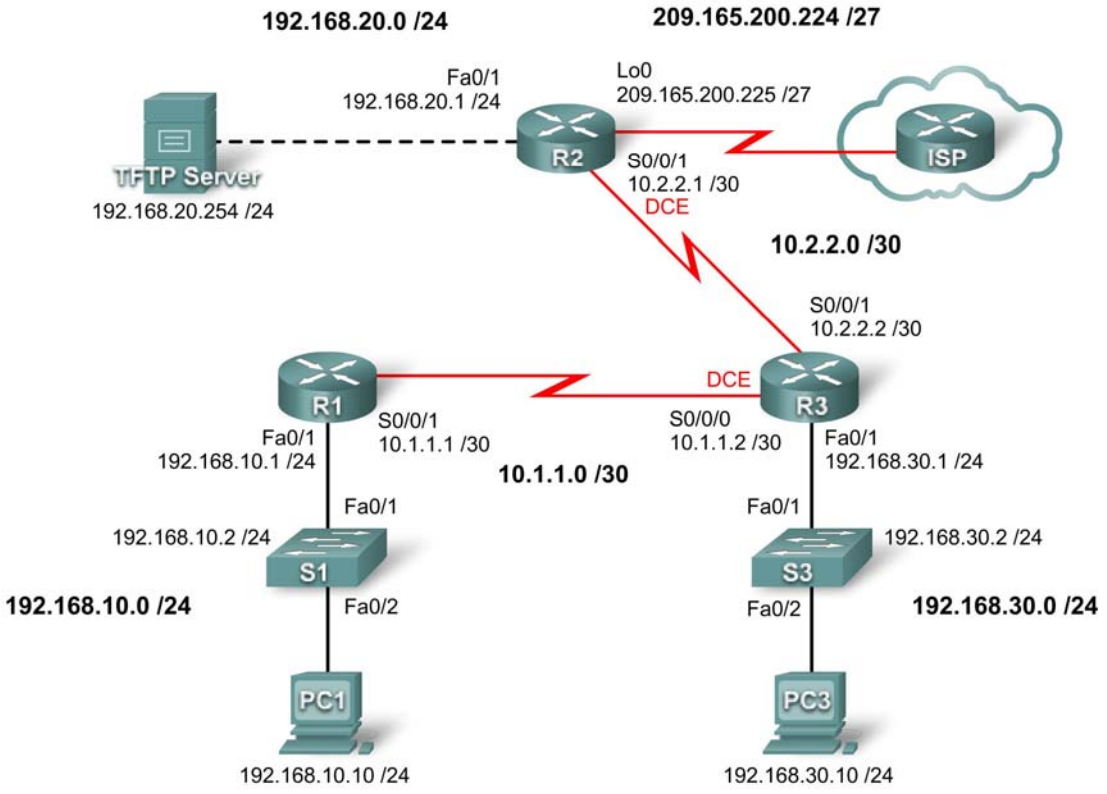
Lab 4.6.2: Challenge Security Configuration

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1	192.168.10.1	255.255.255.0	N/A
	S0/0/1	10.1.1.1	255.255.255.252	N/A
R2	Fa0/1	192.168.20.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
R3	Fa0/1	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
S1	VLAN10	192.168.10.2	255.255.255.0	N/A
S3	VLAN30	192.168.30.2	255.255.255.0	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
TFTP Server	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Perform basic configuration tasks on a router
- Configure and activate interfaces
- Configuring basic router security
- Disable unused Cisco services and interfaces
- Protect enterprise networks from basic external and internal attacks
- Understand and manage Cisco IOS configuration files and Cisco file system
- Set up and use Cisco SDM (Security Device Manager) to configure basic router security .

Scenario

In this lab, you will configure security using the network shown in the topology diagram. If you need assistance, refer to the Basic Security lab. However, try to do as much on your own as possible. For this lab, do not use password protection or login on any console lines because they might cause accidental logout. However, you should still secure the console line using other means. Use **ciscoccna** for all passwords in this lab.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configurations

Step 1: Configure routers.

Configure the R1, R2, and R3 routers according to the following guidelines:

- Configure the router hostname according to the topology diagram.
- Disable DNS lookup.
- Configure a message-of-the-day banner.
- Configure IP addresses on interfaces on R1, R2, and R3.
- Enable RIPv2 on all routers for all networks.
- Create a loopback interface on R2 to simulate the connection to the Internet.
- Create VLANs on switch S1 and S3 and configure the respective interfaces to participate in the VLANs
- Configure router R3 for SDM secure connectivity
- Install SDM on either PC3 or R3 if it is not installed already

Step 2: Configure Ethernet interfaces.

Configure the Ethernet interfaces of PC1, PC3, and TFTP Server with the IP addresses and default gateways from the addressing table at the beginning of the lab.

Step 3: Test the PC configuration by pinging the default gateway from each PC and the TFPT server.

Task 3: Secure Access to Routers

Step 1: Configure secure passwords and AAA authentication using a local database.

Create a secure password for router access. Create the username **ccna** to store locally on the router. Configure the router to use the local authentication database. Remember to use **ciscoccna** for all passwords in this lab.

Step 2: Secure the console the vty lines.

Configure the console and vty lines to block a user who enters an incorrect username and password five times within 2 minutes. Block additional login attempts for 2 minutes.

Step 3: Verify that connection attempts are denied after the failed attempt limit is reached.

Task 4: Secure Access to the Network

Step 1: Secure the RIP routing protocol.

Do not send RIP updates to non-network routers. Authenticate RIP updates and encrypt them.

Step 2: Verify that RIP routing still works.

Task 5: Logging Activity with SNMP (Simple Network Management Protocol)

Step 1: Configure SNMP logging to the syslog server at 192.168.10.250 on all devices.

Step 2: Log all messages with severity level 4 to the syslog server.

Task 6: Disabling Unused Cisco Network Services

Step 1: Disable unused interfaces on all devices.

Step 2: Disable unused global services on R1.

Step 3: Disable unused interface services on R1.

Step 4: Use AutoSecure to secure R2.

Remember to use **ciscoccna** for all passwords in this lab.

Task 7: Managing Cisco IOS and Configuration Files

Step 1: Identify where the running-config file is located in router memory.

Step 2: Transfer the running-config file from R1 to R2 using TFTP.

Step 3: Break R1 and recover it using ROMmon.

Copy and paste the following commands on R1, and then recover R1 using ROMmon.

```
line vty 0 4
 exec-timeout 0 20
line console 0
 exec-timeout 0 20
end
copy run start
exit
```

Step 4: Restore the saved configuration to R1 from R2 using TFTP.

Step 5: Erase the saved configuration from R2.

Task 8: Using SDM to Secure R3

Step 1: Connect to R2 using PC1.

Step 2: Navigate to the Security Audit feature.

Step 3: Perform a Security Audit.

Step 4: Choose settings to apply to the router.

Step 5: Commit the configuration to the router.

Task 9: Document the Router Configurations

On each router, issue the **show run** command and capture the configurations.

Task 10: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

