Writing Zone Files

Presented by Joe Abley
SANOG 4, 2004

Writing a zone file.

- Zone file is written by the zone administrator
- Zone file is read by the master server and it's content is replicated to slave servers
- What is in the zone file will end up in the database

- Because of timing issues it might take some time before the data is actually visible at the client side.

First attempt

- The 'header' of the zone file
  - Start with a SOA record
  - Include authoritative name servers and, if needed, glue
  - Add other information

- Add other RRs

- Delegate to other zones

The SOA record
Line break   **Comments**

```
secret-wg.org. 3600 IN SOA bert.secret-wg.org. (
                    olaf\.kolkman.ripe.net.
                    2002021301    ; serial
                    1h            ; refresh
                    30M           ; retry
                    1W            ; expiry
                    3600 )        ; neg. answ. ttl
```

- Olaf.Kolkman@ripe.net ➜ olaf\.kolkman.ripe.net
- Serial number: 32bit circular arithmetic
  - People often use date format
  - To be increased after editing
- The timers above qualify as reasonable

Authoritative NS records and related A records

```
secret-wg.org.          3600 IN NS  bert.secret-
wg.org.
secret-wg.org.          3600 IN NS  NS2.secret-wg.org.
bert.secret-wg.org.     3600 IN A  193.0.0.4
NS2.secret-wg.org.      3600 IN A  193.0.0.202
```

- NS record for all the authoritative servers.
  - They need to carry the zone at the moment you publish
- A records only for "in-zone" name servers.
  - Delegating NS records might have glue associated.

Other 'APEX' data

```
secret-wg.org. 3600 IN MX  50 mailhost.secret-wg.org.
secret-wg.org. 3600 IN MX  150 mailhost2.secret-wg.org.

secret-wg.org. 3600 IN LOC (
        52 21 23.0 N 04 57 05.5 E 0m 100m 100m 100m )
secret-wg.org. 3600 IN TXT  "Demonstration and test zone"
```

Examples:
- MX records for mail
  (see next slide)
- Location records

TXT records
A records
KEY records for dnssec

Intermezzo: MX record

- SMTP (simple mail transfer protocol) uses MX records to find the destination mail server.
- If a mail is sent to olaf@ripe.net the sending mail agent looks up 'ripe.net MX'
- MX record contains mail relays with priority.
  - ◆ The lower the number the higher the priority.

- Don't add MX records without having a mail relay configured.

Other data in the zone

```
localhost.secret-wg.org. 3600 IN A 127.0.0.1

bert.secret-wg.org.    4500 IN A 193.0.0.4
www.secret-wg.org.     3600 IN CNAME bert.secret-wg.org.
```

- Add all the other data to your zone file.
- Some notes on notation.
  - ◆ Note the fully qualified domain name including trailing dot.
  - ◆ Note TTL and CLASS

Zone file format short cuts nice formatting

```
secret-wg.org.            3600  IN SOA bert.secret-wg.org. (
                                    olaf\.kolkman.ripe.net.
                                    2002021301  ; serial
                                    1h          ; refresh
                                    30M         ; retry
                                    1W          ; expiry
                                    3600 )      ; neg. answ. Ttl
secret-wg.org.            3600 IN NS    bert.secret-wg.org.
secret-wg.org.            3600 IN NS    NS2.secret-wg.org.
secret-wg.org.            3600 IN MX    50 mailhost.secret-wg.org.
secret-wg.org.            3600 IN MX    150 mailhost2.secret-wg.org.

secret-wg.org.            3600 IN LOC   ( 52 21 23.0 N 04 57 05.5 E
                                          0m 100m 100m 100m )
secret-wg.org.            3600 IN TXT   "Demonstration and test zone"
bert.secret-wg.org.       4500 IN A     193.0.0.4
NS2.secret-wg.org.        3600 IN A     193.0.0.202
localhost.secret-wg.org.  3600 IN A     127.0.0.1

bert.secret-wg.org.       3600 IN A     193.0.0.4
www.secret-wg.org.        3600 IN CNAME bert.secret-wg.org.
```

Zone file format short cuts: repeating last name

```
secret-wg.org.            3600  IN SOA bert.secret-wg.org. (
                                    olaf\.kolkman.ripe.net.
                                    2002021301  ; serial
                                    1h          ; refresh
                                    30M         ; retry
                                    1W          ; expiry
                                    3600 )      ; neg. answ. Ttl
                          3600 IN NS    bert.secret-wg.org.
                          3600 IN NS    NS2.secret-wg.org.
                          3600 IN MX    50 mailhost.secret-wg.org.
                          3600 IN MX    150 mailhost2.secret-wg.org.

                          3600 IN LOC   ( 52 21 23.0 N 04 57 05.5 E
                                          0m 100m 100m 100m )
                          3600 IN TXT   "Demonstration and test zone"
bert.secret-wg.org.       3600 IN A     193.0.0.4
NS2.secret-wg.org.        3600 IN A     193.0.0.202

localhost.secret-wg.org.  4500 IN A     127.0.0.1

bert.secret-wg.org.       3600 IN A     193.0.0.4
www.secret-wg.org.        3600 IN CNAME bert.secret-wg.org.
```

Zone file format short cuts: default TTL

```
$TTL    3600 ; Default TTL directive
secret-wg.org.            IN SOA bert.secret-wg.org. (
                                    olaf\.kolkman.ripe.net.
                                    2002021301  ; serial
                                    1h          ; refresh
                                    30M         ; retry
                                    1W          ; expiry
                                    3600 )      ; neg. answ. Ttl
                          IN NS    bert.secret-wg.org.
                          IN NS    NS2.secret-wg.org.
                          IN MX    50 mailhost.secret-wg.org.
                          IN MX    150 mailhost2.secret-wg.org.

                          IN LOC   ( 52 21 23.0 N 04 57 05.5 E
                                     0m 100m 100m 100m )
                          IN TXT   "Demonstration and test zone"
bert.secret-wg.org.       IN A     193.0.0.4
NS2.secret-wg.org.        IN A     193.0.0.202

localhost.secret-wg.org.  IN A          127.0.0.1

bert.secret-wg.org. 4500 IN A          193.0.0.4
www.secret-wg.org.       IN CNAME bert.secret-wg.org.
```

Zone file format short cuts: ORIGIN

```
$TTL    3600 ; Default TTL directive
$ORIGIN secret-wg.org.
@                   IN SOA bert (
                                    olaf\.kolkman.ripe.net.
                                    2002021301  ; serial
                                    1h          ; refresh
                                    30M         ; retry
                                    1W          ; expiry
                                    3600 )      ; neg. answ. Ttl
                    IN NS   bert
                    IN NS   NS2
                    IN MX   50 mailhost
                    IN MX   150 mailhost2

                    IN LOC  ( 52 21 23.0 N 04 57 05.5 E
                              0m 100m 100m 100m )
                    IN TXT   "Demonstration and test zone"
bert                IN A     193.0.0.4
NS2                 IN A     193.0.0.202

localhost           IN A     127.0.0.1

bert        4500 IN A     193.0.0.4
www              IN CNAME bert
```
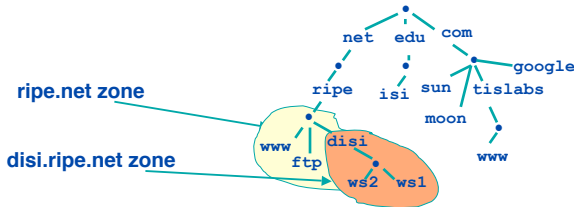
Delegating a zone (becoming a parent)

- Delegate authority for a sub domain to another party (splitting of disi.ripe.net from ripe.net)

Concept: Glue

- Delegation is done by adding NS records:

  ```
  disi.ripe.net.    NS    ns1.disi.ripe.net.
  disi.ripe.net.    NS    ns2.disi.ripe.net.
  ```

- How to get to ns1 and ns2… We need the addresses.

- Add glue records to so that resolvers can reach ns1 and ns2.

  ```
  ns1.disi.ripe.net. A 10.0.0.1
  ns2.disi.ripe.net. A 10.0.0.2
  ```

Concept: Glue (continued)

- Glue is 'non-authoritative' data
- Don't include glue for servers that are not in sub zones

```
disi.ripe.net.       NS    ns1.disi.ripe.net.
disi.ripe.net        NS    ns2.ripe.net.
disi.ripe.net        NS    ns.bert.secret-wg.org.
ns1.disi.ripe.net.   A     10.0.0.1
```

Only this record needs glue

Delegating disi.ripe.net. from ripe.net.

disi.ripe.net

- Setup minimum two servers
- Create zone file with NS records
- Add all disi.ripe.net data

ripe.net

- Add NS records and glue
- Make sure there is no other data from the disi.ripe.net. zone in the zone file.`

Becoming a child In general

- Buy your domain at favorite registry
- Set up your name servers
- Register the name servers: your registry will communicate the name servers to the registrar who will make sure the name servers are published.
  - ◆ This process might take hours-days.
- Registrars may require a sensible setup