

Registering Self-generated IPv6 Addresses using DHCPv6



draft-wkumari-dhc-addr-notification

Who are we?

Dynamic Host Configuration
Internet-Draft
Intended status: Experimental
Expires: 29 January 2023

W. Kumari
Google, LLC
S. Krishnan
Kaloom
S. Jiang

R. Asati
Cisco Systems, Inc.
L. Colitti
Google
28 July 2022

Registering Self-generated IPv6 Addresses using DHCPv6
draft-wkumari-dhc-addr-notification-02

Why?!

Asking “have you tried turning it off and on again?” gets real old real fast...



Helpdesk

Scenario: CEO cannot print to his printer, and he's super grumpy...

- IPv4:
 - Step 1: Look in DHCP logs for 'ceo-printer-color', find address
 - Step 2: Ping address...
 - Step 3: ???
 - Step 4: Profit!
- IPv6 with SLAAC:
 - Step 1: "Have you tried turning it off and on again?"
 - Step 2: "Um... try turning it off and on again again?..."
 - Step 3: ???
 - Step 4: Post resume on monster.com

SecOps

Scenario: IDS logs show machine with IP <X> uploaded entire source tree to <https://stackoverflow.com/> on Thursday at 2:43PM

- IPv4:
 - Step 1: Look in DHCP logs for IP <X>. Find MAC address
 - Step 2: Lookup MAC address in asset database
 - Step 3: HR has a “chat” with employee
 - Step 4: Profit!
- IPv6 with SLAAC:
 - Step 1: “Um.... well, that’s not good...”
 - Step 2: “Erm.... ”
 - Step 3: ???
 - Step 4: Post resume on monster.com

“Doctor, doctor, it hurts when I do this...”?

- **Lots** of networks run SLAAC
- Many client devices don't do DHCP
- Telling operators that they are doing it wrong doesn't really end well.

Proposal

- Based on “[Registering Self-generated IPv6 Addresses in DNS using DHCPv6 - draft-ietf-dhc-addr-registration](#)”
 - This died in WGLC because of the DNS bits
 - Replacement is this, but without the DNS bits :-)
- It is “a method to **inform** a DHCPv6 server that a device has a self-generated or statically configured address.”
 - Solves the Helpdesk use-case
 - Solves the SecOps use-case
 - Allows the DHCP server to know what addresses have been “taken” and avoid them

'K, I'm sold.... but how?

- DHCPv6 ADDR-REG-NOTIFICATION Message
 - "The DHCPv6 client sends an ADDR-REG-NOTIFICATION message to inform that an IPv6 address is in use."
 - Informational DHCPv6 message
 - "Heyya! I'm using address 2001:DB8::DEAD:BEEF:17. Figured you should know..."
 - DHCP server records this information, just like it would if it had assigned it itself
 - Implementations log this, just like any other assignment
 - probably want to note it in the leases database
- Does this actually solve the SecOps problem?!
 - Weeeeell - DUID is better than nothing....
 - We also need [RFC6939 - "Client Link-Layer Address Option in DHCPv6"](#)
 - Tested with Cisco IOS XE, IETF WiFi network (Cisco WLC), ISC DHCPd, Microsoft
 - Required in RIPE-772
 - Or [RFC6221 - "Lightweight DHCPv6 Relay Agent"](#)
 - `[edit interfaces ge-0/0/0 auto-configure vlan-ranges authentication username-include]`
`user@host# set username-include mac-address`
 - chaddr supported on most BNGs, many switches.

Questions?

But why don't you just:

- Scrape this from routers & switches?
 - Fugly...
 - Wrote something to poll / screen-scrape this
 - Don't really want a management station logging in every 30 seconds
 - 'K, but Streaming Telemetry FTW!!!! Nope...
 - Tried this, did not end well:
 - `$ gnmic --file junos/rpc --dir common/ -a rtr1.pao.kumari.net [...]`
`--path "/nd6-information/ipv6/neighbors/neighbor" --mode stream`
`--stream-mode on-change`
 - IPv6 ND is very chatty: INCOMPLETE-->STALE->DELAY->PROBE->REACH
(30s)->STALE->DELAY->PROBE->REACH
 - For a switch with ~20 servers it was scrolling way faster than I could read...