

REPORTE DE PRACTICA



CISCO
Networkin
Academy

Nombre Del Alumno: Gael Adrian De Santiago Uribe

Matricula: 22075877

Nombre de la materia: Redes II

Nombre del maestro: Dr Jose Edgar Lugo Castro

Modulo o Unidad de aprendizaje: Modulo1

Nombre de la practica: Configuracion de acceso local

Fecha 02/09/2025

TITULO: PRÁCTICA: CONFIGURACIÓN DE ACCESO REMOTO SEGURO CON SSH EN UN SWITCH CISCO

Materiales:

Software: Cisco Packet Tracer v8.2.2 (o superior).

Equipo Simulado:

1 Switch Cisco modelo 2960.

1 Computadora de escritorio (PC).

1 Cable de Consola virtual.

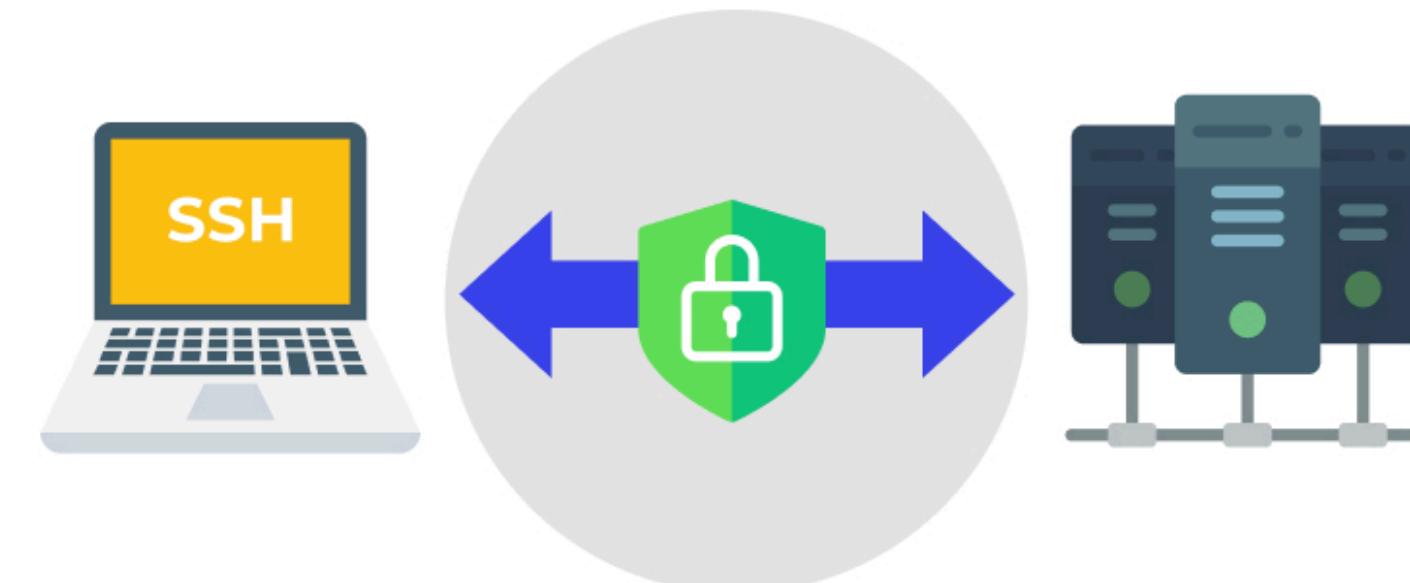
1 Cable de Cobre Directo (Copper Straight-Through) virtual.

MARCO CONCEPTUAL

La administración remota de dispositivos de red es una tarea fundamental para cualquier administrador de sistemas. Si bien protocolos como TELNET ofrecen esta funcionalidad, su principal debilidad es la falta de encriptación, transmitiendo todos los datos, incluidas las contraseñas, en texto plano.}

SSH (Secure Shell) es un protocolo de red criptográfico que soluciona esta vulnerabilidad, permitiendo una administración remota segura a través de una red no segura. SSH opera en un modelo cliente-servidor, estableciendo un canal cifrado entre ambos extremos. Toda la sesión, incluyendo la autenticación de contraseñas y los comandos ejecutados, está protegida contra escuchas y ataques de intermediario (man-in-the-middle).

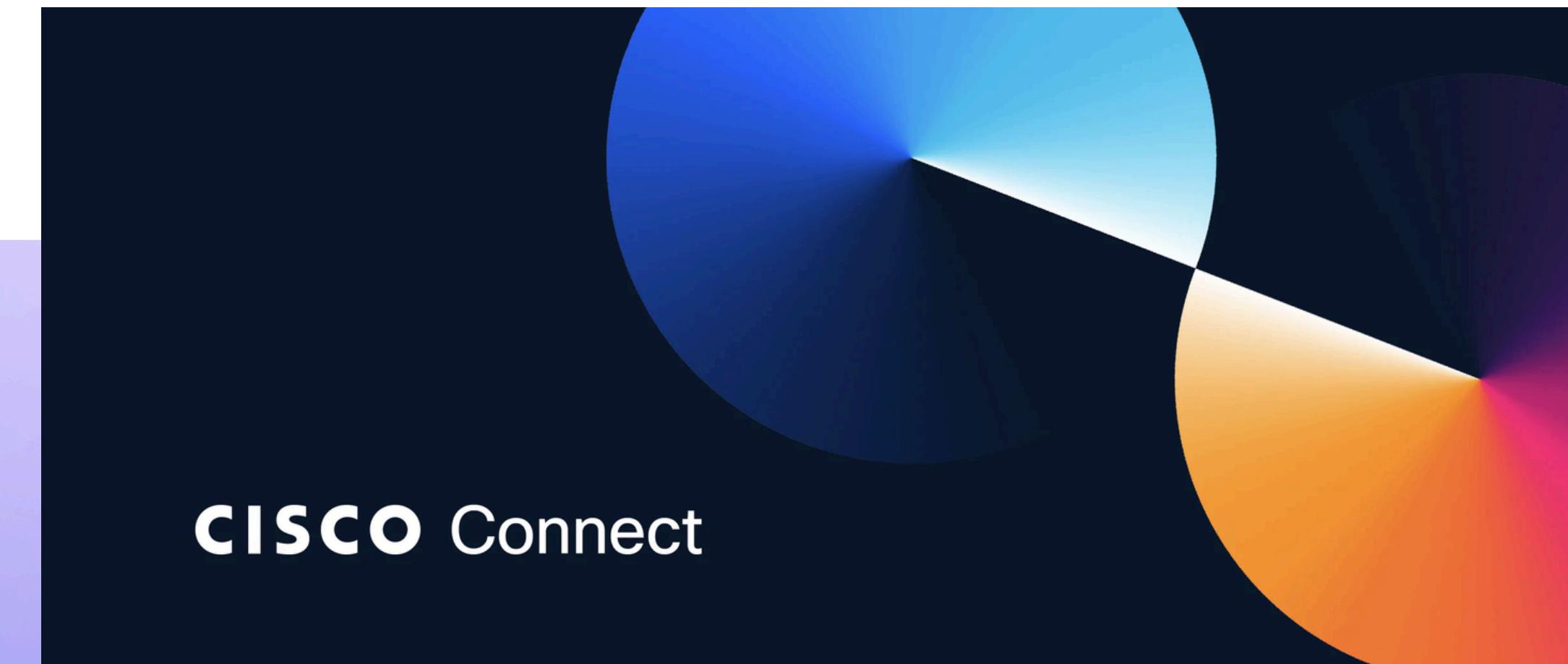
Protocolo de shell seguro



MARCO CONCEPTUAL

Para habilitar SSH en un dispositivo Cisco, se deben cumplir varios requisitos. Primero, el dispositivo debe tener un nombre de host y un nombre de dominio IP . Estos dos elementos se combinan para formar el nombre completo que se asocia a las claves criptográficas. Posteriormente, se deben generar estas claves, comúnmente usando el algoritmo RSA , que crea un par de claves para el cifrado asimétrico.

A diferencia de TELNET, que puede autenticar solo con una contraseña de línea, SSH requiere una autenticación basada en usuario y contraseña. Esto se logra creando una base de datos de usuarios locales en el dispositivo. Finalmente, las líneas de terminal virtual deben ser configuradas para aceptar únicamente conexiones SSH y para validar las credenciales contra la base de datos de usuarios locales .



DESARROLLO

Topología y Acceso Inicial: Se construyó una topología simple con un switch 2960 y una PC. Se utilizó un cable de consola para establecer la conexión inicial y acceder a la CLI del switch desde la aplicación Terminal de la PC.



DESARROLLO

Configuración Básica: Se accedió al modo de configuración global del switch. Se configuró una dirección IP de administración en la interfaz virtual (interface vlan 1) con la IP 192.168.1.20 y máscara 255.255.255.0.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.20 255.255.255.0
Switch(config-if)#no shutdown
```

DESARROLLO

Configuración de Prerrequisitos para SSH: Se estableció un nombre de dominio IP con el comando ip domain-name sistemas.lan. luego, se generaron las claves criptográficas RSA con el comando crypto key generate rsa pero fallo ya que se me olvido asignarle el nombre al host asi que con el comando hostname SW_SSH nombre al host y ahora si me dejo hacer el comando crypto key generate rsa ahora si seleccione un módulo de 512 bits para probar aunque se recomienda bits de 1024.

```
Switch(config)#ip domain-name sistemas.lan
Switch(config)#crypto key generate rsa
% Please define a hostname other than Switch.
Switch(config)#hostname SW_SSH
SW_SSH(config)#config key generate rsa
      ^
% Invalid input detected at '^' marker.

SW_SSH(config)#crypto key generate rsa
The name for the keys will be: SW_SSH.sistemas.lan
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

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

DESARROLLO

Creación de Usuario y Contraseña de enable:

Se creó un usuario local para la autenticación de SSH con el comando username admin secret cisco123.

```
SW_SSH(config)#username admin secret cisco123
*Mar 1 0:7:0.969: RSA key size needs to be at least 768 bits for ssh version 1
*Mar 1 0:7:0.969: %SSH-5-ENABLED: SSH 1.5 has been enabled
```

DESARROLLO

Configuración de Líneas VTY: Se configuraron las líneas de acceso remoto (line vty 0 15) para que utilizaran la base de datos de usuarios locales para la autenticación (login local) y para que aceptaran exclusivamente conexiones SSH (transport input ssh), bloqueando así el acceso inseguro vía TELNET.

```
SW_SSH(config)#line vty 0 15
SW_SSH(config-line)#login local
SW_SSH(config-line)#transport input ssh
SW_SSH(config-line)#end
```

DESARROLLO

Guardado y Verificación: La configuración se guardó en la NVRAM con el comando copy running-config startup-config. Para la verificación, se conectó la PC al switch mediante un cable Ethernet y se le asignó una IP estática (192.168.1.10). Se inició una conexión desde el Command Prompt de la PC con el comando ssh -l admin 192.168.1.20.

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

IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.1.10
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server	0.0.0.0

```
C:\>ssh -l admin 192.168.1.20
Password: |
```

DESARROLLO

Resultados Obtenidos: Se solicitó la contraseña del usuario admin, y tras introducirla correctamente, se obtuvo acceso al modo de usuario S1> Comprobando que efectivamente se iso bien la configuracion.

```
[Connection to 192.168.1.20 closed by foreign host]
C:\>ssh -l admin 192.168.1.20

Password:

SW_SSH>
```

CONCLUSION PERSONAL

Es importante aprender este tipo de seguridad en el anterior ejercicio se vio como es posible configurar la seguridad en forma basica para conectarse de forma telnet ahora con el protocolo SSH aprendi que es mas segura que la de telnet y tambien aprendi que es importante proteger bien los datos para un posible ataque de seguridad y para terminar aprendi la generacion de claves criptografiacas y aplique lo aprendido anteriormente que son la creacion de usuarios locales y nombrar un dominio

**¡GRACIAS POR
SU ATENCIÓN!**