Module 5a Mastery Assessment – Securing the Router for Administrative Access

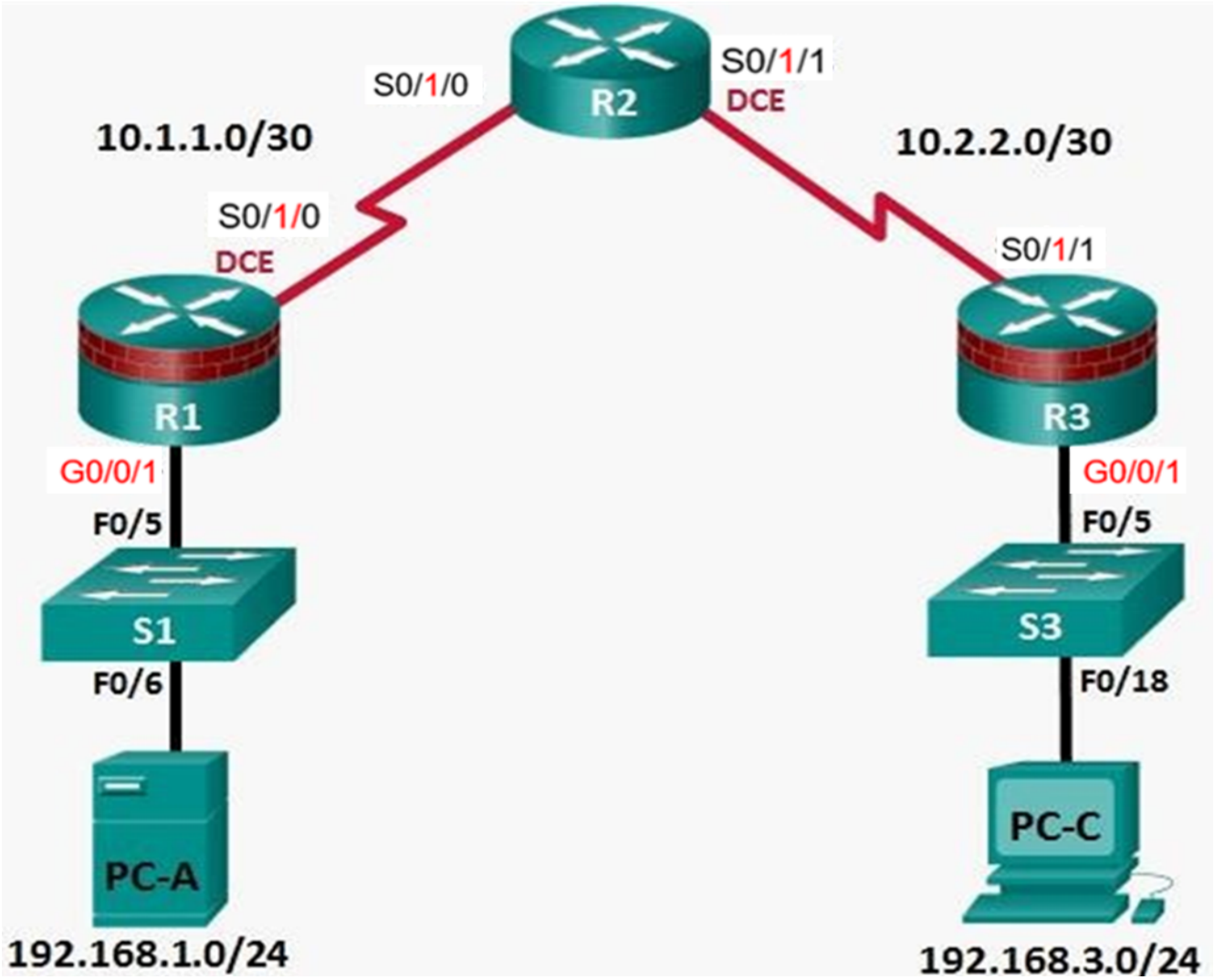
NetLab+ Class Selection: CCNA Security v2.0 for use with MAP w/ASA
2.6.1.2 Lab - Securing the Router for Administrative Access

NDG

This lab has been updated for use on NETLAB+.

TSTC SITE: https://netlab.tstc.edu/

Topology



NOTE: NETLAB Lab TOPOLOGY and CONTENT TAB details do not reflect details in this lab document. Use this document as your complete instructions for this lab.

IP Addressing Table

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

Red Text denotes changes from NDG NetLab defaults

Objectives

Part 1: Configure Basic Device Settings

- 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 all passwords.
- Configure an SSH server on a router.
- Configure an SSH client and verify connectivity.
- Configure AAA on a router.

Part 3: Management Reporting

- 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.

Background / Scenario

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

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

Required Resources

- 3 Routers (Cisco 4321 with Cisco IOS with a Security Technology Package license)
- 2 Switches (Cisco 2960 or comparable) (Not Required)
- 2 PCs (Windows 10, SSH Client, Kiwi or Tftpd32 Syslog server)
- Serial and Ethernet cables as shown in the topology
- Console cables to configure Cisco networking devices

Part 1: Configure Basic Device Settings

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

Step 1: 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 of 6400 for routers with a DCE serial cable attached to their serial interface

d. To prevent the router from attempting to translate incorrectly entered commands as though they were host names, disable DNS lookup.

Step 2: Configure OSPF routing on the routers.

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

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

c. Configure OSPF on R2 and R3.

d. Issue the **passive-interface** command to change the G0/0/1 interface on R1 and R3 to passive.

Step 3: 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.

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

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 PC-C.

a. Ping from R1 to R3.

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

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

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

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

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

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

Part 2: Control Administrative Access for Routers

In Part 2, you will:

- Configure passwords.
- Configure virtual login security.
- Configure an SSH server on R1.
- 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 the enable secret password.

Configure the enable secret encrypted password on both routers. Use the type 9 (SCRYPT) hashing algorithm. Password: **cisco123456**

Step 2: Configure basic console and virtual access lines.

a. Configure a console password of **ciscoconpass** and enable login for routers.

b. Configure the password of **ciscovtypass** on the vty lines for router R1.

Task 2: Configure Username Password Security on Routers R1 and R3.

Step 1: Create username user01 and password user01pass.

Step 2: Test the new account by logging in to the console.

Step 3: Take a screenshot.

Task 3: Configure the SSH Server on Router R1 and R3.

Step 1: Configure a domain name of ccnasecurity.com.

Step 2: Configure a privileged user for login from the SSH client.
Username: admin Password: cisco12345

Task 4: SSH connectivity with a SSH Client.

Step 1: Verify SSH connectivity to R1 from PC-A.
Step 2: Take Screenshot.

Task 5: Configure AAA authentication and authorization on R1.

Task 5.1: Configure the Local User Database Using Cisco IOS.

Step 1: Configure the local user database.

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

```
Username: Admin01 Password: Admin01pass using privilege 15
```

Task 5.2: Configure AAA Local Authentication Using Cisco IOS.

Step 1: Enable AAA services.

Step 2: Implement AAA services for console access using the local database.

a. Create the default login authentication list by issuing the **aaa authentication login default** *method1[method2][method3]* command with a method list using the **local** and **none** keywords.

Note: If you do not set up a default login authentication list, you could get locked out of the router and be forced to use the password recovery procedure for your specific router.

Note: The **local-case** parameter is used to make usernames case-sensitive.

b. Exit to the initial router screen that displays:

c. Log in to the console as **Admin01** with a password of **Admin01pass**.

d. Take Screenshot

Step 5.3: Create an AAA authentication profile for Telnet using the local database.

a. Create a unique **authentication** list for Telnet access to the router. Specify a list name of TELNET_LINES and apply it to the vty lines.

b. Create an authentication profile that is not the default.

c. Verify that this authentication profile is used by opening a Telnet session from PC-C to R3.

d. Take Screenshot

Task 6: Configure SNMPv3 Security using an ACL.

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**.

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

Step 2: Configure the SNMP view.

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

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.**

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**.

Step 5: Verify your SNMP configuration.

a. 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.

b. View the SNMP user information.

c. Take Screenshot

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.

Task 7: Configure a Synchronized Time Source Using NTP.

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

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

R2 is the master NTP server in this lab.

a. Display the current time set on the router R2.

b. To set the time on the router **15 minutes ahead** of the current time.

c. Configure NTP authentication.

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

e. Enable the NTP authentication feature on R2.

f. Configure R2 as the NTP master. For this lab, use a stratum number of **3** on R2.

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

a. Configure NTP authentication.

b. Configure the trusted key that will be used for authentication.

c. Enable the NTP authentication feature.
d. R1 and R3 will become NTP clients of R2.
e. Verify that R1 has made an association with R2
f. Turn on debugging to see NTP activity on R1 as it synchronizes with R2.
g. Turn off debugging.
h. Verify the time on R1 after it has made an association with R2.
i. Take Screenshot

Task 8: Configure syslog Support on R1 and PC-A.

Step 1: Ready PC-A Ttftpd to collect syslog.

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 G0/0/1 interface IP address 192.168.1.1. If it is not successful, troubleshoot as necessary before continuing.
b. Verify that the timestamp service for logging is enabled on the router.
c. Configure the syslog service on the router to send syslog messages to the syslog server.

Step 3: Configure the logging severity level on R1.

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

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

a. Use the **show logging** command to see the type and level of logging enabled.
b. Take Screenshot from PC-A of Ttftpd of the syslog messages.

Grading Rubric

	Exemplary (10)	Beginning /Incomplete (0)	Score
Part A - Task 2 Step 3	Screenshot submitted pts.10	(0) Nothing recorded or submitted	
Part A - Task 4 Step 2	Screenshot submitted pts.10	(0) Nothing recorded or submitted	
Part A - Task 5.2 Step 2	Screenshot submitted pts.10	(0) Nothing recorded or submitted	
Part A - Task 5.3	Screenshot submitted pts.10	(0) Nothing recorded or submitted	
Part A - Task 6 Step 5	Screenshot submitted pts.10	(0) Nothing recorded or submitted	
Part A - Task7 Step 2	Screenshot submitted pts.10	(0) Nothing recorded or submitted	
Part A - Task 8 Step 4	Screenshot submitted pts.10	(0) Nothing recorded or submitted	