Early observations from BT DoH Trials

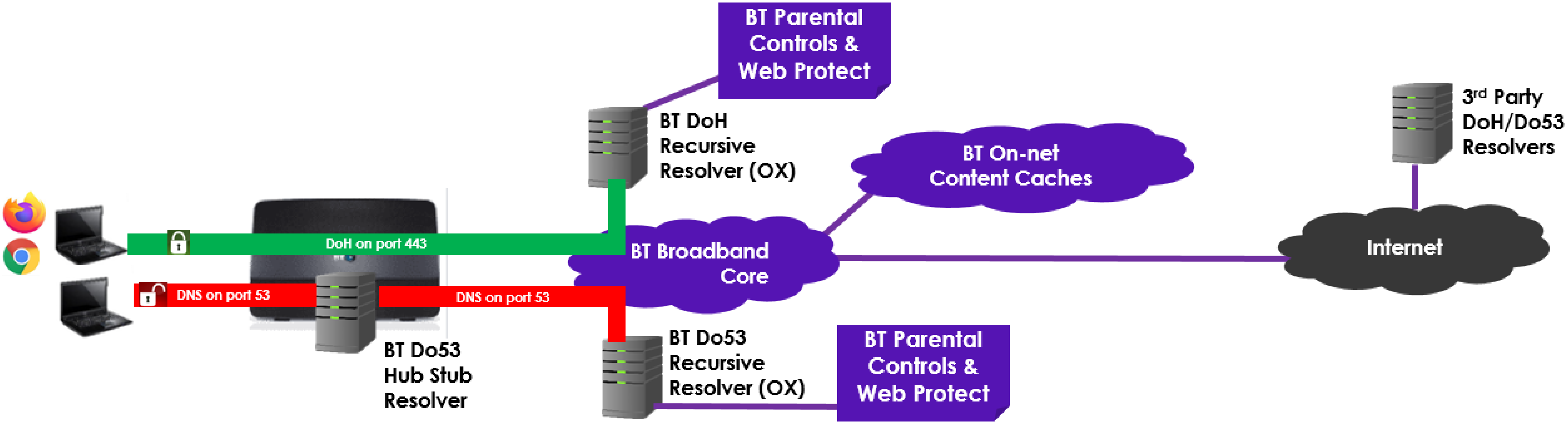
EDDI – 30th January 2020, London.

Andy Fidler, Principal Network Architect, BT
andrew.fidler@bt.com

NOTE: ALL OBSERVATIONS ARE EARLY FINDINGS AND SUBJECT TO CHANGE

BT DoH Experimental Trial

- Shared with industry technical community on 6th December, 2019.
- Available* at https://doh.bt.com/dns-query/ with test page at http://splashpage.doh.bt.com
- Currently testing across small base of BT employees.
- Built on and working with OpenXchange / PowerDNS.
- Supporting only IPv4 and RFC8484 implementation.
- For the trial providing a public / open resolver.
- Shortly planning to enable DNSSEC validation.


BT Parental Controls & Web Protect
BT DoH Recursive Resolver (OX)
3rd Party DoH/Do53 Resolvers
BT On-net Content Caches
DoH on port 443
BT Broadband Core
Internet
DNS on port 53
DNS on port 53
BT Do53 Hub Stub Resolver
BT Do53 Recursive Resolver (OX)
BT Parental Controls & Web Protect

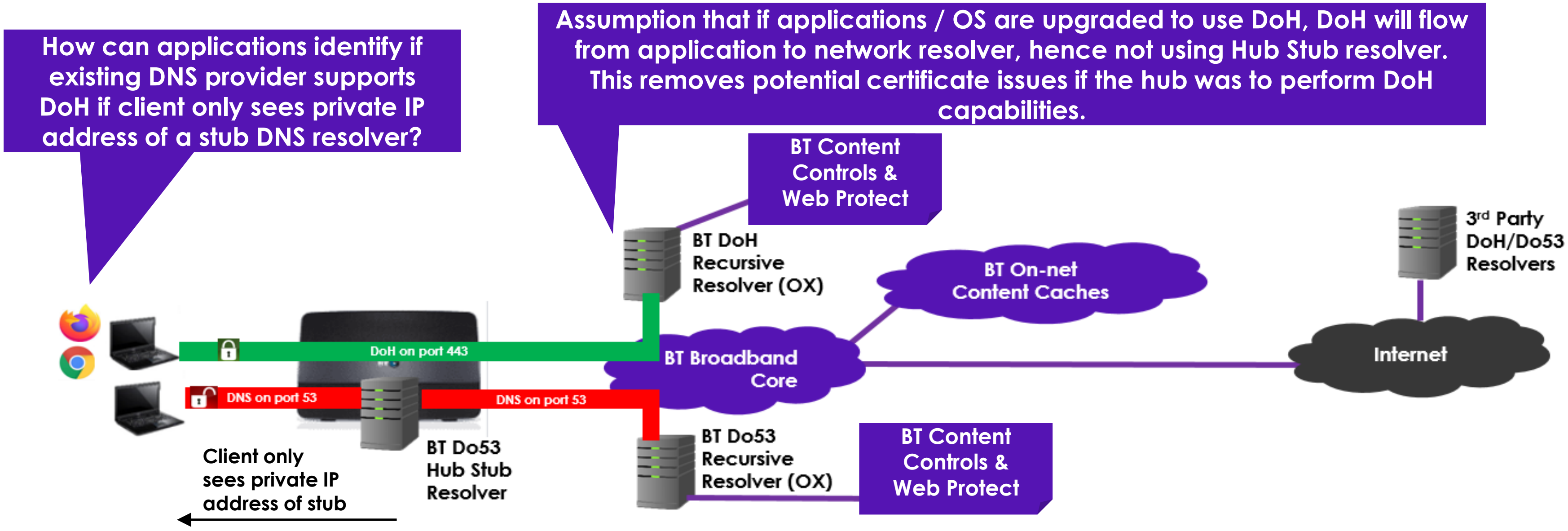
***Please note this is not an official service in any way.** It is purely experimental, may not offer similar service performance to live services and may be taken out of service without notice. The experimental capability should support any existing BT customer parental control and/or web protect settings, however if you are testing the capability on family devices we would recommend that you check that parental controls are still applied. Personal data will be processed in accordance with BT's Privacy Policy - https://www.bt.com/privacy-policy/

Early Customer Experience observations from BT Trial

Customer Experience	Status	Observations	Industry Opportunity
Browser Manual Custom Entry Set-up	🟨	Firefox: Simple manual custom entry. Chrome: Via executable flags now, but should be addressed via options in 81.	Consideration on: 1) applying policy detection to custom entry as well as auto enablement. 2) providing visual notification to customer on DoH usage.
Future auto discovery	🟥	For customers using BT Hubs with stub resolvers presenting private IP addresses to clients, inability for applications to discover BT as ISP and DoH status.	Demonstrates clear need for a context aware DoH discovery protocol to be developed within proposed new IETF Adaptive DNS Discovery (ADD) group.
Browsing Experience	🟨	For general users a good browsing experience, however early technical measurements appear to be showing additional latency from TLS set-up and variations based on encryption settings approach.	Demonstrates benefits to be gained from creating Best Current Practices (BCP) recommendations on DoH encryption options. BCPs could be within IETF, EDDI, ISPA or GSMA.
DNS Parental Control	🟩	Verified successful co-existence of BT Parental Controls with DNS over HTTPS.	Industry standardisation of policy detection protocol and use with custom entry as well as auto enablement.
DNS Malware Protection	🟩	Verified successful co-existence of BT Web Protect with DNS over HTTPS.	Industry standardisation of policy detection protocol and use with custom entry as well as auto enablement.
Context Awareness	🟥	If custom DoH entry is unavailable (e.g. off network), then browsers may still try this first then fall-back to default Do53 settings, potentially creating a slower response.	Demonstrates need for IETF ADD group to develop a context aware DoH discovery protocol supporting broadband, mobile and 3rd party wi-fi options.
Hub / Device Set-up	🟥	Breaks simple BT hub set up GUI URL – "hub.home" link.	Future ISP hubs will need to avoid using private domains.

DoH Discovery

Problem Space	Initial Industry Response	Mitigation Options
DoH “same provider automatic upgrade” only works for a subset of users as it requires sight of the existing DNS server public IP address to identify the provider. Many UK and European ISPs use stub resolvers in home hubs and only make available a private DNS server IP address to clients, thus rendering this method of discovery not possible. A more all-encompassing discovery approach needs to be identified.	Recognise the issue, but are looking to a standard discovery approach for future options and are questioning whether hub configurations could be altered. Changing hub configurations is not a trivial matter for many network operators given support for multiple legacy hubs and also use of 3rd party hubs by some customers. Hence operator preference for a more all-encompassing discovering approach.	Potential topic for new IETF ADD working group. Identify a DoH discovery approach which supports all user cases irrespective of public or private IP addressing.



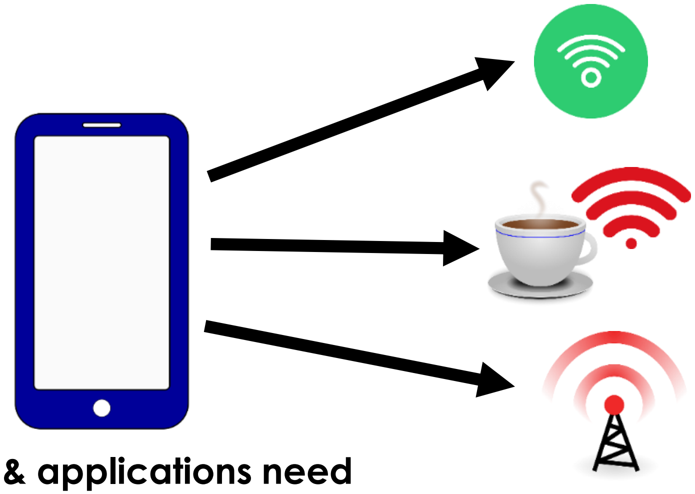
How can applications identify if existing DNS provider supports DoH if client only sees private IP address of a stub DNS resolver?

Assumption that if applications / OS are upgraded to use DoH, DoH will flow from application to network resolver, hence not using Hub Stub resolver. This removes potential certificate issues if the hub was to perform DoH capabilities.

BT Content Controls & Web Protect
BT DoH Recursive Resolver (OX)
BT On-net Content Caches
3rd Party DoH/Do53 Resolvers
Internet
DoH on port 443
BT Broadband Core
DNS on port 53
DNS on port 53
BT Do53 Hub Stub Resolver
BT Do53 Recursive Resolver (OX)
BT Content Controls & Web Protect
Client only sees private IP address of stub

DoH Discovery - Context Awareness

Problem Space / Question	Initial Industry Response	Mitigation Options
Question - going forward does DoH discovery need to be context aware, e.g. support individual resolver options for broadband, mobile and Wi-Fi connectivity especially if some resolvers are closed and only available to specific customers / networks?	Potential topic for new IETF ADD working group.	Potential topic for new IETF ADD working group.



Trusted Home Broadband Wi-fi:
ISP DoH or Cloud DoH

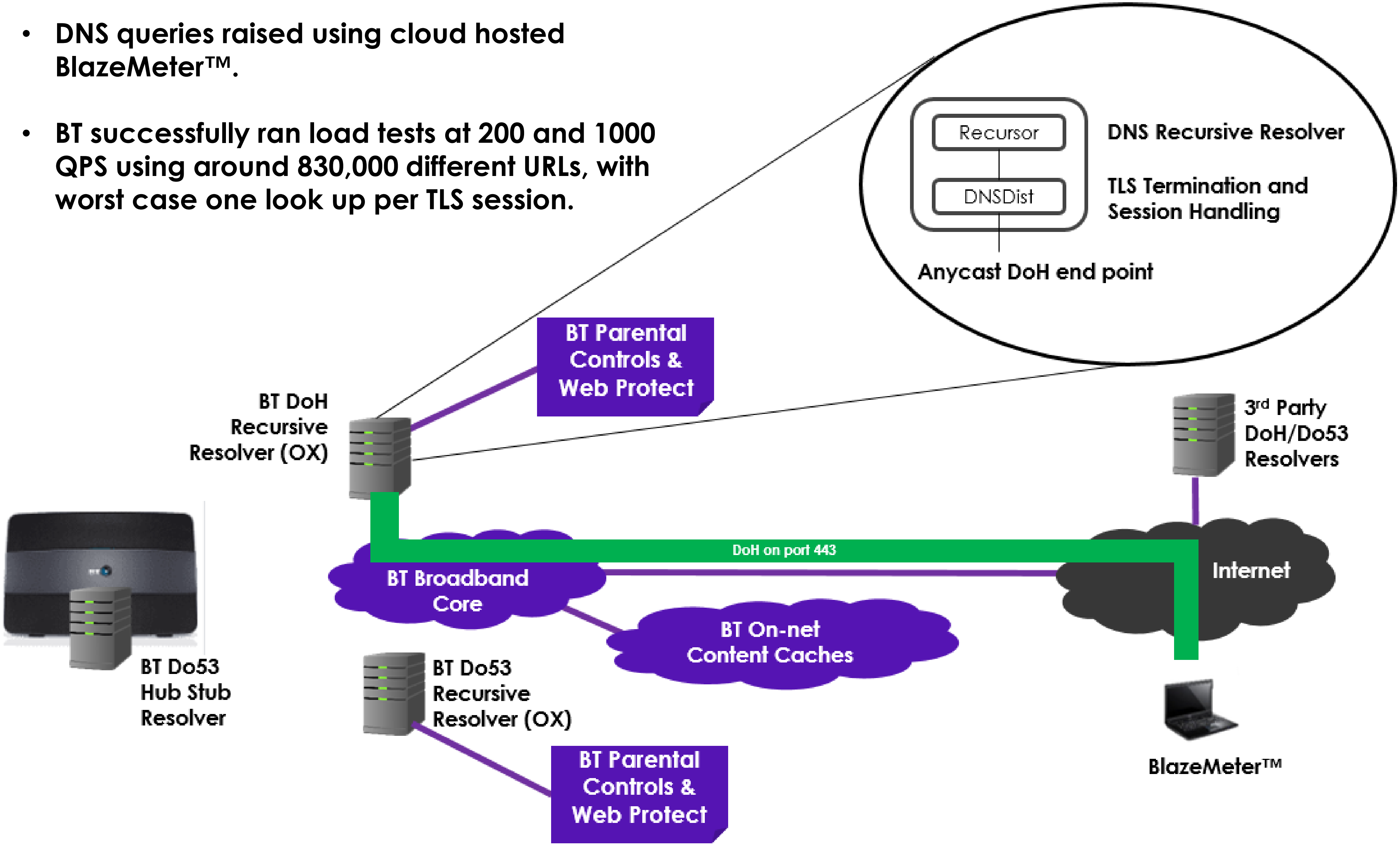
Un-Trusted Coffee Shop Wi-fi:
Cloud DoH

Trusted Mobile Network:
ISP DoH or Cloud DoH

Devices & applications need to be context aware, offering DoH options for various network connection scenarios.

BT DoH Load Test Configuration

- DNS queries raised using cloud hosted BlazeMeter™.
- BT successfully ran load tests at 200 and 1000 QPS using around 830,000 different URLs, with worst case one look up per TLS session.



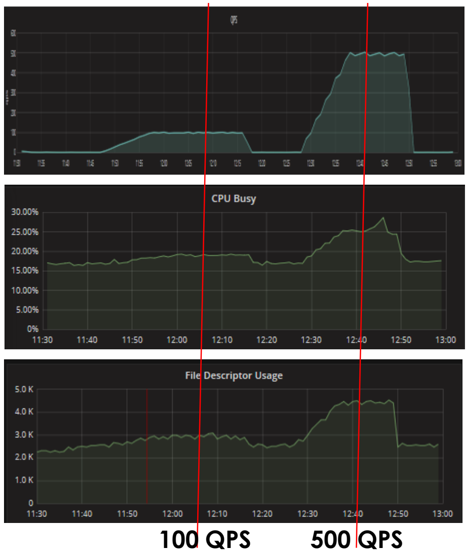
Recursor
DNSDist
DNS Recursive Resolver
TLS Termination and Session Handling
Anycast DoH end point
BT Parental Controls & Web Protect
BT DoH Recursive Resolver (OX)
3rd Party DoH/Do53 Resolvers
DoH on port 443
BT Broadband Core
Internet
BT On-net Content Caches
BT Do53 Hub Stub Resolver
BT Do53 Recursive Resolver (OX)
BT Parental Controls & Web Protect
BlazeMeter™

Early Performance Observations from BT DoH Trial

Full look up time in seconds from UK BT Broadband line	Cloudflare DoH	Google DoH	BT (UK) DoH	DT (Germany) DoH	Comcast (US) DoH
	TLS 1.3			TLS 1.2	
Facebook.com	0.260	0.267	0.262	0.414	0.610
a2.w10.akamai.net	0.263	0.271	0.277	0.317	0.835
google.co.uk	0.239	0.245	0.272	0.326	0.608
BT is observing that TLS 1.2 adds an overhead compared TLS 1.3					

Full look up time (s)	BT	Cloudflare	Google
DoH curl	0.34 (TLS 1.2)	0.26 (TLS 1.3)	0.20 (TLS 1.3)
Do53 pingu	0.013	0.014	0.02
Do53 curl	0.066	tbc	0.109

Early measurements are suggesting DoH has greater latency due to TLS set-up. However BT is still exploring whether existing test probes are ideal for DoH. To assist this BT will shortly be testing with whiteboxes.
It should also be noted that Curl measurements reflects worse case – TLS session per query scenario.

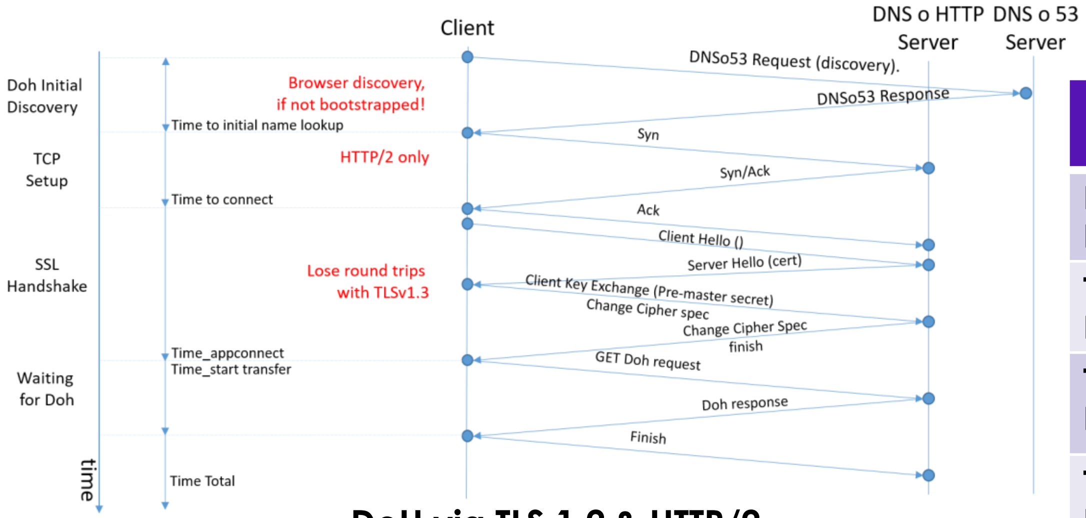


Early results from load tests seem to be indicating a higher than expected TLS overhead on server capacity.

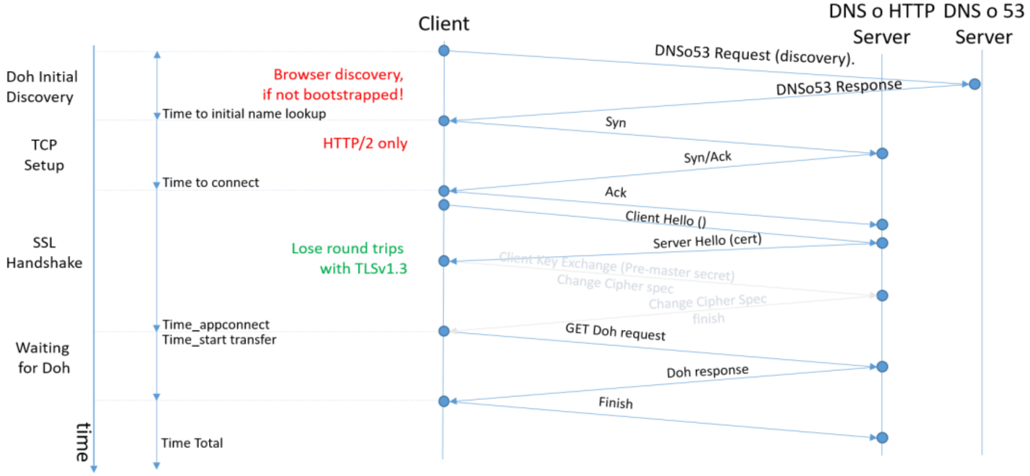
200 & 1k QPS distributed servers.
10% CPU increase
100% file descriptor increase

NB: Background trial usage < 10 QPS

DoH via TLS 1.2 vs TLS 1.3



DoH via TLS 1.2 & HTTP/2



DoH via TLS 1.3 & HTTP/2

DOH Option	Round Trips	Perfect Forward Secrecy
DoH via Curl on HTTP/2 & TLS 1.2	6	Yes
Theoretical DoH on HTTP/2 & TLS 1.3	5	Yes
Theoretical DoH on HTTP/3 & TLS1.3	3.5	Yes
Theoretical DoH on HTTP/3 & TLS 1.3 Plus 0-RTT	2.5	No
Theoretical DoH on HTTP/3 & TLS 1.3 Plus 0-RTT, hardcode & no discovery	1.5	After initial

Moving to TLS 1.3 and HTTP/3 will significantly reduce TLS overheads and should ensure comparable DoH performance with Do53.

Variation in DoH resolver encryption settings

- BT has run Curl tests* against 21 DoH providers, highlighting some interesting variations and need for Best Current Practices deployment guidelines.

DoH Provider	TLS 1.3	OCSP Stapling	Session ID Duration (s)	Ticket Session (s)	Cipher Choice
Cloudflare	Yes	No	7200	172800 (2 days)	TLS_AES_256_GCM_SHA384
NextDNS	Yes	No	7200	604800 (7 days)	TLS_AES_256_GCM_SHA384
PowerDNS	Yes	No	7200	7200	TLS_AES_256_GCM_SHA384
Comcast	No (TLS 1.2)	No	7200	No	ECDHE-RSA-AES256-GCM-SHA384
Deutsche Telekom	No (TLS 1.2)	No	7200	7200	ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384
Andrews & Arnold	Yes	No	7200	7200	TLS_AES_256_GCM_SHA384
Google	Yes	No	7200	172800 (2 days)	TLS_AES_256_GCM_SHA384
BT Plc	No (TLS 1.2)	Yes (7 days)	7200	300	ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384

*Results based on tests run on 27/12/19

Saves client having to check status with CA.

Plus what about in-band authentication?

Clients & servers need to hold session resumption artefacts. Will 7200s take-up too much memory as DoH scales, should it be lower?

Why so varied and some so long?

What's the best balance here between privacy and user experience?

Variation in Cipher Choice.

Variation in DoH Protocol Support & HTTP Response Status Codes

DoH Provider	DoH RFC8484	DoH-JSON (response code)	Support HTTP/1.0 Head Request (Response Code)	Support HTTP/1.1 Head Request (Response Code)	Support HTTP/2 Head Request (Response Code)	HTTP/3 Head Request (Response Code)
Cloudflare	Yes	Yes	No (200)	Yes (200)	Yes (200)	No (200)
NextDNS	Yes	Yes	Yes (405)	Yes (405)	Yes (405)	No
PowerDNS	Yes	No (400)	No (400)	Yes (400)	Yes (400)	No
Comcast	Yes	No (400)	No (400)	Yes (400)	Yes (400)	No
Deutsche Telekom	Yes	No (400)	No (404)	Yes (404)	Yes (404)	No
Andrews & Arnold	Yes	No (400)	?	Yes (302)	Yes (302)	No (302)
Google	Yes	No (400)	Yes (200)	Yes (200)	Yes (200)	Yes
BT Plc	Yes	No (400)	No (400)	Yes (400)	Yes (400)	No

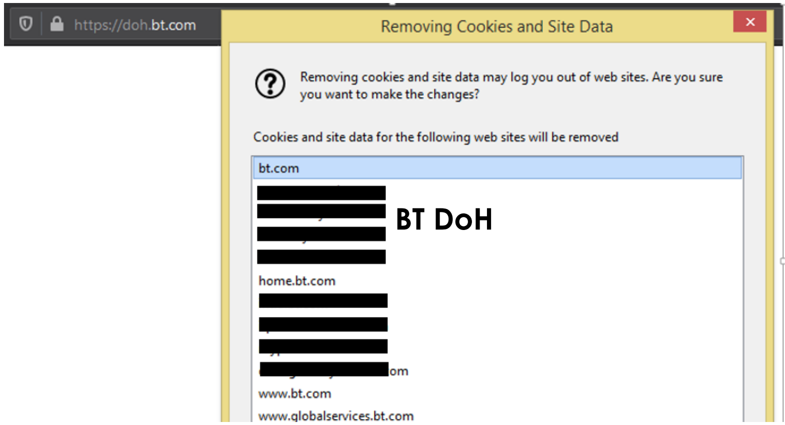
Only Cloudflare & NextDNS supporting non-standard JSON

Noticed different listeners and variation in HTTP response status codes return for head requests, how will clients handle this variation?

Does DoH HTTP status response codes approach need to be covered in BCPs and thoughts on test tools?

DoH Cookie Observations from BT Trial

- User interfaces and policies may not be clear on how cookies are handled across browser and DoH databases. We appear to be seeing the browser side mention cookies for DoH domains.
  - We assume this is due to visiting the domain itself, but would welcome user interface clarity on which cookies are present in which database, and confirmation that browsers and DoH servers are not sending / accepting cookies in DoH messages.

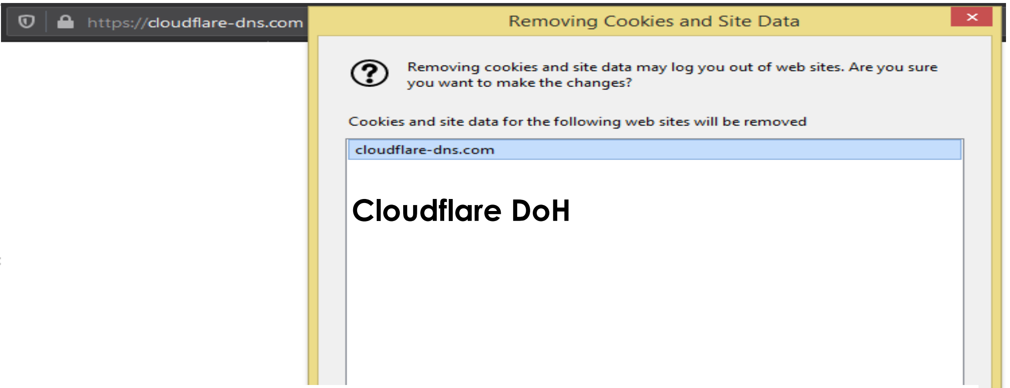


Removing cookies and site data may log you out of web sites. Are you sure you want to make the changes?

Cookies and site data for the following web sites will be removed

bt.com
[redacted]
home.bt.com
[redacted]
www.bt.com
www.globalservices.bt.com

BT DoH

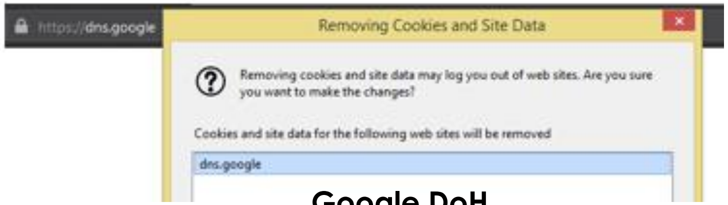


Removing cookies and site data may log you out of web sites. Are you sure you want to make the changes?

Cookies and site data for the following web sites will be removed

cloudflare-dns.com

Cloudflare DoH

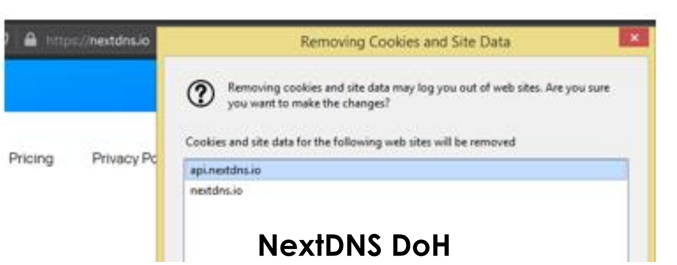


Removing cookies and site data may log you out of web sites. Are you sure you want to make the changes?

Cookies and site data for the following web sites will be removed

dns.google

Google DoH



Removing cookies and site data may log you out of web sites. Are you sure you want to make the changes?

Cookies and site data for the following web sites will be removed

api.nextdns.io
nextdns.io

NextDNS DoH

- Further clarification may needed in DoH BCPs and subsequent I-D's / RFCs to state that:
  - Clients should not accept "Set-Cookie" as part of a DoH response.
  - Clients should not send "Cookie" headers they have previously learned for the relevant domain.
  - DoH servers should disregard Cookies.
  - Guidance on DoH namespace.