mDNS X-link review
draft-otis-dnssd-mdns-xlink-02

Abstract

Multicast DNS will not normally extend beyond the MAC Bridge. Such limitations are problematic when desired services are beyond the reach of multicast mDNS. This document explores options for overcoming this limitation.

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 [RFC2119].

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 18, 2014.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents.
carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction .............................................. 3
2. Possible Solutions ......................................... 3
   2.1. Selective Forwarding based on IGMP or MLD snooping .... 3
   2.2. RBridge ............................................. 4
   2.3. L2TP VPN ........................................... 4
   2.4. VLAN ............................................... 4
   2.5. Convert mDNS to DNS .................................. 5
3. IANA Considerations ........................................ 6
4. Security Considerations ..................................... 6
5. Acknowledgements .......................................... 7
6. References - Informative ................................... 7
Author’s Address .............................................. 9
1. Introduction

mDNS [RFC6762] normally allows MAC entities to make their services known on MAC Bridged LANs without use of centralized discovery services. Multicast limits the range of this publication to LANs able to forward mDNS frames. A Bridge is a mechanism transparent to end stations on LANs interconnected by Bridges designated to forward frames normally through participation in a Spanning Tree Algorithm.

A Bridge forwards frames based on prior source MAC associations with incoming frames on different LAN ports. Source MAC and LAN port associations are recommended to expire in 300 seconds. Frames containing source multicast MAC are silently discarded as invalid. Frames containing a destination MAC on the same LAN port already associated with the MAC are silently discarded. A valid incoming frame with a destination not previously associated with a different LAN port is forwarded (flooded) to all other LAN ports, otherwise when a MAC destination address is associated with a different LAN port from which the frame was received, the frame is selectively forwarded to this port. All broadcast and multicast MAC are flooded to all other LAN ports because the MAC does not represent a valid source. Flooding operation may create a storm of replicated frames having an unknown MAC destination whenever forwarding is enabled on LAN ports connected in a loop.

In IEEE 802.11 wireless networks, multicast frames are transmitted at a low data rate supported by all receivers. Multicast on wireless networks may thereby lower overall network throughput. 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 compared against wired network technologies.

2. Possible Solutions

2.1. Selective Forwarding based on IGMP or MLD snooping

Internet Group Management Protocol (IGMP) [RFC3376] supports multicast on IPv4 networks. Multicast Listener Discovery (MLD) [RFC3810] supports multicast management on IPv6 networks using ICMPv6 messaging in contrast to IGMP’s bare IP encapsulation. This
management allows routers to announce their multicast membership to neighboring routers. To optimize which LANs receive forwarded multicast frames, IGMP or MLD snooping can be used to determine the presence of listeners as a means to permit selective forwarding of multicast frames.

2.2. RBridge

R Bridges [RFC6325] are compatible with previous IEEE 802.1 customer bridges as well as IPv4 and IPv6 routers and end nodes. R Bridges may support either IEEE 802.3 or other link technologies. R Bridges are invisible to current IP routers as bridges are and, like routers, terminate the Bridge spanning tree protocol. The R Bridge design supports VLANs and optimization of the distribution of multi-destination frames based on VLAN ID or on IP-derived multicast groups. It also allows unicast forwarding tables at transit R Bridges to be sized according to the number of R Bridges (rather than the number of end nodes), which allows their forwarding tables to be substantially smaller than in conventional customer bridges.

[RFC3927] provides an overview of IPv4 address complexities related with dealing with multiple segments and interfaces. IPv6 introduces new paradigms in respect to interface address assignments which offer scoping as explained in [RFC4291]. The use of R Bridge has the capacity of greatly simplifying this environment while also eliminating bottlenecks imposed by a Spanning Tree Algorithm.

If it can be determined an additional layer can be added within R Bridge to implement selective multicast forwarding, input for this extension should be defined to assist with mDNS management.

2.3. L2TP VPN

L2TP VPN [RFC3931] with experimental [RFC4045] attempt to handle multicast by mitigating redundant traffic which remains fairly problematic.

2.4. VLAN

There are several products being introduced into the market that attempt to solve the problem stated in the charter. They normally use VLAN [RFC5517] to selectively extend multicast forwarding beyond Bridge limitations. This does not represent a general solution but can support specific services being offered by dynamic devices within a local IP address space.
2.5. Convert mDNS to DNS

Rather than using MAC as an exchange basis, IP addresses made visible by DNS [RFC1035] that conform with [RFC6763] can be used instead. Direct access to an IP address is better assured with a single DHCP [RFC2131] or [RFC3315] server for IPv4 and IPv6 respectively that responds to interconnected networks. In such a configuration, it is possible to have DHCP indicate which DNS server is to be used as a means to offer combined local and Internet namespace.

Automation needed to populate the information published in DNS normally depends on Kerberos [RFC4120] and LDAP [RFC2251] servers supporting either a campus or corporate network.

Automated conversion of mDNS into unicast DNS can be problematic from a security standpoint as can the propagation of multicast frames. mDNS only requires compliance with [RFC5198] rather than IDNA2008 [RFC5895]. This means mDNS does not ensure instances are visually unique and may contain spaces and punctuation not permitted by IDNA2008. mDNS also permits name compression of SRV target names that DNS currently does not ensure support.

Public Suffix lists might help simplify the creation of A-Labels from UTF-8 user input by offering matching items for user selection. A Public Suffix list represents DNS domain names reserved for registrations by appropriate authorities. This still leaves the domain registered above the public suffix, but its validation should involve fewer transactions.

Replacing ASCII punctuation and spaces in the label with the ‘_’ character, except when located as the leftmost character, may reduce some handling issues related to end of string parsing, since labels in DNS normally do not contain spaces or punctuation. Nevertheless, DNS is able to handle such labels within sub-domains of registered domains.

Services outside the ".local." domain may have applications obtaining domain search lists provided by DHCP ([RFC2131] and [RFC3315] for IPv4 and IPv6 respectively or RA DNSSL [RFC6106] also for IPv6. Internet domains need to be published in DNS as A-Labels [RFC3492] because IDNA2008 compliance depends on A-label enforcement by registrars. Therefore A-Labels and not U-Labels must be published in DNS for Internet domains at this time. There is also a DNS extension to support the live browse feature found in mDNS.

The SRV scheme used by mDNS has also been widely adopted in the Windows OS since it offered a functional replacement for Windows Internet Name Service (WINS) as their initial attempt which lacked
sufficient name hierarchy.

It is unknown whether sufficient filtering of mDNS to expose just those services likely needed will sufficiently protect wireless networks. The extent RBridge use and something analogous to IGMP or MLD for selective forwarding might help to mitigate otherwise spurious traffic is unknown.

Open source of corporate server implementations based on a Debian distro are currently available with plug-ins able to support Windows and OS X.

2.5.1. Reliable Wireless Multicast

[RFC6951] transport protocol was designed to efficiently exchange frames rather than byte streams. It can operate with partial reliability [RFC3758] while still allowing receivers to detect and request specific lost frames. This might be possible while also using multicast MACs and IP Addresses. This protocol currently has not been structured to support multicast. This transport also extends the DNS 16 bit transactional nonce not even present in mDNS with an additional 32 bit random session ID.

3. IANA Considerations

This document requires no IANA consideration.

4. Security Considerations

Layer 2 Bridging that might be used to extend mDNS is not inherently secure. See [RFC6325] for a list of possible concerns and mitigation methods.

Conveying both the MAC and IP address beyond the LAN may enable attacks that would have otherwise been prevented.

Moving mDNS services into DNS MUST only publish services able to withstand this greater exposure.

Any query for a name ending with ".local." MUST be resolved using mDNS.

It is not uncommon for CPE equipment’s DNS settings being maliciously modified. Often this equipment does not create or retain settings logs, where a reset or power cycling removes evidence of tampering.
Establishing ".local." as the first domain offered in a domain search list could ensure local services receive higher priority, but such a priority could also permit local spoofing of services otherwise resolved using DNS. A priority on local resolution may also result in a 3 second additional delay for global resolutions.

5. Acknowledgements

The authors wish to acknowledge valuable contributions from the following: Dave Rand, Michael Tuexen

6. References - Informative


Author’s Address

Douglas Otis
Trend Micro
10101 N. De Anza Blvd
Cupertino, CA  95014
USA

Phone: +1.408.257-1500
Email: doug_otis@trendmicro.com