**Lab – Configuring Switch Security Features**

# Topology



# Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device**  | **Interface**  | **IP Address**  | **Subnet Mask**  | **Default Gateway**  |
| R1  | G0/1  | 172.16.1.1  | 255.255.255.0  | N/A  |
| S1  | VLAN 1  | 172.16.1..11  | 255.255.255.0  | 172.16.1.1  |
| PC-A  | NIC  | 172.16.1.3  | 255.255.255.0  | 172.16.1.1  |

# 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.

**Part 4: Configure and Verify Security Features on S1**

* Configure and verify general security features.

# Background / Scenario

It is quite common to lock down access and install good 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.

**Note**: The router used with CCNA hands-on labs is a Cisco 1941 Integrated Services Router (ISR) with Cisco

IOS Release 15.2(4)M3 (universalk9 image). The switch used is a Cisco Catalyst 2960 with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

**Note**: Make sure that the router and switch have been erased and have no startup configurations. If you are unsure, contact your instructor or refer to the previous lab for the procedures to initialize and reload devices.

# Required Resources

* 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
* 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
* 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
* Console cables to configure the Cisco IOS devices via the console ports
* Ethernet cables as shown in the topology

# 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 basic configurations.

# Part 2: Configure Basic Device Settings and Verify Connectivity

In Part 2, you 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.**

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

1. Configure the device name.
2. Disable DNS lookup.
3. Configure interface IP address as shown in the Addressing Table.
4. Assign **class** as the privileged EXEC mode password.
5. Assign **cisco** as the console and vty password and enable login.
6. Encrypt plain text passwords.
7. Save the running configuration to startup configuration.

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

A good security practice is to assign the management IP address of the switch to a VLAN other than VLAN 1 (or any other data VLAN with end users). In this step, you will create VLAN 1 on the switch and assign it an IP address.

1. Configure the device name.
2. Disable DNS lookup.
3. Assign **class** as the privileged EXEC mode password.
4. Assign **cisco** as the console and vty password and then enable login.
5. Configure a default gateway for S1 using the IP address of R1.
6. Encrypt plain text passwords.
7. Save the running configuration to startup configuration.
8. Configure the VLAN 1 management interface IP address, as shown in the Addressing Table, and enable the interface.

S1(config)# **interface vlan 1**

S1(config-if)# **ip address 172.16.1.11 255.255.255.0**

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

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

S1#

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

Why is the protocol down, even though you issued the **no shutdown** command for interface VLAN 1?

1. ~~Assign ports F0/5 and F0/6 to VLAN 1 on the switch.~~

~~S1#~~ **~~config t~~**

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

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

~~S1(config-if)#~~ **~~switchport access vlan 1~~**

~~S1(config-if)#~~ **~~interface f0/6~~**

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

~~S1(config-if)#~~ **~~switchport access vlan 1~~**

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

1. Issue the **show ip interface brief** command on S1. What is the status and protocol showing for interface VLAN 1?

**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. Were your pings successful?
2. From PC-A, ping the management address of S1. Were your pings successful?
3. From S1, ping the default gateway address on R1. Were your pings successful?
4. From PC-A, open a web browser and go to http://172.16.1.11. If it prompts you for a username and password, leave the username blank and use **class** for the password. If it prompts for secured connection, answer **No**. Were you able to access the web interface on S1?
5. Close the browser session on PC-A.

**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.**

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

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

1. 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**

1. 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**

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

S1(config)# **crypto key generate rsa ~~modulus 1024~~**

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)

S1(config)#

S1(config)# **end**

1. Verify the SSH configuration and answer the questions below.

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?

**Step 3: Verify the SSH configuration on S1.**

1. Using SSH client software on PC-A (such as Tera Term), 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.

Was the connection successful?

What prompt was displayed on S1? Why?

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

# Part 4: Configure and Verify Security Features on S1

In Part 4, you will shut down unused ports, turn off certain services running on the switch, and configure port security based on MAC addresses. Switches can be subject to MAC address table overflow attacks, MAC spoofing attacks, and unauthorized connections to switch ports. You will configure port security to limit the number of MAC addresses that can be learned on a switch port and disable the port if that number is exceeded.

**Step 1: Configure general security features on S1.**

1. Configure a message of the day (MOTD) banner on S1 with an appropriate security warning message.
2. Issue a **show ip interface brief** command on S1. What physical ports are up?

1. Shut down all unused physical ports on the switch. Use the **interface range** command.

S1(config)# **interface range f0/1 – 4**

S1(config-if-range)# **shutdown**

S1(config-if-range)# **interface range f0/7 – 24**

S1(config-if-range)# **shutdown**

S1(config-if-range)# **interface range g0/1 – 2**

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

S1#

1. Issue the **show ip interface brief** command on S1. What is the status of ports F0/1 to F0/4?

**Step 2: MAC address table**

1. Record the R1 G0/1 MAC address. From the R1 CLI, use the **show interface g0/1** command and record the MAC address of the interface.

R1# **show interface g0/1**

GigabitEthernet0/1 is up, line protocol is up

 Hardware is CN Gigabit Ethernet, address is 30f7.0da3.1821 (bia 3047.0da3.1821)

What is the MAC address of the R1 G0/1 interface?

1. From the S1 CLI, issue a **show mac address-table** command from privileged EXEC mode. Find the dynamic entries for ports F0/5 and F0/6. Record them below.

F0/5 MAC address:

F0/6 MAC address:

## Reflection

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