ADD Working Group
Internet-Draft
Intended status: Informational
Expires: 22 September 2026

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

21 March 2026

DNS-Based Service Discovery for Encrypted DNS Services
draft-liu-add-dnssd-edns-02

Abstract

This document defines a 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 service parameters to enable zero-configuration discovery of DNS over TLS (DoT), DNS over HTTPS (DoH), and DNS over QUIC (DoQ) resolvers. The mechanism works over both multicast DNS (mDNS) and unicast DNS-SD, addressing critical privacy gaps in local networks while maintaining backward compatibility with RFC 6763. This document leverages SVCB and HTTPS resource records (RFC 9460) for parameter negotiation, with TXT records provided for compatibility with legacy implementations.

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. DNS-SD as a Solution for Privacy-Aware Discovery

DNS-Based Service Discovery (DNS-SD, [RFC6763]) and its multicast variant (mDNS, [RFC6762]) 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: SVCB records (or TXT records for compatibility) 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 in home networks where no DHCP server is present or when users bring devices to temporary locations.

Enterprise Network Segmentation: Departments can advertise isolated DNS services (e.g., _dot.finance.corp.local) with policy enforcement, even in air-gapped segments.

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, disaster recovery scenarios).

Ad-hoc and Temporary Networks: When devices form a temporary network (e.g., during a conference, emergency response), they can discover and use encrypted DNS services without any pre-existing infrastructure.

1.4. Relationship to Existing Standards

[RFC9463] defines DHCP and Router Advertisement options for encrypted DNS discovery (DNR), and [I-D.ietf-add-ddr] specifies Discovery of Designated Resolvers (DDR) using DNS queries. These mechanisms require infrastructure support (DHCP server, router, or recursive resolver) and are suitable for managed networks. This document provides a complementary solution that operates without any infrastructure, making it ideal for ad-hoc, isolated, or zero-configuration environments. The following table summarizes the differences:

Capability	DNR (RFC 9463)	DDR (draft-ietf-add-ddr)	This Specification
Infrastructure Required	DHCP/RA server	Recursive DNS server	None (zero-configuration)
Update Latency	Minutes-hours (lease time)	DNS TTL dependent	Seconds (event-driven)
Parameter Flexibility	Limited by option space	SVCB-based	SVCB-based
Primary Use Cases	Managed networks	Managed networks with DNS	Ad-hoc/IoT/dynamic/ isolated networks

Table 1: Comparison with Existing Encrypted DNS Discovery Mechanisms

This document defines new DNS-SD service types (_dot._tcp, _doh._tcp, _doq._udp) and leverages SVCB/HTTPS resource records for service parameter exchange, while maintaining backward compatibility with TXT-based discovery for legacy implementations.

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

* Encrypted DNS: Collective term for DoT, DoH, and DoQ.

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

* Service Instance: Unique identifier for an encrypted DNS 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." for mDNS, or any domain for unicast DNS-SD.

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 (Legacy Compatibility)

For compatibility with existing DNS-SD implementations, services MAY include TXT records with the following keys. However, new implementations SHOULD use SVCB/HTTPS records as described in Section 4.4.

Key	Format	Description	Example
path	String	DoH URI path (required for DoH when using TXT)	path=/dns-query
alpn	Comma-list	Supported ALPN protocols	alpn=h2,h3
pri	Number	Service selection preference (0-65535), lower is more preferred	pri=10
fp_sha256	Hex string	Certificate SHA-256 fingerprint (optional if ADN used)	fp_sha256=9F86D0...
adn	FQDN	Authentication Domain Name for certificate validation	adn=dns.corp.example

Table 3: Legacy TXT Record Keys

Full Example (TXT-based):

```
HomeDoH._doh._tcp.local. 120 IN TXT "path=/dns" "alpn=h2"
"adn=dns.home.net"
"fp_sha256=9F86D081884C7D659A2FEA0C55AD015A3BF4F1B2B0B822CD15D6C15B0F00A08"
```

4.4. SVCB/HTTPS Records for Service Parameters

Following [RFC9460], services SHOULD use SVCB (for DoT/DoQ) or HTTPS (for DoH) resource records to convey connection parameters. The SvcParam keys used are:

Key	Description	Example
port	Port number (if different from SRV or default)	port=443
alpn	ALPN protocol list. When containing HTTP versions (h2, h3), the 'dohpath' key MUST be present.	alpn=h2,h3
dohpath	DoH URI template (for DoH only)	dohpath=/dns-query{?dns}
adn	Authentication Domain Name	adn=dns.example.com
fp_sha256	Certificate SHA-256 fingerprint (alternative to adn)	fp_sha256=9F86D0...

Table 4: SVCB Parameters for Encrypted DNS

The SVCB record also provides the target hostname and priority, which may override the SRV record. Clients MUST first check for SVCB records; if absent, they MAY fall back to SRV+TXT.

Example SVCB record for a DoH service:

```
_doh._tcp.local. 7200 IN HTTPS 1 dns-home.local. alpn=h2,h3 dohpath=/dns-query adn=dns.ho
me.net
```

For DoT, use SVCB (not HTTPS) with appropriate ALPN (e.g., "dot").

5. Discovery Process

5.1. Service Advertisement

1. Encrypted DNS resolver periodically announces its services via mDNS (or unicast DNS update).

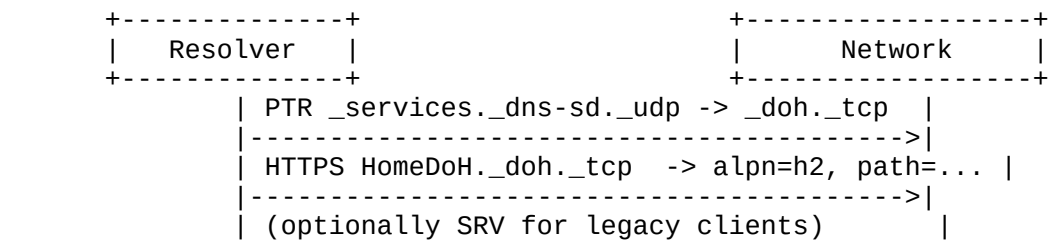

Figure 1: Example mDNS Advertisement with SVCB

5.2. Client Discovery

1. Client queries for service types:

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

2. Query specific instances:

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

3. Resolve selected service: first request SVCB/HTTPS, fallback to SRV+TXT.

```
; Request SVCB/HTTPS record
HomeDoH._doh._tcp.local. IN HTTPS
; If no HTTPS record, request SRV and TXT
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 (link-local scope).

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

* TLS Enforcement: Clients MUST validate server certificates against the ADN (from adn parameter) or the fingerprint (fp_sha256).

* Clients SHOULD NOT automatically trust discovered services; user confirmation or policy (e.g., only on trusted networks) is RECOMMENDED.

In open or untrusted networks (e.g., public Wi-Fi), malicious devices may advertise fake encrypted DNS services. To mitigate such risks, clients SHOULD adopt additional trust considerations:

* Only auto-discover on networks designated as trusted (e.g., home SSID, corporate network).

* Require user confirmation before using a discovered resolver.

* Allow administrators to pre-configure trusted ADNs or fingerprints.

6.2. Certificate Validation Models

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

Table 5: Certificate Validation Models

In addition to the models above, clients MAY establish trust via out-of-band mechanisms, such as scanning a QR code that encodes the server's certificate fingerprint (fp_sha256) or authentication domain name (ADN). Such mechanisms can be used to bootstrap secure connections in environments where public PKI is unavailable or where higher assurance is required.

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 to reduce leakage. In unicast DNS-SD, queries are not broadcast.

7. IANA Considerations

7.1. New DNS-SD Service Types

This document requests IANA to register the following service names in the "Service Name and Transport Protocol Port Number Registry" [RFC6335] and the corresponding service types in the "DNS-SD Service Type Bindings" registry.

Service Name	Transport Protocol	Reference	Assignment Policy
dot	tcp	RFC-TBD	Standard
doh	tcp	RFC-TBD	Standard
doq	udp	RFC-TBD	Standard

Table 6: New DNS-SD Service Types

The registration templates for these service types are as follows:

Service Name: dot

Transport Protocol(s): tcp

Assignee: IESG <iesg@ietf.org>

Contact: IESG <iesg@ietf.org>

Description: DNS over TLS (DoT) Resolver Service Discovery

Reference: RFC-TBD

Assignment Notes: This service type is used for discovering encrypted DNS services. The corresponding DNS-SD type is _dot._tcp.

Service Name: doh

Transport Protocol(s): tcp

Assignee: IESG <iesg@ietf.org>

Contact: IESG <iesg@ietf.org>

Description: DNS over HTTPS (DoH) Resolver Service Discovery

Reference: RFC-TBD

Assignment Notes: This service type is used for discovering encrypted DNS services. The corresponding DNS-SD type is _doh._tcp.

Service Name: doq

Transport Protocol(s): udp

Assignee: IESG <iesg@ietf.org>

Contact: IESG <iesg@ietf.org>

Description: DNS over QUIC (DoQ) Resolver Service Discovery

Reference: RFC-TBD

Assignment Notes: This service type is used for discovering encrypted DNS services. The corresponding DNS-SD type is _doq._udp.

7.2. TXT Record Key Registry

This document requests IANA to create a new registry titled "Encrypted DNS Service Discovery (DNS-SD) TXT Record Keys" under the "DNS-Based Service Discovery (DNS-SD) Parameters" registry.

The registration policy for this registry is "Expert Review" as defined in [RFC8126].

The initial contents of this registry are as follows:

Key	Meaning	Reference
path	HTTP URI path (for DoH)	RFC-TBD
alpn	Supported ALPN protocols	RFC-TBD
pri	Service selection preference	RFC-TBD
fp_sha256	Certificate SHA-256 fingerprint	RFC-TBD
adn	Authentication Domain Name (ADN)	RFC-TBD

Table 7: TXT Record Key Registry

New assignments require Expert Review. This registry is primarily for compatibility; new implementations should use SVCB parameters as defined in [RFC9460].

7.3. SVCB Parameters Usage

The SVCB parameters defined in [RFC9460] are used as described in Section 4.4. No new IANA registrations are required for SVCB keys; implementers should follow the registration procedures of RFC 9460 if new keys are needed.

8. Examples

8.1. Full DoT Service Advertisement with SVCB

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

; SVCB record (preferred)
_dot._tcp.local. 7200 IN SVCB 1 router.home.local. alpn=dot adn=dns.home.net

; Legacy SRV and TXT for compatibility
HomeDoT._dot._tcp.local. 120 IN SRV 0 5 853 router.home.local.
HomeDoT._dot._tcp.local. 120 IN TXT "adn=dns.home.net" "fp_sha256=9F86D08188..."
router.home.local. 120 IN A 192.168.1.1
router.home.local. 120 IN AAAA fd12:3456::1
```

8.2. DoH Service with Custom Path using HTTPS RR

```
OfficeDoH._doh._tcp.local. 7200 IN HTTPS 1 dnsgateway.corp.local. alpn=h2,h3 dohpath=/int
ernal/dns adn=dns.corp.example
```

8.3. Client Discovery Sequence with SVCB

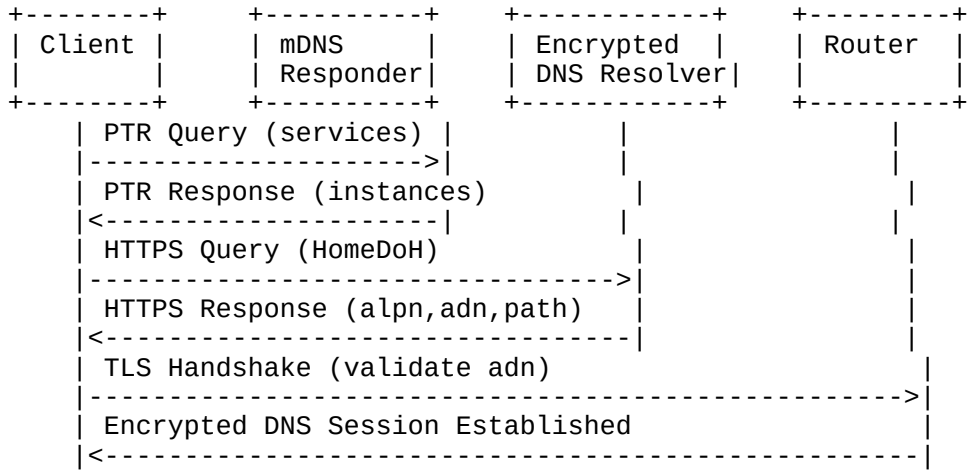

Figure 2: Client Discovery Sequence

9. References

9.1. Normative References

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[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>.

[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>.

[RFC6335] Cotton, M., Eggert, L., Touch, J., Westerlund, M., and S. Cheshire, "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry", BCP 165, RFC 6335, DOI 10.17487/RFC6335, August 2011, <https://www.rfc-editor.org/info/rfc6335>.

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>.

[I-D.ietf-add-ddr] Reddy.K, T., Boucadair, M., Cook, N., and D. Wing, "Discovery of Designated Resolvers", Work in Progress, Internet-Draft, draft-ietf-add-ddr-latest, <https://datatracker.ietf.org/doc/html/draft-ietf-add-ddr-latest>.

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

9.3. Other References

[RFC-TBD] Liu, D., Yan, Z., Geng, G., and G. Zeng, "DNS-Based Service Discovery for Encrypted DNS Services", RFC TBD, 2025, <https://www.rfc-editor.org/rfc/rfcTBD>.

Acknowledgements

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

The authors would like to thank Stuart Cheshire, Chris Box, Tommy Jensen, Michel Franテァois, Lorenzo, Tommy Pauly, Jim Reid, Petr Menナ。テュk, Amanda Baber (IANA), テ詠ic Vyncke and the ADD working group chairs for their valuable feedback during IETF 124 and on the mailing list. We also appreciate comments from other participants in the ADD working group.

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

G. Zeng
Jinan University
Email: zeng.guoqiang5@gmail.com