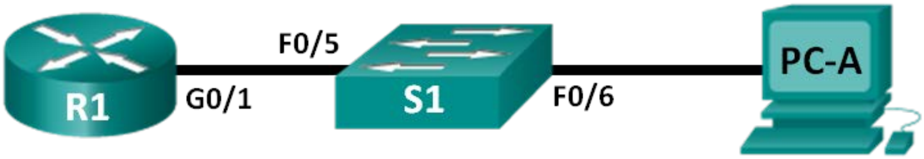
Lab – Configuring Switch Security Features

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	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.

Part 4: Configure and Verify Security Features on S1

- Configure and verify general security features.
- Configure and verify port security.

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.

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 this lab. 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.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

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)
- 1 Console cable to configure the Cisco IOS devices via the console ports
- 2 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 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.

a. Console into R1 and enter global configuration mode.

b. 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 g0/1
 ip address 172.16.99.1 255.255.255.0
 no shutdown
end
```

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

c. Save the running configuration to startup configuration.

Step 3: Configure basic settings on S1.

a. Console into S1 and enter global configuration mode.

b. 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
```

c. 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)#
```

d. 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)# end
S1#
```

e. Issue the **show vlan** command on S1. What is the status of VLAN 99? 99 Management active

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

up down

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

No physical ports on the switch have been assigned to 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
```

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

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

h. Save the running configuration to startup configuration.

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

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

Step 4: Verify connectivity between devices.

a. From PC-A, ping the default gateway address on R1. Were your pings successful? yes

b. From PC-A, ping the management address of S1. Were your pings successful? yes

c. From S1, ping the default gateway address on R1. Were your pings successful? yes

d. From PC-A, open a web browser and go to 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? yes

e. 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
```

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 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)
```

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

```
S1(config)#
S1(config)# end
```

e. 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? 3 by default

What is the timeout setting for SSH? 120   Verify the SSH configuration on S1.

a. Using the 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?   yes

   What prompt was displayed on S1? Why?

   Priviliged exec because privilege 15 was used

b. 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.

a. Change the message of the day (MOTD) banner on S1 to, “Unauthorized access is strictly prohibited. Violators will be prosecuted to the full extent of the law.”

b. Issue a **show ip interface brief** command on S1. What physical ports are up?

   f0/5 f0/6

c. 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
```

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

```
S1(config-if-range)# interface range g0/1 – 2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

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

administrativly down

e. Issue the **show ip http server status** command.

What is the HTTP server status?

What server port is it using?

What is the HTTP secure server status?

What secure server port is it using?

f. HTTP sessions send everything in plain text. You will disable the HTTP service running on S1.

```
S1(config)# no ip http server
```

g. From PC-A, open a web browser and go to http://172.16.99.11. What was your result?

nothing

h. From PC-A, open a web browser and go to https://172.16.99.11. Accept the certificate. Log in with no username and a password of **class**. What was your result?

packet tracer

i. Close the web browser.

Step 2: Configure and verify port security on S1.

a. 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?

0001.c933.b002

b. 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: 0001.c933.b002

F0/6 MAC address: 0001.c7b8.774d

c. Configure basic port security.

Note: This procedure would normally be performed on all access ports on the switch. F0/5 is shown here as an example.

1) From the S1 CLI, enter interface configuration mode for the port that connects to R1.

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

2) Shut down the port.

```
S1(config-if)# shutdown
```

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

3) Enable port security on F0/5.

```
S1(config-if)# switchport port-security
```

Note: Entering the **switchport port-security** command sets the maximum MAC addresses to 1 and the violation action to shutdown. The **switchport port-security maximum** and **switchport port-security violation** commands can be used to change the default behavior.

4) Configure a static entry for the MAC address of R1 G0/1 interface recorded in Step 2a.

```
S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx
```

(xxxx.xxxx.xxxx is the actual MAC address of the router G0/1 interface)

Note: Optionally, you can use the **`switchport port-security mac-address sticky`** command to add all the secure MAC addresses that are dynamically learned on a port (up to the maximum set) to the switch running configuration.

5) Enable the switch port.

```
S1(config-if)# no shutdown
S1(config-if)# end
```

d. Verify port security on S1 F0/5 by issuing a **show port-security interface** command.

```
S1# show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

What is the port status of F0/5?

Secure-up

e. From R1 command prompt, ping PC-A to verify connectivity.

```
R1# ping 172.16.99.3
```

f. You will now violate security by changing the MAC address on the router interface. Enter interface configuration mode for G0/1 and shut it down.

```
R1# config t
R1(config)# interface g0/1
R1(config-if)# shutdown
```

g. Configure a new MAC address for the interface, using **aaaa.bbbb.cccc** as the address.

```
R1(config-if)# mac-address aaaa.bbbb.cccc
```

h. If possible, have a console connection open on S1 at the same time that you do the next two steps. You will eventually see messages displayed on the console connection to S1 indicating a security violation. Enable the G0/1 interface on R1.

```
R1(config-if)# no shutdown
```

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

i. From R1 privileged EXEC mode, ping PC-A. Was the ping successful? Why or why not?

no port security disables my attempt and shutdown on the port

j. On the switch, verify port security with the following commands.

```
S1# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
--------------------------------------------------------------------
      Fa0/5            1           1                 1         Shutdown
----------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :0
Max Addresses limit in System (excluding one mac per port) :8192

S1# show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : aaaa.bbbb.cccc:99
Security Violation Count   : 1

S1# show interface f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
<output omitted>

S1# show port-security address
                Secure Mac Address Table
------------------------------------------------------------------------
Vlan     Mac Address       Type                 Ports      Remaining Age
                                                           (mins)
----     -----------       ----                 -----   -------------
  99     30f7.0da3.1821    SecureConfigured     Fa0/5        -
-----------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :0
Max Addresses limit in System (excluding one mac per port) :8192
```

k. On the router, shut down the G0/1 interface, remove the hard-coded MAC address from the router, and re-enable the G0/1 interface.

```
R1(config-if)# shutdown
R1(config-if)# no mac-address aaaa.bbbb.cccc
```

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

```
R1(config-if)# no shutdown
R1(config-if)# end
```

l. From R1, ping PC-A again at 172.16.99.3. Was the ping successful?

m. On the switch, issue the **show interface f0/5** command to determine the cause of ping failure. Record your findings.

F0/5 port on S1 is still in an error disabled state

n. Clear the S1 F0/5 error disabled status.

```
S1# config t
S1(config)# interface f0/5
S1(config-if)# shutdown
S1(config-if)# no shutdown
```

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

o. Issue the **show interface f0/5** command on S1 to verify F0/5 is no longer in error disabled mode.

```
S1# show interface f0/5
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

p. From the R1 command prompt, ping PC-A again. The ping should be successful.

Reflection

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

it prevents physically attaching a cable to your switch. security

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

same reason

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Router Interface Summary Table

<table>
<tr><th colspan="5">Router Interface Summary</th></tr>
<tr><th>Router Model</th><th>Ethernet Interface #1</th><th>Ethernet Interface #2</th><th>Serial Interface #1</th><th>Serial Interface #2</th></tr>
<tr><td>1800</td><td>Fast Ethernet 0/0 (F0/0)</td><td>Fast Ethernet 0/1 (F0/1)</td><td>Serial 0/0/0 (S0/0/0)</td><td>Serial 0/0/1 (S0/0/1)</td></tr>
<tr><td>1900</td><td>Gigabit Ethernet 0/0 (G0/0)</td><td>Gigabit Ethernet 0/1 (G0/1)</td><td>Serial 0/0/0 (S0/0/0)</td><td>Serial 0/0/1 (S0/0/1)</td></tr>
<tr><td>2801</td><td>Fast Ethernet 0/0 (F0/0)</td><td>Fast Ethernet 0/1 (F0/1)</td><td>Serial 0/1/0 (S0/1/0)</td><td>Serial 0/1/1 (S0/1/1)</td></tr>
<tr><td>2811</td><td>Fast Ethernet 0/0 (F0/0)</td><td>Fast Ethernet 0/1 (F0/1)</td><td>Serial 0/0/0 (S0/0/0)</td><td>Serial 0/0/1 (S0/0/1)</td></tr>
<tr><td>2900</td><td>Gigabit Ethernet 0/0 (G0/0)</td><td>Gigabit Ethernet 0/1 (G0/1)</td><td>Serial 0/0/0 (S0/0/0)</td><td>Serial 0/0/1 (S0/0/1)</td></tr>
<tr><td colspan="5"><b>Note</b>: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.</td></tr>
</table>