Using Global Measurements to Understand the Evolution of the Internet

Vaibhav Bajpai and Jürgen Schönwälder*

Computer Science, Jacobs University Bremen, Germany
{v.bajpai,j.schoenwaelder}@jacobs-university.de

Abstract. The abstract should summarize the contents of the paper and should contain at least 70 and at most 150 words. It should be written using the *abstract* environment.

1 Research Statement

In the past, we performed an experimental evaluation of IPv6 transitioning technologies to identify how well current applications and protocols interoperate in such a deployement scenario [1].

2 Related Work

An interest to understand the evolution of the Internet from the user' vantage point started with establishing techniques to remotely probe the broadband links. Dischinger *et al.* in [3] for instance, inject packet trains and use the responses received from gateway to infer the broadband link characteristics. This led to development of a number of software-based solutions, `netalyzr` [12], for instance, that requires explicit interactions with the broadband consumer. Recently, the requirement for accurate measurements, coupled with Federal Communications Commission (FCC)' initiated efforts to define data-driven standards has led to the deployment of a number of large-scale measurement platforms that perform measurements using dedicated hardware probes not only from within the ISP' network but also directly from the home gateway.

SamKnows [1] specializes in such measurements to study the performance of broadband access networks. It functions by deploying dedicated hardware probes in the home gateway, that perform active measurements when the user is less aggresively using the network. In a recent study, sponsered by the FCC, Sundaresan *et al.* [13] have used this measurement data to investigate the throughput and latency of access network links across multiple ISP's. in the United States. They have coupled this data with their own Bismark platform [14] to investigate different traffic shaping policies enforced by the ISP and understand the

* This work was supported by the European Community's Seventh Framework Programme (FP7/2007-2013) grant no. 317647 (Leone)

[1] `http://www.samknows.com`

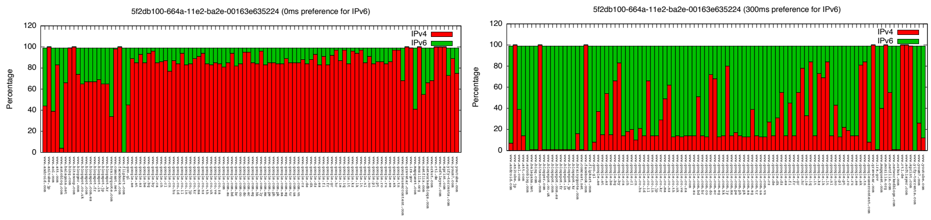

Fig. 1. IPv4 and IPv6 Happy Eyeball Competition

bufferbloat phenomenon [7]. The empirical findings of this study has recently been repraised by Canadi *et al.* in [2] where they use crowdsourced data from `speedtest.net` to compare both results.

Ripe Atlas [2] is another independent measurement infrastructure deployed by RIPE Network Coordination Centre (RIPE NCC). It consists of thousands of probes distributed around the globe that perform round-trip time (RTT) and traceroute measurements to a number of preconfigured destinations alongside DNS queries to root DNS servers.

Measurement Lab (M-Lab) [5] is an open, distributed platform to deploy internet measurement tools and the resulting measurement data on Google' storage infrastructure. The tools vary from measuring TCP throughput and available bandwidth to emulating clients to identify end-user traffic differentiation policies [4, 10] to performing reverse traceroute lookups from arbitrary destinations [11]. All of the collected data is available in the public domain.

3 Preliminary Results

A dual-stacked user when attempting to connect to a dual-stacked service traditionally prefers connecting over IPv6. This is because in POSIX systems, the internal domain name resolution system call `getaddrinfo(...)` [8] returns the list of addresses in an order that prioritizes an IPv6-upgrade path [15]. The dictated order can dramatically reduce the application responsiveness in situations where IPv6 connectivity is broken. This is because, the attempt to connect over an IPv4 address will take place only when the IPv6 connection attempt has timed out, which can be in the order of seconds.

This noticeable degraded user experience can be subverted by making applications apply the happy eyeballs algorithm [16]. The algorithm recommends that a dual-stacked application try resolving a dual-stacked service for both IPv4 and IPv6 addresses at once. If the resolver returns both addresses, the application must try a TCP `connect(...)` to both the resolved addresses and pick the one that completes first.

In this pursuit, to determine whether applications will use IPv4 or IPv6 on a dual stacked service, we developed `happy`, a simple TCP happy eyeballs probing

[2] `https://atlas.ripe.net`

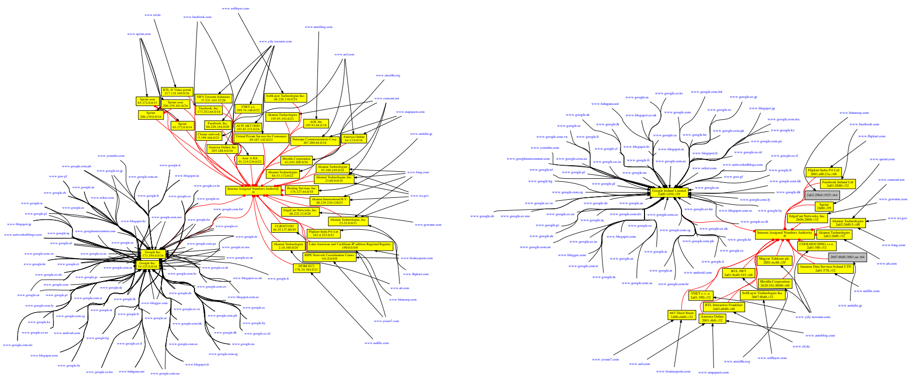

Fig. 2. IPv4 and IPv6 aggregation cloud

tool. It uses non-blocking `connect(...)` calls to establish concurrent connections to a number of possible endpoints of a service. The tool, however, does not check whether the endpoints of a given target all provide the same service. Hence, it is possible to impact the results by setting up fake servers that do not provide the service tested and which are designed and deployed with the only purpose to provide fast connection setup times.

We have cross-compiled `happy` for the OpenWRT [3] platform. As a result, the tool can now be run on widely deployed SamKnows probes [4], and the collected measurement data can be further analysed. In order to ascertain the value in this exercise, we prepared an internal test-bed of multiple measurement points. The measurement points have different flavors of IPv4 and IPv6 connectivity ranging from native IPv4, native IPv6, IPv6 tunnel broker endpoints [6], Teredo [9] and tunnelled IPv4. We used the top 100 domains compiled by Hurricane Electric Internet Services [5] and ran `happy` on the set of dual-stack services represented by these domains.

A preliminary result comparing the preference of a happy-eyeballed application to IPv6 and IPv4 from one of our measurement points is shown in Fig. 1. The measurement point represented in this plot is located at Braunschweig and has a native IPv4 and a IPv6 connection through the German Research Network [6]. The initial results show that happy eyeballs prevents IPv6 access to Facebook, with only a 20% chance to get to Google related services over IPv6. The plot looks very different if IPv6 endpoints are allowed a 300ms chance to succeed, but even then it appears the application will prefer to use IPv4 when reaching more popular web services. In addition, it appears, some of the related (and few of the unrelated) services show similar preferences. These services either resolve to the

[3] `https://openwrt.org`
[4] `http://www.samknows.com`
[5] `http://bgp.he.net/ipv6-progress-report.cgi`
[6] `http://www.dfn.de`

same endpoint or a set of endpoints that belong to an allocated block. Digging through the `whois` information for each of the endpoints from their Regional Internet Registry (RIR) seems to indicate that major portion of the services map to a cloud of an address block owned by popular organizations like Google and Akamai Technologies as shown in Fig. 2.

4 Conclusion

In our preliminary study, we have witnessed that a major portion of the services in practicality centralize either on core content delivery networks or major cloud platforms. We want to investigate this effect in more detail and understand to what extend does this network aggregation and the eventual user experience depend on the localization information. We want to take this further by comparing the performance of IPv6 with respect to IPv4 and not only define IPv6 related metrics but also identify Carrier-Grade NAT (CGN)s and/or several layers of Network Address Translation (NAT)s enforced by the ISP on the home gateway.

References

1. Bajpai, V., Melnikov, N., Sehgal, A., Schönwälder, J.: Flow-Based Identification of Failures Caused by IPv6 Transition Mechanisms. In: Proceedings of the 6th IFIP WG 6.6 International Autonomous Infrastructure, Management, and Security Conference on Dependable Networks and Services. pp. 139–150. AIMS'12, Springer-Verlag, Berlin, Heidelberg (2012), `http://dx.doi.org/10.1007/978-3-642-30633-4_19`
2. Canadi, I., Barford, P., Sommers, J.: Revisiting broadband performance. In: Proceedings of the 2012 ACM conference on Internet measurement conference. pp. 273–286. IMC '12, ACM, New York, NY, USA (2012), `http://doi.acm.org/10.1145/2398776.2398805`
3. Dischinger, M., Haeberlen, A., Gummadi, K.P., Saroiu, S.: Characterizing Residential Broadband Networks. In: Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement. pp. 43–56. IMC '07, ACM, New York, NY, USA (2007), `http://doi.acm.org/10.1145/1298306.1298313`
4. Dischinger, M., Marcon, M., Guha, S., Gummadi, K.P., Mahajan, R., Saroiu, S.: Glasnost: Enabling End Users to Detect Traffic Differentiation. In: Proceedings of the 7th USENIX Conference on Networked Systems Design and Implementation. pp. 27–27. NSDI'10, USENIX Association, Berkeley, CA, USA (2010), `http://dl.acm.org/citation.cfm?id=1855711.1855738`
5. Dovrolis, C., Gummadi, K., Kuzmanovic, A., Meinrath, S.D.: Measurement Lab: Overview and an Invitation to the Research Community. SIGCOMM Computer Communications Review 40(3), 53–56 (Jun 2010), `http://doi.acm.org/10.1145/1823844.1823853`
6. Durand, A., Fasano, P., Guardini, I., Lento, D.: IPv6 Tunnel Broker. RFC 3053 (Informational) (Jan 2001), `http://www.ietf.org/rfc/rfc3053.txt`
7. Gettys, J., Nichols, K.: Bufferbloat: Dark Buffers in the Internet. Communications of the ACM 55(1), 57–65 (Jan 2012), `http://doi.acm.org/10.1145/2063176.2063196`

8. Gilligan, R., Thomson, S., Bound, J., McCann, J., Stevens, W.: Basic Socket Interface Extensions for IPv6. RFC 3493 (Informational) (Feb 2003), http://www.ietf.org/rfc/rfc3493.txt
9. Huitema, C.: Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs). RFC 4380 (Proposed Standard) (Feb 2006), http://www.ietf.org/rfc/rfc4380.txt, updated by RFCs 5991, 6081
10. Kanuparthy, P., Dovrolis, C.: ShaperProbe: End-to-End Detection of ISP Traffic Shaping using Active Methods. In: Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference. pp. 473–482. IMC '11, ACM, New York, NY, USA (2011), http://doi.acm.org/10.1145/2068816.2068860
11. Katz-Bassett, E., Madhyastha, H.V., Adhikari, V.K., Scott, C., Sherry, J., Van Wesep, P., Anderson, T., Krishnamurthy, A.: Reverse Traceroute. In: Proceedings of the 7th USENIX Conference on Networked Systems Design and Implementation. pp. 15–15. NSDI'10, USENIX Association, Berkeley, CA, USA (2010), http://dl.acm.org/citation.cfm?id=1855711.1855726
12. Kreibich, C., Weaver, N., Nechaev, B., Paxson, V.: Netalyzr: Illuminating the Edge Network. In: Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement. pp. 246–259. IMC '10, ACM, New York, NY, USA (2010), http://doi.acm.org/10.1145/1879141.1879173
13. Sundaresan, S., de Donato, W., Feamster, N., Teixeira, R., Crawford, S., Pescapè, A.: Broadband Internet Performance: A View from the Gateway. In: Proceedings of the ACM SIGCOMM 2011 Conference. pp. 134–145. SIGCOMM '11, ACM, New York, NY, USA (2011), http://doi.acm.org/10.1145/2018436.2018452
14. Sundaresan, S., de Donato, W., Feamster, N., Teixeira, R., Crawford, S., Pescapè, A.: Measuring Home Broadband Performance. Communications of the ACM 55(11), 100–109 (Nov 2012), http://doi.acm.org/10.1145/2366316.2366337
15. Thaler, D., Draves, R., Matsumoto, A., Chown, T.: Default Address Selection for Internet Protocol Version 6 (IPv6). RFC 6724 (Proposed Standard) (Sep 2012), http://www.ietf.org/rfc/rfc6724.txt
16. Wing, D., Yourtchenko, A.: Happy Eyeballs: Success with Dual-Stack Hosts. RFC 6555 (Proposed Standard) (Apr 2012), http://www.ietf.org/rfc/rfc6555.txt