MAC flooding attack

Switches maintain a MAC Table that maps individual MAC addresses on the network to the physical ports on the switch. This allows the switch to direct data to the destination port as unicast messages and there by avoiding broadcasting all messages.

In MAC flooding attack, a switch is flooded with ethernet frames, each containing different source MAC addresses.This frames with unique invalid source MAC address flood the switch and exhaust CAM table space.The result is that new entireis cannot be inserted because of the exhausted CAM table space and traffic is subsequently flooded out all ports

The result of this attack causes the switch to enter a state called failopen mode, in which all incoming packets are broadcast out on all ports (Same as hub), instead of sending unicasts in normal operation. A malicious user could then use a packet sniffer to capture sensitive data from other computers, which would not be accessible were the switch operating normally.

MAC Flooding attack can be prevented by

1. Implement port security.
2. Implement VLAN access maps