Testing IPv6 Address Records in the DNS Root

APNIC 23
February 2007

Geoff Huston
Chief Scientist
APNIC

Priming a DNS name server

1. Take the provided “root hints” file
2. Generate a DNS query for resource records of type “NS” for the DNS root zone (“.”)
3. Send the query to one of the servers listed in the root hints file
4. Load the response into the server state as the root name servers

Example of a Priming Query

```
dig NS . @192.5.5.241

; <<>> DiG 9.3.2 <<>> NS . @192.5.5.241
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45507
;; flags: qr aa rd; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 13

;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       518400  IN      NS      E.ROOT-SERVERS.NET.
.                       518400  IN      NS      F.ROOT-SERVERS.NET.
.                       518400  IN      NS      G.ROOT-SERVERS.NET.
.                       518400  IN      NS      H.ROOT-SERVERS.NET.
.                       518400  IN      NS      I.ROOT-SERVERS.NET.
.                       518400  IN      NS      J.ROOT-SERVERS.NET.
.                       518400  IN      NS      K.ROOT-SERVERS.NET.
.                       518400  IN      NS      L.ROOT-SERVERS.NET.
.                       518400  IN      NS      M.ROOT-SERVERS.NET.
.                       518400  IN      NS      A.ROOT-SERVERS.NET.
.                       518400  IN      NS      B.ROOT-SERVERS.NET.
.                       518400  IN      NS      C.ROOT-SERVERS.NET.
.                       518400  IN      NS      D.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET.     3600000 IN      A       198.41.0.4
B.ROOT-SERVERS.NET.     3600000 IN      A       192.228.79.201
C.ROOT-SERVERS.NET.     3600000 IN      A       192.33.4.12
D.ROOT-SERVERS.NET.     3600000 IN      A       128.8.10.90
E.ROOT-SERVERS.NET.     3600000 IN      A       192.203.230.10
F.ROOT-SERVERS.NET.     3600000 IN      A       192.5.5.241
G.ROOT-SERVERS.NET.     3600000 IN      A       192.112.36.4
H.ROOT-SERVERS.NET.     3600000 IN      A       128.63.2.53
I.ROOT-SERVERS.NET.     3600000 IN      A       192.36.148.17
J.ROOT-SERVERS.NET.     3600000 IN      A       192.58.128.30
K.ROOT-SERVERS.NET.     3600000 IN      A       193.0.14.129
L.ROOT-SERVERS.NET.     3600000 IN      A       198.32.64.12
M.ROOT-SERVERS.NET.     3600000 IN      A       202.12.27.33

;; Query time: 22 msec
;; SERVER: 192.5.5.241#53(192.5.5.241)
;; WHEN: Sun Feb 11 14:54:50 2007
;; MSG SIZE  rcvd: 436
```

Note!

```
dig NS . @192.5.5.241

; <<>> DiG 9.3.2 <<>> NS . @192.5.5.241
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45507
;; flags: qr aa rd; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 13

;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       518400  IN      NS      E.ROOT-SERVERS.NET.
.                       518400  IN      NS      F.ROOT-SERVERS.NET.
.                       518400  IN      NS      G.ROOT-SERVERS.NET.
.                       518400  IN      NS      H.ROOT-SERVERS.NET.
.                       518400  IN      NS      I.ROOT-SERVERS.NET.
.                       518400  IN      NS      J.ROOT-SERVERS.NET.
.                       518400  IN      NS      K.ROOT-SERVERS.NET.
.                       518400  IN      NS      L.ROOT-SERVERS.NET.
.                       518400  IN      NS      M.ROOT-SERVERS.NET.
.                       518400  IN      NS      A.ROOT-SERVERS.NET.
.                       518400  IN      NS      B.ROOT-SERVERS.NET.
.                       518400  IN      NS      C.ROOT-SERVERS.NET.
.                       518400  IN      NS      D.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET.     3600000 IN      A       198.41.0.4
B.ROOT-SERVERS.NET.     3600000 IN      A       192.228.79.201
C.ROOT-SERVERS.NET.     3600000 IN      A       192.33.4.12
D.ROOT-SERVERS.NET.     3600000 IN      A       128.8.10.90
E.ROOT-SERVERS.NET.     3600000 IN      A       192.203.230.10
F.ROOT-SERVERS.NET.     3600000 IN      A       192.5.5.241
G.ROOT-SERVERS.NET.     3600000 IN      A       192.112.36.4
H.ROOT-SERVERS.NET.     3600000 IN      A       128.63.2.53
I.ROOT-SERVERS.NET.     3600000 IN      A       192.36.148.17
J.ROOT-SERVERS.NET.     3600000 IN      A       192.58.128.30
K.ROOT-SERVERS.NET.     3600000 IN      A       193.0.14.129
L.ROOT-SERVERS.NET.     3600000 IN      A       198.32.64.12
M.ROOT-SERVERS.NET.     3600000 IN      A       202.12.27.33

;; Query time: 22 msec
;; SERVER: 192.5.5.241#53(192.5.5.241)
;; WHEN: Sun Feb 11 14:54:50 2007
;; MSG SIZE  rcvd: 436
```

Note!

1. The Priming Response contains only IPv4 address records for the root name servers
2. The response is a DNS message of size 436 bytes

What happens when …

we want to add IPv6 support to the root of the DNS?

- Be able to query the root name servers using an IPv6 transport instead of only being able to use IPv4 transport
- Be able to establish the IPv6 addresses of the DNS root name servers through a priming query, just like we can with IPv4 today

Implications

- Same query (NS records for “.”)
- Larger priming response
  - AAAA records in the Additional Section of the response
  - 5 servers with IPv6 = 587 byte DNS response
  - 13 servers with IPv6 =>800 byte DNS response

Implications

- RFC1035 sets a maximum DNS message size of 512 bytes
  - Larger responses require the query to have EDNS0 extension (RFC 2671) to notify the root name servers that larger that 512 byte responses can be processed
  - Intermediate systems must forward these larger DNS messages to the resolvers that issued the query
- The DNS response now has AAAA records
  - Intermediate systems that perform deep packet inspection and filtering need to allow these packets through as valid DNS priming response packets

What's the change from today?

1. DNS name servers should "understand" AAAA records in the additional section as a signal for IPv6 transport support

2. This should be the case even if the priming query is made over IPv4 transport

3. DNS name servers should support EDNS0 to signal a capability to process large (>512 byte) DNS messages

4. Middleware should not filter such priming queries or the corresponding responses

Is this going to be a problem?

- We aren't sure!
  - ICANN RSSAC and SSAC have set up an experiment
  - They invite you to test your local configuration to see if your environment is capable to supporting IPv6 AAAA records in the priming response for the DNS root
  - Details of the experiment are at:

    http://www.icann.org/committees/security/sac017.htm
  - The test runs from 1 February through to 1 May

What you should see in the test:

```
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:

            …

;; 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
```

What you should see in the test:

```
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:

            …

;; 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
```

Thank You

http://www.icann.org/committees/security/sac017.htm

Questions?