Network Working Group
Internet-Draft
Expires: August 21, 2002

A. Williams
Motorola

February 20, 2002

A Private DNS Namespace for Automatic Configuration
draft-williams-dnsext-private-namespace-00.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on August 21, 2002.

Abstract

This memo defines a locally scoped private DNS namespace. Such a namespace supports self-configured authoritative nameservers in home or zeroconf environments where global names for devices are not required, yet local name resolution is beneficial.

Table of Contents

1. Introduction

An attraction of the multicast DNS proposals discussed on the dnsext mailing list recently is that they can be used by non-administrators in environments like the home. This has been achieved by a combination of a transport change and a well defined namespace. The transport change (i.e. the use of multicast) is intended to avoid the need to configure information like DNS server addresses. The namespace that has usually gone along with the proposals is intended to allow automatic population of a DNS zone. Implicit in the discussion has been the notion that devices will be configured with a name, which is then used to populate the DNS zone.

It has also been recognised that the namespace and the lookup mechanism are largely independent and should be defined seperately. The current dnsext working group multicast DNS proposal no longer specifies a private namespace, and so this document has been written to fill that gap.

As yet, there does not appear to be consensus that the approach described here is a good idea. This draft is an attempt to collect together the ideas presented on the mailing list and provide a focus for further discussion. Participants may require a flame retardant suit.

2. Rationale

The primary motivation for proposing a well defined locally scoped private address space is to support automatic self-configuration of DNS servers. Environments which stand to benefit are home networks and zeroconf networks.

In home networks, users tend to name their devices and expect their device names to be automatically visible in the namespace. This is in contrast to the usual method of populating DNS zones by listing device names and addresses in a master file. Manual construction and maintenance of DNS zone files cannot be expected because many home networks are without administrators.

Home and zeroconf networks for the most part do not have part of the global DNS namespace delegated to them. A well defined private namespace (e.g. "private.arpa.") allows devices to construct a fully qualified domain name for use locally, and corrals the automatically configured names in the global DNS namespace.

A well defined namespace allows ISPs to provide authoritative negative responses to DNS requests that leak out of private networks. DNS response times are reduced for applications inside the private

network, and top level nameserver traffic is reduced.

Private namespaces are already in use in environments like the home. Each vendor currently makes an arbitrary choice as to what domain suffix to use. Suggesting an appropriate private domain name encourages interoperability and avoids some truly bad choices (e.g. a domain suffix of "." so that each device has a FQDN of "thing1.", "thing2.", etc. This runs the risk of hiding a global TLD should a user happen to name their device "com").

3. Definitions

3.1 The "private.arpa." namespace

The DNS domain "private.arpa." using the address class "IN" is defined to be a locally scoped private address space. Local scoping implies that names registered inside this domain are available only within a physical or administrative network boundary. As a private namespace, names in "private.arpa." are not visible across the global internet in much the same way as RFC1918[1] private addresses are not globally usable addresses. The sets of names available in the "private.arpa." namespace of each site are disjoint.

The "private.arpa." namespace co-exists with and is orthogonal to the global DNS namespace. It is desirable that a network using "private.arpa." for local names still be able to look up the global DNS.

Any DNS server may be authoritative for the "private.arpa." domain. If a site contains more than one DNS server, coordination between them will be required.

The "private.arpa." zone may be populated automatically using Dynamic DNS, zone file updates, from a co-located DHCP server, via hosts using multicast DNS, or some other technique.

The "arpa" top-level DNS server is authoritative for "private.arpa.", which is an empty zone. This will result in negative responses being sent for all lookups in the zone.

DNS servers or backend resolvers run by network providers may also be authoritative for "private.arpa.". This zone is expected to be empty, and serves to limit useless queries to the root nameservers. See RFC1912 for similar examples ("localhost", "0.0.127.in-addr.arpa", etc).

Within a site, "private.arpa." may have additional structure according to the usual rules of the DNS namespace (RFC1034[2],

RFC1035[3]).

3.2 Duplicate detection and resolution

Hosts wanting to automatically update RRs in the "private.arpa." namespace must perform collision detection and resolution. If DDNS is being used, collision resolution should be performed as described in RFC2136[4] and draft-ietf-dhc-ddns-resolution-??.txt[6].

A DNS server updated by a co-located a DHCP server that does not use DDNS must also perform collision detection and resolution.

4. Other issues

4.1 Relationship to mDNS

The "private.arpa." namespace is orthogonal to the use of multicast DNS. Names in the "private.arpa." namespace may be queried via unicast or multicast DNS.

4.2 Relationship to DDNS

DNS Dynamic Updates may be used in "private.arpa." namespace. Other methods for automatically registering DNS names in the "private.arpa." namespace may also be used.

4.3 Why not use a seperate QCLASS?

Another way to support self-configuring authoritative DNS servers is to use a different DNS query class. This would have the effect of creating a new DNS namespace consisting only of automatically configured names and resource records. It is assumed that the majority of the resource records already defined for the "IN" class would be used in this new class.

The drawbacks of this approach are essentially related to backward compatibility and deployment. Existing clients would need to be modified to query names using the new QCLASS. In contrast, a home gateway (see for example "The Mini-DHCP Server"[5]) with a DNS proxy may support the "private.arpa." namespace and existing clients can query it using their existing resolver code.

4.4 Why not local.arpa or lcl.arpa?

The particular name chosen is not particularly important. Historically the "local.arpa." and "lcl.arpa." namespaces have been associated with various multicast DNS proposals. Rather than reuse the name, a distinct name was chosen to highlight that the

"private.arpa." namespace has nothing to do with how it is looked up, and has no dependencies on multicast.

Another factor is that code has already been written and deployed which uses the "local.arpa" namespace as a trigger to make multicast DNS queries. If a name is in the "local.arpa" domain, then multicast will be used. This behaviour is not desirable for the "private.arpa" namespace.

References

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

[2] Mockapetris, P., "DOMAIN NAMES - CONCEPTS AND FACILITIES", RFC 1034, November 1987.

[3] Mockapetris, P., "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION", RFC 1035, November 1987.

[4] Vixie, P., Thomson, S., Rekhter, Y. and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, November 2001.

[5] Aboba, B., "The Mini-DHCP Server", ID draft-aboba-dhc-mini-04.txt, September 2001.

[6] Stapp, M., "Resolution of DNS Name Conflicts Among DHCP Clients", ID draft-ietf-dhc-ddns-resolution-03.txt, November 2001.

Author's Address

Aidan Williams
Motorola Australian Research Centre
Locked Bag 5028
Botany, NSW 1455
Australia

Phone: +61 2 9666 0500
EMail: Aidan.Williams@motorola.com
URI: http://www.motorola.com.au/marc/

Appendix A. Acknowledgements

Many people on the dnsext mailing list have contributed to the discussions on multicast DNS and the namespace issues it brought up. The discussion was helpful and at times most enlightening.

Contributors to the discussion include: Bernard Aboba, Harald Alvestrand, Richard Barr Hibbs, Eric Brunner-Williams, Randy Bush, Stuart Cheshire, Matt Crawford, Alain Durand, Robert Elz, Levon Esibov, Patrick Falstrom, Olafur Gudmundsson, Erik Guttman, Eric A. Hall, Jun-ichiro itojun Hagino, Christian Huitema, Richard Johnson, Bill Manning, Tomohide Nagashima, Thomas Narten, Dan Nicolae, Erik Nordmark, Masataka Ohta, JINMEI Tatuya, David Terrell, Dave Thaler, Sander Van-Valkenburg, Paul A Vixie, Bill Woodcock, and Brian Zill.

The author also wishes to thank Kwan-Wu Chin for a number of stimulating conversations.

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.