ADANAC SOFTWARE

Troubleshooting network connections with arp

By Dirk Hart

I was driving down the pike minding my own business when my cellphone rang. A friend was on vacation and one of his clients was having problems. This client has an Intelliserver, made by Computone Corp., which is one of those 'serial ports over ethernet' devices. It was having a problem that the client chronologically traced back to a thunderstorm the previous Friday.

The Intelliserver would work just fine for an hour or so then stop working for 5 or 10 minutes, then start working again. This was curious as my experience with lightning strikes involves smoke, a bad smell in the air and inert equipment. I sure don't expect lightning damaged equipment to die and resurrect itself with great frequency.

Nevertheless, I trotted over to the client site, and replaced the Intelliserver as instructed, and noted that it behaved the same as the original item. Curious indeed. Since the Intelliserver was clearly not broken I decided that this must be a network issue. After some thought I typed in *arp -a* and got a list of hostnames, IP addresses and MAC addresses:

iceberg (192.168.1.1) at 0:06:25:76:24:bd (802.3)
growler (192.168.1.2) at 0:7:e9:e0:c3:c7 (802.3)
intelliserver (192.168.1.200) at 0:06:25:74:12:05

I noted that the hostnames had come from /etc/hosts and saw that the IP addresses matched the names shown. MAC address ranges are assigned by the IEEE to electronics manufacturers to ensure that MAC addresses are globally unique. The Intelliserver claimed to be from a manufacturer identified by 00:06:25 and that there was another device on the LAN from the same manufacturer. I thought this was unlikely and used a PC to browse to http://standards.ieee.org/regauth/oui/index.shtml where I typed in 000625 and out popped Linksys Corporation. Since the manufacturer of the Intelliserver was Computone Corp., I had a strong suspicion that someone had configured a device with the same address as the Intelliserver. I re-addressed the Intelliserver and changed /etc/hosts to match .

The experience reinforced a couple of lessons. First, never, never do stuff the day before you go on vacation. Second, always, always take the time to finish the usual sysadmin housekeeping - in this case record the ip address of the router and its name in /etc/hosts.