

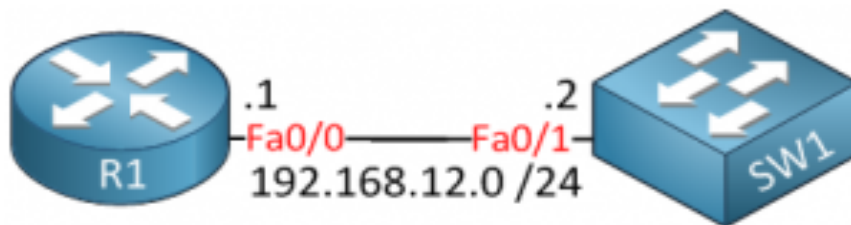
Static MAC Address Table Entry | NetworkLessons.com

13 votes

Normally your switch will automatically learn MAC addresses and fill its MAC address table (CAM table) by looking at the source MAC address of incoming frames and flooding frames if it doesn't know where to forward the frame.

This process is vulnerable to layer 2 MAC address spoofing attacks where an attacker spoofs a certain MAC address to change entries in the MAC address table. A really simple method to deal with this issue is to manually configure entries in the MAC address table, a static entry will always overrule dynamic entries. You can either specify the interface where the MAC address is located or tell the switch to **drop the traffic**.

Let's look at an example!



To demonstrate this we only require two devices. A router to generate some traffic and a switch to look at (and configure) the MAC address table. Here's the configuration:

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#no shutdown
R1(config-if)#ip address 192.168.12.1 255.255.255.0
```

```
SW1(config)#interface vlan 1
SW1(config-if)#no shutdown
SW1(config-if)#ip address 192.168.12.2 255.255.255.0
```

We'll do a quick ping to generate some traffic so SW1 can learn about the mac address of R1's FastEthernet 0/0 interface:

```
R1#ping 192.168.12.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms
```

Let's take a look at the MAC address table:

```
SW1#show mac address-table dynamic vlan 1
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
1       001d.a18b.36d0    DYNAMIC Fa0/1
Total Mac Addresses for this criterion: 1
```

Here's the MAC address of R1, learned dynamically. Let's turn this into a static entry:

```
SW1(config)#mac address-table static 001d.a18b.36d0 vlan 1 interface fastEthernet
0/1
```

Use the mac address-table static command to create a static entry. Here's what the MAC address table looks like now:

```
SW1#show mac address-table static | include Fa0/1
1       001d.a18b.36d0    STATIC    Fa0/1
```

There it is, a static entry. No way to overrule this unless you have access to our switch. This prevents us from moving R1 to another interface on SW1 unless we change the static entry. Like I mentioned before we can also change a static entry so it will drop all traffic. Here's how to do it:

```
SW1(config)#mac address-table static 001d.a18b.36d0 vlan 1 drop
```

All frames destined for the MAC address of R1 will now be dropped:

```
R1#ping 192.168.12.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Because of our static drop entry, our pings are failing. That's all there is to it...I hope you enjoyed this lesson!

Rate this Lesson: