Name _____ Date _____

# Module 11 - Switch Security Configuration

## Switching, Routing, and Wireless Essentials – Semester 2

## Student Version

**Module 11 Sections:**

11.0 Introduction
11.1 Implement Port Security
11.2 Mitigate VLAN Attacks
11.3 Mitigate DHCP Attacks
11.4 Mitigate ARP Attacks
11.5 Mitigate STP Attacks
11.6 Module Practice and Quiz

**Required Materials:**

Reading Organizer

Packet Tracer Activities: 11.1.10 - Implement Port Security
11.6.1 - Switch Security Configuration

Labs: 11.6.2 - Switch Security Configuration

Module's 10- 13 Exam

Page intentionally left blank.

| Points_____ / ___97___ |
|---|

Name_____ Date _____

# Module 11 - Switch Security Configuration
# Reading Organizer
## Student Version

**Note**: The Reading Organizer has weighted scoring. Any question with the word **explain**, **define, or describe** in it is expected to have a longer answer and is worth two points each.

**After completion of this module, you should be able to:**

- Implement port security to mitigate MAC address table attacks.
- Explain how to configure DTP and native VLAN to mitigate VLAN attacks.
- Explain how to configure DHCP snooping to mitigate DHCP attacks.
- Explain how to configure ARP inspection to mitigate ARP attacks.
- Explain how to configure PortFast and BPDU Guard to mitigate STP attacks.

### 11.1 Implement Port Security

1. _____ devices are considered to be the weakest link in a company's security infrastructure.

2. What is a simple method that many administrators use to help secure the network from unauthorized access?

3. What command can you  use to configure a range of port?

4. Explain in detail how enabling port security on a switch prevents MAC address table overflow attacks.

5. Fill in the correct commands to enable port security on interface f0/1.

```
S1(config)# interface f0/1
S1(config-if)# _____
S1(config-if)# _____
S1(config-if)# end
S1#
```

6. What command can you use to display current port security settings?

7. What command do you use to set the maximum number of MAC addresses allowed on a port to 5?

8. List and describe the three ways a switch can be configured to learn about MAC addresses on a secure port.

a. _____ –

b. _____ –

c. _____ –

9. Describe what port security aging does.

10. List and describe the two types of aging that are supported per port.

a. _____ –

b. _____ –

11. Use the _____ command to enable or disable static aging for the secure port, or to set the aging time or type.

12. List and describe the parameters that can be used with the aging command.

a. _____ –

b. _____ –

c. _____ –

d. _____ –

13. If port security is set up on a switch and the MAC address of a device attached to the port differs from the list of secure addresses, then a port violation occurs. By default, what happens to the port?

14. List and describe the security violation modes.

a. _____ –

b. _____ –

c. _____ –

15. What happens when a port is shutdown and placed in the error-disabled state?

16. When the port protocol and link status are changed to down what happens to the port LED?

17. What is the correct procedure to re-enable a port that has been shutdown?

18. How can you verify that MAC addresses are “sticking” to the configuration?

19. How can you display all secure MAC addresses that are manually configured or dynamically learned on all switch interfaces?

## 11.2 Mitigate VLAN Attacks

20. Explain the three ways a VLAN hopping attack can be launched.

a.

b.

c.

21. Describe the steps to mitigate VLAN hopping attacks.

Step 1

Step 2

Step 3

Step 4

Step 5

## 11.3 Mitigate DHCP Attacks

22. What is the goal of a DHCP starvation attack?

23. How can DHCP spoofing attacks can be mitigated?

24. Explain in detail how DHCP snooping works.

25. Describe the steps to enable DHCP snooping.

Step 1

Step 2

Step 3

Step 4

26. Use the show _____ privileged EXEC command to verify DHCP snooping and _____ to view the clients that have received DHCP information

## 11.4 Mitigate ARP Attacks

27. Explain what happens in a typical ARP attack.

28. Describe the ways dynamic ARP inspection (DAI) helps prevent ARP attacks.

a.

b.

c.

d.

e.

29. List the DAI guidelines should you follow to mitigate the chances of ARP spoofing and ARP poisoning.

a.

b.

c.

d.

30. It is generally advisable to configure all access switch ports as _____ and to configure all uplink ports that are connected to other switches as _____.

31. What does the ***ip arp inspection validate {[src-mac] [dst-mac] [ip]***} global configuration command do?

## 11.5 Mitigate STP Attacks

32. List and describe the two methods that can be used to mitigate Spanning Tree Protocol (STP) manipulation attacks.

a. _____ –

b. _____ –

33. PortFast bypasses the STP _____ and _____ states to minimize the time that access ports must wait for STP to converge.

34. What command is used to enable PortFast on an interface?

35. If any BPDUs are received on a BPDU Guard enabled port, that port is put into error-disabled state. This means the port is shut down and must be manually re-enabled or automatically recovered through the _____global command.

36. BPDU Guard can be enabled on a port by using the _____ interface configuration command.

37. To display information about the state of spanning tree, use the _____ command.