Network Working Group
INTERNET-DRAFT
Obsoletes: RFC 1279

Expires in six months from
Intended Category: Standards Track

S. Kille
Isode Ltd.
M. Wahl
Critical Angle Inc.

February 6, 1997

An Approach for Using Domains in LDAP Distinguished Names
<draft-ietf-asid-ldap-domains-01.txt>

Status of this Memo

1. Abstract

The Lightweight Directory Access Protocol (LDAP) uses X.500-compatible distinguished names for providing unique identification of entries. distinguished names in currently-deployed X.500 directories have the properties that they are descriptive, hierarchical, and follow common organizational models. However, there is not today a registration mechanism to permit individuals and organizations to obtain distinguished names, regardless of their physical location.

This document defines a mechanism by which a name registered with the Internet Domain Name Service [1], for which there are active registration services, can be represented as a distinguished name so that it may be used with the LDAP protocol. This is not intended to have LDAP replace the DNS protocol, but to permit further deployment of LDAP into organizations connected to the Internet.

This algorithm automatically assigns a distinguished name to any enterprise which has obtained a domain name for use in the Internet. This distinguished name may be used as a prefix for their names of entries in that enterprise.

This document does not define how to represent objects which do not have domain names. Several RFCs, such as [3] and [4], and more recent

documents provide additional guidance on representing and structuring information in these entries. Nor does this document define the procedure to locate an enterprises' LDAP directory server, given their domain name. Such as procedure may be defined in future RFCs.

2. Introduction to Domain Names and Distinguished Names

The Domain (Nameserver) System (DNS) provides a hierarchical resource labeling system.   A name is made up of an ordered set of components, each of which are short strings. An example domain name with two components would be "CRITICAL-ANGLE.COM".

The X.500 Directory provides a more general hierarchical naming framework. A primary difference in specification of distinguished names from domain names is that each component of an distinguished name has an explicit attribute type indication.

An example distinguished name represented in the LDAP string format [2] is "DC=CRITICAL-ANGLE,DC=COM". As with a domain name, the most significant component, closest to the root of the namespace, is written last.

3. Mapping Domain Names into Distinguished Names

This section defines a subset of the X.500 naming structure for use in representing names allocated in the Internet Domain Name System. It is expected that it would be possible to algorithmically transform any Internet domain name into a distinguished name, and to be able to convert such a name back into a domain name.

The algorithm for transforming a domain name is to begin with an empty DN and then attach RDNs for each component of the domain, most significant first. Each of these RDNs have a single AttributeTypeAndValue, where the type is DC and the value is an IA5 string containing the component.

```
Thus the domain name "CS.UCL.AC.UK" can be transformed into
     DC=CS,DC=UCL,DC=AC,DC=UK
and similarly "11.168.192.IN-ADDR.ARPA" to
     DC=11,DC=168,DC=192,DC=IN-ADDR,DC=ARPA
```

X.500 distinguished names in which there are one or more RDNs, all with the attribute type DC, can be mapped back into domain names. Note that this document does not define a domain name equivalence for any other distinguished names.

4. Attribute Type and Object Class Definitions

The DC (short for domainComponent) attribute type is defined as follows:

```
 ( 0.9.2342.19200300.100.1.25 NAME 'dc' EQUALITY caseIgnoreIA5Match
   SUBSTR caseIgnoreIA5SubstringsMatch SYNTAX 'IA5String' SINGLE-VALUE )
```

The value of this attribute is a string holding one component of a domain name. The encoding of IA5String for use in LDAP is simply the characters of the string itself. The equality matching rule is case insensitive, as is today's DNS.

Objects with names derived from their domain name using the algorithm of section 3 may be represented as an entry in the directory. This allows information (attributes) to be associated with that entry. The entry will have as its structural object class the "domain" object class, or a subclass of "domain".

```
 ( 0.9.2342.19200300.100.4.13 NAME 'domain' SUP top STRUCTURAL
   MUST dc
   MAY ( userPassword $ searchGuide $ seeAlso $ businessCategory $
   x121Address $ registeredAddress $ destinationIndicator $
   preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $
   telephoneNumber $ internationaliSDNNumber $ facsimileTelephoneNumber $
   street $ postOfficeBox $ postalCode $ postalAddress $
   physicalDeliveryOfficeName $ st $ l $ description $ o $
   associatedName ) )
```

The optional attributes of the domain class are used for describing the object represented by this domain, and may also be useful when searching. The semantics of these attributes are defined in X.520 [5].

The DC attribute is used for naming entries of the domain class. This is reflected by the following name form rule.

```
 ( 1.3.6.1.4.1.1466.345 NAME 'domainNameForm' OC domain MUST ( dc ) )
```

If it is desired to be able to store or retrieve DNS record attributes of the domain via LDAP, the dNSDomain object class can be used as well. This object class should only be present in the entry if the DNS records are listed as attributes.

```
 ( 0.9.2342.19200300.100.4.15 NAME 'dNSDomain' SUP domain STRUCTURAL
   MAY dNSRecord )
```

The dNSRecord attribute may take one or more values.

```
 ( 0.9.2342.19200300.100.1.26 NAME 'dNSRecord'
   EQUALITY caseExactIA5Match SYNTAX 'IA5String' )
```

5. Relationship between LDAP and DNS Directories

Implementations should be aware of the differences in deployment between LDAP and DNS directories.

To effectively search the entries in an LDAP service, it is necessary to know the base object of the entries held by that service. Generally that base object will be in one of the naming contexts in the LDAP service.

While most objects with domain names are listed in an DNS-capable directory system, it is currently expected that only a small subset of the objects with domain names will be listed in LDAP-capable directories.

Furthermore, there may not necessarily be exactly one LDAP-capable directory listing service for many top-level domains (such as ".COM" or ".US"). There many be multiple distinct entries with the same name held by different, disconnected directory services. There may be some objects accessible in a directory service, for which the superior objects are not held by any directory server.

LDAP client implementations should not assume that subtree searches may be based at the root of the DIT, or at immediately subordinate entries. Nor should LDAP client implementations assume that a name transformed from a contacted server's domain name will be a context prefix held by that server. If the client and server both implement LDAP version 3, the client may interrogate the server for the naming contexts it holds.

6. References

[1] P. Mockapetris. Domain names - concepts and facilities. RFC 1034, November 1987.

[2] S. Kille, M.Wahl. Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names. INTERNET DRAFT draft-ietf-asid-ldapv3-dn-00.txt. July 1996.

[3] P. Barker, S. Kille, T. Lenggenhager, "Naming and Structuring Guidelines for X.500 Directory Pilots". RFC 1617 May 1994.

[4] B. Jennings, "Building an X.500 Directory Service in the US", RFC 1943, May 1996.

7. Security Considerations

This memo describes how attributes of objects may be discovered and retrieved. Servers should ensure that an appropriate security policy is maintained.

8. Author's Address

Steve Kille
Isode Ltd.
The Dome
The Square
Richmond, Surrey
TW9 1DT
England
Phone: +44-181-332-9091
EMail: S.Kille@ISODE.COM

Mark Wahl
Critical Angle Inc.
4815 W. Braker Lane #502-385
Austin, TX 78759
USA
EMail: M.Wahl@critical-angle.com