Recommendations for DNS SOA Values

Peter Koch
June 1999

Abstract

The configuration and maintainance of DNS zones offer many degrees of freedom and thus several opportunities for making mistakes. Most DNS zones today are small and have to be set up and maintained by non-experts. This document gives recommendations on which values to use for the SOA resource record of small, stable DNS zones to aid novice administrators and to contribute to DNS stability end efficiency.

1. Conventions used in this document

Domain names used in this document are for explanatory purposes only and should not be expected to lead to useful information in real life [RFC2606].

2. Background

Various DNS surveying activities show that the vast majority of today's DNS zones are populated by very few hosts. In most cases there is only an HTTP server announced under the common name "www", sometimes accompanied by distinct mail or DNS servers or a bastion host. For many of these zones the configuration is touched once when it is set up and then left alone without modification for a long time. These recommendations are aimed at small and stable DNS zones. There are many legitimate reasons to use different values, e.g. proposed changes or special purpose applications. Administrators of those zones should consult one of the various more detailed DNS guidelines or books. Several other recommendations for SOA values exist [RFC1535, RFC1912], which are not obsoleted by this document but which have a different focus. At the time of their writing DNS zones were usually more densely populated and their target audience was supposed to have more interest in DNS. ISPs and DNS server vendors are encouraged to use this information for their customers, in configuration tools or as default values. Additional hints for initial name server setup and configuration of this type of zone can be found in [DNSGUIDE1], [DNSGUIDE2].

3. Recommended SOA Values

```
example.com.  3600  SOA  dns.example.com. hostmaster.example.com. (
                         1999022301   ; serial YYYYMMDDnn
                         86400        ; refresh (  24 hours)
                         7200         ; retry   (   2 hours)
                         3600000      ; expire  (1000 hours)
                         172800 )     ; minimum (   2 days)
```

4. Remarks and Explanation

The values presented in the example.com SOA RR are discussed in detail. One main goal was to provide for fixed cut-and-paste values wherever possible instead of intervals to reduce the chance of operational problems caused by unfortunate combinations. Other values or sets of values will work as well, this is one set of values which reflects successful current practice with respect to scalability and stability.

4.1 The MNAME Value

The DNS specification explicitly states that the primary master server be named here. The value must be determined and used. Especially it is a mistake to repeat the zone name here, unless this also leads to a valid address of the primary master.

4.2 The RNAME Value

The RNAME is to publish a mail address of a person or role account dealing with this zone with the "@" converted to a ".". The best practice is to define (and maintain) a dedicated mail alias "hostmaster" [RFC2142] for DNS operations.

4.3. The Serial Number

The most important issue is that this value be incremented after any modification to the zone data. For debugging purposes it has shown to be helpful to encode the modification date into the serial number. The value "1999022301" so is an example of the YYYYMMDDnn scheme and must be replaced by proper values for the year (YYYY, four digits), month (MM, two digits), day of month (DD, two digits) and version per day (nn, two digits). The first version of the day should have the value "01". It is important to preserve the order year - month - day. People using this as a debugging aid must, however, not rely on the date informnation, since experience shows that after initial setup maintainance of this value is often left to the auto-increment feature the software sometimes provides. Other schemes exist - documentation of which is out of the scope of this document.

4.4. The Refresh and Retry Values

The refresh and retry values primarily affect the zone maintainer and the secondary service providers and may be negotiated between them. The values chosen here are aimed at scalability. Modern DNS software implements NOTIFY [RFC1996] and reduces the need for frequent SOA checks, as does the assumption of stability of the zone. While lower values would only slightly increase the bandwidth usage, they would increase the load on servers which are slaves for thousands of zones.

4.5. The Expire Value

The primary goal is to ensure stability of the zone data, even if a mistake invalidating (non-authorizing) the zone or a network outage last for several days. A value of a week or two has proven to be way too short, so a longer time must be used. The specific value was chosen for aesthetic and historic reasons and to disambiguate between the different proposed values of "long".

4.6. The Minimum TTL Value

There are two meanings for this value with practical relevance. First, it serves as a default value for the TTL of all RRs without a given value. To be cache-friendly this value was chosen to be two days, which also follows the stability assumption. The second meaning is the default negative TTL [RFC2308], which would call for a lower value. We are in a transition phase now with software implementing either of both meanings, so the TTL of one hour is recommended for the SOA itself, which will lead to nearly the same effect.

5. Security Considerations

Filling in the recommended values will not directly influence security of the name servers for the particular zone, any system with a name in that zone or any other system in the Internet. However, following these guidelines will likely contribute to DNS stability and thus to reachability. Maintaining proper contact information in the SOA RNAME field helps people in reporting problems, although the address distributed there is not recommended as a primary security contact.

6. Acknowledgements

This work is a product of the RIPE DNS working group.

7. References


```
[RFC1034]     Mockapetris,P.,  "Domain Names - Concepts and Facilities",
              RFC 1034, STD 13, November 1987
[RFC1035]     Mockapetris,P., "Domain Names - Implementation and  Speci
              fication", RFC 1035, STD 13, November 1987
[RFC1123]     Braden,R., "Requirements for Internet Hosts -- Application
              and Support", RFC 1123, STD 3, October 1989
[RFC1537]     Beertema,P., "Common DNS Data File Configuration  Errors",
              RFC 1537,  October 1993
[RFC1912]     Barr,D.,  "Common  DNS  Operational  and Configuration Er
              rors", RFC 1912,  February 1996
[RFC1996]     Vixie,P., "A Mechanism for  Prompt  Notification  of  Zone
              Changes (DNS NOTIFY)", RFC 1996, August 1996
[RFC2142]     Crocker,D.,  "MAILBOX NAMES FOR COMMON SERVICES, ROLES AND
              FUNCTIONS", RFC 2142, May 1997
[RFC2308]     Andrews,M.,  "Negative  Caching  of   DNS   Queries   (DNS
              NCACHE)", RFC 2308, March 1998
[RFC2606]     Eastlake,D.,  Panitz,A.,  "Reserved  Top Level DNS Names",
              RFC 2606, BCP 32, June 1999
[DNSGUIDE1]   Liman,L., "SIMPLE  DNS  CONFIGURATION  EXAMPLE",  work  in
              progress
[DNSGUIDE2]   Koch,P.,  "RIPE Guide To Setting Up a DNS Server", work in
              progress
```


8. Author's Address

Peter Koch
Universitaet Bielefeld
Technische Fakultaet
Postfach 10 01 31

D-33501 Bielefeld
Germany
+49 521 106 2902
<pk@TechFak.Uni-Bielefeld.DE>