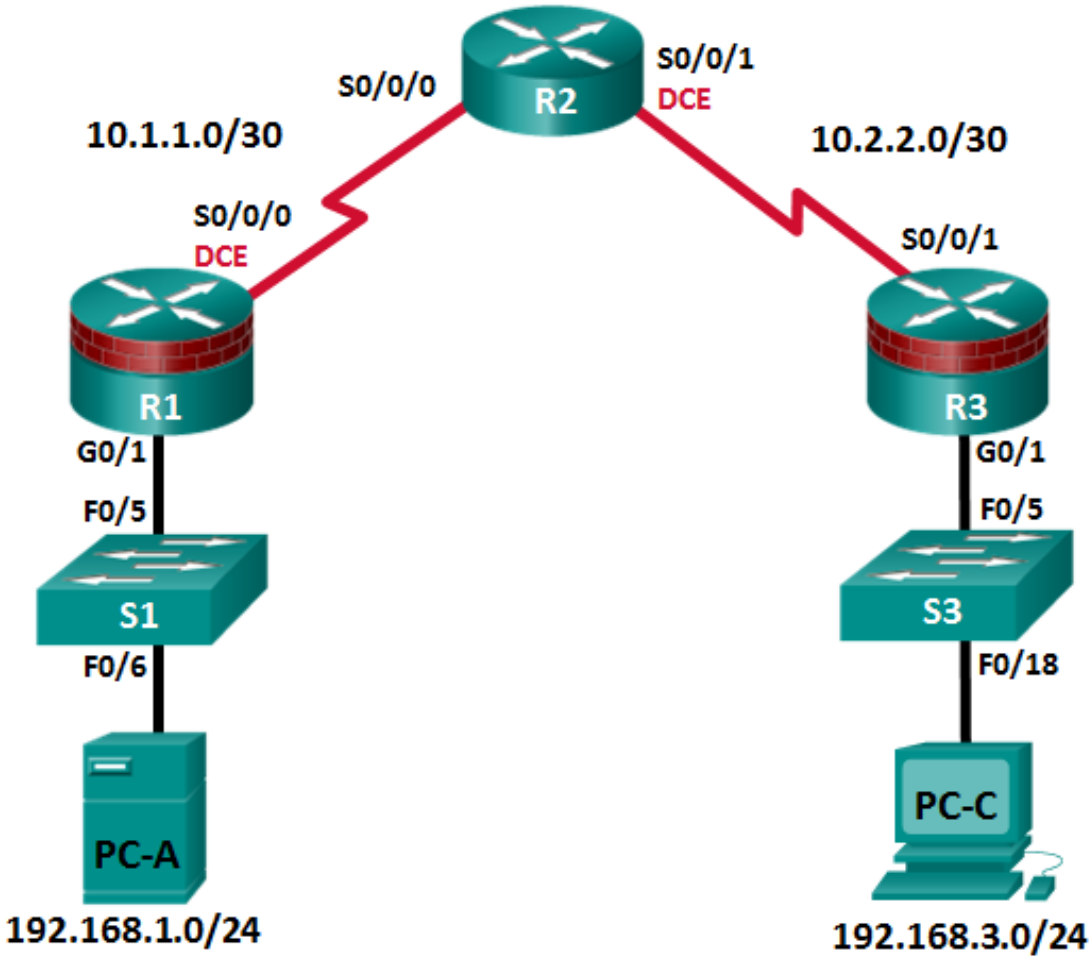
CCNA Security

Lab - Securing the Router for Administrative Access (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology



Note: ISR G1 devices use FastEthernet interfaces instead of GigabitEthernet Interfaces.

IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Objectives

Part 1: Configure Basic Device Settings

- Cable the network as shown in the topology.
- Configure basic IP addressing for routers and PCs.
- Configure OSPF routing.
- Configure PC hosts.
- Verify connectivity between hosts and routers.

Part 2: Control Administrative Access for Routers

- Configure and encrypt all passwords.
- Configure a login warning banner.
- Configure enhanced username password security.
- Configure an SSH server on a router.
- Configure an SSH client and verify connectivity.
- Configure an SCP server on a router.

Part 3: Configure Administrative Roles

- Create multiple role views and grant varying privileges.
- Verify and contrast views.

Part 4: Configure Cisco IOS Resilience and Management Reporting

- Secure the Cisco IOS image and configuration files.
- Configure SNMPv3 Security using an ACL.
- Configure a router as a synchronized time source for other devices using NTP.
- Configure syslog support on a router.
- Install a syslog server on a PC and enable it.
- Make changes to the router and monitor syslog results on the PC.

Part 5: Secure the Control Plane

- Configure OSPF Authentication using SHA256
- Verify OSPF Authentication

Part 6: Configure Automated Security Features

- Lock down a router using AutoSecure and verify the configuration.
- Contrast using AutoSecure with manually securing a router using the command line.

Background / Scenario

The router is a critical component in any network. It controls the movement of data into and out of the network and between devices within the network. It is particularly important to protect network routers because the failure of a routing device could make sections of the network, or the entire network, inaccessible. Controlling access to routers and enabling reporting on routers is critical to network security and should be part of a comprehensive security policy.

In this lab, you will build a multi-router network and configure the routers and hosts. Use various CLI tools to secure local and remote access to the routers, analyze potential vulnerabilities, and take steps to mitigate them. Enable management reporting to monitor router configuration changes.

The router commands and output in this lab are from a Cisco 1941 router using Cisco IOS software, release 15.4(3)M2 (with a Security Technology Package license). Other routers and Cisco IOS versions can be used. See the Router Interface Summary Table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the model of the router, the commands available and output produced may vary from what is shown in this lab.

Note: Before you begin, ensure that the routers and the switches have been erased and have no startup configurations.

Instructor Note: Instructions for erasing switches and routers are provided in Lab 0.0.0.0.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.4(3)M2 image with a Security Technology Package license)
- 2 Switches (Cisco 2960 or comparable) (Not Required)
- 2 PCs (Windows 7 or 8.1, SSH Client, syslog server)
- Serial and Ethernet cables as shown in the topology
- Console cables to configure Cisco networking devices

Part 1: Configure Basic Device Settings

In Part 1, set up the network topology and configure basic settings, such as interface IP addresses.

Step 1: Cable the network.

Attach the devices, as shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for each router.

a. Configure host names as shown in the topology.

b. Configure interface IP addresses as shown in the IP Addressing Table.

c. Configure a clock rate for routers with a DCE serial cable attached to their serial interface. R1 is shown here as an example.

```
R1(config)# interface S0/0/0
R1(config-if)# clock rate 64000
```

d. To prevent the router from attempting to translate incorrectly entered commands as though they were host names, disable DNS lookup. R1 is shown here as an example.

```
R1(config)# no ip domain-lookup
```

Step 3: Configure OSPF routing on the routers.

a. Use the **router ospf** command in global configuration mode to enable OSPF on R1.

```
R1(config)# router ospf 1
```

b. Configure the **network** statements for the networks on R1. Use an area ID of 0.

```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
```

c. Configure OSPF on R2 and R3.

d. Issue the **passive-interface** command to change the G0/1 interface on R1 and R3 to passive.

```
R1(config)# router ospf 1
R1(config-router)# passive-interface g0/1

R3(config)# router ospf 1
R3(config-router)# passive-interface g0/1
```

Step 4: Verify OSPF neighbors and routing information.

a. Issue the **show ip ospf neighbor** command to verify that each router lists the other routers in the network as neighbors.

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.2.2.2          0   FULL/  -        00:00:31    10.1.1.2        Serial0/0/0
```

b. Issue the **show ip route** command to verify that all networks display in the routing table on all routers.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
```

```
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.1/32 is directly connected, Serial0/0/0
O        10.2.2.0/30 [110/128] via 10.1.1.2, 00:03:03, Serial0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/1
L        192.168.1.1/32 is directly connected, GigabitEthernet0/1
O     192.168.3.0/24 [110/129] via 10.1.1.2, 00:02:36, Serial0/0/0
```

Step 5: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-C as shown in the IP Addressing Table.

Step 6: Verify connectivity between PC-A and PC-C.

a. Ping from R1 to R3.

   If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A, on the R1 LAN, to PC-C, on the R3 LAN.

   If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-A to PC-C you have demonstrated that OSPF routing is configured and functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct, use the **show run, show ip ospf neighbor,** and **show ip route** commands to help identify routing protocol-related problems.

Step 7: Save the basic running configuration for each router.

Save the basic running configuration for the routers as text files on your PC. These text files can be used to restore configurations later in the lab.

Part 2: Control Administrative Access for Routers

In Part 2, you will:

- Configure and encrypt passwords.
- Configure a login warning banner.
- Configure enhanced username password security.
- Configure enhanced virtual login security.
- Configure an SSH server on R1.
- Research terminal emulation client software and configure the SSH client.
- Configure an SCP server on R1.

Note: Perform all tasks on both R1 and R3. The procedures and output for R1 are shown here.

Task 1: Configure and Encrypt Passwords on Routers R1 and R3.

Step 1: Configure a minimum password length for all router passwords.

Use the **security passwords** command to set a minimum password length of 10 characters.

```
R1(config)# security passwords min-length 10
```

Step 2: Configure the enable secret password.

Configure the enable secret encrypted password on both routers. Use the type 9 (SCRYPT) hashing algorithm.

```
R1(config)# enable algorithm-type scrypt secret cisco12345
```

How does configuring an enable secret password help protect a router from being compromised by an attack?

_____

_____

_____

_____

_____

_____

The goal is to always prevent unauthorized users from accessing a device using Telnet, SSH, or via the console. If attackers are able to penetrate this first layer of defense, using an enable secret password prevents them from being able to alter the configuration of the device. Unless the enable secret password is known, a user cannot go into privileged EXEC mode where they can display the running config and enter various configuration commands to make changes to the router. This provides an additional layer of security.

Step 3: Configure basic console, auxiliary port, and virtual access lines.

Note: Passwords in this task are set to a minimum of 10 characters but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

a. Configure a console password and enable login for routers. For additional security, the **exec-timeout** command causes the line to log out after 5 minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry.

   Note: To avoid repetitive logins during this lab, the **exec-timeout** command can be set to 0 0, which prevents it from expiring. However, this is not considered a good security practice.

```
R1(config)# line console 0
R1(config-line)# password ciscocon
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous
```

   When you configured the password for the console line, what message was displayed?

   _____

   _____

   % Invalid Password length - must contain 10 to 25 characters. Password configuration failed.

b. Configure a new password of **ciscoconpass** for the console.

c. Configure a password for the AUX port for router R1.

```
R1(config)# line aux 0
R1(config-line)# password ciscoauxpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
```

d. Telnet from R2 to R1.

```
R2> telnet 10.1.1.1
```

Were you able to login? Explain.

_____

_____

No. The **transport input none** command is set by default on the vty lines. A password would also need to be set before Telnet would be allowed.

What messages were displayed?

_____

_____

Trying 10.1.1.1 ...

% Connection refused by remote host

e. Configure the password on the vty lines for router R1.

```
R1(config)# line vty 0 4
R1(config-line)# password ciscovtypass
R1(config-line)# exec-timeout 5 0
R1(config-line)# transport input telnet
R1(config-line)# login
```

Note: The default for vty lines is now **transport input none**.

Telnet from R2 to R1 again. Were you able to login this time?

_____

Yes. The vty lines have been configured to accept Telnet and a password has been set.

f. Enter privileged EXEC mode and issue the **show run** command. Can you read the enable secret password? Explain.

_____

_____

No. The enable secret password has been encrypted with the SCRYPT hash algorithm.

Can you read the console, aux, and vty passwords? Explain.

_____

_____

Yes. They are all in clear text.

g. Repeat the configuration portion of steps 3a through 3g on router R3.

Step 4: Encrypt clear text passwords.

a. Use the **service password-encryption** command to encrypt the console, aux, and vty passwords.

```
R1(config)# service password-encryption
```

b. Issue the **show run** command. Can you read the console, aux, and vty passwords? Explain.

_____

_____

No. The passwords are now encrypted.

At what level (number) is the default enable secret password encrypted? _____ 9

At what level (number) are the other passwords encrypted? _____ 7

Which level of encryption is harder to crack and why?

_____

_____

9, because the algorithm is stronger than 7. Type 9 (SCRYPT) is currently the strongest algorithm.

Task 2: Configure a Login Warning Banner on Routers R1 and R3.

Step 1: Configure a warning message to display prior to login.

a. Configure a warning to unauthorized users with a message-of-the-day (MOTD) banner using the **banner motd** command. When a user connects to one of the routers, the MOTD banner appears before the login prompt. In this example, the dollar sign ($) is used to start and end the message.

```
R1(config)# banner motd $Unauthorized access strictly prohibited!$
R1(config)# exit
```

b. Issue the **show run** command. What does the $ convert to in the output?

_____

_____

The $ is converted to ^C when the running-config is displayed.

Task 3: Configure Enhanced Username Password Security on Routers R1 and R3.

Step 1: Investigate the options for the username command.

In global configuration mode, enter the following command:

```
R1(config)# username user01 algorithm-type ?
```

What options are available?

_____

_____

_____

```
md5     Encode the password using the MD5 algorithm
scrypt  Encode the password using the SCRYPT hashing algorithm
sha256  Encode the password using the PBKDF2 hashing algorithm
```

Step 2: Create a new user account with a secret password.

a. Create a new user account with SCRYPT hashing to encrypt the password.

```
R1(config)# username user01 algorithm-type scrypt secret user01pass
```

b. Exit global configuration mode and save your configuration.

c. Display the running configuration. Which hashing method is used for the password?

_____

_____

Type 9 (SCRYPT) hashing algorithm.

Step 3: Test the new account by logging in to the console.

a. Set the console line to use the locally defined login accounts.

```
R1(config)# line console 0
R1(config-line)# login local
R1(config-line)# end
R1# exit
```

b. Exit to the initial router screen which displays: R1 con0 is now available, Press RETURN to get started.

c. Log in using the previously defined username **user01** and the password **user01pass**.

What is the difference between logging in at the console now and previously?

_____

_____

You are prompted to enter a username as well as a password.

d. After logging in, issue the **show run** command. Were you able to issue the command? Explain.

_____

_____

No. It requires privileged EXEC level.

e. Enter privileged EXEC mode using the **enable** command. Were you prompted for a password? Explain.

_____

_____

Yes. Any new users that are created will still be required to enter the enable secret password to enter privileged EXEC mode.

Step 4: Test the new account by logging in from a Telnet session.

a. From PC-A, establish a Telnet session with R1. Telnet is disabled by default in Windows 7. If necessary, search online for the steps to enable Telnet in Windows 7.

```
PC-A> telnet 192.168.1.1
```

Were you prompted for a user account? Explain.

_____

_____

No. The vty lines were not set to use the locally defined accounts as the line 0 console was.

b. Set the vty lines to use the locally defined login accounts.

```
R1(config)# line vty 0 4
R1(config-line)# login local
```

c. From PC-A, telnet to R1 again.

```
PC-A> telnet 192.168.1.1
```

Were you prompted for a user account? Explain.

_____

_____

Yes. The vty lines are now set to use the locally defined accounts.

d. Log in as **user01** with a password of **user01pass**.

e. During the Telnet session to R1, access privileged EXEC mode with the **enable** command.

What password did you use?

_____

The enable secret password, cisco12345.

f. For added security, set the AUX port to use the locally defined login accounts.

```
R1(config)# line aux 0
R1(config-line)# login local
```

g. End the Telnet session with the **exit** command.

Task 4: Configure the SSH Server on Router R1 and R3.

In this task, use the CLI to configure the router to be managed securely using SSH instead of Telnet. Secure Shell (SSH) is a network protocol that establishes a secure terminal emulation connection to a router or other networking device. SSH encrypts all information that passes over the network link and provides authentication of the remote computer. SSH is rapidly replacing Telnet as the remote login tool of choice for network professionals.

Note: For a router to support SSH, it must be configured with local authentication, (AAA services, or username) or password authentication. In this task, you configure an SSH username and local authentication.

Step 1: Configure a domain name.

Enter global configuration mode and set the domain name.

```
R1# conf t
R1(config)# ip domain-name ccnasecurity.com
```

Step 2: Configure a privileged user for login from the SSH client.

a. Use the **username** command to create the user ID with the highest possible privilege level and a secret password.

```
R1(config)# username admin privilege 15 algorithm-type scrypt secret
cisco12345
```

Note: Usernames are not case sensitive by default. You will learn how to make usernames case sensitive in Chapter 3.

b. Exit to the initial router login screen. Log in with the username admin and the associated password. What was the router prompt after you entered the password?

_____

_____

The privileged EXEC (enable) prompt #. With a privilege level of 15, the login defaults to privileged EXEC mode.

Step 3: Configure the incoming vty lines.

Specify a privilege level of **15** so that a user with the highest privilege level (15) will default to privileged EXEC mode when accessing the vty lines. Other users will default to user EXEC mode. Use the local user accounts for mandatory login and validation and accept only SSH connections.

```
R1(config)# line vty 0 4
R1(config-line)# privilege level 15
```

```
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

Note: The **login local** command should have been configured in a previous step. It is included here to provide all commands, if you are doing this for the first time.

Note: If you add the keyword **telnet** to the **transport input** command, users can log in using Telnet as well as SSH, however, the router will be less secure. If only SSH is specified, the connecting host must have an SSH client installed.

Step 4: Erase existing key pairs on the router.

```
R1(config)# crypto key zeroize rsa
```

Note: If no keys exist, you might receive this message: `% No Signature RSA Keys found in configuration`.

Step 5: Generate the RSA encryption key pair for the router.

The router uses the RSA key pair for authentication and encryption of transmitted SSH data.

a. Configure the RSA keys with **1024** for the number of modulus bits. The default is 512, and the range is from 360 to 2048.

```
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.ccnasecurity.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
*Dec 16 21:24:16.175: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

b. Issue the **ip ssh version 2** command to force the use of SSH version 2.

```
R1(config)# ip ssh version 2
R1(config)# exit
```

Note: The details of encryption methods are covered in Chapter 7.

Step 6: Verify the SSH configuration.

a. Use the **show ip ssh** command to see the current settings.

```
R1# show ip ssh
```

b. Fill in the following information based on the output of the **show ip ssh** command.

SSH version enabled: _____ Version 2.0

Authentication timeout: _____ Default is 120 seconds

Authentication retries: _____ Default is 3 tries

Step 7: Configure SSH timeouts and authentication parameters.

The default SSH timeouts and authentication parameters can be altered to be more restrictive using the following commands.

```
R1(config)# ip ssh time-out 90
R1(config)# ip ssh authentication-retries 2
```

Step 8: Save the running-config to the startup-config.

```
R1# copy running-config startup-config
```

Task 5: Research Terminal Emulation Client Software and Configure the SSH Client.

Step 1: Research terminal emulation client software.

Conduct a web search for freeware terminal emulation client software, such as TeraTerm or PuTTy. What are some capabilities of each?

_____

_____

_____

_____

_____

_____

_____

_____

TeraTerm: This Telnet client provides VT100 emulation, selected VT200/300 emulation, TEK4010 emulation and Kermit, XMODEM, ZMODEM, B-PLUS, and Quick-VAN file transfer protocols. It also offers the ability to connect to SSH2 hosts, a built-in Web server for HTTP pass-through commands, and macro language abilities, including ODBC support, recurring commands, and directory-independent operation.

PuTTy: A free and open-source terminal emulator, serial console, and network file transfer application. It supports several network protocols, including SCP, SSH, Telnet and rlogin.

Step 2: Install an SSH client on PC-A and PC-C.

a. If the SSH client is not already installed, download either TeraTerm or PuTTY.

b. Save the application to the desktop.

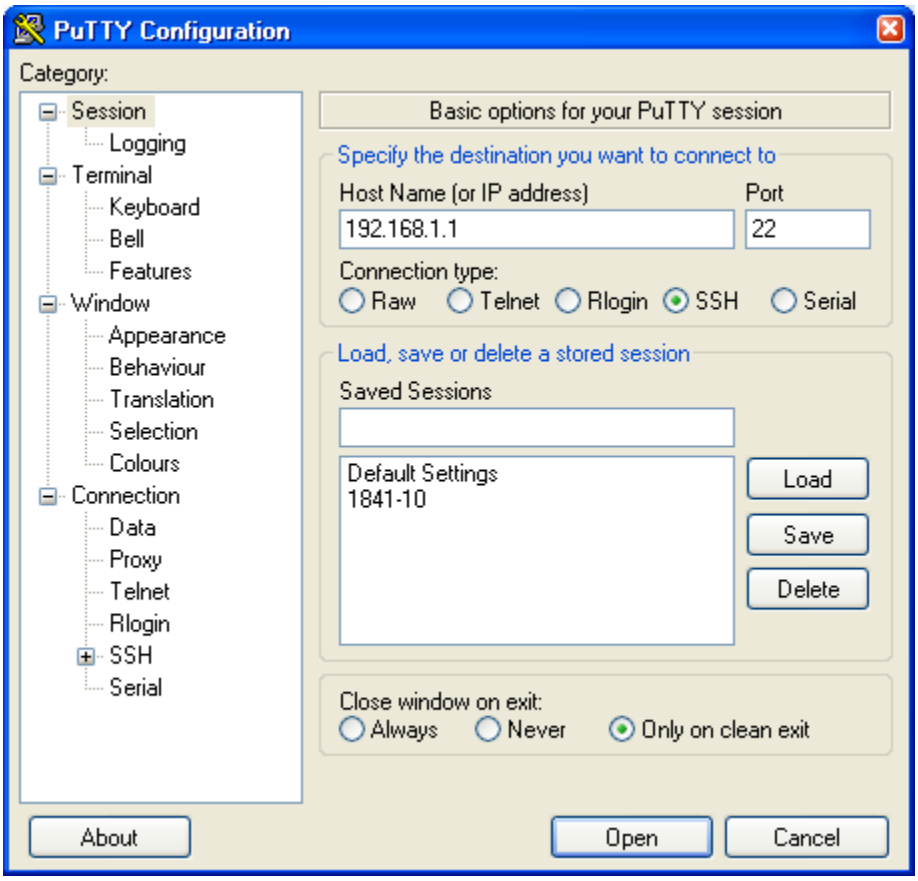
Note: The procedure described here is for PuTTY and pertains to PC-A.

Step 3: Verify SSH connectivity to R1 from PC-A.

a. Launch PuTTY by double-clicking the putty.exe icon.

b. Input the R1 F0/1 IP address **192.168.1.1** in the **Host Name (or IP address)** field.

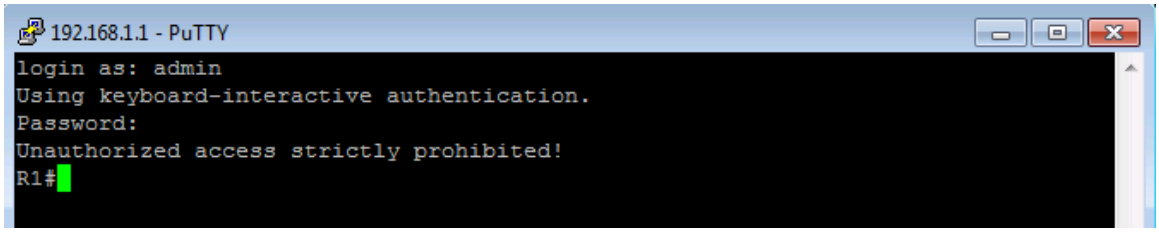
c. Verify that the **SSH** radio button is selected.



d. Click **Open**.

e. In the PuTTY Security Alert window, click **Yes**.

f. Enter the **admin** username and password **cisco12345** in the PuTTY window.



g. At the R1 privileged EXEC prompt, enter the **show users** command.

```
R1# show users
```

What users are connected to router R1 at this time?

_____

_____

_____

You should see at least two users, one for your console connection and another for the SSH interface.

```
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:00:00
*132 vty 0     admin      idle                 00:00:33    192.168.1.3
```

h. Close the PuTTY SSH session window.

i. Try to open a Telnet session to your router from PC-A. Were you able to open the Telnet session? Explain.

_____

_____

No. The Telnet session fails because only SSH is enabled for the vty lines.

j. Open a PuTTY SSH session to the router from PC-A. Enter the **user01** username and password **user01pass** in the PuTTY window to try connecting for a user who does not have privilege level of 15.

If you were able to login, what was the prompt?

_____

_____

Because user01 was not created with a privilege level of 15 (the default is level 1), the prompt is user EXEC (>).

k. Use the **enable** command to enter privilege EXEC mode and enter the enable secret password **cisco12345**.

Task 6: Configure an SCP server on R1.

Now that SSH is configured on the router, configure the R1 router as a secure copy (SCP) server.

Step 1: Use the AAA authentication and authorization defaults on R1.

Set the AAA authentication and authorization defaults on R1 to use the local database for logins.

Note: SCP requires the user to have privilege level 15 access.

a. Enable AAA on the router.

```
R1(config)# aaa new-model
```

b. Use the **aaa authentication** command to use the local database as the default login authentication method.

```
R1(config)# aaa authentication login default local
```

c. Use the **aaa authorization** command to use the local database as the default command authorization.

```
R1(config)# aaa authorization exec default local
```

d. Enable SCP server on R1.

```
R1(config)# ip scp server enable
```

Note: AAA is covered in Chapter 3.

Step 2: Copy the running config on R1 to flash.

SCP server allows files to be copied to and from a router's flash. In this step, you will create a copy of the running-config on R1 to flash. You will then use SCP to copy that file to R3.

a. Save the running configuration on R1 to a file on flash called R1-Config.

```
R1# copy running-config R1-Config
```

b. Verify that the new R1-Config file is on flash.

```
R1# show flash
-#- --length-- -----date/time------ path
1     75551300 Feb 16 2015 15:19:22 +00:00 c1900-universalk9-mz.SPA.154-3.M2.bin
2         1643 Feb 17 2015 23:30:58 +00:00 R1-Config

181047296 bytes available (75563008 bytes used)
```

Step 3: Use SCP command on R3 to pull the configuration file from R1.

a. Use SCP to copy the configuration file that you created in Step2a to R3.

```
R3# copy scp: flash:
Address or name of remote host []? 10.1.1.1
Source username [R3]? admin
Source filename []? R1-Config
Destination filename [R1-Config]? [Enter]
Password: cisco12345
!
2007 bytes copied in 9.056 secs (222 bytes/sec)
```

b. Verify that the file has been copied to R3's flash.

```
R3# show flash
-#- --length-- -----date/time------ path
1     75551300 Feb 16 2015 15:21:38 +00:00 c1900-universalk9-mz.SPA.154-3.M2.bin
2         1338 Feb 16 2015 23:46:10 +00:00 pre_autosec.cfg
3         2007 Feb 17 2015 23:42:00 +00:00 R1-Config

181043200 bytes available (75567104 bytes used)
```

c. Issue the **more** command to view the contents of the R1-Config file.

```
R3# more R1-Config
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
<Output omitted>
!
end
```

Step 4: Save the configuration.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R1# copy running-config startup-config
```

Part 3: Configure Administrative Roles

In Part 3 of this lab, you will:

- Create multiple administrative roles, or views, on routers R1 and R3.
- Grant each view varying privileges.
- Verify and contrast the views.

The role-based CLI access feature allows the network administrator to define views, which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration (config) mode commands. Views restrict user access to the Cisco IOS CLI and configuration information. A view can define which commands are accepted and what configuration information is visible.

Note: Perform all tasks on both R1 and R3. The procedures and output for R1 are shown here.

Task 1: Enable Root View on R1 and R3.

If an administrator wants to configure another view to the system, the system must be in root view. When a system is in root view, the user has the same access privileges as a user who has level-15 privileges, but the root view user can also configure a new view and add or remove commands from the view. When you are in a CLI view, you have access only to the commands that have been added to that view by the root view user.

Step 1: Enable AAA on router R1.

To define views, be sure that AAA was enabled with the **`aaa new-model`** command in Part 2.

Step 2: Enable the root view.

Use the command **enable view** to enable the root view. Use the **enable secret** password **cisco12345**. If the router does not have an enable secret password, create one now.

```
R1# enable view
Password: cisco12345
```

Task 2: Create New Views for the Admin1, Admin2, and Tech Roles on R1 and R3.

Step 1: Create the admin1 view, establish a password, and assign privileges.

a. The admin1 user is the top-level user below root that is allowed to access this router. It has the most authority. The admin1 user can use all **show**, **config**, and **debug** commands. Use the following command to create the admin1 view while in the root view.

```
R1(config)# parser view admin1
R1(config-view)#
```

Note: To delete a view, use the command **no parser view** *viewname*.

b. Associate the admin1 view with an encrypted password.

```
R1(config-view)# secret admin1pass
R1(config-view)#
```

c. Review the commands that can be configured in the admin1 view. Use the **commands ?** command to see available commands. The following is a partial listing of the available commands.

```
R1(config-view)# commands ?
  RITE-profile           Router IP traffic export profile command mode
  RMI Node Config        Resource Policy Node Config mode
```

```
  RMI Resource Group      Resource Group Config mode
  RMI Resource Manager    Resource Manager Config mode
  RMI Resource Policy     Resource Policy Config mode
  SASL-profile            SASL profile configuration mode
  aaa-attr-list           AAA attribute list config mode
  aaa-user                AAA user definition
  accept-dialin           VPDN group accept dialin configuration mode
  accept-dialout          VPDN group accept dialout configuration mode
  address-family          Address Family configuration mode
<output omitted>
```

d. Add all **config**, **show**, and **debug** commands to the admin1 view and then exit from view configuration mode.

```
R1(config-view)# commands exec include all show
R1(config-view)# commands exec include all config terminal
R1(config-view)# commands exec include all debug
R1(config-view)# end
```

e. Verify the admin1 view.

```
R1# enable view admin1
Password: admin1pass

R1# show parser view
Current view is 'admin1'
```

f. Examine the commands available in the admin1 view.

```
R1# ?
Exec commands:
  <0-0>/<0-4>  Enter card slot/sublot number
  configure    Enter configuration mode
  debug        Debugging functions (see also 'undebug')
  do-exec      Mode-independent "do-exec" prefix support
  enable       Turn on privileged commands
  exit         Exit from the EXEC
  show           Show running system
```

Note: There may be more EXEC commands available than are displayed. This depends on your device and the IOS image used.

g. Examine the **show** commands available in the admin1 view.

```
R1# show ?
  aaa                     Show AAA values
  access-expression       List access expression
  access-lists            List access lists
  acircuit                Access circuit info
  adjacency               Adjacent nodes
  aliases                 Display alias commands
  alignment               Show alignment information
  appfw                   Application Firewall information
  archive                 Archive functions
```

```
  arp                       ARP table
<output omitted>
```

Step 2: Create the admin2 view, establish a password, and assign privileges.

a. The admin2 user is a junior administrator in training who is allowed to view all configurations but is not allowed to configure the routers or use debug commands.

b. Use the **enable view** command to enable the root view, and enter the enable secret password **cisco12345**.

```
R1# enable view
Password: cisco12345
```

c. Use the following command to create the admin2 view.

```
R1(config)# parser view admin2
R1(config-view)#
```

d. Associate the admin2 view with a password.

```
R1(config-view)# secret admin2pass
R1(config-view)#
```

e. Add all **show** commands to the view, and then exit from view configuration mode.

```
R1(config-view)# commands exec include all show
R1(config-view)# end
```

f. Verify the admin2 view.

```
R1# enable view admin2
Password: admin2pass

R1# show parser view
Current view is 'admin2'
```

g. Examine the commands available in the admin2 view.

```
R1# ?
Exec commands:
  <0-0>/<0-4>  Enter card slot/sublot number
  do-exec      Mode-independent "do-exec" prefix support
  enable       Turn on privileged commands
  exit         Exit from the EXEC
  show         Show running system information
```

Note: There may be more EXEC commands available than are displayed. This depends on your device and the IOS image used.

What is missing from the list of admin2 commands that is present in the admin1 commands?

_____

configure and **debug**

Step 3: Create the tech view, establish a password, and assign privileges.

a. The tech user typically installs end-user devices and cabling. Tech users are only allowed to use selected **show** commands.

b. Use the enable **view** command to enable the root view, and enter the enable secret password **cisco12345**.

```
R1# enable view
Password: cisco12345
```

c. Use the following command to create the tech view.

```
R1(config)# parser view tech
R1(config-view)#
```

d. Associate the tech view with a password.

```
R1(config-view)# secret techpasswd
R1(config-view)#
```

e. Add the following **show** commands to the view and then exit from view configuration mode.

```
R1(config-view)# commands exec include show version
R1(config-view)# commands exec include show interfaces
R1(config-view)# commands exec include show ip interface brief
R1(config-view)# commands exec include show parser view
R1(config-view)# end
```

f. Verify the tech view.

```
R1# enable view tech
Password: techpasswd

R1# show parser view
Current view is 'tech'
```

g. Examine the commands available in the tech view.

```
R1# ?
Exec commands:
  <0-0>/<0-4>  Enter card slot/sublot number
  do-exec      Mode-independent "do-exec" prefix support
  enable       Turn on privileged commands
  exit         Exit from the EXEC
  show         Show running system information
```

Note: There may be more EXEC commands available than are displayed. This depends on your device and the IOS image used.

h. Examine the **show** commands available in the tech view.

```
R1# show ?
  banner      Display banner information
  flash0:     display information about flash0: file system
  flash1:     display information about flash1: file system
  flash:      display information about flash: file system
  interfaces  Interface status and configuration
  ip          IP information
  parser      Display parser information
  usbflash0:  display information about usbflash0: file system
  version     System hardware and software status
```

Note: There may be more EXEC commands available than are displayed. This depends on your device and the IOS image used.

i. Issue the **show ip interface brief** command. Were you able to do it as the tech user? Explain.

_____

_____

Yes. It is one of the allowed commands.

j. Issue the **show ip route** command. Were you able to do it as the tech user?

_____

_____

No. It is not one of the allowed commands.

```
R1# show ip route
          ^
% Invalid input detected at '^' marker.
```

k. Return to root view with the **enable view** command.

```
R1# enable view
Password: cisco12345
```

l. Issue the **show run** command to see the views you created. For tech view, why are the **show** and **show ip** commands listed as well as **show ip interface** and **show ip interface brief**?

_____

_____

All parts of the command must be listed for the more specific parameters to work.

Step 4: Save the configuration on routers R1 and R3.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

Part 4: Configure IOS Resilience and Management Reporting

In Part 4 of this lab, you will:

- Secure the Cisco IOS image and configuration files.
- Configure SNMPv3 security using an ACL.
- Using NTP, configure a router as a synchronized time source for other devices.
- Configure syslog support on a router.
- Install a syslog server on a PC and enable it.
- Configure the logging trap level on a router.
- Make changes to the router and monitor syslog results on the PC.

Note: Perform all tasks on both R1 and R3. The procedure and output for R1 is shown here.

Task 1: Secure Cisco IOS Image and Configuration Files on R1 and R3.

The Cisco IOS resilient configuration feature enables a router to secure the running image and maintain a working copy of the configuration. This ensures that those files can withstand malicious attempts to erase the contents of persistent storage (NVRAM and flash). This feature secures the smallest working set of files to

preserve persistent storage space. No extra space is required to secure the primary Cisco IOS image file. In this task, you configure the Cisco IOS Resilient Configuration feature.

Note: Cisco IOS resilient configuration feature is not available on the Cisco 1921 router.

Note: The output of the commands in this Task are for example purposes only. Your output will be different.

Step 1: Display the files in flash memory for R1.

The **show flash:** command displays the contents of sub-directories. The **dir** command only displays contents of the current directory.

```
R1# show flash:
-#- --length-- -----date/time------ path
1     75551300 Feb 5 2015 16:53:34 +00:00 c1900-universalk9-mz.SPA.154-3.M2.bin
2            0 Jan 6 2009 01:28:44 +00:00 ipsdir
3       334531 Jan 6 2009 01:35:40 +00:00 ipsdir/R1-sigdef-default.xml
4          461 Jan 6 2009 01:37:42 +00:00 ipsdir/R1-sigdef-delta.xml
5         8509 Jan 6 2009 01:33:42 +00:00 ipsdir/R1-sigdef-typedef.xml
6        38523 Jan 6 2009 01:33:46 +00:00 ipsdir/R1-sigdef-category.xml
7          304 Jan 6 2009 01:31:48 +00:00 ipsdir/R1-seap-delta.xml
8          491 Jan 6 2009 01:31:48 +00:00 ipsdir/R1-seap-typedef.xml
9         1410 Oct 26 2014 04:44:08 +00:00 pre_autosec.cfg

76265535 bytes available (180221889 bytes used)


R1# dir
Directory of flash:/

    1  -rw-      75551300 Feb 5 2015 16:53:34 +00:00 c1900-universalk9-mz.SPA.154-
3.M2.bin
    2  drw-           0   Jan 6 2009 01:28:44 +00:00  ipsdir
    9  -rw-        1410  Oct 26 2014 04:44:08 +00:00  pre_autosec.cfg

256487424 bytes total (180221889 bytes free)
```

Step 2: Secure the Cisco IOS image and archive a copy of the running configuration.

a. The **secure boot-image** command enables Cisco IOS image resilience, which hides the file from the **dir** command and **show** commands. The file cannot be viewed, copied, modified, or removed using EXEC mode commands. (It can be viewed in ROMMON mode.) When turned on for the first time, the running image is secured.

```
R1(config)# secure boot-image
.Feb 11 25:40:13.170: %IOS_RESILIENCE-5-IMAGE_RESIL_ACTIVE: Successfully secured
running image
```

b. The **secure boot-config** command takes a snapshot of the router running configuration and securely archives it in persistent storage (flash).

```
R1(config)# secure boot-config
.Feb 11 25:42:18.691: %IOS_RESILIENCE-5-CONFIG_RESIL_ACTIVE: Successfully secured
config archive [flash:.runcfg-20150211-224218.ar]
```

Step 3: Verify that your image and configuration are secured.

You can use only the **show secure bootset** command to display the archived filename. Display the status of configuration resilience and the primary bootset filename.

```
R1# show secure bootset
IOS resilience router id FTX1111W0QF

IOS image resilience version 15.4 activated at 25:40:13 UTC Wed Feb 11 2015
Secure archive flash: c1900-universalk9-mz.SPA.154-3.M2.bin type is image (elf)
[]
  file size is 75551300 bytes, run size is 75730352 bytes
  Runnable image, entry point 0x8000F000, run from ram

IOS configuration resilience version 15.4 activated at 25:42:18 UTC Wed Feb 11 2015
Secure archive flash:.runcfg-20150211-224218.ar type is config
configuration archive size 3293 bytes
```

What is the name of the archived running config file and on what is the name based?

_____

_____

Answers will vary but will in the following format: runcfg-20150211-254218.ar. It is based on the date and time archived by the **secure boot-config** command.

Step 4: Display the files in flash memory for R1.

a. Display the contents of flash using the **show flash** command.

```
R1# show flash:
-#- --length-- -----date/time------ path
2            0 Jan 6 2009 01:28:44 +00:00 ipsdir
3       334531 Jan 6 2009 01:35:40 +00:00 ipsdir/R1-sigdef-default.xml
4          461 Jan 6 2009 01:37:42 +00:00 ipsdir/R1-sigdef-delta.xml
5         8509 Jan 6 2009 01:33:42 +00:00 ipsdir/R1-sigdef-typedef.xml
6        38523 Jan 6 2009 01:33:46 +00:00 ipsdir/R1-sigdef-category.xml
7          304 Jan 6 2009 01:31:48 +00:00 ipsdir/R1-seap-delta.xml
8          491 Jan 6 2009 01:31:48 +00:00 ipsdir/R1-seap-typedef.xml
9         1410 Oct 26 2014 04:44:08 +00:00 pre_autosec.cfg

76265535 bytes available (180221889 bytes used)
```

Is the Cisco IOS image or the archived running config file listed?

_____

No. They are hidden.

b. How can you tell that the Cisco IOS image is still there?

_____

_____

The bytes available and bytes used are approximately the same as before (minus the space taken by the archived running config file).

Step 5: Disable the IOS Resilient Configuration feature.

a. Disable the Resilient Configuration feature for the Cisco IOS image.

```
R1# config t
R1(config)# no secure boot-image
.Feb 11 25:48:23.009: %IOS_RESILIENCE-5-IMAGE_RESIL_INACTIVE: Disabled secure
image archival
```

b. Disable the Resilient Configuration feature for the running config file.

```
R1(config)# no secure boot-config
.Feb 11 25:48:47.972: %IOS_RESILIENCE-5-CONFIG_RESIL_INACTIVE: Disabled
secure config archival [removed flash:.runcfg-20150211-224218.ar]
```

Step 6: Verify that the Cisco IOS image is now visible in flash.

Use the **show flash:** command to display the files in flash.

```
R1# show flash:
-#- --length-- -----date/time------ path
1     75551300 Feb 5 2015 16:53:34 +00:00 c1900-universalk9-mz.SPA.154-3.M2.bin
2            0 Jan 6 2009 01:28:44 +00:00 ipsdir
3       334531 Jan 6 2009 01:35:40 +00:00 ipsdir/R1-sigdef-default.xml
4          461 Jan 6 2009 01:37:42 +00:00 ipsdir/R1-sigdef-delta.xml
5         8509 Jan 6 2009 01:33:42 +00:00 ipsdir/R1-sigdef-typedef.xml
6        38523 Jan 6 2009 01:33:46 +00:00 ipsdir/R1-sigdef-category.xml
7          304 Jan 6 2009 01:31:48 +00:00 ipsdir/R1-seap-delta.xml
8          491 Jan 6 2009 01:31:48 +00:00 ipsdir/R1-seap-typedef.xml
9         1410 Oct 26 2014 04:44:08 +00:00 pre_autosec.cfg


76265535 bytes available (180221889 bytes used)
```

Step 7: Save the configuration on both routers.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

Task 2: Configure SNMPv3 Security using an ACL.

Simple Network Management Protocol (SNMP) enables network administrators to monitor network performance, mange network devices, and troubleshoot network problems. SNMPv3 provides secure access by authenticating and encrypting SNMP management packets over the network. You will configure SNMPv3 using an ACL on R1.

Step 1: Configure an ACL on R1 that will restrict access to SNMP on the 192.168.1.0 LAN.

a. Create a standard access-list named **PERMIT-SNMP**.

```
R1(config)# ip access-list standard PERMIT-SNMP
```

b. Add a permit statement to allow only packets on R1's LAN.

```
R1(config-std-nacl)# permit 192.168.1.0 0.0.0.255
R1(config-std-nacl)# exit
```

Step 2: Configure the SNMP view.

Configure a SNMP view called **SNMP-RO** to include the ISO MIB family.

```
R1(config)# snmp-server view SNMP-RO iso included
```

Step 3: Configure the SNMP group.

Call the group name **SNMP-G1**, and configure the group to use SNMPv3 and require both authentication and encryption by using the **priv** keyword. Associate the view you created in Step 2 to the group, giving it read only access with the **read** parameter. Finally specify the ACL **PERMIT-SNMP**, configured in Step 1, to restrict SNMP access to the local LAN.

```
R1(config)# snmp-server group SNMP-G1 v3 priv read SNMP-RO access PERMIT-SNMP
```

Step 4: Configure the SNMP user.

Configure an **SNMP-Admin** user and associate the user to the **SNMP-G1** group you configured in Step 3. Set the authentication method to **SHA** and the authentication password to **Authpass**. Use AES-128 for encryption with a password of **Encrypass**.

```
R1(config)# snmp-server user SNMP-Admin SNMP-G1 v3 auth sha Authpass priv aes
128 Encrypass
R1(config)# end
```

Step 5: Verify your SNMP configuration.

a. Use the show **snmp group** command in privilege EXEC mode to view the SNMP group configuration. Verify that your group is configured correctly.

Note: If you need to make changes to the group, use the command **no snmp group** to remove the group from the configuration and then re-add it with the correct parameters.

```
R1# show snmp group
groupname: ILMI                             security model:v1
contextname: <no context specified>         storage-type: permanent
readview : *ilmi                            writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: ILMI                             security model:v2c
contextname: <no context specified>         storage-type: permanent
readview : *ilmi                            writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: SNMP-G1                          security model:v3 priv
contextname: <no context specified>         storage-type: nonvolatile
readview : SNMP-RO                          writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active  access-list: PERMIT-SNMP
```

b. Use the command **show snmp user** to view the SNMP user information.

Note: The **snmp-server user** command is hidden from view in the configuration for security reasons. However, if you need to make changes to a SNMP user, you can issue the command **no snmp-server user** to remove the user from the configuration, and then re-add the user with the new parameters.

```
R1# show snmp user

User name: SNMP-Admin
Engine ID: 80000009030030F70DA30DA0
storage-type: nonvolatile   active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: SNMP-G1
```

Task 3: Configure a Synchronized Time Source Using NTP.

R2 will be the master NTP clock source for routers R1 and R3.

Note: R2 could also be the master clock source for switches S1 and S3, but it is not necessary to configure them for this lab.

Step 1: Set Up the NTP Master using Cisco IOS commands.

R2 is the master NTP server in this lab. All other routers and switches learn the time from it, either directly or indirectly. For this reason, you must ensure that R2 has the correct Coordinated Universal Time set.

a. Use the **show clock** command to display the current time set on the router.

```
R2# show clock
*19:48:38.858 UTC Wed Feb 18 2015
```

b. To set the time on the router, use the **clock set** *time* command.

```
R2# clock set 20:12:00 Dec 17 2014
R2#
*Dec 17 20:12:18.000: %SYS-6-CLOCKUPDATE: System clock has been updated from
01:20:26 UTC Mon Dec 15 2014 to 20:12:00 UTC Wed Dec 17 2014, configured from
console by admin on console.
```

c. Configure NTP authentication by defining the authentication key number, hashing type, and password that will be used for authentication. The password is case sensitive.

```
R2# config t
R2(config)# ntp authentication-key 1 md5 NTPpassword
```

d. Configure the trusted key that will be used for authentication on R2.

```
R2(config)# ntp trusted-key 1
```

e. Enable the NTP authentication feature on R2.

```
R2(config)# ntp authenticate
```

f. Configure R2 as the NTP master using the **ntp master** *stratum-number* command in global configuration mode. The stratum number indicates the distance from the original source. For this lab, use a stratum number of **3** on R2. When a device learns the time from an NTP source, its stratum number becomes one greater than the stratum number of its source.

```
R2(config)# ntp master 3
```

Step 2: Configure R1 and R3 as NTP clients using the CLI.

a. Configure NTP authentication by defining the authentication key number, hashing type, and password that will be used for authentication.

```
R1# config t
```

```
R1(config)# ntp authentication-key 1 md5 NTPpassword
```

b. Configure the trusted key that will be used for authentication. This command provides protection against accidentally synchronizing the device to a time source that is not trusted.

```
R1(config)# ntp trusted-key 1
```

c. Enable the NTP authentication feature.

```
R1(config)# ntp authenticate
```

d. R1 and R3 will become NTP clients of R2. Use the command **ntp server** *hostname*. The host name can also be an IP address. The command **ntp update-calendar** periodically updates the calendar with the NTP time.

```
R1(config)# ntp server 10.1.1.2
R1(config)# ntp update-calendar
```

e. Verify that R1 has made an association with R2 with the **show ntp associations** command. You can also use the more verbose version of the command by adding the **detail** argument. It might take some time for the NTP association to form.

```
R1# show ntp associations

address         ref clock       st   when   poll reach   delay   offset    disp
~10.1.1.2       127.127.1.1      3     14     64     3    0.000  -280073   3939.7
*sys.peer, # selected, +candidate, -outlyer, x falseticker, ~ configured
```

f. Issue the **debug ntp all** command to see NTP activity on R1 as it synchronizes with R2.

```
R1# debug ntp all
NTP events debugging is on
NTP core messages debugging is on
NTP clock adjustments debugging is on
NTP reference clocks debugging is on
NTP packets debugging is on

Dec 17 20.12:18.554: NTP message sent to 10.1.1.2, from interface 'Serial0/0/0'
(10.1.1.1).
Dec 17 20.12:18.574: NTP message received from 10.1.1.2 on interface 'Serial0/0/0'
(10.1.1.1).
Dec 17 20:12:18.574: NTP Core(DEBUG): ntp_receive: message received
Dec 17 20:12:18.574: NTP Core(DEBUG): ntp_receive: peer is 0x645A3120, next action is
1.
Dec 17 20:12:18.574: NTP Core(DEBUG): receive: packet given to process_packet
Dec 17 20:12:18.578: NTP Core(INFO): system event 'event_peer/strat_chg' (0x04)
status 'sync_alarm, sync_ntp, 5 events, event_clock_reset' (0xC655)
Dec 17 20:12:18.578: NTP Core(INFO): synchronized to 10.1.1.2, stratum 3
Dec 17 20:12:18.578: NTP Core(INFO): system event 'event_sync_chg' (0x03) status
 'leap_none, sync_ntp, 6 events, event_peer/strat_chg' (0x664)
Dec 17 20:12:18.578: NTP Core(NOTICE): Clock is synchronized.
Dec 17 20:12:18.578: NTP Core(INFO): system event 'event_peer/strat_chg' (0x04)
status 'leap_none, sync_ntp, 7 events, event_sync_chg' (0x673)
Dec 17 20:12:23.554: NTP: Calendar updated.
```

g. Issue the **undebug all** or the **no debug ntp all** command to turn off debugging.

```
R1# undebug all
```

h. Verify the time on R1 after it has made an association with R2.

```
R1# show clock
*20:12:24.859 UTC Wed Dec 17 2014
```

Task 4: Configure syslog Support on R1 and PC-A.

Step 1: Install the syslog server.

Free or trial versions of syslog server can be downloaded from the Internet. Use a web browser to search for "free windows syslog server" and refer to the software documentation for more information. Your instructor may also recommend a suitable syslog server for classroom use.

If a syslog server is not currently installed on the host, download a syslog server and install it on PC-A. If it is already installed, go to Step 2.

Step 2: Configure R1 to log messages to the syslog server using the CLI.

a. Start the syslog server.

b. Verify that you have connectivity between R1 and PC-A by pinging the R1 G0/1 interface IP address 192.168.1.1. If it is not successful, troubleshoot as necessary before continuing.

c. NTP was configured in Task 2 to synchronize the time on the network. Displaying the correct time and date in syslog messages is vital when using syslog to monitor a network. If the correct time and date of a message is not known, it can be difficult to determine what network event caused the message.

Verify that the timestamp service for logging is enabled on the router using the **show run** command. Use the following command if the timestamp service is not enabled.

```
R1(config)# service timestamps log datetime msec
```

d. Configure the syslog service on the router to send syslog messages to the syslog server.

```
R1(config)# logging host 192.168.1.3
```

Step 3: Configure the logging severity level on R1.

Logging traps can be set to support the logging function. A trap is a threshold that when reached, triggers a log message. The level of logging messages can be adjusted to allow the administrator to determine what kinds of messages are sent to the syslog server. Routers support different levels of logging. The eight levels range from 0 (emergencies), indicating that the system is unstable, to 7 (debugging), which sends messages that include router information.

Note: The default level for syslog is 6, informational logging. The default for console and monitor logging is 7, debugging.

a. Use the **logging trap** command to determine the options for the command and the various trap levels available.

```
R1(config)# logging trap ?
<0-7>          Logging severity level
alerts         Immediate action needed           (severity=1)
critical       Critical conditions               (severity=2)
debugging      Debugging messages                (severity=7)
emergencies    System is unusable                (severity=0)
errors         Error conditions                  (severity=3)
informational  Informational messages            (severity=6)
notifications  Normal but significant conditions (severity=5)
warnings       Warning conditions                (severity=4)
```

```
<cr>
```

b. Define the level of severity for messages sent to the syslog server. To configure the severity levels, use either the keyword or the severity level number (0–7).

Severity Level	Keyword	Meaning
0	emergencies	System is unusable
1	alerts	Immediate action required
2	critical	Critical conditions
3	errors	Error conditions
4	warnings	Warning conditions
5	notifications	Normal but significant condition
6	informational	Informational messages
7	debugging	Debugging messages

Note: The severity level includes the level specified and anything with a lower severity number. For example, if you set the level to 4, or use the keyword **warnings**, you capture messages with severity level 4, 3, 2, 1, and 0.

c. Use the **logging trap** command to set the severity level for R1.

```
R1(config)# logging trap warnings
```

d. What is the problem with setting the level of severity too high or too low?

_____

_____

Setting it too high (lowest level number) could generate logs that missed some very useful but not critical messages. Setting it too low (highest level number) could generate a large number of messages and fill up the logs with unnecessary information.

e. If the command **logging trap critical** were issued, which severity levels of messages would be logged?

_____

_____

Emergencies, alerts, and critical messages.

Step 4: Display the current status of logging for R1.

Use the **show logging** command to see the type and level of logging enabled.

```
R1# show logging
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)

No Active Message Discriminator.



No Inactive Message Discriminator.


    Console logging: level debugging, 72 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
```

```
    Buffer logging:  level debugging, 72 messages logged, xml disabled,
                     filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level warnings, 54 message lines logged
        Logging to 192.168.1.13  (udp port 514, audit disabled,
              link up),
              3 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
        Logging to 192.168.1.3  (udp port 514, audit disabled,
              link up),
              3 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
        Logging Source-Interface:       VRF Name:
<output omitted>
```

At what level is console logging enabled?

_____

Level 7 - debugging

At what level is trap logging enabled?

_____

Level 4 - warnings

What is the IP address of the syslog server?

_____

192.168.1.3

What port is syslog using?

_____

udp port 514

Part 5: Securing the Control Plane

In Part 5 of this lab, you will do as follows:

- Configure OSPF routing protocol authentication using SHA256.
- Verify that OSPF routing protocol authentication is working.

Task 1: Configure OSPF Routing Protocol Authentication using SHA256 Hashing.

Step 1: Configure a key chain on all three routers.

a. Assign a key chain name and number.

```
R1(config)# key chain NetAcad
R1(config-keychain)# key 1
```

b. Assign the authentication key string.

```
R1(config-keychain-key)# key-string CCNASkeystring
```

c. Configure the encryption algorithm to be used for authentication, use SHA256 encryption.

```
R1(config-keychain-key)#cryptographic-algorithm hmac-sha-256
```

Step 2: Configure the serial interfaces to use OSPF authentication.

a. Use the **ip ospf authentication** command to assign the key-chain to the serial interface on R1 and R3.

```
R1(config)# interface s0/0/0
R1(config-if)# ip ospf authentication key-chain NetAcad
R1(config)#
Feb 17 21:24:45.309: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on Serial0/0/0 from FULL
to DOWN, Neighbor Down: Dead timer expired


R3(config)# interface s0/0/1
R3(config-if)# ip ospf authentication key-chain NetAcad
R3(config)#
*Feb 17 21:23:14.078: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on Serial0/0/1 from FULL
to DOWN, Neighbor Down: Dead timer expired
```

b. Use the **ip ospf authentication** command to assign the key-chain to both serial interfaces on R2.

```
R2(config)# interface s0/0/0
R2(config-if)# ip ospf authentication key-chain NetAcad
R2(config)# interface serial 0/0/1
R2(config-if)# ip ospf authentication key-chain NetAcad
R2(config-if)#
Feb 17 21:36:25.114: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from
LOADING to FULL, Loading Done
Feb 17 21:36:30.686: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from
LOADING to FULL, Loading Done
```

Step 3: Verify OSPF Routing and Authentication is Correct.

a. Issue the show **ip ospf interface** command to verify that Authentication Key has been assigned to the serial interfaces on all routers.

```
R1# show ip ospf interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet Address 10.1.1.1/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 192.168.1.1, Network Type POINT_TO_POINT, Cost: 64
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           64        no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
```

```
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.2.2.2
  Suppress hello for 0 neighbor(s)
  Cryptographic authentication enabled
     Sending SA: Key 1, Algorithm HMAC-SHA-256 - key chain NetAcad
```

b. Issue the **show ip ospf** neighbor command to verify that each router lists the other routers in the network as neighbors.

```
R2# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.3.1       0   FULL/  -        00:00:39    10.2.2.1        Serial0/0/1
192.168.1.1       0   FULL/  -        00:00:37    10.1.1.1        Serial0/0/0
R2#
```

c. Issue the **show ip route** command to verify that all networks display in the routing table on all routers.

```
R3# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O        10.1.1.0/30 [110/1562] via 10.2.2.2, 00:01:56, Serial0/0/1
C        10.2.2.0/30 is directly connected, Serial0/0/1
L        10.2.2.1/32 is directly connected, Serial0/0/1
O     192.168.1.0/24 [110/1563] via 10.2.2.2, 00:01:46, Serial0/0/1
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, GigabitEthernet0/1
L        192.168.3.1/32 is directly connected, GigabitEthernet0/1
```

d. Use the **ping** command to verify connectivity between PC-A and PC-C.

If the pings are not successful, troubleshoot before continuing.

Part 6: Configure Automated Security Features

In Part 6 of this lab, you will do as follows:

- Use AutoSecure to secure R3.
- Review router security configurations with CLI.

Task 1: Use AutoSecure to Secure R3.

By using a single command in CLI mode, the AutoSecure feature allows you to disable common IP services that can be exploited for network attacks. It can also enable IP services and features that can aid in the defense of a network when under attack. AutoSecure simplifies the security configuration of a router and hardens the router configuration.

Step 1: Use the AutoSecure Cisco IOS feature.

a. Enter privileged EXEC mode using the **enable** command.

b. Issue the **auto secure** command on R3 to lock down the router. R2 represents an ISP router, so assume that R3 S0/0/1 is connected to the Internet when prompted by the AutoSecure questions. Respond to the AutoSecure questions as shown in the following output. The responses are bolded.

```
R3# auto secure
                --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: yes
Enter the number of interfaces facing the internet [1]: [Enter]

Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         unassigned      YES manual administratively down down
GigabitEthernet0/1         192.168.3.1     YES manual up                    up
Serial0/0/0                unassigned      YES NVRAM  administratively down down
Serial0/0/1                10.2.2.1        YES manual up                    up
Enter the interface name that is facing the internet: Serial0/0/1

Securing Management plane services...
```

```
Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp

Here is a sample Security Banner to be shown
at every access to device. Modify it to suit your
enterprise requirements.

Authorized Access only
  This system is the property of So-&-So-Enterprise.
  UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
  device. All activities performed on this device
  are logged. Any violations of access policy will result
  in disciplinary action.

Enter the security banner {Put the banner between
k and k, where k is any character}:
#  Unauthorized Access Prohibited #
Enter the new enable password: cisco67890
Confirm the enable password: cisco67890
Configuring AAA local authentication
Configuring console, Aux and vty lines for
local authentication, exec-timeout, transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected: 60

Maximum Login failures with the device: 2

Maximum time period for crossing the failed login attempts: 30

Configure SSH server? [yes]: [Enter]

Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:
```

```
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
Disabling mop on Ethernet interfaces

Securing Forwarding plane services...

Enabling unicast rpf on all interfaces connected
to internet

Configure CBAC Firewall feature? [yes/no]: no

This is the configuration generated:

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
banner motd ^C  Unaauthorized Access Prohibited ^C
security authentication failure rate 10 log
enable password 7 121A0C0411045A53727274
aaa new-model
aaa authentication login local_auth local
line console 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
line tty 1 2
 login authentication local_auth
 exec-timeout 15 0
```

```
login block-for 60 attempts 2 within 30
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
 transport input ssh telnet
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface Embedded-Service-Engine0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface GigabitEthernet0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface GigabitEthernet0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface Serial0/0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
access-list 100 permit udp any any eq bootpc
interface Serial0/0/1
 ip verify unicast source reachable-via rx allow-default 100
```

```
!
end


Apply this configuration to running-config? [yes]: [Enter]

Applying the config generated to running-config
% You already have RSA keys defined named R3.ccnasecurity.com.
% They will be replaced.

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

*Feb 18 20:29:18.159: %SSH-5-DISABLED: SSH 2.0 has been disabled
R3#
000066: *Feb 18 20:29:21.023 UTC: %AUTOSEC-1-MODIFIED: AutoSecure configuration has
been Modified on this device
R3#
```

Note: The questions asked and the output may vary depend on the features on the IOS image and device.

Step 2: Establish an SSH connection from PC-C to R3.

a. Start PuTTy or another SSH client, and log in with the **admin** account and password **cisco12345** created when AutoSecure was run. Enter the IP address of the R3 G0/1 interface **192.168.3.1**.

b. Because SSH was configured using AutoSecure on R3, you will receive a PuTTY security warning. Click **Yes** to connect anyway.

c. Enter privileged EXEC mode, and verify the R3 configuration using the **show run** command.

d. Issue the **show flash** command. Is there a file that might be related to AutoSecure, and if so what is its name and when was it created?

_____

_____

Yes. The filename is pre_autosec.cfg. It is a backup file that was created when AutoSecure ran.

e. Issue the command **more flash:pre_autosec.cfg**. What are the contents of this file, and what is its purpose?

_____

_____

This file is a saved file that contains the R3 configuration before AutoSecure ran.

f. How would you restore this file if AutoSecure did not produce the desired results?

_____

_____

Copy this file from flash to startup-config using the command **copy flash:pre_autosec.cfg start** and issue the **reload** command to restart the router.

Step 3: Contrast the AutoSecure-generated configuration of R3 with the manual configuration of R1.

a. What security-related configuration changes were performed on R3 by AutoSecure that were not performed in previous sections of the lab on R1?

Answers will vary but could include: AutoSecure enables AAA and creates a named authentication list (local_auth). Console, AUX, and vty logins are set up for local authentication. The security authentication failure rate 10 log command was added. The tcp intercept feature was enabled, ip http server was disabled, cdp was disabled, security passwords min-length was changed from 8 to 6. Logging trap debugging was enabled. Other minor but potentially exploitable services were disabled. An enable password was created. Logging buffered and logging console critical were enabled.

b. What security-related configuration changes were performed in previous sections of the lab that were not performed by AutoSecure?

Answers will vary but could include: Telnet access was excluded from vty transport input. Additional accounts were created.

c. Identify at least five unneeded services that were locked down by AutoSecure and at least three security measures applied to each interface.

Note: Some of the services listed as being disabled in the AutoSecure output above might not appear in the **show running-config** output because they are already disabled by default for this router and Cisco IOS version.

Services disabled include:

```
no service finger
```

```
no service pad
no service udp-small-servers
no service tcp-small-servers
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
```

For each interface, the following were disabled:

_____

_____

_____

_____

_____

_____

```
no ip redirects
no ip proxy-arp
no ip unreachables
no ip directed-broadcast
no ip mask-reply
```

Step 4: Test connectivity.

Ping from PC-A on the R1 LAN to PC-C on the router R3 LAN. If pings from PC-A to PC-C are not successful, troubleshoot before continuing.

Reflection

1. Explain the importance of securing router access and monitoring network devices.

_____

_____

_____

_____

_____

_____

Answers will vary but it should be clear after this lab that there are many potential vulnerabilities for routers that can be exploited. Securing these devices is a very important part of a network administrator's job and the security policy of an organization.

2. What advantages does SSH have over Telnet?

_____

_____

SSH encrypts all data and is much more secure than Telnet. Telnet data is transmitted in clear text, so password information can easily be compromised.

3. How scalable is setting up usernames and using the local database for authentication?

Because usernames would need to be set up on each device, using the local router database for authentication does not scale well. AAA with an external centralized server is a much more scalable solution. AAA is covered in detail in Chapter 3.

4. Why it is better to have centralized logging servers rather than to have the routers only log locally?

It is better to use centralized logging servers because it is much easier to manage and track events. In larger organizations it is almost impossible to keep track of the events of every individual router without having a centralized way to view information.

5. What are some advantages to using AutoSecure?

This tool can catch security vulnerabilities that many network administrators might overlook or be unaware of. It can lock down a router much faster than entering one command at a time and the tools result in less potential for entry errors. Also, the tool avoids the need to use complex Cisco IOS commands and procedures.

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Device Configs - Part 1 and 2 combined for R1 and R3

Router R1

```
R1# show run
Building configuration...

Current configuration : 2258 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable secret 9 $9$LrPqKyYl.EchgE$VCZn31W59uAo9RFD7VONSj1Tvhq/EjO3KmmCLZPfUyc
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
!
aaa session-id common
!
```

```
no ip domain lookup
ip domain name ccnasecurity.com
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
cts logging verbose
!
username user01 secret 9
$9$Uqn3n4m2O3rAo.$jyHU3iQPvV5sA5OjFA2Cj7wjq0RuR9eTO/0l.x2py7I
username admin privilege 15 secret 9
$9$mYvdwKU3M9li1E$4SFwoHz4EJwphYiinpcAk90te307iH/6kB8GfTAmk3w
!
redundancy
!
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 64000
!
interface Serial0/0/1
 no ip address
 shutdown
!
router ospf 1
 passive-interface GigabitEthernet0/1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^CUnauthorized access is strictly prohibited!^C
```

```
!
line con 0
 exec-timeout 5 0
 password 7 094F471A1A0A141D051C053938
 logging synchronous
line aux 0
 exec-timeout 5 0
 password 7 00071A1507540A1317314D5D1A
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 exec-timeout 5 0
 privilege level 15
 password 7 121A0C0411041A10333B253B20
 transport input ssh
!
scheduler allocate 20000 1000
!
end
```

Router R2

```
R2# show run
Building configuration...

Current configuration : 1361 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
cts logging verbose
!
redundancy
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
```

```
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 clock rate 64000
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 10.2.2.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input none
!
scheduler allocate 20000 1000
!
end
```

Router R3

```
R3# show run
Building configuration...

Current configuration : 2351 bytes
!
! Last configuration change at 19:17:15 UTC Wed Feb 18 2015
!
version 15.4
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable secret 9 $9$aEGzfeEiMDTbHE$tapocAnm/ghKbrxomsgNkCD3kUd4K/d/Zn3/o4GUt26
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
!
aaa session-id common
memory-size iomem 15
!
no ip domain lookup
ip domain name ccnasecurity.com
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
cts logging verbose
!
username user01 secret 9
$9$1EoFgBJoBlSna.$la2PMligey4qS84AkzIT5/ywSvT9a7ignhfFXRY/ezA
username admin privilege 15 secret 9
$9$deuZ2bl2gXRs4E$ri5TV1mXYvkVx..fdEAniGoyBuYULc3KDJvZ/XNCAp2
!
redundancy
!
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
```

```
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
!
router ospf 1
 passive-interface GigabitEthernet0/1
 network 10.2.2.0 0.0.0.3 area 0
 network 192.168.3.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^CUnauthorized access is strictly prohibited!^C
!
line con 0
 exec-timeout 5 0
 password ciscoconpass
 logging synchronous
line aux 0
 exec-timeout 5 0
 password ciscoauxpass
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 exec-timeout 5 0
 privilege level 15
 password ciscovtypass
 transport input ssh
!
scheduler allocate 20000 1000
!
end
```

Router configs added for Part 3

Routers R1 and R3

```
aaa new-model
!
parser view admin1
 secret 5 $1$MWgB$WpAllwq5gjLB457F70p0M.
 commands exec include all configure terminal
 commands exec include configure
 commands exec include all show
 commands exec include all debug
!
parser view admin2
```

```
 secret 5 $1$E7M.$OQfsFG5u3/BO.J4PKZ6WK1
 commands exec include all show
!
parser view tech
 secret 5 $1$qZGu$SQzAqmLGtewUPjwRO06ls0
 commands exec include show ip interface brief
 commands exec include show ip interface
 commands exec include show ip
 commands exec include show version
 commands exec include show parser view
 commands exec include show parser
 commands exec include show interfaces
 commands exec include show
```

Router R2 – No change

Router configs added for Part 4

Routers R1 and R3

```
ip access-list standard PERMIT-SNMP
 permit 192.168.1.0 0.0.0.255
 exit
snmp-server view SNMP-RO iso included
snmp-server group SNMP-G1 v3 priv read SNMP-RO access PERMIT-SNMP
snmp-server user SNMP-Admin SNMP-G1 v3 auth sha Authpass priv aes 128 Encrypass
ntp authentication-key 1 md5 NTPpassword
ntp authenticate
ntp trusted-key 1
ntp update-calendar
ntp server 10.1.1.2
```

Additional configurations for R1

```
service timestamps log datetime msec
logging host 192.168.1.3
loggin trap warnings
```

Router R2

```
ntp authentication-key 1 md5 NTPpassword
ntp authenticate
ntp trusted-key 1
ntp master 3
```

Router configs after Part 5

Router R1

```
R1# show run
Building configuration...

Current configuration : 3247 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable secret 9 $9$LrPqKyYl.EchgE$VCZn31W59uAo9RFD7VONSj1Tvhq/EjO3KmmCLZPfUyc
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
!
aaa session-id common
!
no ip domain lookup
ip domain name ccnasecurity.com
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
key chain NetAcad
 key 1
  key-string 7 08026F60282A0E120B181816232523
  cryptographic-algorithm hmac-sha-256
cts logging verbose
!
username user01 secret 9
$9$Uqn3n4m2O3rAo.$jyHU3iQPvV5sA5OjFA2Cj7wjq0RuR9eTO/0l.x2py7I
username admin privilege 15 secret 9
$9$mYvdwKU3M9li1E$4SFwoHz4EJwphYiinpcAk90te307iH/6kB8GfTAmk3w
!
redundancy
!
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
```

```
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 ip ospf authentication key-chain NetAcad
 clock rate 64000
!
interface Serial0/0/1
 no ip address
 shutdown
!
router ospf 1
 passive-interface GigabitEthernet0/1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
logging trap warnings
logging host 192.168.1.3
!
control-plane
!
banner motd ^CUnauthorized access is strictly prohibited!^C
parser view admin1
 secret 5 $1$AWY8$jBzt3rUtyObaDyvf.Ceh5.
 commands exec include all configure terminal
 commands exec include configure
 commands exec include all show
 commands exec include all debug
!
parser view admin2
 secret 5 $1$yBqL$HQ7yBsIIaWIelDCGW4sxM0
 commands exec include all show
!
parser view tech
 secret 5 $1$Hmq8$lkTJdPFcWQKGk0cLd9GXk0
 commands exec include show ip interface brief
 commands exec include show ip interface
 commands exec include show ip
 commands exec include show version
 commands exec include show parser view
 commands exec include show parser
 commands exec include show interfaces
 commands exec include show
!
line con 0
 exec-timeout 5 0
 password 7 094F471A1A0A141D051C053938
 logging synchronous
line aux 0
 exec-timeout 5 0
 password 7 00071A1507540A1317314D5D1A
line 2
 no activation-character
 no exec
```

```
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 exec-timeout 5 0
 privilege level 15
 password 7 121A0C0411041A10333B253B20
 transport input ssh
!
scheduler allocate 20000 1000
ntp authentication-key 1 md5 11272D350713181F13253920 7
ntp authenticate
ntp trusted-key 1
ntp update-calendar
ntp server 10.1.1.2
!
end
```

Router R2

```
R2# show run
Building configuration...

Current configuration : 1643 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
key chain NetAcad
 key 1
  key-string CCNASkeystring
  cryptographic-algorithm hmac-sha-256
cts logging verbose
!
redundancy
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
```

```
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 ip ospf authentication key-chain NetAcad
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 ip ospf authentication key-chain NetAcad
 clock rate 64000
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 10.2.2.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input none
!
scheduler allocate 20000 1000
ntp authentication-key 1 md5 0525323F314D5D1A0E0A0516 7
ntp authenticate
ntp trusted-key 1
ntp master 3
!
end
```

Router configs after Part 6

Router R3 (after running AutoSecure)

```
R3# show run
Building configuration...
```

```
Current configuration : 3622 bytes
!
version 15.4
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
security authentication failure rate 10 log
security passwords min-length 10
logging console critical
enable secret 9 $9$aEGzfeEiMDTbHE$tapocAnm/ghKbrxomsgNkCD3kUd4K/d/Zn3/o4GUt26
enable password 7 121A0C0411045A53727274
!
aaa new-model
!
aaa authentication login default local
aaa authentication login local_auth local
aaa authorization exec default local
!
aaa session-id common
memory-size iomem 15
!
no ip source-route
no ip gratuitous-arps
!
no ip bootp server
no ip domain lookup
ip domain name ccnasecurity.com
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
key chain NetAcad
 key 1
  key-string 7 022527752A350424555D1D0B0C1915
  cryptographic-algorithm hmac-sha-256
cts logging verbose
!
archive
 log config
  logging enable
username user01 secret 9
$9$1EoFgBJoBlSna.$la2PMligey4qS84AkzIT5/ywSvT9a7ignhfFXRY/ezA
username admin privilege 15 secret 9
$9$deuZ2bl2gXRs4E$ri5TV1mXYvkVx..fdEAniGoyBuYULc3KDJvZ/XNCAp2
!
```

```
redundancy
!
no cdp run
!
ip ssh time-out 60
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
interface Embedded-Service-Engine0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
 no mop enabled
!
interface GigabitEthernet0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
 duplex auto
 speed auto
 no mop enabled
!
interface GigabitEthernet0/1
 ip address 192.168.3.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 duplex auto
 speed auto
 no mop enabled
!
interface Serial0/0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip verify unicast source reachable-via rx allow-default 100
 ip ospf authentication key-chain NetAcad
!
router ospf 1
 passive-interface GigabitEthernet0/1
 network 10.2.2.0 0.0.0.3 area 0
 network 192.168.3.0 0.0.0.255 area 0
!
```

```
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
logging trap debugging
logging facility local2
!
access-list 100 permit udp any any eq bootpc
!
control-plane
!
banner motd ^C  Unaauthorized Access Prohibited ^C
parser view admin1
 secret 5 $1$1f3o$GItFgg1MEe51.QiPgtnxW/
 commands exec include all configure terminal
 commands exec include configure
 commands exec include all show
 commands exec include all debug
!
parser view admin2
 secret 5 $1$.ynW$LYQpSo74jn5radYOa8CrM/
 commands exec include all show
!
parser view tech
 secret 5 $1$qHMh$KgIgb/ej9vO/3d2xnzL7c1
 commands exec include show ip interface brief
 commands exec include show ip interface
 commands exec include show ip
 commands exec include show version
 commands exec include show parser view
 commands exec include show parser
 commands exec include show interfaces
 commands exec include show
!
line con 0
 exec-timeout 5 0
 password 7 02050D4808090C2E425E080A16
 logging synchronous
 login authentication local_auth
 transport output telnet
line aux 0
 exec-timeout 15 0
 password 7 02050D4808090E34545E080A16
 login authentication local_auth
 transport output telnet
line 2
 exec-timeout 15 0
 login authentication local_auth
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 exec-timeout 5 0
 privilege level 15
```

```
 password 7 104D000A0618041F15142B3837
 login authentication local_auth
 transport input telnet ssh
!
scheduler allocate 20000 1000
ntp authentication-key 1 md5 132B23221B0D17393C2B3A37 7
ntp authenticate
ntp trusted-key 1
ntp update-calendar
ntp server 10.1.1.2
!
end
```