ARP tables are simple databases that reside on routers and keep records of which devices on the network correspond to which IP address. So, for example, if the server sends out a packet onto a new network segment aimed at ComputerX, it's being sent to an IP address which has been assigned to that computer. But which physical interface does that IP address belong to? That's where the router looks up the MAC address that corresponds to that IP address, and shunts the packet there.

ARP poisoning is a kind of MITM (Man In The Middle) security attack, and requires that the attacker is on the same network segment. What they do is they set their machine up to spoof the MAC addresses of the two computers that they're attempting to spy on. They basically fool the router into thinking that their computer IS both of those machines, by registering their IP addresses to MAC addresses that it's spoofing. By "poisoning" the router's ARP table, they can then intercept all the traffic between those machines. The attacker's computer can forward the packets to their final destinations as it intercepts them, so the people on either end don't realize that they're being monitored.







