INTERNET-DRAFT

Donald E. Eastlake 3rd (IBM)
Eric Brunner (Nokia)
Bill Manning (ISI)

Expires: March 2000 September 1999

draft-ietf-dnsind-iana-dns-01.txt

Domain Name System (DNS) IANA Considerations

Status of This Document

Distribution of this draft <draft-ietf-dnsind-iana-dns-01.txt> is unlimited. Comments should be sent to the DNS Working Group mailing list <namedroppers@internic.net> or to the authors.

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months. Internet-Drafts may be updated, replaced, or obsoleted by other documents at any time. It is not appropriate to use Internet-Drafts as reference material or to cite them other than as a ``working draft'' or ``work in progress.''

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

Internet Assigned Number Authority (IANA) considerations are given for the allocation of Domain Name System (DNS) classes, RR types, operation codes, error codes, etc.

Table of Contents

Status of This Document....................................1

Abstract...2
Table of Contents..2

1. Introduction..3

2. DNS Query/Response Headers..............................4
2.1 One Spare Bit?...4
2.2 Opcode Assignment......................................5
2.3 RCODE Assignment.......................................5

3. DNS Resource Records....................................7
3.1 RR TYPE IANA Considerations............................8
3.1.1 Special Note on the OPT RR...........................8
3.1.2 Special Note on the SINK RR..........................9
3.2 RR CLASS IANA Considerations...........................9
3.3 RR NAME IANA Considerations...........................10
3.3.1 Reserved TLDs in the Internet CLASS.................10
3.3.2 'Country Code' TLDs in the Internet CLASS...........11
3.3.3 Other TLDs in the Internet CLASS....................12

4. Security Considerations................................13
References..13

Appendix A: Single Letter or Digit Labels.................15
Appendix B: On Becoming Root and TLD Interoperability.....15

Authors Addresses...17
Expiration and File Name..................................17

1. Introduction

The Domain Name System (DNS) provides replicated distributed secure hierarchical databases which hierarchially store "resource records" (RRs) by CLASS under domain names.

This data is structured into CLASSes and zones which can be independently maintained. See [RFC 1034, 1035, 2136, 2181, 2535] familiarity with which is assumed.

This document covers, either directly or by reference, general IANA considerations applying across DNS query and response headers and all RRs. There may be additional IANA considerations that apply to only a particular RR type or query/response opcode. See the specific RFC defining that RR type or query/response opcode for such considerations if they have been defined.

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 RFC 2119.

The terms of art used herein with respect to IANA Considerations are as defined in [RFC 2434].

2. DNS Query/Response Headers

The header for DNS queries and responses contains field/bits in the following diagram taken from [RFC 2136/2535]:

```
                                           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  |AA|TC|RD|RA| Z|AD|CD|   RCODE   |
            +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
            |                QDCOUNT/ZOCOUNT                |
            +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
            |                ANCOUNT/PRCOUNT                |
            +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
            |                NSCOUNT/UPCOUNT                 |
            +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
            |                    ARCOUNT                    |
            +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

The ID field identifies the query and is echoed in the response so they can be matched.

The QR bit indicates whether the header is for a query or a response.

The AA, TC, RD, RA, AD, and CD bits are each theoretically meaningful only in queries or only in responses, depending on the bit. However, many DNS implementations copy the query header as the initial value of the response header without clearing bits. Thus any attempt to use a "query" bit with a different meaning in a response or to define a query meaning for a "response" bit is dangerous given existing implementation. Such meanings may only be assigned by an IETF standards action.

The QDCOUNT, ANCOUNT, NSCOUNT, and ARCOUNT fields give the number of queries in the Query section, answer RRs in the Answer section, RRs in the Authority section, and informational RRs in the Additional Information section, respectively, for all opcodes except Update. These fields have the same structure and data type for update but are instead the counts for the Zone (ZOCOUNT), Prerequisite (PRCOUNT), Update (UPCOUNT), and Additional Information (ARCOUNT) sections.

2.1 One Spare Bit?

It would appear that the "Z" bit is spare and [RFC 1035] says that it must be zero in all queries and responses. However, there have been

DNS implementations for which that bit being on in a query meant that only a response from the primary server for a zone is acceptable.

It is believed that modern DNS implementations ignore this bit.

Assigning a meaning to this bit requires an IETF standards action.

2.2 Opcode Assignment

Currently DNS OpCodes are assigned as follows:

OpCode	Name	Reference
0	Query	[RFC 1035]
1	IQuery (Inverse Query)	[RFC 1035]
2	Status	[RFC 1035]
3	available for assignment	
4	Notify	[RFC 1996]
5	Update	[RFC 2136]
6-15	available for assignment	

New OpCode assignments require an IETF consensus.

IANA currently maintains an on list listing of assigned DNS OpCodes at <ftp://ftp.isi.edu/in-notes/iana/assignments/dns-parameters>.

2.3 RCODE Assignment

It would appear from the DNS header above that only four bits of RCODE, or response/error code are available. However, RCODEs can appear not only at the top level of a DNS response but also inside TSIG RRs [RFC XXX3] and OPT RRs [RFC 2671]. The OPT RR provides an eight bit extension resulting in a 12 bit RCODE field and the TSIG RR has a 16 bit RCODE field.

RCODE	Name		Reference
0	NoError	No Error	[RFC 1035]
1	FormErr	Format Error	[RFC 1035]
2	ServFail	Server Failure	[RFC 1035]
3	NXDomain	Non-Existent Domain	[RFC 1035]
4	NotImp	Not Implemented	[RFC 1035]
5	Refused	Query Refused	[RFC 1035]
6	YXDomain	Name Exists when it should not	[RFC 2136]
7	YXRRSet	RR Set Exists when it should not	[RFC 2136]
8	NXRRSet	RR Set that should exist does not	[RFC 2136]

9   NotAuth   Server Not Authoritative for zone [RFC 2136]

10	NotZone	Name not contained in zone	[RFC 2136]
11-15		available for assignment	
16	BADSIG	Signature Failure	[RFC XXX3]
17	BADKEY	Key not recognized	[RFC XXX3]
18	BADTIME	Signature out of time window	[RFC XXX3]
19-0xFFFF		available for assignment	

Since it is important that RCODEs be understood for interoperability, new RCODE assignment requires an IETF consensus.

Current IANA DNS RCODE assignments are shown at <ftp://ftp.isi.edu/in-notes/iana/assignments/dns-parameters>...

3. DNS Resource Records

All RRs have the same top level format shown in the figure below taken from [RFC 1035]:

```
                                    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                     /
    /                                               /
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

NAME is an owner name, i.e., the name of the node to which this resource record pertains. NAMEs are specific to a CLASS as described in section 3.2. NAMEs consist of an ordered sequence of one or more labels each of which has a label type [RFC 1035, 2671]. See also IANA NAME considerations in section 3.3.

TYPE is a two octet unsigned integer containing one of the RR TYPE codes. See section 3.1.

CLASS is a two octet unsigned integer containing one of the RR CLASS codes. See section 3.2.

TTL is a four octet (32 bit) bit unsigned integer that specifies the number of seconds that the resource record may be cached before the source of the information should again be consulted. Zero is interpreted to mean that the RR can only be used for the transaction in progress.

RDLENGTH is an unsigned 16 bit integer that specifies the length in octets of the RDATA field.

RDATA is a variable length string of octets that constitutes the resource. The format of this information varies according to the

TYPE and in some cases the CLASS of the resource record.

3.1 RR TYPE IANA Considerations

There are three subcategories of RR TYPE numbers: data TYPEs, QTYPEs, and MetaTYPEs.

Data TYPEs are the primary means of storing data QTYPES can only be used in queries. Meta-TYPEs designate transient data associated with an particular DNS message and in some cases can also be used in queries. Thus far, data TYPEs have been assigned from 1 upwards plus the block from 100 through 103 while Q and Meta Types have been assigned from 255 downwards (??? except for the OPT RR which is assigned TYPE 41 ???).

There are currently three Meta-TYPEs: TSIG [RFC XXX3], TKEY [RFC XXX5], and OPT [RFC 2671].

There are currently five QTYPEs: * (all), MAILA, MAILB, AXFR, and IXFR.

Considerations for the allocation of new RR TYPEs are as follows:

0x0000 - TYPE zero is used as a special indicator for the SIG RR [RFC 2535] and in other circumstances and must never be allocated for ordinary use.

0x0001 - 0x007F - remaining TYPEs in this range are assigned for data TYPEs only by IETF consensus.

0x0080 - 0x00FF - remaining TYPEs in this rage are assigned for Q and Meta TYPEs only by IETF consensus.

0x0100 - 0x7FFF - assigned for data, Q, or Meta TYPE use by IETF consensus.

0x8000 - 0xFEFF - assigned based on RFC publication.

0xFF00 - 0xFFFF - this block is assigned for private experimental use. Because their use is not coordinated, values/uses may conflict between different experiments.

IANA currently maintains a table of RR TYPE assignments at <ftp://ftp.isi.edu/in-notes/iana/assignments/dns-parameters>.

3.1.1 Special Note on the OPT RR

The OPT (OPTion) RR, number 41 (???), is specified in [RFC 2671]. Its primary purpose is to extend the effective field size of various

DNS fields including RCODE, label type, OpCode, flag bits, and RDATA size. In particular, for resolvers and servers that recognize it, it extends the RCODE field from 4 to 12 bits.

3.1.2 Special Note on the SINK RR

The (Kitchen) SINK RR, number 40, is specified in RFC [XXX2]. It is designed to accommodate requirements for proprietary RRs and provides flexible encoding and semantic labeling of the RDATA potion. This should virtually eliminate the need to allocate RR types codes for private or proprietary purposes.

3.2 RR CLASS IANA Considerations

DNS CLASSes have been little used but constitute another dimension of the DNS distributed database. In particular, there is no necessary relationship between the namespace or roots servers for one CLASS and those for another CLASS. The same name can have completely different meanings in different CLASSes. However, as global networking and DNS have evolved, the IN, or Internet, CLASS has dominated DNS use.

There are two subcategories of DNS CLASSes: normal data containing classes and QCLASSes that are only meaningful in queries or updates.

The current data class assignments and considerations for future assignments are as follows:

0x0000 - assignment requires an IETF standards action.

0x0001 - Internet (IN).

0x0002 - available for assignment by IETF consensus as a data CLASS.

0x0003 - Chaos (CH) [Moon 81].

0x0004 - Hesiod (HS) [Dyer 87].

0x0005 - 0x007F - available for assignment by IETF consensus as data CLASSes only.

0x0080 - 0xFFFD - available for assignment by IETF consensus as QCLASSes only.

0x00FE - QCLASS None [RFC 2136].

0x00FF - QCLASS Any [RFC 1035].

0x0100 - 0x7FFF - assigned by IETF consensus.

0x8000 - 0xFEFF - assigned by RFC publication.

0xFF00 through 0xFFFE are assigned for private experimental use. Because their use is not coordinated, it values/uses may conflict between different experiments.

0xFFFF - can only be assigned by an IETF standards action.

Currently IANA documents CLASS assignments at <ftp://ftp.isi.edu/in-notes/iana/assignments/dns-parameters>.

3.3 RR NAME IANA Considerations

DNS NAMEs are sequences of labels [RFC 1035]. The last label in each NAME is "ROOT" which is the zero length label. By definition, the null or ROOT label can not be used for any other NAME purpose.

At the present time, there are two categories of label types, data labels and compression labels. Compression labels are pointers to data labels elsewhere within an RR or DNS request or reply and are intended to shorten the wire encoding of NAMEs. The two existing data label types will be referred to as ASCII and Binary. ASCII labels can, in fact, include any octet value including zero octets but most current uses involve only [US-ASCII] For retrieval ASCII labels are defined to treat upper and lower case letters the same. Binary labels are bit sequences [RFC 2673].

IANA considerations for label types are given in [RFC 2671].

NAMEs are local to a CLASS. The Hesiod [Dyer 87] and Chaos [Moon 81] CLASSes are essentially for local use. The IN or Internet LASS is thus the only DNS CLASS in global use on the Internet at this time.

The following subsections give IANA considerations for the allocation of names in the IETF recommended root zone. An old snap shoot of such considerations is given in [RFC 1591]. As described in Appendix B, there is nothing to prevent other root zones from existing or being used by those who wish to use the IETF recommended root zone.

3.3.1 Reserved TLDs in the Internet CLASS

All Binary label TLDs [RFC 2673] and other new non-ASCII TLD label data types are reserved.

The remainder of this subsection and 3.3.2 and 3.3.3 refer only to ASCII labels.

All TLDs including any octets that are not letters, digits, or hyphen are reserved. Expression of internationalized names in the DNS is an active area of investigation within the IETF at this time and may make use of these reserved TLD octet values.

All numeric TLDs from "0" through "4294967295" (2**32 -1) are reserved to avoid conflict with IPv4 integer and dotted quad address notations. While many standards distinguish readable addresses by surrounding them with square brackets ("[]"), other widely used standards such as URIs [RFC 2396] do not provide any syntactic way to distinguish these.

All single octet length top level domain (TLD) names are reserved. Should the root zone ever get very large, there are technical solutions involving referral to servers providing splits of the zone based on the first name octet, which would be eased by having the single byte TLDs available. In addition, these provide a potential additional axis for DNS expansion. For like reasons, it is recommended that within TLD zones or indeed within any zone that is or might become very large, in the absence of a strong reason to the contrary, all single octet names be reserved. See Appendix A.

Finally, the four ASCII TLDs "example", "invalid", "localhost", and "test" are reserved as described in [RFC 2606].

Assignment of any of the above reserved names requires an IETF consensus.

3.3.2 'Country Code' TLDs in the Internet CLASS

Two octet length ASCII label TLDs in the Internet CLASS consisting of letters are for assignment to geo-political territories. Those (1) allocated by [ISO 3166-1] and (2) allocated by the Universal Postal Union [UPU] and reserved in [ISO 3166-1] even though not formally assigned by [ISO 3166-1], are assigned as so allocated. Two letter codes reserved by [ISO 3166-1] for local use or the like are also reserved as TLDs as are two letter TLDs not yet allocated or reserved by [ISO 3166-1]. A generally recognized acting government of the territory associated with a "country code" has priority to act as or designate the registrar for such TLDs. If no such government has exercised its authority, non-governmental entities may act as the registrar under rules established by IANA (see www.iana.org).

Normal diplomatic usage recognizes that special consideration can be given to founders. For example, at every Olympics, three flags are equally honored: the Olympic flag, the host nation flag, and the Greek flag because Greece was the founder of the modern Olympics. The Universal Postal Union [UPU] requires all stamps used internationally to indicate the country issuing them except for the stamps of Great Britain. As the first nation to issue stamps, it is exempt from this restriction. Similarly, as the founder of the Internet and due to historical factors, the United States of America is assigned the three letter TLDs ".gov" and ".mil" in addition to ".us".

Two byte codes consisting of other than letters and not reserved in 3.3.1 above are not currently used by [ISO 3166-1] or the [UPU]. However, to permit possible expansion of the two octet country codes, they are reserved for future allocation with priority to be given for usage by [ISO 3166-1]

3.3.3 Other TLDs in the Internet CLASS

IANA manages the ".arpa" and ".int" TLDs. The "arpa" TLD is assigned for use in the IPv4 inverse mapping and IANA delegates /8 subzones to holders of a /8 chunk of address space, including the regional address registries. "int" includes the IPv6 inverse address mapping which is at "ip6.int", international treaty organizations, and international registrations at "reg.int". IANA considerations for IP address assignment are given elsewhere.

Control and assignment of various other existing or prospective Internet CLASS TLDs and the authority for the creation of new TLDs is being transferred to the ICANN (www.icann.org) and the DNSO (Domain Name Support Organization, www.dnso.org). Traditionally ".edu" was used for educational institutions, ".net" for network infrastructure organizations, "com" for commercial organizations, and ".org" for other non-profit organizations.

New registrations in ".edu" are currently restricted to four year or longer institutions of higher learning.

4. Security Considerations

This document addresses IANA considerations in the allocation of general DNS parameters, not security. See [RFC 2535] for secure DNS considerations.

References

[Dyer 87] - Dyer, S., and F. Hsu, "Hesiod", Project Athena Technical Plan - Name Service, April 1987,

[ISO 3166-1] - "Codes for the representation of names of countries", <http://www.din.de/gremien/nas/nabd/iso3166ma/>.

[Moon 81] - D. moon, "Chaosnet", A.I. Memo 628, Massachusetts Institute of Technology Artificial Intelligence Laboratory, June 1981.

[RFC 1034] - P. Mockapetris, "Domain Names - Concepts and Facilities", STD 13, November 1987.

[RFC 1035] - P. Mockapetris, "Domain Names - Implementation and Specifications", STD 13, November 1987.

[RFC 1591] - J. Postel, "Domain Name System Structure and Delegation", March 1994.

[RFC 1996] - P. Vixie, "A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)", August 1996.

[RFC 2119] - S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", March 1997.

[RFC 2136] - P. Vixie, S. Thomson, Y. Rekhter, J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", 04/21/1997.

[RFC 2181] - Robert Elz, Randy Bush, "Clarifications to the DNS Specification", July 1997.

[RFC 2396] - T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", August 1998.

[RFC 2434] - "Guidelines for Writing an IANA Considerations Section in RFCs", T. Narten, H. Alvestrand, October 1998.

[RFC 2535] - D. Eastlake, "Domain Name System Security Extensions", March 1999.

[RFC 2606] - D. Eastlake, A. Panitz, "Reserved Top Level DNS Names", June 1999.

[RFC 2671] - P. Vixie, "Extension mechanisms for DNS (EDNS0)", August 1999.

[RFC 2672] - M. Crawford, " Non-Terminal DNS Name Redirection", August 1999.

[RFC 2673] - M. Crawford, "Binary Labels in the Domain Name System", August 1999.

[RFC XXX2] - D. Eastlake, "The Kitchen Sink DNS Resource Record", xxx 1999 (draft-ietf-dnsind-kitchen-sink-*.txt).

[RFC XXX3] - P. Vixie, O. Gundmundsson, D. Eastlake, B. Wellington, "Secret Key Transaction Signatures for DNS (TSIG)", xxx 1999 (draft-ietf-dnsind-tsig-*.txt).

[RFC XXX5] - D. Eastlake, "Secret Key Establishment for DNS (TKEY RR)", xxx 1999 (draft-ietf-dnsind-tkey-00.txt).

[UPU] - Universal Postal Union, <http://www.upu.int>

[US-ASCII - ANSI, "USA Standard Code for Information Interchange", X3.4, American National Standards Institute: New York, 1968.

Appendix A: Single Letter or Digit Labels

As described in Section 3.3.1, single octet ASCII labels should generally be reserved.

In furtherance of this, on December 1st, 1993, IANA explicitly reserved all available single letter and single digit second level domain names in ".com", ".net", and ".org". Existing assignments, listed below, were not disturbed.

```
      q.com    JG (Q225-DOM)
      x.com    Weinstein & DePaolis (X-DOM)
      z.com    HomePage.com, Inc (Z87-DOM)

      i.net    inet solutions pty.ltd. (I274-DOM)
      q.net    Q Net (Q-DOM)

      x.org    The Open Group (X57-DOM)
```

There was no need to explicitly reserve other single octet second level domain names in these TLDs because such non-letter non-digit names were not being assigned. There was no need to explicitly reserve single octet top level domain names because those required IANA approval in any case.

Appendix B: On Becoming Root and TLD Interoperability

This appendix is commentary by Donald Eastlake.

In practice, it is quite easy to put up a set of root servers. DNS resolvers which use those root servers will see the namespace they support. DNS has only downward pointers from zone to subzone and no upward pointers going from zone to superzone. Thus, in creating a root zone, it works technically to pick whatever top level domains (TLDs) you want including, if you wish, TLDs that are not generally recognized or variant versions of TLDs that are generally recognized.

Setting up your own root zone like this is commonly done within local enclaves to hide some local names, for security and efficiency. In some cases, local TLDs are added. This is reasonable because such names are only supposed to be used locally. But for the global Internet, the use of variant root zones would lead to non-interoperability at the societal and application level. Users would find that email addresses didn't work or addressed different accounts for those using different root zone contents. Links in web pages wouldn't work or would address different web resources for those using different root zone contents. It would no longer be possible to globally advertise URLs, email addresses, or anything else incorporating a domain name, either by word of mouth or by mass media such as television networks.

As a result, despite strenuous attempts to promote alternatives, no significant portion of the global Internet has ever used other than the IETF recommended root zone contents (except, in some cases, for strictly local names).

Authors Addresses

Donald E. Eastlake 3rd
IBM
65 Shindegan Hill Road
Carmel, NY 10512 USA

Telephone: +1-914-784-7913 (w)
+1-914-276-2668 (h)
fax: +1-914-784-3833 (w)
email: dee3@us.ibm.com

Eric Brunner
Nokia Research Center
3 Burlington Woods Drive, Suite 250
Burlington, MA 01803 USA

Telephone: +1 781-359-5159
fax: +1 781-359-5196
email: brunner@maine.rr.com

Bill Manning
USC/ISI
4676 Admiralty Way, #1001
Marina del Rey, CA 90292 USA

Telephone: +1 310 822 1511
email: bmanning@isi.edu

Expiration and File Name

This draft expires March 2000.

Its file name is draft-ietf-dnsind-iana-dns-01.txt.