Mark Andrews
CSIRO

INTERNET DRAFT
Expires: October 1996
April 1996

Clarification on the use of Hostnames, Mail Boxes and Mail Domains in the DNS

draft-andrews-dns-hostnames-02.txt

1. Status of This Memo

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."

Please check the 1id-abstracts.txt listing contained in the internet-drafts Shadow Directories to learn the current status of any Internet Draft.

2. Abstract

At the protocol level, DNS domain names and records may contain arbitrary binary data. However, many domain names and records are, or refer to, hostnames, which are restricted by RFCs 952 and 1123 to contain only certain characters. Similar restrictions apply to mail domain names, RFC-821. This document identifies the types of domain names and records which are hostnames / mail domain names, and specifies the circumstances under which validation checks should be performed within the class IN.

3. Scope

This document addresses restrictions that apply to records of class IN. Similar restrictions may apply to other classes but no attempt has been made to address them here.

"hostname" is an ASCII string as specified by [RFC-952] and modified by [RFC-1123].

"mail domain name" is an ASCII string as specified by [RFC-821]. It is syntactically identical to a hostname. While a broader definition

is described in [RFC-822] only the subset described within [RFC-821] will be allowed. [RFC-1123] does not explicitly change the syntax for mail domain names, the changes to hostnames MUST flow through indicating an implicit change. For the purposes of this document hostname refers to either a hostname or a mail domain name.

"mailbox" is a ASCII string specified by [RFC-821] and mapped into the DNS using the mapping specified by [RFC-1035] Section 8. The first label represents the local part and the second and subsequent labels MUST form a hostname / mail domain name. The local part is restricted to printable ASCII (0x21 - 0x7e) plus single interior SPACE (0x21), that is a SPACE MUST be surrounded by printable ASCII. This definition is tighter than [RFC-821].

```
        legal:
                "abc def.foo.bar"
                "ab cd ef.foo.bar"
        illegal:
                " abcdef.foo.bar"
                "abcdef .foo.bar"
                "abc  def.foo.bar" (sequence of two spaces)
```

Field names are as described by [RFC-1035] unless otherwise noted.

The terms "SHOULD", "SHOULD NOT", "MUST" and "MUST NOT" are defined in [RFC-1123] and specify the latitude developers may take.

4. Owner Name: Unconditional

The owner names of the following resource records MUST be hostnames:

A	[RFC-1035]
WKS	[RFC-1035]
MD	[RFC-1035] (Obsolete)
MF	[RFC-1035] (Obsolete)
MINFO	[RFC-1035] MUST be a mailbox
MR	[RFC-1035] MUST be a mailbox
MX	[RFC-974]
AAAA	[RFC-1886]
X25	[RFC-1183]
ISDN	[RFC-1183]
RT	[RFC-1183]
AFSDB	[RFC-1183]

Records which do not conform MUST NOT be accepted or sent by nameservers, and queries containing non-conforming names MUST NOT be generated by library routines. Nameservers MUST return FORMERR to these queries.

If a query of type ANY is made, non-conforming records with the types specified above MUST be discarded by library routines before the results are returned to the application.

5. Owner Name: Conditional

The owner names of the following resource records MUST be hostnames when the following conditions are met. Library routines must return an error indication if passed a non-conforming name.

When looking up network numbers or subnet masks [RFC-1101] the lookup name MUST be verified as conforming or an error indication MUST be returned. That is, if the PTRDNAME field ends in IN-ADDR.ARPA [RFC-1033] or IP6.INT [RFC-1886].

6. Hostnames in data fields: Unconditional

The following records contain entries in their data components that MUST refer to hostnames. Nameservers MUST reject records which fail to conform and MUST NOT forward non-conforming records. FORMERR MUST be returned if non-conforming records are received.

```
SOA   MNAME field MUST be a hostname.
SOA   RNAME field.  All but the first label MUST be a hostname.
MX    EXCHANGE field MUST be a hostname.
NS    NSDNAME field MUST be a hostname.
MB    MADNAME field MUST be a hostname.
MD    MADNAME field MUST be a hostname (Obsolete).
MF    MADNAME field MUST be a hostname (Obsolete).
MG    MGMNAME field MUST be a mailbox.
MINFO RMAILBX field MUST be a mailbox.
MINFO EMAILBX field MUST be a mailbox.
AFSDB <hostname> field [RFC-1183] MUST be a hostname.
RP    <mbox-dname> field [RFC-1183] MUST be a mailbox.
      Empty <mbox-dname> field, e.g. ".", need not be checked.
RT    <intermediate-host> field [RFC-1183] MUST be a hostname.
```

If a query of type ANY is made, non-conforming records with the types specified above MUST be discarded by library routines before the results are returned to the application.

7. Hostnames in the data field: Conditional

The following resource record MAY contain hostnames in its data fields. Library routines MUST ignore the resource record and indicate an error to the calling routine.

PTR records in the IP6.INT [RFC-1886] and IN-ADDR.ARPA [RFC-1033]

domains are used for mapping addresses into host and network names. The data fields of PTR records in these two domains MUST be hostnames. Records which do not conform MUST NOT be accepted or sent by nameservers. FORMERR MUST be returned if received. In addition the data fields of PTR records referred to by CNAMES within this space MUST also conform [EIDNES]. Servers and libraries MUST ensure conformance. REFUSED MUST be returned in this case.

When looking up address records, A or AAAA, the CNAME data field MUST be checked for conformance and the query terminated if required. REFUSED MUST be returned in this case.

8. Security Considerations

This document addresses security issues raised by the use of non-conforming hostnames.

Some applications use hostnames as returned by the DNS without checking their conformance. This has caused security problems in those applications. This document addresses these problems by requiring DNS resolvers and nameservers to enforce conformance, and specifying exactly which parts of the DNS namespace are subject to these restrictions.

This document is believed to introduce no additional security problems to the current DNS protocol, except perhaps by lulling application developers into a false sense of security by having DNS servers and resolver libraries implement conformance checks that applications should implement in any case. DNS servers and resolver libraries may be out-of-date, or compromised by malicious users, and no application should depend on them actually performing conformance checks.

Requiring DNS servers and resolver libraries to perform the checks is only an attempt to protect against faulty applications which fail to perform these checks.

7. References

[RFC-821]
J. Postel, ``SIMPLE MAIL TRANSFER PROTOCOL'', USC/Information Sciences Institute, August 1982.

[RFC-822]
D. Crocker, ``STANDARD FOR THE FORMAT ARPA INTERNET TEXT MESSAGES'', University of Delaware, August 1982.

[RFC-952]
K. Harrenstien, M. Stahl, E. Feinler, ``DoD Internet Host Table Specification'', RFC-952, SRI, October 1985.

[RFC-974]
Craig Partridge, ``MAIL ROUTING AND THE DOMAIN SYSTEM'', RFC-974, CSNET CIC BBN Laboratories Inc, January 1986

[RFC-1033]
M. Lottor, ``DOMAIN ADMINISTRATORS OPERATIONS GUIDE'', RFC-1033, SRI International, November 1987

[RFC-1035]
P. Mockapetris, ``Domain Names - Implementation and Specification'', RFC-1035, USC/Information Sciences Institute, November 1987.

[RFC-1101]
P. Mockapetris, ``DNS Encoding of Network Names and Other Types'', RFC-1101, ISI, April 1989

[RFC-1123]
Internet Engineering Task Force, R. Braden, Editor, ``Requirements for Internet Hosts -- Application and Support'', RFC-1123, October 1989

[RFC-1183]
C. Everhart, L. Mamakos, R. Ullmann, P. Mockapetris, ``New DNS RR Definitions'', RFC-1183, Transarc, University of Maryland, Prime Computer, ISI, October 1990

[RFC-1886]
S. Thomson, C. Huitema, ``DNS Extensions to support IP version 6'', RFC-1886, Bellcore, INRIA, December 1995

[EIDNES]
WORK IN PROGRESS

Havard Eidnes, Geert Jan de Groot ``Classless in-addr.arpa delegation'', draft-ietf-cidrd-classless-inaddr-00.txt, SINTEF RUNIT, RIPE NCC, Jan 1996

8. Author's Address

Mark Andrews
CSIRO
Division of Mathematics and Statistics
Locked Bag 17

North Ryde NSW 2113
AUSTRALIA

Mark.Andrews@dms.csiro.au [MA88]