Abstract

Directory services based on the Lightweight Directory Access Protocol (LDAP) [1] and X.500 [2] provide a general-purpose means to store information about users and other network entities. One such use is to store information on groups. There are LDAP standards established for this purpose, e.g. the groupOfUniqueNames [3]. However, currently there are no standards for a very important use of Groups, as SMTP Mailing Lists or Aliases.

This document discusses how we at Netscape have made this extension, with the intent of providing useful information towards perhaps creating standards for this important use of LDAP.

1. Background and Motivation

LDAP-based directory services are currently being used in many organizations as a repository of information about users and other "network entities" (such as groups of users, network resources, etc.). Some information is stored in the directory for the consumption of persons browsing for information (e.g., telephone numbers, postal addresses, secretary's name), while other information (e.g., login name, password, disk quota) is stored for use by one or more network applications or services. It is the latter kind of information that is of interest in this discussion. In general, it is advantageous for different network applications and services to refer to the directory for user account information, rather than each service keeping its own collection of user account records, which requires the network administrator to separately create or destroy user entities, passwords, etc., in many different systems each time a
user joins or leaves the organization. The goals of centralized user management and sharing of information with other service types drove our decision in the design of Netscape Messaging Server (an SMTP mail server product) to use LDAP-based directory services as a common repository for mail delivery information.

One of the "network entities" that LDAP currently stores are groups of users. In X.500 this was done in the groupOfNames objectClass - at Netscape we have updated that to the groupOfUniqueNames objectClass.

One thing that is not provided by this group is the capability of sending mail thru that group to the members. In light of making LDAP a central repository for information for all network servers, it seems appropriate to add this capability. There are also obvious advantages of handling mail to groups within LDAP, making use of the storage of all other mail recipients there.

2. General Considerations of the mailGroup

Since SMTP is the internet standard for email, that is the only type of email we considered for our purposes. Proprietary email companies may have other needs.

As the groupOfUniqueNames objectClass was already published at the time we embarked on email enabling groups, and because not all groupOfUniqueNames require email enabling, it was decided to create a new objectClass -- a mailGroup. Since it would be common to wish to send mail to a groupOfUniqueNames, a mailGroup class can be 'mixed-in' with groupOfUniqueNames (that is, for an LDAP entry to contain both objects). This way, a groupOfUniqueNames can be "mail-enabled", but a mailGroup can also stand on its own.

Looking at existing list managers such as ListProc or Majordomo, there are a number of pieces of extra information for a mailGroup other than just the members and the group mailing address. These tend to fall into two groups: mail handling features (e.g. restrictions on mail to the group, directing where to process a group,...), and group management features (e.g. who has what rights to alter group attributes, visibility of group to management tools such as a mail list manager,...).

Since the management features do not require handling within the Mail Server, they can be handled separately and so we do not include them in the mailGroup attributes. Some of these features can be handled by LDAP access control, and the rest we decided could be handled by a separate (mix-in) objectClass. These features will not be covered in this document. We hope to document these in a separate document at a later time.

3. Details of the mailGroup attributes

The group mail handling features needed fall into 3 subclasses: Mail processing attributes that define how to deliver to the group, Membership attributes that define who belongs to the group, and Mail restriction attributes that define who can send what to the group. The following sections provide the details on these attributes.

3.1 URL type for attributes containing addresses
There are several mailGroup attributes that could reasonably contain mail addresses, or DN's of LDAP entities. Because of the dual nature of mailGroups (being both an LDAP and email entity), it would be appropriate to allow both types of addressing. Therefore we made these attributes (mgrpErrorsTo, mgrpAllowedBroadcaster, and mgrpModerator) URL's, to allow this dual use. If preceded by "mailto:" then the entry is taken as an SMTP RFC822 address. If preceded by "ldap://" then it is taken as an LDAP entry.

### 3.2 Mail processing attributes

There are two key mail processing features: how to address the mail group, and which type of mail group is this (mailing list or alias). In addition, there are two attributes that deal with the outgoing headers of mail to the group, and two for optimized processing.

#### 3.2.1 ‘mail’ attribute (cis, 1)

(0.9.2342.19200300.100.1.3
  NAME ‘mail’
  DESC ‘RFC822 email address for this person’
  EQUALITY caseIgnoreIA5Match
  SYNTAX ‘IA5String(256)’
  SINGLE-VALUE)

For addressing the group the primary attribute, and the only required attribute of this objectClass, is ‘mail’. This contains the RFC822 mail name of the group.

#### 3.2.2 ‘mailAlternateAddress’ attribute (cis, 0-many)

(2.16.840.1.113730.3.1.13
  NAME ‘mailAlternateAddress’
  DESC ‘alternate RFC822 email addresses used to reach this person’
  EQUALITY caseIgnoreIA5Match
  SYNTAX ‘IA5String(256)’)

There may also be a need for more than one way to address the group. There may be a desire for alternate names for the group (e.g. marketing@acme.com and marketing_dept@acme.com). Or there may be a requirement for more specific or alternate domains (e.g. marketing@server.acme.com). For any of these cases, we created an attribute ‘mailAlternateAddress’, which contains as many alternate mail addresses for the group as desired. For our purposes, we found no need to exclude the ‘mail’ entry from being duplicated in the ‘mailAlternateAddress’, but don’t encourage it.

#### 3.2.3 ‘mailHost’ attribute (cis, 0-many)

(2.16.840.1.113730.3.1.18
  NAME ‘mailHost’
  DESC ‘the fully qualified mail server hostname for this person’
  EQUALITY ‘caseIgnoreMatch’
  SYNTAX ‘DirectoryString’)

For the organization that has multiple MTA’s, we include a mailHost attribute, to optionally force handling of a mailGroup to a
particular server. Note that in our implementation this is not required: if left empty then any Messaging Server can expand the mailGroup. For various reasons it’s use is generally not encouraged. However, it may be advantageous in some circumstances to do this (e.g. if may be desired to expand a very large mailGroup on an underutilized server). Note that this must be entered as a Fully Qualified Domain Name (e.g. "server.acme.com", not just "server").

3.2.4 ‘mgrpErrorsTo’ attribute (ces, 0-1)

(2.16.840.1.113730.3.1.26
 NAME ‘mgrpErrorsTo’
 DESC ‘person or group to receive error messages for this group’
 SYNTAX ‘DirectoryString’
 SINGLE-VALUE
)

In SMTP there are two notions that are roughly analogous to a ‘group’ - a ‘Mailing List’ and an ‘Alias’. The difference between them [6] is whether list errors (e.g. bounce messages) are returned to the sender of the message, or to a ‘list administrator’. The former are considered ‘Aliases’, and the later ‘Mailing Lists’. In the later case, the ‘list administrator’ address is then used as the envelope ‘from’ address for any mail sent to members of the group (so that errors are returned to the ‘list administrator’ instead of the sender.

It is reasonable to want mailGroup to be able to support both entities, so we have the attribute ‘mgrpErrorsTo’ which contains an address for the ‘list administrator’. As mentioned in section 3.1 above, this is one of the fields that use a URL for entry. If an LDAP URL for a DN is entered (e.g. ldap://cn=Joe Jones, o=Ace, c=US) then the ’mail’ attribute of that DN will be retrieved for use as the mail address for errors. If no ’mail’ attribute is found for the DN entry then it is thrown out. Implementation note: For our implementation, if neither "mailto:" nor "ldap://" is found as a prefix then the assumption is that the entry is an RFC822 address.

As the envelope ‘from’ address is only expected to be a single address by some MTA’s, we will only allow one ’mgrpErrorsTo’ entry. However, if an admin wishes errors for a group to be handled by more then one person, that one entry may be the DN or address of a mailGroup iteslf, causing error messages to go to all members of that group.

3.2.5 ‘mgrpNoMatchAdds’ attribute (Boolean, 0-1)

( NAME ‘mgrpNoMatchAdds’
 DESC ‘if true then no duplicate adding from this group’
 SYNTAX ‘BOOLEAN’
 SINGLE-VALUE
)

One thing that an MTA should try to do is to keep from sending duplicate messages to people who are members of the group and also explicitly addressed in a message, or are in another group that’s also addressed in the message. However, this can take a large amount of time and memory for a large list, and administrators may desire the capability to turn this feature off. This attribute provides
that.

3.2.6 ‘mgrpRemoveHeader’ and ‘mgrpAddHeader’ attributes (cis, 0-many)

{
  NAME ‘mgrpRemoveHeader’
  DESC ‘headers to remove from messages to group’
  SYNTAX ‘IA5String’
}
{
  NAME ‘mgrpAddHeader’
  DESC ‘headers and contents to add to messages to group’
  SYNTAX ‘DirectoryString’
}

There are some headers that administrators may want to add and remove from messages being distributed to the group members. Examples of these are Reply-To:, which list administrators may want to add the list address to, or even remove the original sender from (when it is desired to have all correspondence go by default thru the group). Another example would be the Precedence: header, which is controversial but is used in some cases.

3.3 Membership attributes

The other key requirement for a mail group is to be able to specify members to receive mail.

3.3.1 Mixing with a groupOfUniqueNames for members

One way in which we accomplish this is to allow the mailGroup to mix-in with a groupOfUniqueNames. This provides the uniqueMembers from the groupOfUniqueNames as our mail recipients. The DN entry for the uniqueMember would then have the information necessary in order to send mail to them. Any interested in Netscape’s method of routing mail can view our draft [7].

3.3.2 ‘mgrpRFC822MailMember’ attribute (cis, 0-many)

(2.16.840.1.113730.3.1.30
  NAME ‘mgrpRFC822MailMember’
  DESC ‘RFC822 mail address of email only member of group’
  EQUALITY CaseIgnoreIA5Match
  SYNTAX ‘IA5String(256)’
)

However, there are other ways to specify mail members for the group. One case is that group mail members may be desired that do not have LDAP entries in our directory. For this reason we added the attribute ‘mgrpRFC822MailMember’. This contains members specified by RFC822 mail address. Another motivation for this attribute is that it can be used to specify people to receive mail sent to a group, but not acquire the privileges given to the mixed-in uniqueMembers of the groupOfUniqueNames.

NOTE on mgrpRFC822MailMember: The format for this does not just include the mail address. There are optional parameters after the address, of the form below. These are used for group management and are not detailed here.
LDAP also provides us with a truly unique and powerful method of specifying groups membership - with an attribute (mgrpDeliverTo) that is an LDAP search URL [8]. This allows us to create a dynamic search of the directory for entries that match a criteria, rather than having to specify each individual member. This uses the LDAP URL format to specify the criteria for a search. This URL has the form:

```
ldap://(server):(port)/(baseDN)?(attrs)?(scope)?(filter)
```

The `attrs` portion of the URL is not applicable for this use and is ignored.

Implementation notes: If the 'server' and 'port' are missing then they would default to the LDAP server being used by the MTA. The 'baseDN' specifies the base for the search and if not present then the default is the baseDN being used by the MTA.

The 'scope' defines the tree levels searched and it's default value is 'base' (standard for an LDAP URL). And finally, the default for 'filter' is "(mail=*)" since we only want to get mailable entities.

3.4 Mail Restriction attributes

There are also several restrictions that are useful on who can send to a mail group, or what they can send. We instituted two optional restrictions on senders, and one on messages. We also added an attribute to define what to do with rejected messages, and one for optional text to send back to the sender of a rejected message.

3.4.1 Sender Restrictions

First let it be noted that due to the inherent (alas) spoofability of SMTP mail, these restrictions are not normally to be thought of as security for the group, but merely a method of reducing the amount of mail to a group. Exceptions that provide more security are the mgrpApprovePassword, and the use of Certificates for mgrpAllowedBroadcasters (see below).

3.4.1.2 'mgrpAllowedDomain' attribute (cis, 0-many)

```
(2.16.840.1.113730.3.1.23
 NAME 'mgrpAllowedDomain'
 DESC 'allowed domains for sender of mail to group'
 SYNTAX 'IA5String'
)
```

The first Sender restriction is by domain. The domain of the sender's address is compared against those in the attribute 'mgrpAllowedDomain'. If there are no entries in the attribute then
all domains are allowed. If no match is found then the mail is rejected (see 3.3.3 below for handling).

3.4.1.3 'mgrpAllowedBroadcaster' attribute {cis, 0-many}

(2.16.840.1.113730.3.1.22
NAME 'mgrpAllowedBroadcaster'
DESC 'mailto: or LDAP: URL of allowed sender of mail to the group'
SYNTAX 'IA5String'
}

The other Sender restriction is by address. The attribute 'mgrpAllowedBroadcaster' contains the senders allowed to send mail to this group. As in 'mgrpErrorsTo' above, either DN's or RFC822 mail addresses may be used, and groups (groupOfUniqueNames or mailGroups) may also be used. As in mgrpAllowedDomain, if there are no entries for this attribute, then no restrictions are assumed.

3.4.2 Message Restrictions

There was only one restriction on messages that was considered valuable enough to be worth using, that of message size. The attribute mgrpMsgMaxSize contains the maximum number of bytes allowed for a message to this group (as above, if empty then there is no restriction).

3.4.3 Rejected Message Disposition - mgrpMsgRejectAction & mgrpMsgRejectText

(2.16.840.1.113730.3.1.28
NAME 'mgrpRejectAction'
DESC 'The action to be taken for a rejected message to the group'
SYNTAX 'GroupRejectSyntax'
)

<GroupRejectSyntax> :: [RejectType] <RejectAction>

<RejectType> :: 'SIZE:' | 'DOMAIN:' | 'SENDER:'
<RejectAction> :: 'REPLY' | 'BOUNCE' | 'TOMODERATOR'

(2.16.840.1.113730.3.1.29
NAME 'mgrpRejectText'
DESC 'Text to be returned with a rejected message'
SYNTAX 'GroupRejectTextSyntax'
)

<GroupRejectTextSyntax> :: [RejectType] DirectoryString

<RejectType> :: 'SIZE:' | 'DOMAIN:' | 'SENDER:'

There are three different actions that are currently allowed on a rejected message. These are controlled by the mgrpMsgRejectAction attribute. Other actions may be added later, but no compelling ones appear imminent. The current options are:

"REPLY" - sends an error reply back to the message sender.

"BOUNCE" - sends the reply as above, along with the original message.
"TOMODERATOR" - sends the message to (a) moderator address(es). The attribute mgrpModerator contains these addresses to mail to. The addresses may include mailGroups. This may be used (as one might guess from the title) for moderated groups, but also for other uses, e.g. forwarding messages 'unworthy' of sending to the whole group to a newsgroup, to be read by people interested in them.

For the REPLY and BOUNCE options, the reply sent back is contained in the attribute mgrpMsgRejectText. If desired, separate actions and/or messages can be stored for any of the rejection types, by preceeding the text in the entry by "SIZE:", "DOMAIN:" or "SENDER:". The mgrpMsgRejectText message is '$-encoded' - that is, all carriage returns/line feeds are encoded as "$", and any "$"s in the text are encoded to "\36". [10]

3.4.4 Mailing List moderation

It is often useful to have moderated mailing lists. For this type of group, all mail that does not pass the restrictions is sent to (a) moderator(s), possibly being a program to automatically handle moderation tasks. The moderator(s) would then forward the message back to the mailing list to 'resubmit' it.

3.4.4.1 ‘mgrpApprovePassword’ attribute (ces, 0-1)

{
  NAME ‘mgrpApprovePassword’
  DESC 'password used for approval of message to a moderated group'
  EQUALITY octetStringMatch
  SYNTAX 'Password{128}'
  SINGLE-VALUE
}

This contains the password used for moderated message approval. If it is present, and moderators exist, then all messages submitted to the group must have an Approval line which includes this password (actual implementation of this is left to the MTA). Exceptions are permitted only as given in section 3.4.4.2 below.

3.4.4.2 ‘mgrpBroadcasterModeration’ attribute (ces, 0-1)

{
  NAME ‘mgrpBroadcasterModeration’
  DESC 'controls functionality of allowedBroadcaster list'
  SYNTAX 'groupBroadcasterModeration'
  SINGLE-VALUE
}

<groupBroadcasterModeration>:: 'BROADCASTERS_OVERRIDE' | 'CERT_BROADCASTERS_OVERRIDE' | 'BROADCASTERS_ARE' | 'CERT_BROADCASTERS_ARE'

This attribute controls the relation of moderation to the allowedBroadcaster list. This can have any one of the following values:

  BROADCASTERS_OVERRIDE - if the sender is a member of allowedBroadcaster then their message is posted to the group even if moderation is on. This is the default.
CERT_BROADCASTERS_OVERRIDE - same as above except the sender's Certificate must be present and checked (see xxxxx above).
BROADCASTERS_ARE - allowedBroadcasters are given 'moderation' privilege.
CERT_BROADCASTERS_ARE - again same as above except the sender's Certificate must be present and checked.

Each of the CERT_ options would require mail to be sent 'signed', with an X.509 Certificate [11]. The MTA would then check that this matches the Certificate stored for that person.

4.0 Other notes

We did not bother to add any 'physical location' type attributes to the mailGroup class (e.g. Mailing Address, Phone Number,...), as none are necessary for processing, and they would seem to be of marginal use anyway.

There is a 'cn', which is as expected the name of the group.

5.0 mailGroup Schema

The following is the LDAP schema for the mailGroup objectClass:

(2.16.840.1.113730.3.2.4
 NAME 'mailGroup'
 SUP top
 STRUCTURAL
 MUST mail
 MAY ( cn $ mailAlternateAddress $ mailHost $ mailRequireAuth $ mgrpAddHeader $ mgrpAllowedBroadcaster $ mgrpAllowedDomain $ mgrpApprovePassword $ mgrpBroadcasterModeration $ mgrpDeliverTo $ mgrpErrorsTo $ mgrpModerator $ mgrpMsgMaxSize $ mgrpMsgRejectAction $ mgrpMsgRejectText $ mgrpNoMatchAddrs $ mgrpRemoveHeader $ mgrpRFC822MailMember )
)

6.0 Examples

Some example mailGroups, and their operation, might be useful. Here are some (in LDIF format):

6.1 Example #1

dn: cn=Birds, ou=sales, o=Writable, c=US
objectclass: top
objectclass: mailGroup
cn: Birds
mail: birds@Writable.com
mailalternateaddress: birds@server.writable.com
mgrpdeliverto: ldap://ou=sales, o=Writable Corp, c=US??sub?(&
 (objectClass=mailRecipient)(cn=*Bird))
mgrperrorsto: ldap://cn=Mickey Mouse, ou=sales, o=Writable, c=US
mgrpmsgrejectaction: bounce
mgrpmsgrejecttext: This is a test of the emergency broadcasting network.
mgrpalloweddomain: grunge.com

This group will send mail to all inetOrgPersons in the Sales org unit of Writable Corp, with a name ending in "Bird" (very useful - eh!).
It is a 'mailing list' (rather than an 'alias'), as mgrpErrorsTo is set. It will reject any mail where the sender’s domain is not grunge.com - rejected messages will be ‘bounced’ back to the sender, with a reply message of "This is a test of the emergency broadcasting network." Mail to this group can be sent to either birds@writable.com or birds@server.writable.com.

6.2 Example #2

dn: cn=Real People, ou=sales, o=Writable, c=US
objectclass: top
objectclass: mailGroup
objectclass: groupOfUniqueNames
cn: Real People
mail: real@Writable.com
mgrprfc822mailmember: bruces@netscape.com
mgrpallowedbroadcaster: ldap:///cn=Real People, ou=sales, o=Writable, c=US
mgrperrorsTo: mailto:bruces@netscape.com
mgrpmsgrejectaction: size: toModerator
mgrpmsgrejectaction: reply
mgrpmsgrejecttext: Sorry, Charlie
mgrpmoderator: ldap:///cn=Marvin the Martian, ou=marketing, o=Writable, c=US
mgrpmsgmaxsize: 2000000
uniquemember: cn=Rose Bird, ou=legal, o=Writable, c=US
uniquemember: cn=Larry Bird, ou=finance, o=Writable, c=US
uniquemember: cn=Bird Man of Alcatraz, ou=legal, o=Writable, c=US

This group gets it’s members partly from a the uniqueMembers of a mixedin groupOfUniqueNames and one mgrpRFC822MailMember (bruces@netscape.com) that will receive email sent to the group, but have none of the other privileges of the uniqueMembers. Messages over 2meg will be sent to "Marvin the Martian", but senders not in the Real People group will merely have a reply sent to them. Also note that the mgrpErrorsTo is specified here as an email address, as opposed to a DN above.

6.3 Example #3

dn: cn=big moderated group, o=Writable, c=US
cn: big moderated group
mail: big_mod@writable.com
mgrpdeliverto: ldap:///??sub?(objectClass=inetOrgPerson)
mgrpaddheader: Reply-To: big_mod@writable.com
mgrpremoveheader: Precedence:
mgrpallowedbroadcaster: bruces@netscape.com
mgrpapprovepassword: ohdear
mgrpbroadcastermoderation: BROADCASTERS_OVERRIDE

And this group is one that would mail to everyone in the company. The baseDN is the default (which would assumedly be the base for the organization), and this would include all ‘people’. This is a moderated group, with a password of ohdear. Any "Precedence:" header in a message to this group would get stripped, and big_mod@writable.com would be added as a "Reply-To:" address for any message to the group (or the Reply-To: header added if not already present).

6.4 Example #4
Finally, this group includes an mgrpRFC822MailMember that is another group (birds@writable.com - see example #1 above). It is also an ‘alias’ (as opposed to a ‘mailing list’) as there is no mgrpErrorsTo specified. There are no restrictions on who can mail to this list. Also, mail sent to this group will not check to avoid duplicate addresses, so multiple copies of this message could be sent to the same person (mgrpnomatchadrs: TRUE).

7.0 Security Considerations

As mentioned in sections 3.4.1 and 3.4.4.2, one of the features of mailGroups is to restrict who can send mail to the group. There are several ways to accomplish this that vary significantly in how secure they are, ranging from just trusting the sender’s headers, to a clear text password, and finally Certificates. The needs will be different for different groups, hence the range of possibilities provided.

8.0 Acknowledgements

There were many people of great assistance in producing this document, but special thanks go to: Bill Fitler, who made the mistake of hiring me in the first place, Tien Tran, who cheerfully brought me up to speed on our Mail Server, and John Kristian, who has patiently steered me towards a better understanding of LDAP.

9.0 References

[3] X.521 (groupOfUniqueNames)
[6] R. Braden, "Requirements for Internet Hosts", RFC 1123, October 1989 (specifically, section 5.3.6 "Mailing Lists and Aliases").

[10] ($-encoding)


9.0 Author’s Address

Bruce Steinback
Netscape Communications Corp.
501 East Middlefield Rd. Mail Stop MV-029
Mountain View, CA 94943
USA

Phone Number: (415) 937-3466
Email: bruces@netscape.com