

Remote Login Protocols

telnet & ssh

SDC CNW (CSE 4541)

CSE, FET, ITER
SOA University, BBSR-30



Glen E. Clarke & Richard Deal

CCT/CCNA

Routing & Switching Exam Guide

McGrawHill



Todd Lammle

CCNA

Routing & Switching Study Guide

SYBEX, A Wiley Brand

Discussion Flow

- Introduction
 - SSH - Secure Shell
- Remote Access to Cisco Device
 - SSH Configuration
- Telnet - Terminal Network
 - Practice on SSH

Review Questions

Introduction

- Telnet and secure shell(ssh) are application layer protocols used for remote login.
- Both uses TCP at transport layer with port number for telnet is 23 and for ssh is 22.
- They allow a user on a remote client machine to access the resources of another machine.
- Secure Shell (SSH) is more secure than telnet as telnet does not support any encryption techniques.
- Secure Shell (SSH) protocol sets up a secure session that's similar to Telnet over a standard TCP/IP connection.

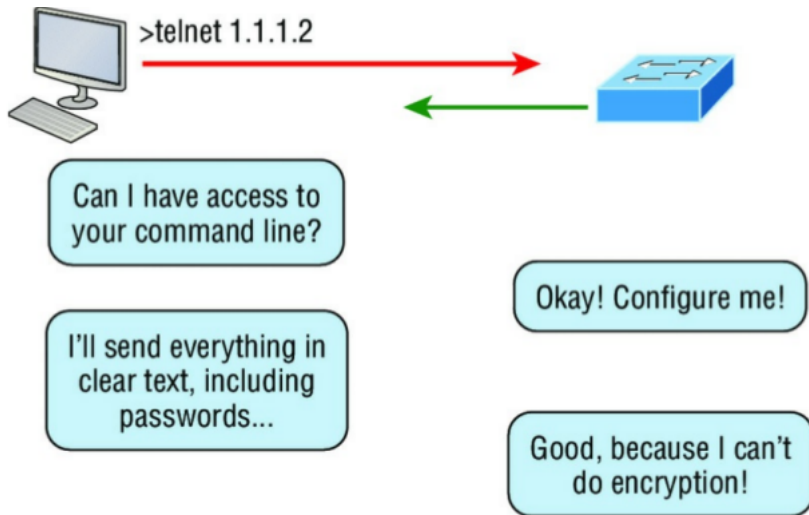
Remote Access to Cisco Device

- In many instances, it may not be possible to be physically in front of your IOS device to manage it.
- It can be optionally managed remotely by accessing its CLI via **telnet** or **SSH**, or it can be managed using GUI with a web browser.
- To access IOS devices CLI remotely, first it's **VTY** is set.
- If a layer 2 IOS **switch** is accessed, It will need to assign an IP address to a VLAN interface.
- If a **router** is accessed, it will need to assign an IP address to one of its interfaces and enable it

Telnet- Terminal Network

- A terminal emulation program that is used to access remote servers.
- It was one of the first Internet standards, developed in 1969.
- It is an application layer protocol that uses TCP with port number 23.
- It uses an 8-bit, byte-oriented data connection over TCP
- It allows a user on a remote client machine, called the **Telnet client**, to access the resources of another machine, the **Telnet server**, in order to access a command-line interface.
- There are no encryption techniques available within the Telnet protocol, so everything must be sent in clear text, including passwords.
- Users begin a Telnet session by running the Telnet client software and then logging into the Telnet server.

A Telnet client trying to connect to a Telnet server



Telnet on CISCO Devices

line vty command: To set the user-mode password for Telnet access into the router or switch.

Switch: Telnet configuration

```
switch>enable
switch#config t
switch(config)#line vty 0 5
switch(config-line)#password telnet
switch(config-line)#login
switch(config-line)#exit
```

Router: Telnet configuration

```
Router>enable
Router#config t
...    #line vty 0 4
        #password telnet2
        #login
Router(config-line)#exit
```

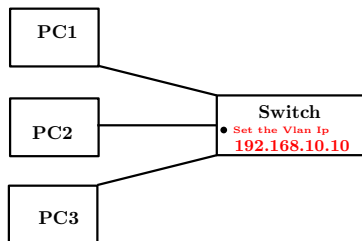
Command Description:

- **line vty:** line configuration
- **line vty 0 4:** No of concurrent users
- **password:** command to set passwordtext
- **login:** Telnet connection with password
- **no login:** Telnet connections without password
- Telnet access: from any command prompt (DOS or Cisco)

Telnet on Layer 2 Switch

Set vty line, telnet password and login for local authentication

```
switch>enable
switch#config t
switch(config)#line vty 0 5
switch(config-line)#password telnet
switch(config-line)#login
switch(config-line)#ctrl+z
```



Set enable password and vlan IP

```
switch#config t
switch(config)#enable password user
switch(config)#interface vlan 1
switch(config-if)#ip address 192.168.10.10 255.255.255.0
switch(config-if)#no shutdown
switch(config-if)#exit
```

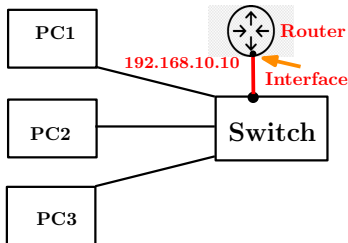
Access from PC/IOS Device

- 1) On PC command prompt: `c:\>telnet 192.168.10.10`
- 2) On **switch** cli prompt: `telnet 192.168.10.10`

Telnet on Router

Set vty line, telnet password and login for local authentication

```
Router>enable
Router#config t
Router(config)#line vty 0 5
Router(config-line)#password telnet
Router(config-line)#login
Router(config-line)#ctrl+z
```



Set enable password and Interface IP

```
Router#config t
Router(config)#enable password user
Router(config)#interface gig0/0/0
Router(config-if)#ip address 192.168.10.10 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

Access from PC/IOS Device

- 1) On PC command prompt: `c:\>telnet 192.168.10.10`
- 2) On Router cli prompt: `telnet 192.168.10.10`

Telnet on a Switch present in OFF-Network

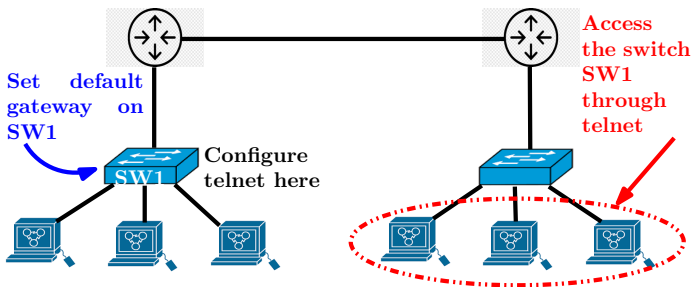


Figure: Accessing a switch from distant network through telnet

Configuration






- Configure IP addresses for the topology.
- Add routing as per requirement.
- Configure telnet at switch SW1.
- Assign IP address at the **Vlan 1 interface** on switch SW1.
- Configure: **SW1 (config)#ip default-gateway <gateway ip>**

SSH - Secure Shell

- ✍ The most common tools used by network administrators to manage their devices remotely is the telnet application.
- ✍ Telnet enables access to the CLI of a device.
- ✍ **The problem with telnet** : all information are sent in clear text, including username and/or password.
- ✍ Since we dont want someone eavesdropping on our connection and seeing everything we do - logging in, viewing the operation of the device, configuring the device, and *authentication traffic*. So, we need to protect ourself by encrypting the traffic.
- ✍ The easiest way to accomplish this is to replace the use of telnet with **SSH (Secure Shell)**.
- ✍ SSH uses RSA as an encryption algorithm to encrypt any data sent between us and our networking device.
- ✍ SSH uses TCP at transport layer with port number 22.
- ✍ SSH is actually disabled by default on your IOS device.

SSH Configuration

The following configuration will be needed to set up SSH on our Cisco device so that we can use an SSH client to access it,

-  **A local username and password:** SSH requires both a username and password configured on the device (command: `username` configures both).
-  **A hostname and a domain name:** Hostname and domain name are required to label the RSA key pair on the IOS device (command: `hostname` and `ip domain-name`).
-  **RSA public and private keys:** We will need to generate the encryption keys. These are used to encrypt and decrypt data that travels through the remote-access connection (command: `crypto key generate rsa`).
-  **The SSH version to use:** We should configure the specific SSH version we want to use. The default is version 1, but the recommended version to use is 2 (`ip ssh version`).
-  **Restricting VTY access:** Finally, we will ensure that remote access can be achieved only through SSH and not telnet, because telnet does not encrypt communication. By default, telnet is allowed on the VTYS- we should ensure that only SSH access is allowed (command: `login local` and `transport input line-subconfiguration`).

SSH Configuration Putting all together

- ① **Set the local user name and password:**

```
Router(config)#username admin password admin@123
```

- ② **Set the hostname:** Router(config)#hostname
③ **Set the domain name:** Router(config)#ip domain-name cnw.edu
④ **Generate the encryption key for securing the session:**

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

- ⑤ **Enable SSH version 2 on the device (Not mandatory, recommended):**

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

- ⑥ **Connect to VTY line of the device:**

```
Router(config)#line vty 0 5
```

- ⑦ **Tell the line to use the local database for username and password:**

```
Router(config-line)#login local
```

- ⑧ **Configure access protocol:**

```
Router(config-line)#transport input ?  
Router(config-line)#transport input ssh  
Router(config-line)#exit
```

Connecting SSH Client to SSH Server

① Through PC's command prompt:

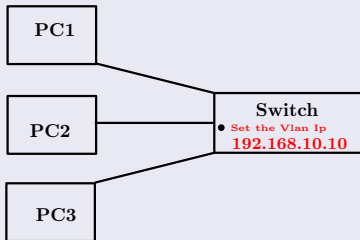
```
C:\>ssh -l username server_ip_address  
  
or  
  
C:\>ssh username@server_ip_address
```

② Through SSH client

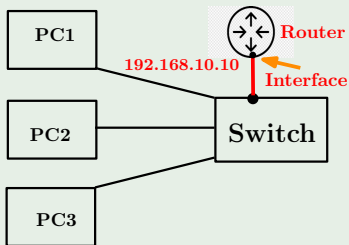
- (a) Click on the SSH client from Desktop menu of the PC
- (b) Add the required informations
- (c) Click on coonect

Practice Question

Configure SSH on Switch



Configure SSH on Router



Review Questions

1. Which of the following commands will configure all the default VTY ports on a switch?

- (A) `Switch# line vty 0 4` (C) `Switch(config-if)#line console 0`
(B) `Switch(config)#line vty 0 4` (D) `Switch(config)#line vty all`

2. Which of the following prompts indicates that the switch is currently in privileged mode?

- (A) `Switch(config)#` (C) `Switch#`
(B) `Switch>` (D) `Switch(config-if)#`

3. To which interface an IP can be assigned to a switch

- (A) interface fa0/1 (C) Both
(B) VLAN interface (D) None of the interface

THANK YOU