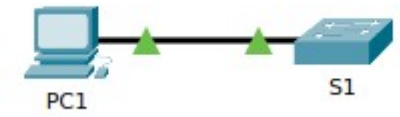
Packet Tracer - Configure SSH



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0

Part 1: Secure Passwords

a. On **PC1**, Telnet to **S1**. The user EXEC and privileged EXEC password is **cisco**.

```
C:\>telnet 10.10.10.2
Trying 10.10.10.2 ...Open


User Access Verification

Password:
S1>ena
S1>enable
Password:
S1#
```

b. Save the current configuration.

```
S1#wr
Building configuration...
[OK]
S1#
```

c. Show the current configuration and note that the passwords are in plain text.

```
S1#show running-config
Building configuration...

Current configuration : 1150 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
!
enable password cisco
!
```

d. In the global configuration mode, enter the command that encrypts plain text passwords:

S1(config)# service password-encryption

e. Verify that the passwords are encrypted.

```
S1#show running-config
Building configuration...

Current configuration : 1174 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!
!
enable password 7 0822455D0A16
!
```

Part 2: Encrypt Communications

Step 1: Set the IP domain name and generate secure keys.

a. Configure the domain name to be netacad.pka.

```
S1(config)#ip domain-name netacad.pka
```

b. Secure keys are needed to encrypt the data. Generate the RSA keys using a 1024 key length.

```
S1(config)#crypto key generate rsa
The name for the keys will be: S1.netacad.pka
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]
```

Step 2: Create an SSH user and reconfigure the VTY lines for SSH-only access.

a. Create an **administrator** user with **cisco** as the secret password.

```
S1(config)#username administrator password cisco
```

b. Configure the VTY lines to check the local username database for login credentials and to only allow SSH for remote access. Remove the existing vty line password.

```
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config-line)#no password cisco
```

Part 3: Verify SSH Implementation

a. Exit the Telnet session and attempt to log back in using Telnet. The attempt should fail.

```
C:\>telnet 10.10.10.2
Trying 10.10.10.2 ...Open

[Connection to 10.10.10.2 closed by foreign host]
C:\>
```

b. Attempt to log in using SSH

```
C:\>ssh -l administrator 10.10.10.2

Password:



S1>enable
Password:
S1#
```