Telnet & SSH

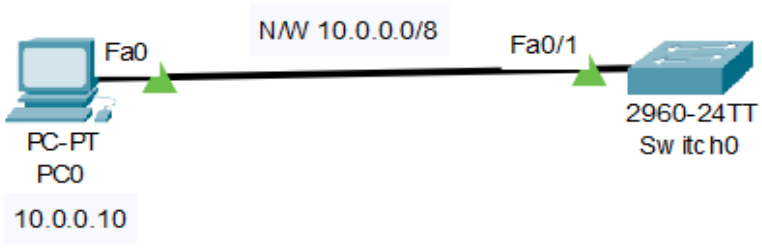
Telnet (Teletype Network): An application layer protocol that allows a network administrator to access and manage remote devices. Developed in 1969. All commands are in clear text.

Telnet Client: A user on a client machine can use software to access a command-line interface of another remote machine that is running a **Telnet server** program. Ex: PC, Laptop, etc.

Telnet Server: A machine that is running a Telnet server program. Ex: Switch, Router, etc.

1. Telnet configuration on a switch

We will configure Telnet on the switch so that as the admin, you'll be able to access and manage the switch remotely.



✔ Configure **enable password** or **enable secret password** on the switch

If you fail to do this, you won't pass the executive mode of the switch even after you establish a telnet connection to the switch.

```
Switch>enable
Switch#config terminal
Switch(config)#enable password admin
```

✔ Configure a VLAN interface on the switch

In a network, a VLAN (Virtual Local Area Network) is a logical grouping of network devices that are connected together, even if they are physically separate. A VLAN allows network administrators to create virtual LANs, which can help them to control and segment network traffic, improving security and network performance.

To configure a VLAN on a switch, you need to assign an IP address to the VLAN interface of the switch. This IP address is used as the management address for the VLAN. By assigning an IP address to the VLAN interface, you can use this address to remotely manage the switch using Telnet or other network management protocols.

For example, if you have a laptop connected to a switch that has multiple VLANs, you can Telnet the switch using the IP address assigned to the VLAN interface of the switch. This allows you to remotely manage the switch from your laptop, even if the switch is physically located in a different room or building.

By assigning an IP address to the VLAN interface of the switch, you can also configure the switch to communicate with other network devices on the VLAN. This enables devices on different VLANs to communicate with each other, while still keeping their traffic separated and secure.

We assign an IP address to the **VLAN** interface of the switch so that we can Telnet the switch from the laptop using this address.

```
Switch(config)#int VLAN 1
Switch(config-if)#ip address 10.0.0.20   255.0.0.0
Switch(config-if)#no shut
Switch(config-if)#exit
```

Telnet & SSH

✔ Configure a **Telnet password** on VTY lines for remote access

VTY (Virtual Teletype) is a term used to describe the virtual terminal lines used for remote management of a network device such as a switch or router. VTY lines allow network administrators to remotely access and configure the device through a Telnet or Secure Shell (SSH) session.

To secure access to the switch through VTY lines, network administrators can configure a password on the VTY lines. This password serves as a form of authentication and must be provided before accessing the switch remotely via Telnet.

By configuring a password on the VTY lines, network administrators can ensure that only authorized users are allowed remote access to the switch. This helps to prevent unauthorized access and strengthens the overall security of the network.

This password is configured on VTY lines. Before you can manage the switch remotely via Telnet, you'll have to provide this password.

```
Switch(config)#line vty 0 15
Switch(config-line)#password cisco
Switch(config-line)#login
```

✔ Test Telnet connectivity from **admin PC**

Go to the PC and give the command: **telnet 10.0.0.20** (VLAN IP address). Then provide the password (**cisco**). Then to enter privileged mode provide enable password (**admin**).

In a Cisco network device such as a switch or a router, there are two types of passwords that can be configured: the line password and the enable secret password.

The line password is used to secure access to a specific line on the network device, such as the console or VTY lines used for remote management. This password is configured on the specific line and is required to access that line of the device. For example, if a line password is configured on the console line of a switch, anyone who wants to access the switch through the console port must provide the correct password.

On the other hand, the enable secret password is used to secure access to privileged EXEC mode on the network device. Privileged EXEC mode is a mode that provides access to all the commands and configurations available on the device. This password is configured in the global configuration mode and is required to gain access to privileged EXEC mode from user EXEC mode.

The key difference between these two types of passwords is the level of access they provide. The line password provides access to a specific line on the device, while the enable secret password provides access to the entire device configuration.

Telnet & SSH

2. Telnet configuration on a router

✔ Configure **enable password** or **enable secret password** on the router

- Router>enable
- Router#config terminal
- Router(config)#enable password admin

✔ Configure IP addresses on the **admin PC** and **interface gig0/0** of the router

Router

- Router(config)#int gig0/0
- Router(config-if)#ip address 10.0.0.1 255.0.0.0
- Router(config-if)#no shut

PC

- IP address 10.0.0.10 Subnet mask 255.0.0.0 Default gateway 10.0.0.1

✔ Configure **VLAN interface** on the router

This interface allows for remote access on a switch or router via protocols such as Telnet or Secure Shell(SSH).

- Router(config)#int VLAN 1
- Router(config-if)#no shutdown

As you can see, we've not configured the VLAN interface with an IP address. We could do this but it is unnecessary. We already have an interface fa0/0 of the router with an IP address through which we can Telnet the router from the PC.

✔ Configure a **Telnet password** on VTY lines for remote access

This password is configured on VTY lines. Before you can manage the switch remotely via Telnet, you'll have to provide this password.

- Router(config)#line vty 0 15
- Router(config-line)#password cisco
- Router(config-line)#login

✔ Test Telnet connectivity from **admin PC**

Go to the PC and give the command **telnet 10.0.0.1** (interface gig0/0) and then provide the password (**cisco**). Then to enter privileged mode provide enable password (**admin**).

Telnet & SSH

VLAN: A custom network that is created from one or more local area networks. It enables a group of devices available in multiple networks to be combined into one logical network. The result becomes a virtual LAN that is administered like a physical LAN. The full form of VLAN is defined as Virtual Local Area Network.

Line VTY: VTY stands for Virtual Teletype and is used to configure a virtual port to get the telnet or ssh access of Cisco Router/Switch.

The command, line vty 0 4, will open 5 virtual interfaces, i.e. (0,1,2,3,4) for remote access. That means, 5 different administrators/connections can access the Cisco Router/Switch simultaneously using Telnet or SSH. Cisco hardware supports a maximum of 16 line virtual interfaces, i.e. (0,1,2,3,…,15).

Real-life Example:

✔ Turn on the Telnet client on Windows 10 (Control Panel -> Programs and Features -> Turn windows features on or off).

✔ In Command Prompt enter the following command to show the **Star War** movie in ASCII format.

```
C:\Users\Admin> telnet towel.blinkenlights.nl
```

✔ In Command Prompt enter the following command to play the **Chess Game** of telnet version.

```
C:\Users\Admin> telnet freechess.org 5000
```

✔ In Command Prompt enter the following command to know the weather forecast of specific city.

```
C:\Users\Admin> telnet rainmaker.wunderground.com
```

✔

✔

Telnet & SSH

Telnet is inherently **insecure**. Credential information (usernames and passwords) submitted through telnet is not encrypted and is therefore vulnerable to identity theft. However, users can establish a Secure Shell connection instead to prevent this type of intrusion.

SSH (Security Shell): A client-server protocol, with a **SSH client** and a **SSH server**.

SSH Client: The client machine (such as a PC) establishes a connection to a **SSH server** running on a remote device (such as a router). Once the connection has been established, a network admin can execute commands on the remote device.

1. SSH configuration on a switch

✔ Configure a VLAN interface on the switch

We assign an IP address to the **VLAN** interface of the switch so that we can SSH the switch from the PC using this address.

```
Switch(config)#int VLAN 1
Switch(config-if)#ip address 10.0.0.20   255.0.0.0
Switch(config-if)#no shut
Switch(config-if)#exit
```

✔ Set **hostname** and **domain name** of the switch

Both the hostname and the domain name will be used in the process of generating encryption keys.

Configure hostname

```
Switch(config)# hostname SW1
```

Configure IP domain name

```
SW1(config)# ip domain name admin
```

✔ Generate **encryption keys** for securing the session

```
SW1(config)# crypto key generate rsa
```

✔ Set an **enable password** to enter privileged executive mode and **username and password** for local login

```
SW1(config)# enable password admin
SW1(config)#username admin password cisco
```

✔ Specify the **SSH version** to use

```
Switch(config)# ip ssh version 2
```

✔ Connect to **VTY lines** and configure **SSH** on the lines

```
SW1(config)#line vty 0 15
SW1(config-line)#transport input ssh
SW1(config-line)#login local
```

✔ Test SSH connectivity from the **admin PC**

Go to the PC and give the command: **SSH –l admin** (username) **10.0.0.20** (VLAN IP address) and then provide the password (**cisco**). Then to enter privileged mode provide enable password (**admin**).

1. SSH configuration on a router

Telnet & SSH

✔ Configure IP addresses on the **admin PC** and **interface gig0/0** of the router

Router

- Router(config)#int gig0/0
- Router(config-if)#ip address 10.0.0.1 255.0.0.0
- Router(config-if)#no shut

PC

- IP address 10.0.0.10 Subnet mask 255.0.0.0 Default gateway 10.0.0.1

✔ Set router's **hostname** and **domain name**

Both the hostname and the domain name will be used in the process of generating encryption keys.

Configure hostname

```
Router(config)#hostname myRouter
```

Configure IP domain name

- myRouter(config)# ip domain name admin

✔ Generate **encryption keys** for securing the session

- myRouter(config)# crypto key generate rsa

✔ Set an **enable password** to enter privileged executive mode and **username and password** for local login

- myRouter(config)# enable password admin
- myRouter(config)#username admin password cisco

✔ Specify the **SSH version** to use

- myRouter(config)# ip ssh version 2

✔ Connect to **VTY lines** and configure **SSH** on the lines

- myRouter(config)#line vty 0 15
- myRouter(config-line)#transport input ssh
- myRouter(config-line)#login local

✔ Test SSH connectivity from the **admin PC**

Go to the PC and give the command: **SSH –l admin** (username) **10.0.0.1** (interface IP address) and then provide the password (**cisco**). Then to enter privileged mode provide enable password (**admin**).