Lab 3 – Implement Port Security

Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	172.16.10.1	255.255.255.0
S2	VLAN 1	172.16.10.2	255.255.255.0
PC-A	NIC	172.16.10.10	255.255.255.0
PC-B	NIC	172.16.10.11	255.255.255.0
Web Server	NIC	172.16.10.100	255.255.255.0
Rouge Endpoint	NIC	172.16.10.12	255.255.255.0

Part 1: Configure Basic Device Settings for Switches and Endpoints

1. Configure device names for switches S1 and S2.

2. Configure the IP address listed in the Addressing Table for S1 and S2.

3. Configure the IP addresses for the endpoints PC-A, PC-B and the Web Server. No need to configure the Rouge Endpoint as it has already been configured.

4. Test ping connectivity between S1, S2, PC-A, PC-B and the Web Server. All these devices should be able to ping each other. If not, please troubleshoot before continuing with the lab.

Part 2: Configure Access Control on Switches

Managing administrative device access is crucial. Many types of authentication can be performed on networking devices, and each method offers varying levels of security. In this part of the lab you will implement two methods of access control – local password (on S1) and local database (on S2).

1. Restrict console access on **S1** by configuring a password of **ciscolab3** on the console line.

2. Encrypt all plain text passwords on **S1**.

3. On **S2**, create a username of **admin1** with a secret password of **lab3cisco**.

   See slide 13 of last lecture (lecture 4) if you cannot remember how to create a username entry on a device.

4. Configure the console line on **S2** to use the local database for authentication using the **login local** command in line configuration mode.

5. Verify the configured access control on both switches. S1 should just ask for a password and S2 should ask for a username and password combination. If not, please troubleshoot before continuing with the lab.

QUESTION 1: What is the advantage of the username-password approach over just a password?

Before proceeding, go to the "Lab 3 - Implement Port Security – QUESTIONS 2024" quiz on the Brightspace page and enter your answer for question 1. Leave the quiz open while you complete the rest of the lab sheet.

Part 3: Secure Unused Ports

A simple method that many admins use to help secure the network from unauthorised access is to disable all unused ports on a switch. In this part of the lab you will disable all ports currently not in use on S1 & S2.

1. S1 has 24 Fast Ethernet ports (F0/1 – F0/24) and 2 Gigabit Ethernet ports (G0/1 & G0/2). Currently, only ports F0/1, F0/2 and G0/1 are in use. Disable all unused ports on **S1**. The **interface range** command can be used to apply this configuration to multiple ports simultaneously.

2. S2 also has 24 Fast Ethernet ports (F0/1 – F0/24) and 2 Gigabit Ethernet ports (G0/1 & G0/2). Currently, only ports F0/1 and G0/1 are in use. Disable all unused ports on **S2**. The **interface range** command can again be used to apply this configuration to multiple ports simultaneously.

3. Verify all unused ports have been shutdown on each switch by issuing the **show ip interface brief** command. If any unused ports are still not showing as administratively down troubleshoot as needed.

4. Attach the Rogue Endpoint to port F0/3 on S1 (use a straight-through cable). Try to ping from the Rouge Endpoint to any device on the network.

QUESTION 2: What colour is the link light on the port that the Rouge Endpoint is connected to?
Note: if no link lights are visable on any of the switches, go to Options->Preferences and make sure the "Show Link Lights" checkbox is ticked.
QUESTION 3: Were the Rouge Endpoint pings to other devices successful?

Before proceeding, return to the "Lab 3 - Implement Port Security – QUESTIONS 2024" quiz and enter your answers for questions 2 & 3. Leave the quiz open while you complete the rest of the lab sheet.

Part 4: Configure Port Security

Port security allows admin to statically specify MAC addresses for a port or permit switch to dynamically learn a limited number of MAC addresses. In this part of the lab, you will configure port security on S1 & S2.

1. Enable port security on **S1** for Fast Ethernet ports 0/1 and 0/2.

```
S1(config)# interface range f0/1 – 2
S1(config-if-range)# switchport port-security
```

QUESTION 4: Was the above command successful?

Before proceeding, return to the "Lab 3 - Implement Port Security – QUESTIONS 2024" quiz and enter your answers for question 4. Leave the quiz open while you complete the rest of the lab sheet.

2. Configure the ports (Fast Ethernet ports 0/1 and 0/2 on S1) as access ports and attempt to enable port security on them again.
   See slide 30 of last lecture (lecture 4) if you cannot remember how to set a port as an access port.

3. Verify the port security default settings by issuing the **show port-security interface F0/1** command on S1.

QUESTION 5: What is the current violation mode?
QUESTION 6: What is the current maximum MAC addresses?
QUESTION 7: What is the current total MAC addresses?
Before proceeding, return to the "Lab 3 - Implement Port Security – QUESTIONS 2024" quiz and enter your answers for questions 5, 6 & 7. Leave the quiz open while you complete the rest of the lab sheet.

4. Configure the ports so that the MAC address of a device is dynamically learned and added to the running configuration.

```
S1(config)# interface range f0/1 – 2
S1(config-if-range)# switchport port-security mac-address sticky
```

5. Ping from PC-A to PC-B and then re-issue the **show port-security interface F0/1** command on S1.

QUESTION 8: Has the total MAC addresses value changed (and if so why)?
Before proceeding, return to the "Lab 3 - Implement Port Security – QUESTIONS 2024" quiz and enter your answers for question 8. Leave the quiz open while you complete the rest of the lab sheet.

6. Disconnect PC-A and connect the Rogue Endpoint to F0/1 on S1 (which is the port to which PC-A was originally connected). Verify that the Rogue Endpoint is unable to ping PC-B. Re-issue the **show port-security interface F0/1** command one final time on S1.

QUESTION 9: What is the current port status?
QUESTION 10: What is the current violation count?
Before proceeding, return to the "Lab 3 - Implement Port Security – QUESTIONS 2024" quiz and enter your answers for questions 9 & 10. Leave the quiz open while you complete the rest of the lab sheet.

7. Enable port security on port G0/1 on **S2**.

8. Port security has 3 possible violation modes.

Mode	Description
shutdown (default)	The port transitions to the error-disabled state immediately, turns off the port LED, and sends a syslog message. It increments the violation counter. When a secure port is in the error-disabled state, an administrator must re-enable it by entering the **shutdown** and **no shutdown** commands.

Mode	Description
`restrict`	The port drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the maximum value. This mode causes the Security Violation counter to increment and generates a syslog message.
`protect`	This is the least secure of the security violation modes. The port drops packets with unknown MAC source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the maximum value. No syslog message is sent.

In some situations we may want to use port security to block traffic from unknown addresses but still stay active for known addresses.

Set the violation mode on G0/1 on S2 so it is not disabled when a violation occurs, but a notification of the security violation is generated and packets from the unknown source are dropped.

```
S2(config-if)# switchport port-security violation restrict
```

If you have correctly configured all parts of the lab your activity score should now be showing as 100%. If so, click on “check results” in the activity window. Return to the Brightspace quiz one last time and enter the code into the appropriate question box (Q11) of the quiz.

You have completed the lab – please submit the Brightspace quiz.