6.4.2 Switch Attack Facts

The following table lists common attacks that are perpetrated against switches.

Attack	Description
MAC Flooding	*MAC flooding* overloads the switch's MAC forwarding table to make the switch function like a hub. MAC flooding is performed using the following method: 1. The attacker floods the switch with packets, each containing a different source MAC address. 2. The flood of packets fills up the forwarding table and consumes so much of the memory in the switch that it causes the switch to enter a state called *fail open mode*, in which all incoming packets are broadcast out all ports (as with a hub) instead of just to the correct ports, as per normal operation. 3. The attacker captures all the traffic with a protocol analyzer/sniffer.

ARP Spoofing/Poisoning	*ARP spoofing/poisoning* associates the attacker's MAC address with the IP address of victim devices.
	▪ When computers send an ARP request for the MAC address of a known IP address, the attacker's system responds with its MAC address.
	▪ The source device sends frames to the attacker's MAC address instead of the correct device.
	▪ Switches are indirectly involved in the attack because they do not verify the MAC address/IP address association.
	▪ A default gateway is a prime target because local traffic goes through a default gateway to get to non-local destinations, like the internet. When the attacker associates his MAC address with the default gateway's IP address:
	  ▪ Traffic could be forwarded to the actual default gateway (*passive sniffing*).
	  ▪ Data could be modified before forwarding it (*man-in-the-middle*).

MAC Spoofing	*MAC spoofing* is changing the source MAC address on frames sent by the attacker.
	▪ MAC spoofing is typically used to bypass 802.1x port-based security.
	▪ MAC spoofing can be used to bypass wireless MAC filtering.
	▪ MAC spoofing can be used to hide the identity of the attacker's computer or to impersonate another device on the network.
	▪ The attacker's system sends frames with the spoofed MAC address. The switch reads the source address contained in the frames and associates the MAC address with the port where the attacker is connected.
	▪ MAC spoofing can be used to:
	  ▪ Impersonate another device on the network to capture frames addressed to the other device.
	  ▪ Impersonate a valid device on the network to gain network access--for example, to gain access when the switch is using the MAC address to allow or deny a network connection.

Dynamic Trunking Protocol (DTP)	Switches have the ability to automatically detect trunk ports and negotiate the trunking protocol used between devices. DTP is not secure and allows unauthorized devices to possibly modify configuration information. You should disable the DTP services on the switch's end user (access) ports before implementing the switch configuration into the network.