

Network Working Group
Internet Draft
Intended status: Informational
Updates: [2874](#), [3363](#)
Expires: March 23, 2012

S. Jiang
Huawei Technologies Co., Ltd
D. Conrad
Cloudflare, Inc.
B. Carpenter
Univ. of Auckland
September 20, 2011

Moving A6 to Historic Status
draft-jiang-dnsexst-a6-to-historic-00.txt

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on March 23, 2012.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Internet-Draft [draft-jiang-dnsext-a6-to-historic](#)

September 2011

Abstract

This document provides a summary of issues and discusses the current usage status of A6 DNS records and moves the A6 specifications to Historic status, providing clarity to implementers and operators.

Table of Contents

1.	Introduction & Background	3
2.	A6 Issues	3
2.1.	Resolution Latency	4
2.2.	Resolution failure	4
2.3.	Cross administration domains	4
2.4.	Difficult Maintenance	5
2.5.	Existence of Multiple RR Types for one Purpose is Harmful	5
2.6.	Higher Security Risks	5
3.	Status of A6 current usage	5
3.1.	Reasons for Current A6 Usage	6
4.	Moving A6 to Historic Status	6
4.1.	Impact on Current A6 Usage	6
4.2.	Transition phase for current A6	6
5.	Security Considerations	7
6.	IANA Considerations	7
7.	Acknowledgments	7
8.	References	7
8.1.	Normative References	7
8.2.	Informative References	7
	Author's Addresses	8

1. Introduction & Background

The IETF began the process of standardizing two different DNS protocol enhancements for IPv6 addresses in DNS (Domain Name System) records: AAAA [[RFC3596](#)] in 1995 [[RFC1886](#)] and A6 [[RFC2874](#)] in 2000. Both protocol enhancements reached Proposed Standard status.

The existence of multiple ways of representing IPv6 address in the DNS has led to confusion and conflicts about which of these protocol enhancements should be implemented and/or deployed. Having more than one choice of how IPv6 addresses are to be represented within the DNS can be argued to have led to delays in the deployment of IPv6. In 2002, "Representing IPv6 Addresses in the DNS" [[RFC3363](#)] moved A6 to Experimental status, with an aim to clear up any confusion in this area. [[RFC3363](#)] and [[RFC3364](#)] compared AAAA and A6, and examined many of the issues in the A6 standard, these issues being summarized in this document.

However, after ten years, the Experimental status of A6 has resulted in continued confusion and parallel deployment of both A6 and AAAA, albeit AAAA predominates by a large degree. Even in recent IPv6 transition tests and deployments, some providers informally mentioned A6 support as a possible future choice.

This document provides a brief summary of the issues related to the use of A6 records and discusses the current usage status of A6. Given the implications of A6 on the DNS architecture and the state of A6 deployment, this document moves the A6 specifications to Historic status, thereby clarifying that implementers and operators should represent IPv6 addresses in the DNS only by using AAAA records.

1.1 Standards Action Taken

This document requests the IESG to change the status of [RFC 2874](#) from Experimental to Historic.

[2. A6 Issues](#)

This section summarizes the known issues associated with the use of A6 resource records, including the analyses explored in [[RFC3363](#)]. The reader is encouraged to review that document to fully understand the issues relating to A6.

Jiang

Expires March 23, 2012

[Page 3]

Internet-Draft

[draft-jiang-dnsext-a6-to-historic](#)

September 2011

[2.1. Resolution Latency](#)

Resolving an A6 Record chain can involve resolving a series of sub-queries that are likely to be independent of each other. Each of these sub-queries takes a non-negligible amount of time unless the answer already happens to be in the resolver's cache. The worst-case time resolving a N-link chain A6 record would be the sum of the latency resulting from each of the N resolutions. As a result, long A6 chains would be likely to increase user frustration due to excessive waiting times for domain names to resolve.

In practice, it is very hard to derive a reasonable timeout handling strategy for the reassembly of all the results from A6 sub-queries. It is proved difficult to decide multiple timeout parameters, including (1) the communication timeout for a single A6 fragment, (2) the communication timeout for the IPv6 address itself (total time needed for reassembly) and (3) the TTL timeout for A6 fragment records.

[2.2. Resolution Failure](#)

The probability of A6 resolution failure during the process of resolving an N-link A6 chain is sum of the probabilities of failure of each sub-query, since each of the queries involved in resolving an A6 chain has a non-zero probability of failure and an A6 resolution cannot complete until all sub-queries have succeeded.

Furthermore, the failure may happen at any link among 1~N of a N-Link A6 chain. Therefore, it would take an indeterminate time to return a failure result.

[2.3. Cross Administrative Domains](#)

One of the primary motivations for the A6 RR was to facilitate renumbering and multihoming, where the prefix name field in the A6 RR points to a target that is not only outside the DNS zone containing the A6 RR, but is administered by a different organization entirely.

While pointers out of zone are not a problem per se, experience both with glue RRs and with PTR RRs in the IN-ADDR.ARPA tree suggests that pointers to other organizations are often not maintained properly, perhaps because they're less amenable to automation than pointers within a single organization would be.

[2.4.](#) Difficult Maintenance

In A6, changes to components of an RR are not isolated from the use of the composite IPv6 address. Any change to a non-128-bit component of an A6 RR may cause change to a large number of IPv6 addresses. The dependence relationship actually makes the maintenance of addresses much more complicated and difficult. Without understanding these complicated relationships, any arbitrary change for a non-128-bit A6 RR component may result in undesired consequences.

Multiple correlative sub-components of A6 records may have different TTLs, which can make cache maintenance very complicated.

[2.5.](#) Existence of Multiple RR Types for one Purpose is Harmful

If both AAAA and A6 records were widely deployed in the global DNS, it would impose more query delays to the client resolvers. DNS clients have insufficient knowledge to choose between AAAA and A6 queries, requiring local policy to determine which record type to query. If local policy dictates parallel queries for both AAAA and A6 and if those queries returned different results for any reason, the clients would have no knowledge about which address to choose.

[2.6.](#) Higher Security Risks

The dependency relationships inherent in A6 chains increase security risks. An attacker may successfully attack a single sub-component of an A6 record, which would then influence many query results, and

possibly every host on a large site. There is also the danger of unintentionally or maliciously creating a resolution loop - an A6 chain may create an infinite loop because an out of zone pointer may point back to another component farther down the A6 chain.

3. Current Usage of A6

Full support for IPv6 in the global DNS can be argued to have started when the first IPv6 records were associated with root servers in early 2008.

One of the major DNS server software packages, BIND9 [[BIND](#)], supports both A6 and AAAA and is unique among the major DNS resolvers in that certain versions of the BIND9 resolver will attempt to query for A6 records and follow A6 chains.

According to published statistics for two root DNS servers (the "K" root server [[KROOT](#)] and the "L" root server [[LR00T](#)]), there are between 9,000 and 14,000 DNS queries per second on the "K" root

Jiang

Expires March 23, 2012

[Page 5]

Internet-Draft

[draft-jiang-dnsext-a6-to-historic](#)

September 2011

server and 13,000 to 19,000 queries per second on the "L" root server. The distributions of those queries by RR type are similar: roughly 60% A queries, 20~25% AAAA queries, and less than 1% A6 queries.

3.1. Reasons for Current A6 Usage

That there is A6 query traffic does not mean that A6 is actually in use; it is likely the result of some recursive servers that issue internally-generated A6 queries when looking up missing name server addresses in addition to issuing A and AAAA queries.

BIND versions 9.0 through 9.2 could be configured to make A6 queries and it is possible that some active name servers running those versions have not yet been upgraded.

In the late 1990s, A6 was considered to be the future in preference to AAAA [[RFC2874](#)]. As a result, A6 queries were tried by default in BINDv9 versions. When it was pointed out that A6 had some fundamental issues (discussed in [[I-D.ietf-dnsext-aaaa-a6](#)] with the deprecation codified in [RFC 3363](#)), A6 was abandoned in favor of AAAA and BINDv9 no longer tried A6 records by default. A6 was removed from the query order in the BIND distribution in 2004 or 2005.

Some Linux/glibc versions may have had A6 query implementations in `gethostbyname()` 8-10 years ago. These operating systems/libraries may not have been replaced or upgraded everywhere yet.

[4. Moving A6 to Historic Status](#)

This document moves the A6 specification to Historic status. This move provides a clear signal to implementers and/or operators that A6 should NOT be implemented or deployed.

[4.1. Impact on Current A6 Usage](#)

If A6 were in use and it were to be treated as an 'unknown record' ([RFC3597](#)) as discussed below, it might lead to some interoperability issues since resolvers that support A6 are required to do additional section processing for these records on the wire. However, as there are no known production uses of A6, this impact is considered negligible.

[4.2. Transition phase for current A6](#)

Since there is no known A6-only client in production use, the transition phase may not be strictly necessary. However, clients that

attempt to resolve A6 before AAAA will suffer a performance penalty. Therefore, we recommend:

- * Removing A6 handling from all new or updated host stacks;
- * Recommend removing all existing A6 records; and
- * All resolver and server implementations return the same response as for any unknown or deprecated RR type for all A6 queries. If an AAAA record exists for the name being resolved, a suitable response would be 'no answers/no error', i.e. the response packet has an answer count of 0 but no error is indicated.

[5. Security Considerations](#)

Eliminating A6 records will eliminate any security exposure related to that RR type, and should introduce no new vulnerabilities.

6. IANA Considerations

IANA is requested to change the annotation of the A6 RR type from "Experimental" to "Obsolete" in the DNS Parameters registry.

7. Acknowledgments

The authors would like to thank Ralph Droms, Roy Arends, Edward Lewis, Andreas Gustafsson, Mark Andrews, Jun-ichiro "itojun" Hagino and other members of DNS WGs for valuable contributions.

8. References

8.1. Normative References

- [RFC2874] M. Crawford, C. Huitema, "DNS Extensions to Support IPv6 Address Aggregation and Renumbering", [RFC 2874](#), July 2000.
- [RFC3596] S. Thomson, C. Huitema, V. Ksinant, M. Souissi, "DNS Extensions to Support IP Version 6", [RFC 3596](#), October 2003.

8.2. Informative References

- [RFC1886] S. Thomson and C. Huitema, "DNS Extensions to Support IP Version 6", [RFC 1886](#), December 1995.

Jiang

Expires March 23, 2012

[Page 7]

Internet-Draft

[draft-jiang-dnsexst-a6-to-historic](#)

September 2011

- [RFC3363] R. Bush, A. Durand, B. Fink, O. Gudmundsson, T. Hain, "Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS)", [RFC 3363](#), August 2002.
- [RFC3364] R. Austein, "Tradeoffs in Domain Name System (DNS) Support for Internet Protocol version 6 (IPv6)", [RFC 3364](#), August 2002.
- [I-D.ietf-dnsexst-aaaa-a6]
J. Hagino, "Comparison of AAAA and A6 (do we really need A6?)", working in progress, 2001.
- [BIND] <http://www.isc.org/software/bind>

[KROOT] <http://k.root-servers.org/>

[LR00T] <http://dns.icann.org/lroot/>

Author's Addresses

Sheng Jiang
Huawei Technologies Co., Ltd
Huawei Building, No.3 Xinxu Rd., Hai-Dian District, Beijing
P.R. China
Phone: 86-10-82882681
Email: jiangsheng@huawei.com

David Conrad
Cloudflare, Inc.
665 3rd Street, Suite 207
San Francisco CA 94107
USA
Email: drc@cloudflare.com

Brian Carpenter
Department of Computer Science
University of Auckland
PB 92019
Auckland, 1142
New Zealand
Email: brian.e.carpenter@gmail.com