



GOBIERNO DEL
ESTADO DE
MÉXICO



ESTADO DE
MÉXICO
¡El poder de servir!

EDUCACIÓN

SECRETARÍA DE EDUCACIÓN, CIENCIA, TECNOLOGÍA E INNOVACIÓN



"2024. Año del Bicentenario de la Erección del Estado Libre y Soberano de México"

UNIVERSIDAD TECNOLÓGICA DEL VALLE DE TOLUCA

Dirección de Carrera de Tecnologías de la Información y Comunicación

Ingeniería en Desarrollo y Gestión de Software

Asignatura

SEGURIDAD INFORMÁTICA

Nombre del Trabajo

Seguridad informática en Conectividad L2-Ethernet

Nombre del Docente

ITE RUBÉN FÉLIX GONZÁLEZ RIVERA

Nombre de los Estudiantes

García Nolasco Elías – 222310426

Mena Garduño Miguel Ángel – 222310538

Gonzalez Ramirez Luis Enrique – 222310427

Grupo

IDGS - 74

Cuatrimestre

7º

Lugar

Santa María Atarasquillo, Lerma, México.

Fecha de Entrega

Septiembre 2025



Practica 1.0

Seguridad informática en Conectividad L2-Ethernet

Introducción

A través de esta práctica se identifican problemas de vulnerabilidades en capa L2-Ethernet e IP y la configuración de las interfaces de los dispositivos de red para reducir el acceso de posibles intrusos y ataques.

Se monitorea la red LAN para examinar las estructuras de los paquetes en tiempo real con analizadores de red de capa 2 en forma practica para revisión de efectividad de la configuración de seguridad.

Para obtener información adicional de conceptos y aplicaciones refiérase a las notas de clase.

Objetivos

Sección 1: Establecer la topología e inicializar los dispositivos

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

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

- Configurar el acceso por SSH.
- Modificar los parámetros de SSH.

- Verificar la configuración de SSH.

Sección 4: configurar y verificar las características de seguridad en el S1

- Configurar y verificar las características de seguridad general.
- Configurar y verificar la seguridad del puerto.

Información básica/situación

- Es muy común bloquear el acceso e instalar buenas características de seguridad en computadoras y servidores a nivel de L2. Es importante también que los dispositivos de infraestructura de red, como los switches y routers, también se configuren con características de seguridad.
- En esta práctica de laboratorio, seguirá algunas de las prácticas recomendadas para configurar características de seguridad en switches LAN. Solo permitirá las sesiones de SSH y de HTTPS seguras.
- También configurará y verificará la seguridad de puertos para bloquear cualquier dispositivo con una dirección MAC que el switch no reconozca.

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)
- 1 computadora (Windows 7, Vista o XP con un programa de emulación de terminal, como Putty)
- 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 : 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 este laboratorio.

NOTA IMPORTANTE: AL FINAL DE LABORATORIO NO DEBERA SALVAR NINGUNA CONFIGURACION EN LOS EQUIPOS CISCO, USTED PUEDE REALIZAR UN RESPALDO EN SU COMPUTADORA

Desarrollo de Actividades

Topología.



Tabla de direccionamiento

Dispositivo	Interface	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	172.16.99.1	255.255.255.0	N/A
S1	VLAN 99	172.16.99.11	255.255.255.0	172.16.99.1
PC-A	NIC	172.16.99.3	255.255.255.0	172.16.99.1

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

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

Si los archivos de configuración se guardaron previamente en el router y el switch, inicialice y vuelva a cargar estos dispositivos con los parámetros básicos.

Sección 2. Configurar los parámetros básicos de los dispositivos y verificar la conectividad

Configure los parámetros básicos en el router, el switch y la computadora. Consulte la topología y la tabla de direccionamiento incluidos al comienzo de esta práctica de laboratorio para conocer los nombres de los dispositivos y obtener información de direcciones.(Si usted es el equipo No.1 el nombre del dispositivo es R1, S1 PC-A, si usted es Equipo No.2 el nombre de dispositivo es R2, S2 y así sucesivamente)

Paso 1. Configurar una dirección IP en la PC-A.

Paso 2. Configurar los parámetros básicos en el R1.

- Configure el nombre del dispositivo.
- Desactive la búsqueda del DNS.
- Configure la dirección IP de interfaz que se muestra en la tabla de direccionamiento.
- Asigne **class** como la contraseña del modo EXEC privilegiado.
- Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.
- Cifre las contraseñas de texto no cifrado.

Paso 3. configurar los parámetros básicos en el S1.

Una buena práctica de seguridad es asignar la dirección IP de administración del switch a una VLAN distinta de la VLAN 1 (o cualquier otra VLAN de datos con usuarios finales). En este paso, creará la VLAN 99 en el Switch y le asignará una dirección IP.

- a. Configure el nombre del dispositivo.
- b. Desactive la búsqueda del DNS.
- c. Asigne **class** como la contraseña del modo EXEC privilegiado.
- d. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y luego habilite el inicio de sesión.
- e. Configure un gateway predeterminado para el S1 con la dirección IP del R1.
- f. Cifre las contraseñas de texto no cifrado.
- g. Cree la VLAN 99 en el switch y asígnele el nombre **Management**.

```
S1(config)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# exit
S1(config)#
```

- h. 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#
```

- i. Escriba el comando **show vlan** en el S1. ¿Cuál es el estado de la VLAN 99? _____ activate_____
- j. Escriba el comando **show ip interface brief** en el S1. ¿Cuál es el estado y el protocolo para la interfaz de administración VLAN 99?

_____El estado está en up y el protocolo de la interfaz está en down_____

¿Por qué el protocolo figura como down, a pesar de que usted emitió el comando **no shutdown** para la interfaz VLAN 99? explique?

__El protocolo de la interfaz VLAN 99 está down porque, en ese momento, no había ningún puerto físico activo asignado a la VLAN 99._____

- k. Asigne los puertos F0/5 y F0/6 a la VLAN 99 en el switch.

```
S1# config t
S1(config)# interface f0/5
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# end
```

- I. Escriba el comando **show ip interface brief** en el S1. ¿Cuál es el estado y el protocolo que se muestra para la interfaz VLAN 99? __Ahora el estado está en up y también el protocolo está en up__

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

Paso 4. Verificar la conectividad entre los dispositivos.

- a. Desde la PC-A, haga ping a la dirección de gateway predeterminado en el R1. ¿Los pings se realizaron correctamente? __Sí, recibí respuestas exitosas en los 4 paquetes enviados.
- b. En la PC-A, haga ping a la dirección de administración del S1. ¿Los pings se realizaron correctamente?
__Sí, todos los paquetes respondieron sin pérdida__
- c. En el S1, haga ping a la dirección de gateway predeterminado en el R1. ¿Los pings se realizaron correctamente?
__Sí, obtuve respuestas completas, ya que el default gateway está configurado correctamente en el switch.__
- d. En la PC-A, abra un navegador web y acceda a <http://172.16.99.11>. Si le solicita un nombre de usuario y una contraseña, deje el nombre de usuario en blanco y utilice la contraseña **class**.

Si le solicita una conexión segura, conteste **No**. ¿Pudo acceder a la interfaz web en el S1?
__Sí, la página de administración HTTP se cargó correctamente, mostrando el dashboard del switch con opciones de configuración.__
- e. Cierre la sesión del explorador en la PC-A.

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.

Sección 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 **UTVTLab.com**.
`S1(config)# ip domain-name UTVT-Lab.com`
- b. Cree una entrada de 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`

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

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

The name for the keys will be: S1.UTVT-Lab.com

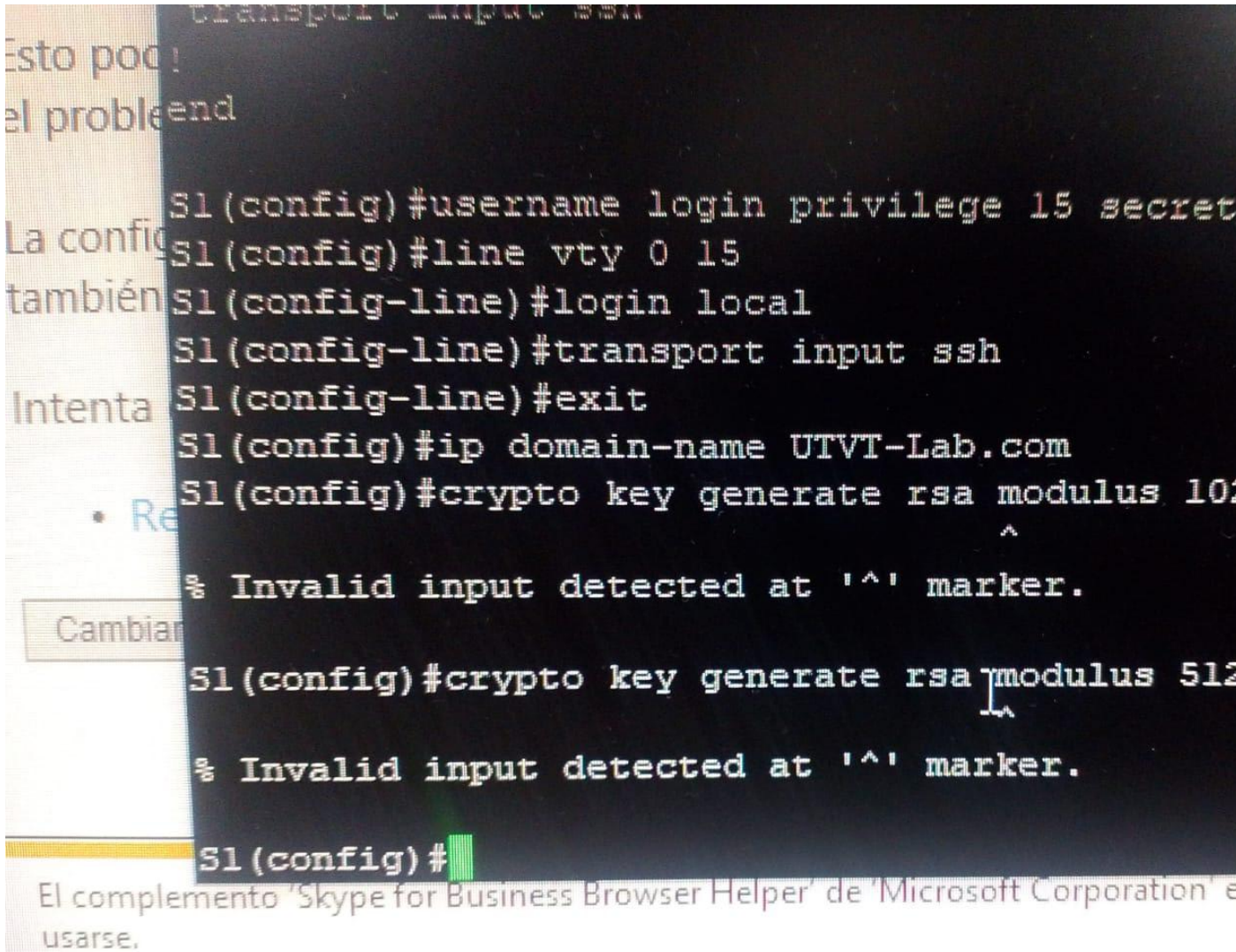
% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable... [OK]

(elapsed time was 3 seconds)

```
S1(config)#
```

```
S1(config)# end
```

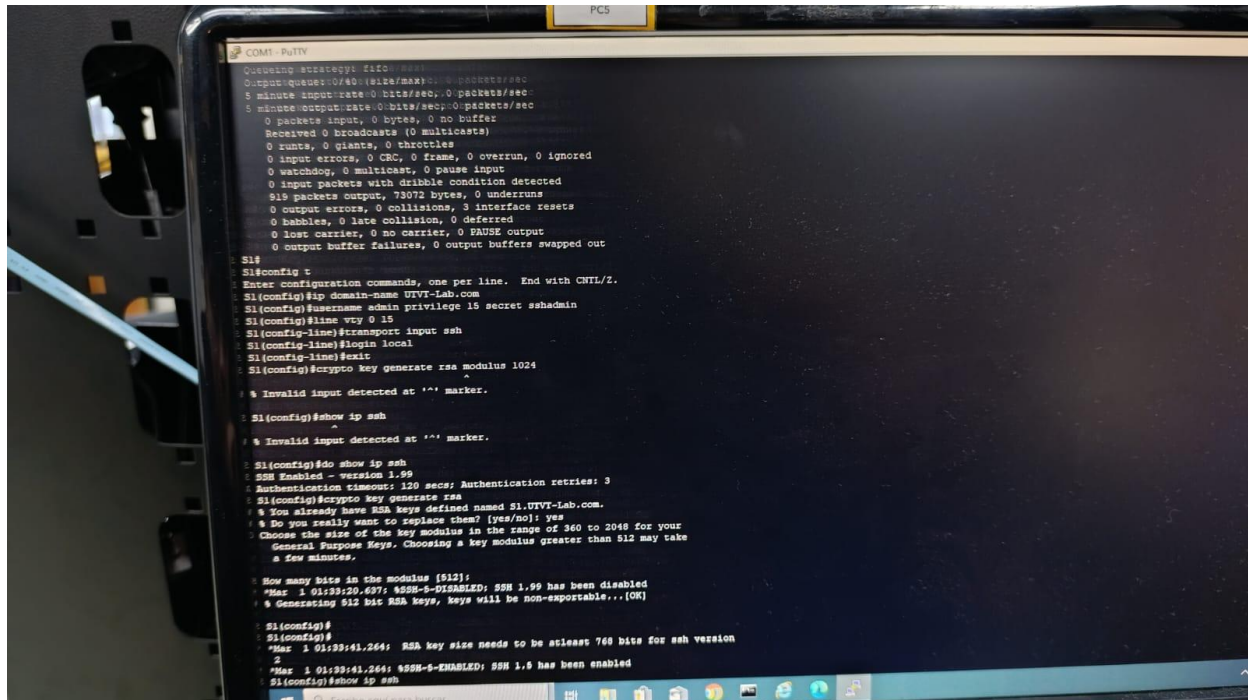


- e. Verifique la configuración de SSH y responda las siguientes preguntas. S1# `show ip ssh`

¿Qué versión de SSH usa el switch? _____2_____

¿Cuántos intentos de autenticación permite SSH? _____ 3 _____

¿Cuál es la configuración predeterminada de tiempo de espera para SSH? _____ 120 segundos _____



Paso 2. modificar la configuración de SSH en el S1.

Modifique la configuración predeterminada de SSH.

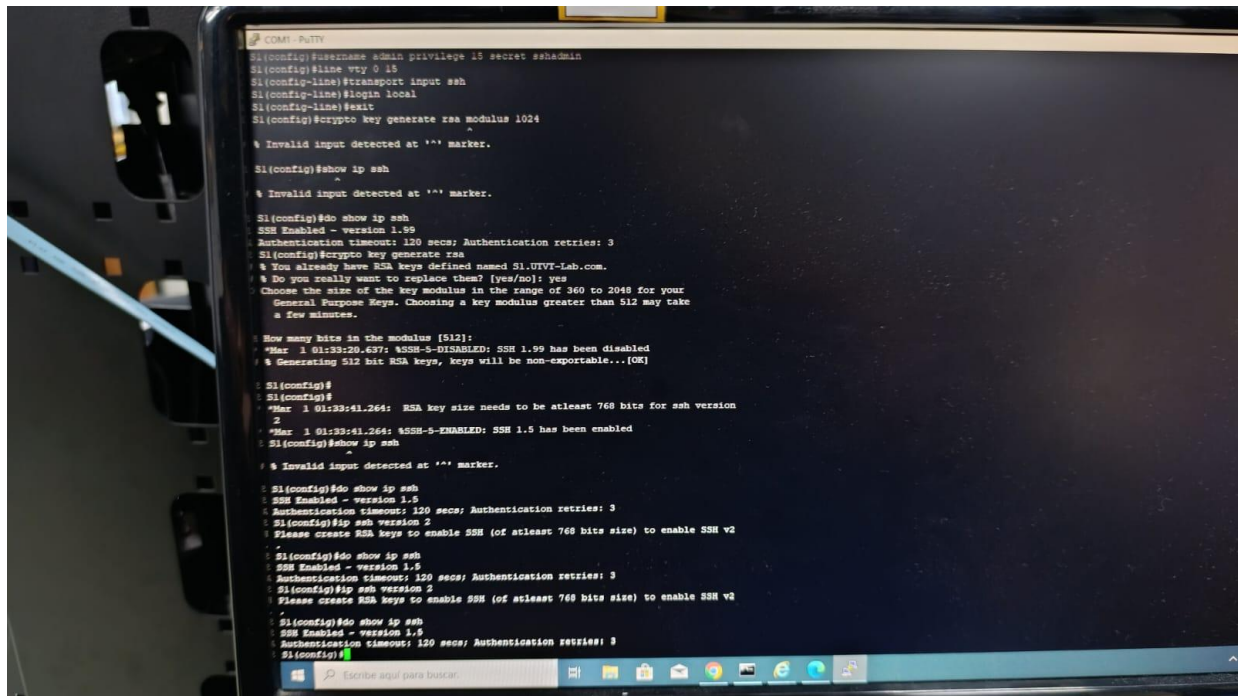
```
S1# config t
```

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

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

¿Cuántos intentos de autenticación permite SSH? _____ 2 _____

¿Cuál es la configuración de tiempo de espera para SSH? _____ 75 segundos _____



Paso 3. verificar la configuración de SSH en el S1.

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

¿La conexión se realizó correctamente? _ Sí, me conecté exitosamente y entré al modo EXEC del switch_____

¿Qué petición de entrada se mostró en el S1? ¿Por qué?

___ En el S1, se mostró el prompt de modo EXEC privilegiado directamente en S1 sin una contraseña adicional,___

___esto ocurrió porque el usuario admin se configuró como privilegio 15 que es el modo administrador completo___

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

Sección 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. Configuraré 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.

- Configure un aviso de mensaje del día (MOTD) en el S1 con un mensaje de advertencia de seguridad adecuado.
- Emita un comando **show ip interface brief** en el S1. ¿Qué puertos físicos están activos?

___ Los puertos físicos activos son F0/5 y F0/6_____

- 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#

```

- d. Escriba el comando **show ip interface brief** en el S1. ¿Cuál es el estado de los puertos F0/1 a F0/4?

_____ El estado de los puertos F0/1 a F0/4 es administratively down. _____

- e. Escriba el comando **show ip http server status**.

¿Cuál es el estado del servidor HTTP? __Enable_____

¿Qué puerto del servidor utiliza? _____ 80 _____

¿Cuál es el estado del servidor seguro de HTTP? _____ Disabled _____

¿Qué puerto del servidor seguro utiliza? _____ 443 _____

- 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
```

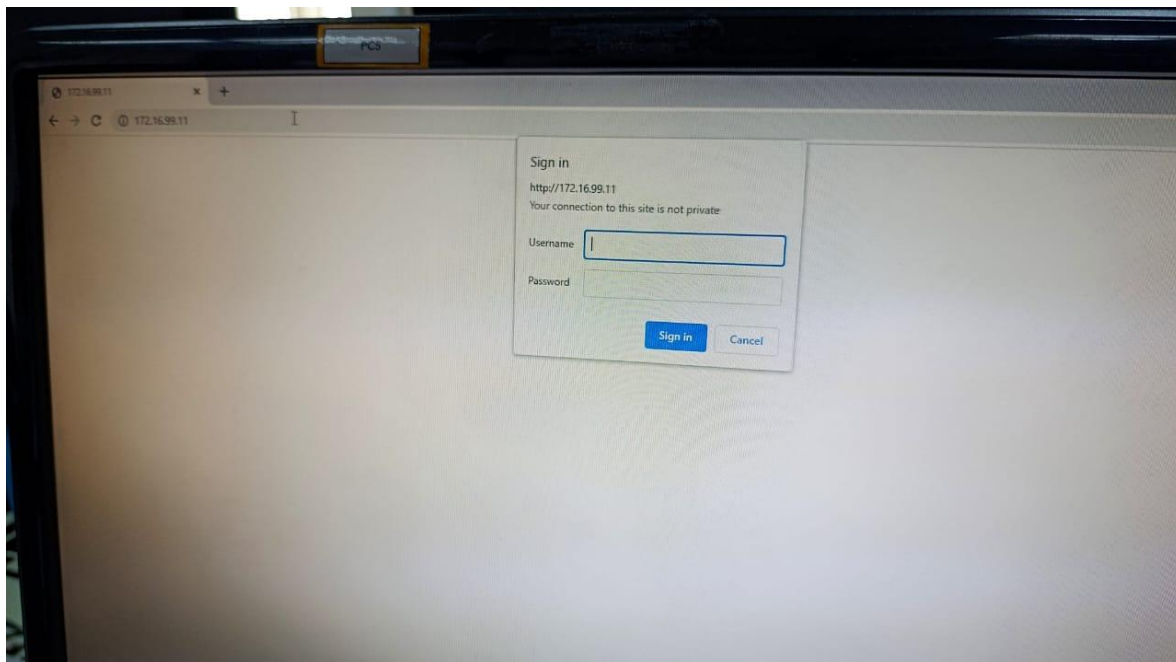
- g. En la PC-A, abra una sesión de navegador web a http://172.16.99.11. ¿Cuál fue el resultado?

_____ El resultado fue página no encontrada _____

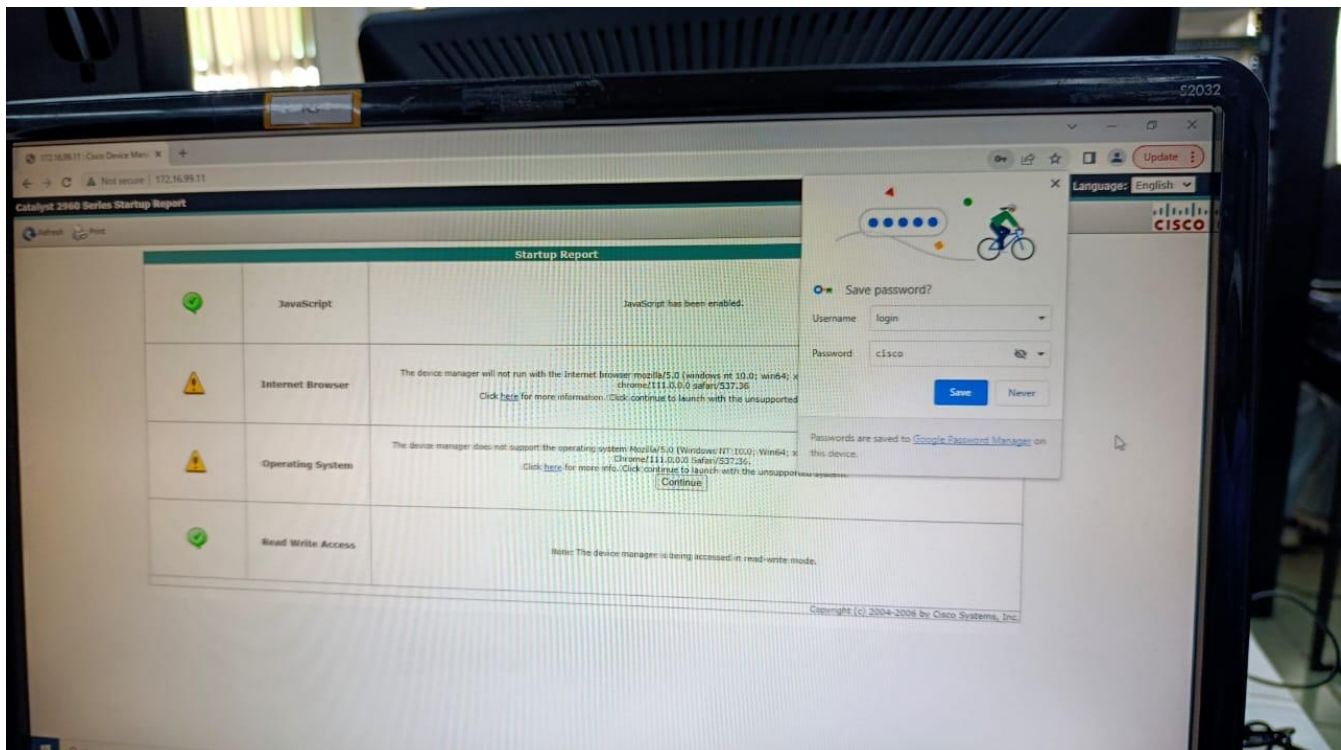
- h. En la PC-A, abra una sesión segura de navegador web en https://172.16.99.11. Acepte el certificado. Inicie sesión sin nombre de usuario y con la contraseña **class**. ¿Cuál fue el resultado?

_____ El resultado fue conexión rechazada _____

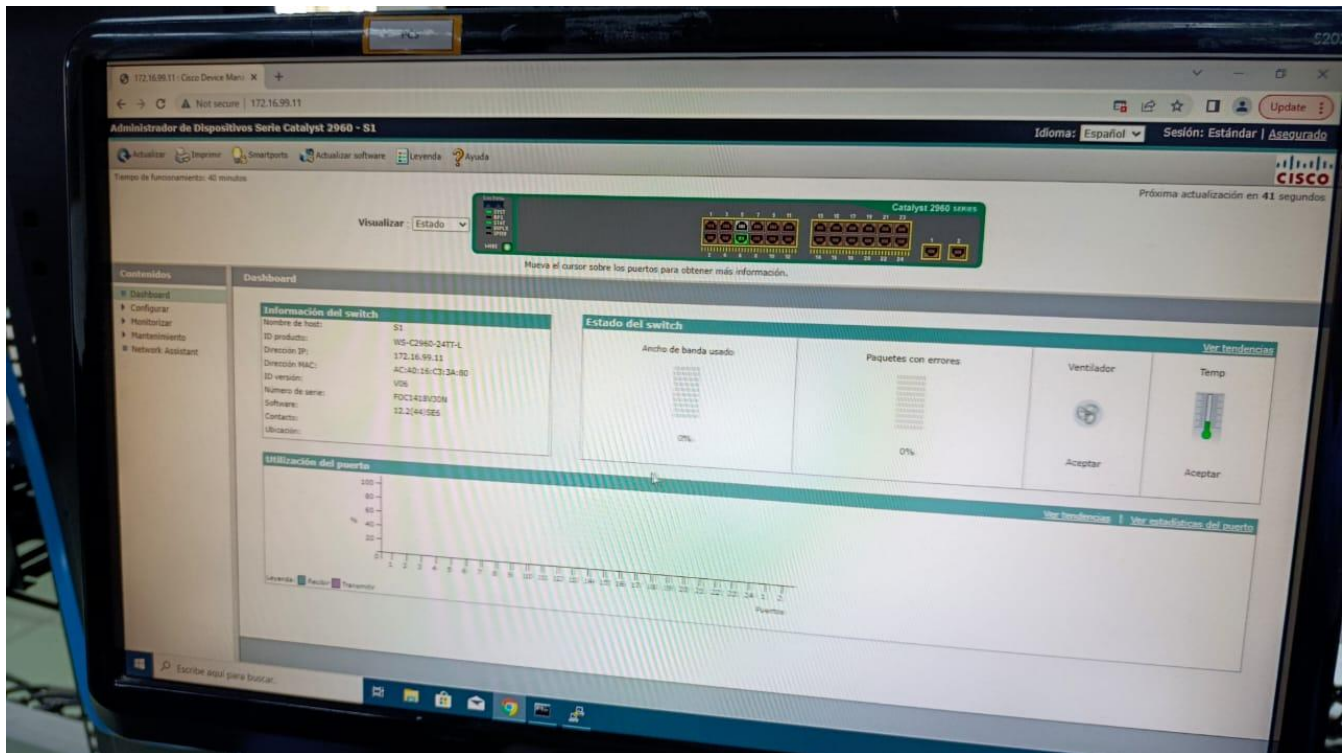
- i. Cierre la sesión web en la PC-A.



UNA VES INGRESADO AL IP DEL SWITCH, CON EL PROTOCOLO HTTP, NO PEDIRA LAS CREDENCIALES QUE COLOCAMOS, LAS INSERTAMOS Y NOS DARA ACCESO.



NOS MANDARA A ESTA VISTA Y EN LA SEGUNDA FIAL EN LA TERCERA COLUMNA DE DAREMOS EN CONTUNUAR Y NOS MADARA A VER LA ITERFAZ DE SWITCH, DONDE VAMOS A PODER VER LOS PURTOS DE fast ETHERNET ACTIVOS Y DESACTIVADOS.



NOS MOSTRADA ESTA VISTA CON TODA LA INFORMACION DE SWITCH, DONDE PODEMOS VER LA VESION QUE TENEMOS, EL ESTADO DEL MISMO, TODO SU ESTADO.

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

- 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**

GigabitEthernet0/1 is up, line protocol is up

Hardware is CN Gigabit Ethernet, address is 30f7.0da3.1821 (bia 3047.0da3.1821)

¿Cuál es la dirección MAC de la interfaz G0/1 del R1?

____ La dirección MAC de la interfaz G0/1 del R1 es 30f7.0da3.1821. _____

- 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.

Dirección MAC de F0/5: ____ Dirección MAC de F0/5: 30f7.0da3.1821 _____

Dirección MAC de F0/6: ____ Dirección MAC de F0/6: 0200.000a.0b0c _____

- 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 solo para F0/5 como ejemplo.

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

R1.
S1(config)# **interface f0/5**

- 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
```

- d. Verifique la seguridad de puertos en F0/5 del S1 mediante la emisión de un comando **show port-security interface**.

```
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 : 0000.0000.0000:0
Security Violation Count : 0
```

¿Cuál es el estado del puerto de F0/5?

_____ El estado del puerto de F0/5 es 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**

El ping fue exitoso

- 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
```

- 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 una conexión de consola abierta en el S1 al mismo tiempo que realiza este paso. Verá que se muestran varios mensajes en la conexión de consola al S1 que indican una violación de seguridad. Habilite la interfaz G0/1 en R1.

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

- i. En el modo EXEC privilegiado del R1, haga ping a la PC-A. ¿El ping se realizó correctamente? ¿Por qué o por qué no?

_____ El ping no se realizó correctamente _____

- j. En el switch, verifique la seguridad de puertos con los comandos que se muestran a continuación.

```
S1# show port-security
```

```
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action  
          (Count) (Count) (Count)
```

```
-----  
          Fa0/5          1          1          1          Shutdown  
-----
```

```
Total Addresses in System (excluding one mac per port)      :0 Max  
Addresses limit in System (excluding one mac per port) :8192
```

```
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:99  
Security Violation Count : 1
```

```
S1# show interface f0/5
```

```
FastEthernet0/5 is down, line protocol is down (err-disabled)
```

```
Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05)
```



```

    MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
<output omitted>

```

S1# **show port-security address**

```

                Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
      (mins)
-----
   99    30f7.0da3.1821 SecureConfigured   Fa0/5      -
-----

Total Addresses in System (excluding one mac per port)    :0
Max Addresses limit in System (excluding one mac per port) :8192

```

- 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

```

- l. Desde el R1, vuelva a hacer ping a la PC-A en 172.16.99.3. ¿El ping se realizó correctamente?
 _____El ping no se realizó correctamente_____

- m. Emita el comando **show interface f0/5** para determinar la causa de la falla del ping. Registre sus conclusiones.

_____El puerto está down, line protocol is down debido a la violación de seguridad de puertos_____

- 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

```

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.

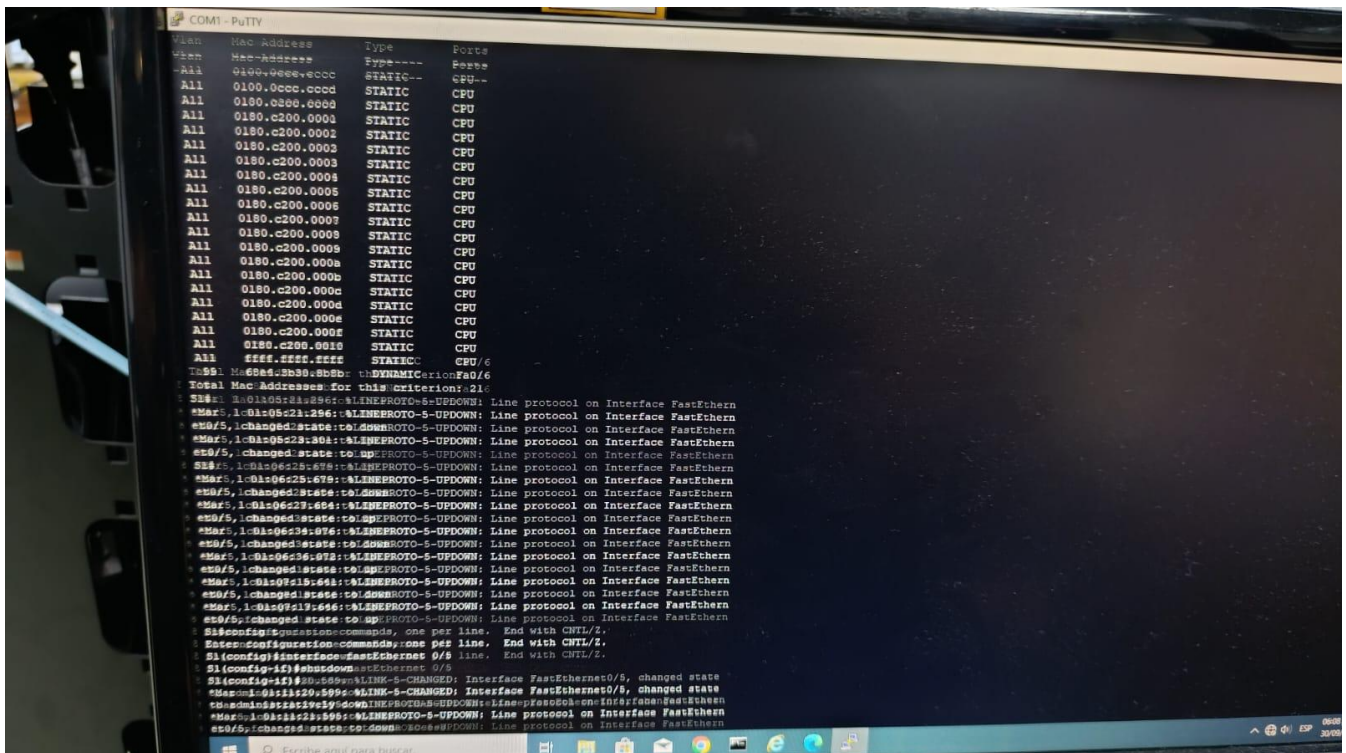
S1# **show interface f0/5**

```

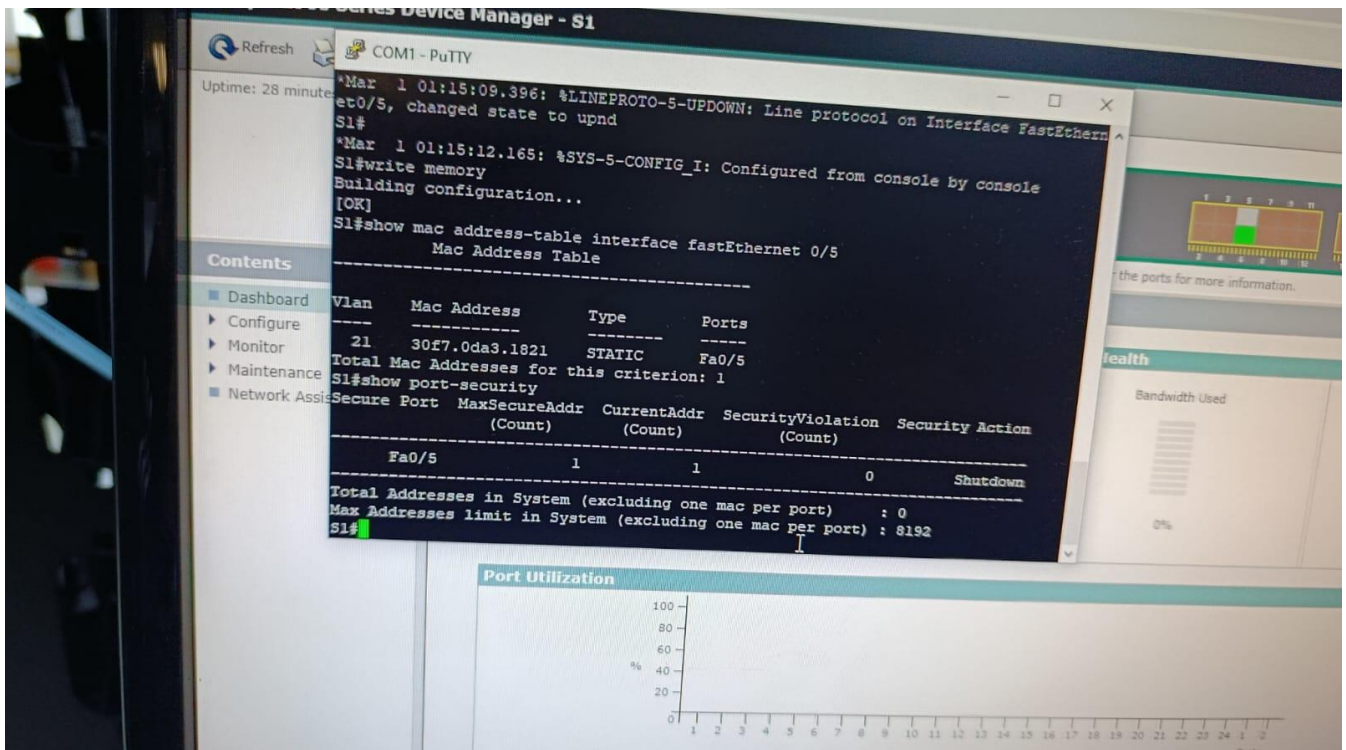
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia
  0023.5d59.9185) MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec, reliability
  255/255, txload 1/255, rxload 1/255

```

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



VER LAS DIRECCIONES MAC REGISTRADAS.



VER LA INFORMACION DE F0/5 QUE CONFIGURAMOS. PARA VER SU STATUS. DE LA CUAL EL SWITCH SU FOCO SE PONIA EN COLOR NARANJA Y DESUES A VERDE,

Reflexión

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

La seguridad de puertos se habilita para restringir el acceso a los puertos del switch basándose en direcciones MAC permitidas, limitando el número máximo de dispositivos por puerto y definiendo acciones ante violaciones como shutdown. Esto previene ataques como la suplantación de MAC, mejorando la seguridad general de la red al asegurar que solo dispositivos conocidos puedan comunicarse.

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

Los puertos no utilizados deben deshabilitarse para reducir la superficie de ataque, ya que puertos abiertos pueden ser explotados por atacantes para conectar dispositivos no autorizados

“AVISE A SU PROFESOR SI USTED HA LLEGADO A ESTE PUNTO DE LA PRACTICA DE LABORATORIO”

Firma de la practica

Practica 2.1 Seguridad Informatica en Conectividad L2 ethernet

- Garcia Nolasco Elias
- Mena Garduño Miguel Angel
- Gonzalez Ramirez Luis Enrique

HTTP - OK
HTTPS - version
SSH - OK
SPS - Pend.

> 30/09/25