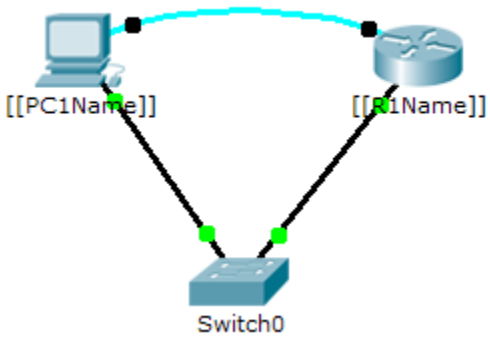
Packet Tracer – Configuring Secure Passwords and SSH (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
[[R1Name]]	G0/0	[[R1Add]]	255.255.255.0	N/A
[[PC1Name]]	NIC	[[PC1Add]]	255.255.255.0	[[R1Add]]

Scenario

The network administrator has asked you to prepare **[[R1Name]]** for deployment. Before it can be connected to the network, security measures must be enabled.

Requirements

- Configure IP addressing on **[[PC1Name]]** according to the Addressing Table.
- Console into **[[R1Name]]** from the Terminal on PC-A.
- Configure IP addressing on **[[R1Name]]** and enable the interface.
- Configure the hostname as **[[R1Name]]**.
- Encrypt all plaintext passwords.

  `[[R1Name]](config)#` **`service password-encryption`**
- Set a strong secret password of your choosing.
- Set the domain name to **[[R1Name]].com** (case-sensitive for scoring in PT).

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

  `[[R1Name]](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.

  `[[R1Name]](config)#` **`crypto key generate rsa`**

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

```
The name for the keys will be: [[R1Name]].[[R1Name]].com
Choose the size of the key modulus in the range of 360 to 2048 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]
```

- Block anyone for three minutes who fails to log in after four attempts within a two-minute period.
  `[[R1Name]](config)# **login block-for 180 attempts 4 within 120**`
- Configure the VTY lines for SSH access and use the local user profiles for authentication.
  `[[R1Name]](config)# **line vty 0 4**`
  `[[R1Name]](config-line)# **transport input ssh**`
  `[[R1Name]](config-line)# **login local**`
- Save the configuration to NVRAM.
- Be prepared to demonstrate to your instructor that you have established SSH access from **[[PC1Name]]** to **[[R1Name]]**.

Isomorph ID: [[indexNames]][[indexAdds]]

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.