Attack Prevention Strategy - VLAN
CAM-Overflow_Prevention – Prevention of CAM Table Overflow Attack. To prevent CAM Table Overflow Attacks, we recommend: i) Enable the port security configuration on devices (port-security); ii) Restrict access to devices ports; iii) Limit the number of MAC addresses that each device port can accept; iv) Ignore MAC addresses after device port limit is reached.
ARP-Attack_Prevention – Prevention of ARP Attack. To prevent ARP Attacks, we recommend: i) Implement DHCP Snooping, which must be configured first, otherwise, there will be no binding table to be used in dynamic ARP inspection; ii) Implement DAI (Dynamic ARP Inspection), a security feature that discards ARP packets with invalid IP and MAC addresses; iii) Enable device port security features and consider static ARP for critical routers and hosts; iv) Adjust IDS systems to monitoring exceptionally high amounts of ARP traffic.
VLAN-Hopping_Prevention – Prevention of VLAN Hopping Attack. To prevent VLAN Hopping Attacks, we recommend: i) Using dedicated VLAN IDs for all trunk ports; ii) Disable unused ports and place them in an unused VLAN; iii) Disable automatic trunking on user-facing ports (DTP disabled); iv) Explicitly configure trunking on infrastructure ports; v) Use all tagged mode for native VLAN on trunks; vi) Use PC Voice VLAN Access on phones that support it; vii) Use 802.1q tags on VLAN frames on trunk connection; viii) Do not use VLAN 1; ix) Avoid default settings.
Double-Tagging_Prevention - Prevention of Double Tagging Attack. To prevent of Double Tagging Attack we recommend: As it is a variant of VLAN Hopping Attack use the same recommendations.
VMPS-VQP-Attack_Prevention - Prevention of VMPS/VQP Attack. To prevent VMPS/VQP Attack, we recommend: i) Consider sending VQP Out-of-Band (OOB) messages; ii) Monitor network traffic; iii) Use ACLs to filter unwanted access. **Obs:** VQP and VMPS are rarely used for MAC-based VLAN assignment because of the management burden of maintaining the MAC address to VLAN mapping table. The URT component is also not frequently used, especially since a standards-based method of effectively doing the same thing (802.1x) is now available.
Multicast-Brute-Force_Prevention - Prevention of Multicast Brute Force Attack. To prevent Multicast Brute Force Attack, we recommend: i) Storm control limits the amount of broadcast or multicast traffic sent by switches in the network; ii) Port security to limit the number of MAC addresses that can be learned per port on the switch. **Obs:** This type of attack generally proves ineffective, because the switches must contain all frames within their proper broadcast domain; Layer 2 multicast packets must be restricted within the incoming VLAN. No packets should be 'leaked' to other VLANs.
Randon-Frame-Stress_Prevention - Prevention of Randon Frame Stress Attack. To prevent Randon Frame Stress Attack, we recommend: i) Storm control limits the amount of broadcast or multicast traffic sent by switches in the network; ii) Port security to limit the number of MAC addresses that can be learned per port on the switch. **Obs:** This type of attack generally proves ineffective, because the switches must contain all frames within their proper broadcast domain; Layer 2 multicast packets must be restricted within the incoming VLAN. No packets should be 'leaked' to other VLANs.

PVLAN-Attack_Prevention - Prevention of PVLAN Attack. To prevent of PVLAN Attack, we recommend: i) Configure an ACL (Access Control List) on the router interface, preventing IP addresses from talking to each other or; ii) Use VACL (VLAN ACL).
STP-Attack_Prevention - Prevention of STP Attack. To prevent STP Attack, we recommend: i) Do not disable STP (network loop would become another attack); ii) Disable spanning tree function for entire user interface; iii) Use BPDU Guard and Root Guard features on switches; iv) The Bridge Protocol Data Units (BPDU) Guard must be run on all user-facing ports and infrastructure-facing ports; v) Root Guard - Configured per port. Disables ports that would become the root bridge due to BPDU advertisement; vi) Try to design loop-free topologies whenever possible so you don't need STP.
MAC-Spoofing_Prevention - Prevention of MAC Spoofing Attack. To prevent MAC Spoofing Attack, we recommend: i) IP Source Guard prevents IP/MAC Spoofing.
DHCP-Spoofing_Prevention - Prevention of DHCP Spoofing Attack. To prevent DHCP Spoofing Attack, we recommend: i) Multilayer switch that has the ability to drop packets; ii) Use the DHCP Snooping feature, which discards DHCP-OFFER and DHCP-ACK messages on untrusted ports; iii) For switches on the network that do not support DHCP Snooping, configure VLAN ACLs to block UDP port 68.
DHCP-Starvation_Prevention - Prevention of DHCP Starvation. To prevent DHCP Starvation, we recommend: i) Enable the port-security feature; ii) Restrict Access on Switch Ports; iii) Limit the number of MAC addresses each switch port can learn; iv) Ignore the number of MAC addresses after the port limit is reached. **Obs:** (Same recommendations applied in CAM Overflow).
VTP-Attack_Prevention - Prevention of VTP Attack. To prevent VTP Attack, we recommend: i) Configuration VTP operating mode to "off" (CatOS only); ii) For devices that don't require the use of VTP, administrators should set the VTP mode to "transparent" ; iii) If VTP is needed, use MD5 authentication.
CDP-Attack_Prevention - Prevention of CDP Attack. To prevent CDP Attack, we recommend: i) Limit CDP usage on devices or ports; ii) Disable the CDP protocol on each of the ports on the switch or on the end ports that connect to untrusted devices. **Obs:** Link Layer Discovery Protocol (LLDP) is also vulnerable to reconnaissance attacks. i)To disable LLDP on the interface, configure no lldp transmit and no lldp receive; ii) Update your IOS frequently, current versions of CatOS.