1. What is the command to enable port security on an access port?

a. enable port-security
b. switchport mode trunk
c. switchport port-security
d. port-security enable

Explanation: To enable port security on a switch port, you use the command switchport port-security in interface configuration mode. The commands enable port-security and port-security enable are not valid Cisco IOS commands. While switchport mode trunk is a valid command, it configures a port as a trunk port rather than enabling security.

2. What does the command "switchport port-security mac-address sticky" do?

a. Clears MAC Address tables.
b. Convers dynamic MAC to static
c. Makes learned MAC addresses saved in running-configuration
d. Adds MAC to NVRAM

Explanation: The "sticky" feature causes dynamically learned MAC addresses to be added to the running configuration as if they were statically configured. This means they persist across link flaps (port going down and up) as long as the switch is running. If you save the configuration, these MAC addresses will also persist across reboots.

3. Which setting allows a port to learn MAC addresses dynamically *and* retain them after a reboot if saved?

a. Sticky
b. Dynamic
c. Manual
d. Absolute

Explanation: The sticky option allows the port to dynamically learn MAC addresses and also adds them to the running configuration. If you save the configuration (with write memory or copy running-config startup-config), these learned MAC addresses will be retained after a reboot.

Saving the running configuration will commit the dynamically learned MAC address to NVRAM allowing them to persist across reboots.

4. A student connects their laptop and the port shuts down immediately. What is the likely cause?

a. The port was configured for trunk
b. DHCP is disabled
c. Port security violation occurred
d. The port's MTU was exceeded

Explanation: When port security is configured and a violation occurs (such as an unauthorized MAC address connecting to the port), the default behavior is to put the port in an error-disabled state, effectively shutting it down. This is commonly seen when a student connects a device with a MAC address that's not allowed on that port.

5. You run show port-security interface f0/2 and see "Port Status: Secure-down". What does this mean?

a. Port is secured and active

b. Port has a security violation
c. Port has security but no active device
d. Port has aged out all MACs

Explanation: "Secure-down" status indicates that the port has been shut down due to a security violation. This happens when the default violation mode (shutdown) is in effect and an unauthorized MAC address attempts to connect to the port.

6. By default, how many MAC addresses are allowed per port when port security is enabled?

a. 0
b. 1
c. 5
d. Unlimited

Explanation: When port security is first enabled on a port, the default maximum number of MAC addresses allowed is 1. This means only a single device can connect to that port unless the maximum is explicitly increased.

7. What does the following command set do?

```
switchport port-security aging time 10
switchport port-security aging type inactivity
switchport port-security aging static
```

a. Clears MACs every 10 mins
b. Enables dynamic sticky aging
c. Removes static MACs if inactive for 10 mins
d. Prevents aged MACs from being used again

Explanation: This combination of commands configures MAC address aging so that:

- The aging time is 10 minutes
- Aging is based on inactivity (not absolute time)
- Static MAC addresses are also subject to aging

Together, these remove MAC addresses (including static ones) from the port security table if they're inactive for 10 minutes.

8. Which violation mode shuts down the port completely and sends a syslog message?

a. Restrict
b. Protect
c. Shutdown
d. Passive

Explanation: The "shutdown" violation mode is the most severe - it error-disables the port (shutting it down completely), sends a SNMP trap notification, and generates a syslog message. This is the default violation mode for port security.

9. You want to ensure a lab port allows up to 3 specific MAC addresses and stores them persistently. What config is correct?

a. Set port security enabled on the switchport and set it to dynamic.
b. Set port security enabled on the switchport and manually configure MAC addresses.
c. Set port security enabled on the switchport and set it to dynamic sticky.
d. Set port security enabled.

Explanation: To allow 3 specific MAC addresses that are stored persistently, you would enable port security, set the maximum to 3, and enable sticky learning. This way, the first 3 MAC addresses that connect will be learned and stored in the running configuration, and can be saved to startup for persistence across reboots.

10. Which port mode must be set before enabling port security?

a. Dynamic
b. Access or Trunk
c. Passive
d. On

Explanation: Port security can only be configured on switchports that are set to either access or trunk mode. The port must be configured as a Layer 2 switchport (not a Layer 3 interface) before port security can be enabled.

11. Which violation mode silently drops unauthorized frames but does not log or shut down?

a. Restrict
b. Shutdown
c. Protect
d. Passive

Explanation: The "protect" violation mode simply drops frames from unauthorized MAC addresses without taking any additional actions - it doesn't generate notifications, logs, or shut down the port. It's the most lenient violation mode.

12. What happens when an unauthorized MAC address is detected on a port with default violation settings?

a. A warning is logged
b. The packet is dropped
c. The port shuts down
d. The MAC is added automatically

Explanation: The default violation mode for port security is "shutdown," which means when an unauthorized MAC address is detected, the port will be error-disabled (shut down), requiring manual intervention to re-enable it.

13. What is the primary purpose of port security on a switch?

a. Increase bandwidth
b. Allow only specific MAC addresses
c. Limit VLAN traffic

d. Enable DHCP

Explanation: The primary purpose of port security is to restrict a port to only allow connections from authorized devices by limiting which MAC addresses can use the port. This helps prevent unauthorized devices from connecting to the network.

14. Which command displays the current status of port security for an interface?

a. show mac-address-table
b. show interfaces g0/1
c. show port-security interface f0/1
d. show interface vlan 1

Explanation: The show port-security interface f0/1 command shows all port security settings and status for the specified interface, including violation count, security violation mode, maximum allowed MAC addresses, and currently secured MAC addresses.

15. What is the effect of switchport port-security maximum 5?

a. Limits bandwidth to 5 Mbps
b. Allows up to 5 MAC addresses on the port
c. Enables sticky aging
d. Sets the port to shutdown after 5 minutes

Explanation: This command increases the maximum number of MAC addresses allowed on the port from the default value (1) to 5. This means up to 5 different devices (identified by their MAC addresses) can connect to this port without triggering a security violation.