Internet Engineering Task Force
INTERNET-DRAFT
Expires February 2001
draft-manning-dnsext-mdns-00.txt

B. Woodcock
Zocalo
B. Manning
ISI

August 2000

Multicast Domain Name Service

Status of this Memo

Copyright Notice

Abstract

This document describes a method by which DNS resolvers may reach multicast-capable DNS servers which may exist within a multicast local scope, by issuing a single UDP query to a static multicast address.

Acknowledgments

Vital contributions to this document were made by Erik Guttman, Paul

Vixie, Dave Meyer, David Conrad, Andreas Gustafsson, Stuart Cheshire, Richard Ford, Tony McGregor, Stuart Kwan, Alex Hoppman and Peter Ford.

Overview and rationale

The addition of multicast capability into the DNS protocol will facilitate retirement of legacy protocols such as AppleTalk and NetBIOS and may enable the development of new methods of service location and ZeroConf bootstrapping.

Discussion

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. Specifically, this extension allows UDP DNS queries, as documented in RFC 1035, sections 4.1.1, 4.1.2 and 4.2.1, to be addressed to port 53 of statically-assigned relative offset -4 within the range of multicast addresses defined as "administratively scoped" by RFC 2365, section 9. Within the full /8 of administratively scoped addresses, this corresponds to the destination address 239.255.255.251. Until MZAP or a similar protocol is implemented to allow hosts to discover the extent of the local multicast scopes which enclose them, it is anticipated that implementations will simply utilize the destination address 239.255.255.251. Queries sent via multicast MUST NOT request recursion.

In order to receive multicasted queries, DNS server implementations MUST listen on the -4 offset to their local scope (as above, in the absence of a method of determining the scope, this will be assumed to be relative to the full /8 allocated for administratively-scoped multicast use, or 239.255.255.251), and respond via ordinary unicast UDP to ONLY those queries for which they have a positive answer which originated within a locally-configured zone file. That is, a server MUST NOT answer a multicasted query with cached information which it received from another server, nor may it request further resolution from other servers on behalf of a multicasted query. A multicast-capable server may, however, utilize multicast queries to perform further resolution on behalf of queries received via ordinary unicast. This is referred to as "proxy" operation. Multicast-enabled DNS servers MUST answer multicasted queries non-authoritatively. That is, when responding to a query which was received via multicast, they MUST NOT include an NS record which contains data which resolves back to their own IP address and MUST NOT set the AA bit.

Resolvers MUST anticipate receiving no replies to some multicasted queries, in the event that no multicast-enabled DNS server implementations are active within the local scope, or in the event that no positive responses exist to the transmitted query. That is, a query for the MX record for host.domain.com would go

unanswered if no local server was able to resolve that request, if no MX record exists for host.domain.com, or if no local servers were capable of receiving multicast queries. The resolver which initiated

the query MUST treat such non-response as a non-cacheable negative response. Since this multicast transmission does not provide reliable delivery, resolvers MAY repeat the transmission of a query in order to assure themselves that is has been received by any hosts capable of answering, however any resolvers which repeat a query MUST increase the interval by a factor of two between each repetition. It is more likely, however, that any repeated queries will be performed under the explicit direction of the application driving the query, rather than autonomously by the resolver implementation.

It will often be the case that multicast queries will result in responses from multiple servers. In the event that the multicast query was generated via a current API such as gethostbyname, or as the result of a proxy operation, the first response received must be passed to the requesting application or host, and all subsequently-received responses must be discarded. Future multicast-aware APIs should anticipate receiving multiple independent RR-sets in response to queries.

Security Considerations

While this extension to DNS introduces no known security problems to DNS or Multicast, it should be emphasized that distributed directories, common to other networking protocols, have not hitherto been widely used in the IP networking community. Distributed directories do require that users and system administrators assume some conscious balance between the level of trust which they accord to the responding entities on their network, and the degree of credence which they pay to the responses they receive.

References

RFC 1034: Mockapetris, P., "Domain Names - Concepts and Facilities", RFC 1034, November, 1987.

RFC 1035: Mockapetris, P., "Domain Names - Implementation and Specification", RFC 1035, November, 1987.

RFC 2052: Gulbrandsen, A., Vixie, P., "A DNS RR for specifying the location of services (DNS SRV)", RFC 2052, October, 1996.

RFC 2365: Meyer, D., "Administratively Scoped IP Multicast", RFC 2365, July, 1998.

Handley, M., Thaler, D., "Multicast-Scope Zone Announcement Protocol (MZAP)", MBoneD Internet Draft, October, 1998.

Sidhu, G.S., Andrews, R.F., and Oppenheimer, A., "Inside AppleTalk, Second Edition", Addison-Wesley, 1990.

Authors' Addresses

Bill Woodcock
Zocalo
2355 Virginia Street
Berkeley, CA 94709-1315
USA

Phone: +1 510 540 8000
EMail: woody@zocalo.net

Bill Manning
USC/ISI
4676 Admiralty Way, #1001
Marina del Rey, CA. 90292
USA

Phone: +1 310 822 1511
EMail: bmanning@isi.edu

Full Copyright Statement