CLOUDFLARE®

DNS: One wireformat how many protocols?

Ólafur Guðmundsson

What DNS is depends on the context and perspective

- Protocol in the IETF sense
- Eco system
- System of control
- Kitchen sink
- Something to avoid

1983 DNS born
1984 TLD list “frozen”
1993 .com starts charging
1993 Dynamic updates
1997 DNSSEC-v1
1998 ICANN created
2002 Sitefinder
2004 10 STLD’s approved
2007 Kaminski bug
2013 New GTLD’s
2016 Dyn Attack
2018 Route53 Hijack

My DNS background

Academian

Protocol Implementor

Protocol politician

Protocol researcher/promoter

Consultant

Operator

1987 Touch DNS first
1987 First IETF meeting
1994 first DNSSEC implementation attempt in Bind8
1997 DNSSEC-v1 RFC2065
1999 DNSSEC-v2 RFC2565
1999 DNSIND chair
2000 DNSEXT chair
2001 Propose DS record
2005 DNSSEC-v3 RFC4035
2007 Kaminsky "bug"
2008 NSEC3 disaster
2013 DANE wg chair
2014 Join Cloudflare
2015 Refuse ANY
2016 DNSSEC at scale

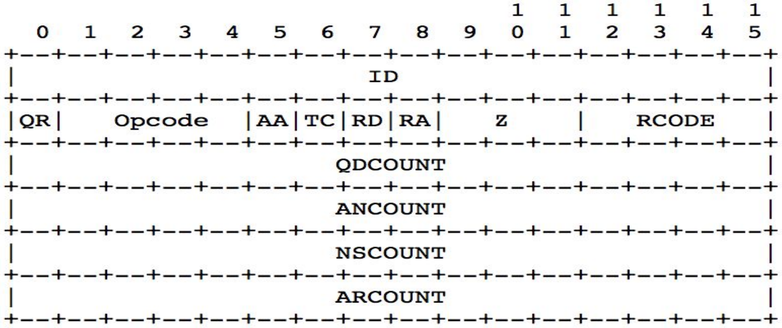
What is DNS ?

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

DNS in the Protocol sense

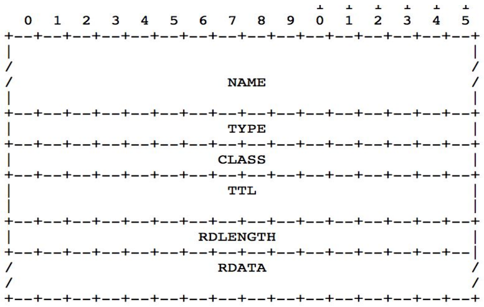
Wire format RFC1034



```
                                    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    |   RCODE   |
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |                    QDCOUNT                    |
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |                    ANCOUNT                    |
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |                    NSCOUNT                    |
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |                    ARCOUNT                    |
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

Header

Resource record



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

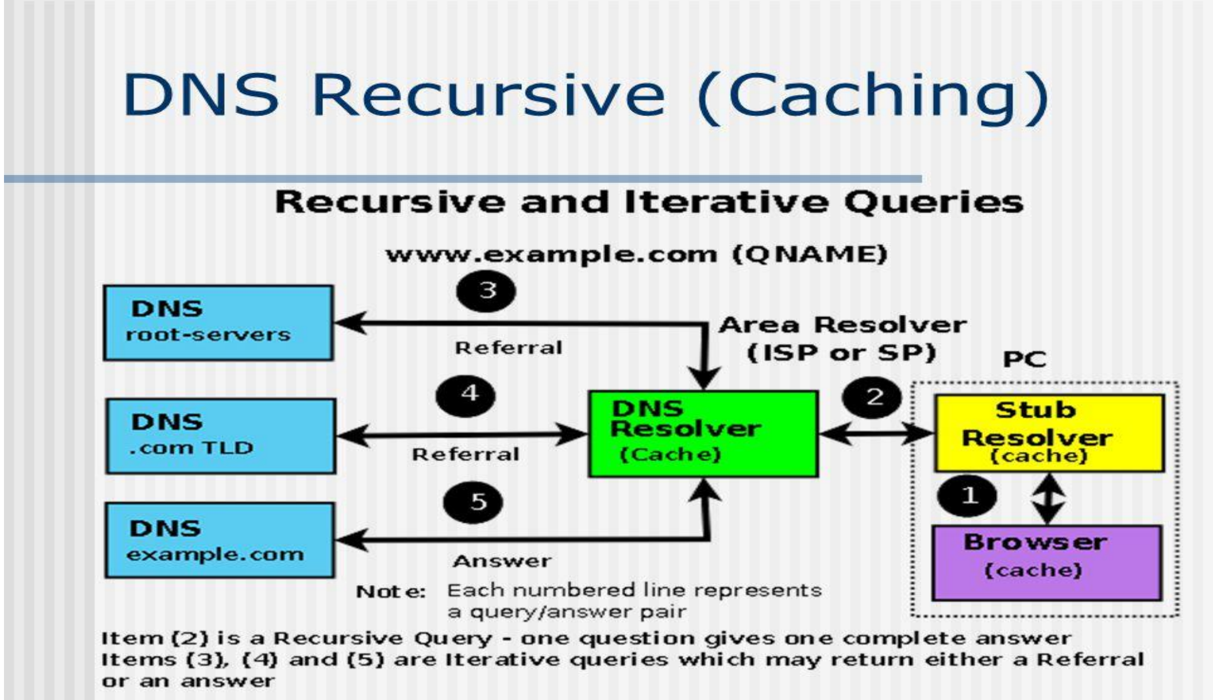
All DNS protocol elements understand this basic wireformat

Arpanet, Bitnet, X25, OSI, DECNET ….

Unifiers:

- Ethernet
- TCP/IP
- Network effect

DNS participants



DNS Recursive (Caching)

Recursive and Iterative Queries

www.example.com (QNAME)

3

DNS
root-servers

Referral

Area Resolver
(ISP or SP)

PC

4

DNS
.com TLD

Referral

DNS
Resolver
(Cache)

2

Stub
Resolver
(cache)

1

5

DNS
example.com

Answer

Browser
(cache)

Note: Each numbered line represents
a query/answer pair

Item (2) is a Recursive Query - one question gives one complete answer
Items (3), (4) and (5) are Iterative queries which may return either a Referral
or an answer

All the hard work is done by Resolver

Lots of Authority servers

Only a handful of Resolvers in wide use

DNS unique: connectionless

UDP main transport

Hard to determine what other side supports ?

- Optimistic or pessimistic behavior ?
- No good way to say “this is why”
- Narrow error channel: RCODE
- What’s at fault: Other side or Network

1990:
UDP
TCP Zone transfer

2000:
UDP queries
UDP updates
UDP notifies
TCP zone transfers

Y2010:
UDP queries
TCP retry
UDP updates
UDP notfies
UDP zone transfers

Y2020:
+DNSoHTTP
+DNSoTLS
+DNSo????

Wireformat “exceptions”

- Zone transfer: adds a field
- Update: modifies the interpretation of header
- EDNS0: Allows additional records in query
- TSIG/SIG(0) more additional records
- DNSSEC: records and header bits

EDNS0: not everyone got that the E was for “Extension”

The black holes

- Provision systems:
  - Garbage in/out
- DNS libraries:
  - Dictate what can be done
- OS and Language “libraries”
  - Can be real old so no modern crypto
- Firewalls
- Captive Portals
- …..

Not maintained
Only as support what underling

DNS Ecosystem

Participants

- Software/hardware vendors
- Registrars/Registries/Resellers
- Governments/Enforcers
- Operators
- Domain “holders”

Authoritative servers
Resolvers
Firewalls
Provision systems
Registry Systems
Registrar systems
Load Balancers
Browsers
Applications
Monitoring systems
Drop catchers
DDoS attackers
DDoS tools
DDoS defenders
DNSSEC provision tools
Debug tools
Domain reselling tools
Abuse detection
Abuse takedown
Regulators
Intellectual Property rights
CPE/IoT
etc

Do what I want not what I say

Consumers want DNS to

- Work but according to ? ?
- Fast and reliable
- Problems are somebody's else fault

Resolvers get blamed

DNS is what "I" think it is

Software written many years ago is not up to date with **current** IETF standards

How dares the IETF to update DNS specifications!!!!

Too many RFC's to read !!!

All software is written from an "experience" point of view

- RFC's
- Product spec
- PCAP
- Need
-

CLOUDFLARE

Now there are too many

Most DNS “implementations” have “warts” that Resolvers need to overcome

- Query Minimization
- Cookies
- IDN …..

Each is a protocol “variant”

Missing types
Query minimization
Name compression
Upper case in labels
EDNS0 options
Trailing garbage
Header bits not “normal”
fragments handling
Etc. …

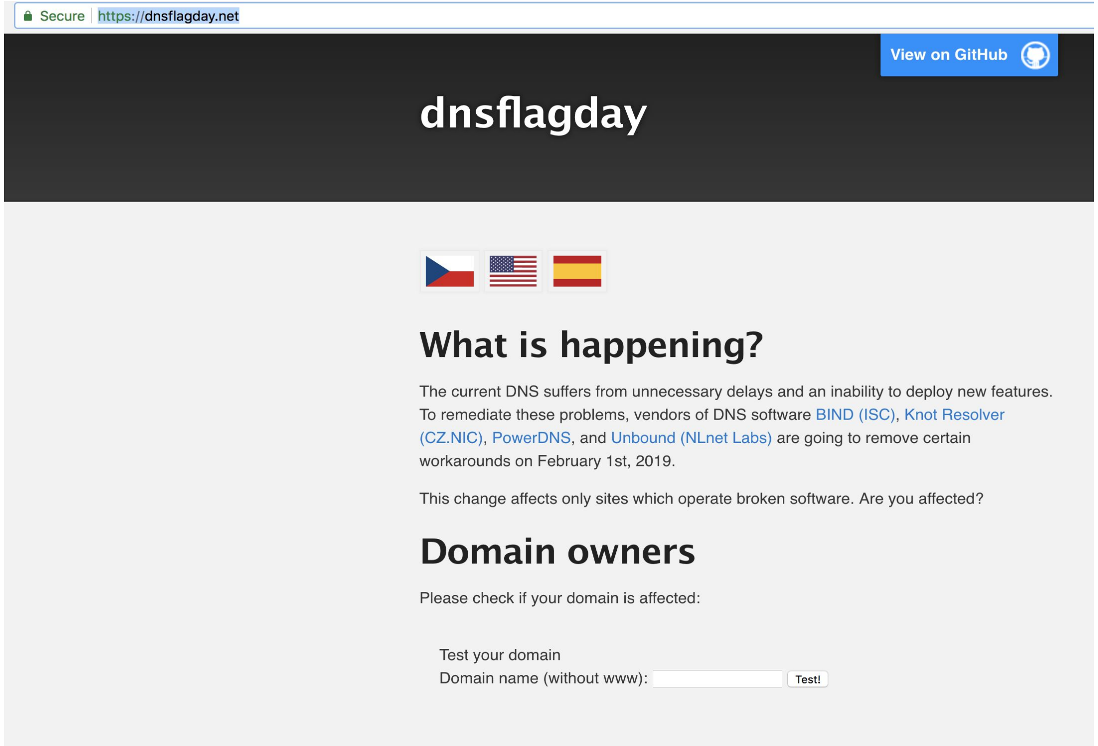
Decades of compromises

© Ron Leishman * www.ClipartOf.com/442230

Do you speak

- German
- French
- Chinese
- Russian
- Urdu
- ……
- Esperanto

https://dnsflagday.net/



dnsflagday

What is happening?

The current DNS suffers from unnecessary delays and an inability to deploy new features. To remediate these problems, vendors of DNS software BIND (ISC), Knot Resolver (CZ.NIC), PowerDNS, and Unbound (NLnet Labs) are going to remove certain workarounds on February 1st, 2019.

This change affects only sites which operate broken software. Are you affected?

Domain owners

Please check if your domain is affected:

Test your domain
Domain name (without www): Test!

The more crap we can fix and remove the better we are going to be in the long run

The DNS future?

- Connection oriented?
  - TLS, HTTP2,
- DNS Camel diet ?
- New formats: Json, yaml ....
- Side channels ?
- Replace it ?

Q: when will DNSoUPD die?

What year will we reach those milestones?

1. Majority over non-UDP?
2. 90%?
3. 99%?