Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Thesis B.Sc.

Thesis M.Sc.

Analysis of Aliased Prefixes in the Internet

Motivation

Our research group (GINO [4]) at the chair of network architectures and services performs active Internet-wide measurements. In the course of a previous research in our group on IPv6 hitlists, Gasser et al. [1, 2] defined the term *aliased prefix*. An *aliased prefix* is a prefix where every IP address responds to the same request, e.g., all have port TCP/80 open. For IPv6 hitlists this is a major issue as prefixes contain a huge number of possible addresses. Including all of these would make the list huge and useless.

Not only in IPv6 but also in IPv4 such prefixes can be observed but due to the limited address space and the smaller assigned prefixes, their visibility and impact is smaller.

The existence of *aliased prefixes* can have different reasons. It can be a single host managing and answering for all addresses (e.g., due to a firewall host answering to all SYN packets as a DoS protection [3]). Furthermore, there are also CDNs, e.g., Cloudflare, where we can observe *aliased prefixes* for hosted services. During the course of this work the goal is to find and classify such *aliased prefixes*. The main questions are: Where are they used and why are they used?

Your Task

- Familiarize with *aliased prefixes* and appearances in related literature
- Analyze IPv4 port scans to find evidence of *aliased prefixes*
- Evaluate the presence of these prefixes (e.g., AS, DNS resolutions)
- Develop a classification method for the prefixes (can include additional active scans)
- Analyze the historic evolution of aliased prefixes on our IPv6 measurements

Requirements

- Basic programming knowledge in Python or Go
- Familiarity with GIYF-Based work approaches

Bibliography

[1] Gasser et al. ”Scanning the IPv6 Internet: Towards a Comprehensive Hitlist.” TMA 2016.
[2] Gasser et al. ”Clusters in the expanse: Understanding and unbiasing IPv6 hitlists.” IMC 2018.
[3] Izhikevich et al. ”LZR: Identifying Unexpected Internet Services.” USENIX Security 2021.
[4] Murdock et al. ”Target Generation for Internet-wide IPv6 Scanning.” IMC 2017.
[5] https://net.in.tum.de/projects/gino/

Contact

Patrick Sattler	sattler@net.in.tum.de
Johannes Zirngibl	zirngibl@net.in.tum.de
Oliver Gasser	oliver.gasser@mpi-inf.mpg.de

http://go.mytum.de/286232