

Configuring Cryptographically Generated Addresses (CGA) using DHCPv6

draft-jiang-dhc-cga-config
IETF 77, DHC WG
March 25, 2010

Sheng Jiang (Speaker)
Sam Zhongqi Xia

Requirements & Motivation (1)

- **DHCPv6 can be extended to:**

propagate to the parameters that a host needs to generate a CGA

- **Parameters needed for the generation of CGA**

- ✓ Prefix (RA or draft-xia-dhc-host-gen-id)
- ✓ Sec value (new DHCPv6 option in this draft)
- ✓ A Key Pair (Pre-configured or self generated)
- ✓ Extension Fields (not have user case currently)

Requirements & Motivation (2)

- **CGA generation can computational consumption**

Proposed new interaction: a host may send a request to ask a DHCPv6 server to help computing a CGA for it

- **Test Results of CGA Generating Time**

- Platform

- An Intel Due 2 (2.53GHz) workstation
- An laboratory implementation of CGA & SEND

- Results of average CGA generating time

- SEC=0: 100 μ s
- SEC=1: 60 ms
- SEC=2: 2000s (varies from 100~7000sec)
- SEC=3: N/A (theoretically estimating, more than 30,000 hours are required)

- Each SEC level, computational consumption is increased by 2^{16}

Comments are welcomed!

Thank You!

Sheng Jiang (shengjiang@huawei.com)
Sam (Zhongqi) Xia (xiazhongqi@huawei.com)