THE EVOLUTION OF DNS

DNS OVER HTTPS (DOH) & DNS OVER TLS (DOT)

VERSION 1.1, 09.02.2020
NICOLAI LEYMANN, SENIOR ARCHITECT
N.LEYMANN@TELEKOM.DE

LIFE IS FOR SHARING.

AGENDA

01 DT DNS Architecture and Deployment

02 DNS-over-{HTTPS | TLS | QUIC}

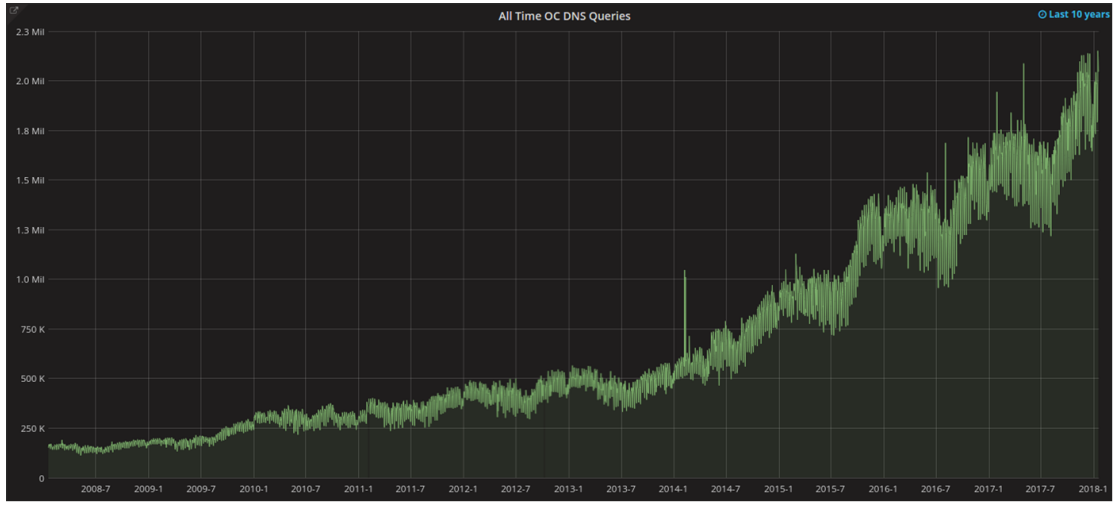
03 Impact on DT Platform

04 Summary and Next Steps

THE EVOLUTION OF DNS
DT DNS PLATFORM

DT runs a huge, high performance DNS infrastructure, fully redundant IPv4/IPv6 enabled.

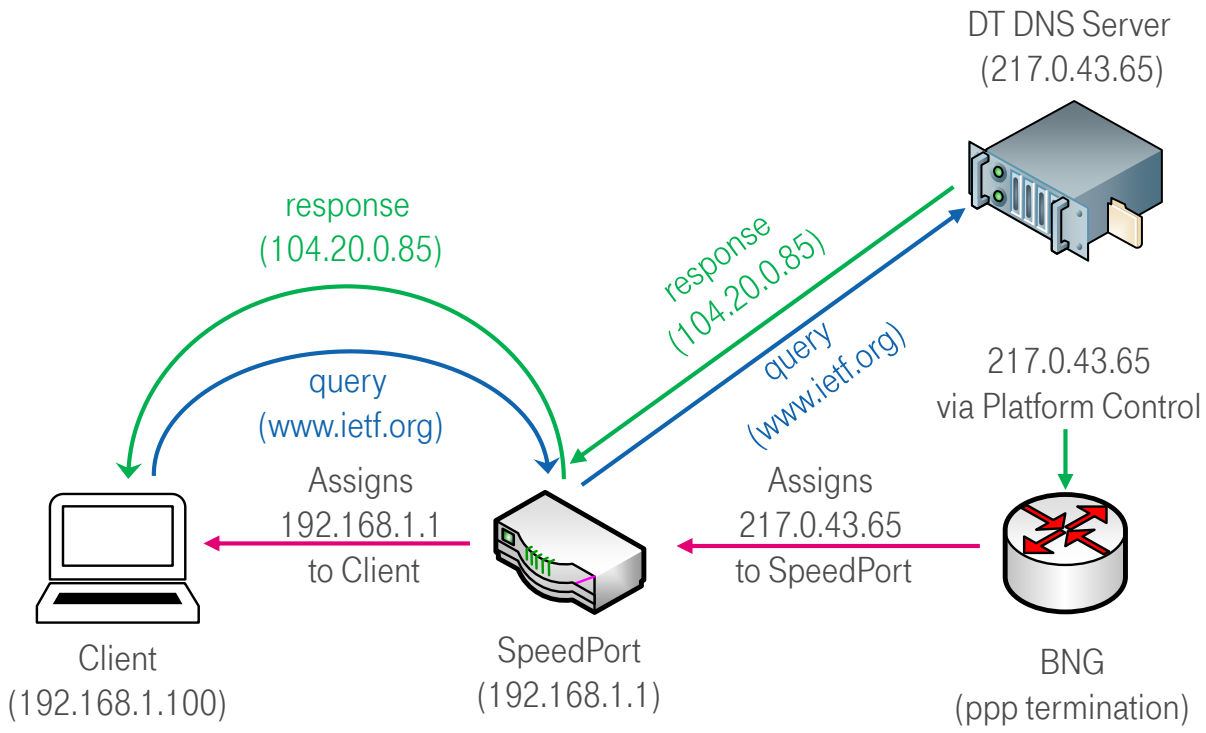
About 2 Million DNS requests per second are handled



The DT DNS platform is the foundation for implementing a wide variety of user services. Those services REQUIRE that end users are using the DT DNS infrastructure. This includes security features, NAT64/DNS64 in Mobile Networks, Load Balancing for CDNs, ...

THE EVOLUTION OF DNS

STANDARD DNS DEPLOYMENT IN DT HOME NETWORK



(*) Customer is able to overwrite/change DNS settings in Home Gateway

Remarks

- BNG obtains addresses of DT DNS servers via Platform Control
- BNG assigns addresses of DT DNS servers to Home Gateway (e.g. SpeedPort) during PPPoE session setup.
- Home Gateway acts as a DNS Proxy on behalf of home network devices
- Address for DNS queries is assigned to all local clients by Home Gateway (usually via DHCP) (*)
- All end devices in home network are using the IP address of the Home Router as DNS server address.
- Home Router forwards requests to DT DNS servers

DNS Server addresses are under control of the service provider.

THE EVOLUTION OF DNS
STATUS OF DNS IMPLEMENTATION AT DT

- **Several different DNS platforms, Mobile and Fixed Line DNS largest implementations (ongoing consolidation of DNS at DT)**
  - Same software platform
- **DNS under control of DT, platform provides name resolution and DNS based services**
  - Guarantees privacy, reliability and high performance DNS implementation
  - DNS problems can be tracked and solved by DNS operations (only if customer uses DT platform)
  - Note: Customer is not forced to use DT DNS platform (more than 90% of customers are using the DT DNS as default)
- **Currently only DNS53 implemented (due to lack of client implementation in home gateways)**
  - DoT seen as evolution path from DNS53 towards encrypted DNS, not changing the deployment model and responsibilities
- **DT evaluating DoT and DoH implementation in existing DNS platform (for mobile and fixed network customers)**

THE EVOLUTION OF DNS

OVERVIEW – ALTERNATIVE TRANSPORT OF DNS

DOT – DNS over TLS

- Encrypts DNS traffic with TLS
- Implemented in Operating System/Router
- Clients are using DNS servers assigned by operating system
- Probing mechanism recommended
- Uses well known port (853)
- Does not change communication behavior between client/end system and DNS servers
- RFC8310

No impact on operational model

DoH – DNS over HTTPS

- Uses HTTPS for DNS (Encrypts DNS traffic)
- Implemented directly in the client (e.g. web browser, app on mobile devices)
- Bypasses DNS servers assigned to (and by) the underlying operating system
- Changes communication behavior between client/end system and DNS servers
- RFC8484

Impact on operational model

DoQ – DNS over QUIC

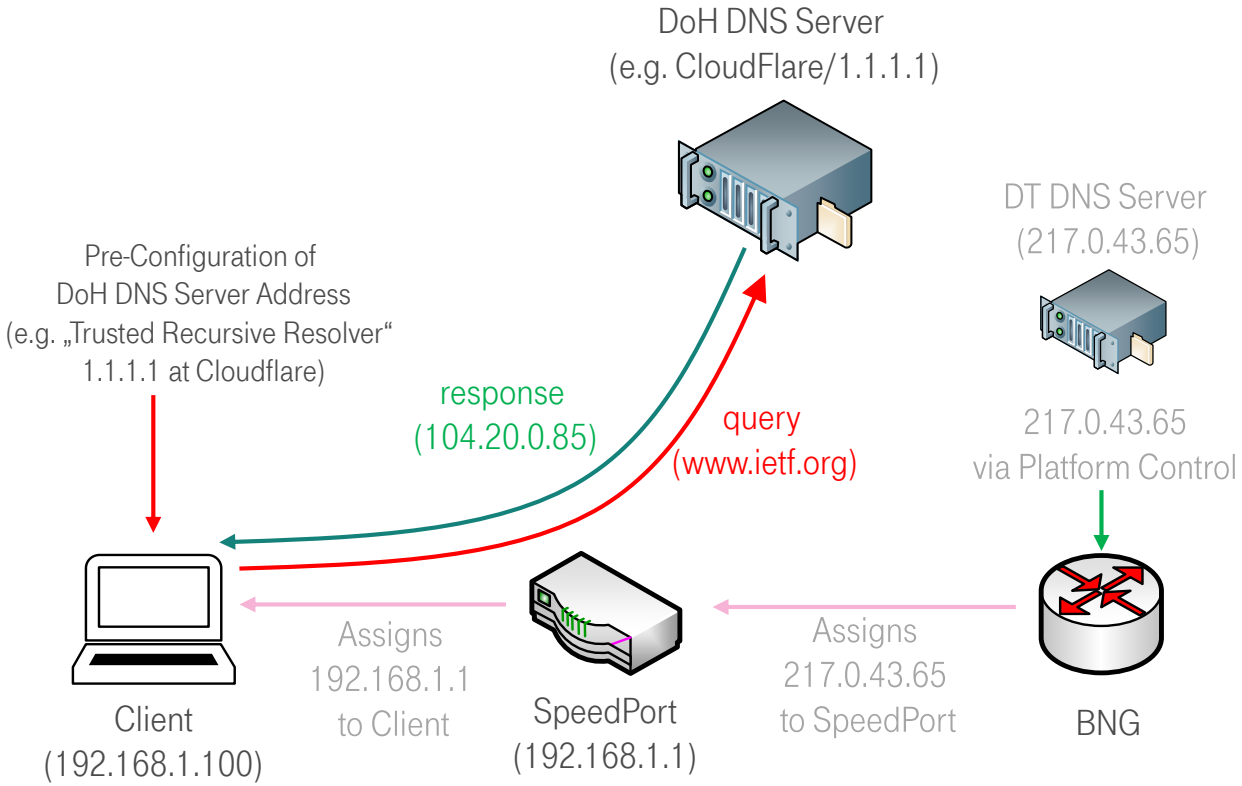
- Same model as DoH, but based on QUIC as transport
- Similar behavior as DoH (but draft recommends a discovery mechanism/use of network provided resolvers)
- Under standardization, still IETF draft
- draft-huitema-quic-dnsoquic

No impact on operational model

THE EVOLUTION OF DNS – DOH

DNS OVER HTTPS DEPLOYMENT IN HOME NETWORK

(SIMILAR IN MOBILE NETWORK)



(*) Please note, that there are some exceptions. E.g. chromecast uses Google DNS as default

Remarks

- Client still obtains DNS server address from SpeedPort, but:
  - DNS address provided by Service Provider is ignored by the clients (applications).
  - Application at the client uses it’s own DNS server, provided by the application via an “out of band” mechanism (e.g. preconfigured within application)

DNS Servers of Service Provider bypassed.

THE EVOLUTION OF DNS – DOH
RESTRICTIONS AND CHALLENGES FOR SERVICE PROVIDERS

Technical Challenges affecting operational model

- Functionality build into DT DNS servers not being used anymore
  - DNS based Security
  - DNS64/NAT64 for IPv6 only Mobile Networks
  - Local Domain Names for private addresses (“speedport.ip”)
  - DNS in Enterprise Networks (“internal.company.com”), same problem as above
    - Leaking of information (e.g. company structure, server names, ...) to cloud provider
  - DNS “split” (local DNS results differ from public resolvers) – heavily used in DT mobile network
  - CDN load balancing / endpoint selection
  - Redirection for captive portals (wireless hotspots, fixed network)
  - EDNS Subnet Option not working anymore

Other Challenges

- New partnerships between content providers and application programmers to provide DNS
- Risk of new monopolies for DNS services, few, centralized cloud providers offering DNS
- ISPs in many cases seen as the “evil provider”, violating privacy and customer rights (“DNS in the cloud provides better privacy”)
  - Very strict privacy laws in Europe (can not be applied if DNS provider outside of Europe)
- Privacy issues
  - DoH providers are collecting information and DoH Hosting outside Germany/EU
- DoH provider impacts overall DT’s customers’ experience
  - Downtime of OTT DNS seen as DT downtime
  - OTT DNS performance seen as DT performance
  - Outstanding connectivity to OTT DNS necessary

THE EVOLUTION OF DNS
DOT AND DOH IMPLEMENTATION @ DT

DOT – DNS over TLS

- Preferred solution for encrypting DNS traffic
- Implementation in Home Gateway (straight forward approach to encrypt DNS traffic)
- Same DNS IP addresses as standard DNS53, as transparent as possible for end customers (no customer impact)
- Home Gateway (or client) should probe for DoT support on existing DNS addresses and chose based on customers settings
  - Additional configurations (e.g. certificates) need to be provided

DoH – DNS over HTTPS

- Implemented to address move towards OTT DNS/DoH
  - Not our preferred solution for encrypted DNS
- More complex operational model, different (additional) DNS server infrastructure (to protect DNS53/DoT servers)
  - Due to the lack of dynamic discovery, DoH infrastructure open to all users (not only DT customers)
  - Larger target of attacks
- Without discovery, complex model for providing DoH addresses to end customers
  - Customer impact, they need to be educated (most of the customers have no clue what DNS stands for)

THE EVOLUTION OF DNS
OPEN ISSUES TO BE ADDRESSED

- **Discovery mechanism for DoH necessary**
  - Server information need to be provided by the network (no static configuration without asking customer in application)
  - Same operational model as today, DoH only used if provider supports DoH (or if end customer changes manually the DNS configuration)
  - If DoH is not supported by provider, fallback to either DoT or standard DNS53
  - Necessary to minimize customer impact
- **Set of uses cases for DoH necessary, including clear policies how OTT DNS is handled and controlled**
- **DoH can cause a lot of operational impact, if OTT services are used**
  - Poor performance, debugging, non working services, ...
- **How does the user know if DoH is used (especially in the opportunistic scenarios)?**

THE EVOLUTION OF DNS
SUMMARY

- **Secure DNS communication (DoT/DoH) as evolutionary path for DNS**
  - Good direction, but should be done in a way that it does not interfere with existing DNS based services
  - Benefit also depends on deployment scenarios usually does not apply to all networks by default (there are many service provider and enterprise networks providing a very high level on security and privacy)
- **DT evaluating DoT and DoH**
  - No real advantage for DoH compared to DoT
  - DoT the straight forward evolutionary path, plays very well together with existing DNS53 deployments
- **Still many open issues for DoH which need to be addressed**
  - e.g. HTTP has potentially more attack vectors compared to DNS53/DNS853