

ARP, IARP, RARP, and Proxy ARP

When I first started studying for my CCNA years ago, one of the (many) things that confused me was ARP. Or rather, what ARP did as opposed to Reverse ARP, Inverse ARP, and Proxy ARP! One book would mention ARP without mentioning the other variations, one would mention RARP but not Proxy ARP, and so on...

I got through my Intro and ICND exams, but I never forgot how confusing this was to me when I started. (And we all start somewhere!) To help current CCNA candidates with this confusing topic, let's take a look at each one of these technologies.

ARP - Address Resolution Protocol

You may well know what ARP does from your networking studies or work on a LAN, but to effectively troubleshoot ARP issues on a WAN (and pass the 640-801, 640-811, and 640-821 exams!), you need to take network devices into account that may be separating the workstations in question.

The basic ARP operation is simple enough. We concentrate on IP addressing a great deal in our studies and our jobs, but it's not enough to have a destination IP address in order to send data; the transmitting device must have a destination MAC address as well.

If the sender doesn't know the MAC address of the destination, it has to get that address before data can be sent. To obtain the unknown Layer Two address when the Layer Three address is known, the sender transmits an ARP Request. This is a Layer Two broadcast, which has a destination address of ff-ff-ff-ff-ff-ff. Since Ethernet is a broadcast media, every other device on the segment will see it. However, the only device that will answer it is the device with the matching Layer Three address. That device will send an ARP Reply, unicast back to the device that sent the original ARP Request. The sender will then have a MAC address to go with the IP address and can then transmit.

There are several network devices that may be between our two hosts, and for the most part, there is no impact on ARP. Since this is Cisco, though, there's gotta be an exception! Let's take a look at how these devices impact ARP.

Repeaters and Hubs are Layer One (Physical Layer) devices, and they have no impact on ARP. A repeater's job is simply to regenerate a signal to make it stronger, and a hub is simply a multiport repeater. Therefore, neither a repeater nor a hub have impact on ARP.

Switches are Layer Two devices, so you might think they impact ARP's operation; after all, ARP deals with getting an unknown MAC address to correspond with a known IP address. While that's certainly true, switches don't impact ARP for one simple reason: Switches forward broadcasts out every port except the one it was originally received on. The ARP Reply will be unicast to the device requesting it, as with the previous example.

Now here's the exception -- a router. Routers accept broadcasts, but routers will not forward them. For example, consider a PC with the address 20.1.1.1 /16. That host assumes it's on the same physical segment as the device 20.1.2.200 /16, since their IP addresses are both on the same subnet (20.1.0.0 /16). The problem here is that a router separates the two devices, and the router will not forward the ARP broadcast.

The Cisco router will answer the ARP Request, however, with the MAC address of the router interface the ARP Request was received on. In this case, the router will respond to the ARP Request with its own E1 interface's MAC address.

When the device at 20.1.1.1 receives this ARP Response, it thinks the MAC address of 20.1.2.200 is 11-11-11-11-11-11. Therefore, the destination IP for traffic destined for the remote host will be 20.1.2.200, but the MAC destination will actually be that of the router's E1 interface.

Proxy ARP runs by default on a Cisco 2500 router, but it can be turned off at the interface level with the `no ip proxy-arp` command.

RARP and Inverse ARP

Reverse ARP is a lot simpler! RARP obtains a device's IP address when it already knows its own MAC address. (If the device doesn't know its own MAC address, you have bigger problems than RARP!) A separate device, a RARP Server, tells the device what its MAC address is in response to the RARP Request. As you can see, RARP and DHCP have a lot in common.

Inverse ARP doesn't deal with MAC or IP addresses. Inverse ARP dynamically maps local DLCIs to remote IP addresses when you configure Frame Relay. Many organizations prefer to statically create these mappings; you can turn this default behavior off with the interface-level command `no frame inverse-arp`.