## DNS over HTTPS (DoH) vs DNS over TLS (DoT)

### Introduction

Domain Name System (DNS) is a fundamental component of the internet, translating human-readable domain names (like `example.com`) into IP addresses. Traditionally, DNS queries are sent in plaintext over UDP or TCP, exposing them to surveillance, manipulation, and censorship.

To mitigate these privacy and security concerns, two encrypted DNS protocols have emerged:

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

While both encrypt DNS traffic, they differ in transport mechanisms, performance, and deployment models.

## DNS over HTTPS (DoH)

**Definition**: DNS over HTTPS sends DNS queries over standard HTTPS connections (port **443**) using the HTTP/2 or HTTP/3 protocol.

### Key Characteristics:

- Encapsulates DNS queries inside HTTPS traffic
- Uses port `443`—the same as regular web traffic
- Often integrated directly into browsers (e.g., Firefox, Chrome)
- Harder to distinguish from normal HTTPS traffic

### Pros:

- **Difficult to block or censor** due to use of port 443
- **Provides privacy even in restrictive networks**
- **Easily integrated into browsers and apps** for per-app privacy

**Cons:**

- **Harder to filter or log** DNS traffic by enterprises
- **Can bypass local DNS controls**, causing security or compliance concerns
- **Potential centralization** of DNS data with third-party DoH providers

## Use Cases

- **DoH is ideal for**:
- Circumventing DNS-based censorship
- Privacy in public or hostile networks
- Applications needing built-in DNS privacy
- **DoT is ideal for**:
- Securing DNS at the network or system resolver level
- Enterprises that want DNS privacy with more control
- Networks that rely on traditional DNS monitoring tools

## Conclusion

DoH and DoT represent significant improvements in DNS privacy and integrity, each suited for different environments:

- Use **DoH** when you need stealth, app-level integration, or must bypass network controls.
- Use **DoT** when you want system-wide encrypted DNS with more visibility and control.