Investigation in the possibilities to reference between the X.521 naming and the Domain Componant naming

TERENA Task Force LDAP Service Deployment, Deliverable F

Authors: Luuk Oostenbrink (SURFnet), Diego Lopez (RedIRIS), Licia Florio (TERENA), Peter Gietz (DAASI International)
Final Version, 23.1.2003

Abstract

The aim of this deliverable is to investigate the possibilities to reference between the X.521 [X.521] naming and the Domain Component naming [RFC 2247] as well as the referral mechanisms to set up a Directory Information Tree between LDAP servers via distribution of knowledge information. The results of the DIRECT Project and the current respective IETF efforts are base for this item.

The first part of this deliverable is a report, written by Luuk Oostenbrink (SURFnet) about research on the mapping of dc and X.521 naming. The report describes why a dynamic (real-time) mapping between the two schemas proved to be unfeasible for an organization like SURFnet.

The second part of the report describes the structure for the new LDAPv3-based Directory service at RedIRIS. At the moment RedIRIS uses two DITs in parallel: dc and X.521.

1. Dynamic DC2X521 ldap mapping service

The purpose of this project was to investigate the possibilities of dynamical mapping DC ldap requests to X.521 and vice versa. Hereto a referral server had to be created in which the following steps were to be taken:

a. If an entry is present in the default root DC server for the given DC-naming context a referral will be generated to the ldap server in that entry.
b. If an entry is present in the default root X.521 server for the DC to X.521 mapped DN, a referral will be generated to the ldap server in that entry, with the mapped X.521 DN (for instance, "DC=surfnet, DC=nl" generates a referral to "ldap://ldap.surfnet.nl/O=SURFnet, C=NL")
c. The DC base name will be resolved in the DNS. In case a TXT record exists for that domain a referral will be generated for it (like openldap's dns backend).
d. Heuristic methods. For instance look-up ldap.<DC name> and generate a referral to this host. This referral server could be beneficial for SURFnets root referral ldap service, which is the root server for C=NL.

Implementation:

The referral server is based on the dns backend code provided with the openldap v2.0.7 source. The referral.c module was heavily adapted. The reason this backend is used was that a lot of the code was re-usable.

Result:

A prototype referral root server was implemented and tested. With this prototype server the steps a, b and c as described in the goal section were implemented.

Continuation:

For continuation of this project a mapping of dc to X.521 mapping through the Dutch Domain registrar (SIDN) was planned. Unfortunately, SIDN only provides a domain to organisational

name look-up and not vice versa. Furthermore a static DC-X.521 mapping service method was provided by red IRIS. This mapping method seems very usable for the Dutch root referral service.

Therefore the decision was made not to continue this project.

2. Structure for the new LDAPv3-based Directory service at RedIRIS

In the RedIRIS community both types of naming are being used. To integrate all LDAP services a new structure was developed that solves the mapping problem.

This new structure is based on three elements:

1. LDAP servers at the institutions affiliated to RedIRIS.
2. LDAP-ES: A LDAPv3 server acting as the national root for the Spanish Academic Network.
3. LDAP-SEARCH: A LDAP server optimised for searches.

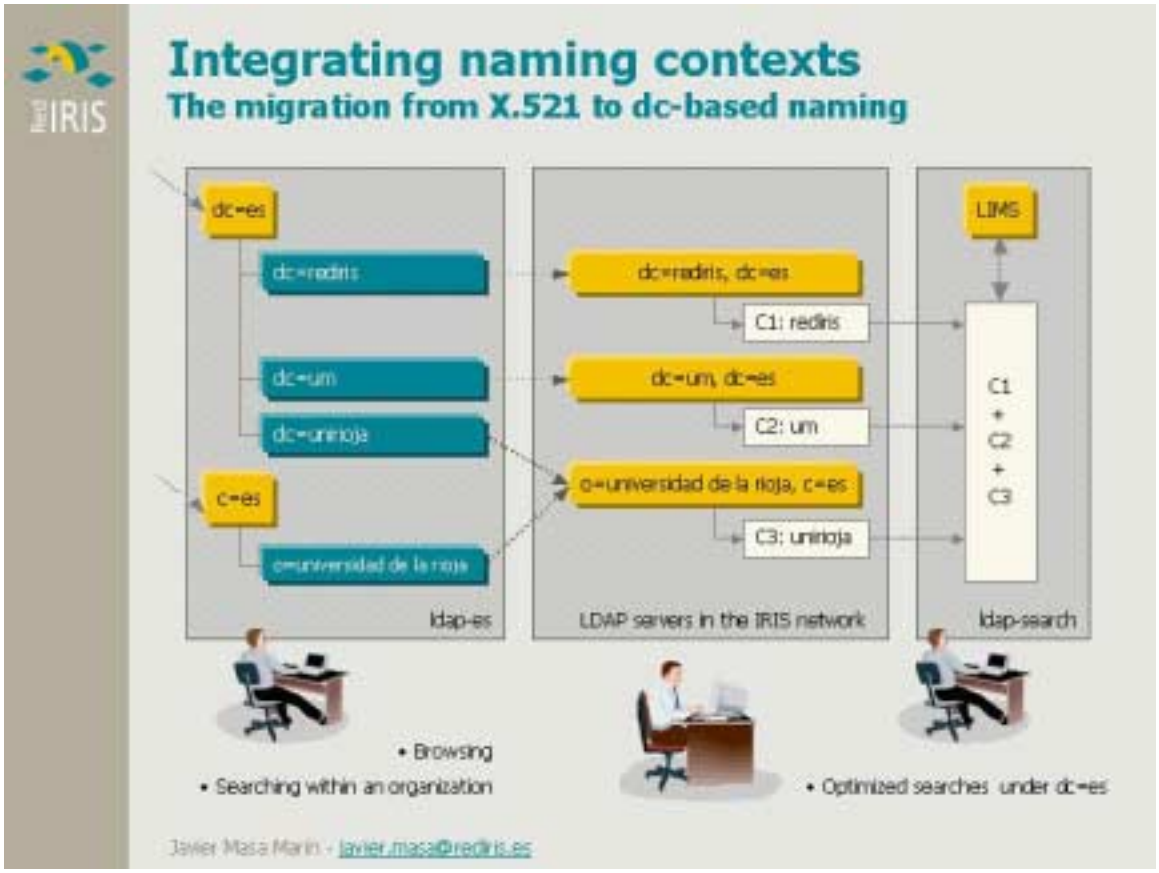
The LDAP-ES server manages both the 'dc=es' and the 'c=es' naming contexts.

The entries under 'dc=es' are LDAPv3 references to other LDAP servers at the affiliated institutions. DNs for these entries are based on 'dc' attributes, using the domain name of the corresponding organisation.

If an organisation only manages an X.521-based namimg context under 'c=es', two references are created, pointing to the same destination server.

One is based on 'dc' attributes (using the domain name of the organisation), under 'dc=es'. The second one is under 'c=es' and uses the X.521-based name. Therefore, all organisations included in the Academic Directory are accessible using the 'dc=es' naming context through their domain names.

The following diagram shows the architecture in which the mapping is being used:



This server is only intended to be used as a reference point for the access to LDAP servers participating in the Directory. Searches are performed through a special-purpose server optimised for searches, based on software called LIMS, a CIP-based [RFC 2651] LDAP referral server. LIMS has been evaluated as the basis for the search facilities in an European-wide white pages service based on LDAP.

The Spanish Academic Directory is accessible through the WWW at:

http://www.rediris.es/ldap/ldap-es/navega
http://www.rediris.es/ldap/ldap-search/

Conclusion

The two studies from SURFnet and RedIRIS show that a mapping between the two naming schemes X.521 and Domain Component is possible in principle.

The usage of dynamic DNS-based mappings have been proven as possible but impractical, since it would require the establishment of a considerable infrastructure. Naming scheme mapping, since it is a temporary service, can be achieved in a much simpler way by means of a country-level LDAP server offering static maps. This service can be complemented by the use of CIP-based retrieval systems like LIMS.

References

[RFC 2247] Kille, S., Wahl, M., Grimstad, A., Huber, R., Salaturi, S., " Using Domains in LDAP/X.500 Distinguished Names, RFC 2247, January 1998

[RFC 2651] Allen, J., Mealling, M., The Architecture of the Common Indexing Protocol (CIP), RFC 2651, August 1999

[X.521] ITU-T Rec. X.521, "The Directory: Selected Object Classes", 1993