Workgroup: Internet Engineering Task Force
Published: 15 January 2024
Intended Status: Informational
Expires: 18 July 2024
Authors: H. Salgado M. Vergara D. Wessels
NIC Chile DigitalOcean Verisign

The DNS Zone Version (ZONEVERSION) Option

Abstract

The DNS ZONEVERSION option is a way for DNS clients to request, and for authoritative DNS servers to provide, information regarding the version of the zone from which a response is generated. The Serial field from the Start Of Authority (SOA) resource record is a good example of a zone's version, and the only one defined by this specification. Additional version types may be defined by future specifications.

Including zone version data in a response simplifies and improves the quality of debugging and and diagnostics since the version and the data are provided atomically. This can be especially useful for zones and DNS providers that leverage IP anycast or multiple backend systems. It functions similarly to the NSID option.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 18 July 2024.

Copyright Notice

Table of Contents

1. Introduction

The ZONEVERSION option allows DNS queriers to request, and authoritative DNS severs to provide, a token representing the version of the zone from which a DNS response was generated. It is similar to the NSID option, which can be used to convey the identification of a name server that generates a response.

The Domain Name System allows data to be loosely coherent [RFC3254], because synchronization can never be instantaneous, and some uses of DNS do not require strong coherency anyway. This means that a record obtained by one response could be out-of-sync with other authoritative sources of the same data at the same point in time. This can make it difficult to debug some problems when there is a need to couple the data with the version of the zone it came from. Furthermore, in today's Internet, it is common for high volume and

important DNS zones to utilize IP anycast Section 4.9 of [RFC4786] and/or load-balanced backend servers. In general, there is no way to ensure that two separate queries are delivered to the same server. The ZONEVERSION option both simplifies and improves the DNS monitoring and debugging by directly associating the data and the version together in a single response.

The SOA Serial field (Section 4.3.5 of [RFC1034]) is one example of zone versioning. Its purpose is to facilitate the distribution of zone data between primary and secondary name servers. It is also often useful in DNS monitoring and debugging. This document specifies the SOA Serial as one type of ZONEVERSION data.

Some DNS zones may use other distrubtion and synchronization mechanisms not based on the SOA Serial number, such as relational databases or other proprietary methods. In those cases the SOA Serial field may not be relevant with respect to the versioning of its content. To accomodate these use cases, new ZONEVERSION types should be defined in future specifications. Alternatively, zone operators may use one of the private use ZONEVERSION code points allocated by this specification.

The ZONEVERSION option is OPTIONAL to implement by DNS clients and name servers. It is designed for use only when a name server provides authoritative response data. It is intended only for hop-to-hop communication and is not transitive.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

1.2. Terminology

In this document "original QNAME" is used to mean what the DNS terminology document [RFC8499] calls "QNAME (original)":

> The name actually sent in the Question section in the original query, which is always echoed in the (final) reply in the Question section when the QR bit is set to 1.

2. The ZONEVERSION Option

This document specifies a new EDNS(0) Section 6.1.2 of [RFC6891] option, ZONEVERSION, which can be used by DNS clients and servers to provide information regarding the version of the zone from which a response is generated.

2.1. Wire Format

The ZONEVERSION option is encoded as follows:

OPTION-CODE for the ZONEVERSION option is <TBD>.

[RFC Editor: change <TBD> to the proper code when assigned by IANA.]

OPTION-LENGTH for the ZONEVERSION option MUST have a value of 0 for queries, and MUST have the value of the length (in octets) of the OPTION-DATA for responses.

OPTION-DATA for the ZONEVERSION option is omitted in queries. For responses it is composed of three fields:

- An unsigned 1 octet Label Count (LABELCOUNT) indicating the number of labels for the name of the zone that VERSION value refers to.

- An unsigned 1 octet type number (TYPE) that distinguishes the format and meaning of VERSION.

- An opaque octet string conveying the zone version data (VERSION).

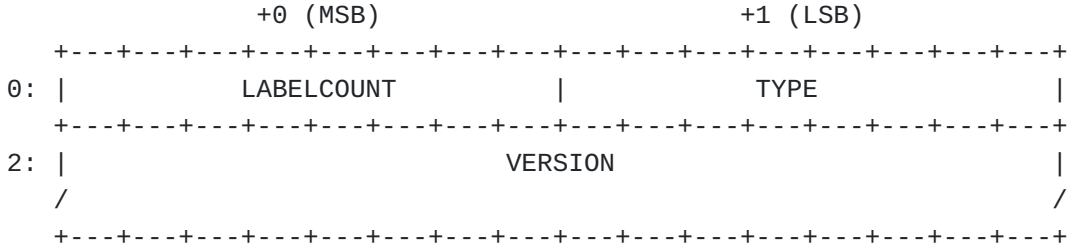

Figure 1: Diagram with the OPTION-DATA format for ZONEVERSION option

The LABELCOUNT field indicates the name of the zone that the ZONEVERSION option refers to, by means of taking the last LABELCOUNT labels of the original QNAME. For example, an answer with QNAME "a.b.c.example.com" and a ZONEVERSION option with a LABELCOUNT of value 2, indicates that the zone name that this ZONEVERSION refers is "example.com.".

The LABELCOUNT number helps to differentiate in the case of a downward referral response, where the parent server is authoritative for some portion of the QNAME that differs from a child server that is below the zone cut. Also, if the ANSWER section has more than one RR set with different zones (like a CNAME and a target name in

another zone) the number of labels in the QNAME disambiguates such a situation.

The value of the LABELCOUNT field MUST NOT count the null (root) label that terminates the original QNAME. The value of the LABELCOUNT field MUST be less than or equal to the number of labels in the original QNAME. The Root zone (".") has a LABELCOUNT field value of 0.

2.2. Presentation Format

The presentation format of the ZONEVERSION option is as follows:

The OPTION-CODE field MUST be represented as the mnemonic value ZONEVERSION.

The OPTION-LENGTH field MAY be omitted, but if present it MUST be represented as an unsigned decimal integer.

The LABELCOUNT value of OPTION-DATA field MAY be omitted, but if present it MUST be represented as an unsigned decimal integer. The corresponding zone name SHOULD be displayed (i.e., LABELCOUNT labels of the original QNAME) for easier human consumption.

The TYPE and VERSION fields of the option SHOULD be represented according to each specific TYPE.

3. ZONEVERSION Processing

3.1. Initiators

A DNS client MAY signal its support and desire for zone version information by including an empty ZONEVERSION option in the EDNS(0) OPT pseudo-RR of a query to an authoritative name server. An empty ZONEVERSION option has OPTION-LENGTH set to zero.

A DNS client SHOULD NOT send the ZONEVERSION option to non-authoritative name servers.

A DNS client MUST NOT include more than one ZONEVERSION option in the OPT RR of a DNS query.

3.2. Responders

A name server that (a) understands the ZONEVERSION option, (b) is authoritative for the original QNAME, and (c) chooses to honor a particular ZONEVERSION request responds by including a TYPE and corresponding VERSION value in a ZONEVERSION option in an EDNS(0) OPT pseudo-RR in the response message.

Otherwise, a server MUST NOT include a ZONEVERSION option in the response.

A name server MUST ignore any non-empty ZONEVERSION payload data that might be present in the query message.

A name server MAY include more than one ZONEVERSION option in the response if it supports multiple TYPEs. A name server MUST NOT include more than one ZONEVERSION option for a given TYPE.

A name server SHOULD include zone version information for downward referral responses (see "Referrals" in Section 4 of [RFC8499]). Even though the response's Authoritative Answer bit is not set, the name server is authoritative for the zone from which the referral was generated. In this case, the ZONEVERSION data MUST correspond do version of the referring zone.

A name server SHOULD include zone version information in a server failure (SERVFAIL) response when it is authoritative for the original QNAME.

A name server SHOULD include zone version information in a NODATA response (Section 3 of [RFC8499]). Even though the NODATA response does not include an Answer section RRs, RCODE is NOERROR and the name server is still authoritative for the zone.

4. The SOA-SERIAL ZONEVERSION Type

The first and only ZONEVERSION option TYPE defined in this document is a zone's serial number as found in the Start of Authority (SOA) RR.

The value for this type is: 0

The mnemonic of this type is: SOA-SERIAL.

The OPTION-LENGTH for this type MUST be set to 6 in responses.

The VERSION value for the SOA-SERIAL type MUST be a copy of the unsigned 32-bit SERIAL field of the SOA RR, as defined in Section 3.3.13 of [RFC1035].

4.1. Type SOA-SERIAL Presentation Format

The presentation format of this type content is as follows:

The TYPE field MUST be represented as the mnemonic value "SOA-SERIAL".

The VERSION field MUST be represented as an unsigned decimal integer.

5. Example usage

A name server which (a) implements this specification, (b) receives a query with the ZONEVERSION option, (c) is authoritative for the original QNAME, and (d) utilizes the SOA serial field for versioning of said zone should include a ZONEVERSION option in its response. In the response's ZONEVERSION option the OPTION-LENGTH would be set to 6 and the OPTION-DATA would consist of the 1-octet LABELCOUNT, the 1-octet TYPE with value 0, and 4-octet SOA SERIAL value.

The example below demonstrates expected output of a diagnostic tool that implements the ZONEVERSION option, displaying a response from a compliant authoritative DNS server:

```
$ dig @ns.example.com www.example.com aaaa +zoneversion

; <<>> DiG 9.17.14-patched <<>> @ns.example.com www.example.com aaaa +
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7077
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; ZONEVERSION: 02 00 78 95 a4 e9 ("SOA-SERIAL: 2023073001 (example.com
;; QUESTION SECTION:
;www.example.com.    IN  AAAA

;; ANSWER SECTION:
www.example.com.  43200  IN  AAAA  2001:db8::80

;; AUTHORITY SECTION:
example.com.    43200  IN  NS  ns.example.com.

;; ADDITIONAL SECTION:
ns.example.com.    43200  IN  AAAA  2001:db8::53

;; Query time: 15 msec
;; SERVER: 2001:db8::53#53(2001:db8::53) (UDP)
;; WHEN: dom jul 30 19:51:04 -04 2023
;; MSG SIZE  rcvd: 129
```

Figure 2: Example usage and dig output

6. Acknowledgements

The authors thanks all the comments and support made in the DNSOP mailing list, chats and discussions. In special for the suggestions to generalize the option using a registry of types from Petr Špaček and Florian Obser, suggestions for implementation from Stéphane Bortzmeyer, security clarifications from George Michaelson, zone name disambiguation from Joe Abley and Brian Dickson, and reviews from Tim Wicinski and Peter Thomassen.

7. IANA Considerations

7.1. DNS EDNS0 Option Code Registration

This document defines a new EDNS0 option, entitled ZONEVERSION (see Section 2), and assigns a value of <TBD> from the DNS EDNS0 Option Codes (OPT) Option space:

Value	Name	Status	Reference
<TBD>	ZONEVERSION	Standard	[this document]

Table 1: DNS EDNS0 Option code

[RFC Editor: change <TBD> to the proper code when assigned by IANA.]

[RFC Editor: change "this document" with the proper RFC number for this document when assigned by IANA.]

7.2. ZONEVERSION Registry

The ZONEVERSION option also defines a 8-bit TYPE field, for which IANA is requested to create and maintain a new registry entitled "ZONEVERSION TYPE Values" (abbreviation ZONEVERSION) used by the ZONEVERSION option, inside the "Domain Name System (DNS) Parameters" group. Initial values for the ZONEVERSION TYPE values registry are given below; future assignments in the 1-245 values are to be made through Specification Required Review [BCP26]. Assignments consist of a TYPE value as an unsigned 8-bit integer recorded in decimal, a Mnemonic name as an uppercase ASCII string with maximum length of 15 characters, and the required document reference.

ZONEVERSION TYPE	Mnemonic	Reference
0	SOA-SERIAL	[this document]
1-245	Unassigned	
246-254	Reserved for Local/Experimental Use	[this document]

ZONEVERSION TYPE	Mnemonic	Reference
255	Reserved for future expansion	[this document]

Table 2: ZONEVERSION Registry

[RFC Editor: change "this document" with the proper RFC number for this document when assigned by IANA.]

The change control for this registry should be by means of an Standard action.

7.2.1. Expert Review Directives

Allocation procedures for new code points in the ZONEVERSION TYPE registry require Specification Required review, and so it requires Expert Reviews as stated in [BCP26].

The expert should consider the following points:

- *Duplication of code point allocations should be avoided.
- *A Presentation Format section should be provided, with a clear code point mnemonic.
- *The referenced document and stated use of the new code point should be appropriate for the intended use of a ZONEVERSION TYPE assignment. In particular the reference should state clear instructions for implementers about the syntax and semantic of the data. Also the Length of the Data must have proper limits.

The expert reviewing the request MUST approve or disapprove the request within 10 business days from when she or he received the expert review request.

8. Security Considerations

The EDNS extension data it's not covered by RRSIG records, so there's no way to verify its authenticity nor integrity using DNSSEC and could theoretically be tampered by a person-in-the-middle if the transport is made by insecure means. Caution should be taken to use the EDNS ZONEVERSION data for any means besides troubleshooting and debugging.

If there's a need to certify the ZONEVERSION trustworthiness, it will be necessary to use an encrypted and authenticated DNS transport.

If there's a need to authenticate data origin for the ZONEVERSION value, an answer with the SOA-SERIAL type as defined above could be

compared to a separate regular SOA query with DO flag, whose answer shall be DNSSEC signed, with the cautions about Anycast and others as already stated in Introduction.

With the SOA-SERIAL type defined above, there's no risk on disclosure of private information, as the SERIAL of the SOA record is already publicly available.

Please note that the ZONEVERSION option can not be used for checking the correctness of an entire zone in a server. For such cases, the ZONEMD record [RFC8976] might be better suited at such a task. ZONEVERSION can help identify and correlate a certain specific answer with a version of a zone, but it has no special integrity or verification function besides a normal field value inside a zone, as stated above.

9. Normative References

[BCP26] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, RFC 6891, DOI 10.17487/RFC6891, April 2013, <https://www.rfc-editor.org/info/rfc6891>.

10. Informative References

[ImplRef] Salgado, H., "Zoneversion Implementations", 2024, <https://github.com/huguei/rrserial>.

[RFC3254] Alvestrand, H., "Definitions for talking about directories", RFC 3254, DOI 10.17487/RFC3254, April 2002, <https://www.rfc-editor.org/info/rfc3254>.

[RFC4786] Abley, J. and K. Lindqvist, "Operation of Anycast Services", BCP 126, RFC 4786, DOI 10.17487/RFC4786, December 2006, <https://www.rfc-editor.org/info/rfc4786>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

[RFC8976] Wessels, D., Barber, P., Weinberg, M., Kumari, W., and W. Hardaker, "Message Digest for DNS Zones", RFC 8976, DOI 10.17487/RFC8976, February 2021, <https://www.rfc-editor.org/info/rfc8976>.

Appendix A. Implementation Considerations

With very few exceptions, EDNS options which elicit an EDNS option in the response are independent of the queried name. This is not the case of ZONEVERSION, so its implementation may be more or less difficult depending on how EDNS options are handled in the name server.

Appendix B. Implementation References

There's a patched NSD server version 4.7.0 with support for ZONEVERSION with an experimental opcode, with live test servers installed for compliance tests. Also there is a client command "dig" with added zoneversion support, along with test libraries in Perl, Python and Go. More information in the working document [ImplRef].

Authors' Addresses

Hugo Salgado
NIC Chile
Miraflores 222, piso 14
CP 8320198 Santiago
Chile

Phone: +56 2 29407700
Email: hsalgado@nic.cl

Mauricio Vergara Ereche
DigitalOcean
101 6th Ave
New York, NY 10013
United States of America

Email: mvergara@digitalocean.com

Duane Wessels

Verisign
12061 Bluemont Way
Reston, VA 20190
United States of America

Phone: +1 703 948-3200
Email: dwessels@verisign.com
URI: https://verisign.com