6.5.3 Switch Security Facts

The following table lists switch features that can be implemented to increase network security:

Feature	Description
Virtual LAN (VLAN)	A virtual LAN (VLAN) is a logical grouping of computers based on switch port. - VLAN membership is configured by assigning a switch port to a VLAN. - A switch can have multiple VLANs configured on it, but each switch port can only be a member of a single VLAN (with one exception described below). - VLANs can be defined on a single switch or configured on multiple interconnected switches. With multiple switches, each switch can be configured with the same VLANs, and devices on one switch can communicate with devices on other switches as long as they are members of the same VLAN. - A *trunk* port is used to connect two switches together. - Typically, Gigabit Ethernet ports are used for trunk ports, although any port can be a trunking port. - A trunk port is a member of all VLANs defined on a switch and carries traffic between the switches. - When trunking is used, frames that are sent over a trunk port are tagged by the first switch with the VLAN ID so that the receiving switch knows to which VLAN the frame belongs. - The trunking protocol describes the format that switches use for frame tagging with the VLAN ID. - Because end devices do not understand the VLAN tags, the tag is removed from the frame by the switch before the frame is forwarded to the destination device. - VLAN tagging is only used for frames that travel between switches on the trunk ports. - In a typical configuration with multiple VLANs, workstations in one VLAN will not be able to communicate with workstations in other VLANs. To enable inter-VLAN communication, you will need to use a router (or an OSI Layer 3 switch). - Using VLANs, the switch can be used to create multiple IP broadcast domains. Each VLAN is in its own broadcast domain, and broadcast traffic is sent only to members of the same VLAN.
MAC Filtering/Port Security	With switch port security, the devices that can connect to a switch through the port are restricted. - Port security uses the MAC address to identify allowed and denied devices. - On the switch, MAC addresses are stored in RAM in a table and are associated with the port. - The table can be manually configured, or learning devices can automatically build with the table. - You can specify only a single MAC address that is allowed or allow multiple addresses per port. - With automatic configuration, the next device or specified number of devices can connect to the port and additional devices are denied. - A *port violation* occurs when an unauthorized device tries to connect. The switch configuration determines how the switch handles frames from an unauthorized device. The switch can either drop all frames from the unauthorized device or shut down the port, disabling all communications through that port.
Port Authentication (802.1x)	Port authentication is provided by the 802.1x protocol and allows only authenticated devices to connect to the LAN through the switch. Authentication uses user names and passwords, smart cards, or other authentication methods. - When a device first connects, the port is set to an unauthorized state. Ports in unauthorized states can be used only for 802.1x authentication traffic. - The process begins by the switch sending an authentication request to the device. - The device responds with authentication credentials, which are forwarded by the switch to the authentication device (such as a RADIUS server). - After the server authenticates the device or the user, the switch port is placed in an authorized state, and access to other LAN devices is allowed. - When a device disconnects, the switch places the port in the unauthorized state.

Be aware of the following when implementing switch security:

- Creating VLANs with switches offers many administrative benefits. You can:
  - Create virtual LANs based on criteria such as workgroup, protocol, or service
  - Simplify device moves (devices are moved to new VLANs by modifying the port assignment)
  - Control broadcast traffic based on logical criteria (only devices in the same VLAN receive broadcast traffic)
  - Control security (isolate traffic within a VLAN)
- When you use switches to create VLANs, you will still need routers to:
  - Route data into and out of the local area network
  - Route data between VLANs
  - Port Filtering: Filter network packets into and out of devices based on their application type or port number.
- VLANs are commonly used with Voice over IP (VoIP) to distinguish voice traffic from data traffic. Traffic on the voice VLAN can be given a higher priority to ensure timely delivery.
- MAC filtering uses the MAC address of a device to drop or forward frames through the switch. Port authentication requires that the user or device authenticates before frames are forwarded through the switch.

- In general, all switch ports are enabled by default. To increase the security of the switch and network, you should disable individual ports that are not in use.

To provide fault tolerance, many networks implement redundant paths between devices using multiple switches. However, providing redundant paths between segments causes packets to be passed between the redundant paths endlessly. This condition is known as a *switching loop*. Switching loops lead to incorrect entries in a MAC address table, making a device appear to be connected to the wrong port and causing unicast traffic being circulated in a loop between switches. The spanning tree protocol runs on switches to prevent switching loops by making only a single path between switches active at a single time. The spanning tree protocol also:

- Provides redundant paths between devices.
- Recovers automatically from a topology change or device failure by unblocking redundant paths.
- Identifies the optimal path between any two network devices.
- Calculates the best loop-free path through a network by assigning a role to each bridge or switch and by assigning roles to the ports of each bridge or switch.

The type of ports used by the spanning tree protocol are:

- Root ports, which are configured to communicate directly to the root switch.
- Designated ports, which forward frames to and from attached hosts.
- Blocked ports, which form a loop and are used for redundancy.

Ports in the spanning tree protocol exist in one of five states:

- Blocking
- Listening
- Learning
- Forwarding
- Disabled