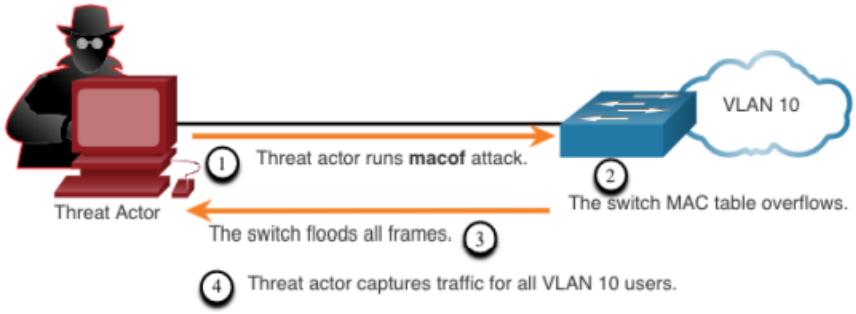
Example: MAC address flooding attack

MAC table has fixed size to store mac addresses, when the table is full, Switch run out of resources

Attacker takes advantage of MAC address table limitation.
Attacker can use macof tools to send fake source MAC addresses till the Switch MAC address table is full
Once the mac table is full, the switch becomes like hub by sending all incoming traffic out all ports on the same VLAN.
Then the attacker can capture traffic sent between hosts in the same LAN or VLAN.



(Cisco,2016)

If Switch MAC address table size is 132,000 MACs, macof tool can send 8000 frame per second which result in creating MAC address table overflow attack within a few seconds.

Another reason that makes macof tool dangerous, it can affect other layer 2 switches that are connected to the attacked switch. The infected switch will flood out all ports including those connected to other switch.

Mitigation

Admin must implement port security
Port security will only allow specified number of source MAC to be learned on the port

Practice LAB

Attacker will run macof to flood MAC address-table with fake source MACs

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# macof -i eth0
```

SW1 Before attack

```
SW1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

```
SW1#show mac address-table count

Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count   : 0
Static  Address Count   : 0
Total Mac Addresses     : 0

Total Mac Address Space Available: 210490424
```

```
SW1#show processes cpu
SW1#show processes cpu
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0           3          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2          16         482         33  0.00%  0.00%  0.00%   0 Load Meter
   3          76         623        121  0.07%  0.04%  0.02%   0 Exec
   4         276         316        873  0.00%  0.01%  0.00%   0 Check heaps
   5           0          41          0  0.00%  0.00%  0.00%   0 Pool Manager
   6           0           1          0  0.00%  0.00%  0.00%   0 DiscardQ Backgro
 --More--
```

SW1 after attack occurred:

```
SW1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0003.593b.4cff    DYNAMIC     Et0/0
   1    0004.8923.b603    DYNAMIC     Et0/0
   1    0005.bc55.cb98    DYNAMIC     Et0/0
   1    0006.0106.cb6f    DYNAMIC     Et0/0
   1    0006.e756.142c    DYNAMIC     Et0/0
   1    0007.374b.a7a8    DYNAMIC     Et0/0
   1    000b.4605.3c9f    DYNAMIC     Et0/0
   1    000b.750c.e707    DYNAMIC     Et0/0
   1    000d.5d48.f3cd    DYNAMIC     Et0/0
   1    000e.5174.ad5e    DYNAMIC     Et0/0
   1    0012.c748.abc5    DYNAMIC     Et0/0
   1    0018.433d.9caf    DYNAMIC     Et0/0
   1    001b.4847.0fe9    DYNAMIC     Et0/0
   1    001c.b22a.835c    DYNAMIC     Et0/0
   1    001d.8242.3d6d    DYNAMIC     Et0/0
   1    001e.1072.9bdb    DYNAMIC     Et0/0
   1    001e.9721.d6aa    DYNAMIC     Et0/0
   1    001e.a40a.d4fb    DYNAMIC     Et0/0
 --More--
```

```
SW1#show mac address-table count

Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count  : 23365
Static  Address Count  : 0
Total Mac Addresses    : 23365

Total Mac Address Space Available: 210490424
```

```
SW1#show processes cpu
CPU utilization for five seconds: 40%/55%; one minute: 65%; five minutes: 29%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0           3          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2       16526         551      29992 13.26% 14.03%  5.22%   0 Load Meter
   3         100         739        135  0.45%  0.04%  0.02%   0 Exec
   4         325         357        910  0.36%  0.04%  0.00%   0 Check heaps
   5           0          46          0  0.08%  0.00%  0.00%   0 Pool Manager
   6           0           1          0  0.00%  0.00%  0.00%   0 DiscardQ Backgro
   7           0           2          0  0.00%  0.00%  0.00%   0 Timers
   8           0          56          0  0.00%  0.00%  0.00%   0 WATCH_AFS
   9           0           1          0  0.00%  0.00%  0.00%   0 OIR Handler
  10           0           1          0  0.00%  0.00%  0.00%   0 IFS Agent Manage
  11           0           5          0  0.00%  0.00%  0.00%   0 ARP Input
 --More--
```

Mitigation by implementing port security on e0/0 interface on SW1

```
SW1(config)#interface e0/0
SW1(config-if)#switchport mode access
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security max 2
SW1(config-if)#switchport port-security mac-address sticky
SW1(config-if)#end
SW1#
*Aug 26 14:20:19.306: %SYS-5-CONFIG_I: Configured from console by console
SW1#show port-security interface e0/0
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

By configuring the complete port security above on interface e0/0, once attacker run macof against SW1 the port will change to (err-disable) mode due to violation mode is set to Shutdown by default.

Important Note: to enable port security, you should manually change switch port mode to Access or Trunk as the switchport set to Dynamically by default.

```
*Aug 26 19:07:23.446: %PM-4-ERR_DISABLE: psecure-violation error detected on Et0/0, putting E
t0/0 in err-disable state
SW1(config-if)#
*Aug 26 19:07:23.446: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused
 by MAC address a0c1.111d.5dc7 on port Ethernet0/0.
SW1(config-if)#
*Aug 26 19:07:24.446: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed st
ate to down
*Aug 26 19:07:25.446: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to down
```

```
SW1#show interface status

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/0                        err-disabled 1            auto   auto unknown
Et0/1                        connected    1            auto   auto unknown
Et0/2                        connected    1            auto   auto unknown
Et0/3                        connected    1            auto   auto unknown
```

The security Admin will investigate issue and ensure it is secure then enable the port again.

The command below also shows that the port status is Shutdown due to security violation (1)

```
SW1#show port-security interface e0/0
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 2
Last Source Address:Vlan   : 0c35.4a6a.1df0:1
Security Violation Count   : 1
```

Another mode of violation is restrict : the port drops packets with unknown source addresses and security messages generated on console

```
SW1(config-if)#switchport port-security violation restrict
SW1(config-if)#
SW1(config-if)#
SW1(config-if)#
*Aug 26 18:55:30.658: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation o
ccurred, caused by MAC address c065.4021.14c9 on port Ethernet0/0.
SW1(config-if)#
*Aug 26 18:55:35.657: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation o
ccurred, caused by MAC address 3279.db01.ad00 on port Ethernet0/0.
SW1(config-if)#
*Aug 26 18:55:40.657: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation o
ccurred, caused by MAC address 10a5.ed46.c763 on port Ethernet0/0.
SW1(config-if)#
```

```
SW1#show port-security interface e0/0
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 2
Last Source Address:Vlan   : 02dc.b054.ac8c:1
Security Violation Count   : 32159
```

```
SW1#show int status

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/0                        connected    1            auto   auto unknown
Et0/1                        connected    1            auto   auto unknown
Et0/2                        connected    1            auto   auto unknown
Et0/3                        connected    1            auto   auto unknown
```