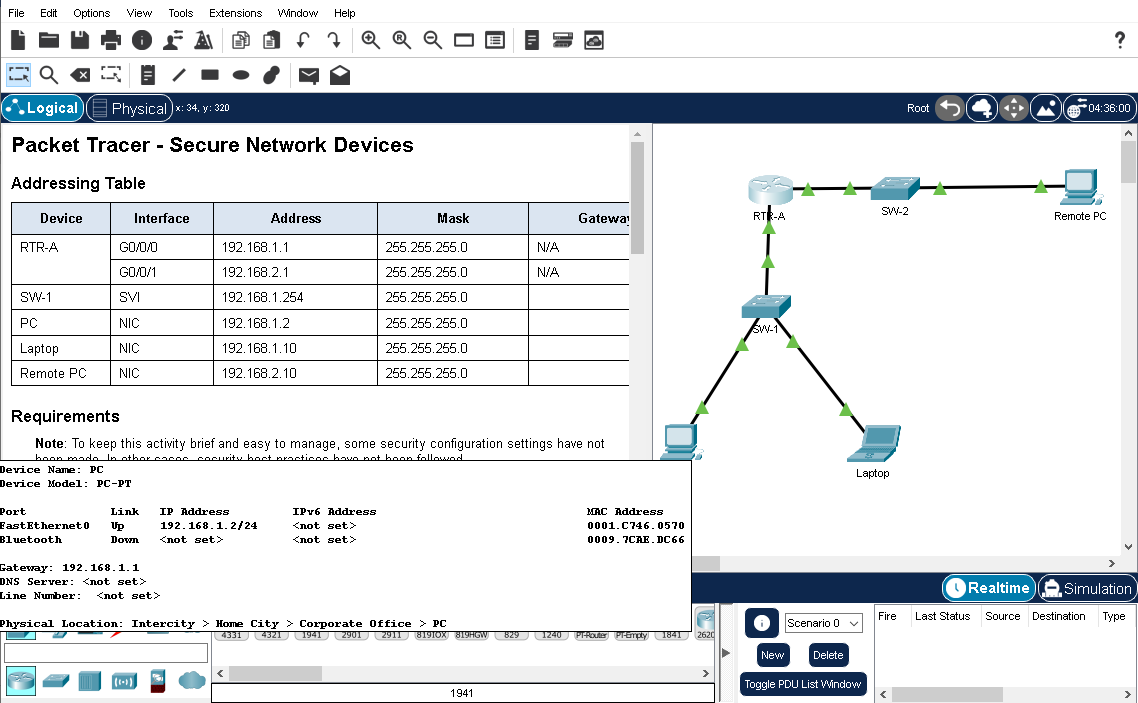
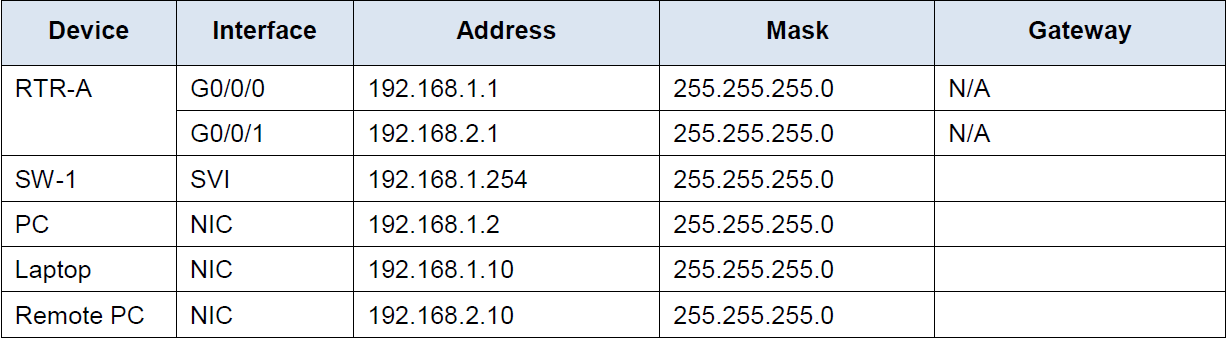
**Computer Networks**

**Problem-solving session: Secure Network Devices**



**Addressing Table**



**Background**

In this activity, you will configure a router and a switch based on a list of requirements.

**Note:** To keep this activity brief and easy to manage, some security configuration settings have not been made. In other cases, security best practices have not been followed.

**Step 1: Document the Network**

What is the gateway for the SW-1, PC, and Laptop?

\_\_\_\_\_\_\_\_\_N/A ,N/A, 192.168.1.1\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the gateway for the Remote PC?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_192.168.2.1\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Step 2: Router configuration requirements:**

* Prevent IOS from attempting to resolve mistyped commands to domain names.- no ip domain-lookup
* Hostnames that match the values in the addressing table.hostname RTR-A
* Require that newly created passwords be at least 10 characters in length.security password min-length 10
* A strong ten-character password for the console line. Use **@Cons1234!- line console 0, passoword @Cons1234!, login**
* Ensure that console and VTY sessions close after 7 minutes exactly.exec-timeout 7 ?, exit, line vty 0 15, exec-timeout 7
* A strong, encrypted ten-character password for the privileged EXEC mode. For this activity, it is permissible to use the same password as the console line.enable secret @Cons1234!
* A MOTD banner that warns about unauthorized access to the devices.RTR-A(config)#banner motd $Unathorized access is prohibited $
* Password encryption for all passwords.TR-A(config)#service password-encryption
* A username of **NETadmin** with encrypted password **LogAdmin!9**.R-A(config)#username NETadmin secret LogAdmin!9
* Enable SSH. Use **security.com** as the domain name. Use a modulus of **1024**.
* The VTY lines should use SSH for incoming connections.
* The VTY lines should use the username and password that were configured to authenticate logins.
* Impede brute force login attempts by using a command that blocks login attempts for 45 seconds if someone fails three attempts within 100 seconds.RTR-A(config)#login block-for 45 attempts 3 within 100

**Step 3: Switch configuration requirements:**

* All unused switch ports are administratively down.Switch(config)#interface range fastEthernet 0/1, fa0/3-9, fa0/11-24, g0/2

Switch(config-if-range)#shutdown

* The SW-1 default management interface should accept connections over the network. Use the information shown in the addressing table. The switch should be reachable from remote networks.Switch(config-if-range)#exit

Switch(config)#interface vlan 1

Switch(config-if)#ip address 192.168.1.254 255.255.255.0

Switch(config-if)#no shutdown

Switch(config-if)#

%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch(config-if)#exit

Switch(config)#ip default-gateway 192.168.1.1

* Use **@Cons1234!** as the password for the privileged EXEC mode.Switch(config)#enable secret @Cons1234!
* Configure SSH as was done for the router.
* Switch(config)#ip domain-name security.com

Switch(config)#crypto key generate rsa

Switch(config)#hostname SW-1

SW-1(config)#crypto key generate rsa

The name for the keys will be: SW-1.security.com

Choose the size of the key modulus in the range of 360 to 4096 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: 1024

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

SW-1(config)#line vty 0 15

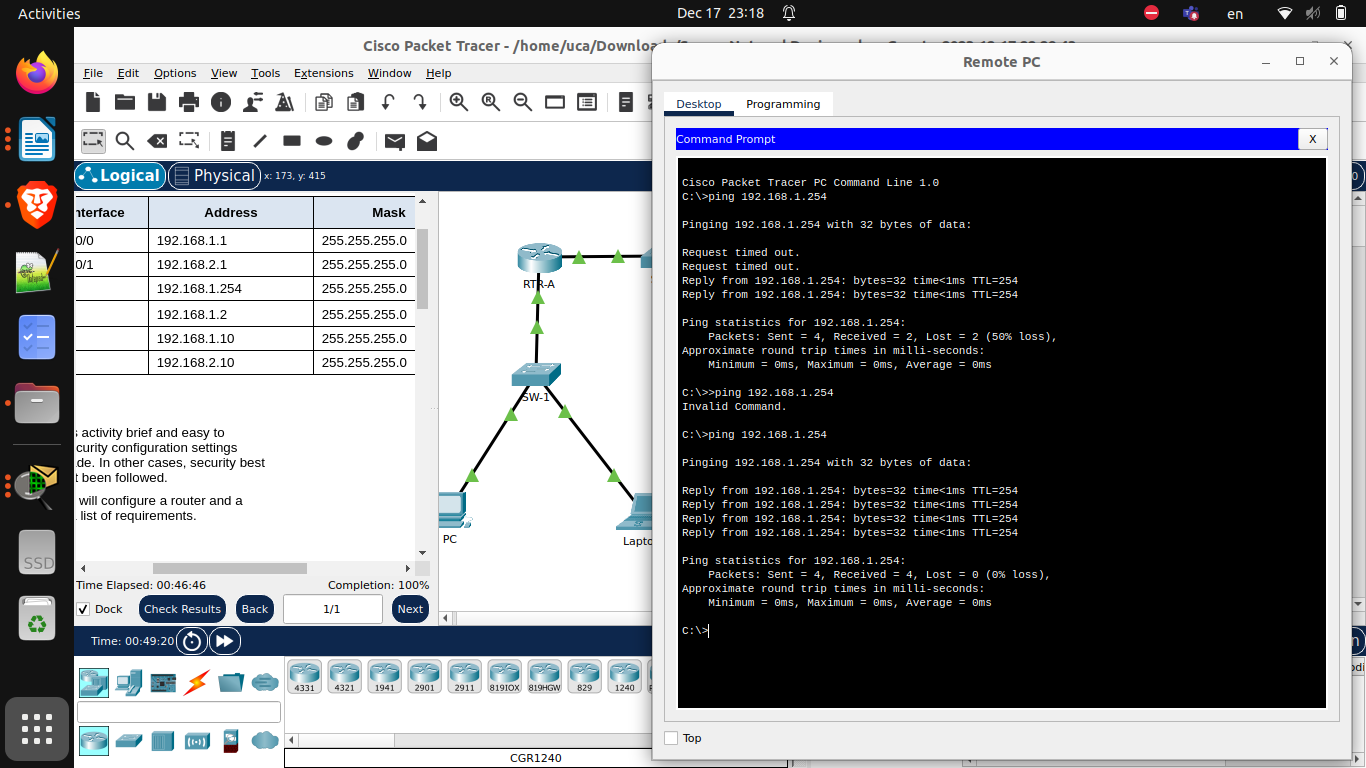
\*Mar 1 10:43:42.7: %SSH-5-ENABLED: SSH 1.99 has been enabled

SW-1(config-line)#transport input ssh

SW-1(config-line)#login local

exit

* Create a user name of **NETadmin** with encrypted secret password **LogAdmin!9, SW-1(config)#username NETadmin secret LogAdmin!9**
* The VTY lines should only accept connections over SSH.
* The VTY lines should only allow the network administrator account to access the switch management interface.
* Hosts on both LANs should be able to ping the switch management interface.



The completion must be 100%:

