

## Packet Tracer - Configure Secure Passwords and SSH

### Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
RTA	G0/0/0	172.16.1.1	255.255.255.0	N/A
PCA	NIC	172.16.1.10	255.255.255.0	172.16.1.1
SW1	VLAN 1	172.16.1.2	255.255.255.0	172.16.1.1

### Scenario

The network administrator has asked you to prepare **RTA** and **SW1** for deployment. Before they can be connected to the network, security measures must be enabled.

### Instructions

#### Part 1: Configure Basic Security on the Router

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

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

- Set the minimum password length to 10.

```
RTA(config)# security passwords min-length 10
```

- Set a strong secret password of your choosing.

**Note:** Choose a password that you will remember, or you will need to reset the activity if you are locked out of the device.

- Disable DNS lookup.

```
RTA(config)# no ip domain-lookup
```

- Set the domain name to **netsec.com** (case-sensitive for scoring in PT).

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

- Create a user of your choosing with a strong encrypted password.

```
RTA(config)# username any_user secret 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
```

The name for the keys will be: **RTA.netsec.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**

- l. 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
```

- m. Configure all 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
```

- n. Set the EXEC mode timeout to 6 minutes on the VTY lines.

```
RTA(config-line)# exec-timeout 6
```

- o. Save the configuration to NVRAM.

- p. Access the command prompt on the desktop of **PCA** to establish an SSH connection to **RTA**.

```
C:\> ssh /?
Packet Tracer PC SSH
Usage: SSH -l username target
C:\>
```

## Part 2: Configure Basic Security on the Switch

Configure switch **SW1** with corresponding security measures. Refer to the configuration steps on the router if you need additional assistance.

- a. Console into **SW1** from the Terminal on PCA.
- b. Configure the hostname as **SW1**.
- c. Configure IP addressing on SW1 **VLAN1** and enable the interface.
- d. Configure the default gateway address.
- e. Disable all unused switch ports.

**Note:** On a switch it is a good security practice to disable unused ports. One method of doing this is to simply shut down each port with the '**shutdown**' command. This would require accessing each port individually. There is a shortcut method for making modifications to several ports at once by using the **interface range** command. On **SW1** all ports except FastEthernet0/1 and GigabitEthernet0/1 can be shutdown with the following command:

```
SW1(config)# interface range F0/2-24, G0/2
SW1(config-if-range)# shutdown
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
<Output omitted>
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
```

The command used the port range of 2-24 for the FastEthernet ports and then a single port range of GigabitEthernet0/2.

- f. Encrypt all plaintext passwords.

- g. Set a strong secret password of your choosing.
- h. Disable DNS lookup.
- i. Set the domain name to **netsec.com** (case-sensitive for scoring in PT).
- j. Create a user of your choosing with a strong encrypted password.
- k. Generate 1024-bit RSA keys.
- l. Configure all VTY lines for SSH access and use the local user profiles for authentication.
- m. Set the EXEC mode timeout to 6 minutes on all VTY lines.
- n. Save the configuration to NVRAM.

PCA

Physical
Config
Desktop
Programming
Attributes

Terminal

```

router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname RTA
RTA(config)#ip domain-lookup cisco.com
                        ^
% Invalid input detected at '^' marker.

RTA(config)#int g0/0/0
RTA(config-if)#ip address 172.16.1.1 255.255.255.0
RTA(config-if)#ip domain-lookup cisco.com
                        ^
% Invalid input detected at '^' marker.

RTA(config-if)#no ip domain-lookup
RTA(config)#ip domain-name netsec.com
RTA(config)#security password min-length 10
RTA(config)#service password -encryption
                        ^
% Invalid input detected at '^' marker.

RTA(config)#service password-encryption
RTA(config)#enable secret cisco_admin
RTA(config)#username admin secret cisco_admin
RTA(config)#crypto key generate rsa
The name for the keys will be: RTA.netsec.com
Choose the size of the key modulus in the range of 360 to 4096 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]

RTA(config)#ip ssh version 2
*Mar 1 15:10:33.447: %SSH-5-ENABLED: SSH 1.99 has been enabled
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)#login local
RTA(config-line)#exec-timeout 6
RTA(config-line)#end
RTA#
%SYS-5-CONFIG_I: Configured from console by console

RTA#write memory
Building configuration...

```

☐ Top

PCA

Physical Config **Desktop** Programming Attributes

**IP Configuration**

Interface

IP Configuration

☐ DHCP ☒ Static

IPv4 Address

Subnet Mask

Default Gateway

DNS Server

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address

Link Local Address

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication

Username

Password

☐ Top





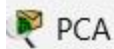
Physical Config **Desktop** Programming Attributes

## Terminal

```
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
SW1(config-if-range)#end
SW1#
%SYS-5-CONFIG_I: Configured from console by console

SW1#write memory
Building configuration...
[OK]
SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#line vty 0 15
SW1(config-line)#transport input ssh
SW1(config-line)#login local
SW1(config-line)#exec-timeout 6
SW1(config-line)#
```

☐ Top



Physical Config Desktop Programming Attributes

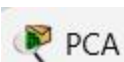
## Terminal

```
SW1(config)#ip ssh version 2
*Mar 1 13:17:30.988: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW1(config)#line vty 0 4
SW1(config-line)#transport input ssh
SW1(config-line)#login local
SW1(config-line)#exec-timeout 6
SW1(config-line)#! Disable unused ports
SW1(config-line)#interface range f0/2-24, g0/2
SW1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
```

☐ Top





Physical Config Desktop Programming Attributes

## Terminal

```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch>ena
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW1
Switch(config)#^
% Invalid input detected at '^' marker.

Switch(config)#hostname SW1
SW1(config)#no ip domain-lookup
SW1(config)#ip domain-name netsec.com
SW1(config)#security password min-length 10
SW1(config)#^
% Invalid input detected at '^' marker.

SW1(config)#service password-encryption
SW1(config)#security passwords min-length 10
SW1(config)#^
% Invalid input detected at '^' marker.

SW1(config)#enable secret cisco_admin
SW1(config)#username admin secret cisco_admin
SW1(config)#int vlan 1
SW1(config-if)#ip address 172.16.1.2 255.255.255.0
SW1(config-if)#no shutdown

SW1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

SW1(config-if)#ip default-gateway 172.16.1.1
SW1(config)#crypto key generate rsa
The name for the keys will be: SW1.netsec.com
Choose the size of the key modulus in the range of 360 to 4096 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]
```

☐ Top



PCA

Physical Config Desktop Programming Attributes

Terminal

```
RTA#  
  
RTA con0 is now available  
  
Press RETURN to get started.  
  
RTA>ena  
Password:  
RTA#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
RTA(config)#int g0/0/0  
RTA(config-if)#ip address 172.16.1.1 255.255.255.0  
RTA(config-if)#no shutdown  
  
RTA(config-if)#  
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up  
  
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up  
RTA(config-if)#
```

☐ Top

