Configuring VTY Lines for Multiple Connection Types

About VTY Lines:

VTY, or virtual teletype, are virtual lines available on networking equipment to provide an option for remote management when configured. As a standard, you can set up either Telnet, SSH, or both using just one or multiple VTY lines. There are 17 lines total, ranging from line 0 to line 16. Each line is for a separate connection, so you can have a total of 16 active management connections open to your device. You can assign any number of these lines to a connection type. You can even assign both connection types to varying different lines.

Starting Off

To start off with, you will be using a generic desktop computer, a Cisco 2960 switch, and a Cisco 2911 router in the provided packet tracer project. The only connection you will need between the three devices is a copper straight-through cable which is already connected. An IP address and subnet has already been assigned to the router and computer.

Setting Up a Telnet Connection

For the first part, you will set up a telnet connection on three ports on the router.

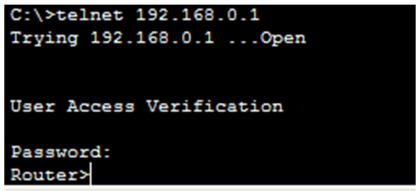
a. Click on the cisco 2911 router and select the "CLI" tab.
b. Enter configure terminal and select the first three VTY lines using "**line vty 0 2**"
c. Set a password for telnet connections using "**password cisco**"
d. Assign telnet to the lines using the command "**login**"

```
Router(config)#
Router(config)#line vty 0 2
Router(config-line)#password cisco
Router(config-line)#login
```

You should now be able to test your setup.

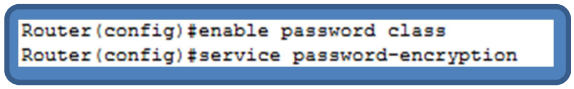
a. Click on PC0 and choose the "Desktop" tab.
b. Select the "**Command Prompt**" option.
c. In command prompt, you enter "**telnet**" followed by the IP of the device you are connecting too, so enter "**telnet 192.168.0.1**"

d. If successful, you will be prompted to enter a password, which you will enter your chosen password "**cisco**".



You will probably notice at this point that you cannot enter "**Enable**" mode without first setting a password. Go back into your routers CLI and enter configure terminal.

a. To set an enable password, enter "enable password class".
b. Since you don't want your passwords being stored in plain text, you can also enter "service password-encryption".



You should now be able to enter enable and configuration modes when using a telnet connection. Since you have assigned lines 0-2, you can have up to three active telnet connections to the router.

Setting Up a SSH Connection

Telnet may be easily set up on your devices, but the one thing it is not is secure. If someone on your network was viewing packets, they could easily see what you enter through telnet since it's not encrypted. That is why it is much better to set your device up with ssh connections as well. It requires a few more steps but is still relatively easy to set up.

a. The first thing you will need to do is assign a hostname and an IP domain name to the router. Select the routers CLI tab and enter configure terminal.
b. Set the hostname using "**hostname R1**" and assign a domain name with "**IP domain-name cisco.com**".
c. In order to have your traffic encrypted and to enable ssh, you will need to enter the command "**crypto key generate rsa**".
d. It will then prompt you to enter a bit length, go ahead and enter 768. The standard length of an RSA key is 512 or 768 for SSHv2.

```
Router(config)#ip domain-name cisco.com
Router(config)#hostname R1
R1(config)#crypto key generate rsa
The name for the keys will be: R1.cisco.com
Choose the size of the key modulus in the range of 360 to 2048
for your
  General Purpose Keys. Choosing a key modulus greater than 512
may take
  a few minutes.

How many bits in the modulus [512]: 768
% Generating 768 bit RSA keys, keys will be non-exportable...[OK]
```

e. Select the remaining VTY lines using "**line vty 3 15**".
f. Assign the lines for SSH use only using "**login local**" and "**transport input ssh**".
g. You will now need to create an account to sign into the router with ssh. First exit out of the VTY line configuration.
h. Create an account using "**username admin privilege 15 secret cisco**"
   - *The privilege number indicates how much rights the user will have, you can lower this number to restrict certain accesses. The secret is the password used to log into the account*.

```
R1(config)#line vty 3 15
R1(config-line)#login local
R1(config-line)#transport input ssh
```

You can now test your SSH setup.

i. Click on the computer and go to the desktop tab and select command prompt.
j. To connect using ssh, packet tracer uses the command "ssh –l username target", so you will need to enter "**ssh –l admin 192.168.0.1**".
k. If successful, it should request a password for the username entered, which would be "**cisco**".

```
C:\>ssh -l admin 192.168.0.1
Open
Password:


R1>
```

If set up correctly, you can now manage your router (or many other Cisco devices) with both Telnet and SSH through remote devices.