Where we came from

- Wish to add AAAA for the Root Servers
- Priming process not formally specified, no BCP document
- WG adopted individual submission
Q1: Root Server Address Validation

- Do we want DNSSEC validation of the Root Servers’ Addresses in the Priming Response?

**Pro:** Could protect crucial part of the process

**Con:** We’ve never done that
Q2: Should the Priming Response be self contained?

- Should *all* information (full trust chain) be in the Priming Response?
  - Root NS RRSet
  - A and AAAA RRSets (up to 26)
  - *all* KSKs and ZSKs necessary (including RRSIGs)
Q3.1: How much special casing for the Priming Response?

- Adding Root KSK/ZSK and all other keys to additional section?
- How does the server know it’s a Priming Query? Does it matter?
Q3.2: Prime by asking for the Root’s DNSKEY?

• Query for Root DNSKEY gives
  – DNSKEY RRSet plus RRSIGs
  – NS RRSet in authority section,
  – addresses plus RRSIGs in additional section

• triggered by the presence of a Root Trust Anchor

• How to ensure completeness? (size is an issue)

• (still missing NET’s, ROOT-SERVERS.NET’s keys)
Q3.3: Renaming the Root Servers . . . ?

- If renaming the Root Servers would simplify 3.2, what would be the operationally optimal naming scheme?
- Move from NET to ARPA?
- Even move the names up the tree?
Q4: Emphasize need for logging?

- Security section suggests logging inconsistent (with hints) Priming Response
- Relocate that to (new) section 3.3?
Q5: TTL synchronization issue

- What happens if resolver expires Root Servers A and AAAA RRSets at different times?
- Can we avoid that? How and Where?
Thank You!