IPv6 AAAA DNS Whitelisting

A BROADBAND INTERNET TECHNICAL ADVISORY GROUP
TECHNICAL WORKING GROUP REPORT

A Near-Uniform Agreement Report
(100% Consensus Achieved)

Issued:
September 2011

Executive Summary

Internet Protocol version 6 (IPv6) is the new form of addressing for the Internet. IPv6 is being deployed as a result of the exhaustion of the supply of the older form of addressing, Internet Protocol version 4 (IPv4). The Internet is now beginning a global transition from IPv4 to IPv6, although most websites and networks will run both address families in parallel for many years.

This document describes the emerging practice of Internet web sites (or, more broadly, "Internet domains"), such as example.com, selectively returning IPv6-related resources from Domain Name System (DNS) servers. As a result, the domain can enable or disable a network (and, as a consequence, that network's users) from accessing the domain's content over IPv6. This practice is known as "DNS Whitelisting" and is intended as a means to smooth the global transition from IPv4 to IPv6.

DNS Whitelisting was first used by major web content sites. These web site operators observed that when they added IPv6 records to their DNS servers in order to support IPv6 access to their content, a fraction of end users had slow or otherwise impaired access to this content **[IPv6 Dual-Stack Client Loss in Norway]**.

Major domains are motivated by a desire to maintain a high-quality user experience for all of their users, as well as to shift traffic to IPv6 in a controlled manner. Thus, domains engaging in DNS Whitelisting are attempting to shield users with impaired access from the symptoms of those impairments until they can be remedied. Those domains are also interested in having a degree of control over their own migration to IPv6 that they would otherwise lack without DNS Whitelisting, so that IPv6 traffic can be added gradually as IPv6 operations and network practices mature.

At the same time, critics of the practice have articulated a range of technical and non-technical concerns and are focused on ensuring that DNS Whitelisting, when implemented, is done in a manner that is transparent, non-discriminatory, and not anti-competitive.

Generally speaking, a domain that implements DNS Whitelisting does so manually. This means that the domain manually maintains a list of networks that are permitted to receive IPv6 records (via their DNS resolver IP addresses) and that these networks typically submit applications in order to be added to the DNS Whitelist.

Domain operators foresee that a second phase of DNS Whitelisting may emerge in the future, possibly in the near future. In this new phase a domain would return IPv6 and/or IPv4 records dynamically based on automatically detected technical capabilities, location, or other factors. It would then function much like (or as part of) global server load balancing, a common suite of practices already in use today. Furthermore, in this second phase, networks might be added to and removed from a DNS Whitelist automatically, and possibly on a near-real-time basis. This means that

networks may no longer need to apply to be added to a whitelist, which could alleviate some of the issues addressed herein.

Since this future phase has yet to emerge, this document and its suggestions apply only to the DNS Whitelisting practices currently known to the BITAG. The BITAG reserves its opinion on future alternative practices until they can be articulated and evaluated.

Although current implementations are not perceived to have this impact, the BITAG is interested in this issue on that grounds that, without careful and monitored deployment, some whitelisting services could in the future be viewed as anti-competitive, discriminatory or in violation of some other public policy objective. The practice may be viewed as controversial and the manner in which it is employed could result in concerns or complaints. As a result, it is important to inform the public and policymakers about why DNS Whitelisting is used and how it functions, to identify concerns surrounding its use, and to outline some potential implementation steps that domains could take to minimize the risk of complaints and controversy.

The BITAG has formulated a set of suggested practices regarding the implementation of DNS Whitelisting to help reduce such complaints, acknowledging that practices may vary as a domain moves from experimentation with whitelisting and IPv6 to a point of operational stability. The suggested (and voluntary) practices are as follows:

- **Limit the Duration of the Use of DNS Whitelisting** – The BITAG suggests that domain operators use DNS Whitelisting as briefly as possible for those critical domains that will encounter significant end user IPv6-related impairments. The BITAG recognizes that the primary purpose for DNS Whitelisting is to permit IPv6 address service to networks that are essentially problem-free while preferring IPv4 for those that are not and that the duration of Whitelisting is tied to that assessment.

- **Transparently Publish Policies and Processes** – The BITAG suggests that domains make their policies and processes easy to find and understand. The contact persons should be easy to find and reach as well.

- **Clearly Describe Decision-Making Criteria –** The BITAG suggests that policies and procedures that a domain publishes include criteria used to make DNS Whitelisting and de-whitelisting decisions.

- **Use Primarily Quantitative Decision-Making Criteria –** The BITAG suggests that domains use quantitative data (such as the number of IPv6-related impairments or the performance of IPv6 network routes) to make whitelisting and de-whitelisting decisions.

- **Set and Publish Service Level Goals for Decision-Making** – The BITAG suggests that domains publish clearly detailed and timely service level goals for how long the DNS Whitelisting decision-making process will take.

- **Specify an Appeals Process** – The BITAG suggests that domains may wish to consider specifying a process for networks to appeal both whitelisting and de-whitelisting decisions.

- **Maintain Updated Contacts for Whitelisted Domains** – The BITAG suggests that domains establish a list of contacts for whitelisted organizations and adopt practices that assure that the list is current.

- **Set a Joint-Troubleshooting Interval Before De-Whitelisting Occurs** – The BITAG suggests that domains set a reasonable period of time and process for a whitelisted party to resolve any problems that may arise that could lead to de-whitelisting. The BITAG recognizes that there may be emergency conditions that require immediate action.

- **Transparently Publish Whitelisted Parties** – The BITAG suggests that domains identify the networks that are currently listed in their DNS whitelists.

- **Openly Share IPv6-Related Impairment Statistics** – The BITAG suggests that domains share detailed statistics about IPv6 impairments with any party (campus network, enterprise, ISP, etc.) that may be affected by DNS Whitelisting. The BITAG recognizes that privacy concerns may limit the kinds of data that can be shared.

- **Detect and Notify End Users with IPv6-Related Impairments** – The BITAG suggests that, where practical, domains take reasonable steps to detect IPv6-related impairments and take reasonable steps to communicate this in an easy-to-understand way to affected users.

Table of Contents

1. About the BITAG

The Broadband Internet Technical Advisory Group (BITAG) is a non-profit, multi-stakeholder organization focused on bringing together engineers and technologists in a Technical Working Group (TWG) to develop consensus on broadband network management practices and other related technical issues that can affect users' Internet experience, including the impact to and from applications, content and devices that utilize the Internet.

The BITAG's mission includes: (a) educating policymakers on such technical issues; (b) addressing specific technical matters in an effort to minimize related policy disputes; and (c) serving as a sounding board for new ideas and network management practices. Specific TWG functions also may include: (i) identifying "best practices" by broadband providers

and other entities; (ii) interpreting and applying "safe harbor" practices; (iii) otherwise providing technical guidance to industry and to the public; and/or (iv) issuing advisory opinions on the technical issues germane to the TWG's mission that may underlie disputes concerning broadband network management practices.

BITAG TWG reports focus primarily on technical issues. While the reports may touch on a broad range of questions associated with a particular network management practice, the reports are not intended to address or analyze in a comprehensive fashion the economic, legal, regulatory or public policy issues that the practice may raise.

2. Issue Overview

Internet Protocol version 6 (IPv6) is the new form of addressing for the Internet. IPv6 is being deployed as a result of the exhaustion of the supply of the older form of addressing, Internet Protocol version 4 (IPv4). The Internet is now beginning a global transition from IPv4 to IPv6, although most websites and networks will run both address families in parallel for many years.

This document describes the emerging practice of Internet web sites (or, more broadly, "Internet domains"), such as example.com, selectively returning IPv6-related resources from Domain Name System (DNS) servers. As a result, the domain can enable or disable a network (and, as a consequence, that network's users) from accessing the domain's content over IPv6. In the IPv6 community this practice is generally referred to as "DNS Whitelisting" or, more formally, "IPv6 AAAA DNS Whitelisting" (since "AAAA" is a type of DNS record associated with IPv6 addresses). DNS Whitelisting is intended as an IPv6 transition technique to enable domains to gradually add IPv6 traffic and/or to protect users from IPv6-related technical impairments.

At the current time, generally speaking, a domain that implements DNS Whitelisting does so manually. This means that the domain manually maintains a list of networks that are permitted to receive IPv6 records (via their DNS resolver IP addresses) and that these networks typically submit applications in order to be added to the DNS Whitelist.

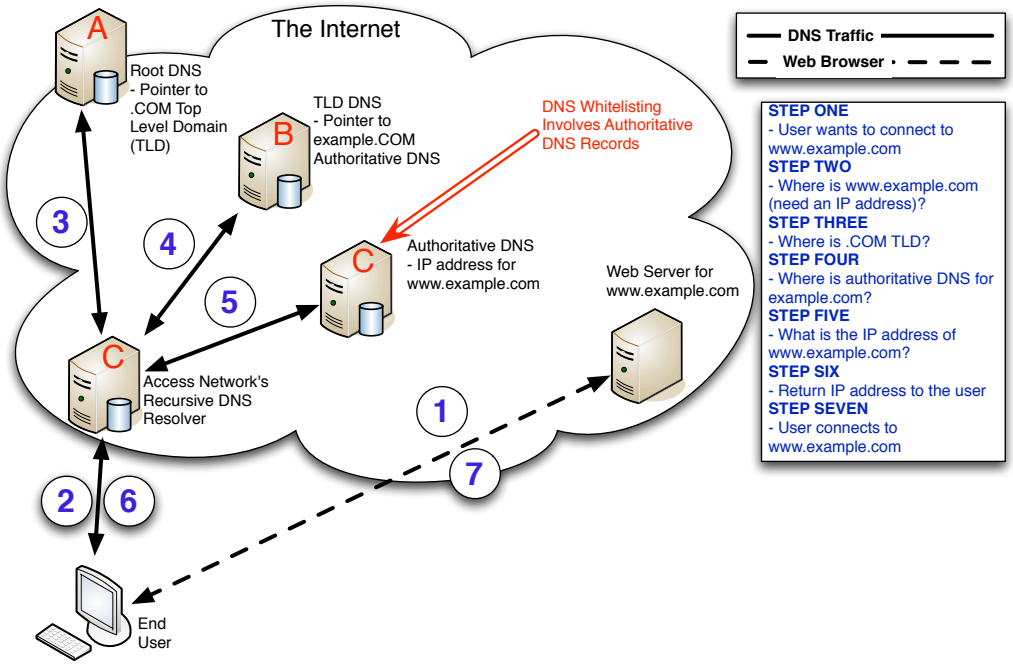
Domain operators foresee that a future phase of DNS Whitelisting may emerge in the future, possibly in the near future. In this new phase, were it successfully implemented, a domain could return IPv6 and/or IPv4 records dynamically based on automatically detected technical capabilities, location, or other factors. It may then function much like or as part of global server load balancing, a common suite of practices already in use today. Furthermore, in this future phase, networks might be added to and removed from a DNS Whitelist automatically, and possibly on a near-real-time basis. This means that networks may no longer need to apply to be added to a whitelist.

Since this future phase has yet to emerge, this document and its suggestions apply only to the DNS Whitelisting practices currently known to the BITAG. The BITAG reserves its opinion on future alternative practices until they can be articulated and evaluated.

The DNS **[RFC1035]** provides what is essentially a directory for the Internet, translating names such as www.example.com into numeric or hexadecimal IP addresses, which is the process of performing a so-called "DNS lookup." One type of DNS server is an "authoritative DNS server" which has authoritative control over, and is responsible for providing DNS lookups for a given domain such as example.com. A domain owner typically controls an authoritative DNS server. Another type of DNS server resides in networks and is called a "DNS recursive resolver." End user computers are configured to send their DNS lookups to these DNS recursive resolvers, which then contact the relevant authoritative DNS servers to obtain IP addresses for a particular name. A network operator typically controls a DNS recursive resolver.

In the authoritative DNS servers there are both IPv4 address records, called "A resource records" (hereinafter "IPv4 DNS records"), and IPv6 address records, called "AAAA resource records" (hereinafter "IPv6 DNS records"), among other types of records. When DNS Whitelisting is used, the authoritative DNS server will not reply to a DNS lookup with the IPv6 DNS records, unless that server sending the request (the DNS recursive resolver) is listed in the DNS Whitelist.

Figure 1 – The DNS Lookup Process



DNS Whitelisting was first used by major web content sites (sometimes described herein as "high-traffic domains"). These web site operators, or domain operators, observed that when they added IPv6 records to their DNS servers in order to support IPv6 access to their content, a small fraction of end users had slow or otherwise

impaired access to this content. The fraction of users with such impaired access has been and continues to be monitored within the Internet community **[IETF-77-DNSOP] [NW-Article-DNSOP] [Evaluating IPv6 Adoption] [IPv6 Brokenness] [World IPv6 Day Observations] [World IPv6 Day @ Microsoft] [World IPv6 Day – What Did We Learn?]**. (It should be noted that an unknown and potentially small fraction of all Internet Access Providers actually assigned both IPv4 and IPv6 addresses to end users on World IPv6 Day.)

Due to this impairment affecting end users of a given domain, as well as a desire for high-traffic domains to gradually add IPv6 traffic, a few domains have either implemented DNS Whitelisting or are considering doing so **[NW-Article-DNS-WL] [IPv6 Whitelist Operations]**, and many other domains may follow suit.

Major domains are motivated by a desire to maintain a high-quality user experience for all of their users, as well as to shift traffic to IPv6 in a controlled manner. Thus, domains engaging in DNS Whitelisting are attempting to shield users with impaired access from the symptoms of those impairments until they can be remedied. Those domains are also interested in having a degree of control over their own migration to IPv6 that they would otherwise lack without DNS Whitelisting, so that IPv6 traffic can be added gradually as IPv6 operations and network practices mature.

At the same time, critics of the practice have articulated a range of technical and non-technical concerns and are focused on ensuring that DNS Whitelisting, when implemented, is done in a manner that is transparent, non-discriminatory, and not anti-competitive.

This document explores the issue of DNS Whitelisting and, crucially, *the steps that implementers could take in order to mitigate any potential concerns*.

2.1. DNS Whitelisting in Detail

DNS Whitelisting is typically implemented in authoritative DNS servers. These servers selectively return DNS IPv6 records in response to DNS queries. In order to determine which recursive DNS servers can receive responses that include IPv6 address records (such as for www.example.com), a given domain (such as example.com) maintains a "whitelist" containing the IP addresses of authorized recursive DNS resolvers.

The list is populated with the IPv4 and/or IPv6 addresses or prefix ranges of DNS recursive resolvers on the Internet that have been authorized to receive IPv6 DNS record responses. These DNS recursive resolvers, constituting many millions, are operated by ISPs, universities, governments, businesses, and individual end users. If a DNS recursive resolver IS NOT matched in the list, then IPv6 DNS records will NOT be sent in response to a query for a hostname in the example.com domain. However, if a

DNS recursive resolver IS matched in the list, then IPv6 DNS records will be sent in response to a query for a given hostname in the example.com domain.

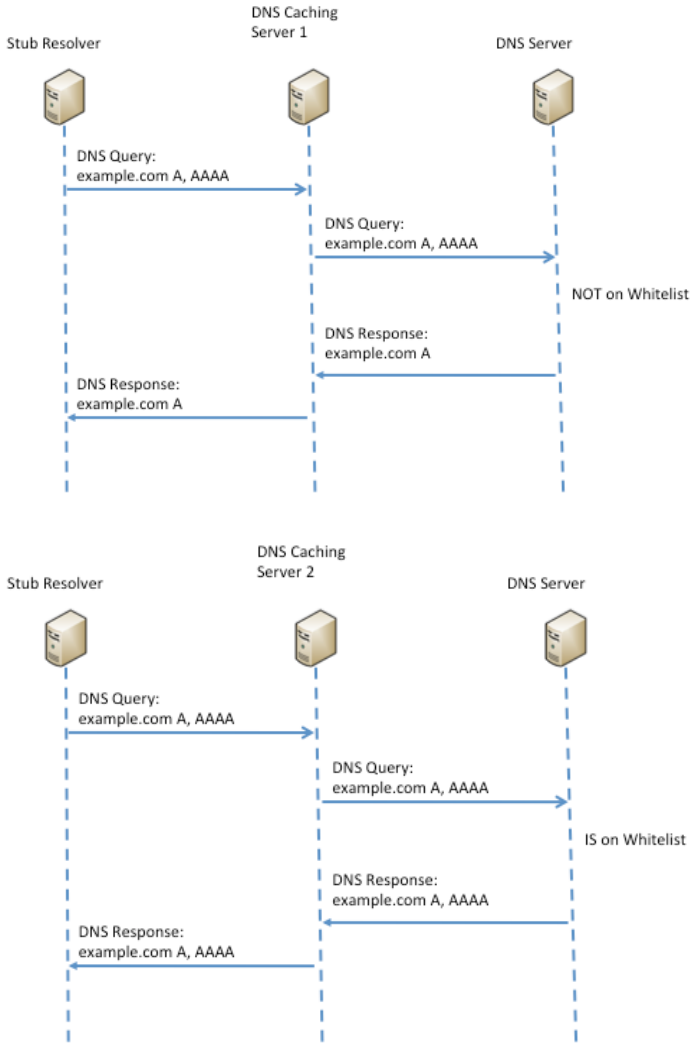
In practice, DNS Whitelisting generally means that a very small fraction of the DNS recursive resolvers on the Internet (those on the whitelist) will receive IPv6 DNS record responses, since there are millions of DNS servers and DNS Whitelists are likely to allow only a small portion of those to receive IPv6 records. The large majority of DNS resolvers on the Internet will therefore receive only IPv4 DNS records. Thus, quite simply, the authoritative server hands out different answers depending upon who is asking; those on the whitelist receive IPv4 and IPv6 DNS records while everyone else receives only IPv4 DNS records. See Section 2.2 and *Figure 2* for a description of how this works.

2.2. Description of the Operation of DNS Whitelisting

The basic system logic of DNS Whitelisting is as follows (see also *Figure 2*):

1. An authoritative DNS server for the domain example.com receives both the IPv4 and IPv6 DNS address record requests for the website www.example.com. Both records exist in example.com's authoritative name server.
2. The authoritative DNS server examines the IP address of the DNS recursive resolver that relayed the original end-user's request for an IPv6 DNS record.
3. The authoritative DNS server checks this IP address against a list of approved IP addresses (the DNS whitelist) created by example.com's administrators.
4. If the DNS recursive resolver's IP address IS validated against the approved list, then the response to that specific DNS recursive resolver can contain IPv6 DNS records.
5. If the DNS recursive resolver's IP address IS NOT validated against the approved list, then the response to the request contains ONLY the IPv4 address record – not both the IPv4 and IPv6 records that were originally requested.

Figure 2 – DNS Whitelisting – Functional Diagram



2.3. Rationale for IPv6 DNS Whitelisting

Domains that implement DNS Whitelisting are doing so for two primary reasons. First, they are attempting to protect those users of their domain who have impaired IPv6 access from having a negative user experience. This negative user experience can range from somewhat slower than usual (as compared to native IPv4-based access), to extremely slow, to no access to the domain whatsoever. Second, they are trying to gradually add IPv6 traffic to their domain as network operations, tools, processes and procedures are less mature for IPv6 as compared to IPv4. One can imagine that suddenly turning on a significant amount of IPv6 traffic – especially for one of the top ten sites globally – is quite daunting operationally.

It is also worth noting the differences between domains containing primarily subscription-based services compared to those containing primarily free services. In the case of free

services, such as search engines, end users have no direct billing relationship with the domain and can switch sites simply by changing the address they enter into their browser (ignoring other value-added services that may tie a user's preference to a given domain or otherwise create switching costs). As a result, such sites are understandably sensitive to the quality of the services within their domain. If the user has issues when the domain turns on IPv6, that user could switch to another domain that is not using IPv6.

Thus, domains may use DNS Whitelisting due to end-user IPv6-related impairments and/or to enable an incremental transition to IPv6 (modulating the traffic load). These domains view DNS Whitelisting as a necessary, although clearly temporary, risk-reduction tactic intended to ease their transition to IPv6 and minimize any perceived risk during the transition. It is not clear how long DNS Whitelisting may be used. This is likely to depend on the global state of the transition to IPv6 rather than on the specific capabilities of individual content sites or networks.

Finally, the view of the scope of the end user impairments and the perceived seriousness of the problem varies within the Internet community. While some domains are considering DNS Whitelisting, other domains that have run IPv6 experiments whereby they added IPv6 DNS records have observed that only a few users had difficulty and chose not to use DNS Whitelisting **[Heise Online Experiment]**.

2.4. Current Deployments

To date, DNS Whitelisting has been deployed on an ad hoc basis and only a fraction of authoritative DNS server operators implement the practice. Thus, only the domains that are interested in implementing a whitelist will need to upgrade their authoritative DNS servers (or otherwise configure their systems).

For example, it was reported in March 2010 **[NW-Article-DNS-WL]** that "[l]eading Web content providers – including Google, Yahoo, Netflix and Microsoft – are conducting early-stage conversations about creating a shared list" of DNS resolvers that have been approved for accessing IPv6 DNS records.

This is all that is known at this time. It is very difficult to determine existing deployments because there is no standard mechanism for a company to disclose that it is engaged in whitelisting. If the practice becomes more prevalent, it may be impossible for recursive resolver operators to be aware of all existing domains that are using whitelists, unless there is a centralized list indicating which domains are engaged in the practice.

3. BITAG Interest in This Issue

Although current implementations are not perceived to have adverse policy effects, the BITAG is interested in this issue on the grounds that, without a careful and monitored

deployment, some whitelisting services could in the future be viewed as anti-competitive, discriminatory or in violation of some other public policy objective. The practice may be viewed as controversial and the manner in which it is employed could result in concerns or complaints. As a result, it is important to inform the public and policymakers about why DNS Whitelisting is used and how it functions, to identify concerns surrounding its use, and to outline some potential steps that implementers can take to minimize the risk of complaints and controversy.

4. Implications of, and Concerns Relating to, the Issue

Parts of the Internet community have raised concerns with a number of potential implications relating to DNS Whitelisting. These are broadly related to Internet architecture, operations, monitoring, and troubleshooting and are addressed in an IETF document **[I-D.v6ops-v6-aaaa-whitelisting-implications]**. A brief summary is provided here.

4.1. Architectural, Operational, Monitoring and Troubleshooting Concerns

Some parties in the Internet community, including ISPs, are concerned that the practice of DNS Whitelisting for IPv6 DNS records departs from the practices regarding IPv4 DNS records in the DNS on the Internet **[Whitelisting Concerns]**.

Other architectural implications include alterations to the prevailing end-to-end model of Internet connectivity, a potential increase in homogeneity of Internet endpoints, and interference with the positive "network effects" resulting from connecting new devices and content to the Internet. It should be recognized that the practice of generating different responses to the same domain lookup for different users has been adopted in most cases for operational and performance reasons. For example, content distribution systems assign users to different servers as a load-sharing or latency-reducing tactic. These are operational practices intended to provide better quality of service based on the user's location in the Internet. This practice is known as Global Server Load Balancing (GSLB).

Other concerns relate to the impact of whitelisting on the IPv6 transition. Whitelisting may impact the public reachability of IPv6 addresses, slow the transition to IPv6, or otherwise reduce the motivations for transitioning, which could result in the use of widespread multi-layer network address translation (NAT) techniques on a long-term basis (breaking some applications and presenting other challenges). Conversely, implementers also point out that without a mechanism like DNS Whitelisting to gradually add IPv6 traffic to content sites, these sites may be unable to transition to IPv6 or may need to significantly delay the transition. Moreover, where impairments are an issue, and IPv4 remains available, whitelisting shields users from a poor operational experience until the impairments can be remedied.

Whitelisting also might raise operational, monitoring, and troubleshooting concerns. Whitelisting will create operational burdens for authoritative DNS server operators that implement whitelisting, and might create operational burdens for DNS recursive resolver operators.

4.2. Concerns About Potential Abuse of Whitelisting

The current, first phase of DNS Whitelisting requires networks to manually submit applications to be whitelisted by a given domain. The establishment of this new policy control point creates the concern that decisions to whitelist or de-whitelist could be abused (intentionally or merely as a byproduct of a particular technical design choice) to accomplish non-technical objectives that could be viewed as anti-competitive, discriminatory or in violation of some other public policy objective.

These results could come about as an expression of commercial or other conflicts. Possible scenarios that could arise include (these are examples only):

- A domain could withhold adding a network to its whitelist unless that network agreed to some sort of financial payment, legal agreement, or agreement to sever a relationship with a competitor of the domain.
- A music-oriented domain may be engaged in some sort of dispute with an academic network concerning copyright infringement concerns within that network, and may choose to de-whitelist that network as a negotiating technique as part of a commercial negotiation.
- A major email domain may choose to de-whitelist a network due to that network sending a large volume of spam.
- A domain implementing DNS Whitelisting as a means of an incremental IPv6 deployment plan over a multi-year period may severely impact new entrants or rural network operators forced to deploy IPv6–only services due to lack of IPv4 address availability for new customers.

The BITAG recognizes that as long as IPv4 access is available, users can still reach a domain operator's services. The matter only becomes critical if users have only IPv6 access to the services of domain operators.

5. Technical Working Group (TWG) Suggested Practices

DNS Whitelisting is not an inherently good or bad practice. *It can be useful to domains that desire a method to gradually transition to IPv6, especially if they are high-traffic domains.* However, the manner in which it is implemented, at least in its first phase, could in some cases lead to complaints or other conflicts. A future phase, if it is successfully implemented as expected in a manner similar to or as part of global server load balancing, is likely to involve significantly less potential for conflict. Since this future phase has yet to emerge, this document and its suggestions apply only to the

DNS Whitelisting practices currently known to the BITAG. The BITAG reserves its opinion on future alternative practices until they can be articulated and evaluated.

While large high-traffic domains and other domain operators use DNS Whitelisting as a gradual IPv6 transition mechanism, this could discourage network operators and others that run DNS recursive resolvers from rolling out IPv6 or it could prompt some of them to use large-scale IPv4-based NAT in order to avoid dealing with DNS Whitelisting altogether. DNS Whitelisting might also create operational burdens for a range of different organizations and could subject some organizations to discriminatory or anti-competitive treatment.

DNS Whitelisting may help ensure continuity in end users' experiences in accessing Internet domains, but it may also mask the underlying problem – broken IPv6 implementations – and thereby hinder users' ultimate ability to enjoy the IPv6-capable Internet. It also will create new control points within the network (although these may not be dissimilar from global server load balancing in some respects), with potential negative consequences for reliability, transparency, innovation, and the traditional end-to-end architecture of the Internet. One possible solution to the potential masking of problems would be to temporarily enable broader IPv6 DNS responses on a planned schedule to allow for testing. These could be thought of as "micro IPv6 days."

The BITAG recognizes that DNS Whitelisting can be an essential IPv6 transition technique for high-traffic domains. The BITAG also suggests that domains choosing to implement DNS Whitelisting consider a number of tactics that can be employed to make whitelisting work better, to minimize disruptions in the wider Internet community, and to reduce the likelihood of conflicts and complaints related to the practice. These *suggested practices* are listed in the following sub-sections, though they may vary as a domain moves from experimentation with IPv6 to a point of "operational stability."

5.1. Limit the Duration of the Use of DNS Whitelisting

Up to this point, implementers of DNS Whitelisting consider it to be a temporary measure. It is unclear how implementers will judge when the network conditions will have changed sufficiently to justify disabling DNS Whitelisting and/or what the process and timing will be for discontinuing this practice, though the extent of IPv6 deployment to end users in networks is clearly one factor.

Since DNS Whitelisting has technical and non-technical implications and costs, beyond those borne by implementers themselves, it is in the best interest of the Internet community that the use of DNS Whitelisting is as short-lived as possible. At the same time though, the interests of the broader Internet community must be balanced against domains' reasonable business needs to both maintain a good experience for their end users and to gradually enable IPv6.

As a result, it is impossible to set a specific duration for the use of DNS Whitelisting on the Internet. The BITAG therefore suggests that implementers limit DNS Whitelisting to only those critical domains that will encounter significant end user IPv6-related impairments or that receive a high volume of traffic. The BITAG suggests that if DNS Whitelisting is employed, it should be eliminated when impairments fall below a threshold that meets domain operator needs. The BITAG also suggests that implementers take into consideration the reality that, as a practical matter, it will be impossible to get to a point where there are no longer any IPv6-related impairments; some reasonably small number of systems will inevitably be left behind as end users elect not to upgrade them or as some systems are incapable of being upgraded.

5.2. Transparently Publish Policies and Processes

The BITAG suggests that implementers publish their DNS Whitelisting policies and processes in a transparent manner for end users, network operators, and others. The information should be easy to find, easy to understand, and there should be an easy way to contact an implementer to ask additional questions. This would demonstrate a spirit of openness and transparency. If there is a centralized list of DNS Whitelisting domains on the Internet, a domain may wish to add their domain to that list.

5.3. Clearly Describe All Decision-Making Criteria

The BITAG suggests that the policies and procedures that an implementer publishes clearly describe criteria used to make DNS Whitelisting and de-whitelisting decisions. *If all criteria cannot be published, the BITAG suggests that implementers publish, at a minimum, a general description of the basis for their decision-making.* This avoids ambiguity or opacity in the decision-making process, and enables any third-party to assess the decision-making criterion and how it may apply to a particular network or organization. This also can help to minimize any impression of discrimination or arbitrariness in the decision-making process.

5.4. Use Primarily Quantitative Decision-Making Criteria

To further minimize any impression of discrimination or arbitrariness in the decision-making process, the BITAG suggests that implementers use quantitative data (such as the number of IPv6-related impairments, the performance of IPv6 network routes, or the volume of traffic from a particular network) to make whitelisting and de-whitelisting decisions. This avoids any ambiguity or opacity in the decision-making process, and enables any third-party to assess the decision-making criteria and how it may apply to a particular network or organization. It can also help implementers and those potentially affected by DNS Whitelisting to systematically (and perhaps via automated systems) measure their qualification readiness for a given domain.

Of course, some quantitative criteria may be internal and proprietary, pertaining to things such as the inbound traffic from particular networks to a domain. In such cases, this data may not be externally verifiable, but disclosing that such information is a factor in decision-making is nonetheless important.

By using quantitative measures to determine whether to whitelist or de-whitelist, an implementer can also minimize any impression that a decision was made on an arbitrary, discriminatory, and/or anti-competitive basis.

5.5. Set and Publish Service-Level Goals for Decision-Making

The BITAG suggests that implementers establish and publish clear, detailed, and timely service-level goals for how long the decision to add a network to a DNS White list will take, from the point at which an application is submitted. This will set expectations and reduce uncertainty for all parties involved, including applicants and end users. This can also help to minimize any impression that the process has been unreasonably or unduly delayed for discriminatory, anti-competitive, or other reasons.

Of course, these service-level goals may only specify a timeframe for deciding whether or not a party is to be whitelisted. They may not necessarily include how long it might take to add the party to the actual DNS Whitelist, as this is subject to various operational considerations that will vary from domain to domain and that are likely quite dynamic in nature.

5.6. Specify an Appeals Process

The BITAG suggests that implementers specify a fair and reasonable process for appealing both whitelisting and de-whitelisting decisions. This could include specification of reasonably short service level goals for the duration of an appeal, from the point of submission. This can set expectations and reduce uncertainty for the appealing party and any other concerned parties, including end users. Also, this can help to minimize any impression that the process has been unreasonably or unduly delayed for discriminatory, anti-competitive, or other reasons.

5.7. Maintain Updated Contacts for Whitelisted Domains

In order to facilitate rapid communication with organizations that have been whitelisted (such as to troubleshoot problems that could lead to de-whitelisting if not resolved), the BITAG suggests that implementers establish a list of contacts for whitelisted organizations and ensure that a process is established to keep the list current. It is quite likely that this will best be conducted via an automated process, much in the same way mailing lists often send a subscription confirmation every month.

5.8. Set a Joint-Troubleshooting Interval Before De-Whitelisting Occurs

The BITAG suggests that implementers set a reasonable period of time and process for a whitelisted party to resolve any problems that may arise and could lead to de-whitelisting. If an implementer detects such problems it can contact the whitelisted party as soon as is reasonably practicable, using current/up-to-date contact information for that party. That communication could include as much technical detail as possible to enable the affected party to understand the problem and determine what steps they may need to take to cure the problem. The implementer could also specify a reasonable mechanism and reasonable length of time that they can make themselves available to work jointly with the affected party to discuss the problem and work towards a resolution. This is an important step to ensure that the de-whitelisting actions of an implementer are perceived as fair and reasonable, rather than unreasonable, sudden, discriminatory, or anti-competitive.

It is important to note that there are necessary exceptions to such a joint-troubleshooting interval for operational issues or other emergencies within the domain using DNS Whitelisting, which may be solely related to the domain in question and not have anything to do with a particular network. However, it is reasonable that the longer a given party is whitelisted, the more difficult it should be to de-whitelist them. Thus, once "operational stability" has been achieved between the parties, then de-whitelisting should generally not occur except in cases of operational emergencies, and in those cases there should be opportunities for joint troubleshooting since suddenly changing a large volume of traffic from IPv6 to IPv4 could have dramatic effects on both users and servers.

5.9. Transparently Publish Whitelisted Parties

The BITAG suggests that implementers identify the networks currently listed in the DNS whitelist for a particular domain and to publish them in the same location as DNS Whitelisting policies and procedures. This demonstrates a spirit of openness and transparency, and can assist any potentially affected parties, such as end users, in determining if DNS Whitelisting is the reason they cannot access a particular site via IPv6 transport. This also helps to slightly mitigate some of the aforementioned troubleshooting implications.

5.10. Openly Share IPv6-Related Impairment Statistics

In order for implementers to demonstrate that they are working to shorten the duration of DNS Whitelisting and/or resolve IPv6-related impairments in their user population, the BITAG suggests that they share detailed statistics with networks that may be affected by DNS Whitelisting. For example, upon request a campus network, enterprise, or ISP could be provided with detailed statistics on the level of IPv6-related impairments in their respective networks, which will facilitate the repair of hosts in a

given network. Automating the publishing of such statistics in the aggregate – for anyone on the Internet to see – may even be a better solution. The BITAG recognizes that privacy concerns may limit some of the statistics that can be shared (see also Section 5.14).

5.11. Detect and Notify End Users with IPv6-Related Impairments

In order for implementers to demonstrate they are working to shorten the duration of DNS Whitelisting and/or resolve IPv6-related impairments in their user population, the BITAG suggests that, where practical, they undertake reasonable efforts to detect IPv6-related impairments communicate this to affected users. For example, an implementer that operates a webmail platform could implement a detection tool on the main mailbox screen and, if the user was affected, send them an email or display an error message that the user could then act upon. Any messaging to the end user should be easy to understand and, where practical, should clearly explain the steps that a non-technical user might take in order to resolve the problem. For example, several content providers did so prior to World IPv6 Day on June 8, 2011, which likely assisted many end users in resolving IPv6-related impairments **[World IPv6 Day Observations]**. The BITAG recognizes that neither domain operators nor even Internet access providers may be able to diagnose or prescribe solutions for impairments whose origins cannot be remotely detected.

5.12. Solve Current End User IPv6 Impairments

The BITAG suggests that the Internet community continues working to identify and fix end user IPv6 impairments. This can motivate affected device and software vendors to fix their devices and software, and can assist users in solving any impairment on their own.

In order to solve these impairments, a first step is to identify which end users have such impairments, and then to communicate this information to them. Such end user communication is likely to be more helpful if the end user is not only alerted to a potential problem, but is also given careful and detailed advice on how to resolve it on their own, or where they can seek help in doing so. The BITAG recognizes that operators may not be able to diagnose and recommend cures for all possible impairments.

While this effort may not end the practice of DNS Whitelisting immediately, it could help shorten its duration and decrease the number of authoritative server operators that choose to deploy DNS Whitelisting.

5.13. Gain Experience Using IPv6 Transition Names

The BITAG suggests that domains may find value in gaining experience using a special fully qualified domain name (FQDN) that has become common for domains beginning the transition to IPv6: ipv6.example.com or www.ipv6.example.com. This can be a way for a domain to gain IPv6 experience and increase IPv6 use on a relatively controlled basis, without the need for whitelisting. However, a special name is likely to be accessed primarily by more technically skilled end users who are unlikely to be representative of a domain's broader user population. It also means that the traffic volume will be relatively small. All of these factors may make a special FQDN only moderately useful for a domain, and as such may be useful only as a first step in a transition to IPv6. The BITAG recognizes this method as a way for Internet access providers and application service providers to test IPv6 access without other special arrangements including whitelisting.

5.14. Protect User Privacy When Sharing Impairment Data

The BITAG suggests that domains and network operators take reasonable steps to protect users' privacy when sharing impairment data. As noted earlier, there may be methods to detect IPv6-related impairments for a particular end user. For example, this may be possible when an end user visits the website of a particular domain, though there are likely no privacy considerations in automatically communicating to such an end user that the domain has detected a particular impairment. However, if that domain decided to share information concerning that particular end user with the user's network operator or another party, then the visited domain may wish to in some manner advise the end user of this or otherwise seek to obtain the user's consent to this type of information-sharing. This may be achieved in a wide variety of ways, including from presenting a message asking the user for consent (which will, of course, help them solve a technical problem of which they are likely unaware) or adding this to a domain's website terms of use / service. Such information sharing and communication of such sharing to end users may well vary by geographic area and/or legal jurisdiction.

To the extent that domains or network operators decide to publish impairment statistics, they should *not* identify individual hosts, host identifiers, or users.

6. References

[I-D.v6ops-v6-aaaa-whitelisting-implications] Livingood, J., "IPv6 AAAA DNS Whitelisting Implications", draft-ietf-v6ops-v6-aaaa-whitelisting-implications-03 (work in progress), February 2011.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC1958] Carpenter, B., "Architectural Principles of the Internet", RFC 1958, June 1996.

[RFC3234] Carpenter, B. and S. Brim, "Middleboxes: Taxonomy and Issues", RFC 3234, February 2002.

[RFC3724] Kempf, J., Austein, R., and IAB, "The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture", RFC 3724, March 2004.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005.

[Evaluating IPv6 Adoption] Colitti, L., Gunderson, S., Kline, E., and T. Refice, "Evaluating IPv6 adoption in the Internet", Passive and Active Management (PAM) Conference 2010, April 2010, <http://research.google.com/pubs/archive/36240.pdf>.

[Heise Online Experiment] Heise.de, "World IPv6 Day - June 8, 2011", Heise.de Website http://www.h-online.com, January 2011, <http://www.h-online.com/features/The-big-IPv6-experiment-1165042.html>.

[I-D.shirasaki-nat444] Yamagata, I., Shirasaki, Y., Nakagawa, A., Yamaguchi, J., and H. Ashida, "NAT444", draft-shirasaki-nat444-03 (work in progress), January 2011.

[IETF-77-DNSOP] Gashinsky, I., "IPv6 & recursive resolvers: How do we make the transition less painful?", IETF 77 DNS Operations Working Group, March 2010, <http://www.ietf.org/proceedings/77/slides/dnsop-7.pdf>.

[IPv6 Brokenness] Anderson, T., "Measuring and Combating IPv6 Brokenness", Reseaux IP Europeens (RIPE) 61st Meeting, November 2011, <http://ripe61.ripe.net/presentations/162-ripe61.pdf>.

[IPv6 Dual-Stack Client Loss in Norway] Anderson, T., “IPv6 Dual-Stack Client Loss in Norway”, May 5, 2011, <http://www.fud.no/ipv6/>.

[IPv6 Whitelist Operations] Kline, E., "IPv6 Whitelist Operations", Google IPv6 Implementers Conference, June 2010,

<http://sites.google.com/site/ipv6implementors/2010/agenda/IPv6_Whitelist_Operations.pdf>.

[NW-Article-DNS-WL] Marsan, C., "Google, Microsoft, Netflix in talks to create shared list of IPv6 users", Network World, March 2010, <http://www.networkworld.com/news/2010/032610-dns-ipv6-whitelist.html>.

[NW-Article-DNSOP] Marsan, C., "Yahoo proposes 'really ugly hack' to DNS", Network World, March 2010, <http://www.networkworld.com/news/2010/032610-yahoo-dns.html>.

[Rethinking the Internet] Blumenthal, M. and D. Clark, "Rethinking the design of the Internet: The end to end arguments vs. the brave new world", ACM Transactions on Internet Technology Volume 1, Number 1, Pages 70-109, August 2001, <dspace.mit.edu/bitstream/handle/1721.1/1519/TPRC_Clark_Blumenthal.pdf>.

[Tussle in Cyberspace] Braden, R., Clark, D., Sollins, K., and J. Wroclawski, "Tussle in Cyberspace: Defining Tomorrow's Internet", Proceedings of ACM Sigcomm 2002, August 2002, <http://groups.csail.mit.edu/ana/Publications/PubPDFs/Tussle2002.pdf>.

[Whitelisting Concerns] Brzozowski, J., Griffiths, C., Klieber, T., Lee, Y., Livingood, J., and R. Woundy, "IPv6 DNS Whitelisting - Could It Hinder IPv6 Adoption?", ISOC Internet Society IPv6 Deployment Workshop, April 2010, <http://www.comcast6.net/IPv6_DNS_Whitelisting_Concerns_20100416.pdf>.

[World IPv6 Day @ Microsoft] Palmer, C. and Thaler, D., "World IPv6 Day @ Microsoft", IETF v6ops Working Group, July 2011, <http://www.ietf.org/proceedings/81/slides/v6ops-1.pptx>.

[World IPv6 Day – What Did We Learn?] Wijnen, B., Aben, E., Wilhem, R., and Kisteleki, R., "World IPv6 Day – What Did We Learn", IETF v6ops Working Group, July 2011, <http://www.ietf.org/proceedings/81/slides/v6ops-4.pdf>.

[World IPv6 Day Observations] Daigle, L., "World IPv6 Day Observations", IETF Plenary, July 2011, <www.ietf.org/proceedings/81/slides/plenaryt-9.pdf>.

7. Glossary of Terms

- Authoritative DNS server: It is the name server that resolves only that domain name to an IP address or vice versa that it has authority to do so for. To resolve a domain name to an IP address, DNS messages are transferred between the user and the DNS server. The DNS messages consist of a query message asked by the user to the DNS server and a response message by the DNS server to that same user, where the user

generally expects an answer in the form of an IP address. As adapted from Forouzan, B., TCP/IP Protocol Suite, Fourth Edition, 2010, pp. 582-609.

- Domain: A term that is used in this document to refer to the portion of a domain name that is wholly owned or managed by a particular authoritative DNS server (such as example.com), or that is used to refer to the operator of that authoritative DNS server. In the second usage, it is synonymous with the term "domain operator."

- Domain Name System (DNS) Server: It is the server used to translate common language Internet addresses to machine-readable IP addresses. For, example, a website like www.example.com is translated to 172.236.166.12 (IPv4 address) or 2001:0:0:0:0:0:0:12 (IPv6 address) by the DNS server. As adapted from Forouzan, B., TCP/IP Protocol Suite, Fourth Edition, 2010, pp. 582-609.

- DNS blacklist: The opposite of a whitelist, it is the list in the DNS server that is used to block traffic. For example, if www.example.com is blacklisted from the DNS server then the user request to resolve www.example.com will be ignored or not answered by the DNS server. As adapted from IETF, RFC-5782: "DNS Blacklists and Whitelists," Feb. 2010, <http://tools.ietf.org/html/rfc5782>.

- DNS record query: It is the user query asking the DNS server to resolve a common language name such as www.example.com into an IP address or, vice versa, asking to resolve an IP address to a common language name. It is the record used by a client to get information from the DNS server. As adapted from Forouzan, B., TCP/IP Protocol Suite, Fourth Edition, 2010, pp. 582-609.

- DNS record responses: It is the response provided by the DNS server to the user after the user has made a DNS record query. As adapted from Forouzan, B., TCP/IP Protocol Suite, Fourth Edition, 2010, pp. 582-609.

- DNS recursive resolver: A resolver is a DNS client employed by the user to map an IP address to a name or a name to an IP address. A recursive resolver takes the DNS record query from the user and checks its database to see if it both has the domain name and authority to resolve that domain name, if the recursive resolver has both then it replies to the user with a DNS record response and otherwise the resolver sends the request to another server, where the process is repeated until a DNS server can resolve the query. Once the query is resolved, the response is sent to the requesting client and then to the user. As adapted from Forouzan, B., TCP/IP Protocol Suite, Fourth Edition, 2010, pp. 582-609.

- Fully Qualified Domain Name (FQDN): A fully qualified domain name (FQDN) is the complete domain name for a specific computer, or host, on the Internet that determines the exact location of devices in the domain name system (DNS). For example, www.example.com is a fully qualified domain name where "www." is the host, "example" is second-level domain and ".com" is the top level domain. As adapted from Forouzan, B., TCP/IP Protocol Suite, Fourth Edition, 2010, pp. 582-609.

- Global Server Load Balancing (GSLB): Large websites commonly run on multiple servers that can run on multiple machines at more than one geographic location worldwide. If the load on one server increases, i.e. if the number of users accessing that particular website from one server increases, the workload will be balanced with other servers depending on the sensitivity to the physical location of the visitor to the site. This is known as Global Server Load Balancing. One advantage is redundancy, in that even when users are not able to connect to a particular server they will be directed to another, at potentially a different data center. For example, www.example.com has servers at location A and B, if server A fails then the request is redirected to server B. As adapted from Gaurav, J., "How GSLB Works", Citrix Community, Dec. 2009, <http://community.citrix.com/display/ns/How+GSLB+Works>.

- Network Address Translation (NAT): Network Address Translation is used to conserve public IP addresses and is where IP addresses are mapped from one address realm to another, providing transparent routing to end hosts; in other words using a single public IP address to route to multiple private IP addresses. Private IP addresses are those addresses that are used within an internal network (e.g., within a home or business network) and cannot go out to the public Internet. There are many variations of network address translation. As adapted from IETF, RFC-2663: "IP Network Address Translator (NAT) Terminology and Considerations," August 1999, <http://tools.ietf.org/html/rfc2663>; see also "Assessing the Impact of NAT444 on Network Applications draft-donley-nat444-impacts-01," October 2010, <http://tools.ietf.org/html/draft-donley-nat444-impacts-01>.

- Resource Record: Each domain name is associated with a record held in the DNS server database called the resource record. Resource records are used by DNS servers to return the IP address of the domain name requested by the user. For example, an IPv6 record is the listing of an IPv6 website on a DNS server database. As adapted from Forouzan, B., TCP/IP Protocol Suite, Fourth Edition, 2010, pp. 582-609.

- Top Level Domain (TLD): It is one of the domains at the highest level in the hierarchical Domain Name System (DNS) of the Internet. The global Internet Domain Name System defines a tree of names starting with root, ".", immediately below which are top level domain names such as ".com" or ".org". Below top level domain names there are normally additional levels of names. For example, in the domain name www.example.com, the top-level domain is ".com." As adapted from IETF, RFC-2606: "Reserved Top Level DNS Names," June 1999, <http://tools.ietf.org/html/rfc2606>.

8. Document Contributors and Reviewers

- Richard Bennett, Information Technology & Innovation Foundation
- Rex Bollinger, National Cable & Telecommunications Association
- Vint Cerf, Google
- William Check, National Cable & Telecommunications Association
- Alissa Cooper, Center for Democracy and Technology
- Mark Clougherty, Alcatel-Lucent
- Leslie Daigle, Internet Society
- Michael Fargano, CenturyLink
- Ken Florance, Netflix
- Jeff Good, Disney
- Bill Goodman, Verizon
- Amer Hassan, Microsoft
- Stephen Hayes, Ericsson
- Trace Hollifield, Bright House Networks
- Kevin Kahn, Intel
- Chuck Kalmanek, AT&T
- Jason Livingood, Comcast
- Milo Medin, Google
- George Ou, Digital Society
- Pieter Poll, CenturyLink
- Phil Roberts, Internet Society
- Andrew Setos, FOX Networks
- Barbara Stark, AT&T
- Jason Weil, Time Warner Cable
- Steve Weinstein, MovieLabs