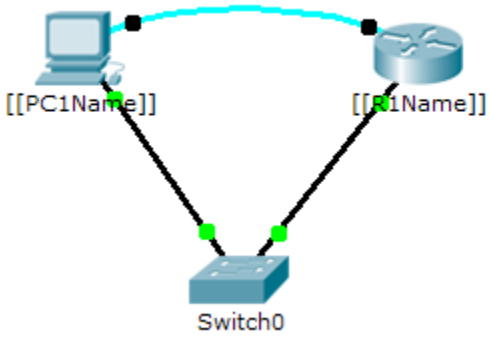
Packet Tracer – Configuring Secure Passwords and SSH

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
RTA	G0/0	10.10.10.1	255.255.255.0	N/A
PCA	NIC	10.10.10.2	255.255.255.0	10.10.10.1

Scenario

The network administrator has asked you to prepare RTA for deployment. Before it can be connected to the network, security measures must be enabled.

Requirements

- Configure IP addressing on PCA according to the Addressing Table.
- Console into RTA from the Terminal on PC-A.
- Configure IP addressing on RTA and enable the interface.
- Configure the hostname as RTA .
- Encrypt all plaintext passwords.

  RTA (config)# **service password-encryption**
- Set a strong secret password of your choosing.
- Set the domain name to RTA **.com** (case-sensitive for scoring in PT).

  RTA (config)# **ip domain-name [[R1Name]].com**
- Create a user of your choosing with a strong password.

  RTA (config)# **username *any_user* password *any_password***
- Generate 1024-bit RSA keys.

  Note: In Packet Tracer, enter the **crypto key generate rsa** command and press Enter to continue.

  RTA (config)# **crypto key generate rsa**

- Block anyone for three minutes who fails to log in after four attempts within a two-minute period.

  RTA (config)# **login block-for 180 attempts 4 within 120**

- Configure the VTY lines for SSH access and use the local user profiles for authentication.

  RTA (config)# **line vty 0 4**
  RTA (config-line)# **transport input ssh**
  RTA (config-line)# **login local**

- Save the configuration to NVRAM.
- Be prepared to demonstrate to your instructor that you have established SSH access from PCA to RTA .

Isomorph ID: 10