IT NE 2005
Securing the Router for Administrative Access

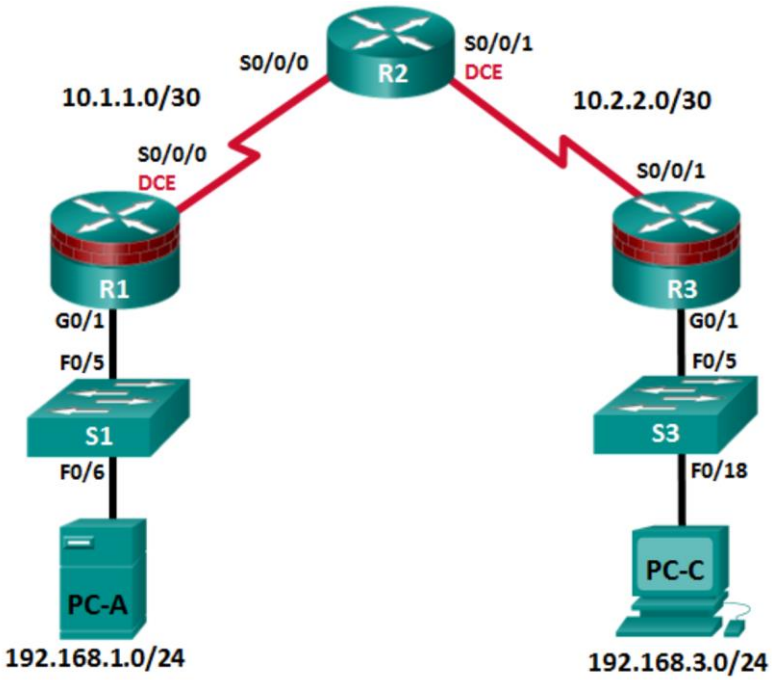
LAB 3

WEEK - 3

CONTENTS

Week 3 Securing Router

Objective: Securing the Router for Administrative Access



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1-S0000	F0/1	192.168.1.1	255.255.255.0	N/A	S1-S0000 F0/1
	S0/0 (DEC)	10.1.1.1	255.255.255.252	N/A	N/A
R2-S0000	S0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3-S0000	F0/1	192.168.3.1	255.255.255.0	N/A	S3-S0000 F0/1
	S0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A-S0000	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-C-S0000	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S2 F0/3

In this lab, you will perform the following tasks:

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

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.

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

Task 1: Configure Basic Device Settings

The desktop system assigned to you serves as an end-user terminal. You access and manage the lab environment from the student desktop system using GNS3 Software.

Students should perform the steps in this task individually.

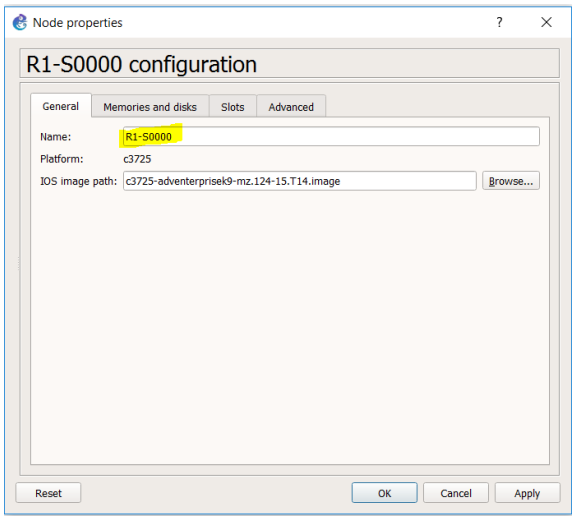
In Part 1, set up the network topology and configure basic settings, such as interface IP addresses.

Step 1: Deploy router in GNS3 network.

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

Step 2: Configure basic settings for each router.

a. Configure host names as shown in the topology plus your student ID and cable the network as shown in the topology.



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

R1 Config

```
R1-S0000#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1-S0000(config)#interface f0/1
R1-S0000(config-if)#ip address 192.168.1.1 255.255.255.0
R1-S0000(config-if)#no shutdown
R1-S0000(config-if)#exit
R1-S0000(config)#interface s0/0
R1-S0000(config-if)#ip address 10.1.1.1 255.255.255.252
R1-S0000(config-if)#no shutdown
R1-S0000(config-if)#exit
R1-S0000(config)#exit
R1-S0000#copy running-config startup-config
Destination filename [startup-config]?
```

R3 Config

```
R3-S0000#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3-S0000(config)#interface f0/1
R3-S0000(config-if)#ip address 192.168.3.1 255.255.255.0
R3-S0000(config-if)#no shutdown
R3-S0000(config-if)#exit
R3-S0000(config)#interface s0/1
R3-S0000(config-if)#ip address 10.2.2.1 255.255.255.252
R3-S0000(config-if)#no shutdown
R3-S0000(config-if)#exit
R3-S0000(config)#exit
R3-S0000#copy running-config startup-config
Destination filename [startup-config]?
```

R2 Config

```
R2-S0000#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2-S0000(config)#interface s0/0
R2-S0000(config-if)#ip address 10.1.1.2 255.255.255.252
```

```
R2-S0000(config-if)#no shutdown
R2-S0000(config-if)#exit
R2-S0000(config)#interface s0/1
R2-S0000(config-if)#ip address 10.2.2.2 255.255.255.252
R2-S0000(config-if)#no shutdown
R2-S0000(config-if)#exit
R2-S0000(config)#exit
R2-S0000#copy running-config startup-config
Destination filename [startup-config]?
```

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

```
R1-S0000# Conf t

R1-S0000(config)# interface S0/0

R1-S0000(config-if)# clock rate 64000

R1-S0000(config-if)# Exit

R1-S0000(config)# Exit

R3:

R3-S000 # Conf t

R3-S0000(config)# interface S0/1

R3-S0000(config-if)# clock rate 64000

R3-S0000(config-if)# Exit

R3-S0000(config)# Exit

R2:

R2-S000 # Conf t

R2-S0000(config)# interface S0/0

R2-S0000(config-if)# clock rate 64000

R2-S0000(config-if)# exit

R2-S0000(config)# interface S0/1

R2-S0000(config-if)# clock rate 64000

R2-S0000(config-if)# Exit

R2-S0000(config)# Exit
```

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

R1-S000 # Conf t

R1-S0000(config)# no ip domain-lookup

R1-S0000(config-if)# Exit

R1-S0000(config)# Exit

R2:

R2-S000 # Conf t

R2-S0000(config)# no ip domain-lookup

R2-S0000(config-if)# Exit

R2-S0000(config)# Exit

R3:

R3-S000 # Conf t

R3-S0000(config)# no ip domain-lookup

R3-S0000(config-if)# Exit

R3-S0000(config)# Exit

Step 3: Configure OSPF routing on the routers.

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

R1-S0000(config)# Conf t

R1-S0000(config)# router ospf 1

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

R1-S0000(config-router)# network 192.168.1.0 0.0.0.255 area 0

R1-S0000(config-router)# network 10.1.1.0 0.0.0.3 area 0

R1-S0000(config-if)# Exit

R1-S0000(config)# Exit

c. Configure OSPF on R2-STUDENTID and R3-STUDENTID.
R3:
R3-S0000# Conf t

R3-S0000(config)# router ospf 1
R3-S0000(config-router)# network 192.168.3.0 0.0.0.255 area 0
R3-S0000(config-router)# network 10.2.2.0 0.0.0.3 area 0

R3-S0000(config-if)# Exit

R3-S0000(config)# Exit

R2:
R2-S0000# Conf t
R2-S0000(config)# router ospf 1
R2-S0000(config-router)# network 10.1.1.0 0.0.0.3 area 0
R2-S0000(config-router)# network 10.2.2.0 0.0.0.3 area 0

R2-S0000(config-if)# Exit

R2-S0000(config)# Exit

d. Issue the passive-interface command to change the f0/1 interface on R1-STUDENTID and R3-STUDENTID to passive.

R1-S0000# Conf t

R1-S0000(config)# router ospf 1

R1-S0000(config-router)# passive-interface f0/1

R1-S0000(config-if)# Exit

R1-S0000(config)# Exit

R3:

R3-S0000# Conf t

R3-S0000(config)# router ospf 1

R3-S0000(config-router)# passive-interface f0/1

R3-S0000(config-if)# Exit

R3-S0000(config)# Exit

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-S0000 # 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
```

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

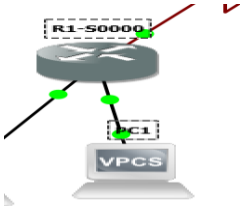
R1-S0000 # show ip route

```
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
```

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.

Deploy VPCS A: Connect to port R1 f0/2



PC-A-S0000> ip 192.168.1.2/24 192.168.1.1

PC-A-S0000> Save

Deploy VPCS C: Connect to S3 f0/2

PC-C-S0000> ip 192.168.3.3/24 192.168.3.1

PC-A-S0000> Save

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

a. Ping from R1-STUDENTID to R3-STUDENTID.

Ping 192.168.3.3

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

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

Task2: Control Administrative Access for Routers

- 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-STUDENTID.
- Research terminal emulation client software and configure the SSH client.
- Configure an SCP server on R1-STUDENTID.

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

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

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-S0000# conf t

R1-S0000(config)# security passwords min-length 10

R2-S0000# conf t

R2-S0000(config)# security passwords min-length 10

R1-S0000# conf t

R3-S0000(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-S0000(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-S0000# conf t

R1-S0000(config)# line console 0

R1-S0000(config-line)# password ciscocon

R1-S0000(config-line)# exec-timeout 5 0

R1-S0000(config-line)# login

R1-S0000(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-STUDENTID.

```
R1-S0000(config)# line aux 0
R1-S0000(config-line)# password ciscoauxpass
R1-S0000(config-line)# exec-timeout 5 0
R1-S0000(config-line)# login
```

d. Telnet from R2-STUDENTID to R1-STUDENTID.

```
R2-S0000> telnet 10.1.1.1
```

Were you able to login? Explain.

_____

_____

What messages were displayed?

_____

_____

Configure the password on the vty lines for router R1-STUDENTID.

```
R1-S0000(config)# line vty 0 4
R1-S0000(config-line)# password ciscovtypass
R1-S0000(config-line)# exec-timeout 5 0
R1-S0000(config-line)# transport input telnet
R1-S0000(config-line)# login
```

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

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

_____

_____

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

_____

_____

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

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

Step 4: Encrypt clear text passwords.

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

```
R1-S0000(config)# service password-encryption
```

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

At what level (number) is the default 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-STUDENTID and R3-STUDENTID.

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-S0000(config)# banner motd $Unauthorized access strictly prohibited!$
R1-S0000(config)# exit
```

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

c. Configure Banner on R2-STUDENTID and R3-STUDENTID?

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

Step 1: Investigate the options for the username command.

In global configuration mode, enter the following command:

R1-S0000(config)# username user01?

What options are available?

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-S0000(config)# username user01 secret user01pass

b. Exit global configuration mode and save your configuration.

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

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-S0000(config)# line console 0

R1-S0000(config-line)# login local

R1-S0000(config-line)# end

R1-S0000# exit

b. Exit to the initial router screen which displays: R1-STUDENTID 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?

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

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

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

a. From Router2-STUDENTID, establish a Telnet session with R1-STUDENTID. Telnet is disabled by default in Windows 7. If necessary, search online for the steps to enable Telnet in Windows 7.

R2-S0000# telnet 192.168.1.1

Were you prompted for a user account? Explain.

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

R1-S0000(config)# line vty 0 4

R1-S0000(config-line)# login local

c. From Router2-STUDENTID, telnet to R1-STUDENTID again.

R2-S0000# 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-STUDENTID, 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-S0000(config)# line aux 0

R1-S0000(config-line)# login local

g. End the Telnet session with the exit command.

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

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-S0000# conf t

R1-S0000(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-S0000(config)# username admin privilege 15 secret cisco12345
```

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

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-S0000(config)# line vty 0 4

R1-S0000(config-line)# privilege level 15

R1-S0000(config-line)# login local

R1-S0000(config-line)# transport input ssh

R1-S0000(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-S0000(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-S0000(config)# crypto key generate rsa general-keys modulus 1024

The name for the keys will be: R1-STUDENTID.ccnasecurity.com

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1-S0000(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-S0000(config)# ip ssh version 2

R1-S0000(config)# exit

Note: The details of encryption methods later.

Step 6: Verify the SSH configuration.

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

R1-S0000# 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-S0000(config)# ip ssh time-out 90

R1-S0000(config)# ip ssh authentication-retries 2

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

R1-S0000# 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?

Step 2: Verify SSH connectivity to R1 from R2.

a. From Router2-STUDENTID, telnet to R1-STUDENTID again.

R2-S0000# ssh -l admin 192.168.1.1

(l = L lower case)

User cisco12345 as password

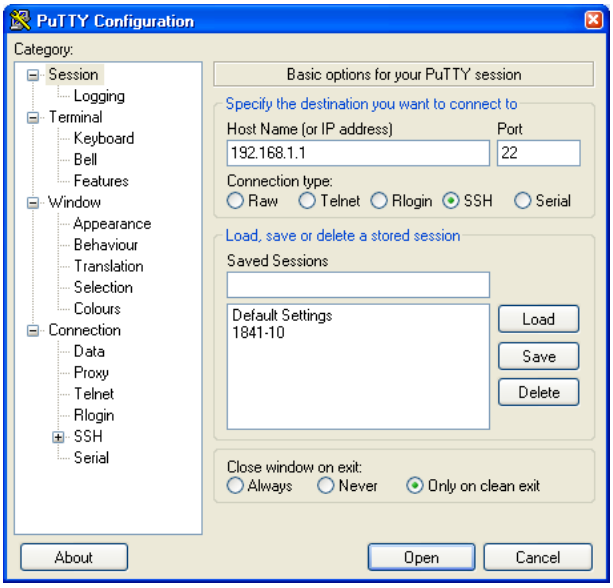
OR

Use Host 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.

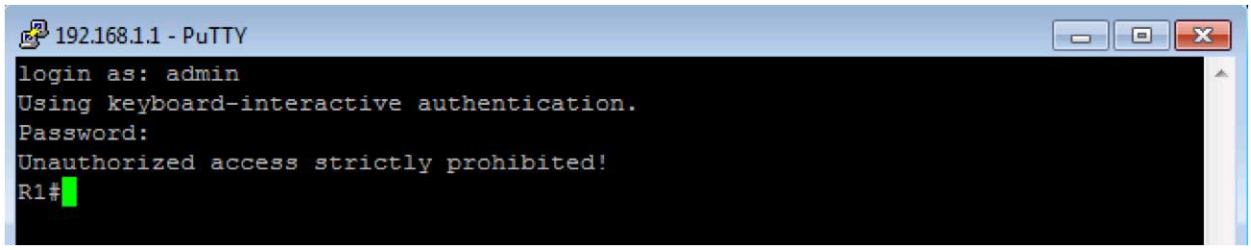
c. Verify that the SSH radio button is selected



d. Click Open.

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

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



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

R1-S0000# show users

What users are connected to router R1 at this time?

_____
_____
_____

h. Close the PuTTY SSH session window or Telent from R2-StudentID.

i. Try to open a Telnet session to your router from PC-A or R2-S0000. Were you able to open the Telnet session?

Explain.

_____

_____

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?

_____

_____

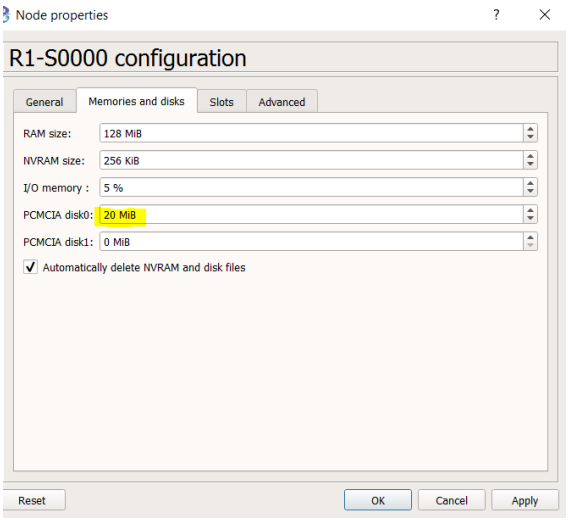
k. Use the enable command to enter privilege EXEC mode and enter the enable secret password cisco12345.

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.

Add flash storage to R1-StudentID and R3-SutdentID



Stop and Start Routers and Format Flash:

R1-S0000#erase flash:

R3-S0000#erase flash:

R1-S0000#format flash:

R3-S0000#format flash:

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

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 Step 2a 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

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
```

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

R1#
```

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
```

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?

_____

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.

_____

_____

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

_____

_____

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:

- 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 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

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

```
R2# clock set 20:12:00 Aug 16 2017

R2#
```

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

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