

Re: Pure IP & ARP broadcasts

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.networking/2004-05/0150.html>

From: Phillip Windell (_at_)

Date: 05/03/04

Date: Mon, 3 May 2004 15:48:11 -0500

Hello again. You're keeping me busy :-)

That's an interesting question to me. I think a lot of people don't understand what is behind it.

You see a LAN (Ethernet) does not really communicate by IP# like many may think. It actually communicates via the MAC address of the Nics (aka Layer2 address, hardware address, ethernet address, all mean the same thing). The ARP request is what happens when the IP# is known but the MAC is not, since the MAC is required to communicate the MAC must be discovered,...that is what the ARP request does.

IP#s really only have two purposes:

- #1. Provide the mechanism for Layer3 routing. Routers make routing decisions based to the "network" portion of the IP# by comparing it to their Routing Table.
- #2. Provide the means to find the MAC address. The IP# (including the "host" portion this time) is used in the ARP request to discover the MAC address.

A host has a packet to send, it has the IP# and nothing else. It broadcasts an ARP request out onto the segment. If the owner of that IP# exists on the segment it responds with its MAC address. The sender then sends the packet to that MAC address. All done, everybody is happy.

But if the owner of the IP# is not on that segment then the Router replies with its own IP#, in other words it "lies" to the sender (aka "Proxy Arp"). The sender passes the packet to the Router's MAC address as if that was the destination. The router examine's its Routing Table using the IP# to find the proper port leading to the destination and broadcasts it own ARP request out that port and the whole process repeats again. If another Router is required then that second Router "lies" to the first Router and the whole process repeats again. This happens over and over until the broadcast hits the right segment and the "real" host responds to the ARP with its own MAC address and the packet is sent there an has finally made it "home".

Also every host (Routers, Switches, PCs, Servers) on a network keeps a small "cache" of MAC/IP# pairs. If an entry exists in this cache it will send the

microsoft.public.windows.server.networking: Re: Pure IP & ARP broadcasts

packet to that MAC address without doing an "ARP" but if the entry has expired then it must do another "ARP".

There may be a little more detail to the process than this, particularly when there are multiple routes with routers that are Default Gateway and those that aren't, I'm a little fuzzy on some of that myself. But it should give you an idea of what those ARPs are all about. They are normal, they are supposed to be there.

--

Phillip Windell [MCP, MVP, CCNA]

www.wandtv.com

"sw" <anonymous@discussions.microsoft.com> wrote in message
news:C9B80A00-3559-4F54-870D-E5BF1417F741@microsoft.com...

> Hi, I'm only using IP on my network and I have several W2K DNS servers yet
I still see quite a lot of ARP broadcasts (approx 40%). If DNS maintains a
list of all IP and Mac addresses why the need for ARP broadcasts? Am I
missing something?

>

> Many thanks