```
Cisco Config Elements
=====================

Notes:
------
* Commands preceded with "$" imply that you should execute the command as
  a general user - not as root.
* Commands preceded with "#" imply that you should be working as root.
* Commands with more specific command lines (e.g. "rtr>" or "mysql>")
  imply that you are executing commands on remote equipment, or within
  another program.
* If a command line ends with "\" this indicates that the command continues
  on the next line and you should treat this as a single line.

Exercises Part I
===============

1. Connect to your router
-------------------------

Log in to your vm/pc image and install Telnet:

        $ sudo apt-get install telnet

Connect to router in your group. If you are not sure remember to review the
classroom network diagram:

        http://noc.ws.nsrc.org/wiki/Diagram

Now connect to your router:

        $ telnet 10.10.N.254

        username: cisco
        password: cisco

Display information about your router

        rtrN>enable                             (default pw "cisco")
        rtrN#show run                           (space to continue)
        rtrN#show int FastEthernet0/0
        rtrN#show ?                             (lists all options)
        rtrN#exit                               (log off router)



2. Configure your router to only use SSH
----------------------------------------

These steps will do the following:

        * Create an ssh key for your router
        * Create an encrypted password for the user cisco
        * Encrypt the enable password (cisco)
```

* Turn off telnet (unencrypted) access to your router
        * Turn on SSH (version 2) access to your router

You need to work in groups of 4. Get together with the members of your router
group and assign one person to enter commands. To start connect to one of the
PCs in use by your group. From that PC image telnet to your router:

        $ telnet rtrN.ws.nsrc.org   (or "telnet 10.10.N.254")

        username: cisco
        password: cisco

        rtrN> enable   (en)
        password: cisco
        rtrN# configure terminal   (conf t)
        rtrN(config)# aaa new-model
        rtrN(config)# crypto key generate rsa

        How many bits in the modulus [512]: 2048

Wait for the key to generate. You can now specify passwords and they will be
encrypted. First let's remove our cisco user temporarily, then we'll recreate
the user:

        rtrN(config)# no username cisco
        rtrN(config)# username cisco secret 0 cisco

Now the cisco user's password (of cisco) is encrypted. Next let's encrypt
the enable password as well:

        rtrN(config)# enable secret 0 cisco

Now we'll tell our router to only allow SSH connections on the 5 defined
consoles (vty 0 through 4):

        rtrN(config)# line vty 0 4
        rtrN(config-line)# transport input ssh
        rtrN(config-line)# exit

This drops us out of the "line" configuration mode and back in to the general
configuration mode. Now we'll tell the router to log SSH-related events and to
only allow SSH version 2 connections:

        rtrN(config)# ip ssh logging events
        rtrN(config)# ip ssh version 2

Now exit from configuration mode:

        rtrN(config)# exit

And, write these changes to the routers permament configuration:

        rtrN# write memory   (wr mem)

Ok. That's it. You can no longer use telnet to connect to your router. You must connect using SSH with the user "cisco" and password "cisco". The enable password is, also, "cisco" - Naturally in a real-world situation you would use much more secure passwords.

Let's exit from the router interface and reconnect using SSH:

        rtrN# exit

First, try connection again with telnet:

        $ telnet rtrN.ws.nsrc.org

What happens? You should see something like:

        Trying 10.10.N.254...
        telnet: Unable to connect to remote host: Connection refused

Now try connecting with SSH:

        $ ssh cisco@rtrN.ws.nsrc.org

You should see:

        The authenticity of host 'rtr2.ws.nsrc.org (10.10.2.254)' can't be
        established. RSA key fingerprint is 93:4c:eb:ad:5c:4a:a6:3e:8b:9e:
        4f:e4:e2:eb:e4:7f. Are you sure you want to continue connecting
        (yes/no)?

Enter in "yes" and press ENTER to continue...

Now you'll see the follwoing:

        Password: cisco
        rtrN>

Type "enable" to allow us to execute privileged commands:

        rtrN> enable
        Password: cisco
        rtrN#

Now let's view the current router configuration:

        rtrN# show running   (sh run)

Press the space bar to continue. Note some of the entries like:

        enable secret 5 1p4/E$PnPk6VaF8QoZMhJx56oXs.
        .
        .
        .
        username cisco secret 5 1uNg1$M1yscHhYs..upaPP4p8gX1
        .

```
         .
         .
      line vty 0 4
       exec-timeout 0 0
       transport input ssh
```

You can see that both the enable password and the password for the user cisco
have been encrypted. This is a good thing.

Now you should exit the router interface to complete this exercise:

        rtrN# exit

NOTES

1.) If you are locked out of your router after this exercise let your
    instructor know and they can reset your router's configuration back to its
    original state.

2.) Please only do this exercise once. If multiple people do this exercise
    it's very likely that access to the router will be broken.
3.) During the week you will configure items such as SNMP, Netflow and more on
    your group's router. From now on you can simply connect to the router
    directly from your laptop or desktop machine using SSH.