



IETF 81

v6ops Meeting

IPv6 DNS Whitelisting



DNS Whitelisting

I-D: [draft-ietf-v6ops-v6-aaaa-whitelisting-implications-06](#)

- Updated since WGLC based on changes requested in IESG review
- These included reorganizing some sections of the document and making other changes
- As a result, it is appropriate to bring this back to the WG for review
- There are a few open questions for the WG to resolve (see the following slides)

Section 2 & 5.1 – Universal Deployment

- Universal deployment is mentioned as an possible was of deploying, in addition to ad hoc.
- However, the document makes clear universal deployment is unlikely.
- One IESG member requested text in 5.1 that this is “harmful” but another IESG member took issue with that.
- Options:
 - Leave universal as a possible option *but* work with the IESG to come up with more agreeable text.
 - Remove Section 5.1 and only say that universal deployment, while possible, is so unlikely that it is not explored in the I-D (as a minor update to the relevant paragraph in Section 2).
 - ...or something else?

Section 3.2 – Similarities to DNS Load Balancing

- This section currently contains text that includes this sentence:
 - *However, what is different is that in this case the resolvers are not deliberately blocked from receiving DNS responses containing an entire class of addresses; this load balancing function strives to perform a content location-improvement function and not an access control function.*
- Concerns have been raised regarding this text. What would the WG like to do?
 - Keep it as-is
 - Delete the sentence
 - ...something else?

Section 4 – Motivations

- Volume-based concerns (recently added, Section 4.1) and IPv6-related impairments (Section 4.2) are listed.
 - This is an important section as it makes clear that this is not just about IPv6-related impairment.
 - Volume
 - And the stability & process/procedure/monitoring maturity that follows from volume over time
 - Is this addition okay? Are there more major categories to add?
- Section 4.3 was added at the suggestion of someone at an implementer (Free vs. Subscription Services)
 - Keep as-is
 - Modify
 - Remove

Section 5.3 – Do Not Implement Whitelisting Variations

- Philip Homburg suggests adding a new section, 5.3.X, to describe the option of returning AAAA RRs at some periodic or random interval, increase over time, to gradually ramp up IPv6 traffic.
 - Add this?
 - Or do not add this?
- For implementers, do the updates to 5.3.2, Gain Experience Using IPv6 Transition Names, better note the relatively limited value of this tactic? (which ties to Section 4.1, volume-based concerns)

Section 8 – Is this recommended?

- The text here was updated to try to reflect a more balanced view of the practice.
- For implementers (and others), does this section look okay?
 - Leave as-is
 - Modify in some way (specific suggestions needed)

One Last Question

- Describing whitelisting as a form of “Access Control” has raised some concerns.
 - Is a whitelist a sort of access control list (a list controlling access to certain DNS resource records)?
 - If not, what is it?
- Options:
 - Leave as-is when “access control” is mentioned anywhere in the I-D
 - Change to:
 - policy control
 - DNS response control
 - authoritative DNS control
 - DNS control
 - ... or something else?

Thank You!

