

IPv6 DNS Whitelisting - Could It Hinder IPv6 Adoption?

Prepared by:

- John Brzozowski, Comcast
- Chris Griffiths, Comcast
- Tom Klieber, Comcast
- Yiu Lee, Comcast
- Jason Livingood, Comcast
- Rich Woundy, Comcast

What is DNS Whitelisting?

On the public Internet today, when using IPv4 addresses, a resolver can query and receive IPv4 Address Resource Records (A RRs) from an authoritative nameserver. When an authoritative DNS administrator adds IPv6 Address Resource Records (AAAA RRs) to a given zone, it is expected behavior that those AAAA RRs would be available to any resolver, in the same manner as A RRs and other RRs.

However, many large content providers are concerned that users have "broken" IPv6 connectivity. No data has yet been shared with or is available to the community that provides details on how "broken" is defined (see "Lack of Data" section below). As a result, ISPs and other networks (enterprises, universities, etc.) have no information about any potential IPv6 problems, which in turn is preventing discovery of a solution. As a result of this concern over "broken" IPv6 connectivity, large content providers have started to implement a system of so-called DNS Whitelisting, whereby unless your resolver's IP address is added to a privileged whitelist then your resolver will never receive AAAA responses, despite the fact that these exist for a given zone and that other networks may have access to those AAAA RRs.

Challenges:

This could result in a two-tiered public IPv6-based Internet, segregated into those who have been added to privileged whitelists of large content providers and those who have not. In addition, the process of an operator requesting that their resolvers are added to a given whitelist, addressing any objections raised to complete the whitelisting, verifying successful whitelisting, successfully maintaining whitelisted status, and working to be re-whitelisted (in the case of de-whitelisting) *does not scale well* across the millions of domains and autonomous networks across the Internet. It is clear that advertising content and services via DNS using AAAA RRs is critical to the deployment of IPv6. Thus, it is highly likely that if such a system of whitelisting took hold as a common practice, that IPv6 deployment and adoption could be *significantly* impaired in the long run.

We have heard of two possible approaches to DNS whitelisting: one where each content provider uses their own DNS whitelist, and another where a central, Internet-wide whitelist is employed. In the case of one being used by each content provider, this creates a vast permutation of differing whitelisting and de-whitelisting policies, whitelisting contacts, prerequisites, requirements, etc. In the case of one central whitelist being used across the public Internet as a whole, there could be concerns surrounding how and by whom such lists will be securely distributed, what organization will approve whitelisting, policies surrounding whitelisting and de-whitelisting, and the process for managing appeals. In addition, both whitelisting implementation approaches are likely to face a variety of challenges (potentially including legal challenge), which may further delay either implementation approach.

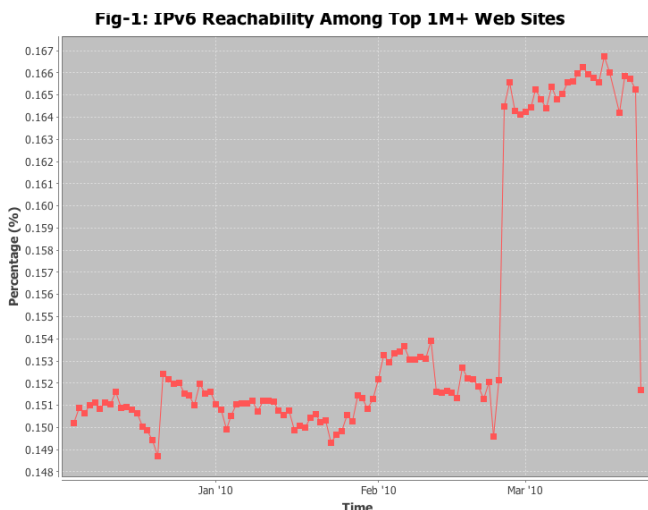
IPv6 DNS Whitelisting - Could It Hinder IPv6 Adoption?

Lack of Data:

Content providers are starting to use this DNS whitelisting system based upon data, which has not been shared with the Internet community. It is essential, if a problem does exist, for information about that problem to be openly and widely shared and discussed. Otherwise, it is not possible to justify such a system, and the motivations for whitelisting, as well as decision-making concerning whitelisting and de-whitelisting, could be considered arbitrary. Thus, agreement on the nature and scope of the problem is a key first step. We believe ISPs and content providers can partner with others in the Internet community to collect such data.

Real-World Example of These Challenges:

The chart below shows an example from the Comcast network during the week of IETF 77 (March 21 – March 26, 2010). *Source: <http://ipv6monitor.comcast.net>*



We measure the percentage of the top 1M websites on the Alexa list, which are accessible via IPv6 from our network. The image shows a single large content provider whitelisting the majority of Comcast's resolvers, shown with the red line going up, to a point in time with coverage of roughly 10M Internet users. Due to a small number of problem reports, these resolvers were de-whitelisted, shown in the drop in IPv6-accessible sites on that chart (from ~1,660 to ~1,500).

Specific details of the problem reports were not available prior to de-whitelisting. When these problems were detected, there was no opportunity for Comcast to jointly troubleshoot any possible issues prior to de-whitelisting. During the approximate six-week period of time where Comcast's recursive name servers were whitelisted, Comcast did not observe any noticeable increase in call center volumes or trouble reports.

There has also been no articulated basis or timing for being fully re-whitelisted. The most recent information we now have indicates that de-whitelisting of DNS servers covering ~10M users *may* have been based on a report from a single individual.

Given this experience, we have concerns over how whitelisting and de-whitelisting would work in practice, whether it would scale well, how this would be managed by ISPs around the world, and whether it would lead ISPs to consider delaying native IPv6 deployments.

IPv6 DNS Whitelisting - Could It Hinder IPv6 Adoption?

Other Solutions Should Be Considered:

After the problem has been documented and understood, ISPs, and Comcast in particular, are eager to work with content providers to develop tools with which to identify any "broken" users. ISPs are uniquely equipped, based on their relationship with their connected customers, to remediate any potential network issues. One statistic which was shared by Yahoo at IETF-77 (in the DNSOPS WG), claims that 0.078% of users are "broken." That is a trivial percentage of users to most ISPs. For example, in the Comcast network, this represents fewer than 12,000 users. If the problem could be solved with a new home gateway device, to use one possible example, Comcast could rapidly ship replacement devices to affected users. *We believe, given the small number claimed, that most ISPs could rapidly solve this problem (if it can be precisely defined) on their own, without content providers having to resort to DNS whitelisting.*

In addition to relying upon ISPs to serve in their traditional role of working with their customers to solve connectivity problems, it is also conceivable there may well be other solutions that should be performed in parallel. Depending upon the problem definition, these may include approaches such as OS patches, web browser patches, etc. As a result, it is important to begin with an agreement on what the problem is prior to determining solutions.

An ISP's Viewpoint:

In the IPv4 public Internet today, content providers do not block users from accessing their content if a small number of the other users on their particular ISP exhibit "broken" or impaired IPv4 connectivity. It has always been the responsibility of end users to properly configure their hosts, with support from their ISP. As such, we are not aware of content providers engaging in wholesale blocking of an ISP and the ISP's customers from accessing their content, except when a malicious attack of some significance is underway (and such blocking is usually much more targeted - possibly down to the single IP-address level). So one might fairly ask why this should change in an IPv6-based Internet.

In addition, ISPs could be concerned that when users are blocked from accessing content via IPv6, they will contact the ISP to complain (rather than the content provider which made the decision), thereby increasing customer support costs, decreasing customer satisfaction rates, and potentially negatively affecting the number of subscribers on the ISP network. Thus, ISPs are likely to bear an undue burden of costs relating to the side effects of DNS whitelisting.

As indicated above, we see a role for ISPs in collaborating with content providers to detect and identify users with IPv6 problems. Then, ISPs can play their traditional role in assisting users in configuring working connectivity to the Internet.

Leading By Example - Our Plans and Thoughts On How to Proceed:

Engagement: We have attempted to engage proponents of DNS whitelisting in discussion on relevant IETF mailing lists, in an attempt to define each of the following, on a step-by-step basis:

1. Definition: Define the problem
2. Measurement: Determine how to detect and measure the problem, and identify affected users
3. Scope: Determine the scale or scope the problem following measurement
4. Solutions: Develop a list of possible solutions and then act to implement these solutions

IPv6 DNS Whitelisting - Could It Hinder IPv6 Adoption?

Definition: Based on this (very recent) list discussion, we believe that problems may be caused by use of certain implementations and/or end user configurations of 6to4 and Teredo transition mechanisms. This can conspire to cause an end user to have either markedly slower access to a web site when a AAAA RR was found, or even a lack of reachability when a AAAA RR was found.

Measurement: Comcast is developing JavaScript and other data analysis tools which could be used on a website to detect the above-noted condition. Once ready, we will make these tools freely and openly available for comment and re-use by the Internet community. We will also quickly share with the Internet community what statistics we gather as a result of this, and will further attempt to show these statistics on our Comcast IPv6 Information Center's website (<http://www.comcast6.net>).

Comcast's Policy on Whitelisting of Our Domains:

As a matter of policy, Comcast has no plans to perform DNS whitelisting for any of the thousands of domains we own. When we publish AAAA RRs, it will be available to anyone on the public Internet, just as with our A records and other RRs. We plan to begin publishing AAAA RRs on selected sites no later than the end of May 2010.

Encouraging Industry Action:

As with the recent Digital TV transition in the U.S., we should not underestimate the power of consumer awareness campaigns. For example, if a good web-based mechanism is developed to detect a problem condition and recommends a user take some action, such as contacting their ISP, then such a mechanism could be deployed across ISP websites, content provider websites, regulator websites, and trade association websites. As such, an awareness campaign could be used to find affected users, communicate with them, and motivate them to help solve any underlying technical problems that will cause IPv6 transition problems. Comcast is happy to work with other key players to coordinate such an effort across the Internet community and we feel this is a key area in which ISOC and other organizations can add value.