An Automated Synchronization Mechanism for Configuration Data of DNS Name Servers

(draft-kong-dns-conf-auto-sync-01)

Ning Kong

DNSOP

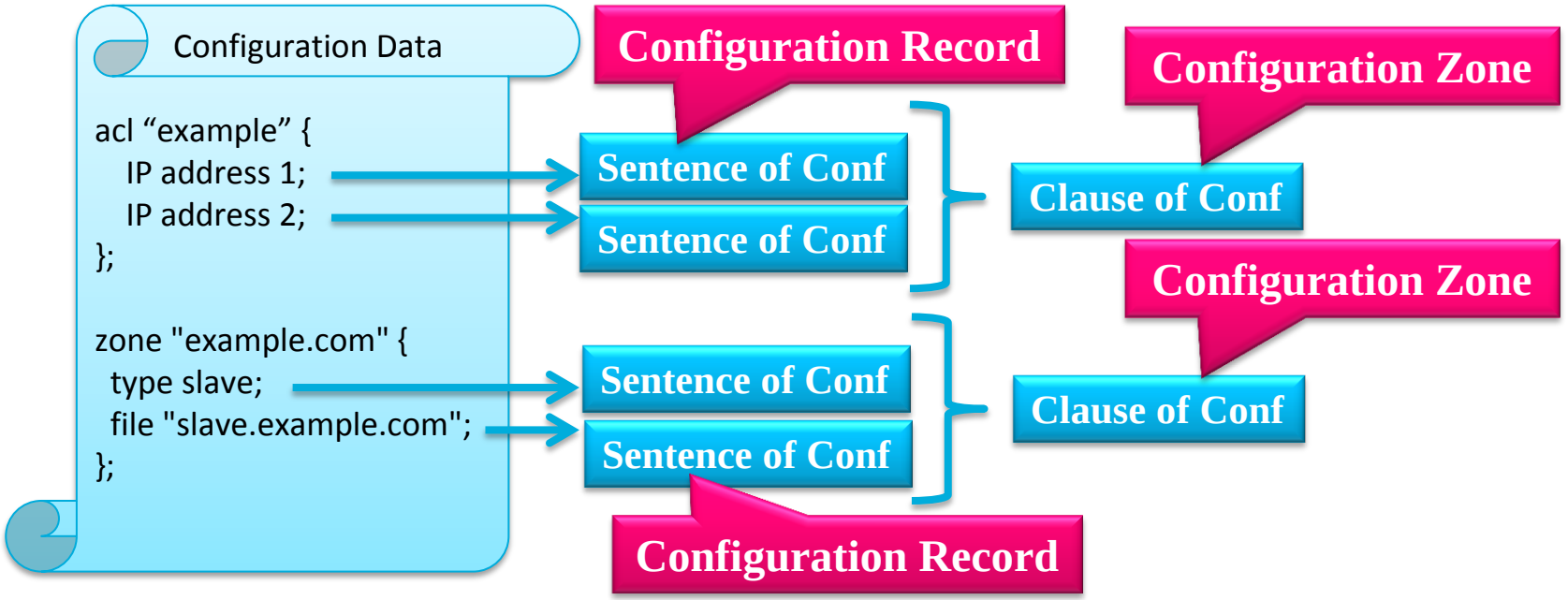
November 11, 2010

Overview

- By the proposed mechanism, some configuration zones containing several configuration records which are similar to DNS RRs can be constructed from configuration data.
- Once a configuration zone has been changed, the performing name server will advise a set of other name servers within a predefined Notify Set of the modification.
- If the notification could be verified, the notified name servers could request the new configuration data via the current DNS messaging mechanism and then do the re-configuration according to the obtained configuration data.

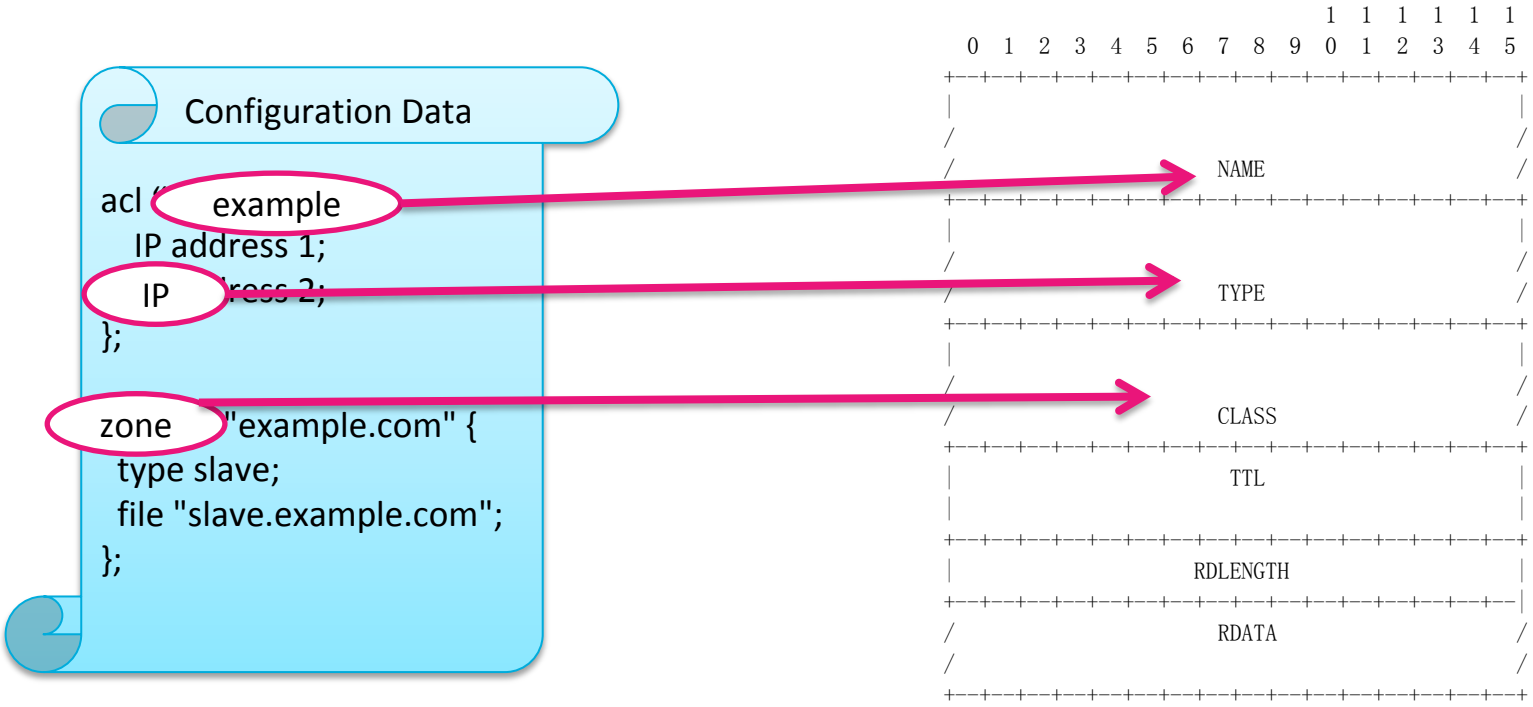
Configuration Zone and Record

- The configuration data of a name server can be constructed as some similar DNS zones, and these kind of zones are named as Configuration Zone (CZ).
- Each item of a Configuration data can be constructed as Configuration Record (CR).



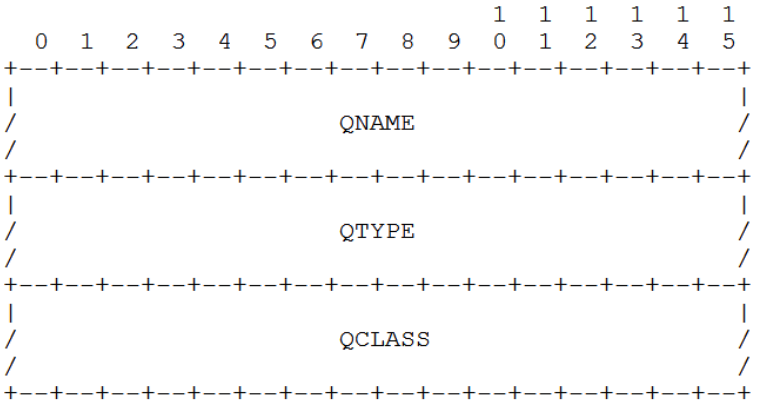
Format of CRs

- All CRs have the same top level format which is defined in section 3.2.1 of [RFC1035], with some fields redefined.



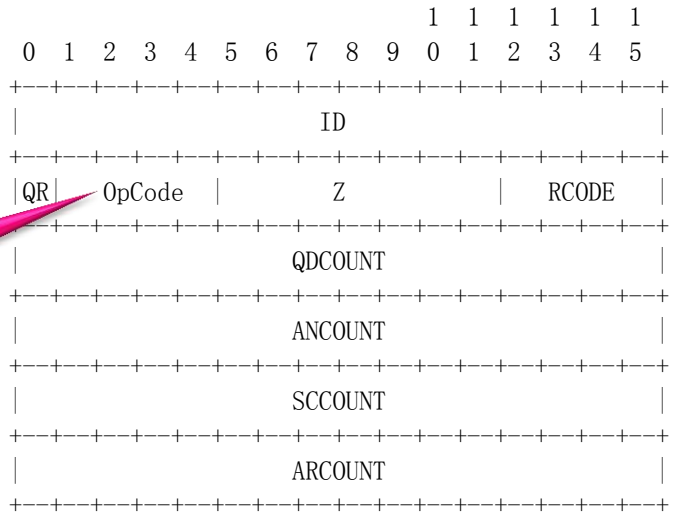
Messages

- The automated synchronization mechanism uses the DNS message format defined by [RFC1035], although it makes some extensions and overload some fields.



Question Section

Header Section



New OpCode needs to be assigned by IANA

Class and Type

- The definitions of Classes and Types should be expected, which are used to express specific configuration items.
- Note that the list of Classes and Types which is necessary to be defined in future need to be discussed, and then the new TYPE, CLASS and RDATA formats should be defined later.
  - the “Zone” Class used to contain configuration data for DNS zones
    - the “Zone_Transfer” Type used to contain “AXFR” or “IXFR”
  - the “ACL” Class used to contain configuration data for access control list
    - the “IP” Type used to contain the IP address

NOTIFY

- The mechanism of NOTIFY is the similar with DNS NOTIFY defined by [RFC1996].
- By the function of NOTIFY, a name server may advises a set of other name servers within a predefined Notify Set of a CZ that the CZ's data has been changed and that a query should be initiated to request the new data.
- A new OpCode for NOTIFY needs to be assigned by IANA.

Transport

- The transport of the messages is the same as the one of standard DNS message defined by section 4.2 of [RFC1035]. Both UDP and TCP are acceptable, but TCP is recommended.
- The mechanisms for DNS zone transfer (AXFR [RFC5936] and IXFR [RFC1995]) could be used for CZ transfer.

Security considerations

- Because the configuration data of a name server can be synchronized by other name servers using this solution, it's possible that the behavior and functionality of a name server will be maliciously modified by other name server.
- So any implementation of this document is strongly suggested to realize the Access Set of CZ and the Synchronization Set of CZ.
- Access Set of CZ: A set of name servers to be allowed to access (acquire) the zone data of a CZ.
- Synchronization Set of CZ: A set of name servers to be allowed to synchronize (modify) the zone data of a CZ.
- Moreover, TSIG is supposed to be used for authentication.

Meeting the Requirements

- Requirements for Management of Name Servers for the DNS (draft-ietf-dnsop-name-server-management-reqs-04)
  - 3.2. Configuration Requirements
    - 3.2.1. Served Zone Modification
    - 3.2.2. Trust Anchor Management
    - 3.2.3. Security Expectations
    - 3.2.4. TSIG Key Management
    - 3.2.5. DNS Protocol Authorization Management

Meeting the Requirements

- Efficiency
  - The configuration data of a name server might be frequently modified, for example, some name servers needs to be added or removed numerous zones within an hour [draft-ietf-dnsop-name-server-management-reqs-04].
  - The configuration data among multiple name servers SHOULD be efficiently synchronized, because the number of name servers could be significantly large and the service of DNS should be prompt for the Internet users.
- Generality
  - The requirement of synchronizing the configuration data among different name server implementations (such as BIND, NSD, LDNS, Unbound…) SHOULD be considered.

Meeting the Requirements

- Variety
  - The different parts of the configuration data of a name server maybe need to be shared with other different name servers.
- Security
  - The configuration data could be used to configure the behavior and functionality of a name server, so the modification or synchronization of configuration data MUST be under some absolutely safe ways.

Questions

nkong@cnnic.cn