UNIVERSIDAD EIA

Administración de Redes

Simulación # 3

OBJETIVOS DE APRENDIZAJE:

- Borrar una configuración existente en un switch.
- Verificar la configuración predeterminada del switch.
- Crear una configuración básica de switch.
- Administrar la tabla de direcciones MAC.
- Configurar la seguridad de puertos.

DIAGRAMA DE TOPOLOGÍA:

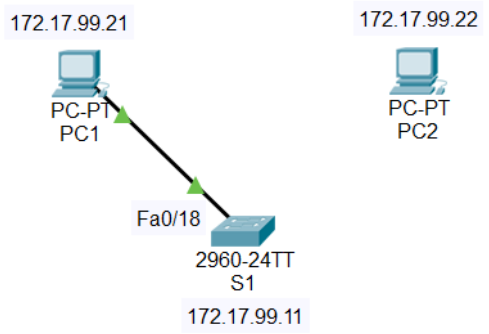

Figura 1 Diagrama de Topología

TABLA DE DIRECCIONAMIENTO:

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway Predeterminado
PC1	NIC	172.17.99.21	255.255.255.0	172.17.99.1
PC2	NIC	172.17.99.22	255.255.255.0	172.17.99.1
S1	VLAN 99	172.17.99.11	255.255.255.0	172.17.99.1

INTRODUCCIÓN:

En esta actividad se examinará y configurará un switch de LAN independiente. Pese a que el switch realiza funciones básicas en su estado predeterminado de manera no convencional, existe una cantidad de parámetros que un administrador de red debe modificar para garantizar una LAN segura y optimizada. Esta actividad presenta los conceptos básicos de la configuración del switch. Es necesario que responda todas las preguntas mientras vaya efectuando la simulación.

TAREA 1: Borrar una configuración existente en un switch

Paso 1. Ingrese al modo EXEC privilegiado escribiendo el comando enable.
Haga clic en S1 y luego en la pestaña **CLI**. Ejecute el comando **enable** para ingresar al modo EXEC privilegiado.

```
Switch>enable
Switch#
```

Paso 2. Elimine el archivo de información de la base de datos de la VLAN.
La información de la base de datos de la VLAN se almacena por separado de los archivos de configuración de vlan.dat in flash. Para eliminar el archivo de la VLAN, ejecute el comando **delete flash:vlan.dat**.

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

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

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

Paso 4. Verifique que la información de la VLAN se haya eliminado.
Verifique que la configuración de la VLAN se haya eliminado utilizando el comando **show vlan**.

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

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 enet  101002     1500  -      -      -        -    -        0      0
1003 enet  101003     1500  -      -      -        -    -        0      0
1004 enet  101004     1500  -      -      -        -    -        0      0
1005 enet  101005     1500  -      -      -        -    -        0      0
```

La información de la VLAN aún se encuentra en el switch. Siga el próximo paso para borrarla.

Paso 5. Vuelva a cargar el switch.
En el indicador del modo EXEC privilegiado, introduzca el comando **reload** para comenzar el proceso.

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

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

<se omite el resultado>

Press RETURN to get started! [Intro]

Switch>
```

TAREA 2: Verificar la configuración predeterminada del switch

Paso 1. Ingrese al modo privilegiado.
Puede acceder a todos los comandos del switch en modo privilegiado. Sin embargo, dado que muchos de los comandos privilegiados configuran parámetros operativos, el acceso privilegiado se debe proteger con una contraseña para evitar el uso no autorizado. El conjunto de comandos privilegiados incluye aquellos comandos incluidos en el modo EXEC del usuario, así como también el comando **configure** a través del cual se obtiene acceso a los modos de comandos restantes.

```
Switch>enable
Switch#
```

Observe que el indicador cambia en la configuración para reflejar el modo EXEC privilegiado.

Paso 2. Examine la configuración actual del switch.

a. Examine la configuración en ejecución actual con el comando **show running-config**.
   i. ¿Cuántas interfaces Fast Ethernet tiene el switch?
   ii. ¿Cuántas interfaces Gigabit Ethernet tiene el switch?
   iii. ¿Cuál es el rango de valores que se muestra para las líneas vty?

b. Examine el contenido actual de la NVRAM con el comando **show startup-config**.
   i. ¿Por qué el switch emite esta respuesta?

c. Examine las características de la interfaz virtual VLAN1 con el comando **show interface vlan1**.
   i. ¿Hay una dirección IP establecida en el switch?
   ii. ¿Cuál es la dirección MAC de esta interfaz virtual del switch?
   iii. ¿Está activa esta interfaz?

d. Ahora visualice las propiedades de la dirección IP de la interfaz con el comando **show ip interface vlan1**.
   i. ¿Qué resultado ve?

Paso 3. Muestre la información del IOS de Cisco.

a. Muestre la información del IOS de Cisco con el comando **show version**
   i. ¿Cuál es la versión del IOS de Cisco que está ejecutando el switch?
   ii. ¿Cuál es el nombre del archivo de imagen del sistema?
   iii. ¿Cuál es la dirección MAC base de este switch?

Paso 4. Examine las interfaces Fast Ethernet.

a. Examine las propiedades predeterminadas de la interfaz Fast Ethernet que utiliza PC1 con el comando **show interface fastethernet 0/18**.

```
Switch#show interface fastethernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Lance, address is 0090.2bae.7412 (bia 0090.2bae.7412)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s

<Se omite el resultado>
```

i. ¿La interfaz está activa o desactivada?
ii. ¿Qué haría que una interfaz se active?
iii. ¿Cuál es la dirección MAC de la interfaz?
iv. ¿Cuál es la configuración de velocidad y de dúplex de la interfaz?

Paso 5. Examine la información de la VLAN.

a. Examine la configuración VLAN predeterminada del switch con el comando **show vlan**.
   i. ¿Cuál es el nombre de la VLAN 1?
   ii. ¿Qué puertos hay en esta VLAN?
   iii. ¿La VLAN 1 está activa?
   iv. ¿Qué tipo de VLAN es la VLAN predeterminada?

Paso 6. Examine la memoria flash.

a. Hay dos comandos para analizar la memoria flash:
   dir flash: o
   show flash

   Ejecute uno de los dos comandos para examinar el contenido del directorio flash.
   i. ¿Qué archivos o directorios se encuentran?
   ii. Los archivos poseen una extensión, como .bin, al final del nombre del archivo. Los directorios no tienen una extensión de archivo. ¿Cuál es el nombre del archivo de imagen del IOS de Cisco?

Paso 7. Examine y guarde el archivo de configuración de inicio.

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

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

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

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

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

TAREA 3: Crear una configuración básica del switch

Paso 1. Asigne un nombre al switch.

Ingrese al modo de configuración global. El modo de configuración le permite administrar el switch. Ingrese los comandos de configuración, uno en cada línea. Observe que el indicador de la línea de comandos cambia para reflejar el indicador actual y el nombre del switch. En el último paso de la tarea anterior, usted configuró el nombre de host. Lo siguiente es un repaso de los comandos que se utilizan.

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

Paso 2. Configure las contraseñas de acceso.

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

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

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

Paso 3. Configure las contraseñas del modo de comando.

Establezca la contraseña secreta de enable como clase.

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

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

Configure la dirección IP del switch en 172.17.99.11 con una máscara de subred de 255.255.255.0 en la interfaz virtual interna VLAN 99. La VLAN se debe crear primero en el switch antes de que se pueda asignar la dirección.

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

Paso 5. Asigne puertos al switch VLAN.
Asigne Fastethernet 0/1, 0/8 y 0/18 a los puertos de VLAN 99.

```
S1(config)#interface fa0/1
S1(config-if)#switchport access vlan 99
S1(config)#interface fa0/8
S1(config-if)#switchport access vlan 99
S1(config)#interface fa0/18
S1(config-if)#switchport access vlan 99
S1(config-if)#exit
```

Paso 6. Configure el gateway predeterminado del switch.
S1 es un switch de Capa 2, por lo tanto, toma decisiones de envío según el encabezado de la Capa 2. Si se conectan múltiples redes a un switch, es necesario que especifique cómo el switch envía las tramas de internetwork, ya que la ruta se debe determinar en la Capa tres. Esto se logra especificando una dirección de gateway predeterminado que apunta a un router o un switch de Capa 3. Aunque esta actividad no incluye un gateway IP externo, se debe tener en cuenta que finalmente usted conectará la LAN a un router para tener acceso externo. Si suponemos que la interfaz de LAN en el router es 172.17.99.1, configure el gateway predeterminado para el switch.

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

Paso 7. Verifique las configuraciones de administración de las LAN.
Verifique las configuraciones de interfaz en la VLAN 99 con el comando **show interface vlan 99**.

```
S1#show interface vlan 99
Vlan99 is up, line protocol is up
  Hardware is CPU Interface, address is 0030.f2e2.5472 (bia 0060.47ac.1eb8)
  Internet address is 172.17.99.11/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo

<se omite el resultado>
```

¿Cuál es el ancho de banda en esta interfaz?

¿Cuál es la estrategia para formar las colas?

Paso 8. Configure la dirección IP y el gateway predeterminado para PC1.
Configure la dirección IP de PC1 en 172.17.99.21 con una máscara de subred de 255.255.255.0. Configure un gateway predeterminado de 172.17.99.1. Haga clic en PC1 y en la ficha **Escritorio**, luego en Configuración IP para introducir los parámetros de direccionamiento.

Paso 9. Verifique la conectividad.
Para verificar que los hosts y los switches estén configurados correctamente, haga ping en el switch desde PC1. Si el ping no es exitoso, resuelva los problemas de configuración del switch y del host. Tenga en cuenta que esto puede requerir de varios intentos para que los pings tengan éxito.

Paso 10. Configure la velocidad del puerto y la configuración de dúplex para una interfaz Fast Ethernet.
Realice la configuración de velocidad y dúplex en Fast Ethernet 0/18. Utilice el comando **end** para regresar al modo EXEC privilegiado al finalizar.

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

El valor predeterminado de la interfaz Ethernet del switch es de detección automática, de manera que prepara automáticamente las configuraciones óptimas. Debe establecer el modo dúplex y la velocidad manualmente sólo si un puerto debe funcionar a una cierta velocidad y en modo dúplex. Configurar puertos en forma manual puede conducir a una falta de concordancia en el dúplex, lo que puede disminuir el rendimiento en forma significativa.

Observe cómo se cerró el enlace entre PC1 y S1. Elimine los comandos **speed 100** y **duplex full**. Ahora verifique las configuraciones de la interfaz Fast Ethernet con el comando **show interface fa0/18**.

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

Paso 11. Guarde la configuración.
Usted ha completado la configuración básica del switch. Haga ahora una copia de seguridad del archivo de configuración en ejecución en la NVRAM para asegurarse de no perder los cambios realizados si el sistema se reinicia o se apaga.

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

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

Paso 12. Examine el archivo de configuración de inicio.
Para ver la configuración guardada en la NVRAM, ejecute el comando **show startup-config** en el modo EXEC privilegiado (modo enable).

¿Todos los cambios realizados están grabados en el archivo?

TAREA 4: Administrar la tabla de direcciones MAC

Paso 1. Anote las direcciones MAC de los hosts.
Determine y anote las direcciones de la Capa 2 (física) de las tarjetas de interfaz de red de la PC utilizando los siguientes pasos:

- Haga clic en la PC.
- Seleccione la ficha **Escritorio**.
- Haga clic en **Indicador del sistema**.
- Escriba el comando **ipconfig /all**.

Paso 2. Determine las direcciones MAC que el switch ha adquirido.
Muestre las direcciones MAC con el comando **show mac-address-table** en el modo EXEC privilegiado. Si no hay direcciones MAC; haga ping desde PC1 a S1 y luego verifique nuevamente.

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

Paso 3. Borre la tabla de direcciones MAC.
Para quitar las direcciones MAC existentes, utilice el comando **clear mac-address-table dynamic** en el modo EXEC privilegiado.

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

Paso 4.Verifique los resultados.
Verifique que la tabla de direcciones MAC se haya eliminado.

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

Paso 5. Examine de nuevo la tabla MAC.
Observe la tabla de direcciones MAC en el modo EXEC privilegiado otra vez. La tabla no ha cambiado, haga ping en S1 desde PC1 y verifique nuevamente.

Paso 6. Configure una dirección MAC estática.
Para especificar a qué puertos se puede conectar un host, una posibilidad es crear una asignación estática de la dirección MAC del host a un puerto.

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

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

Paso 7. Verifique los resultados.
Verifique las entradas de la tabla de direcciones MAC.

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

Paso 8. Elimine la entrada MAC estática.
Ingrese al modo de configuración y elimine la MAC estática colocando un **no** frente a la cadena de comandos.

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

Paso 9. Verifique los resultados.
Verifique que la dirección MAC estática se haya borrado con el comando **show mac-address-table static**.

TAREA 5: Configurar la seguridad del puerto

Paso 1. Configure un segundo host.
Se necesita un segundo host para esta tarea. Establezca la dirección IP de PC2 en 172.17.99.22, con una máscara de subred de 255.255.255.0 y un gateway predeterminado de 172.17.99.1. No conecte todavía esta PC al switch.

Paso 2. Verifique la conectividad.
Verifique que PC1 y el switch estén correctamente configurados haciendo ping a la dirección IP de la VLAN 99 del switch desde el host. Si los pings no tienen éxito, resuelva los problemas de configuración del switch y del host.

Paso 3. Determine las direcciones MAC que el switch ha adquirido.
Muestre las direcciones MAC aprendidas con el comando **show mac-address-table** en el modo EXEC privilegiado.

Paso 4. Enumere las opciones de seguridad de los puertos.
Explore las opciones para configurar la seguridad de los puertos en la interfaz Fast Ethernet 0/18.

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

Paso 5. Configure la seguridad de los puertos en un puerto de acceso.
Configure el puerto del switch Fast Ethernet 0/18 para que acepte sólo dos dispositivos para que aprenda las direcciones MAC de esos dispositivos en forma dinámica y para que desactive el puerto en caso de violación.

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

Paso 6. Verifique los resultados.
Muestre las configuraciones de seguridad del puerto con el comando **show port-security interface fa0/18**.

¿Cuántas direcciones seguras están permitidas en Fast Ethernet 0/18?
¿Qué medida de seguridad debe tomarse para este puerto?

Paso 7. Examine el archivo de configuración en ejecución.

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

¿Hay afirmaciones enumeradas que reflejan directamente la implementación de seguridad de la configuración en ejecución?

Paso 8. Modifique las configuraciones de seguridad de los puertos en un puerto.

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

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

Paso 9. Verifique los resultados.

Muestre las configuraciones de seguridad de los puertos con el comando **show port-security interface fa0/18**.

¿Reflejan las configuraciones de seguridad de los puertos las modificaciones del Paso 8?

Haga ping en la dirección VLAN99 del switch desde PC1 para verificar la conectividad y actualizar la tabla de direcciones MAC.

Paso 10. Introduzca un host malicioso.

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

¿Qué sucedió cuando intentó hacer ping en S1?

Nota: La convergencia puede tardar hasta un minuto. Cambie entre el modo **simulación** y **tiempo real** para acelerar este proceso.

Paso 11. Reactive el puerto.

Mientras el host no autorizado esté conectado a Fast Ethernet 0/18, no puede haber tráfico entre el host y el switch. Vuelva a conectar PC1 a Fast Ethernet 0/18 e ingrese los siguientes comandos en el switch para reactivar el puerto:

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

Paso 12. Verifique la conectividad.

Después de la convergencia, PC1 debe estar en condiciones de hacer ping nuevamente en S1.

PRÁCTICA FINALIZADA. GUARDE LA SIMULACIÓN.

NOTA: Práctica basada en CCNA EXPLORATION, 2010