INTERNET-DRAFT
Informational Draft
Expires February 1999

T. Miller
B. Narayana
P. Quinto
Novell, Inc.
August 1998

Lightweight Directory Access Protocol (v3): Schema for Domain Name System (DNS) <draft-miller-dns-ldap-schema-00.txt>

Status of this Memo

This distribution of this memo is unlimited. It is filed as <draft-miller-dns-ldap-schema-00-txt>, and expires February 1999.

Abstract

This document defines a schema for the Domain Name System (DNS). This schema makes it possible to integrate DNS servers with an LDAP-based directory service, allowing an organization to maintain a single store of DNS information. Integration of DNS into LDAP directories is desirable since it reduces administrative overhead and eliminates the need to maintain multiple server centric configuration databases for DNS and other services.

It is anticipated that this schema will be useful for providing a standardized format for the representation of attributes needed by DNS implementations within LDAP-based directory services.

1. Introduction

DNS [RFC1035] is the naming system of the internet. It provides for name to address mapping, as well as address to name mapping for devices on the internet.

Organizations need to manage names and addresses for widely dispersed (often, global) networks. While many DNS servers may be needed within an organization's network, it is highly desirable to be able to manage them from a single point, along with other network services such as DHCP. Integrating DNS into an LDAP directory allows for a single point of administration for a distributed set of DNS servers, along with other network services. See [DHCPSCHEMA] for an example of another network service which may be administered through LDAP.

In order to support DNS, new object classes are defined for Locator, Zone, Resource Record Sets, and DNS Server. These object classes are described in the next section, _DNS Object Descriptions_ with the detailed class attribute definitions following each description. [RFC2252] describes the syntaxes used in these definitions.

2. DNS Object Descriptions

OIDs have been assigned for these schema extensions (as well as DHCP extensions described in [DHCPCHEMA]) as follows (note that these are Novell assigned numbers for documentation purposes which are likely to be replaced by IANA numbers as this document advances):

```
 joint-iso-ccitt(2).country(16).us(840)
.organization(1).novell(113719).applications(1).DNIP(25)
.DNIPAttributeType(4)

 joint-iso-ccitt(2).country(16).us(840)
.organization(1).novell(113719).applications(1).DNIP(25)
.DNIPAttributeSyntax(5)

 joint-iso-ccitt(2).country(16).us(840)
.organization(1).novell(113719).applications(1).DNIP(25)
.DNIPObjectClass(6)
```

2.1 DNS/DHCP Locator

The DNS/DHCP Locator object is an object used to store relevant information for IP configuration common to both DNS and DHCP. [DHCPSCHEMA] describes a LDAP schema for DHCP.

These two services interact in some cases, such as for Dynamic

DNS updates. Also, the administration of the two services is often linked.

The Locator object has two purposes. First, it contains DNs (Distinguished Names) of other objects of interest for DNS and DHCP. For DNS these include Zones and DNS servers. By having DNs of all these objects, an application, such as a GUI, is able to present a list of all these objects without needing to search the entire tree for the objects. Instead, the application just needs to find the locator, and then read the DNs of the other objects. This can offer a significant performance advantage.

The second usage of the locator object is to store configuration information that is to apply generally to services using this LDAP namespace. Currently, this application of the Locator is only utilized by [DHCPSCHEMA].

Object Class Definition:

```
(2.16.840.1.113719.1.25.6.1.1
     NAME `DNS/DHCP Locator'
     SUP top
     PARENT (country $ organization $ organizationalUnit $
locality)
     NAMING ATTRIBUTE (cn)
     STRUCTURAL
     MUST (cn
     )
     MAY (DNIPSubnetAttr $ DNIPDNSServers $ DNIPDHCPServers $
     DNIPDNSZones $ DNIPSubnetPoolList $ DNIPConfigOptions $
     DNIPCfgPreferences $ DNIPExcludedMac $ DNIPGroupReference
     )
)
```

Attribute Definitions:

```
(2.16.840.1.113719.1.25.4.1.1
     NAME `DNIPSubnetAttr'
     DESC(`The distinguished names of Subnets.
          ')
     SYNTAX `DN'
     MULTI-VALUED
)

(2.16.840.1.113719.1.25.4.1.2
     NAME `DNIPDNSServers'
     DESC(`The distinguished names of DNS servers.
          ')
     SYNTAX `DN'
     MULTI-VALUED
)

(2.16.840.1.113719.1.25.4.1.3
     NAME `DNIPDHCPServers'
     DESC(`The distinguished names of DHCP servers.
          ')
     SYNTAX `DN'
     MULTI-VALUED
)

(2.16.840.1.113719.1.25.4.1.4
     NAME `DNIPDNSZones'
     DESC(`The distinguished names of DNS Zones.
          ')
     SYNTAX `DN'
     MULTI-VALUED
)

(2.16.840.1.113719.1.25.4.1.5
     NAME `DNIPSubnetPoolList'
     DESC(`The distinguished names of Subnet Pools.
          ')
     SYNTAX `DN'
     MULTI-VALUED
)

(2.16.840.1.113719.1.25.4.1.6
     NAME `DNIPConfigOptions'
     DESC(`DHCP options are included in this string.  The
first four octets are reserved.  The rest of the string
contains encoded DHCP options.
          ')
     SYNTAX `OCTETSTRING'
     SINGLE-VALUE
)

(2.16.840.1.113719.1.25.4.1.8
     NAME `DNIPCfgPReferences'
     DESC(`Configuration preferences for the administrative
utility.
          ')
     SYNTAX `OCTETSTRING'
     MULTI-VALUED
)

(2.16.840.1.113719.1.25.4.1.9
     NAME `DNIPExcludedMac'
     DESC(`A list of MAC addresses which the administrator
wishes to exclude from receiving addresses by DHCP. Each
address is described as in [RFC2131] with the first octet as
hlen, second octet a htype, and the remaining octets are the
```

actual hardware address. A wildcard format is also supported. If the length is greater than 17 octets this indicates a wildcard. A wildcard MAC address has an _*_ to indicate the portion of the address that is a wildcard. For example, _00:02:*_ would indicate that all addresses starting with 00:02 should be excluded.

```
            ')
     SYNTAX `OCTETSTRING'
     MULTI-VALUED
)

(2.16.840.1.113719.1.25.4.1.11
     NAME `DNIPGroupReference'
     DESC(`The distinguished name of the group object through
which servers gain their rights to the tree.
          ')
     SYNTAX `DN'
     SINGLE-VALUED
)
```

2.2 Zone

The Zone represents a DNS Zone. It is a container for all the resource records within a zone. A zone can be primary or secondary. This concept is slightly different from traditional DNS in that the zone itself is primary or secondary within the LDAP namespace, rather than on a server by server basis. If the zone is primary, this LDAP namespace is the DNS master; secondary servers can zone transfer copies of the data, but the LDAP namespace is where changes are made and distributed from. If the zone is secondary, it was transferred in from a DNS master external to the LDAP namespace. Once, inside the LDAP namespace, data is replicated using the same mechanisms as are used for other directory data.

In addition to being a container, the Zone object has attributes related to the management of the zone. These include the Zone's SOA information, an indicator of whether the zone is primary or secondary within the tree, DNs of all the DNS server objects representing DNS servers who will be authoritative for this zone, as well as the DN of the designated server. The designated server is a single server identified to carry out certain management functions for the zone that only need to be carried out by a single server.

Object Class Definition:

```
(2.16.840.1.113719.1.25.6.1.7
     NAME `DNS Zone'
     SUP top
     PARENT (country $ organization $ organizationalUnit $
locality)
     NAMING ATTRIBUTE (cn)
     STRUCTURAL
     MUST (cn $ DNIPZoneDomainName $ DNIPSecondaryZone  $
     DNIPSOASerial $ DNIPSOARefresh $ DNIPSOARetry $
     DNIPSOAExpire $ DNIPSOAMinimum $
```

```
       DNIPSOAAdminMailbox $ DNIPSOAZoneMaster
     )
     MAY ( DNIPZoneOptions $ DNIPZoneServers $
     DNIPDesignatedServer $ DNIPZoneType     $
     DNIPMasterServerIPAddr $ DNIPZoneOutFilter $ DNIPRRCount
     )
)
```

Attribute Definitions:

```
(2.16.840.1.113719.1.25.4.1.60
     NAME `DNIPZoneDomainName'
     DESC(`The fully qualified domain name of the DNS zone. ')
     SYNTAX `IA5STRING'
     SINGLE-VALUE
)

(2.16.840.1.113719.1.25.4.1.65
     NAME `DNIPSecondaryZone'
     DESC('Flag to indicate DNS zone is primary or secondary
within the tree. True indicates a secondary zone. False
indicates a primary zone.')
     SYNTAX `BOOLEAN'
     SINGLE-VALUE
)

(2.16.840.1.113719.1.25.4.1.56
     NAME `DNIPSOASerial'
     DESC('32 bit serial number of the DNS zone.  Incremented
whenever zone data is modified. This is transferred in from
the master when the zone is secondary within the tree. For a
zone that is primary within the tree this attribute is
incremented by the designated server.')
     SYNTAX `INTEGER'
     SINGLE-VALUE
)

(2.16.840.1.113719.1.25.4.1.54
     NAME `DNIPSOARefresh'
     DESC('The time interval, in seconds,  before the DNS zone
should be refreshed. ')
     SYNTAX `INTEGER'
     SINGLE-VALUE
)

(2.16.840.1.113719.1.25.4.1.55
     NAME `DNIPSOARetry'
     DESC('The time interval, in seconds, before a failed DNS
zone refresh should be retried. ')
     SYNTAX `INTEGER'
     SINGLE-VALUE
)

(2.16.840.1.113719.1.25.4.1.52
      NAME `DNIPSOAExpire'
      DESC('For a secondary zone, the upper limit of the time
interval that can elapse, in seconds, before the servers
become non authoritative when the master server cannot be
contacted. ')
     SYNTAX `INTEGER'
     SINGLE-VALUE
)

(2.16.840.1.113719.1.25.4.1.53
     NAME `DNIPSOAMinimum'
     DESC('The minimum TTL (time to live) field, in seconds,
that should be exported with any RR from this zone.')
     SYNTAX `INTEGER'
     SINGLE-VALUE
)

(2.16.840.1.113719.1.25.4.1.58
     NAME `DNIPSOAAdminMailbox'
     DESC('DNS domain name which specifies the mailbox of the
administrator responsible for this zone. ')
     SYNTAX `IA5STRING'
     SINGLE-VALUE
)

(2.16.840.1.113719.1.25.4.1.57
     NAME `DNIPSOAZoneMaster'
     DESC('DNS domain name of the master server for this zone.
If this is a primary zone, this is the domain name of the
designated primary server of this zone.  If this is a
secondary zone this is the domain name of the server outside
of the LDAP name space that is the master of this zone. ')
     SYNTAX `IA5STRING'
     SINGLE-VALUE
)

(2.16.840.1.113719.1.25.4.1.62
     NAME `DNIPZoneServers'
     DESC(`The Distinguished Names of all DNS server serving
this Zone from the directory.')
     SYNTAX `DN'
     MULTI-VALUED
)

(2.16.840.1.113719.1.25.4.1.61
     NAME `DNIPDesignatedServer'
     DESC(`The Distinguished Name of the server designated to
perform management functions for the DNS zone. These include
```

doing a zone transfer from the master for a secondary zone or

```
  updating the serial number when there are changes in the case
of a primary zone.')
     SYNTAX `DN'
     MULTI-VALUED
)

(2.16.840.1.113719.1.25.4.1.66
     NAME `DNIPZoneType'
     DESC(`The type of zone. Values are:
               0 = Forward Zone
               4 = Ipv4 Reverse Zone (IN-ADDR.ARPA)
               6 = Ipv6 Reverse Zone (IP6.INT)
               `)
     SYNTAX `INTEGER'
     SINGLE-VALUED
)

(2.16.840.1.113719.1.25.4.1.63
     NAME `DNIPMasterServerIPAddr'
     DESC(`If this is a secondary zone, this is the IP address
of the foreign master which the designated server will request
transfers.  This attribute is not used for a primary zone.')
     SYNTAX `OCTET_STRING'
     SINGLE-VALUED
)

(2.16.840.1.113719.1.25.4.1.64
     NAME `DNIPZoneOutFilter'
     DESC(`A list of IP addresses authorized to do zone out
transfers from this zone.  A part of a network can be
specified by applying a network mask to the IP address.  The
IP addresses are represented as dotted-octet numeric text
strings')
     SYNTAX `IA5STRING'
     MULTI-VALUED
)

(2.16.840.1.113719.1.25.4.1.67
     NAME `DNIPRRCount'
     DESC(`A count of the number of resource record sets in
the zone')
     SYNTAX `INTEGER'
     SINGLE-VALUED
)
```

2.3 Resource Record Set

The Resource Record Set represents all of the resource records for a given host name within a zone. It is contained by the zone object. It must contain an attribute identifying the domain name it represents.

Class Definition:

```
(2.16.840.1.113719.1.25.6.1.8
     NAME `DNS RR Set'
     SUP top
     PARENT (DNS Zone)
     NAMING ATTRIBUTE (cn)
     STRUCTURAL
     MUST (cn $ DNIPDNSDomainName
     )
     MAY (DNIPAliasedObjectName $ DNIPRRStatus    $ DNIPRR $
     DNIPMacAddress
     )
)
```

Attribute Definitions:

```
(2.16.840.1.113719.1.25.4.1.68
     NAME `DNIPDNSDomainName'
     DESC(`The domain name of the RR Set.')
     SYNTAX `IA5STRING'
     SINGLE-VALUE
)

(2.16.840.1.113719.1.25.4.1.69
     NAME `DNIPAliasedObjectName'
     DESC(`The DN of another object in the tree which the
adminstrator wishes to reference from the RRSet.')
     SYNTAX `DN'
     SINGLE-VALUE
)

(2.16.840.1.113719.1.25.4.1.72
     NAME `DNIPRRStatus'
     DESC(`This attribute is used to indicate whether or not
the RRSet is in use.  Having this attribute allows an RRSet to
be marked as unused, rather than deleted.  It can then later
be used again by changing the attribute. The values for this
field are:
          0 = RRSet in use
          1 = RRSet is unused. Other attributes, with the
     exception of the domain name, have no meaning)
     SYNTAX `INTEGER'
     SINGLE-VALUE
)
```

```
(2.16.840.1.113719.1.25.4.1.71
     NAME `DNIPRR'
```

```
      DESC(`A resource record for this RR Set.  The format of
this octet string is:
     RR Type--2 Octets
     RR Class_2 Octets
     TTL_4 Octets
     Data Length_2 Octets
     Data--variable
     .')
     SYNTAX `OCTET_STRING'
     MULTI-VALUE
)

(2.16.840.1.113719.1.25.4.1.51
     NAME `DNIPMACAddress'
          DESC(`This attribute is used for Dynamic DNS (DDNS).
With DDNS, the DNS server saves the MAC address of devices
that are assigned an IP address.  This allows the DNS server
to determine whether a device is being assigned a new IP
address or whether a second device with the same host name as
another device is being assigned an IP address.
     .')
     SYNTAX `OCTET_STRING'
     SINGLE-VALUE
)
```

2.4 DNS Server

The DNS Server object has attributes for server oriented configuration. This includes distinguished names of Zones ranges assigned to the server to act as a name server for.

Object Class Definition:

```
(2.16.840.1.113719.1.25.6.1.9
     NAME `DNS Server'
     SUP top
     PARENT (country $ organization $ organizationalUnit $
locality)
     NAMING ATTRIBUTE (cn)
     STRUCTURAL
     MUST (cn
     )
     MAY ( DNIPFwdList $ DNIPNoFwdList $  DNIPZoneList $
     DNIPServerDNSNames $ DNIPServerIPAddress $ DNIPAuditLevel
     )
)
```

Attribute Definitions:

```
(2.16.840.1.113719.1.25.4.1.75
     NAME `DNIPFwdList'
```

```
       DESC(`List of IP Addresses of DNS server to forward
queries to.
          ')
     SYNTAX `OCTET_STRING'
     SINGLE-VALUED
)

(2.16.840.1.113719.1.25.4.1.76
     NAME `DNIPNoFwdList'
     DESC(`List of DNS Domain names whose queries will not be
forwarded.
          ')
     SYNTAX `IA5STRING'
     MULTI-VALUED
)

(2.16.840.1.113719.1.25.4.1.73
     NAME `DNIPZoneList'
     DESC(`The DNs of all zones served by this DNS server.
          ')
     SYNTAX `DN'
     MULTI-VALUED
)

(2.16.840.1.113719.1.25.4.1.78
     NAME `DNIPServerDNSNames'
     DESC(`The DNS names assigned of the DNS server.
          ')
     SYNTAX `IA5STRING'
     MULTI-VALUED
)

(2.16.840.1.113719.1.25.4.1.29
     NAME `DNIPServerIPAddress'
     DESC(`List of IP addresses the DNS server is bound to.
          ')
     SYNTAX `OCTET_STRING'
     MULTI-VALUED
)

(2.16.840.1.113719.1.25.4.1.27
     NAME `DNIPAuditLevel'
     DESC(`Level of auditing that the DNS server is to
perform:
          1 = No auditing
          2 = Log major events
          3 = Log leases and major events
```

```
            4 = Log all events
          ')
SYNTAX `INTEGER'
```

3. Acknowledgements

Thanks to Ed Reed of Novell for his review.

4. References

[DHCPSCHEMA]
T. Miller, A. Patel, P. Rao _Lightweight Directory Access Protocol (v3): Schema for Dynamic Host Configuration Protocol_, INTERNET-DRAFT <id-miller-dhcp-ldap-schema.txt>, June 1998

[RFC1035]
P. Mockapetris, "Domain Names: Implementation and Specification_, RFC 1035, November 1987.

[RFC2252]
M. Wahl, A. Coulbeck, T. Howles, S. Kille, "Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions, RFC 2252, December 1997.

5. Authors' Addresses

Tom Miller
Novell, Inc.
2180 Fortune Dr.
San Jose, CA 95131

Phone: 408-577-8781
Fax: 408-577-5560
e-mail: Tom_Miller@novell.com

Badari Narayana
Novell, Inc.
2180 Fortune Dr.
San Jose, CA 95131

Phone 408-577-8906
Fax: 408-577-5560
Email: Badari_Narayana@novell.com

Peter Quinto
Novell, Inc.
2180 Fortune Dr.
San Jose, CA 95131

Phone 408-577-8344
Fax: 408-577-5560
Email: Peter_Quinto@novell.com