DNS-SD/mDNS Extensions
Internet-Draft
Intended status: Informational
Expires: August 17, 2014

K. Lynn, Ed.
Consultant
S. Cheshire
Apple, Inc.
M. Blanchet
Viagenie
D. Migault
Orange

February 13, 2014

Requirements for Scalable DNS-SD/mDNS Extensions
draft-ietf-dnssd-requirements-01

Abstract

DNS-SD/mDNS is widely used today for discovery and resolution of services and names on a local link, but there are use cases to extend DNS-SD/mDNS to enable service discovery beyond the local link. This document provides a problem statement and a list of requirements.

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 http://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 August 17, 2014.

Copyright Notice

Table of Contents

1. Introduction

DNS-Based Service Discovery [DNS-SD] in combination with its companion technology Multicast DNS [mDNS] is widely used today for discovery and resolution of services and names on a local link. However, as users move to multi-link home or campus networks they find that mDNS does not work across routers. DNS-SD can also be used in conjunction with conventional unicast DNS to enable wide-area service discovery, but this capability is not yet widely deployed. This disconnect between customer needs and current practice has led to calls for improvement, such as the Educause petition [EP].

In response to this and similar evidence of market demand, several products now enable service discovery beyond the local link using different ad-hoc techniques. However, it is unclear which approach represents the best long-term direction for DNS-based service discovery protocol development.

DNS-SD/mDNS in its present form is also not optimized for network technologies where multicast transmissions are relatively expensive. Wireless networks such as [IEEE.802.11] may be adversely affected by excessive mDNS traffic due to the higher network overhead of multicast transmissions. Wireless mesh networks such as 6LoWPAN [RFC4944] are effectively multi-link subnets where multicasts must be forwarded by intermediate nodes.

It is in the best interests of end users, network administrators, and vendors for all interested parties to cooperate within the context of the IETF to develop an efficient, scalable, and interoperable standards-based solution.

This document defines the problem statement and gathers requirements for Scalable DNS-SD/mDNS Extensions.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in "Key words for use in RFCs to Indicate Requirement Levels" [RFC2119].

1.2. Terminology and Acronyms

Service: An endpoint (host and port) for a given application protocol. Services are identified by Service Instance Names.

DNS-SD: DNS-Based Service Discovery, as specified in [DNS-SD], is a conventional application of DNS Resource Records and messages to facilitate the discovery and location of services.

mDNS: Multicast DNS, as specified in [mDNS], is a transport protocol that facilitates DNS-SD on a local link in the absence of DNS infrastructure.

SSD: Scalable DNS-SD is a future extension of DNS-SD/mDNS that meets the requirements set forth in this document.

Scope of Discovery: A node in a local or global namespace, e.g., a DNS zone, that is the target of a given DNS-SD query.

Zero Configuration: A set of technologies including DNS-SD/mDNS that enable local address and name assignment in the absence of DHCP or DNS infrastructure. May also refer more generally to a deployment of SSD that requires no administration.

Incremental Deployment: An orderly transition, as a network installation evolves, from DNS-SD/mDNS to SSD.

2. Problem Statement

Service discovery beyond the local link is perhaps the most important feature currently missing from the DNS-SD/mDNS framework. Other issues and requirements are summarized below.

2.1. Multi-link Naming and Discovery

A list of desired DNS-SD/mDNS improvements from network administrators in the research and education community was issued in

the form of the Educause petition [EP]. The following is a summary of the technical issues:

- Products that advertise services such as printing and multimedia streaming via DNS-SD/mDNS are not currently discoverable by devices on other links. It is common practice for enterprises and institutions to use wireless links for client access and wired networks for server infrastructure, typically on different subnets. DNS-SD used with conventional unicast DNS does work when devices are on different links, but the resource records that describe the service must somehow be entered into the unicast DNS namespace.

- Entering DNS-SD records manually into a unicast DNS zone file works, but requires a DNS administrator to do that and is fragile when IP addresses of devices change dynamically, as is common when DHCP is used.

- Automatically adding DNS-SD records using DNS Update works, but requires that the DNS server be configured to allow DNS Updates, and requires that devices be configured with the DNS Update credentials to permit such updates, which has proven to be onerous.

- Therefore, a mechanism is desired that populates the DNS namespace with the appropriate DNS-SD records with less manual administration than typically needed for a unicast DNS server.

The following is a summary of the technical requirements:

- It must scale to a range of hundreds to thousands of DNS-SD/mDNS enabled devices in a given environment.

- It must simultaneously operate over a variety of network link technologies, such as wired and wireless networks.

- It must not significantly increase network traffic (wired or wireless).

- It must be cost-effective to manage at up to enterprise scale.

2.2. IEEE 802.11 Wireless LANs

Multicast DNS was originally designed to run on Ethernet - the dominant link-layer at the time. In shared Ethernet networks, multicast frames place little additional demand on the shared network medium compared to unicast frames. In IEEE 802.11 networks however, multicast frames are transmitted at a low data rate supported by all

receivers. In practice, this data rate leads to a larger fraction of airtime being devoted to multicast transmission. Some network administrators block multicast traffic or convert it to a series of link-layer unicast frames.

Wireless links may be orders of magnitude less reliable than their wired counterparts. To improve transmission reliability, the IEEE 802.11 MAC requires positive acknowledgement of unicast frames. It does not, however, support positive acknowledgement of multicast frames. As a result, it is common to observe much higher loss of multicast frames on wireless as compared to wired network technologies.

Enabling service discovery on IEEE 802.11 networks requires that the number of multicast frames be restricted to a suitably low value, or replaced with unicast frames to use the MAC's reliability features.

2.3. Low Power and Lossy Networks (LLNs)

Emerging wireless mesh networking technologies such as RPL [RFC6550] and 6LoWPAN present several challenges for the current DNS-SD/mDNS design. First, Link-Local multicast scope [RFC4291] is defined as a single-hop neighborhood. A single subnet prefix in a wireless mesh network may often span multiple links, therefore a larger multicast scope is required to span it [I-D.ietf-6man-multicast-scopes]. mDNS is not currently specified for greater than Link-Local scope.

Additionally, low-power nodes may be offline for significant periods either because they are "sleeping" or due to connectivity problems. In such cases LLN nodes might fail to respond to queries or defend their names using the current design.

3. Basic Use Cases

The following use cases are defined with different characteristics to help motivate, distinguish, and classify the target requirements. They cover a spectrum of increasing deployment and administrative complexity.

(A) Personal Area networks: the simplest example of a DNS-SD/mDNS network may consist of a single client and server, e.g., one laptop and one printer, on a common link. Such networks may not contain a router, but instead use Zero Configuration to mitigate the lack of infrastructure.

(B) Classic home networks, consisting of:

* Single exit router: the network may have multiple upstream providers or networks, but all outgoing and incoming traffic goes through a single router.

* One-level depth: multiple links on the network are bridged to form a single subnet, which is connected to the default router.

* Single administrative domain: all nodes under the same admin entity. (However, this does not necessarily imply a network administrator.)

(C) Advanced home and small business networks [I-D.ietf-homenet-arch]:

Like B but consist of multiple wired and/or wireless links, connected by routers, behind the single exit router. However, the forwarding nodes are largely self-configuring and do not require routing protocol administration. Such networks should also not require DNS administration.

(D) Enterprise networks:

Like C but consist of arbitrary network diameter under a single administrative domain. A large majority of the forwarding and security devices are configured.

(E) Higher Education networks:

Like D but core network may be under a central administrative domain while leaf networks are under local administrative domains.

(F) Mesh networks such as RPL/6LoWPAN:

Multi-link subnets with prefixes defined by one or more border routers. May comprise any part of networks C, D, or E.

4. Requirements

Any successful SSD solution(s) will have to strike the proper balance between competing goals such as scalability, deployability, and usability. With that in mind, none of the requirements listed below should be considered in isolation.

REQ1: The scope of the discovery should be either automatically determined by the discovering devices or configured (selected) in the case of multiple choices.

REQ2: For use cases A, B, and C, there should be a zero configuration mode of operation.

REQ3: For use cases D and E, there should be a way to configure the scope of the discovery and also support both smaller (e.g., department) and larger (e.g., campus-wide) discovery scopes.

REQ4: For use cases D and E, there should be an incremental way to deploy the solution.

REQ5: SSD should integrate or at least should not break any current link scope DNS-SD/mDNS protocols and deployments.

REQ6: SSD must be capable of spanning multiple links (hops) and network technologies.

REQ7: SSD must be scalable to thousands of nodes with minimal configuration and without degrading network performance. A possible figure of merit is that, as the number of services increases, the amount of traffic due to SSD on a given link remains relatively constant.

REQ8: SSD should enable a way to provide a consistent user experience whether local or global services are being discovered.

REQ9: The information presented by SSD should reflect reality. That is, new information should be available in a timely fashion and stale information should not persist.

5. Namespace Considerations

The unicast DNS namespace contains globally unique names. The mDNS namespace contains locally unique names. Clients discovering services may need to differentiate between local and global names or to determine that names in different namespaces identify the same service.

SSD should support rich internationalized labels within Service Instance Names, as DNS-SD/mDNS does today. SSD must not negatively impact the global DNS namespace or infrastructure.

The problem of publishing local services in the global DNS namespace may be generally viewed as exporting local resource records and their associated labels into some DNS zone. The issues related to defining labels that are interoperable between local and global namespaces are discussed in [I-D.sullivan-dnssd-mdns-dns-interop].

6. Security Considerations

Insofar as SSD may automatically gather DNS-SD resource records and publish them over a wide area, the security issues are likely to be the union of those discussed in [mDNS] and [DNS-SD]. The following sections highlight potential threats that are posed by deploying DNS-SD over multiple links or by automating DNS-SD administration.

6.1. Scope of Discovery

As mDNS is currently restricted to a single link, the scope of the advertisement is limited, by design, to the shared link between client and server. In a multi-link scenario, the owner of the advertised service may not have a clear indication of the scope of its advertisement.

If the advertisement propagates to a larger set of links than expected, this may result in unauthorized clients (from the perspective of the owner) connecting to the advertised service. It also discloses information (about the host and service) to a larger set of potential attackers.

If the scope of the discovery is not properly setup or constrained, then information leaks will happen outside the appropriate network.

6.2. Multiple Namespaces

There is a possibility of conflicts between the local and global DNS namespaces. Without adequate feedback, a client may not know if the target service is the correct one, therefore enabling potential attacks. [Example? KEL]

6.3. Authorization

DNSSEC can assert the validity but not the veracity of records in a zone file. The trust model of the global DNS relies on the fact that human administrators either a) manually enter resource records into a zone file, or b) configure the DNS server to authenticate a trusted device (e.g., a DHCP server) that can automatically maintain such records.

An imposter may register on the local link and appear as a legitimate service. Such "rogue" services may then be automatically registered in wide area DNS-SD.

6.4. Authentication

Up to now, the "plug-and-play" nature of mDNS devices has relied only on physical connectivity. If a device is visible via mDNS then it is assumed to be trusted. This is no longer likely to be the case in larger networks.

If there is a risk that clients may be fooled by the deployment of rogue services, then application layer authentication should probably be considered.

6.5. Privacy Considerations

Mobile devices such as smart phones that can expose the location of their owners by registering services in arbitrary zones pose a risk to privacy. Such devices must not register their services in arbitrary zones without the approval of their operators. However, it should be possible to configure one or more "safe" zones, e.g., based on subnet prefix, in which mobile devices may automatically register their services.

7. IANA Considerations

This document currently makes no request of IANA.

Note to RFC Editor: this section may be removed upon publication as an RFC.

8. Acknowledgments

We gratefully acknowledge contributions and review comments made by RJ Atkinson, Tim Chown, Guangqing Deng, Ralph Droms, Educause, David Farmer, Matthew Gast, Peter Van Der Stok, and Thomas Narten.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, September 2007.

[RFC6550] Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, March 2012.

[mDNS] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, February 2013.

[DNS-SD] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, February 2013.

9.2. Informative References

[I-D.ietf-6man-multicast-scopes]
Droms, R., "IPv6 Multicast Address Scopes", draft-ietf-6man-multicast-scopes-02 (work in progress), November 2013.

[I-D.ietf-homenet-arch]
Chown, T., Arkko, J., Brandt, A., Troan, O., and J. Weil, "IPv6 Home Networking Architecture Principles", draft-ietf-homenet-arch-11 (work in progress), October 2013.

[I-D.sullivan-dnssd-mdns-dns-interop]
Sullivan, A., "Requirements for Labels to Interoperate Between mDNS and DNS", draft-sullivan-dnssd-mdns-dns-interop-00 (work in progress), January 2014.

[EP] "Educause Petition", https://www.change.org/petitions/from-educause-higher-ed-wireless-networking-admin-group, July 2012.

[IEEE.802.11]
"Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11-2012, 2012, <http://standards.ieee.org/getieee802/download/802.11-2012.pdf>.

[static] "Manually Adding DNS-SD Service Discovery Records to an Existing Name Server", July 2013, <http://www.dns-sd.org/ServerStaticSetup.html>.

Authors' Addresses

Kerry Lynn (editor)
Consultant

Phone: +1 978 460 4253
Email: kerlyn@ieee.org

Stuart Cheshire
Apple, Inc.
1 Infinite Loop
Cupertino , California 95014
USA

Phone: +1 408 974 3207
Email: cheshire@apple.com

Marc Blanchet
Viagenie
246 Aberdeen
Quebec , Quebec G1R 2E1
Canada

Email: Marc.Blanchet@viagenie.ca
URI: http://www.viagenie.ca

Daniel Migault
Orange
38-40 rue du General Leclerc
Issy-les-Moulineaux 92130
France

Phone: +33 1 45 29 60 52
Email: mglt.biz@gmail.com