DNS

A Love Affair with Lovecraftian Horrors

by Shane Kerr <shane@time-travellers.org>

The Cthulhu Mythos

- H. P. Lovecraft was an American writer about 100 years ago.
- He created a dark, hidden world where humans are mostly beneath the notice of the terrible creatures that inhabit it.
- True knowledge of the workings of the universe and man's place in it would drive a human to madness.

On Madness, and Ancient Lore

- Does a crazy person know they are insane?
- Lovecraft posited that pulling back the veil of reality by discovering long-hidden secrets would slowly drive one mad.
- Of course, this is just fiction...

On Madness, and Ancient Lore

- Does a crazy person know they are insane?
- Lovecraft posited that pulling back the veil of reality by discovering long-hidden secrets would slowly drive one mad.
- Of course, this is just fiction...
- I've worked more than 25 years on a protocol now more than 40 years old, and I'm fine.

Serial Numbers?

SOA records have a serial number:

```
$ dig -t soa +multiline fosdem.org | grep -vE "^(;|$)"
fosdem.org.         600 IN SOA ns1.fosdem.org. hostmaster.fosdem.org. (
                            5916        ; serial
                            1800        ; refresh (30 minutes)
                            600         ; retry (10 minutes)
                            2419200     ; expire (4 weeks)
                            300         ; minimum (5 minutes)
                            )
```

Serial numbers are mostly used to synchronize DNS zone information between primary and secondary servers.

Serial Numbers? Strange Numbers.

Serial numbers wrap at 4,294,967,295 (which is 2^{32}).

Comparisons are defined between any two numbers. These more-or-less make sense, given ever-increasing numbers.

So **0 > 4,294,967,295**, because 4,294,967,295+1 = 0.

But, this means ordering serial numbers with three or more numbers is sometimes impossible... although other times possible.

Also, if two numbers are exactly 2,147,483,647 (2^{31}-1) apart, neither is defined as greater than, less than, or equal to the other.

Time to Live

- Time to Live, TTL, define how long a DNS record may be cached after query.
- These are stored with redundancy in Resource Record Sets (RRset), since all RR must have the same TTL.
- In addition, half of the TTL space is missing... the values are 32 bits, but only 31 bits are allowed. (2^{31} is 68 years.)

Class and Chaos

Speaking of space... every RR has a wasted 16-bit field for CLASS, which is almost always 1 (IN, for Internet). Like TTL, this is on every RR in an RRset.

CLASS can be 2 (CH, meaning CHAOS), for certain queries of a quizzical nature.

```
$ dig @ns1.fosdem.org ch txt +short version.bind
"PowerDNS Authoritative Server 4.7.3"
```

Ancient TXT

- A TXT record seems very simple. It has arbitrary 8-bit byte values.
- However, a TXT record is actually a list of strings, each with an 8-bit length specifier.
- Many applications ‘helpfully’ split and join longer strings than 255 characters. But not all.
- This does have the nice property of being an ordered list in DNS. Normally RR are in RRsets, which are more-or-less unordered.

Ancient TXT

A set of TXT records:

```
$ dig formless.time-travellers.org -t txt +short
"Nyarlathotep"
"Azathoth"
"Yog-Sothoth"
"Shub-Niggurath"

$ dig formless.time-travellers.org -t txt +short
"Yog-Sothoth"
"Azathoth"
"Shub-Niggurath"
"Nyarlathotep"
```

A TXT record with multiple values:

```
$ dig gods.time-travellers.org -t txt +short
"Azathoth" "Nyarlathotep" "Yog-Soothoth" "Shub-Niggurath"

$ dig gods.time-travellers.org -t txt +short
"Azathoth" "Nyarlathotep" "Yog-Soothoth" "Shub-Niggurath"
```

Ancient TXT

TXT [SHOW RAW]

Type	Domain Name	TTL	Record
TXT	gods.time-travellers.org	300	Azathoth Nyarlathotep Yog-Sothoth Shub-Niggurath

TXT records for **gods.time-travellers.org**:

Record	Type	Value	TTL
gods.time-travellers.org	TXT	"AzathothNyarlathotepYog-SothothShub-Niggurath"	300

TXT Record [Show Raw]

type	Domain Name	TTL	Record
TXT	gods.time-travellers.org	197	Azathoth Nyarlathotep Yog-Sothoth Shub-Niggurath

Question and response

QUESTION

```
dig @one.one.one.one. gods.time-travellers.org. TXT
```

ANSWER

```
gods.time-travellers.org. 300 TXT "AzathothNyarlathotepYog-SothothShub-Niggurath"
```

Answer

Type	Text	Name	Class	TTL
TXT	Azathoth Nyarlathotep Yog-Sothoth Shub-Niggurath	gods.time-travellers.org	IN	300

A World without Status?

THAT IS NOT DEAD WHICH CAN ETERNAL LIE,
AND WITH STRANGE AEONS EVEN DEATH MAY DIE.

OpCode	Name	Reference
0	Query	[RFC1035]
1	IQuery (Inverse Query, OBSOLETE)	[RFC3425]
2	Status	[RFC1035]
3	Unassigned	
4	Notify	[RFC1996]
5	Update	[RFC2136]
6	DNS Stateful Operations (DSO)	[RFC8490]
7-15	Unassigned	

To the author's knowledge there is no implementation of the Status OpCode. A quick test shows inconsistent responses to a Status request with different DNS server implementations returning NotImp, Refused or giving no response at all.

The Status OpCode MUST be marked OBSOLETE.
The correct response to the Status OpCode MUST be NotImp.

All Is Not as It Seems

We all know that "\040" is a string with a space character:

```
$ echo -e "Elder\040Things"
Elder Things
$ echo -e "Mi\055Go"
Mi-Go
```

Except that in zone files, "\040" is a string with a left parenthesis:

```
$ nsupdate
> add antarctica.time-travellers.org 300 TXT "Elder\040Things"
> add pluto.time-travellers.org 300 TXT "Mi\055Go"
> quit
$ dig antarctica.time-travellers.org -t txt +short
"Elder(Things"
$ dig pluto.time-travellers.org -t txt +short
"Mi7Go"
```

RNAME

RNAME A <domain-name> which specifies the mailbox of the person responsible for this zone.

The mailbox encoding standard assumes a mailbox name of the form "<local-part>@<mail-domain>". While the syntax allowed in each of these sections varies substantially between the various mail internets, the preferred syntax for the ARPA Internet is given in [RFC-822].

The DNS encodes the <local-part> as a single label, and encodes the <mail-domain> as a domain name. The single label from the <local-part> is prefaced to the domain name from <mail-domain> to form the domain name corresponding to the mailbox. Thus the mailbox HOSTMASTER@SRI-NIC.ARPA is mapped into the domain name HOSTMASTER.SRI-NIC.ARPA. If the <local-part> contains dots or other special characters, its representation in a master file will require the use of backslash\ quoting to ensure that the domain name is properly encoded. For example, the mailbox Action.domains@ISI.EDU would be represented as Action\.domains.ISI.EDU.

```
$ dig -t soa +multiline fosdem.org | grep -vE "^(;|$)"
fosdem.org.         600 IN SOA ns1.fosdem.org. hostmaster.fosdem.org. (
                            5916       ; serial
                            1800       ; refresh (30 minutes)
                            600        ; retry (10 minutes)
                            2419200    ; expire (4 weeks)
                            300        ; minimum (5 minutes)
```

Summoning RNAME

The process of delving into the black abyss
is to me the keenest form of fascination.
– H. P. Lovecraft

- E-mail addresses in RNAME look different from normal format.
- Let's peer into the abyss, and see what RNAME looks like. We can download the .se domain and query the SOA of every record, and see what we get.
- Only 0.5% of domains in SE have very strange RNAME. Not bad considering RNAME is so rarely helpful...

Mistakes... All Too Human?

.
admin.
administrator.
hostmaster.
HostmasterEmail.
info.
----at-----dotse.
postmaster.
root.

172800.
28800.
3600.

2023050400.

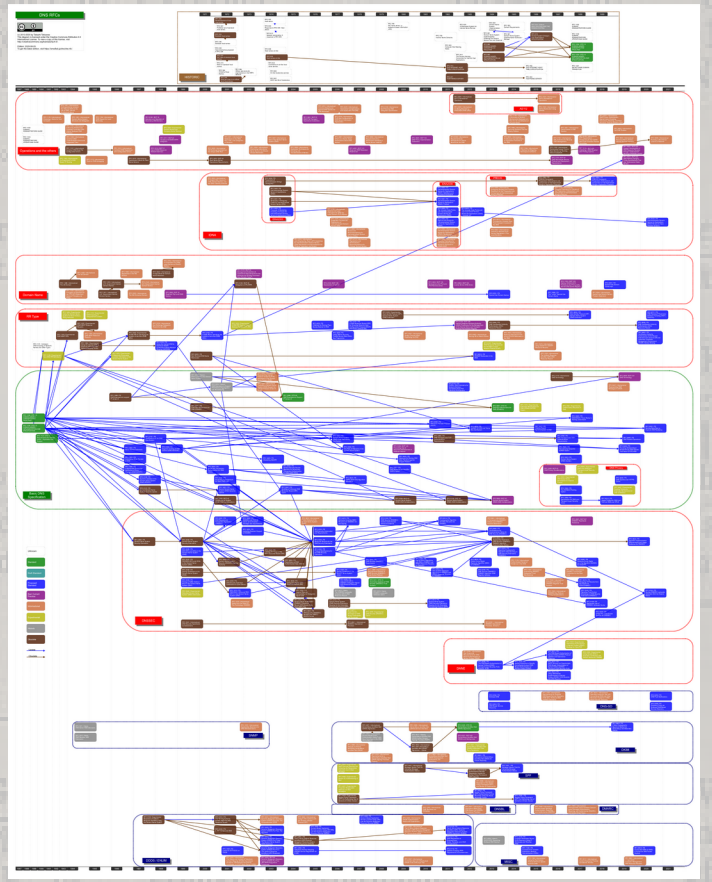
5.179.112.12.

abuse.admax\.se.
----\@webworld\@ie.
nobody\@invalid.
postmaster\@mkweb.se
registry.n62-se.
support\@diagonal\@se.
----\@-----\@fi.

please_set_email.absolutely.nowhere.

DNS Expanded Mythos

- DNS is defined in IETF RFCs. Numerous RFCs.
- There are many DNS features that are not defined in any IETF RFC.
- There is also lore that everyone writing DNS software learns through experience.



DNS Expanded Mythos

- BIND views: Implements split-brain DNS, where you give different answers to different clients.
- Response Policy Zones (RPZ): A way to transmit information about zones to block using XFR. Used by both people selling security blocklists and censors of all stripes.
- Response Rate Limit (RRL): Makes DNS servers less useful in reflection or amplification attacks.
- dnstap: An efficient way for DNS servers to log queries and answers.

References

Main font
https://fontmeme.com/call-of-cthulhu-font/
https://fontmeme.com/fonts/jmh-cthulhumbus-font/
Free for personal use

Enochian font
https://www.fontspace.com/enochian-font-f6183
Freeware, non-commercial

Typewriter font (JMH Typewriter mono)
https://www.fontspace.com/jmh-typewriter-mono-font-f29857
Free, non-commrecial

Nineteenth font
https://www.fontspace.com/nineteenth-font-f40615
Free for personal use

Vanilla creme font (handwriting)
https://www.1001fonts.com/vanilla-cream-ox-font.html
FFEEARR - Free License v4.txt (Free for personal or commercial use)

Tentacles image
https://pngimg.com/image/47007
CC BY-NC 4.0

Background
https://www.myfreetextures.com/excellent-old-brown-paper-texture-background/
Credit must be given

Shadow Over Innsmouth 1st edition cover
https://www.lwcurrey.com/pages/books/170062/lovecraft/the-shadow-over-innsmouth
Public domain in Europe

The Alchemist Discovering Phosphorus
https://en.wikipedia.org/wiki/The_Alchemist_Discovering_Phosphorus
Public domain worldwide

Tensegrity Tower
https://ropesandpoles.blogspot.com/2006/03/step-by-step-tensegrity-tower-part-1.html
CC BY-NC-SA

https://en.wikipedia.org/wiki/Tensegrity
https://photos1.blogger.com/blogger/3732/1264/1600/Needle%20Tower%200002.0.jpg

From Beyond first page
https://en.wikipedia.org/wiki/From_Beyond_(short_story)#/.../File:From_Beyond_(short_story).jpg
Public domain

Hammer and Anvil (used for chaos)
https://www.deviantart.com/sunnyclockwork/art/SCP-2217-491387318
CC BY-SA 3.0

Ancient text (Isha Upanishad)
https://en.wikipedia.org/wiki/Isha_Upanishad
https://en.wikipedia.org/wiki/Isha_Upanishad#/media/File:MS_Indic_37,_Isa_upanisad._Wellcome_L0027330.jpg
Public domain

Factories in fog
https://www.cam.ac.uk/research/news/industrial-revolution-damaging-psychological-imprint-persists-in-todays-populations
CC BY

https://www.cam.ac.uk/sites/default/files/styles/content-885x432/public/news/research/news/m7jarbgt.jpg

References

Cthulhu
https://bytescapes.com/science-fiction/bestiary/cthulhu/
CC BY-NC

IANA DNS Parameters Page
https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-2
CC0 1.0

Proposal to deprecate the Status opcode
https://datatracker.ietf.org/doc/html/draft-dickinson-dnsop-deprecating-status-opcode-00
Copyright IETF Trust

Dunwich Horror
https://www.newgrounds.com/art/view/ccrawler/the-dunwich-horror
CC BY-NC

View of DNS RFCs
https://emaillab.jp/dns/dns-rfc/
CC BY

SE TLD data
https://internetstiftelsen.se/en/zone-data/
CC BY 4.0

DNS RFCs
RFC 1034
https://www.rfc-editor.org/info/rfc1034

RFC 1035
https://www.rfc-editor.org/info/rfc1035

King of Denmark family tree
https://www.pinterest.com/pin/denmark--361765782580412142/
Public domain

Indian post card from 1918-1920
https://rareindiancollectibles.blogspot.com/2011/01/1918-1920-george-v-india-postal-cards.html
Public Domain

Nautilus
https://pxhere.com/en/photo/946269
CC0