# Path to Encrypted DNS with DDR: Adoption, Configuration Patterns, and Privacy Implications

vasilis ververis
Hasso Plattner Institute, University of Potsdam, Germany
vasilis.ververis@hpi.de

Steffen Sassalla
Hasso Plattner Institute, University of Potsdam, Germany
Steffen.Sassalla@student.hpi.uni-potsdam.de

Felix Roth
Hasso Plattner Institute, University of Potsdam, Germany
Felix.Roth@student.hpi.uni-potsdam.de

Vaibhav Bajpai
Hasso Plattner Institute, University of Potsdam, Germany
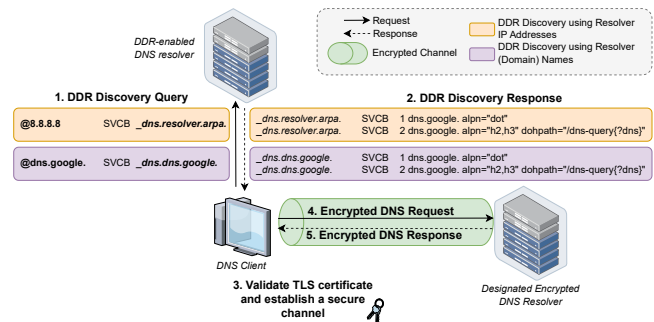vaibhav.bajpai@hpi.de

Figure 1: Illustration of the DDR protocol. Orange boxes indicate the DDR discovery query and response using the resolver IP address, while purple boxes indicate the same discovery using the resolvers' domain name. We use Google's DDR-enabled resolver (`8.8.8.8`/`dns.google`) to illustrate a sample response. Bold text highlights differences between the DDR discovery queries and responses.

## Abstract

DNS is crucial for the Internet, but vulnerable due to plaintext traffic. Despite efforts to standardize Domain Name System (DNS) encryption, its adoption remains limited. Users often lack awareness of privacy risks and the knowledge to enable encryption. To address this, the IETF standardized a new protocol; Discovery of Designated Resolvers (DDR), enabling automatic discovery and upgrade from unencrypted to encrypted DNS traffic. In this study, we present an empirical investigation of the DDR protocol, focusing on its adoption, configuration, and the operational challenges associated with enabling automated transitions to encrypted DNS communication via DNS over Encryption (DoE) protocols. Our results reveal widespread misconfigurations, including incomplete and incorrect DDR configurations that prevent clients from successfully transitioning to encrypted resolvers. In over 99 % of observed cases, DDR-compliant clients may fail to upgrade to DoE due to these deployment issues, underscoring the limitations of DDR in the wild. Additionally, we note a severe resolver consolidation induced by current DDR deployments, as >97 % of DDR-enabled resolvers delegate to major DNS cloud providers, raising concerns about privacy and governance.

## Keywords

DDR, Discovery of Designated Resolvers, DNS, DNS centralization, network measurement

## 1 Introduction

DoE protocols provide confidentiality and integrity for the *stub-to-resolver* communication, but do not offer provisions for resolver selection by client applications [72]. As such, stub-resolvers have limited means to discover encrypted DNS resolvers and end up relying on the (often unencrypted) resolver assigned by the Internet Service Provider (ISP) via Dynamic Host Configuration Protocol (DHCP). In addition, users are often unaware of the privacy risks associated with using unencrypted DNS by default, and there is insufficient understanding on how to effectively transition to encrypted DNS configurations [24]. Consequently, there is a pressing

need for mechanisms that enable clients to identify available encrypted DNS services and automatically switch to them without requiring user intervention. To address this gap, the Internet Engineering Task Force (IETF) has standardized DDR, a mechanism for clients to use Service Binding and Parameter Record (SVCB) Resource Records (ResRs), to leverage DNS queries to discover a resolver's encrypted DNS configuration [53]. The encrypted DNS resolvers discovered by this mechanism are called *Designated Resolver(s)* operated by the same entity or cooperating entities [53]. With DDR, stub-resolvers are enabled to automatically upgrade from unencrypted DNS to encrypted DNS. Although the DoE protocols target secure *stub-to-resolver* communication, DDR can also be applied to discover DoE endpoints of authoritative endpoints, i.e., *recursive-to-authoritative* DoE traffic [21]. The DDR discovery process is illustrated in Figure 1. DDR consists of two steps: the encrypted resolver discovery and the encrypted resolver verification.

The DDR protocol shows promise for enhancing DNS security and privacy, but its real-world deployment and configuration are underexplored. Major DNS cloud providers like *Google* and *Cloudflare* support DDR, indicating its growing adoption. Understanding the adoption rates, configuration patterns, and challenges of DDR is crucial for evaluating its effectiveness in transitioning to encrypted DNS protocols. This study empirically investigates DDR's deployment and role within the DNS ecosystem.

Throughout this study, we aim to answer the following Research Questions (RQs):

**RQ1:** What are the adoption rates and trends of public DDR-enabled resolvers in IPv4 and IPv6, and how do they vary across geographical regions and network types over time?

**RQ2:** What configuration patterns are observed in DDR-enabled resolvers, and how do these patterns differ across networks and over time?

**RQ3:** What observable challenges hinder clients from successfully transitioning from plain DNS to DoE protocols in real-world DDR deployments?

To address these research questions, we developed an open-source, adaptable, and highly scalable three-stage measurement architecture. In the first stage, we collect responsive IPv4 and IPv6 addresses on port UDP/53. In the second stage, these addresses are used to discover DDR-enabled public resolvers and their delegated encrypted resolvers. Finally, in the third stage, we query these encrypted resolvers using the respective DoE protocols and query for other protocols like DNS Security Extensions (DNSSEC) as well. Our contributions are as follows:

(1) **Adoption and Configuration Analysis:** We provide a comprehensive analysis of the adoption rates and trends of public DDR-enabled resolvers across different regions and network types, and identify the configuration patterns of these resolvers, highlighting the dominance of major DNS cloud providers. Importantly, we uncover significant instances of non-compliance with recommended DDR configurations among resolvers.

(2) **Security and Privacy:** We evaluate the security and privacy implications of DDR deployments, including the effectiveness of encrypted DNS communication and the risks associated with misconfigurations.

(3) **Centralization Concerns:** We examine the impact of DDR on DNS centralization, revealing how the reliance on a few major providers can affect the decentralization of DNS infrastructure and user privacy.

## 2 Background and Related Work

DDR supports two types of discoveries [53] (see Figure 1): **discovery using resolver IP addresses** (orange boxes) and **discovery using resolver (domain) names** (purple boxes).

DDR *discovery using resolver IP addresses* applies to scenarios where the client knows only the IP address of a DNS resolver (e.g., a Recursive Resolver (RR)) and seeks to discover and upgrade to DoE endpoints. In this case, the client can issue a DNS query of type SVCB with the query name `_dns.resolver.arpa.` directed to the resolver's IP address [53]. The `resolver.arpa.` domain is a Special Use Domain Name (SUDN), serving as a locally defined zone specifically designated for DDR discovery [6, 53].

As a SUDN, `resolver.arpa.` is not part of the public DNS hierarchy and cannot be resolved recursively. Instead, the ResRs within the `resolver.arpa.` zone are locally served, enabling efficient discovery of DoE endpoints without dependence on the DNS over UDP (Do53) hierarchy. Conversely, the *discovery using resolver (domain) names* applies to scenarios where the client already knows an encrypted resolver by its Fully-Qualified Domain Name (FQDN) and

seeks to determine the resolver's supported DoE protocols or its current configuration [53]. In this process, the client issues an SVCB query with the query name `_dns.<FQDN>`. This query can either be sent directly to the resolver or resolved recursively, as — different to the first discovery method — the SVCB resource resides within the public DNS hierarchy. For instance, if the client already knows the encrypted resolver `dns.google.`, it can issue an SVCB query with the Query Name (QNAME) `_dns.google.dns.` to retrieve its current DoE configuration (see purple boxes in Figure 1).

### 2.1 Discovery Response

In response to the DDR discovery, the resolver returns a set of SVCB ResRs [66]. Each SVCB record contains a priority field (`SvcPriority`), the encrypted resolver's domain name (`TargetName`), and the supported protocol(s), specified in the SvcParam *alpn* (application layer protocol negotiation) field. For example, the DDR response from Google's DNS resolver advertises the DNS over TLS (DoT) protocol on its default port 853, at the domain `dns.google.`, with the highest priority set to 1 (see Figure 1). A secondary advertised resolver supports both DNS over HTTPS (DoH)/2 and DoH/3 on port 443 with a lower priority of 2, and the URI path `/dns-query{?dns}`. Ultimately, the decision regarding which DoE resolver to use remains with the client.

Further, DDR also allows for the advertisement of deviating default ports. For example, if the encrypted resolver runs DoH/2 on 8884 instead of the default port 443, the DDR-enabled resolver can advertise a deviating port with `port=8884`. An encrypted resolver is advertised by DDR with its FQDN. Thus, if a client chooses to upgrade to the advertised encrypted resolver, it first needs to look up its IPv4 or IPv6 address. To minimize these additional Round-Trip Times (RTTs), the DDR-enabled resolver can advertise the encrypted resolver's IP addresses with `ipv4hint` and `ipv6hint`, although these should also be supplied via additional records in the DNS response. The DDR-enabled resolver can indicate Oblivious DNS over HTTPS (ODoH) by setting the SvcParam `ohttp` without any value, i.e., just `ohttp` [54]. Additional information about public key material and proxy information can be retrieved using a `.well-known/` URI at the advertised encrypted resolver's domain name.

### 2.2 Discovery Verification

In all cases, when a client performs DDR to discover encrypted resolvers, it must verify the response [53]. The verification method depends on the discovery approach employed, whether it involves *discovery using resolver IP addresses* or *discovery using resolver (domain) names*. If a client performs DDR's **discovery using resolver IP addresses**, two verification methods are available: *verified discovery* and *opportunistic discovery*. Alternative approaches, such as policy- or heuristic-based methods, are left to the client's discretion.

The DDR protocol is explicitly designed for upgrades from unencrypted to encrypted resolvers operated by the same entity. This ensures that the discovered encrypted resolver is equivalent and trusted, as verified by matching ownership indicators such as TLS certificates or IP address inclusion in the certificate's subjectAltName TLS extension (SAN) field [53].

The *verified discovery* method requires two verification steps a client must complete before accepting an automatic upgrade to an encrypted resolver. First, the certificate chain presented during the Transport Layer Security (TLS) handshake must be valid. All DoE protocols use TLS. Second, the IP address of the DDR-enabled resolver advertising the encrypted resolver must be included in the SAN field of the encrypted resolver's certificate. The SAN field allows additional FQDNs or IP addresses to be specified, under which the certificate is also valid [28, 61].

However, the verified discovery process may not always be applicable [53]. For example, when a client attempts to verify an advertised encrypted resolver accessible via a local IP address, the verification process may fail. This limitation arises because local IP addresses are not globally unique [57] and therefore cannot definitively establish ownership or control of the advertised service. In such cases, the decision to use the encrypted resolver defaults to the client, following the `opportunistic discovery` method. Under this approach, clients may rely on the information in the SVCB records only if the IP address of the advertised encrypted resolver matches that of the DDR-enabled resolver.

If a client performs DDR's **discovery using resolver (domain) names**, it must execute the verified discovery procedure, similar to the one specified for *discovery using a resolver's IP address* [53]. In this process, the domain name of the DDR-enabled resolver, on which the DDR discovery query was executed, must appear in the encrypted resolver's certificate SAN field. For instance, in the example shown in Figure 1, the encrypted resolver name `dns.google.` must correspond to the advertised encrypted resolver name, which, in this case, is also `dns.google.`. Encrypted resolvers may, however, delegate to other encrypted resolvers. For example, if the DoH service is provided by `doh.dns.google.`, the certificate for `doh.dns.google.` must include `dns.google.` in the SAN field to enable proper resolver verification. Additionally, since the SVCB record resides within the public DNS hierarchy, DNSSEC can be applied to DDR responses to provide additional response authentication. However, DNSSEC is not explicitly addressed in the DDR specification. If any verification method outlined above fails, the client should disregard the information in the DDR response [53]. In such cases, the client would fall back to unencrypted Do53 traffic.

## 2.3 Discovery of Network-Designated Resolvers

Next to DDR, another standard for discovering encrypted resolvers is Discovery of Network-designated Resolvers (DNR) [4]. With DNR, DHCP, and Router Advertisement are extended with options that provide clients with encrypted DNS servers, directly from their DHCP server, without requiring additional queries as in DDR. However, since DHCP traffic remains within a local network, DNR usage cannot be tested from a single vantage point scanning the Internet as in our setup; therefore, this work focuses on DDR.

## 2.4 Related Work

**Actively and Passively Collected DNS Datasets**: Recent studies have created diverse datasets through Internet-wide scans, enhancing our understanding of Internet traffic dynamics [2, 18]. These datasets, collected via active probing and passive monitoring, include platforms like *Censys* [17, 18], *Shodan* [?], *Rapid7 Open Data* [?

], *Zoomeye* [?], and *RIPE Atlas* [?]. *OpenINTEL* [71] and *DNS Coffee* [44] provide extensive DNS-related data, while *DNSDB* [?] offers passively collected DNS traffic insights. The *IPv6 Hitlist* [19, 65] addresses the challenge of scanning the vast IPv6 address space. Our previous work on the DDR highlighted the limitations of current DNS encryption practices and provided a large-scale measurement of DNS resolver support for DDR [62].

**Tools and Measurements in DNS**: Custom data collection is often necessary due to the dynamic nature of DNS. Tools like *ZMap* [18], *ZDNS* [33], *MassDNS* [3], and *dnsrecon* [55] have been developed for efficient DNS measurements. Studies have contributed to understanding DNS infrastructure and resolver behavior.

**Adoption and Performance Measurements of DoE**: The deployment of DoE protocols has been studied extensively. Research has analyzed DoE protocols, finding minimal latency overhead [45]. Reviews on DoE encryption techniques highlight performance and security challenges [46]. Studies have examined DoE performance and its impact on DNS resolution [7, 9, 25, 35, 37, 49, 67].

## 2.5 Privacy and Governance Implications

DoE protocols are primarily designed to secure DNS communication and to enhance user privacy. However, recent studies have evaluated the security implications of DoE and its impact on user privacy [14]. While DNS has long been a common target for censorship (e.g., DNS hijacking), studies have further investigated whether DoE protocols can circumvent censorship. Hoang et al. [23] investigated the DoH and DoT protocols in the context of censorship, given the fact that DNS blocking in the unencrypted Do53 is a common censorship technique. They developed *DNEye*, a measurement system built on a distributed network of Vantage Points (VPs), which they used to assess the efficacy and accessibility of DoH and DoT in circumventing censorship. Over six months, their study examined the accessibility of 1.6K domains from around 20K VPs, targeting 71 DoH and DoT resolvers. Their findings demonstrated that using DoE protocols enabled them to unblock over 55 % of blocked domains in China and more than 95 % of blocked domains in other countries employing DNS-based filtering. Differently, Jin et al. [36] found evidence of DNS manipulation and censorship in DoE protocols. They performed around 7M DNS lookup measurements on approximately 3.8M DoT and 75 DoH resolvers. They found that more than two-thirds of the DoT and DoH resolvers manipulated DNS responses.

At first glance, one might assume that encrypted communication, such as DoT, does not reveal information about user activities. However, Houser et al. [27] developed a DoT fingerprinting method aimed at analyzing DoT traffic to determine whether a user has visited a specific website of interest, e.g, health insurance, gambling, or dating websites. Their approach infers visited websites by modeling the temporal patterns of packet sizes and sequences. Interestingly, their method showed a false negative rate of less than 17 %, which drops to less than 0.5 % if DNS messages are not padded. They proposed using padding and uniform time intervals for message exchanges as a mitigation. While message delays could also help to obfuscate packet sequences, this conflicts with the demand for low-latency DNS communications.

DoE protocols in general have two usage profiles. Huang et al. [29] investigated downgrade attacks on DoH due to the opportunistic privacy profile [10], which allows a fallback to unencrypted DNS if the DoH channel cannot be established. They found that every major browser like *Firefox*, *Safari*, or *Google Chrome* used the opportunistic privacy profile, while all of them are vulnerable to every downgrade attack vector. Furthermore, none notified users when the connection returned to unencrypted DNS. As a result, users are often unaware of attacks on their privacy. Conversely, DoE in web browsers also poses a privacy risk, as private data may be collected by major DNS cloud providers without users' awareness. Nisenoff et al. [50] confirmed that most users are unaware of the development of DoE. For instance, *Firefox* forwards all DNS requests to *Cloudflare* in the U.S. by default using DoE, with these settings being changed without explicit user consent. This occurs because users do not fully understand the implications of DoE settings in their browsers, owing to their technical complexity and the lack of sufficient information provided by web browsers.

Li et al. [41] investigated the deployment of DoH and DoT with a focus on the strict privacy profile (see Section 2.5). They conducted monthly scans with *ZMap* between November 2021 and September 2022 to discover DoT and DoH resolvers, along with daily scans of TLS/HTTPS-related security features in the resolvers found. To discover valid DoT resolvers, they probed DNS queries via DoT on port 853. In the case of DoH, they queried on the URI paths /dns-query, /query, /resolve, and / on port 443. Their scans identified around 26K DoH and 21K DoT resolvers, while only approximately 65 DoH and 290 DoT resolvers were authoritative DNS servers. They found that around 60 % of the DoT and 44 % of the DoH RRs lacked valid certificates. In line with previous studies, they confirmed that DoT and DoH resolvers were becoming centralized. Additionally, they noted that 25 % of the DoH resolvers supporting strict privacy failed to meet the minimum privacy requirements.

In a follow-up study, Li et al. [42] further examined DoE resolvers and was the first to look at DDR. Over a 15-month scan, they identified approximately 1.3K operational DoE resolvers, of which 448 supported IPv6. They conducted 10M IPv4 and 570K IPv6 DoE queries from around 5K VPs over two months in 2023, discovering that approximately 6 % of IPv4 and 5 % of IPv6 queries were blocked. Their study also revealed that IPv6 DoE resolvers, particularly for DNS over QUIC (DoQ) and DoH, exhibited better reachability than their IPv4 counterparts. As an underlying measurement technique, they used *ZMap* probing the IPv4 address space on ports Transmission Control Protocol (TCP)/853 (DoT), TCP/443 (DoH/2), User Datagram Protocol (UDP)/443 (DoH/3), and UDP/853 (DoQ). While it is possible to directly check for valid DNS resolver service in the case of DoQ and DoT, they mentioned it is challenging in the case of DoH due to the more complex configuration needed, leading to the same probing configuration as in their previous study [41]. They also classified various blocking types and claimed their dataset to be the most comprehensive on DoE resolvers to date. Finally, they pointed out the lack of a standardized method for clients to discover DoE configuration details for open resolvers. In a related DDR scan, they identified around 317K DDR-enabled resolvers, with 77 % redirecting to *Google* and 12 % to *Cloudflare*. However, neither did they analyze the DDR results in detail (e.g., priorities of advertised DoE protocols, DoE configurations, discrepancies between DDR configuration and real-world, validating advertised DoE resolvers, security considerations, etc.) nor did they conduct a long-term DDR scan.

## 2.6 DNS Centralization

While DoE enhances the security and privacy of DNS queries by preventing eavesdropping and machine-in-the-middle attacks, it also contributes to DNS centralization. Unlike traditional Do53, where clients use local resolvers (often set via DHCP), DoE protocols frequently route queries to centralized architectures, concentrating user data with a few third-party providers [26, 31, 41–43]. This trend poses risks to both the decentralized nature of the Internet and user privacy [26].

Doan et al. [15] measured latency differences between public DoE cloud providers and ISP resolvers using RIPE Atlas probes. They found that about one in three users uses at least one public DNS service, with *Google* being the most popular, accounting for roughly 78 % of public cloud usage. While some studies suggest performance benefits as a motivation, Doan et al. [15] showed that public DNS services can sometimes outperform local ISP resolvers in lookup latency. Centralization impacts DNS resilience and performance. The Internet's robustness depends on diversity, but centralization increases the risk of single points of failure [39]. Moreover, performance can degrade if DoE resolvers lack nearby infrastructure, as accurate client-to-replica mapping becomes difficult [39, 52]. To address these concerns, several works [22, 26, 39] propose distributing DNS queries across multiple pre-configured DoE resolvers. Such approaches prevent any single resolver from reconstructing a user's full query history, enhancing privacy and decentralization. However, large-scale, unified discovery and configuration of diverse DoE endpoints remains challenging. In this context, if widely and properly implemented, DDR could help foster decentralization.

## 3 Methodology

In this section, we present the rationale for developing a custom measurement platform, including our tailored measurement approach, in response to the limitations of existing datasets and tools in addressing our specific research questions (see Section 1). Our platform is capable of discovering IPv4 addresses running potential DNS services via *ZMap* [18], downloading the latest responsive IPv6 addresses from *IPv6 Hitlist Service* [19, 65] on a daily frequency, and executing DDR probes in time to prevent bias through IP address churn [38]. Based on the DDR responses, it can schedule follow-up scans, including DoE probes and TLS certificate scans, to analyze the broader DDR ecosystem.

While datasets like *OpenINTEL* [? ], *DNS Coffee* [44], and *DNSDB* [? ] offer valuable insights into DNS traffic and records, they lack information about IP addresses or hosts running DNS services, nor do they collect SVCB ResRs, which are essential for studying the DDR protocol. *Censys* appeared to be the closest match as a starting point, which provides daily snapshots of the entire Internet, including DNS hosts. However, the prohibitive costs associated with querying their data via *Google BigQuery*, coupled with unsuccessful negotiations for smaller, more specific datasets, made this option unfeasible for us. As a result, we were compelled to discover IPv4

DNS servers ourselves, while relying on *IPv6 Hitlist Service* for UDP/53 responsive IPv6 addresses.

Existing DNS measurement tools, such as *ZDNS* [33], *dnsrecon* [55], and *MassDNS* [3]. However, effective for scanning for common DNS records such as A or MX ResRs, do not support large-scale scanning of IP addresses for SVCB ResRs, which are vital for our research. Integrating the required functionality into their complex codebases would be inefficient compared to the simplicity offered by lightweight DNS libraries like *miekg/dns* [20] in Go. Furthermore, *ZMap* already provides modules to discover potential DNS servers, so our platform only needed to extend this by adding DDR probes and DoE scans, making it both efficient and adaptable in the context of our research.

We compare our measurement architecture and findings regarding found DNS servers, response times, and retry strategy on a meta-level with existing research and databases, validating our methodology. Acknowledging the responsibility of large-scale measurements, particularly regarding potential impacts on networks and privacy, we incorporate ethical considerations drawn from established best practices and guidelines, as discussed in Section 3.3. To address the research questions outlined in Section 1, we developed an open-source, adaptable, and highly scalable three-stage, fully containerized and monitored measurement architecture written in Go. Go is a fast programming language, provides an active community, well-maintained libraries for DNS [20], and supports lightweight but highly efficient threads (*Goroutines*) for parallel execution.

Our measurement architecture covers multiple standards, includes our own DNS authoritative name servers, and follows a three-stage measurement approach. In the first stage, we collect responsive IPv4 and IPv6 addresses on port UDP/53. In the second stage, these addresses are used to discover DDR-enabled resolvers and their delegated encrypted resolvers. Finally, in the third stage, we query these encrypted resolvers using the respective DoE protocols and query for other protocols like DNSSEC as well. To facilitate a more fine-grained analysis of the results, we enhance the collected dataset by incorporating Autonomous System (AS)-related data (see Table 6).

## 3.1 RFCs, Scans and their Relation

Our architecture implements several standards (RFCs), as illustrated in Figure 2. Initially, we use *ZMap* [18] and the *IPv6 Hitlist Service* [19, 65] to gather IP addresses that respond on UDP port 53. These addresses are then processed by our DDR scanner. If the server replies with any DNS response, we schedule Pointer Record (PTR) and fingerprinting scans to track the discovered servers over time. In cases where the DNS server replies with a DDR response, the system parses the information and schedules DoE scans based on the advertised encrypted resolvers and their associated protocols. We establish a tree-like data structure to interconnect scans, with the DDR scan as the root node. This structure allows us to trace relationships between scans, such as tracking which DoE scan followed a particular DDR scan or which certificate belongs to a specific DoE scan.

We implement a caching mechanism to avoid redundant scans of known encrypted resolvers. This ensures that DoE scans are only
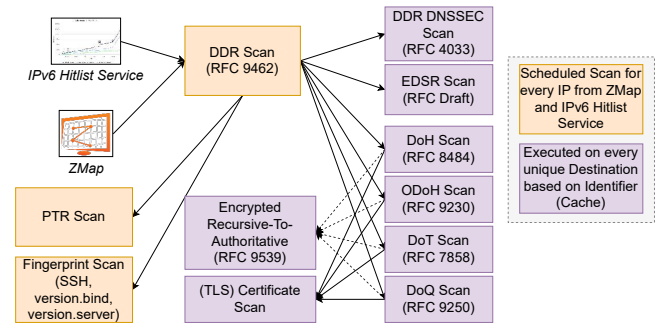


**Figure 2: Relation of standards (RFCs) and their scheduled scans in our measurement architecture.**

performed for newly discovered encrypted resolvers, reducing the amount of disk space required for measurement results and the overall network traffic. Further, this reduces the likelihood of being blocked by RRs. To maintain the tree-like structure, we link the root (DDR) scan with the corresponding DoE, certificate, and DNSSEC scans from the cache. Since DoE protocols rely on TLS, every DDR scanner schedules separate scans to collect certificate information about the encrypted resolver. These are executed in a dedicated scan using Go's *crypto/tls* library, as not all connection handlers (e.g., Go's QUIC (QUIC) implementation) support certificate extraction from an established connection. This ensures that every stored certificate follows a consistent scheme. Additionally, we set the Server Name Indication (SNI) to the hostname of the advertised DoE resolver (targetName) to signal to the server which certificate to return for the requested domain.

## 3.2 Software and Dataset

In order to promote reproducibility and facilitate ongoing research, the measurement tool DoE-Hunter [63], along with the corresponding research study dataset, has been made available to the public online [64].

## 3.3 Ethical Considerations

In conducting our measurements, we adhere to established best practices and guidelines [2, 5, 40, 48, 70] to ensure responsible and ethical research. We do not collect user-related or personally identifiable information to mitigate privacy concerns. Our focus is solely on gathering publicly resolvable data regarding DNS servers' DDR and DoE configurations, without attempting to elicit user-specific data. We do not seek to exploit or circumvent systems with inadequate security. To avoid overloading servers with excessive measurement traffic, we limit our DNS server discovery frequency to twice per week. Furthermore, we implement a caching mechanism to prevent multiple queries for the same DoE resolver, thereby reducing unnecessary traffic. By using well-established scanning tools such as *ZMap* [18] and data from *IPv6 Hitlist Service* [19, 65], we ensure that our measurements do not overwhelm networks. For instance, *ZMap* employs a permutation approach, which randomly selects IP addresses to scan rather than following a sequential numerical order, thus preventing concentrated network load [18]. We have also proactively configured our scanner nodes

and the authoritative name servers to ensure that our measurements are transparent and traceable. This includes adding relevant TXT ResRs and reverse DNS entries to the DoE probes, linking to a web page that explains our measurement approach and provides contact information.

## 3.4 Discovery and Probing of DNS Resolvers

We gather IPv4 and IPv6 DNS resolvers by performing large-scale scans using *ZMap* and the *IPv6 Hitlist Service*. For IPv4, *ZMap* identifies publicly available DNS servers by resolving the A record for *www.google.com*. For IPv6, we use the *Hitlist-Downloader* to automate the retrieval of responsive IPv6 addresses. In the second stage, we discover DDR-enabled resolvers by querying the SVCB ResR with the query name _.dns.resolver.arpa. The DDR scanner runs multiple threads in parallel to keep up with the hit rate of *ZMap*. Each scan result is stored in MongoDB for later analysis. If a DNS server supports DDR, we schedule DoE scans according to the advertised designated encrypted resolvers. In the final stage, we execute DoE probes and additional scans using dedicated consumers that pull scheduled scans from Apache Kafka. Each scan queries a unique A ResR to correlate recursive-to-authoritative communications. We set a ten-second timeout for DoE probes and schedule new scans if a resolver fails to provide a valid certificate.

Our measurements are limited to DNS resolvers that are accessible from the public Internet via our VP on a university network. As a result, we do not capture (recursive) resolvers that are hidden from the public, such as ISP-operated resolvers that exclusively serve their customers or DNS servers located within private networks, nor do we include servers that do not respond to requests from external networks.

## 3.5 Change Rates, Response Patterns and Trends

Over four months, from 12 July 2024 to 11 November 2024, we scanned 746.6M IPv4 addresses that potentially offer DNS services. For the IPv4 address space, *ZMap* covered 3.7B addresses for each scan run, yielding an average hit rate of about 0.8 %. Consequently, each run resulted in an average of around 29.9M IPv4 servers potentially running a DNS service. These results are not necessarily actual DNS servers, as *ZMap* counts any response as a "hit", including non DNS-services that reply to DNS probes. Using *ZMap*'s result set, we conducted DDR discovery queries, which yielded some response from approximately 4M (13.9 %) DNS servers on average. While the number of IPv4 addresses detected by *ZMap* increased from the initial scan in July to the final scan in November, by around 4.9M, the number of actual DNS servers responding remained stable at approximately 4.1M throughout all scans. For IPv6, we conducted DDR discovery queries directly from the set of *IPv6 Hitlist Service*'s responsive IPv6 addresses. In total, we scanned 3.5M IPv6 addresses, while the number of addresses scanned in each run varied due to the fluctuation of *IPv6 Hitlist Service*'s result set. In contrast to the relatively low response rate for IPv4 addresses (13.7 %), an average of 287K (82 %) returned a DNS response. This high response rate is almost the inverse of the IPv4 timeout rate, depicting a reversal in responsiveness between IPv4 and IPv6.

Focusing on the IPv4 DNS servers that replied with any DNS response to the DDR discovery, we observe a shift in DNS Return Codes (RCODEs) between IPv4 Recursive Resolver (v4RR) and IPv4 Non-Recursive Resolver (v4NRR) over time. Specifically, there is an increase in v4NRRs returning NXDOMAIN (non-existing domain), rising from around 1.2 % (35K) in the first scan to 13.3 % (406K) in the latest scan. This trend likely reflects the fact that DDR is primarily standardized for RRs [53], meaning that authoritative name servers are not the intended targets of the protocol. Similarly, we see a rise in SERVFAIL (server failure) responses from v4NRRs, increasing from around 33K (1.2 %) in September to approximately 159K (5.2 %) by mid-November. Conversely, the portion of REFUSED responses from v4NRRs decreased, from 2.5M (86.6 %) to 2.2M (70.7 %). The number of NOERR (no error) replies remained stable. Interestingly, the RCODE distribution for v4RRs (the target group for the DDR protocol) was relatively stable across scans. Notably, while v4RRs returned NOERR in about 379K (34.5 %) responses on average, v4NRRs returned this RCODE in only about 163K responses (5.5 %). This indicates that v4RRs are more likely to successfully respond to DDR discovery queries than v4NRRs, highlighting again DDR's focus on RRs. Additionally, v4NRRs refused the DDR discovery in 2.2M responses (75 %) on average, compared to only 64K (5.8 %) refusals from v4RRs per scan.

We observe a different RCODE distribution for IPv6 DNS servers compared to IPv4. For instance, IPv6 Recursive Resolver (v6RR) returned NOERR in only about 16 % of the responses, compared to around 35 % for IPv4, indicating that v4RRs are more familiar with DDR discovery queries than v6RRs. Similar to IPv4 resolvers, we see an increasing trend of IPv6 Non-Recursive Resolver (v6NRR) returning NXDOMAIN and a declining trend in REFUSED responses. Initially, around 4K (1.6 %) v6NRRs returned NXDOMAIN, which rose to 28K (14.9 %) by the final scan. For REFUSED responses, about 240K (94.9 %) of v6NRRs returned this code in the first scan, which dropped to around 152K (80.7 %) by the last scan. In general, it appears that v6RRs exhibit greater instability in RCODEs distribution over time compared to IPv4 resolvers.

## 3.6 IP-based Verified Discovery

When DoE resolvers are discovered via their IP address, the DDR standard recommends the *Verified Discovery* method. This requires clients to validate the resolver's certificate and confirm the resolver's IP is listed in the SAN field of the TLS certificate. The standard explicitly states that if these checks fail, "[...] the client MUST NOT automatically use the discovered Designated Resolver if this designation was only discovered via a _dns.resolver.arpa. query" [53]. Our scans from November 2024 show very low compliance: only 2.02 % of IPv4 and 9.5 % of IPv6 TLS certificates include the IP in the SAN. Among hundreds of thousands of DDR-to-DoE resolver pairs, fewer than 0.005 % pass Verified Discovery. Major cloud providers (*Google*, *Cloudflare*, *Cisco*, *Quad9*) are fully compliant, as their resolvers reference themselves. Outside these, only a handful of organizations host compliant configurations.

This widespread non-compliance severely limits automatic upgrades to encrypted resolvers, which are generally only feasible when clients use major cloud providers' IPs. Clients relying on ISP-assigned resolvers face barriers, since many ISPs delegate to

large clouds (see Section 5.3). Without proper verification, clients risk redirection attacks (*DNS Hijacking* [1]) and privacy breaches if redirected to rogue servers. DDR also increases the attack surface by specifying connection details (e.g., *dohpath* for DoH), which attackers could manipulate to redirect or trigger harmful requests without user awareness, thus amplifying risks beyond unencrypted DNS.

## 4 Analysis of Discovered DoE Resolvers

In this section, we examine the deployment of DoE resolvers, analyzing their global distribution, connection failures across five categories, and operational nuances of DoE protocols. We also assess TLS versions, cipher suites, and Mutual Transport Layer Security (mTLS), offering insights into the security of the TLS layer in DoE resolvers.
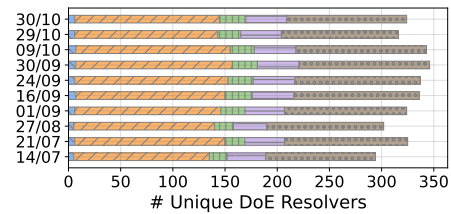
### 4.1 Unique DoE Resolvers

During our DDR discovery study, we found 3288 unique DoE resolvers. A unique DoE resolver is defined as one that is advertised with a distinct domain name (target) in a DDR configuration. Figure 3 shows the number of unique DoE resolvers per measurement, which also breaks down the resolvers by protocol and origin, i.e., whether the DoE resolver was discovered through an IPv4 or IPv6 DDR-enabled resolver.

Breaking this down by protocols, we identified 566 DoH/1.1, 2935 DoH/2, 596 DoH/3, 3064 DoQ, and 711 DoT resolvers. It is important to note that a single unique DoE resolver may support multiple protocols, so the sum of individual protocols does not equal the total number of discovered unique DoE resolvers. The number of DoQ resolvers stands out: while our analysis of DDR configurations revealed that DoQ is relatively infrequently advertised, the number of unique DoQ resolvers is the highest among all DoE protocols. It is comparable to the number of unique DoH/2 resolvers, which is the most frequently advertised DoE protocol by DDR-enabled resolvers. This discrepancy arises because, although there is a similar number of distinct DDR configurations offering DoQ and DoH/2, the most common DDR configuration for DoH/2 was observed approximately 6.1M times throughout all of our measurements, whereas the most frequent configuration for DoQ was seen only about 22K times. This suggests that while there is a wide variety of DoQ resolvers, they are advertised much less frequently.

Notably, our dataset of unique DoQ resolvers constitutes the most extensive collection of DoQ resolvers by Authentication Domain Name (ADN) identified and analyzed in any comparable study to date. This dataset provides a unique opportunity to analyze DoQ adoption and deployment in the wild and investigate the performance and reachability of DoQ resolvers. Incorporating the temporal dimension into the analysis of unique DoE resolvers reveals an increase in the number of DoE resolvers discovered through IPv4 DDR-enabled resolvers during our measurements. This growth is primarily driven by new DoQ resolvers (rising from 1157 to 1580) and DoH/2 resolvers (increasing from 1152 to 1524). Interestingly, the legacy protocol DoH/1.1 recorded the highest increase at 47.25 % (from 218 to 321) when considering percentage growth. In contrast, we do not observe this growth trend among unique DoE resolvers discovered through IPv6 DDR-enabled resolvers.
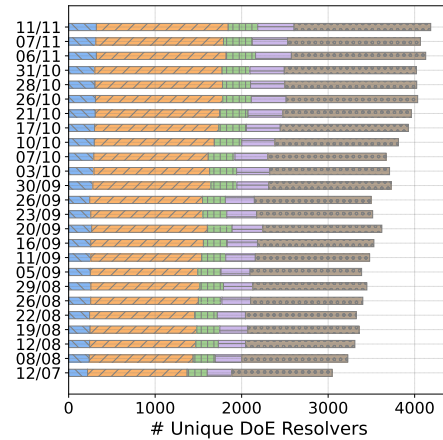


**(a) Number of DoE resolvers discovered by IPv4 DDR-enabled resolvers.**



**(b) Number of DoE resolvers discovered by IPv6 DDR-enabled resolvers.**

**Figure 3: Evolution of unique DoE resolvers discovered through IPv4 and IPv6 DDR-enabled servers, separated by respective DoE protocol.**

### 4.2 Global and AS-Level Distribution

The distribution of DoE resolvers indicates that DoQ and DoH/2 resolvers are the most globally dispersed, whereas the remaining protocols show fewer points, with many servers concentrated in the same locations. For instance, all 566 DoH/1.1 resolvers map to only three locations (Canada, Cyprus, Ireland), while the 3064 DoQ resolvers are spread across 72 countries. Similarly, DoH/2 resolvers are distributed across 71 countries, whereas the 711 DoT resolvers span only 14 countries, with none located in China.

Focusing on the ASes hosting the DoE resolvers, we observe that for each DoE protocol, the majority of resolvers are hosted in *AS 212772* (*AdGuard*). Notably, more than 95 % of unique DoH/1.1 resolvers and over 91 % of unique DoH/3 resolvers reside in this AS. In contrast, DoQ resolvers demonstrate greater AS diversity, with only 17.68 % of resolvers hosted by *AdGuard*. We observe the highest AS diversity among DoQ and DoH/2 resolvers are distributed across more than 479 ASes. In comparison, DoT and DoH/3 resolvers are confined to only 33 and 17 ASes, respectively.

### 4.3 Errors and Reliability

We systematically logged and categorized all errors encountered during our measurements to assess the reliability of advertised DoE

resolvers. Errors were grouped into five main categories: Connection, TLS, HTTP, DNS, and non-zero RCODE values. The most common issues were connection failures, such as unresolved hostnames, unreachable hosts, timeouts, and TLS errors, including expired or invalid certificates. HTTP errors, particularly 4xx and 5xx status codes, also contributed to the resolver unreliability.

We observed 44 distinct error types, reflecting the technical diversity and challenges in DoE deployments. Error trends varied by protocol: DoH/1.1, DoH/3, and DoT resolvers were generally reliable, successfully answering over 93 % of queries. In contrast, DoH/2 and DoQ resolvers exhibited much higher error rates, with frequent connection and TLS failures. For these protocols, the majority of errors were due to connectivity issues, often caused by timeouts, and a significant portion of TLS errors resulted from expired or untrusted certificates.

Interestingly, many of the problematic DoQ and DoH/2 resolvers were hosted within large ASes such as Cloudflare, though it remains unclear whether the provider directly operates these or uses its infrastructure. Overall, our findings highlight that, despite the growing adoption of encrypted DNS, a notable fraction of DDR-advertised resolvers are still misconfigured or unreliable, potentially undermining the benefits of automatic protocol upgrades for end users. Table 1 shows the overall error distribution for each DoE protocol. The evolution of these errors over time is presented in Figure 4 for the DoE resolvers discovered via IPv4 and IPv6 DDR-enabled resolvers throughout our measurements.

It is concerning not only that DDR configurations often point to resolvers that are unreachable, but also that many DoQ and DoH/2 resolvers experience issues establishing secure connections via TLS. Approximately 16 % of DoQ errors and 20 % of DoH/2 errors are attributed to TLS issues. For all TLS errors we observed with DoQ, certificate-related problems are the root cause: in 78 % of cases, the certificate is expired, 18 % are signed by an unknown Certificate Authority (CA) (self-signed or expired TLS certificates), and the remaining cases involve invalid certificates (e.g., mismatched signatures). For DoH, while expired certificates account for only 66 % of TLS issues, we could identify eight different TLS errors.

Finally, we examine DNS responses with non-zero RCODEs. Over 87 % (1045) of these cases returned a *Refused* RCODE, indicating that the DoE resolver rejected the query. Similar to the 404 HTTP status code, this error may indicate a discrepancy between the DDR configuration and the actual server configuration, as the DDR configuration points to a DoE resolver that refuses to resolve the requested resource. DoH/1.1, DoH/3 and DoT resolvers returned this RCODE in more than 98 % of the non-zero RCODE cases, while DoH/2 and DoQ resolvers returned it in 86 % and 80 % of cases, respectively. Notably, in 33 cases (2.75 %), the RCODE is *NXDomain*, which is unusual since the requested resource remains available on our authoritative name servers throughout the entire measurement period without any downtime. Yet, the resolver claimed the non-existence of the requested resource. These responses originated from servers in Taiwan and Singapore. The exact cause of this error remains unclear. The remaining RCODEs *FormErr* and *ServFail* occurred in 10 % (33) and 0.083 % (1) of all requests, respectively.
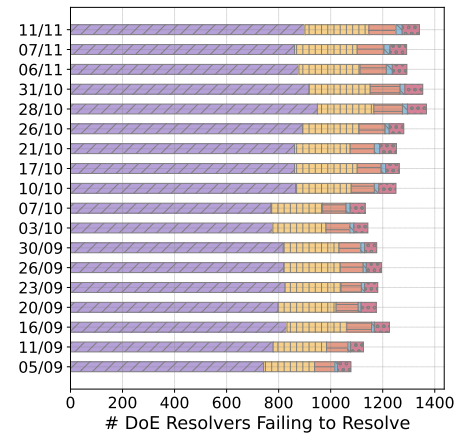


**(a) Error distribution of DoE resolvers discovered by IPv4 DDR-enabled resolvers.**
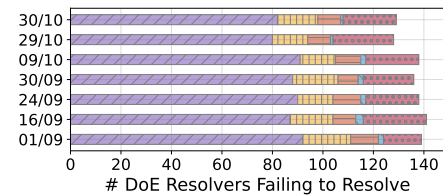


**(b) Error distribution of DoE resolvers discovered by IPv6 DDR-enabled resolvers.**

**Figure 4: Evolution of the encountered error categories of all DoE resolvers. The upper figure shows the error distribution across DoE resolvers discovered by IPv4 DDR-enabled resolvers, while the lower one depicts the distribution across DoE resolvers discovered by IPv6 DDR-enabled resolvers.**

## 4.4 TLS Analysis

Our measurement architecture also tracks information that is negotiated on the TLS layer during connection establishment, i.e., negotiated TLS version and cryptographic protocols (cipher suites), and whether DoE resolvers require clients to present a certificate (mTLS) [34]. During probing, we support TLS versions greater than or equal to 1.0 and all available cipher suites, regardless of the DoE protocol. The DoE resolver then selects the most appropriate TLS version and cipher suite, as described in the relevant TLS standards [11–13, 58].

None of the DoE resolvers required clients to present a certificate during the TLS handshake, i.e., mTLS. This behavior aligns with an early IETF draft, which defines mTLS in the context of DoE protocols and specifies that DoE resolvers must not offer client authentication for connections established through prior discovery via DDR [34]. Consequently, all the DoE resolvers we discovered adhere to the specifications outlined in this early draft. All DoE resolvers negotiate either TLS 1.2 or TLS 1.3. Notably, every connection to DoH/1.1 and DoT resolvers uses TLS 1.3. Since QUIC's handshake is based on TLS 1.3 [32, 69], DoQ and DoH/3 connections

**Table 1: Distribution of error categories per DoE protocol. Percentages show each category's share of total errors.**

| Protocol | # Req. | # Errors | Connection | TLS | HTTP | DNS | RCODE != 0 |
|----------|--------|----------|------------|-----|------|-----|------------|
| DoH/1.1 | 6055 | 70 (1.16 %) | 15 (21.43 %) | 1 (1.43 %) | 1 (1.43 %) | - | 53 (75.71 %) |
| DoH/2 | 27 758 | 10 713 (38.59 %) | 6052 (56.49 %) | 2187 (20.41 %) | 1638 (15.29 %) | 300 (2.80 %) | 536 (5.00 %) |
| DoH/3 | 6606 | 317 (4.80 %) | 126 (39.75 %) | 30 (9.46 %) | 107 (33.75 %) | 1 (0.32 %) | 53 (16.72 %) |
| DoQ | 27 074 | 11 433 (42.23 %) | 9204 (80.50 %) | 1857 (16.24 %) | - | - | 372 (3.25 %) |
| DoT | 7806 | 545 (6.98 %) | 360 (66.06 %) | - | - | - | 185 (33.94 %) |

also consistently use version 1.3. For DoH/2, TLS 1.3 is negotiated in over 99 % of cases. We classified all negotiated cipher suites using the *Ciphersuite.info API* [? ]. We only observed recommended or secure cipher suites. The most commonly negotiated cipher suite is TLS_AES_128_GCM_SHA256, which is used in over 94 % of TLS connections, followed by TLS_AES_256_GCM_SHA384 (3 %) and TLS_CHACHA20_POLY1305_SHA256 (2 %). In all cases, Diffie-Hellman key exchange is executed to determine the session key. These results do not imply that DoE resolvers are inherently secure in terms of TLS configurations. According to the standards [13, 58], the highest TLS version supported by both parties is selected, while the choice of cipher suite typically depends on the server operator and their security policies. Our measurements do not include probes to determine whether DoE resolvers support insecure TLS versions or cipher suites.

## 5 DDR Adoption Among DoE Resolvers

If the hostname of a DoE resolver is known, DDR can be utilized to discover its current configuration through the *discovery using resolver (domain) names* method (see Section 2). To perform this analysis, we executed DDR using this discovery method on all 3204 unique DoE resolvers identified during the second stage of our measurements. Of these resolvers, 626 (19.54 %) responded to the DDR discovery query. However, 601 (96 %) of the responses contained invalid DDR configurations, missing mandatory keys such as the priority.

Interestingly, among the resolvers providing invalid DDR configurations are DoE resolvers from *AdGuard*, whose hostnames follow the pattern *.d.adguard-dns.com. *Quad9*, in contrast, does not provide any DDR configuration for its DoE resolvers. Analyzing the remaining 25 DoE resolvers with valid DDR configurations, we observe that they all delegate to themselves. This behavior is expected, as these DoE resolvers already offer DoE protocols on the same host. Among these 25 resolvers, two belong to our DDR-enabled resolvers and measurement architecture. Notably, 18 of the 25 resolvers belong to major DNS cloud providers, including *Google*, *Cloudflare* and *Cisco*.

### 5.1 Name-based Verified Discovery and DNSSEC

When clients use the *discovery using resolver (domain) names* method, the DDR standard [53] requires them to verify the hostname's presence in the TLS certificate of the advertised resolvers (see Section 2.2). All 25 DDR-enabled DoE resolvers comply with this requirement, including their hostname in the TLS certificates. This is because they do not delegate outside their own AS, as observed in most of the DDR configurations (see Section 5.3), but delegate to themselves.

Another non-standard method to validate DDR configurations discovered by the *discovery using resolver (domain) names* method is DNSSEC. However, DNSSEC applies only to *discovery using resolver (domain) names*, as these records exist within the public DNS hierarchy, enabling resolvers to sign and clients to validate them. Among the 626 resolvers that responded to our DDR discovery queries, only 24 (3.83 %) implement DNSSEC. While this adoption rate remains low, it is marginally higher than the rates reported in recent studies [8]. Further, 8 of the 25 DDR-enabled DoE resolvers returning a valid configuration have DNSSEC enabled (32 %). Of the 17 having no DNSSEC support, 11 belong to *Cisco* and two to *AdGuard*. We want to note that we did not validate the returned signatures. In general, further research is necessary to evaluate the cryptographic robustness of the signature and the reliability of client-side validation for both the DNSSEC signatures in the context of DoE and DDR's verification method, as in general DNS only a small ratio of resolvers validate signatures [8].

Although many DoE resolvers provide non-compliant configurations, clients have viable options for validating DDR responses retrieved via the discovery using hostnames. All DoE resolvers offering a valid DDR configuration theoretically passes the verification methods defined by the standard, and some resolvers additionally leverage DNSSEC for enhanced authenticity validation.

### 5.2 Delegation Trends across Network Categories

To better understand how DDR-enabled resolvers are configured across different network categories, we analyze the distribution of configurations concerning the most offered DoE target delegations (alternative domains). The results, depicted in Table 6, present the alternative domains of IPv4 and IPv6 DDR-enabled resolvers, sorted by the total number of occurrences. To gain further insights, we also provide the relative proportions of each configuration within its respective network category. We only consider the latest available measurement results for this analysis, as DDR configurations exhibited minimal changes over our measurement period. This is different from Section 5.3, where we focus on the most common configurations, we now analyze the distribution of alternative domains within each DDR configuration, as each configuration can have multiple alternative domains (SVCB ResRs) advertised (see Section 2.1).

We observe 1668 unique alternative domains across 902 179 advertisements in configurations of IPv4 DDR-enabled resolvers. The most common alternative domain is dns.google., advertised approximately 700K times (77.63 %), making *Google* the most advertised alternative domain across all network categories. The second

**(a) IPv4 DDR Resolver Delegation Graph**

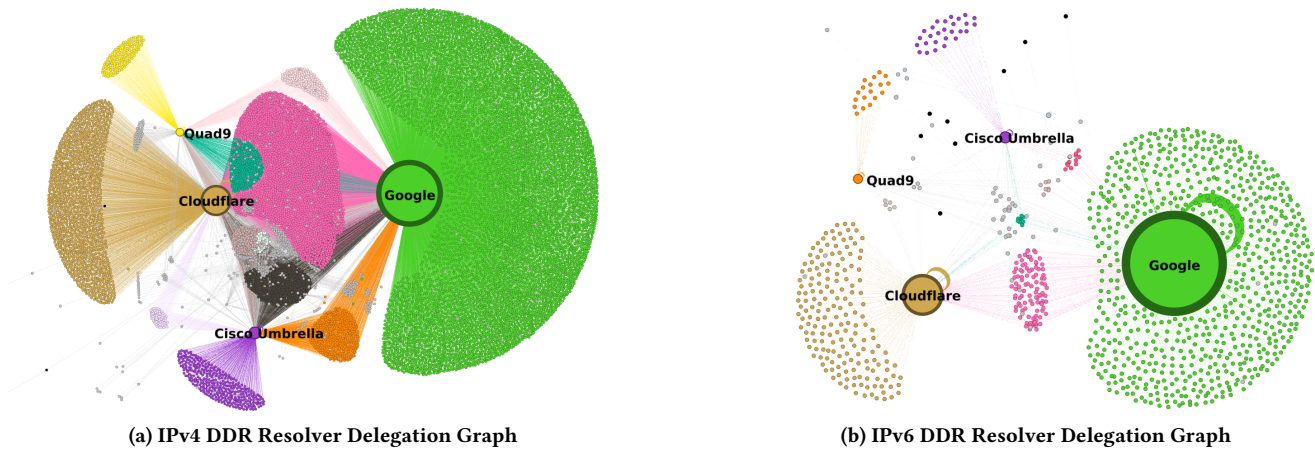**(b) IPv6 DDR Resolver Delegation Graph**

**Figure 5: Nodes represent ASes, while edges illustrate redirections to either the same or a different AS. Colors group DDR-enabled resolvers that share the same configuration in terms of AS target combination. The size of each node reflects the number of incoming edges, representing how many other ASes delegate their clients to that specific AS.**

most common domain is one.one.one.one. from *Cloudflare*, observed 120 420 times (13.35 %), followed by *Cisco*'s .opendns.com and .umbrella.com. In general, these findings align with the AS delegation observations in Section 5.3. Examining the delegations to *Google* across network categories reveals that resolvers classified as Route Servers delegate the most of their clients to *Google* (82 %), while in the case of Educational/Research resolvers, it is only 39.90 %. Network Services resolvers account for the largest number of delegations to *Google*'s DNS, with 402 278 delegations, as they host the most DDR-enabled resolvers. This observation is particularly relevant because Network Services resolvers include ISP resolvers, meaning that their clients, i.e., oftentimes residential broadband consumers, would frequently be redirected to *Google* when automatically upgrading to DoE using DDR. Among all unique IPv4 DDR-enabled resolvers classified as Network Services, only 0.71 % offer at least one entry in their DDR configuration pointing to a DoE resolver within the same AS. For IPv6, this figure is slightly higher at 1.21 %.

In IPv6 DDR-enabled resolvers, we observe 152 unique alternative domains across 23 822 advertisements. Government and Route Server categories are absent, as no IPv6 DDR-enabled resolvers are identified in these categories. IPv6 resolvers delegate to *Google*'s DNS more frequently than IPv4 resolvers, with 83.12 % (19.8K) entries referring clients to *Google*. *Cloudflare* remains the second most common, used by 2.1K (9.17 %) IPv6 resolvers, followed by *Cisco*'s dns.opendns.com and dns.umbrella.com. Similar to the alternative domains in IPv4, resolvers in the Network Services category show a higher tendency to delegate to *Google* in IPv6 (87.76 %) but redirect to *Cloudflare* less frequently (7.58 % versus 14.29 % in IPv4). Additionally, the domain doh.cox.net, associated with Cox, a major U.S. ISP, is notable, though its overall share is low (0.22 %). As a result, these findings highlight the dominance of major DNS cloud providers, particularly *Google*. We can conclude that the current deployment of DDR in-the-wild does not contribute to creating a diversified DoE landscape, but rather supports the centralization of DNS infrastructure.

### 5.3 DNS Centralization through DDR

As prior work has shown (see Section 2), the RR market in DNS — especially with DoE protocols — exhibits signs of DNS centralization [15, 31, 43]. The primary issue with DoE has been the limited options for automatically discovering DoE resolvers and configurations [42]. This challenge is one reason why the IETF standardized DDR, enabling clients to automatically discover encrypted resolvers and their configurations such that an automatic upgrade to encryption protocols is possible. However, the DDR standard states: "[DDR] mechanisms are designed to be limited to cases where unencrypted DNS Resolvers and their Designated Resolvers are operated by the same entity or cooperating entities" [53].

Yet, our measurements show that 97 % of all DDR-enabled resolvers fully delegate to four major cloud DNS providers. This widespread configuration may stem from the major providers' ability to ensure high availability and performance through globally distributed infrastructure [15], their support for DoE protocols enabling encrypted communication without additional deployment efforts, or simply their reputation as trusted entities in the DNS ecosystem. The configurations of major providers are replicated in most DDR-enabled resolvers, suggesting they were directly copied. However, this heavy reliance on cloud providers raises concerns about DNS centralization, where a few entities control a large portion of the recursive resolution process. Such concentration poses risks to user privacy, security, and the broader decentralization of internet governance, as the resolution process is critical to the Internet's integrity and honest functionality.

We analyze the payloads (i.e., DDR configurations) of the 309K IPv4 DDR-enabled resolvers (7.6K IPv6) to investigate their real-world configurations. To identify the most common configurations, we hash and group them by their hash values. In total, we identify 3378 unique configurations among IPv4 DDR-enabled resolvers and 263 among IPv6 ones, indicating low configuration diversity compared to the overall number of DDR-enabled resolvers. The most common configuration is that of Google's cloud DNS service (dns.google.), used by an average of 79.3 % of IPv4 DDR-enabled

resolvers and 82.54 % of IPv6 ones, redirecting to the DoE resolvers of Google. The configuration of *Cloudflare* follows, with 12.17 % (9.73 % IPv6). The third and fourth most deployed configurations are from *Cisco Umbrella (OpenDNS)*. While the third most deployed configuration occurs in 4.46 % (3.33 % IPv6) of cases and delegates to `dns.opendns.com` and `dns.umbrella.com`, the fourth most used configuration delegates to `familyshield.opendns.com` in 0.76 % of the cases (none in IPv6). However, both DoE resolver belong to *Cisco Umbrella*, as the latter one provides additional features like content filtering. The fifth most used configuration is from Quad9, delegating to their servers in 0.72 % (0.99 % IPv6). These five configurations collectively represent over 97 % of all DDR-enabled resolvers' configurations, demonstrating a high degree of consolidation of configurations within the DDR ecosystem. The details of these five most advertised configurations are provided in Section B.

Assuming clients use DDR to upgrade to DoE protocols automatically, the current in-the-wild configurations suggest that DDR-enabled resolvers delegate their resolving activities away from their own AS to other ASes, primarily those of major cloud DNS providers like *Google*, *Cloudflare*, *Cisco*, or *Quad9*. To better understand this delegation, we visualize redirections as a graph network for IPv4 and IPv6 in Figure 5. Nodes represent ASes, while edges illustrate redirections to either the same or different ASes. Colors group ASes with identical AS-target combinations. For example, if all DDR-enabled resolvers within the AS X and AS Y redirect only to *Cloudflare* and *Google*, they share the same color. Only the top eight AS-target combinations are color-coded. The node size reflects the number of incoming edges, indicating how many other ASes redirect their clients to a given AS.

The graph reveals the dominance of *Google*, *Cloudflare*, *Cisco*, and *Quad9*, but also highlights variation in DDR configurations within the same AS. For instance, pink-colored nodes in both figures demonstrate that DDR-enabled resolvers in the same AS may not share identical configurations. This is since the top five most common DDR configurations do not include any configurations jointly offered by *Cloudflare* and *Google*, but at the same time, the pink-colored nodes make up to 17 %. This suggests that there must be DDR-enabled resolvers within the same AS configured with either one or the other configuration.

On a closer look, the graph also shows only a few nodes with self-loops, representing DDR-enabled resolvers that redirect traffic within the same AS without delegating externally. These include the major cloud DNS providers like *Google* and *Cloudflare*, as they offer a DDR configuration targeting themselves. In the IPv4 space, 0.23 % (48) of ASes hosting DDR-enabled resolvers have at least one resolver that does not delegate clients to another AS. For IPv6, this figure is slightly higher at 1.42 % (27). However, considering the absolute number of DDR-enabled resolvers, only 0.69 % (8K) in IPv4 and 1.60 % (327) in IPv6 refrain from redirecting their requests to other ASes. We emphasize that the distributions of configurations observed during our measurement period have shown only negligible changes. For instance, we cannot confirm a shift away from configurations relying on DNS cloud providers towards independently crafted setups delegating to DoE servers within the same organization, as intended by the DDR standard [53].
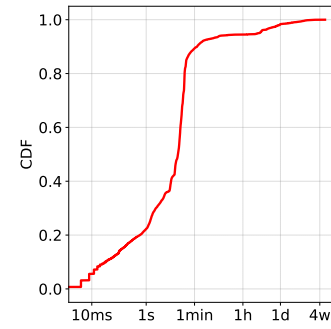


**Figure 6: The CDF considers all replayed DNS queries and their time difference between the first and the last replayed query.**

## 5.4 Traffic Shadowing Behavior

From September 1, 2024, to November 11, 2024, we sent 75 299 uniquely crafted DNS queries to all available DoE resolvers. In the following, we refer to DoE queries as the DNS queries we initially sent to the DoE resolvers during the DoE probing in our methodology. The resources to be resolved by the DoE queries resided on our authoritative name servers. Our name servers received 52 392 of these requests, none of which were logged as errors, meaning our name servers successfully answered every request.

However, we observe a high number of DoE queries that are repeated. The name servers' logs contain 218 352 query requests with our uniquely crafted DNS query names. Approximately 12K of the 49K (22 %) DoE queries are repeated one or more times. Notably, one query (i.e., having the same QNAME) is repeated 5250 times. Tracing these 5250 queries on our name server reveals that they originate from 115 different servers across 15 distinct ASes. Of these servers, 68 (59 %) are located in China, with 33 (28 %) belonging to AS *4837* (*China Backbone*). Based on the organization names associated with these ASes, all but three appear to belong to Chinese companies. Interestingly, 34 requests are replayed by 26 different servers in Google's network (AS *15169*), and 16 requests originate from 13 distinct servers in *Cloudflare*'s network (AS *13335*).

We believe these requests are replayed through *Cloudflare*'s and *Google*'s cloud DNS services. A notable outlier includes 21 requests from four different servers hosted in AS *49544* (*i3D.net B.V.*), which provides servers for video games and is owned by *Ubisoft*, a French video game company. We probed these IP addresses ourselves, and none of these source IP addresses seem to act as open resolvers. The reason why these DNS servers appear to reply to our original DNS queries multiple times remains unclear. We have reported this unusual activity to the company.

We shift the perspective from absolute numbers of repeated DoE queries to their temporal behavior. Specifically, we analyze the time difference between the first and the last repeated DoE query. Figure 6 shows the cumulative distribution function of these time differences. We observe that 50 % of the repeated DoE queries are replayed within 16 seconds. The longest observed period between the first and the last repeated DoE query is 70 days, replaying these queries at irregular intervals. We determine the locations of servers that send more than one DoE query, with a time difference between the first and last query exceeding one day. Since each DoE request

is uniquely identifiable due to its one-time QNAME, we can link the original query to the repeated queries on our name servers.

First, we focus on servers that may have intercepted and replayed our initial DoE queries. These servers are distributed across 20 countries and 59 ASes. Over 22 % are located in China, followed by approximately 15 % in Russia and over 7 % in the United States. However, these servers do not replay the queries themselves; instead, they utilize RRs worldwide to perform the repeated requests. In most cases, RRs from Singapore are used (35 %), followed by China (17 %) and the United States (13 %). On our name servers, we observe queries originating from 36 countries and 109 distinct ASes. In 45 % of the cases, RRs from *Google*'s AS *15169* are used, followed by *Cloudflare* (AS *13335*) with over 8 % and *Yandex* (AS *13238*) with more than 7 %. As a result, most of the queries are intercepted in China, Russia, and the United States, and then mostly replayed through RRs in Singapore through *Google*'s cloud DNS services.

This behavior is described as *traffic shadowing* by Xing et al. [73] and as *DNS Zombies* by Huston [30]. However, our study differs from theirs. Xing et al. analyzed behavior using Do53, HTTP, and TLS, including non-DNS protocols. For Do53, they assumed that transmitted Do53 packets were intercepted and subsequently replayed. We can narrow down the interception possibilities through our methodology (see Section 3). Since we sent queries through secure channels to the DoE resolvers, they cannot be intercepted between the client and the RR. Additionally, the adoption rate of QNAME Minimization (QNAME Min.) has risen to over 50 % in recent years [47], making the interception and replay of our queries on the recursive-to-authoritative connection even less likely. Consequently, it is more plausible that the RRs, which received the initial DoE query, record and replay the queries after some time. However, we suggest further analyses and investigations into the *traffic shadowing* in the context of DoE protocols to understand why this behavior occurs.

## 5.5 Encrypted Recursive-To-Authoritative Communication

Finally, our specially crafted DoE queries enable us to assess the extent to which DoE resolvers use encrypted communication to resolve requested resources over a secure channel. This encrypted *recursive-to-authoritative* communication was standardized by the IETF in March 2024 through the RFC 9539 [21]. To enable encrypted communication with our name servers, we support DoT and DoH/2 in their standard configurations, i.e., DoT on port 853 and DoH/2 on port 443, with DoH/2 receiving DNS queries on the URI path */dns-query{?dns}*. Additionally, our name servers also support DDR to facilitate discovery of these configurations by RRs.

None of the DoE resolvers tried to resolve the requested resource via DoH/2 or DoT. Although the DoE resolvers themselves received DNS queries through a DoE protocol, indicating they have implemented this functionality, they did not use DoE for resolving resources in the public DNS. Moreover, none of the RRs utilized DDR to discover our encrypted endpoints. However, RFC 9539 [21] leaves the choice of using encryption during the recursive resolving process to the RR. This decision is due to the computational and network overhead that encryption adds to each resolving process.

Of particular interest is that RFC 9539 states in the context of DoH: "Currently, there are no mechanisms for a DNS recursive resolver to predict the [*dohpath*] on its own, in an opportunistic or unilateral fashion, without incurring an excessive use of resources" [21]. Yet, DDR was specifically designed for this purpose and was standardized prior to RFC 9539, in November 2023.

## 5.6 Implementation Status of DDR on Resolvers

The predominant use of the same configuration designating the same cloud providers raise the question of why these invalid configurations have been adopted. Table 2 presents open-source resolvers along with their implementation status for DoE protocols and DDR. While DoE enjoys broad adoption, many of the resolvers examined do not offer straightforward methods to configure DDR, nor do they include default settings — except for *AdGuard Home*, which provides automatic DDR configuration. Therefore, the frequent use of identical configurations cannot be attributed to vendor-specific defaults, at least among open-source resolvers.

Implementation of DDR on clients requires further research, as it remains to be seen if clients comply with the standardized verified discovery methods or use discovered DoE resolvers without or with other verification methods.

## 6 Discussion and Conclusion

In this section, we discuss the findings from our study on the adoption rates, configuration patterns, and challenges associated with DDR-enabled resolvers. We address three key RQs to provide a comprehensive understanding of the current state and trends in DDR deployment.

**RQ1**: *What are the adoption rates and trends of public DDR-enabled resolvers in IPv4 and IPv6, and how do they vary across geographical regions and network types over time?* Our study reveals that among the approximately 4M IPv4 DNS servers discovered on average, 7.59 % are DDR-enabled (i.e., return a DDR configuration), compared to only 2.65 % of the 287K IPv6 DNS servers. During the four-month measurement period, IPv4 DDR-enabled resolvers increased by 3.5K, but DDR density declined slightly by 0.14 %, indicating slower relative growth compared to the overall IPv4 DNS population. Conversely, IPv6 experienced a 1K decrease in DDR-enabled resolvers but showed a positive trend in DDR density of 2.8 %, reflecting proportional growth. These trends suggest differing dynamics between IPv4 and IPv6 adoption, though the short measurement period of four months limits the robustness of these conclusions.

Geographically, Asia hosts the most significant number of IPv4 DDR-enabled resolvers (152K, 50.05 %), while Africa leads in DDR density, with 34.46 % of all DNS servers supporting DDR. While Asia, Africa, and Europe saw increases of DDR-enabled servers throughout our measurement period (>3 %), South America and North America experienced declines of −9.05 % and −4.56 %, respectively. The IPv6 space exhibits different patterns. South America dominates the number and density of DDR-enabled resolvers, with Bolivia alone contributing 22.31 % of the global total through 1.8K servers. Further, it achieves an exceptional DDR density of 98.11 %, highlighting its unique role as a leader in IPv6 DDR adoption. By contrast, Europe, despite hosting the most significant number of

**Table 2: Comparison of DNS Resolver Software**

| Name | Description | DoE Support | DDR Behavior |
|---|---|---|---|
| AdGuard Home | Local DNS Proxy for Ad-Blocking | DoT and DoH support | DDR supported, designated to DoE services on the same server |
| BIND9 | Widely used DNS software suite, including DNS resolver | DoT and DoH support | DDR can be configured |
| dnsmasq | Light-weight DNS resolver and proxy | Not supported | DDR is not supported, SVCB queries may be forwarded |
| Pi-Hole | Local DNS Proxy for Ad-Blocking | Not supported | Returns `NODATA` on DDR queries, preventing forwarding |
| Knot Resolver | Open-source DNS resolver | DoT and DoH support | Not supported |
| smartDNS | Local DNS proxy | DoT and DoH support | Not supported |
| unbound | Open-source DNS resolver | DoT, DoH and DoQ support | The `resolver.arpa.` zone is marked as local by default; DDR can be configured |

IPv6 DNS servers, lags in DDR adoption, with IPv4 and IPv6 DDR densities of only 3.47 % and 0.95 %, respectively. On a country level, Bangladesh achieves the highest IPv4 DDR density with 81.89 %.

From a network perspective, DDR-enabled servers are primarily hosted within "Network Services" (e.g., ISP networks), accounting for 58.60 % of IPv4 and 77.37 % of IPv6 DDR-enabled servers. While IPv4 DDR density remains relatively low and stable across ASes, IPv6 networks show a trend towards centralization, meaning IPv6 DDR-enabled servers concentrate within fewer ASes. This trend is particularly pronounced in South America, where the top-performing ASes achieve DDR densities approaching 100 %. Overall, DDR adoption remains uneven across regions, countries, and network types. While some areas stagnate or decline, our findings confirm that DDR adoption is concentrated within networks of ISPs, consistent with the protocol's design focus on *stub-to-recursive* communication (see Tables 3 and 4).

**RQ2:** *What configuration patterns are observed in DDR-enabled resolvers, and how do these patterns differ across networks and over time?* During the measurement period, the configurations of DDR-enabled resolvers exhibited little change, remaining relatively stable over time. However, a key finding is the limited diversity in DDR configurations, with over 97 % of DDR-enabled resolvers delegating their clients to just four major providers: *Google, Cloudflare, Cisco,* and *Quad9. Google*'s dominance is particularly striking, as 79.3 % of IPv4 and 82.54 % of IPv6 DDR-enabled resolvers delegate to its DoE resolver. In contrast, only 0.69 % of IPv4 and 1.60 % of IPv6 DDR-enabled resolvers delegate within their own AS. This overwhelming reliance on a few dominant providers raises concerns regarding DDR's contribution to DNS resolver centralization and its implications for user privacy and governance.

The distribution of advertised DoE protocols reveals that DoH/2, DoT, and DoH/3 are the most commonly supported. The legacy protocol DoH/1.1 remains in use, often associated with delegations to *AdGuard*'s resolvers. Conversely, DoQ adoption remains notably low (<7 %), primarily due to limited support from major cloud DNS providers. However, outside these dominant providers, DoQ shows a more substantial presence in specific network types, particularly in non-profit, content, and enterprise networks (>87 %). In these contexts, DoQ frequently surpasses DoH/3 and DoT in DDR configurations, especially in enterprise and content-oriented networks.

The resulting low DDR configuration diversity results from resolvers replicating the exact configurations used by major DNS cloud providers. This raises concerns that operators may copy these configurations without adapting them to their specific needs (e.g., to their own DoE resolvers). Such practices could inadvertently contribute to DNS resolver centralization, although DDR provides valuable methods to counteract centralization if properly applied.

**RQ3:** *What observable challenges hinder clients from successfully transitioning from plain DNS to DoE protocols in real-world DDR deployments?* Real-world DDR deployments reveal severe challenges that impede clients from transitioning seamlessly from unencrypted DNS (Do53) to DoE protocols. One of the primary hurdles lies in DDR's *IP-based Verified Discovery*, which requires clients to validate TLS certificates and ensure that the DDR-enabled resolver's IP address is listed in the certificate's SAN field. Our analysis shows that this method succeeds in only 75 IPv4 (0.0002 %) and 40 IPv6 (0.0048 %) DDR-to-DoE resolver combinations. Large DNS providers such as *Google* and *Cloudflare* comply with these verification requirements as they delegate to their own DoE resolvers, but the majority of other resolvers, particularly those managed by ISPs, fail to meet these requirements. **Consequently, DDR-compliant clients cannot upgrade to advertised DoE protocols in over 99 % of cases, leaving users vulnerable to privacy risks associated with unencrypted DNS.**

The complexity of DoE protocols introduces additional operational challenges. Across the 44 distinct error types observed, protocols such as DoE/1.1, DoH/3, and DoT exhibited high success rates of 93 % to 98 % during probing, while DoH/2 and DoQ showed elevated error rates of 38.6 % and 42.2 %, respectively. Timeouts were the predominant cause of failure, accounting for over 50 % of DoH/2 errors and 66 % of DoQ errors. HTTP errors in DoH/2 (15 %) and DoH/3 (34 %) were often linked to invalid URI paths, while query refusals (87 % of non-zero RCODEs) reflected misalignments in DDR configurations. Such errors undermine the intended security and privacy benefits of DDR and DoE and showcase discrepancies between DDR configurations and real-world deployments of DoE protocols. Addressing these challenges requires concerted efforts from operators to improve DDR configurations, stricter adherence to protocol specifications, and further research into robust mechanisms for secure and reliable upgrades to encrypted DNS communication.

## Acknowledgments

## References

[1] Gautam Akiwate, Raffaele Sommese, Mattijs Jonker, Zakir Durumeric, kc claffy, Geoffrey M. Voelker, and Stefan Savage. 2022. Retroactive identification of targeted DNS infrastructure hijacking. In *Proceedings of the 22nd ACM Internet Measurement Conference, IMC 2022, Nice, France, October 25-27, 2022*, Chadi Barakat, Cristel Pelsser, Theophilus A. Benson, and David R. Choffnes (Eds.). ACM, 14–32. https://doi.org/10.1145/3517745.3561425

[2] Mark Allman and Vern Paxson. 2007. Issues and etiquette concerning use of shared measurement data. In *Proceedings of the 7th ACM SIGCOMM Internet Measurement Conference, IMC 2007, San Diego, California, USA, October 24-26, 2007*, Constantine Dovrolis and Matthew Roughan (Eds.). ACM, 135–140. https://doi.org/10.1145/1298306.1298327

[3] Birk Blechschmidt. 2016. *GitHub — blechschmidt/massdns: A high-performance DNS stub resolver for bulk lookups and reconnaissance (subdomain enumeration)*. https://github.com/blechschmidt/massdns/ (visited on October 4, 2024).

[4] Mohamed Boucadair, T. Reddy K., Dan Wing, Neil Cook, and Tommy Jensen. 2023. DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR). *RFC* 9463 (2023), 1–23. https://doi.org/10.17487/RFC9463

[5] Vinton G. Cerf. 1991. Guidelines for Internet Measurement Activities. *RFC* 1262 (1991), 1–3. https://doi.org/10.17487/RFC1262

[6] Stuart Cheshire and Marc Krochmal. 2013. Special-Use Domain Names. *RFC* 6761 (2013), 1–13. https://doi.org/10.17487/RFC6761

[7] Rishabh Chhabra, Paul Murley, Deepak Kumar, Michael D. Bailey, and Gang Wang. 2021. Measuring DNS-over-HTTPS performance around the world. In *IMC '21: ACM Internet Measurement Conference, Virtual Event, USA, November 2-4, 2021*, Dave Levin, Alan Mislove, Johanna Amann, and Matthew Luckie (Eds.). ACM, 351–365. https://doi.org/10.1145/3487552.3487849

[8] Taejoong Chung, Roland van Rijswijk-Deij, Balakrishnan Chandrasekaran, David R. Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson. 2017. A Longitudinal, End-to-End View of the DNSSEC Ecosystem. In *26th USENIX Security Symposium, USENIX Security 2017, Vancouver, BC, Canada, August 16-18, 2017*, Engin Kirda and Thomas Ristenpart (Eds.). USENIX Association, 1307–1322. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/chung

[9] Casey T. Deccio and Jacob Davis. 2019. DNS privacy in practice and preparation. In *Proceedings of the 15th International Conference on Emerging Networking Experiments And Technologies, CoNEXT 2019, Orlando, FL, USA, December 09-12, 2019*, Aziz Mohaisen and Zhi-Li Zhang (Eds.). ACM, 138–143. https://doi.org/10.1145/3359989.3365435

[10] Sara Dickinson, Daniel Kahn Gillmor, and Tirumaleswar Reddy. 2018. Usage Profiles for DNS over TLS and DNS over DTLS. *RFC* 8310 (2018), 1–27. https://doi.org/10.17487/RFC8310

[11] Tim Dierks and Christopher Allen. 1999. The TLS Protocol Version 1.0. *RFC* 2246 (1999), 1–80. https://doi.org/10.17487/RFC2246

[12] Tim Dierks and Eric Rescorla. 2006. The Transport Layer Security (TLS) Protocol Version 1.1. *RFC* 4346 (2006), 1–87. https://doi.org/10.17487/RFC4346

[13] Tim Dierks and Eric Rescorla. 2008. The Transport Layer Security (TLS) Protocol Version 1.2. *RFC* 5246 (2008), 1–104. https://doi.org/10.17487/RFC5246

[14] Pratyush Dikshit, Jayasree Sengupta, and Vaibhav Bajpai. 2023. Recent Trends on Privacy-Preserving Technologies under Standardization at the IETF. *Comput. Commun. Rev.* 53, 2 (2023), 22–30. https://doi.org/10.1145/3610381.3610385

[15] Trinh Viet Doan, Justus Fries, and Vaibhav Bajpai. 2021. Evaluating Public DNS Services in the Wake of Increasing Centralization of DNS. In *IFIP Networking Conference, IFIP Networking 2021, Espoo and Helsinki, Finland, June 21-24, 2021*, Zheng Yan, Gareth Tyson, and Dimitrios Koutsonikolas (Eds.). IEEE, 1–9. https://doi.org/10.23919/IFIPNETWORKING52078.2021.9472831

[74] ]dnsdb DomainTools. [n. d.]. Introducing DNSDB 2.0 - Passive DNS. https://domaintools.com/products/farsight-dnsdb/ (visited on September 26, 2024).

[17] Zakir Durumeric, David Adrian, Ariana Mirian, Michael D. Bailey, and J. Alex Halderman. 2015. A Search Engine Backed by Internet-Wide Scanning. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-16, 2015*, Indrajit Ray, Ninghui Li, and Christopher Kruegel (Eds.). ACM, 542–553. https://doi.org/10.1145/2810103.2813703

[18] Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. 2013. ZMap: Fast Internet-wide Scanning and Its Security Applications. In *Proceedings of the 22th*

[19] Oliver Gasser, Quirin Scheitle, Sebastian Gebhard, and Georg Carle. 2016. Scanning the IPv6 Internet: Towards a Comprehensive Hitlist. In *Traffic Monitoring and Analysis - 8th International Workshop, TMA 2016, Louvain la Neuve, Belgium, April 7-8, 2016*, Alessio Botta, Ramin Sadre, and Fabian E. Bustamante (Eds.). IFIP. http://dl.ifip.org/db/conf/tma/tma2016/tma2016-final51.pdf

[20] Miek Gieben. 2012. *miekg/dns - DNS library in Go*. https://github.com/miekg/dns/ (visited on October 8, 2024).

[21] Daniel Kahn Gillmor, Joey Salazar, and Paul Hoffman. 2024. Unilateral Opportunistic Deployment of Encrypted Recursive-to-Authoritative DNS. *RFC* 9539 (2024), 1–24. https://doi.org/10.17487/RFC9539

[22] Nguyen Phong Hoang, Ivan Lin, Seyedhamed Ghavamnia, and Michalis Polychronakis. 2020. K-resolver: Towards Decentralizing Encrypted DNS Resolution. In *Proceedings 2020 Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb 2020)*. Internet Society. https://doi.org/10.14722/madweb.2020.23009

[23] Nguyen Phong Hoang, Michalis Polychronakis, and Phillipa Gill. 2022. Measuring the Accessibility of Domain Name Encryption and Its Impact on Internet Filtering. In *Passive and Active Measurement - 23rd International Conference, PAM 2022, Virtual Event, March 28-30, 2022, Proceedings (Lecture Notes in Computer Science, Vol. 13210)*, Oliver Hohlfeld, Giovane Cesar Moreira Moura, and Cristel Pelsser (Eds.). Springer, 518–536. https://doi.org/10.1007/978-3-030-98785-5_23

[24] Paul E. Hoffman and Patrick McManus. 2018. DNS Queries over HTTPS (DoH). *RFC* 8484 (2018), 1–21. https://doi.org/10.17487/RFC8484

[25] Austin Hounsel, Kevin Borgolte, Paul Schmitt, Jordan Holland, and Nick Feamster. 2020. Comparing the Effects of DNS, DoT, and DoH on Web Performance. In *WWW '20: The Web Conference 2020, Taipei, Taiwan, April 20-24, 2020*, Yennun Huang, Irwin King, Tie-Yan Liu, and Maarten van Steen (Eds.). ACM / IW3C2, 562–572. https://doi.org/10.1145/3366423.3380139

[26] Austin Hounsel, Paul Schmitt, Kevin Borgolte, and Nick Feamster. 2021. Encryption without centralization: distributing DNS queries across recursive resolvers. In *ANRW '21: Applied Networking Research Workshop, Virtual Event, USA, July 24-30, 2021*. ACM, 62–68. https://doi.org/10.1145/3472305.3472318

[27] Rebekah Houser, Zhou Li, Chase Cotton, and Haining Wang. 2019. An investigation on information leakage of DNS over TLS. In *Proceedings of the 15th International Conference on Emerging Networking Experiments And Technologies, CoNEXT 2019, Orlando, FL, USA, December 09-12, 2019*, Aziz Mohaisen and Zhi-Li Zhang (Eds.). ACM, 123–137. https://doi.org/10.1145/3359989.3365429

[28] Russell Housley, W. Timothy Polk, Warwick Ford, and David Solo. 2002. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. *RFC* 3280 (2002), 1–129. https://doi.org/10.17487/RFC3280

[29] Qing Huang, Deliang Chang, and Zhou Li. 2020. A Comprehensive Study of DNS-over-HTTPS Downgrade Attack. In *10th USENIX Workshop on Free and Open Communications on the Internet, FOCI 2020, August 11, 2020*, Roya Ensafi and Hans Klein (Eds.). USENIX Association. https://www.usenix.org/conference/foci20/presentation/huang

[30] Geoff Huston. 2016. *DNS Zombies - APNIC Blog*. https://blog.apnic.net/2016/04/04/dns-zombies/ (visited on November 11, 2024).

[31] Geoff Huston. 2019. *DNS resolver centrality — APNIC Blog*. https://blog.apnic.net/2019/09/23/dns-resolver-centrality/ (visited on October 2, 2024).

[32] Jana Iyengar and Martin Thomson. 2021. QUIC: A UDP-Based Multiplexed and Secure Transport. *RFC* 9000 (2021), 1–151. https://doi.org/10.17487/RFC9000

[33] Liz Izhikevich, Gautam Akiwate, Briana Berger, Spencer Drakontaidis, Anna Ascheman, Paul Pearce, David Adrian, and Zakir Durumeric. 2022. ZDNS: a fast DNS toolkit for internet measurement. In *Proceedings of the 22nd ACM Internet Measurement Conference, IMC 2022, Nice, France, October 25-27, 2022*, Chadi Barakat, Cristel Pelsser, Theophilus A. Benson, and David R. Choffnes (Eds.). ACM, 33–43. https://doi.org/10.1145/3517745.3561434

[34] Tommy Jensen, Jessica Krynitsky, Jeffrey Damick, Matt Engskow, and Joe Abley. 2024. *Client Authentication Recommendations for Encrypted DNS*. Internet-Draft draft-jaked-cared-00. Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-jaked-cared/00/ Work in Progress.

[35] Liang Jiao, Yujia Zhu, Baiyang Li, and Qingyun Liu. 2023. Measuring DNS-over-Encryption Performance Over IPv6. In *22nd IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2024, Exeter, UK, November 1-3, 2023*, Jia Hu, Geyong Min, Guojun Wang, and Nektarios Georgalas (Eds.). IEEE, 444–451. https://doi.org/10.1109/TRUSTCOM60117.2023.00075

[36] Lin Jin, Shuai Hao, Haining Wang, and Chase Cotton. 2021. Understanding the Impact of Encrypted DNS on Internet Censorship. In *WWW '21: The Web Conference 2021, Virtual Event / Ljubljana, Slovenia, April 19-23, 2021*, Jure Leskovec, Marko Grobelnik, Marc Najork, Jie Tang, and Leila Zia (Eds.). ACM / IW3C2, 484–495. https://doi.org/10.1145/3442381.3450084

[37] Mike Kosek, Luca Schumann, Robin Marx, Trinh Viet Doan, and Vaibhav Bajpai. 2022. DNS privacy with speed?: evaluating DNS over QUIC and its impact on web performance. In *Proceedings of the 22nd ACM Internet Measurement Conference, IMC 2022, Nice, France, October 25-27, 2022*, Chadi Barakat, Cristel

Pelsser, Theophilus A. Benson, and David R. Choffnes (Eds.). ACM, 44–50. https://doi.org/10.1145/3517745.3561445

[38] Marc Kührer, Thomas Hupperich, Jonas Bushart, Christian Rossow, and Thorsten Holz. 2015. Going Wild: Large-Scale Classification of Open DNS Resolvers. In *Proceedings of the 2015 ACM Internet Measurement Conference, IMC 2015, Tokyo, Japan, October 28-30, 2015*, Kenjiro Cho, Kensuke Fukuda, Vivek S. Pai, and Neil Spring (Eds.). ACM, 355–368. https://doi.org/10.1145/2815675.2815683

[39] Rashna Kumar and Fabián E. Bustamante. 2021. Decentralization, privacy and performance for DNS. In *SIGCOMM '21: ACM SIGCOMM 2021 Conference, Virtual Event, August 23-27, 2021, Poster and Demo Sessions*, Marco Chiesa, David R. Choffnes, Athina Markopoulou, and Marinho P. Barcellos (Eds.). ACM, 56–58. https://doi.org/10.1145/3472716.3472869

[40] Iain R. Learmonth, Mallory Knodel, and Gurshabad Grover. 2024. *Guidelines for Performing Safe Measurement on the Internet*. Internet-Draft draft-irtf-pearg-safe-internet-measurement-10. Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-irtf-pearg-safe-internet-measurement/10/ Work in Progress.

[41] Ruixuan Li, Xiaofeng Jia, Zhenyong Zhang, Jun Shao, Rongxing Lu, Jingqiang Lin, Xiaoqi Jia, and Guiyi Wei. 2023. A Longitudinal and Comprehensive Measurement of DNS Strict Privacy. *IEEE/ACM Trans. Netw.* 31, 6 (2023), 2793–2808. https://doi.org/10.1109/TNET.2023.3262651

[42] Ruixuan Li, Baojun Liu, Chaoyi Lu, Haixin Duan, and Jun Shao. 2024. A World-wide View on the Reachability of Encrypted DNS Services. In *Proceedings of the ACM on Web Conference 2024, WWW 2024, Singapore, May 13-17, 2024*, Tat-Seng Chua, Chong-Wah Ngo, Ravi Kumar, Hady W. Lauw, and Roy Ka-Wei Lee (Eds.). ACM, 1193–1202. https://doi.org/10.1145/3589334.3645539

[43] Jason Livingood, Manos Antonakakis, Bob Sleigh, and Alister Winfield. 2019. *Centralized DNS over HTTPS (DoH) Implementation Issues and Risks*. Internet-Draft draft-livingood-doh-implementation-risks-issues-04. Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-livingood-doh-implementation-risks-issues/04/ Work in Progress.

[44] Vorsk LLC. 2016. DNS Coffee. https://dns.coffee/ (visited on September 26, 2024).

[45] Chaoyi Lu, Baojun Liu, Zhou Li, Shuang Hao, Hai-Xin Duan, Mingming Zhang, Chunying Leng, Ying Liu, Zaifeng Zhang, and Jianping Wu. 2019. An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come?. In *Proceedings of the Internet Measurement Conference, IMC 2019, Amsterdam, The Netherlands, October 21-23, 2019*. ACM, 22–35. https://doi.org/10.1145/3355369.3355580

[46] Minzhao Lyu, Hassan Habibi Gharakheili, and Vijay Sivaraman. 2023. A Survey on DNS Encryption: Current Development, Malware Misuse, and Inference Techniques. *ACM Comput. Surv.* 55, 8 (2023), 162:1–162:28. https://doi.org/10.1145/3547331

[47] Jonathan Magnusson, Moritz Müller, Anna Brunström, and Tobias Pulls. 2023. A Second Look at DNS QNAME Minimization. In *Passive and Active Measurement - 24th International Conference, PAM 2023, Virtual Event, March 21-23, 2023, Proceedings (Lecture Notes in Computer Science, Vol. 13882)*, Anna Brunström, Marcel Flores, and Marco Fiore (Eds.). Springer, 496–521. https://doi.org/10.1007/978-3-031-28486-1_21

[48] Arvind Narayanan and Bendert Zevenbergen. 2015. No Encore for Encore? Ethical Questions for Web-Based Censorship Measurement. *SSRN Electronic Journal* (2015). https://doi.org/10.2139/ssrn.2665148

[49] Marcin Nawrocki, Pouyan Fotouhi Tehrani, Raphael Hiesgen, Jonas Mücke, Thomas C. Schmidt, and Matthias Wählisch. 2022. On the interplay between TLS certificates and QUIC performance. In *Proceedings of the 18th International Conference on emerging Networking EXperiments and Technologies, CoNEXT 2022, Roma, Italy, December 6-9, 2022*, Giuseppe Bianchi and Alessandro Mei (Eds.). ACM, 204–213. https://doi.org/10.1145/3555050.3569123

[50] Alexandra Nisenoff, Ranya Sharma, and Nick Feamster. 2023. User Awareness and Behaviors Concerning Encrypted DNS Settings in Web Browsers. In *32nd USENIX Security Symposium, USENIX Security 2023, Anaheim, CA, USA, August 9-11, 2023*, Joseph A. Calandrino and Carmela Troncoso (Eds.). USENIX Association, 3117–3133. https://www.usenix.org/conference/usenixsecurity23/presentation/nisenoff-awareness

[74] ]openintelwebsite OpenINTEL. [n. d.]. *Active DNS Measurement Project*. https://openintel.nl/ (visited on September 26, 2024).

[52] John S. Otto, Mario A. Sánchez, John P. Rula, and Fabián E. Bustamante. 2012. Content delivery and the natural evolution of DNS: remote dns trends, performance issues and alternative solutions. In *Proceedings of the 12th ACM SIGCOMM Internet Measurement Conference, IMC '12, Boston, MA, USA, November 14-16, 2012*, John W. Byers, Jim Kurose, Ratul Mahajan, and Alex C. Snoeren (Eds.). ACM, 523–536. https://doi.org/10.1145/2398776.2398831

[53] Tommy Pauly, Eric Kinnear, Christopher A. Wood, Patrick McManus, and Tommy Jensen. 2023. Discovery of Designated Resolvers. *RFC* 9462 (2023), 1–16. https://doi.org/10.17487/RFC9462

[54] T. Reddy K. Tommy Pauly. 2024. Discovery of Oblivious Services via Service Binding Records. *RFC* 9540 (2024), 1–10. https://doi.org/10.17487/RFC9540

[55] Carlos Perez. 2010. *GitHub — darkoperator/dnsrecon: DNS Enumeration Script*. https://github.com/darkoperator/dnsrecon/ (visited on October 4, 2024).

[74] ]rapid7 Rapid7. [n. d.]. *Rapid7 Open Data*. https://opendata.rapid7.com/ (visited on September 26, 2024).

[57] Yakov Rekhter, Bogert G. Moskowitz, Daniel Karrenberg, Geert Jan de Groot, and Eliot Lear. 1996. Address Allocation for Private Internets. *RFC* 1918 (1996), 1–9. https://doi.org/10.17487/RFC1918

[58] Eric Rescorla. 2018. The Transport Layer Security (TLS) Protocol Version 1.3. *RFC* 8446 (2018), 1–160. https://doi.org/10.17487/RFC8446

[74] ]ripeatlas RIPE Network Coordination Centre. [n. d.]. *RIPE Atlas*. https://atlas.ripe.net/ (visited on September 27, 2024).

[74] ]ciphersuiteinfo Hans Christian Rudolph and Nils Grundmann. [n. d.]. *Ciphersuite Info*. https://ciphersuite.info/ (visited on September 6, 2024).

[61] Stefan Santesson. 2007. Internet X.509 Public Key Infrastructure Subject Alternative Name for Expression of Service Name. *RFC* 4985 (2007), 1–10. https://doi.org/10.17487/RFC4985

[62] Steffen Sassala, vasilis ververis, and Vaibhav Bajpai. 2025. A First Look on Discovery of Designated Resolvers. In *2025 IFIP Networking Conference (IFIP Networking)*.

[63] Steffen Sassalla. 2025. *DoE-Hunter*. https://doi.org/10.5281/zenodo.15276648

[64] Steffen Sassalla and Felix Roth. 2025. *Path to Encrypted DNS with DDR: Adoption, Configuration Patterns, and Privacy Implications - Data from DoE-Hunter*. https://doi.org/10.5281/zenodo.15647923

[65] Quirin Scheitle, Oliver Hohlfeld, Julien Gamba, Jonas Jelten, Torsten Zimmermann, Stephen D. Strowes, and Narseo Vallina-Rodriguez. 2018. A Long Way to the Top: Significance, Structure, and Stability of Internet Top Lists. In *Proceedings of the Internet Measurement Conference 2018, IMC 2018, Boston, MA, USA, October 31 - November 02, 2018*. ACM, 478–493. https://dl.acm.org/citation.cfm?id=3278574

[66] Ben Schwartz, Mike Bishop, and Erik Nygren. 2023. Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records). *RFC* 9460 (2023), 1–47. https://doi.org/10.17487/RFC9460

[67] Ranya Sharma, Nick Feamster, and Austin Hounsel. 2022. Measuring the Availability and Response Times of Public Encrypted DNS Resolvers. *CoRR* abs/2208.04999 (2022). https://doi.org/10.48550/ARXIV.2208.04999 arXiv:2208.04999

[74] ]shodan Shodan. [n. d.]. *Shodan*. https://www.shodan.io/ (visited on September 26, 2024).

[69] Martin Thomson and Sean Turner. 2021. Using TLS to Secure QUIC. *RFC* 9001 (2021), 1–52. https://doi.org/10.17487/RFC9001

[70] Jeroen van der Ham. 2017. Ethics and Internet Measurements. In *2017 IEEE Security and Privacy Workshops, SP Workshops 2017, San Jose, CA, USA, May 25, 2017*. IEEE Computer Society, 247–251. https://doi.org/10.1109/SPW.2017.17

[71] Roland van Rijswijk-Deij, Mattijs Jonker, Anna Sperotto, and Aiko Pras. 2016. A High-Performance, Scalable Infrastructure for Large-Scale Active DNS Measurements. *IEEE J. Sel. Areas Commun.* 34, 6 (2016), 1877–1888. https://doi.org/10.1109/JSAC.2016.2558918

[72] Tim Wicinski. 2021. DNS Privacy Considerations. *RFC* 9076 (2021), 1–22. https://doi.org/10.17487/RFC9076

[73] Yunpeng Xing, Chaoyi Lu, Baojun Liu, Haixin Duan, Junzhe Sun, and Zhou Li. 2024. Yesterday Once More: Global Measurement of Internet Traffic Shadowing Behaviors. In *Proceedings of the 2024 ACM on Internet Measurement Conference, IMC 2024, Madrid, Spain, November 4-6, 2024*, Narseo Vallina-Rodriguez, Guillermo Suarez-Tangil, Dave Levin, and Cristel Pelsser (Eds.). ACM, 230–240. https://doi.org/10.1145/3646547.3689023

[74] ]zoomeye zoomeye.ai. [n. d.]. *ZoomEye*. https://www.zoomeye.ai/ (visited on September 26, 2024).

## A   DNS Server Types: Classification and Autonomous Systems Discovery

**Table 3: Classification of v4RR and v4NRR DNS servers by network category for the first and last scan, including the percentage change in the number of DNS servers and ASes.**

### (a) Classification of v4RR servers by network category.

| Category | First Scan 12.07.24 | | Last Scan 11.11.24 | | % Change First to Last | |
|---|---|---|---|---|---|---|
| | # DNS Servers | # ASes | # DNS Servers | # ASes | # DNS Serv. | # ASes |
| Network Services | 656 324 (61.18 %) | 8421 (35.59 %) | 693 919 (59.01 %) | 8375 (35.48 %) | 37 595 (5.73 %) | -46 (−0.55 %) |
| Unknown | 318 288 (29.67 %) | 14 001 (59.18 %) | 318 024 (27.04 %) | 14 011 (59.36 %) | -264 (−0.08 %) | 10 (0.07 %) |
| Content | 66 233 (6.17 %) | 643 (2.72 %) | 66 879 (5.69 %) | 645 (2.73 %) | 646 (0.98 %) | 2 (0.31 %) |
| Educational/Research | 24 749 (2.31 %) | 211 (0.89 %) | 91 132 (7.75 %) | 193 (0.82 %) | 66 383 (268.22 %) | -18 (−8.53 %) |
| Enterprise | 6279 (0.59 %) | 274 (1.16 %) | 5545 (0.47 %) | 276 (1.17 %) | -734 (−11.69 %) | 2 (0.73 %) |
| Non-Profit | 496 (0.05 %) | 72 (0.30 %) | 289 (0.02 %) | 66 (0.28 %) | -207 (−41.73 %) | -6 (−8.33 %) |
| Route Server | 307 (0.03 %) | 9 (0.04 %) | 71 (0.01 %) | 9 (0.04 %) | -236 (−76.87 %) | 0 (0.00 %) |
| Government | 90 (0.01 %) | 27 (0.11 %) | 125 (0.01 %) | 30 (0.13 %) | 35 (38.89 %) | 3 (11.11 %) |
| **Total** | 1072,766 | 23 658 | 1175,984 | 23 605 | 103 218 (9.62 %) | -53 (−0.22 %) |

### (b) Classification of v4NRR servers by network category.

| Category | First Scan 12.07.24 | | Last Scan 11.11.24 | | % Change First to Last | |
|---|---|---|---|---|---|---|
| | # DNS Servers | # ASes | # DNS Servers | # ASes | # DNS Serv. | # ASes |
| Content | 1347,575 (45.84 %) | 1364 (3.55 %) | 1342,896 (43.89 %) | 1369 (3.58 %) | −4679 (−0.35 %) | 5 (0.37 %) |
| Unknown | 864 065 (29.39 %) | 25 493 (66.28 %) | 866 592 (28.32 %) | 25 170 (65.83 %) | 2527 (0.29 %) | -323 (−1.27 %) |
| Network Services | 634 256 (21.57 %) | 10 060 (26.16 %) | 641 475 (20.97 %) | 10 149 (26.54 %) | 7219 (1.14 %) | 89 (0.88 %) |
| Enterprise | 65 783 (2.24 %) | 729 (1.90 %) | 54 270 (1.77 %) | 727 (1.90 %) | −11 513 (−17.50 %) | -2 (−0.27 %) |
| Educational/Research | 24 765 (0.84 %) | 460 (1.20 %) | 150 892 (4.93 %) | 463 (1.21 %) | 126 127 (509.30 %) | 3 (0.65 %) |
| Non-Profit | 2915 (0.10 %) | 274 (0.71 %) | 3009 (0.10 %) | 280 (0.73 %) | 94 (3.22 %) | 6 (2.19 %) |
| Government | 416 (0.01 %) | 54 (0.14 %) | 388 (0.01 %) | 49 (0.13 %) | -28 (−6.73 %) | -5 (−9.26 %) |
| Route Server | 117 (0.00 %) | 26 (0.07 %) | 154 (0.01 %) | 28 (0.07 %) | 37 (31.62 %) | 2 (7.69 %) |
| **Total** | 2939,892 | 38 460 | 3059,676 | 38 235 | 119 784 (4.07 %) | -225 (−0.59 %) |

**Table 4: Classification of v6RR and v6NRR DNS servers by network category for the first and last scan, including the percentage change in the number of DNS servers and ASes.**

### (a) Classification of v6RR servers by network category.

| Category | First Scan 12.07.24 | | Last Scan 30.10.24 | | % Change First to Last | |
|---|---|---|---|---|---|---|
| | # DNS Servers | # ASes | # DNS Servers | # ASes | # DNS Serv. | # ASes |
| Network Services | 84 145 (80.70 %) | 1384 (53.71 %) | 45 144 (74.78 %) | 1247 (53.11 %) | −39 001 (−46.35 %) | -137 (−9.90 %) |
| Unknown | 16 805 (16.12 %) | 851 (33.02 %) | 12 555 (20.80 %) | 795 (33.86 %) | −4250 (−25.29 %) | -56 (−6.58 %) |
| Content | 2353 (2.26 %) | 167 (6.48 %) | 1939 (3.21 %) | 143 (6.09 %) | -414 (−17.59 %) | -24 (−14.37 %) |
| Educational/Research | 674 (0.65 %) | 86 (3.34 %) | 495 (0.82 %) | 83 (3.53 %) | -179 (−26.56 %) | -3 (−3.49 %) |
| Enterprise | 176 (0.17 %) | 48 (1.86 %) | 147 (0.24 %) | 43 (1.83 %) | -29 (−16.48 %) | -5 (−10.42 %) |
| Non-Profit | 109 (0.10 %) | 38 (1.47 %) | 86 (0.14 %) | 35 (1.49 %) | -23 (−21.10 %) | -3 (−7.89 %) |
| Government | 3 (0.00 %) | 3 (0.12 %) | 2 (0.00 %) | 2 (0.09 %) | -1 (−33.33 %) | -1 (−33.33 %) |
| **Total** | 104 265 | 2577 | 60 368 | 2348 | −43 897 (−42.10 %) | -229 (−8.89 %) |

### (b) Classification of v6NRR servers by network category.

| Category | First Scan 12.07.24 | | Last Scan 30.10.24 | | % Change First to Last | |
|---|---|---|---|---|---|---|
| | # DNS Servers | # ASes | # DNS Servers | # ASes | # DNS Serv. | # ASes |
| Content | 122 583 (48.58 %) | 676 (9.27 %) | 94 077 (50.01 %) | 638 (9.61 %) | −28 506 (−23.25 %) | -38 (−5.62 %) |
| Unknown | 76 844 (30.45 %) | 2858 (39.20 %) | 52 293 (27.80 %) | 2531 (38.11 %) | −24 551 (−31.95 %) | -327 (−11.44 %) |
| Network Services | 43 337 (17.17 %) | 3005 (41.22 %) | 33 032 (17.56 %) | 2779 (41.85 %) | −10 305 (−23.78 %) | -226 (−7.52 %) |
| Educational/Research | 5323 (2.11 %) | 335 (4.59 %) | 5173 (2.75 %) | 309 (4.65 %) | -150 (−2.82 %) | -26 (−7.76 %) |
| Enterprise | 2453 (0.97 %) | 200 (2.74 %) | 2103 (1.12 %) | 184 (2.77 %) | -350 (−14.27 %) | -16 (−8.00 %) |
| Non-Profit | 1696 (0.67 %) | 190 (2.61 %) | 1383 (0.74 %) | 177 (2.67 %) | -313 (−18.46 %) | -13 (−6.84 %) |
| Government | 60 (0.02 %) | 15 (0.21 %) | 43 (0.02 %) | 12 (0.18 %) | -17 (−28.33 %) | -3 (−20.00 %) |
| Route Server | 37 (0.01 %) | 12 (0.16 %) | 28 (0.01 %) | 11 (0.17 %) | -9 (−24.32 %) | -1 (−8.33 %) |
| **Total** | 252 333 | 7291 | 188 132 | 6641 | −64 201 (−25.44 %) | -650 (−8.92 %) |

**Table 5: Top 10 ASes by number of DNS servers, including their country and network type.**

**(a) IPv4 DNS server figures as of November 11, 2024.**

| | AS No. | AS Organization | Country | Network Type | # DNS Servers |
|---|---|---|---|---|---|
| 1 | 46606 | UNIFIEDLAYER-AS-1 | United States | Content | 171 793 (4.06 %) |
| 2 | 19551 | INCAPSULA | United States | Content | 160 040 (3.78 %) |
| 3 | 53166 | UNIVERSIDADE ESTADUAL PAULISTA | Brazil | Educational/Research | 126 777 (2.99 %) |
| 4 | 16276 | OVH SAS | France | Content | 99 995 (2.36 %) |
| 5 | 4538 | China Education and Research Network | China | Educational/Research | 90 183 (2.13 %) |
| 6 | 19871 | NETWORK-SOLUTIONS-HOSTING | United States | Unknown | 73 694 (1.74 %) |
| 7 | 24940 | Hetzner Online GmbH | Germany | Content | 70 948 (1.68 %) |
| 8 | 4837 | CHINA UNICOM Backbone | China | Network Services | 67 206 (1.59 %) |
| 9 | 4134 | Chinanet | China | Network Services | 65 729 (1.55 %) |
| 10 | 17488 | Hathway IP Over Cable Internet | India | Network Services | 50 685 (1.20 %) |

**(b) IPv6 DNS server figures as of September 30, 2024.**

| | AS No. | AS Organization | Country | Network Type | # DNS Servers |
|---|---|---|---|---|---|
| 1 | 8966 | Emirates Telecommunications Group | United Arab Emirates | Network Services | 23 691 (9.53 %) |
| 2 | 198066 | Grupo Loading Systems, S.L. | Spain | Unknown | 14 653 (5.90 %) |
| 3 | 16276 | OVH SAS | France | Content | 13 362 (5.38 %) |
| 4 | 205016 | HERN Labs AB | Unknown | Unknown | 9931 (4.00 %) |
| 5 | 20940 | Akamai International B.V. | United States | Content | 7110 (2.86 %) |
| 6 | 19551 | INCAPSULA | United States | Content | 4717 (1.90 %) |
| 7 | 12876 | Scaleway S.a.s. | France | Content | 4408 (1.77 %) |
| 8 | 20857 | Signet B.V. | The Netherlands | Content | 4162 (1.67 %) |
| 9 | 63949 | Akamai Connected Cloud | United States | Content | 4036 (1.62 %) |
| 10 | 4837 | CHINA UNICOM Backbone | China | Network Services | 3595 (1.45 %) |

**Table 6: Top 10 advertised alternative domains of IPv4 and IPv6 DDR-enabled resolvers, categorized by their respective network types. Note that IPv6 DDR-enabled resolvers are distributed across fewer network categories, resulting in fewer columns.**

**(a) IPv4 DDR-enabled resolvers' most advertised alternative domains (November 11, 2024).**

| Alternative Domain | Total | Content | Ed. Research | Enterprise | Govern-ment | Network Services | Non-Profit | Route Server | Unknown |
|---|---|---|---|---|---|---|---|---|---|
| dns.google. | 700,376 77.63 % | 19,912 64.94 % | 1,549 39.90 % | 5,257 75.32 % | 51 62.96 % | 402,278 75.89 % | 213 78.31 % | 96 82.05 % | 271,020 82.11 % |
| one.one.one.one. | 120,420 13.35 % | 6,198 20.21 % | 396 10.20 % | 1,044 14.96 % | 15 18.52 % | 75,741 14.29 % | 18 6.62 % | 21 17.95 % | 36,987 11.21 % |
| dns.opendns.com. | 16,221 1.80 % | 752 2.45 % | 124 3.19 % | 122 1.75 % | | 10,656 2.01 % | 6 2.21 % | | 4,561 1.38 % |
| dns.umbrella.com. | 16,220 1.80 % | 752 2.45 % | 124 3.19 % | 122 1.75 % | | 10,655 2.01 % | 6 2.21 % | | 4,561 1.38 % |
| doh.umbrella.com. | 8,006 0.89 % | 374 1.22 % | 62 1.60 % | 61 0.87 % | | 5,260 0.99 % | 3 1.10 % | | 2,246 0.68 % |
| doh.opendns.com. | 8,005 0.89 % | 374 1.22 % | 62 1.60 % | 61 0.87 % | | 5,260 0.99 % | 3 1.10 % | | 2,245 0.68 % |
| dns.quad9.net. | 6,924 0.77 % | 560 1.83 % | 24 0.62 % | 68 0.97 % | | 4,310 0.81 % | 2 0.74 % | | 1,960 0.59 % |
| familyshield.opendns.com. | 5,068 0.56 % | 28 0.09 % | 958 24.68 % | 108 1.55 % | 2 2.47 % | 3,110 0.59 % | | | 862 0.26 % |
| family.cloudflare-dns.com. | 3,699 0.41 % | 117 0.38 % | 84 2.16 % | 9 0.13 % | | 2,733 0.52 % | 15 5.51 % | | 741 0.22 % |
| security.cloudflare-dns.com. | 2,706 0.30 % | 93 0.30 % | 6 0.15 % | 15 0.21 % | 12 14.81 % | 2,151 0.41 % | | | 429 0.13 % |

**(b) IPv6 DDR-enabled resolvers' most advertised alternative domains (October 30, 2024).**

| Alternative Domain | Total | Content | Ed. Research | Enterprise | Network Services | Non-Profit | Unknown |
|---|---|---|---|---|---|---|---|
| dns.google. | 19,800 83.12 % | 558 37.20 % | 150 66.96 % | 102 58.29 % | 16,221 87.76 % | 45 56.96 % | 2,724 81.05 % |
| one.one.one.one. | 2,184 9.17 % | 336 22.40 % | 24 10.71 % | 33 18.86 % | 1,401 7.58 % | 15 18.99 % | 375 11.16 % |
| dns.opendns.com. | 298 1.25 % | 130 8.67 % | 2 0.89 % | 4 2.29 % | 112 0.61 % | | 50 1.49 % |
| dns.umbrella.com. | 298 1.25 % | 130 8.67 % | 2 0.89 % | 4 2.29 % | 112 0.61 % | | 50 1.49 % |
| dns.quad9.net. | 212 0.89 % | 44 2.93 % | 2 0.89 % | 6 3.43 % | 138 0.75 % | 4 5.06 % | 18 0.54 % |
| doh.opendns.com. | 146 0.61 % | 65 4.33 % | | 2 1.14 % | 54 0.29 % | | 25 0.74 % |
| doh.umbrella.com. | 146 0.61 % | 65 4.33 % | | 2 1.14 % | 54 0.29 % | | 25 0.74 % |
| family.cloudflare-dns.com. | 63 0.26 % | | 27 12.05 % | | 21 0.11 % | 12 15.19 % | 3 0.09 % |
| dns.adguard-dns.com. | 55 0.23 % | | | | 45 0.24 % | | 10 0.30 % |
| doh.cox.net. | 53 0.22 % | | | | 53 0.29 % | | |

# B Most Advertised DDR Configurations

**Listing 1: The most used DDR configuration, redirecting to Google.**

```
1 dns.google.
    alpn="dot"
2 dns.google.
    alpn="h2,h3"
    dohpath="/dns-query{?dns}"
```

**Listing 2: The second most used DDR configuration, redirecting to *Cloudflare*.**

```
1 one.one.one.one.
    alpn="h2,h3"
    port=443
    ipv4hint=1.1.1.1,1.0.0.1
    ipv6hint=2606:4700:4700::1111,2606:4700:4700::1001
    dohpath="/dns-query{?dns}"
2 one.one.one.one.
    alpn="dot"
    port=853
    ipv4hint=1.1.1.1,1.0.0.1
    ipv6hint=2606:4700:4700::1111,2606:4700:4700::1001
```

**Listing 3: The third most used DDR configuration, redirecting to *Cisco Umbrella (OpenDNS)*.**

```
5 dns.opendns.com.
    alpn="dot"
    port=853
    ipv4hint=208.67.220.220,208.67.222.222
    ipv6hint=2620:119:35::35,2620:119:53::53
5 dns.umbrella.com.
    alpn="dot"
    port=853
    ipv4hint=208.67.220.220,208.67.222.222
    ipv6hint=2620:119:35::35,2620:119:53::53
10 dns.opendns.com.
    alpn="h2"
    ipv4hint=208.67.220.220,208.67.222.222
    ipv6hint=2620:119:35::35,2620:119:53::53
    dohpath="/dns-query{?dns}"
10 dns.umbrella.com.
    alpn="h2"
    ipv4hint=208.67.220.220,208.67.222.222
    ipv6hint=2620:119:35::35,2620:119:53::53
    dohpath="/dns-query{?dns}"
20 doh.opendns.com.
    alpn="h2"
    ipv4hint=146.112.41.2
    ipv6hint=2620:119:fc::2
    dohpath="/dns-query{?dns}"
20 doh.umbrella.com.
    alpn="h2"
    ipv4hint=146.112.41.2
    ipv6hint=2620:119:fc::2
    dohpath="/dns-query{?dns}"
```

**Listing 4: The fourth most used DDR configuration, redirecting to *Cisco Umbrella (OpenDNS)*.**

```
 1  5 familyshield.opendns.com.
 2      alpn="dot"
 3      port=853
 4      ipv4hint=208.67.220.123,208.67.222.123
 5      ipv6hint=2620:119:35::123,2620:119:53::123
 6  10 familyshield.opendns.com.
 7      alpn="h2"
 8      ipv4hint=208.67.220.123,208.67.222.123
 9      ipv6hint=2620:119:35::123,2620:119:53::123
10      dohpath="/dns-query{?dns}"
11  20 doh.familyshield.opendns.com.
12      alpn="h2"
13      ipv4hint=146.112.41.3
14      ipv6hint=2620:119:fc::3
15      dohpath="/dns-query{?dns}"
```

**Listing 5: The fifth most used DDR configuration, redirecting to Quad9.**

```
 1  1 dns.quad9.net.
 2      alpn="dot"
 3      port=853
 4      ipv4hint=9.9.9.9,149.112.112.112
 5      ipv6hint=2620:fe::fe
 6  2 dns.quad9.net.
 7      alpn="h2"
 8      port=443
 9      ipv4hint=9.9.9.9,149.112.112.112
10      ipv6hint=2620:fe::fe
11      dohpath="/dns-query{?dns}"
```