

Alternate Service Mechanisms

Theodor Ogeday Özuluca, Tim Betzer*

**Chair of Network Architectures and Services*

School of Computation, Information and Technology, Technical University of Munich, Germany

Email: theodor.oezuluca@tum.de, betzer@net.in.tum.de

Abstract—Alternative service mechanisms allow servers to advertise authoritative endpoints and protocol configurations to improve performance and security. This paper compares HTTP-based Alt-Svc and DNS-based SVCB and HTTPS resource records, analyzes connection establishment latency, protocol negotiation, fallback behavior, security and real-world deployment. It shows that Alt-Svc enables incremental and backwards compatible deployment but cannot optimize initial connections, while SVCB and HTTPS records allow earlier and more authoritative service discovery with more complex deployment. The evaluation highlights that both mechanisms serve complementary roles in incremental deployment and early connection optimization, and discusses the current adoption in practice.

Index Terms—alternative services, alt-svc, svcb, https records, dns, protocol negotiation, http/3, quic

1. Introduction

Modern web communication relies on efficient connection establishment and the negotiation of appropriate protocols for both security and performance. Clients must be able to determine not only how to reach the service of an origin, but also which protocols, endpoints, and transport options are supported by the server. Without the ability to discover this information, the client may connect via a slower or less secure protocol, even if better alternatives are available [1], [2]. The absence of standardized mechanisms for discovering alternative services delays protocol upgrades, underutilizes performance optimizations, and may negatively affect security. Therefore, mechanisms are required that enable the client to discover alternative services while still preserving backwards compatibility with existing web infrastructure.

To address these problems, the Internet Engineering Task Force has standardized multiple alternative service mechanisms. These allow servers to advertise alternative ways of access to the same resource. An alternative service is identified by the protocol name, host and port [2].

This paper focuses on two such alternative service mechanisms. The first approach uses the Alt-Svc HTTP header field, which enables the server to advertise alternative services in its HTTP response header after the client has established its initial connection to the origin's resource [2]. The second approach is DNS-based service discovery using Service Binding (SVCB) and HTTPS DNS resource records, which enable clients to learn of alternative services before establishing the initial connection [3].

This paper describes and compares these two alternative service mechanisms regarding performance, protocol negotiation, security, and deployment status. Furthermore, advantages and disadvantages of each approach are discussed.

2. Related work

HTTP-based alternative service discovery is standardized in RFC 7838 by Nottingham et al. [2]. It enables incremental deployment of new protocols, and early studies on QUIC deployment by Zirngibl et al. [1] and Matsuzawa and Ichikawa [4] show that it helps with protocol transition while keeping backwards compatibility. DNS-based alternative service discovery was standardized more recently in RFC 9460 by Schwartz et al. [3], introducing the SVCB and HTTPS resource records. This allows for more authoritative service advertisements. Measurement studies by Dong et al. [5] and Zirngibl et al. [6] show that these records are primarily deployed by large providers and commonly used for QUIC-capable endpoints granting performance improvements, but face operational problems and misconfiguration during deployment.

3. Alternate Service Mechanisms

Alternative service mechanisms enable an origin to authoritatively advertise access to its resources via alternative network locations, potentially employing different protocol configurations. The goal is to reduce connection establishment overhead, improve overall performance and security while maintaining compatibility with existing web infrastructure [2]. This section introduces two standardized approaches to alternative service discovery and outlines their fundamental design principles.

3.1. HTTP Alt-Svc Header

The HTTP Alternative Services mechanism, defined in RFC 7838 [2], allows servers to advertise alternative services through the Alt-Svc HTTP header field. An alternative service represents an authoritative way of accessing the same origin's resource. Each alternative service is identified by an Application-Layer Protocol Negotiation (ALPN) protocol name, a host, and a port.

When a client receives an Alt-Svc advertisement, it may open a new connection to the advertised alternative service if the alternative presents a TLS certificate that is valid for the original site. Once the connection is established, the client can use it for subsequent requests. The

use of alternative services is transparent to the application layer. This means that, if the client uses an alternative, it may internally change the protocol, host, or port but these changes must not be propagated to the application.

The Alt-Svc mechanism allows servers to suggest a different protocol or network location without changing the original URL. Typical use cases include offering access to a new protocol, such as HTTP/2, redirecting clients to servers that are under less load or geographically closer to the client, or segmenting clients based on capability support. For incremental deployment, using an alternative service is optional for clients and fallback to the original service remains possible if the alternative service is unavailable or unresponsive.

Clients cache alternative services for usage. The freshness parameter (ma) dictates, how long the advertised alternative service is considered valid. Clients should use fresh/valid alternative services but can continue using an alternative service after the freshness has expired. Furthermore, a persist flag can be used to manage, if an entry for an alternative service should be kept in the clients cache after the network configuration has changed. If not set, the clients should delete the entry in the cache.

Despite its advantages like flexibility and backwards compatibility, the Alt-Svc mechanism has inherent limitations [2]. Because this mechanism advertises alternative services via HTTP, clients can only learn about them after establishing an initial connection to the origin. Thus, only subsequent connections can benefit from potential performance and security improvements. Moreover, the server cannot force the client to use a certain connection. This results in unpredictable behavior of clients which can complicate load balancing or lead to clients continuing using a less secure or less efficient protocol. There are also other potential security and privacy considerations, such as downgrade attacks and the possibility of tracking clients by advertising a unique host name to each [2].

Alt-Svc provides a flexible and backwards compatible mechanism for alternative service discovery but it is also constrained by being based on HTTP. This motivates mechanisms that enable the discovery of alternative services before connection establishment. In the next section, such a mechanism will be discussed.

3.2. SVCB and HTTPS DNS Resource Records

SVCB and HTTPS DNS resource records, defined in RFC 9460 [3], provide a DNS-based mechanism for advertising and discovering alternative services for an origin. While the SVCB record type is designed for general service binding, HTTPS records offer a specialization tailored to HTTPS services. Both record types use the same encoding, structure, and high-level semantics.

SVCB and HTTPS resource records enable domain owners, via authoritative DNS servers, to advertise service-related information during DNS resolution. In contrast to HTTP-based mechanisms, this allows clients to learn about alternative endpoints and supported protocol configurations before establishing a connection. The primary goal of these records is to enable clients to obtain required information for establishing a connection to an authoritative endpoint with at most one additional DNS

query. While in practice, typically no additional round trip is needed [3], [5].

SVCB records support two modes of operation. In AliasMode, the record delegates a service name to another domain name. This provides CNAME-like functionality with the benefit that it can also be used at the zone apex where CNAME records are not permitted. In Service-Mode, the record specifies alternative endpoints together with sets of service parameters that describe how the endpoints should be used [3].

For HTTPS origins, HTTPS resource records provide special handling [3]. They can advertise support for newer protocols such as HTTP/3 over QUIC, signal a preference for HTTPS and enable automatic upgrade where possible when an HTTPS record is present. Additionally, they can enable the usage of non-default port numbers for TCP and UDP, provided no port restricting firewall is between the client and the service endpoint. HTTPS records can also advertise configuration required for Encrypted Client Hello (ECH). This enables encryption of sensitive parts of the TLS handshake.

While DNS-based service discovery offers advantages, such as discovering endpoints prior to connection, compared to HTTP-based Alt-Svc, it introduces new aspects to consider, including DNS caching and interaction with DNS security mechanisms. This architectural difference forms the basis of the comparative evaluation of the two mechanisms in the next sections.

4. Comparative Evaluation

The alternative service mechanisms described in the previous section differ fundamentally in the stage at which service information becomes available to the client and in the protocol used for service advertisement. These differences have a direct impact on performance, protocol negotiation, security, privacy, and deployment. Figure 1 illustrates the workflow of both mechanisms and highlights the difference in the timing of service discovery.

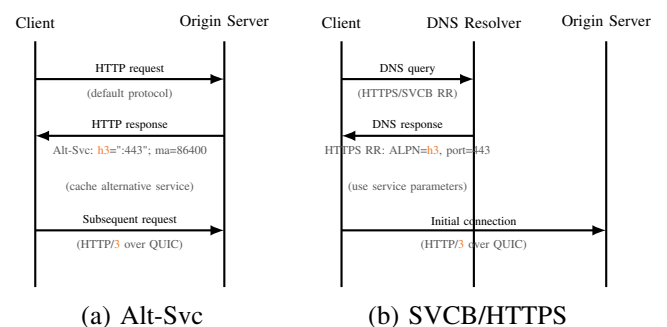


Figure 1: Alternative service discovery mechanisms: (a) HTTP Alt-Svc advertisement after the initial HTTP connection [2]; (b) DNS-based discovery via SVCB/HTTPS records during DNS resolution [3].

This structured evaluation aims to provide a systematic comparison of Alt-Svc and SVCB and HTTPS DNS resource records regarding performance, protocol negotiation, security, privacy, and deployment, and to clarify the benefits and trade-offs of HTTP-based and DNS-based service discovery. Additionally, at the end complementary use of both mechanisms is discussed.

4.1. Performance

The primary performance goal of alternative service mechanisms is to decrease connection establishment time (latency) and to minimize the number of round trips needed before a client can use the best possible transport and protocol configuration for a given request. The performance of these mechanisms, therefore, significantly depends on when the client receives the appropriate service information for an alternative service and how this information is integrated into the existing connection establishment process.

Because HTTP Alt-Svc advertises alternative services after the initial HTTP connection to the origin server has been established, the first connection uses the default protocol and endpoint. Thus, any potential performance improvements due to using a different protocol or a closer server can only occur on subsequent connections. Although Alt-Svc supports both protocol upgrade and endpoint migration without changing the URL of the requested origin's resource, the initial connection latency is consequently not reduced. When connections are relatively short-lived or clients frequently access new origins, this limits the performance benefits that can be achieved by using alternative service mechanisms.

On the other hand, SVCB and HTTPS DNS resource records enable clients to discover alternative endpoints and the protocol capabilities during DNS resolution, before the actual connection is established. By utilizing the provided service parameters of the record, such as supported application-layer protocols and alternative transport endpoints, DNS-based service discovery can enable the client to establish a direct connection to the server using an optimized configuration for each specific request. This can prevent additional round trips that would have been needed to negotiate the protocol and/or redirect the client to an alternative endpoint after the initial connection has been established. Measurement studies [6], [7] have shown that the early availability of service information can reduce the connection establishment latency, particularly if the client supports protocols like HTTP/3 over QUIC, which can reduce round trips significantly by cutting out the TCP and TLS handshake.

Empirical analyses by Zirngibl et al. [6] show that these records are often used to advertise QUIC-capable endpoints and to direct clients to alternative services operated by content delivery networks (CDNs). Their analysis further shows that HTTPS resource records are primarily provided by large providers and CDNs, where the performance benefits of faster connection establishment and optimized protocol selection are greatest. When supported by resolvers and clients, SVCB and HTTPS records can both reduce the number of DNS queries required and speed up the connection establishment process by providing protocol information and, in case address records are not available, supplying IP address hints via the `ipv4hint` and `ipv6hint` parameters, allowing clients to connect without issuing another DNS query [3].

Despite the above advantages, the performance benefits of DNS-based service discovery are dependent on the behavior of resolvers and client support. While SVCB-aware DNS resolvers can include SVCB results in the additional section of DNS responses, legacy resolvers may

force clients to request additional queries or to fallback to traditional DNS resolution. To mitigate the negative effect of legacy resolvers, it is recommended that clients perform the SVCB resolution in parallel to usual A and AAAA lookups [3]. This is confirmed by measurement studies [5] and ensures that DNS-based service discovery does not negatively affect the connection establishment time.

Ultimately, the performance comparison illustrates the trade-off between the two approaches. While Alt-Svc improves performance for subsequent connections without affecting the initial connection establishment latency, SVCB and HTTPS DNS resource records aim to optimize the first connection by moving the service discovery to an earlier point in the connection process. How much the theoretical benefits of each mechanism affect the real-world performance depends on the supported protocols and the resolvers' capabilities.

4.2. Protocol Negotiation and Fallback Behavior

Alternative service mechanisms not only differ in the timing of when the service information is discovered, but also in the handling of protocol negotiation, upgrades, downgrades, and fallback.

Alt-Svc enables the server to advertise alternative services to the client after the initial connection has been established. With the information advertised in the Alt-Svc HTTP header field, the client can use the ALPN protocol name, host, and port to connect to the alternative resource. The client dictates, whether and when to use an alternative service. Fallback is straightforward: If the client cannot connect to the alternative service, it uses the original connection or a different cached alternative service. This grants backwards compatibility [4] but limits the server's capability to influence protocol selection. This also has the risk of protocol downgrade attacks which are discussed in Section 4.3 [2].

In contrast, with SVCB and HTTPS DNS resource records, the alternative service discovery is moved to the DNS resolution phase. Through the advertised service parameters, the client can learn about supported application-layer protocols before the connection is established. Multiple protocol options can be advertised, the client chooses one and directly connects to it. Additionally, an HTTPS resource record indicates that the service is only available over HTTPS, which prevents clients from using HTTP. Fallback is more complex: If resolution via `AliasMode` terminates without finding a `ServiceMode` record, the client treats the final target name as a valid endpoint and tries to connect to it using conventional address resolution. For compatibility, clients for pre-existing protocols such as HTTP should be SVCB-optional. This means, that a client is able to connect to a resource without SVCB via the traditional DNS lookup with A/AAAA records in case the SVCB resolution is not possible. However, when DNS resolution is cryptographically protected and SVCB resolution fails, the client must not fallback to non-SVCB resolution, as it could be a downgrade attack [3]. Measurement studies confirm that clients often implement parallel resolution via SVCB and traditional address resolution [5].

Overall, SVCB and HTTPS records allow earlier and more authoritative protocol negotiation but have more

complex fallback handling. Protocol negotiation of Alt-Svc is less authoritative and leaves more control to clients while having simpler fallback behavior.

4.3. Security and Privacy Implications

The security and privacy of the alternative service mechanisms are primarily influenced by the channel through which the services are advertised.

Alt-Svc advertisements are delivered via an already established HTTP connection. Therefore, Alt-Svc inherits the security properties of the underlying transport, typically TLS over TCP or QUIC [8]. Clients have to confirm that an alternative service is authoritative for the origin's resource by validating that it has a TLS certificate that is valid for the origin. Because Alt-Svc advertisements are optional, the client may ignore them and fallback to the original service with a potentially less secure protocol configuration or a cached alternative endpoint. Downgrade attacks are possible by blocking access to a more secure alternative due to the fallback behavior described earlier. Additionally, from a privacy point of view, Alt-Svc enables servers to advertise unique host names to clients which can be used for tracking them.

As DNS responses are not inherently authenticated, clients must treat SVCB information as advisory, unless the SVCB information is secured, for example using DNSSEC [3]. To mitigate downgrade attacks, clients must not fallback to non-SVCB resolution when the DNS resolution is cryptographically protected. HTTPS RRs enforce HTTPS usage instead of HTTP and enable features like ECH to reduce the leakage of sensitive TLS handshake data.

As discussed, measurements show that SVCB and HTTPS records are primarily used by large providers and CDNs so far. They often use DNSSEC and modern TLS configurations to increase security. On the other hand, DNS-based alternative service discovery exposes service metadata stored in SVCB and HTTPS records to recursive resolvers during name resolution. While this information might not be very sensitive, it introduces a privacy concern that is not present on HTTP-based alternative service mechanisms.

In summary, Alt-Svc uses strong encryption via TLS but is more prone to downgrade attacks, has difficulty of enforcing secure protocols and poses the risk of clients being tracked when a server is under control of an attacker. SVCB and HTTPS records enable a stricter protocol enforcement and security guarantees while being more reliant on DNS and exposing more metadata.

4.4. Deployment Status, Real-World Adoption, and Discussion

Real-world adoption of alternative service mechanisms varies significantly between HTTP-based Alt-Svc and DNS-based SVCB and HTTPS resource records because they differ fundamentally in their operational requirements and deployment complexity.

Alt-Svc is widely adopted into major browsers and servers because it is implemented solely at the HTTP layer and does not require any updates to the underlying DNS

infrastructure or resolvers. This means it can be adopted incrementally for each origin server individually. There are reports showing Alt-Svc has been primarily used to add new protocol versions such as HTTP/3 over QUIC in a backwards compatible way [1], [4].

SVCB and HTTPS resource records are at an earlier stage of deployment. Large-scale measurements show that most HTTPS records are served by a small number of large CDNs, especially Cloudflare [6]. This concentration reflects the need for control over the DNS infrastructure, resolver behavior and service configuration which is not given for broad ecosystem deployment.

The primary barrier to widespread deployment of DNS-based service discovery is its deployment complexity [5]. Empirical studies report that SVCB and HTTPS resource records may have misconfigured ALPN values, IP hints and ECH key management [5], [9]. Additionally, client support is not widespread yet and resolver behavior varies.

However, despite the difficulties associated with deploying DNS-based service discovery, it is becoming increasingly adopted in scenarios where early protocol negotiation, privacy enhancements, and close integration with CDN routing are important.

In conclusion, the design of Alt-Svc [2] and observations from real-world deployments [6] indicate that HTTP Alt-Svc and SVCB and HTTPS Resource Records are likely to be used in a complementary fashion. As such, HTTP Alt-Svc will probably remain for backwards compatibility and to enable incremental adoption of new protocols [4], while SVCB and HTTPS Resource Records are likely to be used primarily by larger organizations to enable early optimizations of connections and stronger security guarantees. The success of DNS-based service discovery will depend on the support of resolvers and clients for it, as well as the proper and consistent configuration of the SVCB and HTTPS records.

5. Conclusion and Future Work

This paper presents a comparative analysis of HTTP-based Alt-Svc and DNS-based SVCB and HTTPS resource records for alternative service discovery. The evaluation concludes that both approaches have a similar goal of enabling clients to access an origin's resource via an authoritative alternative service. However, the two mechanisms vary significantly in several aspects, including the timing of discovery, the difficulty of deployment and security guarantees [2], [3].

Alt-Svc is backwards compatible, relatively easily deployed, and widely supported. Servers can only advertise alternative services to the client after the initial connection has been made. This limits the possible performance and security improvements to subsequent connections. In contrast, with SVCB and HTTPS resource records alternative endpoints can be discovered during DNS resolution, prior to connecting. Thus, performance and security improvements can apply to the initial connection [3], [6]. SVCB and HTTPS records also allow for a more authoritative protocol negotiation and have stronger security guarantees but are more complex to deploy and depend heavily on DNS infrastructure, resolver behavior, and client support [3], [6].

Real-world measurements indicate that both mechanisms are used. Alt-Svc is useful for incremental rollout of new protocols [1], while SVCB and HTTPS records are provided by large CDNs and enable early connection improvements regarding performance and security.

Ongoing work is necessary to evaluate the adoption of SVCB and HTTPS RRs as client and resolver support improves [5]. Additional future work is needed to create best practice guidelines for the deployment of SVCB and HTTPS RRs to help avoid misconfigurations and to allow for a broader adoption across the web [5].

References

- [1] J. Zirngibl, P. Buschmann, P. Sattler, B. Jaeger, J. Aulbach, and G. Carle, "It's over 9000: analyzing early QUIC deployments with the standardization on the horizon," in *Proceedings of the ACM Internet Measurement Conference*, ser. IMC '21. New York, NY, USA: Association for Computing Machinery, 2021, pp. 261–275, [Online]. Available: <https://doi.org/10.1145/3487552.3487826>.
- [2] M. Nottingham, P. McManus, and J. Reschke, "HTTP Alternative Services," RFC 7838, April 2016, [Online]. Available: <https://www.rfc-editor.org/info/rfc7838>.
- [3] B. Schwartz, M. Bishop, and E. Nygren, "Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records)," RFC 9460, November 2023, [Online]. Available: <https://www.rfc-editor.org/info/rfc9460>.
- [4] T. Matsuzawa and K. Ichikawa, "Implementation and Evaluation of HTTP/3 Connectivity Check Using Happy Eyeballs Algorithm," *Network*, vol. 2, pp. 389–397, 2022. [Online]. Available: <https://doi.org/10.3390/network2030024>
- [5] H. Dong, Y. Zhang, H. Lee, S. Huque, and Y. Sun, "Exploring the Ecosystem of DNS HTTPS Resource Records: An End-to-End Perspective," in *Proceedings of the ACM Internet Measurement Conference*, ser. IMC '24. New York, NY, USA: Association for Computing Machinery, 2024, pp. 423–440, [Online]. Available: <https://doi.org/10.1145/3646547.3688410>.
- [6] J. Zirngibl, P. Sattler, and G. Carle, "A First Look at SVCB and HTTPS DNS Resource Records in the Wild," in *International Workshop on Traffic Measurements for Cybersecurity 2023*, ser. WTMTC, 2023.
- [7] J. Iyengar and M. Thomson, "QUIC: A UDP-Based Multiplexed and Secure Transport," RFC 9000, May 2021, [Online]. Available: <https://www.rfc-editor.org/info/rfc9000>.
- [8] P. Hoffmann and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA," RFC 6698, August 2012, [Online]. Available: <https://www.rfc-editor.org/info/rfc6698>.
- [9] J. Liang, J. Jiang, H. Duan, K. Li, T. Wan, and J. Wu, "When https meets cdn: A case of authentication in delegated service," in *2014 IEEE Symposium on Security and Privacy*, 2014, pp. 67–82.