Where will encrypted DNS transports push DNS operators?

Sara Dickinson   sara@sinodun.com
                sinodun.com
                @SinodunCom
The DNS protocol is evolving

**DoT**: DNS-over-TLS
**DoH**: DNS-over-HTTPS

- **DoT** [RFC7858](https://tools.ietf.org/html/rfc7858) standard May 2016 (Port 853)
  - Implemented/deployed in much ‘standard’ open source DNS software (system resolvers, OS DNS implementations)

- **DoH** [draft-ietf-doh-dns-over-https](https://tools.ietf.org/html/draft-ietf-doh-dns-over-https) is accepted for publication
  - Draft focusses on protocol (query initiation on HTTP)
  - Use case: “web apps access DNS via existing browser APIs”
  - Much wider use cases and DoT, not fully explored yet…..
The DNS protocol is evolving

DoT: DNS-over-TLS
DoH: DNS-over-HTTPS

• DoT RFC7858 standard May 2016 (Port 853)
  - Implemented/deployed in much ‘standard’ open source DNS software (system resolvers, OS DNS implementations)

• DoH draft-ietf-doh-dns-over-https is accepted for publication
  - Draft focusses on protocol (query initiation on HTTP)
  - Use case: “web apps access DNS via existing browser APIs”
  - Much wider use cases and DoT, not fully explored yet…..
The DNS protocol is evolving

DoT: DNS-over-TLS
DoH: DNS-over-HTTPS

- **DoT** [RFC7858](https://tools.ietf.org/html/rfc7858) standard May 2016 (Port 853)
  - Implemented/deployed in much ‘standard’ open source DNS software (system resolvers, OS DNS implementations)

- **DoH** [draft-ietf-doh-dns-over-https](https://tools.ietf.org/html/draft-ietf-doh-dns-over-https) is accepted for publication
  - Draft focusses on protocol (query initiation on HTTP)
  - Use case: “web apps access DNS via existing browser APIs”
  - Much wider use cases and DoT, not fully explored yet…..

Don’t upset the camel!

Lots of drive from browser community
What will encryption change?

- **Defeats passive surveillance, provides data integrity**
- Can **authenticate** the server (Prevents redirects, ’increases’ trust (DNSSEC, filtering))

- But…as with other contexts for encryption providing user privacy adds **operational challenges** for operators
  - RFC8404 “Effects of Pervasive Encryption on Operators” but new for DNS operators

- And… big question is **resolver choice**
  - Discovery, defaults or user choice?
What will encryption change?

- Defeats passive surveillance, provides data integrity
- Can authenticate the server (Prevents redirects, ’increases’ trust (DNSSEC, filtering))

- But…as with other contexts for encryption providing user privacy adds operational challenges for operators
  - RFC8404 “Effects of Pervasive Encryption on Operators” but new for DNS operators

- And… big question is resolver choice
  - Discovery, defaults or user choice?
What will encryption change?

- Defeats passive surveillance, provides data integrity
- Can authenticate the server (Prevents redirects, 'increases' trust (DNSSEC, filtering))
- But… as with other contexts for encryption providing user privacy adds operational challenges for operators
  - RFC8404 “Effects of Pervasive Encryption on Operators” but new for DNS operators
- And… big question is resolver choice
  - Discovery, defaults or user choice?
# Open Source Implementations

<table>
<thead>
<tr>
<th></th>
<th>Client</th>
<th>Recursive Resolver</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DoT</strong></td>
<td>System resolvers:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Android Pie</strong>: Opportunistic default</td>
<td>• Unbound, Knot Resolver</td>
</tr>
<tr>
<td></td>
<td>• <strong>systemd</strong> support</td>
<td>• <strong>dnsdist</strong></td>
</tr>
<tr>
<td>Clients</td>
<td>• <strong>getdns</strong> library &amp; <strong>Stubby</strong> (fwd)</td>
<td>• BIND on the way</td>
</tr>
<tr>
<td></td>
<td>• Unbound/Knot resolver (fwd)</td>
<td></td>
</tr>
<tr>
<td><strong>DoH</strong></td>
<td>Browsers:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Firefox</strong> config option</td>
<td>• <strong>dnsdist</strong> (WIP)</td>
</tr>
<tr>
<td></td>
<td>• Chrome/Bromite</td>
<td>• Knot resolver (patches)</td>
</tr>
<tr>
<td>Clients</td>
<td>• getdns/Stubby (next release)</td>
<td>• Various experimental</td>
</tr>
<tr>
<td></td>
<td>• Android ‘Intra’ App</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cloudflared/dnscrypt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Various experimental</td>
<td></td>
</tr>
</tbody>
</table>

More details on [dnsprivacy.org](http://dnsprivacy.org)

Where will encrypted DNS transports push DNS operators?
## Recursive Resolver Deployment

<table>
<thead>
<tr>
<th></th>
<th>Standalone</th>
<th>Large Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DoT</strong></td>
<td>20 test servers</td>
<td>Quad9 (9.9.9.9)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cloudflare (1.1.1.1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CleanBrowsing</td>
</tr>
<tr>
<td><strong>DoH</strong></td>
<td>~10 test servers</td>
<td>Cloudflare (<a href="https://cloudflare-dns.com/dns-query">https://cloudflare-dns.com/dns-query</a>)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Google (<a href="https://dns.google.com/experimental">https://dns.google.com/experimental</a>)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Quad9 (<a href="https://dns*.quad9.net/dns-query">https://dns*.quad9.net/dns-query</a>)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 flavours of service</td>
</tr>
</tbody>
</table>

Where will encrypted DNS transports push DNS operators?
## Recursive Resolver Deployment

<table>
<thead>
<tr>
<th></th>
<th>Standalone</th>
<th>Large Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DoT</strong></td>
<td>20 test servers</td>
<td><strong>Quad9</strong> (9.9.9.9)</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Cloudflare</strong> (1.1.1.1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>CleanBrowsing</strong></td>
</tr>
<tr>
<td><strong>DoH</strong></td>
<td>~10 test servers</td>
<td><strong>Cloudflare</strong> (<a href="https://cloudflare-dns.com/dns-query">https://cloudflare-dns.com/dns-query</a>)</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Google</strong> (<a href="https://dns.google.com/experimental">https://dns.google.com/experimental</a>)</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Quad9</strong> (<a href="https://dns*.quad9.net/dns-query">https://dns*.quad9.net/dns-query</a>)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 3 flavours of service</td>
</tr>
</tbody>
</table>

Increasing deployment within networks (particularly DoT for Android)

Where will encrypted DNS transports push DNS operators?
How is DoH different to DoT?

- **DoH Discovery - MUST use a URI template** (not IP address)
  - Proposals in the works (more later….)

- **Two models:**
  - **Dedicated** connections (only DoH traffic) - hard to block
  - **Mixed** connections (send DoH on existing HTTPS connections)
    - Better privacy? Not leaking queries

- **Increased tracking**: HTTP headers allow tracking of query via e.g. ‘User-agent’ (application), language, etc.
How is DoH different to DoT?

- **DoH Discovery** - MUST use a **URI template** (not IP address)
  - Proposals in the works (more later....)

- **Two models:**
  - **Dedicated** connections (only DoH traffic) - hard to block
  - **Mixed** connections (send DoH on existing HTTPS connections)
    - Better privacy? Not leaking queries

- **Increased tracking:** HTTP headers allow tracking of query via e.g. ‘User-agent’ (application), language, etc.

Can’t probe DHCP servers (unlike Opportunistic DoT)
How is DoH different to DoT?

- **DoH Discovery** - MUST use a URI template (not IP address)
  - Proposals in the works (more later....)

- **Two models:**
  - **Dedicated** connections (only DoH traffic) - hard to block
  - **Mixed** connections (send DoH on existing HTTPS connections)
    - Better privacy? Not leaking queries

**Impossible to block JUST DNS traffic**

- **Increased tracking:** HTTP headers allow tracking of query via e.g. ‘User-agent’ (application), language, etc.

Can’t probe DHCP servers (unlike Opportunistic DoT)

Specification differences

Where will encrypted DNS transports push DNS operators?
How is DoH different to DoT?

- **DoH Discovery** - MUST use a URI template (not IP address)
  - Proposals in the works (more later….)

- **Two models:**
  - **Dedicated** connections (only DoH traffic) - hard to block
  - **Mixed** connections (send DoH on existing HTTPS connections)
    - Better privacy? Not leaking queries

**Impossible to block JUST DNS traffic**

- **Increased tracking**: HTTP headers allow tracking of query via e.g. ‘User-agent’ (application), language, etc.

Can’t probe DHCP servers (unlike Opportunistic DoT)

Classic conflict of encryption vs visibility

Where will encrypted DNS transports push DNS operators?
How is DoH different to DoT?

- **DoH Discovery** - MUST use a **URI template** (not IP address)
  - Proposals in the works (more later….)

- **Two models:**
  - **Dedicated** connections (only DoH traffic) - hard to block
  - **Mixed** connections (send DoH on existing HTTPS connections)
    - Better privacy? Not leaking queries

**Impossible to block JUST DNS traffic**

- **Increased tracking**: HTTP headers allow tracking of query via e.g. ‘User-agent’ (application), language, etc.

**Can’t probe DHCP servers** (unlike Opportunistic DoT)

**Classic conflict of encryption vs visibility**

**Brand new privacy concerns for users!**
DoH in Browsers

- Why encrypt directly from the browser? **Browser folks say:**
  - OS’s are slow to offer new DNS features (DoT/DoH)
  - Selling point: “we care about the privacy of our users”
  - Performance: “reduce latency/better user experience”

- **Firefox** since 61, not enabled by default
  - Firefox Nightly DoH experiments….
- **Chrome** has a DoH implementation
  - Not currently exposed/advertised but [now a PR to add config option](#)
DoH in Browsers

- Why encrypt directly from the browser? **Browser folks say:**
  - OS’s are slow to offer new DNS features (DoT/DoH)
  - Selling point: “we care about the privacy of our users”
  - Performance: “reduce latency/better user experience”

- **Firefox** since 61, not enabled by default
  - Firefox Nightly DoH experiments…. 🌐
- **Chrome** has a DoH implementation
  - Not currently exposed/advertised but [now a PR to add config option](https://www.example.com)

‘secure DNS’: Dedicated DoH connections (NO DNSSEC!)
DoH in Browsers

- Why encrypt directly from the browser? **Browser folks say:**
  - OS’s are slow to offer new DNS features (DoT/DoH)
  - Selling point: “we care about the privacy of our users”
  - Performance: “reduce latency/better user experience”

- **Firefox** since 61, not enabled by default
  - Firefox Nightly DoH experiments….
- **Chrome** has a DoH implementation
  - Not currently exposed/advertised but [now a PR to add config option](https://chromestatus.com/feature/5276443777790048)

Browser vendors control the client and update frequently (remember QUIC)
DoH Experiments in Firefox

- Mozilla blogs:
  - **Experiment & Future plans** (May 2018):
    - “We’d like to turn this [DoH] on as the default for all of our users”
    - “Cloudflare is our ‘Trusted Recursive Resolver’ (TRR)… This means Firefox can ignore the resolver that the network provides and just go straight to
  - **Firefox Nightly ‘Experiment’** (June) & **Experiment results** (Aug)
    - **Does the use of a cloud DNS service perform well enough to replace traditional DNS?**” (Send to system resolver AND to Cloudflare, compare the results.)
  - **Another experiment in Firefox Beta announced**…(Sept)
DoH Experiments in Firefox

- Mozilla blogs:
  - **Experiment & Future plans** (May 2018):
    - “We’d like to **turn this [DoH] on as the default** for all of our users”
    - “Cloudflare is our ‘**Trusted Recursive Resolver’** (TRR)... This means Firefox can ignore the resolver that the network provides and just go straight to
  
  RESULTS: 6ms performance overhead is acceptable

  “We’re committed long term to building a larger ecosystem of trusted DoH providers that live up to a high standard of data handling.”

  **Another experiment in Firefox Beta announced** ...(Sept)
1. **System resolver** default - today use DHCP
   - IETF concluded **DHCP** is insecure (limited use for auth names/URLs)
     BUT: operators want DHCP!
   - **In band DNS** mechanisms? Query server to find services….
     Associated [DoH server draft](#) but not secure either, WIP

2. **Application default**
   - DHCP (if/when discovery available)
   - Manual config (fixed list or user defined)
   - Hardcoded default TRR list
Resolver choice

1. **System resolver** default - today use DHCP
   - IETF concluded **DHCP** is insecure (*limited* use for auth names/URLs)
     BUT: operators want DHCP!
   - **In band DNS** mechanisms? Query server to find services….
     Associated DoH server draft but not secure either, WIP

2. **Application default**
   - DHCP (if/when discovery available)
   - Manual config (fixed list or user defined)
   - Hardcoded default TRR list

Where will encrypted DNS transports push DNS operators?
Resolver choice

1. **System resolver** default - today use DHCP
   - IETF concluded **DHCP** is insecure *(limited use for auth names/URLs)*
     BUT: operators want DHCP!
   - **In band DNS** mechanisms? Query server to find services….
     Associated DoH server draft but not secure either, WIP

2. **Application default**
   - DHCP (if/when discovery available)
   - Manual config (fixed list or user defined)
   - Hardcoded default TRR list

Discovery is the missing link

More later…
3. **Organisation policy:**
   - What if the government or bank started requiring encrypted DNS where possible?

4. **Privacy aware users:**
   - Actively choose to use a specific resolver (for good reason)
   - Trusted vs untrusted network, privacy policy becomes important!
     - Lack of net neutrality in US - many users view their ISP as a threat!
     - GDPR provides restrictions on ISPs in EU (good option)
     - Would you trust your coffee shop DNS if you had option?
Resolver choice

3. **Organisation policy:** It happened with DNSSEC & US gov
   - What if the a government or bank started requiring encrypted DNS where possible?

4. **Privacy aware users:**
   - Actively choose to use a specific resolver (for good reason)
   - Trusted vs untrusted network, privacy policy becomes important!
     - Lack of net neutrality in US - many users view their ISP as a **threat**!
     - GDPR provides restrictions on ISPs in EU (**good option**)
     - Would you trust your coffee shop DNS if you had option?
Resolver choice

3. **Organisation policy:** It happened with DNSSEC & US gov
   - What if the a government or bank started requiring encrypted DNS where possible?

4. **Privacy aware users:**
   - Actively choose to use a specific resolver (for good reason)
   - Trusted vs untrusted network, privacy policy becomes important!
     - Lack of net neutrality in US - many users view their ISP as a threat!
     - GDPR provides restrictions on ISPs in EU (**good option**)
   - Would you trust your coffee shop DNS if you had option?

Transparency and accountability build trust
Impact of encrypted DNS within networks (DHCP)

• DNS: Switching from UDP to session based
  • Performance concerns (for client and server) - scaling!
  • DDoS concerns (attack vectors shift)
  • Operating DNS service over multiple transports (added complexity)

• Operational challenges ([RFC8404](https://www.rfc-editor.org/rfc/rfc8404))
  • Monitoring/troubleshooting/etc. probably needs to change
  • Data handling practices come under scrutiny ([Best Current Practices](https://www.iana.org/registries/dns/))
Impact of encrypted DNS within networks (DHCP)

- DNS: Switching from UDP to session based
  - Performance concerns (for client and server) - scaling!
  - DDoS concerns (attack vectors shift)
  - Operating DNS service over multiple transports (added complexity)

- Operational challenges (RFC8404)
  - Monitoring/troubleshooting/etc. probably needs to change
  - Data handling practices come under scrutiny (Best Current Practices)

Benchmarking needed but complex
Impact of encrypted DNS within networks (DHCP)

- DNS: Switching from UDP to session based
  - Performance concerns (for client and server) - scaling!
  - DDoS concerns (attack vectors shift)
  - Operating DNS service over multiple transports (added complexity)

- Operational challenges (RFC8404)
  - Monitoring/troubleshooting/etc. probably needs to change
  - Data handling practices come under scrutiny (Best Current Practices)

Benchmarking needed but complex
Luxury of passive monitoring gone
Impact of encrypted DNS within networks (DHCP)

- DNS: Switching from UDP to session based
  - Performance concerns (for client and server) - scaling!
  - DDoS concerns (attack vectors shift)
  - Operating DNS service over multiple transports (added complexity)

- Operational challenges (RFC8404)
  - Monitoring/troubleshooting/etc. probably needs to change
  - Data handling practices come under scrutiny (Best Current Practices)

DNS traffic is PII
Impact of default TRRs

- Firefox are not committing:
  - typical answer: “We haven't announced what that config will be or when it will be deployed (because we're still working on it :)).”

- So… DNS community in limbo waiting for decision from browser vendors on potentially major change to DNS infrastructure!
Impact of default TRRs

- Firefox are not committing:
  - **typical answer:** “We haven't announced what that config will be or when it will be deployed (because we're still working on it :)).”

- So… **DNS community in limbo** waiting for decision from browser vendors on potentially major change to DNS infrastructure!

**Change to trust model:** Applications using default TRRs fundamentally change the existing **implicit** consent model for DNS:

- (Current) Log onto a network and use the DHCP provided resolver
- (New?) Use an app and agree to app T&C’s (including DNS?)
Impact of default TRRs

- Firefox are not committing:
  - typical answer: “We haven't announced what that config will be or when it will be deployed (because we're still working on it :)).”

- So… **DNS community in limbo** waiting for decision from browser vendors on potentially major change to DNS infrastructure!

*Change to trust model:* Applications using default TRRs fundamentally change the existing *implicit* consent model for DNS:

- (Current) Log onto a network and use the DHCP provided resolver
- (New?) Use an app and agree to app T&Cs (including DNS?)

Is informed consent possible if users don’t understand DNS (GDPR)?
Impact of default TRRs

Potential centralisation of DNS resolution to a few providers?
Impact of default TRRs

- Potential centralisation of DNS resolution to a few providers?
- Led by Mozilla, really? (They do so many other good things)
  - Potentially drive good practice?
- Where browsers go other applications and some router vendors go….
- Government regulation of TRRs, monetary incentives for apps?
  - Analysis of third party DNS by PowerDNS
    - Neutrality of DNS operators (won’t CDN’s have a conflict of interest?)
    - Transparency of legislation for blocking/filtering/interception?
Impact of default TRRs

Potential centralisation of DNS resolution to a few providers?

- Led by Mozilla, really? (They do so many other good things)
  - Potentially drive good practice?
- Where browsers go other applications and some router vendors go….
- Government regulation of TRRs, monetary incentives for apps?
  - Analysis of third party DNS by PowerDNS
    - Neutrality of DNS operators (won’t CDN’s have a conflict of interest?)
    - Transparency of legislation for blocking/filtering-interception?
Where will encrypted DNS transports push DNS operators?

Operational Impact of TRR

- **Breaks Split horizon DNS** (fallback is possible but slow and leaks internal names) Similar to e.g. using 8.8.8.8 but encrypted…Big impact on enterprises.

- More importantly
Operational Impact of TRR

• **Breaks Split horizon DNS** (fallback is possible but slow and leaks internal names) Similar to e.g. using 8.8.8.8 but encrypted…Big impact on enterprises.

• More importantly

**Encrypted traffic bypasses current local monitoring & security policies**
Operational Impact of TRR

- **Breaks Split horizon DNS** (fallback is possible but slow and leaks internal names) Similar to e.g. using 8.8.8.8 but encrypted...Big impact on enterprises.

- More importantly

  * Encrypted traffic bypasses current local monitoring & security policies

  - Many operators have legal and regulatory requirements on DNS for network protection (because historically possible)
  - Some say: Block/Proxy traffic - ‘My network, my rules’
Operational Impact of TRR

- **Breaks Split horizon DNS** (fallback is possible but slow and leaks internal names) Similar to e.g. using 8.8.8.8 but encrypted…Big impact on enterprises.

- More importantly

```
Encrypted traffic bypasses current local monitoring & security policies
```

- Many operators have legal and regulatory requirements on DNS for network protection (because historically possible)
- Some say: Block/Proxy traffic - ‘My network, my rules’

```
Proposal: Offer an equivalent service locally - minimise justification for using external TRR in a trusted network
```
What’s next for DoH?

- What about **JSON** format (DNS in JSON - [RFC8427](https))?

- **Server Push** has some interesting applications.....

- How long before mixed connections used? Proposals for ‘**Resoverless DNS**’
  - Resolution happens within a ‘context’ e.g. browser tab
  - Does the DoH server have to be a traditional caching recursive resolver?
  - Queries could be customised (geo-loction but what else)?
  - DNS is another form of ‘content’
What’s next for DoH?

- What about **JSON** format (DNS in JSON - [RFC8427](https://tools.ietf.org/html/rfc8427))?  
- **Server Push** has some interesting applications.....
- How long before mixed connections used? Proposals for ‘**Resoverless DNS**’  
  - Resolution happens within a ‘context’ e.g. browser tab  
  - Does the DoH server have to be a traditional caching recursive resolver?  
  - Queries could be customised (geo-location but what else)?  
  - DNS is another form of ‘content’
What’s next for DoH?

- What about JSON format (DNS in JSON - RFC8427)?
- Server Push has some interesting applications.....
- How long before mixed connections used? Proposals for ‘Resoverless DNS’
  - Resolution happens within a ‘context’ e.g. browser tab
  - Does the DoH server have to be a traditional caching recursive resolver?
  - Queries could be customised (geo-location but what else)?
  - DNS is another form of ‘content’

Again, driven by browser community?
Potential fragmentation of DNS configuration across applications?

- Loss of central point of config on an end device?
- Loss of network settings as the default
- DNS no longer part of the device infrastructure?
What to do?

• Think about running a **DoT server** in your network: for system level resolvers e.g. *Android, Stubby, systemd* it is the right thing!

• Think about running a **DoH server** in your network: gives users the option to use that, centralisation of DNS to a few players is a bad thing!

• Review your privacy policy and practice (**BCP**)

• Be aware of changes and how they could affect you (**dnsprivacy.org**)!
What to do?

• Think about running a DoT server in your network: for system level resolvers e.g. Android, Stubby, systemd it is the right thing!

• Think about running a DoH server in your network: gives users the option to use that, centralisation of DNS to a few players is a bad thing!

• Review your privacy policy and practice (BCP)

• Be aware of changes and how they could affect you (dnsprivacy.org)!

WHATEVER YOU DO
DON'T BLINK
Thank you!

dnsprivacy.org
@DNSPrivacyProject
Where will encrypted DNS transports push DNS operators?
DNS-over-TLS (DoT)

RFC7258: Pervasive Monitoring is an attack

Snowdon Revelations

1987  2012  2013  2014  2016  2018

Where will encrypted DNS transports push DNS operators?
DNS-over-TLS (DoT)

- RFC7258: Pervasive Monitoring is an attack
- DPRIVE WG formed
- Goals:
  1) Encrypt Stub-Rec DNS
  2) Think about Rec-Auth?

Snowdon Revelations

Where will encrypted DNS transports push DNS operators?

Timeline:
- 1987:?
- 2012:?
- 2013:?
- 2014:?
- 2016:?
- 2018:?
DNS-over-TLS (DoT)

- **RFC7258**: Pervasive Monitoring is an attack
- **DPRIVE WG** formed
- **Goals**: 1) Encrypt Stub-Rec DNS 2) Think about Rec-Auth?
- **RFC7766**: DNS-over-TCP

Snowdon Revelations

- 1987
- 2012
- 2013
- 2014
- 2016
- 2018

Where will encrypted DNS transports push DNS operators?
Where will encrypted DNS transports push DNS operators?

**DNS-over-TLS (DoT)**

- **RFC7258**: Pervasive Monitoring is an attack
- DPRIVE WG formed
- Goals:
  1) Encrypt Stub-Rec DNS
  2) Think about Rec-Auth?
- **RFC7766**: DNS-over-TCP
- **RFC7858**: DNS-over-TLS
-雪龙登揭露
- DPRIVE WG formed
- Goals:
  1) Encrypt Stub-Rec DNS
  2) Think about Rec-Auth?
- **Port 853**

1987 2012 2013 2014 2016 2018
Where will encrypted DNS transports push DNS operators?

DNS-over-HTTPS (DoH)
DNS-over-HTTPS (DoH)

First DoH draft published (query init)

IETF 98

March 2017

May 2017

Sep 2017

Oct 2017

Jul 2017

Aug 2018

Where will encrypted DNS transports push DNS operators?
DNS-over-HTTPS (DoH)

First DoH draft published (query init)

DoH WG formed

Goals: “This working group will standardize encodings for DNS queries and responses that are suitable for use in HTTPS.”

IETF 98

March 2017

May 2017

Sep 2017

Oct 2017

Jul 2017

Aug 2018

20

Where will encrypted DNS transports push DNS operators?
DNS-over-HTTPS (DoH)

**Goals:** “This working group will standardize encodings for DNS queries and responses that are suitable for use in HTTPS.”

- **First DoH draft published (query init)**: March 2017
- **IETF 98**: May 2017
- **DoH WG formed**: Sep 2017
- **DoH draft adopted**: Oct 2017
- **First DoH draft published**: Jul 2017
- **Aug 2018**

Where will encrypted DNS transports push DNS operators?
DNS-over-HTTPS (DoH)

Goals: “This working group will standardize encodings for DNS queries and responses that are suitable for use in HTTPS.”

First DoH draft published (query init)

IETF 98
March 2017

DoH WG formed

May 2017

DoH draft adopted

Sep 2017
Oct 2017

Submitted to IESG

Jul 2017

Aug 2018

Where will encrypted DNS transports push DNS operators?
Where will encrypted DNS transports push DNS operators?

**Goals:** “This working group will standardize encodings for DNS queries and responses that are suitable for use in HTTPS.”

- **IETF 98**
- **First DoH draft published (query init)**
- **DoH WG formed**
- **DoH draft adopted**
- **Submitted to IESG**
- **Approved**

- **Mar 2017**
- **May 2017**
- **Sep 2017**
- **Oct 2017**
- **Jul 2017**
- **Aug 2018**
Where will encrypted DNS transports push DNS operators?

Goals: “This working group will standardize encodings for DNS queries and responses that are suitable for use in HTTPS.”

First DoH draft published (query init)

DoH WG formed

DoH draft adopted

Submitted to IESG

Approved

IETF 98

March 2017

May 2017

Sep 2017

Oct 2017

Jul 2017

Aug 2018

FAST!