172.168.254.11

Fuente: Datos del Informe

Paso 2. completar la tabla de direcciones de interfaces de dispositivos.

Asigne la primera dirección host en la subred a las interfaces Ethernet. A HQ se le debería asignar la primera dirección host en los enlaces seriales a BR1 y BR2. A BR1 se le debería asignar la primera dirección host para el enlace serial a BR2.

Tabla 8. Tabla de Direcciones de Interfaces de Dispositivos

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Interfaz del dispositivo
HQ	G0/0	172.16.128.1	255.255.192.0	LAN de 16 000 hosts
	G0/1	172.16.192.1	255.255.224.0	LAN de 8000 hosts
	S0/0/0	172.16.254.1	255.255.255.252	BR1 S0/0/0
	S0/0/1	172.16.254.5	255.255.255.252	BR2 S0/0/1
BR1	G0/0	172.16.240.1	255.255.248.0	LAN de 2000 hosts
	G0/1	172.16.224.1	255.255.240.0	LAN de 4000 hosts
	S0/0/0	172.16.254.2	255.255.255.252	HQ S0/0/0
	S0/0/1	172.16.254.9	255.255.255.252	BR2 S0/0/0

BR2	G0/0	172.16.252.1	255.255.254.0	LAN de 500 hosts
	G0/1	172.16.248.1	255.255.252.0	LAN de 1000 hosts
	S0/0/0	172.16.254.10	255.255.255.252	BR1 S0/0/1
	S0/0/1	172.16.254.6	255.255.255.252	HQ S0/0/1

Parte 3: realizar el cableado y configurar la red IPv4

En la parte 3, realizará el cableado de la topología de la red y configurará los tres routers con el esquema de direcciones VLSM que elaboró en la parte 2.

Paso 3. realizar el cableado de red tal como se muestra en la topología.

Paso 4. configurar los parámetros básicos en cada router.

a. Asigne el nombre de dispositivo al router.
b. Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.
c. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
d. Asigne **cisco** como la contraseña de consola y habilite el inicio de sesión.
e. Asigne **cisco** como la contraseña de vty y habilite el inicio de sesión.
f. Cifre las contraseñas de texto no cifrado.
g. Cree un aviso que advierta a todo aquel que acceda al dispositivo que el acceso no autorizado está prohibido.

Paso 5. configurar las interfaces en cada router.

a. Asigne una dirección IP y una máscara de subred a cada interfaz utilizando la tabla que completó en la parte 2.
b. Configure una descripción de interfaz para cada interfaz.
c. Establezca la frecuencia de reloj en 128000 en todas las interfaces seriales DCE.

HQ(config-if)# **clock rate 128000**

d. Active las interfaces.

Paso 6. guardar la configuración en todos los dispositivos.

Paso 7. Probar la conectividad

a. Haga ping de HQ a la dirección de la interfaz S0/0/0 de BR1.

HQ#ping 172.16.254.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.254.2, timeout is 2 seconds:

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms

HQ#
b. Haga ping de HQ a la dirección de la interfaz S0/0/1 de BR2.
HQ#ping 172.16.254.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.254.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/17 ms

HQ#
c. Haga ping de BR1 a la dirección de la interfaz S0/0/0 de BR2.
BR1#ping 172.16.254.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.254.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/17 ms

BR1#
d. Si los pings no se realizaron correctamente, resuelva los problemas de conectividad.

Nota: los pings a las interfaces GigabitEthernet en otros routers no son correctos. Las LAN definidas para las interfaces GigabitEthernet son simuladas. Debido a que no hay ningún dispositivo conectado a estas LAN, están en estado down/down. Debe haber un protocolo de routing para que otros dispositivos detecten esas subredes. Las interfaces de GigabitEthernet también deben estar en estado up/up para que un protocolo de routing pueda agregar las subredes a la tabla de routing. Estas interfaces permanecen en el estado down/down hasta que se conecta un dispositivo al otro extremo del cable de interfaz Ethernet. Esta práctica de laboratorio se centra en VLSM y en la configuración de interfaces.

6.1.1 REFLEXIÓN

¿Puede pensar en un atajo para calcular las direcciones de red de las subredes /30 consecutivas?
Rta: Recordemos que una red /30 cuanta con 4 IP, la dir. de red, dos IP utilizables y 1 IP de broadcast, entonces debemos contar de 4 en cuatro con lo que se nos facilita nuestro proceso.

Tabla de resumen de interfaces del router

Tabla 9. Tabla de Resumen Interface Router Informe 6.3.3.7

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.				

Fuente: Datos del Informe

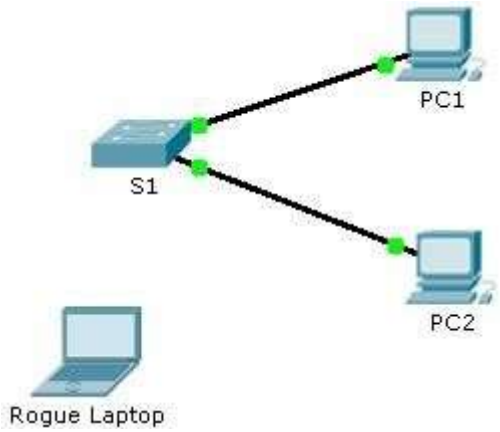
7 INFORME: 6.4.2.5 LAB - CALCULATING SUMMARY ROUTES WITH IPV4 AND IPV6

8

8.1 INFORME: 2.2.4.9 PACKET TRACER - CONFIGURING SWITCH PORT SECURITY

8.1.1 TOPOLOGÍA

Imagen 8. Topología Informe 6.4.2.5



Fuente: Datos del Informe

Addressing Table

Tabla 10. Tabla de Direccionamiento Informe 6.4.2.5

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0
PC2	NIC	10.10.10.11	255.255.255.0
Rogue Laptop	NIC	10.10.10.12	255.255.255.0

Fuente: Datos del Informe

Objective

Part 1: Configure Port Security

Part 2: Verify Port Security

Background

In this activity, you will configure and verify port security on a switch. Port security allows you to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port.

Part 1: Configure Port Security

a. Access the command line for **S1** and enable port security on Fast Ethernet ports 0/1 and 0/2.

S1(config)# **interface range fa0/1 - 2**

S1(config-if-range)# **switchport port-security**

b. Set the maximum so that only one device can access the Fast Ethernet ports 0/1 and 0/2.

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

c. Secure the ports so that the MAC address of a device is dynamically learned and added to the running configuration.

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

d. Set the violation so that the Fast Ethernet ports 0/1 and 0/2 are not disabled when a violation occurs, but packets are dropped from an unknown source.

S1(config-if-range)# **switchport port-security violation restrict**

e. Disable all the remaining unused ports. Hint: Use the **range** keyword to apply this configuration to all the ports simultaneously.

S1(config-if-range)# **interface range f 0/3 - 24 , g 0/1 - 2**

S1(config-if-range)# **shutdown**

Part 2: Verify Port Security

a. From **PC1**, ping **PC2**.

b. Verify port security is enabled and the MAC addresses of **PC1** and **PC2** were added to the running configuration.

c. Attach **Rogue Laptop** to any unused switch port and notice that the link lights are red.

d. Enable the port and verify that **Rogue Laptop** can ping **PC1** and **PC2**. After verification, shut down the port connected to **Rogue Laptop.**

S1(config)# int f 0/12
S1(config-if)#sh

e. Disconnect **PC2** and connect **Rogue Laptop** to **PC2's** port. Verify that **Rogue Laptop** is unable to ping
PC1.

f. Display the port security violations for the port **Rogue Laptop** is connected to.

S1# show port-security interface fa0/2

g. Disconnect **Rouge Laptop** and reconnect **PC2**. Verify **PC2** can ping **PC1**.

h. Why is **PC2** able to ping **PC1**, but the **Rouge Laptop** is not? The port security that was enabled on the port only allowed the device, whose MAC was learned first, access to the port while preventing all other devices access.

9 INFORME: 3.2.1.7 PACKET TRACER - CONFIGURING VLANS

Addressing Table

Tabla 11. Tabla de Direccionamiento Informe 3.2.1.7

Device	Interface	IP Address	Subnet Mask	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	10
PC2	NIC	172.17.20.22	255.255.255.0	20
PC3	NIC	172.17.30.23	255.255.255.0	30
PC4	NIC	172.17.10.24	255.255.255.0	10
PC5	NIC	172.17.20.25	255.255.255.0	20
PC6	NIC	172.17.30.26	255.255.255.0	30

Fuente: Datos del Informe

Objectives

Part 1: Verify the Default VLAN Configuration
Part 2: Configure VLANs
Part 3: Assign VLANs to Ports
Background

VLANs are helpful in the administration of logical groups, allowing members of a group to be easily moved, changed, or added. This activity focuses on creating and naming VLANs, and assigning access ports to specific VLANs.

Part 1: View the Default VLAN Configuration
Step 1: Display the current VLANs.

On S1, issue the command that displays all VLANs configured. By default, all interfaces are assigned to VLAN 1.

Comando: show vlan brief

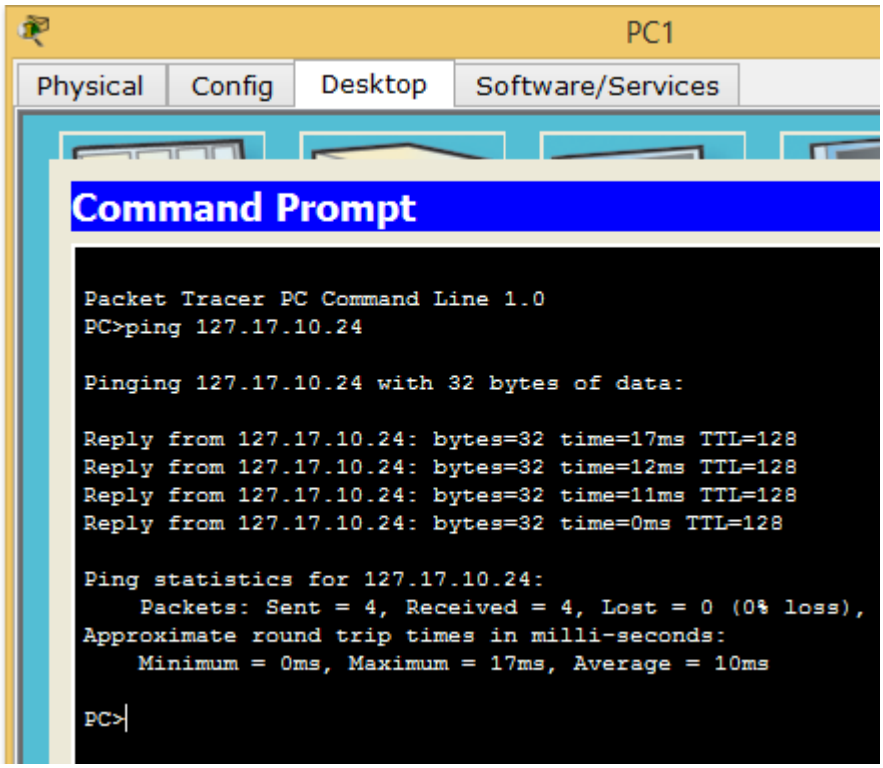
```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S1#
```

Copy Pas

Step 2: Verify connectivity between PCs on the same network.

Notice that each PC can ping the other PC that shares the same network.

- **PC1 can ping PC4**
- **PC2 can ping PC5**
- **PC3 can ping PC6**



```
Pinging 172.17.20.25 with 32 bytes of data:

Reply from 172.17.20.25: bytes=32 time=57ms TTL=128
Reply from 172.17.20.25: bytes=32 time=12ms TTL=128
Reply from 172.17.20.25: bytes=32 time=3ms TTL=128
Reply from 172.17.20.25: bytes=32 time=0ms TTL=128

Ping statistics for 172.17.20.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 57ms, Average = 18ms

PC>
```

```
Reply from 172.17.30.26: bytes=32 time=25ms TTL=128
Reply from 172.17.30.26: bytes=32 time=11ms TTL=128
Reply from 172.17.30.26: bytes=32 time=11ms TTL=128
Reply from 172.17.30.26: bytes=32 time=12ms TTL=128

Ping statistics for 172.17.30.26:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 25ms, Average = 14ms

PC>
```

Pings to PCs in other networks fail.

```
PC>ping 172.17.10.24

Pinging 172.17.10.24 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.17.10.24:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 172.17.10.225

Pinging 172.17.10.225 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.17.10.225:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

What benefit will configuring VLANs provide to the current configuration?
Rta: tiene múltiples aplicaciones y beneficios:

- **Seguridad: separa la red del tráfico normal**
- **Reducción de costos: no hay necesidad de implementar redes caras, uso más eficiente de los enlaces**
- **Mejor rendimiento: reduce el tráfico innecesario de la red y potencia el rendimiento de la red**
- **Mitigación del broadcast**

Part 2: Configure VLANs
Step 1: Create and name VLANs on S1.

Create the following VLANs. Names are case-sensitive:

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

```
S1>
S1>ena
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 10
S1(config-vlan)#name Faculty/Staff
S1(config-vlan)#vlan 20
S1(config-vlan)#name Students
S1(config-vlan)#vlan 30
S1(config-vlan)#name Guest(Default)
S1(config-vlan)#vlan 99
S1(config-vlan)#name Management&Native
S1(config-vlan)#
```

Step 2: Verify the VLAN configuration.
Which command will only display the VLAN name, status, and associated ports on a switch?

```
S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   Faculty/Staff                    active
20   Students                         active
30   Guest(Default)                   active
99   Management&Native                active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S1#
```

Copy Pa

Step 3: Create the VLANs on S2 and S3.

Using the same commands from Step 1, create and name the same VLANs on S2 and S3.

```
S2>
S2>ena
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#vlan 10
S2(config-vlan)#name Faculty/Staff
S2(config-vlan)#vlan 20
S2(config-vlan)#name Students
S2(config-vlan)#Vlan 30
S2(config-vlan)#name Guest(Default)
S2(config-vlan)#vlan 99
S2(config-vlan)#name Management&Native
S2(config-vlan)#exit
S2(config)#
```

```
S3>ena
S3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#vlan 10
S3(config-vlan)#name Faculty/Staff
S3(config-vlan)#vlan 20
S3(config-vlan)#name Students
S3(config-vlan)#vlan 30
S3(config-vlan)#name Guest(Default)
S3(config-vlan)#vlan 99
S3(config-vlan)#name Management&Native
S3(config-vlan)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

Step 4: Verify the VLAN configuration.

```
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
10   Faculty/Staff                     active
20   Students                          active
30   Guest(Default)                    active
99   Management&Native                 active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S3#
```

Copy Pas

Part 3: Assign VLANs to Ports

Step 1: Assign VLANs to the active ports on S2.

Assign the VLANs to the following ports:

- **VLAN 10: Fast Ethernet 0/11**
- **VLAN 20: Fast Ethernet 0/18**
- **VLAN 30: Fast Ethernet 0/6**

```
S2(config-if)#sw
S2(config-if)#switchport mode acc
S2(config-if)#switchport acc
S2(config-if)#switchport access vlan 10
S2(config-if)#int fa0/18
S2(config-if)#switchport access vlan 20
S2(config-if)#int fa0/6
S2(config-if)#switchport access vlan 30
S2(config-if)#end
S2#
```

Step 2: Assign VLANs to the active ports on S3.

S3 uses the same VLAN access port assignments as S2.

```
                                                   Fa0/24, Gigi
10   Faculty/Staff                 active    Fa0/11
20   Students                      active    Fa0/18
30   Guest(Default)                active    Fa0/6
99   Management&Native             active
```

Step 3: Verify loss of connectivity.

Previously, PCs that shared the same network could ping each other successfully. Try pinging between PC1 and PC4. Although the access ports are assigned to the appropriate VLANs, were the pings successful? Why?

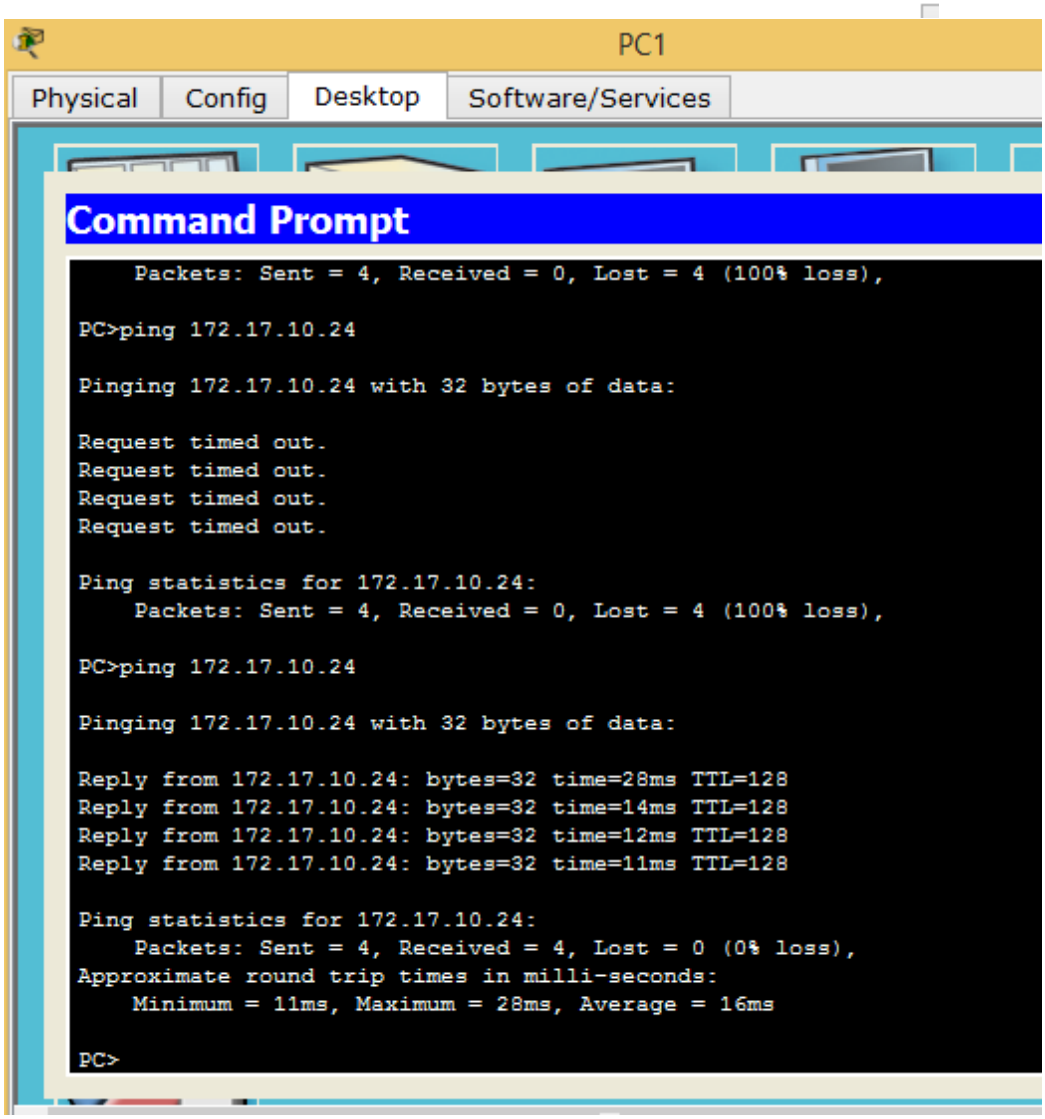
```
PC>ping 172.17.10.24

Pinging 172.17.10.24 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.17.10.24:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

What could be done to resolve this issue?

Rta: Tenemos que configurar los enlaces GigaE, de los switch como troncales:

```
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int g0/1
S2(config-if)#swi
S2(config-if)#switchport mode t
S2(config-if)#switchport mode trunk
```

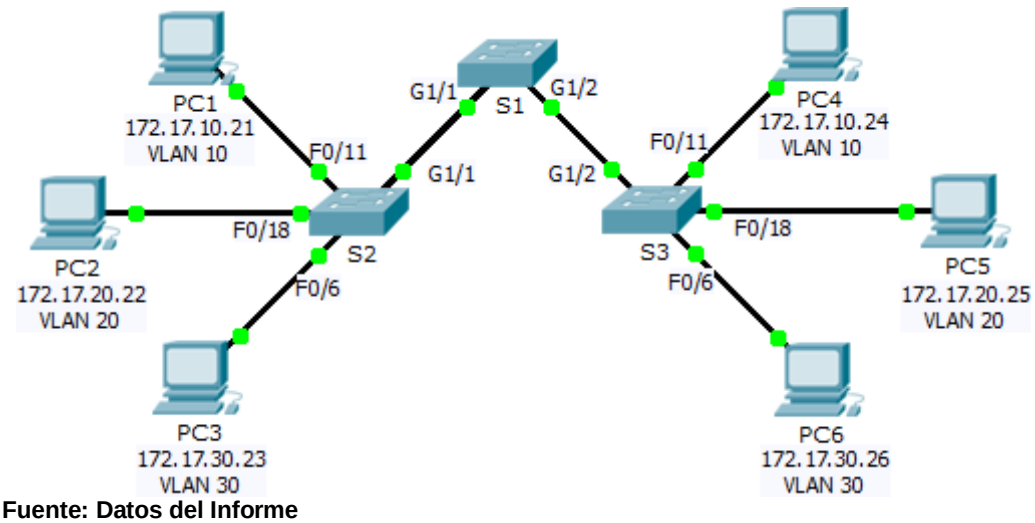
```
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#int g0/1
S3(config-if)#sw
S3(config-if)#switchport mode t
S3(config-if)#switchport mode trunk
S3(config-if)#
S3(config-if)#
```



10 INFORME: 3.2.2.4 PACKET TRACER - CONFIGURING TRUNKS

10.1 TOPOLOGY

Imagen 9. Topología Informe 3.2.2.4



Fuente: Datos del Informe

Addressing table

Tabla 12. Tabla de Direccionamiento Informe 3.2.2.4

Device	Interface	IPAddress	Subnet Mask	Switch Port	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	S2 F0/11	10
PC2	NIC	172.17.20.22	255.255.255.0	S2 F0/18	20
PC3	NIC	172.17.30.23	255.255.255.0	S2 F0/6	30
PC4	NIC	172.17.10.24	255.255.255.0	S3 F0/11	10
PC5	NIC	172.17.20.25	255.255.255.0	S3 F0/18	20
PC6	NIC	172.17.30.26	255.255.255.0	S3 F0/16	30

Fuente: Datos del Informe

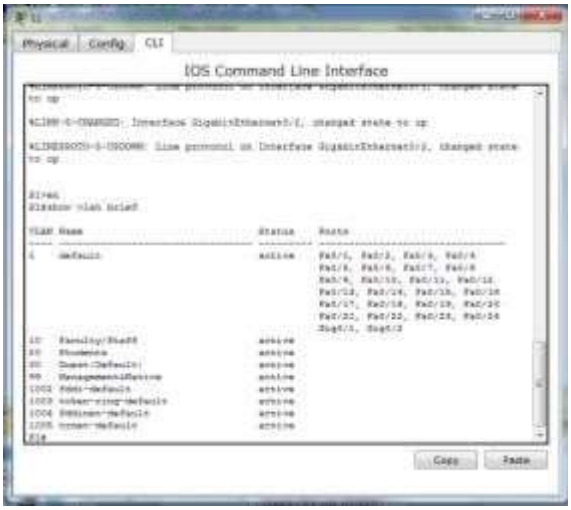
Background

Trunks are required to pass VLAN information between switches. A port on a switch is either an access port or a trunk port. Access ports carry traffic from a specific VLAN assigned to the port. A trunk port by default is a member of all VLANs; therefore, it carries traffic for all VLANs. This activity focuses on creating trunk ports, and assigning them to a native VLAN other than the default

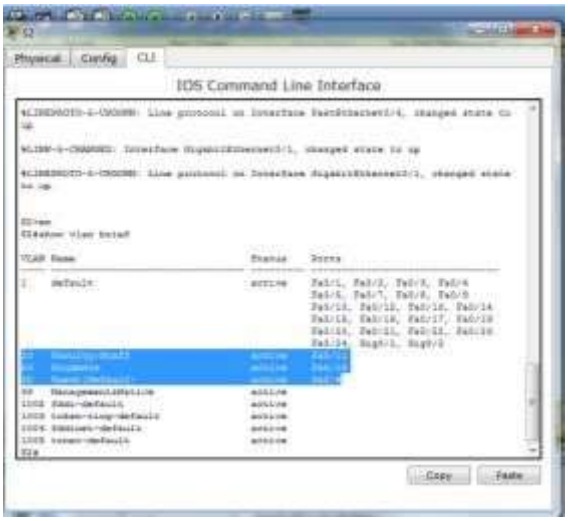
Part 1: Verify VLANs

Step 1: Display the current VLANs.

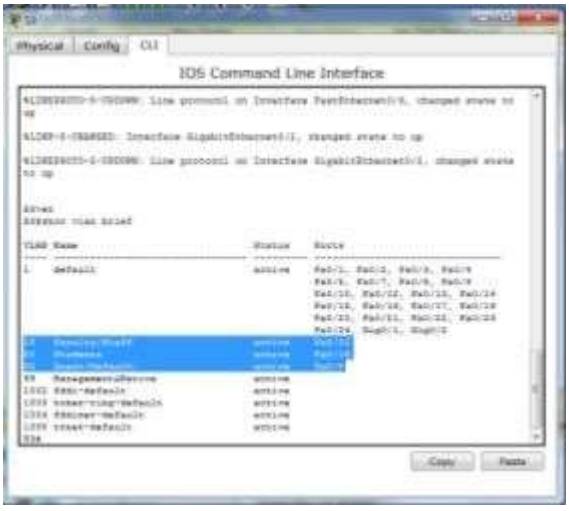
a. On **S1**, issue the command that will display all VLANs configured. There should be 9 VLANs in total.
Notice how all 26 ports on the switch are assigned to one port or another.



b. On **S2** and **S3**, display and verify all the VLANs are configure and assigned to the correct switchports according to the **Addressing Table**.



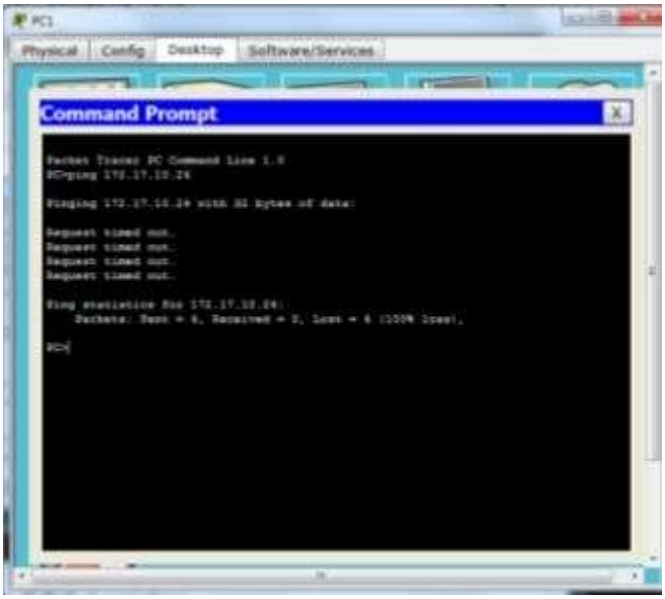
S2 **VLAN**



S3 **VLAN**

Step 2: Verify loss of connectivity between PCs on the same network.

Although **PC1** and **PC4** are on the same network, they cannot ping one another. This is because the ports connecting the switches are assigned to VLAN 1 by default. In order to provide connectivity between the PCs on the same network and VLAN, trunks must be configured.



PC1-PC4 ping is

Part 2: Configure Trunks

Step 1: Configure trunking on S1 and use VLAN 99 as the native VLAN.

a. Configure G1/1 and G1/2 interfaces on S1 for trunking.
S1(config)# **interface range g1/1 - 2**
S1(config-if)# **switchport mode trunk**

b. Configure VLAN 99 as the native VLAN for G1/1 and G1/2 interfaces on **S1**.

S1(config-if)# **switchport trunk native vlan 99**

The trunk port takes about a minute to become active due to Spanning Tree which you will learn in the proceeding chapters. Click **Fast Forward Time** to speed the process. After the ports become active, you will periodically receive the following syslog messages:
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet1/2
(99), with S3 GigabitEthernet1/2 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet1/1
(99), with S2 GigabitEthernet1/1 (1).

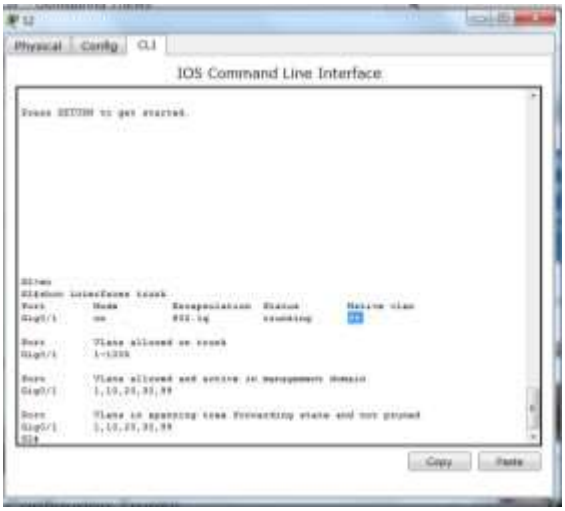
You configured VLAN 99 as the native VLAN on S1. However, the S2 and S3 are using VLAN 1 as the default native VLAN as indicated by the syslog message.

Although you have a native VLAN mismatch, pings between PCs on the same VLAN are now successful. Why?
Pings are successful because trunking has been enabled on S1. Dynamic Trunking Protocol (DTP) has automatically negotiated the other side of the trunk links. In this case, S2 and S3 have now automatically configured the ports attached to S1 as trunking ports.

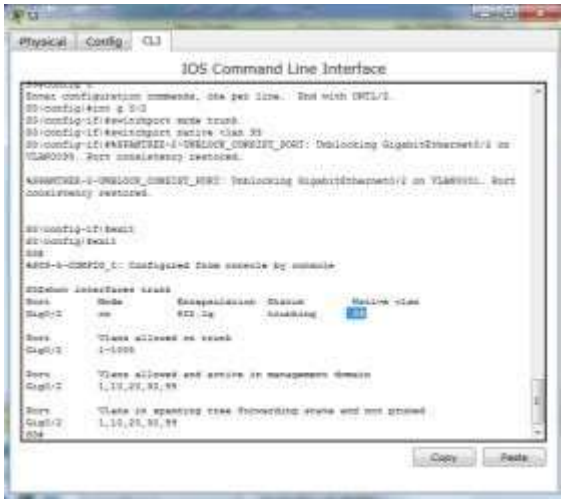
Step 2: Verify trunking is enabled on S2 and S3.

On **S2** and **S3**, issue the **show interface trunk** command to confirm that DTP has successfully negotiated trunking with S1 on S2 and S3. The output also displays information about the trunk interfaces on S2 and S3.
Which active VLANs are allowed to across the trunk?
1,10, 20, 30, and 99.

Step 3: Correct the native VLAN mismatch on S2 and S3.
a. Configure VLAN 99 as the native VLAN for the appropriate interfaces on S2 and S3.
b. Issue **show interface trunk** command to verify the correct native VLAN configuration



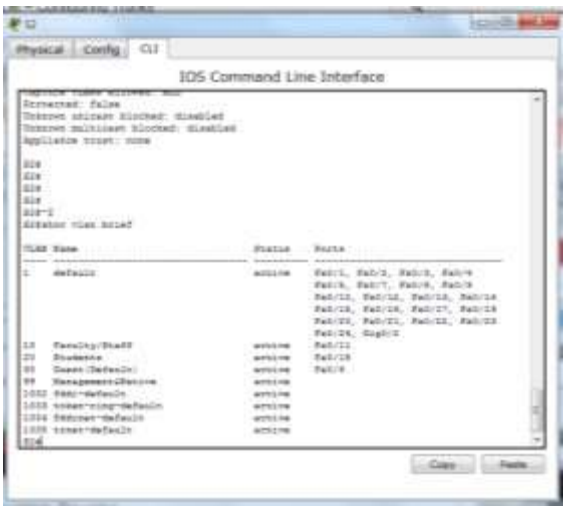
VLAN 99 as native VLAN in

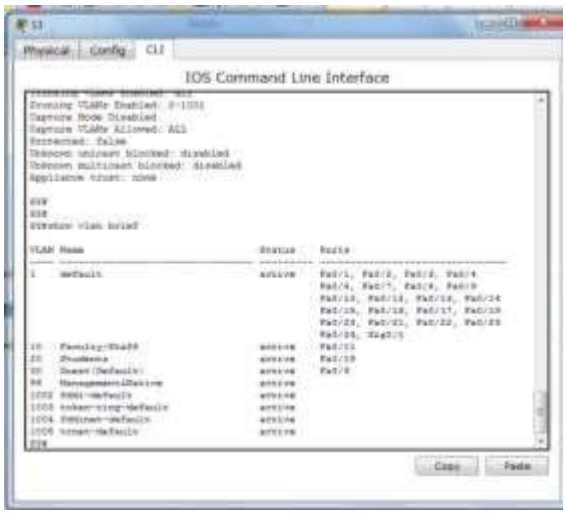


VLAN 99 as native VLAN in

Step 4: Verify configurations on S2 and S3.

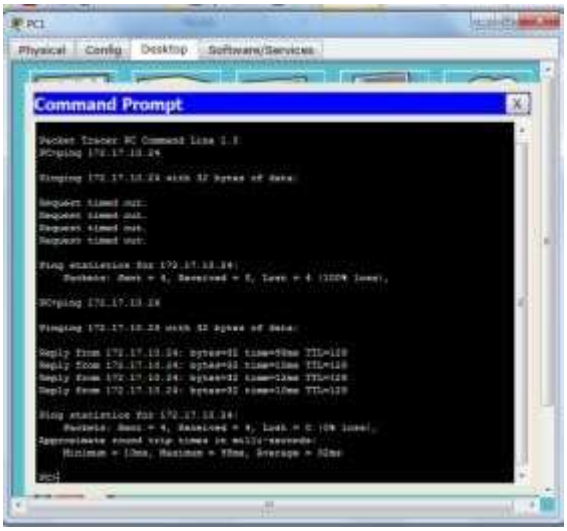
a. Issue the **show interface** *interface* **switchport** command to verify that the native VLAN is now 99.
b. Use the **show vlan** command to display information regarding configured VLANs. Why port G1/1 on S2 is no longer assigned to VLAN 1?
Port G1/1 is a trunk port and trunks ports are not displayed.





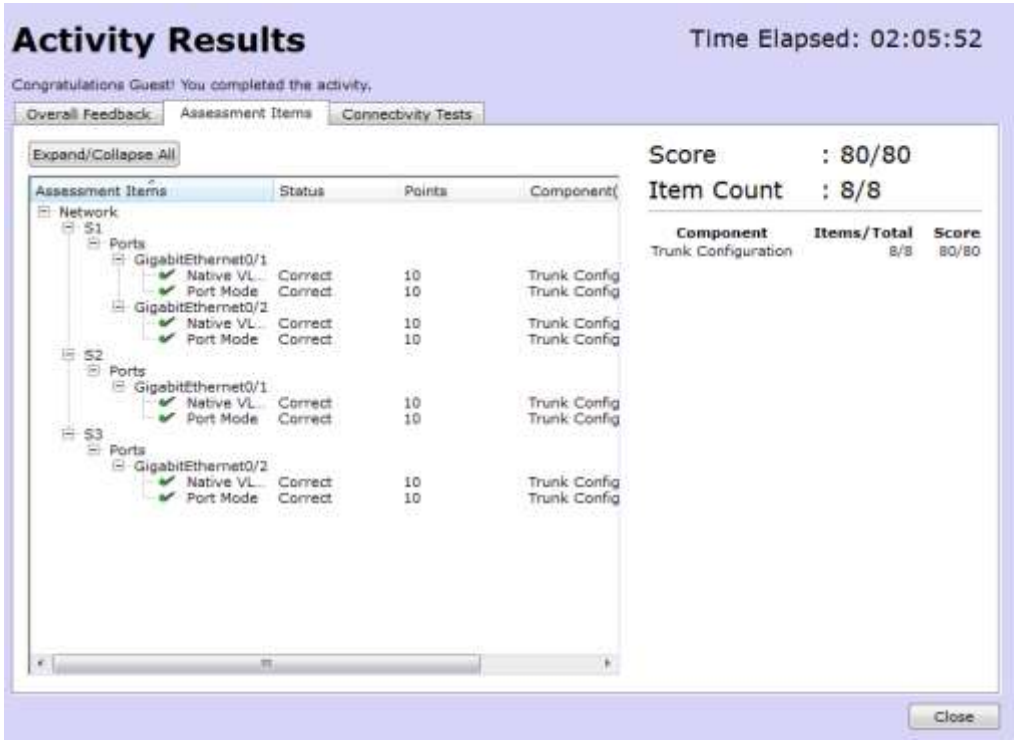
Trunk ports are not displayed in S2

PC1- PC4 ping



PC1-PC4 ping now is successful

RESULTADO FINAL

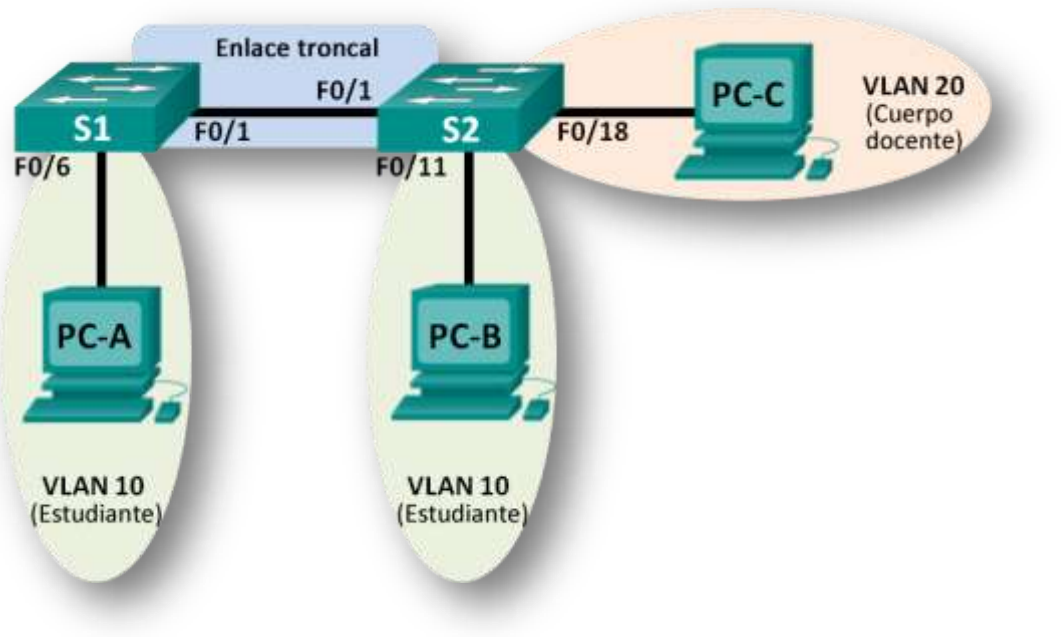


11 INFORME: 3.2.2.5 LAB - CONFIGURING VLANS AND TRUNKING

11.1 PRÁCTICA DE LABORATORIO: CONFIGURACIÓN DE REDES VLAN Y ENLACES TRONCALES

11.1.1 TOPOLOGÍA

Imagen 10. Topología Informe 3.2.2.5



Fuente: Datos del Informe

Tabla de direccionamiento

Tabla 13. Tabla de Direccionamiento Informe 3.2.2.5

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.4	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Fuente: Datos del Informe

Objetivos

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
Parte 2: crear redes VLAN y asignar puertos de switch
Parte 3: mantener las asignaciones de puertos de VLAN y la base de datos de VLAN
Parte 4: configurar un enlace troncal 802.1Q entre los switches

Parte 5: eliminar la base de datos de VLAN
Información básica/situación
Los switches modernos usan redes de área local virtuales (VLAN) para mejorar el rendimiento de la red mediante la división de grandes dominios de difusión de capa 2 en otros más pequeños. Las VLAN también se pueden usar como medida de seguridad al controlar qué hosts se pueden comunicar. Por lo general, las redes VLAN facilitan el diseño de una red para respaldar los objetivos de una organización.

Los enlaces troncales de VLAN se usan para abarcar redes VLAN a través de varios dispositivos. Los enlaces troncales permiten transferir el tráfico de varias VLAN a través de un único enlace y conservar intactas la segmentación y la identificación de VLAN.

En esta práctica de laboratorio, creará redes VLAN en los dos switches de la topología, asignará las VLAN a los puertos de acceso de los switches, verificará que las VLAN funcionen como se espera y, a continuación, creará un enlace troncal de VLAN entre los dos switches para permitir que los hosts en la misma VLAN se comuniquen a través del enlace troncal, independientemente del switch al que está conectado el host.

Nota: los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio.

Nota: asegúrese de que los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología

Parte 7. armar la red y configurar los parámetros básicos de los dispositivos
En la parte 1, establecerá la topología de la red y configurará los parámetros básicos en los equipos host y los switches.

Paso 1. realizar el cableado de red tal como se muestra en la topología.
Conecte los dispositivos tal como se muestra en el diagrama de la topología y realice el cableado según sea necesario.

Paso 2. inicializar y volver a cargar los switches según sea necesario.
Paso 3. configurar los parámetros básicos para cada switch.

a. Desactive la búsqueda del DNS.
b. Configure el nombre del dispositivo como se muestra en la topología.
c. Asigne **class** como la contraseña del modo EXEC privilegiado.
d. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión para las líneas de vty y de consola.
e. Configure **logging synchronous** para la línea de consola.
f. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.
g. Configure la dirección IP que se indica en la tabla de direccionamiento para la VLAN 1 en ambos switches.
h. Desactive administrativamente todos los puertos que no se usen en el switch.
i. Copie la configuración en ejecución en la configuración de inicio

Paso 4. configurar los equipos host.
Consulte la tabla de direccionamiento para obtener información de direcciones de los equipos host.

Paso 5. Probar la conectividad.
Verifique que los equipos host puedan hacer ping entre sí.

Nota: puede ser necesario desactivar el firewall de las computadoras para hacer ping entre ellas.

¿Se puede hacer ping de la PC-A a la PC-B?
Rta: SI

¿Se puede hacer ping de la PC-A a la PC-C?
Rta: NO

¿Se puede hacer ping de la PC-A al S1?
Rta: NO

¿Se puede hacer ping de la PC-B a la PC-C?
Rta: NO

¿Se puede hacer ping de la PC-B al S2?
Rta: NO

¿Se puede hacer ping de la PC-C al S2?
Rta: NO

¿Se puede hacer ping del S1 al S2?
Rta: SI

Si la respuesta a cualquiera de las preguntas anteriores es no, ¿por qué fallaron los pings?
Rta: La red cuenta con una serie de subredes conectadas pero las cuales no se han configurado las rutas que permitan el intercambio entre las mismas.

Parte 8. crear redes VLAN y asignar puertos de switch
En la parte 2, creará redes VLAN para los estudiantes, el cuerpo docente y la administración en ambos switches. A continuación, asignará las VLAN a la interfaz correspondiente. El comando **show vlan** se usa para verificar las opciones de configuración.

Paso 1. crear las VLAN en los switches.
a. Cree las VLAN en S1.
S1(config)# **vlan 10**
S1(config-vlan)# **name Student**
S1(config-vlan)# **vlan 20**
S1(config-vlan)# **name Faculty**
S1(config-vlan)# **vlan 99**
S1(config-vlan)# **name Management**
S1(config-vlan)# **end**

b. Cree las mismas VLAN en el S2.
S2(config)#
S2(config)#vlan 10
S2(config-vlan)#name student
S2(config-vlan)#vlan 20
S2(config-vlan)#name faculty
S2(config-vlan)#vlan 99
S2(config-vlan)#name management
S2(config-vlan)#end
S2#

c. Emita el comando **show vlan** para ver la lista de VLAN en el S1.
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
                                  Gi0/1, Gi0/2
10   Student                      active
20   Faculty                      active
99   Management                   active
1002 fddi-default                 act/unsup
1003 token-ring-default           act/unsup
1004 fddinet-default              act/unsup
1005 trnet-default                act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1
Trans2
---------- ---------- ----- ------ ------ -------- ---- -------- ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
99   enet  100099     1500  -      -      -        -    -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1
Trans2
---------- ---------- ----- ------ ------ -------- ---- -------- ------
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

¿Cuál es la VLAN predeterminada?
Rta: La VLAN default es la VLAN1

¿Qué puertos se asignan a la VLAN predeterminada?
Rta: Todos los puertos o interfaces del router son asignados automáticamente a la VLAN default.

Paso 2. asignar las VLAN a las interfaces del switch correctas.

a. Asigne las VLAN a las interfaces en el S1.

1) Asigne la PC-A a la VLAN Estudiantes.

S1(config)# **interface f0/6**
S1(config-if)# **switchport mode access**
S1(config-if)# **switchport access vlan 10**

```
S1(config)#interface f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
S1(config-if)#
```

2) Transfiera la dirección IP del switch a la VLAN 99.

S1(config)# **interface vlan 1**
S1(config-if)# **no ip address**
S1(config-if)# **interface vlan 99**
S1(config-if)# **ip address 192.168.1.11 255.255.255.0**
S1(config-if)# **end**

```
S1(config)#interface vlan 1
S1(config-if)#no ip address
S1(config-if)#interface vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#ip addres 192.168.1.11 255.255.255.0
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
```

b. Emita el comando **show vlan brief** y verifique que las VLAN se hayan asignado a las interfaces correctas.

S1# **show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, 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	Student	active	Fa0/6
20	Faculty	active	
99	Management	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	

1004 fddinet-default act/unsup
1005 trnet-default act/unsup

c. Emita el comando **show ip interface brief**.

- **S1#show ip interface brief**
- **Interface IP-Address OK? Method Status Protocol**

- **FastEthernet0/1 unassigned YES manual up up**
- **FastEthernet0/2 unassigned YES manual administratively down down**
- **FastEthernet0/6 unassigned YES manual up up**
- **GigabitEthernet1/1 unassigned YES manual administratively down down**
- **GigabitEthernet1/2 unassigned YES manual administratively down down**
- **Vlan1 unassigned YES manual up up**
- **Vlan99 192.168.1.11 YES manual up down**
- **S1#**

¿Cuál es el estado de la VLAN 99? ¿Por qué?

Rta: La VLAN está UP/DOWN, el motivo es porque no le hemos asignado puertos activos.

d. Use la topología para asignar las VLAN a los puertos correspondientes en el S2.
e. Elimine la dirección IP para la VLAN 1 en el S2.
f. Configure una dirección IP para la VLAN 99 en el S2 según la tabla de direccionamiento.
g. Use el comando **show vlan brief** para verificar que las VLAN se hayan asignado a las interfaces correctas.
S2# **show vlan brief**

VLAN Name Status Ports
---- -------------------------------- --------- -------------------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/12, Fa0/13
Fa0/14, Fa0/15, Fa0/16, Fa0/17
Fa0/19, Fa0/20, Fa0/21, Fa0/22
Fa0/23, Fa0/24, Gi0/1, Gi0/2
10 Student active Fa0/11
20 Faculty active Fa0/18
99 Management active

1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup

```
S2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig1/1, Gig1/2
10   student                          active    Fa0/11
20   faculty                          active    Fa0/18
99   management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S2#
```

¿Es posible hacer ping de la PC-A a la PC-B? ¿Por qué?
Rta: No.ya que el enlace aún no ha sido bien configurado.

¿Es posible hacer ping del S1 al S2? ¿Por qué?
Rta: No. Las interfaces están asociadas a la VLAN 99, por lo tanto el tráfico no es enviado a través de la interfaz F0/1.

Parte 9. mantener las asignaciones de puertos de VLAN y la base de datos de VLAN
En la parte 3, cambiará las asignaciones de VLAN a los puertos y eliminará las VLAN de la base de datos de VLAN.

Paso 1. asignar una VLAN a varias interfaces.

a. En el S1, asigne las interfaces F0/11 a 24 a la VLAN 10.
S1(config)# **interface range f0/11-24**
S1(config-if-range)# **switchport mode access**
S1(config-if-range)# **switchport access vlan 10**
S1(config-if-range)# **end**

```
S1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface range f0/11-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 10
S1(config-if-range)#end
S1#
```

b. Emita el comando **show vlan brief** para verificar las asignaciones de VLAN.

- **S1#show vlan brief**
- **VLAN Name Status Ports**
- **1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4**
- **Fa0/5, Fa0/7, Fa0/8, Fa0/9**
- **Fa0/10, Gig1/1, Gig1/2**
- **10 student active Fa0/6, 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**
- **20 faculty active**
- **99 management active**
- **1002 fddi-default active**
- **1003 token-ring-default active**
- **1004 fddinet-default active**
- **1005 trnet-default active**
- **S1#**

c. Reasigne F0/11 y F0/21 a la VLAN 20.

```
S1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface range f0/11, f0/21
S1(config-if-range)#switchport access vlan 20
S1(config-if-range)#end
S1#
```

d. Verifique que las asignaciones de VLAN sean las correctas.

- **S1#show vlan brief**
- **VLAN Name Status Ports**
- **---- -------------------------------- --------- -------------------------------**
- **1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4**
- **Fa0/5, Fa0/7, Fa0/8, Fa0/9**
- **Fa0/10, Gig1/1, Gig1/2**
- **10 student active Fa0/6, Fa0/12, Fa0/13, Fa0/14**
- **Fa0/15, Fa0/16, Fa0/17, Fa0/18**
- **Fa0/19, Fa0/20, Fa0/22, Fa0/23**
- **Fa0/24**
- **20 faculty active Fa0/11, Fa0/21**
- **99 management active**
- **1002 fddi-default active**
- **1003 token-ring-default active**

- **1004 fddinet-default active**
- **1005 trnet-default active**
- **S1#**

Paso 2. eliminar una asignación de VLAN de una interfaz.

a. Use el comando **no switchport access vlan** para eliminar la asignación de la VLAN 10 a F0/24.

S1(config)# **interface f0/24**
S1(config-if)# **no switchport access vlan**
S1(config-if)# **end**

```
S1(config)#interface f0/24
S1(config-if)#no switchport access vlan
S1(config-if)#end
S1#
```

b. Verifique que se haya realizado el cambio de VLAN.

- **S1#show vlan brief**
- **VLAN Name Status Ports**
- **---- -------------------------------- --------- -------------------------------**
- **1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4**
- **Fa0/5, Fa0/7, Fa0/8, Fa0/9**
- **Fa0/10, Fa0/24, Gig1/1, Gig1/2**
- **10 student active Fa0/6, Fa0/12, Fa0/13, Fa0/14**
- **Fa0/15, Fa0/16, Fa0/17, Fa0/18**
- **Fa0/19, Fa0/20, Fa0/22, Fa0/23**
- **20 faculty active Fa0/11, Fa0/21**
- **99 management active**
- **1002 fddi-default active**
- **1003 token-ring-default active**
- **1004 fddinet-default active**
- **1005 trnet-default active**
- **S1#**

¿A qué VLAN está asociada ahora F0/24?

- **Como fue liberada la anterior asociación a la VLAN30 que automáticamente asociada a la VLAN1.**

Paso 3. eliminar una ID de VLAN de la base de datos de VLAN.

a. Agregue la VLAN 30 a la interfaz F0/24 sin emitir el comando VLAN.

S1(config)# **interface f0/24**
S1(config-if)# **switchport access vlan 30**
% Access VLAN does not exist. Creating vlan 30

```
S1(config)#interface f0/24
S1(config-if)#switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
S1(config-if)#
```

Nota: la tecnología de switches actual ya no requiere la emisión del comando **vlan** para agregar una VLAN a la base de datos. Al asignar una VLAN desconocida a un puerto, la VLAN se agrega a la base de datos de VLAN.

b. Verifique que la nueva VLAN se muestre en la tabla de VLAN.
S1# **show vlan brief**

VLAN Name Status Ports
---- --------------------------------- --------- -------------------------------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Gi0/1, Gi0/2
10 Student active Fa0/12, Fa0/13, Fa0/14, Fa0/15
Fa0/16, Fa0/17, Fa0/18, Fa0/19
Fa0/20, Fa0/22, Fa0/23
20 Faculty active Fa0/11, Fa0/21
30 VLAN0030 active Fa0/24
99 Management active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup

```
S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Gig1/1, Gig1/2
10   student                          active    Fa0/6, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/22, Fa0/23
20   faculty                          active    Fa0/11, Fa0/21
30   VLAN0030                         active    Fa0/24
99   management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S1#
```

¿Cuál es el nombre predeterminado de la VLAN 30?
Rta: Como esta VLAN fue creada automáticamente fue creada con el nombre: VLAN0030

c. Use el comando **no vlan 30** para eliminar la VLAN 30 de la base de datos de VLAN.

S1(config)# **no vlan 30**

S1(config)# **end**

```
S1(config)#
S1(config)#no vlan 30
S1(config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

d. Emita el comando **show vlan brief**. F0/24 se asignó a la VLAN 30.

- **S1#show vlan brief**
- **VLAN Name Status Ports**
- **---- -------------------------------- --------- -------------------------------**
- **1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4**
- **Fa0/5, Fa0/7, Fa0/8, Fa0/9**
- **Fa0/10, Gig1/1, Gig1/2**
- **10 student active Fa0/6, Fa0/12, Fa0/13, Fa0/14**
- **Fa0/15, Fa0/16, Fa0/17, Fa0/18**
- **Fa0/19, Fa0/20, Fa0/22, Fa0/23**
- **20 faculty active Fa0/11, Fa0/21**
- **99 management active**
- **1002 fddi-default active**
- **1003 token-ring-default active**
- **1004 fddinet-default active**
- **1005 trnet-default active**
- **S1#**

Una vez que se elimina la VLAN 30, ¿a qué VLAN se asigna el puerto F0/24? ¿Qué sucede con el tráfico destinado al host conectado a F0/24?

Rta: Este puerto F0/24 no se asigna a ninguna VLAN, este debe ser asignado de manera manual.

S1# **show vlan brief**

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Gi0/1, Gi0/2
10   Student                           active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/22, Fa0/23
```

20 Faculty active Fa0/11, Fa0/21
99 Management active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup

e. Emita el comando **no switchport access vlan** en la interfaz F0/24.

- **S1(config)#interface f0/24**
- **S1(config-if)#no switchport access vlan**
- **S1(config-if)#end**
- **S1#**

f. Emita el comando **show vlan brief** para determinar la asignación de VLAN para F0/24. ¿A qué VLAN se asignó F0/24?

- **VLAN1.**
- **S1#show vlan brief**
- **VLAN Name Status Ports**
- **---- --------------------------------- --------- -------------------------------**
- **1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4**
- **Fa0/5, Fa0/7, Fa0/8, Fa0/9**
- **Fa0/10, Fa0/24, Gig1/1, Gig1/2**
- **10 student active Fa0/6, Fa0/12, Fa0/13, Fa0/14**
- **Fa0/15, Fa0/16, Fa0/17, Fa0/18**
- **Fa0/19, Fa0/20, Fa0/22, Fa0/23**
- **20 faculty active Fa0/11, Fa0/21**
- **99 management active**
- **1002 fddi-default active**
- **1003 token-ring-default active**
- **1004 fddinet-default active**
- **1005 trnet-default active**
- **S1#**

Nota: antes de eliminar una VLAN de la base de datos, se recomienda reasignar todos los puertos asignados a esa VLAN.
¿Por qué debe reasignar un puerto a otra VLAN antes de eliminar la VLAN de la base de datos de VLAN?
Rta: Estas interfaces no están disponibles hasta que sean asignadas a otra VLAN.

Parte 10. configurar un enlace troncal 802.1Q entre los switches

En la parte 4, configurará la interfaz F0/1 para que use el protocolo de enlace troncal dinámico (DTP) y permitir que negocie el modo de enlace troncal. Después de lograr y verificar esto, desactivará DTP en la interfaz F0/1 y la configurará manualmente como enlace troncal.

Paso 1. usar DTP para iniciar el enlace troncal en F0/1.

El modo de DTP predeterminado de un puerto en un switch 2960 es dinámico automático. Esto permite que la interfaz convierta el enlace en un enlace troncal si la interfaz vecina se establece en modo de enlace troncal o dinámico deseado.

a. Establezca F0/1 en el S1 en modo de enlace troncal.

S1(config)# **interface f0/1**
S1(config-if)# **switchport mode dynamic desirable**
*Mar 1 05:07:28.746: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
*Mar 1 05:07:29.744: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
S1(config-if)#
*Mar 1 05:07:32.772: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
S1(config-if)#
*Mar 1 05:08:01.789: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
*Mar 1 05:08:01.797: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

También debe recibir mensajes del estado del enlace en el S2.
S2#
*Mar 1 05:07:29.794: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
S2#
*Mar 1 05:07:32.823: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
S2#
*Mar 1 05:08:01.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
*Mar 1 05:08:01.850: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

b. Emita el comando **show vlan brief** en el S1 y el S2. La interfaz F0/1 ya no está asignada a la VLAN 1. Las interfaces de enlace troncal no se incluyen en la tabla de VLAN.

S1# **show vlan brief**

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/24, Gi0/1, Gi0/2
10   Student                           active    Fa0/6, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/22, Fa0/23
20   Faculty                           active    Fa0/11, Fa0/21
99   Management                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

c. Emita el comando **show interfaces trunk** para ver las interfaces de enlace troncal. Observe que el modo en el S1 está establecido en deseado, y el modo en el S2 en automático.

S1# **show interfaces trunk**

```
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       desirable    802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
```

S2# **show interfaces trunk**

```
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       auto         802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99
```

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,20,99
Nota: de manera predeterminada, todas las VLAN se permiten en un enlace troncal. El comando **switchport trunk** le permite controlar qué VLAN tienen acceso al enlace troncal. Para esta práctica de laboratorio, mantenga la configuración predeterminada que permite que todas las VLAN atraviesen F0/1.

d. Verifique que el tráfico de VLAN se transfiera a través de la interfaz de enlace troncal F0/1.
¿Se puede hacer ping del S1 al S2?
Rta: SI

¿Se puede hacer ping de la PC-A a la PC-B?
Rta: SI

¿Se puede hacer ping de la PC-A a la PC-C?
Rta: NO

¿Se puede hacer ping de la PC-B a la PC-C?
Rta: NO

¿Se puede hacer ping de la PC-A al S1?
Rta: NO

¿Se puede hacer ping de la PC-B al S2?
Rta: NO

¿Se puede hacer ping de la PC-C al S2?
Rta: NO

Si la respuesta a cualquiera de las preguntas anteriores es no, justifíquela a continuación.
Rta: Las redes están en VLAN diferentes, por lo tanto no hya caminos o rutas que permitan la comunicación.

Paso 2. configurar manualmente la interfaz de enlace troncal F0/1.
El comando **switchport mode trunk** se usa para configurar un puerto manualmente como enlace troncal. Este comando se debe emitir en ambos extremos del enlace.

a. Cambie el modo de switchport en la interfaz F0/1 para forzar el enlace troncal. Haga esto en ambos switches.
S1(config)# **interface f0/1**
S1(config-if)# **switchport mode trunk**

- **S2(config)# interface f0/1**

- **S2(config-if)# switchport mode trunk**

b. Emita el comando **show interfaces trunk** para ver el modo de enlace troncal. Observe que el modo cambió de **desirable** a **on**.

S2# **show interfaces trunk**

```
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
```

¿Por qué desearía configurar una interfaz en modo de enlace troncal de forma manual en lugar de usar DTP?

Rta: Esta es la forma como podemos asegurar una comunicación confiable independiente del tipo de dispositivo que estemos utilizando.

Parte 11. Eliminar la base de datos de VLAN

En la parte 5, eliminará la base de datos de VLAN del switch. Es necesario hacer esto al inicializar un switch para que vuelva a la configuración predeterminada.

Paso 1. determinar si existe la base de datos de VLAN.

Emita el comando **show flash** para determinar si existe el archivo **vlan.dat** en la memoria flash.

S1# **show flash**

```
Directory of flash:/

   2  -rwx        1285 Mar 1 1993 00:01:24 +00:00  config.text
   3  -rwx       43032 Mar 1 1993 00:01:24 +00:00  multiple-fs
   4  -rwx           5  Mar 1 1993 00:01:24 +00:00  private-config.text
   5  -rwx    11607161  Mar 1 1993 02:37:06 +00:00 c2960-lanbasek9-mz.150-
2.SE.bin
   6  -rwx         736 Mar 1 1993 00:19:41 +00:00  vlan.dat

32514048 bytes total (20858880 bytes free)
```

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

    1  -rw-     4414921          <no date>  c2960-lanbase-mz.122-25.FX.bin
    2  -rw-         736          <no date>  vlan.dat

64016384 bytes total (59600727 bytes free)
S1#
```

Nota: si hay un archivo **vlan.dat** en la memoria flash, la base de datos de VLAN no contiene la configuración predeterminada.

Paso 2. eliminar la base de datos de VLAN.

a. Emita el comando **delete vlan.dat** para eliminar el archivo vlan.dat de la memoria flash y restablecer la base de datos de VLAN a la configuración predeterminada. Se le solicitará dos veces que confirme que desea eliminar el archivo vlan.dat. Presione Enter ambas veces.

S1# delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
S1#

```
S1#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]

S1#
```

b. Emita el comando **show flash** para verificar que se haya eliminado el archivo vlan.dat.
S1# **show flash**

Directory of flash:/

2 -rwx 1285 Mar 1 1993 00:01:24 +00:00 config.text
3 -rwx 43032 Mar 1 1993 00:01:24 +00:00 multiple-fs
4 -rwx 5 Mar 1 1993 00:01:24 +00:00 private-config.text
5 -rwx 11607161 Mar 1 1993 02:37:06 +00:00 c2960-lanbasek9-mz.150-2.SE.bin

32514048 bytes total (20859904 bytes free)

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

    1  -rw-     4414921          <no date>  c2960-lanbase-mz.122-25.FX.bin

64016384 bytes total (59601463 bytes free)
S1#
```

Para inicializar un switch para que vuelva a la configuración predeterminada, ¿cuáles son los otros comandos que se necesitan?

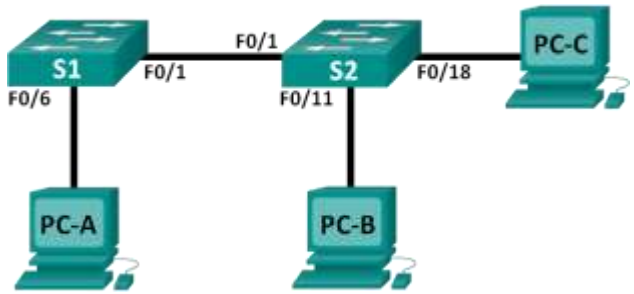
- **Borramos la configuración.**
- **erase startup-config**
- **reiniciamos el dispositivo**
- **reload**

12 INFORME: 3.3.2.2 LAB - IMPLEMENTING VLAN SECURITY

12.1 PRÁCTICA DE LABORATORIO: IMPLEMENTACIÓN DE SEGURIDAD DE VLAN

12.1.1 TOPOLOGÍA

Imagen 11. Topología Informe 3.3.2.2



Fuente: Datos del Informe

Tabla de direccionamiento

Tabla 14. Tabla de direccionamiento Informe 3.3.2.2

Dispositivo	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
PC-A	NIC	172.17.99.3	255.255.255.0	172.17.99.1
PC-B	NIC	172.17.10.3	255.255.255.0	172.17.10.1
PC-C	NIC	172.17.99.4	255.255.255.0	172.17.99.1

Fuente: Datos del Informe

Asignaciones de VLAN

VLAN	Nombre
10	Datos
99	Management&Native
999	BlackHole

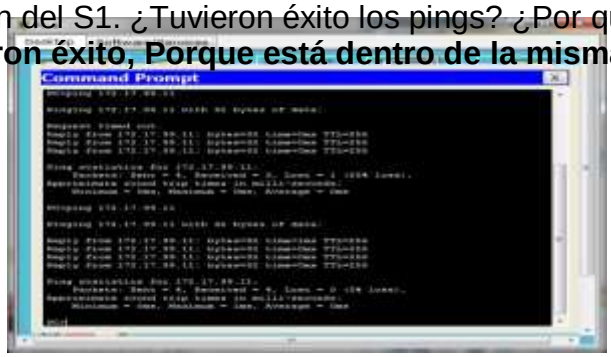
Recursos necesarios

- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola

- Cables Ethernet, como se muestra en la topología

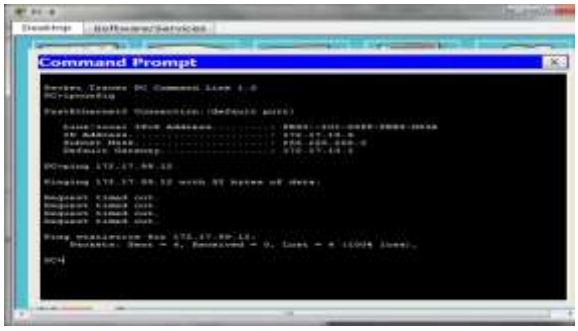
¿A qué VLAN pertenecería un puerto sin asignar, como F0/8 en el S2?
Rta: a la VLAN 1 default (por defecto).

a. En el símbolo del sistema de la PC-A, haga ping a la dirección de administración del S1. ¿Tuvieron éxito los pings? ¿Por qué?
Rta: Si tuvieron éxito, Porque está dentro de la misma red (mismo swiche).



b. Desde el S1, haga ping a la dirección de administración del S2. ¿Tuvieron éxito los pings? ¿Por qué?
Rta: No hay ping porque la fastethernet 0/1 esta asignada en la Vlan1 entonces esta no estaría en la misma Vlan. Para que nos diera ping debería de estar asignada a las Vlan 99

c. En el símbolo del sistema de la PC-B, haga ping a las direcciones de administración del S1 y el S2, y a la dirección IP de la PC-A y la PC-C. ¿Los pings se realizaron correctamente? ¿Por qué?
Rta: no van a responder los ping ya que no están en la misma Vlan. No habría rutas de comunicación.



d. En el símbolo del sistema de la PC-C, haga ping a las direcciones de administración del S1 y el S2. ¿Tuvo éxito? ¿Por qué?
Rta: El S2 si se logra hacer el ping y el S1 no responde el ping, esto es debido a que S2 está en la misma Vlan que es la 99 y en la misma Red y aunque el S1 está en la misma red las fasEthernet 0/1 de los dos swiches están en la Vlan 1 la de defecto y por eso no hay comunicación entre ellos.

Cambiar la VLAN nativa para los puertos de enlace troncal en el S1 y el S2.
Es aconsejable para la seguridad cambiar la VLAN nativa para los puertos de enlace troncal de la VLAN 1 a otra VLAN.

a. ¿Cuál es la VLAN nativa actual para las interfaces F0/1 del S1 y el S2?
Rta: Es la Vlan 1

b. Configure la VLAN nativa de la interfaz de enlace troncal F0/1 del S1 en la VLAN 99 Management&Native.
S1# **config t**
S1(config)# **interface f0/1**
S1(config-if)# **switchport trunk native vlan 99**

c. Espere unos segundos. Debería comenzar a recibir mensajes de error en la sesión de consola del S1. ¿Qué significa el mensaje %CDP-4-NATIVE_VLAN_MISMATCH:?
Rta: Porque en el Swiche 2 aun está configurada la Vlan native como 1 defaul .

Paso 1. verificar que el tráfico se pueda transmitir correctamente a través del enlace troncal.

a. En el símbolo del sistema de la PC-A, haga ping a la dirección de administración del S1. ¿Tuvieron éxito los pings? ¿Por qué?
Rta: Porque esta la Vlan 99 como nativa y administrativa

b. En la sesión de consola del S1, haga ping a la dirección de administración del S2. ¿Tuvieron éxito los pings? ¿Por qué?
Rta: Estos pines si responden con existo ya que hemos creado un troncal.

c. En el símbolo del sistema de la PC-B, haga ping a las direcciones de administración del S1 y el S2, y a la dirección IP de la PC-A y la PC-C. ¿Los pings se realizaron correctamente? ¿Por qué?
Rta: Porque no está en la misma Vlan esté está en la 10 y los otros en la Vlan 99

d. En el símbolo del sistema de la PC-C, haga ping a las direcciones de administración del S1 y el S2, y a la dirección IP de la PC-A. ¿Tuvo éxito? ¿Por qué?
Rta: Estos si responder ya que como creamos una troncal si hay comunicación.

e. Restrinja el puerto de enlace troncal F0/1 en el S1 para permitir solo las VLAN 10 y 99.

S1(config)# **interface f0/1**
S1(config-if)# **switchport trunk allowed vlan 10,99**

f. Restrinja el puerto de enlace troncal F0/1 en el S2 para permitir solo las VLAN 10 y 99.

Verifique las VLAN permitidas. Emita el comando **show interface trunk** en el modo ¿Cuál es el resultado?
Rta: Solo nos dejara pasar las Vlan 10 y 99

12.1.2 REFLEXIÓN
¿Qué problemas de seguridad, si los hubiera, tiene la configuración predeterminada de un switch Cisco?

Rta: Que si la persona que ingresa al swiche tiene conocimientos de configuración sabe que la Vlan 1 siempre esta como defaul.y podría administrar remotamente y podría ingresar a la red.

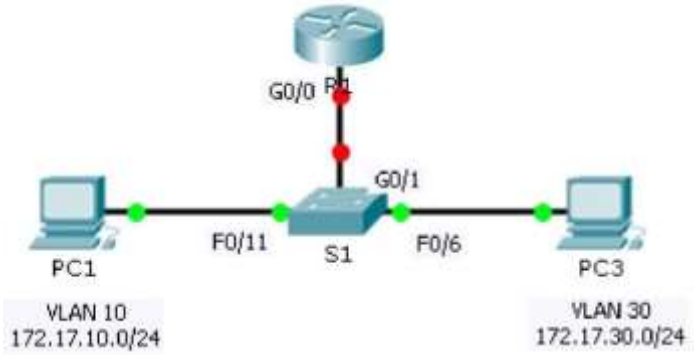
13 INFORME: 5.1.3.6 PACKET TRACER - CONFIGURING ROUTER-ON-A-STICK INTER-VLAN ROUTING

13.1 PACKET TRACER – CONFIGURING ROUTER-ON-A-STICK INTER-VLAN ROUTING (INSTRUCTOR VERSION)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

13.1.1 TOPOLOGÍA

Imagen 12. Topología Informe 5.1.3.6



Fuente: Datos del Informe

Addressing Table

Tabla 15. Tabla de Direccionamiento Informe 5.1.3.6

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	GO/0.10	172.17.10.1	255.255.255.0	N/A
	GO/0.30	172.17.30.1	255.255.255.0	N/A
PC1	NIC	172.17.10.10	255.255.255.0	172.17.10.1
PC2	NIC	172.17.30.10	255.255.255.0	172.17.30.1

Fuente: Datos del Informe

Objectives

- Part 1: Test Connectivity without Inter-VLAN Routing
- Part 2: Add VLANs to a Switch
- Part 3: Configure Subinterfaces
- Part 4: Test Connectivity with Inter-VLAN Routing

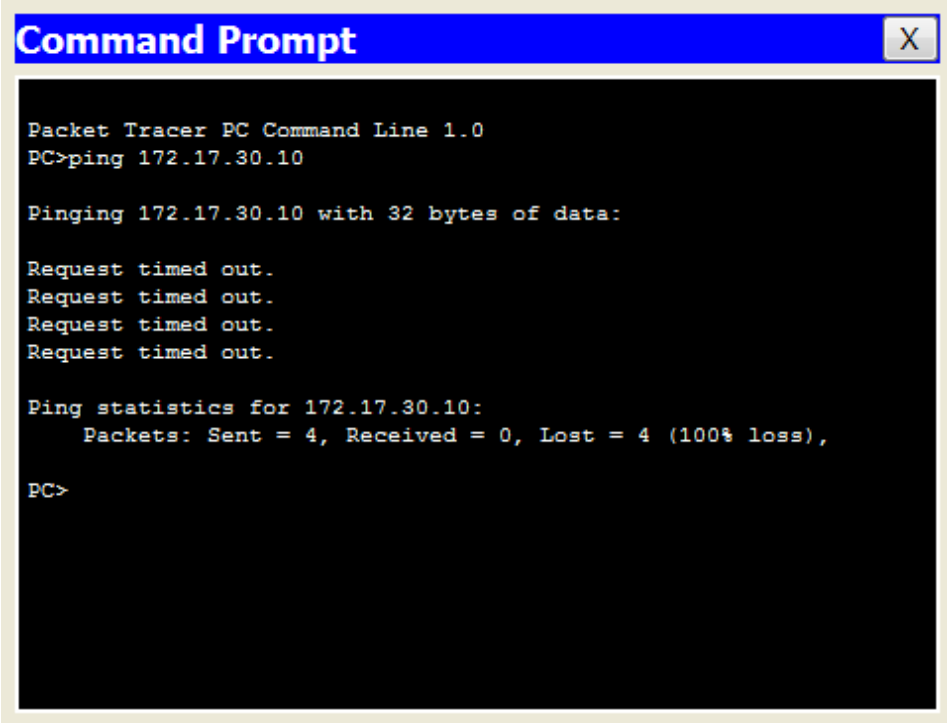
Scenario

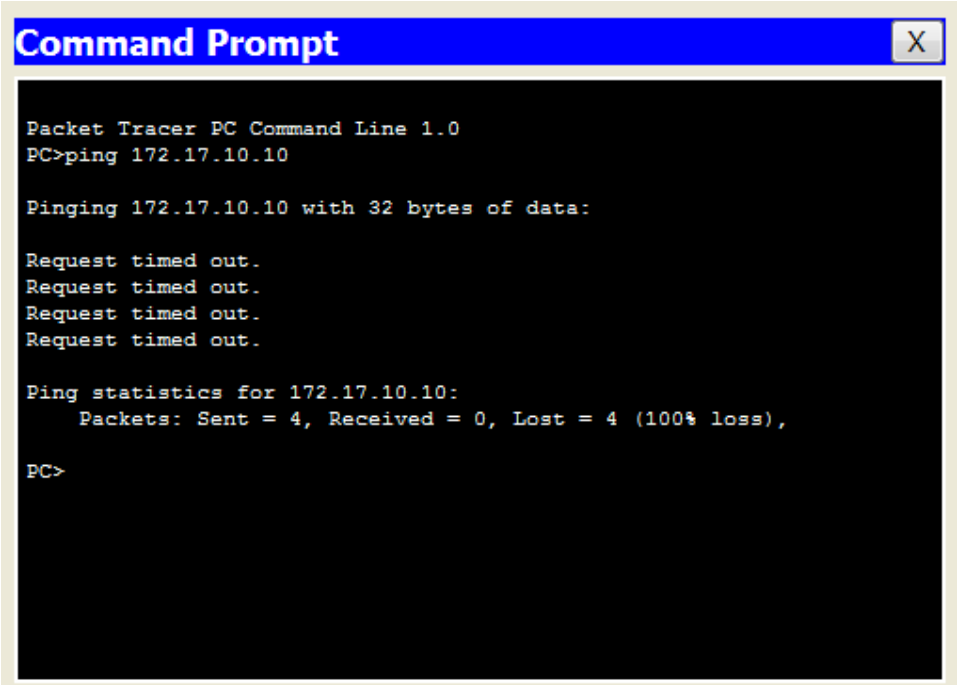
In this activity, you will check for connectivity prior to implementing inter-VLAN routing. You will then configure VLANs and inter-VLAN routing. Finally, you will enable trunking and verify connectivity between VLANs.

Part 1: Test Connectivity Without Inter-VLAN Routing

Step 1: Ping between PC1 and PC3.

Wait for switch convergence or click **Fast Forward Time** a few times. When the link lights are green for **PC1** and **PC3**, ping between **PC1** and **PC3**. Because the two PCs are on separate networks and **R1** is not configured, the ping fails.





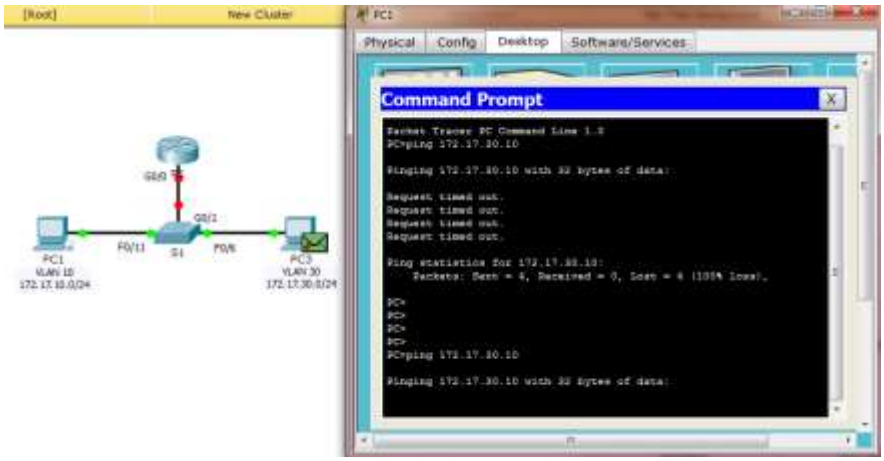
Step 2: Switch to Simulation mode to monitor pings.

a. Switch to Simulation mode by clicking the **Simulation** tab or pressing **Shift+S**.

b. Click **Capture/Forward** to see the steps the ping takes between **PC1** and **PC3**. Notice how the ping never leaves **PC1**. What process failed and why? }

Rta: The ARP process failed because the ARP request was dropped by PC3. PC1 and PC3 are not on the same network, so PC1 never gets the MAC address for PC3. Without a MAC address, PC1 cannot créate an ICMP echo request.

Los dos PC están en capas diferentes, entonces, no hay forma de aprender los datos de las otras redes, este es el motivo por el cual este falla.



Part 2: Add VLANs to a Switch

Step 1: Créate VLANs on S1.

Return to **Realtime** mode and créate VLAN 10 and VLAN 30 on **S1**.

SI(config)# **vlan 10**
SI(config-vlan)# **vlan 30**

Step 2: Assign VLANs to ports.

a. Configure interface FO/6 and F0/11 as access ports and assign VLANs.

- Assign **PC1** to VLAN 10.
- Assign **PC3** to VLAN 30.

SI(config-vlan)# **int fa0/ll**
SI(config-if)# **switchport mode access**
SI(config-if)# **switchport access vlan 10**
SI(config-if)# **int faO/6**
SI(config-if)# **switchport mode access**
SI(config-if)# **switchport access vlan 30**

```
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to
up


S1>
S1>
S1>
S1>enable
S1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#
S1(config)#vlan 10
S1(config-vlan)#vlan 30
S1(config-vlan)#int fa0/11
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
S1(config-if)#int fa0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
S1(config-if)#
```

b. Issue the **show vlan brief** command to verify VLAN configuration.

Sl# **show vlan brief**

VLAN	Ñame	Status	Ports
1	default	active	FaO/1, FaO/2, FaO/3, FaO/4 FaO/5, FaO/7, FaO/8, FaO/9 FaO/10, FaO/12, FaO/13, FaO/14 FaO/15, FaO/16, FaO/17, FaO/18 FaO/19, FaO/20, FaO/21, FaO/22 FaO/23, FaO/24, GigO/1, GigO/2
10	VLAN0010	active	FaO/11
30	VLAN0030	active	FaO/6
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
S1#
S1#
S1#
S1#
S1#
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   VLAN0010                          active    Fa0/11
30   VLAN0030                          active    Fa0/6
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S1#
S1#
```

Step 3: Test connectivity between PC1 and PC3.

From **PC1**, ping **PC3**. The pings should still fail. Why were the pings unsuccessful?
Rta: Each VLAN is a sepárate network and requires a router or a layer 3 switch to provide communication between them.
Las PC están en redes distintas.

Part 3: Configure Subinterfaces
Step 1: Configure subinterfaces on R1 using the 802.1Q encapsulation.
a. Créate the subinterface GO/0.10.
- Set the encapsulation type to 802.1 Q and assign VLAN 10 to the subinterface.
- Refer to the **Address Table** and assign the correct IP address to the subinterface.

b. Repeat for the GO/0.30 subinterface.

```
Rl(config)# int g0/0.10
Rl (config-subif)# encapsulation dotlQ 10
Rl (config-subif)# ip address 172.17.10.1 255.255.255.0
Rl(config-subif)# int gO/0.30
Rl(config-subif)# encapsulation dotlQ 30
Rl(config-subif)# ip address 172.17.30.1 255.255.255.0
```

```
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
R1(config)#int g0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0
R1(config-subif)#int g0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 172.17.30.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state
to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10, changed
state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed
state to up

R1(config-if)#
```

Step 2: Verify Configuration.

a. Use the **show ip interface brief** command to verify subinterface configuration. Both subinterfaces are down. Subinterfaces are virtual interfaces that are associated with a physical interface. Therefore, in order to enable subinterfaces, you must enable the physical interface that they are associated with.

```
R1#
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     unassigned      YES unset  up                    up

GigabitEthernet0/0.10  172.17.10.1     YES manual up                    up

GigabitEthernet0/0.30  172.17.30.1     YES manual up                    up

GigabitEthernet0/1     unassigned      YES unset  administratively down down

Vlan1                  unassigned      YES unset  administratively down down
R1#
```

b. Enable the G0/0 interface. Verify that the subinterfaces are now active.

Part 4: Test Connectivity with Inter-VLAN Routing

Step 1: Ping between PC1 and PC3.

From **PC1**, ping **PC3**. The pings should still fail.

```
Packet Tracer PC Command Line 1.0
PC>ping 172.17.30.10

Pinging 172.17.30.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.17.30.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
Packet Tracer PC Command Line 1.0
PC>ping 172.17.10.10

Pinging 172.17.10.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.17.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Step 2: Enable trunking.

a. On **S1**, issue the **show vlan** command. What VLAN is G0/1 assigned to?

VLAN 1

b. Because the router was configured with múltiple subinterfaces assigned to different VLANs, the switch port connecting to the router must be configured as a trunk. Enable trunking on interface G0/1.

SI(config-if)# **int g0/l**

SI(config-if)# **switchport mode trunk**

```
S1>enable
S1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int g0/1
S1(config-if)#switchport mode trunk
```

b. How can you determine that the interface is a trunk port using the **showvlan** command?

Rta: The interface is no longer listed under VLAN 1.

```
S1#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/2
10   VLAN0010                          active    Fa0/11
30   VLAN0030                          active    Fa0/6
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

c. Issue the **show interface trunk** command to verify the interface is configured as a trunk.

```
Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,10,30
S1#
S1#
S1#
S1#
S1#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,10,30

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,10,30
S1#
S1#
S1#
S1#
```

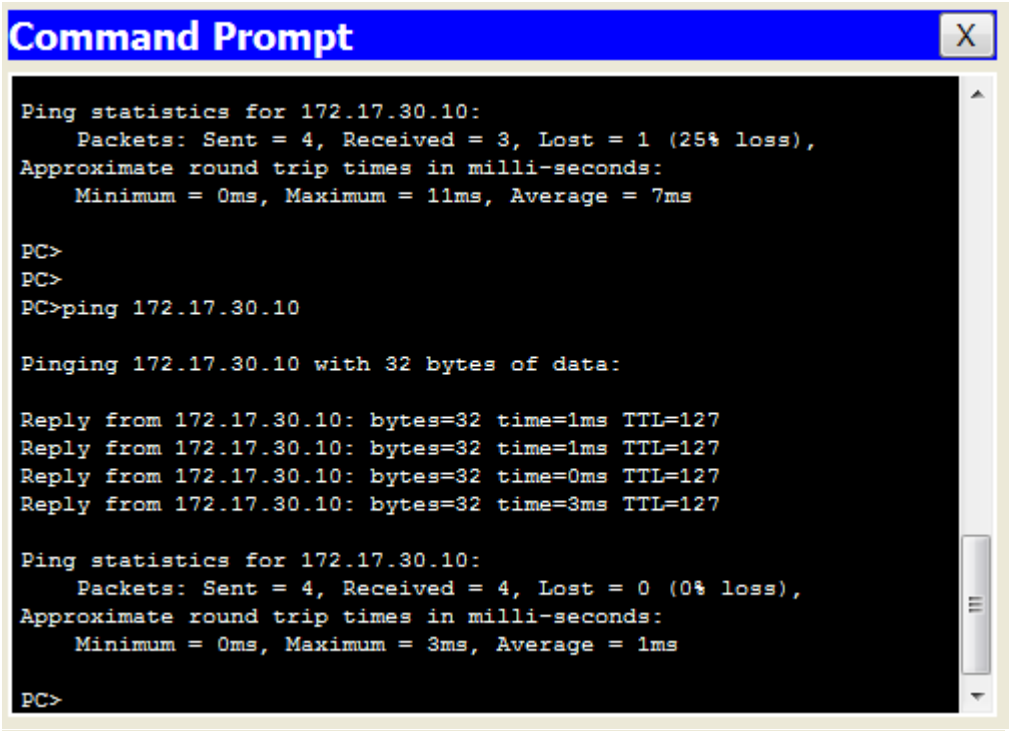
Step 3: Switch to Simulation mode to monitor pings.

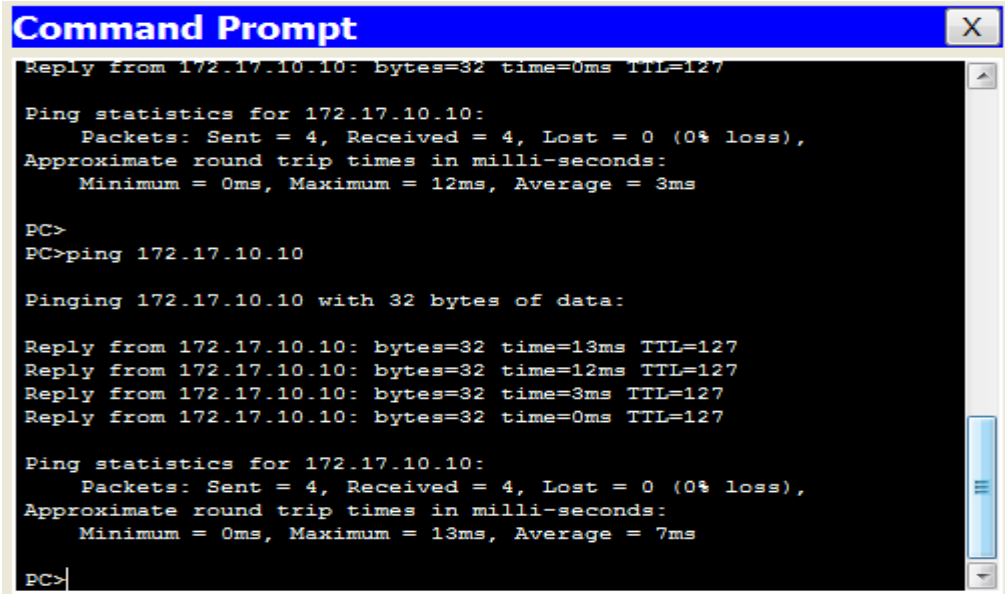
a. Switch to **Simulation** mode by clicking the **Simulation** tab or pressing **Shift+S**.

b. Click **Capture/Forward** to see the steps the ping takes between **PC1** and **PC3**.

c. You should see ARP requests and replies between **S1** and **R1**. Then ARP requests and replies between **R1** and **S3**. Then **PC1** can encapsulate an ICMP

echo request with the proper data-link layer information and R1 will route the request to **PC3**.
Note: After the ARP process finishes, you may need to click Reset Simulation to see the ICMP process complete.





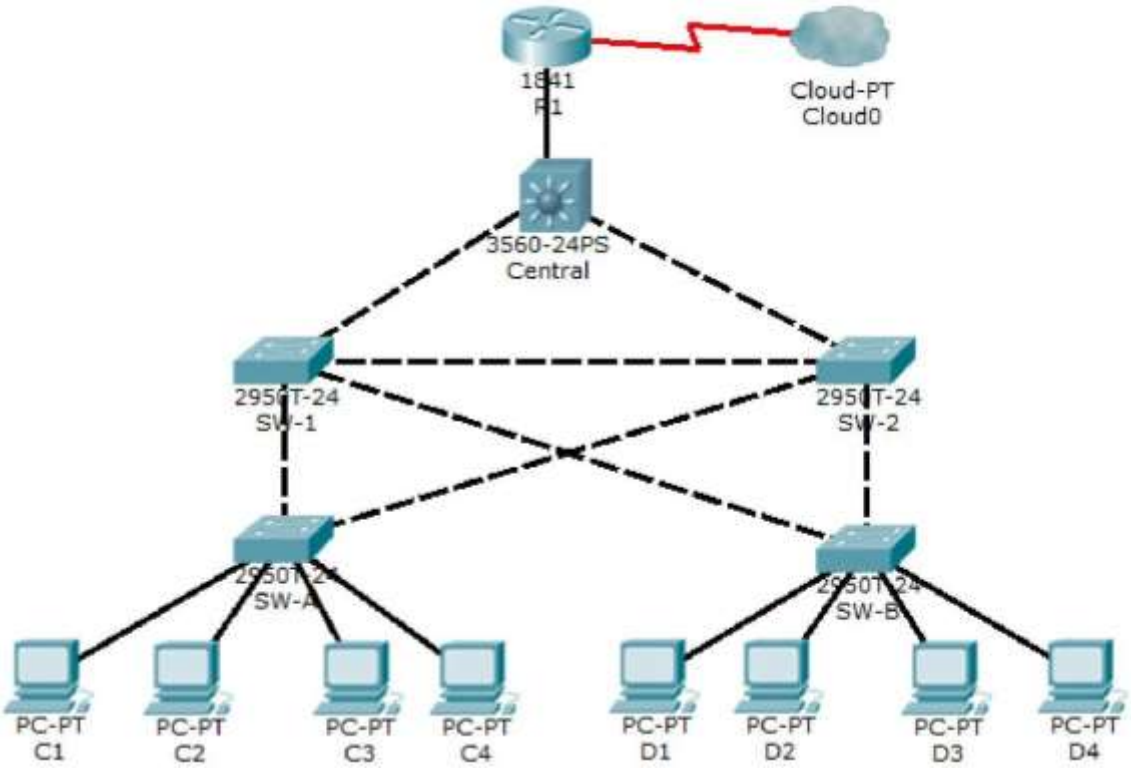
Suggested Scoring Rubric
Packet Tracer scores 60 points. The four questions are worth 10 points each.

14 INFORME: 6.5.1.2 PACKET TRACER - LAYER 2 SECURITY

14.1 PACKET TRACER - LAYER 2 SECURITY

14.1.1 TOPOLOGY

Imagen 13. Topología Informe 6.5.1.2



Fuente: Datos del Informe

Objectives

- Assign the Central switch as the root bridge.
- Secure spanning-tree parameters to prevent STP manipulation attacks.
- Enable storm control to prevent broadcast storms.
- Enable port security to prevent MAC address table overflow attacks.

Background / Scenario

There have been a number of attacks on the network recently. For this reason, the network administrator has assigned you the task of configuring Layer 2 security.

For optimum performance and security, the administrator would like to ensure that the root bridge is the 3560 Central switch. To prevent against spanning-tree manipulation attacks, the administrator wants to ensure that the STP parameters are secure. In addition, the network administrator would like to enable storm control to prevent broadcast storms. Finally, to prevent against MAC address table overflow attacks, the network administrator has decided to configure port security to

limit the number of MAC addresses that can be learned per switch port. If the number of MAC addresses exceeds the set limit, the administrator would like the port to be shutdown.

All switch devices have been preconfigured with the following:

- Enable password: ciscoenpa55
- Console password: **ciscoconpa55**
- VTY line password: **ciscovtypa55**

Part 1: Configure Root Bridge
Step 1: Determine the current root bridge.

From **Central**, issue the **show spanning-tree** command to determine the current root bridge and to see the ports in use and their status.

```
Central#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0009.7C61.9058
              Cost        4
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00D0.D31C.634C
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Gi0/1            Root FWD 4         128.25   P2p
Gi0/2            Desg FWD 4         128.26   P2p

Central#
```

Which switch is the current root bridge?

- SW-1

Based on the current root bridge, what is the resulting spanning tree? (Draw the spanning-tree topology.)

Step 2: Assign Central as the primary root bridge.

Using the **spanning-tree vlan 1 root primary** command, assign **Central** as the root bridge. Central(config)# **spanning-tree vlan 1 root primary**

```
Central#
Central#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Central(config)#spanning-tree vlan 1 root primary
Central(config)#
```

Step 3: Assign SW-1 as a secondary root bridge.
Assign **SW-1** as the secondary root bridge using the **spanning-tree vlan 1 root secondary** command. SW-1(config)# **spanning-tree vlan 1 root secondary**

```
SW-1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
SW-1(config)#spanning-tree vlan 1 root secondary
SW-1(config)#
```

Step 4: Verify the spanning-tree configuration.
Issue the **show spanning-tree** command to verify that **Central** is the root bridge. Which switch is the current root bridge?

```
Central#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     00D0.D31C.634C
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24577  (priority 24576 sys-id-ext 1)
              Address     00D0.D31C.634C
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Gi0/1            Desg FWD 4         128.25   P2p
Gi0/2            Desg FWD 4         128.26   P2p

Central#
```

- Central

Based on the new root-bridge, what is the resulting spanning tree? (Draw the spanning-tree topology.)

Part 2: Protect Against STP Attacks
Secure the STP parameters to prevent STP manipulation attacks.

Step 1: Enable PortFast on all access ports.

PortFast is configured on access ports that connect to a single workstation or server to enable them to become active more quickly. On the connected access ports of the **SW-A** and **SW-B**, use the **spanning-tree portfast** command.
SW-A(config)# **interface range fastethernet 0/1 - 4** SW-A(config-if-range)# **spanning-tree portfast**

SW-B(config)# **interface range fastethernet 0/1 - 4** SW-B(config-if-range)# **spanning-tree portfast**

```
SW-A(config)#interface range fastethernet 0/1 - 4
SW-A(config-if-range)#spanning-tree portfast

SW-B(config)#interface range fastethernet 0/1 - 4
SW-B(config-if-range)#spanning-tree portfast
```

Step 2: Enable BPDU guard on all access ports.

BPDU guard is a feature that can help prevent rogue switches and spoofing on access ports. Enable BPDU guard on **SW-A** and **SW-B** access ports.

SW-A(config)# **interface range fastethernet 0/1 - 4** SW-A(config-if-range)# **spanning-tree bpduguard enable**

```
SW-A(config)#interface range fastethernet 0/1 - 4
SW-A(config-if-range)#spanning-tree bpduguard enable
SW-A(config-if-range)#
```

SW-B(config)# **interface range fastethernet 0/1 - 4** SW-B(config-if-range)# **spanning-tree bpduguard enable**

```
SW-B(config)#interface range fastethernet 0/1 - 4
SW-B(config-if-range)#spanning-tree bpduguard enable
SW-B(config-if-range)#
```

Note: Spanning-tree BPDU guard can be enabled on each individual port using the **spanning-tree bpduguard enable** command in the interface configuration mode or the **spanning-tree portfast bpduguard default** command in the global configuration mode. For grading purposes in this activity, please use the **spanning-tree bpduguard enable** command.

Step 3: Enable root guard.

Root guard can be enabled on all ports on a switch that are not root ports. It is best deployed on ports that connect to other non-root switches. Use the **show spanning-tree** command to determine the location of the root port on each switch. On **SW-1**, enable root guard on ports Fa0/23 and Fa0/24. On **SW-2**, enable root guard on ports Fa0/23 and Fa0/24.

SW-1(config)# **interface range fa0/23 - 24** SW-1(config-if-range)# **spanning-tree guard root**

```
SW-1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
SW-1(config)#interface range fa0/23 - 24
SW-1(config-if-range)#spanning-tree guard root
SW-1(config-if-range)#
```

SW-2(config)# **interface range fa0/23 - 24** SW-2(config-if-range)# **spanning-tree guard root**

```
SW-2#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
SW-2(config)#interface range fa0/23 - 24
SW-2(config-if-range)#spanning-tree guard root
SW-2(config-if-range)#
```

Part 3: Enable Storm Control

Step 1: Enable storm control for broadcasts.

a. Enable storm control for broadcasts on all ports connecting switches (trunk ports).

b. Enable storm control on interfaces connecting **Central**, **SW-1**, and **SW-2**. Set a **50** percent rising suppression level using the **storm-control broadcast** command.

SW-1(config)# **interface range gi1/1 , fa0/1 , fa0/23 - 24** SW-1(config-if)# **storm-control broadcast level 50**

```
SW-1(config)#
SW-1(config)#interface range gi0/1 , fa0/1 , fa0/23 - 24
SW-1(config-if-range)#storm-control broadcast level 50
SW-1(config-if-range)#
```

SW-2(config)# **interface range gi1/1 , fa0/1 , fa0/23 - 24** SW-2(config-if)# **storm-control broadcast level 50**

```
SW-2(config)#
SW-2(config)#interface range gi0/1 , fa0/1 , fa0/23 - 24
SW-2(config-if-range)#storm-control broadcast level 50
SW-2(config-if-range)#
```

Central(config-if)# **interface range gi0/1 , gi0/2 , fa0/1** Central(config-if)# **storm-control broadcast level 50**

```
Central(config)#
Central(config)#interface range gi0/1 , gi0/2 , fa0/1
Central(config-if-range)#storm-control broadcast level 50
Central(config-if-range)#
```

Step 2: Verify storm control configuration.

Verify your configuration with the **show storm-control broadcast** and the **show run** commands.

Part 4: Configure Port Security and Disable Unused Ports

Step 1: Configure basic port security on all ports connected to host devices.

This procedure should be performed on all access ports on **SW-A** and **SW-B**. Set the maximum number of learned MAC address to **2**, allow the MAC address to be learned dynamically, and set the violation to **shutdown**.
Note: A switch port must be configured as an access port to enable port security.
SW-A(config)# **interface range fa0/1 - 22**
SW-A(config-if-range)# **switchport mode access**
SW-A(config-if-range)# **switchport port-security**
SW-A(config-if-range)# **switchport port-security maximum 2**
SW-A(config-if-range)# **switchport port-security violation shutdown**
SW-A(config-if-range)# **switchport port-security mac-address sticky**

```
SW-A(config)#interface range fa0/1 - 22
SW-A(config-if-range)#switchport mode access
SW-A(config-if-range)#switchport port-security
SW-A(config-if-range)#switchport port-security maximum 2
SW-A(config-if-range)#switchport port-security violation shutdown
SW-A(config-if-range)#switchport port-security mac-address sticky
SW-A(config-if-range)#
```

SW-B(config)# **interface range fa0/1 - 22** SW-B(config-if-range)# **switchport mode access** SW-B(config-if-range)# **switchport port-security**
SW-B(config-if-range)# **switchport port-security maximum 2**
SW-B(config-if-range)# **switchport port-security violation shutdown** SW-B(config-if-range)# **switchport port-security mac-address sticky**

```
SW-B(config)#interface range fa0/1 - 22
SW-B(config-if-range)#switchport mode access
SW-B(config-if-range)#switchport port-security
SW-B(config-if-range)#switchport port-security maximum 2
SW-B(config-if-range)#switchport port-security violation shutdown
SW-B(config-if-range)#switchport port-security mac-address sticky
SW-B(config-if-range)#
```

Why would you not want to enable port security on ports connected to other switches or routers?
Ports connected to other switch devices and routers can, and should, have a multitude of MAC addresses learned for that single port. Limiting the number of MAC addresses that can be learned on these ports can significantly impact network functionality.

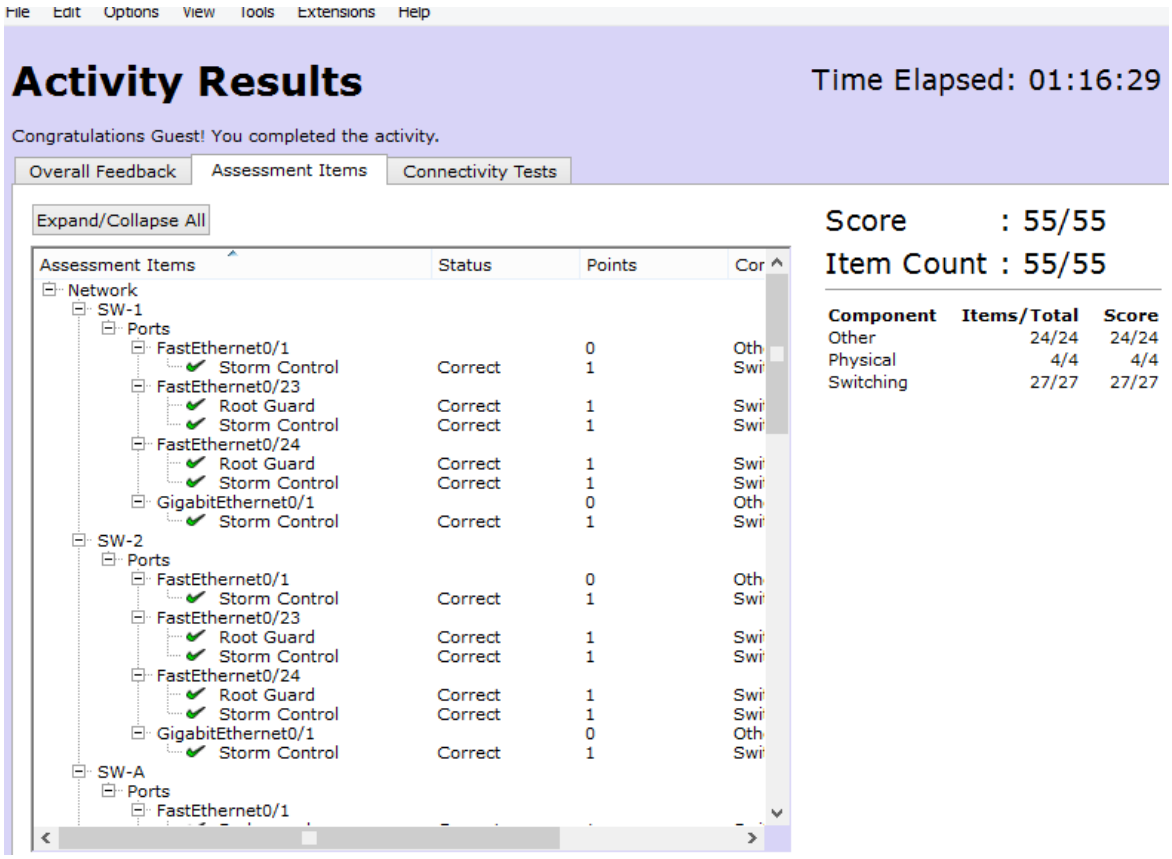
Step 2: Verify port security.
On **SW-A**, issue the **show port-security interface fa0/1** command to verify that port security has been configured.

```
SW-A(config-if-range)#
SW-A(config-if-range)#
SW-A(config-if-range)#
SW-A(config-if-range)#end
SW-A#
%SYS-5-CONFIG_I: Configured from console by console

SW-A#
SW-A#show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

SW-A#
```

Step 3: Disable unused ports.

Disable all ports that are currently unused.
SW-A(config)# **interface range fa0/5 - 22** SW-A(config-if-range)# **shutdown**
SW-B(config)# **interface range fa0/5 - 22** SW-B(config-if-range)# **shutdown**
Step 4: Check results.

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.



!!!Script for Central

conf t
spanning-tree vlan 1 root primary
interface range gi0/1 , gi0/2 , fa0/1
storm-control broadcast level 50 end

!!!Script for SW-1

conf t
spanning-tree vlan 1 root secondary
interface range fa0/23 - 24
spanning-tree guard root interface range gi1/1 , fa0/1 , fa0/23 - 24
storm-control broadcast level 50 end

!!!Script for SW-2

conf t
interface range fa0/23 - 24
spanning-tree guard root interface range gi1/1 , fa0/1 , fa0/23 - 24
storm-control broadcast level 50 end

!!!Script for SW-A

conf t
interface range fastethernet 0/1 - 4

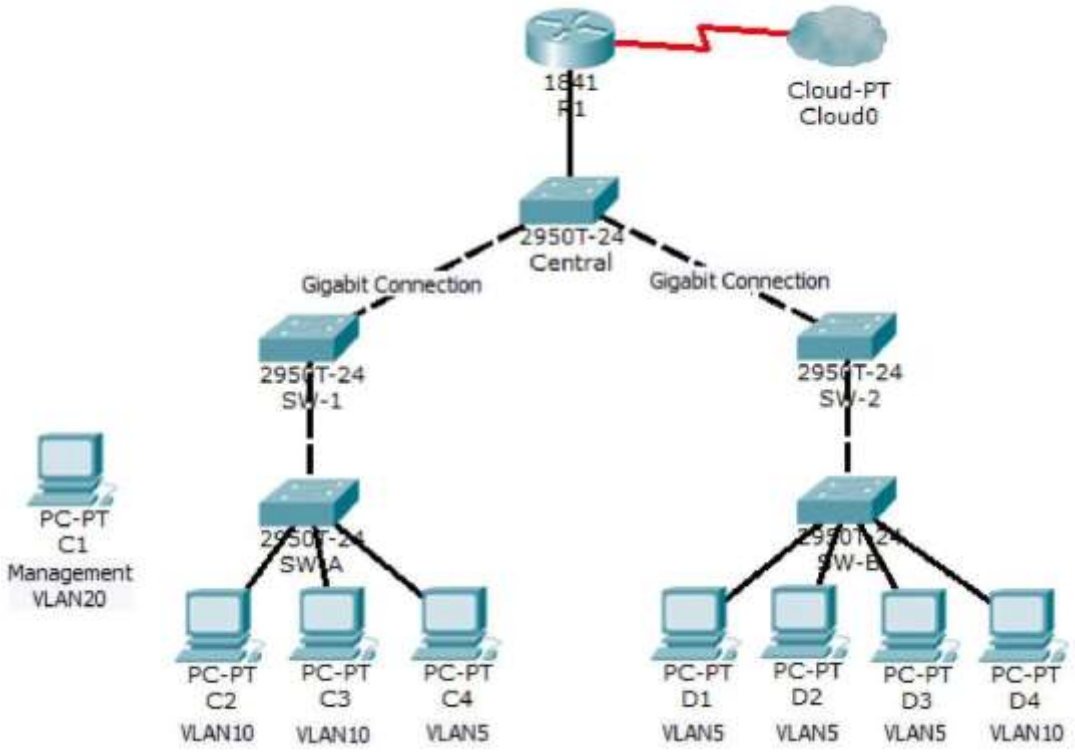
spanning-tree portfast
spanning-tree bpduguard enable interface range fa0/1 - 22
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security violation shutdown
switchport port-security mac-address sticky interface range fa0/5 - 22
shutdowm end
!!!Script for SW-B
conf t
interface range fastethernet 0/1 - 4
spanning-tree portfast
spanning-tree bpduguard enable
interface range faO/1 - 22
switchport mode access
switchport port-security
switchport port-security máximum 2
switchport port-security violation shutdown
switchport port-security mac-address sticky
interface range faO/5 - 22 shutdown
end

15 INFORME: 6.5.1.3 PACKET TRACER - LAYER 2 VLAN SECURITY

15.1 PACKET TRACER - LAYER 2 VLAN SECURITY

15.1.1 TOPOLOGIA

Imagen 14. Topología Informe 6.5.1.3



Fuente: Datos del Informe

Objectives

- Connect a new redundant link between SW-1 and SW-2.
- Enable trunking and configure security on the new trunk link between SW-1 and SW-2.
- Créate a new management VLAN (VLAN 20) and attach a management PC to that VLAN.
- Implement an ACL to prevent outside users from accessing the management VLAN.

Background / Scenario

A company's network is currently set up using two sepárate VLANs: VLAN 5 and VLAN 10. In addition, all trunk ports are configured with native VLAN 15. A network administrator wants to add a redundant link between switch SW-1 and SW-2. The link must have trunking enabled and all security requirements should be in place.

In addition, the network administrator wants to connect a management PC to switch SW-A. The administrator would like to allow the management PC to be able to

connect to all switches and the router, but does not want any other devices to connect to the management PC or the switches. The administrator would like to créate a new VLAN 20 for management purposes.
All devices have been preconfigured with:
o Enable secret password: **ciscoenpa55**
o Consolé password: **ciscoconpa55**
o VTY line password: **ciscovtypa55**

Part 1: Verify Connectivity

Step 1: Verify connectivity between C2 (VLAN 10) and C3 (VLAN 10).

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=44ms TTL=128
Reply from 192.168.10.2: bytes=32 time=0ms TTL=128
Reply from 192.168.10.2: bytes=32 time=0ms TTL=128
Reply from 192.168.10.2: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 44ms, Average = 11ms

PC>
PC>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=1ms TTL=128
Reply from 192.168.10.1: bytes=32 time=0ms TTL=128
Reply from 192.168.10.1: bytes=32 time=0ms TTL=128
Reply from 192.168.10.1: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

Step 2: Verify connectivity between C2 (VLAN 10) and D1 (VLAN 5).

```
PC>ping 192.168.5.2

Pinging 192.168.5.2 with 32 bytes of data:

Reply from 192.168.5.2: bytes=32 time=35ms TTL=127
Reply from 192.168.5.2: bytes=32 time=0ms TTL=127
Reply from 192.168.5.2: bytes=32 time=0ms TTL=127
Reply from 192.168.5.2: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.5.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 35ms, Average = 8ms

PC>
```

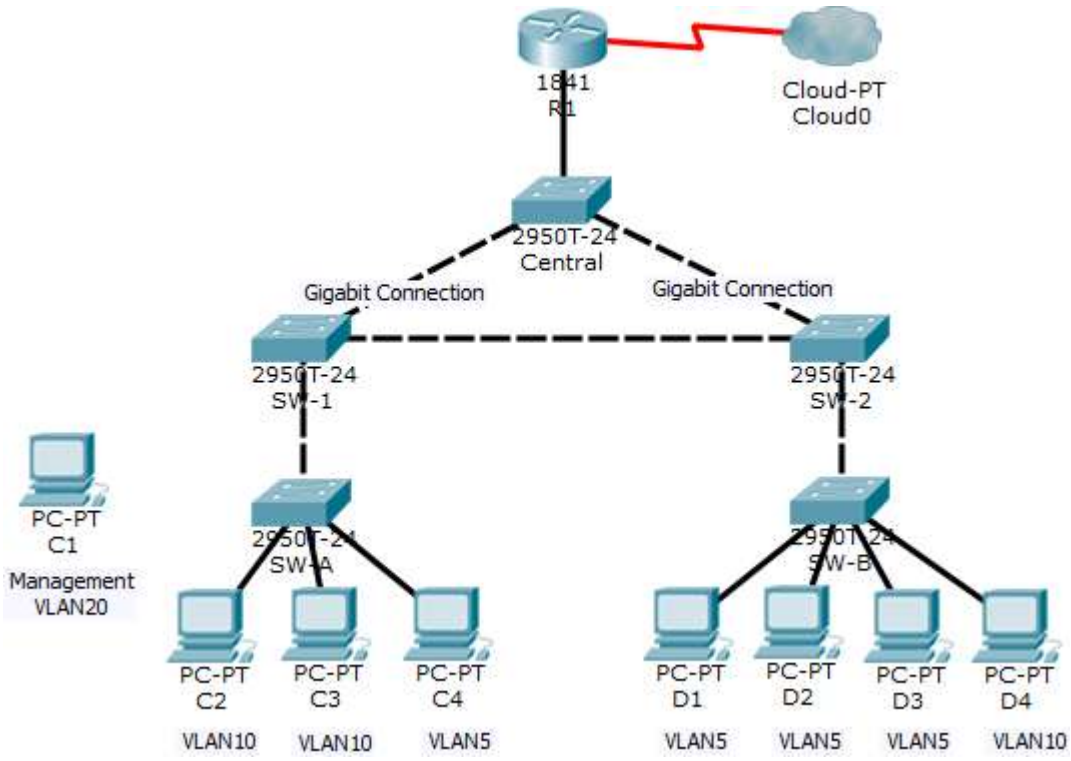
```
PC>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=12ms TTL=127
Reply from 192.168.10.1: bytes=32 time=10ms TTL=127
Reply from 192.168.10.1: bytes=32 time=12ms TTL=127
Reply from 192.168.10.1: bytes=32 time=13ms TTL=127

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 13ms, Average = 11ms

PC>
```

Note: If using the simple PDU GUI packet, be sure to ping twice to allow for ARP.

Part 2: Create a Redundant Link Between SW-1 and SW-2

Step 1: Connect SW-1 and SW-2.

Using a crossover cable, connect port Fa0/23 on **SW-1** to port Fa0/23 on **SW-2**.



Step 2: Enable trunking, including all trunk security mechanisms on the link between SW-1 and SW-2.

Trunking has already been configured on all pre-existing trunk interfaces. The new link must be configured for trunking, including all trunk security mechanisms. On both **SW-1** and **SW-2**, set the port to trunk, assign native VLAN 15 to the trunk port, and disable auto-negotiation.

SW-1(config)# **interface fa0/23** SW-1(config-if)# **switchport mode trunk**
SW-1(config-if)# **switchport trunk native vlan 15** SW-1(config-if)# **switchport nonegotiate** SW-1(config-if)# **no shutdown**
SW-2(config)# **interface fa0/23** SW-2(config-if)# **switchport mode trunk**
SW-2(config-if)# **switchport trunk native vlan 15** SW-2(config-if)# **switchport nonegotiate** SW-2(config-if)# **no shutdown**

Part 3: Enable VLAN 20 as a Management VLAN

The network administrator wants to access all switch and routing devices using a management PC. For security, the administrator wants to ensure that all managed devices are on a separate VLAN.

Step 1: Enable a management VLAN (VLAN 20) on SW-A.

a. Enable VLAN 20 on **SW-A**.
SW-A(config)# **vlan 20**
SW-A(config-vlan)# **exit**

b. Create an interface VLAN 20 and assign an IP address within the 192.168.20.0/24 network.
SW-A(config)# **interface vlan 20**
SW-A(config-if)# **ip address 192.168.20.1 255.255.255.0**

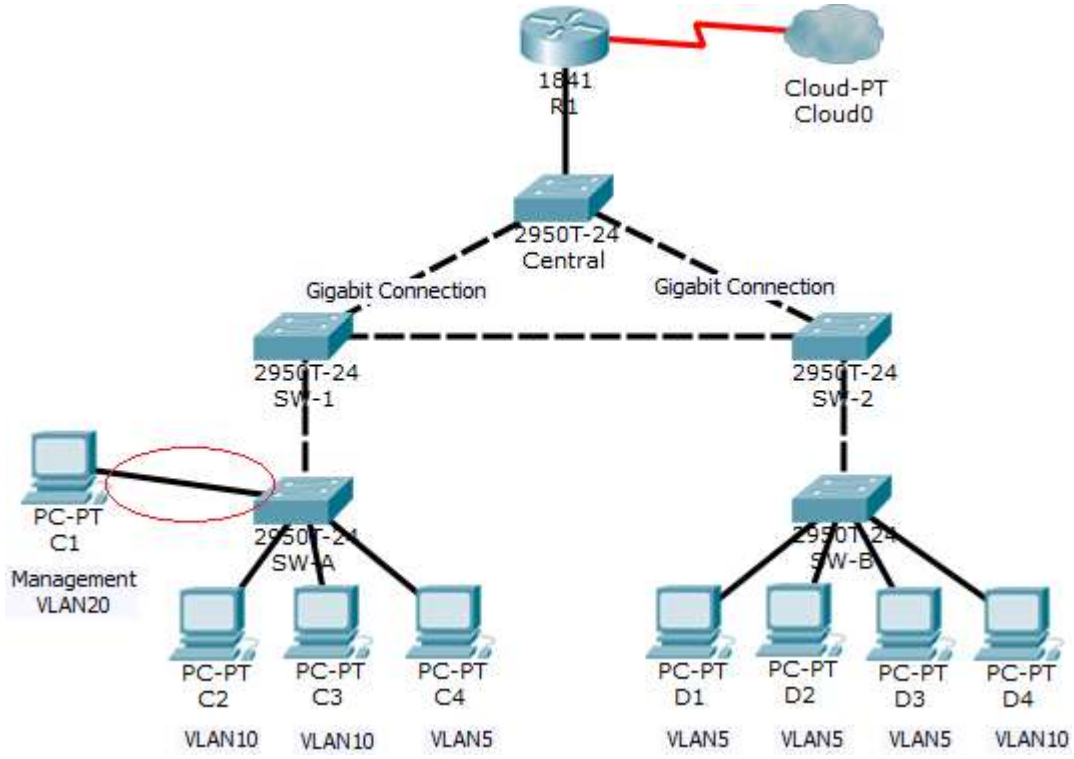
Step 2: Enable the same management VLAN on all other switches.

a. Create the management VLAN on all switches: **SW-B**, **SW-1**, **SW-2**, and **Central**.
SW-B(config)# **vlan 20** SW-B(config-vlan)# **exit**
SW-1(config)# **vlan 20** SW-1(config-vlan)# **exit**
SW-2(config)# **vlan 20** SW-2(config-vlan)# **exit**
Central(config)# **vlan 20** Central(config-vlan)# **exit**

b. Create an interface VLAN 20 on all switches and assign an IP address within the 192.168.20.0/24 network.

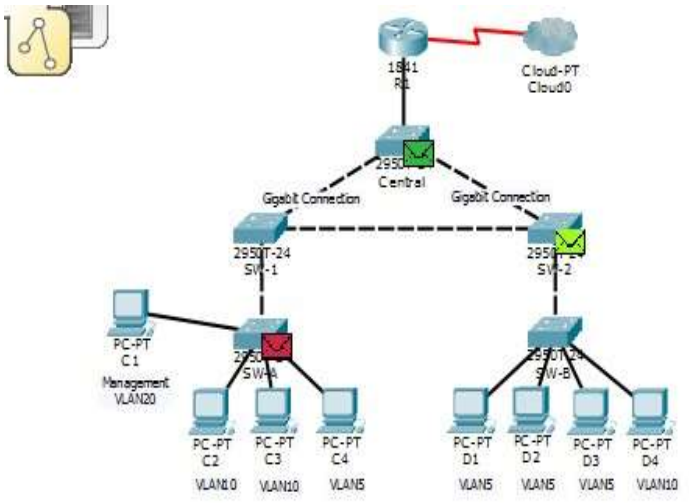
SW-B(config)# **interface vlan 20**
SW-B(config-if)# **ip address 192.168.20.2 255.255.255.0**
SW-1(config)# **interface vlan 20**
SW-1(config-if)# **ip address 192.168.20.3 255.255.255.0**
SW-2(config)# **interface vlan 20**
SW-2(config-if)# **ip address 192.168.20.4 255.255.255.0**
Central(config)# **interface vlan 20**
Central(config-if)# **ip address 192.168.20.5 255.255.255.0**

Step 3: Configure the management PC and connect it to SW-A port Fa0/1.
Ensure that the management PC is assigned an IP address within the 192.168.20.0/24 network. Connect the management PC to **SW-A** port Fa0/1.



Step 4: On SW-A, ensure the management PC is part of VLAN 20.
Interface Fa0/1 must be part of VLAN 20.
SW-A(config)# **interface fa0/1**
SW-A(config-if)# **switchport access vlan 20** SW-A(config-if)# **no shutdown**

Step 5: Verify connectivity of the management PC to all switches.
The management PC should be able to ping **SW-A**, **SW-B**, **SW-1**, **SW-2**, and **Central**.



U List Window

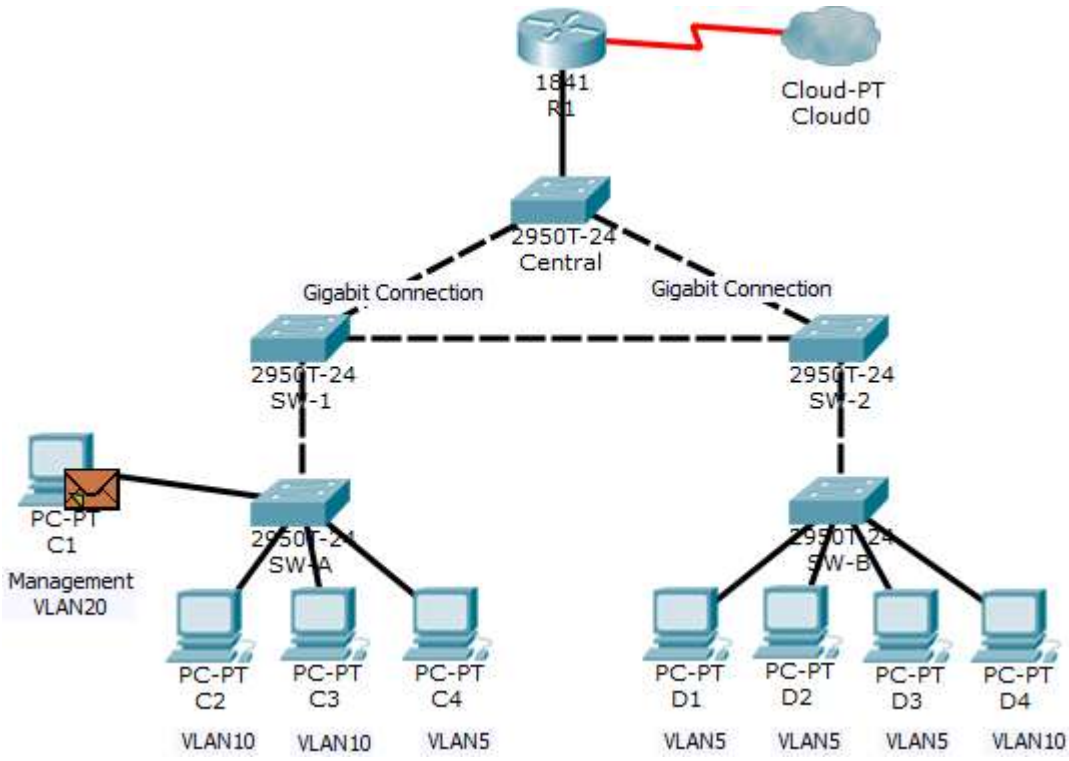
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	C1	SW-A	ICMP		0.000	N	0	(edit)	(delete)
	Successful	C1	SW-1	ICMP		0.000	N	1	(edit)	(delete)
	Successful	C1	Central	ICMP		0.000	N	2	(edit)	(delete)
	Successful	C1	SW-2	ICMP		0.000	N	3	(edit)	(delete)
	Successful	C1	SW-B	ICMP		0.000	N	4	(edit)	(delete)

Part 4: Enable the Management PC to Access Router R1
Step 1: Enable a new subinterface on router R1.

a. Create subinterface Fa0/0.3 and set encapsulation to dot1q 20 to account for VLAN 20.
R1(config)# **interface fa0/0.3**
R1(config-subif)# **encapsulation dot1q 20**

b. Assign an IP address within the 192.168.20.0/24 network.
R1(config)# **interface fa0/0.3**
R1(config-subif)# **ip address 192.168.20.100 255.255.255.0**

Step 2: Verify connectivity between the management PC and R1.
Be sure to configure the default gateway on the management PC to allow for connectivity.



Step 3: Enable security.

While the management PC must be able to access the router, no other PC should be able to access the management VLAN.

a. Create an ACL that denies any network from accessing the 192.168.20.0/24 network, but permits all other networks to access one another.

Example: (may vary from student configuration)

R1(config)# **access-list 101 deny ip any 192.168.20.0 0.0.0.255**

R1(config)# **access-list 101 permit ip any any**

b. Apply the ACL to the proper interface(s).

Example: (may vary from student configuration)

R1(config)# **interface fa0/0.1**

R1(config-subif)# **ip access-group 101 in** R1(config-subif)# **interface fa0/0.2**

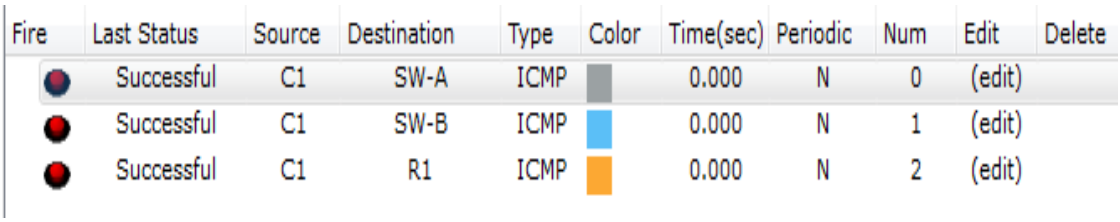
R1(config-subif)# **ip access-group 101 in**

Note: There are multiple ways in which an ACL can be created to accomplish the necessary security. For this reason, grading on this portion of the activity is based on the correct connectivity requirements. The management PC must be able to connect to all switches and the router. All other PCs should not be able to connect to any devices within the management VLAN.

Step 4: Verify security.

a. From the management PC, ping **SW-A**, **SW-B**, and **R1**. Were the pings successful? Explain.

The pings should have been successful because all devices within the 192.168.20.0 network should be able to ping one another. Devices within VLAN20 are not required to route through the router.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	C1	SW-A	ICMP		0.000	N	0	(edit)	
	Successful	C1	SW-B	ICMP		0.000	N	1	(edit)	
	Successful	C1	R1	ICMP		0.000	N	2	(edit)	

PC>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

Reply from 192.168.20.1: bytes=32 time=1ms TTL=255
Reply from 192.168.20.1: bytes=32 time=0ms TTL=255
Reply from 192.168.20.1: bytes=32 time=0ms TTL=255
Reply from 192.168.20.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.20.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time=1ms TTL=255
Reply from 192.168.20.2: bytes=32 time=1ms TTL=255
Reply from 192.168.20.2: bytes=32 time=1ms TTL=255
Reply from 192.168.20.2: bytes=32 time=12ms TTL=255

Ping statistics for 192.168.20.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 12ms, Average = 3ms

PC>ping 192.168.20.100

Pinging 192.168.20.100 with 32 bytes of data:

Reply from 192.168.20.100: bytes=32 time=1ms TTL=255
Reply from 192.168.20.100: bytes=32 time=0ms TTL=255
Reply from 192.168.20.100: bytes=32 time=0ms TTL=255
Reply from 192.168.20.100: bytes=32 time=0ms TTL=255

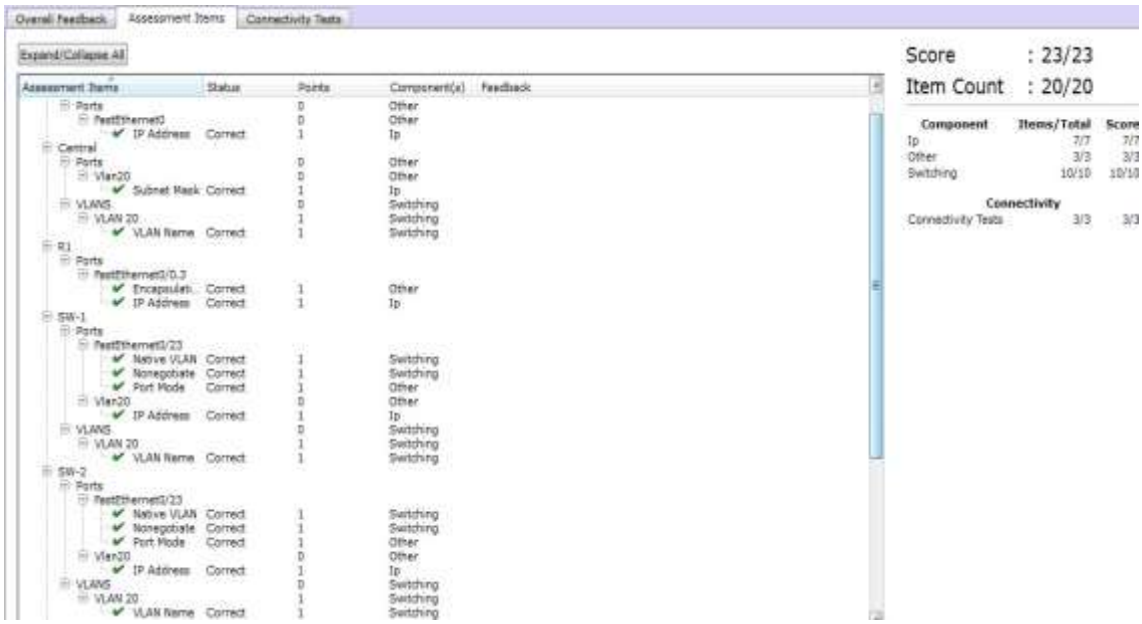
Ping statistics for 192.168.20.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>

b. From **D1**, ping the management PC. Were the pings successful? Explain.
The ping should have failed. This is because in order for a device within a different VLAN to successfully ping a device within VLAN20, it must be routed. The router has an ACL that prevents all packets from accessing the 192.168.20.0 network.

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.20.6

Pinging 192.168.20.6 with 32 bytes of data:

Reply from 192.168.5.100: Destination host unreachable.
Reply from 192.168.5.100: Destination host unreachable.
Reply from 192.168.5.100: Destination host unreachable.
Reply from 192.168.5.100: Destination host unreachable.

Ping statistics for 192.168.20.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Step 5: Check results.
Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed. If all components appear to be correct and the activity still shows incomplete, it could be due to the connectivity tests that verify the ACL operation.



!!! Script for SW-1
conf t
interface fa0/23
switchport mode trunk
switchport trunk native vlan 15
switchport nonegotiate
no shutdown vlan 20
exit interface vlan 20
ip address 192.168.20.3 255.255.255.0
!!! Script for SW-2
conf t
interface fa0/23
switchport mode trunk
switchport trunk native vlan 15
switchport nonegotiate
no shutdown vlan 20
exit interface vlan 20
ip address 192.168.20.4 255.255.255.0
!!! Script for SW-A
conf t vlan 20
exit interface vlan 20
ip address 192.168.20.1 255.255.255.0 interface fa0/1
switchport access vlan 20
no shutdown
!!! Script for SW-B
conf t vlan 20
exit interface vlan 20

ip address 192.168.20.2 255.255.255.0
!!! Script for Central
conf t vlan 20
exit interface vlan 20
ip address 192.168.20.5 255.255.255.0
!!! Script for R1
conf t
interface fa0/0.3
encapsulation dot1q 20
ip address 192.168.20.100 255.255.255.0
access-list 101 deny ip any 192.168.20.0 0.0.0.255
access-list 101 permit ip any any
interface FastEthernet0/0.1
ip access-group 101 in
interface FastEthernet0/0.2
ip access-group 101 in

CONCLUSIONES

- Se comprendió los dispositivos y servicios utilizados para apoyar las comunicaciones en las redes de datos e Internet.
- Se describió la función de capas de protocolo en redes de datos.
- comprendí la importancia de direccionamiento y denominación esquemas en varias capas de redes de datos en entornos IPv4 e IPv6
- se explicó los conceptos de Ethernet fundamentales como los medios de comunicación, servicios, y operaciones.
- .se manejó las utilidades de red más comunes para verificar las operaciones de pequeña red y analizar el tráfico de datos.

BIBLIOGRAFÍA

Entorno de conocimiento del DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN).