dnsext
Internet-Draft
Expires: December 30, 2002

A. Williams
Motorola

July 1, 2002

A Locally Scoped DNS Namespace
draft-williams-dnsext-private-namespace-01.txt

Status of this Memo

Copyright Notice

Abstract

This memo defines a locally scoped private DNS namespace.

Table of Contents

1. Concepts

1.1 The Existence of Scoped Addresses

Privately addressed networks are in widespread use today for a variety of reasons including address space shortage and a desire to have a separate addressing domain bordered by a security gateway. Well defined portions of the IPv4 address space have been reserved to support the desire to use private addresses in [RFC1918].

In IPv6, the site-local address prefix [RFC2373] is reserved for use by those wanting to use private IPv6 addressing. Private addresses are useful for people who wish to use IPv6 but are not connected to the global internet.

IPv6 site local addresses can also be viewed as a way of providing stable addresses in the face of renumbering events. A common case occurs when 6to4 [RFC3056] is used to provide global IPv6 addresses from a DHCP or dialup address subject to relatively frequent change. Site-local addresses allow un-interrupted operation of services within a site during periods when global addresses need to be changed or are unavailable. It is expected that global addresses would be used in simultaneously with site local addresses.

Private address ranges are in wide use today in administered networks (e.g. corporates) and in un-administered networks (e.g. the home). Private addresses are not unique in the global internet, and cannot be uniquely routed to, however they are typically allocated in a fashion that ensures their uniqueness and routeability within an administrative site.

1.2 Scoped Addresses and the DNS

Generally it should be recognised that people wanting to use private addressing also wish to use the DNS to resolve names. The current recommended approach is to set up two "views" of the DNS: one for the privately addressed hosts, and another for global hosts on the internet. Various documents attempt to prohibit the placing non-globally scoped addresses into the global DNS since there are a variety of undesirable effects that come from doing so (e.g. [I-D.ietf-dnsop-dontpublish-unreachable][RFC1918]). The intention of this memo is to provide constructive guidance for people who will make use of locally scoped addresses and name spaces in spite of the admonishments against doing so.

Rather than view these problems as arising "because non-globally scoped addresses are in the DNS", this document takes the view that problems arise because private (not globally useful) and global

addresses are returned together in a single response to a DNS query, and hosts do not or cannot distinguish between them. Unfortunately, attempting to have the DNS server omit locally scoped addresses in responses "as appropriate" is understood to be infeasible. The recommended split DNS approach results in different answers to the same DNS question depending on where you are in the network.

This document proposes a locally scoped namespace to pair with locally scoped addresses: private.arpa. The private.arpa. domain suffix replaces the global domain suffix when a DNS record contains a private address, thus partitioning the private and global addresses into separate portions of the DNS namespace. Clients can prefer local services using locally scoped addresses via a DNS suffix search list.

2. Rationale

The private.arpa namespace provides a usable DNS domain name to use when a network does not have a globally allocated domain name. Typical examples are disconnected networks and also home networks which usually inherit the domain suffix of their ISP via DHCP, often in combination with a NAT. An ISP is unlikely to be able to support DNS for each home for precisely the reasons listed above. Further, most ISPs do not want to allow customers to add or remove DNS entries from their namespace, and getting a global domain name is complication a consumer can do without.

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.

A private DNS namespace allows standard DNS and dynamic updates to be used rather than a proprietary local name service such as NetBIOS naming or Appletalk NBP in the home. 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. Devices can be configured with a name (rather than configuring the name server), and the devices can use dynamic update to populate the local DNS zone automatically.

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[RFC1918] 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[RFC1034], RFC1035[RFC1035]).

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[RFC2136] and draft-ietf-dhc-ddns-resolution-??.txt[ID-name-conflict].

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 Merging of Networks

Two organisations using privately addressed networks that merge run the risk of conflict in their address space. In a similar way, two organisations using the private.arpa address space may also run the risk of conflicts during a subsequent merge of their networks. One possible approach to minimising the risk is to create a sub-domain inside the private.arpa domain that is "reasonably unique". One possibility might be to choose the company name (e.g. acme.private.arpa) as the domain suffix used, but still inside private.arpa. Two organsiations that merge using different sub-domains inside private.arpa will not experience a conflict.

4.2 Configuration Consistency in a Site

Since private.arpa (and the RFC1918 reverse maps for that matter) are not globally delegated, there is no chain of referrals that back-end resolvers may follow to locate a DNS server. A site that makes use of back-end resolvers must ensure that they are configured to refer private.arpa requests (and RFC1918 backward maps if required) to the appropriate DNS server within the site. It appears reasonable to require that all back-end resolvers be within the site.

4.3 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.

4.4 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.

4.5 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"[ID-mini-dhcp]) with a DNS proxy may support the "private.arpa." namespace and existing clients can query it using their existing resolver code.

4.6 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

[I-D.ietf-dnsop-dontpublish-unreachable]	Hazel, P., "IP Addresses that should never appear in the public DNS", draft-ietf-dnsop-dontpublish-unreachable-03 (work in progress), February 2002.
[ID-mini-dhcp]	Aboba, B., "The Mini-DHCP Server", ID draft-aboba-

	dhc-mini-04.txt, September 2001.
[ID-name-conflict]	Stapp, M., "Resolution of DNS Name Conflicts Among DHCP Clients", ID draft-ietf-dhc-ddns-resolution-03.txt, November 2001.
[RFC1034]	Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.
[RFC1035]	Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.
[RFC1918]	Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G. and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.
[RFC2136]	Rekhter, Y., Thomson, S., Bound, J. and P. Vixie, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.
[RFC2373]	Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 2373, July 1998.
[RFC3056]	Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, February 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.