Testing Recursive Name Servers for IPv6 and EDNS0 Support

SAC 017

15 March 2007

Preparation | Test AAAA and EDNS0 support | Share Your Results | Results Reported | Testing Period

Background

The DNS Root Server System Advisory Committee (RSSAC) and ICANN Security and Stability Advisory Committee (SSAC) are jointly studying the topic of adding type AAAA resource records for the IPv6 addresses of the root name servers to the "root hints file" and the DNS root zone. (The official root hints file is located at ftp://ftp.internic.net/domain/.)

Most recursive name servers perform a bootstrap process called *priming* to determine the current list of root name servers, since information in the local copy of the root hints file could be out of date. To prime, a recursive name server sends a DNS query of type NS for the root (".") to one of the root name servers listed in the local root hints file. The recursive name server uses the list of root name servers in the response returned from a live root name server for resolution purposes. Priming ensures that a recursive name server always starts operation with the most up-to-date list of root name servers.

The operators of five root name servers - B, F, H, K, and M -have assigned IPv6 addresses to their systems. These addresses are not included in the root hints file at this time, nor are they present in the root zone. Thus AAAA resource records are not returned in responses to DNS priming queries sent by recursive name servers.

Adding AAAA records to the root hints file and to the root zone will increase the size of the priming response. Ultimately, when all 13 root name servers assign IPv6 addresses, the priming response will increase in size to 811 bytes. This imposes additional conditions for the successful completion of a priming exchange that do not exist today:

- Resolvers and any intermediate systems that are situated between recursive name servers and root name servers must be able to process DNS messages containing type AAAA resource records.
- Resolvers must use DNS Extensions (EDNS0, RFC 2671) to notify root name servers that they are able to process DNS response messages larger than the 512 byte maximum UDP-encapsulated DNS message size specified in RFC 1035.
- Intermediate systems must be configured to forward UDP-encapsulated DNS response messages larger than the 512 byte maximum DNS message size specified in RFC 1035 to resolvers that issued the priming request.

SAC016 solicits feedback from the Internet community on whether commercial firewalls organizations use to protect resolvers will block (silently discard) priming responses because they do not satisfy these conditions. Vendor and user reports from this exercise may be found here.

The joint committees are now soliciting feedback from the Internet community on whether DNS servers (software and hardware appliance) organizations use to provide recursive name service will operate correctly when type AAAA resource records are added to the root hints file and root zone.

Preparing and Testing Recursive Name Server Implementations and Versions

The complete name server bootstrap process must be tested to verify that changes at the root level of DNS service do not adversely affect production name service. Tests must verify that an implementation:

- Use the root name server information in the priming response message without failing when it is configured with a hints file containing type AAAA resource records.
- Perform the priming exchange over UDP, which involves sending a DNS query for type NS for the root (".") to one or more of the root name servers identified in the local copy of the hints file.
- Process the UDP-encapsulated DNS response message from a root name server.
- Use the information in DNS response message to perform iterative name resolution.

Ideally, the test response contains type A and AAAA resource records of the authoritative root name servers and is larger than the 512-byte maximum UDP DNS message size specified in RFC 1035. Several root name server operators have volunteered to operate test name servers for this exercise. These servers have been configured to be authoritative for "test" root and root-servers.net zones that contain both type A and AAAA resource records for the authoritative root name servers.

Test your Recursive Name Server

To test whether your recursive name server will operate correctly, perform the following:

1. Determine whether your firewall supports AAAA and EDNS0 by performing the tests described in SAC016.
2. Download and install a copy of the test hints file, aaaa-test-root-hints [.DAT, 1K] on the host that provides recursive name service. The contents of aaaa-test-root-hints appear below:

   ```
   ;
   ; IMPORTANT NOTE: This root hints file is for TESTING ONLY.  Use this
   ; file to test your recursive name server's support of AAAA records
   ; for the root name servers.  Details of this experiment are available
   ; at http://www.icann.org/committees/security/sac017.htm
   ;

   .                      3600000  IN  NS    aaaa.verisignlabs.com.
   aaaa.verisignlabs.com.   3600000     A     65.201.175.33
   aaaa.verisignlabs.com.   3600000     AAAA  2001:503:39c1::2:26

   .                      3600000  IN  NS    aaaa.dns.br.
   aaaa.dns.br.           3600000     A     200.160.7.135
   aaaa.dns.br.           3600000     AAAA  2001:12ff:0:7::135

   .                      3600000  IN  NS    roto.nlnetlabs.nl.
   roto.nlnetlabs.nl.      3600000     A     213.154.224.153
   roto.nlnetlabs.nl.      3600000     AAAA  2001:7b8:206:1::153

   .                      3600000  IN  NS    rs-net.isc.org.
   rs-net.isc.org.         3600000     A     204.152.186.62
   rs-net.isc.org.         3600000     AAAA  2001:4f8:3:ba::62
   ```

3. Configure your recursive name server to use the test root hints file, either by specifying the new file in its configuration or by copying the test file over the current root hints file. (We of course suggest making a backup of your current root hints file, though the official file is easily obtained from ftp://ftp.internic.net/domain/). Each recursive name server configuration is different, so you may need to consult your server's documentation, a local expert or resources on the Internet if you're not sure how to specify an alternate root hints file.
4. Stop and restart the name server process or service. This should cause your name server to "prime". (In some cases, your operating system or DNS appliance may require a system level restart.)
5. Perform the following DNS lookup using the popular dig program to make sure that your

recursive resolver sends a priming query, if it hasn't already.

```
dig @IP-of-your-recursive-server icann.org
```

6. Perform the following DNS lookup using the popular dig program to obtain the set of type A and AAAA resource records your recursive name server now has:

   ```
   dig +norec +bufsize=1024 @IP-of-your-recursive-server . NS
   ```

   To create a file of the dig output, use

   ```
   dig +norec +bufsize=1024 @IP-of-your-recursive-server  . NS > testAAAA.txt
   ```

   If you are able to run dig on the recursive server itself, you can send queries to the server's loopback (localhost) address by using an IP address of 127.0.0.1 in the dig command above.

7. Compare the output of your dig query against the information below (note that this query is performed at a recursive name server's localhost IPv4 address, 127.0.0.1, and that the TTLs and order of resource records returned in response to your request may be different):

   ```
   $ dig +norec +bufsize=1024 @127.0.0.1 . ns

   ; <<>> DiG 9.3.2 <<>> +norec +bufsize=1024 @IP-of-your-recursive-server . NS
   ; (1 server found)
   ;; global options:  printcmd
   ;; Got answer:
   ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48730
   ;; flags: qr ra; QUERY: 1, ANSWER: 13, AUTHORITY: 13, ADDITIONAL: 19

   ;; OPT PSEUDOSECTION:
   ; EDNS: version: 0, flags:; udp: 4096
   ;; QUESTION SECTION:
   ;.                      IN      ANY

   ;; ANSWER SECTION:
   .                 514104  IN    NS    A.ROOT-SERVERS.NET.
   .                 514104  IN    NS    B.ROOT-SERVERS.NET.
   .                 514104  IN    NS    C.ROOT-SERVERS.NET.
   .                 514104  IN    NS    D.ROOT-SERVERS.NET.
   .                 514104  IN    NS    E.ROOT-SERVERS.NET.
   .                 514104  IN    NS    F.ROOT-SERVERS.NET.
   .                 514104  IN    NS    G.ROOT-SERVERS.NET.
   .                 514104  IN    NS    H.ROOT-SERVERS.NET.
   .                 514104  IN    NS    I.ROOT-SERVERS.NET.
   .                 514104  IN    NS    J.ROOT-SERVERS.NET.
   .                 514104  IN    NS    K.ROOT-SERVERS.NET.
   .                 514104  IN    NS    L.ROOT-SERVERS.NET.
   .                 514104  IN    NS    M.ROOT-SERVERS.NET.

   ;; AUTHORITY SECTION:
   .                 514104  IN    NS    M.ROOT-SERVERS.NET.
   .                 514104  IN    NS    A.ROOT-SERVERS.NET.
   .                 514104  IN    NS    B.ROOT-SERVERS.NET.
   .                 514104  IN    NS    C.ROOT-SERVERS.NET.
   ```

```
.                514104  IN     NS     D.ROOT-SERVERS.NET.
.                514104  IN     NS     E.ROOT-SERVERS.NET.
.                514104  IN     NS     F.ROOT-SERVERS.NET.
.                514104  IN     NS     G.ROOT-SERVERS.NET.
.                514104  IN     NS     H.ROOT-SERVERS.NET.
.                514104  IN     NS     I.ROOT-SERVERS.NET.
.                514104  IN     NS     J.ROOT-SERVERS.NET.
.                514104  IN     NS     K.ROOT-SERVERS.NET.
.                514104  IN     NS     L.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET.    600504  IN     A      198.41.0.4
B.ROOT-SERVERS.NET.    600504  IN     A      192.228.79.201
B.ROOT-SERVERS.NET.    600504  IN     AAAA   2001:478:65::53
C.ROOT-SERVERS.NET.    600504  IN     A      192.33.4.12
D.ROOT-SERVERS.NET.    600504  IN     A      128.8.10.90
E.ROOT-SERVERS.NET.    600504  IN     A      192.203.230.10
F.ROOT-SERVERS.NET.    600504  IN     A      192.5.5.241
F.ROOT-SERVERS.NET.    600504  IN     AAAA   2001:500::1035
G.ROOT-SERVERS.NET.    600504  IN     A      192.112.36.4
H.ROOT-SERVERS.NET.    600504  IN     A      128.63.2.53
H.ROOT-SERVERS.NET.    600504  IN     AAAA   2001:500:1::803f:235
I.ROOT-SERVERS.NET.    600504  IN     A      192.36.148.17
J.ROOT-SERVERS.NET.    600504  IN     A      192.58.128.30
K.ROOT-SERVERS.NET.    600504  IN     A      193.0.14.129
K.ROOT-SERVERS.NET.    600504  IN     AAAA   2001:7fd::1
L.ROOT-SERVERS.NET.    600504  IN     A      198.32.64.12
M.ROOT-SERVERS.NET.    600504  IN     A      202.12.27.33
M.ROOT-SERVERS.NET.    600504  IN     AAAA   2001:dc3::35

;; Query time: 2 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Jan 30 08:50:55 2007
;; MSG SIZE  rcvd: 756
```

If your recursive server successfully used the test root hints file and processed a priming response from one of the test name servers, you may see AAAA resource records for some of the root name servers in the dig output as in the example above. Note, however, that the absence of these records doesn't necessarily mean something is wrong: your server may have received the proper response and but does not return the records when queried for them. (You may be able to confirm this by examining DNS server or system event logs.)

8. **Use your name server**. Does it resolve queries and operate normally?

   Your recursive name server passes the test if it starts normally, continues to run and resolves queries as usual when configured to use the test root hints file.

   We are most interested to find servers that fail the test by refusing to start when presented with the test root hints file containing AAAA resource records, or that don't operate normally or resolve queries properly after receiving AAAA resource records in the priming response from the test root name servers. The scope of this test is not limited to resolvers that have IPv6 transport. We are interested in results for resolvers that have IPv4 transport only as well.

9. hen you have concluded your testing, remove the test file

(aaaa-test-root-hints)

and restore the official hints file.

Share Your Results with the Internet Community

The SSAC and RSSAC committees encourage you to share your test results with the community by sending an email to the ICANN SSAC Fellow containing the following information:

- DNS Name Server (hardware or software) product & manufacturer
- Hardware model (if applicable)
- Operating System and DNS server versions (for BIND version, "dig @nameserver version.bind txt chaos"
- Did the name server implementation succeed or fail to bootstrap when configured with a hints file containing type AAAA resource records? I.e., did your name server issue an error and/or stop running after being restarted with the test root hints file in place?
- If your name server failed to bootstrap over IPv4 transport
  - Can you provide a description of the failure or an error code?
  - Were you able to resolve the failure condition by making a configuration change? If Yes, please describe any changes to your name server configuration that resolved the failure condition.
- If your name server successfully bootstraps over IPv4 transport,
  - Does it support EDNS0?
  - Is it able to parse AAAA resource records?
  - Does your name server retain a local copy of the type AAAA records for the root name servers?

  Please provide a copy of the dig input and output (as illustrated above, this can be obtained by directing the output to a file, e.g., "`dig +norec @IP-of-your-recursive-server . NS > testAAAA.txt`"); alternatively, indicate success or failure. If failure, please provide the Domain System Response Code reported.
- Does the name server continue to function correctly following a priming exchange with a test root name server? (The root and root-servers.net zones used for testing purposes will contain the IPv4 and IPv6 addresses of operational, authoritative root name servers.)

Testing Performed

The following results have been reported to the SSAC fellow:

DNS Software	Operating System	Bootstraps when AAAA RRs present in hints file	Primes using IPv4 transport	Supports EDNS0	Parses AAAA RRs	Functions properly following a priming exchange with a test root name server	Source
BIND 4.9.3-REL	Redhat Fedora Core 6 Linux	YES [5]	YES	NO	NO	YES	User
BIND 4.9.11-REL	Redhat Fedora Core 6 Linux	YES		NO	YES	YES	User
BIND 8.2.2-P5	SunOS Blakey 5.8	YES	YES	NO	NO	YES	User

BIND 9.2.4	Debian GNU/Linux	YES	YES	YES	YES	YES	User
BIND 9.3.2	Mac OS X version 10.4.8, Ubuntu Dapper (Linux 2.6.15-27)	YES	YES	YES	YES	YES	User
BIND 9.3.4	FreeBSD 6.2	YES	YES	YES	YES	YES	User
BIND 9.4.0 rc2	FreeBSD 6.2, Suse Linux 10.1	YES	YES	YES	YES	YES	User
djbdns (dnscache 1.05)	Fedora 6 Core	YES	YES	YES	NO	YES	User
DNS Commander [4]	Windows NT/XP, Linux, Solaris	YES	N/A	YES	YES	N/A	Vendor
DNSJava	Java (any OS with Java support)	N/A	N/A	YES	YES	N/A	Developer
JDNSS [1]	Java (any OS with Java support)	N/A	N/A	NO		N/A	Developer
MaraDNS 1.2.12.04 [2]	BSD, Linux, Windows	NO	NO	NO	YES	N/A	Developer
Men & Mice Suite 5.x with current BIND 8 or BIND 9	Windows 2000/Windows 2003/Linux/FreeBSD/MacOSX/Solaris	YES	YES	YES	YES	YES	Vendor
Mice & Men QuickDNS v1.0 - 3.0	Apple MacOS Classic (System 7 to MacOS 9)	NO	YES	NO	NO	NO	Vendor
Microsoft DNS Server	Windows 2000 5.00.2195 SP4	YES	YES	NO	NO	YES	User
Microsoft DNS Server	Windows 2003	YES	YES	YES	YES	YES	User
Nominum CNS 1.6.5.0	Solaris 10	YES	YES	YES	YES	YES	Vendor
Posadis DNS version 6	Windows XP SP2	YES	NO	NO	YES	YES	User
PowerDNS Recursor 3.1.4	Debian GNU/Linux	YES	YES	YES	YES	YES	User
QuickDNS 3.5 to 4.6 with current BIND 8 or BIND 9	Windows 2000/Windows 2003/Linux/FreeBSD/MacOSX/ Solaris	YES	YES	YES	YES	YES	Vendor
SimpleDNS version	Windows XP SP2	YES	YES	NO	YES	YES	User,

4.00.06 [3]							Vendor

[1] Used as a leaf or stub resolver. Does not perform recursive lookups and does not prime.
[2] Recursive resolver does not have IPv6 support; recursion must be disabled to bind to IPv6 address.
[3] Priming is performed according to a preconfigured time interval (default once every 7 days).
[4] This product does not perform a priming query and relies on root hints configured for the name server.
[5] Server operates despite error messages recorded to syslog ("Unknown type: AAAA", "database format error (AAAA)", and "cache zone '.' rejected due to errors")

Testing Period

Name servers will be available for testing from 01 February 2007 through 01 May 2007.

Published 08 Feb 2007

This file last modified 18-Apr-2007