Lightweight Directory Access Protocol : LDAP

Erhan Ekici
erhan.ekici@lkd.org.tr

15 Mayıs 2004

Lightweight Directory Access Protocol

- Dizin (Directory) nedir?
  - X.500 Nedir ?
  - DAP Nedir ?
  - LDAP Nedir ?
  - X.500 ile LDAP arasındaki farklar nelerdir ?
- LDAP v2 & LDAP v3 ?
- Niçin LDAP ?
- LDAP & Veritabanı ?
- LDAP İsim Alanları
- LDAP Şemaları

Dizin (Directory) nedir?

- Genellikle okuma ve arama gibi amaçlar için düzenlenmiş/optimize edilmiş bir tür veritabanıdır.
- Yazma amaçlı erişim okuma amaçlı erişime göre çok çok düşüktür.
- Örnekler :
  - Adres Defterleri
  - Domain Name System
  - Sözlük Sunucuları
  - Sarı Sayfalar
  - Telefon Defteri
  - Vs....

X.500 Nedir ?

- 1988 te CCITT tarafından tanımlandı, 1990'da ISO 9594 olarak standartlaştı.
- DAP protokolü kullanan Sunucu ve İstemci arasındaki haberleşmeyi tanımlar
- Elektronik Dizin Servislerini kapsayan ITU standartlar dizisi
- X.500 OSI(Open System Interconnection) Dizin Servislerini tanımlar
  - Hiyerarşik
  - Dağıtık Mimarili
  - Replicated
  - Schema destekli

DAP Nedir?

- **DAP**

  Directory Access Protocol – Dizin Erişim Protokolü

  OSI Modelinin Uygulama Katmanında çalışan bir protokoldür

X.500’den LDAP’ye...

- X.500 DAP protokolünü kullanır.
- DAP çalışabilmek için tüm OSI protokol kümesine gereksinim duyar.
- Tüm OSI protokol kümesinin bulunabileceği sistemler ancak kaynak bakımından yeterli, büyük sistemler.
- Daha az kaynak (donanım) barındıran sistemler için elverişsiz
- Peki bu kadar kaynak harcamadan bu iş nasıl yapılır?
- Yok mu bunun “light” sürümü

LDAP Nedir?

- Lightweight Directory Access Protocol
  IETF (Internet Engineering Task Force) tarafından sunulmuş bir standart
- TCP üzerinden X.500 Dizin Servislerine erişmek için tasarlandı.
- Sonra kendi bir dizin servisi haline geldi.
- Sunucu / İstemci mimarisine sahiptir.

X.500 ile LDAP arasındaki farklar nelerdir ?

- X.500 OSI Protokol Kümesini kullanır.
- LDAP TCP/IP protokolünü kullanır.

- X.500 yapısı çok detay içeren, karışık bir yapıdır.
- LDAP basitlik üzerine kurulmuştur.

- X.500 OSI kullanmasından dolayı, küçük sistemler ve masaüstü sistemler için uygun değildir.

- LDAP çok kaynak gerektirmeyen ve her sistemde bulunabilen TCP/IP ye gereksinim duyduğundan yaygın olarak kullanılabilir.

LDAP v2 - RFC (Request for Comment)

- *X.500 Lightweight Access Protocol* (RFC 1487)
- *Lightweight Directory Access Protocol* (RFC 1777)
- *The String Representation of Standard Attribute Syntaxes* (RFC 1778)
- *A String Representation of Distinguished Names* (RFC 1779)
- *An LDAP URL Format* (RFC 1959)
- *A String Representation of LDAP Search Filters* (RFC 1960)

LDAP v3 - RFC (Request for Comment)

- *Lightweight Directory Access Protocol (v3)* (RFC 2251)
- *Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions* (RFC 2252)
- *Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names* (RFC 2253)
- *The String Representation of LDAP Search Filters* (RFC 2254)
- *The LDAP URL Format* (RFC 2255)
- *A Summary of the X.500(96) User Schema for use with LDAPv3 (RFC2256)*

LDAP v2 & LDAP v3 : v3'ün Üstünlükleri

- **Yönlendirme (Referrals)**

  İstemcinin talep ettiği veriye sahip olmayan sunucu istemciyi başka bir sunucuya yönlendirebilir

- **Güvenlik (Security)**

  Simple Authentication and Security Layer (SASL) kullanımı ile genişleyebilir doğrulama mekanizması

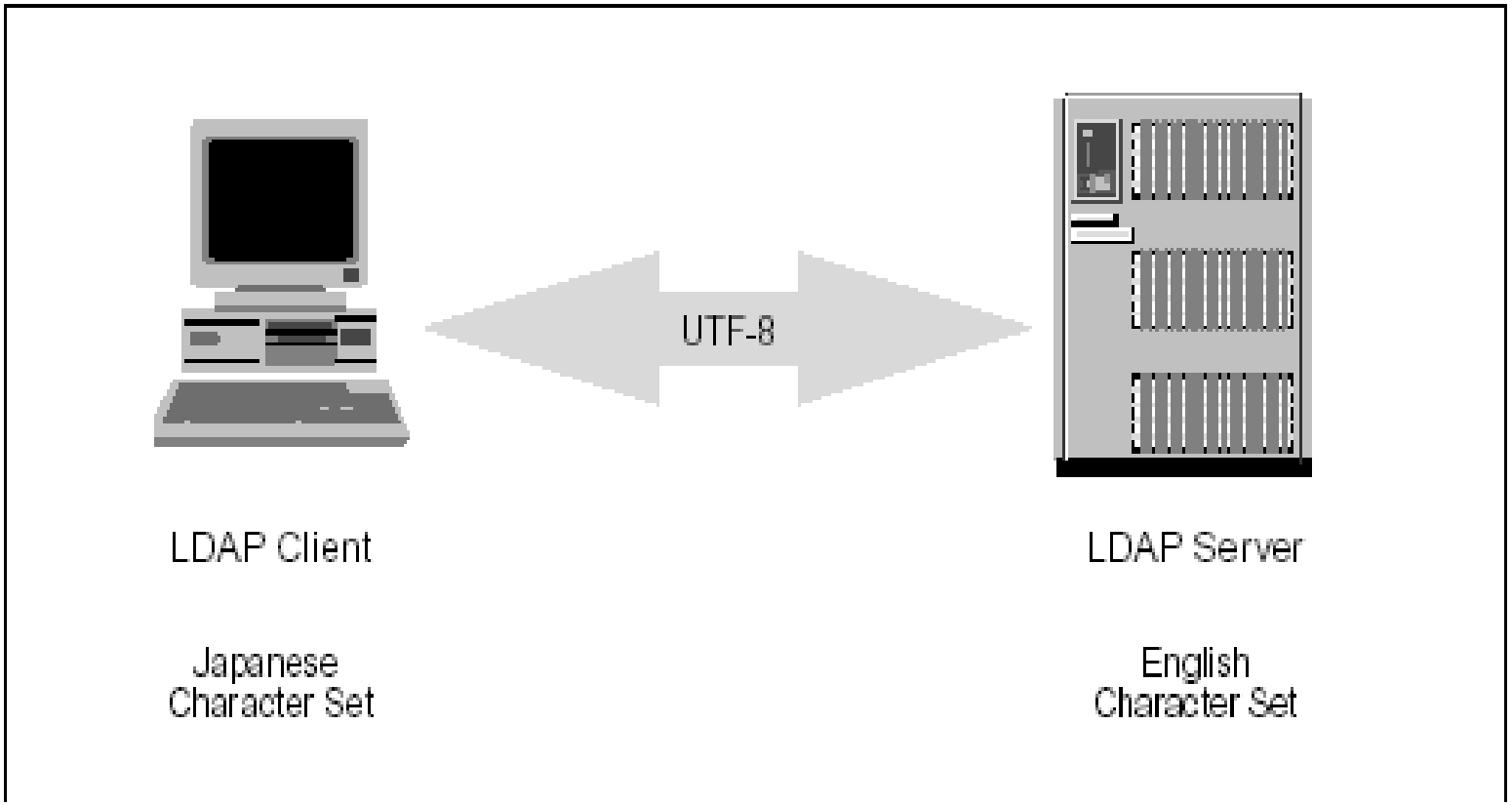
- **UTF-8 Karakterler (Internationalization)**

  Uluslararası karakterler için UTF-8 desteği

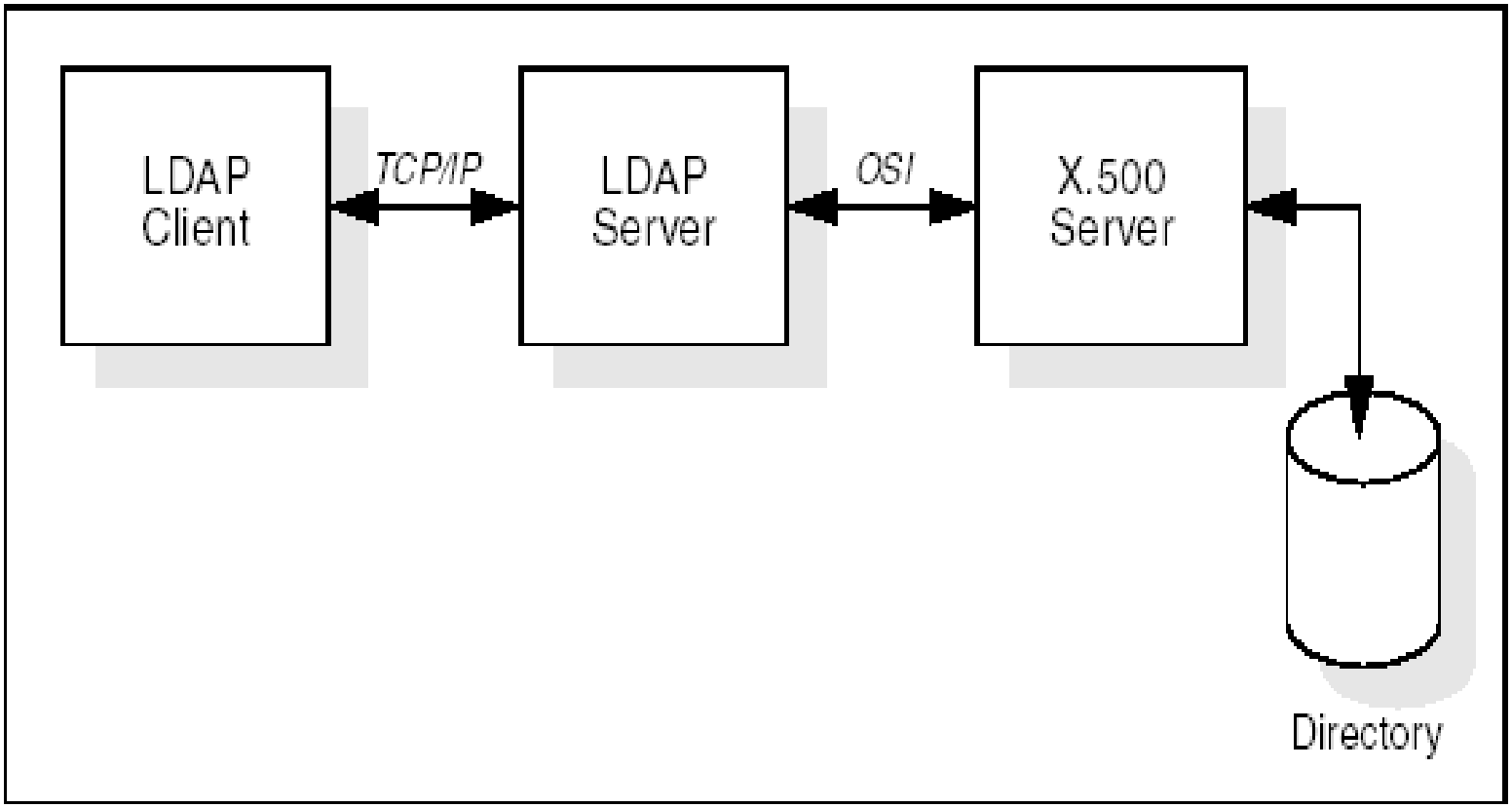
- **Esneklik & Genişleyebilirlik (Extensibility)**

  Yeni nesne türleri ve işlemler dinamik olarak tanımlanabilir ve şema (schema) tanımlama standartları

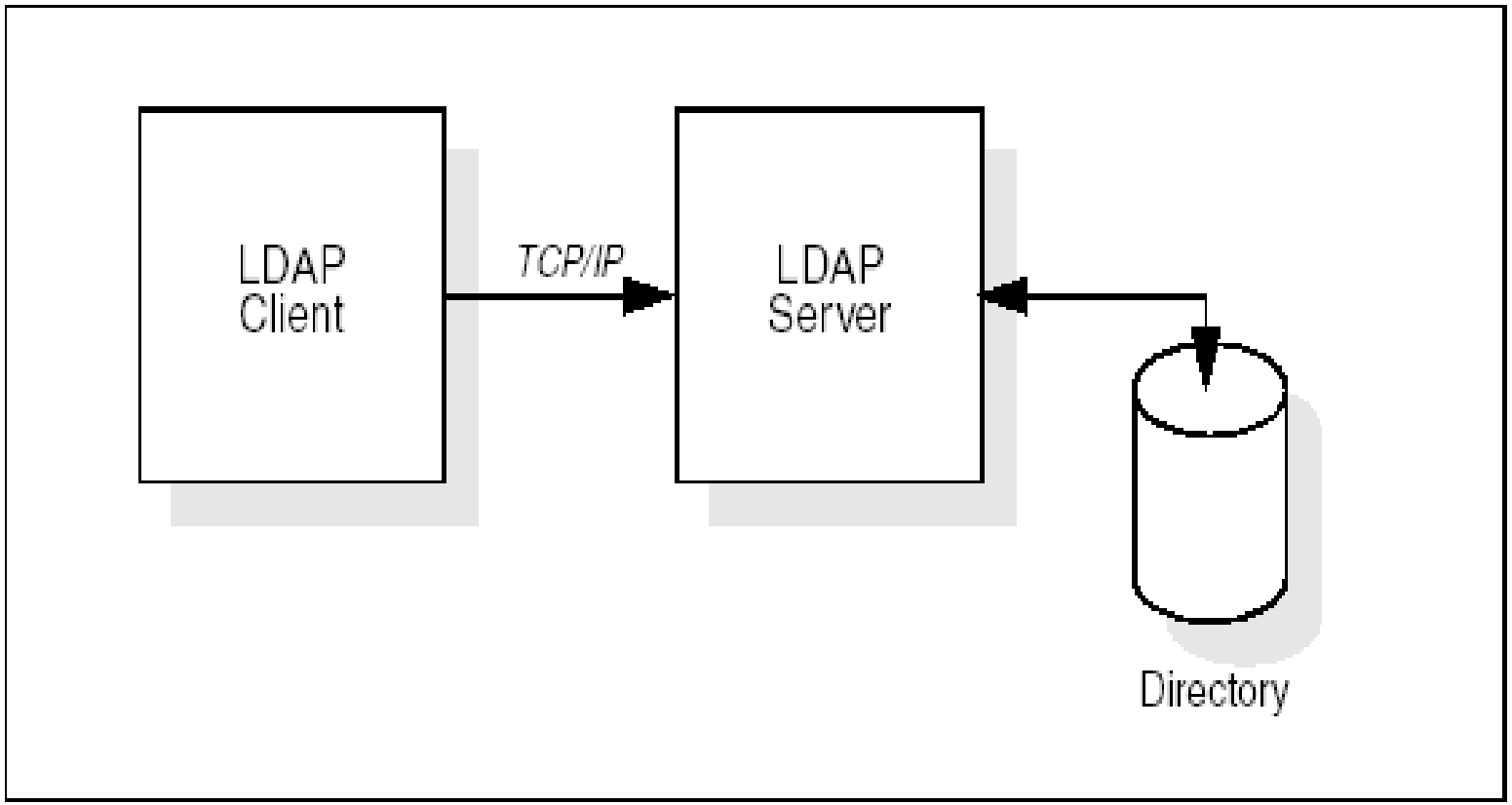
UTF – 8 (UCS Tranformation Format)



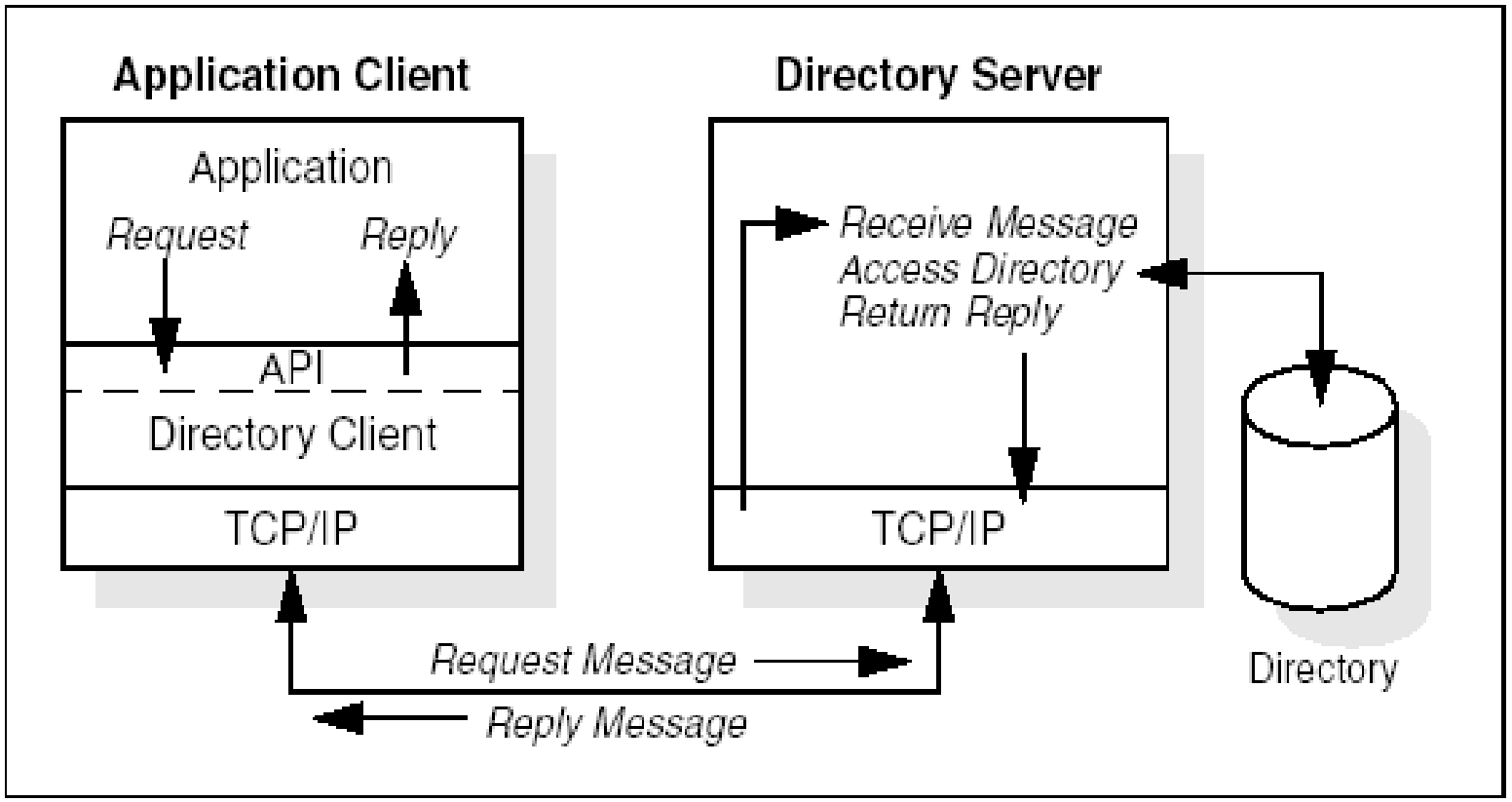
LDAP önceleri X.500 Dizinlerine erişmek için tasarlandı



Sonra...



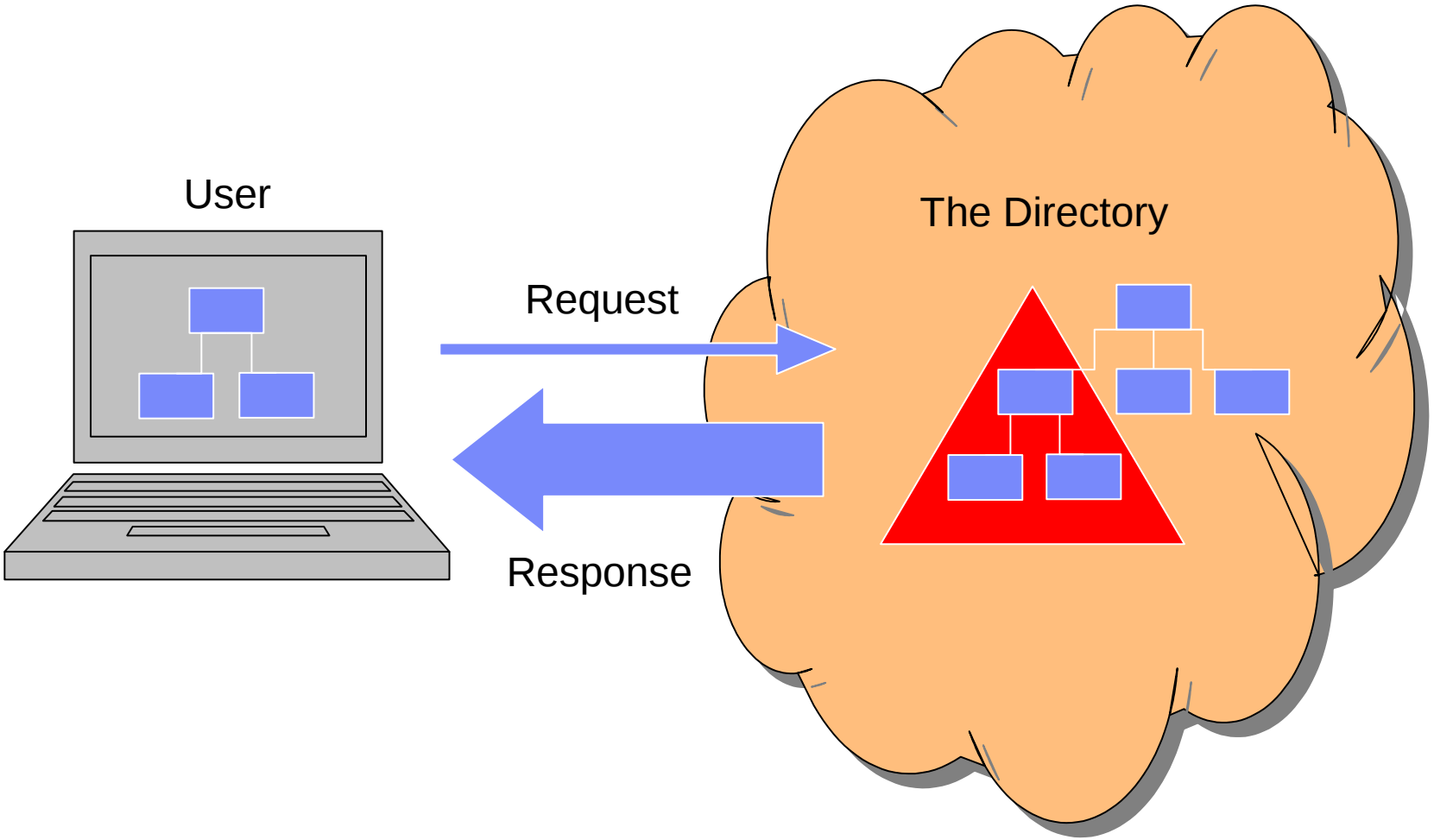
LDAP Sunucu-İstemci Mimarisi



LDAP adres gösterimi

- ldap://<sunucuadresi:port>/ou=seminercg,o=LKD,c=TR
- Port : 389
- SSL Port : 636
- ldap:// protokolü belirtir
- /ou=seminercg,o=lkd,c=tr taranacak dizini belirtir.

LDAP İlişkisi



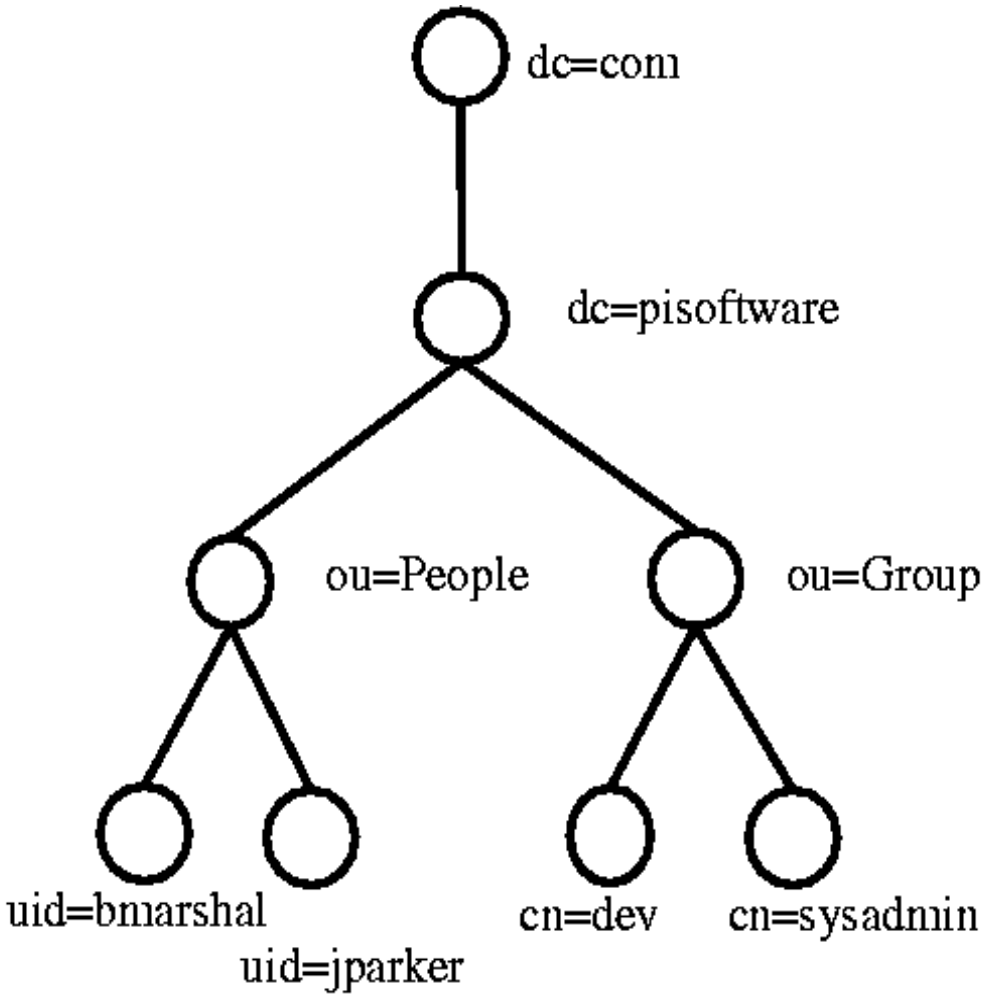
Niçin LDAP?

- Kullanıcı bilgileri,Grup bilgileri vb bilgilerin merkezi yönetimi
- Farklı uygulamalar farklı dizinler kullanmayacak
- Kullanıcıların aradıkları bilgiye hızlı ve kolay ulaşması
- Dağıtık mimariye uygun olması
- Her sistemde kullanılabilmesi

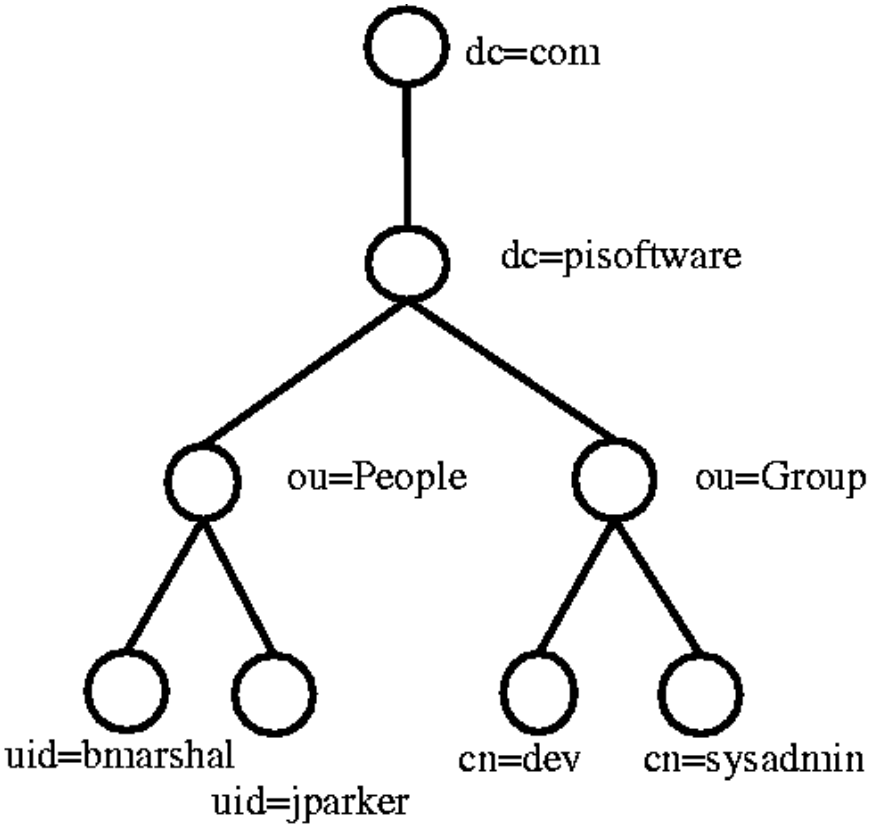
LDAP ve Veritabanı : Farklar

- LDAP özel amaçlı bir veritabanı gibi düşünülebilir.
- Veritabanları hem okuma hemde yazmaya karşı optimize edilmiştir.
- LDAP okuma/arama özellikleri yazma özelliklerine göre çok daha gelişkindir.
- Veritabanları komplex işlemleri (rollback,transaction) destekler.
- LDAP komplex veritabanı işlemlerini desteklemez.(Bazı yazılım firmaları bu desteği ürünlerine eklemişlerdir.)
- LDAP sunucular göreceli statik bilgiler saklarken, Veritabanı sunucuları dinamik veriler saklarlar.
- LDAP standartlar üzerine kurulmuştur.Bir LDAP istemcisi tüm LDAP sunuculara erişebilir.
- Farklı veritabanı araçları sadece kendi ürünlerine erişmek için kullanılabilir.

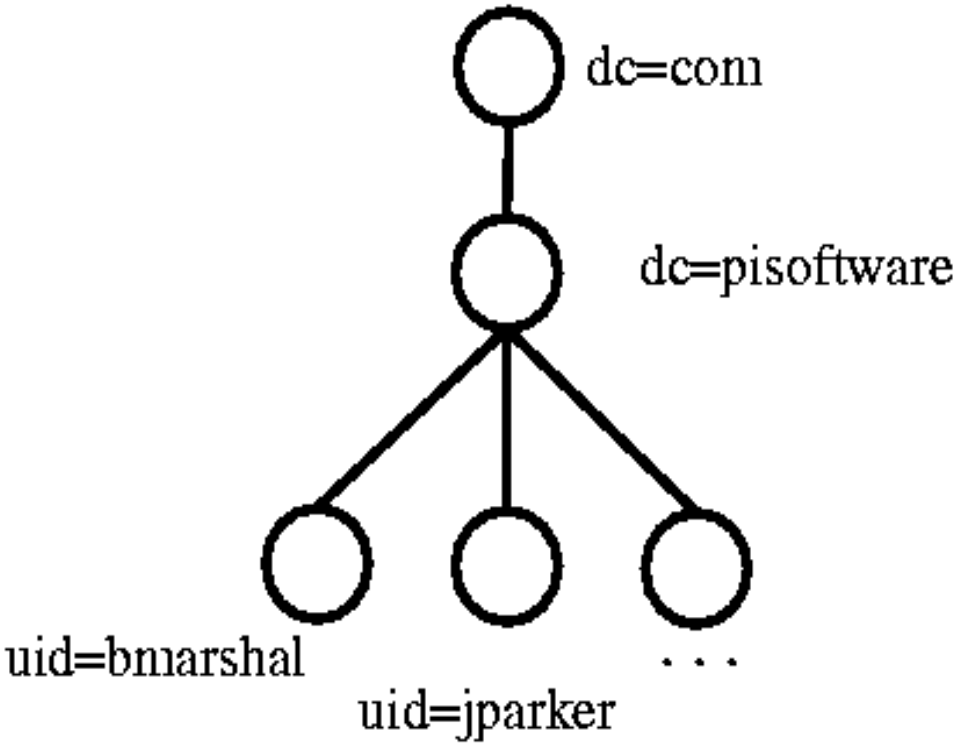
LDAP Directory Information Tree (DIT)



Hiyerarşik Ağaç Yapısı



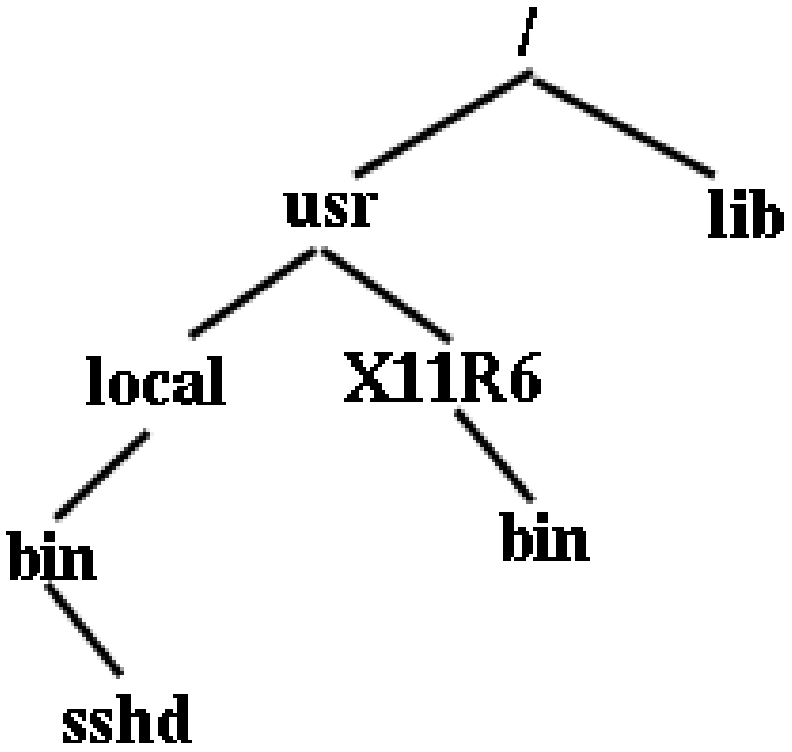
Düz (Flat Ağaç Yapısı)

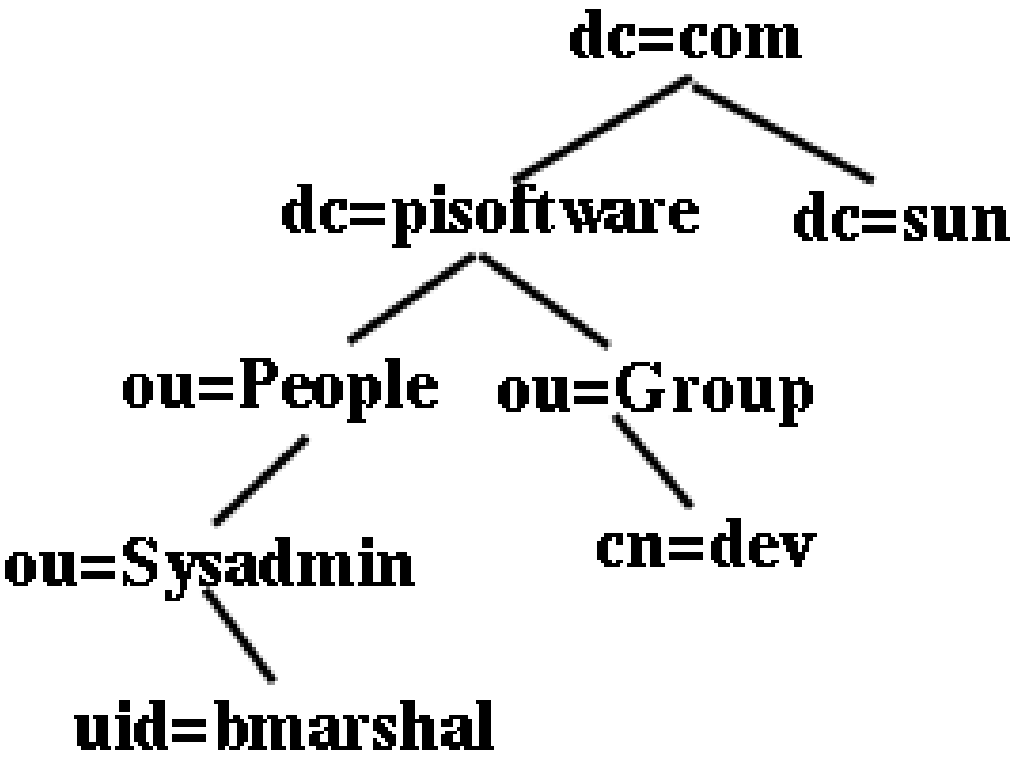


İsim Uzayları (Namespace)

- LDAP Yapısı Linux Dosya Sistemine benzer.
- DNS yapısı LDAP yapısı ile benzerlikler gösterir
- Linux dosya sistemi kökten sona doğru giderken, LDAP DN leri sondan köke doğru gider
- LDAP de her kayıt(entry) veri içerebileceği gibi kendiside veri barındıran(container) olabilir.
- LDAP de tek bir kök (root) yoktur, birden fazla olabilir.

İsim Uzayları (Namespace) devam....





DN : Distinguished Names

- dn: uid=erhan, ou=communication, o=firma, c=tr
- Altan başlayarak her seviyedeki değerler alınır ve virgülle ayrılır.
- İkiye ayrılır:

  En soldaki RDN : Relative Distinguished Name
  Kalan : Base Distinguished Name

- Örnek :

  dn: uid=erhan, ou=communication, o=firma, c=tr

  RDN : uid=erhan
  Base: ou=communication, o=firma, c=tr

- Her base DN de ki RDN tekildir.

LDAP – Kayıt (Entry)

- Kayıtlar özelliklerin (attribute) bir araya gelmesi ile oluşur.
- Özellik (Attribute)
  <tür> : <değer>
- Aynı tipte birden fazla özellik olabilir.

  Cn = Erhan
  Cn = Erhan Ek
- Type : Ne tip bilgi olacağını belirler
  Mail,jpegphoto, url vs...
- Değer: text formatında olabildiği gibi base-64 encoded da olabilir.
- Özelliklerde ne tip bilgiler ve bu bilgilerin hangi formatta olacağı bellidir.
  ObjectClass'lar...

Objectclass

- Özelliklerde ne tip bilgiler ve bu bilgilerin hangi formatta olacağı bellidir.
- Bir kayıt icin birden fazla Objectclass olabilir.
- Hangi objectclass'larin kullanılabileceği şemalar (schema) ile belirlenir.
- Bazı objectclass'lar:

  account

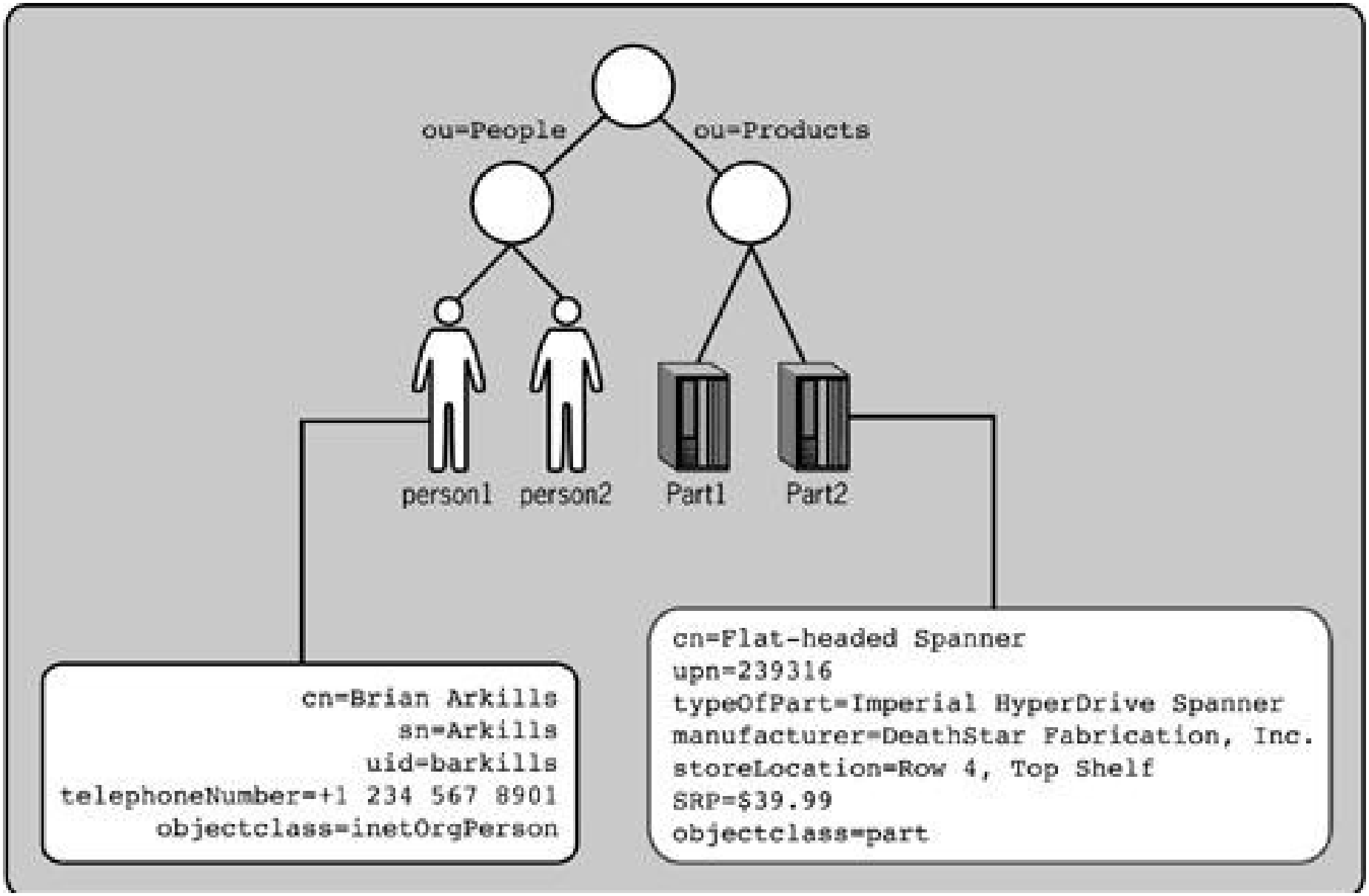
  posixAccount

  posixGroup

  shadowAccount

  top

  organizationalUnit


ou=People
ou=Products
person1
person2
Part1
Part2
cn=Brian Arkills
sn=Arkills
uid=barkills
telephoneNumber=+1 234 567 8901
objectclass=inetOrgPerson
cn=Flat-headed Spanner
upn=239316
typeOfPart=Imperial HyperDrive Spanner
manufacturer=DeathStar Fabrication, Inc.
storeLocation=Row 4, Top Shelf
SRP=$39.99
objectclass=part

Aliases

- Bir LDAP kaydının(entry) diğerini göstermesi
- Hiyerarşik olmayan yapı kurulmasına izin verir
- Unix/Linux daki sembolik link kavramına benzetilebilir
- Performans'tan dolayı tüm LDAP sunucular desteklemeyebilir
- aliasedObjectName

Terimler

- LDAP
  Lightweight Directory Access Protocol
- DN
  Distinguish Name
- RDN
  Relative Distinuished Name
- DIT
  Directory Information Tree
- LDIF
  LDAP Data Interchange Format
- OID
  Object Identifier

LDIF Nedir ?

- LDAP Data Interchange Format
- LDAP kayıtları düz metin formatında sunulur
- Veri değişiklerini kolaylaştırır
- Okunabilir bir formata sahiptir
- Betikler ve çeşitli araçlar ile hazırlanabilir,aktarılabilir vs..
- Yedekleme ve başka bir sisteme aktarma işlemleri yapılabilir
- ldif2db2, ldif2ldbm vb araçlar ile dönüşüm yapılabilir

LDIF Nedir ? devam...

- Örnek bir LDIF dosyası

```
dn: uid=erhan,ou=People,dc=linuxcenter,dc=org
uid: erhan
cn: Erhan Ekici
objectclass: account
objectclass: posixAccount
objectclass: top
loginshell: /bin/bash
uidnumber: 500
gidnumber: 120
homedirectory: /home/erhan
userpassword: {crypt}KYnMoPYF7JSag
```

LDAP Şemaları (Schemas)

- Dizinde saklanacak verinin türünü ve yapısını belirten kurallar bütünü
- Veri bütünlüğü, uyumluluk sağlar
- Benzer veriler girilmesini ve kaynak israfını engeller
- Uygulamalar için kolaylık sağlar
- Object class özelliği kaydın uyması,takip etmesi gereken kuralları, şemalar da objectclass'ların izlemesi gereken kuralları belirler.

Şema (Schema) devam...

- Bir şema aşağıdakileri içermelidir:

  Gerekli özellikler

  İzin verilen özellikler

  Özellikler nasıl karşılaştırılacak

  Özelliğin saklayacağı veri tipi kısıtlama getirebilir (sayı olmasın gibi)

  Özelliğin saklayacağı veri üzerine kısıtlama getirebilir (no dublication gibi)

Şemalar

- corba.schema
- cosine.schema
- core.schema
- openldap.schema
- inetorgperson.schema
- java.schema
- misc.schema
- nis.schema

İnetorgperson.schema dosya yapısı...

- attributetype (2.16.840.1.113730.3.1.241
  NAME 'displayName'
  DESC 'RFC2798: preferred name to be used when displaying entries'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE)

- attributetype (0.9.2342.19200300.100.1.60
  NAME 'jpegPhoto'
  DESC 'RFC2798: a JPEG image'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.28)

Object Class

- Bilgileri gruplamak için kullanılır
- Aşağıdaki kuralları sağlar:

  :: Gerekli özellikler

  :: İzin verilen özellikler

  :: Grup halinde bilgileri almak için kolay bir yol

- Kayıtlar çoklu object class içerebilirler

Özellikler (Attributes)

- Sahip olduğu alanlar:

  Name : tekil, büyük-küçük harf duyarlı değil
  Object Identifier (OID) : Aralarında nokta olan sayılar dizisi
  Attribute Syntax :
  Saklanabilecek veri özellikleri
  Kontrol ve Karşılaştırmalar nasıl yapılacak
  Tekil Değer(Single Value) veya Çoklu Değer(Multiple Value)

Bazı Attribute'lar (bkz: RFC 2256)

- uid -- User id
- cn -- Common Name
- sn -- Surname
- l -- Location
- ou -- Organisational Unit
- o -- Organisation
- dc -- Domain Component
- st -- State
- c -- Country

LDAP Search İşlemi

- Arama işlemi sonucu dönecek veriyi tanımlamak
- Base dn = arama işleminin başlayacağı yer
- Standartlar

  RFC 1960: LDAP String Representation of Search Filters
  RFC 2254: LDAPv3 Search Filters
- Operators

  & = and
  | = or
  ! = not
  ~= = approx equal
  >= = greater than or equal
  <= = less than or equal
  * = any

LDAP Search İşlemi devam...

- Örnek:

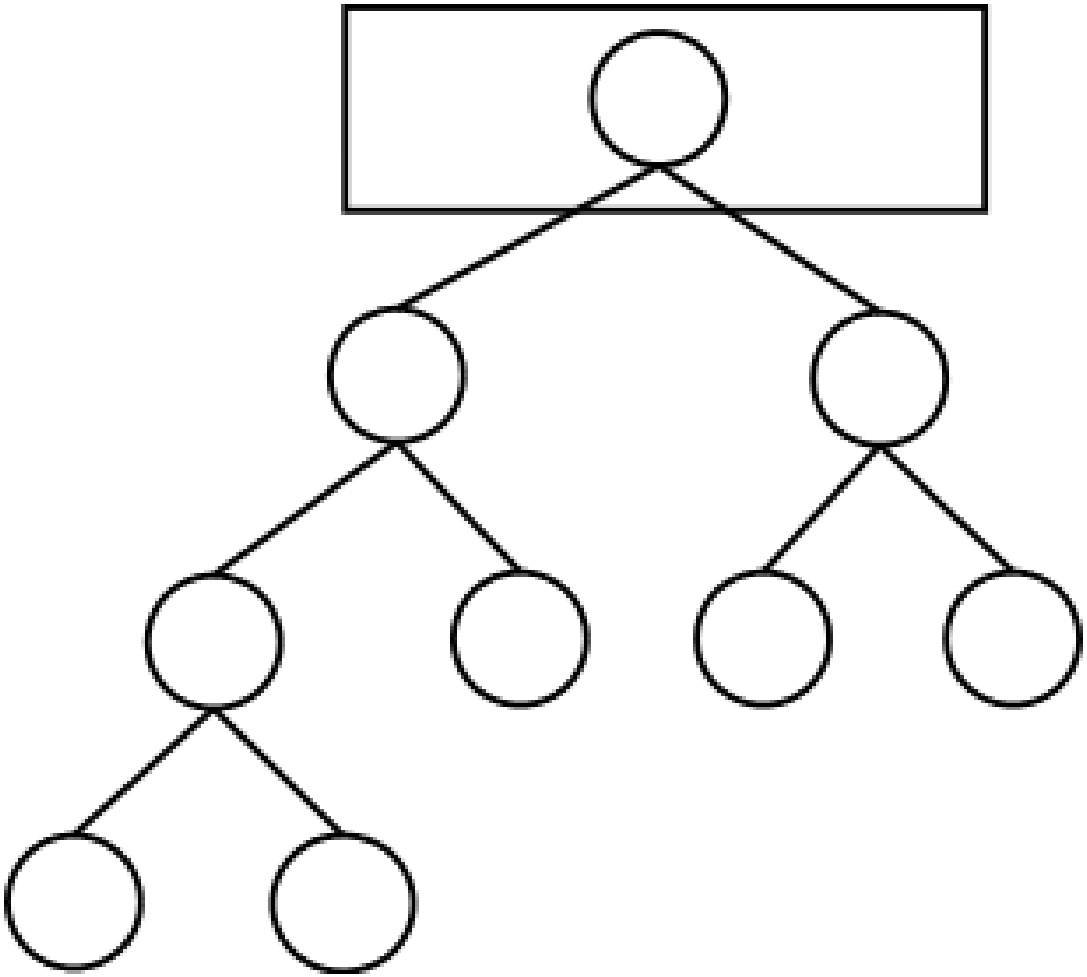
  (objectclass=posixAccount)

  (cn=Erhan E*)

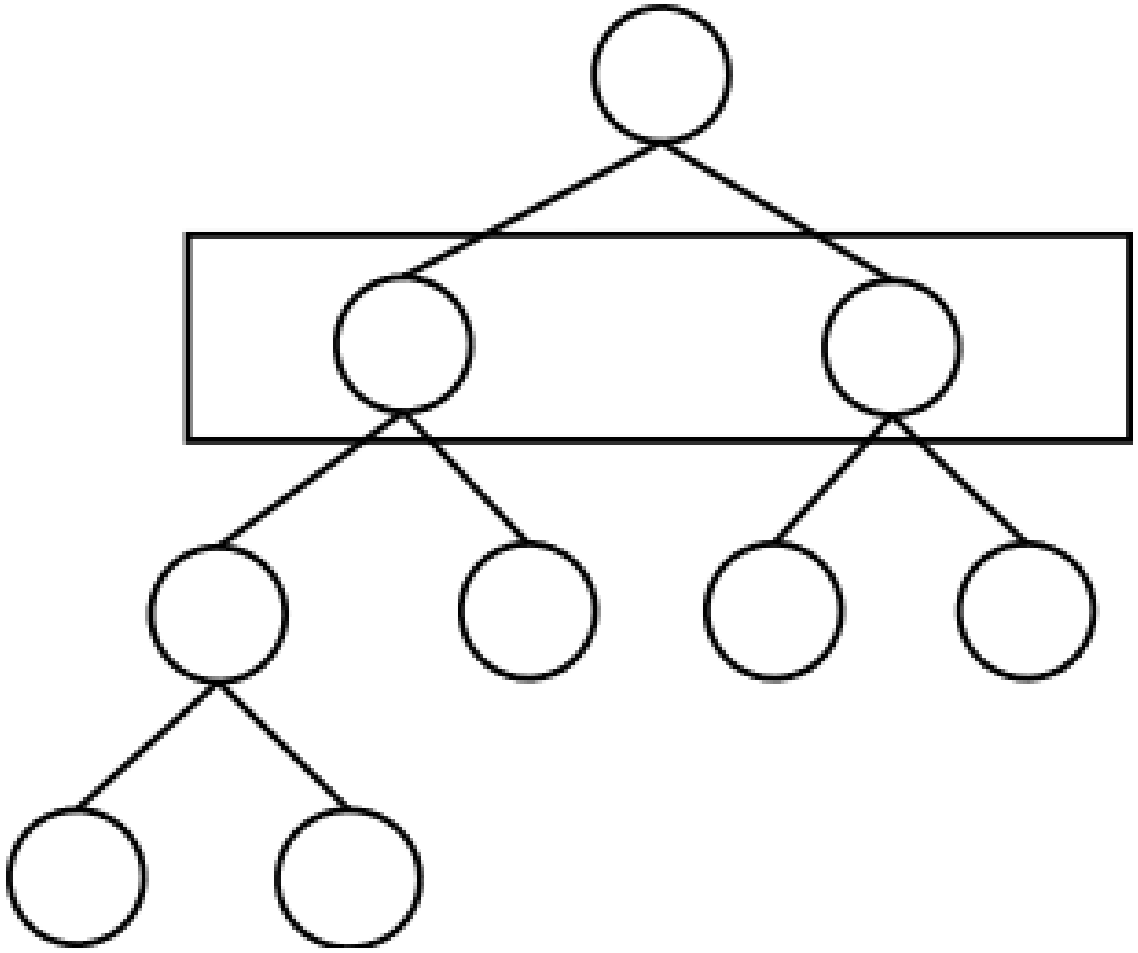
  (|(uid=galileo)(uid=kepler))

  (&(|(uid=galileo)(uid=kepler))(objectclass=posixAccount))

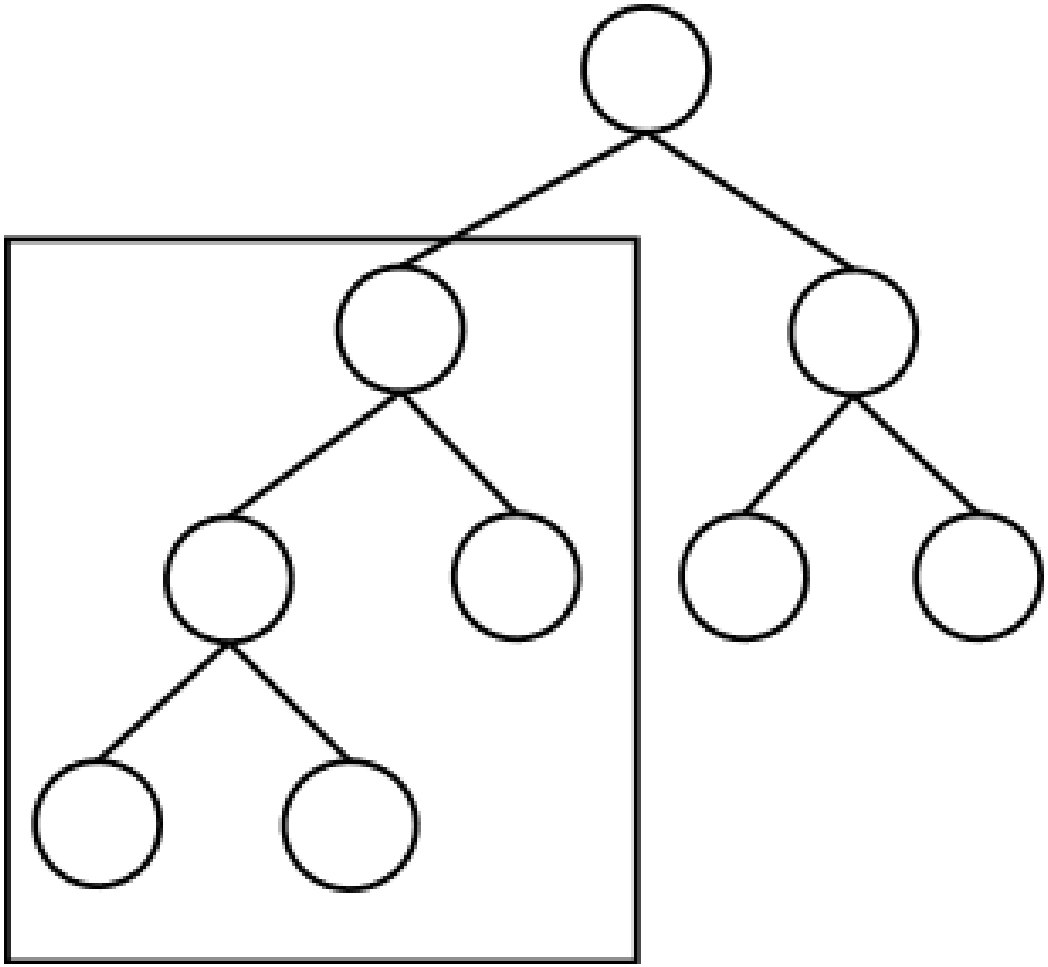
Search Base Scope



Search One Level Scope



Search Subtree Scope



LDAP Komut Satırı Araçları

- ldapadd, ldapmodify

  Kayıt girmek / Düzenlemek

  $ ldapmodify -r -D 'cn=foo,dc=bar,dc=com' -W < /tmp/user.ldif

- ldapdelete

  Kayıt Silmek

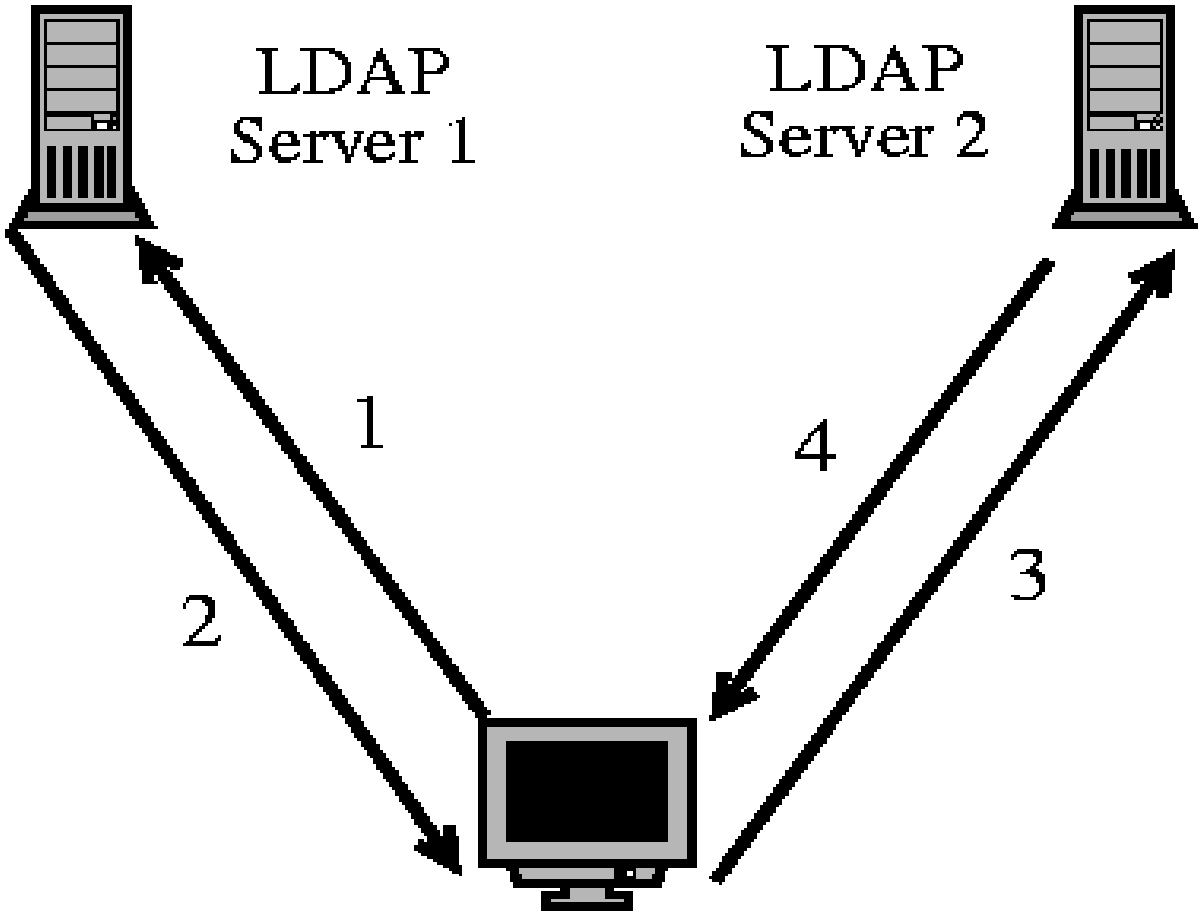
  $ ldapdelete -D 'cn=foo,dc=bar,dc=com' -W 'cn=user,dc=bar,dc=com'

- ldapsearch

  LDAP Sunucuda Arama Yapmak

  $ ldapsearch -L -D 'cn=foo,dc=bar,dc=com' 'objectclass=posixAccount'

Yönlendirme (Referral)



Uygulamalı OpenLDAP Kurulumu

- Planlama
- Yazılım : www.openldap.org
- Kurulum : openldap, dbm , vs..
- slapd.conf
- slurpd.conf
- Test....

Dağıtık LDAP Mimarileri

- Yansılanan Sunucular (Replicated Servers)
- Bölümlenmiş Sunucular (Partitioned Servers)
- Karışık Sunucular (Partitioned & Replicated Servers)

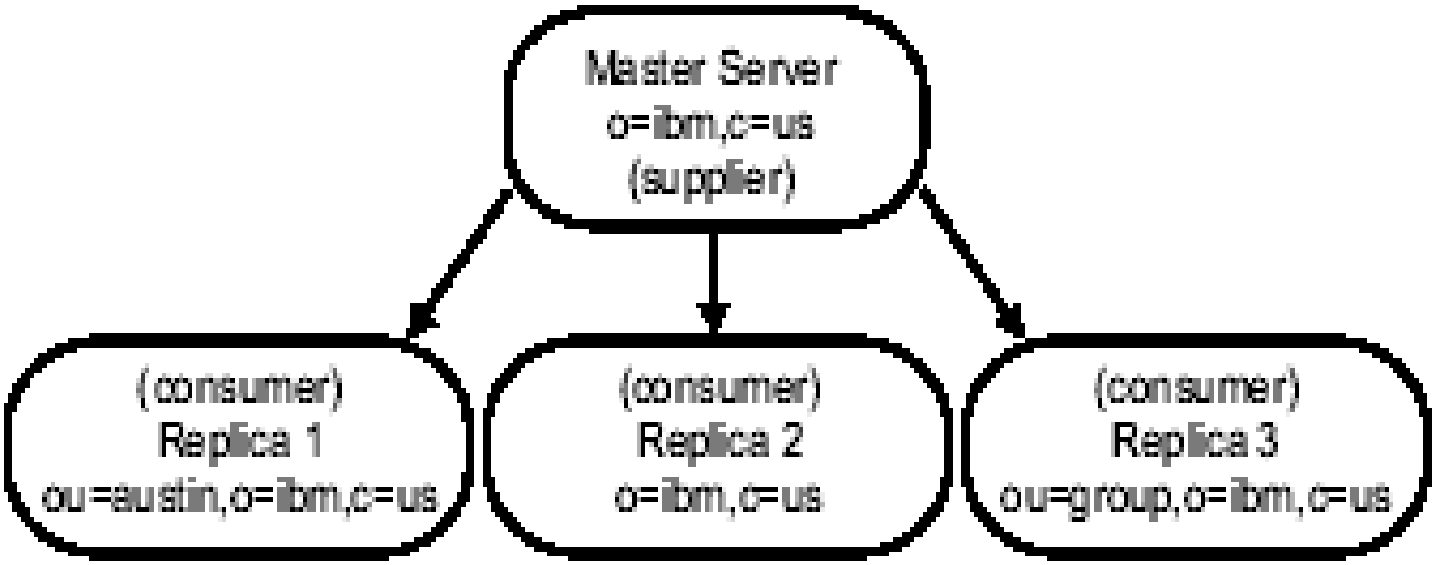
REPLICA : Bir sunucudaki verilerin aynen başka sunucuya aktarılması işlemi “replication”, aktarılan sunucu “replication” sunucu

Yansılanmış Sunucular (Replicated Servers)

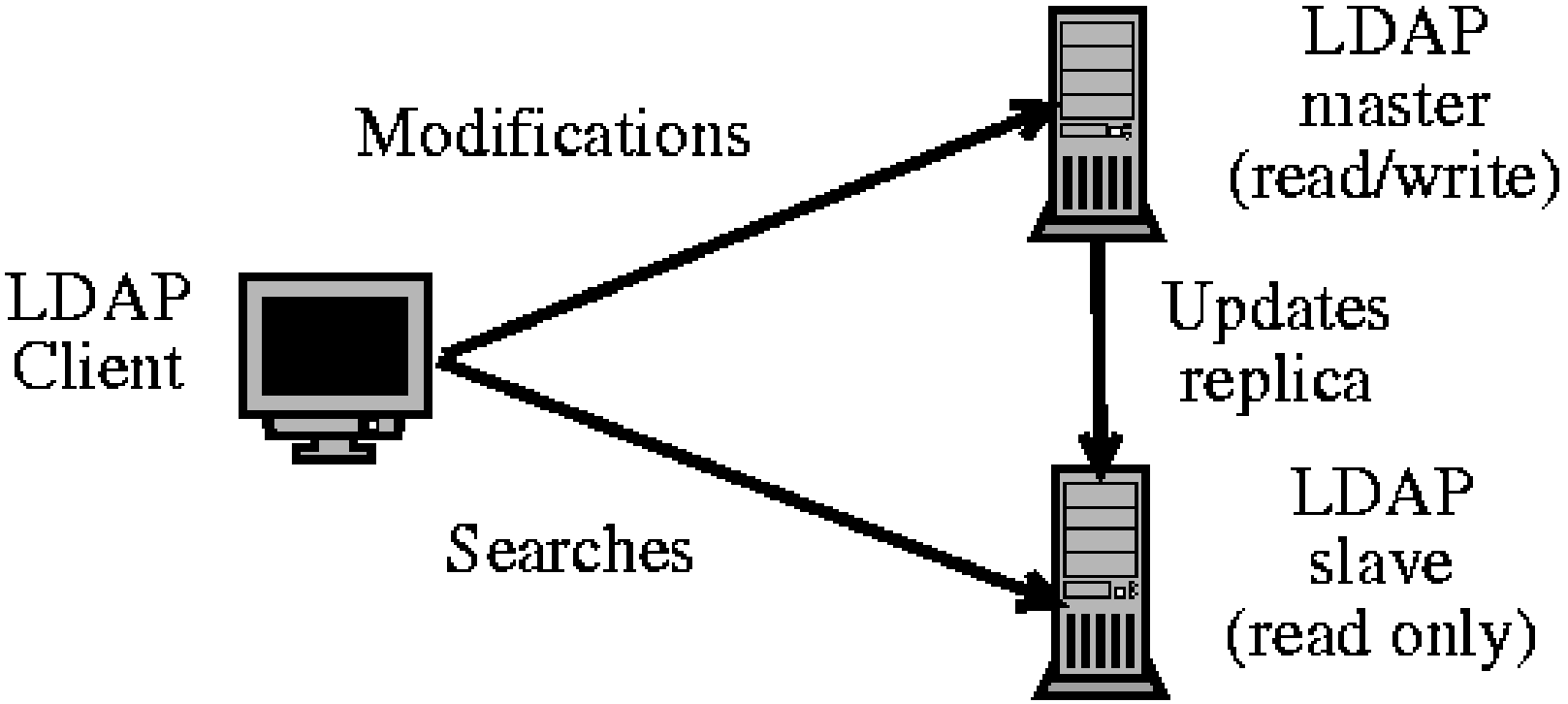
- Faydaları :

  Güvenilirlik (Reliability)
  Bulunurluk (Availability)
  Performans
  Hız
- Geçici uyumsuzluklar olabilir (master ve replica arasında)
- Single Point of Failure olmaz
- İstemcilere yakın noktalarda yansılanmış(replica) sunucular bulunmalı

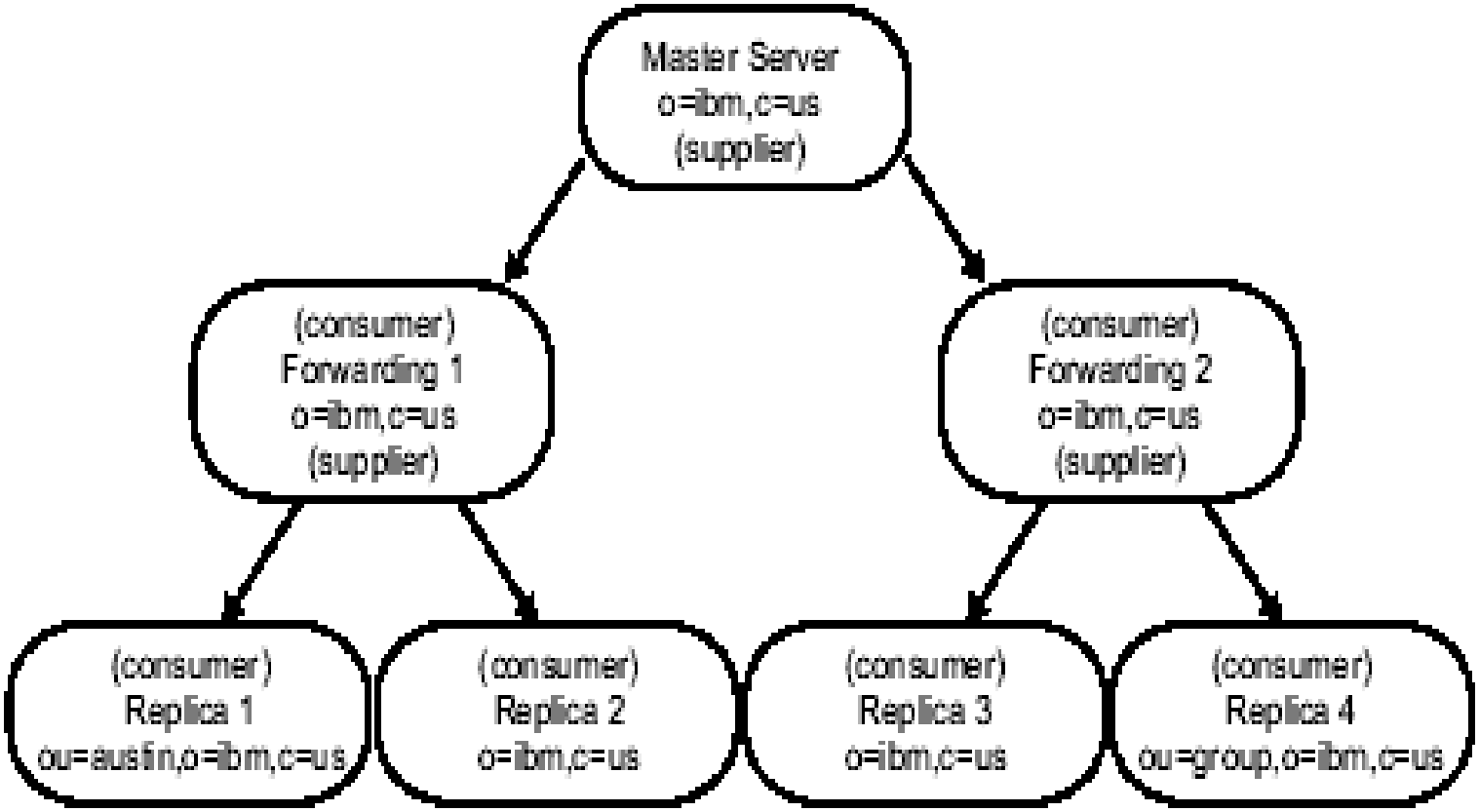
Yansılama Şeması (Replication Figure)



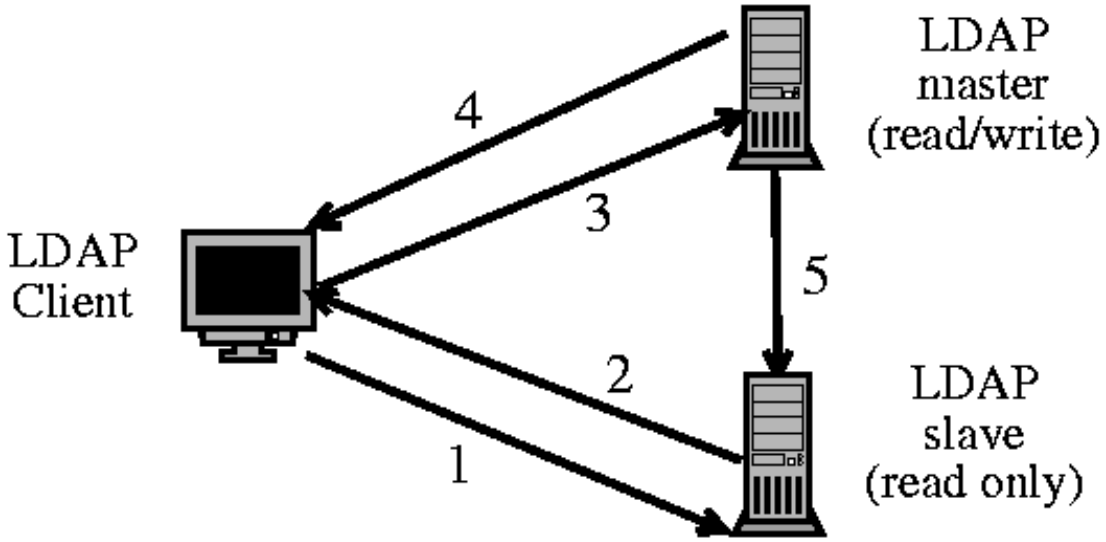
Yansılama Şeması (Replication Figure)



Ardışıl Replication

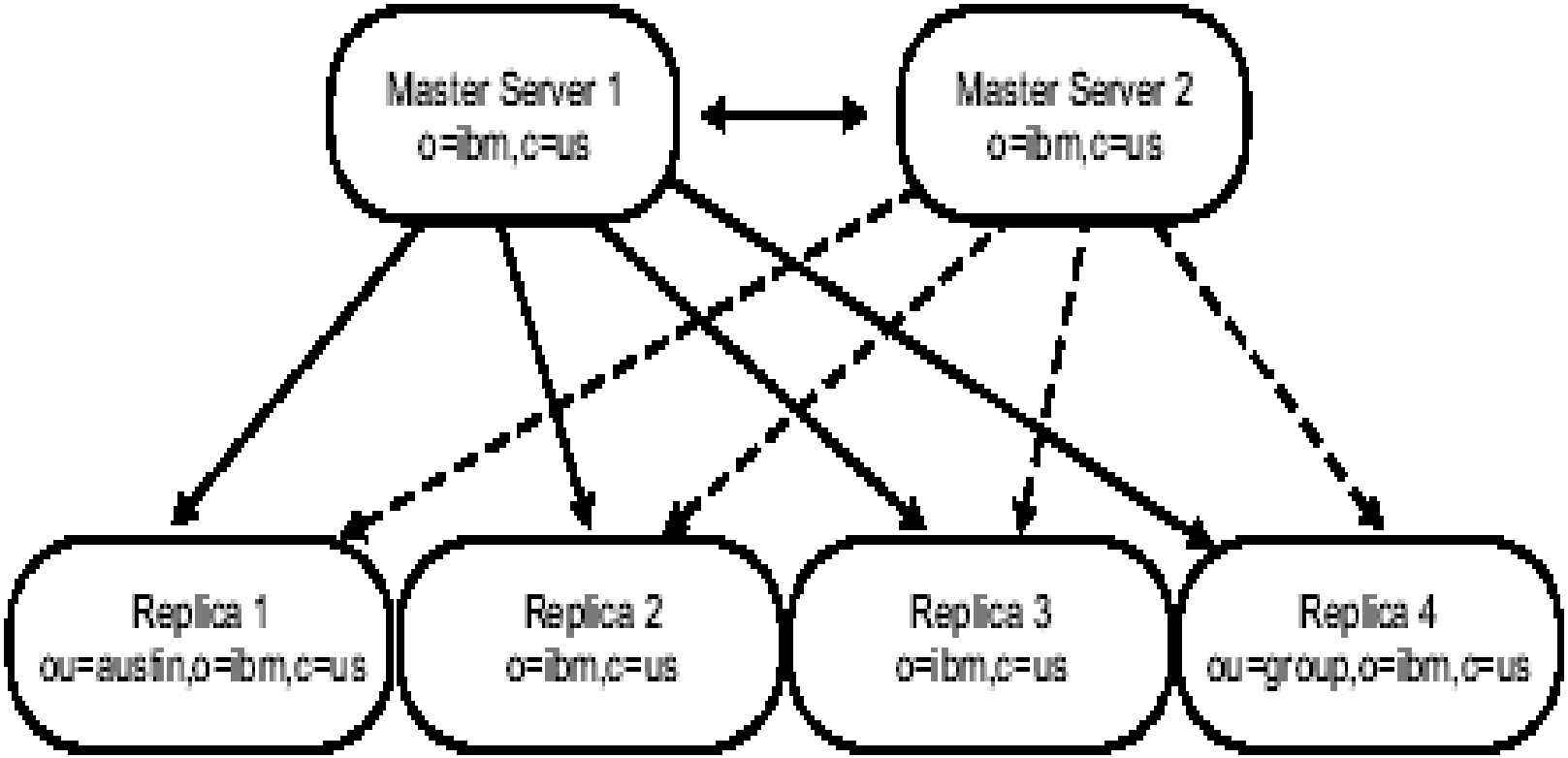


Yansılama & Yönlendirme

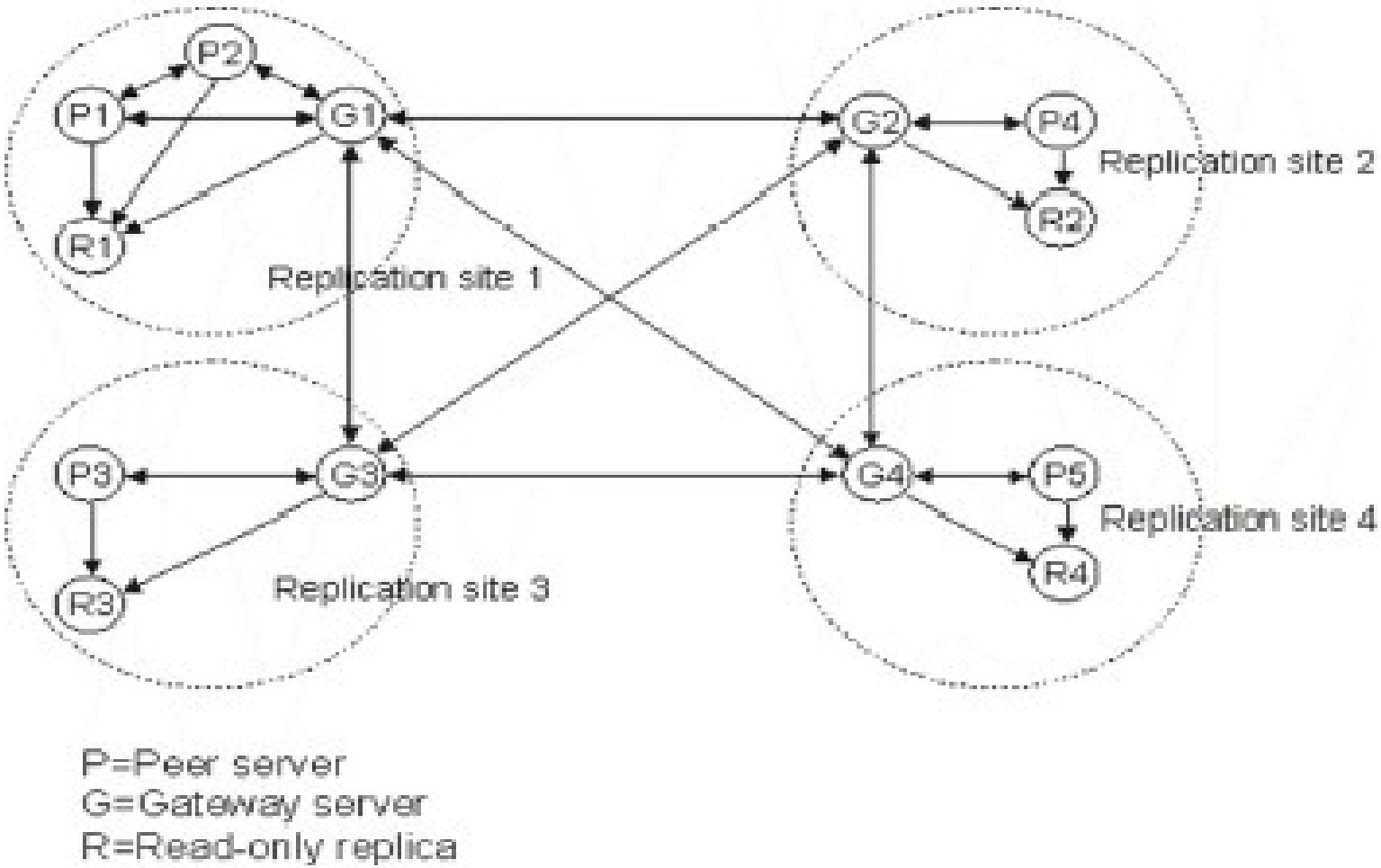


1 - İstemci değişiklik isteğini replicaya gönderir
2 - Replica istemciye master sunucuyu refer eder
3 - İstemci değişiklik isteğini tekrardan master sunucuya gönderir
4 - Master sunucu sonucu istemciye gönderir
5 - Master son değişiklikler ile replicayı günceller

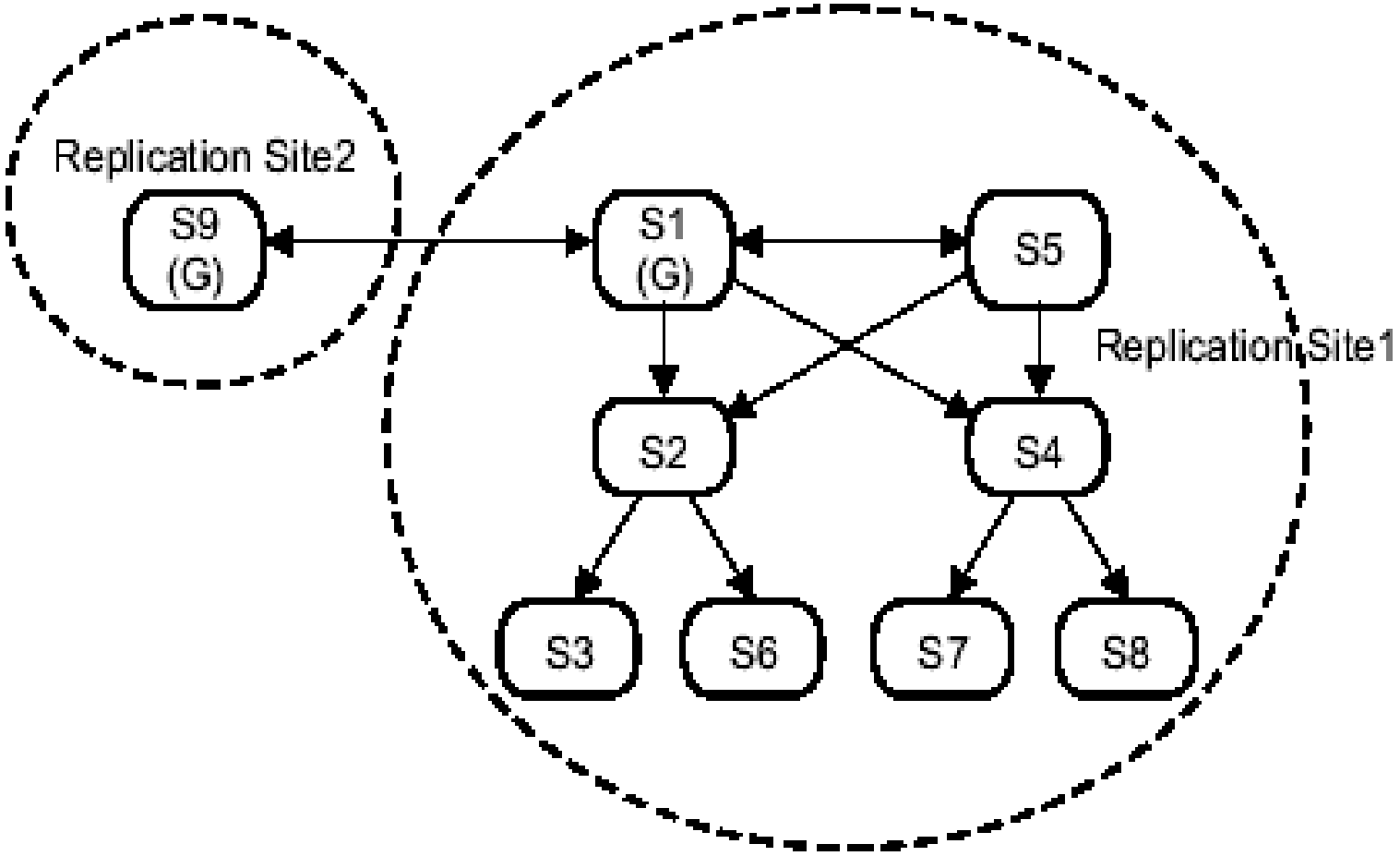
Peer to Peer Replication



Gateway Replication



Replication Site Kavramı



LDAP Uygulama Geliştirme

- C ile LDAP Uygulamaları (LDAP C API)
- Java ile LDAP Uygulamaları (JNDI)
- Python ile LDAP Uygulamaları
- PHP ile LDAP Uygulamaları
- Perl ile LDAP Uygulamaları geliştirilebilir.

LDAP C API

- /* ldapdelete.c - simple program to delete an entry using LDAP */

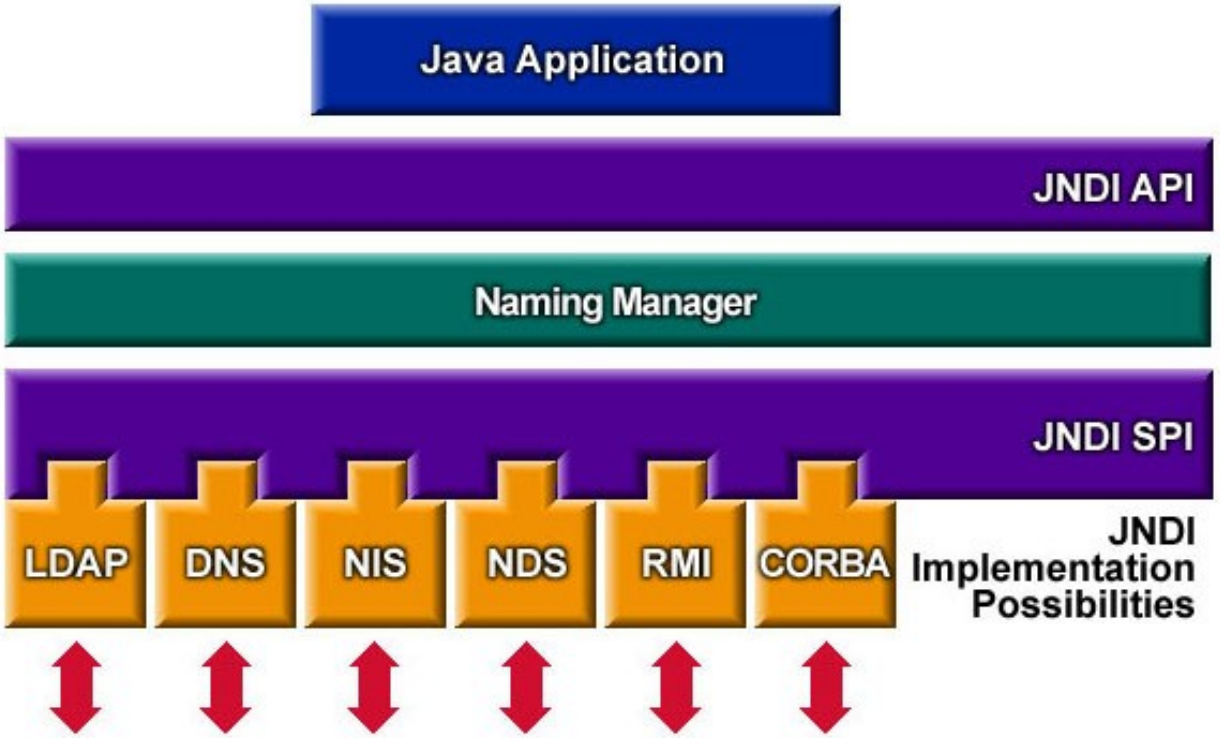
- #include <stdio.h>
- #include <string.h>
- #include <stdlib.h>
- #include <ctype.h>
- #include <ldap.h>
- #include <ldif.h>

- #ifdef LDAP_SSL_MAX
- #include <ldapssl.h>
- #endif
- .....
- .....

LDAP C API ile ilgili bilgi kullanılan LDAP sunucunun dokümantasyonunda bulunabilir.

Java ile LDAP Uygulamaları (JNDI)

- Java Naming and Directory Interface
- Java ile yazılan uygulamalar için Naming ve Directory API



Python ile LDAP Uygulamaları

- Python-Ldap modülü
  http://python-ldap.sourceforge.net

- LDAP C API → Wrappers → Python-ldap

```
>>> import ldap

>>> l = ldap.initialize("ldap://my-ldap-server.my-domain:389")

>>> l.simple_bind_s("","")

>>> l.search_s("o=My Organisation, c=AU", ldap.SCOPE_SUBTREE,
      "objectclass=*")
```

PHP ile LDAP Uygulamaları (OpenLDAP)

```
<?php

echo "Connecting ...";
$ds=ldap_connect("localhost");  // must be a valid LDAP server!

if ($ds) {
   echo "Binding ...";
   $r=ldap_bind($ds);
   echo "Bind result is " . $r . "<br />";

   $sr=ldap_search($ds, "o=My Company, c=US", "sn=S*");
   echo "Search result is " . $sr . "<br />";

   echo "Getting entries ...<p>";
   $info = ldap_get_entries($ds, $sr);
   echo "Data for " . $info["count"] . " items returned:<p>";

   for ($i=0; $i<$info["count"]; $i++) {
       echo "dn is: " . $info[$i]["dn"] . "<br />";
       echo "first cn entry is: " . $info[$i]["cn"][0] . "<br />";
       echo "first email entry is: " . $info[$i]["mail"][0] . "<br /><hr />";
   }

   echo "Closing connection";
   ldap_close($ds);

} else {
   echo "<h4>Unable to connect to LDAP server</h4>";
}
?>
```

Perl ile LDAP Uygulamaları

```
#!/usr/bin/perl -w

use strict;
use Net::LDAP;

my($ldap) = Net::LDAP->new('ldap.test.com') or die "Can't bind to ldap: $!\n";


$ldap->bind;

my($mesg) = $ldap->search( base => "dc=pisoftware,dc=com", filter =>
'(objectclass=*)');

$mesg->code && die $mesg->error; my($entry);

map { $_->dump }

$mesg->all_entries;

$ldap->unbind;
```

LDAP Sunucuları

- Slapd

  University of Michigan
  Openldap

- IBM Tivoli Directory Server
- Netscape Directory Server
- Microsoft Active Directory (AD)
- Novell Directory Services (NDS)
- Sun Directory Services (SDS)
- Lucent's Internet Directory Server (IDS)

Sorular