DNSSD
Internet-Draft
Intended status: Standards Track
Expires: 26 January 2026

T. Lemon
Apple Inc
M. Kardous
Silicon Labs

25 July 2025

Providing DNSSD Service on Infrastructure
draft-tlmk-infra-dnssd-00

Abstract

DNS Service Discovery provides several mechanisms whereby hosts can discover and advertise services on an IP network. Such discovery can be done using Multicast DNS (mDNS) or DNS, and advertising can be done with DNSSD Service Registration Protocol (SRP) or mDNS. This document describes a way to provide a unified DNSSD proxy service that allows hosts to advertise services using SRP and discover services using unicast DNS via a Discovery Proxy rather than using of mDNS, in scenarios where mDNS is currently the only option.

About This Document

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

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-tlmk-infra-dnssd/.

Discussion of this document takes place on the DNSSD Working Group mailing list (mailto:dnssd@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/dnssd/. Subscribe at https://www.ietf.org/mailman/listinfo/dnssd/.

Source for this draft and an issue tracker can be found at https://github.com/https://github.com/Abhayakara/draft-tlmk-infra-dnssd.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

DNS Service Discovery (DNS-SD) [RFC6763] is a general mechanism for advertising and discovering services on IP networks. mDNS is a commonly used transport for DNS-SD. However, it has several shortcomings: it relies entirely on multicast, which works somewhat poorly on WiFi networks. Devices publishing services have to always be available to answer mDNS queries, which can have significant battery impact. When doing service discovery, such devices may do WiFi beacon skipping to save power, and in so doing, miss a large percentage of multicast traffic, making mDNS unreliable.

To address this, this document describes a way of combining several existing technologies to reduce reliance on multicast. This can be done in, for example, a CE router [RFC7084], or a SNAC Router [I-D.ietf-snac-simple]. It can actually be done in any device that is expected to be continuously operational on a network link and has sufficient resources to provide the service.

There are four logical parts to the service: - The DNS [RFC1035] zone in which DNSSD information will be stored - The SRP [RFC9665] service, which is used to add and update services in the DNS zone - The Advertising Proxy [I-D.ietf-dnssd-advertising-proxy] service, which advertises the contents of the zone using mDNS on the infrastructure link - The Discovery Proxy [RFC8766], which enables discovery of local services that are advertised using mDNS using the unicast DNS protocol.

In addition, the service must be advertised so that devices that would like to make use of it can discover it.

1.1. Previous work

This specification relies on existing technology and makes reference to that technology assuming that the reader is already familiar with it. Readers should familiarize themselves with at least the following documents.

* The DNS specification [RFC1035] which discusses DNS zones
* The SRP specificaiton [RFC9665] which explains how to register services in the DNS without a pre-shared key
* The Advertising Proxy specification [I-D.ietf-dnssd-advertising-proxy] which explains how to advertise the contents of a DNS zone using mDNS

* The Discovery Proxy specification [RFC8766] which describes how to discover mDNS services on a link using DNS queries

* The DNS Push Specification [RFC8765] which describes how to efficiently do long-lived DNS queries

* The DNS-SD specification [RFC6763] which describes how to discover services using the DNS and mDNS protocols

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. Modes of deployment

This service can be deployed either as a centralized service provided by infrastructure, or as an ad-hoc service that takes advantage of infrastructure but is not part of infrastructure. An example of the first would be a Customer Edge router (CE Router) [RFC7084]. CE routers are typically autonomously operating devices--although they can be configured by the end user, this is not typical. However, since they are the basis for the network infrastructure of a home network, we think of DNSSD service provided by a CE router as network infrastructure.

An example of a device that provides full DNSSD service on an ad-hoc basis would be a SNAC router. SNAC routers connect infrastructure networks to stub networks on an ad-hoc basis and provide all four of the services required for DNSSD service to the SNAC network, but only provide Advertising Proxy service to the infrastructure network. This means that devices on infrastructure can discover devices on the stub network, but not to register with SRP service nor use the SNAC advertising proxy. A SNAC router that implements the behavior described in this document no longer has this limitation.

4. Content of Service Advertisement

The goal of advertising the service is to provide sufficient information that, having resolved the service advertisement, a user of the service has all the information needed to use the service. This includes at least:

* Name of the domain to use for service discovery

* Name of the domain to use for service registration

* Name of the host providing the DNSSD service

* Ports to use for the UDP DNS protocol when communicating with the service

4.1. Service Advertisement on Infrastructure

Service advertisement on infrastructure is provided using the 'dnssd.service.arpa.' domain. This is a locally-served domain [RFC6303]. The local DNS resolver on infrastructure MUST answer authoratively for queries in the dnssd.service.arpa zone. Because this is an infrastructure-provided service, infrastructure advertises only one service instance, with the service instance name "infrastructure." Therefore, an infrastructure-provided DNSSD service advertises the infrastructure service instance in dnssd.service.arpa as follows:

infrastructure.'service-name'.dnssd.service.arpa IN SRV 'data'
infrastructure.'service-name'.dnssd.service.arpa IN TXT 'data'

The infrastructure DNSSD service MUST support [I-D.ietf-dnssd-multi-qtypes]. Therefore, this query can be done as a single multi-qtype query. Typical DNS servers will, when answering an SRV query, include additional data containing address [RFC2782] pp 4-5. In such situations, if the DNSSD service is provided by infrastructure, all of the information required to discover it will be returned in response to a single query.

4.2. Ad-Hoc Service Advertisement

What we mean by "ad hoc" is something that is not integrated into infrastructure. Ad hoc servers do not have control of the local DNS resolver, and therefore cannot be discovered using DNS, and must instead be discovered using mDNS. Because there is no coordination, it is possible (and in some cases likely) that there will be more than one such server, so the service instance name should be handled normally [RFC6763] section 4.1.1.

Therefore, when advertising with mDNS, the service instance will be advertised as follows:

'instance-name'.'service-name'.local IN SRV 'data'
'instance-name'.'service-name'.local IN TXT 'data'

4.3. Content of SRV record

mDNS APIs typically do not provide a way of setting the priority and weight of the SRV record, and the infrastructure service always has the highest priority. Therefore, these fields SHOULD be set to zero, and MUST be ignored. The reason they MUST be ignored is that since they SHOULD be zero, and most devices will not be able to set them to any other value, treating them as described in [RFC2782] presents an opportunity for an attack by advertising a service with a weight of 65535.

The port field should be set to the UDP port on which SRP service is provided.

The target is the hostname of the host providing the service.

4.4. Content of the TXT record

TXT records are made up of a series of name=value pairs. The following names are defined:

srp-tcp=’port’: the port number to use for SRP registrations using the DNS Protocol over TCP. If not present, this service is assumed to be available on the port provided in the SRV record.

dns-udp=’port’: the port number to use for DNSSD queries using the DNS protocol over UDP. If not present, this service is assumed to be available on the port provided in the SRV record.

dns-tcp=’port’: the port number to use for DNSSD queries using the DNS protocol over TCP. If not present, this service is assumed to be available on the port provided in the SRV record.

srp-tls=’port’: the port number to use for SRP registrations using TLS. If not present, port 853 is assumed.

dns-tls=’port’: the port number to use for DNSSD queries using the DNS protocol over TLS. If not present, port 853 is assumed.

reg-dn=’domain’: the domain name to use in SRP registrations. If not present, default.service.arpa is assumed.

domains=’domain-list’: a comma-separated list of domains in which service discovery is available. If not present, dnssd.service.arpa and local are assumed to be the only domains.

’domain’=’ip-subnet-list’: a link-specific domain that can be used to query services on that specific IP link. The link is identified by a comma-separated list of IPv4 and/or IPv6 prefixes that are present on that link. See Section 4.4.1.

priority=’priority’: a priority for this service. See Section 4.4.2

4.4.1. Interface-specific domains

A DNSSD service may support link-specific discovery proxy service. In such cases, each IP link must have its own unique domain, which is specific to the individual DNSSD service. Each such domain must have an name=value entry in the TXT record. This entry has as its name a domain name. Its value is a comma-separated list of IP prefixes that are on-link for the IP link identified by the domain.

IP subnets are in the form ’IP address’/’prefix-length’. IP addresses are represented according to the IP address family. IPv4 addresses are in the dotted-decimal format as defined in [RFC952] in the section titled GRAMMATICAL HOST TABLE SPECIFICATION, in subsection A under ’address’. IPv6 addresses are represented as described in [RFC5952].

As a special (common) case, if the service only provides discovery proxy for a single link, and that is the link on which the DNSSD service is advertised, discovery of services on that link can use the "local" domain. In this case, no domains will be listed in the TXT record; if "local" discovery is to be supported alongside other domains, then the "local" domain must be included in the TXT record. If a service DNSSD service is advertised on more than one link, the local domain is specific to the link for which the destination address for the query is on-link. If the destination address is not on-link for any link, queries in .local are not valid and MUST be responded to with the REFUSED response code.

4.4.2. Service Priority

Infrastructure service is always the highest priority, and there can be only one such service. When infrastructure service is discovered, this is done using infrastructure. Consequently there is no need to try to discover an ad hoc service, and no need to choose amongst services. The infrastructure service therefore MUST NOT include a priority. Ad-hoc servers SHOULD include a priority. If a priority is not included, the priority of the Ad-Hoc service is assumed to be 65535.

Services should choose a priority based on their capabilities. The following priorities are defined:

0: Server is not constrained and is connected to a high-speed wired network link (that is, not WiFi, probably Ethernet or a fiber optic network).

100: Server is not constrained and is connected to a WiFi link

200: Server is constrained, but otherwise well able to provide service.

65535: Server can provide service if needed, but should not be preferred.

5. Discovering the DNSSD service

A host that wishes to use the DNSSD service must first discover it. Discovery follows a series of steps:

1. Attempt to discover an infrastructure-provided DNSSD service

2. Failing that, browse for a list of Ad-Hoc services.

3. If one or more Ad-Hoc services are returned by the browse, choose one using the priority specified in the TXT record.

4. If no server is discovered, or if no discovered server appears to work, fall back to mDNS-based DNSSD service

5.1. Advertising using RAs

DNSSD servers that send RAs MUST include a DNSSD-Service RA option in RAs that they send when the DNSSD service is active. DNSSD clients can distinguish infrastructure DNSSD service from ad-hoc service because infrastructure routers have nonzero lifetimes.

It can be the case that there is more than one infrastructure router. In some cases these routers will be part of a managed infrastructure, in which case DNSSD service provided by these routers MUST be a common service.

6. Dual-homed infrastructure DNSSD service

In a dual-homed network, there is more than one default router and potentially more than one DNSSD service. In the case of managed networks, the network operator MUST ensure that there is a single DNSSD service, even if it is advertised by more than one default router.

6.1. Unmanaged networks

In an unmanaged network, there is no way for the operator to decide which default router will provide the DNSSD service when more than one default router is able to do so. So we have the following options:

1. One router defers to the other

2. The routers share a common DNS zone either using SRP replication or DNS zone transfers with secondary failover

3. SRP clients are required to register with both services

Practically speaking option 3 is the only easy option, although it places a greater burden on the client. With option 1, the SRP client may take some time to notice that an SRP service has gone away and then reregister, and this is not ideal. Option 2 requires mechanisms that are not yet described in a standard. Consequently, when more than one infrastructure DNSSD service is present, consumers of the DNSSD service that will register their service using SRP MUST register with all infrastructure DNSSD servers.

7. Security Considerations

TODO Security

8. IANA Considerations

ALlocate ’service-name’, "_dnssd-server" is preferred

9. References

9.1. Normative References

[I-D.ietf-dnssd-advertising-proxy]
Cheshire, S. and T. Lemon, "Advertising Proxy for DNS-SD Service Registration Protocol", Work in Progress, Internet-Draft, draft-ietf-dnssd-advertising-proxy-04, 4 March 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-dnssd-advertising-proxy-04>.

[I-D.ietf-dnssd-multi-qtypes]
Bellis, R., "DNS Multiple QTYPEs", Work in Progress, Internet-Draft, draft-ietf-dnssd-multi-qtypes-08, 7 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-dnssd-multi-qtypes-08>.

[I-D.ietf-snac-simple]
Lemon, T. and J. Hui, "Automatically Connecting Stub Networks to Unmanaged Infrastructure", Work in Progress, Internet-Draft, draft-ietf-snac-simple-07, 7 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-snac-simple-07>.

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

[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>.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, DOI 10.17487/RFC2782, February 2000, <https://www.rfc-editor.org/rfc/rfc2782>.

[RFC5952] Kawamura, S. and M. Kawashima, "A Recommendation for IPv6 Address Text Representation", RFC 5952, DOI 10.17487/RFC5952, August 2010, <https://www.rfc-editor.org/rfc/rfc5952>.

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

[RFC7084] Singh, H., Beebee, W., Donley, C., and B. Stark, "Basic Requirements for IPv6 Customer Edge Routers", RFC 7084, DOI 10.17487/RFC7084, November 2013, <https://www.rfc-editor.org/rfc/rfc7084>.

[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>.

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

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

[RFC952] Harrenstien, K., Stahl, M., and E. Feinler, "DoD Internet host table specification", RFC 952, DOI 10.17487/RFC0952, October 1985, <https://www.rfc-editor.org/rfc/rfc952>.

[RFC9665] Lemon, T. and S. Cheshire, "Service Registration Protocol for DNS-Based Service Discovery", RFC 9665, DOI 10.17487/RFC9665, June 2025, <https://www.rfc-editor.org/rfc/rfc9665>.

9.2. Informative References

[RFC6303] Andrews, M., "Locally Served DNS Zones", BCP 163, RFC 6303, DOI 10.17487/RFC6303, July 2011, <https://www.rfc-editor.org/rfc/rfc6303>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

Ted Lemon
Apple Inc
Email: mellon@fugue.com

Mathieu Kardous
Silicon Labs
Email: somebody@example.com