TALLER 2.

CONFIGURACIÓN BÁSICA SEGURIDAD SWITCH

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

LUIS MIGUEL POLO – 20182020158

NICOLÁS DAVID SABOGAL – 20202020008

LUIS SEBASTIAN MARTINEZ GUERRERO - 20191005153

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

INGENIERÍA DE SISTEMAS

REDES DE COMUNICACIONES III

PAULO ALONSO GAONA GARCIA

2024-III

INTRODUCCIÓN

El objetivo del siguiente taller es configurar y verificar características de seguridad en un switch de red. Esto incluye la configuración de acceso seguro mediante SSH, la seguridad de los puertos para controlar las direcciones MAC permitidas, y la desactivación de servicios no seguros como HTTP. Además, se busca proteger los puertos no utilizados y garantizar que el switch solo permita conexiones autorizadas, mejorando así la seguridad de la red.

OBJETIVOS

- Configurar la topología e inicializar los dispositivos.
- Configurar parámetros básicos de los dispositivos y verificar la conectividad.
- Configurar y verificar el acceso por SSH en S1.
- Configurar y verificar las características de seguridad en S1.

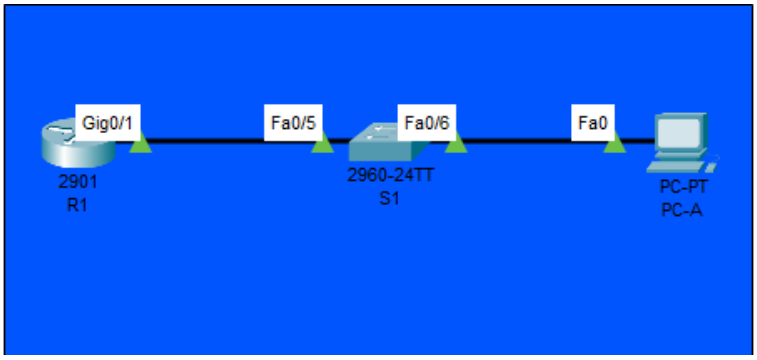
DESARROLLO

Parte 1: Establecer la topología e inicializar los dispositivos

En la parte 1, establecerá la topología de la red y borrará cualquier configuración, si fuera necesario.

Paso 1: Seleccionar los medios físicos de red tal como se muestra en la topología

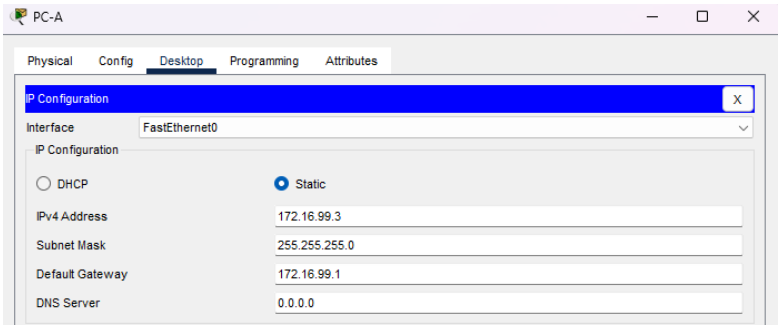
Paso 2: *Iniciar router y el switch*



Parte 2: Configurar los parámetros básicos de los dispositivos y verificar la conectividad

En la Parte 2, configurará los ajustes básicos en el router, el switch y la PC. Consulte la topología y la tabla de direccionamiento incluidos al comienzo de esta práctica para conocer los nombres de los dispositivos y obtener información de direcciones.

Paso 1: Configurar una dirección IP en la PC-A Consulte la tabla de direcciones para obtener la información sobre las direcciones IP.



Paso 2: Configurar los parámetros básicos en el R1

a. Abra la consola de R1 y entre en el modo de configuración global.
b. Copie la siguiente configuración básica y péguela en la configuración en ejecución en el R1.

```
no ip domain-lookup
hostname R1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0 password cisco
login
logging synchronous
line vty 0 4
password cisco
login
interface g0/1
 ip address 172.16.99.1 255.255.255.0
 no shutdown
end
```

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#service password-encryption
R1(config)#enable secret class
R1(config)#banner motd #Unauthorized access is strictly prohibited.#
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#interface g0/1
R1(config-if)#ip address 172.16.99.1 255.255.255.0
R1(config-if)#no shutdown

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

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

c. Guarde la configuración en ejecución en la configuración de inicio.

```
R1#wr
Building configuration...
[OK]
```

Paso 3: Configurar los parámetros básicos en el S1

a. Abra la consola en el S1 e ingrese en el modo de configuración global.
b. Copie la siguiente configuración básica y péguela en la configuración en ejecución en el S1

```
no ip domain-lookup
hostname S1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
Exit
```

```
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#service password-encryption
S1(config)#enable secret class
S1(config)#banner motd #Unauthorized access is strictly prohibited.#
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#logging synchronous
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```

Pregunta. Qué significa comando no ip domain-lookup

Rta: Desactiva la traducción de nombres de dominio, por lo que evita que el dispositivo (Router o Switch) trate de resolver si el comando ejecutado existe o no.

c. Cree la VLAN 99 en el switch y asígnele el nombre Management.
S1(config)# vlan 99

```
S1(config-vlan)# name Administracion
S1(config-vlan)# exit
S1(config)#
```

d. Configure la dirección IP de la interfaz de administración VLAN 99, tal como se muestra en la tabla de direccionamiento, y habilite la interfaz.
S1(config)# interface vlan 99

```
S1(config-if)# ip address 172.16.99.11 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
S1#
```

```
S1(config)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#exit
S1(config)#interface vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#ip add 172.16.99.11 255.255.255.0
S1(config-if)#no sh
S1(config-if)#end
S1#
%SYS-5-CONFIG I: Configured from console by console
```

e. Emita el comando show vlan en el S1. ¿Cuál es el estado de laVLAN 99? **Rta:** Activo

```
S1#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
99   Administracion                    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
99   enet  100099     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
```

f. Emita el comando show ip interface brief en el S1. ¿Cuál es el estado y el protocolo para la interfaz de administración VLAN 99? **Rta:** Estado: Up; Protocol : Down.

```
Vlan1                  unassigned      YES manual administratively down down
Vlan99                 172.16.99.11    YES manual up                    down
```

¿Por qué el protocolo figura como down, a pesar de que usted emitió el comando no shutdown para la interfaz VLAN 99? **Rta:** Porque hasta el momento no hay puertos fisicos asignados a la VLAN 99.

Paso 4: Verificar la conectividad entre los dispositivos

a. En la PC-A, haga ping a la dirección de gateway predeterminado en el R1. ¿Los pings se realizaron correctamente? Si, fueron satisfactorios.

```
C:\>ping 172.16.99.1

Pinging 172.16.99.1 with 32 bytes of data:

Reply from 172.16.99.1: bytes=32 time=16ms TTL=255
Reply from 172.16.99.1: bytes=32 time<1ms TTL=255
Reply from 172.16.99.1: bytes=32 time<1ms TTL=255
Reply from 172.16.99.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.99.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 16ms, Average = 4ms
```

b. En la PC-A, abra un navegador web y acceda a http://172.16.99.11. Si se le solicita un nombre de usuario y contraseña, deje el nombre de usuario en blanco y use class como contraseña.
c. Se le solicita una conexión segura?, SI, NO, Porque?
d. Cierre el navegador.

Nota: La interfaz web no segura (servidor HTTP) en un switch Cisco 2960 está habilitada de manera predeterminada. Una medida de seguridad frecuente es deshabilitar este servicio, tal como se describe en la parte 4.

Parte 3: Configurar y verificar el acceso por SSH en el S1

Paso 1: Configurar el acceso por SSH en el S1

a. Habilite SSH en el S1. En el modo de configuración global, cree el nombre de dominio CCNA-Lab.com.

S1(config)# ip domain-name CCNA-Lab.com

b. Cree una entrada en la base de datos de usuarios local para que se utilice al conectarse al switch a través de SSH. El usuario debe tener acceso de nivel de administrador.

Nota: La contraseña que se utiliza aquí NO es una contraseña segura. Simplemente se usa a los efectos de esta práctica de laboratorio.

```
S1(config)# username admin privilege 15 secret sshadmin
```

c. Configure la entrada de transporte para que las líneas vty permitan solo conexiones SSH y utilicen la base de datos local para la autenticación.

```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
```

```
S1(config)#ip domain-name CCNA-Lab.com
S1(config)#username admin privilege 15 secret sshadmin
S1(config)#line vty 0 15
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#exit
```

d. Genere una clave criptográfica RSA con un módulo de 1024 bits.

```
S1(config)# crypto key generate rsa modulus 1024
S1(config)#
S1(config)# end
```

```
S1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: S1.CCNA-Lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:21:9.253: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#
```

e. Verifique la configuración de SSH.

S1# show ip ssh Copie la configuración

```
S1#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
```

¿Qué versión de SSH usa el switch? **Rta:** La 1.99

¿Cuántos intentos de autenticación permite SSH? **Rta:** 3 intentos

¿Cuál es la configuración predeterminada de tiempo de espera para SSH? **Rta:** 120 segundos

Paso 2: Modificar la configuración de SSH en el S1 Modifique la configuración predeterminada de SSH.

```
S1# config t
S1(config)# ip ssh time-out 75
```

```
S1(config)# ip ssh authentication-retries 2
S1# show ip ssh
```

Copie la configuración

```
S1(config)#ip ssh time-out 75
S1(config)#ip ssh authentication-retries 2
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 75 secs; Authentication retries: 2
```

¿Cuántos intentos de autenticación permite SSH? **Rta:** 2 intentos

¿Cuál es la configuración de tiempo de espera para SSH? **Rta:** 75 segundos

Paso 3: *Verificar la configuración de SSH en el S1*

a. Utilice el software de cliente SSH en PC-A (como Tera Term) para abrir una conexión SSH a S1. Si recibe un mensaje en el cliente SSH con respecto a la clave de host, acéptela. Inicie sesión con admin como nombre de usuario y sshadmin como contraseña.

¿La conexión se realizó correctamente? **Rta:** Sí, se realizó correctamente.

¿Qué petición de entrada se mostró en el S1? ¿Por qué? **Rta:** No se muestra porque la conexión SSH es independiente de la línea de comandos 0, que se muestra en el CLI de S1.

b. Escriba exit para finalizar la sesión de SSH en el S1.

Parte 4: Configurar y verificar las características de seguridad en el S1

En la parte 4, desactivará los puertos sin utilizar, desactivará determinados servicios que se ejecutan en el switch y configurará la seguridad de puertos según las direcciones MAC. Los switches pueden estar sujetos a ataques de desbordamiento de la tabla de direcciones MAC, a ataques de suplantación de direcciones MAC y a conexiones no autorizadas a los puertos del switch. Configurará la seguridad de puertos para limitar la cantidad de direcciones MAC que se pueden detectar en un puerto del switch y para deshabilitar el puerto si se supera ese número.

Paso 1: *Configurar las características de seguridad general en el S1*

a. Cambie el mensaje del día (MOTD) en el S1 a: “El acceso no autorizado queda terminantemente prohibido. Los infractores serán procesados con todo el rigor de la ley”.

```
S1(config)#banner motd #El acceso no autorizado queda terminantemente prohibido.Los
infractores seran procesados con todo el rigor de la ley#
```

b. Emita un comando show ip interface brief en el S1. ¿Qué puertos físicos están activos? **Rta:** FastEthernet0/5 , FastEthernet0/6 y Vlan99.

c. Desactive todos los puertos sin utilizar en el switch. Use el comando interface range.

```
S1(config)# interface range f0/1 – 4
S1(config-if-range)# shutdown
S1(config-if-range)# interface range f0/7 – 24
S1(config-if-range)# shutdown
S1(config-if-range)# interface range g0/1 – 2
S1(config-if-range)# shutdown S1(config-if-range)# end
S1#
```

```
S1(config)#interface range f0/1 - 4
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
S1(config-if-range)#interface range f0/7 - 24
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
```

d. Emita el comando show ip interface brief en el S1. ¿Cuál es el estado de los puertos F0/1 a F0/4? **Rta:** administratively down

```
S1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual administratively down down
FastEthernet0/2        unassigned      YES manual administratively down down
FastEthernet0/3        unassigned      YES manual administratively down down
FastEthernet0/4        unassigned      YES manual administratively down down
```

e. Emita el comando show ip http server status.

```
S1# show ip http server status
```

copie configuración

¿Cuál es el estado del servidor HTTP?

¿Qué puerto del servidor utiliza?

¿Cuál es el estado del servidor seguro de HTTP?

¿Qué puerto del servidor seguro utiliza?

f. Las sesiones HTTP envían todo como texto no cifrado. Deshabilite el servicio HTTP que se ejecuta en el S1.

S1(config)# no ip http server

g. En la PC-A, abra un navegador web y acceda a http://172.16.99.11. ¿Cuál fue el resultado?

h. Desde PC-A, abra un navegador web y vaya a https://172.16.99.11. Acepte el certificado. Inicie sesión sin nombre de usuario y con la contraseña class. ¿Cuál fue el resultado?

I. Cierre el navegador web.

Paso 2: Configurar y verificar la seguridad de puertos en el S1

a. Registre la dirección MAC de G0/1 del R1. Desde la CLI del R1, use el comando show interface g0/1 y registre la dirección MAC de la interfaz.

R1# show interface g0/1
Copie resultado

```
R1#show interface g0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 0001.64d8.0702 (bia 0001.64d8.0702)
  Internet address is 172.16.99.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     8 packets input, 400 bytes, 0 no buffer
     Received 8 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 1017 multicast, 0 pause input
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

¿Cuál es la dirección MAC de la interfaz G0/1 del R1? **Rta:** 0001.64d8.0702.

b. Desde la CLI del S1, emita un comando show mac address-table en el modo EXEC privilegiado. Busque las entradas dinámicas de los puertos F0/5 y F0/6. Regístrelos a continuación.

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

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

   1    0001.64d8.0702    DYNAMIC     Fa0/5
   1    0030.f21a.0242    DYNAMIC     Fa0/6
```

Dirección MAC de F0/5: **Rta:** 0001.64d8.0702

Dirección MAC de F0/6: **Rta:** 0030.f21a.0242

c. Configure la seguridad básica de los puertos.

Nota: Normalmente, este procedimiento se realizaría en todos los puertos de acceso en el switch. Aquí se muestra F0/5 como ejemplo.

1) Desde la CLI del S1, ingrese al modo de configuración de interfaz para el puerto que se conecta al R1.

```
S1(config)# interface f0/5
```

2) Desactive el puerto.

```
S1(config-if)# shutdown
```

3) Habilite la seguridad de puertos en F0/5.

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

Nota: La introducción del comando switchport port-security establece la cantidad máxima de direcciones MAC en 1 y la acción de violación en shutdown. Los comandos switchport port-security maximum y switchport port-security violation se pueden usar para cambiar el comportamiento predeterminado.

4) Configure una entrada estática para la dirección MAC de la interfaz G0/1 del R1 registrada en el paso 2ª.

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

(xxxx.xxxx.xxxx es la dirección MAC real de la interfaz G0/1 del router)

Nota: De manera optativa, puede usar el comando switchport port-security mac-address sticky para agregar todas las direcciones MAC seguras que se detectan dinámicamente en un puerto (hasta el máximo establecido) a la configuración en ejecución del switch.

5) Habilite el puerto del switch.

```
S1(config-if)# no shutdown
S1(config-if)# end
```

```
S1(config)#interface f0/5
S1(config-if)#switchport mode access
S1(config-if)#shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

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

S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security mac-address 0001.64d8.0702
S1(config-if)#no sh

S1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
```

d. Verifique la seguridad de puertos en F0/5 del S1 mediante la emisión de un comando show portsecurity interface.

```
S1# show port-security interface f0/5
```

Copie el resultado

```
S1#show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0001.64D8.0702:1
Security Violation Count   : 0
```

¿Cuál es el estado del puerto de F0/5? **Rta:** Secure-up

e. En el símbolo del sistema del R1, haga ping a la PC-A para verificar la conectividad.

```
R1# ping 172.16.99.3
```

```
R1#ping 172.16.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

f. Ahora violará la seguridad mediante el cambio de la dirección MAC en la interfaz del router. Ingrese al modo de configuración de interfaz para G0/1 y desactívela.

```
R1# config t
R1(config)# interface g0/1
R1(config-if)# shutdown
```

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface g0/1
R1(config-if)#shutdown

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

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

g. Configure una nueva dirección MAC para la interfaz, con la dirección aaaa.bbbb.cccc.

```
R1(config-if)# mac-address aaaa.bbbb.cccc
```

h. De ser posible, tenga abierta una conexión de consola en S1 al mismo tiempo que lleva cabo los dos próximos pasos. Eventualmente verá mensajes en la conexión de la consola a S1 que indicarán una violación de seguridad. Habilite la interfaz G0/1 en R1.

```
R1(config-if)# no shutdown
```

R1

```
R1(config-if)#exit
R1(config)#interf g0/1
R1(config-if)#mac-address aaaa.bbbb.cccc
R1(config-if)#no sh

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

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

S1

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

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

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

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

El acceso no autorizado queda terminantemente prohibido.Los infractores seran procesados
con todo el rigor de la ley
```

i. Desde el modo EXEC privilegiado en el R1, haga ping a la PC-A. ¿El ping fue exitoso? ¿Por qué o por qué no? **Rta:** No fue exitoso porque S1 apagó el puerto cuando verificó la dirección MAC de la interfaz conectada a F0/5.

```
R1#ping 172.16.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

j. En el switch, verifique la seguridad de los puertos con los comandos siguientes.

`S1# show port-security`

Copie resultado

```
S1#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
------------------------------------------------------------------------
        Fa0/5        1           1                1          Shutdown
------------------------------------------------------------------------
S1#
```

`S1# show port-security interface f0/5`

Copie el resultado

```
S1#show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : AAAA.BBBB.CCCC:1
Security Violation Count   : 1
```

`S1# show interface f0/5`

Copie el resultado

```
S1#show interface f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Lance, address is 0001.9670.e105 (bia 0001.9670.e105)
 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
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
```

`S1# show port-security address`

Copie el resultado

```
S1#show port-security address
               Secure Mac Address Table
------------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    0001.64D8.0702    SecureConfigured              Fa0/5         -
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

k. En el router, desactive la interfaz G0/1, elimine la dirección MAC codificada de forma rígida del router y vuelva a habilitar la interfaz G0/1.

```
R1(config-if)# shutdown
R1(config-if)# no mac-address aaaa.bbbb.cccc
R1(config-if)# no shutdown
R1(config-if)# end
```

```
R1(config)#inter g0/1
R1(config-if)#sh

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

R1(config-if)#no mac-address aaaa.bbbb.cccc
R1(config-if)#no sh

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

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

l. Desde el R1, vuelva a hacer ping a la PC-A en 172.16.99.3. ¿El ping se realizó correctamente? **Rta:** No. El ping falló.

```
%SYS-5-CONFIG_I: Configured from console by console

R1#ping 172.16.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

m. En el switch, emita el comando show interface f0/5 para determinar la causa del fallo del ping. Registre sus conclusiones. **Rta:** La primera línea indica que la interfaz está desactivada, no de manera administrativa como sucede en las interfaces FastEthernet de la 0 a la 4, sino a causa de un error.

Copie el resultado

```
S1#show interface f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Lance, address is 0001.9670.e105 (bia 0001.9670.e105)
 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
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
     0 output errors, 0 collisions, 10 interface resets
```

n. Borre el estado de inhabilitación por errores de F0/5 en el S1.

```
S1# config t
S1(config)# interface f0/5
S1(config-if)# shutdown
S1(config-if)# no shutdown
```

```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#inter f0/5
S1(config-if)#sh

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down
S1(config-if)#no sh

S1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up

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

Nota: puede haber una demora mientras convergen los estados de los puertos.

o. Emita el comando show interface f0/5 en el S1 para verificar que F0/5 ya no esté en estado de inhabilitación por errores.

S1# show interface f0/5
Copie el resultado

```
S1#show interface f0/5
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Lance, address is 0001.9670.e105 (bia 0001.9670.e105)
 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
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
     0 output errors, 0 collisions, 10 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

p. En el símbolo del sistema del R1, vuelva a hacer ping a la PC-A. El ping debería realizarse correctamente.

```
R1#ping 172.16.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/1/5 ms
```

Reflexión

1. ¿Por qué habilitaría la seguridad de puertos en un switch?

   Previene accesos no autorizados donde un atacante podría conectar su equipo físicamente al switch a través de puertos usados. Por otro lado, también previene los ataques por MAC flooding, donde un Switch cuya tabla de direcciones MAC desbordada revierte su funcionamiento al de un Hub, lo que hace que el tráfico en los puertos sea visible.

2. ¿Por qué deben deshabilitarse los puertos no utilizados en un switch?

   Deshabilitar los puertos no utilizados en un switch es previene accesos físicos no autorizados mitigando posibles ataques. También mejora la eficiencia al optimizar el uso de recursos del switch y facilita la gestión al permitir un control más preciso sobre la infraestructura. Finalmente, también permite registrar y consultar intentos de acceso restringidos.

CONCLUSIONES

- Implementar seguridad de puertos, como la limitación de direcciones MAC y la respuesta a violaciones de seguridad, protege la red contra ataques y accesos no deseados.
- Configurar SSH y verificar su funcionamiento permite la administración segura de dispositivos de red, crucial para evitar accesos no autorizados y asegurar la administración remota.
- Deshabilitar puertos no utilizados ayuda a prevenir accesos no autorizados y mejora la seguridad física de la red.