Encrypted DNS Factsheet

May 2023

What is DNS, and Why is it Critical?[1]

The domain name system (DNS) is fundamental to everything we do online. Serving as a directory lookup for the Internet, it makes the Internet easier for humans to navigate and makes it easier for services online to be highly resilient.

DNS means that humans and machines can each use the kind of Internet address format most suitable to them. For instance, you can just type internetsociety.org in your web browser instead of the site's IP (Internet Protocol) address, which would look like "104.18.16.166" (its IPv4 address) or 2606:4700::6812:10a6 (its IPv6 address).

For apps and devices, DNS is often less about making Internet destinations easier to remember—apps don't have as much difficulty remembering things—and more about making them resilient. That is, DNS makes it possible for an organization to make itself available across many servers, not just one. How is that possible? DNS can be used to point an app to the server that is most appropriate for the user of the service. For example, it could point to a server that is close to the user of the app, instead of a server on the other side of the planet, which would cause a very laggy experience. Most cloud services operate in this manner, with DNS an essential component connecting a user to a computer that is close to them.

What are Some of the Risks of Using DNS?

While the DNS has been refined and extended since it was standardized in 1983, its privacy properties have not. As designed, DNS information is sent unencrypted across the Internet, and thus is viewable by anyone along the path, resulting in lack of privacy.

1 A detailed explanation of DNS is beyond the scope of this document. There are many good references available for anyone wishing to learn more. Good and simple examples can be found at
https://www.internetsociety.org/resources/deploy360/dns-privacy/faq/
https://www.cloudflare.com/learning/dns/what-is-dns/
https://www.networkworld.com/article/3268449/what-is-dns-and-how-does-it-work.html

Perhaps the biggest risk is that it's so easy to forget DNS exists...! It's hard to know or care about something you never see. Most users don't know how the DNS works (and they shouldn't need to, they should be able to just use the Internet) and are therefore unaware that third parties can see the name of every site and URL they request.

DNS, the Internet, and the World Wide Web

Web browsers, like Chrome, Edge, Firefox, and Brave, allow users to rely on using human-friendly domain names. This is illustrated in Figure 1 in a simplified form.

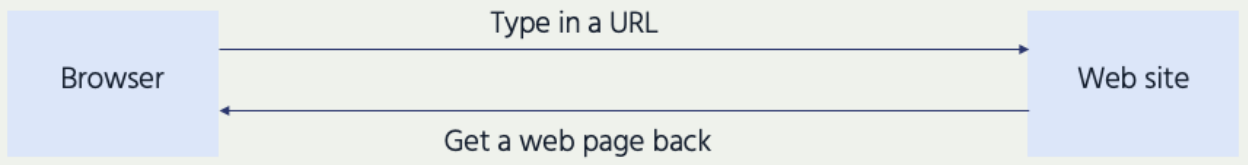

Figure 1

In fact, browsers are using numeric IP addresses to identify and connect to the desired resources, as illustrated in Figure 2. To do this, they rely upon DNS to translate the domain name to the correct IP address, which is invisible to the user.

Figure 2

Behind the scenes, the browser is sending a request to a DNS server, asking "what is the correct IP address for this domain name?"

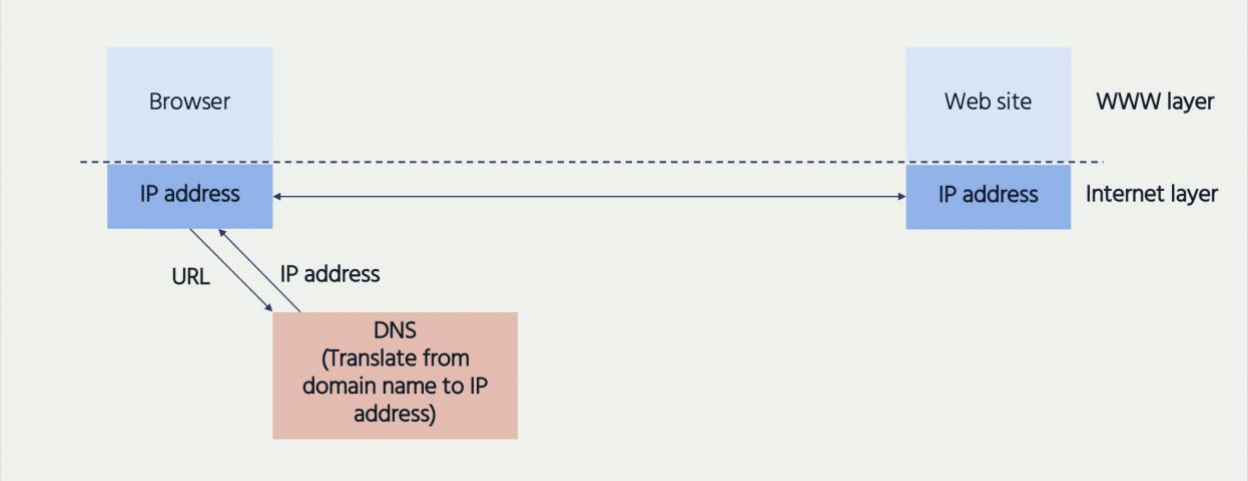

Figure 3

Expanding upon the simplified model in Figure 3, Figure 4 shows how a browser or app relies on several DNS servers to process its request for an IP address. It relies on a Recursive Resolver, so named because it tries to resolve DNS queries by going through hierarchical sets of name servers until it gets an answer.

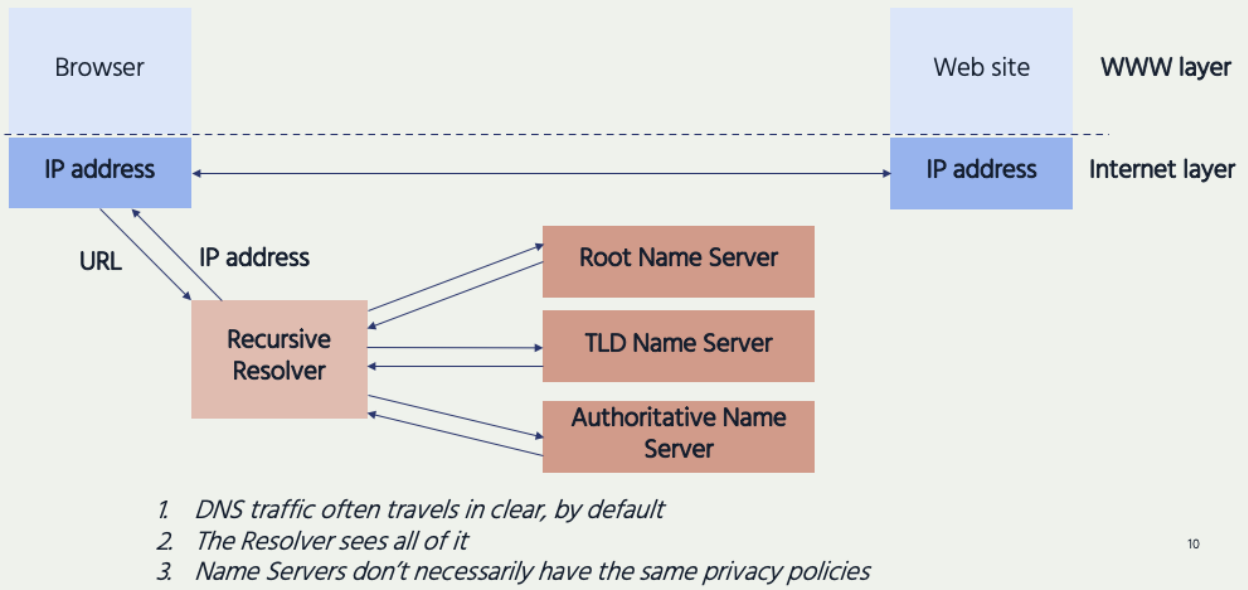

Figure 4

Why Does This Matter?

Users have to trust the DNS resolver in several ways.

- The resolver can read everything it's sent, which represents a potential privacy threat.
- Users also have to trust the resolver to be available, responsive, and accurate—if the mapping of domain names to IP addresses is faulty, unavailable or too slow, users don't get to the sites they expected.
- Where DNS traffic is unencrypted, users are also trusting that their dependence on DNS does not expose them to further privacy violations from other entities who happen to be in the communications path.

At least part of the solution to this problem, protecting the privacy of DNS queries collected by resolvers, is not technical. It is to rely upon published commitments from the DNS resolver operator. In other words, trusting that the provider will do what it promises. As one example, Mozilla's Trusted Recursive Resolver (TRR) program provides privacy guarantees for a specific set of DNS resolver behaviors, including data collection and retention, transparency, and blocking policies. A number of providers have contractually agreed to abide by these policy requirements including CIRA, Cloudflare, Comcast, NextDNS, and Shaw.

Learn more about Mozilla's Trusted Recursive Resolver (TRR) program: Trusted Recursive Resolver Security/DOH Resolver Policy

Trusted Resolver commitments still do not solve the problem of third-party observation of DNS traffic on the Internet.

What Can Be Done to Provide Confidentiality on the Network? Encryption!

DNS traffic is, by default, unencrypted, which means third parties can see users' queries.

However, DNS traffic can be protected from unwanted third- party access by making sure queries are encrypted between the browser and the DNS resolvers. The Internet Engineering Task Force (IETF), which develops the protocols that make the Internet work, continues to work on secure protocols to protect DNS queries.

There are three major secure transport protocols which have been, or are being, standardized for DNS. These are DoT, DoH, and DoQ:

- DoT (DNS over TLS): this encrypts the DNS traffic but doesn't try to hide it.
- DoH (DNS over HTTPS): this hides the DNS traffic by making it look like any other (HTTPS[2]) web traffic.
- DoQ (DNS over QUIC): like DoH, this hides the DNS traffic by making it look like any other (HTTPS) web traffic, but for a more modern variant of web traffic.

Why mask DNS queries by making them look like other web traffic? When DNS queries can be interfered with, this can be a mechanism for Internet censorship, filtering, and blocking. Masking DNS queries makes this kind of interference more difficult.

Read more technical explanations:

- DoH – DNS over HTTPS: maps DNS queries onto HTTP request responses and runs them over HTTP over TLS (HTTPS).
  https://blog.apnic.net/2018/10/12/doh-dns-over-https-explained/
  https://www.rfc-editor.org/rfc/rfc8484.html
- DoT – DNS over TLS: you open a TLS channel to the server and send DNS queries over it.
  https://www.cloudflare.com/learning/dns/dns-over-tls/
  https://www.rfc-editor.org/rfc/rfc7858.html
- DoQ – DNS over QUIC: sets up a connection over the QUIC secure transport protocol and sends DNS queries over it.
  https://blog.apnic.net/2022/03/29/a-first-look-at-dns-over-quic/
  https://www.rfc-editor.org/rfc/rfc9250.html

2 HTTPS is the encrypted (and thus secure) version of HTTP – Hypertext Transport Protocol – which is the fundamental protocol used to transmit data between a website and a web browser. In most if not all modern browsers, websites that do not use HTTPS are flagged somehow so that the user is aware that their data is being send and received "in the clear." This is particularly important when sensitive information is involved, such when logging into a service using a password.

Protecting Privacy as Well as Confidentiality

Encrypting the traffic between the browser and the DNS will keep it confidential from third parties. But the DNS servers still need to see the unencrypted queries to do their job, and this is a potential privacy threat to the user, even with promises from DNS resolvers not to misuse the information (see above). Several working groups at the IETF are addressing the privacy and confidentiality issues relating to DNS:

- DPRIVE – IETF DNS Privacy Working Group
  This IETF working group develops confidentiality mechanisms for DNS, to counter the threat of pervasive monitoring of Internet communication, as described in RFC 7258 (Pervasive Monitoring Is an Attack). This RFC was the IETF's response to the disclosure of mass surveillance of Internet traffic by governments.
  https://datatracker.ietf.org/wg/dprive/about/
  https://www.rfc-editor.org/rfc/rfc7258

- ADD – IETF Adaptive DNS Discovery Working Group
  This working group explores the many different contexts in which DNS is used (including public networks, private networks, and VPNs), supporting both encrypted and unencrypted resolvers. The purpose of ADD is to resolve the tension between users' legitimate wish for privacy, and the equally legitimate security and safety requirements of network operators and enterprises. This tension can give rise to controversy, which is discussed below in "Why is there controversy?"
  https://datatracker.ietf.org/wg/add/about/

- Protection using a trusted proxy - ODoH – Oblivious DNS over HTTPS: Even if you are connected to a known and trusted DNS resolver, there is still the privacy issue that the resolver can see all of your DNS queries as well as your source IP address. ODoH routes your encrypted DNS queries through a proxy which conceals your IP address from the DNS resolver. In doing this, your queries and IP address are never in the same place.
  https://blog.cloudflare.com/oblivious-dns/
  https://www.rfc-editor.org/info/rfc9230

Making DoH "Oblivious" (ODoH)

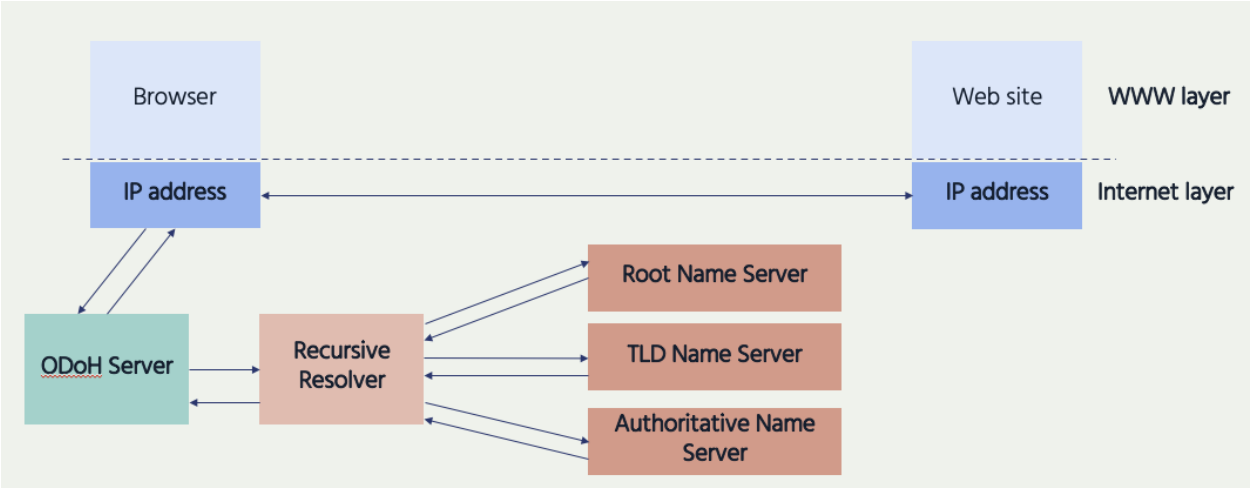

Figure 5

- The ODoH Server sees the Requester ID but not the domain name in the URL requested, or the destination
  IP address
- The Resolver sees the domain name in the URL but not the Requester ID

Is Encrypted DNS the Answer?

- Right now the vast majority of client-to-resolver DNS traffic remains unencrypted. Encrypting this traffic protects its confidentiality from third party access.
- As seen above, trusting DNS to provide the right IP address is not the same as trusting the DNS resolver not to abuse your personal data. Also, if the DNS is resolving addresses incorrectly, it will probably be obvious to the user. But, if the DNS resolver is abusing the user's personal data, there may be little or no sign that this is happening. Encrypting the DNS traffic will not prevent the resolver from misusing it.
- Because there is no indication to the user as to what is happening with their DNS queries and the responses, they may think the DNS resolver is trustworthy when it is not.

To mitigate these problems, there are two things that can be done: you can choose a DNS resolver that supports encrypted queries (how to specify your DNS resolver varies by device and is beyond the scope of this document), and make sure that your DNS resolver is signed up to the Mozilla TRR program, described above.

- Your privacy and security is only as good or as bad as the entity you entrust to run the DNS resolver you are using—whether local or remote. Fundamentally you are changing who you trust to do what, much like with a virtual private network (VPN) provider, through which

you entrust visibility into all of your network traffic while keeping it shielded from your local network and ISP (Internet Service Provider).

- Regardless of whether your DNS queries are encrypted, associated metadata is still a potentially rich source of information to anyone monitoring your traffic. Examples include timing and query, response traffic characteristics, as well as your social graph—the people you are connected to, follow online, or have in your address book.

Why is There Controversy?

Encrypting DNS traffic provides confidentiality and, with added privacy protections such as ODoH, greater privacy for users. However, not everyone wants DNS traffic to be encrypted. The main controversy arises between users and network operators—because DNS confidentiality and privacy impacts the way that network operators and enterprises have traditionally managed their networks. They have relied on the ability to see DNS queries and interrupt them to block sources of malware and other content. Network operators and enterprises are trying to meet a legitimate requirement, and that is the focus of the IETF ADD (Adaptive DNS Discovery) working group referred to above.

This can be condensed down to two positions: "encrypt it all!" versus "my network: my rules!" Let's unpack the issues:

Encrypt All DNS Traffic

- Encrypting DNS traffic using the methods developed to date relies upon the availability of appropriately configured DNS resolvers. Currently the proportion of resolvers that support encryption is small, relative to the overall number of resolvers.

  Centralization (consolidation) is therefore a real concern, as it has been in many aspects of the Internet, because there are only a handful of options available.[3] Among other problems, this provides attractive targets for attacks or surveillance. In many if not most implementations of encrypted DNS, although the user may be able to select which DNS resolver to use, this is often challenging for non-technical users. The default choice may or may not be the best one (e.g., due to concerns about the organization operating it or the jurisdiction in which it is based).
- It is extremely difficult to discern the trustworthiness of the operators of these centralized servers, forcing us to rely upon their public privacy statements and possibly self-assessments or external audits.

3 Internet Society 2019 Global Internet Report: Consolidation in the Internet Economy - How will consolidation impact the Internet's technical evolution and use? https://future.internetsociety.org/2019/

Even audits may not be foolproof, since they are often desk exercises relying upon information provided by those under audit and lacking actual detailed forensic investigation. A self-assessment approach ultimately boils down to management of business risk on the part of the operator—and experience tells us that sometimes, businesses decide to take the risk rather than invest in onerous compliance processes. A best, they are snapshots in time, and may not be reliable predictors of future behavior. And even viewing audits in their best light, circumstances may and often do change dramatically, whether due to malicious compromise or upon changes of control (e.g., by acquisition, merger, or management shifts).

- DNS is certainly not the only protocol used when browsing the Web or using online services, and there are many other sources of revealing data that can, and do, track users. Thus encrypted DNS cannot be viewed as a panacea, and certainly not "the solution" for preventing user tracking, but rather it is an option for limiting one source of user tracking data. As noted above, unencrypted metadata is still easily available and is a rich source of information.
- Even if DNS traffic is encrypted, the ISP will still know what sites the user is connecting to because some parts of the HTTPS connection are not encrypted, such as SNI (Server Name Indication)[4], OSCP (Online Certificate Status Protocol)[5], IP addresses, and other concurrent HTTP(S) connections.
- DNS encryption has been used to bypass DNS-based blocklists, though DNS-based blocklists can also be bypassed by accessing the site directly via its IP address.
- Although this is by no means a complete solution to this problem, since there are many other means available for user tracking (as noted above).
- If a user's main concern is tracking and surveillance, they should equally be considering measures such as using virtual private networks (VPNs)[6] and Tor[7] because these make traffic analysis more difficult.

"My Network, My Rules"

- Encrypting DNS queries can reduce the operator's ability to examine and thus control and troubleshoot network behavior and problems. Examples include parental controls, or any enterprise wanting or needing visibility into their DNS queries for troubleshooting, network security, traffic filtering, malware detection, meeting compliance requirements, etc.

4 SNI is an extension to the TLS protocol, enabling a client or browser to signal which hostname it is attempting to connect to at the start of the TLS "handshake." This enables the server to present multiple certificates on the same IP address and port number. This is useful for those hosting multiple sites, or proxies which need to determine which server to forward client traffic to.

5 OCSP is used by browsers or apps for obtaining the revocation status of a server's X.509 digital certificate when initiating a connection to a website. It was developed as an alternative to Certificate Revocation Lists (CRLs).

6 Bareckas, Karolis. 2022. "VPN for dummies: a guide for beginners" NordVPN.. https://nordvpn.com/blog/vpn-for-dummies/

7 The Tor Project, Inc. n.d. "Tor Project | Anonymity Online". Tor Project. Accessed 17 February. 2023. https://torproject.org/

- With the rise of Bring Your Own Device (BYOD), which allow enterprise users to access protected systems using their personal phones, tablets, or laptops, this can present major hurdles, especially for highly regulated environments found in industries like financial services and healthcare.

Conclusions and Recommendations

Different stakeholders have legitimate arguments for and against pervasive encryption of DNS traffic, so this needs informed multistakeholder discussion, and a recognition that users' privacy interests are currently poorly reflected in the available options. The most appropriate choice will depend upon your circumstances and risk profile.

DNS is Critical to the Internet's Correct Functioning. It also Raises Issues of Confidentiality, Privacy, and Security.

- If DNS is either inaccurate or unavailable, users (and apps and devices) get routed to the wrong resources, and the Internet ceases to be a useful communications infrastructure.
- Insecure DNS queries may reveal detailed user behavior to third parties.
- DNS servers need to see the contents of DNS queries to do their job, therefore they are in a position to violate the user's privacy.
- Some kinds of stakeholders rely on DNS traffic to perform network management, security, or compliance tasks.

User Agency is Often Limited.

- Users may be unaware of the potential privacy and confidentiality issues with their default DNS service, not know what alternatives are available, or not know how to change from the default.
- When using mobile devices or apps (as opposed to browsers), users may struggle to change the default DNS options.
- Value-add services based on DNS, such as user-configurable filters, may represent an opportunity for service providers to offer a compelling alternative to the default consumer DNS service (as generally offered by ISPs). This potentially increases user agency, but they must have a trusted DNS provider.

This is a Multistakeholder Problem.

- Users often lack agency. Even though they are the stakeholders most likely to be at risk if their DNS is insecure, there may be little they themselves can do to manage that risk. If you are a user, you can investigate the DNS options available to you. Changing your default DNS resolver can be challenging, but now you know what factors to take into account.

DNS should also form part of national and regional cybersecurity considerations—to increase resilience, remove single points of failure, and improve security and data governance. If you are a policymaker, you should encourage measures that increase the privacy and security of the DNS infrastructure, not just because this is a fundamental component of Internet access, but because these measures also protect users' rights.

- For DNS resolver operators, adopting the principles consistent with the Mozilla Trusted Recursive Resolver (TRR) program, and signing on, benefit you and your customers.
- If you are an enterprise operator, you may elect to have your DNS traffic unencrypted for compliance, security, or troubleshooting reasons. But it is still important to investigate options that strike a balance, such as running a DNS recursive resolver local to your network and encrypting any resulting outbound DNS traffic.