ARP SPOOFING / POISONING :

1. It is the kind of cyber attack where attacker fakes IP – MAC pair by using its own MAC for other legitimate device’s IP.
2. It is by default possible due to the structure of arp protocol
3. It is weak in the sense that it doesn’t provide authentication of reply messages for checking its validity and messages can be unsolicited (no need of sending request for obtaining reply)
4. ARP spoofing happens mainly for following purposes:
5. To intercept the conversation in LAN

* Attacker continuously sends ARP reply packets in network with IP of router or gateway (to listen to conversation with external network)
* Thus , devices update their arp cache with this information (since no security measures in built)
* So, all the actual transaction will now get their route towards attacker .
* To be safe, attacker usually forwards the packets to the actual destination (attacker may edit the packet by replacing the mac of the victim with spoofed dest – router ip OR it can project itself as a intermediate router with IP forwarding)
* Bi-directional ARP spoofing for interception is also possible (MAN IN THE MIDDLE ATTACK)

1. Slowing down the entire LAN

* By sending excessive fake ARP replies to the devices in LAN in unsolicited manner with non existing mac addresses for different IP’s

1. ARP spoofing is due to authentication less protocol structure and trust based implementation with both static and dynamic entries being allowed.
2. This can be avoided by using following methods :

* Deep ARP Inspection
* Limiting the arp entries
* Allowing only static arp entries for critical devices like gateway, router etc.
* Using arp detection tools
* Using IPv6 since it uses Neighbor Discovery Check protocol instead of ARP, which by default is secured.

In cisco packet tracer, it is possible to view and delete the entire ARP table. But statically giving ARP entries is not possible .

