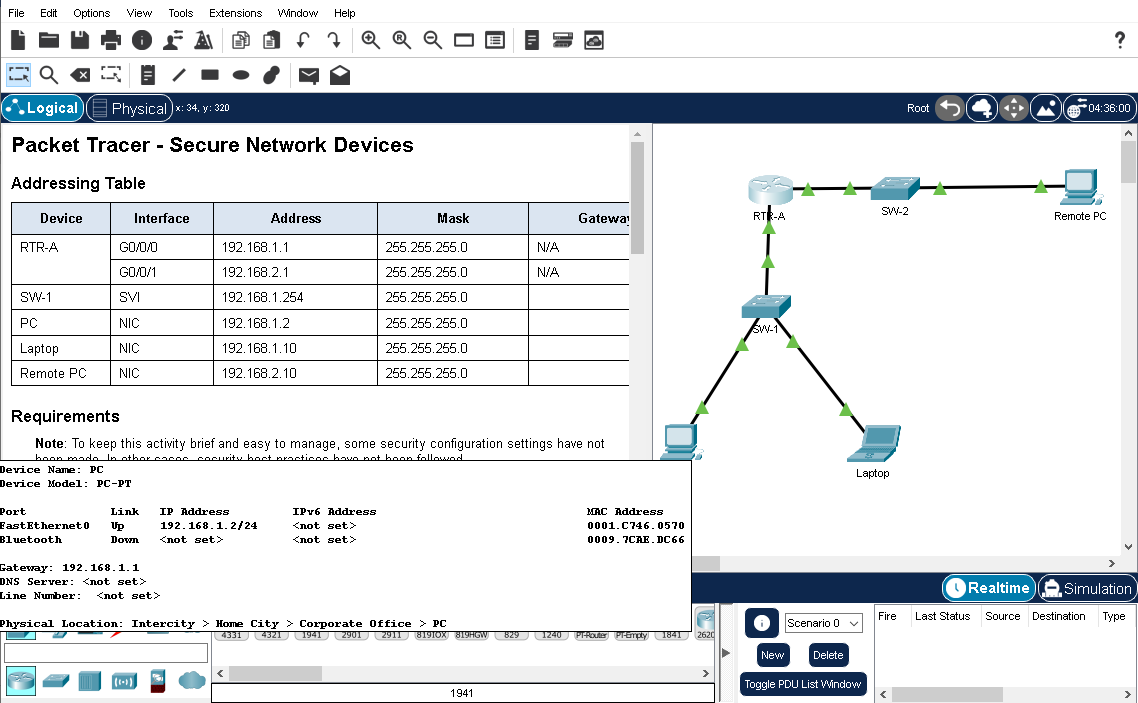
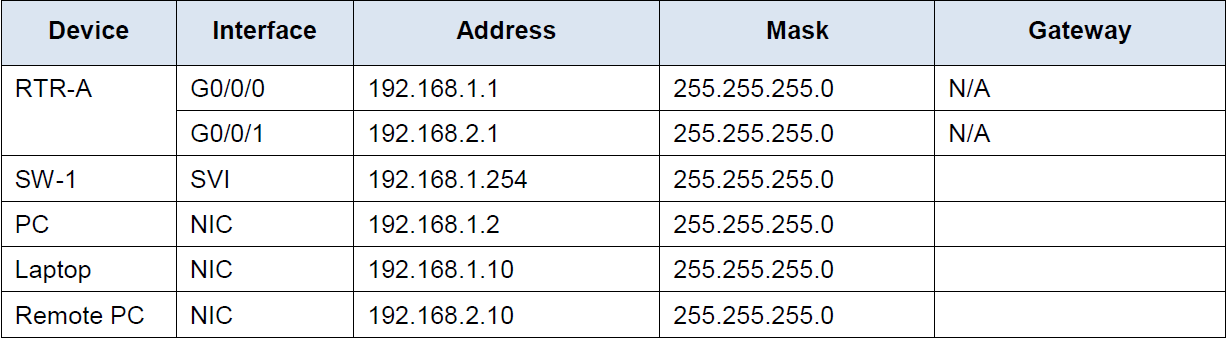
**Computer Networks**

**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?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the gateway for the Remote PC?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Step 2: Router configuration requirements:**

* Prevent IOS from attempting to resolve mistyped commands to domain names.
* Hostnames that match the values in the addressing table.
* Require that newly created passwords be at least 10 characters in length.
* A strong ten-character password for the console line. Use **@Cons1234!**
* Ensure that console and VTY sessions close after 7 minutes exactly.
* 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.
* A MOTD banner that warns about unauthorized access to the devices.
* Password encryption for all passwords.
* A username of **NETadmin** with encrypted password **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.

**Step 3: Switch configuration requirements:**

* All unused switch ports are administratively down.
* 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.
* Use **@Cons1234!** as the password for the privileged EXEC mode.
* Configure SSH as was done for the router.
* Create a user name of **NETadmin** with encrypted secret password **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%:

