                 A String Representation of LDAP Search Filters
                      <draft-ietf-asid-string-filter-v2-00.txt>

1. **Status of this Memo**

This document is an Internet-Draft. Internet-Drafts are working docu-
ments 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
and may be updated, replaced, or obsoleted by other documents at any
time. It is inappropriate to use Internet- Drafts as reference material
or to cite them other than as ``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 (US East Coast), nic.nordu.net (Europe),
ftp.isi.edu (US West Coast), or munnari.oz.au (Pacific Rim).

2. **Abstract**

The Lightweight Directory Access Protocol (LDAP) [1] defines a network
representation of a search filter transmitted to an LDAP server. Some
applications may find it useful to have a common way of representing
these search filters in a human-readable form. This document defines a
human-readable string format for representing LDAP search filters.

This document replaces RFC 1960, extending the string LDAP filter defin-
ition to include support for LDAP version 3 extended match filters.

3. **LDAP Search Filter Definition**

An LDAPv3 search filter is defined in [1] as follows:

    Filter ::= CHOICE {
            and   [0] SET OF Filter,
            or   [1] SET OF Filter,
            not   [2] Filter,
            equalityMatch   [3] AttributeValueAssertion,
            substrings   [4] SubstringFilter,
            greaterOrEqual   [5] AttributeValueAssertion,

```
        lessOrEqual          [6] AttributeValueAssertion,
        present              [7] AttributeType,
        approxMatch          [8] AttributeValueAssertion,
        extensibleMatch      [9] MatchingRuleAssertion
}

SubstringFilter ::= SEQUENCE {
        type    AttributeType,
        SEQUENCE OF CHOICE {
                initial        [0] LDAPString,
                any            [1] LDAPString,
                final          [2] LDAPString
        }
}

AttributeValueAssertion ::= SEQUENCE {
        attributeType   AttributeType,
        attributeValue  AttributeValue
}

MatchingRuleAssertion ::= SEQUENCE {
        matchingRule    [1] MatchingRuleID OPTIONAL,
        type            [2] AttributeType OPTIONAL,
        matchValue      [3] AssertionValue,
        dnAttributes    [4] BOOLEAN DEFAULT FALSE
}

AttributeType ::= LDAPString

AttributeValue ::= OCTET STRING

MatchingRuleID ::= LDAPString

LDAPString ::= OCTET STRING
```

where the LDAPString above is limited to the IA5 character set.   The
AttributeType is a string representation of the attribute type name and
is defined in [1].   The AttributeValue OCTET STRING has the form defined
in [2].   The Filter is encoded for transmission over a network using the
Basic Encoding Rules defined in [3], with simplifications described in
[1].

4. String Search Filter Definition

The string representation of an LDAP search filter is defined by the
following grammar. It uses a prefix format.

```
    <filter> ::= '(' <filtercomp> ')'
```

```
     <filtercomp> ::= <and> | <or> | <not> | <item>
     <and> ::= '&' <filterlist>
     <or> ::= '|' <filterlist>
     <not> ::= '!' <filter>
     <filterlist> ::= <filter> | <filter> <filterlist>
     <item> ::= <simple> | <present> | <substring> | <extensible>
     <simple> ::= <attr> <filtertype> <value>
     <filtertype> ::= <equal> | <approx> | <greater> | <less>
     <equal> ::= '='
     <approx> ::= '~='
     <greater> ::= '>='
     <less> ::= '<='
     <extensible> ::= ( NULL | <attr> ) [ ':dn' ] [ ':' <matchingrule> ]
                             ':=' <value>
     <matchingrule> ::= <matchingrulename> | <oid>
     <present> ::= <attr> '=*'
     <substring> ::= <attr> '=' <initial> <any> <final>
     <initial> ::= NULL | <value>
     <any> ::= '*' <starval>
     <starval> ::= NULL | <value> '*' <starval>
     <final> ::= NULL | <value>
```

<attr> is a string representing an AttributeType, and has the format
defined in [1]. <value> is a string representing an AttributeValue, or
part of one, and has the form defined in [2]. If a <value> must contain
one of the characters '*' or '(' or ')' or '\', these characters should
be escaped by preceding them with the backslash '\' character.   Note
that although both the <substring> and <present> productions can produce
the 'attr=*' construct, this construct is used only to denote a presence
filter.

<oid> is a dotted string representation of an object identifier (e.g.,
"1.2.3.4") identifying a matching rule to use when comparing <value>.
<matchingrulename> is a name given to a matching rule, as defined in
[2]. One of <attr> or <matchingrule> is required in the <extensible>
production.

[5]. Examples

This section gives a few examples of search filters written using this
notation.

```
     (cn=Babs Jensen)
     (!(cn=Tim Howes))
     (&(objectClass=Person)(|(sn=Jensen)(cn=Babs J*)))
     (o=univ*of*mich*)
     (o=Parentheses r all your parenthetical needs))
```

The following two examples illustrate the use of extensible matching.

```
(cn:1.2.3.4.5:=Fred Flintstone)
(sn:dn:2.4.6.8.10:=Barney Rubble)
(o:dn:=Ace Industry)
```

The second example illustrates the use of the ":dn" notation to indicate
that matching rule "2.4.6.8.10" should be used when making comparisons,
and that the attributes of an entry's distinguished name should be con-
sidered part of the entry when evaluating the match.

The third example denotes an equality match, except that DN components
should be considered part of the entry when doing the match.

6. Security Considerations

Security considerations are not discussed in this document.

7. Bibliography

[1] Lightweight Directory Access Protocol (v3), M. Wahl, T. Howes, S.
     Kille,   Internet   Draft   draft-ietf-asid-ldapv3-protocol-03.txt,
     October 1996.

[2] Lightweight Directory Access Protocol: Standard and Pilot Attribute
     Definitions, M. Wahl, A. Coulbeck, T. Howes, S. Kille, Internet
     Draft draft-ietf-asid-ldapv3-attributes-03.txt, October 1996.

[3] Specification of Basic Encoding Rules for Abstract Syntax Notation
     One (ASN.1). CCITT Recommendation X.209, 1988.

8. Author's Address

Tim Howes
Netscape Communications Corp.
501 E. Middlefield Road
Mountain View, CA 94043
USA
+1 415 937-3419
howes@netscape.com