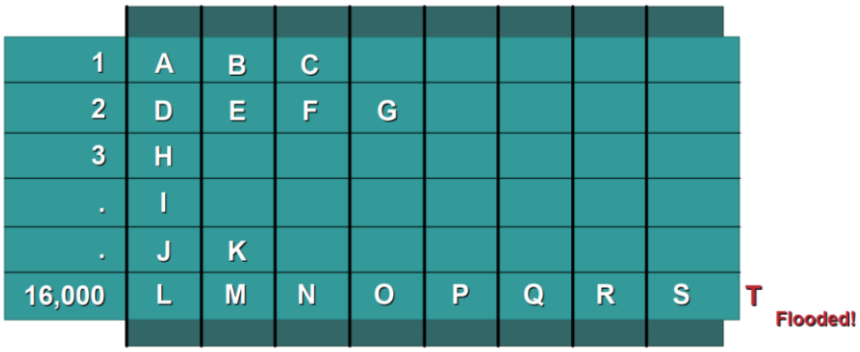
حملات لایه دوم
منبع : Cisco.com

حملات در لایه دوم عبارتند از:

MAC Attacks / CAM Overflow

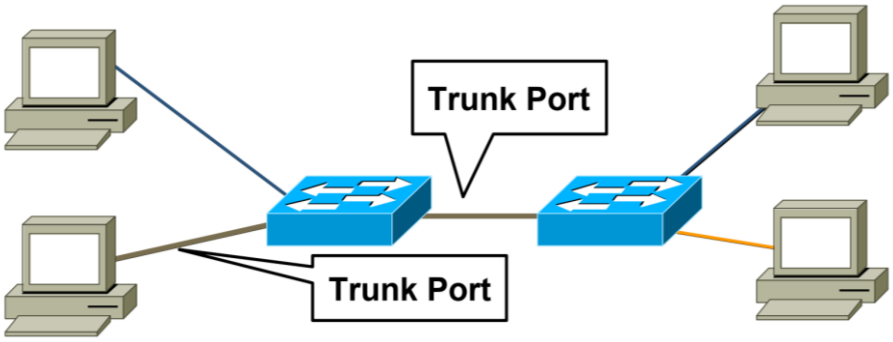
Catalyst switches use hash to place MAC in CAM table. 63 bits of source (MAC, VLAN, misc) creates a 17-bit hash value. If the value is the same there are 8 columns to place CAM entries, if all 8 are filled the packet is flooded. Dsniff (macof) can generate 480,000 MAC entries on a switch per minute 8000/s*60. Assuming a perfect hash function, the CAM table will total out at 128,000 (16,000 x 8) 131,052 to be exact. Since hash isn't perfect it actually takes 70 seconds to fill the CAM table Once table is full, traffic without a CAM entry floods on the VLAN, but NOT existing traffic with an existing CAM entry.



VLAN Hopping Attacks

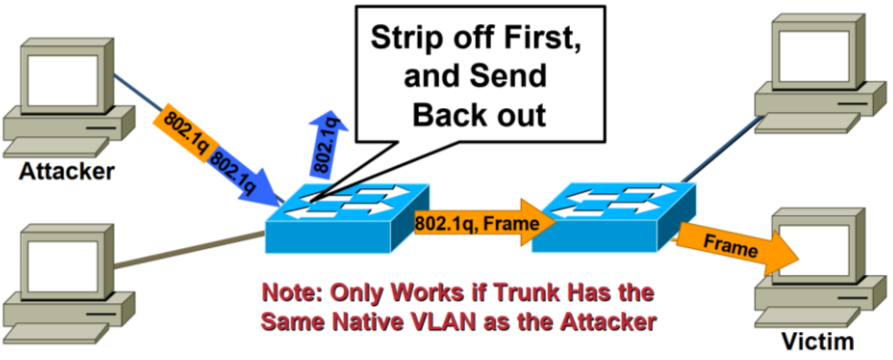
Dynamic Trunk Protocol (DTP):
Automates ISL/802.1Q trunk
configuration - Operates between switches - Does not operate on routers

A station can spoof as a switch with ISL or 802.1Q signaling (DTP signaling is usually required as well)
The station is then member of all VLANs
Requires a trunking favorable setting on the port



Double Encapsulated 802.1q VLAN Hopping Attack

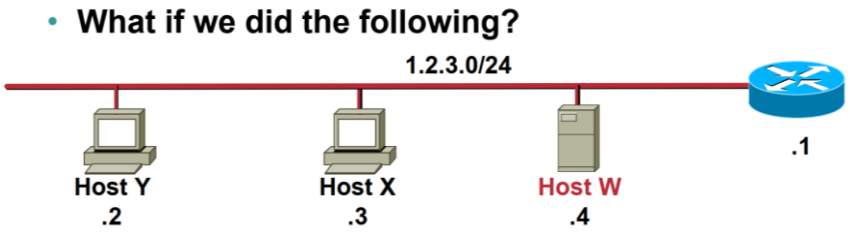
Send double encapsulated 802.1Q frames
Switch performs only one level of decapsulation
Unidirectional traffic only
Works even if trunk ports are set to off



GARP Attacks

An ARP request message should be placed in a frame and broadcast to all computers on the network. Each computer receives the request and examines the IP address. The computer mentioned in the request sends a response; all other computers process and discard the request without sending a response

Gratuitous ARP is used by hosts to “announce” their IP address to the local network and avoid duplicate IP addresses on the network; routers and other network hardware may use cache information gained from gratuitous ARPs. Gratuitous ARP is a broadcast packet (like an ARP request). ARP has no security or ownership of IP or MAC addresses.



*Host W broadcasts I’m 1.2.3.1 with MAC 12:34:56:78:9A:BC
*(Wait 5 seconds)
*Host W broadcasts I’m 1.2.3.1 with MAC 12:34:56:78:9A:BC
*When host Y requests the MAC of 1.2.3.1 the real router will reply and communications will work until host W sends a gratuitous ARP again
*Even a static ARP entry for 1.2.3.1 on Y will get overwritten by the Gratuitous ARP on some OSs

More on Arpspoof

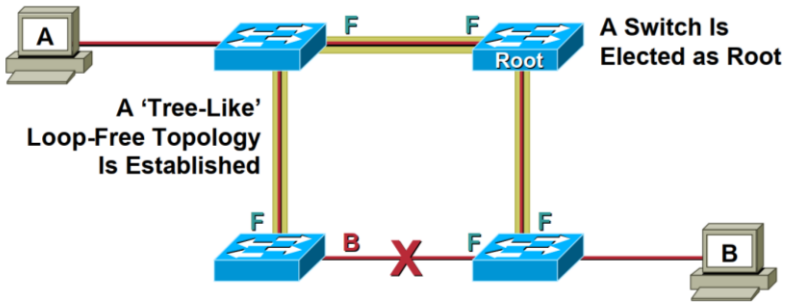
• All traffic now flows through machine running dsniff in a half-duplex manner
Not quite a sniffer but fairly close
• Port security doesn’t help
• Static ARP doesn’t help
• Note that attack could be generated in the

opposite direction by spoofing the destination host when the router sends its ARP request

Spanning Tree Attacks

Spanning Tree

- Purpose: To maintain loop-free topologies in a redundant Layer 2 infrastructure
- Provides path recovery services



Loop-Free Connectivity

Send BPDU (Bridge protocol data unit) messages from attacker to force spanning tree recalculations Impact likely to be DoS • Send BPDU messages to become root bridge The hacker then sees frames he shouldn't MITM, DoS, etc. all possible	

Any attack is very sensitive to the original topology, trunking, PVST, etc.

Requires attacker to be dual homed to two different switches