

Workgroup: add
Internet-Draft: draft-ietf-add-svc-b-dns-01
Published: 21 October 2021
Intended Status: Standards Track
Expires: 24 April 2022
Authors: B. Schwartz
Google LLC
Service Binding Mapping for DNS Servers

Abstract

The SVCB DNS record type expresses a bound collection of endpoint metadata, for use when establishing a connection to a named service. DNS itself can be such a service, when the server is identified by a domain name. This document provides the SVCB mapping for named DNS servers, allowing them to indicate support for new transport protocols.

Discussion Venues

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the ADD Working Group mailing list (add@ietf.org), which is archived at <https://mailarchive.ietf.org/arch/browse/add/>.

Source for this draft and an issue tracker can be found at <https://github.com/bemasc/svc-b-dns>.

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 24 April 2022.

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

- [1. Introduction](#)
- [2. Conventions and Definitions](#)
- [3. Identities and Names](#)
 - [3.1. Special case: non-default ports](#)
- [4. Applicable existing SvcParamKeys](#)
 - [4.1. alpn](#)
 - [4.2. port](#)
 - [4.3. Other applicable SvcParamKeys](#)
- [5. New SvcParamKeys](#)
 - [5.1. dohpath](#)
- [6. Limitations](#)
- [7. Examples](#)
- [8. Security Considerations](#)
 - [8.1. Adversary on the query path](#)
 - [8.2. Adversary on the transport path](#)
- [9. IANA Considerations](#)
- [10. References](#)
 - [10.1. Normative References](#)
 - [10.2. Informative References](#)
- [Appendix A. Mapping Summary](#)
- [Acknowledgments](#)
- [Author's Address](#)

1. Introduction

The SVCB record type [[SVCB](#)] provides clients with information about how to reach alternative endpoints for a service, which may have improved performance or privacy properties. The service is identified by a "scheme" indicating the service type, a hostname, and optionally other information such as a port number. A DNS server is often identified only by its IP address (e.g. in DHCP), but in some contexts it can also be identified by a hostname (e.g. "NS")

records, manual resolver configuration) and sometimes also a non-default port number.

Use of the SVCB record type requires a mapping document for each service type, indicating how a client for that service can interpret the contents of the SVCB SvcParams. This document provides the mapping for the "dns" service type, allowing DNS servers to offer alternative endpoints and transports, including encrypted transports like DNS over TLS and DNS over HTTPS.

2. Conventions and Definitions

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, as shown here.

3. Identities and Names

SVCB record names (i.e. QNAMEs) are formed using Port-Prefix Naming ([Section 2.3](#) of [[SVCB](#)]), with a scheme of "dns". For example, SVCB records for a DNS service identified as "dns1.example.com" would be queried at "_dns.dns1.example.com".

In some use cases, the name used for retrieving these DNS records is different from the server identity used to authenticate the secure transport. To distinguish them, we use the following terms:

- *Binding authority - The service name ([Section 1.4](#) of [[SVCB](#)]) and optional port number used as input to Port-Prefix Naming.

- *Authentication name - The name used for secure transport authentication. It must be a DNS hostname or a literal IP address. Unless otherwise specified, it is the service name from the binding authority.

3.1. Special case: non-default ports

Normally, a DNS service is identified by an IP address or a domain name. When connecting to the service using unencrypted DNS over UDP or TCP, clients use the default port number for DNS (53). However, in rare cases, a DNS service might be identified by both a name and a port number. For example, the dns: URI scheme [[DNSURI](#)] optionally includes an authority, comprised of a host and a port number (with a default of 53). DNS URIs normally omit the authority, or specify an IP address, but a hostname and non-default port number are allowed.

When the binding authority specifies a non-default port number, Port-Prefix Naming places the port number in an additional a prefix

on the name. For example, if the binding authority is "dns1.example.com:9953", the client would query for SVCB records at "_9953._dns.dns1.example.com". If two DNS services operating on different port numbers provide different behaviors, this arrangement allows them to preserve the distinction when specifying alternative endpoints.

4. Applicable existing SvcParamKeys

4.1. alpn

This key indicates the set of supported protocols ([Section 6.1](#) of [\[SVCB\]](#)). There is no default protocol, so the no-default-alpn key does not apply, and the alpn key **MUST** be present.

If the protocol set contains any HTTP versions (e.g. "h2", "h3"), then the record indicates support for DNS over HTTPS [\[DOH\]](#), and the "dohpath" key **MUST** be present ([Section 5.1](#)). All keys specified for use with the HTTPS record are also permissible, and apply to the resulting HTTP connection.

If the protocol set contains protocols with different default ports, and no port key is specified, then protocols are contacted separately on their default ports. Note that in this configuration, ALPN negotiation does not defend against cross-protocol downgrade attacks.

4.2. port

This key is used to indicate the target port for connection ([Section 6.2](#) of [\[SVCB\]](#)). If omitted, the client **SHALL** use the default port for each transport protocol (853 for DNS over TLS [\[DOT\]](#), 443 for DNS over HTTPS).

This key is automatically mandatory if present. (See [Section 7](#) of [\[SVCB\]](#) for the definition of "automatically mandatory".)

4.3. Other applicable SvcParamKeys

These SvcParamKeys from [\[SVCB\]](#) apply to the "dns" scheme without modification:

*ech

*ipv4hint

*ipv6hint

Future SvcParamKeys may also be applicable.

5. New SvcParamKeys

5.1. dohpath

"dohpath" is a single-valued SvcParamKey whose value (both in presentation and wire format) MUST be a URI Template [RFC6570] encoded in UTF-8 [RFC3629]. If the "alpn" SvcParamKey indicates support for HTTP, "dohpath" MUST be present, and clients MAY construct a DNS over HTTPS URI Template as follows:

1. Let \$HOST be the authentication name encoded as a "host" value ([Section 3.2.2](#) of [RFC3986]).
2. Let \$PORT be the port from the "port" key if present, otherwise 443. (The binding authority's port number MUST NOT be used.)
3. Let \$DOHPATH be the "dohpath" value, decoded from UTF-8.
4. The DNS over HTTPS URI Template is "https://\$HOST:\$PORT\$DOHPATH".

The "dohpath" value MUST be chosen such that the resulting URI Template is valid for use with DNS over HTTPS. For example, DNS over HTTPS servers are required to support requests using GET and POST methods. The GET method relies on the "dns" URI Template parameter, and the POST method does not use it. Therefore, the URI Template is required to make use of a "dns" variable, and result in a valid URI whether or not "dns" is defined.

Clients SHOULD NOT query for any "HTTPS" RRs when using the constructed URI Template. Instead, the SvcParams and address records associated with this SVCB record SHOULD be used for the HTTPS connection, with the same semantics as an HTTPS RR. However, for consistency, service operators SHOULD publish an equivalent HTTPS RR, especially if clients might learn this URI Template through a different channel.

6. Limitations

This document is concerned exclusively with the DNS transport, and does not affect or inform the construction or interpretation of DNS messages. For example, nothing in this document indicates whether the service is intended for use as a recursive or authoritative DNS server. Clients must know the intended use in their context.

7. Examples

*A resolver at "simple.example" that supports DNS over TLS on port 853 (implicitly, as this is its default port):

```
_dns.simple.example. 7200 IN SVCB 1 simple.example. alpn=dot
```

*A resolver at "doh.example" that supports only DNS over HTTPS (DNS over TLS is not supported):

```
_dns.doh.example. 7200 IN SVCB 1 doh.example. (
    alpn=h2 dohpath=/dns-query{?dns} )
```

*A resolver at "resolver.example" that supports:

- DNS over TLS on "resolver.example" ports 853 (implicit in record 1) and 8530 (explicit in record 2), with "resolver.example" as the Authentication Domain Name,

- DNS over HTTPS at https://resolver.example/dns-query{?dns} (record 1), and

- an experimental protocol on fooexp.resolver.example:5353 (record 3):

```
_dns.resolver.example. 7200 IN SVCB 1 resolver.example. (
    alpn=dot,h2,h3 dohpath=/dns-query{?dns} )
_dns.resolver.example. 7200 IN SVCB 2 resolver.example. alpn=dot port=8
_dns.resolver.example. 7200 IN SVCB 3 fooexp port=5353 alpn=foo foo-inf
```

*A nameserver at "ns.example" whose service configuration is published on a different domain:

```
_dns.ns.example. 7200 IN SVCB 0 _dns.ns.nic.example.
```

8. Security Considerations

8.1. Adversary on the query path

This section considers an adversary who can add or remove responses to the SVCB query.

During secure transport establishment, clients MUST authenticate the server to its authentication name, which is not influenced by the SVCB record contents. Accordingly, this draft does not mandate the use of DNSSEC. This draft also does not specify how clients authenticate the name (e.g. selection of roots of trust), which might vary according to the context.

Although this adversary cannot alter the authentication name of the service, it does have control of the port number and "dohpath" value. As a result, the adversary can direct DNS queries for \$HOSTNAME to any port on \$HOSTNAME, and any path on "https://\$HOSTNAME", even if \$HOSTNAME is not actually a DNS server. If the DNS client uses shared TLS or HTTP state, the client could be

correctly authenticated (e.g. using a TLS client certificate or HTTP cookie).

This behavior creates a number of possible attacks for certain server configurations. For example, if "https://\$HOSTNAME/upload" accepts any POST request as a public file upload, the adversary could forge a SVCB record containing dohpath=/upload. This would cause the client to upload and publish every query, resulting in unexpected storage costs for the server and privacy loss for the client.

To mitigate this attack, a client of this SVCB mapping MUST NOT provide client authentication for DNS queries, except to servers that it specifically knows are not vulnerable to such attacks, and a DoH service operator MUST ensure that all unauthenticated DoH requests to its origin maintain the DoH service's privacy guarantees, regardless of the path. Also, if an alternative service endpoint sends an invalid response to a DNS query, the client SHOULD NOT send more queries to that endpoint.

8.2. Adversary on the transport path

This section considers an adversary who can modify network traffic between the client and the alternative service (identified by the TargetName).

For a SVCB-reliant client ([SVCB] Section 3), this adversary can only cause a denial of service. However, because DNS is unencrypted by default, this adversary can execute a downgrade attack against SVCB-optional clients. Accordingly, when use of this specification is optional, clients SHOULD switch to SVCB-reliant behavior if SVCB resolution succeeds. Specifications making use of this mapping MAY adjust this fallback behavior to suit their requirements.

9. IANA Considerations

Per [SVCB] IANA would be directed to add the following entry to the SVCB Service Parameters registry.

Number	Name	Meaning	Reference
7	dohpath	DNS over HTTPS path template	(This document)

Table 1

Per [Attrleaf], IANA would be directed to add the following entry to the DNS Underscore Global Scoped Entry Registry:

RR TYPE	_NODE NAME	Meaning	Reference
SVCB	_dns	DNS SVCB info	(This document)

Table 2

10. References

10.1. Normative References

- [DOH] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <<https://www.rfc-editor.org/rfc/rfc8484>>.
- [DOT] 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>>.
- [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>>.
- [RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November 2003, <<https://www.rfc-editor.org/rfc/rfc3629>>.
- [RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <<https://www.rfc-editor.org/rfc/rfc3986>>.
- [RFC6570] Gregorio, J., Fielding, R., Hadley, M., Nottingham, M., and D. Orchard, "URI Template", RFC 6570, DOI 10.17487/RFC6570, March 2012, <<https://www.rfc-editor.org/rfc/rfc6570>>.
- [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>>.
- [SVCB] Schwartz, B., Bishop, M., and E. Nygren, "Service binding and parameter specification via the DNS (DNS SVCB and HTTPS RRs)", Work in Progress, Internet-Draft, draft-ietf-dnsop-svcb-https-08, 12 October 2021, <<https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-svcb-https-08>>.

10.2. Informative References

- [Attrleaf] Crocker, D., "Scoped Interpretation of DNS Resource Records through "Underscored" Naming of Attribute Leaves", BCP 222, RFC 8552, DOI 10.17487/RFC8552, March 2019, <<https://www.rfc-editor.org/rfc/rfc8552>>.

[DNSURI]

Josefsson, S., "Domain Name System Uniform Resource Identifiers", RFC 4501, DOI 10.17487/RFC4501, May 2006, <<https://www.rfc-editor.org/rfc/rfc4501>>.

Appendix A. Mapping Summary

This table serves as a non-normative summary of the DNS mapping for SVCB.

Mapped scheme	"dns"
RR type	SVCB (64)
Name prefix	_dns for port 53, else _\$PORT._dns
Required keys	alpn
Automatically Mandatory Keys	port
Special behaviors	Supports all HTTPS RR SvcParamKeys
	Overrides the HTTPS RR for DoH
	Default port is per-transport
	No encrypted -> cleartext fallback

Table 3

Acknowledgments

Thanks to the many reviewers and contributors, including Daniel Migault, Paul Hoffman, Matt Norhoff, Peter van Dijk, Eric Rescorla, and Andreas Schulze.

Author's Address

Benjamin Schwartz
Google LLC

Email: bemasc@google.com