IT’S DNS, JIM...
... BUT NOT AS WE KNOW IT

Jim Hague
Sinodun Internet Technologies
jim.hague@acm.org
@banbury_bill
https://github.com/banburybill
Abstract

This document defines a protocol for sending DNS queries and getting DNS responses over HTTPS. Each DNS query-response pair is mapped into an HTTP exchange.
The Beginning
1. STATUS OF THIS MEMO

This RFC is an introduction to the Domain Name System (DNS), and omits many details which can be found in a companion RFC, "Domain Names - Implementation and Specification" [RFC-1035]. That RFC assumes that reader is familiar with the concepts discussed in this memo.

A subset of DNS functions and data types constitute an official protocol. The official protocol includes standard queries and their responses and most of the Internet class data formats (e.g., host addresses).
DNS

- A consistent namespace used for referring to resources.
- Maintained in a distributed manner.
- Local caching to improve performance.
THE DOMAIN NAMESPACE
DELEGATION OF AUTHORITY
ROOT SERVERS

- A fixed list of IPv4 and IPv6 addresses for 13 servers.
  - a.root-servers.net
  - m.root-servers.net
ROOT SERVERS OPERATORS


IANA has the details
AUTHORITATIVE SERVERS

- Contain the data for a zone
- Run by the zone owner
RECURSIVE SERVERS

- Search the hierarchy to resolve queries
- Cache results and reuse them in future queries
- Typically run by ISP…
- … or 3rd party, e.g. Google, OpenDNS
STUB RESOLVER

- Your local name resolution
- Typically using recursive server(s) supplied by DHCP
A LOOK AT THE WIRE
Format of a DNS message
Format of a Question section
Format of a RR section
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>IPv4 address</td>
</tr>
<tr>
<td>AAAA</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>MX</td>
<td>SMTP servers for domain</td>
</tr>
<tr>
<td>NS</td>
<td>Name servers for domain</td>
</tr>
<tr>
<td>PTR</td>
<td>Pointer to canonical name (for address)</td>
</tr>
<tr>
<td>SRV</td>
<td>Location of servers providing given service</td>
</tr>
<tr>
<td>TXT</td>
<td>General textual information</td>
</tr>
<tr>
<td>SOA</td>
<td>Start of Authority record for zone</td>
</tr>
</tbody>
</table>
TRANSMISSION
TRANSMISSION

- DNS uses UDP
TRANSMISSION

- DNS uses UDP
- Except when it uses TCP
Abstract

The Domain Name System's wire protocol includes a number of fixed fields whose range has been or soon will be exhausted and does not allow clients to advertise their capabilities to servers. This document describes backward compatible mechanisms for allowing the protocol to grow.
EDNS0

- Extends RCODE range and number of flags.
- Mechanism to allow larger UDP messages. This is necessary because of an increase in DNS RR sizes:
  - AAAA records
  - Large TXT records
  - DNSSEC
<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Always 00</td>
<td></td>
</tr>
<tr>
<td>TYPE</td>
<td>16 bits</td>
<td>OPT (41)</td>
</tr>
<tr>
<td>CLASS</td>
<td>16 bits</td>
<td>Sender UDP payload size</td>
</tr>
<tr>
<td>TTL</td>
<td>32 bits</td>
<td>uint8 extended RCODE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>uint8 version (0)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>uint16 flags</td>
</tr>
<tr>
<td>RDLEN</td>
<td>16 bits</td>
<td>Length of RDATA</td>
</tr>
<tr>
<td>RDATA</td>
<td></td>
<td>Options. Any number of:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>uint16 Option Code</td>
</tr>
<tr>
<td></td>
<td></td>
<td>uint16 Option length</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Option data</td>
</tr>
</tbody>
</table>
Client Subnet in DNS Queries

Abstract

This document describes an Extension Mechanisms for DNS (EDNS0) option that is in active use to carry information about the network that originated a DNS query and the network for which the subsequent response can be cached. Since it has some known operational and privacy shortcomings, a revision will be worked through the IETF for improvement.
EDNS0 ECS CLIENT SUBNET

- An unusual RFC
- Encodes client subnet into the query
  - So CDN knows geographic location of client
DNS Security Introduction and Requirements

The Domain Name System Security Extensions (DNSSEC) add data origin authentication and data integrity to the Domain Name System. This document introduces these extensions and describes their capabilities and limitations. This document also discusses the services that the DNS security extensions do and do not provide.
DNSSEC

- Assures authenticity of DNS data
- Assures integrity of DNS data
  - Note it authenticates DNS data, NOT DNS servers
- Does NOT ensure confidentiality
mythic-beasts.com
(2019-04-02 10:53:18 UTC)
NEW DNSSEC RRS

- DNSKEY: A public key
- RRSIG: Signature of RR sets
- NSEC/NSEC3: Name existence
- DS: Digest of DNSKEY record on parent side of delegation
DNSSEC - BACK TO THE WIRE

- EDNS0 flag DO: Client groks DNSSEC.
- New main flags:
  - Authenticated Data (AD): Data is authenticated
  - Checking Disabled (CD): Client is OK to receive non-authenticated data
USING DNSSEC

- If your resolver does DNSSEC:
  - AD indicates data is authenticated
  - SERVFAIL if authentication fails
LAST MILE PROBLEM
LAST MILE PROBLEM

- Can your stub resolver validate?
LAST MILE PROBLEM

- Can your stub resolver validate?
- Can your resolving server validate?
LAST MILE PROBLEM

• Can your stub resolver validate?
• Can your resolving server validate?
• … and even if it can, can you trust the link between you and the resolving server?
LOCAL VALIDATION

- DNSSEC-trigger: https://www.nlnetlabs.nl/projects/dnssec-trigger/
- Stubby: https://getdnsapi.net/blog/dns-privacy-daemon-stubby/
DNSSEC AS PUBLIC KEY INFRASTRUCTURE
• IPSec keys (RFC4025)
• SSH host keys (RFC4255)
• Storing Certificates, CERT RR (RFC4398)
• DKIM keys (RFC4871)
• CA Authorisation (RFC6844)
• DNS Authentication of Named Entities (DANE), X.509 for TLS (RFC6698, 7671)
• OpenPGP key (RFC7929)
IETF RESPONSE - TIMELINE

- 2013:
  - Snowden

- 2014:
  - RFC7285 Pervasive Monitoring is an Attack
  - DPRIVE Working Group formed - goals:
    - Encrypt Stub-Resolver DNS
    - Think about encrypting Resolver-Authoritative
DPRIVE

- 2015:
  - RFC7626 DNS Privacy Considerations
- 2016:
  - RFC7766 DNS over TCP
  - RFC7858 DNS over TLS
Specification for DNS over Transport Layer Security (TLS)

Abstract

This document describes the use of Transport Layer Security (TLS) to provide privacy for DNS. Encryption provided by TLS eliminates opportunities for eavesdropping and on-path tampering with DNS queries in the network, such as discussed in RFC 7626. In addition, this document specifies two usage profiles for DNS over TLS and provides advice on performance considerations to minimize overhead from using TCP and TLS with DNS.
DNS OVER TLS (DOT)

DNS over TCP, but using TLS and to port 853
DOT MODES
DOT MODES
DOT MODES
DOT SUPPORT

- Clients: Android Pie, systemd, Stubby
  - Native Windows/macOS/iOS support still needed
- Servers: Unbound, Knot resolver, dnsdist, Bind via proxy
- November 2017: Quad9 public DNS (9.9.9.9)
- March 2018: Cloudflare public DNS (1.1.1.1)
- January 2019: Google public DNS (8.8.8.8)
DNS Query Name Minimisation to Improve Privacy

Abstract

This document describes a technique to improve DNS privacy, a technique called "QNAME minimisation", where the DNS resolver no longer sends the full original QNAME to the upstream name server.
QNAME MINIMISATION
The inexorable growth of DNS
TACKLING THE CAMEL

https://powerdns.org/hello-dns/
https://powerdns.org/dns-camel/
DOH TIMELINE

- March 2017: Discussed at IETF 98
- May 2017: First draft published
- September 2017: DoH Working Group formed - goals:
  - Standardise encodings for DNS queries and responses that are suitable for use in HTTPS
DOH TIMELINE

- October 2017: DoH draft adopted by WG
- July 2018: Submitted to IESG
- August 2018: Approved
- October 2018: RFC8484 published
DNS OVER HTTPS

- Each DNS query/response is a HTTP exchange
- Must use https URI scheme
  - HTTP/2 is minimum recommended HTTP version
  - SHOULD use 0 in DNS ID
- Client configured via URI template (RFC6570)
  - https://dnsserver.example.net/dns-query{?dns}
DNS OVER HTTPS

- Defined application/dns-message media type
  - Same as the payload of a DNS UDP packet
  - Maximum size 65535
  - Door open to future definitions of alternate media types: DNS/JSON perhaps?
- HTTP cache control and DNS TTL need to be coordinated
DOH: HTTP GET QUERY

::method = GET
::scheme = https
::authority = dnsserver.example.net
::path = /dns-query?dns=AAABAAABAAAAA2d3dwdleGFtcGxlA2NvbQAAAAQAB
accept = application/dns-message

- Query data is encoded in base64url.
DOH: HTTP POST QUERY

:method = POST
:scheme = https
:authority = dnsserver.example.net
:path = /dns-query
accept = application/dns-message
content-type = application/dns-message
content-length = 33

<33 bytes represented by the following hex encoding>
00 00 01 00 00 01 00 00 00 00 00 00 03 77 77 77
07 65 78 61 6d 70 6c 65 03 63 6f 6d 00 00 01 00
01
DOH: HTTP RESPONSE

:status = 200
content-type = application/dns-message
content-length = 61
cache-control = max-age=3709

<61 bytes represented by the following hex encoding>
00 00 81 80 00 01 00 01 00 00 00 00 03 77 77 77
07 65 78 61 6d 70 6c 65 03 63 6f 6d 00 00 1c 00
01 c0 0c 00 1c 00 01 00 00 0e 7d 00 10 20 01 0d
b8 ab cd 00 12 00 01 00 02 00 03 00 04

• Query: IN AAAA records for www.example.com
• Response: 1 answer record
  ▪ Address of 2001:db8:abcd:12:1:2:3:4
  ▪ TTL of 3709s (0xe7d)
DOH: COMPARISON WITH DOT
One use case: "Allow web applications to access DNS information via existing browser APIs"
DOH: COMPARISON WITH DOT

- One use case: "Allow web applications to access DNS information via existing browser APIs"
- Discovery: MUST use URI template
  - So no Opportunistic
DOH: COMPARISON WITH DOT

- One use case: "Allow web applications to access DNS information via existing browser APIs"
- Discovery: MUST use URI template
  - So no Opportunistic
- *Increased* tracking potential via HTTP headers (User-Agent, language, etc.)?
DOH: COMPARISON WITH DOT

- One use case: "Allow web applications to access DNS information via existing browser APIs"
- Discovery: MUST use URI template
  - So no Opportunistic
- *Increased* tracking potential via HTTP headers (User-Agent, language, etc.)?
- New privacy concerns
DOH: CONNECTION MODELS

- *Dedicated*: DoH traffic only
DOH: CONNECTION MODELS

- *Dedicated*: DoH traffic only
- *Mixed*: DoH traffic mixed with other HTTPS traffic
DOH: CONNECTION MODELS

- *Dedicated*: DoH traffic only
- *Mixed*: DoH traffic mixed with other HTTPS traffic
  - Better privacy?
DOH: CONNECTION MODELS

- **Dedicated**: DoH traffic only
- **Mixed**: DoH traffic mixed with other HTTPS traffic
  - Better privacy?
  - Impossible to block just DNS traffic
DOH: CONNECTION MODELS

- *Dedicated*: DoH traffic only
- *Mixed*: DoH traffic mixed with other HTTPS traffic
  - Better privacy?
  - Impossible to block just DNS traffic
  - **THE** big differentiator with DoT
DOH: SERVER DEPLOYMENT
STATUS
DOH: SERVER DEPLOYMENT

STATUS

- Large scale:
  - Cloudflare https://cloudflare-dns.com/dns-query
  - Google https://dns.google.com/experimental
  - Quad9 https://dns*.quad9.net/dns-query (3 flavours of service)
DOH: SERVER DEPLOYMENT
STATUS

- Large scale:
  - Cloudflare [https://cloudflare-dns.com/dns-query](https://cloudflare-dns.com/dns-query)
  - Google [https://dns.google.com/experimental](https://dns.google.com/experimental)
- ~12 other test servers
DOH: CLIENT STATUS

- Firefox
- Chrome (Chromium, Bromite)
- curl
- *Intra* Android app
- **cloudflared**
- Various experimental
- **GetDNS/Stubby** in progress
DOH: SERVER IMPLEMENTATIONS

- dnsdist load balancer
- Knot resolver (branch)
DOH IN BROWSERS

- OSs are slow to offer new DNS features
- “We care about the privacy of our users”
- “Reduced latency within the browser”
WHY DOH NOT DOT - MOZILLA
WHY DOH NOT DOT - MOZILLA

- Integration: "leverage the HTTP ecosystem"
WHY DOH NOT DOT - MOZILLA

- Integration: "leverage the HTTP ecosystem"
- HTTPS everywhere: “it works … just use port 443, mix traffic”
WHY DOH NOT DOT - MOZILLA

- Integration: "leverage the HTTP ecosystem"
- HTTPS everywhere: “it works … just use port 443, mix traffic”
- Cool stuff:
  - JSON
  - Server push
  - Get DNS from location other than configured resolver
‘MOZIFLARE’
‘MOZIFLARE’

• “We’d like to turn this on for all our users”
‘MOZIFLARE’

• “We’d like to turn this on for all our users”
• “Cloudflare is our Trusted Recursive Resolver (TRR)”
‘MOZIFLARE’

• “We’d like to turn this on for all our users”
• “Cloudflare is our Trusted Recursive Resolver (TRR)”
• “.., we have a resolver we can trust to protect our users' privacy. This means Firefox can ignore the resolver that the network provides and just go straight to CloudFlare”
‘MOZIFLARE’ CONT.
‘MOZIFLARE’ CONT.
'MOZIFLARE' CONT.
‘MOZIFLARE’ CONT.
7 Layers of the OSI Model

- **Application**: End User layer, HTTP, FTP, IRC, SSH, DNS
- **Presentation**: Syntax layer, SSL, SSH, IMAP, FTP, MPEG, JPEG
- **Session**: Synch & send to port, API’s, Sockets, WinSock
- **Transport**: End-to-end connections, TCP, UDP
- **Network**: Packets, IP, ICMP, IPSec, IGMP
- **Data Link**: Frames, Ethernet, PPP, Switch, Bridge
- **Physical**: Physical structure, Coax, Fiber, Wireless, Hubs, Repeaters
<table>
<thead>
<tr>
<th>OSI Layer</th>
<th>Deployment Layer</th>
<th>SOA / OSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>10: Government</td>
<td>User Layer</td>
<td>SOA</td>
</tr>
<tr>
<td>9: Organization</td>
<td>Services Layer</td>
<td></td>
</tr>
<tr>
<td>8: Individual</td>
<td>Middleware Layer</td>
<td>OSA</td>
</tr>
<tr>
<td>7: Application</td>
<td>Operating System Layer</td>
<td></td>
</tr>
<tr>
<td>6: Presentation</td>
<td>Hardware Layer</td>
<td></td>
</tr>
<tr>
<td>5: Session</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4: Transport</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3: Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2: Data-Link</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1: Physical</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Image by Gvseostud - Own work, [CC BY-SA 3.0](http://creativecommons.org/licenses/by-sa/3.0/)
WILL THIS BE THE 5 MINUTE ARGUMENT?
INDIVIDUAL LAYER
INDIVIDUAL LAYER

- Split between system and browser resolving
  - Home router naming
  - VPN naming
INDIVIDUAL LAYER

• Split between system and browser resolving
  ▪ Home router naming
  ▪ VPN naming
• Configure DNS for each application?
INDIVIDUAL LAYER

- Split between system and browser resolving
  - Home router naming
  - VPN naming
- Configure DNS for each application?
- Breaks parental control service
INDIVIDUAL LAYER

- Split between system and browser resolving
  - Home router naming
  - VPN naming
- Configure DNS for each application?
- Breaks parental control service
- Informed consent
INDIVIDUAL LAYER

- Split between system and browser resolving
  - Home router naming
  - VPN naming
- Configure DNS for each application?
- Breaks parental control service
- Informed consent
- What is best choice for user?
Contract with TalkTalk is based in the same legal jurisdiction, and TalkTalk are subject to GDPR. Regulatory environment for handling of privacy data is understood. Cloudflare’s privacy policy appears satisfactory, but Cloudflare is a US corporation, so subject to different regulatory regime, with laxer requirements.
TalkTalk 2015 data breach is compelling evidence that TalkTalk isn’t a safe host for privacy-related data. Cloudflare’s record is not spotless, but on balance they are more trustworthy than TalkTalk.
... OR THE FULL HALF HOUR?
ORGANISATION LAYER
ORGANISATION LAYER

- Split-horizon DNS
ORGANISATION LAYER

- Split-horizon DNS
- Local content caches
ORGANISATION LAYER

- Split-horizon DNS
- Local content caches
- Service support
ORGANISATION LAYER

- Split-horizon DNS
- Local content caches
- Service support
- Organisation does not regard its own network as belonging to attacker
ORGANISATION LAYER

- Split-horizon DNS
- Local content caches
- Service support
- Organisation does not regard its own network as belonging to attacker
- “My network, my rules”
ORGANISATION LAYER

- Split-horizon DNS
- Local content caches
- Service support
- Organisation does not regard its own network as belonging to attacker
- “My network, my rules”
  - Though if org is an ISP, do customers have a choice of ISP?
GOVERNMENT LAYER
GOVERNMENT LAYER

- Filtering banned content using DNS
GOVERNMENT LAYER

- Filtering banned content using DNS
- Malware detection and mitigation
GOVERNMENT LAYER

- Filtering banned content using DNS
- Malware detection and mitigation
- There are valid reasons organisations need some visibility on their DNS lookups
RELIGIOUS LAYER
RELIGIOUS LAYER

• Will DNS resolving go the way of email?
RELIGIOUS LAYER

- Will DNS resolving go the way of email?
- Internet future:
RELIGIOUS LAYER

- Will DNS resolving go the way of email?
- Internet future:
  - Are we moving inexorably towards an internet totally reliant on a few big corporations?
RELIGIOUS LAYER

- Will DNS resolving go the way of email?
- Internet future:
  - Are we moving inexorably towards an internet totally reliant on a few big corporations?
  - Are we heading for an internet where everything runs on HTTPS to port 443?
DNS PRIVACY NOW

- DoT via system
- Opportunistic or Strict to organisation’s chosen resolver
FIN

https://dnsprivacy.org/