DNS Delegation Requirements
draft-wallstrom-dnsop-dns-delegation-requirements-03

Abstract

This document outlines a set of requirements on a well-behaved DNS delegation of a domain name. A large number of tools have been developed to test DNS delegations, but each tool uses a different set of requirements for what is a correct setup for a delegated domain name. However, there are few requirements on how to set up DNS in order to just make the delegation work. In order to have a well-behaved delegation that is robust to failures and also makes DNS resolvers behave consistently, there are a large number of things to consider.

Based on this document, it should be possible to set up a fully functional DNS delegation for a domain name, but also to create a set of test specifications for how to test a DNS delegation.

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 http://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 April 29, 2017.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.
This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction ............................................. 3
   1.1. DNS Terminology .................................... 4
   1.2. Reserved Words .................................... 4
2. Basic requirements ...................................... 5
   2.1. The domain name MUST be valid ........................ 5
   2.2. The domain MUST have a parent domain ................. 5
   2.3. The domain MUST have at least one working name server . 5
3. Address requirements ..................................... 5
   3.1. Name server address MUST be globally routable ......... 5
   3.2. The IP address of a name server MUST be delegated by IANA 6
4. Connectivity requirements ............................... 6
   4.1. All name servers MUST have UDP connectivity over port 53 7
   4.2. All name servers MUST have TCP connectivity over port 53 7
5. Name server requirements ................................ 7
   5.1. Authoritative name servers SHOULD NOT be recursive ..... 7
   5.2. Name servers SHOULD support EDNS0 .................... 7
   5.3. Name servers MUST process QNAME case insensitive .... 8
6. Consistency requirements ............................... 8
   6.1. All name servers SHOULD respond with the same SOA serial number ................................. 8
   6.2. All name servers SHOULD respond with the same SOA RNAME .... 9
   6.3. All name servers SHOULD respond with the same SOA parameters .................................. 9
   6.4. All name servers MUST respond with the same NS RR Set .... 9
7. Delegation requirements .................................. 9
   7.1. The delegation SHOULD contain at least two name servers .... 9
   7.2. The NS RR set in the parent SHOULD be a subset of the NS RR set in the child ................ 10
   7.3. The name servers SHOULD have network path diversity ... 10
   7.4. The name servers MUST have distinct IP addresses .... 10
   7.5. The referral SHOULD fit into a non-truncated 512 byte UDP packet ............................. 10
   7.6. All name servers MUST be authoritative for the domain name ........................................ 11
   7.7. The delegation name MUST exactly match the apex of the child zone ............................... 11
7.8. Glue records in delegation SHOULD exactly match records in child zone .............................................. 11
7.9. SOA MNAME SHOULD be authoritative for the zone ................. 11
8. DNSSEC requirements .................................................. 12
  8.1. The DS Digest Type MUST be assigned by IANA ................. 12
  8.2. The DNSKEY algorithm MUST be assigned by IANA ............... 12
  8.3. The chain of trust for the delegation MUST be valid ........... 12
  8.4. One DS MUST match a least one DNSKEY in the child zone .... 12
  8.5. The number of NSEC3 iterations must not be higher than what is allowed ........................................... 13
  8.6. RRSIG validity period SHOULD NOT be too short nor too long ....................................................... 13
  8.7. The name server MUST include RRSIG in all responses to DNSSEC queries ......................................... 13
  8.8. The name servers MUST include valid NSEC/NSEC3 record in NXDOMAIN responses ................................ 13
9. Syntax requirements .................................................. 14
  9.1. Illegal characters MUST NOT be in the domain name ........... 14
  9.2. Hyphens SHOULD NOT be in position 3 and 4 of the domain name ....................................................... 14
  9.3. The NS names MUST be valid hostnames .......................... 14
  9.4. The NS names MUST NOT be an alias ............................. 14
  9.5. The SOA RNAME MUST not contain the ‘@’ character ........... 14
  9.6. The SOA RNAME MUST be a legal hostname ..................... 15
  9.7. The SOA MNAME MUST be a legal hostname ..................... 15
  9.8. The MX record in apex MUST point to a valid hostname ....... 15
10. Security Considerations ............................................ 15
11. IANA Considerations ................................................ 15
12. Acknowledgements .................................................. 15
13. References .......................................................... 16
  13.1. Normative References .......................................... 16
  13.2. Informative References ....................................... 17
Authors’ Addresses .................................................... 20

1. Introduction

This document outlines a set of requirements on a well-behaved DNS delegation of a domain name. Many domain name registries use a set of requirements on what they may consider a valid delegation. Such requirements can be used to implement tools that are used for pre- or post-delegation checks of the delegations in that registry.

To test the quality of the delegation there has been a number of different tools developed, each based on a different set of requirements. This document outlines a set of baseline requirements on a correct setup for a delegated domain name. This document is based on current RFCs and documents requirements that are protocol
specific, but also administrative policy requirements drawn from best practices and recommendations.

The DNS requirements are split into these different areas, to easier differentiate between what they are for:

- Basic
- Address
- Connectivity
- Name server
- Consistency
- Delegation
- DNSSEC
- Syntax

A secondary name server operator should follow the advice in the BCP document [RFC2182].

Nothing in this document precludes others testing servers for protocol compliance. DNS operators should test their servers to ensure that their vendors have shipped protocol compliant products. Name server vendors can use these tests as a part of this release processes. Registrants can use these tests to check their DNS operators servers.

1.1. DNS Terminology

This document attempts to fully follow the DNS terminology as defined in [RFC7719].

Many requirements in this document deal with the properties of a name server that is used as part of a delegation, therefore the wording mentioning the use - authoritative or recursive - of a name server as part of this is omitted.

1.2. Reserved Words

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].
2. Basic requirements

The Basic requirements are fundamental to a working DNS delegation. Without these properties, the rest of the requirements are irrelevant.

2.1. The domain name MUST be valid

The domain name MUST follow the rules defined in Section 2.1 of [RFC1123] in order to be able to map the domain into a DNS packet. A domain name is normally valid if the name has been registered with a domain name registry.

Internationalized domain names, [RFC5891], are expected to be encoded using Punycode [RFC3492], thus following the rules outlined in Section 2.3.1 of [RFC1035]. Any validation of the domain name in U-label form is out of scope for this document.

2.2. The domain MUST have a parent domain

A DNS delegation MUST have a parent domain from which it is delegated. The concept of zone cuts was first described in [RFC1034] and later clarified in Section 6 of [RFC2182]. The only exception is the root zone, which do not have a parent zone.

2.3. The domain MUST have at least one working name server

A fully working DNS delegation has a parent zone delegating the zone to a set of child name servers. At least one name server MUST be able to answer DNS queries in order to be able to authoritatively serve data for the child zone.

3. Address requirements

A delegation in the public Internet DNS hierarchy will use the globally unique address space.

3.1. Name server address MUST be globally routable

In order for the domain and its resources to be accessible from the Internet, authoritative name servers must have addresses in the routable public addressing space.

IANA is responsible for global coordination of the IP addressing system. Aside its address allocation activities, it maintains reserved address ranges for special uses. There are two IANA registries for Special-Purpose Addresses, the IANA IPv6 Special-
Purpose Address Registry and the IANA IPv4 Special-Purpose Address Registry.

[RFC6890] instructs IANA on how to structure the IPv4 and IPv6 Special-Purpose Address Registries. The registries [IANA-IPv4-Special] and [IANA-IPv6-Special] are maintained by IANA, and are also described in Section 2.2 and 2.3 of [RFC7249].

A name server MUST NOT be using any IP address within any of these registries that are marked with False in the Global column.

3.2. The IP address of a name server MUST be delegated by IANA

IP addresses not delegated by IANA MUST NOT be used used by a name server. Thus, IP addresses within a prefix not delegated to a RIR by IANA MUST be rejected.

The IANA registry [IANA-IPv6-Unicast] SHOULD be used to determine the status of an IPv6 prefix. Only prefixes with the status ALLOCATED are allowed.

The IANA registry [IANA-IPv4-Registry] SHOULD be used to determine the status of an IPv4 prefix. Only prefixes with the status ALLOCATED and LEGACY are allowed. Note that IPv4 LEGACY is not allocated to a RIR.

Martians [RFC1208] is a humorous term applied to packets that turn up unexpectedly on the wrong network because of bogus routing entries. Bogons [RFC3871] are packets sourced from addresses that have not yet been allocated by IANA or a RIR, or not delegated to a RIR by IANA as described above. Martians and Bogons SHOULD NOT be used as an addressed used by a name server.

4. Connectivity requirements

The use of underlying protocols for DNS is described in Section 4.2 of [RFC1035].

The Internet supports name server access using TCP on server port 53 (decimal) as well as datagram access using UDP on UDP port 53 (decimal). Today DNS is used in conjunction with both IPv4 and IPv6, Name servers configured for a zone in a delegation MUST be able to answer queries using the DNS protocol.
4.1. All name servers MUST have UDP connectivity over port 53

DNS queries are sent using UDP on port 53, as described in Section 4.2.1 of [RFC1035]. A name server MUST respond to DNS queries over UDP for each IP address configured for that name server.

4.2. All name servers MUST have TCP connectivity over port 53

In addition to UDP, DNS queries can also be sent using TCP on port 53, as described in Section 4.2.2 of [RFC1035]. A name server MUST respond to DNS queries over TCP for each IP address configured for that name server. This requirement has also been further clarified in [RFC7766], which makes TCP a REQUIRED part of a full DNS protocol implementation.

It should be noted that even though [RFC7766] requires TCP for a DNS protocol implementation, it does not make specific recommendations to operators of DNS servers. However, it also notes that failure to support TCP (or the blocking of DNS over TCP at the network layer) may result in resolution failure and/or application-level timeouts. The operational requirements on DNS Transport over TCP are further discussed [I-D.kristoff-dnsop-dns-tcp-requirements].

5. Name server requirements

5.1. Authoritative name servers SHOULD NOT be recursive

To ensure consistency in DNS, an authoritative name server SHOULD NOT be configured to do recursive lookups. Also, open recursive resolvers are considered bad Internet practice due to their capability of assisting in large scale DDoS attacks. The introduction to [RFC5358] elaborates on mixing recursor and authoritative functionality. Section 2.5 of [RFC2870] have very specific requirement on disabling recursion functionality on root name servers.

5.2. Name servers SHOULD support EDNS0

EDNS0 is a mechanism to announce capabilities of a DNS implementation, and is now basically required by any new functionality in DNS such as DNSSEC. Initially standardized in [RFC2671] and later updated by [RFC6891], EDNS0 is a mechanism to announce capabilities of a DNS implementation.
5.3. Name servers MUST process QNAME case insensitive

The DNS standards require that name servers treat names with case insensitivity. That is, the names example.com and EXAMPLE.COM should resolve to the same IP address. However, in the response, most name servers echo back the name as it appeared in the request, preserving the original case. This is specified in [RFC1034] and [RFC1035], and further clarified by [RFC4343].

Therefore, another way to add entropy to requests is to randomly vary the case of letters in domain names queried. This technique, also known as "0x20" because bit 0x20 is used to set the case of US-ASCII letters, was first proposed in [I-D.vixie-dnsext-dns0x20], Use of Bit 0x20 in DNS Labels to Improve Transaction Identity. With this technique, the name server response must match not only the query name, but the case of every letter in the name string; for example, www.eXaMpLe.COm or WwW.ExamPLe.COM. This may add little or no entropy to queries for the top-level and root domains, but it’s effective for most hostnames.

6. Consistency requirements

For DNS resolver behaviour to be consistent for a domain, it is important that the authoritative data for the domain to be consistent. All authoritative name servers for a zone should serve the same data, although it should be noted that there exists cases where authoritative name servers are configured to reply with different answers depending on the client source address and/or query options such as EDNS0 client subnet option as specified in [RFC7871].

An indicator of inconsistency is that infrastructure records (e.g., SOA and NS) differs between the authoritative name servers.

Section 4.6 in [RFC4786] advices that data synchronisation in an anycast setup should be done in a manner so that anycast nodes operate in a consistent manner.

6.1. All name servers SHOULD respond with the same SOA serial number

An indication that not all authoritative name servers have a consistent and updated copy of the zone is that the serial numbers differ. When querying for the SOA RR all name servers SHOULD respond with the same SOA serial number.

Section 4.3.5 in [RFC1034] explains the typical function of the serial numbers in zone maintenance and transfers.
One should note that even though different SOA serial numbers are a strong indicator of an inconsistent setup, there are several scenarios where the serial number varies between name servers. One example is a zone with frequent updates to zone data, where propagation delay between the name servers may result in limited inconsistency.

6.2. All name servers SHOULD respond with the same SOA RNAME

As per Section 3.3.13 of [RFC1035], the RNAME field in the SOA RDATA refers to the mailbox of the person responsible for the zone. An indication that not all authoritative name servers have a consistent and updated copy of the zone is that the RNAME differs. When querying for the SOA RR all name servers SHOULD respond with the same SOA RNAME.

6.3. All name servers SHOULD respond with the same SOA parameters

The inconsistency of the SOA parameters REFRESH, RETRY, EXPIRE and MINIMUM, defined in Section 3.3.13 of [RFC1035], might lead to operational problems for the zone. These SOA parameters SHOULD be consistent for all authoritative name servers for the zone.

6.4. All name servers MUST respond with the same NS RR Set

All authoritative name servers MUST serve the same RR set in order to ensure consistency in the zone cut as described in Section 4.2.2 of [RFC1034]. Any inconsistency of NS records described in Section 3.3.11 of RFC 1035 might result in operational failures.

7. Delegation requirements

[RFC2182] is a BCP on how to select and operate secondary name servers, and summarize many operational issues with the delegation of a zone. For a delegation to work continuously if one component fails, there are operational considerations to ensure this.

Section 4.2.2 [RFC1034] also adds that the administrators of both the parent and child zone should ensure that NS and glue RRs on both sides of the zone cut are consistent.

7.1. The delegation SHOULD contain at least two name servers

Section 4.1 [RFC1034] states that by administrative fiat we require every zone to be available on at least two name servers. Section 5 of [RFC2182] that answers the question on how many name servers are needed, the recommendation is that "three servers be provided for
most organisation level zones, with at least one which must be well removed from the others."

In order to avoid any operational problems, a delegation SHOULD contain at least two (2) authoritative name servers.

7.2. The NS RR set in the parent SHOULD be a subset of the NS RR set in the child

As per the name resolving algorithm described in [RFC1034] the NS RR in the child zone is authoritative for the zone, and any delegation hints in the parent are discarded in the resolving process. The NS RR set in the parent zone SHOULD be a subset of the NS RR set in the child zone.

7.3. The name servers SHOULD have network path diversity

[RFC2182], Section 3.1 states that distinct authoritative name servers for a child domain should be placed in different topological and geographical locations. The objective is to minimise the likelihood of a single failure disabling all of them. Further support for this is given in Section 5:

It is recommended that three servers be provided for most organisation level zones, with at least one which must be well removed from the others.

To avoid any single point of failure in networking, the name servers SHOULD exhibit network path diversity. Using current routing technology, this means that all name servers SHOULD NOT be placed within a single routing domain, or AS (autonomous system).

7.4. The name servers MUST have distinct IP addresses

A common workaround to a registry policy that requires at least two name servers is to create two (2) names with the same IP address.

To avoid any operational errors and workaround such as this, all name servers used for the zone MUST use distinct IP addresses.

7.5. The referral SHOULD fit into a non-truncated 512 byte UDP packet

The DNS still defaults to using UDP, although efforts into requiring or transitioning to use TCP have come a long way. The UDP packet limit is 512 bytes, and although the EDNS0 [RFC6891] extension mechanism to overcome this limit have been in use for a very long time, many middleboxes and proxies still interfere with DNS packets ([RFC5625]).
To avoid any such problems with the delegation, and to avoid any unexpected truncation of a referral response, the referral containing the delegation from the parent SHOULD fit within 512 bytes.

7.6. All name servers MUST be authoritative for the domain name

A name server that does not answer authoritatively for the zone is a clear sign of misconfiguration, and is a common cause for operational problems.

Section 6.1 of [RFC2181] mandates that the name servers MUST answer authoritatively for the zone.

7.7. The delegation name MUST exactly match the apex of the child zone

The configured zone on the child name servers MUST match the delegated name of the zone. When querying the child name servers for the zone, any authoritative data for another name MUST NOT be in the response.

[RFC2181] states that the SOA RR and the NS RR indicates the origin of the zone, and both are mandatory records in a zone. Both RRs MUST be present and match the name of the zone.

7.8. Glue records in delegation SHOULD exactly match records in child zone

In-bailiwick glue for name servers listed at the parent SHOULD match the in-bailiwick glue for the name servers in the child.

If the glue address mismatch between the parent zone and the child, this is a strong indication of configuration error.

7.9. SOA MNAME SHOULD be authoritative for the zone

The hostname of the MNAME field may or may not be listed among the delegated name servers, but SHOULD still be authoritative for the zone. MNAME may be used for other services, e.g., DNS NOTIFY [RFC1996] and DNS Dynamic Updates [RFC2136].

It should be noted that there are no formal requirement that the name server listed in the SOA MNAME is reachable from the public Internet. Because of this, it may be difficult to implement a reasonable test for this requirement.
8. DNSSEC requirements

If DNSSEC is used for the zone, either by indicating that the zone is signed with a DS record, or the use of a DNSKEY in the zone itself, a number of things are required for a fully functional delegation.

The Domain Name System Security Extensions (DNSSEC) add data origin authentication and data integrity to the Domain Name System, and was first introduced with the RFCs [RFC4033], [RFC4034] and [RFC4035]. There are also a number of additions to DNSSEC such as NSEC3 described in [RFC5155], and a number of algorithms to the cryptographic functions.

8.1. The DS Digest Type MUST be assigned by IANA

The Digest Type Field is defined as part of the DS RDATA Wire Format of Section 5.1.3 in [RFC4034]. The appendix A.2 defines the initial set of digest algorithm types with possible future algorithms. The IANA registry for DS Digest Types [IANA-DNSSEC-DS] was defined by [RFC3658].

Any DS Digest Type used for a zone MUST be assigned by IANA.

8.2. The DNSKEY algorithm MUST be assigned by IANA

The DNSKEY RR is defined in Section 2 of [RFC4034] as part of the DNSKEY RDATA Wire Format. The appendix A.1 defines the initial list of DNSKEY Algorithm Types. The IANA Registry for DNSKEY Algorithm Types [IANA-DNSSEC-DNSKEY] was created with [RFC3755].

Any DNSKEY algorithm number used for in a zone MUST be assigned by IANA.

8.3. The chain of trust for the delegation MUST be valid

A valid authentication chain from the parent DS, as described in Section 3.1 of [RFC4033], MUST exist for the SOA, DNSKEY and NS records of the child zone if a DS record is published in the parent zone.

8.4. One DS MUST match a least one DNSKEY in the child zone

DNS delegations from a parent to a child are secured with DNSSEC by publishing one or several Delegation Signer (DS) resource records in the parent zone, along with the NS records for the delegation.

As stated in Section 2.4 of [RFC4035], a DS RR SHOULD point to a DNSKEY RR that is present in the child’s apex DNSKEY RRset. If there
is a DS RR published at the parent, there MUST be at least one DNSKEY
RR in the child zone that matches at least one DS RR for every
signature algorithm, otherwise the authentication of the referral
will fail, as described in Section 5.2 of [RFC4035].

For each unique algorithm from the DS RRs present, there MUST be a
matching DNSKEY using that algorithm in use in the child.

8.5. The number of NSEC3 iterations must not be higher than what is
allowed

Section 10.3 of [RFC5155] specifies the max number of NSEC3
iterations allowed for different key sizes. This requirement is
enforced by several resolver implementations.

The number of NSEC3 iterations MUST NOT be higher than what is
allowed by Section 10.3 of [RFC5155]. It should be noted that the
values in the table MUST be used independent of the key algorithm.

8.6. RRSIG validity period SHOULD NOT be too short nor too long

[RFC6781] describes operational considerations on the choice of
validity periods for RRSIGs. Having too short validity periods might
cause operational failure in case of unexpected events, but is good
for protecting against replay attacks. Having too long validity
periods may be good for operational security, but opens up for replay
attacks.

The RRSIG validity periods in the zone SHOULD NOT be too short nor
too long.

8.7. The name server MUST include RRSIG in all responses to DNSSEC
queries

If the zone is signed, the name servers MUST be able to include RRSIG
RRs as additional data in any response when the query has the DO bit
set, as described in Section 3.1.1 of [RFC4035].

8.8. The name servers MUST include valid NSEC/NSEC3 record in NXDOMAIN
responses

If the zone is signed, the name servers MUST be able to include NSEC/
NSEC3 RRs as additional data in any response when the query has the
DO bit set, as described in Section 3.1.1 of [RFC4035].
9. Syntax requirements

All domain- and host names in DNS MUST follow the rules outlined in Section 2.3.1 of [RFC1035]. The Name Syntax and LDH Label have been further clarified in Section 11 in [RFC2181] and Section 2.3.1 in [RFC5890]. From this follow the requirements below.

9.1. Illegal characters MUST NOT be in the domain name

There MUST NOT be any illegal characters used in the domain name. The domain name MUST follow the rules defined in Section 2.3.1 of [RFC1035], Section 2.1 of [RFC1123], Section 11 of [RFC2182] and Section 2 of [RFC3696].

9.2. Hyphens SHOULD NOT be in position 3 and 4 of the domain name

The effort of internationalization of domain names and the development of IDNA brought us the extension mechanism of using the string ‘xn--’ to have a special meaning. To allow future extensions to DNS there SHOULD be no instances of labels in the DNS that start with two characters, followed by two hyphens, where the two characters are not “xn”. This has been described in Section 5 of [RFC3696].

9.3. The NS names MUST be valid hostnames

The Name Server name MUST be a valid hostname according to the rules defined in Section 2.3.1 of [RFC1035], in Section 2.1 in [RFC1123], Section 11 in [RFC2181] and Section 2 and 5 in [RFC3696].

9.4. The NS names MUST NOT be an alias

As specified in Section 10.3 of [RFC2181], the Name Server name MUST NOT be an alias (CNAME).

9.5. The SOA RNAME MUST not contain the ‘@’ character

The SOA RNAME field is a mailbox address defined in Section 3.3 of [RFC1034] and Section 2.2 of [RFC1912]. The RNAME field MUST follow the rules of an e-mail address defined in Section 3.4.1 of [RFC2822], and the ‘@’ character MUST be changed so that the whole e-mail address is converted into a single domain name as described in Section 3.3 of [RFC1034] and Section 2.1 of [RFC1123].
9.6. The SOA RNAME MUST be a legal hostname

The SOA RNAME field is a mailbox address. The SOA RNAME field is defined in Section 3.3 of [RFC1034] and Section 2.2 of [RFC1912]. As a field containing a domain name, the content of the RNAME field MUST follow the rules outlined in Section 2.3.1 of [RFC1035] and Section 2.1 of [RFC1123].

9.7. The SOA MNAME MUST be a legal hostname

The SOA MNAME field is a hostname. The SOA MNAME field is defined in Section 3.3.13 of [RFC1035]. As a field containing a domain name, the content of the RNAME field MUST follow the rules outlined in Section 2.3.1 of [RFC1035].

Furthermore, Section 7.3 in [RFC2181] makes it clear that the SOA MNAME field SHOULD NOT be the name of the zone itself.

9.8. The MX record in apex MUST point to a valid hostname

The requirement on the existence of an MX RR in the apex of the child zone may vary by policy from different parent zones. However, it is strongly recommended in Section 7 of [RFC2142] that all domains should have a mailbox named hostmaster@domain. SMTP can make a delivery without the MX, using the A or AAAA record as specified in Section 5.1 of [RFC5321].

If an MX RR exists in the apex of the child zone, the hostname that the MX RR points to MUST follow the rules outlined in Section 2.3.1 of [RFC1035] and Section 2.1 of [RFC1123].

10. Security Considerations

This document has no security considerations (yet).

11. IANA Considerations

This document has no IANA actions.

12. Acknowledgements

The requirements documented in this document were developed within the CENTR Test Requirements Task Force (TRTF). Most of the original requirements and text come from the Zonemaster project.
13. References

13.1. Normative References


13.2. Informative References

[I-D.kristoff-dnsop-dns-tcp-requirements]
Kristoff, J., "DNS Transport over TCP - Operational Requirements", draft-kristoff-dnsop-dns-tcp-requirements-01 (work in progress), August 2016.

[I-D.vixie-dnsext-dns0x20]
Vixie, P. and D. Dagon, "Use of Bit 0x20 in DNS Labels to Improve Transaction Identity", draft-vixie-dnsext-dns0x20-00 (work in progress), March 2008.

[IANA-DNSSEC-DNSKEY]

[IANA-DNSSEC-DS]

[IANA-IPv4-Registry]
IANA, "IANA IPv4 Address Space Registry", August 2015, <https://www.iana.org/assignments/ipv4-address-space>.

[IANA-IPv4-Special]

[IANA-IPv6-Special]

[IANA-IPv6-Unicast]


Authors' Addresses

Patrik Wallström
Email: pawal@blipp.com

Jakob Schlyter
Kirei AB
Email: jakob@kirei.se