WIKIPEDIA

# MAC flooding

In computer networking, a **media access control attack** or **MAC flooding** is a technique employed to compromise the security of network switches. The attack works by forcing legitimate MAC table contents out of the switch and forcing a unicast flooding behavior potentially sending sensitive information to portions of the network where it is not normally intended to go.

## Attack method

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 out of the physical port where the recipient is located, as opposed to indiscriminately broadcasting the data out of all ports as an Ethernet hub does. The advantage of this method is that data is bridged exclusively to the network segment containing the computer that the data is specifically destined for.

In a typical MAC flooding attack, a switch is fed many Ethernet frames, each containing different source MAC addresses, by the attacker. The intention is to consume the limited memory set aside in the switch to store the MAC address table.[1]

The effect of this attack may vary across implementations, however the desired effect (by the attacker) is to force legitimate MAC addresses out of the MAC address table, causing significant quantities of incoming frames to be flooded out on all ports. It is from this flooding behavior that the MAC flooding attack gets its name.

After launching a successful MAC flooding attack, a malicious user can use a packet analyzer to capture sensitive data being transmitted between other computers, which would not be accessible were the switch operating normally. The attacker may also follow up with an ARP spoofing attack which will allow them to retain access to privileged data after switches recover from the initial MAC flooding attack.

MAC flooding can also be used as a rudimentary VLAN hopping attack.[2]

## Counter measures

To prevent MAC flooding attacks, network operators usually rely on the presence of one or more features in their network equipment:

- With a feature often called "port security" by vendors, many advanced switches can be configured to limit the number of MAC addresses that can be learned on ports connected to end stations.[3] A smaller table of *secure* MAC addresses is maintained in addition to (and as a subset to) the traditional MAC address table.
- Many vendors allow discovered MAC addresses to be authenticated against an authentication, authorization and accounting (AAA) server and subsequently filtered.[4]
- Implementations of IEEE 802.1X suites often allow packet filtering rules to be installed explicitly by an AAA server based on dynamically learned information about clients, including the MAC address.
- Security features to prevent ARP spoofing or IP address spoofing in some cases may also perform additional MAC address filtering on unicast packets, however this is an implementation-dependent side-effect.
- Additional security measures are sometimes applied along with the above to prevent normal unicast flooding

for unknown MAC addresses.[5] This feature usually relies on the "port security" feature to retain all *secure* MAC addresses for at least as long as they remain in the ARP table of layer 3 devices. Hence, the aging time of learned *secure* MAC addresses is separately adjustable. This feature prevents packets from flooding under normal operational circumstances, as well as mitigating the effects of a MAC flood attack.

# References


1. "VLAN Security White Paper: Cisco Catalyst 6500 Series Switches" (https://web.archive.org/web/20110608051916/http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml#wp39054). *Cisco Systems*. 2002. Archived from the original (http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml#wp39054) on 8 June 2011. Retrieved 31 January 2015.
2. Steve A. Rouiller, *Virtual LAN Security: weaknesses and countermeasures* (https://www.sans.org/reading-room/whitepapers/networkdevs/virtual-lan-security-weaknesses-countermeasures-1090), SANS Institute, retrieved 2017-11-17
3. *Business Series Smart Gigabit Ethernet Switch User Guide*, Linksys, 2007, p. 22
4. "guide/Mac Auth" (http://wiki.freeradius.org/guide/Mac%20Auth). *Freeradius.org*. 2015. Retrieved 31 January 2015.
5. "Blocking Unknown Unicast Flooding" (http://packetlife.net/blog/2010/jun/4/blocking-unknown-unicast-flooding/). *PacketLife.net*. 4 June 2010. Retrieved 31 January 2015.