Consolidated Review of
Understanding IPv6 Background Radiation

1. Strengths

This paper presents a comprehensive longitudinal study of IPv6 background radiation: a four month study of five large /12 prefixes. The authors conduct a meticulous study using telescopes configured with covering BGP IPv6 prefixes. This is the largest study to date.

Additionally they compare the IPv6 telescope data to IPv4 telescope data during the same period to validate their results.

The paper presents the first large and long running study of the IPv6 internet space. The paper does a comprehensive study of the background traffic along several dimensions. It makes several interesting observations:

- The IPv6 addresses space is relatively unstable, with fewer peering points and more withdrawals.
- They found misconfigurations were common, some prefixes were not well routed even though they were allocated.
- The malicious activity in the IPv6 is almost negligible currently.

2. Weaknesses

Very little was done with the data. Identifying that a phenomenon was probably caused by a misconfiguration is much less informative than identifying the actual misconfiguration.

The results and analysis is pretty straight forward. The paper mainly reports (albeit well) what was observed on the network traffic without providing any secondary or deeper analysis of the observed behaviors.

There is not yet that much to see or to expect from IPv6. Therefore the paper at times feels like too much in too much depth rather than sticking to the exciting parts of the data.

Many of the results are superficial observations such as the fraction of traffic destined for different ports, and the fact that this often differs from IPv4. However, there is minimal attempt to explain why this may be the case, and almost no attempt to test these hypotheses. For example, why are DNS and ICMP so much more prevalent in IPv6?

3. Comments

The writing consists of statistic after statistic in sections 4 and 5. One thing that may help make these sections more readable is to include summaries of key measurement results, i.e., those that are the most surprising.

The paper suffers from a lack of key takeaways. It would really help to see the authors discuss takeaways that have operational implications: e.g., can traffic characteristics you report, e.g., ports and protocols, help with more accurate configuration of unwanted traffic filters? Are there similar takeaways from temporal analysis?

While the authors don't point out implications, it does seem that there are important consequences for routing configuration and end-to-end routing availability in section 5.

The paper does not provide explanations for some of the key observations. For example, one observation that really struck is the much higher level of routing instability in IPv6. Is this due to routing misconfiguration? If so, I'm amazed that such misconfigurations should happen at a much higher rate for IPv6. Is there some other reason for this?

The ability of this data to identify misconfigurations is very appealing. The paper would be vastly improved if the authors had identified several cases of misconfiguration, and then contacted the operators concerned to identify the actual misconfiguration. That would help other operators to avoid this problem, and given other researchers insight into the probably causes of anomalies that they may observe.

4. Summary from PC Discussion

The paper was discussed extensively and was accepted in the end on the merit of the topic under consideration and the breadth of the analysis.

Suggestions for improvement: The PC would really like to see some more depth to the analysis. Please delve into the details of the background radiation you see and give explanations as to where the traffic may be arising from.

Strengths:

- Interesting and comprehensive data set
- First look at IPv6 background radiation.
- Comparison to IPv4 was interesting.

Weaknesses:

- Very little depth to the analysis; most observations are left at a fairly superficial level.
- Results are generally expected and unsurprising; not much going on in IPv6.

5. Authors' Response

We are grateful for the reviewers' many suggestions and feedback. For the camera-ready submission, we worked hard to address the two major criticisms of this work from the reviewers, namely:

- a better summary of key measurement results
- additional analysis explaining the sources of traffic in our study

Specifically, we:

- provided additional explanations and summaries pervasively throughout the text to better highlight key results. This is most evident in Sections 4 and 5 and in the key contributions that appear in a bulleted form at the end of the introduction.

- expanded discussion of why we see higher routing instability in IPv6. Briefly, this is due to lower network connectivity in IPv6 compared to IPv4. These changes appear in Sections 5.1.2 and 5.1.3.

- better explored in Section 4.5 why ports and protocols in IPv6 differ from v4. Briefly, there is less pollution from malicious activity. Rather, we see mostly ICMPv6 traffic from testing, research purposes, probing, and misconfiguration.

- sections 4 and 5 have been reorganized to better highlight the causes of misconfiguration. These causes are explained broadly via the breakdown of the observed traffic into four categories: dark (UU), allocated routed (AR), allocated unrouted (AU) and unallocated routed (UR). Additional analysis in each of the new subsections identified misconfigured heavy hitters. We are now able to explain 72% of the packets we captured and narrowly characterize another 5%.

- contacted five operators and received confirmation of misconfiguration from two and experimental traffic from three others; we discuss these in section 5. For example, one of the main reasons of high DNS traffic was a misconfigured DNS resolver from a large hosting provider that was using allocated but unrouted IP address to make outbound queries, whose responses we got. This misconfiguration accounted for approximately 10% of all packets we captured and the misconfiguration has now been remediated.

- corrected numerous, minor grammar and formatting issues throughout the text.