DNSEXT Working Group
INTERNET-DRAFT
Category: Standards Track
<draft-aboba-dnsext-mdns-01.txt>
14 July 2000

Levon Esibov
Bernard Aboba
Dave Thaler
Microsoft

Multicast DNS

1. Copyright Notice

2. Abstract

Today, with the rise of home networking, there are an increasing number of small networks operating without a DNS server. In order to allow DNS name resolution in such environments, the use of a multicast DNS is proposed.

3. Introduction

Multicast DNS enables DNS name resolution in the scenarios when conventional DNS name resolution is not possible. Namely, when there are no DNS servers available on the network or available DNS servers do not provide the name resolution for the names of the hosts on the local network. The latter case, for example, corresponds to a scenario when a home network that doesn't have a DNS server is connected to the Internet through an ISP and the home network hosts are configured with the ISP's DNS server for the name resolution. The ISP's DNS server provides the name resolution for the names registered on the Internet, but doesn't provide name resolution for the names of the hosts on the home network.

This document discusses multicast DNS, an extension to the DNS protocol which consists of a single change to the method of use, and no change to the format of DNS packets.

4. Terminology

In this document, the key words "MAY", "MUST, "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [1].

5. Name resolution using Multicast DNS

This extension to the DNS protocol consists of a single change to the method of use, and no change whatsoever to the current format of DNS packets. Namely, this extension allows multicast DNS queries to be sent to and received on port 53 using the LINKLOCAL addresses for IPv4 and IPv6, which are yet to be assigned by IANA. LINKLOCAL addresses are used since the expectation is that if a network has a router, then this router can function as a mini-DHCP server, as described in [3], and a DNS proxy, possibly implementing dynamic DNS. Thus there is not expected to be a need for use of multicast DNS in networks with multiple segments.

Hosts actively using mDNS behave as DNS servers, and inherit all the obligations of DNS servers, as described in [8], including the need to increment the serial number in SOA records. It is suggested that the serial number be taken from a monotonically increasing clock which implies that the serial number will be monotonic across reboots. However, this is not crucial if the DNS TTL is set to a low value.

In order to prevent a DNS server from recursive resolution of the multicast DNS queries, the RD (Recursion Desired) bit in the Header section of the query MUST be set to 0. If the RD bit is set to 1, then it is ignored.

DNS resolvers configured to use multicast DNS for name resolution listen on port 53 on the LINKLOCAL mDNS address. Responses SHOULD contain a AA (Authoritative Answer) bit set to 0.

Issue: Handling of the AA bit was flagged as a subject for more discussion.

If a query sent to the LINKLOCAL mDNS addresses is not positively resolved ("positively resolved" refers in this document to the response with the RCODE set to 0) during a limited amount of time, then the

resolver MAY repeat the transmission of a query in order to assure themselves that the query has been received by any hosts capable of answering the query.

Resolvers MUST anticipate receiving no replies to some multicasted queries, in the event that no multicast-enabled clients are available within the multicast scope, or in the event that no positive non-null responses exist to the transmitted query.

If no positive response is received, a resolver treats it as a response that no records of the specified type and class for the specified name exist (NXRRSET), which should be cached according to RFC 2308 [15].

6. Usage model

Multicast DNS usage is determined by the domain search configuration as well as by special treatment of the ".lcl.arpa" namespace. The resolver treat queries for ".lcl.arpa" as a special case, thus avoiding the need to formally allocate a new top level domain. The domain search list can be configured manually or automatically via a DHCP option. There is therefore no need for another mDNS configuration mechanism.

The resolver will always do a multicast query for names in the ".lcl.arpa" namespace if there is no NS record corresponding to the name. mDNS is only used to resolve unqualified names. This means, for example, that queries for "www.microsoft.com" will never be resolved via mDNS.

If ".lcl.arpa" is not in the domain search list, then mDNS MUST NOT be used by that host. An auto-configured host will typically have ".lcl.arpa" first in its search list so that it will be enabled to use mDNS. Typically an enterprise host will not have ".lcl.arpa" in its searchlist at all so that it will not use mDNS.

6.1. Sequence of events

The sequence of events for usage of multicast DNS is as follows:

1. **A host multicasts a query for ANY record for a name within the ".lcl.arpa" domain. The query is sent to the LINKLOCAL** multicast address. The response is multicast to the LINKLOCAL address, and uses DNS TTL=0, with the exception of NS, which uses a default TTL, with a value TBD.

2. **Hosts only respond to queries if they are the name server for the domain (e.g. they are foo.lcl.arpa). Hosts never** respond based on cached information. The responding host responds with SOA and NS records.

3. **Now that the querying host has discovered the name server for the domain, subsequent queries are sent unicast to the discovered** name server.

Note that this implies that multicast DNS cannot be used for discovering services (e.g. trying to query for all printers on the segument via a "*._lpr._udp" SRV [4] query). While this is not an objective of the current specification, this functionality may be added in a subsequent extension.

Since mDNS queries are sent on to a LINKLOCAL multicast address, mDNS cannot even be used to discover the location of DNS servers off the local segment. As a result, mDNS is not useful for IPv6 or IPv4 DNS server discovery.

7. Name conflicts

It is required to verify the uniqueness of the host DNS name when a host boots, when its name is changed, or when it is configured to use multicast DNS (such as when the domain search option is changed to include ".lcl.arpa").

A gratuitious name resolution query SHOULD be done to check for a name conflict. This is done by having the resolver send a multicast ANY type query for its own name. If the query is not positively resolved then host starts using its name. If the query is positively resolved, then the host should verify that the IP addresses specified in the response are its own IP addresses, possibly from another adapter. If the host verifies it, then it starts using its name. If the host cannot match the returned A records to its IP addresses, then a conflict has been detected. In order to resolve ownership conflicts, if the host has a lower IP address it will keep the name, else if the device has a higher IP address it will change names.

A host that has detected a name conflict and has loses the name election MUST NOT use the name. This means that the host MUST NOT respond to multicast queries for that name and MUST NOT respond to other multicast queries with the records that contain in RDATA name in conflict (for example, PTR record).

Note that this name conflict detection mechanism doesn't prevent name conflicts when previously separate networks are connected by a bridge. Name conflict in such situation is detected when a host receives an multicast response to a query for its name or when a client receives more than one response to a multicast query that it sent. A host that receives a response for a query for it's own name, even if it didn't send such query, behaves as if it sent this query.

In order to prevent denial of service attacks, it is recommended that "lcl.arpa" be placed last in the domain searchlist. As long as this is the case, there should be no way for a server with a FQDN to encounter name conflict problems which would cause it to become unreachable.

8. IANA Considerations

Authors will contact IANA to reserve LINKLOCAL IPv4 and IPv6 addresses.

9. Security Considerations

This draft does not prescribe a means of securing the multicast DNS mechanism. It is possible that hosts will allocate conflicting names for a period of time, or that non-conforming hosts will attempt to deny service to other hosts by allocating the same name.

These threats are most serious in wireless networks such as 802.11, since attackers on a wired network will require physical access to the home network, while wireless attackers may reside outside the home. In order to provide for privacy equivalent to a wired network, the 802.11 specification provides for RC4-based encryption. This is known as the "Wired Equivalency Privacy" (WEP) specification. Where WEP is implemented, an attacker will need to obtain the WEP key prior to gaining access to the home network.

10. Acknowledgements

The authors would like to thank Stuart Cheshire, Michael Patton, Erik Guttman, Olafur Gudmundsson, Thomas Narten, Mark Andrews, Erik Nordmark, Myrong Hattig and Bill Manning for comments on this draft, provided at the mDNS lunch in Adelaide, Australia on 3/29/00.

11. Authors' Addresses

Levon Esibov
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

EMail: levone@microsoft.com

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: +1 (425) 936-6605
EMail: bernarda@microsoft.com

Dave Thaler
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: +1 (425) 703-8835
EMail: dthaler@microsoft.com

12. References

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

[2] Meyer, D., "Administratively Scoped IP Multicast", BCP 23, RFC 2365, July 1998.

[3] Aboba, B., "The Mini-DHCP Server", Internet draft (work in progress), draft-aboba-dhc-mini-01.txt, April 2000.

[4] Gulbrandsen, A., Vixie, P., Esibov, L. "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[5] Braden, R., "Requirements for Internet Hosts -- Application and Support", RFC 1123, October 1989.

[6] Hanna, S., Patel, B., and Shah, M., "Multicast Address Dynamic Client Allocation Protocol (MADCAP)", RFC 2730, December 1999.

[7] Gulbrandsen, A., "A DNS RR for encoding DHCP information", Internet draft (work in progress), draft-ietf-dnsind-dhcp-rr-00.txt, October 1999.

[8] Mockapetris, P., "Domain Names - Implementation and Specification", RFC 1035, November 1987.

[9] IANA, "Single-source IP Multicast Address Range", http://www.isi.edu/in-notes/iana/assignments/single-source-multicast, October 1998.

[10] Handley, M., Thaler, D., and Kermode, R., "Multicast-Scope Zone Announcement Protocol (MZAP)", Work in progress, draft-ietf-mboned-mzap-06.txt, December, 1999.

[11] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., Lear, E., "Address Allocation for Private Internets", RFC 1918, February, 1996.

[12] Stapp, M., Rekhter, Y., "Interaction between DHCP and DNS", Internet draft (work in progress), draft-ietf-dhc-dhcp-dns-11.txt, October 1999.

[13] Vixie, P., et. al., "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April, 1997.

[14] Troll, R., "DHCP Option to Disable Stateless Auto-Configuration in IPv4 Clients", RFC 2563, May 1999.

[15] Andrews, M., "Negative Caching of DNS Queries (DNS NCACHE)", RFC 2308, March 1998.

[16] Auerbach, K., "PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: CONCEPTS AND METHODS", RFC 1001, March, 1987.

13. Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

14. Full Copyright Statement

15. Expiration Date

This memo is filed as <draft-aboba-dnsext-mdns-01.txt>, and expires February 1, 20001.