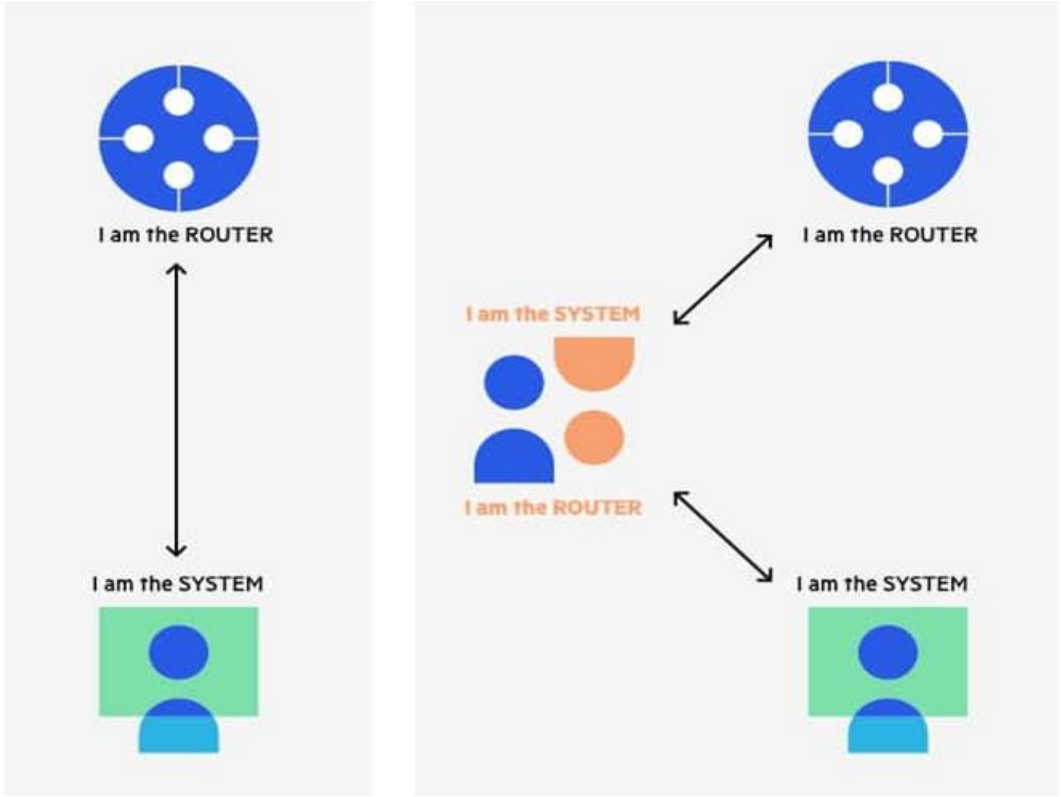
TITLE : MITM ATTACK DETECTION

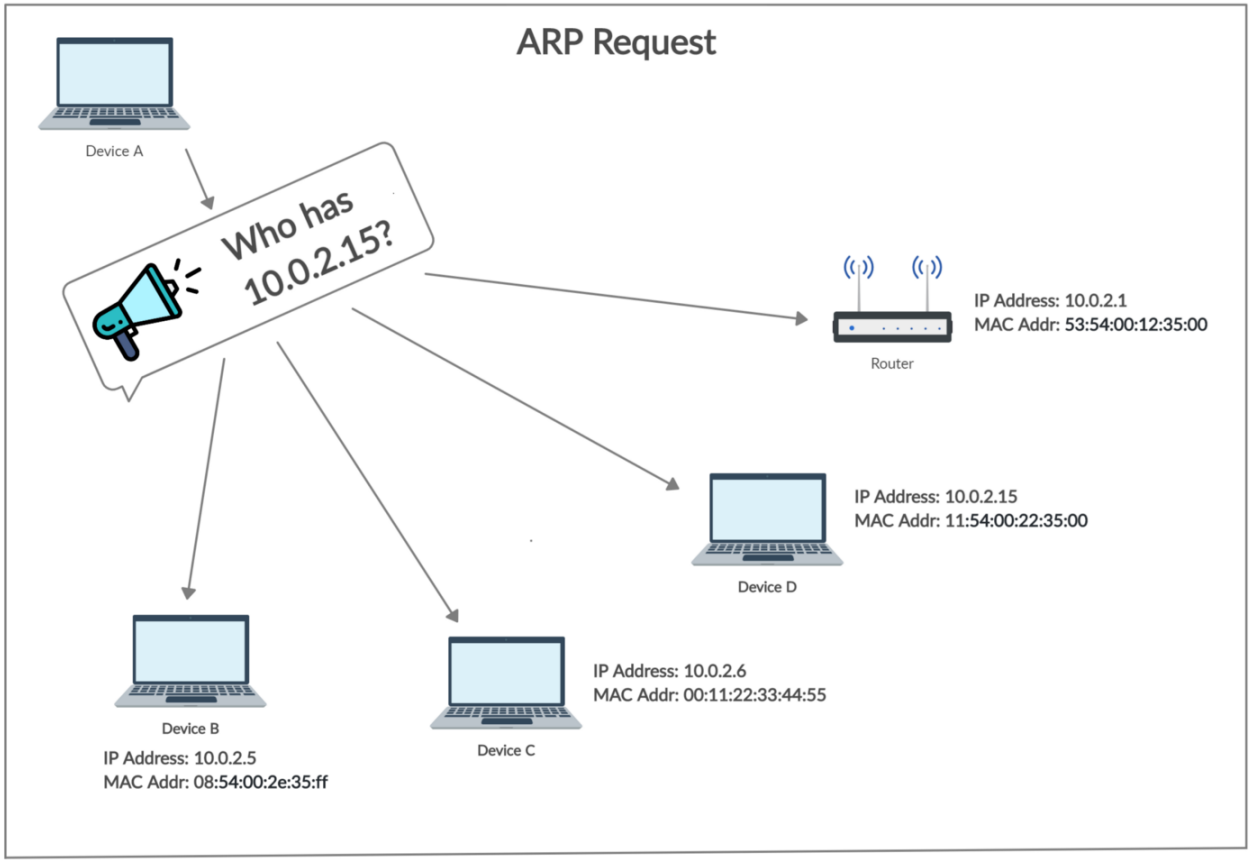
KRISHNAKUMAR .G

ARP spoofing and ARP cache poisoning

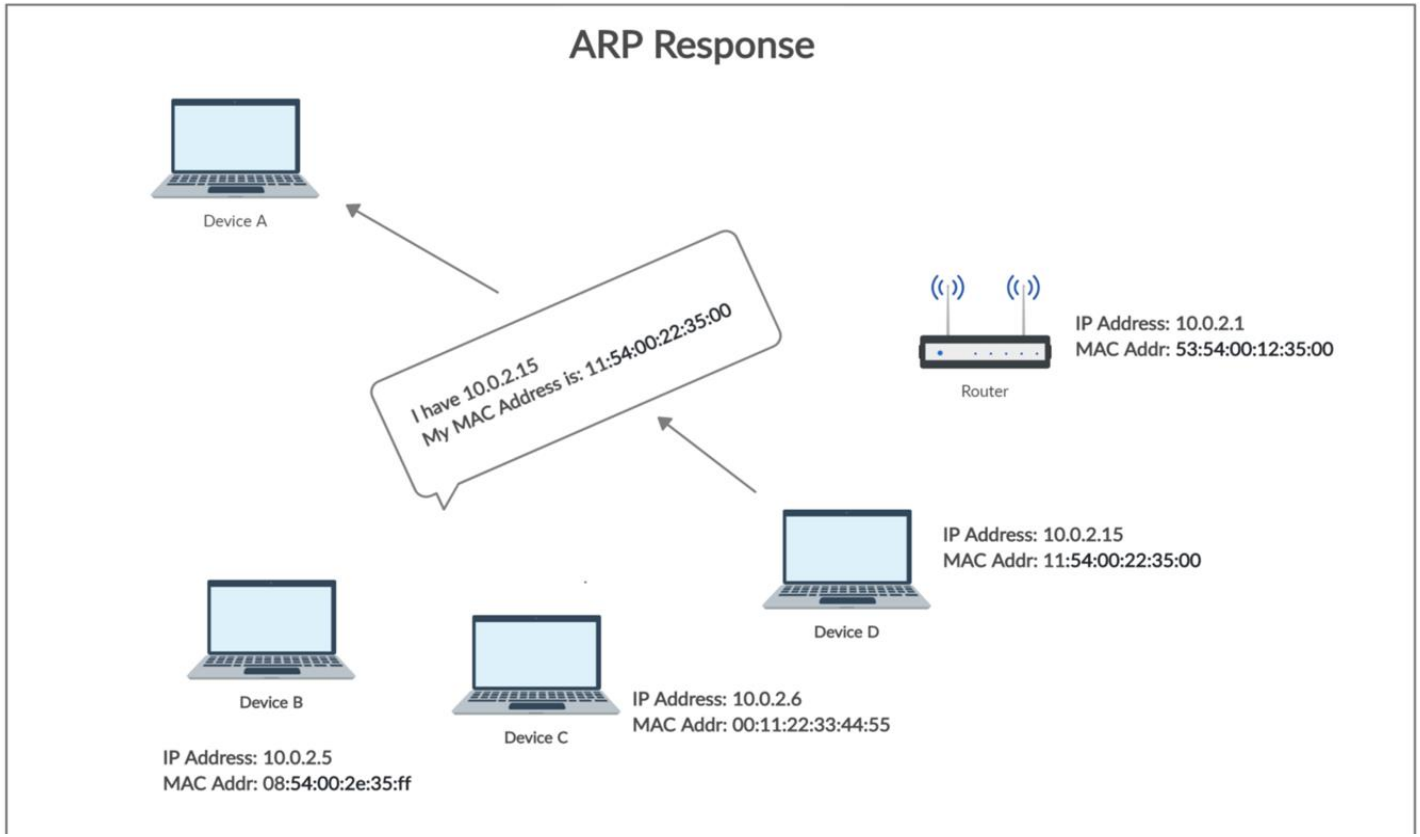
MITM:-

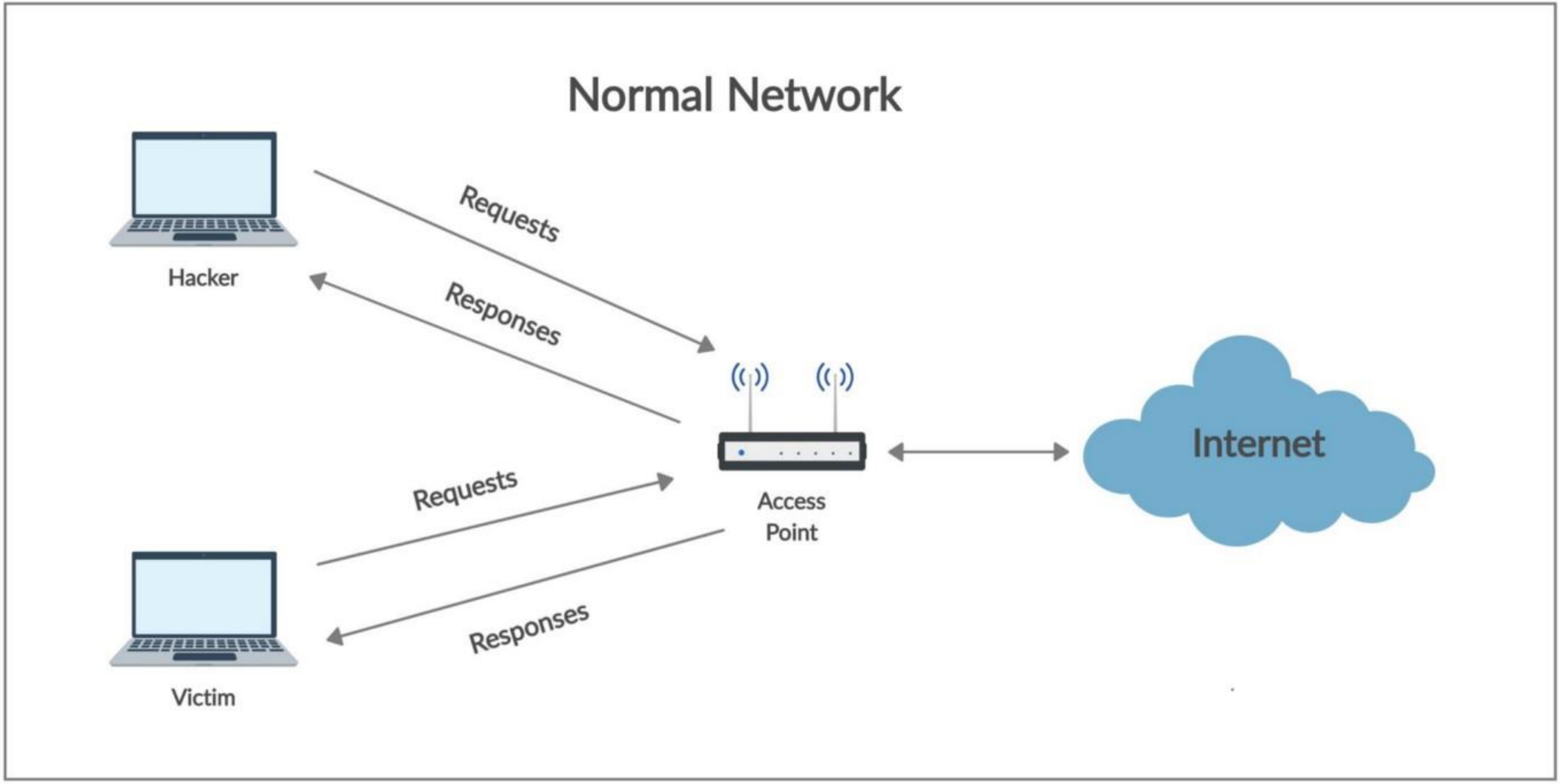

I am the ROUTER
I am the SYSTEM
I am the ROUTER
I am the SYSTEM
I am the ROUTER
I am the SYSTEM

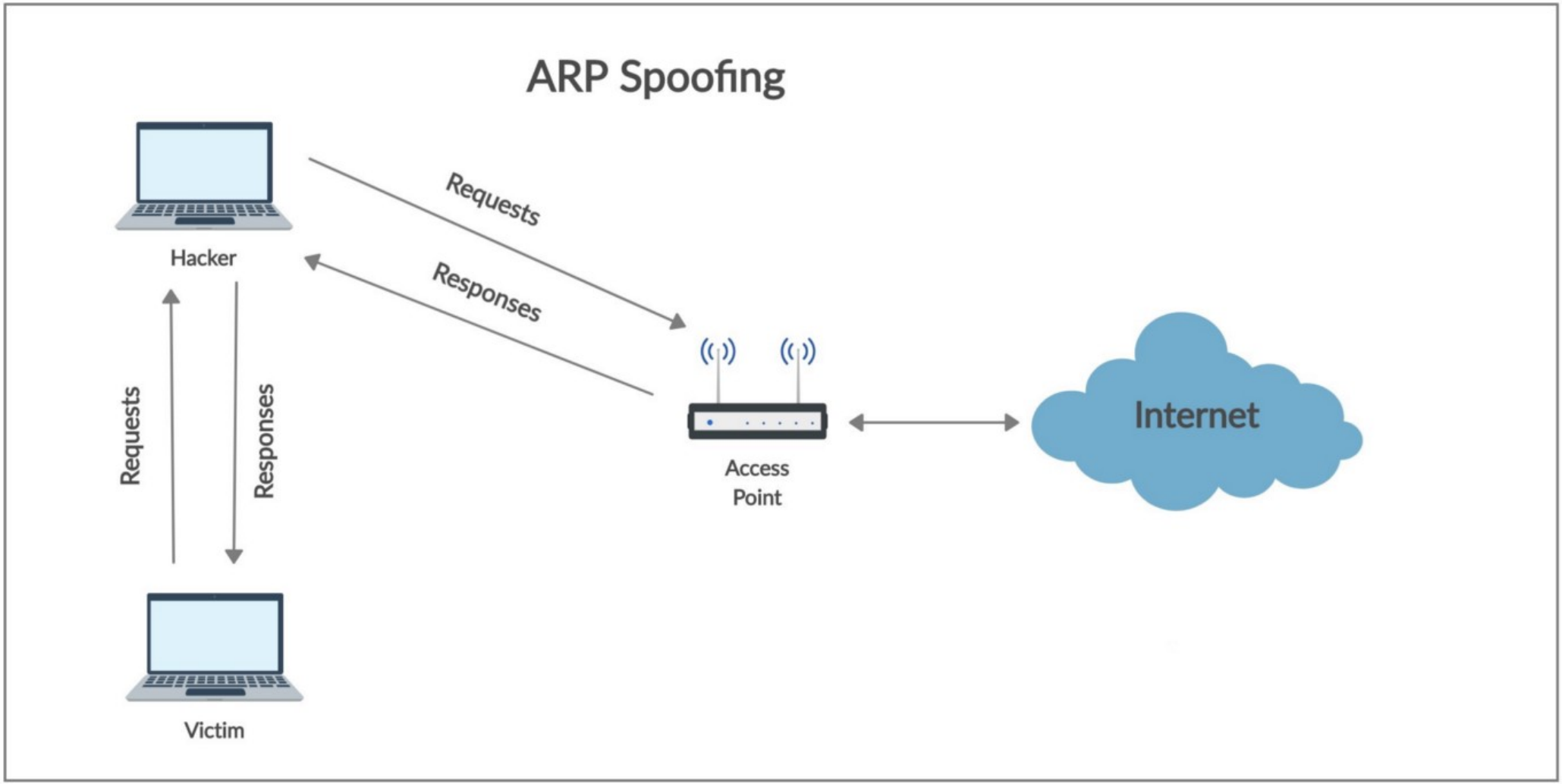
How ARP(Address Resolution Protocol) works :-

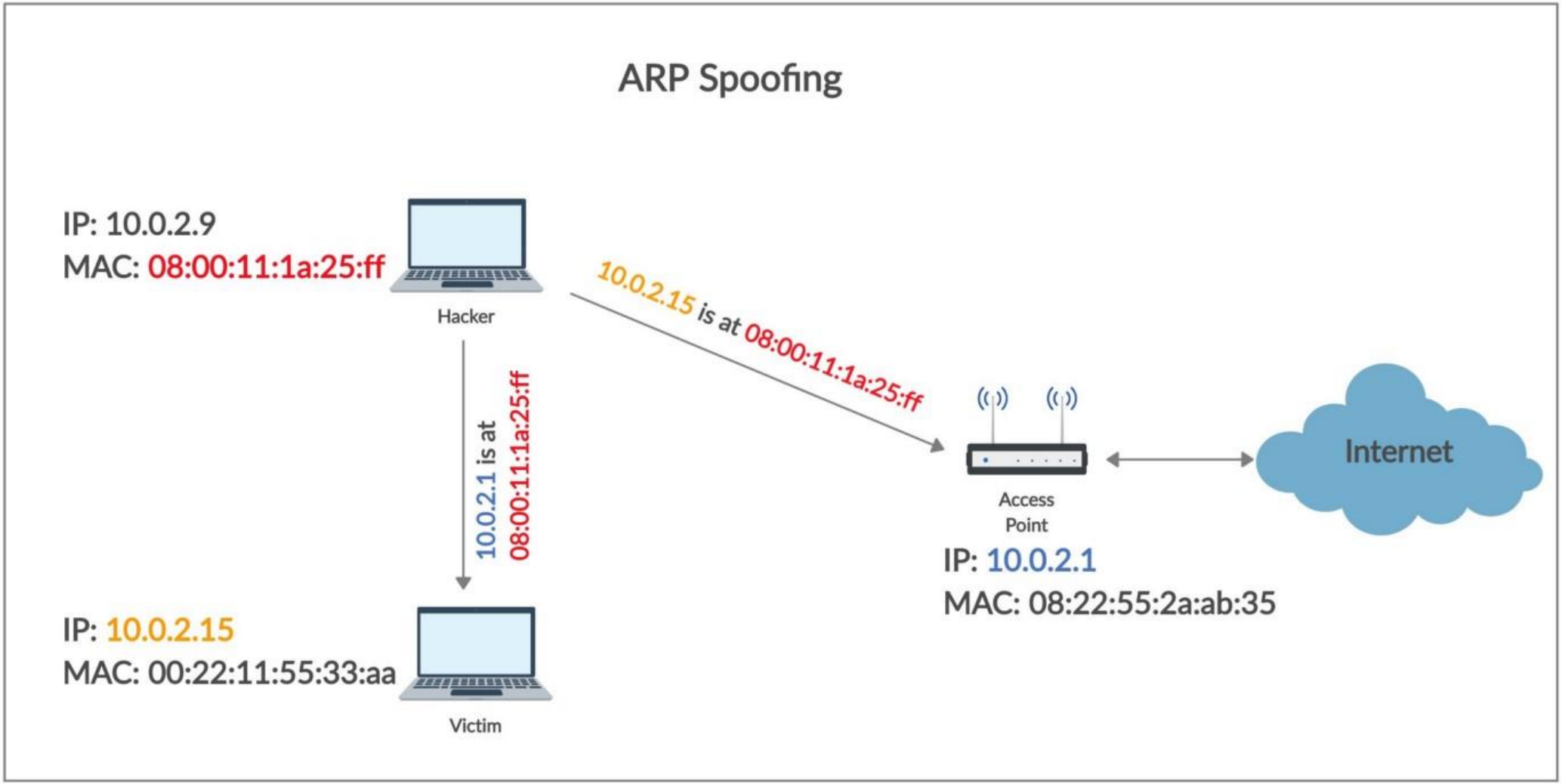


ARP Response:-




Normal Network
Hacker
Requests
Responses
Access
Point
Internet
Requests
Responses
Victim


ARP Spoofing
Hacker
Requests
Responses
Requests
Responses
Access
Point
Internet
Victim


ARP Spoofing
IP: 10.0.2.9
MAC: 08:00:11:1a:25:ff
Hacker
10.0.2.15 is at 08:00:11:1a:25:ff
10.0.2.1 is at 08:00:11:1a:25:ff
Internet
Access Point
IP: 10.0.2.1
MAC: 08:22:55:2a:ab:35
IP: 10.0.2.15
MAC: 00:22:11:55:33:aa
Victim

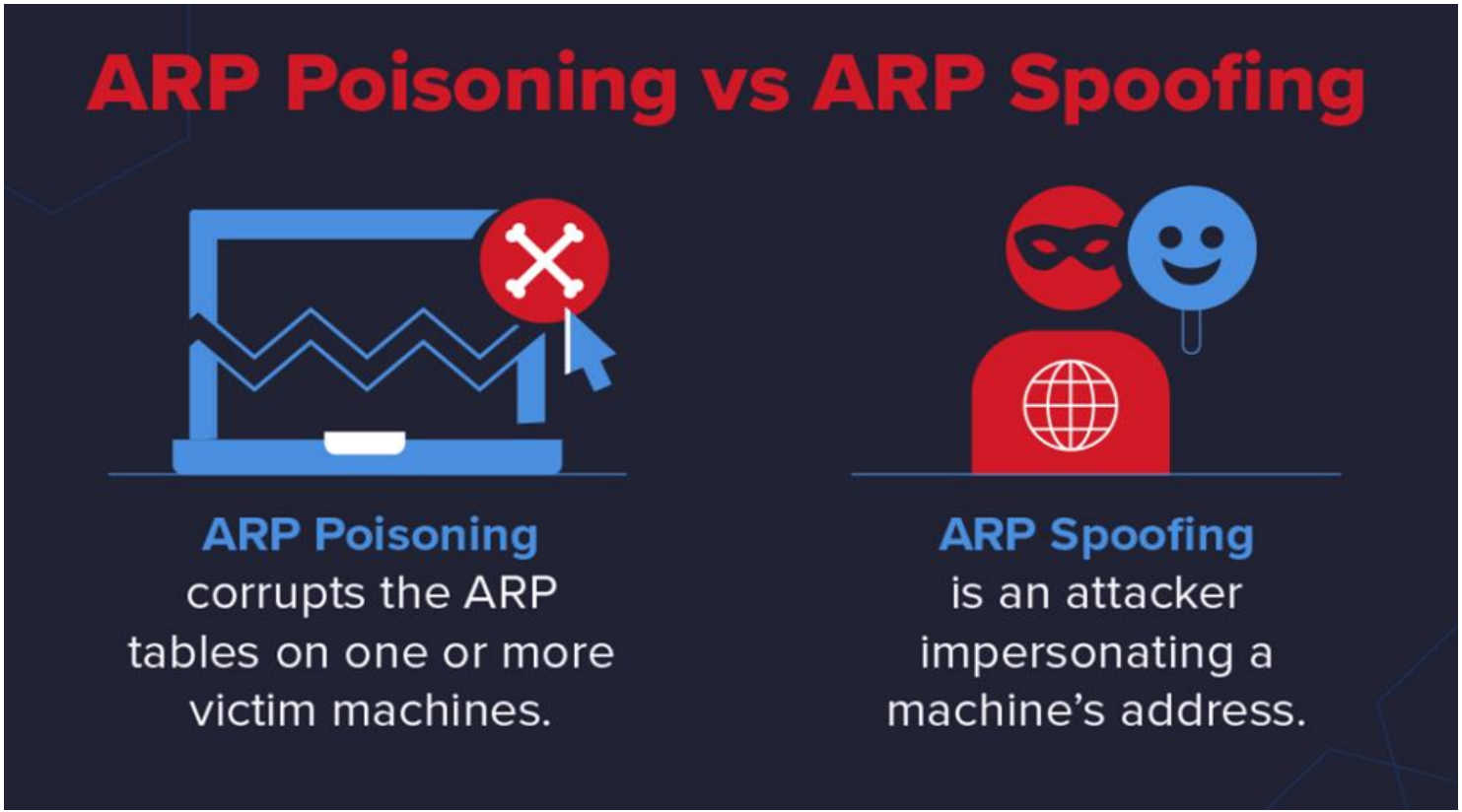
Why is ARP Spoofing possible?

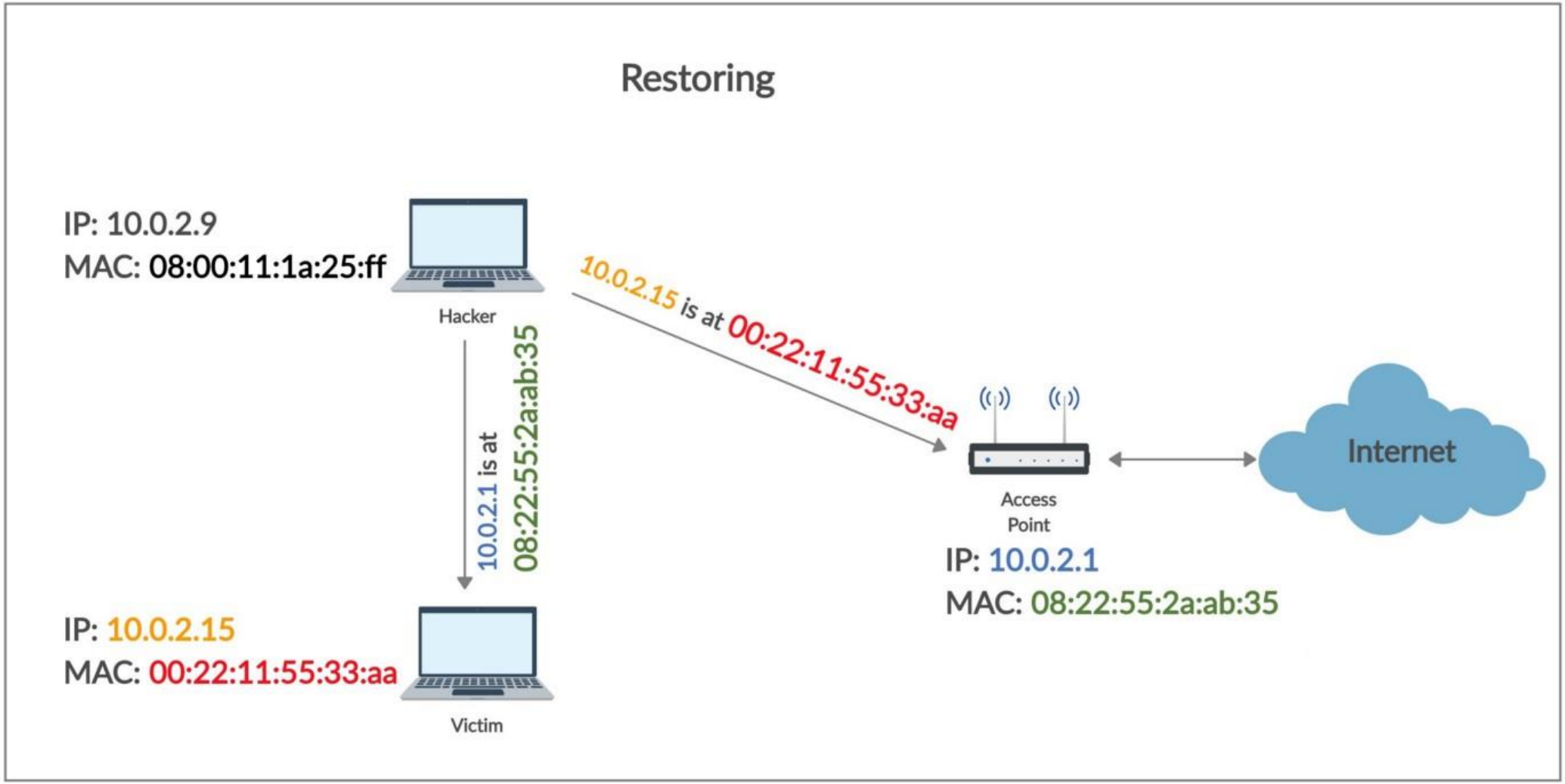
- There are two reasons why ARP spoofing is possible.
  - The machines in a network accept ARP Responses even if they haven't sent an ARP Request.
  - The machines trust these ARP Responses without any verification.

ARP spoofing and ARP cache poisoning:-

- LANs that use ARP are vulnerable to ARP spoofing, also called ARP poison routing or ARP cache poisoning.
- ARP spoofing is a device attack in which a hacker broadcasts false ARP messages over a LAN in order to link an attacker's MAC address with the IP address of a legitimate computer or server within the network. Once a link has been established, the target computer can send frames meant for the original destination to the hacker's computer first as well as any data meant for the legitimate IP address.
- ARP spoofing can seriously affect enterprises. When used in their simplest form, ARP spoofing attacks can steal sensitive information.

Poisoning vs spoofing:-




Restoring
IP: 10.0.2.9
MAC: 08:00:11:1a:25:ff
Hacker
10.0.2.15 is at 00:22:11:55:33:aa
10.0.2.1 is at 08:22:55:2a:ab:35
Internet
Access Point
IP: 10.0.2.1
MAC: 08:22:55:2a:ab:35
IP: 10.0.2.15
MAC: 00:22:11:55:33:aa
Victim

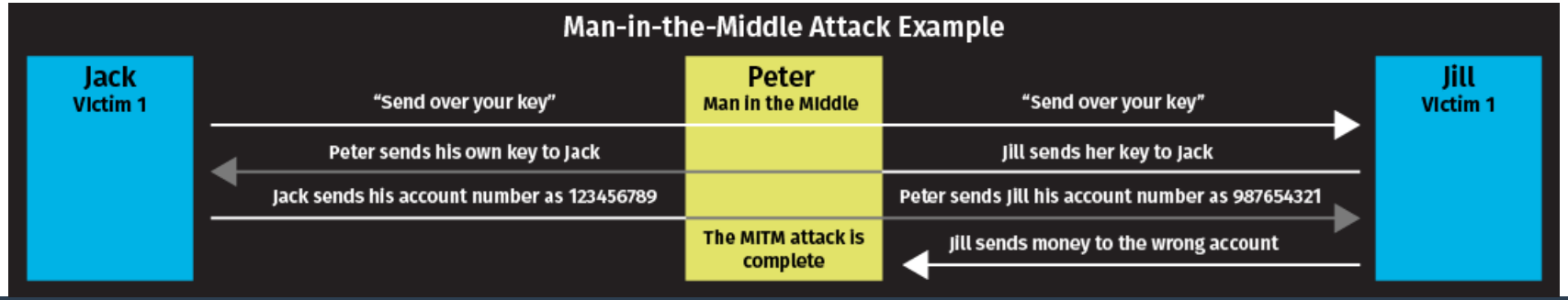
Threats:-

.Data theft like password , otp and literary all data , Modification of data.

.DNS spoofing , Website redirection.

.Cut off the internet connection and Denial of services attack .

.Hacker Gaining Access to Funds



MITM attack detection Algorithm:-

Step 1: start the program.

Step 2: get the ARP table data which contains ip,mac address.

Step 3: manually send ARP request to the ip in the arp table which helps you to get the real mac address of the particular host with that ip address.

Step 4 : cross verify the ARP table mac address with original mac address get from the ARP request. If it is equal no problem.

Step 5:else we are under attack.

Step 6:stop the program


Thanks