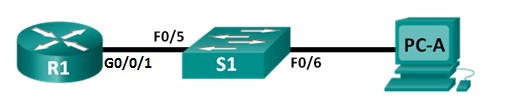
**Lab 5.2.2.9 – Configuring Switch Security Features**

## Topology



## Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| R1 | G0/0/1 | 172.16.99.1 | 255.255.255.0 | N/A |
| S1 | VLAN 99 | 172.16.99.11 | 255.255.255.0 | 172.16.99.1 |
| PC-A | NIC | 172.16.99.3 | 255.255.255.0 | 172.16.99.1 |

**Objectives**

#### Part 1: Set up the Topology and Initialize Devices

**Part 2: Configure Basic Device Settings and Verify Connectivity Part 3: Configure and Verify SSH Access on S1**

* Configure SSH access.
* Modify SSH parameters.
* Verify the SSH configuration.

## Background / Scenario

It is quite common to lock down access and install strong security features on PCs and servers. It is important that your network infrastructure devices, such as switches and routers, are also configured with security features.

In this lab, you will follow some best practices for configuring security features on LAN switches. You will only allow SSH and secure HTTPS sessions. You will also configure and verify port security to lock out any device with a MAC address not recognized by the switch.

# Part 1: Set Up the Topology and Initialize Devices

In Part 1, you will set up the network topology and clear any configurations if necessary.

### Step 1: Cable the network as shown in the topology. Step 2: Initialize and reload the router and switch.

If configuration files were previously saved on the router or switch, initialize and reload these devices back to their default configurations.

# Part 2: Configure Basic Device Settings and Verify Connectivity

In Part 2, you will configure basic settings on the router, switch, and PC. Refer to the Topology and Addressing Table at the beginning of this lab for device names and address information.

### Step 1: Configure an IP address on PC-A.

Refer to the Addressing Table for the IP Address information.

### Step 2: Configure basic settings on R1.

1. Console into R1 and enter global configuration mode.
2. Copy the following basic configuration and paste it to running-configuration on R1.

**no ip domain-lookup**

**hostname R1**

**service password-encryption**

**enable secret class**

**banner motd # Unauthorized access is strictly prohibited. #**

**line con 0**

**password cisco login**

**logging synchronous**

**line vty 0 4 password cisco login**

**interface G0/0/1**

**ip address 172.16.99.1 255.255.255.0**

**no shutdown**

**end**

**Step 3: Configure basic settings on S1.**

1. Console into S1 and enter global configuration mode.
2. Copy the following basic configuration and paste it to running-configuration on S1.

**no ip domain-lookup**

**hostname S1**

**service password-encryption**

**enable secret class**

**banner motd # Unauthorized access is strictly prohibited. #**

**line con 0**

**password cisco login**

**logging synchronous**

**line vty 0 15 password cisco login**

**exit**

1. Create VLAN 99 on the switch and name it **Management**.

S1(config)# **vlan 99**

S1(config-vlan)# **name Management**

S1(config-vlan)# **exit**

S1(config)#

1. Configure the VLAN 99 management interface IP address, as shown in the Addressing Table, and enable the interface.

S1(config)# **interface vlan 99**

S1(config-if)# **ip address 172.16.99.11 255.255.255.0**

S1(config-if)# **no shutdown**

S1(config-if)# **exit**

S1(config)#**ip default-gateway 172.16.99.1**

S1(config)#**end**

S1#

1. Issue the **show vlan** command on S1. What is the status of VLAN 99?
2. Issue the **show ip interface brief** command on S1. What is the status and protocol for management interface VLAN 99?

Why is the protocol down, even though you issued the **no shutdown** command for interface VLAN 99?

------------------------------------------------------------------------------------------------------------------------------------------

g. Assign ports F0/5 and F0/6 to VLAN 99 on the switch.

S1# **config t**

S1(config)# **interface f0/5**

S1(config-if)# **switchport mode access** S1(config-if)# **switchport access vlan 99** S1(config-if)# **interface f0/6**

S1(config-if)# **switchport mode access**

S1(config-if)# **switchport access vlan 99**

S1(config-if)# **end**

h. Issue the **show ip interface brief** command on S1. What is the status and protocol showing for interface VLAN 99?

**Note**: There may be a delay while the port states converge.

### Step 4: Verify connectivity between devices.

1. From PC-A, ping the default gateway address on R1 (172.16.99.1). Were your pings successful?
2. From PC-A, ping the management address of S1 (172.16.99.11). Were your pings successful?
3. From S1, ping the default gateway address on R1 (172.16.99.1). Were your pings successful?
4. From PC-A, open a web browser and go to [http://172.16.99.11.](http://172.16.99.11/) If you are prompted for a username and password, leave the username blank and use **class** for the password. If you are prompted for a secured connection, answer **No**. Were you able to access the web interface on S1?
5. Close the browser.

**Note**: The non-secure web interface (HTTP server) on a Cisco 2960 switch is enabled by default. A common security measure is to disable this service, as described in Part 4.

# Part 3: Configure and Verify SSH Access on S1

### Step 1: Configure SSH access on S1.

a. Enable SSH on S1. From global configuration mode, create a domain name of **CCNA-Lab.com**.

S1(config)# **ip domain-name CCNA-Lab.com**

b. Create a local user database entry for use when connecting to the switch via SSH. The user should have administrative level access.

**Note**: The password used here is NOT a strong password. It is merely being used for lab purposes.

S1(config)# **username admin privilege 15 secret sshadmin**

**Note**: A privilege level of 15 gives the user administrator rights.

The Cisco IOS software CLI has two levels of access to commands.

* User EXEC mode (privilege level 1) - Provides the lowest EXEC mode user privileges and allows only user-level commands available at the router> prompt.
* Privileged EXEC mode (privilege level 15) - Includes all enable-level commands at the router# prompt.

c. Configure the transport input for the vty lines to allow SSH connections only, and use the local database for authentication.

S1(config)# **line vty 0 15**

S1(config-line)# **transport input ssh**

S1(config-line)# **login local**

S1(config-line)# **exit**

d. Generate an RSA crypto key using a modulus of 1024 bits.

S1(config)# **crypto key generate rsa**

The name for the keys will be: S1.CCNA-Lab.com

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 3 seconds)

**NOTE: YOU MUST INSERT THE VALUE OF 1024**

S1(config)# S1(config)# **end**

1. Verify the SSH configuration.

S1# **show ip ssh**

What version of SSH is the switch using? How many authentication attempts does SSH allow?

What is the default timeout setting for SSH?

### Step 2: Modify the SSH configuration on S1.

Modify the default SSH configuration.

S1# **config t**

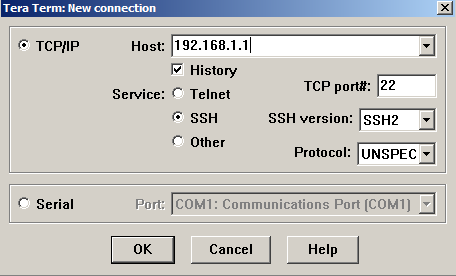
S1(config)# **ip ssh time-out 75**

S1(config)# **ip ssh authentication-retries 2**

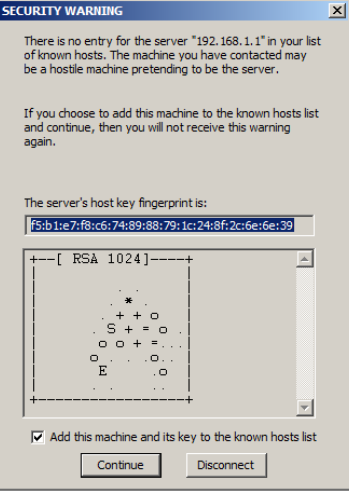
How many authentication attempts does SSH allow? What is the timeout setting for SSH? Verify the SSH configuration on S1.

a. Using the SSH client software on PC-A, open an SSH connection to S1. If you receive a message on your SSH client regarding the host key, accept it. Log in with **admin** for username and **sshadmin** for the password.

* 1. Establish an SSH connection to the router.
     1. Start **Teraterm** from PC-A.
     2. Establish an **SSH** session to **R1**.

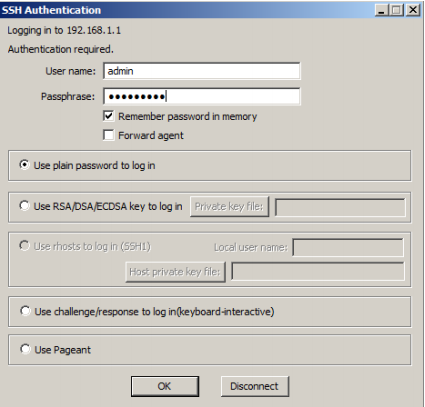


**172.16.99.11**



**NOTA:** La primera vez que establece una sesión de SSH con un dispositivo, se genera una **SECURITY WARNING** (ADVERTENCIA DE SEGURIDAD) para comunicarle que no se conectó a ese dispositivo anteriormente. Este mensaje es parte del proceso de autenticación. Lea la advertencia de seguridad y, luego, haga clic en **Continue** (Continuar).

1. Use the username admin and password adminpass. You should be able to establish an SSH session with R1.



|  |
| --- |
| Was the connection successful? What prompt was displayed on S1? Why? |
|  |
|  |

b. Type **exit** to end the SSH session on S1.

**Reflection**

1. Why would you enable port security on a switch?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. Why should unused ports on a switch be disabled?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_