Local Domain Names

Donald E. Eastlake 3rd

Status of This Document

This draft, file name draft-ietf-dnsind-local-names-03.txt, is intended to be become an Informational RFC. 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. 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."

To learn the current status of any Internet-Draft, please check the 1id-abstracts.txt listing contained in the Internet-Drafts Shadow Directories on ds.internic.net (East USA), ftp.isi.edu (West USA), nic.nordu.net (North Europe), ftp.nis.garr.it (South Europe), munnari.oz.au (Pacific Rim), or ftp.is.co.za (Africa).

Abstract

A set of second level domain names are defined under a new top level domain name such that local private DNS zones can be maintained similar to the private IP addresses reserved in RFC 1918 but which locally appear to be part of the global DNS name tree. Additional second level domain names are assigned under this TLD for loopback addresses and IPv6 link and site local addresses.
Acknowledgements

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
Acknowledgements.......................................2
Table of Contents.......................................2

1. Introduction.........................................3
2. Local Names Via The .local Top Level Domain.......3
  2.1 Local DNS Servers................................4
  2.2 Local in-addr.arpa Zones..........................4
  2.3 Name Conflicts....................................4
  2.4 Nested Enclaves..................................5
3. Other Names in .local.................................5
4. Security Considerations..............................6
  4.1 Strength of Privacy Offered.......................6
  4.2 Interaction with DNSSEC...........................6
  4.3 Network Abuse....................................6

References..............................................8
Author’s Address........................................8
Expiration and File Name...............................8

Appendix A: the .local zone............................9

Appendix B: the .in-addr.arpa zone....................11
1. Introduction

The global Internet Domain Name System (DNS) is documented in RFC 1034, 1035, 1591 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 as discussed in RFC 1591. 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. 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.

In the realm of IP addresses, this has been accomplished by reserving three blocks of addresses as documented in RFC 1918.

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, creating fake local root servers, and similar relatively complex configuration diddling, which is arguably at variance with the simple global tree structure of the DNS.

This document specifies an alternative approach to achieving the effect of local names.

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 addresses would only be routed within the enclave 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.
2.1 Local DNS Servers

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 Appendix A to this document gives the recommended initial content of the .local zone.

Glue records are provided to give private IP addresses for initial 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 servers than were given at the chosen .local delegation point.

It is only necessary for the local DNS servers to have private IP addresses to achieve the effect of local names. Any address pointers associated with these local names would most likely point to private IP addresses but could point to global addresses. 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 zone. Appendix B contains recommended additions to the in-addr.arpa zone (or subzones thereof) to accomplish this. Because of the fixed naming within this zone, different names with different numbers of servers can not be provided but two servers should be sufficient. 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 such names will leak
out and can cause confusion if they can conflict with global names or names local to other enclaves. Use of the .local TLD 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.co.xy

as a globally accessible host and

    host2.company.co.xy.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 choosen for the initial label in the two names above, i.e., host1 and host2.

In many environments, local hosts are refered 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 list of possible suffix qualifications is tried. If, for example, both

    host4.school.ac.xy and host4.school.ac.xy.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.

### 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 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 enclaves 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, interactions with DNS security, and possible interaction with network abuse.

4.1 Strength of Privacy Offered

It should be noted that the privacy of the DNS information protected by storing it in servers with private IP addresses is relatively weak. It is completely dependent on the integrity of enclave perimeter routing to make these servers inaccessible. And it is quite likely to 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 even if the names include the name of the original enclave in an attempt to avoid such conflicts.

4.2 Interaction with DNSSEC

Although an enclave may derive some small amount of security by virtue of its isolation, it will normally be desirable to implement DNS security [RFC 2065] 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 statically configure the public key for the .local subzone in local resolvers or cross sign the KEY RR at the apex of the local subzone of .local with another key that is trusted by local resolvers.

4.3 Network Abuse

Use of the defined private server second level domain names under return addresses, or the like, could cause DNS, SMTP, and many other types of references to IP addresses in the RFC 1918 blocks. This can
occur from within a firewall due to web browsing or email processing of web pages or email from virtually anywhere in the Internet. However, this is not a new situation as anyone who controls any zone in the DNS, say zone.foo.tld, can create entries therein with arbitrary IP addresses (including multicast and undefined formats) and then, by using these name entries in email, web links, etc., attempt to cause a variety of spurious protocol connections to those addresses.

Local names may provide another way for network abusers to create confusion to cover their tracks and make abuse hard to trace. But ephemeral or unreachable names can be created currently via rapid zone changes or delegation to a non-existent server. Use of .local at least provides some warning that a name may be unreachable.
References


draft-ietf-dnsind-test-tlds-*.txt

Author’s Address

Donald E. Eastlake 3rd
CyberCash, Inc.
318 Acton Street
Carlisle, MA 01741 USA

Telephone: +1 978 287 4877
           +1 703 620-4200 (main office, Reston, VA)
FAX:      +1 978 371 7148
EMail:    dee@cybercash.com

Expiration and File Name

This draft expires June 1998.

Its file name is draft-ietf-dnsind-local-names-03.txt.
Appendix A: the .local zone

===== The .local zone suggested initial contents ====

```
local. IN SOA ... ... ( 1234 ; serial
                     90000 ; refresh, 25 hours
                     36000 ; retry, 10 hours
                     3456000 ; expiry, 40 days
                     43200 ) ; minimum of 12 hours
NS ... ; actual servers for .local zone
NS ...
...

loopback A 127.0.0.1
AAAA 0:0:0:0:0:0:0:1
MX 100 loopback.local.

link TXT "Reserved. See RFC xxxx." [the rfc this draft becomes]
site TXT "Reserved. See RFC xxxx." [the rfc this draft becomes]

a2.local. NS ns1.a2.local.
         NS ns2.a2.local.
ns1.a2.local. A 10.1.1.2
ns2.a2.local. A 10.1.2.2

a3.local. NS ns1.a3.local.
         NS ns2.a3.local.
         NS ns3.a3.local.
ns1.a3.local. A 10.1.1.2
ns2.a3.local. A 10.1.2.2
ns3.a3.local. A 10.2.1.2

a4.local. NS ns1.a4.local.
         NS ns2.a4.local.
         NS ns3.a4.local.
         NS ns4.a4.local.
ns1.a4.local. A 10.1.1.2
ns2.a4.local. A 10.1.2.2
ns3.a4.local. A 10.2.1.2
ns4.a4.local. A 10.128.1.2

b2.local. NS ns1.b2.local.
         NS ns2.b2.local.
ns1.b2.local. A 172.16.1.2
ns2.b2.local. A 172.16.2.2

b3.local. NS ns1.b3.local.
         NS ns2.b3.local.
```
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NS</strong></td>
<td><strong>ns3.b3.local.</strong></td>
<td></td>
</tr>
<tr>
<td>ns1.b3.local.</td>
<td>A</td>
<td>172.16.1.2</td>
</tr>
<tr>
<td>ns2.b3.local.</td>
<td>A</td>
<td>172.16.2.2</td>
</tr>
<tr>
<td>ns3.b3.local.</td>
<td>A</td>
<td>172.16.128.2</td>
</tr>
<tr>
<td><strong>c2.local.</strong></td>
<td><strong>NS</strong></td>
<td><strong>ns1.c2.local.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>NS</strong></td>
<td><strong>ns2.c2.local.</strong></td>
</tr>
<tr>
<td>ns1.c2.local.</td>
<td>A</td>
<td>192.168.1.2</td>
</tr>
<tr>
<td>ns2.c2.local.</td>
<td>A</td>
<td>192.168.2.2</td>
</tr>
<tr>
<td><strong>c3.local.</strong></td>
<td><strong>NS</strong></td>
<td><strong>ns1.c3.local.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>NS</strong></td>
<td><strong>ns2.c3.local.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>NS</strong></td>
<td><strong>ns3.c3.local.</strong></td>
</tr>
<tr>
<td>ns1.c3.local.</td>
<td>A</td>
<td>192.168.1.2</td>
</tr>
<tr>
<td>ns2.c3.local.</td>
<td>A</td>
<td>192.168.2.2</td>
</tr>
<tr>
<td>ns3.c3.local.</td>
<td>A</td>
<td>192.168.128.2</td>
</tr>
</tbody>
</table>
Appendix  B: the .in-addr.arpa zone

====  Auggested additional entries in the in-addr.arpa zone ====

10.in-addr.arpa.  NS  ns1.a2.local.
    NS  ns2.a2.local.
ns1.a2.local.     A   10.1.1.2
ns2.a2.local.     A   10.1.2.2

16.172.in-addr.arpa.  NS  ns1.b2.local.
    NS  ns2.b2.local.
ns1.b2.local.     A   172.16.1.2; one set of glue records
ns2.b2.local.     A   172.16.2.2 ; for all the b2 cases

168.192.in-addr.arpa.  NS  ns1.c2.local.
    NS  ns2.c2.local.
ns1.c2.local.     A   192.168.1.2
ns2.c2.local.     A   102.168.2.2