**ARP**

**What is ARP?**

Address resolution protocol

* Resolves IP into MAC

**How does it work?**

When a client tries to send a packet to node, it will try to resolve the IP to MAC addr first

* It will look at the ARP table locally to see if it already exists there
* If it does it’ll use that MAC

If it doesn’t exist locally

* Send request to broadcast addr
* Request will say ‘who has IPADDRESS’
* Only node with that IP will respond to the ARP saying ‘I am IPADDR’
* The MAC addr of this node is loaded into the ARP table and is then used for future communications
  + Often, the node will send out these request frequently to ensure that MAC still has the same IP

**ARP Poisoning**

This is commonly used to perform MITM attacks

Since ARP will refresh its cache with what it already has in the table, the attacker can take advantage of this

* The attacker can consistently send out the ARP response ‘I ma IPofRouter’
* When the client issues the refresh by sending out requests, it will have already seen the response from the attacker and will update the ARP table with the wrong IP (poisoning)
* So any traffic sent to the router will now be sent to the attacker instead