ADD Working Group
Internet-Draft
Intended status: Informational
Expires: 21 January 2026

D. Liu
Jinan University
Z. Yan
CNNIC
G. Geng
G. Zeng
Jinan University

20 July 2025

Multicast DNS-Based Service Discovery for Encrypted DNS Services
draft-liu-add-dnssd-edns-00

Abstract

This document defines a multicast DNS (mDNS) and DNS-Based Service Discovery (DNS-SD) mechanism for discovering encrypted DNS services in local networks. It specifies new service types (_dot, _doh, _doq) and associated TXT record parameters to enable zero-configuration discovery of DNS over TLS (DoT), DNS over HTTPS (DoH), and DNS over QUIC (DoQ) resolvers. This extension addresses critical privacy gaps in local networks while maintaining backward compatibility with RFC 6763.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 21 January 2026.

Copyright Notice

Table of Contents

1. Introduction

1.1. The Local Network Privacy Challenge

While encrypted DNS protocols such as DNS over TLS (DoT)[RFC7858], DNS over HTTPS (DoH)[RFC8484], and DNS over QUIC (DoQ)[RFC9250] have gained widespread adoption for public Internet resolution, local network environments often remain vulnerable to surveillance and manipulation of DNS traffic. Many devices and applications in home, enterprise, and industrial networks still rely on plaintext DNS, exposing sensitive metadata such as device activities, service dependencies, and user behavior patterns. Traditional discovery mechanisms (e.g., DHCP, Router Advertisements) lack the flexibility to negotiate fine-grained encrypted DNS configurations and fail in infrastructure-less environments where centralized servers are unavailable.

1.2. mDNS/DNS-SD as a Solution for Privacy-Aware Discovery

Multicast DNS (mDNS, [RFC6762]) and DNS-Based Service Discovery (DNS-SD, [RFC6763]) provide an ideal foundation for encrypted DNS service discovery due to their:

Zero-configuration operation: Devices autonomously advertise and discover services without requiring a central server.

Topology independence: Functions in isolated networks (e.g., home labs, industrial control systems) even without Internet connectivity.

Real-time updates: Service availability changes propagate within seconds, unlike DHCP’s lease-based delays.

Rich parameter negotiation: TXT records allow flexible exchange of protocol details (ports, ALPN preferences, certificate fingerprints).

1.3. Key Use Cases

This specification enables:

IoT and Smart Home Privacy: Devices (e.g., cameras, voice assistants) automatically discover and use encrypted DNS without manual configuration.

Enterprise Network Segmentation: Departments can advertise isolated DNS services (e.g., _dot.finance.corp.local) with policy enforcement.

Offline and Air-Gapped Networks: Secure DNS resolution in environments where Internet access is restricted but internal name resolution is still required (e.g., industrial control systems, military networks).

1.4. Relationship to Existing Standards

While [RFC9463] provides DHCP/RA-based encrypted DNS discovery, this mDNS-based approach offers complementary advantages:

Capability	DHCP/RA	mDNS/DNS-SD (This Spec)
Infrastructure	Requires DHCP server/router	Works without infrastructure
Update Latency	Minutes-hours (lease time)	Seconds (event-driven)
Parameter Flexibility	Limited by option space	Rich TXT key-value pairs
Use Cases	Managed networks	Ad-hoc/IoT/dynamic networks

Table 1: Relationship to Existing Standards

This document defines new DNS-SD service types (_dot._tcp, _doh._tcp, _doq._udp) and standardized TXT record parameters to enable seamless discovery of encrypted DNS services while maintaining backward compatibility with [RFC6763].

2. Terminology and Requirements

2.1. Requirements Language

Key words: "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", "OPTIONAL" per BCP 14 [RFC2119] [RFC8174]

2.2. Defined Terms

* EDNS: Encrypted DNS (DoT, DoH, DoQ collectively)

* ADN: Authentication Domain Name (FQDN for certificate validation)

* Service Instance: Unique identifier for an EDNS resolver (e.g., Finance DoT._dot._tcp.local)

3. Service Type Definitions

3.1. Encrypted DNS Service Types

Service Type	Protocol	Transport	IANA Assignment
_dot._tcp	DoT	TCP	REQUIRED
_doh._tcp	DoH	TCP	REQUIRED
_doq._udp	DoQ	UDP	REQUIRED

Table 2: Encrypted DNS Service Types

3.2. Service Instance Name Format

<Instance>.<Service>.<Domain>

* Instance: Human-readable identifier (e.g., CorpDNS, HomeGateway)

* Service: One of _dot._tcp, _doh._tcp, _doq._udp

* Domain: local (default) or custom domain

Example: SecurityDoH._doh._tcp.local

4. DNS Resource Records

4.1. PTR Records (Service Discovery)

```
; Service enumeration
_services._dns-sd._udp.local. PTR _dot._tcp.local
_services._dns-sd._udp.local. PTR _doh._tcp.local
_services._dns-sd._udp.local. PTR _doq._udp.local
```

4.2. SRV Records (Service Location)

<Instance>.<Service>.<Domain> [Class] [TTL] SRV <Priority> <Weight> <Port> <Target>

* Target: Hostname offering the service (A/AAAA must resolve)

Example:

HomeDoT._dot._tcp.local. 120 IN SRV 0 5 853 router.home.local.

4.3. TXT Records (Service Parameters)

Defined Keys:

Key	Format	Description	Example
port	Number	Override default port	port=784
path	String	DoH URI path (required for DoH)	path=/dns-query
alpn	Comma-list	Supported ALPN protocols	alpn=h2,h3
pri	Number	Selection priority (0-65535)	pri=10
fp_sha256	Hex string	Certificate SHA-256 fingerprint	fp_sha256=9F86D0...
domain	FQDN	ADN for certificate validation	domain=dns.corp.example

Table 3: TXT Records (Service Parameters)

Full Example:

HomeDoH._doh._tcp.local. 120 IN TXT "port=443" "path=/dns" "alpn=h2" "domain=dns.home.net"

5. Discovery Process

5.1. Service Advertisement

1. EDNS resolver sends mDNS broadcast:

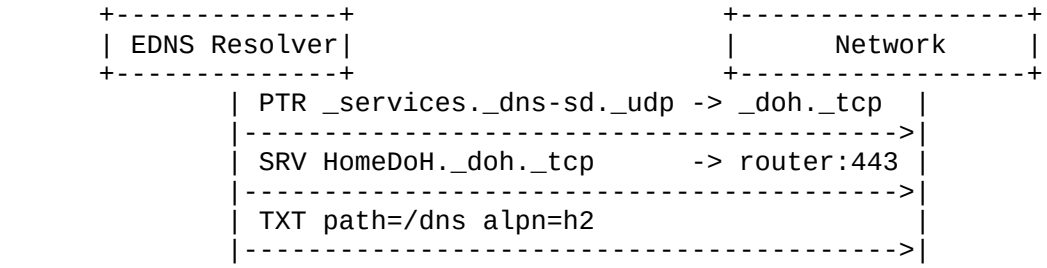

Figure 1: EDNS resolver sends mDNS broadcast

5.2. Client Discovery

1. Client queries for service types:

```
; Query available EDNS services
_services._dns-sd._udp.local. IN PTR
```

2. Query specific instances:

```
; Query DoH instances
_doh._tcp.local. IN PTR
```

3. Resolve selected service:

```
HomeDoH._doh._tcp.local. IN SRV
HomeDoH._doh._tcp.local. IN TXT
router.home.local. IN A
router.home.local. IN AAAA
```

6. Security Considerations

6.1. Spoofing Countermeasures

* mDNS Response Validation: Clients MUST verify source IP matches query target

* Rate Limiting: Implement mDNS response rate limiting Section 11 of [RFC6762]

* TLS Enforcement: Clients MUST validate server certificates against ADN or fingerprint

6.2. Certificate Validation Models

Trust Model	Verification Method	Use Case
Public PKI	ADN (domain= key) + CA validation	General-purpose networks
Fingerprint Pinning	fp_sha256 exact match	High-security/ IoT devices
Private PKI	ADN + custom trust anchors	Enterprise networks

Table 4: Certificate Validation Models

6.3. Privacy Implications

* Metadata Leakage: mDNS queries reveal client interest in encrypted DNS

* Mitigation: Clients SHOULD use service type enumeration (_services._dns-sd) before specific queries

7. IANA Considerations

7.1. New DNS-SD Service Types

Service Name	Protocol	Reference	Assignment Policy
_dot	TCP	RFC-TBD	Standard
_doh	TCP	RFC-TBD	Standard
_doq	UDP	RFC-TBD	Standard

Table 5: New DNS-SD Service Types

7.2. TXT Record Key Registry

Key	Meaning	Reference
port	Transport port	RFC-TBD
path	HTTP URI path (DoH)	RFC-TBD
alpn	ALPN protocol list	RFC-TBD
pri	Service priority	RFC-TBD
fp_sha256	Certificate fingerprint	RFC-TBD
domain	Authentication Domain Name	RFC-TBD

Table 6: TXT Record Key Registry

8. Examples

8.1. Full DoT Service Advertisement

```
; Service type announcement
_services._dns-sd._udp.local. PTR _dot._tcp.local


; Service instance
HomeDoT._dot._tcp.local. SRV 0 5 853 router.home.local.
HomeDoT._dot._tcp.local. TXT "domain=dns.home.net" "fp_sha256=9F86D08188..."
router.home.local. A 192.168.1.1
router.home.local. AAAA fd12:3456::1
```

8.2. DoH Service with Custom Path

```
OfficeDoH._doh._tcp.local. SRV 0 10 443 dnsgateway.corp.local.
OfficeDoH._doh._tcp.local. TXT "path=/internal/dns" "alpn=h2,h3" "pri=5"
```

8.3. Client Discovery Sequence

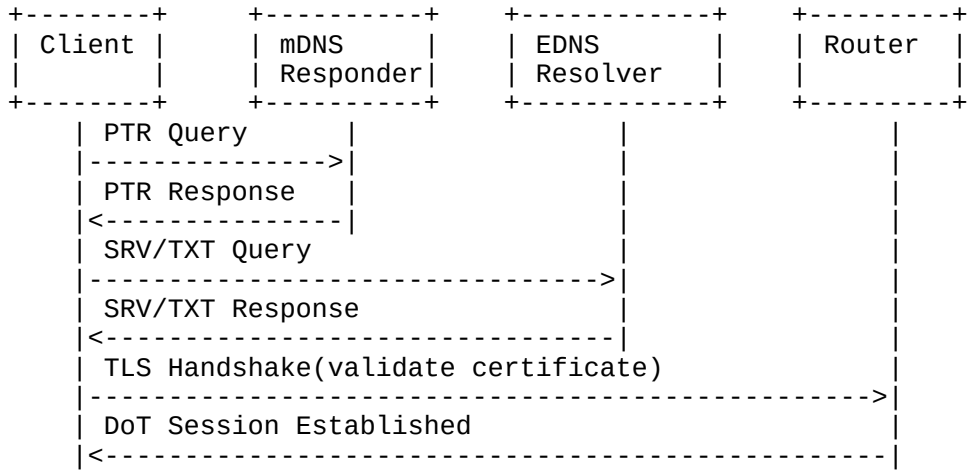

Figure 2: Client Discovery Sequence

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, DOI 10.17487/RFC6762, February 2013, <https://www.rfc-editor.org/info/rfc6762>.

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, DOI 10.17487/RFC6763, February 2013, <https://www.rfc-editor.org/info/rfc6763>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

[RFC9250] Huitema, C., Dickinson, S., and A. Mankin, "DNS over Dedicated QUIC Connections", RFC 9250, DOI 10.17487/RFC9250, May 2022, <https://www.rfc-editor.org/info/rfc9250>.

9.2. Informative References

[RFC9463] Boucadair, M., Ed., Reddy.K, T., Ed., Wing, D., Cook, N., and T. Jensen, "DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR)", RFC 9463, DOI 10.17487/RFC9463, November 2023, <https://www.rfc-editor.org/info/rfc9463>.

[RFC9460] Schwartz, B., Bishop, M., and E. Nygren, "Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records)", RFC 9460, DOI 10.17487/RFC9460, November 2023, <https://www.rfc-editor.org/info/rfc9460>.

[IOT-DNS] ISOC, "IoT Device DNS Privacy Report", 2023.

acknowledgements

This work is supported by the National Key Research and Development Program of China (No.2023YFB3105700).

Authors' Addresses

Dongjie Liu
Jinan University
Email: dongjieliu8917@gmail.com

Zhiwei Yan
CNNIC
Email: yanzhiwei@cnnic.cn

Guanggang Geng
Jinan University
Email: guanggang.geng@gmail.com

Guoqiang Zeng
Jinan University

Email: zeng.guoqiang5@gmail.com