**“Regular” ARP**

The most common use of ARP is what I discussed in this article on ARP caching. That is just “regular ARP”. With ARP, your PC, let’s say, is trying to get an Ethernet MAC address for an IP address.

If you use a packet sniffer like Ethereal / Wireshark, you will see ARP requests just streaming across a production network (they are all broadcasts and go to every station).

Then, there is RARP (reverse ARP) where your PC has a MAC address and is trying to get an IP address for it. Today, RARP is pretty much obsolete because every one uses DHCP.

**Inverse ARP**

Then, you have inverse ARP (called InARP). Now, Happy Router member tuongdq posted some great information on how inverse ARP is used with Frame-Relay. This information is “spot on”. He is correct that inverse ARP can be used with frame relay. Inverse ARP can also be used with ATM. InARP is used to find the Layer 3 address from a Layer 2 address (the DLCI in frame relay). With frame, when using  
inverse ARP, you know the DLCI of the remote router but you don’t know its IP address. Inverse ARP sends a request to obtain that IP address and map it to the Layer 2 frame-relay DLCI. However, it is always recommended to disable & not use inverse ARP because your frame end points could get different IP’s if the network were to be ‘bounced’.

If you are in for some “techie” reading on these different types of ARP, you can always check out the RFC’s:

* RFC 826 – Address Resolution Protocol
* RFC 903 – Reverse Address Resolution Protocol
* RFC 2390 – Inverse Address Resolution Protocol

**Gratuitous ARP**

**Gratuitous ARP** could mean both gratuitous ARP *request* or gratuitous ARP *reply*. Gratuitous in this case means a request/reply that is not normally needed according to the ARP specification (RFC 826) but could be used in some cases. A gratuitous ARP request is an [AddressResolutionProtocol](https://wiki.wireshark.org/AddressResolutionProtocol) request packet where the source and destination IP are both set to the IP of the machine issuing the packet and the destination MAC is the broadcast address ff:ff:ff:ff:ff:ff. Ordinarily, no reply packet will occur. A gratuitous ARP reply is a reply to which no request has been made.

Gratuitous ARPs are useful for four reasons:

* They can help detect IP conflicts. When a machine receives an ARP request containing a source IP that matches its own, then it knows there is an IP conflict.
* They assist in the updating of other machines' [ARP table](https://wiki.wireshark.org/ARP%20table)s. [Clustering solutions](http://en.wikipedia.org/wiki/High-availability_cluster) utilize this when they move an IP from one NIC to another, or from one machine to another. Other machines maintain an ARP table that contains the MAC associated with an IP. When the cluster needs to move the IP to a different NIC, be it on the same machine or a different one, it reconfigures the NICs appropriately then broadcasts a gratuitous ARP reply to inform the neighboring machines about the change in MAC for the IP. Machines receiving the ARP packet then update their ARP tables with the new MAC.
* They inform switches of the MAC address of the machine on a given switch port, so that the switch knows that it should transmit packets sent to that MAC address on that switch port.
* Every time an IP interface or link goes up, the driver for that interface will typically send a gratuitous ARP to preload the ARP tables of all other local hosts. Thus, a gratuitous ARP will tell us that that host just has had a link up event, such as a link bounce, a machine just being rebooted or the user/sysadmin on that host just configuring the interface up. If we see multiple gratuitous ARPs from the same host frequently, it can be an indication of bad Ethernet hardware/cabling resulting in frequent link bounces.