1.6 – ITN – Training - PacketKnows – Configuring Secure Passwords and SSH

Addressing Table

Device	Interface	Address	Subnet Mask	Default Gateway
RTA	Fa0/0	192.168.1.1	255.255.255.0	N/A
S1	Vlan 1	192.168.1.2	255.255.255.0	N/A

NOTE

- **Power all the devices first by clicking the triangle button on the upper navbar.**
- **Right click the device then click the web console first to configure on the device.**
- **Always type "save" when configuring IP addresses of PC's.**

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 **S1** according to the Addressing Table.
- Configure IP addressing on **RTA** and enable the interface.
- Configure the hostname as **RTA**.
- Encrypt all plaintext passwords.
- Configure SSH on RTA and Switch0

Configuration Guide: Setting Up IP Addressing, VLAN, Hostname, Password Encryption, and SSH

Part 1: Configuring RTA Router

Steps:

1. **Configure IP Addressing on RTA:**
    - Enter global configuration mode:

```
Router#configure terminal
```

- Change hostname of R1 to **RTA** and Access the FastEthernet interface and assign IP address and subnet mask:

```
Router(config)#Hostname RTA

Router(config)#interface FastEthernet0/0

Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

2. **Set Up Hostname and Password Encryption:**
    - Set hostname to RTA:

```
Router(config)#hostname RTA
```

- Encrypt passwords:

```
RTA(config)#service password-encryption

RTA(config)#enable secret cl@ss
```

3. **Generate RSA Keys and Configure SSH:**
    - Generate RSA keys (choose 1024 bits when prompted):

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

How many bits in the modulus [512]: 1024
```

- Configure SSH version 2 and set the domain name:

```
RTA(config)#ip ssh version 2
```

```
RTA(config)#ip domain-name RTA.com
```

- Create a local username and password for SSH login:

```
RTA(config)#username any_user password cisco
```

4. **Configure SSH Access:**
    - Set up login failure rate limiting:

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

- Access VTY lines, allow SSH access, and enable local login:

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

5. **Save Configuration and Exit:**
    - Save the configuration changes:

```
RTA#copy running-config startup-config
```

Part 2: Configuring S1

Steps:

1. **Configure VLAN and IP Addressing:**
    - Enter global configuration mode:

```
S1(config)#Configure Terminal
```

- Access VLAN 1 and assign IP address and subnet mask:

```
S1 (config)#interface Vlan1

S1 (config-if)#ip address 192.168.1.2 255.255.255.0
```

2. **Enable SSH and Set Up Local Login:**
    - Set the domain name:

```
Switch0 (config)#ip domain-name RTA.com
```

    - Create a local username and password for SSH login:

```
Switch0 (config)#username any_user password cisco
```

    - Generate RSA keys (choose 1024 bits when prompted):

```
S1 (config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
```

    - Configure SSH version 2:

```
S1 (config)#ip ssh version 2
```

    - Access VTY lines, allow SSH access, and enable local login:

```
S1 (config)#line vty 0 4
S1 (config-line)#transport input ssh
S1 (config-line)#login local
S1 (config-line)#end
```

3. **Save Configuration and Exit:**
    - Save the configuration changes:

```
S1#copy running-config startup-config
```

Note: Ensure that you are in the appropriate configuration mode before executing commands. Verify connectivity after the configurations to confirm proper setup.

Part 3: Verifying SSH Connection between RTA and S1

After configuring SSH on RTA and Switch0, it's important to verify that SSH connectivity is successfully established between the RTA router and S1 switch. Here's how you can do it:

Test SSH Connectivity:

- From RTA, attempt to SSH into S1 using the configured username and password:

RTA#ssh -l any_user192.168.1.2

password: cisco

Verify successful SSH login and access to S1.

S1>

```
Router#configure terminal
Router(config)#interface fa0/0
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#hostname RTA
RTA(config)#service password-encryption

RTA(config)#enable secret cl@ss
```

```
RTA(config)#ip domain-name RTA.com
RTA(config)#username any_user password cisco
RTA(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
RTA(config)#input ssh version 2

RTA(config)#login block-for 180 attempts 4 within 120
RTA(config)#line vty 0 4
RTA(config-line)#transport input ssh
RTA(config-line)#password cisco
RTA(config-line)#login local
RTA(config-line)#exit
RTA(config)#exit

RTA#copy running-config startup-config
```

```
Switch0#configure terminal
Switch0(config)# interface vlan1
Switch0(config-if)# ip address 192.168.1.2 255.255.255.0
Switch0(config-if)# no shutdown

Switch0 (config)#ip domain-name RTA.com
Switch0 (config)#username any_user password cisco
Switch0(config)#crypto key generate rsa
```

```
How many bits in the modulus [512]: 1024
Switch(config)# ip ssh version 2


Switch0(config)#line vty 0 4
Switch0(config-line)#transport input ssh
Switch0(config-line)#login local
Switch0(config-line)#end


Switch0#copy running-config startup-config
```