

Nombre del Alumno: Gael Adrian De Santiago Uribe		Matrícula: 22075877
Nombre de la Materia: Redes II	Nombre del Maestro: Dr. Jose Edgar Lugo Castro	
Módulo o Unidad de Aprendizaje: Modulo 1	Nombre de la Practica: Configuración de Acceso Local TELNET	
Fecha: 30 de agosto de 2025		
Materiales: Software: Cisco Packet Tracer v8.2.2 (o superior). Equipo Simulado: <ol style="list-style-type: none">1 Switch Cisco modelo 2960 virtual.1 Computadora de escritorio virtual.1 Cable de Consola virtual.1 Cable de Cobre Directo virtual.		
Referencias <ul style="list-style-type: none">AIX. (s. f.). https://www.ibm.com/docs/es/aix/7.1.0?topic=protocols-telnet-protocol¿Qué es una CLI? - Explicación sobre la interfaz de línea de comandos - AWS. (s. f.). Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/cli/<i>Small business IT explained in 60 seconds or less: Which switch is which? with captions.</i> (2023, 22 febrero). [Vídeo]. Cisco. https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/network-switch-how.html		

Título:

Marco Conceptual (Teoría de la practica):

Los switches son piezas de construcción clave para cualquier red. Conectan varios dispositivos, como computadoras, Access points inalámbricos, impresoras y servidores; en la misma red dentro de un edificio o campus. Un switch permite a los dispositivos conectados compartir información y comunicarse entre sí.

Switches no administrados

Un switch de red no administrado está diseñado para que pueda simplemente conectarlo y funcione, sin necesidad de configuración. Los switches no administrados se usan generalmente para conectividad básica. En general, se verán en redes domésticas o donde sea que se necesiten unos cuantos puertos más, como en su escritorio, en un laboratorio o en una sala de conferencias.

Switches administrados

Los switches administrados le ofrecen mayor seguridad y más funciones y flexibilidad, dado que puede configurarlos para que se adapten a su red. Con este mayor control, puede proteger mejor su red y mejorar la calidad del servicio para los que acceden a la red.

interfaz de la línea de comandos (CLI)

Una interfaz de la línea de comandos (CLI) es un mecanismo de software que se utiliza para interactuar con el sistema operativo mediante el teclado. Otro mecanismo disponible es la interfaz de usuario gráfica (GUI), la cual se utiliza mucho en la actualidad en todas las aplicaciones y los sistemas de software. Puede usar una GUI para navegar visualmente y hacer clic en íconos e imágenes a fin de poner actividades en funcionamiento. Sin embargo, las GUI resultan ineficientes para las tareas de administración del sistema, en especial cuando se trata de entornos virtuales o remotos. Con una interfaz de línea de comandos, puede escribir comandos de texto para configurar, explorar o ejecutar programas en cualquier servidor o sistema informático. Todos los sistemas operativos, incluidos Linux, macOS y Windows, proporcionan una CLI para agilizar la interacción con el sistema.

Protocolo Telnet (TELNET)

El Protocolo Telnet (TELNET) proporciona un método estándar para que los dispositivos de terminal y los procesos orientados a terminal intercambien información.

Normalmente los programas de emulación de terminal que le permiten iniciar la sesión en un sistema principal remoto utilizan TELNET. Sin embargo, TELNET se puede utilizar para las comunicaciones de terminal a terminal y las comunicaciones entre procesos. TELNET también lo utilizan otros protocolos (por ejemplo, FTP) para establecer un canal de control de protocolo.

TCP/IP implementa TELNET en los mandatos de usuario tn, telnet o tn3270. El daemon telnetd no proporciona ninguna API en TELNET.

Las Líneas VTY

Las Líneas VTY (Virtual Teletype) son líneas virtuales utilizadas para permitir el acceso remoto (TELNET/SSH) a un dispositivo Cisco. A diferencia del puerto de consola físico, no hay un puerto físico asociado a ellas. Es en estas líneas donde se configuran las contraseñas y los parámetros de acceso remoto.

Desarrollo (Pasos Elaborados Durante La Practica E Imágenes Descriptivas):

Paso 1: se puso un switch Cisco 2960 y una PC en el área de trabajo de Packet Tracer. Se conectaron al principio con un cable de consola desde el puerto RS 232 de la PC al puerto Console del switch para la configuración inicial.



Paso 2: le di click al pc y luego al desktop y abrir la aplicación "Terminal", se accedió a la CLI del switch. Se procedió a entrar al modo de configuración global y se asignó un nombre al switch (hostname SW1) para una mejor identificación.

```
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.
64K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:E0:8F:B1:C7:8E
Motherboard assembly number     : 73-10390-03
Power supply part number       : 341-0097-02
Motherboard serial number      : FOC10093R12
Power supply serial number     : AZS1007032H
Model revision number          : B0
Motherboard revision number    : B0
Model number                   : WS-C2960-24TT-L
System serial number           : FOC1010X104
Top Assembly Part Number       : 800-27221-02
Top Assembly Revision Number   : A0
Version ID                    : V02
CLEI Code Number              : COM3L00BRA
Hardware Board Revision Number : 0x01

Switch Ports Model          SW Version  SW Image
-----
*   1 26   WS-C2960-24TT-L    15.0(2)SE4  C2960-LANBASEK9-M

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE
SOFTWARE (fcl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen

Press RETURN to get started!

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

Paso 3: Se configuró la interfaz virtual vlan 1 con la dirección IP 192.168.1.20 y la máscara de subred 255.255.255.0. Se activó la interfaz con el comando no shutdown.

```
Switch(config)# hostname swl
swl(config)# interface vlan 1
swl(config-if)#ip address 192.168.1.20 255.255.255.0
swl(config-if)#no shutdown

swl(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
swl(config-if)#
```

Paso 4: Me salí del modo configuración de interface y luego habilité la encriptación de contraseñas con el comando `servicie password-encryption`. Luego configuré las líneas virtuales de acceso line vty 0 15 con la contraseña telnet y force la solicitud de esta con el comando `login`, y para finalizar establecí una contraseña secreta (`enable secret cisco`) para el acceso al modo privilegiado, un requisito indispensable para el funcionamiento de TELNET.

```
swl(config-if)#exit
swl(config)# se password-encryption
swl(config)#?
```

Nota: puse la parte de ayuda para poder afirmar que era el comando correcto ya que quería empezar a usar más la abreviación y tenía dudas si era así

```
swl(config)#
swl(config)#li vty 0 15
swl(config-line)#password telnet
swl(config-line)#login}
^
% Invalid input detected at '^' marker.

swl(config-line)#login
swl(config-line)#exit
swl(config)#enable secret cisco
```

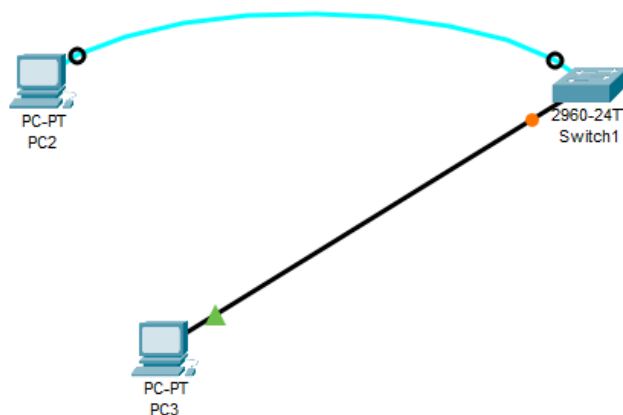
Nota: me equivoque al escribir y se me fue un carácter incorrecto

Paso 5: Finalice la configuración y luego utilice el comando `copy running-config startup-config` para guardar la configuración activa en la memoria no volátil (NVRAM) del switch, asegurando que los cambios persistan tras un reinicio.

```
sw1(config)#end
sw1#
%SYS-5-CONFIG_I: Configured from console by console

sw1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
sw1#
```

Paso Final: después Salí de la terminal y del pc y agregue otro pc para hacer la conexión física con un cable de cobre directo entre la PC (puerto FastEthernet) y un puerto del switch (ej. FastEthernet0/1). Luego asigne una dirección IP estática a la PC (192.168.1.10) dentro de la misma red que el switch. Y al final Desde el Command Prompt de la PC, ejecute el comando `telnet 192.168.1.20`. Se introdujo con éxito la contraseña de VTY (telnet) y posteriormente la contraseña enable (cisco) para obtener control total del switch de forma remota.



Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ 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

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::2E0:A3FF:FE9B:4219

Default Gateway:

DNS Server:

802.1X

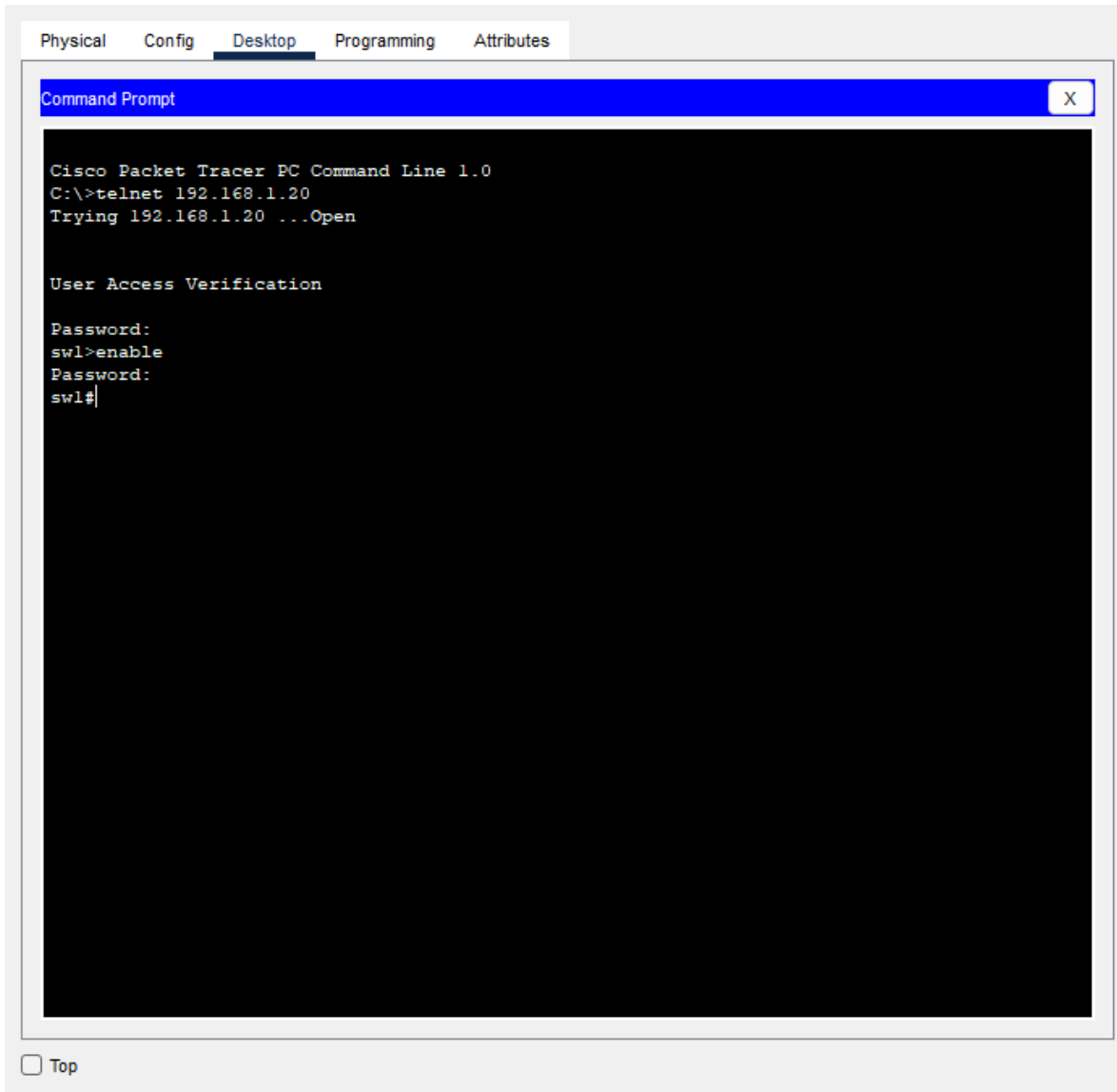
☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top



The screenshot shows a Cisco Packet Tracer PC Command Line window. The window has tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is selected. The command prompt shows the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.1.20
Trying 192.168.1.20 ...Open

User Access Verification

Password:
swl>enable
Password:
swl#
```

At the bottom left of the window, there is a checkbox labeled "Top".

Conclusión Personal:

Mi conclusión es que es importante saber primero como acceder a la configuración de un switch que hoy aprendí que es con un cable especial para acceder a la consola, también entendí como aunque sea básico la seguridad de la red que aunque existan protocolos mas seguros y que este seguramente sea el más fácil de vulnerar sirve como un ejemplo claro de como proteger los accesos al switch también aprendí el rol de una VLAN de administración y la diferencia de estar conectado por consola ósea por administrador y por red ósea con cable de cobre puro