



APNIC Members' Training Course  
Security workshop

**2 - 4 July, 2008**

**Port Vila  
Vanuatu**

**In conjunction with**

**PACNOG 4**

## Router device security lab

### 1. APNIC's remote lab

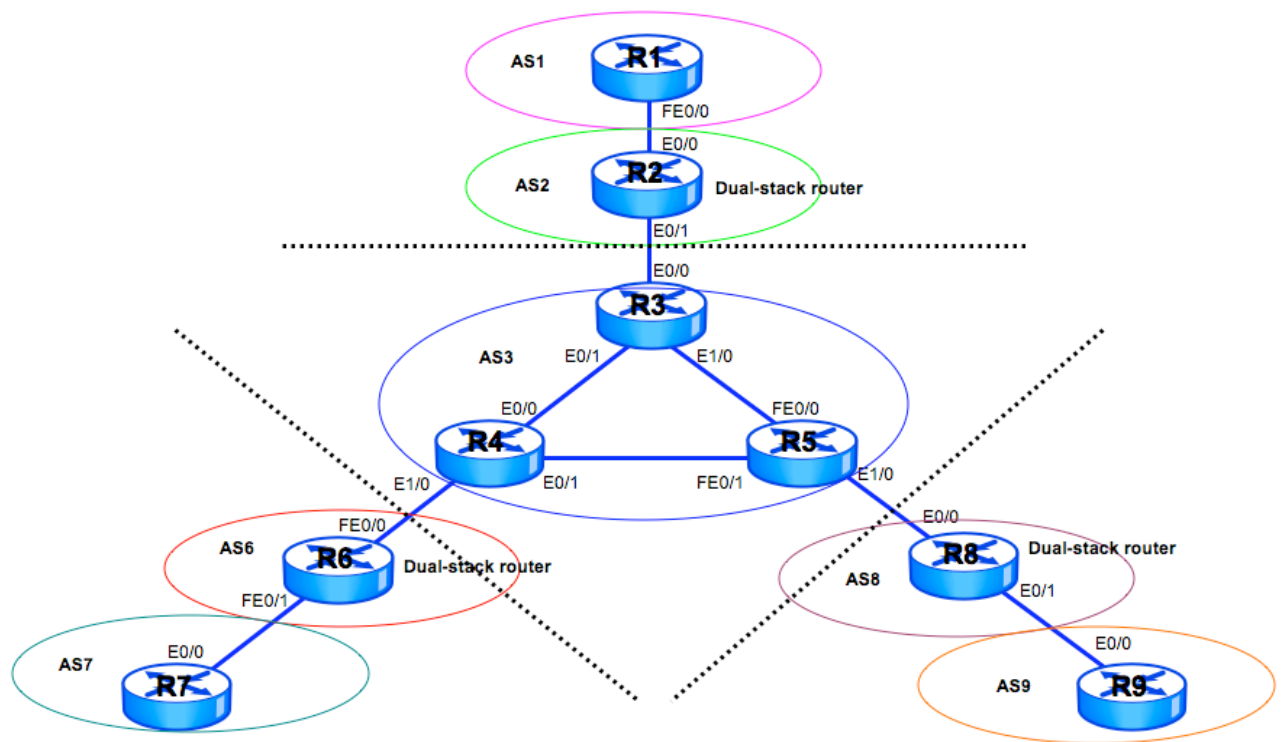
In these exercises you will be remotely accessing and using the APNIC training lab.

The lab can be configured to emulate basic Internet topologies and is made up of 16 routers, 3 switches, a KVM switch and PCs and servers. The majority of the routers are Cisco devices but there are also a number of Juniper machines as well. The lab is intended to support APNIC training by providing the opportunity for practical exercises to be conducted on workshops throughout the region.

The lab topology is configured using VLANs so can easily be adapted and changed to meet the training requirements

Access to the lab is through ssh access to a terminal server and then by reverse ssh access to the router or switch console ports over direct serial connections

For the exercises that will be conducted in this workshop, the lab will be configured as shown in the diagram below. However, the actual **interfaces** may be different to the diagram so please refer to the table listing after this diagram.



## 2. Recap Cisco IOS basic skills

Reference: Cisco 1600 Series Software Configuration Guide

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_mod/1600/1600swcf/swskills.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1600/1600swcf/swskills.htm)

<http://www.ciscopress.com/articles/article.asp?p=99029&seqNum=2&rl=1>

### 2-1. Command modes

The Cisco IOS has several modes. While configuring routers you will go in and out of several different modes. The following section recaps several basic modes.

Mode	Access method	Prompt	Exit method	About this mode
User EXEC	Begin a session with your router.	Router>	<b>logout</b>	A subset of the commands available in this mode: Use this mode to: Change terminal settings Perform basic tests Display system information
Privileged EXEC	Enter the enable command while in user EXEC mode.	Router#	<b>disable</b>  To enter global configuration mode, enter <b>configure</b> command	Use this mode to: Configure your router operating parameters. Perform the verification steps shown in this guide. To prevent unauthorised changes to your router configuration, access to this mode should be protected with a password.
Global configuration	Enter the configure command while in privileged EXEC mode.	Router (config)#	<b>exit, end or Ctrl-z</b>  To enter interface configuration mode, enter the <b>interface</b> command	Use this mode to configure parameters that apply to your router as a whole
Interface configuration	Enter the interface command (with a specific interface) while in the global configuration mode.	Router (config-if)#	<b>end</b>  To exist to privileged EXEC mode, enter the <b>exit</b> command, or press <b>Ctrl-z</b> .  To enter subinterface configuration	Use this mode to configure parameters for the various LAN and WAN interfaces of your router, including the: <ul style="list-style-type: none"><li>• Ethernet interface</li><li>• Serial interface</li><li>• ISDN inerface</li></ul>

			mode, specify a subinterface with the interface command.	
Router configuration	Enter your router command followed by the appropriate keyword while in global configuration mode.	Router(config-router)#	<b>end</b>  To exit to privileged EXEC mode, enter the <b>exit</b> command, or press <b>Ctrl-z</b> .	Use this mode to configure an IP routing protocol.
Line configuration	Specify a line with the line vty command while in the global configuration mode.	Router(config-line)#	<b>exit</b>  To enter privileged EXEC mode, enter the <b>end</b> command, or press <b>Ctrl-Z</b>	Use this mode to configure parameters for the terminal.

## 2.2. Getting help

You can use the question mark “?” and arrow keys to help you enter commands.

For a list of available commands at that command mode, enter a question mark:

Router>?

To complete a command, enter a few known characters followed by a question mark (with no space):

Router>s?

For a list of command variables, enter the command followed by a space and a question mark:

Router>show ?

To display a command you previously entered, press the up-arrow key. You can continue to press the up arrow key for more commands.

## 2.3. Save your configuration

You need to enter the **copy running-config startup-config** command to save your configuration changes to NVRAM (Non-Volatile Random Access Memory) so that they are not lost if there is a system reload or power outage.

Router# **copy running-config startup-config**

Building configuration...

After the configuration has been saved, the following appears:

[OK]

Router#

### 3 Setting up the security lab environment

We will configure a single OSPF network to create the environment for the security lab.

#### 3.1 Configure the router interfaces

Using the table provided below, configure the interfaces on your routers with the appropriate addresses. Note: the address blocks being used are /23s. The point-to-point addresses are /30s taken from the address block of one of the routers on the point-to-point link. Be careful to use the correct mask.

Configure the loopback address as given

Each router is allocated the following /23 address block.

Router number	IP address subnet	Router number	IP address subnet
Router 1	192.168.0.0/23	Router 6	192.168.60.0/23
Router 2	192.168.20.0/23	Router 7	192.168.70.0/23
Router 3	192.168.30.0/23	Router 8	192.168.80.0/23
Router 4	192.168.40.0/23	Router 9	192.168.90.0/23
Router 5	192.168.50.0/23		

The following point-to-point (/30) addresses are used to connect the routers

Routers	IP address	Routers	IP address
Router1 – Router2	192.168.0.0/30	Router6 – Router7	192.168.60.0/30
Router2 – Router3	192.168.20.0/30	Router5 – Router8	192.168.50.0/30
Router3 – Router4	192.168.30.0/30	Router8 – Router9	192.168.80.0/30
Router3 – Router5	192.168.31.0/30		
Router4 – Router5	192.168.40.0/30		
Router4 – Router6	192.168.41.0/30		

**Interface address assignment chart – refer to this when configuring your interfaces**

Router	if	IP address	Router	if	IP address
1	E0/0	192.168.10.1	5	E0/0.2	192.168.40.2
2	F0/0	192.168.10.2	5	E0/0.1	192.168.31.2
2	F0/1	192.168.20.1	5	E0/1	192.168.50.1
3	F0/1	192.168.20.2	6	E0/1	192.168.41.2
3	F0/0.1	192.168.30.1	6	E0/0	192.168.60.1
3	F0/0.2	192.168.31.1	7	F0/0	192.168.60.2
4	E0/0.1	192.168.30.2	7	F0/1	192.168.100.2
4	E0/1	192.168.41.1	8	F0/1	192.168.50.2
4	E0/0.2	192.168.40.1	8	F0/0	192.168.80.1
			9	F0/0	192.168.80.2

```
Router#configure terminal
Router(config)#interface e0/0
```

(<- this is just an example. Please use your own relevant interface id. See the interface address assignment chart at the bottom of this section, if you need some assistance. Most routers (except R1, R7 and R9) have two or three interfaces so configure all of them with relevant IP addresses. Note the use of sub-interfaces)

```
Router(config-if)# ip address address subnet-mask
(e.g. ip address 192.168.1.1 255.255.255.252)
```

**The following loopback addresses are used for each router.**

Router Number	Loopback IP address	Router Number	Loopback IP address
Router 1	192.168.10.254/32	Router 6	192.168.60.254/32
Router 2	192.168.20.254/32	Router 7	192.168.70.254/32
Router 3	192.168.30.254/32	Router 8	192.168.80.254/32
Router 4	192.168.40.254/32	Router 9	192.168.90.254/32
Router 5	192.168.50.254/32		

```
Router(config)#interface loopback 0
Router(config-if)#ip address ip-address mask
(e.g. ip address 192.168.1.254 255.255.255.255)
Routersh(config-if)#exit
```

### 3.2 Configure OSPF for the network

Create a single OSPF network with a single OSPF Area.

```
Router(config)#router ospf process ID
```

(You can use any integer number. Each router can use their own OSPF process ID.)

```
Router(config-router)#network ip-address wildcard-mask
area area-id
```

**Use 0 for the area-id in this lab.**

```
Router(config-router)#network ip-address wildcard-mask
area area-id
```

This is for the point-to-point interfaces.  
(e.g. network 192.168.1.0 0.0.0.3 area 0)

Once you configure the above, verify connectivity with using the following commands.

**ping** (to check IP layer connectivity)

```
sh ip router (to check the routing table)
sh ip ospf interface (to check interface participating
OSPF)
sh ip ospf neighbour (to check neighbour list)
sh ip ospf database (to check database summary list)
```

**Important:** Please ensure that OSPF is correctly configured and that network connectivity is working..

#### 4.1.Enabling password for line vty 0 4

In order to allow reverse telnet from other routers to your router, configure line vty 0 4 with the following command (we will explain more about line vty later ).

```
Router(config)#service password-encryption
Router(config)#line vty 0 4
Router(config-line)#password <password>
```

Check these configurations by telnetting to other routers. You will need to ask for the password!!

#### 4.2 Disable DNS name resolutions

By default all name queries are sent to the broadcast address 255.255.255.255. If no Domain Name System (DNS) server is specifically required for the router configuration, you should change the default behavior and turn off the automatic lookup, Use the following command

```
Router(config)#no ip domain-lookup
```

### 5 Configuring secure passwords

**5.1** Configure the enable secret and password using the following commands.

```
Router(config)#enable secret letmein (<- This is an
example.)
Router(config)#enable password TRUSTME (<- This is an
example.)
```

Try to see the configuration file with the following commands:

```
Router#sh run
```

You should see something like the following.

---

```
service password-encryption
!
hostname Router
!
!
enable secret 5 $1$d5NK$Wx4BgOwa8KAfeg8HLzTII1
enable password 7 071B33595D1D1400
!
```

---

**Note 1-1.**

Note the difference between the number '5' and number '7'. This indicates the encryption technique used to encrypt the password.

Also, note that the command 'service password encryption' is in the configuration file. This command is enabled by default and ensures that passwords and secrets in the configuration files are stored in an encrypted form.

Confirm your password and secret that you typed in as clear text form are now encrypted.

**Verify 1-1.** Confirm enable secret and enable password

Logout from the current telnet session and login again.

Change to privileged mode. You will be prompted for the password. Try using the password "TRUSTME". What happens?

Now try using the password "letmein".

What happens?

---

**Note 1-2.**

**enable secret and enable password**

Reference: <http://www.cisco.com/warp/public/701/64.html>

**The enable password command should no longer be used. Use the enable secret command for better security.** The only instance in which the enable password command might be tested is when the device is running in a boot mode that does not support the enable secret command.



Enable secrets are hashed using the MD5 algorithm. As far as anyone at Cisco knows, it is impossible to recover an enable secret based on the contents of a configuration file (other than by obvious dictionary attacks).

## Configuring console and Vty access

**Exercise 2-1.** Configure the console interface with a timeout of 15 minutes.

```
Router(config)#line console 0
Router(config-line)#exec-timeout 15 0 (<- Default is 10
min.)
```

### Note 2-1.

Reference:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products\\_configuration\\_example09186a0080204528.shtml](http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_configuration_example09186a0080204528.shtml)

The use of password protection to control or restrict access to the Command Line Interface (CLI) of your router is one of the fundamental elements of an overall security plan.

Protecting the router from unauthorized remote access, typically, Telnet, is the most common security that needs configuring, but protecting the router from unauthorised local access cannot be overlooked.

Command line, or EXEC, access to a router can be made in a number of ways, but in all cases the inbound connection to the router is made on a TTY line. There are four main type of TTY lines as below:

Router# sh line

Tty	Type	Tx/Rx	A	Modem	Roty	AccO	AccI	Uses	Noise	Overruns	Int
* 0	CTY		-	-	-	-	-	0	0	0/0	-
64	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
65	AUX	9600/9600	-	-	-	-	-	0	0	0/0	-
66	VTY		-	-	-	-	-	0	0	0/0	-
67	VTY		-	-	-	-	-	0	0	0/0	-
68	VTY		-	-	-	-	-	0	0	0/0	-
69	VTY		-	-	-	-	-	0	0	0/0	-
70	VTY		-	-	-	-	-	0	0	0/0	-

Line(s) not in async mode -or- with no hardware support:  
1-64

The **CTY** line-type is the Console Port. On any router, it appears in the router configuration as **line con 0** and in the output of the show line command as **cty**. The console port is mainly used for local system access using a console terminal.

The **TTY** lines are asynchronous lines used for inbound or outbound modem and terminal connections and can be seen in a router or access server

configuration as **line x**. The specific line numbers are a function of the hardware built into or installed on the router or access server.

The **AUX** line is the Auxiliary port, seen in the configuration as **line aux 0**.

The **VTY** lines are the Virtual Terminal lines of the router, used solely to control inbound Telnet connections. They are virtual, in the sense that they are a function of software – there is no hardware associated with them. They appear in the configuration as **line vty 0 4**.

Each of these types of lines can be configured with password protection. Lines can be configured to use one password for all users, or for user-specific passwords. User-specific passwords can be configured locally on the router, or you can use an authentication server to provide authentication.

There is no prohibition against configuring different lines with different types of password protection. It is, in fact, common to see routers with a single password for the console and user-specific passwords for other inbound connections.

If you are interested in learning about setting up different types of password protection to each line, read the Cisco IOS manual from the above URL.

## 7 Enable SSH connectivity

**Exercise 7-1.** Enable SSH connectivity (by setting up a SSH server). This is much more secure than telnet. Enable your router with SSH by applying the following steps.

**Step1:** To generate an RSA key pair, which is required for SSH, enter the following command:

```
Router(config)#crypto key generate rsa general-keys  
modulus 1024
```

You will see something like the following:

```
Router(config)#crypto key generate rsa general-keys modulus 1024  
The name for the keys will be: Router7.training.net
```

```
% The key modulus size is 1024 bits  
% Generating 1024 bit RSA keys ...[OK]
```

```
Router(config)#  
2w4d: %SSH-5-ENABLED: SSH 1.5 has been enabled
```

**Step2:** To save the RSA keys to persistence flash memory, enter the following command:

```
Router(config)#write mem
```

**Step 3:** Create a filter to allow SSH access. Create a new filter which can be tested and then later the old one can be removed.

```
Router(config)#access-list 104 remark VTY Telnet and SSH  
Access ACL
```

```
Router(config)#access-list 104 permit tcp host <your  
(source) IP address> any <or 'host' + a specific  
destination IP address> eq 22 23 log-input
```

```
Router(config)#access-list 103 deny ip any any log-input
```

**Step 4:** Modify vty access command to allow SSH.

```
Router(config)#line vty 0 4  
Router(config-line)#access-class 104 in  
Router(config-line)#exec-timeout 15 0  
Router(config-line)#transport input telnet ssh
```

### **Verify 3-1:**

To verify the SSH server is enabled and view the version and configuration data for your SSH connection, use the following command and write down the output.

```
Router#show ip ssh
```

---

### **Note 3-1.**

#### **Enabling SSH on a router**

Note that the crypto command is NOT performed in configuration mode.

Reference:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products\\_configuration\\_guide\\_chapter09186a00800ca7d5.html#wp1001139](http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7d5.html#wp1001139)

You may notice that there are a few prerequisites to configure SSH.

Prerequisite 1:

If your router has not been configured with a host name, you need to configure it with a host name

```
Router(config)#hostname Routerx
```

Prerequisite 2:

If your router has not been configured with a domain name, you need to configure it with the following command.

```
Router(config)#ip domain name training.net
```

### Note 3-2.

#### SSH and Telnet

Before 12.0S software, the only method used to access the Vty ports was telnet. Rlogin has been used by some ISPs, especially for executing one-off commands **but the protocol (=telnet) is insecure and can't be recommended.**

Reference: Cisco ISP Essentials ver 2.9 p56

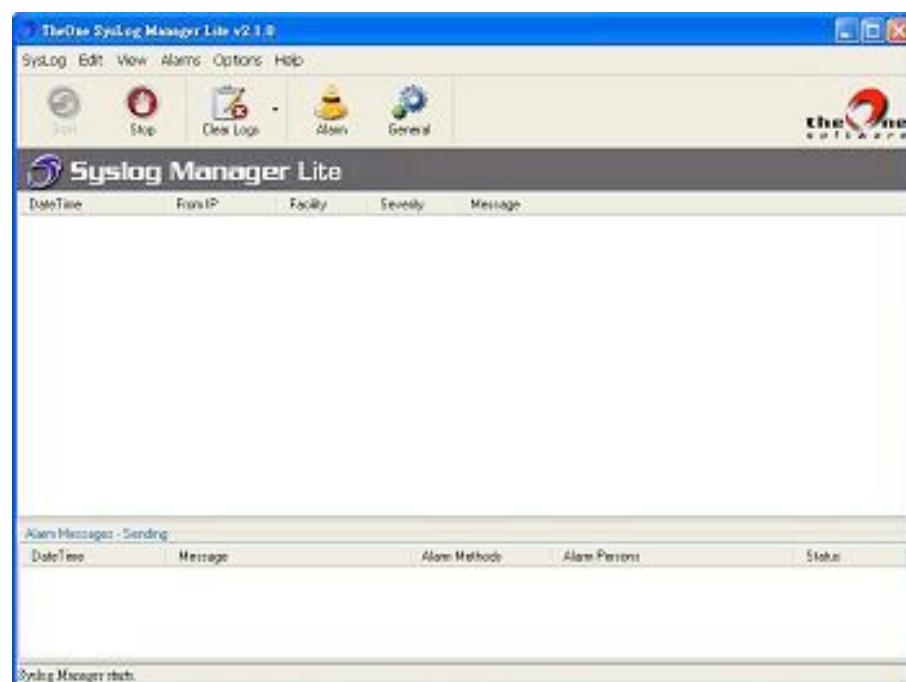
## 8 Configuring a syslog server *(These exercises will not be done and are for your information and reference only)*

**Exercise 8-1.** Configuring your PC with a syslogd server daemon.

Download a windows based syslogd server program. In this workshop, we will use *TheOne Syslog Manager Lite*. <http://www.theonesoftware.com/>

Step 1. Install the Syslog Manager Lite

Step 2. Run the Syslog Manager Lite



Step 3. Enable logging from the router

Step 4. Configure router logging to divert the logging information to the server

Step 5. Test the syslog server messages

**Exercise 8-2.** Configuring Cisco routers for Syslog

On your routers in “configuration terminal” mode enter the following commands:

```
Router(config)#logging on
Router(config)#logging <Syslog server's IP address>
Router(config)#service timestamps debug datetime localtime show-timezone
msec
Router(config)#service timestamps log datetime localtime show-timezone
msec
Router(config)#logging facility local7
Router(config)#logging trap informational
```

**Verify 4-2.** Use “show logging” command to see if the configuration is working.

## **9 Disable all unused access capabilities and services**

**Exercise 9-1.** Disable the http server(s) since they are never used.

```
Router(config)#no ip http server
Router(config)#no ip http secure-server
```

**Verify 5-1.** Confirm http server status with using the following command and see differences before and after “ip http server” and “no ip http server” and record message you saw on your monitor.

```
Router>sh ip http server status
```

---

Try to access to the router via http with the configurations of “ip http server” and “no ip http server” and see the differences and record your observation.

---

**Note 5-1.** Cisco issued a Cisco Security Advisory: IOS HTTP Server Command Injection Vulnerability in January 2006 and it recommended the above configurations if you are not using the http functionality. See more details from:

[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a008059e470.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a008059e470.shtml)

**Exercise 9-2.** The Cisco Discovery Protocol (CDP) is a proprietary protocol that Cisco devices use to identify their directly connected neighbors. CDP is

not frequently used and, like any other unnecessary local service, is considered potentially harmful to security. You can use the following commands to turn off CDP—globally and per interface:

Ref: <http://www.ciscopress.com/articles/article.asp?p=99029&seqNum=2&rl=1>

```
Router(config)#no cdp run
Router(config-if)#no cdp enable
```

**Verify 5-2.** Confirm output differences with using the following command and record your observation.

CDP run

---

no CDP run

---

**Note 5-2.** Explaining how CDP is outside of the scope of this workshop, however if you are interested in see more details from the following URL. [http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products\\_configuration\\_guide\\_chapter09186a00800ca66d.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800ca66d.html)

**Exercise 9-3.** Disable services which can be used for reconnaissance attempts or other attacks:

```
Router(config)#no service pad
Router(config)#no ip source-router
Router(config)#no ip finger
Router(config)#no ip bootp server
Router(config)#no ip domain-lookup
```

**Note 5-3.** Explaining the above services details is outside of the scope of this workshop. If you are interested in learning more details please conduct your own research.

## **10. Secure SNMP access *(These exercises will not be done and are for your information and reference only)***

### **Exercise 10-1.**

Step1: Configure filter which only allows SNMP access to specific hosts.

```
Router(config)#access-list 20 remark SNMP ACL
Router(config)#access-list 20 permit <IP address of SNMP server>
Router(config)#access-list 20 deny any log
```

Step2: Configure SNMP to have READ-ONLY access and treat the COMMUNITY string as a password – keep it difficult to guess.

```
Router(config)#snmp-server community <community> RO 20
```

**Note 6-1.** Configuring a SNMP server is outside of this workshop. If you are interested in learning more details please conduct your own research.

## **11. Configuring an appropriate banner**

**Exercise 11-1.** Set up an appropriate banner with using the following command. The following banner is a good example.

```
Router(config)#banner login %Access to this device is prohibited without
express written permission. All access is logged. Violators will be prosecuted
to the fullest extent o both civil and criminal law.%
```

As you are accessing to the router via the APNIC remote lab, you also need to configure the followings in order to see the effect of the banner configuration. This configuration is required specifically for the APNIC remote lab so it may not be applicable in your network.

```
Router(config)#service password-encryption
Router(config)#line console 0
Router(config-line)#password 7 letmein
Router(config-line)#login
```

**Verify 7-1.** Login the router and exit once and see what response you got and record it.

**12 AAA authentication** *(These exercises will not be done and are for your information and reference only)*

**Exercise 12-1.** Setup the routers to authenticate user access via TACACS+ server to allow centralised and secure access.

STEP 1:

Configure the router with local usernames for local access.

STEP2:

Configure the router to support group TACACS+ access and also local authentication as a back-up if TACACS+ is not accessible from the network.

STEP 3:

Configure the router with TACACS+ Authentication

STEP 4:

Configure the TACACS+ server to allow users to gain access to the routers where authentication is via TACACS+

STEP 5:

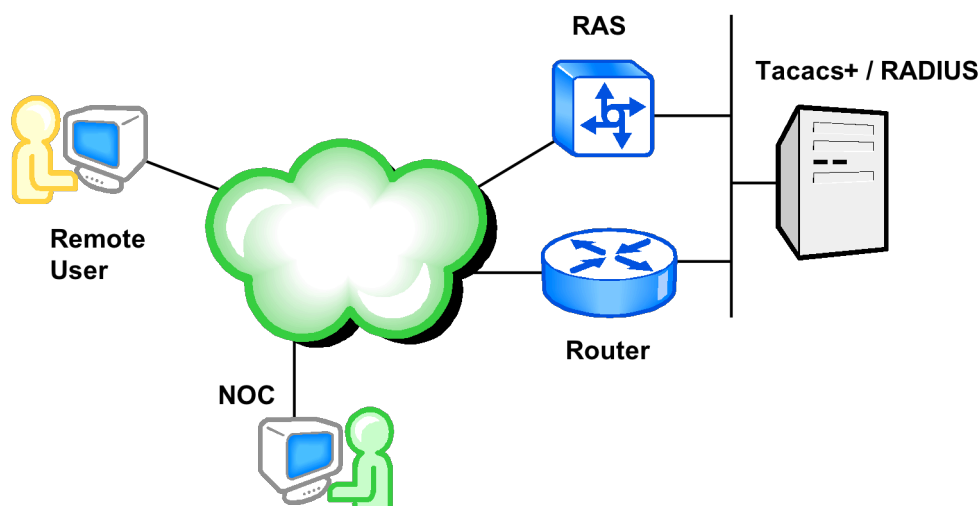
Verify the router and TACACS+ connectivity.

URL:

[http://www.cisco.com/en/US/tech/tk59/technologies\\_configuration\\_example09186a0080093c7c.shtml](http://www.cisco.com/en/US/tech/tk59/technologies_configuration_example09186a0080093c7c.shtml)

**NOTE:** Configuration example was based on a cleared (default) router configuration. For production network please make sure you understand the potential impact of any commands.

**Network Diagram:**





```
Router(config)#aaa new-model
Router(config)#aaa authentication login default group
tacacs+ local
Router(config)#aaa authentication enable default group
tacacs+ enable
Router(config)#aaa accounting exec default start-stop
group tacacs+
```

```
Router(config)#ip tacacs source-interface Loopback0
Router(config)#tacacs-server host 192.168.0.2
Router(config)#tacacs-server host 192.168.1.3
Router(config)#tacacs-server key apnic
```

**Exercise 12-2.** Setup the routers to authenticate user access via a RADIUS server to allow centralised and secure access.

STEP 1:

Configure the router with local usernames for local access.

STEP2:

Configure the router to support group RADIUS access and local authentication as a back-up if RADIUS is not accessible from the network.

STEP 3:

Configure the router with RADIUS Authentication

STEP 4:

Configure the RADIUS server to allow users to gain access to the routers with authentication via RADIUS

STEP 5:

Verify the router and RADIUS connectivity.

---

```
Router(config)#aaa new-model
Router(config)#aaa authentication login default group
radius local
Router(config)#aaa authentication enable default group
radius enable
Router(config)#aaa accounting exec default start-stop
group radius
```

```
Router(config)#ip radius source-interface Loopback0
Router(config)#radius-server host 192.168.0.2 auth-port
1645 acct-port 1646
Router(config)#radius-server host 192.168.1.3 auth-port
1645 acct-port 1646
Router(config)#radius-server key apnic
```