

# Clarifications to the DNS Ranking Data

- **draft-fujiwara-dnsop-ranking-data-01**

**Kazunori Fujiwara**

Japan Registry Services Co., Ltd.

Japan

Email: [fujiwara@jprs.co.jp](mailto:fujiwara@jprs.co.jp)

**Willem Toorop**

NLnet Labs

Science Park 400

1098XH Amsterdam

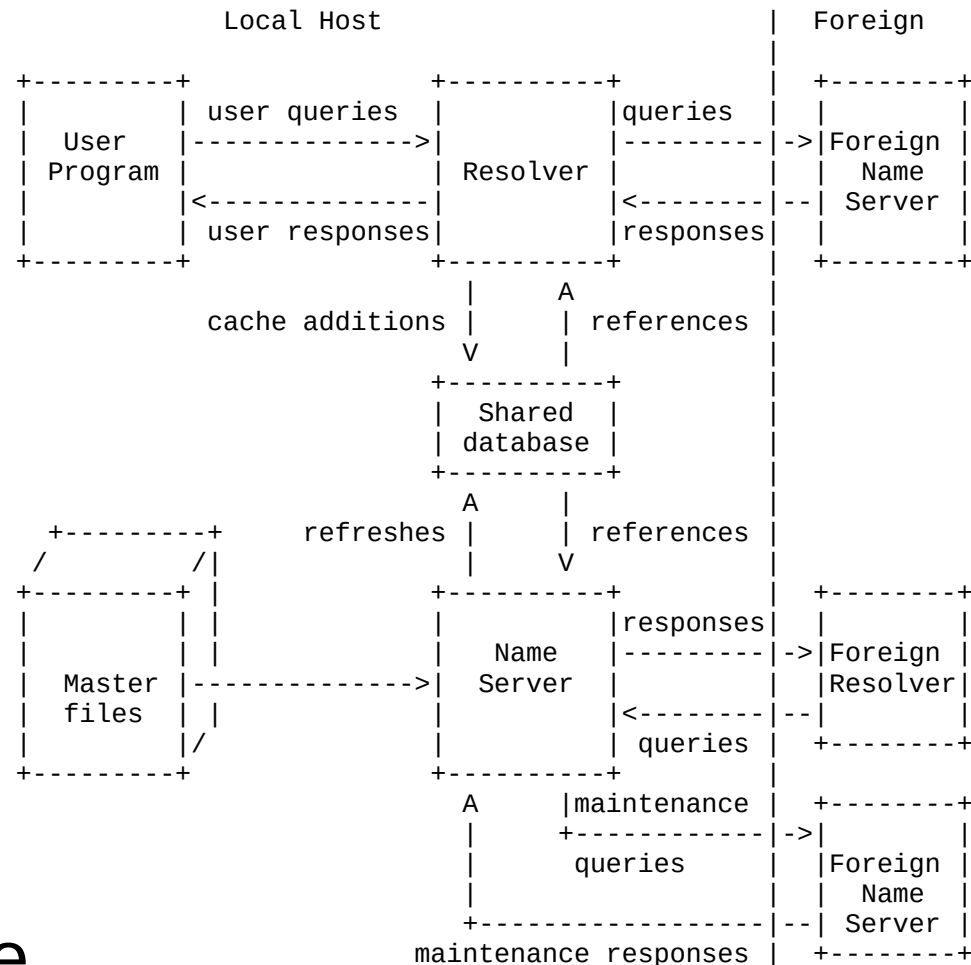
Netherlands

Email: [willem@nlnetlabs.nl](mailto:willem@nlnetlabs.nl)

- Obsolete **Section 5.4.1 (Ranking data) of RFC 2181**
- Specify directives whereby the source of the data determines for what purposes it may be used

# Section 5.4.1 (Ranking data) of RFC 2181

- Assumes mixed Authoritative / Recursive Resolver DNS server
- Assumes that
  - zone files
  - zone transfers
  - and name resolutionwill be mixed together
- This is no longer the practice



# Section 5.4.1 (Ranking data) of RFC 2181

- Only indicates priority  
Not validity
  - Attacks with unnecessary additional data have been reported
  - Unnecessary data should be discarded
1. Data from a primary zone file, other than glue
  2. Data from a zone transfer, other than glue
  3. Authoritative data in the ANSWER section
  4. The AUTHORITY section of an authoritative answer
  5. Glue from a zone file or zone transfer
  6. The ANSWER section of a non-authoritative answer, and Non-authoritative data from the ANSWER section
  7. Additional information from an authoritative answer, The AUTHORITY section of a non-authoritative answer, Additional information from non-authoritative answers.

# Directives

1. Authoritative servers **MUST NOT** merge zone data
2. Name resolution results (Answers, NXDOMAIN & NODATA) **MUST be** authoritative responses with data from authoritative servers that have authority through delegation
3. Non-authoritative responses from authoritative servers **MUST only be used** to query the delegated authoritative server during the name resolution
4. Names and IP addresses of authoritative name servers for zones that are built-in or loaded from "hints" files, **MUST only be used** for priming a resolver for those zones

# Directives (new in version -01)

5. Name servers with multiple functions that act as
    - Authoritative, Recursive Resolver or Forwarder depending on
      - the namespace to which the query name belongs,
      - the server IP address,
      - the "Recursion Desired" bit, etc.
- The data handled by each function **MUST be** separated

# Additional considerations

- Recursive Resolvers **SHOULD only** accept the following data from authoritative servers:
  - NS and DS RRsets (+RRSIG) in the Authority Section of the delegation response and Glue A/AAAA in the Additional Section,
  - SOA RRs (+RRSIG) in the Authority Section of authoritative NXDOMAIN and NODATA responses in response to the query,
  - the Answer Section (+RRSIG) of the authoritative response in response to the query, and
  - any data from the additional section allowed by type (for the delegated domain name),and **SHOULD NOT** accept any other information.

# Additional considerations

- The Additional Section returned as the result of name resolution **MUST** be exactly the same as the Additional Section that came from the authoritative response from the authoritative server, or a separate authoritative response resulting from name resolution

# Clarifications to the DNS Ranking Data

- **draft-fujiwara-dnsop-ranking-data-01**

**Kazunori Fujiwara**

Japan Registry Services Co., Ltd.

Japan

Email: [fujiwara@jprs.co.jp](mailto:fujiwara@jprs.co.jp)

**Willem Toorop**

NLnet Labs

Science Park 400

1098XH Amsterdam

Netherlands

Email: [willem@nlnetlabs.nl](mailto:willem@nlnetlabs.nl)

- Working group interested in working on this?