Do We Need an Automated Synchronization Mechanism for Configuration Data of DNS Name Servers?

Ning Kong

October, 2010

CNNIC
中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

Contents

1 Motivation

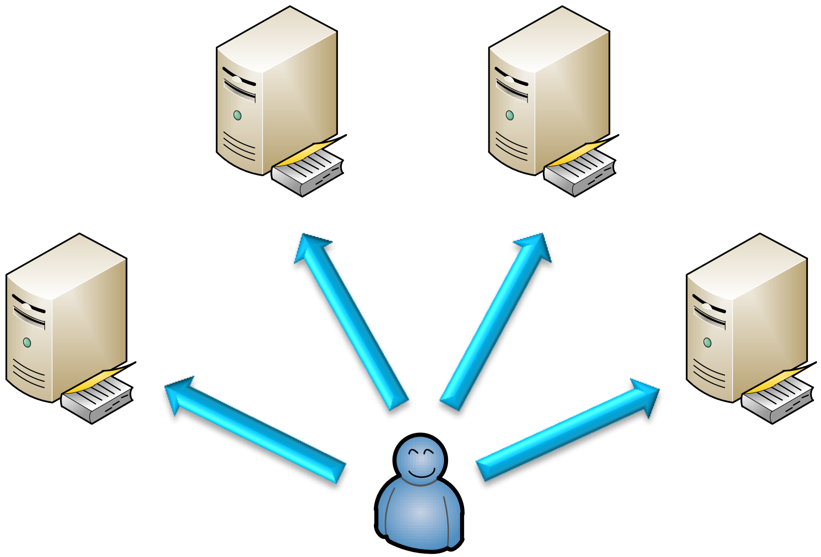
2 Requirements

3 Possible Solutions

4 Discussions

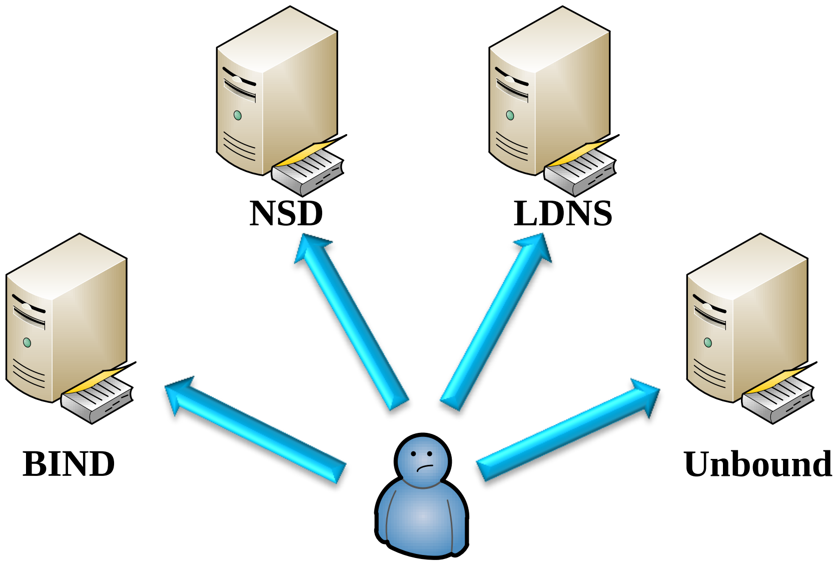
Motivation

- Each name server needs to be instructed by some configuration data, which is normally used to configure the behavior and functionality of the name server.
- Normally, these configuration data are managed by a local system administrator.



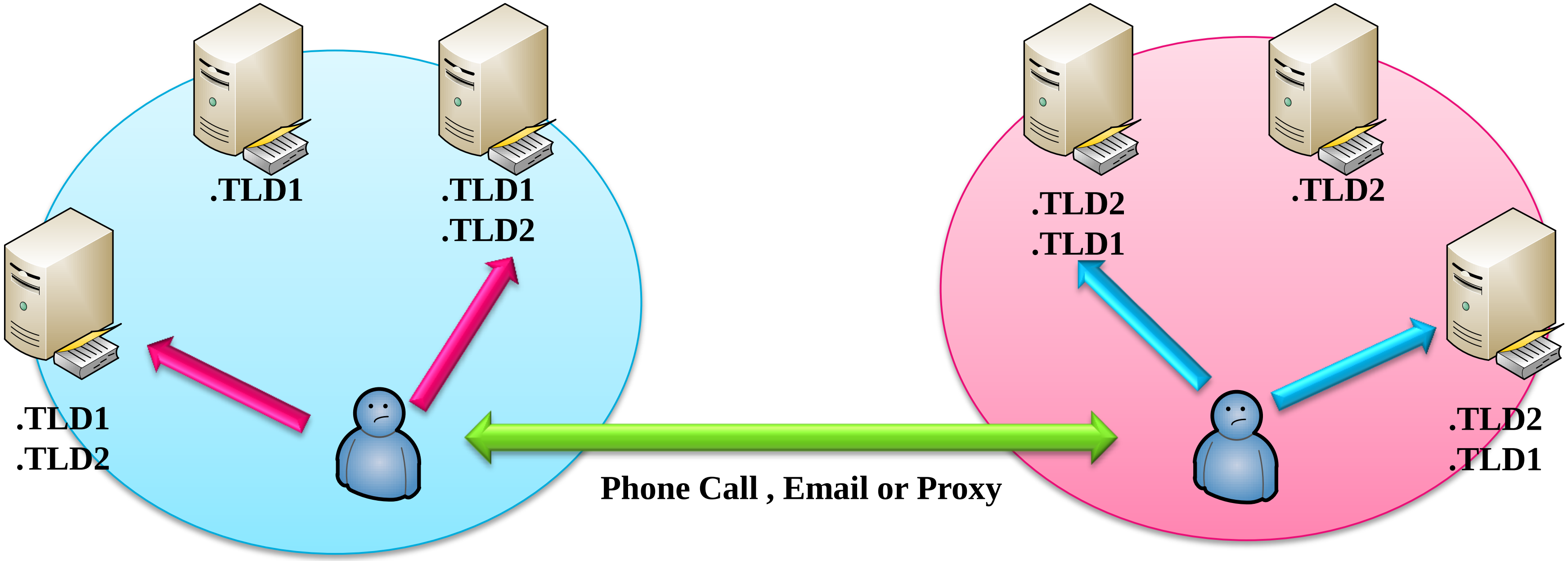
Motivation

- Organizations usually run their name servers implemented by different software, such as BIND, NSD, LDNS, Unbound and so on.
- It becomes more difficult to configure all kinds of name servers for a local system administrator.



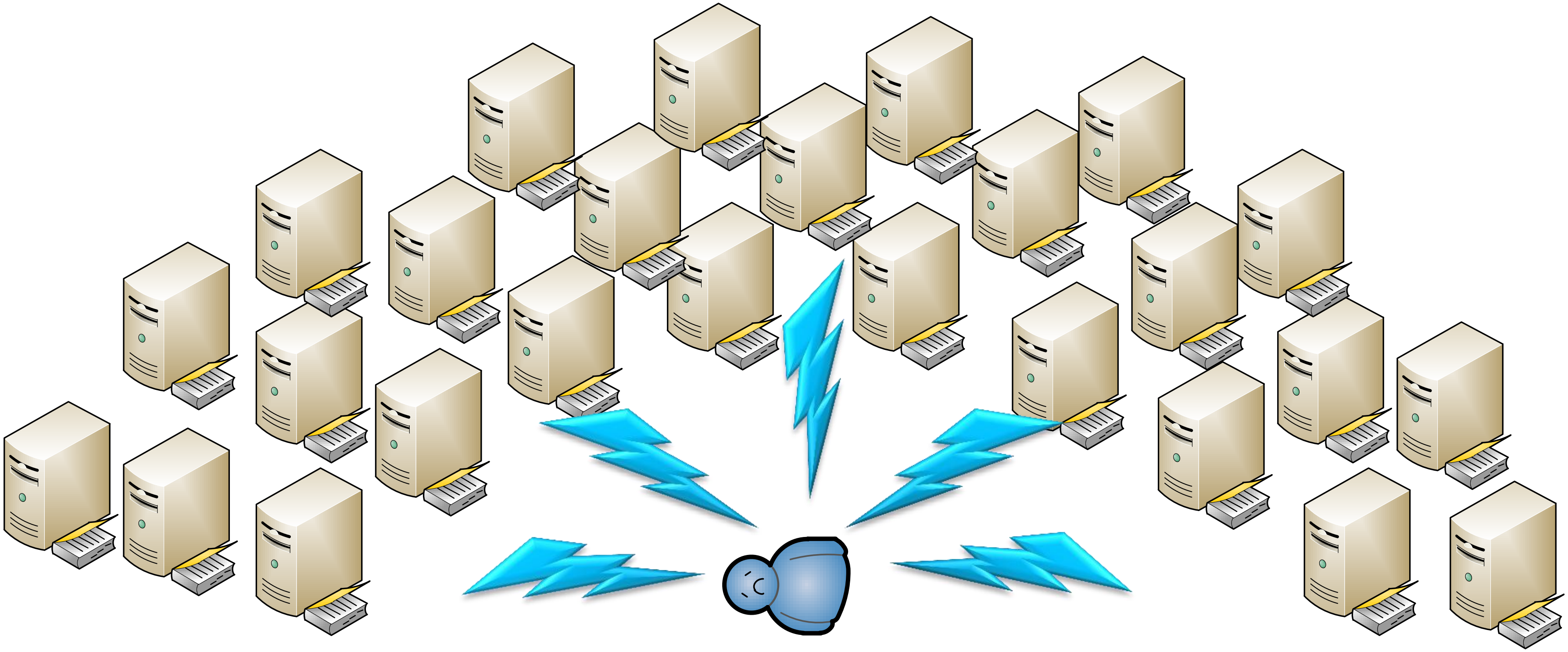
Motivation

- For reliability reasons it is recommended that zone operators follow the guidelines documented in [RFC2182] which recommends that multiple name servers be configured for each zone and that the name servers are separated both physically and via connectivity routes.



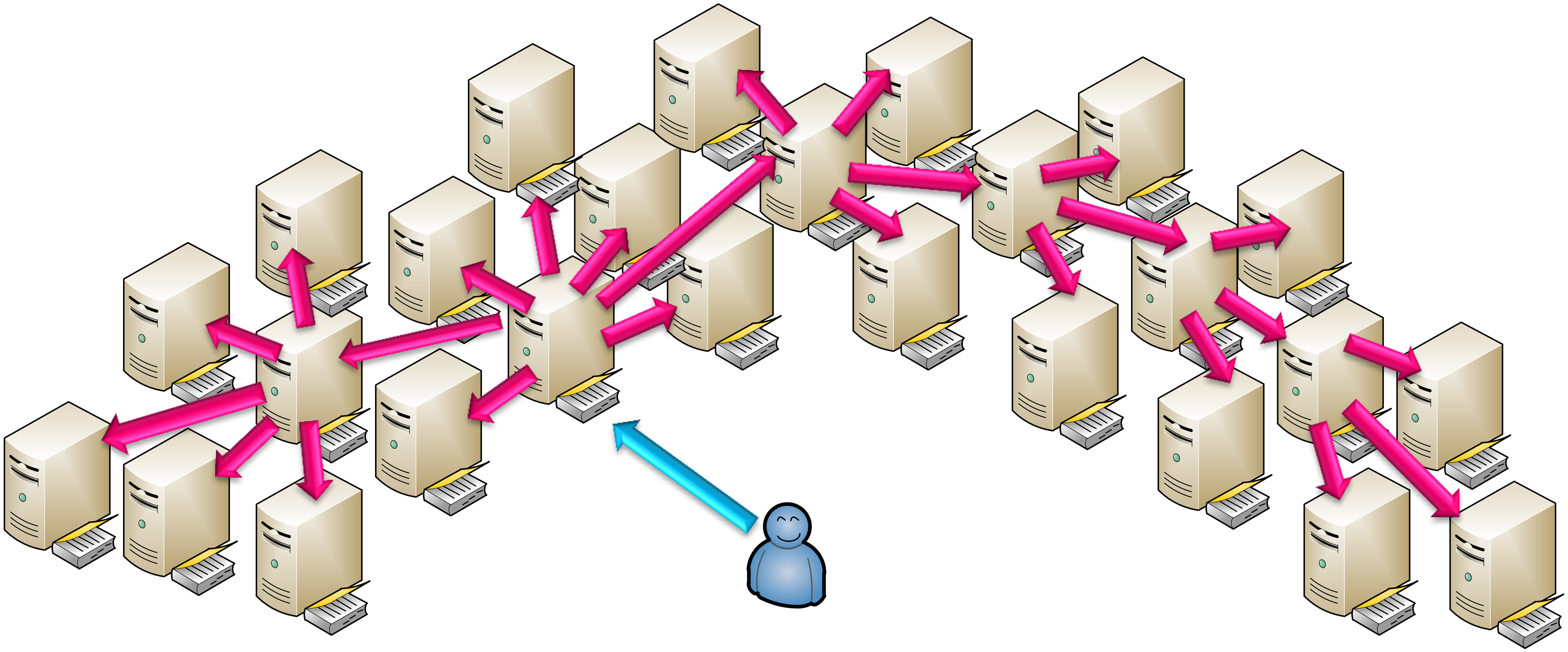
Motivation

- Organizations usually run a fair number of name server implementations to improve their SLA .
- The manual operations of the configuration data turn into heavy burden for administrators.



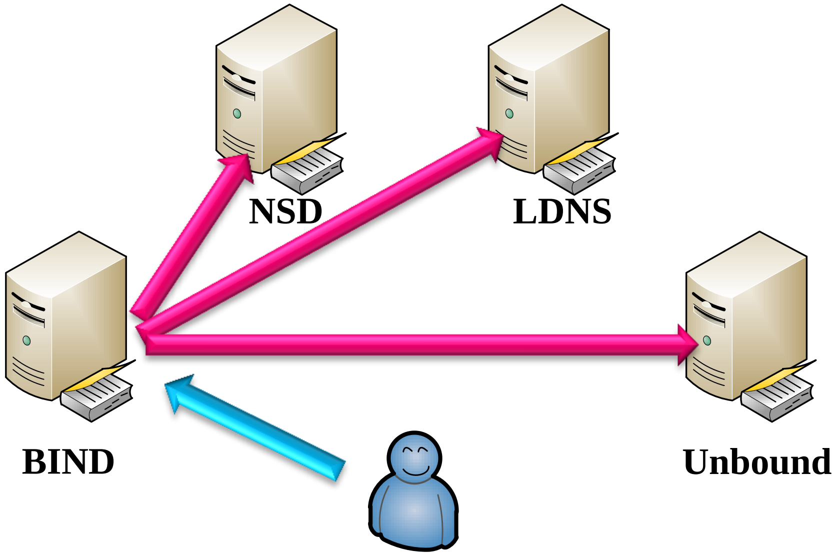
Motivation

- An automated synchronization mechanism for configuration data can simplify administration and reduce cost.



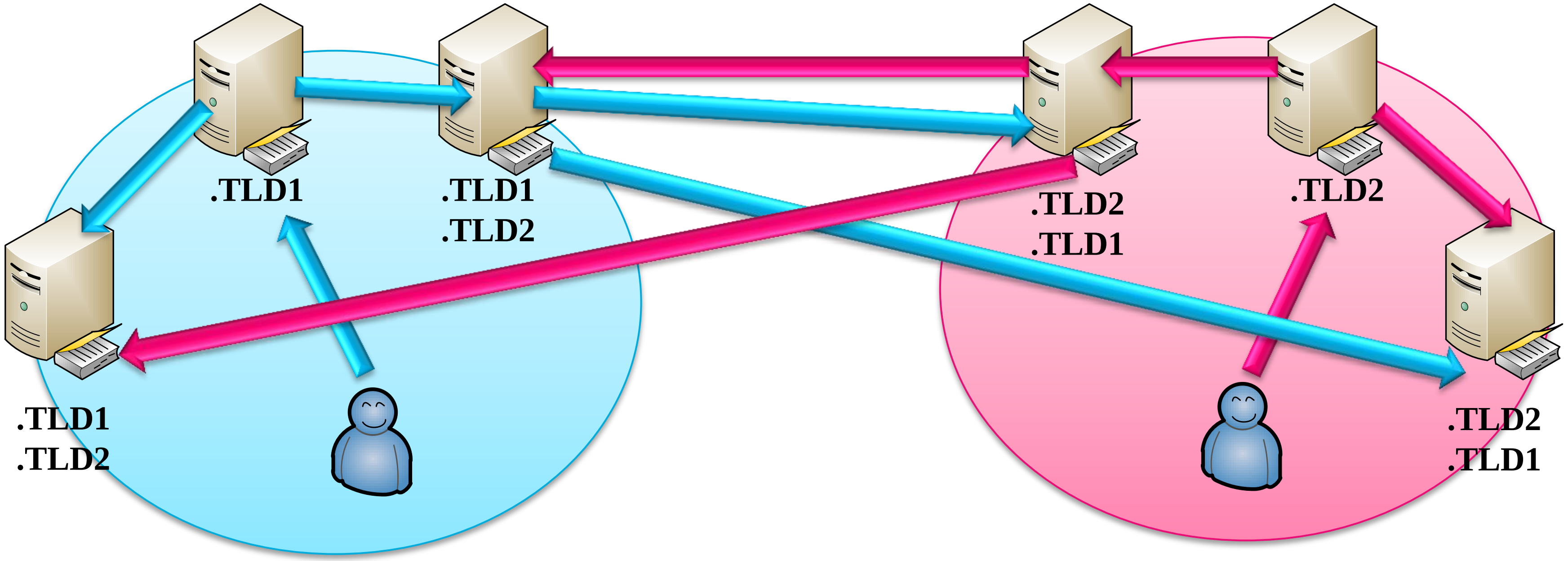
Motivation

- An automated synchronization mechanism for configuration data can simplify administration and reduce cost.



Motivation

- An automated synchronization mechanism for configuration data can simplify administration and reduce cost.



Contents

1 Motivation

2 Requirements

3 Possible Solutions

4 Discussions

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.

Requirements

- **Variety**
  - ✓ The different parts of the configuration data of a name server maybe need to be shared with other different name servers.
  - ✓ The relationship of synchronization among name servers might be dynamically changed.

- **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.

Contents

1 **Motivation**

2 **Requirements**

3 **Possible Solutions**

4 **Discussions**

Possible Out-Band Solutions

- **SNMP-based solution (RFC 1611, RFC 1612)**
  - ✓ DNS MIB objects have been defined by this solution to be used in conjunction with the Internet MIB to allow access to and control of DNS name server software via SNMP by the Internet community.
  - ✓ But this solution is failed to achieve significant implementation and deployment.
  - ✓ RFC 1611 and RFC 1612 have been reclassified as Historical documents by RFC 3197. The reasons behind the failure for the two MIB modules are further documented in RFC3197.

Possible Out-Band Solutions

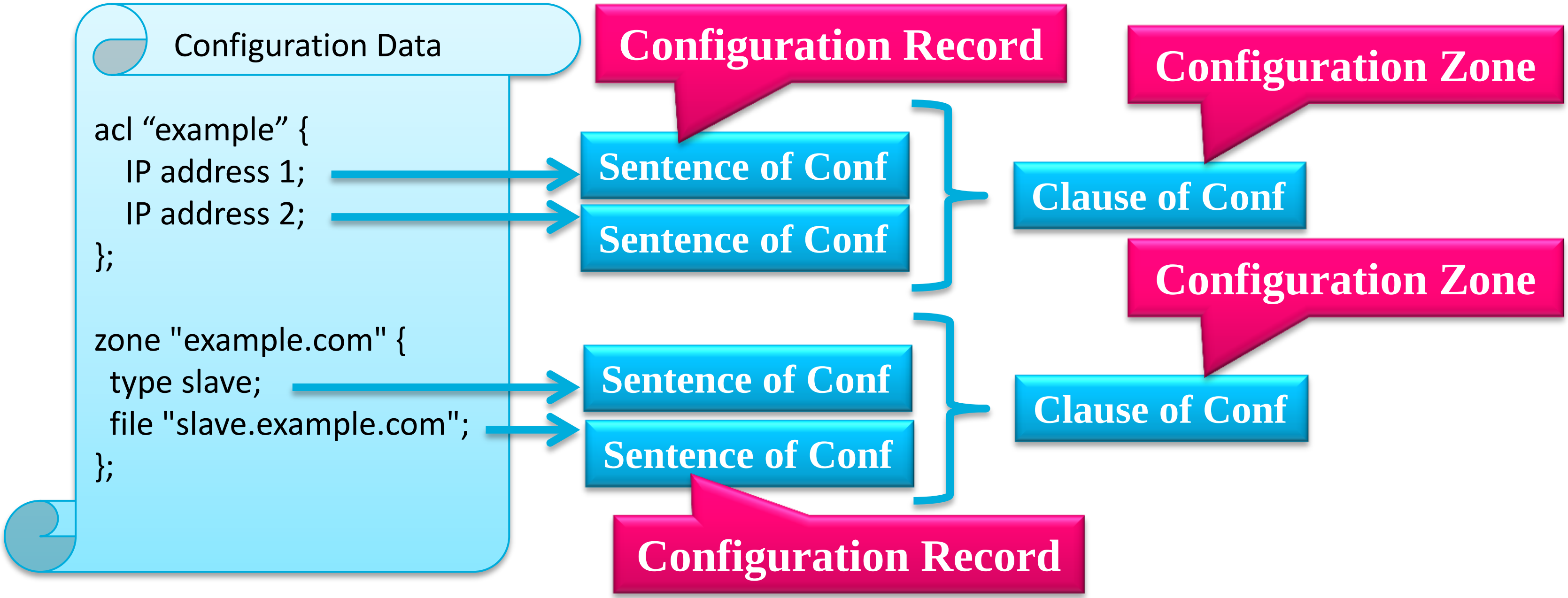
- **NETCONF and YANG based solution**

  (draft-dickinson-dnsop-nameserver-control-00)

  - ✓ This solution proposes a nameserver control protocol (NSCP) based on a formal modeling language (YANG) and NETCONF. Using NSCP, a suitable client should be able to communicate with and manage any name server implementing the protocol.
  - ✓ This draft is expired now.
  - ✓ Maybe this idea is feasible, and worthy of further study.
  - ✓ There will be a formal BoF named NSCP (Name Server Control Protocol) at IETF 79, and this idea will be further discussed at this BoF meeting.

Possible In-Band Solution

- **Configuration Zone solution**
  (draft-kong-dns-conf-auto-sync-01)
  - ✓ Using this solution, the configuration data of a name server can be constructed as some similar DNS zone data, which is named as Configuration Zone, and be automatically synchronized by DNS messaging and similar notifying mechanisms.



Configuration Data

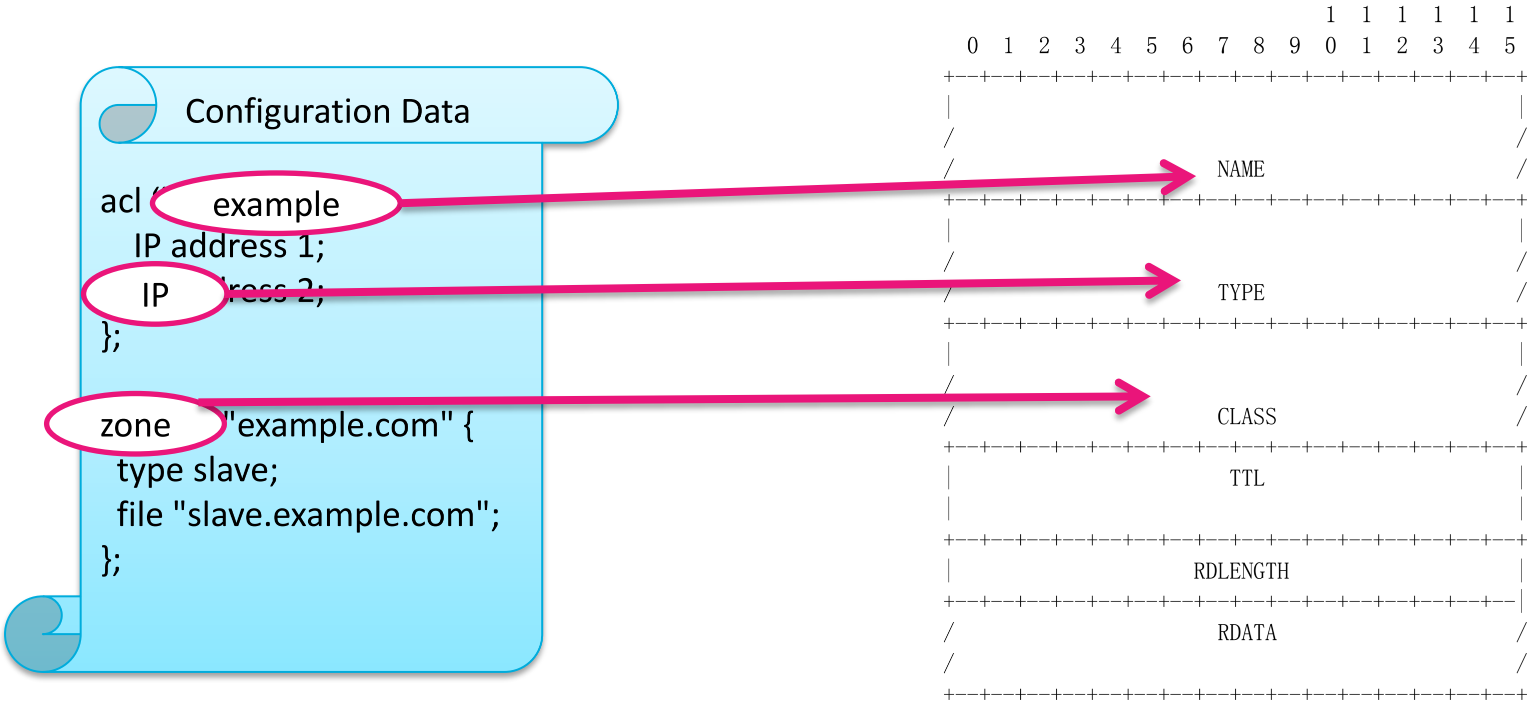
```
acl “example” {
   IP address 1;
   IP address 2;
};

zone "example.com" {
  type slave;
  file "slave.example.com";
};
```

Possible In-Band Solution

➢ Configuration Zone solution

- ✓ Whenever synchronization is to be done from one name server to others, several Configuration Zone (CZ) files which is similar to DNS zone files are constructed and Configuration Records (CR) are included in the CZ files in the following formats.



Configuration Data

```
acl example
   IP address 1;
IP address 2;
};

zone "example.com" {
  type slave;
  file "slave.example.com";
};
```

```
                                    1  1  1  1  1  1
      0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |                                               |
    /                                               /
    /                      NAME                     /
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |                                               |
    /                                               /
    /                      TYPE                     /
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |                                               |
    /                                               /
    /                      CLASS                    /
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |                       TTL                     |
    |                                               |
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |                    RDLENGTH                   |
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--|
    /                     RDATA                     /
    /                                               /
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

Possible In-Band Solution

Configuration Zone solution

- ✓ Once a CZ has been changed, the performing name server will advises a set of other name servers within a predefined Notify Set of the change.
- ✓ If the identity of the notification could be verified, the notified name servers could request the new data via the current DNS messaging mechanism and do the re-configuration according to the obtained configuration data.

```
                                    1  1  1  1  1  1
  0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                      ID                       |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|QR|   OpCode   |          Z          |  RCODE   |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    QDCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ANCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    SCCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ARCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

New OpCodes need to be assigned by IANA

Possible In-Band Solution

- **Configuration Zone solution**
  - ✓ Every CZ SHOULD has a standard CR named SERIAL, which used to indicate the version of a CZ.
  - ✓ The definitions of other CRs should be expected, which are used to express specific configuration items used to control some kind of behavior or functionality of a name server.
  - ✓ Note that the list of other CRs which are necessary to be defined here need to be discussed, and then the new TYPE, CLASS and RDATA formats of these CRs should be defined later.
    - the CR used to contain configuration data for DNS zones
    - the CR used to contain configuration data for access control list
    - the CR used to contain configuration data for DNS logging
    - and so on

Possible In-Band Solution

Configuration Zone solution

- ✓ 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.

Contents

1 Motivation

2 Requirements

3 Possible Solutions

4 Discussions

Discussions

- **Do we need to develop an automated synchronization mechanism for configuration data of DNS name servers?**

- **Which kind of resolution (out-band or in-band) suits best?**
  - Out-Band
    - SNMP?
    - NETCONF?
    - Other solutions?
  - In-Band
    - Configuration Zone?
    - Other solutions?

谢谢.中国

中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

中国和谐信息社会重要的基础设施建设者、运行者和管理者

北京市海淀区中关村南四街四号中科院软件园　　邮编: 100190

www.cnnic.cn