GÉANT
Networks • Services • People

DNS Privacy Protocols

Encrypted DNS queries for privacy protection

Klaus Möller
WP8-T1

Webinar, 10th of December 2020

Public

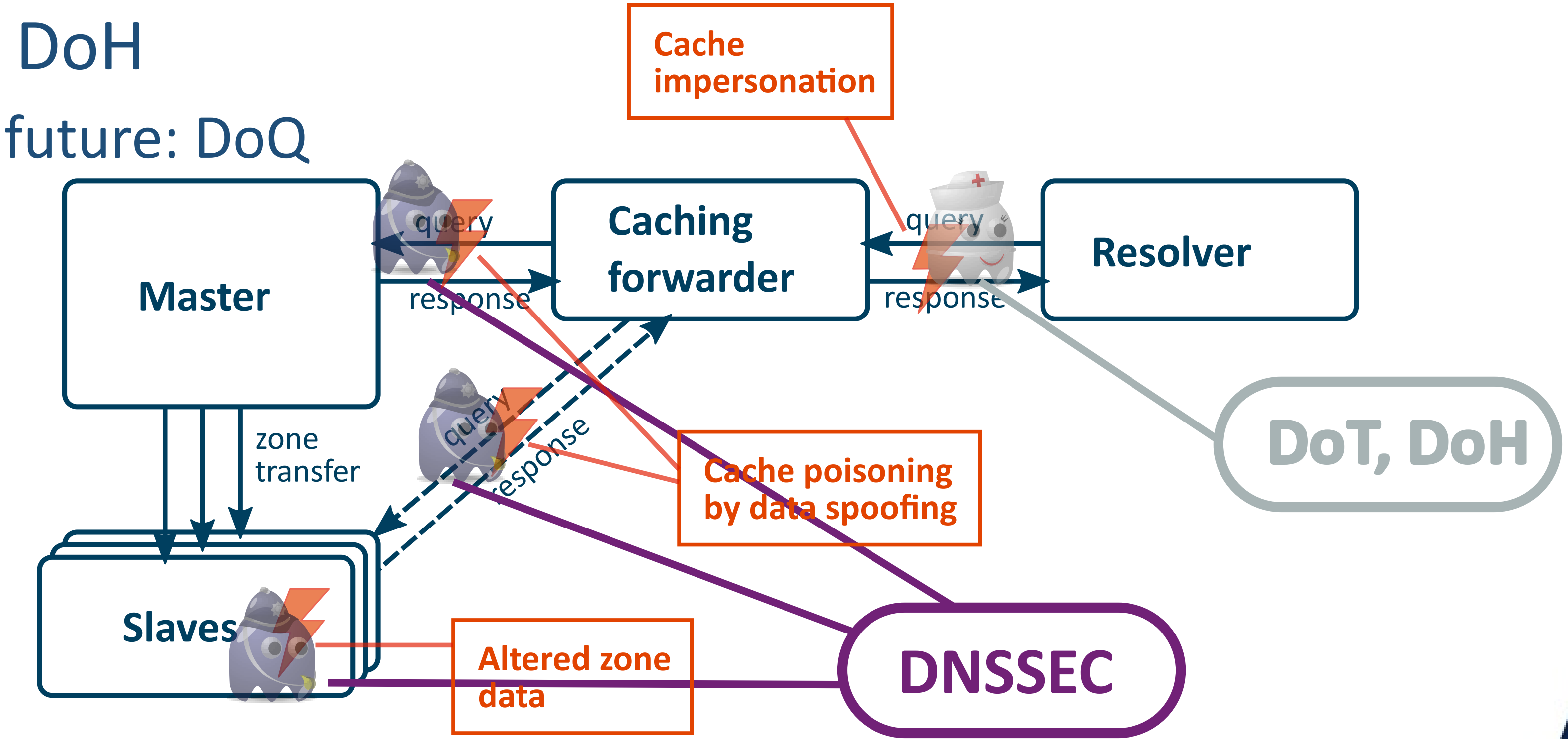
www.geant.org

What we will cover today

- DNS over TLS (DoT)
- DNS over HTTPS (DoH)
- DNS over QUIC (DoQ)
  - Resolverless DNS
- Considerations & Recommendations

DNS Threats

- Haven’ t been entirely correct last time
  - Most stub resolvers don’t do full DNSSEC validation by themselves
  - That means, stub-resolvers have to trust the cache/forwarder
  - And the last leg between stub and cache will have to be secured
- Enter DoT & DoH
  - And in the future: DoQ



Why protect the last leg?

- Ability to interfere with DNS lookups is/was widely abused
- ISPs redirecting to domain selling sites, etc.
- Parental controls, i. e. blocking adult content, etc.
- Governments
  - Regime criticism in authoritarian regimes: North Korea, China,Russia, etc.
  - Various reasons in Western Democracies (i. e. UK, Germany, etc.)
    - Parental controls, child pornography (UK, Germany)
    - Hate speech, Nazis, Islamic State propaganda (Germany)
    - Black markets, Wikileaks, and more on the wish list …
- Power users, home network: Ad-blocking
- Network admins: Malicious Site blocking

GÉANT
Networks • Services • People

DNS over TLS

www.geant.org

© GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).
The research leading to these results has received funding from
the European Union's Horizon 2020 research and innovation
programme under Grant Agreement No. 731122 (GN4-2).

DNS over TLS (DoT)

- Use DNS over either
  - UDP with DTLS (MAY support, RFC 8094)
  - TCP with TLS (**MUST** support, RFC 7854)
- Port number in both cases: 853
- TLS version used will be the most recent one, currently 1.3
- Protocol is otherwise the same
- Scope
  - Stub Resolver to Caching Resolver
  - Zone Transfer
  - Dynamic Updates

DoT Usage Profiles (for DTLS/TLS)

- Strict Privacy profile (RFC 8310)
  - Requires an encrypted connection and successful authentication of the DNS server
  - Mitigates both passive eavesdropping and client redirection
  - But no DNS service if an encrypted, authenticated connection is not available
- Opportunistic Privacy profile (RFC 8310, 7858)
  - Attempts, but does not require, encryption and successful authentication
  - Limited or no mitigation for above attacks but maximizes the chance of DNS service
  - Initial queries (for IP address of the DoT server) use this profile

DoT: Trust the server key problem

- Trust the certificate chain from the CAs or not
- What if your certificate store is poisoned with a Man-in-the-Middle certificate?
  - So that firewalls/IDS/IPS can break up TLS traffic
  - But will you still have web access without that certificate?
- Names in the certificate (chain) require opportunistic lookup
  - Unless Auth name is learned out of band

DoT Client Support

- Linux
  - Not covered by glibc (and will likely never be)
    - `nss-tls` supports only DoH, plugs-in through Name Service Switch (NSS)
  - Locally run resolver daemons:
    - `systemd-resolved`, NLnet Labs `stubby` daemon (getdns), Knot Resolver, …
- Windows
  - Not covered directly (support announced, but DoH will come first)
  - NLnet Labs `stubby` daemon
- iOS 14
  - No user configuration of servers without 3rd party tools
- Android 9 (Pie) – off by default
  - Apps mostly add somewhat more comfortable UI to change the server

DoT Server Support

- Nameservers
  - PowerDNS Dnsdist (1.3.0)
  - Unbound (01/2018)
  - Knot Server
  - Etc.
- Nameservers without support (yet)
  - Windows DNS server
  - BIND
    - Stunnel as workaround
    - Proposals for BIND 9.17, but no code as of now

GÉANT
Networks • Services • People

DNS over HTTPS

www.geant.org

© GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).
The research leading to these results has received funding from
the European Union's Horizon 2020 research and innovation
programme under Grant Agreement No. 731122 (GN4-2).

DNS over HTTPS

- Use Cases (as per RFC)
  - Preventing on-path devices from interfering with DNS operations
  - Allowing web applications to access DNS information via existing browser APIs in a safe way consistent with Cross Origin Resource Sharing (CORS)
- More limited than DoT, only the path between (stub) Resolver and RDNS/Cache

DoH Technical

- DNS operations accessed via URL template
- Examples:
  - `https://doh.opendns.com/dns-query?dns=` (GET)
  - `https://dns.google.com/dns-query` (POST)
  - `https://dns.google.com/resolve?` (JSON)
- Configuration, discovery, and updating of the template not part of the protocol
- Only redirect code 301 (moved permanently) currently supported
- HTTP/2 allowed
  - Recommended for performance: reordering, parallelism, priority, header compression
  - Server Push may be used to send answers in advance to client

DoH Query Methods

- GET
  - **`dns-query?dns=BASE64URL_OF_QUERY`**
  - **`Base64URL`** schema is different from plain Base64 (see RFC 4648, sec. 4)
- POST
  - Query will be transmitted as Base64 encoded DNS message
  - Content Type: **`application/dns-message`**
  - Should be used with care, as return data may not be cached
- JSON
  - All queries use GET method
  - DNS query parameters: **`name, type, cd, do, edns_client_subnet, random_padding`**
  - `Response can be JSON (`**`application/x-javascript`**`) or binary (`**`application/dns-message`**`) determined by ct parameter`

DoH & Proxies

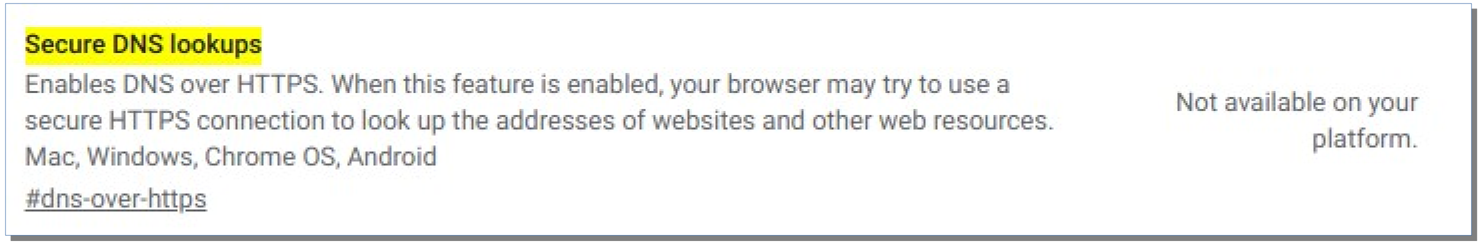
- HTTP proxies & caches are allowed and supported by DoH
  - Of course, MitM SSL proxies can see all queries
- Oblivious DoH (proposal from Cloudflare)
  - HTTPs between Client – Proxy and Proxy – DoH server
  - Additional query encryption between client and DoH server
- But it does very little with regards to privacy
  - DoH server will know **question & answer**, source IP address is incidental
- Lots of ways to leak client addresses due to implementation errors
  - EDNS subnet options (client)
  - DNS XDF pseudo RR (client)
  - X-Forwarded-For HTTP Header (proxy)
- How to be sure that proxy and server do not collude?

DoH Problems

- Correlation through
  - Long lived TCP connections
  - TLS session resumption
  - HTTP headers (Auth, User-Agent, Accept-Language)
- Traffic analysis about queries possible if no/false padding or no compression is used
- EDNS client subnet option should not be used in queries
- No OCSP, AIA lookups or deadlocks may happen
- Chicken or the egg problem for name of DoH server

DoH in Browsers: Chrome

- Chrome *“Secure DNS”*, starting with Chrome 83
  - **`chrome://flags#dns-over-https`**
  - Seems to be unavailable on Linux



Secure DNS lookups

Enables DNS over HTTPS. When this feature is enabled, your browser may try to use a secure HTTPS connection to look up the addresses of websites and other web resources. Mac, Windows, Chrome OS, Android

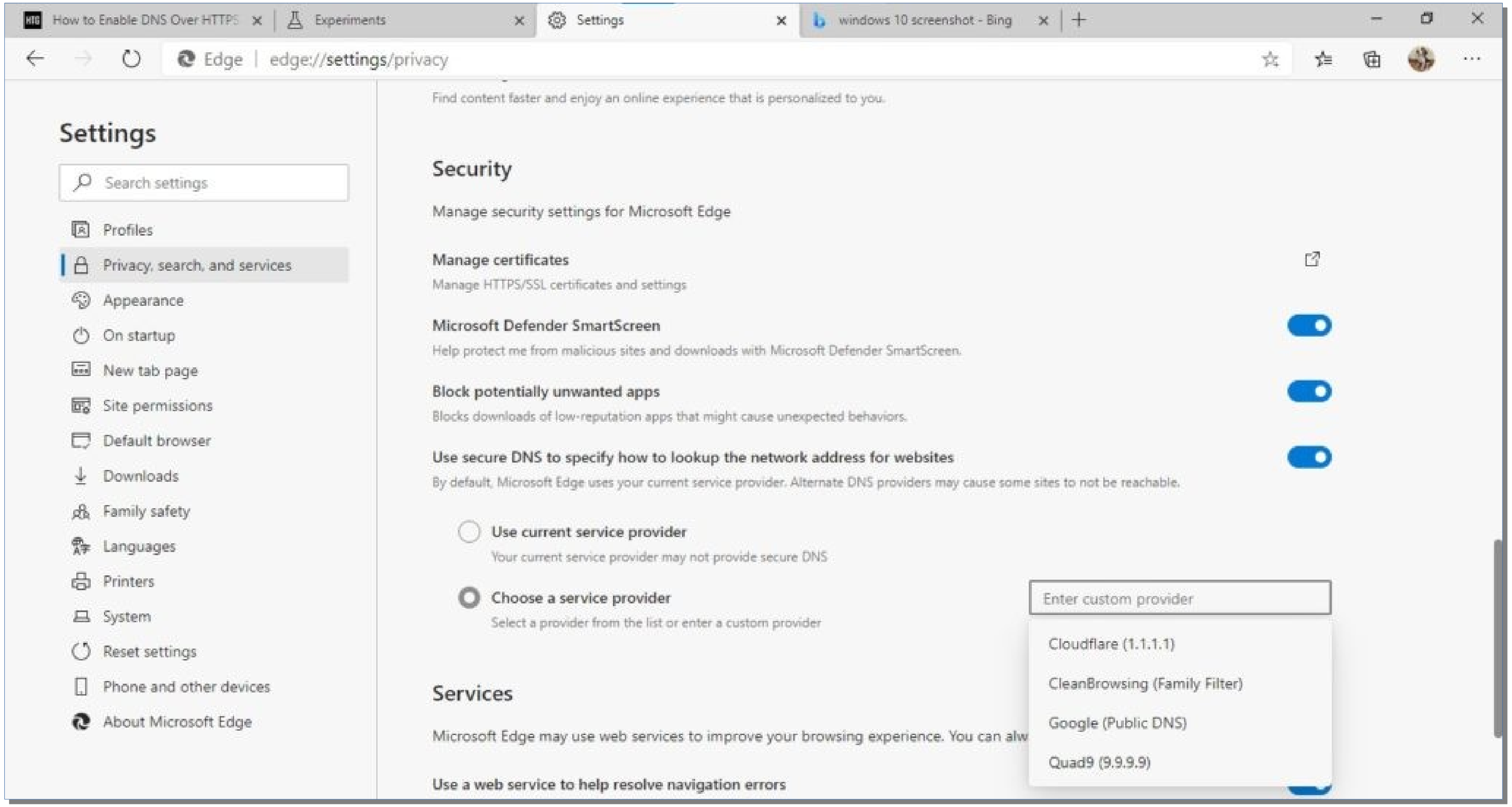
#dns-over-https

Not available on your platform.

- Available on Android and Windows and enabled
  - Default: Use system DNS server, try to use it with DoH
  - Silent fallback to normal DNS lookups in case of problems
- Policies available for managed environments
  - **`DnsOverHttpsMode, DnsOverHttpsTemplates`**

DoH in Browsers: Chrome-based

- Similar procedure for Edge, Brave, Opera, etc.
  - Substitute **`chrome://`** with **`edge://`**, `brave://`, etc.



Find content faster and enjoy an online experience that is personalized to you.

Security

Manage security settings for Microsoft Edge

Manage certificates
Manage HTTPS/SSL certificates and settings

Microsoft Defender SmartScreen
Help protect me from malicious sites and downloads with Microsoft Defender SmartScreen.

Block potentially unwanted apps
Blocks downloads of low-reputation apps that might cause unexpected behaviors.

Use secure DNS to specify how to lookup the network address for websites
By default, Microsoft Edge uses your current service provider. Alternate DNS providers may cause some sites to not be reachable.

○ Use current service provider
Your current service provider may not provide secure DNS

● Choose a service provider
Select a provider from the list or enter a custom provider

Enter custom provider
- Cloudflare (1.1.1.1)
- CleanBrowsing (Family Filter)
- Google (Public DNS)
- Quad9 (9.9.9.9)

Services

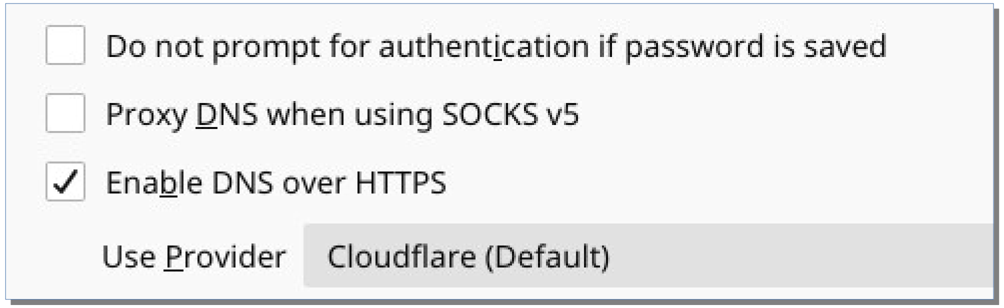
Microsoft Edge may use web services to improve your browsing experience. You can alw

Use a web service to help resolve navigation errors

DoH in Browsers: Firefox

- *"Trusted Recursive Resolver (TRR)"*
  - **Opt-out, not opt-in!**

```
4. The user will be informed that we have enabled use of a TRR and
have the opportunity to turn it off at that time, but will not be
required to opt-in to get DoH with a TRR.
```

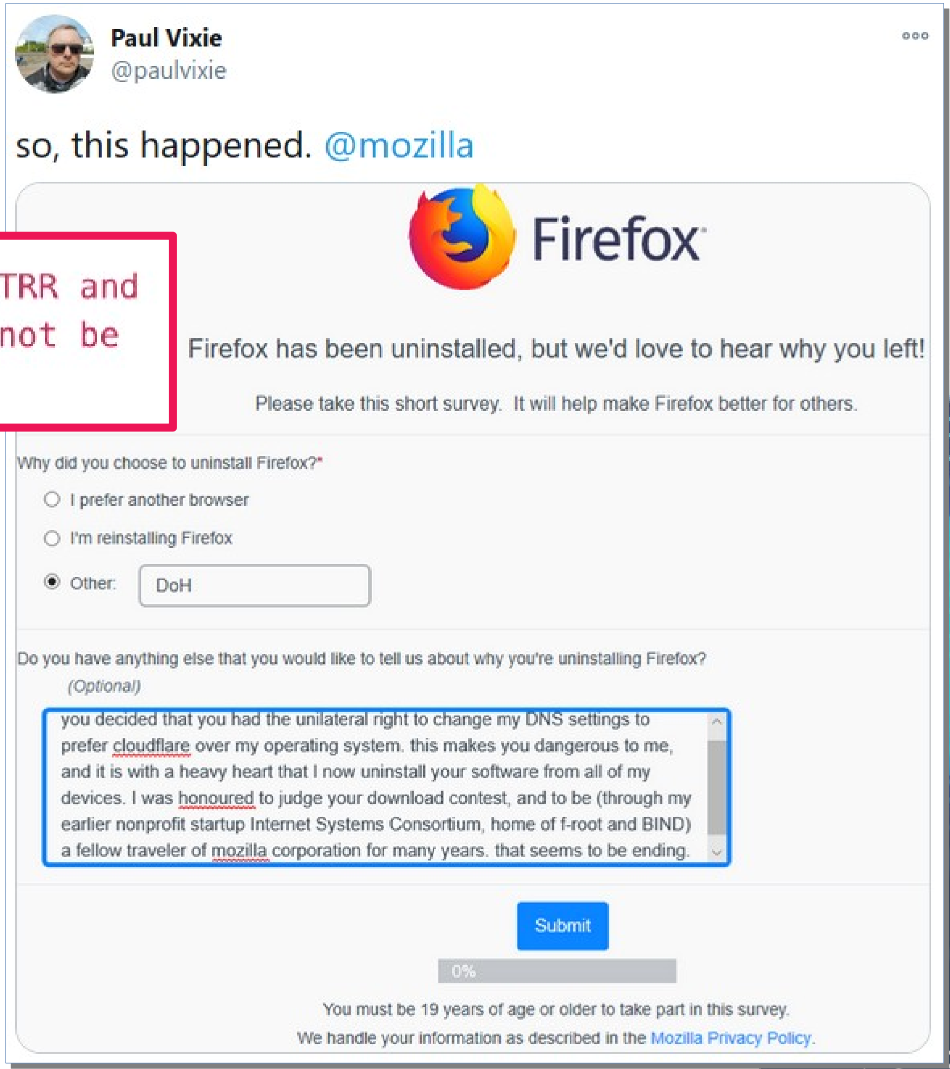


□ Do not prompt for authentication if password is saved

□ Proxy DNS when using SOCKS v5

☑ Enable DNS over HTTPS

Use Provider: Cloudflare (Default)



Paul Vixie
@paulvixie

so, this happened. @mozilla

Firefox has been uninstalled, but we'd love to hear why you left!

Please take this short survey. It will help make Firefox better for others.

Why did you choose to uninstall Firefox?*

○ I prefer another browser

○ I'm reinstalling Firefox

● Other: DoH

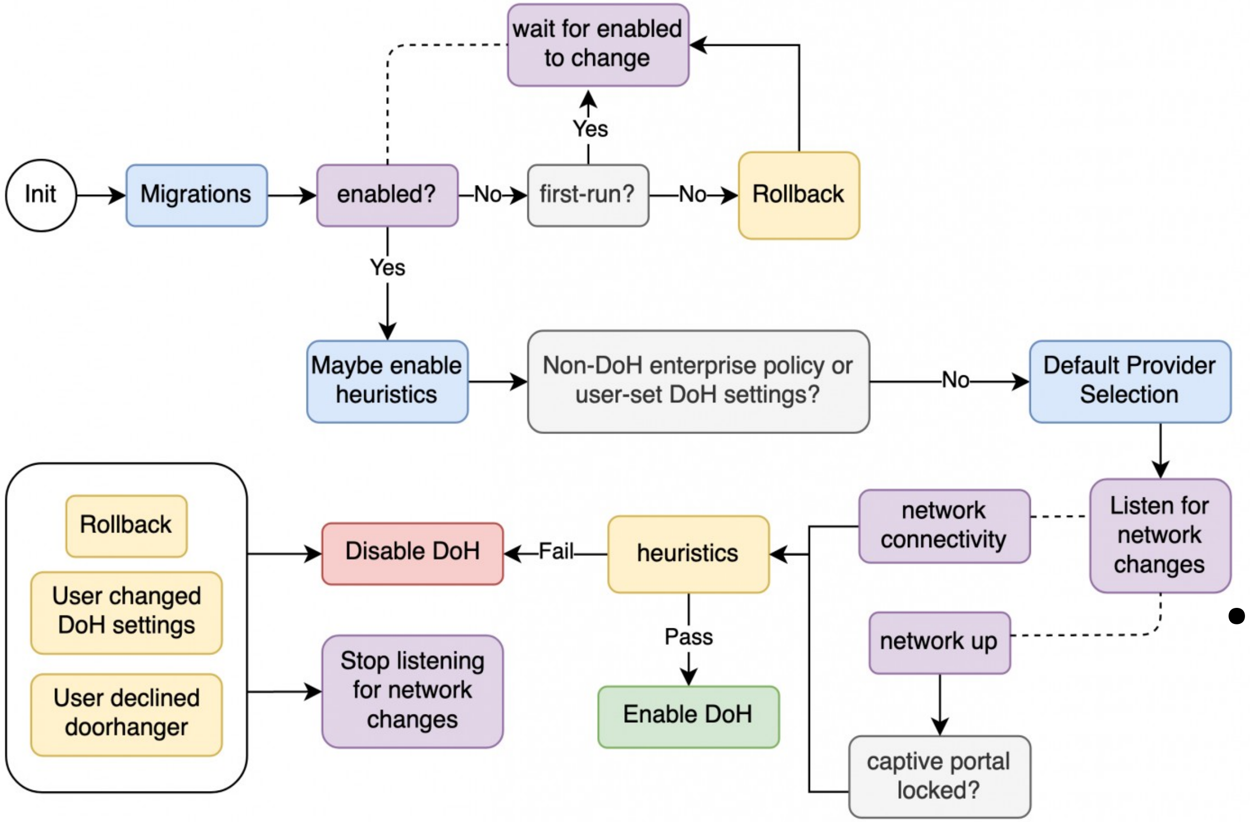
Do you have anything else that you would like to tell us about why you're uninstalling Firefox? (Optional)

you decided that you had the unilateral right to change my DNS settings to prefer cloudflare over my operating system. this makes you dangerous to me, and it is with a heavy heart that I now uninstall your software from all of my devices. I was honoured to judge your download contest, and to be (through my earlier nonprofit startup Internet Systems Consortium, home of f-root and BIND) a fellow traveler of mozilla corporation for many years. that seems to be ending.

You must be 19 years of age or older to take part in this survey.

We handle your information as described in the Mozilla Privacy Policy.

Firefox TRR settings



- Complex heuristic
  - Look for `use-application-dns.net.` domain
  - Look for enterprise or user settings
  - `security.enterprise_roots.enabled` allows installing private root certificates
    - For breaking up of HTTPS by content filtering proxies,
    - I.e. your lookups aren't secret anymore then
- Fine grained control
  - `about:config`
  - `network.trr.*`

Other DoH Implementations

- Supported Client OS
  - Android 9 (Pie)
  - Apple iOS 14
  - Apple macOSX 11
- Not yet supported Client OS
  - Linux glibc (and will likely never be), see DoT
  - Windows: announced
    - Insider Preview Build 19628
    - Configuration GUI with Insider Preview Build 20185
- Nameserver
  - Unbound, Knot DNS, CoreDNS, Technetium DnsServer, …

DNS over QUIC

Resolverless DNS

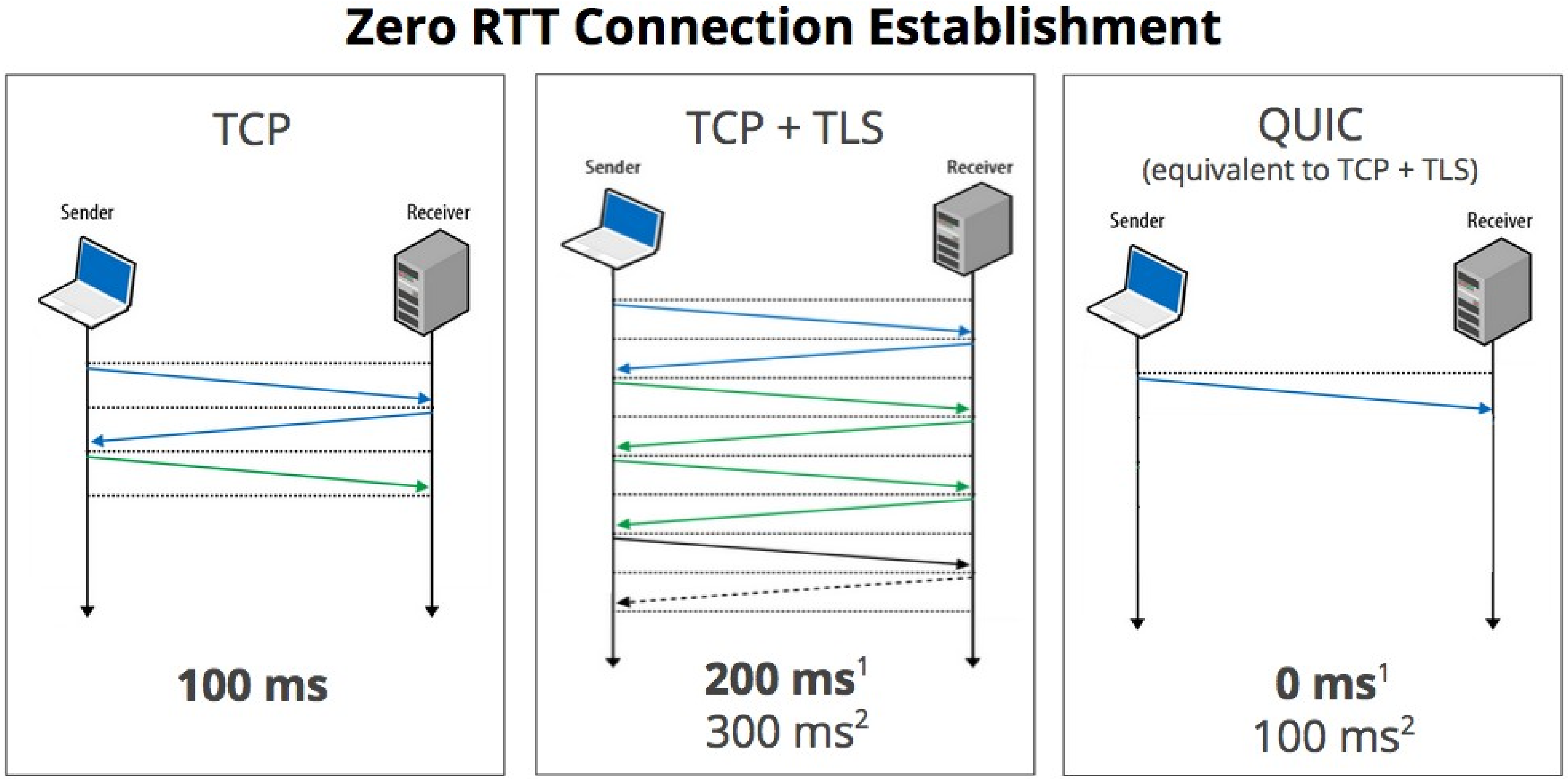
www.geant.org

© GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).
The research leading to these results has received funding from
the European Union's Horizon 2020 research and innovation
programme under Grant Agreement No. 731122 (GN4-2).

QUIC – Quick UDP Internet Connections

- Many transactions have a simple Request – Response pattern
  - But setting up a TCP connection with TLS on top requires several round trips before data can be sent
- Need for a protocol that has fewer round-trips: QUIC
  - Combine TLS and TCP handshake in one setup
  - And take the flow control from TCP up to the application
  - Will use UDP, port numbers may be different from existing applications
- Meant as a replacement/supplement for TCP + TLS or UDP + DTLS
  - Invented by Google, now an IETF standard
  - Standardization not finished, incompatible implementations as yet
  - HTTP/3 will be defined on top of QUIC

QUIC – Round trip savings



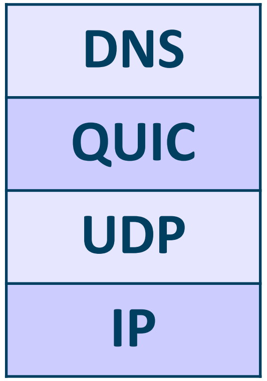
1. Repeat connection
2. Never talked to server before

Source: https://blog.chromium.org/2015/04/a-quic-update-on-googles-experimental.html

DNS over QUIC

- Same principle as with DoT or DoH
  - Internet draft as of now
  - Port number not yet decided, maybe 784/udp?

	UDP	TCP	TLS	DTLS	QUIC
Transport efficiency					
Connection set up time	✓	✗	✗	✗	0-RTT
Head of queue blocking	✓	✗	✗	✓	✓
Retransmission efficiency	✗	✓	✓	✗	✓
Long messages (DNSSEC)	✗	✓	✓	✗	✓
Security					
Three ways handshake	✗	✓	✓	✓	✓
Encryption & Authentication	✗	✗	✓	✓	✓


DNS
QUIC
UDP
IP

Resolverless DNS?

- Idea: DNS Responses are pushed from web servers to the clients
  - Through the HTTP connection
  - No DNSSEC, TLS considered safe enough
- No resolver needed, henceforth “resolverless DNS”
- Motivation/Use Case:
  - Web content includes lots of references to other objects (Pictures, Videos, Ads, etc.)
  - DNS lookups for their sites takes round-trips and thus time
  - And allows Ad-blocking
- Bad idea, because
  - Ties DNS to Web content providers, esp. the very big ones, even more
  - Web site defacement will now mean DNS cache poisoning too
  - Circumvents BHDNS protections and Ad blocking

Considerations

& Recommendations

www.geant.org

© GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).
The research leading to these results has received funding from
the European Union's Horizon 2020 research and innovation
programme under Grant Agreement No. 731122 (GN4-2).

Technical considerations

- Problems with using external RDNS
  - Answers will have the external view of the network not the internal
  - All other programs, even those started by browsers, still use the system resolver
  - Thus, results returned may/will differ → hard to debug problems
  - Additional work for opting out: configuration, canary domains, …
- External RDNS cannot know why (local) DNS manipulation is done
  - Parents
  - Sysadmins
  - Security teams (PDNS monitoring)
  - Governments
  - ISPs

Privacy considerations

- None of them (DoT, DoH) really protects privacy
  - Still can see the metadata of your connections (even with HTTPS)
    - Eavesdropper can infer from metadata what’s been queried in DNS
  - Queries coming from the recursive resolver are not encrypted
- Won’t help against evil governments
  - Need a VPN (and more) for that
  - If you have a VPN (a trustworthy one), what value do “DNS over …” add?
  - They have the resources to block DoH (they already block a lot more)

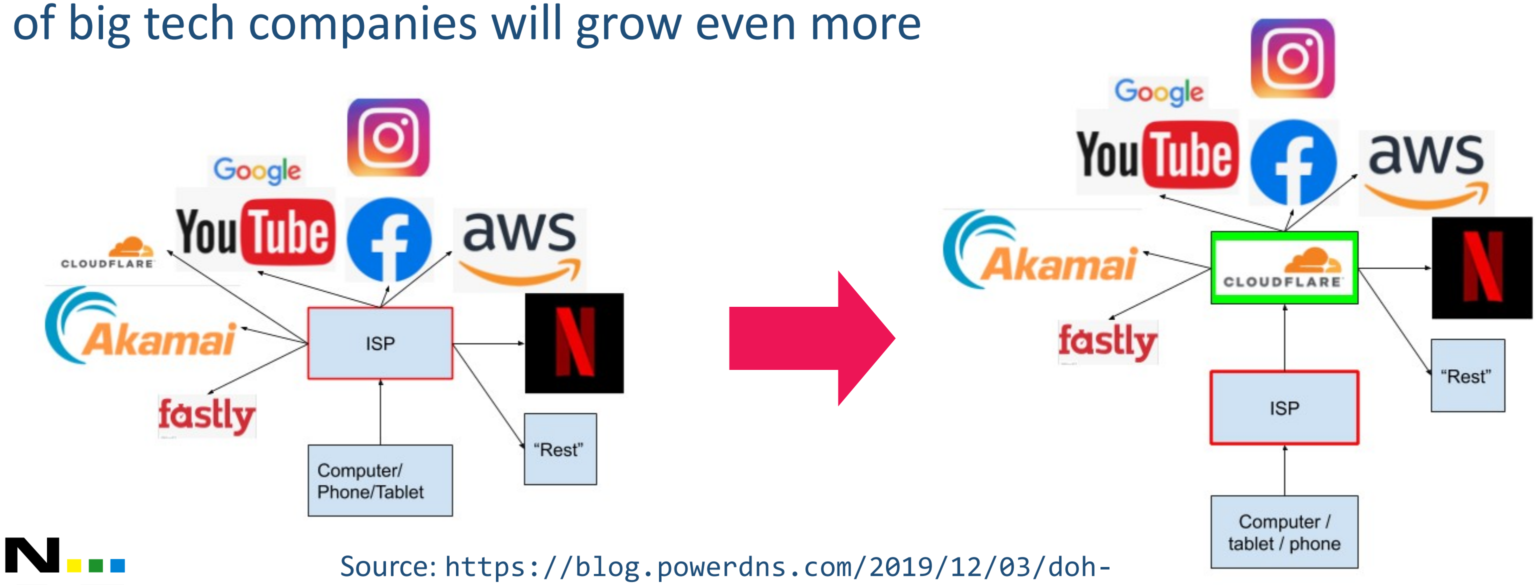
Privacy considerations (cont.)

- Why trusting your local DNS servers is better
  - Big tech companies track record w/ regards to privacy
  - Big (central) data pools will raise desires from governments
    - Tech C. usually budge after some phony resistance
  - Much more leverage against your admins/employers
    - Same jurisdiction
    - Better legal situation (employee rights, GDPR, etc.)
    - At least in Western Europe
- Different situation as ISPs
  - Neutrality obligations?
  - Business opportunities

Political considerations

- DoH & resolverless DNS are political solutions
  - Add nothing security-wise (compared to DoT/DoQ)
  - Add nothing privacy-wise (compared to DoT/DoQ)
  - But breaks Split DNS, RPZ, PDNS, …
  - No added value (for end-users, network admins)
  - Web servers will force their view of the network upon end-users
  - Power of big tech companies will grow even more

- Network landscape
  - Endpoints are insecure and will be so in the future
  - Need to allow/block some kinds of traffic – through Firewalls, DNS, web-proxies



Source: https://blog.powerdns.com/2019/12/03/doh-anti-competitive-and-network-neutrality-aspects/

Recommendations

- For managed networks
  - Block outbound DNS (ports 53, 853, UDP & TCP)
  - Block outbound DoQ (whatever port it will be)
  - Block IP addresses of known DoH providers
  - 1.1.1.1, 4.4.4.4, 8.8.8.8, 9.9.9.9, …, list is short enough (i.e. Cisco Umbrella)
    - Might discourage unreasonable users/vendors
  - Or force all HTTPS traffic through MitM proxy **:((**
- Use DoT/DoQ (even DoH) with internal RDNS
  - Can still use PDNS, RPZ, Split DNS
- May use DoH servers at home/on your device
  - If so, check for servers DNSSEC support, logging & filtering

What have you learned?

The Good

- DoT
- DoQ

The Bad

- DoH
- Resolverless DNS

- Things that have been left out
  - DNSCurve
  - DNSCrypt
  - DNS Protocol Details (EDNS)
  - Response Rate Limiting (RRL) → part of upcoming DDoS course

GÉANT
Networks • Services • People

Thank you

Any questions?

Next course: ***Distributed Denial of Service Protection***

8th of February 2021

www.geant.org

© GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).
The research leading to these results has received funding from
the European Union's Horizon 2020 research and innovation
programme under Grant Agreement No. 731122 (GN4-2).

References:

- PowerDNS blog: “DoH: (Anti-)Competitive and Network Neutrality aspects” https://blog.powerdns.com/2019/12/03/doh-anti-competitive-and-network-neutrality-aspects/
- National Cyber Security Center: “Factsheet DNS Monitoring will get harder”: https://english.ncsc.nl/publications/factsheets/2019/oktober/2/factsheet-dns-monitoring-will-get-harder
- Zdnet: “DNS-over-HTTPS causes more problems than it solves, experts say”, https://www.zdnet.com/article/dns-over-https-causes-more-problems-than-it-solves-experts-say/
- Elbsides 2019 session featuring vixie (pro DoT), Michaelis (pro DoH) and a panel discussion afterwards: https://www.youtube.com/channel/UC1kRI13BZ6KMCwtGttD5Arg/videos
- Running a DNS Privacy server: https://dnsprivacy.org/wiki/display/DP/Running+a+DNS+Privacy+server
- Cloudflares Secure Browse Check: https://www.cloudflare.com/ssl/encrypted-sni/
- Wei & Heidemann, Whac-A-Mole: Six Years of DNS Spoofing, https://arxiv.org/pdf/2011.12978.pdf
- Jordi Palet: A New Internet, https://www2.slideshare.net/apnic/a-new-internet-intro-to-http2-quic-doh-and-dns-over-quic

Tools & Browsers

- JSON API for DNS over HTTPS (DoH) https://developers.google.com/speed/public-dns/docs/doh/json
- DoH in Firefox:
  - https://wiki.mozilla.org/Security/DNS_Over_HTTPS
  - https://wiki.mozilla.org/Security/DNS_Over_HTTPS/Heuristics
  - https://wiki.mozilla.org/Trusted_Recursive_Resolver
- DoH in Chrom* (Edge, Opera, etc.)
  - https://www.tenforums.com/tutorials/145372-how-enable-disable-dns-over-https-doh-google-chrome.html
- Public DNS Server List
  - https://github.com/curl/curl/wiki/DNS-over-HTTPS#publicly-available-servers
  - https://dnscrypt.info/public-servers/
  - https://beebom.com/best-dns-servers/
  - https://www.lifewire.com/free-and-public-dns-servers-2626062
  - https://www.allconnect.com/blog/best-free-dns-servers
- Linux
  - NSS-TLS: https://github.com/dimkr/nss-tls
- List of DoT and DoH implementations:
  - https://doh.defaultroutes.de/implementations.html

RFCs

- RFC 4648, Josefsson: The Base16, Base32, and Base64 Data Encodings, `https://tools.ietf.org/html/rfc4648`
- RFC 7858, Hu et al.: Specification for DNS over Transport Layer Security (TLS), `https://tools.ietf.org/html/rfc7858`
- RFC 8094, Reddy et al.: DNS over Datagram Transport Layer Security (DTLS), `https://tools.ietf.org/html/rfc8094`
- RFC 8310, Dickinson et al.: Usage Profiles for DNS over TLS and DNS over DTLS, `https://tools.ietf.org/html/rfc8310`
- RFC 8484, Hofman & McManus: DNS Queries over HTTPS (DoH), `https://tools.ietf.org/html/rfc8484`
- IRTF Draft, Huitema et al.: Specification of DNS over Dedicated QUIC Connections, `https://datatracker.ietf.org/doc/draft-ietf-dprive-dnsoquic/`
- IRTF Draft, Kinnear et al.: Oblivious DNS Over HTTPS, `https://tools.ietf.org/html/draft-pauly-dprive-oblivious-doh-03`