DNSSEC in the glue...
a operational tale

Peter Losher, Senior Operations Engineer, ISC
plosher@isc.org
Network Impact of DNSSEC

- Signed DNS responses are BIG
  - Have DS, NSEC, DNSKEY, & RRSig data
  - Dramatically increases query response sizes
- 512 byte UDP packets just don’t cut it
- EDNS0 is no longer “nice to have”
Just how much bigger?

- **Without DNSSEC**
  
  ```
  Jim@131-203-50-204:/data/users/jrmii> dig +nodnssec www.isc.org
  ; <<>> DiG 9.6.0-APPLE-P2 <<< +nodnssec www.isc.org
  ;; global options: +cmd
  ;; Got answer:
  ;; >>>HEADER<<<, opcode: QUERY, status: NOERROR, id: 2203
  ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 8
  
  ;; QUESTION SECTION:
  ;www.isc.org.
  
  ;; ANSWER SECTION:
  www.isc.org. 547 IN A 149.20.64.42
  
  { LOTS REMOVED }
  
  ;; Query time: 40 msec
  ;; SERVER: 131.203.1.5#53(131.203.1.5)
  ;; WHEN: Wed Jan 26 17:53:27 2011
  ;; MSG SIZE  rcvd: 320
  ```

- **With DNSSEC**
  
  ```
  Jim@Bikeshed:/data/users/jrmii> dig www.isc.org a +dnssec @204.152.187.13
  ; <<>> DiG 9.6.2-P2 <<< www.isc.org a +dnssec @204.152.187.13
  ;; global options: +cmd
  ;; Got answer:
  ;; >>>HEADER<<<, opcode: QUERY, status: NOERROR, id: 51546
  ;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 13
  
  ;; OPT PSEUDOSECTION:
  ;; EDNS: version: 0, flags: do udp: 4096
  ;; QUESTION SECTION:
  ;www.isc.org.
  
  ;; ANSWER SECTION:
  www.isc.org. 442 IN A 149.20.64.42
  www.isc.org. 442 IN RRSIG A 5 3 600 20110221233210
  20110122233210 26982 isc.org. ZPrxCONvy/c2FEKmEcEqKD7t53YCI4RL9uu3h1w6/XcuiYOAzhFA33ZG i/Q2d9Gq65cTWKf1kTyVDg68fOwpNiwc0nKlOTUoT7GWu4Q6odMx0iAh 111/dIchks5d2amB3pJMO7CMcPAily4AKfaceDss8DlHrrYTQOWyhh4RI lWw=
  
  { LOTS MORE REMOVED }
  
  ;; Query time: 1 msec
  ;; SERVER: 204.152.187.13#53(204.152.187.13)
  ;; WHEN: Wed Jan 26 05:45:12 2011
  ;; MSG SIZE  rcvd: 1623
  ```
ISC Secondary Name Service (SNS)

- Provide both free (SNS-PB) and SLA-Backed (SNS-COM) DNS Secondary Service
- 3 separate AnyCast Clouds with multiple providers
- Largely IPv6 Enabled
- Fully DNSSEC capable
More Obscure Failure Behavior

- We host a large multi-national Internet property in SNS
- Their zones were NOT signed
- Some users couldn’t successfully resolve records in that domain.
The cause of that more obscure failure

- The zone of the content provider were NOT signed
- NS records for the zone referenced records that WERE in a signed zone
- The resultant responses popped above the 512 byte limit, and we’re back at the same behavior as the simple case
Key Rollover

- Periodically the Signing Keys (KSK/ZSK) should be changed
- During the period while ANY server could be passing out the old key, both the old and new keys are included in responses
- Yupp, that response just got bigger!
- This mostly impacts places where EDNS0 is enabled, but a “conservative” (often 1K) limit is chosen
But I don’t have a problem.... really!

• You sure? Use the OARC Reply Size test!

• When it works:

```
Jim@131-203-50-204:/> dig +short rs.dns-oarc.net txt
rst.x4091.rs.dns-oarc.net.
rst.x3837.x4091.rs.dns-oarc.net.
rst.x3843.x3837.x4091.rs.dns-oarc.net.
"Tested at 2011-01-26 03:52:33 UTC"
"202.53.189.253 sent EDNS buffer size 4096"
"202.53.189.253 DNS reply size limit is at least 4091"
```

• When it doesn’t:

```
rivendel:~ jim$ dig +short rs.dns-oarc.net txt
rst.x476.rs.dns-oarc.net.
rst.x485.x476.rs.dns-oarc.net.
rst.x490.x485.x476.rs.dns-oarc.net.
"68.87.76.181 DNS reply size limit is at least 490"
"68.87.76.181 lacks EDNS, defaults to 512"
"Tested at 2011-01-26 05:56:41 UTC"
```
BIND

- Has been doing EDNS0 since 8.3.0
- Got DNSSEC (bis) in 9.3.0
- BUT has known flaws for anything before 9.4-ESV
- It’s highly recommended that you run 9.7.2-P3 or 9.6-ESV-R3
Key Take Aways

• Make sure all your network elements that touch DNS can do EDNS0 and allow 4K responses

• Make sure any network security elements allow IP Fragments

• Use the reply size tester to validate your systems and to identify customer problems

• Educate your customer base.
References

- **DNSSEC**
  http://dnssec.net/

- **Test Tools**
  https://www.dns-oarc.net/oarc/services/replysizetest

- **Name Server (BIND)**
  http://www.isc.org
  http://www.isc.org/software/bind/versions
Questions?

• While you’re thinking of questions:

  • If you want to peer with F-Root, send mail to peering@isc.org

  • We host public-benefit organizations through our Hosted@ and SNS-PB programs. Contact {hosted,sns}@isc.org

  • Remember ISC is a public-benefit and survives through donations, forum memberships, SNS-Com and support contracts.

  • We appreciate any help, and need it to keep doing good work!