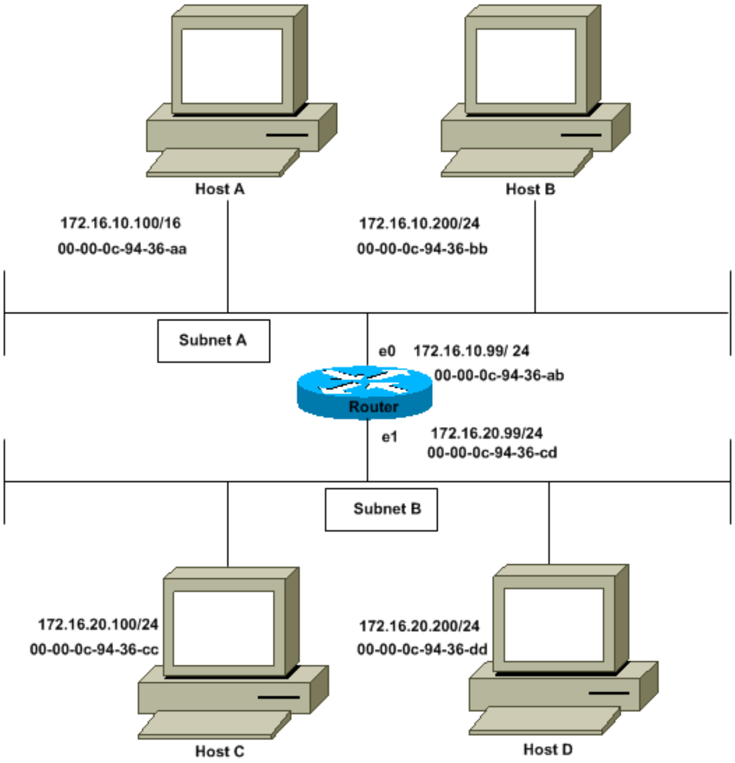
Proxy ARP

ARP (Address Resolution Protocol) is used by network systems to convert system communications from the routable layer 3 IPprotocol to the non-routable layer 2 data link layerprotocols. In most cases, you don't need to modify this behavior at all, and system communications are optimal. In special circumstances it is preferable to have another system or network device answer arp requests for another system. This process is called proxy ARP, because on network system is proxying for anothers ARP communications.

Environments that use Proxy ARP



There are few situations where proxy arp is needed, but some do arise in a networked environment. A few examples are:

- Environments which have layer 3 firewalls performing network address translation.
- Environments which have layer 2 firewalls which filter based on IP address sources and destinations.
- Some dial-in technologies where you have a concentrator forwarding packets for multiple networks behind the dial-in system.
- Environments with security devices that are designed to cleanse packet traffic before it reaches the destination.
- Environments which use bastion hosts not participating in dynamic routing protocols.

- Troubleshooting environments using network switches that have no network monitor, span, or rspan capability.

Creating Static ARP Entries

For one system to proxy arp for another, it is necessary for the administrator to create static ARP entries for the proxy system. This is a simple process. Several examples follow:

- For many Unix systems use “arp -s “.
- For Windows XP systems use “arp -s “. In older versions of windows operating systems, it was necessary for you to state that the arp entry should be “published” to make the static entry actually persistent. Keep this in mind.
- For Cisco routers running IOS use “arp arpa”.

Creating unnecessary static ARP entries, or implementing them incorrectly can cause network interruptions on a very wide scale, use them with caution.

Static ARP Entries are Important for Some Environments

It is common for hackers to use static ARP to hijack connections, reroute traffic, sniff traffic for passwords, and to perform monkey-in-the-middle attacks. These types of attacks usually cause performance issues, but may not be self evident. It is common for administrators to create static ARP entries on systems and routers for high risk systems, such as web servers. Creating static entries for those systems on the connected router can assist in preventing the attacks above. There may be an small impact on performance because of this.

Source:

http://www.tech-faq.com/proxy-arp.html