**TITLE:** To bypass a cisco router password using CISCO Packet Tracer.

**PROJECT MEMBERS:** Utsav Jain(22)

Rachana Kamat(28)

Priya Puranik(54)

**ABSTRACT:**

Using passwords and assigning privilege levels is a simple way of providing terminal access control in your network.Cisco router password can be easily hacked if no encryption is enabled. Cisco Packet Tracer effortlessly provides an additional layer of security, particularly for passwords that cross the network . Cisco commands allows to establish an encrypted password that users must enter to access enable mode (the default), or any privilege level user specify.Unauthorized individuals are prohibited from viewing your password in your configuration file.

**INTRODUCTION:**

**Packet Tracer** is a [cross-platform](https://en.wikipedia.org/wiki/Cross-platform) visual [simulation](https://en.wikipedia.org/wiki/Simulation) program designed by [Cisco Systems](https://en.wikipedia.org/wiki/Cisco_Systems) that allows users to create [network topologies](https://en.wikipedia.org/wiki/Network_topologies) and imitate modern [computer networks](https://en.wikipedia.org/wiki/Computer_networks). The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a [drag and drop](https://en.wikipedia.org/wiki/Drag_and_drop) user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused towards Certified Cisco Network Associate Academy students as an educational tool for helping them learn fundamental CCNA concepts. Students enrolled in a CCNA Academy program can freely download and use the tool free of charge for educational use.

In addition to simulating certain aspects of [computer networks](https://en.wikipedia.org/wiki/Computer_networks), Packet Tracer can also be used for collaboration. As of Packet Tracer 5.0, Packet Tracer supports a multi-user system that enables multiple users to connect multiple topologies together over a [computer network](https://en.wikipedia.org/wiki/Computer_network). Packet Tracer also allows instructors to create activities that students have to complete. Packet Tracer is often used in educational settings as a learning aid. Cisco Systems claims that Packet Tracer is useful for network experimentation.

Packet Tracer is a cross-platform network simulator designed by Cisco Systems to run on Mac OS, Linux and Microsoft Windows. A similar Android app is also available. Packet Tracer allows users to create simulated network topologies by dragging and dropping routers, switches and various other types of network devices. A physical connection between devices is represented by a "cable" item. Packet Tracer supports an array of simulated [Application Layer protocols](https://en.wikipedia.org/wiki/Application_Layer), as well as basic routing with [RIP](https://en.wikipedia.org/wiki/Routing_Information_Protocol), [OSPF](https://en.wikipedia.org/wiki/OSPF), [EIGRP](https://en.wikipedia.org/wiki/EIGRP),[BDP](https://en.wikipedia.org/wiki/Bandwidth-delay_product), to the extents required by the current [CCNA](https://en.wikipedia.org/wiki/CCNA) curriculum. As of version 5.3, Packet Tracer also supports the [Border Gateway Protocol](https://en.wikipedia.org/wiki/Border_Gateway_Protocol).

Version 6.0 added support for IOS version 15 and [Hot Standby Routing Protocol](https://en.wikipedia.org/wiki/Hot_Standby_Routing_Protocol). Version 6.1.1 added support for various DHCP, EIGRP and OSPF commands, improved support for Zone-Based Firewall policies. As of version 6.2, Packet Tracer supports an embedded [web server](https://en.wikipedia.org/wiki/Web_server) with JavaScript and CSS support. The command line can be used for creating a router-to-pc connection.

**ROLE IN EDUCATION**

Packet Tracer[1] allows students to design complex and large networks, which is often not feasible with physical hardware, due to costs. Packet Tracer is commonly used by CCNA Academy students[2], since it is available to them for free. However, due to functional limitations, it is intended by Cisco to be used only as a learning aid, not a replacement for Cisco [routers](https://en.wikipedia.org/wiki/Router_(computing)) and [switches](https://en.wikipedia.org/wiki/Network_switch).The application itself only has a small number of features found within the actual hardware running a current [Cisco IOS](https://en.wikipedia.org/wiki/Cisco_IOS) version. Thus, Packet Tracer is unsuitable for modelling production networks. It has a limited command set, meaning it is not possible to practice all of the IOS commands that might be required.

Packet Tracer can be useful for understanding [abstract](https://en.wikipedia.org/wiki/Abstraction) [networking concepts](https://en.wikipedia.org/w/index.php?title=Networking_concepts&action=edit&redlink=1), such as the [Enhanced Interior Gateway Routing Protocol](https://en.wikipedia.org/wiki/EIGRP) by animating these elements in a [visual form](https://en.wikipedia.org/wiki/Information_visualization).Packet Tracer is also useful in education by providing additional components, including an authoring system, network protocol simulation and an assessment system.

**LITERATURE:**

Packet Tracer is a cross-platform visual simulation program designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface.Bypassing a router is a common and early step in troubleshooting internet connection problems.

1. To bypass the router, simply disconnect the ethernet cable that runs from the modem to the router from the back of the router,
2. Plug that ethernet cable directly into the back of the computer.
3. Then power cycle the modem to make sure that it is able to recognize the computer that is connected to it.

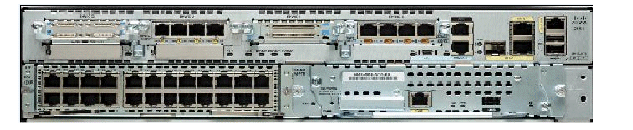


Fig 1.1: The rear of the 2951 router

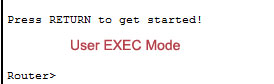
Cisco IOS supports various command modes[3], among those following modes are the highly tested in CCNA level exam.

1. User EXEC Mode
2. Privileged EXEC Mode
3. Global Configuration Mode
4. Interface Configuration Mode
5. Sub Interface Configuration Mode
6. Setup Mode
7. ROM Monitor Mode

We need to execute specific commands to navigate from one mode to another. Following section describe IOS command modes with specific navigation commands in details.

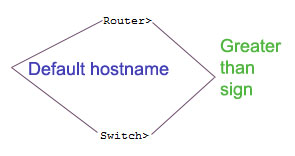
1. **User EXEC Mode**

This is the primary mode when you logged in router. On job environment, it is usually password protected. You need a valid username and password to access this mode. You have three chances to enter a valid password, before connection attempt is refused. On LAB environment, you could access this mode directly ( unless you have configured it for password).



User Exec Mode Command Prompt

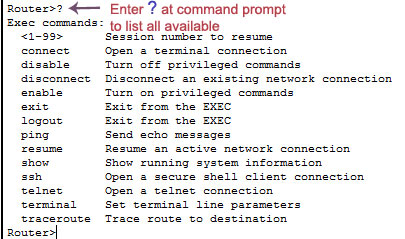
By default, it consists device hostname followed by a greater than sign. For router default hostname isRouter. For switch default hostname is Switch.



Default hostname can be changed from global configuration mode using *hostname* command.

User exec mode is the subset of privileged exec mode. For security purposes, this mode is reserved for tasks that do not change the configuration of router. It has limited commands those allow you to connect to remote devices, change terminal line settings on a temporary basis, perform basic tests and list system information.

Enter ? at command prompt to list all available commands on this mode.



**2. Privileged Exec Mode**

Privileged exec mode is the main exec mode. Same as user exec mode on job environment, this mode is also password protected. You have to enter the password to access this mode. In lab environment, it's usually unprotected. You can access this mode by executing *enable* command at user exec mode.



Most commands of this mode are one time commands, like show or clear commands, which show current configuration status and clear counters on interfaces respectively. You can list all available commands of this mode by entering ? at command prompt.

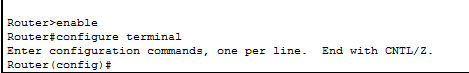
This mode has all commands available for exec mode including user exec mode.

Common commands can be entered either from user exec mode or privileged exec mode.

Exec mode commands are not saved across the reboot of device.

**3. Global Configuration Mode**

Global configuration mode is the next access level in IOS mode sequence. This mode is used to configure device globally, or to enter in element like interface, protocols specific configuration mode. Use *configure terminal* command at privileged exec mode to access global configuration mode.



Global configuration mode and element specific configuration mode allow you to make change in running configuration. By default running configuration is not stored across the reboot, but you can save running configuration to preserve it across the reboot. To save running configuration use *copy running-config startup-config* from privileged EXEC mode commands.

To return in privileged exec mode from global configuration mode or element specific configuration mode we have three commands.

* Ctrl + Z ( Press CTRL key with Z Key)
* exit
* end

Ctrl+Z key combination will work in all mode. But it has a drawback, if you pressed Ctrl+Z at the end of a command line in which a valid command has been typed, that command will be added in the running configuration file.

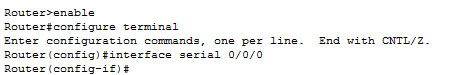
exit command only works in global configuration mode.

end command is the safest way to exit from global configuration mode or interface specific mode. It will always take you back in privileged EXEC mode regardless of which configuration mode or configuration sub-mode you are in.

**4. Interface configuration mode**

Interface configuration mode is used to configure interface related settings. Many settings are enabled on a per-interface basis like as serial port, Ethernet. Interface configuration commands affect interface related settings, such as enable or disable interface, bandwidth, clock rate etc. To configure or change these setting, you need to enter in interface specific mode. To access interface configuration mode use following command.

Router(config)# interface type number



For example, to configure first serial port on 1841 series router we would use following command

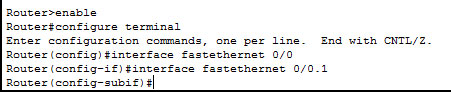
Router(config)#interface serial 0/0/0

**5. Sub Interface Configuration Mode**

If interface supports virtualization, then sub interface mode is used to configure the virtual interface. From sub interface configuration mode you can configure multiple virtual interfaces known as sub interface on a single physical interface. On router usually virtual interfaces are used for wan connection such as Frame Relay. Frame Relay connection supports multiple point-to-point links known as PVC ( Permanent virtual circuits). PVC can be combined under the separate sub interfaces those are configured on a single physical interface. Another example of sub interface is VLAN communication, where we create sub interface on physical FastEthernet port for each VLAN. To access sub interface configuration mode run following command from interface configuration mode.

Router(config-if)#

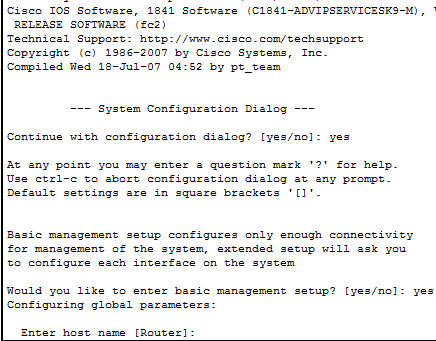
interface type number



In above example fastethernet 0/0.1 is the virtual interface ( sub interface ) of physical interface fastethernet 0/0.

**6. Setup Mode**

At the end of booting process, router tries to locate running configuration. If it finds the configuration, it would load that. If it fails to find valid configuration, it would initiate the setup mode. In Setup Mode router will ask you questions about the initial settings in a sequence for basic configuration values. Depending on answers provided by you, router will automatically build initial configuration.



Router will enter in setup mode only if it does not find the valid configuration.

**7. ROMMON Mode**

During the boot process, router loads IOS image in RAM. If it does not find a valid IOS image, it would enter in ROMMON mode. You can manually enter in this mode by interrupting boot sequence during the startup. This mode is used for diagnostic purpose. By default router does not enter in this mode unless it completely fail to locate the IOS image. To manually enter in this mode, execute reload command from privileged exec mode and then press CTRL + C key combination during the first 60 seconds of startup.



**IMPLEMENTATION DETAILS:**

**Setting up the password**[4]**:**

1. Console into the router and enter the privleged mode EXEC using the command 'enable'
2. Type '# config ter' - This opens the configuration terminal wherein the initial password and the hostname can be set
3. Configure your hostname as required using command 'hostname <>'
4. Using command enable password < > you can set the password of your router
5. The exit command will now redirect you to the user mode from the privileged mode
6. copy run start
7. reload

**Recovering and Encryption of the password:**

1. Reboot the router and press the Break key to interrupt the boot sequence.
2. Type confreg 0x2142. This tells the router to bypass NVRAM during bootup. In other words, your existing configuration won't be loaded. It won't be deleted either.
3. Type reset to reboot the router. Answer No when prompted to run setup.
4. Type copy start run. This loads your startup configuration into memory. Now, if you type a show run config, you'll see the router configuration. Also, you should notice that your router name is now in the prompt instead of the default “Router”.
5. Change the enable secret - “enable secret new\_password”
6. Change the register back to 0x2102:
7. config-register 0x2102
8. When the router reboots it will load the old configuration with the new password.
9. Save the password so that it will be persistent during reboots, type copy run start
10. Reboot the router by typing reload at the enable prompt.
11. The password is now recovered and set.

**SNAPSHOT:**

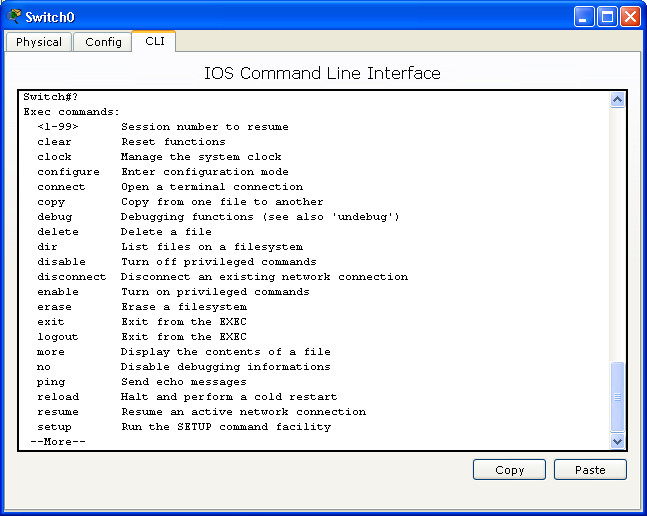


Fig 1.2: Command Line Interface

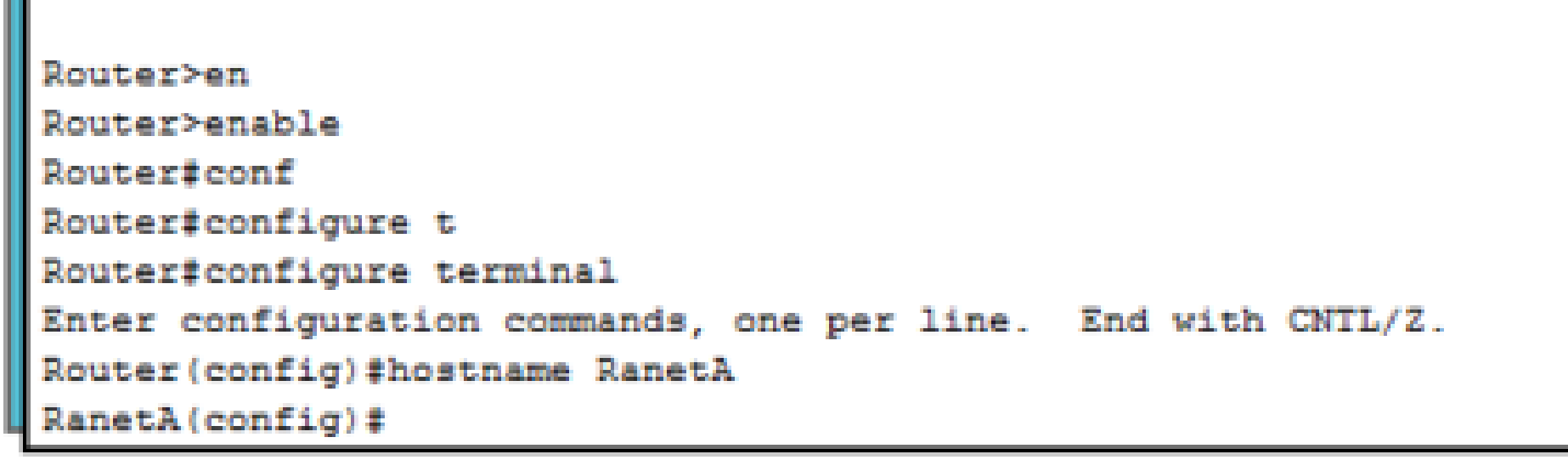


Fig 1.3: Entering Router mode

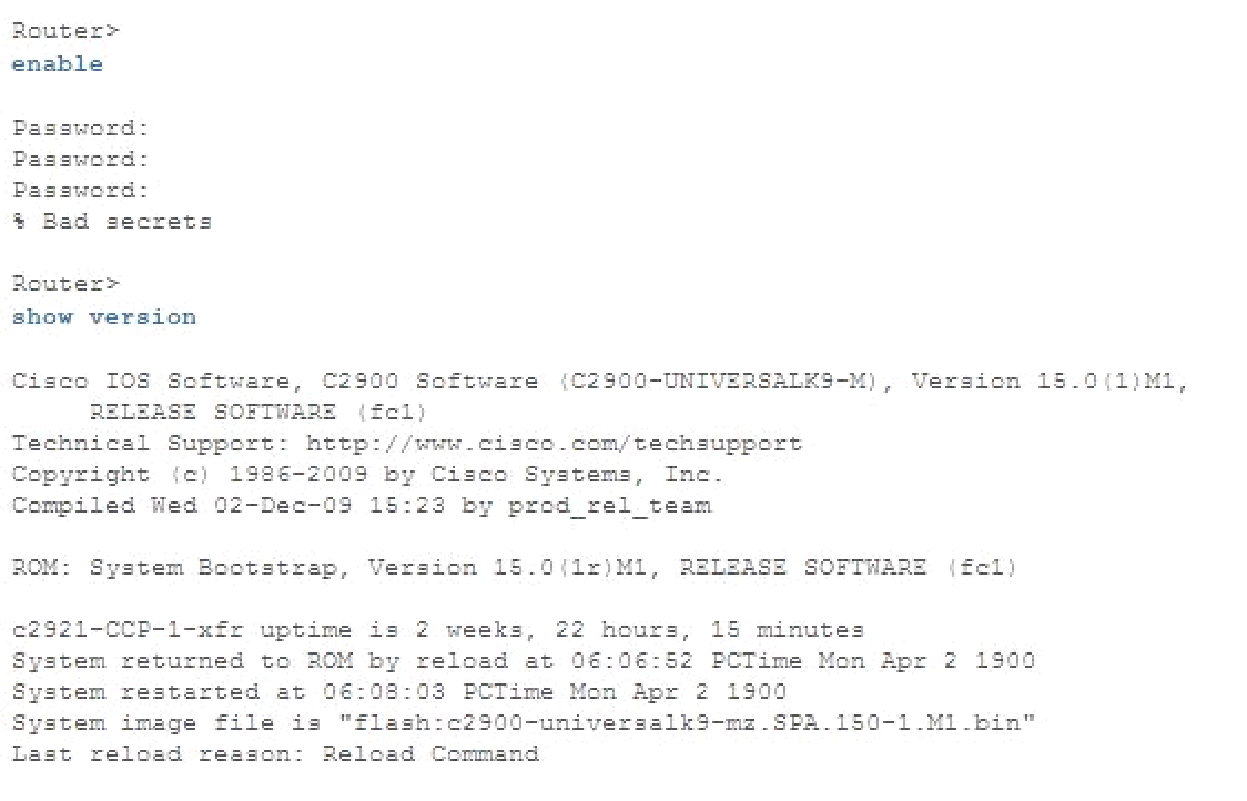


Fig 1.4: Entering incorrect passwords

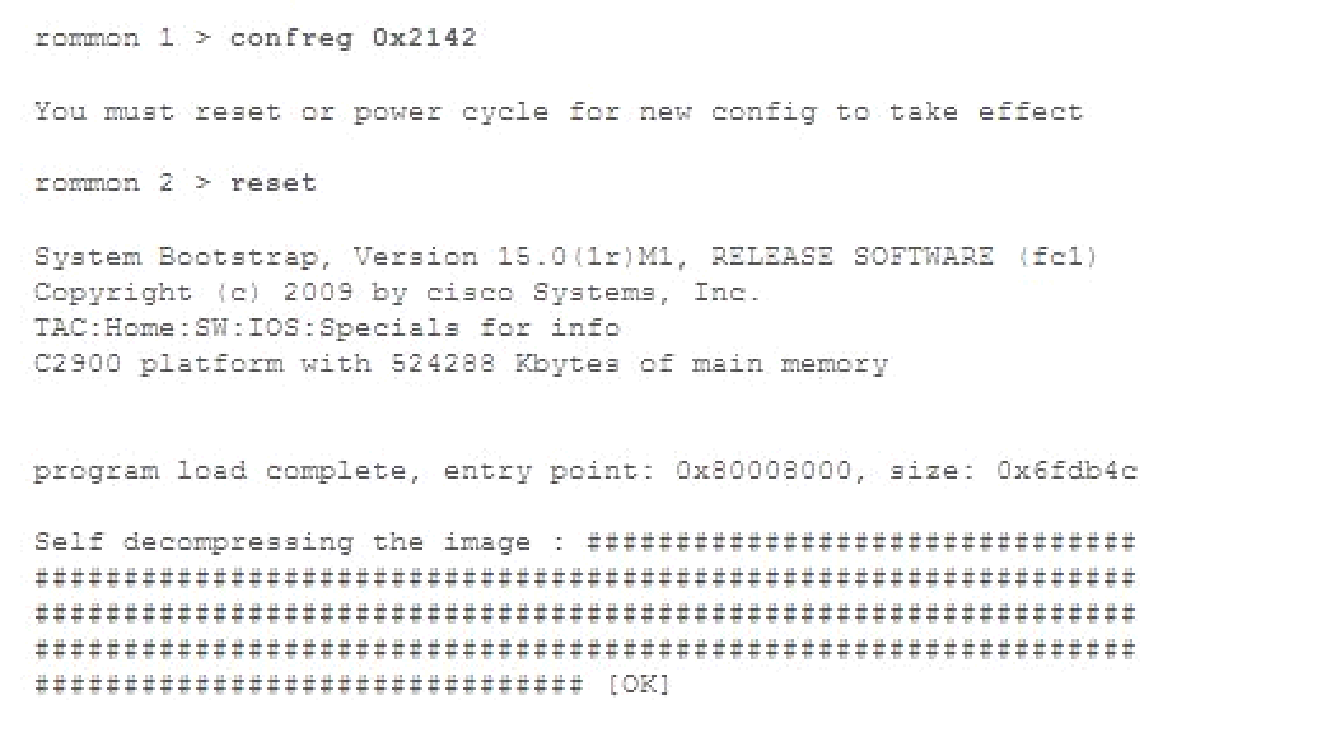


Fig 1.5: Reset the router

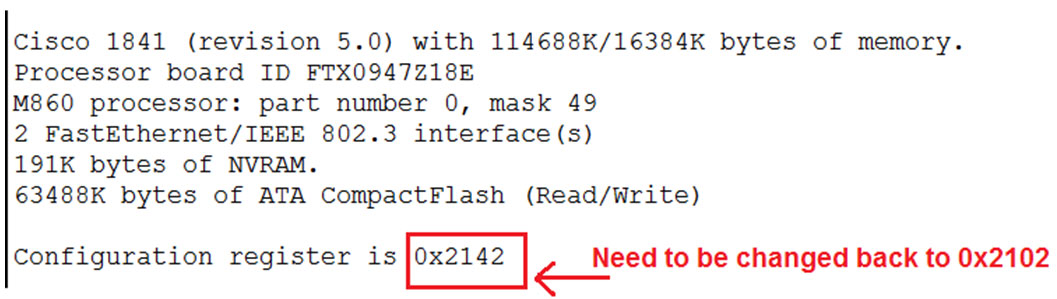


Fig 1.6: Configuration after reseting password

**CONCLUSION:** This demonstration describes how to recover the **enable password** and the **enable secret** passwords. These passwords protect access to privileged EXEC and configuration modes. The **enable password** password can be recovered, but the **enable secret** password is encrypted and must be replaced with a new password.

**REFERENCES:**

[1**]**<http://www.cisco.com/c/en/us/support/docs/routers/2800-series-integrated-services-routers/112033-c2900-password-recovery-00.html>

[2]<http://www.certiology.com/cisco-certifications/ccna/ccna-routing-and-switching/free-cisco-ccna-study-guide/cisco-router-password-recovery.html>

[3]<http://www.computernetworkingnotes.com/ccna-study-guide/cisco-ios-mode-explained-with-examples.html>

[4]<http://www.cisco.com/c/en/us/support/docs/routers/2600-series-multiservice-platforms/22188-pswdrec-2600.html>