Speedtrap: Internet-Scale IPv6 Alias Resolution

Luckie, Matthew

http://hdl.handle.net/10945/36485
SPEEDTRAP: INTERNET-SCALE IPV6 ALIAS RESOLUTION

Matthew Luckie, Robert Beverly*, William Brinkmeyer*, k claffy
mjl@caida.org

CAIDA - University of California, San Diego
*Naval Postgraduate School

ACM SIGCOMM Internet Measurement Conference: Barcelona, Spain, Oct 2013
MOTIVATION

• How is the router-level structure of the IPv6 Internet evolving as IPv6 is deployed?

• Answering this question requires traceroute and alias resolution

• So far, no Internet-scale alias resolution technique for IPv6 exists

• Speedtrap is a step in this direction
  - we use IP-ID to fingerprint IPv6 routers
  - try to send the minimum number of packets given lack of counter velocity

• Related work in IPv4 (Mercator, DisCarte, RadarGun, MIDAR) does not apply
  - Common source address IPv4 hack is ruled out by IPv6 RFCs
  - All IPv6 IDs have similar offset and velocity given lack of counter movement
MONOTONIC BOUNDS TEST

(MBT, from MIDAR [ToN 2013])

- MBT suggests A and C share an IP-ID counter
- A and B do not share a counter

(a) overlapping in time
(b) not derived from same counter
OBTAINING IPV6 IP-IDS

• The IPv6 header does not include an ID field

• We exploit IPv6 fragmentation behaviour (packets are fragmented only at the source) using the ID field in the IPv6 fragmentation header

• **Too-Big-Trick:**
  
  - Send 1300B ICMP echo request.
  
  - If echo reply > 1280B, send Packet Too Big (PTB)

  - Host should respond to further echo requests with fragmented echo replies with IP-ID until Path-MTU cache entry expires (typically >= 2hrs)
DATA

(input)

- All IPv6 interfaces observed by CAIDA’s Archipelago (Ark) infrastructure for March 2013.
  - 27 VPs probed random address in each routed prefix, once per day
  - 52,986 interfaces in 2000::/3 unicast prefix observed
CHALLENGES
(and limitations)

- **32.1%** of interfaces send fragmented responses with incrementing IP-ID values.
  - 17.9% send random IP-IDs
  - 30.2% do not respond to ping
  - 19.8% appear to ignore PTB

- **Little velocity**: fragment counters start at one, increment only when a fragmented packet is sent. Routers rarely send fragmented packets

- **Large packets required**: 1300B 46x larger than equivalent packets in IPv4
SPEEDTRAP ALGORITHM

*(induce IP-ID velocity to catch aliases)*

- In absence of entropy, large packet requirement, try to infer aliases using minimum number of necessary probes.

- We use 20 PPS, but no reason not to use larger PPS

1. Determine IP-ID behaviour of interfaces

2. Solicit **sequence of non-overlapping fragments** from all interface-pairs (for MBT)

3. Distill candidate routers, **force distinct shared counters to diverge**

4. Pair-wise testing of candidate routers to confirm
SPEEDTRAP ALGORITHM

(step 2: solicit non-overlapping sequence)

• Break step 2 into three rounds. Each round solicits a single fragmented response from each interface.

1. Solicit response from all incrementing interfaces, in parallel

2. Probe interfaces which had overlapping samples in step one separately. Probe groups in parallel.

3. Solicit response from all incrementing interfaces, in parallel

• Product is sequence of non-overlapping responses for MBT
SPEEDTRAP ALGORITHM

(step 2: solicit non-overlapping sequence, round 2)

Interfaces

Group #1: A–F
B–F tx’d before A rx’d

Group #1
A–F

Group #2
G–K

Time overlap between F, G, H

Group #3
L–P
# PACKETS AND TIME

*(for 52,986 addresses at 20pps)*

<table>
<thead>
<tr>
<th>Step</th>
<th>Packets</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IPID behaviour</td>
<td>317,814</td>
</tr>
<tr>
<td>2</td>
<td>Non-overlapping sequence</td>
<td>80,017</td>
</tr>
<tr>
<td>3</td>
<td>Distill candidate routers</td>
<td>34,659</td>
</tr>
<tr>
<td>4</td>
<td>Pair-wise testing</td>
<td>63,765</td>
</tr>
<tr>
<td>Total:</td>
<td>496,255</td>
<td>9:08:10</td>
</tr>
</tbody>
</table>

---

The table above lists the steps involved in the process, along with the number of packets and the corresponding time taken for each step. The total number of packets is 496,255, and the total time is 9 hours and 8 minutes and 10 seconds.
ALIASES PER ROUTER

CCDF

Aliases per router
## VALIDATION

(2% of inferred routers validated)

<table>
<thead>
<tr>
<th>Validation name</th>
<th>STP-1</th>
<th>STP-2</th>
<th>AP</th>
<th>Tier1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RANCID</td>
<td>DNS</td>
<td>DNS</td>
<td>DNS</td>
</tr>
<tr>
<td>Data source</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Routers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incrementing IPID</td>
<td>43</td>
<td>40</td>
<td>86</td>
<td>50</td>
</tr>
<tr>
<td>Random IPID</td>
<td>43</td>
<td>85</td>
<td>98</td>
<td></td>
</tr>
<tr>
<td>No Fragments</td>
<td>11</td>
<td>84</td>
<td>77</td>
<td></td>
</tr>
<tr>
<td>No Echo Replies</td>
<td></td>
<td>8</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>Mixed</td>
<td></td>
<td>4</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Total Routers</td>
<td>70</td>
<td>94</td>
<td>267</td>
<td>239</td>
</tr>
<tr>
<td>Interfaces</td>
<td>151/750</td>
<td>85/279</td>
<td>138/1008</td>
<td>79/625</td>
</tr>
<tr>
<td>Correct</td>
<td>150/151</td>
<td>85/85</td>
<td>137/138</td>
<td>79/79</td>
</tr>
</tbody>
</table>
SUMMARY

• We developed and validated an Internet-scale IPv6 alias resolution technique

• **Code freely available**
  
  - http://www.caida.org/tools/measurement/scamper/
  
  - man sc_speedtrap

• Also in paper:
  
  - tomography of where PTBs might be filtered, allowing more aliases to be resolved
  
  - evaluation of scalability
PMTU CACHE

(how long will routers fragment packets?)

CDF

0 1 hour 2 hours 3 hours 4 hours

0 0.2 0.4 0.6 0.8 1
PPS RATE

(are we limited by PPS rate or algorithm?)
RELATED WORK

(IPv4 fingerprinting techniques, $O(N^2)$)

• N. Spring, R. Mahajan, D. Wetherall, “Measuring ISP topologies with Rocketfuel”, ACM SIGCOMM 2002

RELATED WORK
(Scalable IPv4 fingerprinting techniques)


- A. Bender, R. Sherwood, N. Spring, “Fixing Ally’s growing pains with velocity modeling”, ACM SIGCOMM IMC 2008


Mercator:
Common Source Address in ICMP Port Unreachables

DisCarte:
Analytical + Record Route

RadarGun:
Probe addresses in M rounds.
Two addresses are aliases if they produce a linear timeseries and the timeseries are within a threshold

MIDAR:
Probe N addresses in a sliding window according to IP-ID velocity.
Two addresses are aliases if they pass Monotonic Bounds Test (MBT)