

<LONG>Re: Question rephrase

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2004-10/1094.html>

From: Moe Trin (ibuprofin_at_painkiller.example.tld)

Date: 10/28/04

Date: Wed, 27 Oct 2004 21:08:04 -0500

In article <d4f21235.0410261339.322cfff6@posting.google.com>, Iceman wrote:

> * *Problem setup*

> *You have 100 machines (Linux, Windows, MacOS, whatever...).*

No, I have 1700+.

> *one is a master, four are slaves and that any of them can become*

> *master if current master fails (thunderbolt, whatever...).*

Indeed – whatever. A `_minor_` fly in your ointment – all servers have to keep track of what addresses have been handed out, so they don't try to hand it out to some other host.

> *When any host (even one of the 5 Linuxes running the server) turns on,*

> *it tries to get it's IP. The only unique is their ethernet MAC*

> *address. So it sends MAC to FF:FF:FF:FF:FF:FF broadcast. There is*

> *currently only one master NS server, which responds. This is something*

> *like the DHCP's DISCOVER/OFFER/REQUEST/ACK protocol. OK, so now it has*

> *it's address and it can work OK.*

Yes, but to avoid a huge security hole (this host `_claims_` to be \$FOO, and is allowed to do \$BAR – how do I know it really is who it claims to be – even though authentication by IP address is but a baby step beyond no security), you really want to be handing out specific addresses to specific hosts. Here's a test for you – what is the MAC address that COMPUTER A would see when it asks itself for an IP?

> *However, if there was no NS server available, why not configure*

> *itself? Since you are yourself a NS, you are able to do it and, in the*

> *same time, become a master NS for that network.*

<http://www.ietf.org/internet-drafts/draft-ietf-zeroconf-ipv4-linklocal-17.txt>

That was "current" in early July. Microsoft has been trying to get it past the IETF for over two years. When a system can't find it's DHCP server, it reaches up it's ass and grabs an IP in the 169.254.0.0/16 block – so that sales weasels meeting in airport waiting areas can trade

p0rn and viruses without needing to know anything more than how to plug in a crossover cable. Luckily I don't have to deal with windoze, and when a computer is brought back into our facility, the first thing security does is hand it to IT for a wipe and install. We also rarely allow systems out the door.

>- *No static addresses for NS server configurations. Administrators >wouldn't need to configure anything, but a network IP, netmask and >range of IP addresses.*

Oh, so your DHCP server configures itself? I think you are totally missing a concept here. It's simple. When a computer comes into the facility, it gets a clean install, and is configured with a fixed address. Serial numbers, MAC address, location, IP address, and user information all goes into the security and network databases. The box gets put on a cart, delivered to the luser, plugged in and tested, and we're done.

>*They could say: you are a possible NS (there may be other NS servers) >for the 192.168.0.0 network with 255.255.255.0 netmask, you have a >range 192.168.0.10 - 192.168.0.100 to lease.*

Well, that's only 91 hosts, but what is the advantage?

>- *If eth0 is given such network IP, netmask and range, NS which is >joining on a network without a master could say: OK, no master, so >noone can give me the IP. Since I am a potential NS, I will become a >master on that NETWORK (so I still don't have an IP ADDRESS for my >eth0) and I will issue a client request ON THAT NETWORK again.*

Why would your servers all be down? Are they solar powered or something?

>*Since now there is a master now (itself, but why not?), it will issue an >IP for the client (itself again) and it will get a valid IP.*

Except DHCP servers can't issue an address to themselves. Because they can't talk on the net, What happens if two OR MORE of your servers boot at the same time (there was a building power outage) They all look for the DHCP server - and fine none. So, they all become "masters" and hand out the same address to themselves. Honest and true - this BOOTP/DHCP crap has been around for more than a week (try 1985), and there have been people with lots of network skills looking at it. Things really are done certain ways for a reason.

>- *No static NS addresses for clients. Clients would only join a >network and look for a NS server. No static DNS, WINS IPs or whatever*

and DNS doesn't work easily with dynamic addresses.

>- *just broadcast and you will get it from the current master NS. Many >NS possible, at any available IP on that network as they wish.*

>

>* *Cons*

>- *Some security issues may be at stake here,*

Wow, what an understatement. You have a system with nearly zero security. What happens when your baddass buddy drops by with his box, which takes over – even though you never noticed it.

>*but that's not what I am "into" right now.*

I'm sorry – but there are a few of us who are "into" that stuff. It's called the real world.

>*This is a potentially big thing in many network, so a "contra" point here.*

>- *May be slow.*

It would cost a fraction of a second. How often are you rebooting your systems?

>* *The real problem*

>*Back to my apology, I have only 2 machines (OK, it's a big story for such a "huge" network, sorry), one has WinXP/Linux (A) on it and the other WinXP (B). Static IP works just fine. I wanted to make it dynamic.*

Why? You still haven't shown any benefit for having dynamic addresses, and you don't seem to want to think about the disadvantages. Say you have five systems, and want to share the hard disks of all. How do you know which is which? The only sane way around that is to use reservations where MAC address 08:00:20:cd:44:1f will ALWAYS get address 192.168.1.11 whenever it boots – that's doable, at only a moderate increase in the setup of your DHCP server – but why bother, if it's going to get the same address from a DHCP server, just make it static and don't even HAVE the DHCP server – it's a waste of a CPU.

>*Is there a way to name 4 machines Dragon, Torpedo, Mushroom and Turtle, give their network IP, netmask and range of addresses on that network they can occupy and the system does the rest?*

Reserved addresses. This MAC `_always_` gets that IP address. Remember, TCP/IP doesn't know names divorced from IP addresses. That was a windoze NETBEUI concept, and we all know that microsoft abhors security.

>*I don't want to care about their IPs, but I want to control them enough.*

Then don't use IP. Use a non-routable protocol like NETBEUI, IPX, or Banyan Vines. You then have one box that knows this crap, and has a network connection to the IP networks and masquerades for you.

>*I want a way to fit my 4 computers (and maybe afterwards add up to 60 laptops, network printers, etc.) without caring who, when, why, ...*

>assigns IPs. I want simple server configuration. I want to be able to
>simply rip of the above 4 machines (all NS servers) and add 15 NS servers
>more. I don't want to configure them again by assigning 15 static IPs
>- that is boring, error-prone and certainly not DYNAMIC.

Then don't use IP. Use a non-routable protocol like NETBEUI, IPX, or Banyan Vines.

> More questions
>- Is my thinking bad or good? I.e. do you agree in common?

Try to guess why microsoft has invented TCP/IP to replace NETBEUI. Try to think why NOVELL switched from IPX to IP. Try to find someone who even remembers what Banyan Vines is.

>- Is there anything working in practice like this? Is Dynamic DNS what
>I am looking for? Can DHCP do the above?

Possibly.

>- If not, any ideas why not - what are the problems for it not being
>like this?

Security. You may not care - the rest of the world does.

>- How do you manage (if you do) large networks? Static DNS is also
>very demanding, as I see.

Piece of cake. The crews that are acceptance testing/configuring the new hardware can do this in their sleep. The user's boss does all the paperwork about ordering the hardware. It's delivered to the IT shop who do all the setup. The registrar (even with 1700 systems, that's a small part time job that can be done by a student intern), gets a mail with the requested hostnames (3 in case the first two chosen have already been allocated), the location, user name, serial numbers, and MAC address. He chooses an appropriate address, and sends word to the IT crew. The data gets put into the network and security files, and all is gravy.

Old guy