Requirements for Scalable DNS-SD/mDNS Extensions
draft-lynn-dnssd-requirements-00

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

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 [TBD]

Discovery Scope

Zero Configuration

Incremental Deployment

2. Problem Statement

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

2.1. Multilink 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 technical
summary of the issues:

o 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.

o Entering DNS-SD records manually into a unicast DNS zone file
   works, (as has been done for many years for the Terminal Room
   printers at IETF meetings) but requires the DNS administrator to
   know how to do that [static] and is fragile when IP addresses of
   devices may change, as is common when DHCP is used.

o 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.

o 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 technical summary of the requirements:

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

o It must work with wired and wireless networks from different
   vendors.

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

o It must be easily managed at an enterprise scale.

o It must be provided at a reasonable cost. [CapEx + OpEx. KEL]

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 above 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.

Wired 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].

   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 constraints to
   help distinguish and classify the target requirements.

      (A) Personal Area networks; e.g., one laptop and one printer.
      This is the simplest example of a DNS-SD/mDNS network.

      (B) Classic home networks, consisting of:

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

      * One level depth: all links on the network are connected to the
         same default router.

      * Single administrative domain: all nodes under the same admin
         entity.

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

      Like B but consist of two or more 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.

      (D) Enterprise networks:

      Like C but consist of arbitrary 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 network B and any part of networks C, D, or
   E.

4. Internationalization Considerations

   The solution should support rich international text, as do DNS-SD and
   mDNS today. Users will not accept a solution that does not allow the
   richness of service naming that they currently have with mDNS, manual
   zone files, and DNS Update today.

5. Namespace Considerations

   The unicast DNS namespace contains globally unique names. Naming
   services over a local scope contain locally unique names. Clients
   discovering services need to be able to differentiate global names
   from local names.

6. Requirements

   [This is a strawman proposal. MB]

   REQ1: The scope of the discovery should be either automatically
      found by the discovering devices and/or configured.

   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 (ex:
      department) and larger (ex: campus-wide) discovery scopes.

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

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

   REQ6: The new solution MUST be capable of spanning multiple links
      (hops) and network technologies.

   REQ7: The new solution MUST be scalable to thousands of servers with
      minimal configuration and without degrading network performance.

   REQ8: The new solution MUST provide a consistent user experience
      whether local or global services are being discovered.

7. IANA Considerations

   This document currently makes no request of IANA.

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

8. Security Considerations

   [Not complete - initial ideas. MB/KEL]

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

   Visiting nodes on a network may discover more services than desired
   by the network policies, if filtering of discovery packets was not
   properly setup. [Is this a NAC or DNS problem? KL]

   Depending on the chosen solution, there is a possibility of name
   space conflicts between the DNS tree and this solution. In this
   case, a node may not know if the target node or service is the right
   one, therefore enabling ground for various attacks.

   The DNS-SD/mDNS framework security considerations also apply.

   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.

   By contrast, the "plug-and-play" nature of mDNS devices has up to now
   depended 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. Still, the new solution SHOULD
   leverage existing security solutions and not invent new ones.

   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 "home" zones, e.g., based
   on subnet prefix, in which mobile devices may automatically register
   their services.

[9](). Acknowledgments

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

10. References

10.1. 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.

10.2. Informative References

[I-D.ietf-6man-multicast-scopes]
            Droms, R., "IPv6 Multicast Address Scopes", draft-ietf-
            6man-multicast-scopes-00 (work in progress), August 2013.

[I-D.ietf-homenet-arch]
            Chown, T., Arkko, J., Brandt, A., Troan, O., and J. Weil,
            "Home Networking Architecture for IPv6", draft-ietf-
            homenet-arch-10 (work in progress), August 2013.

[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