A First Look on Discovery of Designated Resolvers

27 May 2025, IFIP Networking 2025

Steffen Sassalla, **vasilis ververis**, Vaibhav Bajpai

Hasso Plattner Institute, University of Potsdam, Germany

Outline

DNS Privacy Risks

- DNS queries reveal sensitive user intent and device usage [1, 2].
- Unencrypted DNS enables eavesdropping, tracking, and manipulation [3, 4, 5].
- 89% of DNS queries remain unencrypted [6].

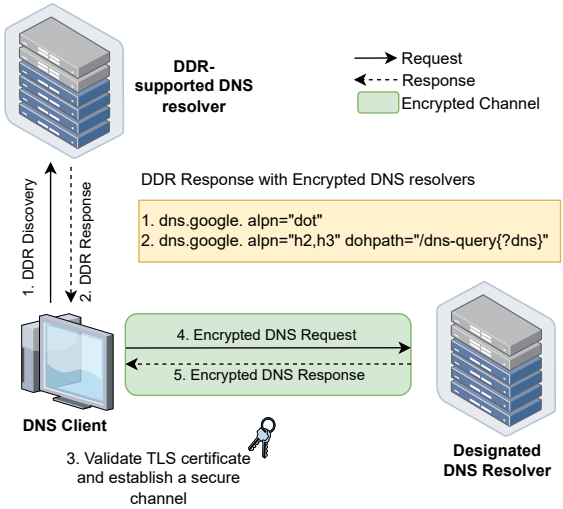
Encrypted DNS Protocols (DoE)

- **DNS-over-HTTPS (DoH)**: Encapsulates DNS in HTTPS, uses port 443.
- **DNS-over-TLS (DoT)**: Encapsulates DNS in TLS, uses port 853.
- **DNS-over-QUIC (DoQ)**: Leverages QUIC for performance and privacy, uses port 853.

DDR Motivation

- Manual transition to encrypted DNS is complex for users.
- DDR enables clients to transition from plaintext to encrypted DNS seamlessly without user interaction.
- IETF standardized the DDR protocol in November 2023 [7].
- DDR streamlines the adoption of encrypted DNS by enabling clients to:
  - Use plaintext DNS to automatically discover DNS over Encryption (DoE) endpoints.
  - Access configurations such as ports or URI paths in the case of DoH.

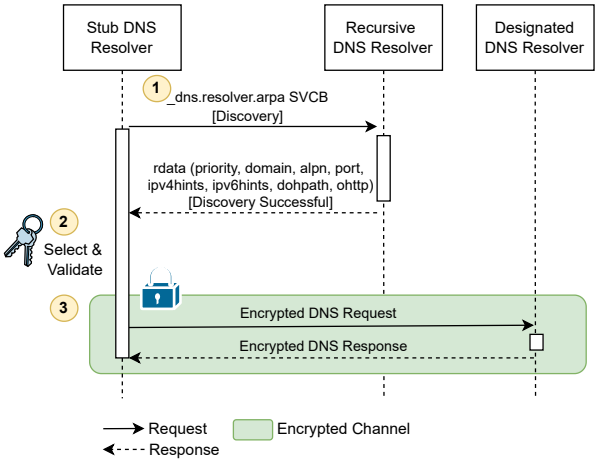
DDR Protocol Overview



DDR Discovery and Validation

- 1. DDR Discovery:
  - Queries `_dns.resolver.arpa` for SVCB records.
  - Returns designated resolvers if DDR is configured (e.g., `8.8.8.8` with DoH/DoT).
  - Returns empty records if not configured.
- 2. Selection & Validation:
  - Selects resolver by priority and protocols.
  - Verifies authenticity via Verified Discovery.
- 3. Verification & Upgrade:
  - Initiates TLS handshake and validates certificate.
  - Allows use of designated resolver for encrypted DNS.

Sequence diagram of DDR discovery



Related Work I

- Large-scale DNS measurements: On-path interception [8], poisoning and malformed configurations [9].
- DoE adoption: Most studies focus on DoH, DoT, and DoQ, server-side availability [10].
- Security: DoE deployments use invalid certificates [11, 12, 13]; DNS manipulation is common [14].
- DoH and DoT performance [15].
- [16] first to examine SVCB records but do not cover DDR.

To the best of our knowledge, no previous research has been conducted on DDR.

Measurement Methodology

- **DNS Server Discovery:** ZMap (IPv4), IPv6 Hitlist Service.
- **DDR Discovery:** SVCB queries to `_dns.resolver.arpa`.
- **DoE Endpoint Validation:** TLS certificate check, query reliability.
- **Data Enrichment:** Augment with AS-related information.
- **DNS dataset:** *ZMap* scan in July 2024 excludes inactive resolvers.
- One-time measurement from an academic network (VP).

Measurement Methodology

- **DNS Server Discovery:** ZMap (IPv4), IPv6 Hitlist Service.
- **DDR Discovery:** SVCB queries to `_dns.resolver.arpa`.
- **DoE Endpoint Validation:** TLS certificate check, query reliability.
- **Data Enrichment:** Augment with AS-related information.
- **DNS dataset:** *ZMap* scan in July 2024 excludes inactive resolvers.
- One-time measurement from an academic network (VP).
- Limitations:
  - AS misclassification by PeeringDB may introduce bias (e.g., Google as both content provider and enterprise).
  - Timeout durations (2.5 seconds for DDR, 5 seconds for DoE probes) may not mitigate bias; 69.07% of DoE probe errors are due to timeouts.
  - Uncertainty about client adherence to third-party designations due to limited client-side DDR support (e.g., `systemd-resolved`).

Research Question: 1

RQ 1: *How many DNS resolvers support DDR over the Internet?*

DDR Adoption Rate

Table: Scan Coverage and DDR Adoption Rates

	IPv4	IPv6
Resolvers Scanned	27 060 938	419 064
DDR-Supported	292 260 (1.08 %)	9520 (2.27 %)

- High concentration among a few providers.

Total Number of Scanned DNS Resolvers

Table: Total scanned DNS resolvers for DDR discovery, categorized by AS network type. The DDR adoption column indicates DNS-supported servers, with the percentage reflecting the rate of compliant DNS servers that responded without errors.

Network Type	# DNS Resolver ↓	# Total ASes	DDR Adoption	# DDR ASes
Unknown	11,600,414 (42.21%)	31,392 (67.67%)	111,585 (8.83%)	8,479 (53.32%)
NSP	11,479,409 (41.77%)	3,206 (6.91%)	68,537 (8.21%)	1,699 (10.68%)
Content	3,039,289 (11.06%)	1,428 (3.08%)	9,584 (0.62%)	393 (2.47%)
Cable/DSL/ISP	881,744 (3.21%)	8,564 (18.46%)	107,002 (17.65%)	4,966 (31.23%)
Enterprise	340,106 (1.24%)	805 (1.74%)	2,705 (3.58%)	179 (1.13%)
Ed./Research	131,772 (0.48%)	587 (1.27%)	1,726 (3.11%)	130 (0.82%)
Non-Profit	6,192 (0.02%)	315 (0.68%)	345 (6.61%)	42 (0.26%)
Government	599 (<0.01%)	67 (0.14%)	21 (4.17%)	7 (0.04%)
Route Server	477 (<0.01%)	28 (0.06%)	275 (70.33%)	6 (0.04%)
Total	27,480,002	46,392	301,780	15,901

DDR Supported Resolvers by Network Type

Table: DoE protocols of designated resolvers advertised by the DDR-supported resolvers depending on the network type.

Networks↓	# DDR resolvers ↓	DoH/1.1 (%)	DoH/2 (%)	DoH/3 (%)	DoT (%)	DoQ (%)
Unknown	111,585	0.82	99.98	95.29	99.78	1.04
Cable/DSL/ISP	107,002	0.20	99.96	92.92	98.38	0.42
NSP	62,096	0.25	99.97	95.04	99.76	0.50
Content	9,584	0.21	99.47	86.23	94.04	6.02
Network Services	6,441	0.09	99.98	97.55	99.91	0.19
Enterprise	2,705	0.11	99.96	90.13	98.82	1.33
Ed./Research	1,726	0.06	100	68.25	99.77	0.29
Non-Profit	345	0.29	100	98.26	100	0.29
Route Server	275	0	100	100	100	0
Government	21	0	100	95.24	100	0

Research Question: 2

RQ 2: *What role do cloud providers (such as Google, Cloudflare) play in DDR support?*

Cloud Provider Centralization I

- 93% of DDR resolvers redirect to Google or Cloudflare.
- Raises concerns about DNS centralization and privacy.
- Few independent or regional providers advertise DDR.

Cloud Provider Centralization II

Table: The popularity of top 10 (out of 1,277) alternative domains designated by the resolvers inside various networks (IPv4 and IPv6 DDR server combined). Note that a DDR discovery can respond with a list of multiple alternative domains.

Domain	Network Type								
	Cable/DSL/ISP	Content	Ed./Research	Enterprise	Government	NSP	Non-Profit	Route Server	Unknown
dns.google. (736,956)	258,510 (78.88%)	19,340 (66.52%)	3,063 (57.56%)	6,000 (72.52%)	42 (66.67%)	162,555 (77.26%)	936 (89.4%)	801 (97.09%)	285,709 (83.43%)
one.one.one.one. (104,715)	36,840 (11.24%)	5,196 (17.87%)	375 (7.05%)	1,176 (14.21%)	12 (19.05%)	31,809 (15.12%)	63 (6.02%)	24 (2.91%)	29,220 (8.53%)
dns.umbrella.com. (17,020)	7338 (2.24%)	782 (2.69%)	110 (2.07%)	230 (2.78%)	0	3688 (1.75%)	8 (0.76%)	0	4864 (1.42%)
dns.opendns.com. (17,019)	7,336 (2.24%)	782 (2.69%)	110 (2.07%)	230 (2.78%)	0	3,690 (1.75%)	8 (0.76%)	0	4,863 (1.42%)
doh.opendns.com. (8,376)	3,645 (1.11%)	391 (1.34%)	55 (1.03%)	67 (0.81%)	0	1,805 (0.86%)	4 (0.38%)	0	2,409 (0.7%)
doh.umbrella.com. (8,375)	3,645 (1.11%)	391 (1.34%)	55 (1.03%)	67 (0.81%)	0	1,805 (0.86%)	4 (0.38%)	0	2,408 (0.7%)
dns.quad9.net. (7,638)	2,780 (0.85%)	618 (2.13%)	34 (0.64%)	126 (1.52%)	0	1,696 (0.81%)	4 (0.38%)	0	2,380 (0.69%)
familyshield.opendns.com. (6,026)	1,464 (0.45%)	22 (0.08%)	938 (17.63%)	112 (1.35%)	2 (3.17%)	740 (0.35%)	0	0	2,748 (0.8%)
dns.adguard-dns.com. (4,245)	650 (0.20%)	75 (0.26%)	5 (0.09%)	10 (0.12%)	0	525 (0.25%)	5 (0.48%)	0	2975 (0.87%)
doh.familyshield.opendns.com (3,013)	732 (0.22%)	11 (0.04%)	469 (8.81%)	56 (0.68%)	1 (1.59%)	370 (0.18%)	0	0	1374 (0.40%)

Cloud Provider Centralization III

Table: The popularity of top 10 (out of 1,277) alternative domains designated by the resolvers inside various networks (IPv4 and IPv6 DDR server combined). Note that a DDR discovery can respond with a list of multiple alternative domains.

Domain	Network Type								
	Cable/DSL/ISP	Content	Ed./Research	Enterprise	Government	NSP	Non-Profit	Route Server	Unknown
dns.google. (736,956)	258,510 (78.88%)	19,340 (66.52%)	3,063 (57.56%)	6,000 (72.52%)	42 (66.67%)	162,555 (77.26%)	936 (89.4%)	801 (97.09%)	285,709 (83.43%)
one.one.one.one. (104,715)	36,840 (11.24%)	5,196 (17.87%)	375 (7.05%)	1,176 (14.21%)	12 (19.05%)	31,809 (15.12%)	63 (6.02%)	24 (2.91%)	29,220 (8.53%)
dns.umbrella.com. (17,020)	7338 (2.24%)	782 (2.69%)	110 (2.07%)	230 (2.78%)	0	3688 (1.75%)	8 (0.76%)	0	4864 (1.42%)
dns.opendns.com. (17,019)	7,336 (2.24%)	782 (2.69%)	110 (2.07%)	230 (2.78%)	0	3,690 (1.75%)	8 (0.76%)	0	4,863 (1.42%)
doh.opendns.com. (8,376)	3,645 (1.11%)	391 (1.34%)	55 (1.03%)	67 (0.81%)	0	1,805 (0.86%)	4 (0.38%)	0	2,409 (0.7
doh.umbrella.com. (8,375)	3,645 (1.11%)	391 (1.34%)	55 (1.03%)	67 (0.81%)	0	1,805 (0.86%)	4 (0.38%)	0	2,408 (0.7
dns.quad9.net. (7,638)	2,780 (0.85%)	618 (2.13%)	34 (0.64%)	126 (1.52%)	0	1,696 (0.81%)	4 (0.38%)	0	2,380 (0.69
familyshield.opendns.com. (6,026)	1,464 (0.45%)	22 (0.08%)	938 (17.63%)	112 (1.35%)	2 (3.17%)	740 (0.35%)	0	0	2,748 (0.8%)
dns.adguard-dns.com. (4,245)	650 (0.20%)	75 (0.26%)	5 (0.09%)	10 (0.12%)	0	525 (0.25%)	5 (0.48%)	0	2975 (0.87%)
doh.familyshield.opendns.com (3,013)	732 (0.22%)	11 (0.04%)	469 (8.81%)	56 (0.68%)	1 (1.59%)	370 (0.18%)	0	0	1374 (0.40

Ethical Considerations

- Adhere to ethical research practices.
- Focus on publicly resolvable DNS data, avoiding personal information.
- Utilize established tools like:
  - *ZMap*
  - *IPv6 Hitlist Service* [17, 18, 19]
- Prevent network congestion with random IP selection [20].
- Implement caching to reduce redundant queries.
- Ensure transparency with `TXT` records and reverse DNS entries.
- Operate within an academic network, informing system administrators.

Conclusion

- DDR automates the upgrade to encrypted DNS, but adoption is low.
- Most DDR-enabled resolvers are controlled by a few large providers.
- DoQ remains underutilized despite technical advantages.
- Reliability and certificate validation are ongoing concerns.
- Centralization could undermine privacy goals.

Conclusion

- DDR automates the upgrade to encrypted DNS, but adoption is low.
- Most DDR-enabled resolvers are controlled by a few large providers.
- DoQ remains underutilized despite technical advantages.
- Reliability and certificate validation are ongoing concerns.
- Centralization could undermine privacy goals.

Contact: vasilis.ververis@hpi.de

Data Artifacts:

Source Code:

Interested in Internet measurements? Our chair is hiring doctoral students and postdocs. Please see: https://hpi.de/en/bajpai

References I

[1] F. Le, J. Ortiz, D. C. Verma, and D. D. Kandlur, “Policy-Based Identification of IoT Devices’ Vendor and Type by DNS Traffic Analysis,” in *PADG@ESORICS 2018*, vol. 11550, Spain, 2018.

[2] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, and N. Feamster, “Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic,” 2017.

[3] S. Bortzmeyer, “DNS privacy considerations,” https://doi.org/10.17487/RFC7626, pp. 1–17, May 2015.

[4] D. Herrmann, C. Gerber, C. Banse, and H. Federrath, “Analyzing characteristic host access patterns for re-identification of web user sessions,” in *NordSec 2010*, vol. 7127, Finland, 2010, pp. 136–154.

[5] G. C. M. Moura, S. Castro, W. Hardaker, M. Wullink, and C. Hesselman, “Clouding up the Internet: how centralized is DNS traffic becoming?” in *ACM IMC*, ser. IMC ’20, 2020, pp. 42–49.

[6] A. W. Christopher Wood, “Announcing experimental ddr in 1.1.1.1,” https://blog.cloudflare.com/announcing-ddr-support/, March 2022.

[7] T. Pauly, E. Kinnear, C. A. Wood, P. McManus, and T. Jensen, “Discovery of designated resolvers,” *RFC*, vol. 9462, pp. 1–16, 2023. [Online]. Available: https://doi.org/10.17487/RFC9462

[8] B. Liu, C. Lu, H. Duan, Y. Liu, Z. Li, S. Hao, and M. Yang, “Who Is Answering My Queries: Understanding and Characterizing Interception of the DNS Resolution Path,” in *USENIX Security*, Aug. 2018.

References III

[9] X. Li, C. Lu, B. Liu, Q. Zhang, Z. Li, H. Duan, and Q. Li, “The Maginot Line: Attacking the Boundary of DNS Caching Protection,” in *USENIX Security*, Aug. 2023.

[10] C. T. Deccio and J. Davis, “DNS privacy in practice and preparation,” in *CoNEXT 2019*. USA: ACM, 2019, pp. 138–143.

[11] R. Li, X. Jia, Z. Zhang, J. Shao, R. Lu, J. Lin, X. Jia, and G. Wei, “A Longitudinal and Comprehensive Measurement of DNS Strict Privacy,” *IEEE/ACM Transactions on Networking*, vol. 31, no. 6, 2023.

[12] T. Fiebig, S. F. Gürses, C. Gañán, E. Kotkamp, F. Kuipers, M. Lindorfer, M. Prisse, and T. Sari, “Heads in the Clouds? Measuring Universities’ Migration to Public Clouds: Implications for Privacy & Academic Freedom,” *Proc. Priv. Enhancing Technol.*, vol. 2023, no. 2, 2023.

References IV

[13] C. Lu, B. Liu, Z. Li, S. Hao, H. Duan, M. Zhang, C. Leng, Y. Liu, Z. Zhang, and J. Wu, “An end-to-end, large-scale measurement of DNS-over-encryption: How far have we come?” in *IMC*, 10 2019.

[14] L. Jin, S. Hao, H. Wang, and C. Cotton, “Understanding the impact of encrypted DNS on internet censorship,” in *WWW 2021*, 4 2021.

[15] A. Hounsel, K. Borgolte, P. Schmitt, J. Holland, and N. Feamster, “Comparing the Effects of DNS, DoT, and DoH on Web Performance,” in *WWW 2020*, 4 2020.

[16] J. Zirngibl, P. Sattler, and G. Carle, “A first look at SVCB and HTTPS DNS resource records in the wild,” in *IEEE European Symposium on Security and Privacy, EuroS&P 2023 - Workshops, Delft, Netherlands, July 3-7, 2023*. IEEE, 2023, pp. 470–474. [Online]. Available: https://doi.org/10.1109/EuroSPW59978.2023.00058

[17] O. Gasser, Q. Scheitle, P. Foremski, Q. Lone, M. Korczynski, S. D. Strowes, L. Hendriks, and G. Carle, “Clusters in the Expanse: Understanding and Unbiasing IPv6 Hitlists,” in *IMC*, 2018.

[18] J. Zirngibl, L. Steger, P. Sattler, O. Gasser, and G. Carle, “Rusty Clusters? Dusting an IPv6 Research Foundation,” in *IMC*, 2022.

[19] L. Steger, L. Kuang, J. Zirngibl, G. Carle, and O. Gasser, “Target Acquired? Evaluating Target Generation Algorithms for IPv6,” in *TMA*, 2023.

[20] Z. Durumeric, E. Wustrow, and J. A. Halderman, “Zmap: Fast internet-wide scanning and its security applications,” in *USENIX Security*, 2013.

Benefits:

- Prevents eavesdropping and manipulation.
- Shields queries from ISPs and attackers.
- Bypasses some censorship and network restrictions.

Limitations:

- Not all resolvers or clients support DoE.
- DoT/DoQ can be blocked by firewalls.
- Centralization risk: Many users default to a few large providers.

Non-default Configurations

- Most DDR-advertised DoE endpoints use default ports and paths.
- Small fraction deviate, which can hinder compatibility.
- Verified Discovery ensures only endpoints with valid certificates are used.

DDR Discovery and Validation (extended)

- 1. DDR Discovery with SVCB Records:
  - DNS client queries `_dns.resolver.arpa` for SVCB records.
  - If DDR is configured, designated resolvers and their DoE parameters are returned.
  - Example: Google's resolver `8.8.8.8` designates `dns.google.` with DoH/DoT support.
  - If not configured, an empty set of SVCB records is returned.
- 2. Selection and Validation:
  - Client selects resolver based on priority and supported protocols.
  - Uses ALPN intersection to choose the best protocol.
  - Must verify resolver authenticity via Verified Discovery.
- 3. Verification and Upgrade
  - Initiates TLS handshake with selected DoE endpoint.
  - Validates certificate chain and checks IP in `subjectAltName`.
  - Successful validation allows use of designated resolver for encrypted DNS queries.

Research Questions I

- **c**) How do resolvers that send DDR configurations prioritize different encrypted DNS protocols?
- **d**) How often do encrypted resolvers deviate from default DoE configurations like standard ports or default URI query paths (DoH)?
- **e**) What is the reliability of the discovered encrypted resolvers in responding to DNS queries?