Workgroup: DNSSD
Published: 9 January 2023
Intended Status: Standards Track
Expires: 13 July 2023
A S. Cheshire T. Lemon
u Apple Inc. Apple Inc.
t
h
o
r
s
:

Advertising Proxy for DNS-SD Service Registration Protocol

Abstract

An Advertising Proxy advertises the contents of a DNS zone, for example maintained using the DNSSD Service Registration Protocol (SRP), using multicast DNS. This allows legacy clients to discover services registered with SRP using multicast 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 13 July 2023.

Table of Contents

1. Introduction

DNS-Based Service Discovery [RFC6763] [ROADMAP] was designed to facilitate Zero Configuration IP Networking [RFC6760] [ZC]. When used with Multicast DNS [RFC6762] with ".local" domain names [RFC6761] this works well on a single link (a single broadcast domain).

However, in some applications, multicast may be a poor choice for advertising. Most obviously, multicast DNS is constrained to a single network link, and for example in the case of stub networks [STUBNET], service discovery for devices on the stub network necessarily requires some kind of proxy.

Also, even in single-link use cases, multicast isn't always the best choice. On some network media, multicast is inefficient and/or unreliable. Also, mDNS-based DNSSD requires that each host providing services receive and process all service discovery requests even for services they don't offer. For power-constrained hosts, keeping a radio listening all the time is prohibitively expensive.

Ideally, in situations where multicast DNS is not the right choice, an obvious alternative is to use regular unicast DNS [RFC1035]. Unfortunately, this isn't always possible: the DNS protocol relies on a delegation hierarchy, and on per-network DNS resolvers.

The operational model for such servers is that any particular network infrastructure provides a DNS resolver, and all DNS queries go to that resolver. So using unicast DNS for discovery of services through a stub network proxy, for example, would require that the stub network proxy be able to somehow register with the infrastructure DNS service. This isn't usually possible.

This document describes a new type of proxy, an Advertising Proxy, which can be used to address some of these issues. An Advertising Proxy advertises the contents of some DNS zone (or zones) [RFC1034]

to one or more network links using multicast DNS. This allows the DNS protocol, for example using the Service Registration Protocol registrar function [SRP], to be used by servers to advertise their services, while using the permissionless model of multicast DNS to make those services discoverable to devices on links supported by the Advertising Proxy.

In its simplest realization, an advertising proxy monitors the contents of a DNS zone. When a new DNS resource record is added to the zone, the advertising proxy rewrites that record, replacing the domain name of the zone with ".local," and advertises the result using mDNS on one or more network links.

However, more commonly, the advertising proxy function is combined with an SRP registrar. In this case, the SRP registrar and the advertising proxy service cooperate to minimize name collisions. Such a service may or may not actually respond to DNS queries.

When an Advertising Proxy is implemented as part of an SRP registrar (a DNS authoritative server that implements Service Registration Protocol), an SRP requestor can send registration requests for any valid DNS records to the SRP registrar. In practice, the most common use is to register the PTR, SRV and TXT records that describe a DNS-SD service [RFC6763], and the A and AAAA records that give the IPv4 and/or IPv6 addresses of the host on which that service can be reached.

Although, as we've said, an Advertising Proxy can monitor a DNS zone and advertise its contents, this is not a compelling use case. The reason for this is that we can assume that all DNSSD implementations will discover and use infrastructure provided service discovery using the DNS protocol if it is available. We do not need to support a use case where a consumer of DNSSD only implements multicast DNS.

An authoritative DNS zone that is not managed as part of the Advertising Proxy really can only exist as an infrastructure service. If it exists as an infrastructure service, the right way to make it available is to make it discoverable using the mechanisms described in Section 11 of [RFC6763]. Since no use case exists for this model of Advertising Proxy, we do not attempt to specify how such an Advertising Proxy could be made to work.

Similarly, an Advertising Proxy that, as part of its functioning, answers unicast DNS queries, would ideally be included in the DNS service provided by the infrastructure, and in this case the Advertising Proxy function would not be necessary. However, because in this case the Advertising Proxy functionality is superfluous, discussion of this topic is out of scope for this document.

Therefore, this document limits itself to describing how to implement an Advertising Proxy that manages service registrations using the Service Registration Protocol. We do talk about how the Service Registration Protocol database should be advertised, but not how it can be integrated into an existing DNS infrastructure.

1.1. Conventions and Terminology Used in This Document

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.

2. Advertising Proxy

An Advertising Proxy advertises the contents of one or more DNS zones that are maintained using the Service Registration Protocol. Such a service consists of three parts, four of which are required, one of which is optional. These are:

* The mDNS Registrar function
* The Advertising Proxy function
* The SRP registrar function, which includes:
  - The SRP protocol implementation
  - The zone database that is updated using the SRP protocol
* The DNS authoritative server function, which may include any or all of:
  - Authoritative DNS service for all zones managed by SRP
  - Discovery Proxy service for all links managed by the Advertising Proxy
  - Full-service DNS resolver or DNS Proxy

These functions are somewhat interdependent, so while we will discuss each separately, there is no way to completely separate them. After discussing each function, we will describe the operation of the system as a whole.

2.1. The mDNS Registrar function

The mDNS registrar function is an mDNS responder, as described in [RFC6762]. We use the term "mDNS registrar" rather than simply "mDNS responder" to emphasize the specific function of advertising mDNS records, as opposed to browsing or resolving services.

If Discovery Proxy authoritative resolution service is being offered by the Advertising Proxy, the mDNS registrar MUST support querying for services and records on the link that are not advertised by the Advertising Proxy.

The mDNS Registrar MUST implement the Time Since Received [TSR] record. This makes it possible to set up redundant Advertising Proxies that use SRP replication [REPLICATION] to maintain a common set of SRP zones and advertise them without SRP Updates creating conflicts. Such conflicts can occur when, for example, the IP address of a host changes and it sends an SRP update. The new IP address conflicts with the old address, which is being advertised. Without TSR, the old address will win the conflict, resulting in stale data being advertised. With TSR, the newer data supersedes the old data.

2.2. The Advertising Proxy function

The Advertising Proxy function mediates between an mDNS registrar and the SRP zone database. Whenever a record is tentatively added to the SRP zone database, the Advertising Proxy registers it with the mDNS registrar. If this registration succeeds, the registration is finalized; otherwise it is rejected. The usual reason for rejection would be that the name is already taken. When records expire in the SRP zone database, the Advertising Proxy function removes those records from its mDNS advertisement.

Each SRP Update includes a KEY record that is applicable to every name claimed in the Update. SRP Update also includes an EDNS0 Update Lease option which may include a KEY-LEASE value that's longer than the LEASE value. In this case, the Advertising Proxy SHOULD advertise the KEY record for the duration of the KEY-LEASE, even if the other records are removed when the LEASE value has expired. The Advertising Proxy MAY advertise the KEY record even if the LEASE and KEY-LEASE values are the same, or the KEY-LEASE valid isn't specified.

Records advertised by the Advertising Proxy all appear in the .local domain. Consequently, these records MUST be rewritten in somewhat the opposite of the way a Discovery Proxy Section 5.5 of [RFC8766] rewrites them.

Each zone managed by the SRP registrar function must have a name. In some cases, SRP requestor will discover the name using the Domain Enumeration process described in Section 11 of [RFC6763]. However in most cases, since advertising proxies aren't integrated into infrastructures, the registration domain used by the SRP requestor will be the 'default.service.arpa.' domain. The SRP registrar may rewrite incoming registrations into a different zone, or retain the 'default.service.arpa.' zone name.

In either case, before advertising a tentative record, the Advertising Proxy function first rewrites the record. First, the owner name is transformed by replacing the zone name with '.local'. Secondly, for any RR that contains a domain name, that domain is transformed in the same way.

In some cases, the SRP requestor may register one or more address records for addresses that aren't valid or reachable on some link on which the advertising proxy could advertise them. The Advertising Proxy function MAY filter out such records entirely, or MAY explicitly advertise such records only on the link(s) on which they are reachable. This is optional because it requires the Advertising Proxy function to have enough information to make such a determination, which may not always be the case.

Where such determinations are possible, the advertising proxy SHOULD NOT advertise an IPv4 or IPv6 link-local address, or any other media-specific link-scoped address, on any link other than the link on which the SRP registration was received.

2.3. The SRP Registrar function

The SRP registrar function comprises two components: the SRP protocol and the zone database (or databases). The details of the SRP protocol are described in [SRP].

In the context of an Advertising Proxy, the SRP protocol will be updating one or more DNS zones. It's possible, for example, for an SRP registrar to provide SRP service on more than one link, and for each link to be treated as a separate DNS zone. SRP requestors may not know what zone they are updating: they may be using 'default.service.arpa' as a placeholder rather than discovering the name of the zone to update. In this case, updates for 'default.service.arpa' will be rewritten into the name of the zone specific to a particular link. Note that this separation is not required, but is possible and may be desirable.

In an Advertising Proxy, when an SRP update is received, it is first validated according to the SRP specification. It is then checked for uniqueness in the context of SRP, using the SRP first-come, first-served mechanism. Unlike a DNS-only SRP registrar, an Advertising Proxy registrar must complete two additional uniqueness checks for any name being registered.

First, the name must be unique across all DNS zones that are being advertised together on the same link by the Advertising Proxy. That is, if the zone being updated is advertised on any link, then the name being registered must be unique in every zone that is being advertised on that link. If the zone is being advertised on multiple links, then for each link, the name must be unique across all the zones advertised on that link.

Secondly, the name must not already be being advertised via mDNS. This is easy to check: the Advertising Proxy tentatively advertises the name on all links that the corresponding zone is being advertised on. If every tentative advertisement succeeds without detecting a conflict, then the advertisement has been successful. At this point the SRP registrar can confirm with the requestor that its registration has succeeded.

If, on the other hand, a conflict is detected in any part of this process, then the SRP registrar informs the requestor that the name is already taken, by returning the YXDOMAIN response code.

2.4. The DNS Authoritative Server function

An Advertising Proxy SHOULD answer DNS queries for the zones it manages. This is not required because in some cases it may not be possible. The zones it manages may not have names in the DNS hierarchy, for example, so even if they have locally-assigned names, answering authoritatively for these names may be problematic.

The primary purpose of the Advertising Proxy is to support DNS Service Discovery. In some use cases where Advertising Proxy is desirable, the mDNS function can only work on some links, while unicast DNS is the only option on others. This is the case, for example, for an Advertising Proxy operating on a stub network router.

In such a situation, devices on the infrastructure link will do service discovery using mDNS. However, devices on the stub network link may not be able to use mDNS, or it may be preferable that they do not. In this case, the Advertising Proxy will need to be able to provide the same information that is provided on the infrastructure link through a DNS resolver, using the DNS protocol, or, ideally, DNS Push [RFC8765].

Any Advertising Proxy implementing this functionality MAY use the 'default.service.arpa.' zone as a catch-all zone. A query to the 'default.service.arpa.' zone SHOULD return the same set of answers that would be returned by an mDNS query to the .local zone on a link served by the Advertising Proxy's mDNS registrar.

When using the 'default.service.arpa.' zone for queries, all responses that reference link-specific domains MUST be rewritten to use 'default.service.arpa.' domain instead. This includes domain names in the resource record data. Because the Advertising Proxy is required to enforce name uniqueness across all the zones it manages, this should not result in any conflicts.

2.4.1. Discovery Proxy

In order to fully support the ability to query the Advertising Proxy either with mDNS or DNS, it is necessary to provide a Discovery Proxy [RFC8766]. The Discovery Proxy provides answers for link-specific domains that represent each of the links supported by the Advertising Proxy. These responses are combined with responses from zones managed by SRP to produce a complete set of answers to any query received by the Advertising Proxy over DNS or DNS Push.

2.4.2. Full Service Resolver

In the case of a stub network, the Advertising Proxy may appear to devices on the stub network as an infrastructure service. This would mean that the DNS Listener on port 53 (TCP and UDP) and port 853 (TLS) could be expected to receive queries for arbitrary domain names, not just domain names for which the Advertising Proxy is authoritative.

Resolution of such names may not be required for devices on the stub network. For instance, if the stub network has only locally-provided IPv6 service using a ULA, devices on the stub network will not be able to contact arbitrary devices on the Internet anyway.

However, in cases where support for connecting to hosts outside of the scope of the Advertising Proxy is needed, the Advertising Proxy will have to provide a full service resolver (or a DNS Proxy [RFC5625]) in addition to its DNS authoritative service and Discovery Proxy service. The details of how this is configured are likely to be implementation-specific, and therefore outside the scope of this document.

2.5. Operation

2.5.1. Late Conflicts

It is possible for two mDNS responders to advertise conflicting records on the same name, but, as a consequence of a network partition or multicast packet loss, for neither server to immediately detect a conflict. When this happens, then at some later time one or the other mDNS responder will notice the conflict, and begin the conflict resolution process. The outcome of this process may be that the record advertised by the Advertising Proxy loses. In this case, the Advertising Proxy MUST stop advertising this record and remove it from its database. There is no way to notify the client when this happens, but when the client tries to renew its registration, the conflict can be reported.

2.5.2. No Text-Encoding Translation

As with a Discovery Proxy [RFC8766], an Advertising Proxy does no translation between text encodings [RFC6055]. Specifically, an Advertising Proxy does no translation between Punycode encoding [RFC3492] and UTF-8 encoding [RFC3629], either in the owner name of DNS records or anywhere in the RDATA of DNS records (such as the RDATA of PTR records, SRV records, NS records, or other record types like TXT, where it is ambiguous whether the RDATA may contain DNS names). All bytes are treated as-is with no attempt at text-encoding translation. A server implementing DNS-based Service Discovery [RFC6763] will use UTF-8 encoding for its unicast DNS-based record registrations, which the Advertising Proxy passes through without any text-encoding translation to the Multicast DNS subsystem. Queries from peers on the configured multicast-capable interface are answered directly from the advertised data without any text-encoding translation.

2.5.3. No Support for Reconfirm

For network efficiency, Multicast DNS [RFC6762] uses fairly long record lifetimes (typically 75 minutes). When a client is unable to reach a service that it discovered, Multicast DNS provides a "reconfirm" mechanism that enables the client to signal to the Multicast DNS subsystem that its cached data may be suspect, which causes the Multicast DNS subsystem to reissue queries, and remove the stale records if the queries are not answered.

Similarly, when using unicast service discovery with a Discovery Proxy [RFC8766], the DNS Push Notifications [RFC8765] protocol provides the RECONFIRM mechanism to signal that the Discovery Proxy should perform a local Multicast DNS reconfirm operation to re-verify the validity of the records.

When an Advertising Proxy is used, to support legacy clients that only implement Multicast DNS, reconfirm operations have no effect. If a device uses unicast Service Registration Protocol [SRP] to register its services with a service registry with Advertising Proxy capability, and the device then gets disconnected from the network, the Advertising Proxy will continue to advertise those records until the registrations expire. If a client discovers the service instance using Multicast DNS and is unable to reach it, and uses a Multicast

DNS reconfirm operation to re-verify the validity of the records, then the Advertising Proxy will continue to answer on behalf of the departed device until the record registrations expire. The Advertising Proxy has no reliable way to determine whether the additional Multicast DNS queries are due to a reconfirm operation, or due to other routine causes, like a client being rebooted, or disconnecting and then reconnecting to the network. The service registry has no reliable automatic way to determine whether a device that registered records has failed or disconnected from the network. Particularly with sleepy battery powered devices, the service registry does not know what active duty cycle any given service is expected to provide.

Consequently, reconfirm operations are not supported with an Advertising Proxy using multicast DNS. In cases where use of the reconfirm mechanism is important, clients should be upgraded to use the unicast DNS Push Notifications [RFC8765] protocol's RECONFIRM message. This RECONFIRM message provides an unambiguous signal to the service registry that it may be retaining stale records. (A future update to the Service Registration Protocol document [SRP] will consider ways that this unambiguous signal can be used to trigger expedited removal of stale data.)

3. Security Considerations

An Advertising Proxy may made data visible to eavesdroppers on the configured multicast-capable link(s).

4. IANA Considerations

This document has no IANA actions.

5. References

5.1. Normative References

[RFC1034] Mockapetris, P. and RFC Publisher, "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[RFC1035] Mockapetris, P. and RFC Publisher, "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC2119] Bradner, S. and RFC Publisher, "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>.

[RFC6760] Cheshire, S., Krochmal, M., and RFC Publisher, "Requirements for a Protocol to Replace the AppleTalk Name Binding Protocol (NBP)", RFC 6760, DOI 10.17487/

RFC6760, February 2013, <https://www.rfc-editor.org/info/rfc6760>.

[RFC6761] Cheshire, S., Krochmal, M., and RFC Publisher, "Special-Use Domain Names", RFC 6761, DOI 10.17487/RFC6761, February 2013, <https://www.rfc-editor.org/info/rfc6761>.

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

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

[RFC8174] Leiba, B. and RFC Publisher, "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>.

[RFC8765] Pusateri, T., Cheshire, S., and RFC Publisher, "DNS Push Notifications", RFC 8765, DOI 10.17487/RFC8765, June 2020, <https://www.rfc-editor.org/info/rfc8765>.

[SRP] Lemon, T. and S. Cheshire, "Service Registration Protocol for DNS-Based Service Discovery", Work in Progress, Internet-Draft, draft-ietf-dnssd-srp-17, 12 October 2022, <https://www.ietf.org/archive/id/draft-ietf-dnssd-srp-17.txt>.

[TSR] Lemon, T. and L. Qin, "Multicast DNS conflict resolution using the Time Since Received (TSR) RR", Work in Progress, Internet-Draft, draft-tllq-tsr-02, 11 July 2022, <https://www.ietf.org/archive/id/draft-tllq-tsr-02.txt>.

5.2. Informative References

[RFC3492] Costello, A. and RFC Publisher, "Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)", RFC 3492, DOI 10.17487/RFC3492, March 2003, <https://www.rfc-editor.org/info/rfc3492>.

[RFC3629] Yergeau, F. and RFC Publisher, "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November 2003, <https://www.rfc-editor.org/info/rfc3629>.

[RFC5625] Bellis, R. and RFC Publisher, "DNS Proxy Implementation Guidelines", BCP 152, RFC 5625, DOI 10.17487/RFC5625, August 2009, <https://www.rfc-editor.org/info/rfc5625>.

[RFC6055] Thaler, D., Klensin, J., Cheshire, S., and RFC Publisher, "IAB Thoughts on Encodings for Internationalized Domain

Names", RFC 6055, DOI 10.17487/RFC6055, February 2011, <https://www.rfc-editor.org/info/rfc6055>.

[RFC7558] Lynn, K., Cheshire, S., Blanchet, M., Migault, D., and RFC Publisher, "Requirements for Scalable DNS-Based Service Discovery (DNS-SD) / Multicast DNS (mDNS) Extensions", RFC 7558, DOI 10.17487/RFC7558, July 2015, <https://www.rfc-editor.org/info/rfc7558>.

[RFC8766] Cheshire, S. and RFC Publisher, "Discovery Proxy for Multicast DNS-Based Service Discovery", RFC 8766, DOI 10.17487/RFC8766, June 2020, <https://www.rfc-editor.org/info/rfc8766>.

[ROADMAP] Cheshire, S., "Service Discovery Road Map", Work in Progress, Internet-Draft, draft-cheshire-dnssd-roadmap-03, 23 October 2018, <https://www.ietf.org/archive/id/draft-cheshire-dnssd-roadmap-03.txt>.

[REPLICATION] Lemon, T., Keshavarzian, A., and J. Hui, "Automatic Replication of DNS-SD Service Registration Protocol Zones", Work in Progress, Internet-Draft, draft-lemon-srp-replication-02, 11 July 2022, <https://www.ietf.org/archive/id/draft-lemon-srp-replication-02.txt>.

[STUBNET] Lemon, T., "Automatically Connecting Stub Networks to Unmanaged Infrastructure", Work in Progress, Internet-Draft, draft-lemon-stub-networks-07, 10 November 2022, <https://www.ietf.org/archive/id/draft-lemon-stub-networks-07.txt>.

[ZC] Cheshire, S. and D. H. Steinberg, "Zero Configuration Networking: The Definitive Guide", O'Reilly Media, Inc., ISBN 0-596-10100-7, December 2005.

Authors' Addresses

Stuart Cheshire
Apple Inc.
One Apple Park Way
Cupertino, California 95014
United States of America

Phone: +1 (408) 996-1010
Email: cheshire@apple.com

Ted Lemon
Apple Inc.
One Apple Park Way
Cupertino, California 95014
United States of America

Phone: +1 (408) 996-1010
Email: elemon@apple.com