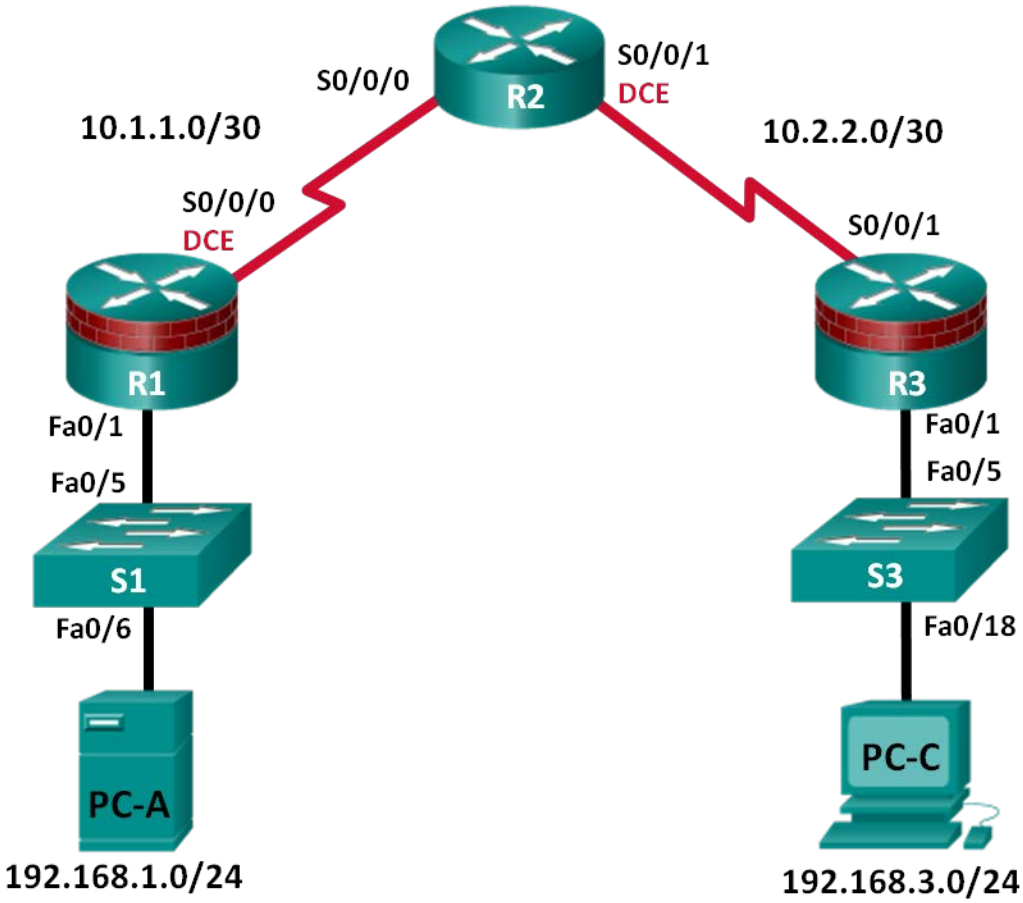
CCNA Security

Lab - Securing the Router for Administrative Access

Topology



Note: ISR G2 devices use GigabitEthernet interfaces instead of FastEthernet Interfaces.

IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	Fa0/1	192.168.1.1	255.255.255.0	N/A	S1 Fa0/5
	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	Fa0/1	192.168.3.1	255.255.255.0	N/A	S3 Fa0/5
	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 Fa0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 Fa0/18

Objectives

Part 1: Configure Basic Device Settings

- Cable the network as shown in the topology.
- Configure basic IP addressing for routers and PCs.
- Configure static routing, including default routes.
- 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 enhanced virtual login security.
- Configure an SSH server on a router.
- Configure an SSH client and verify connectivity.

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 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.
- Configure trap reporting on a router using SNMP.
- Make changes to the router and monitor syslog results on the PC.

Part 5: Configure Automated Security Features

- Lock down a router using AutoSecure and verify the configuration.

Background / Scenario

The router is a key component that 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 are critical to network security and should be part of a comprehensive security policy.

In this lab, you build a multi-router network and configure the routers and hosts. Use various CLI and CCP 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 1841 router using Cisco IOS software, release 15.1(4)M8 (Advanced IP Services image). 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: Make sure that the routers and the switches have been erased and have no startup configurations.

Required Resources

- 3 Routers (Cisco 1841 with Cisco IOS Release 15.1(4)M8 Advanced IP Services image or comparable)
- 2 Switches (Cisco 2960 or comparable)
- 2 PCs(Windows Vista or Windows 7 with CCP 2.5, SSH Client, Kiwi or Tftpd32 Syslog server, latest version of Java, Internet Explorer, and Flash Player)
- 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 and static routing.

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 prevent1 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 static routing on the routers.

a. Configure a static default route from R1 to R2 and from R3 to R2.

b. Configure a static route from R2 to the R1 LAN and from R2 to the R3 LAN.

Step 4: 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 5: Verify connectivity between PC-A and R3.

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 static 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** and **show ip route** commands to help identify routing protocol related problems.

Step 6: Save the basic running configuration for each router.

Save the basic running configuration for the routers as text files on your PC so that they 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 using the CLI.
- Research terminal emulation client software and configure the SSH client.

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.

```
R1(config)# enable secret cisco12345
```

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

_____

_____

_____

_____

_____

_____

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?

_____

_____

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? Why or why not?

_____

_____

_____

_____

What messages were displayed?

_____

_____

_____

_____

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)# login
```

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

_____

g. Enter privileged EXEC mode and issue the **show run** command. Can you read the enable secret password? Why or why not?

_____

_____

Can you read the console, aux, and vty passwords? Why or why not?

_____

_____

h. 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? Why or why not?

_____

_____

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

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

Which level of encryption is harder to crack and why?

_____

_____

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?

_____

_____

c. Exit privileged EXEC mode using the **disable** or **exit** command and press **Enter** to get started. Does the MOTD banner look like what you created with the **banner motd** command?

If the MOTD banner is not as you wanted it, recreate it using the **banner motd** command.

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 password ?
```

What options are available?

_____

_____

_____

Step 2: Create a new user account using the username command.

a. Create the user01 account, specifying the password with no encryption.

```
R1(config)# username user01 password 0 user01pass
```

b. Use the **show run** command to display the running configuration and check the password that is enabled.

Even though unencrypted (0) was specified, you still cannot read the password for the new user account, because the **service password-encryption** command is in effect.

Step 3: Create a new user account with a secret password.

a. Create a new user account with MD5 hashing to encrypt the password.

```
R1(config)# username user02 secret user02pass
```

b. Exit global configuration mode and save your configuration.

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

_____

_____

Step 4: 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 username **user01** and the password **user01pass**, previously defined.

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

_____

_____

d. After logging in, issue the **show run** command. Were you able to issue the command? Why or why not?

_____

_____

e. Enter privileged EXEC mode using the **enable** command. Were you prompted for a password? Why or why not?

_____

_____

Step 5: Test the new account by logging in from a Telnet session.

a. From PC-A, establish a Telnet session with R1.

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

Were you prompted for a user account? Why or why not?

_____

_____

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.

_____

_____

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?

_____

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 Enhanced Virtual Login Security on Routers R1 and R3.

Step 1: Configure the router to protect against login attacks.

Use the **login block-for** command to help prevent brute-force login attempts from a virtual connection, such as Telnet, SSH, or HTTP. This can help slow down dictionary attacks and help protect the router from a possible DoS attack.

a. From the user EXEC or privileged EXEC prompt, issue the **show login** command to see the current router login attack settings.

```
R1# show login
    No login delay has been applied.
    No Quiet-Mode access list has been configured.

    Router NOT enabled to watch for login Attacks
```

b. Use the **login block-for** command to configure a 60 second login shutdown (quiet mode timer) if two failed login attempts are made within 30 seconds.

```
R1(config)# login block-for 60 attempts 2 within 30
```

c. Exit global configuration mode and issue the **show login** command.

```
R1# show login
```

Is the router enabled to watch for login attacks? _____

What is the default login delay?

_____

_____

Step 2: Configure the router to log login activity.

a. Configure the router to generate system logging messages for both successful and failed login attempts. The following commands log every successful login and log failed login attempts after every second failed login.

```
R1(config)# login on-success log
R1(config)# login on-failure log every 2
R1(config)# exit
```

b. Issue the **show login** command. What additional information is displayed?

_____

_____

Step 3: Test the enhanced login security login configuration.

a. From PC-A, establish a Telnet session with R1.

```
PC-A> telnet 10.1.1.1
```

b. Attempt to log in with the wrong user ID or password two times. What message was displayed on PC-A after the second failed attempt?

_____

_____

What message was displayed on the router R1 console after the second failed login attempt?

_____

_____

c. From PC-A, attempt to establish another Telnet session to R1 within 60 seconds. What message was displayed on PC-A after the attempted Telnet connection?

_____

_____

What message was displayed on router R1 after the attempted Telnet connection?

_____

_____

_____

d. Issue the **show login** command within 60 seconds. What additional information is displayed?

_____

_____

Task 5: Configure the SSH Server on Router R1 and R3 Using the CLI.

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 secret cisco12345
```

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?

_____

_____

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 already be configured in a previous step. It is included here to provide all commands if you were 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.

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
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: _____

Authentication timeout: _____

Authentication retries: _____

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 6: 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?

_____

_____

_____

_____

_____

_____

_____

_____

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.

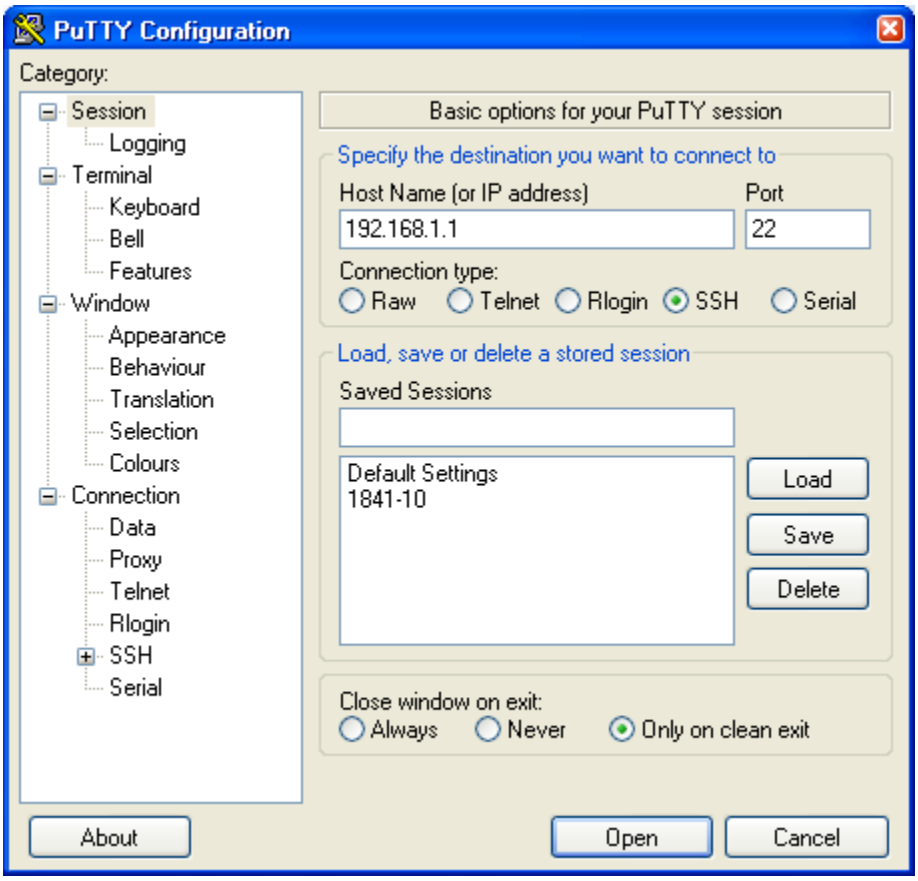
Note: The procedure described here is for PuTTY and pertains to PC-A.

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

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

b. Input the R1 Fa0/1 IP address **192.168.1.1** in the **Host Name (or IP address)** field.

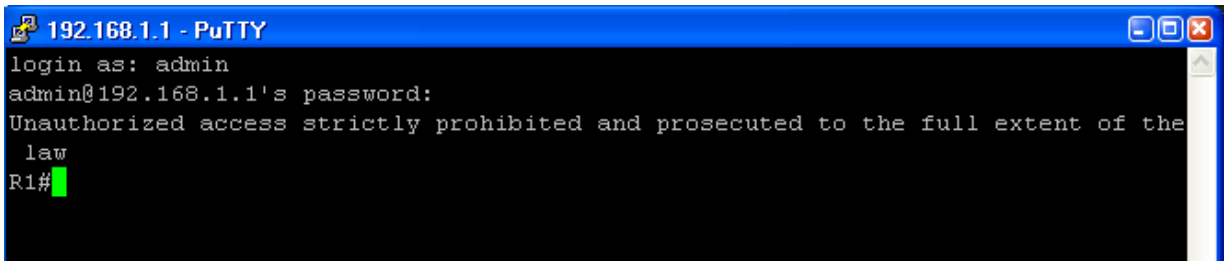
c. Verify that the **SSH** radio button is selected.



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?

_____

_____

_____

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.

_____

_____

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 user who does not have privilege level of 15.

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

_____

_____

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

l. Disable the generation of system logging messages for successful login attempts.

```
R1(config)# no login on-success log
```

Step 4: Save the configuration.

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

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

Note: Complete steps 3 and 4 between PC-C and router R3.

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, AAA must be enabled.

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

Note: AAA is covered in Chapter 3.

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
*Dec 16 22:41:17.483: %PARSER-6-VIEW_SWITCH: user unknown successfully set to view
'root'.
```

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
*Dec 16 22:56:46.971: %PARSER-6-VIEW_SWITCH: user unknown successfully set to
view 'admin1'.

R1# show parser view
Current view is ‘admin1’
```

f. Examine the commands available in the admin1 view.

```
R1# ?
Exec commands:
  configure  Enter configuration mode
  debug      Debugging functions (see also 'undebug')
  enable     Turn on privileged commands
  exit       Exit from the EXEC
  show       Show running system information
```

Note: There can be more EXEC commands available than displayed depending on your device and 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

*Dec 16 23:05:46.971: %PARSER-6-VIEW_SWITCH: user unknown successfully set to
view 'admin2'.
R1# show parser view
Current view is ‘admin2’
```

g. Examine the commands available in the admin2 view.

```
R1# ?
Exec commands:
  enable     Turn on privileged commands
  exit       Exit from the EXEC
  show       Show running system information
```

Note: There can be more EXEC commands available than displayed depending on your device and IOS image used.

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

_____

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
*Dec 16 23:13:46.971: %PARSER-6-VIEW_SWITCH: user unknown successfully set to
view 'tech'.

R1# show parser view
Current view is ‘tech’
```

g. Examine the commands available in the tech view.

```
R1# ?
Exec commands:
  enable     Turn on privileged commands
  exit       Exit from the EXEC
  show       Show running system information
```

Note: There can be more EXEC commands available than displayed depending on your device and IOS image used.

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

```
R1# show ?
  flash:      display information about flash: file system
  interfaces  Interface status and configuration
  ip          IP information
  parser      Show parser commands
  version     System hardware and software status
```

Note: There can be more EXEC commands available than displayed depending on your device and IOS image used.

i. Issue the **show ip interface brief** command. Were you able to do it as the tech user? Why or why not?

_____

_____

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

_____

_____

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**?

_____

_____

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.
- 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.

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     45756600 Apr 30 2014 13:40:20 +00:00 c1841-advipservicesk9-mz.151-4.M8.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
```

```
5840896 bytes available (58171392 bytes used)

R1# dir
Directory of flash:/

    1  -rw-    45756600  Apr 30 2014 13:40:20 +00:00  c1841-advipservicesk9-mz.151-
4.M8.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

65126400 bytes total (18952192 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
.Dec 17 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
.Dec 17 25:42:18.691: %IOS_RESILIENCE-5-CONFIG_RESIL_ACTIVE: Successfully secured
config archive [flash:.runcfg-20081219-224218.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 15.1 activated at 25:40:13 UTC Wed Dec 17 2008
Secure archive flash: c1841-advipservicesk9-mz.151-4.M8.bin type is image (elf)
[]
  file size is 37081324 bytes, run size is 37247008 bytes
  Runnable image, entry point 0x8000F000, run from ram

IOS configuration resilience version 15.1 activated at 25:42:18 UTC Wed Dec 17 2008
Secure archive flash:.runcfg-20081219-224218.ar type is config
configuration archive size 1986 bytes
```

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

_____

_____

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

18944000 bytes available (46182400 bytes used)
```

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

_____

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

_____

_____

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
.Dec 17 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
.Dec 17 25:48:47.972: %IOS_RESILIENCE-5-CONFIG_RESIL_INACTIVE: Disabled
secure config archival [removed flash:.runcfg-20081219-224218.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     45756600 Apr 30 2014 13:40:20 +00:00 c1841-advipservicesk9-mz.151-4.M8.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
```

```
18952192 bytes available (46174208 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 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.

Note: If you are using CCP to configure R2 to support NTP, skip this step and go to Step 2.

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

```
R2# show clock
*01:19:02.331 UTC Mon Dec 15 2008
```

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

```
R2# clock set 20:12:00 Dec 17 2008
R2#
*Dec 17 20:12:18.000: %SYS-6-CLOCKUPDATE: System clock has been updated from
01:20:26 UTC Mon Dec 15 2008 to 20:12:00 UTC Wed Dec 17 2008, configured from
console by admin on console.
```

c. 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
```

Task 3: Configure syslog Support on R1 and PC-A.

Step 1: Install the syslog server.

Tftpd32 includes a TFTP server, TFTP client, and a syslog server and viewer. The Kiwi Syslog Daemon is only a dedicated syslog server. You can use either with this lab. Both are available as a free version and run with Microsoft Windows.

If a syslog server is not currently installed on the host, download the latest version of Tftpd32 from http://tftpd32.jounin.net or Kiwi from http://www.kiwisyslog.com and install it on your desktop. If it is already installed, go to Step 2.

Note: This lab uses the Ttftpd32 application for the syslog server functionality.

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

a. Verify that you have connectivity between R1 and PC-A by pinging the R1 Fa0/1 interface IP address 192.168.1.1. If it is not successful, troubleshoot as necessary before continuing.

b. 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
```

c. 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?

_____

_____

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

_____

_____

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:
```

At what level is console logging enabled?

_____

At what level is trap logging enabled?

_____

What is the IP address of the syslog server?

_____

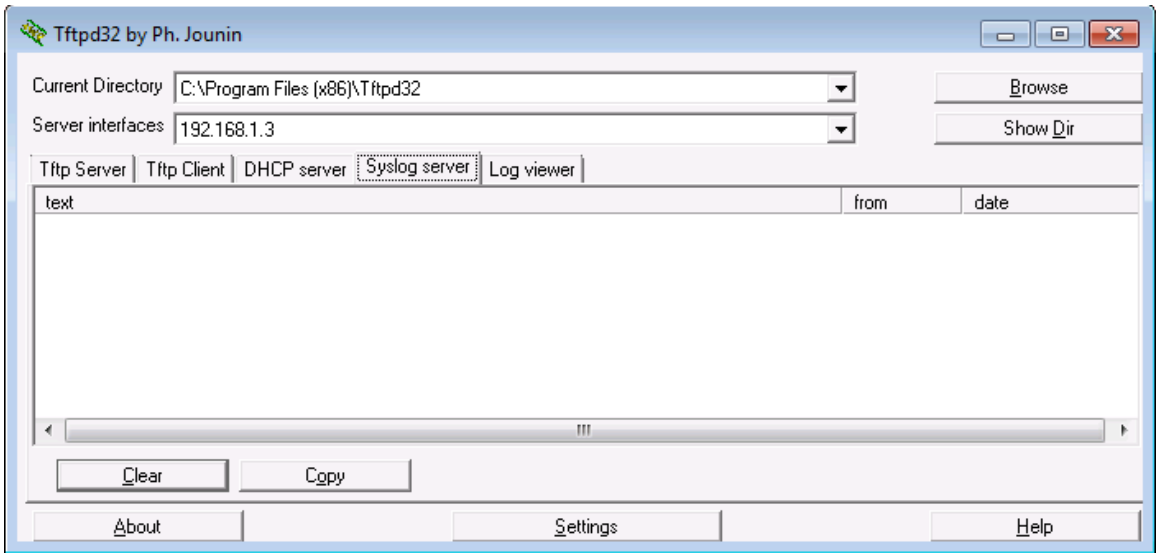
What port is syslog using?

_____

Step 5: Start the Ttftpd32 Syslog Server.

a. Open the Tftpd32 application icon on your desktop or click the **Start** button and choose **All Programs** > **Tftpd32** > **Tftpd32**.

b. Select the **Syslog server** tab.



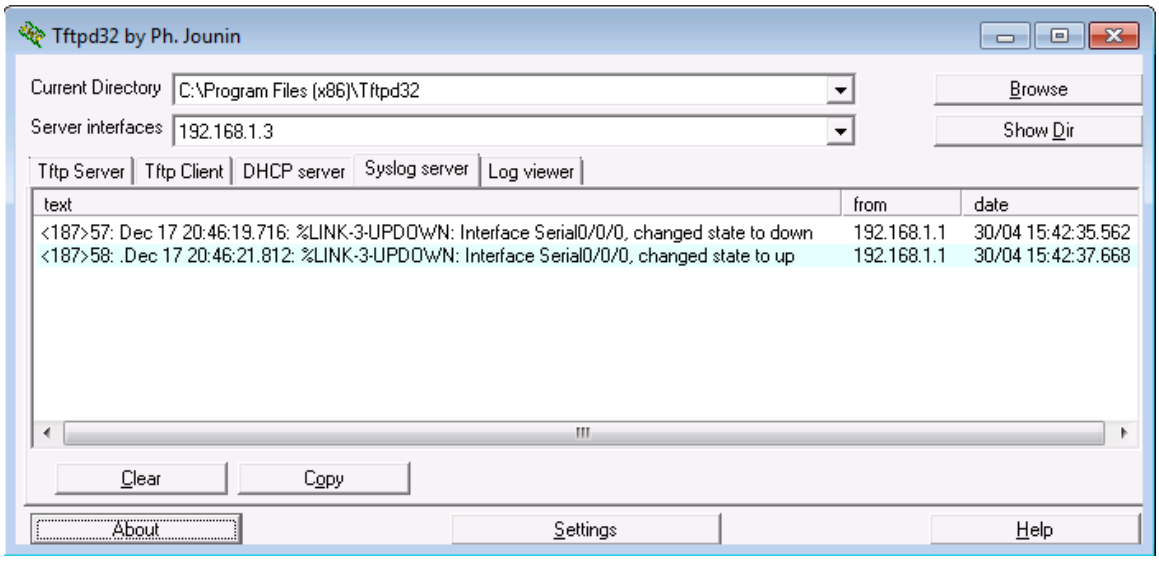
Step 6: Verify that logging to the syslog server is occurring.

On the syslog server host PC-A, observe messages as they are sent from R1 to the syslog server.

Generate a logging message by shutting down the Serial0/0/0 interface on R1 or R2 and then re-enabling it.

```
R2(config)# interface S0/0/0
R2(config-if)# shutdown
R2(config-if)# no shutdown
```

The Tftpd32 screen should look similar to the one below.



What would happen if you shut down the Fa0/1 interface on R1 (do not actually perform this action)?

_____

_____

Part 5: Configure Automated Security Features

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

- Restore routers R1 and R3 to their basic configuration.
- Use AutoSecure to secure R3.
- Fix security problems on R1 using the Security Audit tool.

Task 1: Restore Router R3 to Its Basic Configuration.

To avoid confusion as to what was already entered and what AutoSecure provides for the router configuration, start by restoring router R3 to its basic configuration.

Step 1: Erase and reload the router.

a. Connect to the R3 console and log in as admin.

b. Enter privileged EXEC mode.

c. Erase the startup config and then reload the router.

Step 2: Restore the basic configuration.

a. When the router restarts, restore the basic configuration for R3 that was created and saved in Part 1 of this lab.

b. Issue the **show run** command to view the current running configuration. Are there any security related commands?

_____

_____

c. Test connectivity by pinging from host PC-A on the R1 LAN to PC-C on the R3 LAN. If the pings are not successful, troubleshoot the router and PC configurations until they are.

d. Save the running config to the startup config using the **copy run start** command.

Task 2: 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]:  Press ENTER to
accept the default of 1 in square brackets.

Interface         IP-Address  OK?  Method Status                  Protocol
FastEthernet0/0   unassigned  YES  NVRAM  administratively down   down
FastEthernet0/1   192.168.3.1 YES  NVRAM  up                      up
Serial0/0/0       unassigned  YES  NVRAM  administratively down   down
Serial0/0/1       10.2.2.1    YES  NVRAM  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 #

Enable secret is either not configured or
 is the same as enable password
Enter the new enable secret: cisco12345
Confirm the enable secret : cisco12345
Enter the new enable password: cisco67890
Confirm the enable password: cisco67890

Configuration of local user database
Enter the username: admin
Enter the password: cisco12345
Confirm the password: cisco12345
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and 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]: Press ENTER to accept the default of yes

Enter the domain-name: ccnasecurity.com

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 CEF (This might impact the memory requirements for your platform)
Enabling unicast rpf on all interfaces connected
to internet

Configure CBAC Firewall feature? [yes/no]: no
Tcp intercept feature is used prevent tcp syn attack
on the servers in the network. Create autosec_tcp_intercept_list
to form the list of servers to which the tcp traffic is to be observed

Enable tcp intercept feature? [yes/no]: yes

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 Unauthorized Access Prohibited ^C
security passwords min-length 6
```

```
security authentication failure rate 10 log
enable secret 5 $1$FmV1$.xZUegmNYFJwJv/oFwwvG1
enable password 7 045802150C2E181B5F
username admin password 7 01100F175804575D72
aaa new-model
aaa authentication login local_auth local
line con 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
 login authentication local_auth
 exec-timeout 15 0
login block-for 60 attempts 2 within 30
ip domain-name ccnasecurity.com
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 FastEthernet0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface FastEthernet0/1
 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
interface Vlan1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
ip cef
access-list 100 permit udp any any eq bootpc
interface Serial0/0/1
 ip verify unicast source reachable-via rx allow-default 100
ip tcp intercept list autosec_tcp_intercept_list
ip tcp intercept drop-mode random
ip tcp intercept watch-timeout 15
ip tcp intercept connection-timeout 3600
ip tcp intercept max-incomplete low 450
ip tcp intercept max-incomplete high 550
!
end

Apply this configuration to running-config? [yes]: <ENTER>

Applying the config generated to running-config
The name for the keys will be: R3.ccnasecurity.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 3 seconds)

"ip tcp intercept max-incomplete low <val>" is deprecated
Please use "ip tcp intercept max-incomplete low <val> high <val>"
"ip tcp intercept max-incomplete high <val>" is deprecated
Please use "ip tcp intercept max-incomplete low <val> high <val>"
R3#
000037: *Dec 19 21:18:52.495 UTC: %AUTOSEC-1-MODIFIED: AutoSecure configuration
has been Modified on this device
```

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 Fa0/1 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?

_____

_____

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

_____

_____

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

_____

_____

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?

_____

_____

_____

_____

_____

_____

_____

_____

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

_____

_____

_____

_____

_____

_____

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:

_____

_____

_____

_____

_____

_____

For each interface, the following were disabled:

_____

_____

_____

_____

_____

_____

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.