CCNA 2 RSE Chapter 2 SIC Practice Skills Assessment – Packet Tracer Answers

ccnav6.com/ccna-2-rse-chapter-2-sic-practice-skills-assessment-packet-tracer-answers.html

CCNA Exam Answers 2017
CCNA 2 RSE Chapter 2 SIC Practice Skills Assessment – Packet Tracer Answers
4.75 (4) votes

CCNA Routing and Switching Routing and Switching Essentials

Routing and Switching Essentials Chapter 2 SIC Practice Skills Assessment – Packet Tracer

A few things to keep in mind while completing this activity:

1. Do not use the browser Back button or close or reload any exam windows during the exam.
2. Do not close Packet Tracer when you are done. It will close automatically.
3. Click the Submit Assessment button in the browser window to submit your work.

Introduction

In this practice skills assessment, you will configure **SW-1** with an initial configuration, SSH, and port security.

You are only required to configure **SW-1** in this assessment.

All IOS device configurations should be completed from a direct terminal connection to the device console.

It is possible that information that is required to complete the configurations has not been given to you. In that case, create the values that you need to complete the requirements. These values may include certain IP addresses, passwords, interface descriptions, banner text, and other values. You should always use the values that are provided in the instructions in any case.

You will practice and be assessed on the following skills:

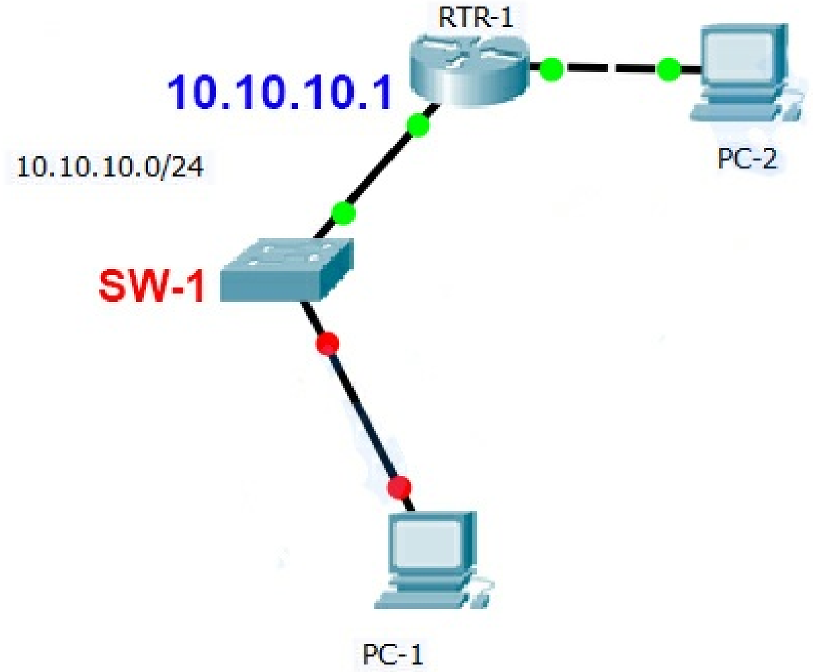
- Configuration of initial device settings
- Configuration of switch ports
- Configuration and addressing of the switch management interface (SVI)
- Configuration of the SSH protocol for remote switch access.
- Configuration of port security features.

Addressing Table

Device	Interface	IP Address	Subnet Mask
SW-1	VLAN 1	**10.10.10.100**	255.255.255.0
PC-1	NIC	10.10.10.10	255.255.255.0
PC-2	NIC	192.168.2.1	255.255.255.0

Scenario

The network administrator has asked you to configure a new switch. In this activity, you will use a list of requirements to configure the new switch with initial settings, SSH, and port security.



1. Configure SW-1 with the following initial settings:

- Configure the switch with the hostname value from the addressing table. Your configured value must match the value in the addressing table exactly.
- Configure a banner message-of-the-day.
- Enable access to the device console with the password **cisco**.
- Create an MD5 encrypted enable password of class.
- Encrypt all plain text passwords.
- Management SVI addressing
- Address the default management interface.
- The switch should be reachable over the network from **PC-1** and **PC-2**.

2. Configure SSH to secure remote access with the following settings:

- A domain name of **cisco.com**
- RSA key-pair parameters to support SSH version 2. Use a modulus of 1024.
- Set SSH to version 2.
- Create a user **admin** with password **ccna**.
- Configure vty lines to only accept SSH connections.
- Require the user created above to supply the user name and password in order to login over SSH.

3. Configure the port security feature to restrict network access:

- Disable all unused ports.
- Set all Fast Ethernet ports to access ports.
- Enable port security to allow only two hosts per port.
- Enable the MAC addresses of hosts that have connected to the switch ports to be recorded in the configuration file.
- Ensure that port violations disable ports.

Instruction

Can apply to all type (Type A, Type B, Type C, …). Please check HOSTNAME and IP on instruction

```
Switch(config)#hostname SW-1[CHECK HOSTNAME ON INSTRUCTIONS]
SW-1(config)#banner motd $This is Switch$
SW-1(config)#line console 0
SW-1(config-line)#password cisco
SW-1(config-line)#login
SW-1(config-line)#exit
SW-1(config)#enable secret class
SW-1(config)#service password-encryption
SW-1(config)#interface vlan1
SW-1(config-if)#ip address 10.10.10.100[check IP on Addressing Table] 255.255.255.0
SW-1(config-if)#ip default-gateway 10.10.10.1[check IP address of router port to
Switch]
SW-1(config-if)#no shutdown
SW-1(config-if)#exit
SW-1(config)#ip domain-name cisco.com
SW-1(config)#crypto key generate rsa
The name for the keys will be: SW-1.cisco.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]
SW-1(config)#ip ssh version 2
SW-1(config)#username admin secret ccna
SW-1(config)#line vty 0 15
SW-1(config-line)#login local
SW-1(config-line)#transport input ssh
SW-1(config-line)#exit
SW-1(config-if)#int fa0/1
SW-1(config-if)#no shutdown
SW-1(config)#int range fa0/2-24
SW-1(config-if-range)#shutdown
SW-1(config-if-range)#int g0/2
SW-1(config-if)#shutdown
SW-1(config)#int range fa0/1-24
SW-1(config-if-range)#switchport mode access
SW-1(config-if-range)#switchport port-security
SW-1(config-if-range)#switchport port-security mac-address sticky
SW-1(config-if-range)#switchport port-security maximum 2
SW-1(config-if-range)# switchport port-security violation shutdown
SW-1(config)#int range g0/1-2
SW-1(config-if-range)#switchport mode access
SW-1(config-if-range)#switchport port-security
SW-1(config-if-range)#switchport port-security mac-address sticky
SW-1(config-if-range)#switchport port-security maximum 2
SW-1(config-if-range)# switchport port-security violation shutdown
```

Prev Article