DNSOP Working Group
Internet-Draft
Intended status: Standards Track
Expires: 23 April 2026

J. Stenstam
L. Fernandez
E. Bergstr旦m
The Swedish Internet Foundation
P. Homberg
NLnet Labs
S. Dickinson
Sinodun IT
20 October 2025

Authoritative DNS Transport Signaling
draft-johani-dnsop-transport-signaling-02

Abstract

This document proposes a mechanism for authoritative DNS servers to signal their support for alternative transport protocols (e.g., DNS over TLS (DoT), DNS over HTTPS (DoH) and DNS over QUIC (DoQ)). This signaling may either be provided within the Additional section of authoritative DNS responses or be the result of direct DNS queries.

The former, "opportunistic mode" is hint-based and aims to enable resolvers to discover alternative transports efficiently and then opportunistically upgrade connections to the authoritative, thereby improving privacy, security, and performance for subsequent interactions. The mechanism is designed to not require any protocol change or additional queries. It is safe, backward-compatible, and effective even when DNSSEC validation of the hint is not possible or desired.

In certain circumstances and with additional overhead it is also possible to use direct queries to securely obtain authentication information for the authoritative that can then be used to authenticate an encrypted connection.

It is also possible to establish a "validated mode" where the communication between the resolver and the authoritative server is provably both secure and authentic. Validated mode may not always be possible, depending on whether the resolver is able to DNSSEC validate the signal or not. When Validated mode is possible it does provide a stronger and more trustworthy connection.

This document proposes an improvement to the opportunistic (but blind) testing of alternative transports suggested in RFC9539 by providing a mechanism by which a responding authoritative server may signal what alternative transports it supports.

TO BE REMOVED: This document is being collaborated on in Github at: https://github.com/johanix/draft-johani-dnsop-transport-signaling (https://github.com/johanix/draft-johani-dnsop-transport-signaling). The most recent working version of the document, open issues, etc, should all be available there. The authors (gratefully) accept pull requests.

Status of This Memo

Copyright Notice

Table of Contents

1. 1. Introduction

The Domain Name System (DNS) primarily relies on UDP and TCP for communication between resolvers and authoritative servers. While these protocols are well-established, there is a growing interest in leveraging modern transport protocols like DNS over TLS (DoT) [RFC7858], DNS over HTTPS (DoH) [RFC9461] and DNS over QUIC (DoQ) [RFC9250] to enhance privacy, security, and performance.

Clients of authoritative servers (recursive resolvers) may employ various policies (usage profiles) when attempting to connect to an authoritative. Two policies are described for the stub to recursive case in RFC8310, Strict and Opportunistic which are also applicable here:

* Strict mode relies on the client having securely discovered authentication information (e.g. a name or SPKI) for the server and then choosing to hard fail if an authenticated encrypted connection cannot be established. This protects against active attack on the resulting connection (however a denial-of-service attack is possible).

* Opportunistic mode ([RFC7435]) starts with cleartext as a baseline with upgrade to encrypted transport and authentication of the connection when available. This is a best effort attempt to set up an encrypted DNS transport connection. This can provide enhanced privacy against a passive attacker. However an active attacker may be able to force a downgrade to unencrypted DNS.

Opportunistic mode can proceed based on, for example, probing of server capabilities (as in [RFC9539]) however a mechanism to signal such capabilities has a number of advantages.

Existing efforts to signal service connection information, such as the SVCB and HTTPS DNS records [RFC9460] [RFC9461], primarily focus on service discovery mechanisms where a client explicitly queries for these records, often from a parent zone. While robust, this approach can introduce additional latency and requires explicit configuration at the parent zone level.

This document proposes a new hint-based "DNS Transport Signaling" (DTS) mechanism. DTS, aka an "DTS Hint" allows an authoritative DNS nameserver to directly convey its transport capabilities as a hint within the Additional section of responses to queries where it identifies itself as an authoritative nameserver for the requested zone. This direct, in-band signaling provides a low-latency discovery path, even when a formal, validated signal is not available. Furthermore, this is achieved without any changes to the DNS Protocol.

The information conveyed by this hint alone signals only the capabilities of the authoritative nameserver serving the zone. It does not, therefore, establish a full chain of trust directly to the zone itself and should be considered as insecure. It should not be used as a basis of a Strict policy, only to enable Opportunistic transport. However, receiving such a signal enables resolvers to immediately attempt to establish an opportunistically encrypted connection to the resolver without further queries being required.

The focus of this document is the hint-based signaling of transport capabilities, however Section 6.2 outlines in detail the specific requirements for how DNSSEC signed authoritatives can provide, and willing resolvers can directly query for, a set of records than can securely provide authentication information for an authoritative nameserver that a resolver could then use to implement a Strict usage policy.

1.1. 1.1. Confidentiality

The above text discusses discovery of transport signals and authentication information in queries made by the recursive resolver. Those queries may or may not occur over encrypted or authenticated connections. Only when all the connections are authenticated are all the queries protected from active surveillance. If all the connections are opportunistically encrypted then the queries are protected from passive surveillance. Otherwise they may occur in cleartext, or a combination of circumstances may exist.

Such queries leak the name of the zone that the resolver wishes to ultimately query which in itself can be sensitive. During the early stages of the incremental rollout of technologies such as recursive to authoritative encrypted connections it is unlikely that fully confidential discovery will be possible due to the nature of the DNS hierarchy. However, if large TLDs and/or those hosted by large CDNs support encrypted transports a significant number of queries from busy resolvers to discovery information on TLD child zones (and below) could be performed confidentially thereby greatly improving the privacy over the current situation.

1.2. 1.2. Prior Art

An attempt at utilizing more modern, and in particular, more private transports between resolvers and authoritative nameservers was introduced in [RFC9539]. The idea there was to opportunistically try to send the query to the authoritative nameserver over multiple transports with no prior knowledge of whether a transport was supported in the receiving end or not.

The drawback with that approach is that without any significant deployment of authoritative support the resolver end will mostly spend cycles and traffic on a wasted effort. For this reason their deployment has been limited.

Furthermore, in Appendix B of [RFC9539] requirements for improving the defense against an active attacker are listed. The first requirement is:

* A signaling mechanism that tells the recursive resolver that the authoritative server intends to offer authenticated encryption.

This document aims to provide exactly such a mechanism while staying within the current DNS protocol. Therefore the DNS transport signaling provided will be hint-based, and as such fit well as an improvement to [RFC9539].

1.3. 1.3. Rationale for Using the Additional Section

See Appendix A for the rationale for using the Additional section for the transport signaling hint.

2. 2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals.

* *Authoritative Nameserver (Auth Server):* A DNS server that holds the authoritative zone data for a specific domain.

* *Recursive Nameserver (Resolver):* A DNS server that processes user queries, performing iterative lookups to authoritative servers to resolve domain names.

* *DTS Hint:* An SVCB record included in the Additional section of an authoritative DNS response, intended to signal the responding authoritative nameserver’s transport capabilities.

* *SVCB Record:* Service Binding record, as defined in [RFC9460].

3. 3. Modes of Operation

This document describes a mechanism of DNS transport signaling intended to result in improved communication between the resolver and the authoritative nameserver. This DNS transport signal is provided via an SVCB record that describes the transport capabilities of the authoritative server.

In the easiest case the resolver will be able to communicate securely with the authoritative server using an encrypted channel (like DoQ or DoT), but the resolver does not have the identity of the authoritative server proven. This is referred to as "opportunistic mode" and is essentially equivalent to the communication used today over UDP/TCP with the addition of privacy.

The second level of communication is when the resolver is able to verify the identity of the authoritative server via validation of a DNSSEC signature over the DNS transport signal (which is contained in an SVCB record). This is referred to as "validated mode" and is equivalent to the opportunistic mode plus knowledge that the DNS transport signal provably describes the authoritative server that the resolver is communicating with.

In opportunistic mode, the authoritative server and the recursive resolver make a best effort attempt to set up an encrypted DNS transport connection. This provides enhanced privacy against a passive attacker. However an active attacker may be able to force a downgrade to unencrypted DNS.

3.1. 3.1. Description of Problem Space

This section looks at the various configurations that need to be supported.

For opportunistic mode to be possible, the authoritative server needs to provide the recursive resolver with the DNS transport signaling record even when the recursive resolver does not explicitly ask for it (i.e. as a hint, in the Additional Section). For example by adding it to the result of an A or AAAA query for a name server. The recursive resolver accepts such a record and uses it to set up a secure transport.

There are three zones that matter in this analysis: the parent zone, the child zone, and the zone that contains the name server addresses and transport signaling records. Note that the name server addresses may be located in the child zone. And some of the three zones may be served by the same name server.

The parent zone contains the delegation NS RRset for the child which is not DNSSEC signed. Therefore it does not matter if the parent zone is DNSSEC signed or not in terms of validating the child NS RRset.

For the child zone there are also two possibilities, the child zone is DNSSEC secure or not.

For the nameserver transport signaling there are two possibilities: either the zone that holds the nameserver information is DNSSEC secure or it is DNSSEC insecure (i.e. the signaling needs to be learned opportunistically and later possibly be validated by direct query to the SVCB owner name).

3.1.1. 3.1.1. Validated Transport Signaling Not Possible

There are cases where validated transport signaling is unavailable. One case is when the zone that holds the nameserver records is not DNSSEC secure. In that case obtaining transport signaling in a validated way is not possible without additional trust.

Another case is where the parent zone does not provide a path that allows validating the child NS RRset and the child zone is not DNSSEC secure. In that case obtaining a list of the child's nameservers in a validated way is impossible.

3.1.2. 3.1.2. Validated Transport Signaling Possible

The remaining cases can be analysed as follows.

If the zone that holds the nameserver records is DNSSEC secure then it is often sufficient if the nameserver adds DNS transport signaling along with an A or AAAA response (including signatures).

If no signed signaling is received opportunistically then the resolver SHOULD issue an explicit query for the SVCB RRset at the SVCB owner name (_dns.{nameserver FQDN}) to obtain a validated signal or a secure denial of existence.

3.2. 3.2. Behaviour of the Two Modes

3.2.1. 3.2.1. Opportunistic Mode

Opportunistic mode applies when the DTS Hint (the SVCB record) for the authoritative nameserver is received opportunistically in the Additional section as part of the response to a DNS query for something else. The hint may or may not be DNSSEC-signed and may or may not be successfully validated by the resolver.

3.2.1.1. Behavior:

* If the SVCB record and its signatures are DNSSEC-validated, the resolver MAY treat it equivalently to Validated mode for the corresponding data.

* If the SVCB record is not validated (e.g., unsigned, or validation fails), then:

  - The resolver MAY use only positive "alpn" entries to attempt a transport upgrade (e.g., dot, doq).

  - The resolver MUST ignore the negative transport signal "-do53", if present.

  - The resolver MUST ignore ipv4hint, ipv6hint, tlsa, and any other parameters that affect addressing or authentication.

  - The resolver MUST be prepared to immediately fall back to traditional UDP/TCP (Do53) upon failure or timeout.

3.2.1.2. Rationale:

* Opportunistic mode enables low-latency discovery without requiring changes at parent zones or prior configuration, while containing risk by limiting use of unvalidated data to only positive upgrade attempts.

3.2.2. 3.2.2. Validated Mode

Validated mode applies when the resolver explicitly queries for the SVCB RRset at the SVCB owner name for the nameserver (i.e., _dns.{nameserver FQDN}) and obtains a DNSSEC-signed response that is successfully validated to the appropriate trust anchor.

3.2.2.1. Requirements and behavior:

* The resolver MUST issue a direct query for the SVCB RRset at _dns.{nameserver FQDN}.

* The resolver MUST successfully DNSSEC-validate the SVCB RRset and its RRSIGs.

* When validated, the resolver MAY use all fields of the SVCB RDATA for connection establishment and policy decisions, including:

  - alpn: positive transport signals (e.g., dot, doq) and the negative transport signal "-do53" (if present).

  - ipv4hint / ipv6hint: address hints for the authoritative nameserver.

  - tlsa: a new SVCB parameter defined by this document that conveys the TLSA record to authenticate TLS/QUIC connections to the authoritative nameserver.

* If a validated SVCB contains the explicit negative transport signal "-do53", the resolver SHOULD honor it. The "-do53" signal indicates that legacy UDP/TCP is NOT supported by this authoritative nameserver and the resolver SHOULD attempt only other advertised transports (if any). If all transport alternatives fail in the validated case the resolver SHOULD treat that server as unreachable and prefer other authoritative servers for the zone.

3.3. 3.3. Precedence and Interaction

* Validated transport signals MUST take precedence over Opportunistic transport signals.

* A validated Opportunistic transport signal is equivalent to a Validated transport signal for policy and usage purposes.

* An Opportunistic (unvalidated) transport signal MUST NOT be used to enforce negative transport policy ("-do53"), alter addressing ("ipv4hint/ipv6hint"), or bootstrap authentication material ("tlsa").

3.4. 3.4. Caching and No-DTS

* Resolvers MAY cache Validated-mode SVCB information according to its TTL and MAY use the EDNS(0) No-DTS option to avoid redundant hints when sufficient information is cached.

* In Opportunistic mode, resolvers MAY cache positive "alpn" results subject to local policy (see Resolver Caching Strategies). When a resolver has sufficient cached information, it SHOULD set No-DTS to reduce response size and limit unnecessary hints.

3.5. 3.5. Summary of Permitted Use by Mode

* Opportunistic:

  - MAY use: alpn: "doq", "dot", "h2" and "h3" only.

  - MUST NOT use: alpn: "-do53", ipv4hint, ipv6hint, tlsa, or any parameter that affects addressing or authentication.

- MUST support fallback to do53 (i.e. UDP/TCP).

* Validated:

  - MAY use: alpn: "doq", "dot", "h2", "h3", "-do53", ipv4hint, ipv6hint, tlsa, and other defined parameters.

Implementation note: - Existing resolvers that do not understand the alpn="-do53" token or the new "tlsa" parameter will ignore them and remain interoperable. Clients implementing this specification MUST follow the above mode-dependent processing and precedence rules.

4. 4. The Opportunistic Signaling Mechanism

The core of this proposal is for an authoritative nameserver to include a DNS transport signal in the form of an SVCB record in the Additional section of its responses under specific conditions.

This consists of three parts. The first two are the behaviour of the authoritative nameserver receiving the query and the behaviour of the recursive nameserver receiving the response. The final part is a new EDNS(0) option that defines an OPT-OUT capability.

5. 5. Authoritative Nameserver Behaviour

5.1. 5.1. Trigger Conditions for Including the DTS Hint

An authoritative nameserver SHOULD include an DTS Hint when _all_ of the following conditions are met:

1. *Self-Identification:* The responding authoritative own Fully Qualified Domain Name (FQDN) (or one of its configured aliases/ identities) is found within the NS RRset for the queried zone.

2. *Transport Capability:* The responding authoritative nameserver supports one or more alternative transport protocols (e.g., DoT, DoH, DoQ) and is configured to advertise these capabilities. Or the nameserver does not (temporarily or permanently) support DNS over legacy UDP/TCP transport and is configured to advertise this fact.

3. *SVCB not present in Answer:* If the SVCB record is present in the Answer section (because it was explicitly queried for), then it does not have to be included again in the Additional section, regardless of whether the resolver has set the DTS Option or not.

5.2. 5.2. Multiple Server Identities

An authoritative nameserver may be known by multiple FQDNs (e.g., ns1.example.com, dns.customer.org, ns.cdnprovider.net). To facilitate condition 1 ("Self-Identification"), authoritative server implementations MAY include a configuration mechanism (e.g., an identities list) where operators can list FQDNs by which the server is known. This allows the server to correctly identify itself regardless of the specific name used in the NS RRset.

5.3. 5.3. Format of the DNS Transport Signal SVCB Record

The DTS Hint MUST be an SVCB record with the following characteristics:

* *OWNER:* The owner name of the SVCB record MUST be the label "_dns" followed by the FQDN of the authoritative nameserver itself, as identified in the NS RRset that triggered its inclusion (e.g., _dns.ns.dnsprovider.com.).

* *CLASS:* IN (Internet).

* *TYPE:* SVCB.

* *TTL:* The TTL of the SVCB record SHOULD be chosen by the authoritative server operator. Choice of TTL is a local configuration decision, but unless the supported transports are subject to frequent change a value on the order of 24h or more is suggested.

* *SVCB_PRIORITY:* 1. The specific priority value is not critical for this hint mechanism, but 1 indicates the highest priority for the service.

* *SVCB_TARGET:* . (root). This indicates that the DNS transport capabilities described by the SVCB record refer to the owner name of the record.

* *SVCB_PARAMS:* A set of Service Parameters indicating the supported transport protocols. This document uses the "alpn" parameter [RFC9460] for signaling DoT (alpn=dot) and DoQ (alpn=doq). It further defines the new alpn parameter token "-do53" for signaling lack of support for UDP/TCP. Resolvers MUST treat "-do53" as actionable only when the SVCB RRset has been DNSSEC-validated (Validated mode).

The SVCB parameters "ipv4hint" and "ipv6hint" MAY be included. Resolvers MUST use these address hints only when the SVCB RRset has been successfully validated (Validated mode).

A new "tlsa" SVCB parameter contains the corresponding TLSA record for the certificate used to secure a DoQ or DoT transport. Resolvers MUST use "tlsa" only when the SVCB RRset has been successfully validated (Validated mode).

If any other parameter is present in the SVCB parameter list it must be ignored by the resolver.

Example 1:

If ns.dnsprovider.net. responds to a query for www.example.com. (in the unsigned zone example.com.) and ns.dnsprovider.net is listed in the NS RRset for example.com., it may respond with a DNS message that contains: ~~~ Header: ...

Answer: www.example.com. IN A 1.2.3.4

Authority: example.com. IN NS ns1.example.com. example.com. IN NS ns.dnsprovider.net.

Additional: ns.dnsprovider.net. IN A 5.6.7.8 ns.dnsprovider.net. IN RRSIG A ... _dns.ns.dnsprovider.net. IN SVCB 1 . "alpn=doq,dot,do53" _dns.ns.dnsprovider.net. IN RRSIG SVCB ... ~~~

Example 2: The resolver explicitly asks for the DNS transport signal for the authoritative nameserver ns.dnsprovider.net. by querying for "_dns.ns.dnsprovider.net. SVCB": ~~~ Header: ...

Answer: _dns.ns.dnsprovider.net. IN SVCB 1 . (alpn="doq,dot,-do53", tlsa="...") _dns.ns.dnsprovider.net. IN RRSIG SVCB ...

Additional: ~~~ Because the resolver uses Validated mode (by querying for the SVCB record at _dns.{nameserver FQDN} and validating the response) all data in the received SVCB record MAY be used. In this case that includes the negative transport signal "-do53", which will effectively turn off UDP/TCP use by the resolver for communicating with this particular authoritative nameserver.

6. 6. Recursive Nameserver Behavior

Recursive nameservers adopting this mechanism SHOULD implement the following logic:

6.1. 6.1. When Sending Queries

1. *OPT-OUT Possibility:* If the resolver already thinks that it knows the transport capabilities of the authoritative nameserver it is about to send a query to it may opt out from DNS transport signaling by including an EDNS(0) "No-DTS" option in the query.

   It is important to be aware that using the No-DTS option consistently will make the resolver blind to any changes in the transport signals, which is clearly not acceptable. Hence any use of "No-DTS" should be restricted to only be used within the TTL of an already received and parsed DTS Hint.

6.2. 6.2. When Receiving Responses

1. *Opportunistic Parsing:* When receiving an authoritative DNS response, the resolver SHOULD parse the Additional section for SVCB records.

2. *Owner Check:* If an SVCB record is found whose owner name matches the "_dns" label followed by an authoritative nameserver name for the zone to which the query belongs, the resolver MAY consider this an DTS Hint.

3. *DNSSEC Validation (Optional but Recommended):*

   * The resolver SHOULD attempt to DNSSEC validate the DTS Hint. This involves validating the SVCB record itself and its corresponding RRSIG (if present) against the DNSSEC chain of trust for the zone that owns the SVCB record (e.g., dnsprovider.com for _dns.ns.dnsprovider.com).

   * If validation succeeds: The DTS Hint is considered a *trusted signal*. The resolver MAY then use all the transport signals provided in the SVCB record when deciding on alternative transport choices for subsequent queries to that specific authoritative nameserver.

   * If validation fails, or no RRSIG is present: The DTS Hint MUST be treated as an *unvalidated hint*. The resolver MAY still opportunistically attempt to use the signaled alternative transports, but MUST be prepared for immediate fallback to traditional transports (UDP/TCP) if the connection fails. This is particularly relevant for scenarios like vanity names (e.g., ns.customer.com where customer.com is an unsigned zone, but the underlying server ns.dnsprovider.com is capable).

4. *Prioritization:* * Any DNSSEC-validated SVCB record found via explicit query (e.g., _dns.ns.example.com for a queried domain) MUST take precedence over any unvalidated DTS Hint.

* The DTS Hint is a mechanism to _discover_ capabilities opportunistically, not to override trusted delegation or service configuration.

1. Fallback: Resolvers MUST always be prepared to fall back to traditional UDP/TCP transport if an attempt to use an alternative transport based on an DTS Hint (especially an unvalidated one) fails or times out.

6.3. 6.3. Upgrading the DNS Transport Signal

If an unvalidated opportunistic transport signal has been received the resolver may choose to upgrade that signal, either immediately or when the transport signal is close to expiration from the resolver cache. An upgraded transport signal allows the resolver to operate in Validated mode, and then use all the information in the SVCB record (including "-do53", ipv4hint/ipv6hint, and tlsa).

6.4. 6.4. Authentication of the Authoritative Nameserver

Authentication of the authoritative nameserver is not an explicit goal in opportunistic mode. The reason is that as an opportunistic mechanism it will not always be possible to do such authentication.

However, even without strong authentication of the authoritative server the proposed mechanism still provides benefits (privacy, potential performance improvements) and for that reason cryptographic verification of the server identity is not a requirement.

In validated mode authentication of the authoritative nameserver is done by validation of the DNSSEC RRSIG over the SVCB record containing the DTS Hint.

Finally, validating the server cert against a list of well-known public Certificate Authorities is possible, but there is no standardized way to determine which CAs are appropriate for DNS server certificates.

6.5. 6.5. Resolver Caching Strategies

Resolvers implementing the DNS DTS Hint mechanism have several options for caching the transport signals received via DTS Hints.

A suggested primary strategy is to set the EDNS(0) No-DTS option when no transport signaling information is needed. This may be because the resolver already knows the authoritative nameserver's transport capabilities from a previous response (with a TTL that has not expired) or for some other reason.

The primary caching strategy SHOULD be "Standard DNS Cache", i.e. treat the SVCB record like any other DNS record, caching it according to its TTL. This is the simplest approach and will simply cause the resolver to fall back to UDP for one query if the transport signal data has expired.

For a more detailed analysis of possible caching logic, see [RFC9539], section 4.

Note that the resolver always has the option of not using the EDNS(0) No-DTS option whenever the cache entry is getting close to expiry.

Given the variety of deployment scenarios and operational requirements, this document does not mandate a specific caching strategy. Implementers SHOULD choose a strategy that best fits their operational needs, considering factors such as:

* The importance of minimizing connection attempts

* The impact of failed connection attempts

* The computational cost of different caching strategies

* The memory requirements of maintaining cache state

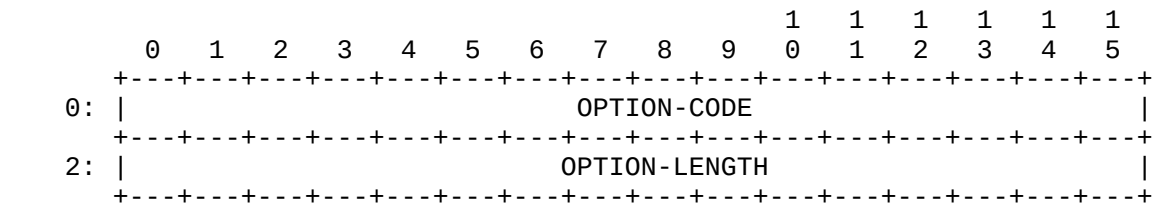
The chosen strategy SHOULD be documented in the implementation's configuration options to allow operators to make informed decisions about its use.

7. 7. The EDNS(0) No-DTS Option

To provide a mechanism for resolvers to explicitly opt out of receiving transport signals, this document defines a new EDNS(0) option called "No-DTS". When included in a query, this option signals to the authoritative server that the resolver does not want to receive any transport signals in the response.

The typical use case is to set the EDNS(0) No-DTS option when the resolver already has the transport information it needs.

The EDNS(0) No-DTS option is structured as follows:



Field definition details:

OPTION-CODE: 2 octets / 16 bits (defined in [RFC6891]) contains the value TBD for No-DTS.

OPTION-LENGTH: 2 octets / 16 bits (defined in [RFC6891]) contains the length of the payload in octets. For the No-DTS option, this value MUST be 0 as there is no payload.

When an authoritative server receives a query containing the EDNS(0) No-DTS option, it SHOULD NOT include any DTS Hints in the response, regardless of whether it would normally do so based on the conditions described in Section 5.1.

This option provides a clean way for resolvers to opt out of receiving transport signals, which may be useful in scenarios where:

* The resolver has recently established transport preferences for a particular authoritative server and that transport signal has not expired.

* The resolver does not support or does not want to use alternative transports

* The resolver wants to minimize response sizes

* The resolver is operating in an environment where transport signals are not needed or desired

The No-DTS option is designed to be a simple, lightweight mechanism that can be used to disable transport signaling without affecting the normal operation of DNS resolution.

8. 8. Comparison with DELEG

The idea to use an SVCB alpn parameter for transport signaling originated with the work on DELEG [I-D.draft-ietf-deleg]. The current document uses the same data format, but as an opportunistic addition to the Additional section rather than as integral part of a changed delegation mechanism.

Both mechanisms have distinct use cases, and pros and cons. The major advantage of the DELEG mechanism is that it cannot be spoofed or filtered, as it is an integral part of an upcoming protocol change.

The opportunistic mechanism described here has the major advantage of being available immediately without any changes to the DNS protocol. Furthermore, as it is a signal directly from an authoritative nameserver, a single DTS Hint may allow the recipient recursive nameserver to upgrade the transport used for all the zones served by that authoritative nameserver (which may be millions) without the need to make any changes to the zones, nor to the parent zones.

Given the current DNS landscape with a limited number of very large providers of authoritative DNS service and a limited number of large providers of recursive DNS service the opportunistic model described here has the potential of enabling upgrading the transport for a significant fraction of the DNS traffic with a limited amount of effort.

9. 9. Security Considerations

* *Spoofing of Unvalidated Hints:* An DTS Hint that cannot be DNSSEC validated (e.g., for ns.example.com where example.com is unsigned) is susceptible to spoofing by an on-path attacker. Such an attacker could insert a fake SVCB record advertising a non-existing transport, thereby denying connection over that transport. However, since the hint is opportunistic and not required for DNS resolution, the worst-case scenario is that the resolver attempts a connection that fails and then falls back to traditional transports. Security for the actual DNS data remains unaffected. The cryptographic validation of TLS/QUIC (via X.509 certificates) for DoT/DoQ would still protect the integrity and privacy of the connection itself.

* *DNSSEC Validation:* When a DTS Hint is signed by DNSSEC (e.g., the ns.dnsprovider.net SVCB record from a signed dnsprovider.net zone), it provides a trusted signal. Resolvers SHOULD leverage DNSSEC validation to distinguish between trusted and unvalidated hints.

* *No New Attack Vectors:* This mechanism does not introduce new attack vectors for DNS data itself, as it primarily concerns transport discovery. It relies on the existing security properties of DoT, DoH and DoQ for actual session security.

* *Safe Rollout:* As existing recursive nameservers carefully avoid data in the Additional section that they do not need, the DTS Hint will be ignored by everyone except recursive nameservers that understand the DTS Hint.

* *No-DTS enables a downgrade attack:* If an attacker is able to inject a No-DTS option to an outbound query then no transport signal will be provided. However, this is a consequence of the opportunistic nature of the DTS Hint and not worse than not being able to do transport signaling at all.

10. 10. Operational Considerations

* *Response Size:* Including an SVCB record in the Additional section will increase the size of UDP responses. Authoritative server operators should consider the potential for UDP fragmentation or TCP fallback if responses become excessively large, though a single SVCB record is typically small. Recursive nameservers should usually set the EDNS(0) No-DTS when they already have the transport signaling information.

* *Server Configuration:* Authoritative server implementations will need configuration options to enable this feature and manage the identities list.

* *Rollout Strategy:* This mechanism supports a gradual rollout. Authoritative servers can begin sending hints without requiring changes from resolvers, and resolvers can begin processing hints without requiring all authoritative servers to implement the feature.

* *Monitoring:* As there is extremely limited data on effects of alternative DNS transports for communication resolver to authoritative nameserver it is strongly suggested that monitoring (of use, resource consumption, etc) is considered.

11. 11. IANA Considerations

11.1. 11.1. No-DTS EDNS(0) Option

This document defines a new EDNS(0) option, entitled "No-DTS", assigned a value of TBD in the "DNS EDNS0 Option Codes" registry.

Value	Name	Status	Reference
TBD	No-DTS	Standard	(This document)

Note to the RFC Editor: In this section, please replace occurrences of "(This document)" with a proper reference.

11.2. 11.2. SVCB/HTTPS Parameter: tlsa

This document requests registration of a new SVCB/HTTPS parameter in the "SVCB and HTTPS Parameters" registry:

Key	Name	Meaning	Reference
TBD	tlsa	Carries TLSA data	(This document)

Presentation and wire format: The value carries one or more TLSA RRs associated with the nameserver endpoint. Exact encoding and size limits are defined by this document (TBD). Use of this parameter is appropriate only when the containing SVCB RRset is DNSSEC-validated (see Section 3).

11.3. 11.3. The New SVCB alpn Token "-do53"

This document updates the "alpn" SVCB parameter with one additional token, "-do53", used to signal lack of support for UDP/TCP, i.e. a negative transport capability. Note that at present support for UDP/TCP is required for authoritative nameservers.

The "-do53" token has two use cases. The first is for temporary service interruptions (i.e. a busy nameserver that only supports UDP/TCP transport may signal alpn="-do53" prior to being offline for maintenance). The second is for a future where a significant fraction of authoritative DNS traffic has migrated to encrypted transports and it may be reasonable to not support every transport at every nameserver.

IANA is requested to add the "-do53" token to the list of defined tokens for the "SVCB and HTTPS Parameters" registry entry for "alpn" and reference this document. A new ALPN ID must be allocated for "-do53".

12. 12. Acknowledgements

* Many people have commented and contributed to this document in different ways. In no particular order and with a significant risk of forgetting someone: The participants of the DELEG Working Group, Peter Thomassen, Christian Elmerot, John Todd, Peter Koch, Willem Toorop, Peter van Dijk.

13. Appendix A. Rationale for Using the Additional Section

Note to the RFC Editor: Please remove this entire section before publication.

13.1. A.1. Opportunistic Mode Via the Additional Section

When designing a mechanism that relies on sending new information in DNS responses without changing the current DNS protocol, the Additional section has the major advantage of being ignored by legacy software. This property makes it possible to essentially deploy the proposed mechanism immediately, as it will not cause problems with existing DNS infrastructure.

* Existing authoritative nameservers will not provide any DTS Hint in the Additional section.

* Existing resolvers will actively ignore any DTS Hint in the Additional section.

Only DNS nameservers (authoritative or recursive) that are aware of the proposed mechanism will use it.

The downside is that it is not possible to strictly rely on anything specific being present in the Additional section, as it may be stripped off by a middle man or even by the sending nameserver (eg. due to packet size constraints). For this reason it is not possible to provide more than an opportunistic transport signal when the signal is not explicitly queried for.

This is usually a major issue and the primary reason that data in the Additional section is actively ignored by resolvers. In this particular case, though, even an untrusted transport signal is better than no signal at all. Furthermore, the only effect of a forged or otherwise incorrect transport signal is a, typically failed, connection attempt to an authoritative nameserver that does not support the advertised transport. This will cause immediate fallback to "Do53", i.e. traditional DNS over UDP/TCP and the non-availability of the advertised transport will be remembered by the resolver (for some suitable time).

Hence, using the Additional section for opportunistic transport signaling has vastly more benefits than drawbacks.

13.2. A.2. Validated Mode Via the Additional Section

If the transport signal is present in the Additional section, it may or may not be possible to validate it (if it has a DNSSEC signature).

This is necessary to bee able to trust more sensitive signals. A positive signal inserted by an on-path attacker (eg. claiming DoQ support when this is false) would not be catastrophic. However, a false negative alpn="-do53" signal (eg. claiming no Do53 support while such support is present) would be potentially catastrophic. For this reason (ability to trust more sensitive signals) the connection between resolver and authoritative server must be in Validated Mode.

14. Appendix B. SVCB ALPN Negative Tokens

This appendix defines a presentation-time extension to the SVCB "alpn" parameter that allows an authoritative nameserver to signal explicit non-support of a transport by prefixing an existing ALPN token with a hyphen ("-"). For example, "-do53" indicates that legacy UDP/TCP transport is not supported.

Processing rules: - The "-do53" negative token is only actionable when the SVCB RRset is DNSSEC-validated (Validated mode). In these cases, resolvers SHOULD honor the "-do53" token when selecting transports. - In Opportunistic (unvalidated) mode, resolvers MUST ignore the "-do53" negative token.

Examples: - alpn="dot,doq" -> Indicates support for DoT and DoQ. - alpn="-do53,dot" -> Indicates no Do53; use DoT (validated modes only). - alpn="-do53,doq,dot" -> Indicates no Do53; prefer DoQ/DoT (validated modes only).

Interoperability considerations: - Implementations that do not understand the alpn "-do53" negative token will ignore it per SVCB parameter processing and remain interoperable. - This alpn token does not alter on-the-wire encoding for ALPN; it is a presentation-layer convention. IANA considerations for documentation of this convention are provided in Section 11.3.

15. References

15.1. 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/rfc/rfc2119>.

[RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, RFC 6891, DOI 10.17487/RFC6891, April 2013, <https://www.rfc-editor.org/rfc/rfc6891>.

[RFC7435] Dukhovni, V., "Opportunistic Security: Some Protection Most of the Time", RFC 7435, DOI 10.17487/RFC7435, December 2014, <https://www.rfc-editor.org/rfc/rfc7435>.

[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/rfc/rfc7858>.

[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/rfc/rfc8174>.

[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/rfc/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/rfc/rfc9460>.

[RFC9461] Schwartz, B., "Service Binding Mapping for DNS Servers", RFC 9461, DOI 10.17487/RFC9461, November 2023, <https://www.rfc-editor.org/rfc/rfc9461>.

[RFC9539] Gillmor, D. K., Ed., Salazar, J., Ed., and P. Hoffman, Ed., "Unilateral Opportunistic Deployment of Encrypted Recursive-to-Authoritative DNS", RFC 9539, DOI 10.17487/RFC9539, February 2024, <https://www.rfc-editor.org/rfc/rfc9539>.

15.2. Informative References

[I-D.draft-ietf-deleg] April, T., ナaek, P., Weber, R., and Lawrence, "Extensible Delegation for DNS", Work in Progress, Internet-Draft, draft-ietf-deleg-05, 20 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-deleg-05>.

Appendix A. Change History (to be removed before publication)

Initial public draft

Authors' Addresses

Johan Stenstam
The Swedish Internet Foundation
Sweden
Email: johan.stenstam@internetstiftelsen.se

Leon Fernandez
The Swedish Internet Foundation
Sweden
Email: leon.fernandez@internetstiftelsen.se

Erik Bergstrm
The Swedish Internet Foundation
Sweden
Email: erik.bergstrom@internetstiftelsen.se

Philip Homberg
NLnet Labs
Email: philip@nlnetlabs.nl

Sara Dickinson
Sinodun IT
United Kingdom
Email: sara@sinodun.com