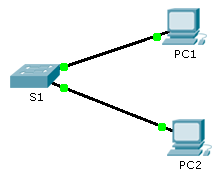
Packet Tracer - Skills Integration Challenge

.

1. Topology



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 |
| PC2 | NIC | 10.10.10.11 | 255.255.255.0 |

1. Scenario

The network administrator 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. Requirements

* Configure **S1** with the following initial settings:
  1. Hostname
  2. Banner that includes the word **warning**
  3. Console port login and password **cisco**
  4. Encrypted enable password of **class**
  5. Encrypt plain text passwords
  6. Management interface addressing
* Configure SSH to secure remote access with the following settings:
  1. Domain name of **cisco.com**
  2. RSA key-pair parameters to support SSH version 2
  3. Set SSH version 2
  4. User **admin** with secret password **ccna**
  5. VTY lines only accept SSH connections and use local login for authentication
* Configure the port security feature to restrict network access:
  1. Disable all unused ports.
  2. Set the interface mode to access.
  3. Enable port security to allow only two hosts per port.
  4. Record the MAC address in the running configuration.
  5. Ensure that port violations disable ports.

1. Script

enable

config t

service password-encryption

!

hostname S1

!

enable secret class

!

ip ssh version 2

ip domain-name cisco.com

!

username admin secret ccna

!

crypto key generate rsa

1024

interface range FastEthernet0/1 - 2

switchport mode access

switchport port-security

switchport port-security maximum 2

switchport port-security mac-address sticky

!

interface range FastEthernet0/3 - 24 , g1/1 - 2

shutdown

!

interface Vlan1

ip address 10.10.10.2 255.255.255.0

no shutdown

!

banner motd #Warning, unauthorized access is prohibited#

!

line con 0

password cisco

login

!

line vty 0 15

login local

transport input ssh

!

end