

DNS Working Group
INTERNET-DRAFT
Expires December 1999

Donald E. Eastlake, 3rd
IBM
June 1999

[draft-ietf-dnsind-local-names-07.txt](#)

Local Domain Name System (DNS) Names

Donald E. Eastlake 3rd

Status of This Document

This draft, file name [draft-ietf-dnsind-local-names-07.txt](#).
Distribution of this document is unlimited. Comments should be sent to the DNS mailing list <namedroppers@internic.net> or to the author.

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. Internet-Drafts may be updated, replaced, or obsoleted by other documents at any time. It is not appropriate to use Internet-Drafts as reference material or to cite them other than as a ``working draft'' or ``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>.

To view the entire list of current Internet-Drafts, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), ftp.nordu.net (Northern Europe), ftp.nis.garr.it (Southern Europe), munnari.oz.au (Pacific Rim), ftp.ietf.org (US East Coast), or ftp.isi.edu (US West Coast).

Abstract

It is increasingly common for their to be "local" domain names which are not intended to be seen from the global Internet. In some cases this is for policy reasons, in other cases because they map to IP addresses or other data which is only locally meaningful [RFC 1918,

2373].

A new top level domain (TLD) name (.local) is reserved and a name structure suggested below this TLD such that local private DNS zones can safely be created without fear of conflict if these names should leak out of a private enclave. In addition, a method of providing DNS service for these names is suggested such that they are maintained privately, similar to the reserved private IP addresses,

yet locally appear to be part of the global DNS name tree and are reachable by a local resolver with no special knowledge. Additional second level domain names are assigned under this TLD for IPv6 link and site local addresses and loopback functions.

Acknowledgments

The valuable contributions of the following persons are gratefully acknowledged:

Dan Harrington

Michael A. Patton

Table of Contents

Status of This Document.....	1
Abstract.....	1
Acknowledgments.....	2
Table of Contents.....	3
1 . Introduction.....	4
2 . Local Names Via The .local Top Level Domain.....	5
2.1 Local DNS Server Specifics.....	7
2.2 Local in-addr.arpa Zones.....	8
2.3 Name Conflicts.....	8
2.4 Nested Enclaves.....	9
3 . Other Names in .local.....	9
4 . Security Considerations.....	9
4.1 Strength of Privacy Offered.....	9
4.2 Interaction with DNSSEC.....	10
References.....	11
Author's Address.....	11
Expiration and File Name.....	11

1. Introduction

The global Internet Domain Name System (DNS) is documented in [RFC 1034, 1035, 1591, 2606] and numerous additional Requests for Comment. It defines a tree of names starting with root, ".", immediately below which are top level domain names such as .com and .us. Below top level domain names there are normally additional levels of names.

Generally the information in the DNS is public and intended to be globally accessible. Certainly, in the past, the model of the Internet was one of end-to-end openness [[RFC 1958](#)]. However, with increasing security threats and concerns, firewalls and enclaves have appeared. In many cases, organizations have hosts or resources that they specifically want to reference with DNS names but which they also want to be walled off from global access and even from global knowledge of the DNS name for the resource.

In the realm of IP addresses, this has been accomplished by reserving three blocks of IPv4 addresses as documented in [[RFC 1918](#)] and by allocating parts of the IPv6 address space for link and site local addresses [[RFC 2373](#)]. Familiarity with the contents of these RFCs is assumed. Addresses in these blocks are not to be globally routed.

In the DNS area, local private names have generally been achieved in the past by "splitting" DNS at the enclave boundary, giving different answers to resolvers depending on whether they are inside or outside of the enclave, using different servers for inside and outside, etc. as mentioned in [[RFC 1918](#)]. Such relatively complex configuration diddling is at variance with the simple global tree structure of the initial DNS concept.

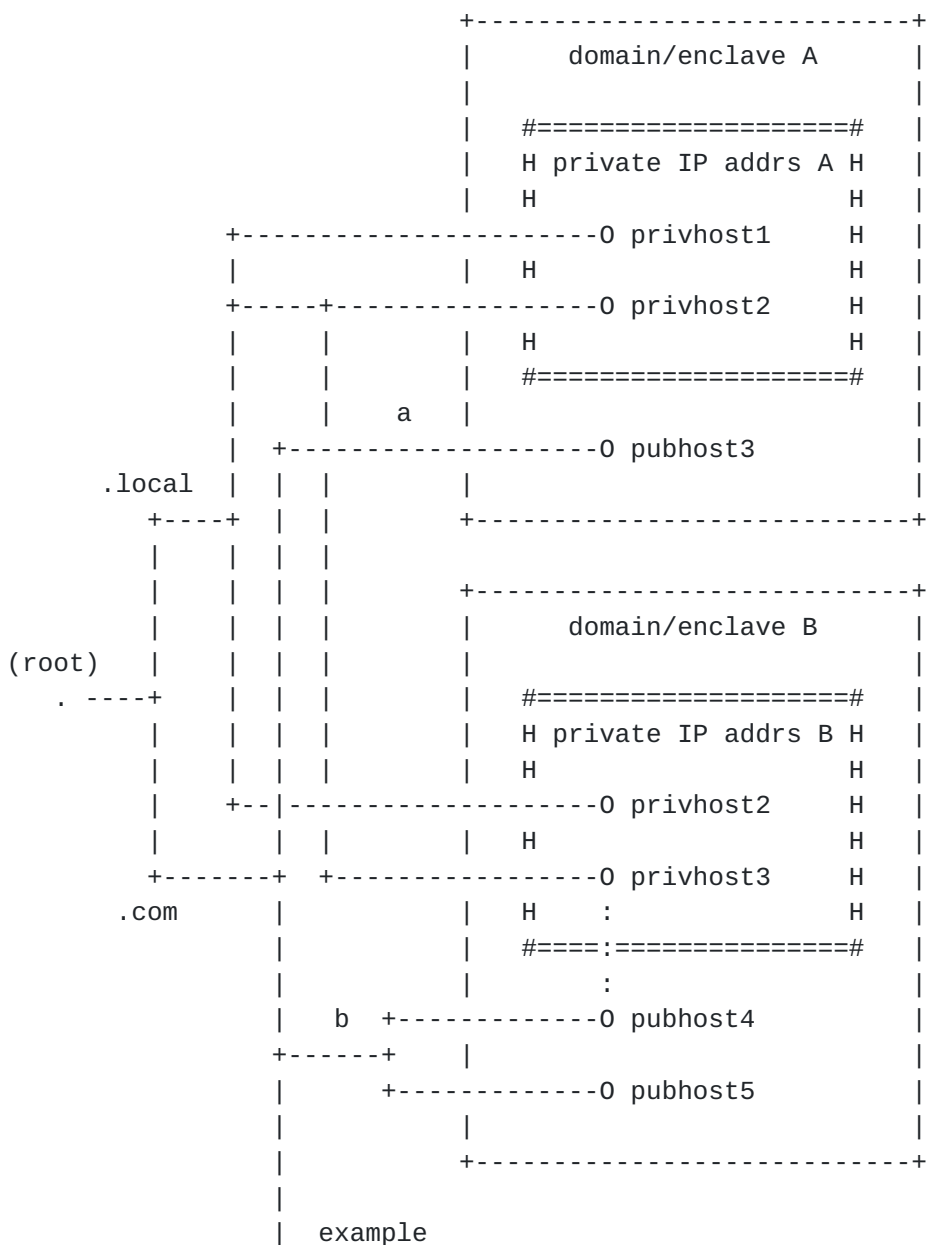
This document specifies an alternative approach to achieving the effect of local names that is more in tune with the concept of a single global DNS tree or at least the appearance of a single tree. Use of this approach is not required and older techniques will continue to work.

[RFC 1918] requires that private IP addresses not be indirectly exposed to the general Internet via DNS records or otherwise. By implication, the same would be true of IPv6 local addresses. This RFC provides the recommended way to accomplish such private IP address hiding and carves out a limited exception thereto for the addresses of the servers for some zones which are children of the .local top level domain name.

2. Local Names Via The .local Top Level Domain

The fundamental idea, as described in more detail below, is to define second level domains under .local which are served by DNS name servers that have private IP addresses. These server's addresses would only be routed within the domain to which the names are local. Thus the servers, and the names and resource records inside them, would not be directly accessible outside the enclave, if the guidelines in this document are followed.

The following figure shows a highly simplified overview of an example configuration:



+-----0 pubhost6

D. Eastlake 3rd

[Page 5]

Starting at the bottom, pubhost6 is intended to illustrate an ordinary host connected to the Internet with domain name pubhost6.example.com. Though not indicated in the above diagram, every DNS zone is in fact served by at least two hosts (and some but substantially more). The addresses of the servers for the root (.), .com, and example.com zones would all be in the public portion of the IP address space, i.e., in the space of all unicast IP addresses not reserved for private use.

Moving to the top of the figure, enclave A represents some organization that wishes to have some hosts with publicly visible names and some with hidden names that are visible only locally. pubhost3.a.com is an example of a publicly visible host which would probably have a public IP address although access to pubhost3 from outside the enclave might be filtered or even blocked by a firewall or the like. privhost1 and privhost2 are examples of hidden names. If a zone with privhost1 and privhost2 in it is served by DNS servers with private IP addresses ("private IP addresses A") such that the servers are accessible within enclave A but not from outside enclave A, then the information is that zone will only be locally visible. As show in the above figure, privhost1 and privhost2 have addresses that are also private IP addresses, making those hosts inaccessible outside enclave A, but it is the private addresses of the DNS servers, not of the hosts pointed to from within the private DNS zone, that provides the protection for the DNS names and other private DNS information. (From the above simplified diagram, it might appear that fully qualified domain names of these hosts would be privhost1.local and privhost2.local but the names are actually more complex as explained in [Section 2.1.](#))

Finally, in the middle, another enclave is shown with two hosts with visible names and public IP addresses, pubhost4.b.com and pubhost5.b.com. In addition, there are two private host names privhost2 and privhost3. The duplication of privhost2 between enclaves A and B would not be a problem as only DNS resolvers in enclave A can access the DNS servers with the zone having the enclave A version of privhost2 and only DNS resolvers in enclave B can access the DNS servers with the zone having the enclave B version of privhost2.

Publicly visible host names are required by [\[RFC 1918\]](#) to have public (i.e., globally unique) IP addresses. Private DNS names would normally have private IP addresses, and all do in the figure above, but this is not required. A public IP address could be stored under a private name. And, of course, it is possible for the same physical host to have multiple IP addresses, including a mix of public and private. The dotted line in the figure above is intended to indicate that privhost3 and pubhost4 are actually the same physical machine.

The could be accomplished equally well by storing a single public address for that host under both the public and private names or by

having the host answer to both a public IP address stored under the public name and a private IP address stored under the private name. In the later case you could even also store the public address along with the private address under the private name.

2.1 Local DNS Server Specifics

A variety of second level names are provided in the .local zone each of which is a delegation point to a zone with some number of name servers in one of the private IP address space blocks. The multiple second level names permit choice between the different private IP blocks and different numbers of servers. Thus the actual fully qualified name for the private host examples in the figure above would be more like privhost1.a2.local, privhost2.a2.local, etc. (but see [Section 2.3](#) below).

Glue records are provided to give private IP addresses for initial name servers; however, it should be noted that the NS and A records in the local zones will dominate the information stored in the .local zone. This means that once a resolver has contacted a local server, the list of NS RRs in the local zone on that server will control and could contain more or different servers than were given at the chosen .local delegation point. Nevertheless, the glue A records in the global .local zone do place some constraints of the private IP address of the local DNS servers implementing zones which are children of .local.

It is also possible for an enclave to locally configure its own version of the .local zone. Depending on its enclave boundary implementation, it might be able to constrain all of its internal references to .local to use its own variant version. This version could have whatever private addresses were desired for the name servers involved. Such a configuration MAY be used, but it is recommended that the globally accessible .local specified herein be used for uniformity. That way, even a unconstrained resolver starting from the normal root servers (i.e., an "out of the box" resolver) will correctly resolve or fail to resolve names under .local depending on the resolvers location in the network as specified herein.

It is only necessary for the local DNS servers to have private IP addresses to achieve the effect of local names. However, care MUST be taken that none of the local DNS servers or any server that might cache their output is accessible by any network interface that has a non-private IP address. Otherwise considerable confusion could result if local names are resolved by a resolver outside a local

enclave to private IP addresses which have a different meaning for that resolver.

2.2 Local in-addr.arpa Zones

Inverse lookup of local names corresponding to private IP addresses needs to be provided via the in-addr.arpa and ip6.int zones. Because of the fixed naming within this zone, different names with different numbers of servers or different addresses can not be provided. As with the forward .local entries, the actual NS RRs in the servers serving the private portions of the inverse in-addr.arpa will dominate. When one of these is queried by a resolver, it can provide information on additional servers for that particular subzone in the private IP address portion of the in-addr.arpa tree.

2.3 Name Conflicts

The intention is that local names would only be used in the enclave where the entities they refer to exist, and these names would not be exported. However, experience indicates that, despite best efforts to avoid it, some such names will leak out via email cc's, URL's in HTML, etc. (Such leakage occurs regardless of how the local names are formed or whether they are accessible via the default root zone.) These leaked private names can cause confusion if they can conflict with global names or names local to other enclaves. Use of the .local top level domain assures no conflict with global names. To assure no conflict with different local fully qualified names, the domain name of the enclave SHOULD always be prefixed to .local.

For example, a company might have

host1.company.example

as a globally accessible host and

host2.company.example.b3.local

as a host for internal use only. The global name could normally be resolvable anywhere on the Internet while the local name could not be resolved anywhere except within the company enclave.

Note that different names were chosen for the initial label in the two names above, i.e., host1 and host2. The reason for this is that, in some environments, local hosts are referred to by an unqualified names, such as host3. For DNS look up purposes, such a name must be expanded into a fully qualified domain name and a "search list" of possible suffix qualifications is tried. If, for example, both host4.school.ac.example and host4.school.ac.example.b3.local existed, then a local reference to "host4" would be ambiguous and could lead to either machine depending on the order of qualifications tried. This order could even be different in different pieces of local software or on different local hosts, resulting in substantial confusion. For this reason, it is strongly recommended that disjoint

name sets be used for global and local entity unqualified domain names and that fully qualified domain names be used wherever

practical.

[2.4](#) Nested Enclaves

It is possible to have enclaves within enclaves. In general the best way to accomplish this is to use a different portion of the private IP address space at each nesting level of enclave. (Private IP address space can be reused in enclaves that are siblings or the like.) Then similar entries to those proposed here for .local can be made in the private zone referring to name servers with addresses in the nested enclave's private IP address space.

[3.](#) Other Names in .local

Three additional second level domain names are assigned in the .local top level domain for other types of local names.

In particular,

link.local and

site.local

are reserved for use in qualifying IPv6 link local names and site local names.

In addition, loopback.local is assigned and given the loopback address.

[4.](#) Security Considerations

This section discusses the strength of the privacy offered by using subzones of .local and interactions with DNS security.

[4.1](#) Strength of Privacy Offered

Local names, as proposed herein, are not intended to be a strong security mechanism.

The privacy of the DNS information protected by storing it in servers with private IP addresses is weak. It is completely dependent on the integrity of enclave perimeter routing to make these servers inaccessible. And it may occasionally leak out in any case due to inclusion in email address fields, web pages, and the like, although such leakage should be no worse than current split DNS

implementations of DNS data hiding.

Software should not depend on local names being accessible only within a particular enclave as someone could deliberately create the same names within a different enclave. This is true even if, as recommended herein, the names incorporate the domain name of the original enclave in an attempt to avoid such conflicts.

[4.2](#) Interaction with DNSSEC

Although an enclave may derive some amount of security by virtue of its isolation, it will normally be desirable to implement DNS security [[RFC 2535](#)] within the enclave. The enclave owner should generate their own keys and sign their subzone of .local. However, a signed copy of their public key can not be included in the .local zone as it is different for every enclave. Thus, to authenticate the .local subzone contents, it will be necessary to sign the KEY RR at the apex of the local subzone of .local with the .local zone key or another key that is trusted by local resolvers or statically configure the public key for the .local subzone in local resolvers.

References

- [RFC 1033](#) - M. Lottor, "Domain Administrators Operations Guide", November 1987.
- [RFC 1034](#) - P. Mockapetris, "Domain Names - Concepts and Facilities", STD 13, November 1987.
- [RFC 1035](#) - P. Mockapetris, "Domain Names - Implementation and Specifications", STD 13, November 1987.
- [RFC 1591](#) - J. Postel, "Domain Name System Structure and Delegation", 03/03/1994.
- [RFC 1918](#) - Y. Rekhter, R. Moskowitz, D. Karrenberg, G. de Groot, E. Lear, "Address Allocation for Private Internets", 02/29/1996.
- [RFC 1958](#) - B. Carpenter, "Architectural Principles of the Internet", 06/06/1996.
- [RFC 2373](#) - R. Hinden, S. Deering, "IP Version 6 Addressing Architecture", July 1998
- [RFC 2535](#) - D. Eastlake, "Domain Name System Security Extensions", March 1999.
- [RFC 2606](#) - D. Eastlake, A. Panitz, "Reserved Top Level DNS Names", June 1999.

Author's Address

Donald E. Eastlake 3rd
IBM
65 Shindegan Hill Road, RR #1
Carmel, NY 10512 USA

Telephone: +1 914-276-2668 (h)
 +1 914-784-7913 (w)
FAX: +1 914-784-3833 (w)
EMail: dee3@us.ibm.com

Expiration and File Name

This draft expires December 1999.

Its file name is [draft-ietf-dnsind-local-names-07.txt](#).

