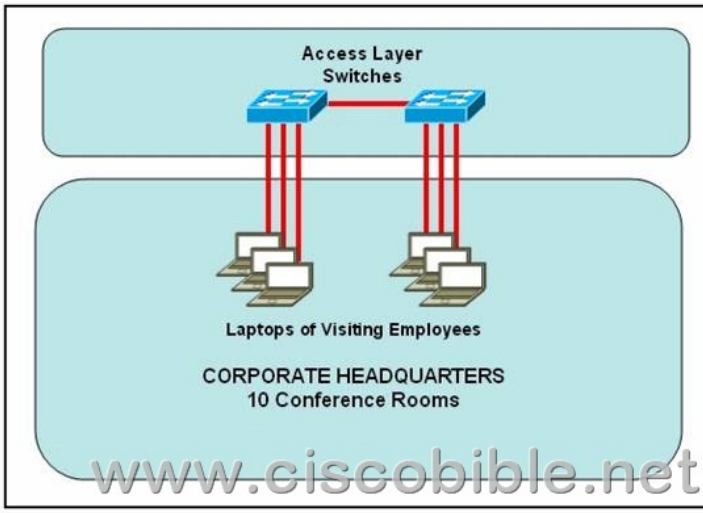
# CCNA 640-802 Bible - Implement Basic Switch Security

1. A network administrator wants to ensure that only the server can connect to port Fa0/1 on a Catalyst switch. The server is plugged into the switch Fa0/1 port and the network administrator is about to bring the server online. What can the administrator do to ensure that only the MAC address of the server is allowed by switch port Fa0/1? (Choose two.) A:Configure port Fa0/1 to accept connections only from the static IP address of the server. B:Employ a proprietary connector type on Fa0/1 that is incompatible with other host connectors. C:Configure the MAC address of the server as a static entry associated with port Fa0/1. D:Bind the IP address of the server to its MAC address on the switch to prevent other hosts from spoofing the server IP address. E:Configure port security on Fa0/1 to reject traffic with a source MAC address other than that of the server. F:Configure an access list on the switch to deny server traffic from entering any port other than Fa0/1. **Correct Answers: C, E** Explanation: You can use port security to block input to an Ethernet, Fast Ethernet, or Gigabit Ethernet port when the MAC address of the station attempting to access the port is different from any of the MAC addresses specified for that port. When a secure port receives a packet, the source MAC address of the packet is compared to the list of secure source addresses that were manually configured or autoconfigured (learned) on the port. If a MAC address of a device attached to the port differs from the list of secure addresses, the port either shuts down permanently (default mode), shuts down for the time you have specified, or drops incoming packets from the insecure host. The port's behavior depends on how you configure it to respond to a security violation. When a security violation occurs, the Link LED for that port turns orange, and a link-down trap is sent to the Simple Network Management Protocol (SNMP) manager. An SNMP trap is not sent if you configure the port for restrictive violation mode. A trap is sent only if you configure the port to shut down during a security violation. 2. Why would a network administrator configure port security on a switch? A: to prevent unauthorized Telnet access to a switch port B: to limit the number of Layer 2 broadcasts on a particular switch port C: to prevent unauthorized hosts from accessing the LAN D: to protect the IP and MAC address of the switch and associated ports E: to block unauthorized access to the switch management interfaces over common TCP ports **Correct Answers: C** Explanation: You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the workstation attached to that port is assured the full bandwidth of the port. If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, when the MAC address of a station attempting to access the port is different from any of the identified secure MAC addresses, a security violation occurs. Also, if a station with a secure MAC address configured or learned on one secure port attempts to access another secure port, a violation is flagged. 3. The network security policy requires that only one host be permitted to attach dynamically to each switch interface. If that policy is violated, the interface should shut down. Which two commands must the network administrator configure on the 2950 Catalyst switch to meet this policy? (Choose two.) A:Switch1(config-if)# switchport port-security maximum 1 B:Switch1(config)# mac-address-table secure C:Switch1(config)# access-list 10 permit ip host D:Switch1(config-if)# switchport port-security violation shutdown E:Switch1(config-if)# ip access-group 10 **Correct Answers: A, D** Explanation Catalyst switches offer the port security feature to control port access based on MAC addresses. To configure port security on an access layer switch port, begin by enabling it with the following interface configuration command: **Switch(config-if)# switchport port-security** Next, you must identify a set of allowed MAC addresses so that the port can grant them access. You can explicitly configure addresses or they can be dynamically learned from port traffic. On each interface that uses port security, specify the maximum number of MAC addresses that will be allowed access using the following interface configuration command: **Switch(config-if)# switchport port-security maximum max-addr** Finally, you must define how each interface using port security should react if a MAC address is in violation by using the following interface configuration command: **Switch(config-if)# switchport port-security violation {shutdown | restrict | protect}** A violation occurs if more than the maximum number of MAC addresses are learned, or if an unknown (not statically defined) MAC address attempts to transmit on the port. The switch port takes one of the following configured actions when a violation is detected: **Shutdown**-The port is immediately put into the errdisable state, which effectively shuts it down. It must be re-enabled manually or through errdisable recovery to be used again. **Restrict**-The port is allowed to stay up, but all packets from violating MAC addresses are dropped. The switch keeps a running count of the number of violating packets and can send an SNMP trap and a syslog message as an alert of the violation. **Protect**-The port is allowed to stay up, as in the restrict mode. Although packets from violating addresses are dropped, no record of the violation is kept. 4. In order to improve the security of switching network , refer to the following options. Which two methods are examples of implementing Layer 2 security on a Cisco switch? (Choose two.) A:disable trunk negotiation on the switch B:use only protected Telnet sessions to connect to the Cisco device C:configure a switch port host where

appropriate D:enable HTTP access to the switch for security troubleshooting **Correct Answers: A, C** 5. You are a network administrator of your company. You are asked to configure 300 switch ports to accept traffic from only the currently attached host devices. Which method will you use to effectively configure MAC-level security on all these ports? A: Configure show mac-address-table to identify the addresses related to each port and then input the commands on each switch for MAC address port-security. B: Certify the MAC addresses visually and then telnet to the switches to input the command switchport-port security mac-address. C: Configure the switchport port-security MAC address sticky command on all switch ports connected to end devices. D: Make end users e-mail their MAC addresses and telnet to the switch to issue the command switchport-port security mac-address. **Correct Answers: C** Explanation: This question is to examine the key points of port security: when you configure a port with the maximum number of security mac addresses, security addresses will be included in a table in the following way: Use the command switchport port-security mac-address <mac address> to configure all mac addresses. You can also dynamically configure security mac addresses using the connected device mac address. You can configure the number of addresses and keep the dynamic configuration. Note: If this port is shutdown, all the dynamic mac addresses will be removed. When reaching the maximum number, the mac addresses will be stored in an address table. Set the maximum number of the addresses to 1 and configure the address connected to the device to ensure the device can use the bandwidth of this port individually. The parameter sticky is to obtain the address dynamically. 6. Refer to the exhibit. Some 2950 series switches are connected to the conference area of the corporate headquarters network. The switches provide two to three jacks per conference room to host laptop connections for employees who visit the headquarters office. When large groups of employees come from other locations, the network administrator often finds that hubs have been connected to wall jacks in the conference area although the ports on the access layer switches were not intended to support multiple workstations. What action could the network administrator take to prevent access by multiple laptops through a single switch port and still leave the switch functional for its intended use?




A. Configure static entries in the switch MAC address table to include the range of addresses used by visiting employees. B. Configure an ACL to allow only a single MAC address to connect to the switch at one time. C. Use the mac-address-table 1 global configuration command to limit each port to one source MAC address. D. Implement Port Security on all interfaces and use the port-security maximum 1 command to limit port access to a single MAC address. E. Implement Port Security on all interfaces and use the port-security mac-address sticky command to limit access to a single MAC address. F. Implement Port Security at global configuration mode and use the port-security maximum 1 command to allow each switch only one attached hub. **Correct Answers:** D 7. Select the action that results from executing these commands. Switch(config-if)# switchport port-security Switch(config-if)# switchport port-security mac-address sticky A. A dynamically learned MAC address is saved in the startup-configuration file. B. A dynamically learned MAC address is saved in the running-configuration file. C. A dynamically learned MAC address is saved in the VLAN database. D. Statically configured MAC addresses are saved in the startup-configuration file if frames from that address are received. E. Statically configured MAC addresses are saved in the running-configuration file if frames from that address are received. **Correct Answers: B**