Port Randomization in the Network Time Protocol Version 4

(draft-gont-ntp-port-randomization)

Fernando Gont
Guillermo Gont

IETF 105
Montreal, Canada. July 20-26, 2019

Introduction

- The NTP spec (RFC5905) suggests that NTP clients employ the NTP service port (123) as the local port number
- This goes **against BCP 156** (RFC6056) on “Recommendations on Transport-Protocol Port Randomization”
- And,
  - Makes blind attacks against NTP easier
  - Hinders DDoS mitigation (one cannot easily tell NTP server vs. NTP client packets)
  - Cannot be complied with for multiple NTP clients behind a NAT
- Most NTP implementations employ port randomization (**already!**) by relying on the underlying OS to pick the client-side port

draft-gont-ntp-port-randomization

- Recommends port randomization on a per-association basis
- Formally updates RFC5905

Moving forward

- Adopt as NTP WG item?