Workgroup: DNSSD
Published: 12 July 2021
Intended Status: Standards Track
Expires: 13 January 2022
Authors: S. Cheshire T. Lemon
Apple Inc. Apple Inc.

Advertising Proxy for DNS-SD Service Registration Protocol

Abstract

An Advertising Proxy allows a device that accepts service registrations using Service Registration Protocol (SRP) to make those registrations visible to legacy clients that only implement 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 January 2022.

Copyright Notice

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).

There is also a desire to have DNS-Based Service Discovery work between multiple links that aren't part of the same broadcast domain [RFC7558]. Even within a single Wi-Fi broadcast domain it is beneficial to reduce multicast traffic, because, in comparison to Wi-Fi unicast traffic, Wi-Fi multicast is inefficient, slow, and unreliable [MCAST].

There are three complementary ways that this move towards decreased reliance on multicast is achieved.

One variant is pure end-to-end unicast, with services using unicast Service Registration Protocol [SRP] to register with a service registry, and clients using unicast DNS Push Notification subscriptions [RFC8765] over DNS Stateful Operations [RFC8490] to communicate with the service registry to discover and track changes to those registered services.

A second variant is a hybrid approach that facilitates legacy devices that only implement link-local Multicast DNS (like your ten-year-old network laser printer) having their services discovered by remote clients using a unicast DNS Push Notifications session to a Discovery Proxy [RFC8766].

The third variant, documented here, is a logical complement to the second variant. It enables legacy clients (that only implement link-local Multicast DNS) to discover services registered (using unicast) with a service registry. The service registry accepts service registrations using unicast Service Registration Protocol [SRP], and makes those service registrations visible, both to remote clients using unicast DNS Push Notifications [RFC8765] and, using the Advertising Proxy mechanism documented here, to local clients using Multicast DNS [RFC6762].

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 can be a component of any DNS authoritative server, though it logically makes most sense as a component of a service registry (a DNS authoritative server that implements Service Registration Protocol [SRP]). A client can send registration requests for any valid DNS records to a service registry, though 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 IPv6 addresses of the target host where that service can be reached.

When a service registry accepts a registration request for DNS records, a service registry that implements an Advertising Proxy also advertises equivalent records using Multicast DNS on one or more configured local multicast-capable interfaces. An Advertising Proxy could also advertise on one or more configured remote multicast-capable interfaces using a Multicast DNS Relay [RELAY]. For the purposes of this document, a local multicast-capable interface directly attached to the host and a remote multicast-capable interface connected via a relay are considered to be equivalent.

2.1. Name Conflicts

In the event that an SRP client attempts to register a record with a name that was already created in that registry by a different SRP client, or is otherwise disallowed by policy, a name conflict is reported and the new client is required to choose a new name.

Similarly, Multicast DNS implements first-come-first-served name allocation. When a registered record is advertised using Multicast

DNS it may suffer a name conflict if a conflicting Multicast DNS record with that name already exists on that link. In the case of network failure and subsequent recovery, Multicast DNS can also signal name conflicts at a later time during the life of a record registration. For example, if the network link is partitioned at the time of record registration, the name conflict may not be discovered until later when the partition is healed.

Specifically, a name conflict can occur:

1. During the SRP validation process, because another SRP client has already registered the same name.

2. Immediately while the Advertising Proxy is registering the name, if the Multicast DNS uniqueness probes detect a conflicting record.

3. After the name has been successfully registered, but before the response has been sent to the client.

4. After the initial response has been sent to the client.

In the first three cases, the client can be notified of the conflict at the time of registration, and is expected to choose a new name. In the last case, SRP clients must be coded defensively to handle the case where an apparently successful record registration is later determined to be in conflict, just as existing Multicast DNS clients have to be coded defensively to handle late conflicts gracefully. With a sleepy SRP client there may be no way to notify it of the conflict until it next re-registers. In the case of late conflicts, the service registry with Advertising Proxy capability is responsible for selecting a temporary new name to be used until the client renews. When the client next renews, the service registry informs the client of the new name the service registry selected on its behalf. The client can choose to accept that new name, or select a new name of its own choosing.

The registration process has several steps. First the hostname claimed by the SRP client must be registered. Once this has succeeded, the Advertising Proxy can register all of the service instances that point to that hostname. When all of these registrations have succeeded, the service registry can finally send its response to the SRP client. If any of them fail, they must all be removed and the client notified of the failure. If the failure is a result of a name conflict, the response code should be YXDOMAIN. Other SRP failures are documented in the SRP specification. Any other failures not contemplated in the SRP specification return SERVFAIL.

2.1.1. Name Conflicts in Managed Namespaces

In some cases, the name conflict resolution behavior described above is neither needed nor desirable. For instance, when the set of expected SRP clients is known to include only clients added with some kind of commissioning or on-boarding protocol that guarantees that hostnames are unique, it may cause serious problems to rename such a device.

In this situation, the Advertising Proxy behavior should be different: it should be assumed that all names registered with SRP that survive SRP's first-come, first-serve name conflict detection are indeed as intended. Any conflict that may be discovered as a result of advertising those names using mDNS can be assumed to either be an error or an attack, and there is no benefit to renaming such a device: it will not be usable under its new name.

In this case, the Advertising Proxy simply performs normal SRP first-come, first-serve naming and then updates its local idea of the SRP namespace. This update is then reflected in mDNS. If a conflict is detected, the Advertising Proxy schedules a new attempt to claim the name at some time in the future: long enough that these re-attempts to not generate excessive multicast traffic, but short enough that an accidental conflict is cured in a reasonable timeframe.

The downside to this approach is that if the device on the multicast network persists in claiming the name, the SRP client that claimed it will be unreachable. Networks that use Advertising Proxies configured to behave in this way should provide a way to rename the device that is suffering the conflict. However, if the failure is the result of a malicious attack by a device on the multicast network, that device will have to be identified and removed before the attack can be eliminated.

In order to address this problem, it may be advisable to provide with a way for the advertising proxy to inform the mDNS service that it should continue to advertise the name that is in conflict, rather than ceasing to do so when the conflict is detected.

2.2. Data Translation

As with a Discovery Proxy [RFC8766] some translation needs to be performed before the Advertising Proxy makes the registered unicast data visible using Multicast DNS. Specifically, the unicast DNS domain name suffix configured for Advertising Proxy use is stripped off and replaced with the top-level label "local".

2.3. 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.

2.4. No Address Suppression

Unlike a Discovery Proxy [RFC8766], an Advertising Proxy does not need to selectively suppress link-local [RFC3927] [RFC4862] or other addresses. Since the clients of the service registry are registering their records in a unicast DNS namespace, there is a presumption they they will only register addresses with sufficient scope to be usable by the anticipated clients. No further filtering or suppression by the service registry is required. In most cases it is acceptable for devices registering with a service registry to register all of their available addresses, and a client implementing Happy Eyeballs [RFC8305] connecting to that service will automatically select an appropriate address to use.

2.5. 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. 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

[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/info/rfc2119>.

[RFC6760] Cheshire, S. and M. Krochmal, "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. and M. Krochmal, "Special-Use Domain Names", RFC 6761, DOI 10.17487/RFC6761, February 2013, <https://www.rfc-editor.org/info/rfc6761>.

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

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

[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/info/rfc8174>.

[RFC8490] Bellis, R., Cheshire, S., Dickinson, J., Dickinson, S., Lemon, T., and T. Pusateri, "DNS Stateful Operations", RFC 8490, DOI 10.17487/RFC8490, March 2019, <https://www.rfc-editor.org/info/rfc8490>.

[RFC8765] Pusateri, T. and S. Cheshire, "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-09, 11 January 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-dnssd-srp-09>.

5.2. Informative References

[RFC3492] Costello, A., "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., "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>.

[RFC3927] Cheshire, S., Aboba, B., and E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses", RFC 3927, DOI 10.17487/RFC3927, May 2005, <https://www.rfc-editor.org/info/rfc3927>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <https://www.rfc-editor.org/info/rfc4862>.

[RFC6055] Thaler, D., Klensin, J., and S. Cheshire, "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., and D. Migault, "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>.

[RFC8305] Schinazi, D. and T. Pauly, "Happy Eyeballs Version 2: Better Connectivity Using Concurrency", RFC 8305, DOI 10.17487/RFC8305, December 2017, <https://www.rfc-editor.org/info/rfc8305>.

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

[MCAST] Perkins, C. E., McBride, M., Stanley, D., Kumari, W., and J. C. Zuniga, "Multicast Considerations over IEEE 802 Wireless Media", Work in Progress, Internet-Draft, draft-ietf-mboned-ieee802-mcast-problems-13, 4 February 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-mboned-ieee802-mcast-problems-13>.

[RELAY] Lemon, T. and S. Cheshire, "Multicast DNS Discovery Relay", Work in Progress, Internet-Draft, draft-ietf-dnssd-mdns-relay-04, 22 February 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-dnssd-mdns-relay-04>.

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

[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