



**INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO**



Administración de Servicios en Red

2.1 Configuración Switch

PROFESORA: Henestrosa Carrasco Leticia

Equipo 3

- Cruz Chávez Alan Francisco
- Gómez Salas Hugo Santiago
- Mendoza Rodríguez Israel
- Ramírez Galindo Karina

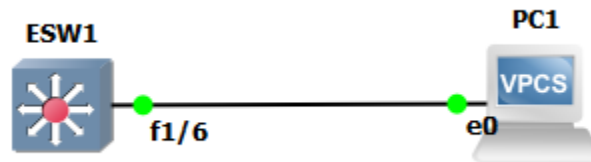
GRUPO: 4CV13

Contenido

Desarrollo	2
Topología	2
Tablas de direccionamiento	2
Objetivos	2
Aspectos básicos / situación	2
Configuración	3
Parte 1: Tender el cableado de red y verificar la configuración predeterminada del switch ..	3
Parte 2: Configurar parámetros básicos de los dispositivos de red	9
Parte 3: Verificación y prueba de la conectividad de red	13
Reflexión	17
Conclusiones:	18

Desarrollo

Topología



Tablas de direccionamiento

El administrador	Interfaces	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 99	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objetivos

Parte 1: Tender el cableado de red y verificar la configuración predeterminada del switch

Parte 2: Configurar parámetros básicos de los dispositivos de red

- Configure los parámetros básicos del switch.
- Configurar la dirección IP de la computadora.

Parte 3: Verificación y prueba de la conectividad de red

- Mostrar la configuración del dispositivo.
- probar la conectividad de extremo a extremo con ping.
- Probar las capacidades de administración remota con Telnet.
- guardar el archivo de configuración en ejecución del switch.

Aspectos básicos / situación

Los switches Cisco se pueden configurar con una dirección IP especial conocida como interfaz virtual de switch (SVI). La SVI, o dirección de administración, se puede usar para el acceso remoto al switch a fin de ver o configurar los ajustes. Si la SVI de la VLAN 1 tiene asignada una dirección IP, de manera predeterminada todos los puertos en la VLAN 1 tienen acceso a la dirección IP de la SVI.

En esta práctica de laboratorio, armará una topología simple mediante cableado LAN Ethernet y accederá a un switch Cisco utilizando los métodos de acceso de consola y remoto. Examinará la configuración predeterminada del switch antes de configurar los parámetros básicos del switch. Estos ajustes básicos de switch incluyen nombre del dispositivo, descripción de la interfaz, contraseñas locales,

mensaje del anuncio del día (MOTD), direcciones IP y dirección MAC estática. También demostrará el uso de una dirección IP de administración para la administración remota del switch. La topología consta de un switch y un host que solo usa puertos Ethernet y de consola.

Configuración

Parte 1: Tender el cableado de red y verificar la configuración predeterminada del switch

En la parte 1, establecerá la topología de la red y verificará la configuración predeterminada del switch.

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

Paso 2: Verificar la configuración predeterminada del switch.

En este paso, examinará la configuración predeterminada del switch, como la configuración actual del switch, la información de IOS, las propiedades de las interfaces, la información de la VLAN y la memoria flash.

Puede acceder a todos los comandos IOS del switch en el modo EXEC privilegiado. Se debe restringir el acceso al modo EXEC privilegiado con protección con contraseña para evitar el uso no autorizado, dado que proporciona acceso directo al modo de configuración global y a los comandos que se usan para configurar los parámetros de funcionamiento. Establecerá las contraseñas más adelante en esta práctica de laboratorio.

El conjunto de comandos del modo EXEC privilegiado incluye los comandos del modo EXEC del usuario y el comando `configure`, a través del cual se obtiene acceso a los modos de comando restantes. Use el comando `enable` para ingresar al modo EXEC privilegiado.

- a. Suponiendo que el switch no tenía almacenado un archivo de configuración en la memoria de acceso aleatorio no volátil (NVRAM), una conexión de consola mediante Tera Term u otro programa de emulación de terminales abrirá la línea de comandos del modo EXEC del usuario en el switch con el comienzo de línea `Switch>`. Use el comando **enable** para ingresar al modo EXEC privilegiado.

```
Switch> enable
```

```
Switch#
```

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

Verifique que haya un archivo de configuración predeterminado limpio en el switch emitiendo el comando del modo EXEC con privilegios **show running-config**. Si se guardó un archivo de configuración anteriormente, se debe eliminar. Según cuál sea el modelo del switch y la versión de IOS, la configuración podría verse diferente. Sin embargo, no debería haber contraseñas ni direcciones IP configuradas. Si su switch no tiene una configuración predeterminada, borre y recargue el switch.

- b. Examine el archivo de configuración activa actual.

Switch# **show running-config**

```
ESW1#sh run
Building configuration...

Current configuration : 2927 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
no service dhcp
!
hostname ESW1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip routing
no ip icmp rate-limit unreachable
no ip cef
!
!
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
!
!
!
!
--More-- [ ]
```

```
!
macro name add_vlan
end
vlan database
vlan $v
exit
@
macro name del_vlan
end
vlan database
no vlan $v
exit
@@
!
!
vtp file nvram:vlan.dat
archive
  log config
  hidekeys
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
  description *** Unused for Layer2 EtherSwitch ***
  no ip address
  no ip route-cache
  shutdown
  duplex auto
  speed auto
!
interface FastEthernet0/1
  description *** Unused for Layer2 EtherSwitch ***
  --More-- [ ]
```

```
!  
interface FastEthernet1/0  
  duplex full  
  speed 100  
!  
interface FastEthernet1/1  
  duplex full  
  speed 100  
!  
interface FastEthernet1/2  
  duplex full  
  speed 100  
!  
interface FastEthernet1/3  
  duplex full  
  speed 100  
!  
interface FastEthernet1/4  
  duplex full  
  speed 100  
!  
interface FastEthernet1/5  
  duplex full  
  speed 100  
!  
interface FastEthernet1/6  
  duplex full  
  speed 100  
!  
interface FastEthernet1/7  
  duplex full  
  speed 100  
!  
interface FastEthernet1/8  
  duplex full  
  speed 100  
!  
--More--
```

```
interface FastEthernet1/9  
  duplex full  
  speed 100  
!  
interface FastEthernet1/10  
  duplex full  
  speed 100  
!  
interface FastEthernet1/11  
  duplex full  
  speed 100  
!  
interface FastEthernet1/12  
  duplex full  
  speed 100  
!  
interface FastEthernet1/13  
  duplex full  
  speed 100  
!  
interface FastEthernet1/14  
  duplex full  
  speed 100  
!  
interface FastEthernet1/15  
  duplex full  
  speed 100  
!  
interface Vlan1  
  no ip address  
  no ip route-cache  
  shutdown  
!  
ip forward-protocol nd  
!  
no ip http server  
--More--
```

- 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?

Porque por el momento el switch no tiene ninguna configuración

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

Switch# **show interface vlan1**

```
ESW1#show int vlan1
Vlan1 is administratively down, line protocol is down
  Hardware is EtherSVI, address is c401.1ce8.0000 (bia c401.1ce8.0000)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 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 never, 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
  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
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 2 interface resets
    0 output buffer failures, 0 output buffers swapped out
ESW1#
```

¿Hay alguna dirección IP asignada a VLAN 1? *Ninguna*

¿Cuál es la dirección MAC de esta SVI? *C401.1ce8.0000*

¿Está activa esta interfaz? *No*

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

Switch# **show ip interface vlan1**

```
ESW1#show ip int vlan1
Vlan1 is administratively down, line protocol is down
  Internet protocol processing disabled
ESW1#
```

¿Qué resultado ve?

Se observa que la interfaz VLAN no ha sido administrada

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

Switch# **show ip interface vlan1**

¿Qué resultado ve?

Se observa el mismo resultado que antes, la IP está sin administración

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

Switch# **show versión**

```

ESW1#sh version
Cisco IOS Software, 3700 Software (C3745-ADVIPSERVICESK9-M), Version 12.4(15)T6, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Mon 07-Jul-08 12:57 by prod_rel_team

ROM: ROMMON Emulation Microcode
ROM: 3700 Software (C3745-ADVIPSERVICESK9-M), Version 12.4(15)T6, RELEASE SOFTWARE (fc2)

ESW1 uptime is 6 minutes
System returned to ROM by unknown reload cause - suspect boot_data[BOOT_COUNT] 0x0, BOOT_COUNT 0, BOOTDATA 19
System image file is "tftp://255.255.255.255/unknown"

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/ww1/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 3745 (R7000) processor (revision 2.0) with 249856K/12288K bytes of memory.
Processor board ID FTX0945W0MY
R7000 CPU at 350MHz, Implementation 39, Rev 2.1, 256KB L2, 512KB L3 Cache
18 FastEthernet interfaces
DRAM configuration is 64 bits wide with parity enabled.
151K bytes of NVRAM.
1024K bytes of ATA System CompactFlash (Read/Write)

--More--

```

¿Cuál es la versión del IOS de Cisco que está ejecutando el switch?
12.4(15)T6

¿Cuál es el nombre del archivo de imagen del sistema? **C3725**

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

Switch# **show interface f0/6**

```

ESW1#show int Fa1/6
FastEthernet1/6 is up, line protocol is up
  Hardware is Fast Ethernet, address is c401.1ce8.f106 (bia c401.1ce8.f106)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, 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
  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
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
ESW1#

```


¿La interfaz está activa o inactiva? *Esta activada*

¿Qué haría que una interfaz se active? *Que tenga una conexión*

¿Cuál es la dirección MAC de la interfaz? *C401.1ce8.f106*

¿Cuál es la configuración de velocidad y de dúplex de la interfaz?
100Mb/s

- i. Examine la configuración VLAN predeterminada del switch.

Switch# **show vlan**

```
ESW1#sh vlan-switch
```

VLAN	Name	Status	Ports
1	default	active	Fa1/0, Fa1/1, Fa1/2, Fa1/3 Fa1/4, Fa1/5, Fa1/6, Fa1/7 Fa1/8, Fa1/9, Fa1/10, Fa1/11 Fa1/12, Fa1/13, Fa1/14, Fa1/15
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	-	-	-	-	-	1002	1003
1002	fddi	101002	1500	-	-	-	-	-	1	1003
1003	tr	101003	1500	1005	0	-	-	srb	1	1002
1004	fdnet	101004	1500	-	-	1	ibm	-	0	0
1005	trnet	101005	1500	-	-	1	ibm	-	0	0

```
ESW1#
```

¿Cuál es el nombre predeterminado de la VLAN 1? *Default*

¿Qué puertos están en VLAN 1? *Todos los Fastethernet*

¿La VLAN 1 está activa? *Si*

¿Qué tipo de VLAN es la VLAN predeterminada? *Enet*

Examine la memoria flash.

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

Switch# **show flash**

Switch# **dir flash:**

```
ESW1#show flash
No files on device

93184 bytes available (0 bytes used)

ESW1#
*Mar 1 00:08:38.523: %PCMCIAFS-5-DIBERR: PCMCIA disk 0 is formatted from a different router or PC. A format in this router
is required before an image can be booted from this device
ESW1#
```

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?

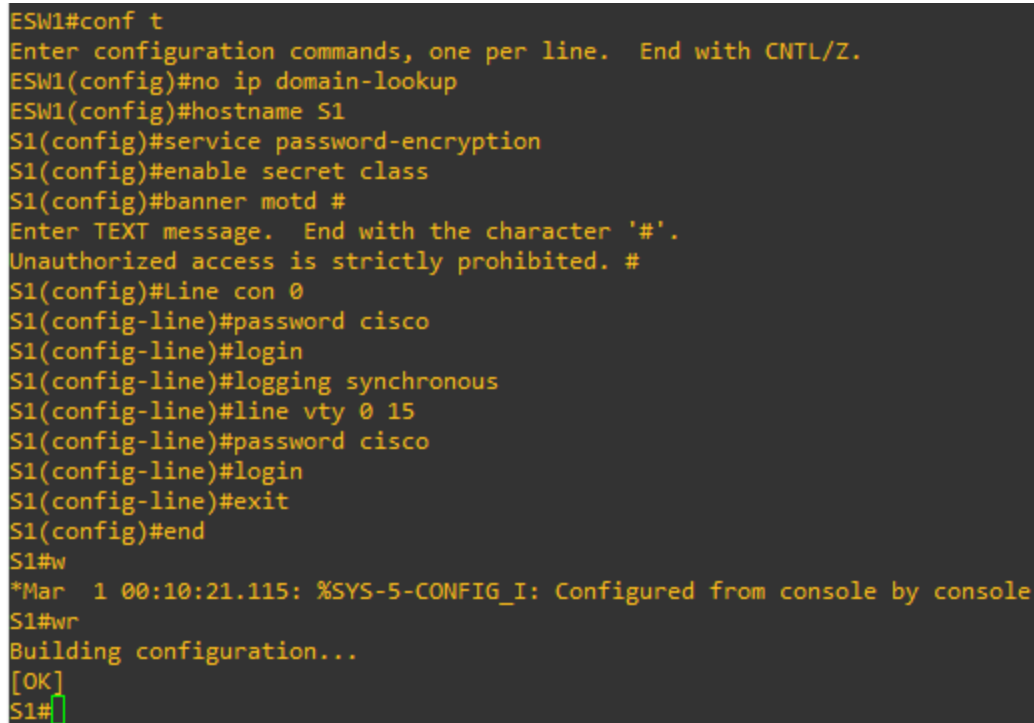
Parte 2: Configurar parámetros básicos de los dispositivos de red

En la Parte 2, configurará los ajustes básicos para el switch y la PC.

Paso 1: Configure los parámetros básicos del switch.

- a. Copie la siguiente configuración básica y péguela en S1 mientras se encuentre en el modo de configuración global.

```
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
```



```
ESW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ESW1(config)#no ip domain-lookup
ESW1(config)#hostname S1
S1(config)#service password-encryption
S1(config)#enable secret class
S1(config)#banner motd #
Enter TEXT message. End with the character '#'.
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)#end
S1#w
*Mar  1 00:10:21.115: %SYS-5-CONFIG_I: Configured from console by console
S1#wr
Building configuration...
[OK]
S1#
```

- b. Establezca la dirección IP de la SVI del switch. Esto permite la administración remota del switch.

Antes de poder administrar el S1 en forma remota desde la PC-A, debe asignar una dirección IP al switch. 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.

Con fines de administración, utilice la VLAN 99. La selección de la VLAN 99 es arbitraria y de ninguna manera implica que siempre deba usar la VLAN 99.

Primero, cree la nueva VLAN 99 en el switch. Luego, establezca la dirección IP del switch en 192.168.1.2 con la máscara de subred 255.255.255.0 en la interfaz virtual interna VLAN 99.

```
S1# configure terminal
```

```
S1(config)# vlan 99
```

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

```
S1(config)# interface vlan99
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
```

```
S1(config-if)# ip address 192.168.1.2 255.255.255.0
```

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

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

```
S1(config)#
```

```
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 99
S1(config-vlan)#exit
S1(config)#interface vlan 99
S1(config-if)#ip address 192.158.1.2 255.255.255.0
S1(config-if)#no shut
S1(config-if)#exit
S1(config)#end
S1#wr
*Mar 1 00:10:57.943: %SYS-5-CONFIG_I: Configured from console by console
S1#wr
Building configuration...
[OK]
S1#
```

Observe que la interfaz VLAN 99 está en estado down, aunque haya introducido el comando **no shutdown**. Actualmente, la interfaz se encuentra en estado down debido a que no se asignaron puertos del switch a la VLAN 99.

- c. Asigne todos los puertos de usuario a VLAN 99.

```
S1(config)# interface range f0/1 - 24,g0/1 - 2
```

```
S1(config-if-range)# switchport access vlan 99
```

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

```
S1(config)#
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

```
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface range f1/0 - 15
S1(config-if-range)#switchport access vlan 99
S1(config-if-range)#exit
S1(config)#
*Mar 1 00:11:49.191: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
S1(config)#end
S1#wr
*Mar 1 00:11:52.727: %SYS-5-CONFIG_I: Configured from console by console
S1#wr
Building configuration...
[OK]
S1#
```

Para establecer la conectividad entre el host y el switch, los puertos que usa el host deben estar en la misma VLAN que el switch. Observe que, en el resultado de arriba, la interfaz VLAN 1 queda en estado down porque no se asignó ninguno de los puertos a la VLAN 1. Después de unos segundos, la VLAN 99 pasa al estado up porque ahora se le asigna al menos un puerto activo (F0/6 con la PC-A conectada).

- d. Emita el comando **show vlan brief** verificar que todos los puertos estén en VLAN 99.

S1# show vlan brief

VLAN	Name	Status	Ports
1	default	active	
99	VLAN0099	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
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

S1#sh vlan-switch br

VLAN	Name	Status	Ports
1	default	active	
99	VLAN0099	active	Fa1/0, Fa1/1, Fa1/2, Fa1/3 Fa1/4, Fa1/5, Fa1/6, Fa1/7 Fa1/8, Fa1/9, Fa1/10, Fa1/11 Fa1/12, Fa1/13, Fa1/14, Fa1/15
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

S1#

- e. Configure el gateway predeterminado para S1. Si no se estableció ningún gateway predeterminado, no se puede administrar el switch desde una red remota que esté a más de un router de distancia. Aunque esta actividad no incluye un gateway IP externo, se debe tener en cuenta que finalmente conectará la LAN a un router para tener acceso externo. Si suponemos que la interfaz de LAN en el router es 192.168.1.1, establezca el gateway predeterminado para el switch.

```
S1(config)# ip default-gateway 192.168.1.1
```

```
S1(config)#
```

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip default-gateway 192.168.1.1
S1(config)#exit
S1#wr
Building configuration...

*Mar  1 00:13:01.731: %SYS-5-CONFIG_I: Configured from console by console[OK]
S1#
```

- f. También se debe restringir el acceso del puerto de consola. La configuración predeterminada permite todas las conexiones de consola sin necesidad de introducir una contraseña. Para evitar que los mensajes de consola interrumpen los comandos, use la opción **logging synchronous**.

```
S1(config)# line con 0
```

```
S1(config-line)# password cisco
```

```
S1(config-line)# login
```

```
S1(config-line)# logging synchronous
```

```
S1(config-line)# exit
```

```
S1(config)#
```

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#logging synchronous
S1(config-line)#exit
S1(config)#end
S1#wr
Building configuration...

*Mar  1 00:13:31.387: %SYS-5-CONFIG_I: Configured from console by console[OK]
S1#
```

- g. Configure las líneas de terminal virtual (vty) para que el switch permita el acceso por Telnet. Si no configura una contraseña de vty, no podrá hacer Telnet al switch.

```
S1(config)# line vty 0 15
```

```
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# end
S1#
*Mar 1 00:06:11.590: %SYS-5-CONFIG_I: Configured from console
by console
```

```
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
S1#wr
Building configuration...

*Mar 1 00:13:55.295: %SYS-5-CONFIG_I: Configured from console by console[OK]
S1#
```

¿Por qué se requiere el comando login? [Configura el switch para que requiera autenticación al iniciar sesión](#)

Paso 2: Configure 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 direccionamiento. Aquí se describe una versión abreviada del procedimiento. Para esta topología, no se requiere ningún gateway predeterminado; sin embargo, puede introducir **192.168.1.1** para simular un router conectado al S1.

```
PC1> ip 192.168.1.10 255.255.255.0 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.10 255.255.255.0 gateway 192.168.1.1
PC1>
```

Parte 3: Verificación y prueba de la conectividad de red

En la parte 3, verificará y registrará la configuración del switch, probará la conectividad de extremo a extremo entre la PC-A y el S1, y probará la capacidad de administración remota del switch.

Paso 1: mostrar la configuración del switch.

Use la conexión de la consola en PC-A para mostrar y verificar la configuración del switch. El comando **show run** muestra la configuración en ejecución completa, de a una página por vez. Utilice la barra espaciadora para avanzar por las páginas.

```
macro name add_vlan
end
vlan database
vlan $v
exit
@@
macro name del_vlan
end
vlan database
no vlan $v
exit
@@
!
vtp file nvram:vlan.dat
archive
  log config
  hidekeys
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
  description *** Unused for Layer2 EtherSwitch ***
  no ip address
  no ip route-cache
  shutdown
  duplex auto
  speed auto
!
interface FastEthernet0/1
  description *** Unused for Layer2 EtherSwitch ***
  no ip address
  --More--
```

```
duplex full
speed 100
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan99
 ip address 192.158.1.2 255.255.255.0
!
ip default-gateway 192.168.1.1
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
banner exec ^C

--More--
```

```
line con 0
  exec-timeout 0 0
  privilege level 15
  password 7 01100F175804
  logging synchronous
  login
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  password 7 030752180500
  login
line vty 5 15
  password 7 030752180500
  login
!
!
end

S1#
```


Verifique la configuración de la VLAN 99 de administración.

```
S1#show int vlan99
Vlan99 is up, line protocol is up
  Hardware is EtherSVI, address is c401.1ce8.0000 (bia c401.1ce8.0000)
  Internet address is 192.158.1.2/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:02:35, 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
  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
    3 packets input, 192 bytes, 0 no buffer
    Received 3 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    2 packets output, 137 bytes, 0 underruns
    0 output errors, 1 interface resets
    0 output buffer failures, 0 output buffers swapped out
S1#
```

¿Cuál es el estado de la VLAN 99? *Activo*

¿Cuál es el estado del protocolo de línea? *Activo*

Paso 2: probar la conectividad de extremo a extremo con ping.

- a. Desde la línea de comandos en PC-A, emita el comando ping a la dirección de PC-A primero.

C:\Users\User1> ping 192.168.1.10

```
PC1> ping 192.168.1.10
192.168.1.10 icmp_seq=1 ttl=64 time=0.001 ms
192.168.1.10 icmp_seq=2 ttl=64 time=0.001 ms
192.168.1.10 icmp_seq=3 ttl=64 time=0.001 ms
192.168.1.10 icmp_seq=4 ttl=64 time=0.001 ms
192.168.1.10 icmp_seq=5 ttl=64 time=0.001 ms
```

- 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

```
PC1> ping 192.168.1.2
84 bytes from 192.168.1.2 icmp_seq=1 ttl=255 time=998.556 ms
84 bytes from 192.168.1.2 icmp_seq=2 ttl=255 time=16.035 ms
84 bytes from 192.168.1.2 icmp_seq=3 ttl=255 time=15.285 ms
84 bytes from 192.168.1.2 icmp_seq=4 ttl=255 time=15.212 ms
84 bytes from 192.168.1.2 icmp_seq=5 ttl=255 time=15.666 ms
```

Debido a que la PC-A debe resolver la dirección MAC del S1 mediante ARP, es posible que se agote el tiempo de espera del primer paquete. Si los resultados del ping siguen siendo incorrectos, resuelva los problemas de configuración de los parámetros básicos del dispositivo. Verifique el cableado físico y las direcciones lógicas.

Reflexión

1. ¿Por qué debería configurar la contraseña de vty del switch?

Para que el switch permita el acceso por Telnet. Si no configura una contraseña de VTY, no podrá acceder al switch mediante Telnet.

2. ¿Para qué se debe cambiar la VLAN 1 predeterminada a un número de VLAN diferente?

Todos los puertos de switch se vuelven parte de la VLAN predeterminada después del arranque inicial de un switch que carga la configuración predeterminada. Los puertos de switch que participan en la VLAN predeterminada forman parte del mismo dominio de difusión. Esto admite cualquier dispositivo conectado a cualquier puerto de switch para comunicarse con otros dispositivos en otros puertos de switch. La VLAN predeterminada para los switches Cisco es la VLAN 1.

Por lo tanto, para poder segmentar la red o administrarla es necesario cambiar las interfaces deseadas a otra VLAN ya que la VLAN 1 no es una elección adecuada para ser VLAN de administración.

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

*Haciendo uso del comando **service password-encryption***

4. ¿Para qué se debe configurar una dirección MAC estática en una interfaz de puerto?

Para que solo acepte esa dirección MAC

Conclusiones:

Cruz Chávez Alan Francisco:

Es importante conocer la administración del switch y tener en cuenta que por si solo no se puede configurar con comandos, en gns3 se utilizo una imagen es específico para poder hacer la configuración, mientras que, en packet tracer se usa la ayuda de un cable de consola conectado a una pc para poder hacer los cambios necesarios.

Gómez Salas Hugo Santiago:

En esta practica entendimos el funcionamiento del swirtch y todos los comandos necesarios para poder administrarlo, también se aprendió a la utilidad de las vlans para poder tener un mejor control de los usuarios.

Mendoza Rodríguez Israel:

En esta esa práctica aprendimos a realizar la configuración de más básica de una vlan solamente con un switch y una pc, es importante que para realizar las vlans encontremos un switch que nos permita crearlas en este caso el switch 3745 fue el que nos funcionó, es importante saber crear vlans poruqe nos permite segmentar mejor los equipos en diferentes subredes y son bastante seguras, ya que podemos denegar o aprobar el tráfico de una vlan a otra.

Ramírez Galindo Karina:

Con esta práctica aprendimos la configuración básica de un switch, ya que anteriormente en redes 1 solo se utilizaba como una especie de capa transparente. Ahora incluso es importante conocer la administración de este dispositivo para poder segmentar mejor la red y tener un mejor control del acceso y seguridad de esta.