

Autenticazione con LDAP

Uso del protocollo LDAP per l'autenticazione
in rete

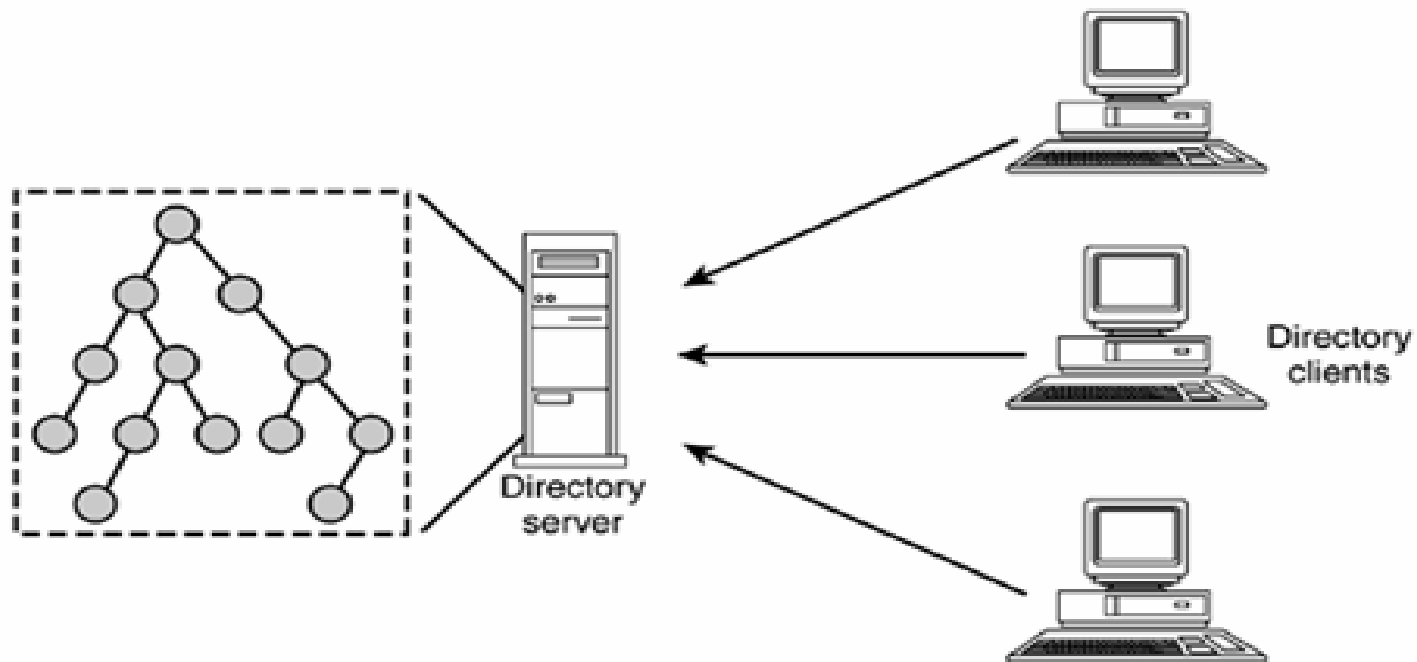
ing. Walter Vendraminetto - vendra@sci.univr.it

15.06.2007

Directory

- Il concetto di Directory è essenzialmente quello di catalogo consultabile
 - Pagine gialle
 - Listino prezzi
 - Guida TVSono esempi di Directory off-line
- Esiste il concetto di Directory *on-line*, che estende il significato comune con delle caratteristiche:
 - *Dinamicità dei contenuti nel tempo*
 - *Flessibilità dei tipi di dati e loro organizzazione*
 - *Sicurezza sugli accessi*
 - *Personalizzazione dei contenuti*Ad esempio:
 - *Application oriented Directories (Address book)*
 - *Network Operating System Directories (AD, NIS)*
 - *Purpose specific directories (DNS)*
 - *General purpose dirs based on standards*

Directory

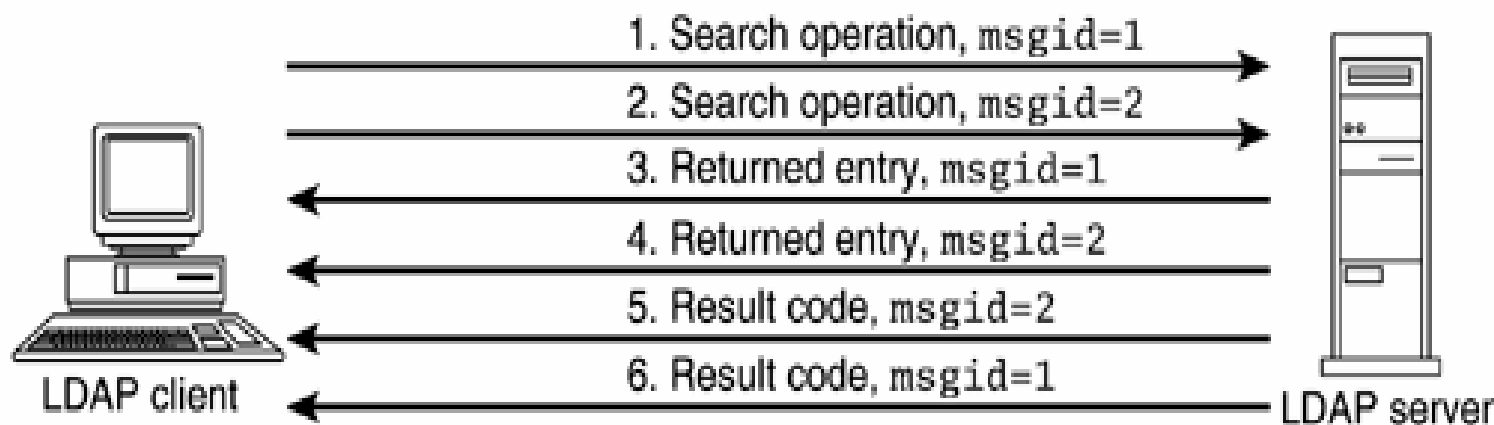


Cos'è LDAP

- LDAP racchiude un serie di elementi:
 - Il protocollo *message-oriented* con un insieme di 9 operazioni predefinite.
 - E' derivato dallo standard X.500 che implementa l'intero stack ISO-OSI. LDAP è Light perché si colloca subito sopra al TCP
 - I 4 modelli che descrivono I dati (information model), i nomi (naming model), le funzioni (functional model) e la sicurezza (security model) di una directory.
 - Il fomato LDIF dei files di scambio tra directory
 - Il server software
 - Le applicazioni di utilità da linea di comando
 - Una LDAP API per la creazione di applicazioni che utilizzano la Directory

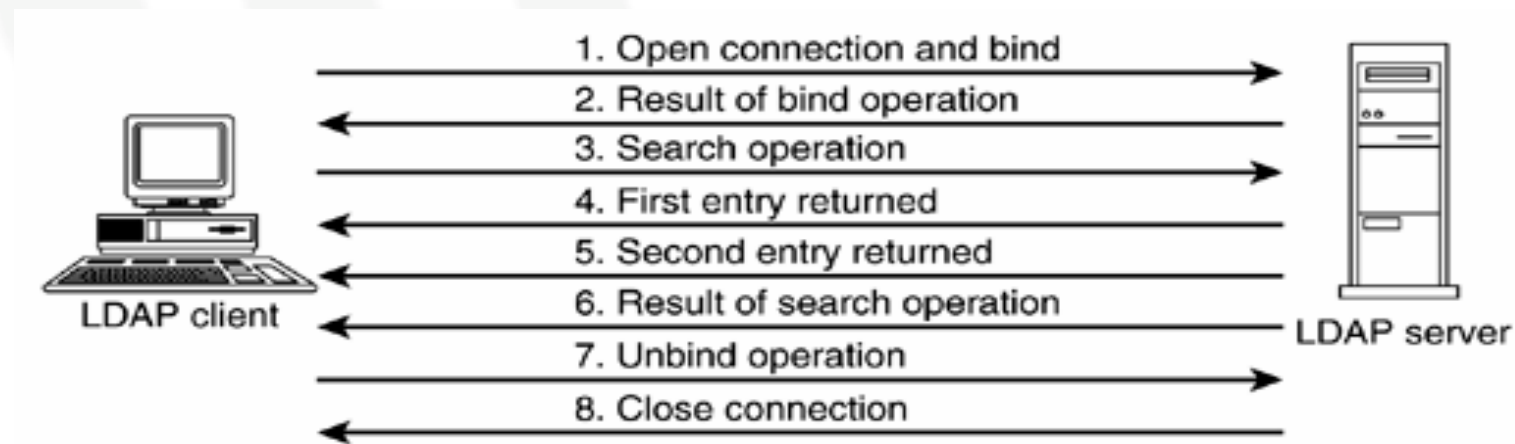
Protocollo message-oriented

- Il client crea una o più richieste concorrenti con *message ID* diversi
- Le possibili operazioni sono: interrogazioni (search, compare), aggiornamento (add, delete, modify, modify DN), autenticazione e controllo (bind, unbind e abandon)
- Il server risponde con un codice di terminazione (*result code*) ad indicare l'esito dell'operazione ed eventuali dati richiesti (*entries*)



Protocollo message-oriented

- Tipica interazione client-server:



Protocollo message-oriented

- Estensioni al protocollo LDAP:
 - LDAP extended operations: l'utente può definire nuove operazioni senza intervenire sul protocollo. L'operazione *startTLS* ne è un esempio
 - LDAP controls: il comportamento di operazioni standard può essere alterato tramite l'invio di controlli aggiuntivi. Ad esempio l'intenzione di accedere a metadati nelle operazioni è indicata al server tramite l'invio di un apposito controllo
 - Simple Authentication and Security Layer (SASL): il protocollo può far uso di questa struttura di sicurezza che dà flessibilità nella scelta del meccanismo di autenticazione

Modelli LDAP

- Il documento RFC 2251 describe LDAP definendo due modelli: uno per il *protocollo* e uno per i *dati*.
- In letteratura è facile trovare una descrizione di LDAP basata su quattro livelli:
 - **Information**: 'entry' come elemento base con un set definito di attributi
 - **Naming**: ogni entry è identificata dal suo DN (Distinguish Name)
 - **Functional**: il protocollo consente le operazioni di accesso e gestione dei dati
 - **Security**: le specifiche del protocollo definiscono anche le modalità di autenticazione e autorizzazione (acl)

Information Model

- Il modello delle informazioni descrive i dati che sono immagazzinati nella Directory
 - **Entry**: elemento fondamentale delle informazioni, rappresentazione degli oggetti come *persone*, *utenti*, *certificati* ecc
 - **Attributi e valori**: una entry è costituita da un insieme di attributi e relativi valori.
 - **Schemas**: sono assimilabili a metadati. Definiscono le caratteristiche degli attributi e le classi di oggetti (objectClass)
 - **attributeType**
 - Sintassi e ricorrenza (-> single or multiple)
 - Matching rules
 - Sorting rules
 - **objectClass**
 - Ereditarietà tra classi di oggetti
 - Attributi obbligatori e facoltativi

Information Model (schemas = metadati)

```
attributetype ( 1.1.2.2.1.11 NAME 'univrIDStruttura'
  DESC 'Identificativo della facoltà principale alla quale un utente afferisce'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

•
•
•
•

SCHEMA

```
objectclass ( 1.1.2.2.4 NAME 'univrUser'
  DESC 'User at University of Verona' SUP top AUXILIARY
  MUST (uid $ gn $ sn $ univrUserStatus $ univrIDStruttura)
  MAY (univrIDAltraStruttura $ univrIDCorso $ univrIDIndirizzo $
    univrAnnoAccademico $ univrAnnoIscrizione $ univrIpQuotaMAX $
    univrID) )
```

•
•
•
•

Naming Model

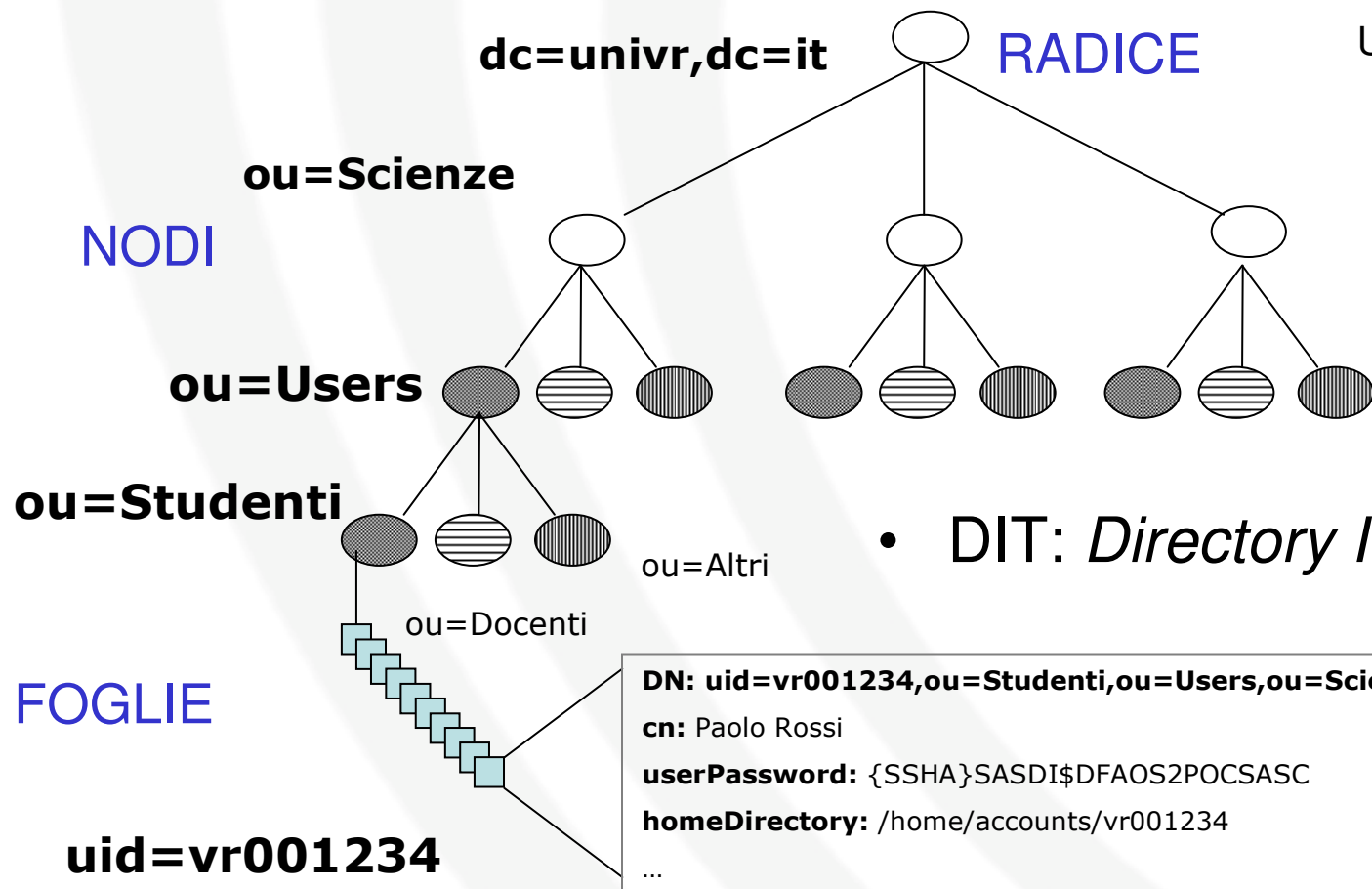
- Le entry della Directory sono organizzate ad albero.
- Esiste una entry per la radice (root) ed ogni altra entry può essere un nodo o una foglia dell'albero.
- Ogni entry è identificata *univocamente* dal suo **Distinguished Name (DN)** che consente il recupero delle informazioni ad essa associata.
- Il DN di una entry è relativo alla posizione della entry nella **struttura ad albero** che essa occupa. Il concetto è molto simile al *path* di un file nel filesystem Unix.
- Il DN di una entry è ottenuto per giustapposizione del DN del nodo padre e del suo **Relative Distinguished Name (RDN)**.
- E' l'utente/amministratore che definisce il DN di una entry

Esempio di DIT

DC = Domain Component

OU = Organizational Unit

UID = User ID



Functional Model

- Definisce le specifiche con cui realizzare le operazioni:
 - Interrogazioni
 - Base: sottoramo della Directory su cui effettuare una ricerca
 - Scope: quanto a fondo ricercare (sub, one, base)
 - Search filter: filtro di ricerca
 - Attributes to return: eventuali attributi da restituire all'utente
 - altri parametri funzionali
 - Aggiornamenti
 - DN dell'entry interessata
 - Parametri di modifica in base all'operazione
 - Vincoli (ad esempio il padre deve esistere per poter aggiungere un figlio, unicità DN, coerenza con gli schemi e autorizzazione)
 - Autenticazione e Controllo
 - Credenziali secondo il Security Model

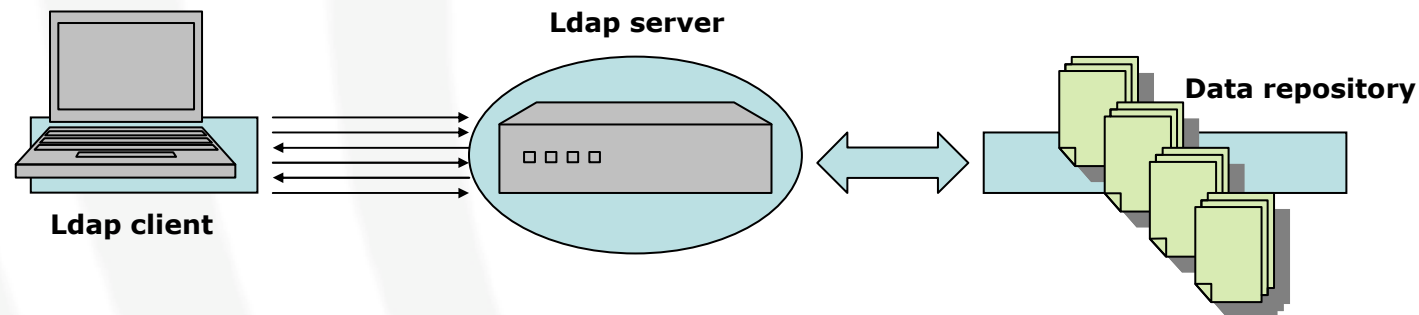
Security Model

- Il modello di sicurezza specifica i meccanismi di sicurezza per il protocollo
- **Autenticazione**: comporta l'invio della password *in chiaro* al server che la usa per verificare che corrisponda con la versione depositata
 - Accesso anonimo
 - Autenticazione semplice
 - Autenticazione tramite SASL
 - Autenticazione con Transport Layer Security
- Access Control List (ACL): direttive di configurazione che consentono di stabilire dei gradi di autorizzazione sui dati
- startTLS: operazione di richiesta al server per avere la crittografia a livello di sessione, per autenticare le due parti ed integrità dei dati

LDAP Data Interchange Format (LDIF)

- Per la rappresentazione dei dati il formato standard è il formato LDIF
- Esiste una definizione per le entry, utile per quando si effettuano delle importazioni verso la Directory, quando si visualizzano a console i risultati delle ricerche e quando si vuole archiviare (back-up).
- Esiste un formato per le modifiche per quando si effettuano degli aggiornamenti.
- La replica verso Directory slave si avvale di questo formato per notificare le modifiche

Server Software: Openldap



Un servizio basato su LDAP è costituito da un front-end e da un back-end.

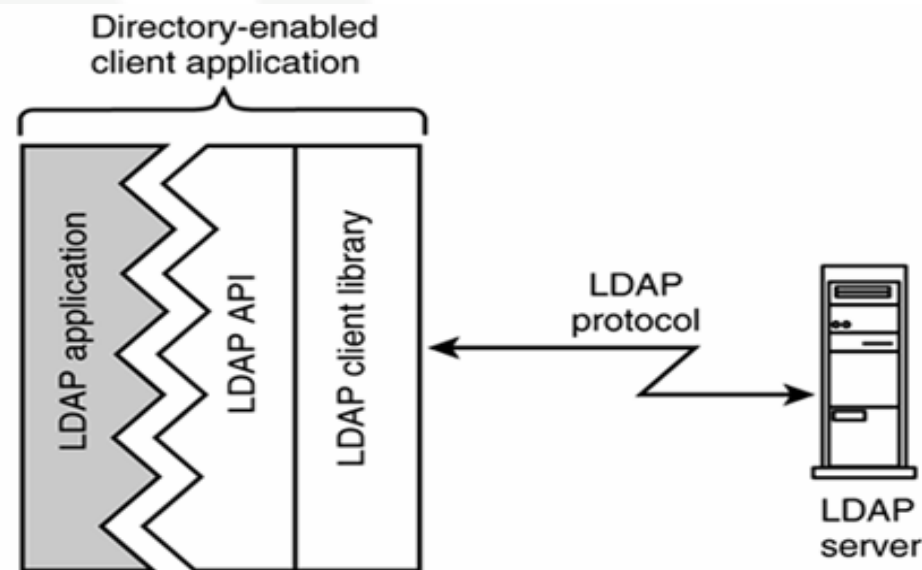
- Il **front-end** è il protocollo di scambio informazioni tra il client ed il server
- Il **back-end** è la parte di interazione con il repository delle informazioni. Questo può essere della più varia natura: da un semplice file di testo ad un complesso database relazionale

Utilità da linea di comando

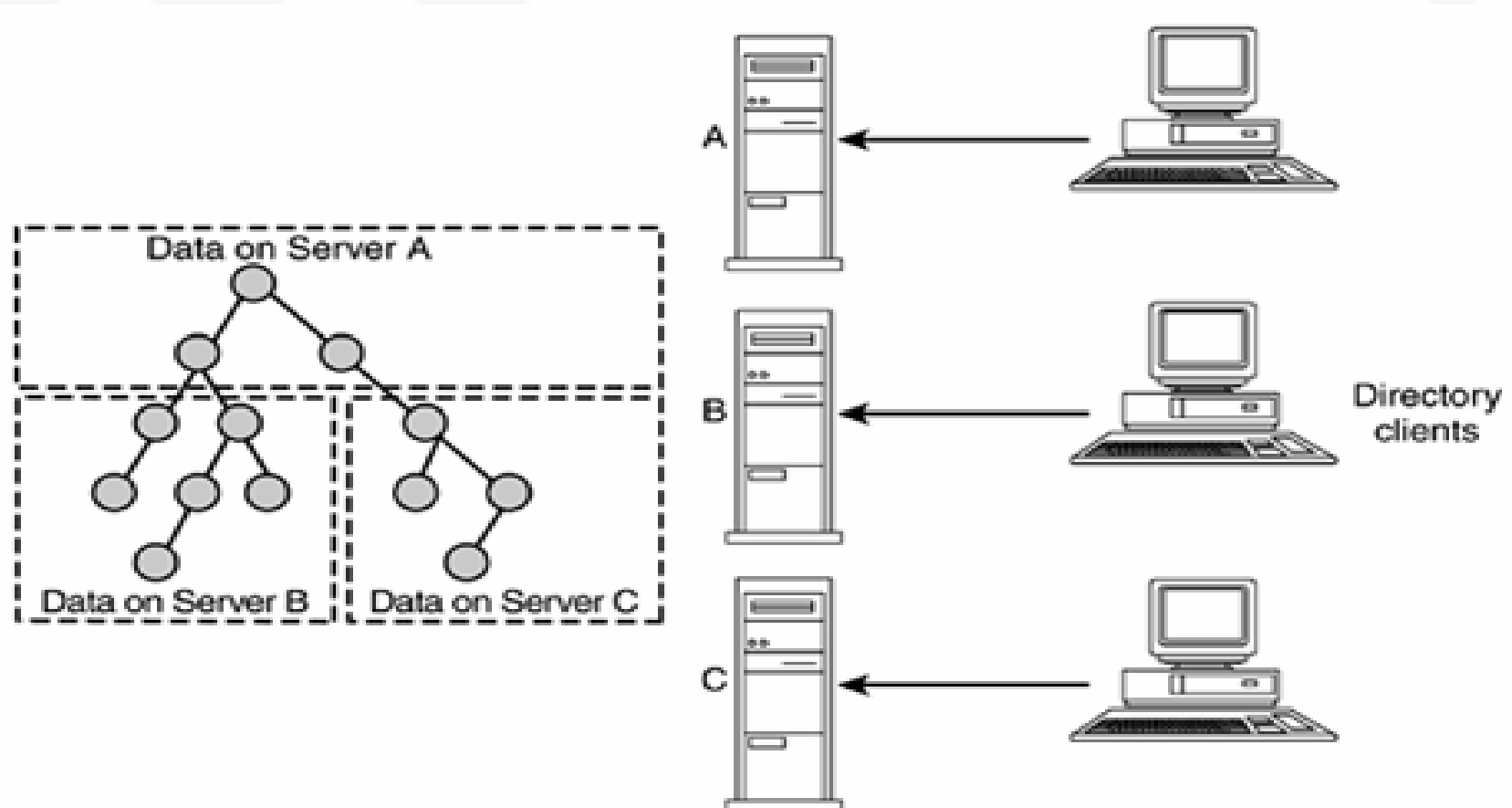
- Usualmente con il server software sono forniti degli strumenti di utilità da riga di comando intesi come strumenti minimi per la gestione dei contenuti e delle operazioni con la directory
- Con OpenLDAP questi sono:
 - `Ldapsearch/compare`
 - `Ldapadd/modify/delete`
 - `Slapcat`
 - `Slapadd`
 - `Slapindex`
 - .. altri

LDAP API

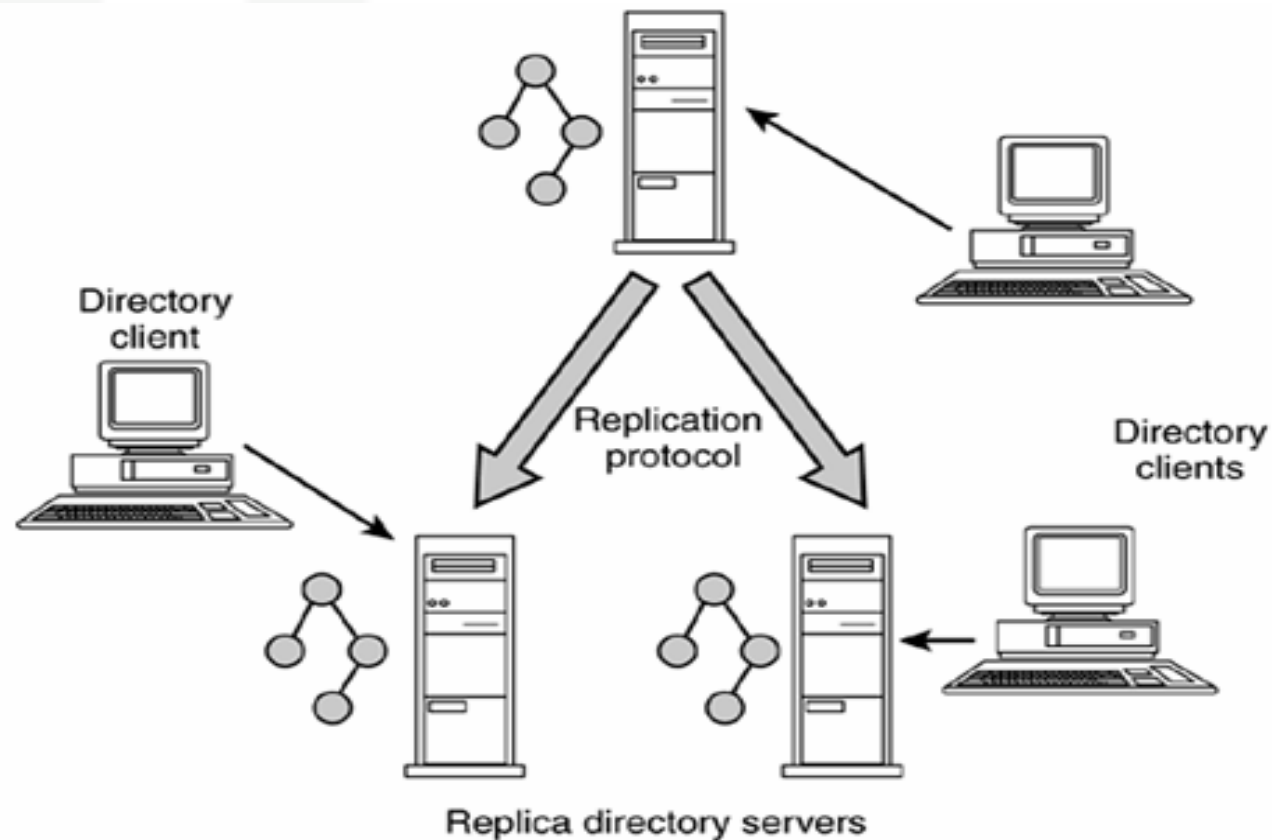
- Esistono diverse Application Program Interface (API) che consentono di realizzare applicazioni per accedere ed interrogare i dati di una Directory
- Un esempio è la versione di PERL utilizzata per gli applicativi di gestione delle informazioni nella Directory centralizzata di ateneo.



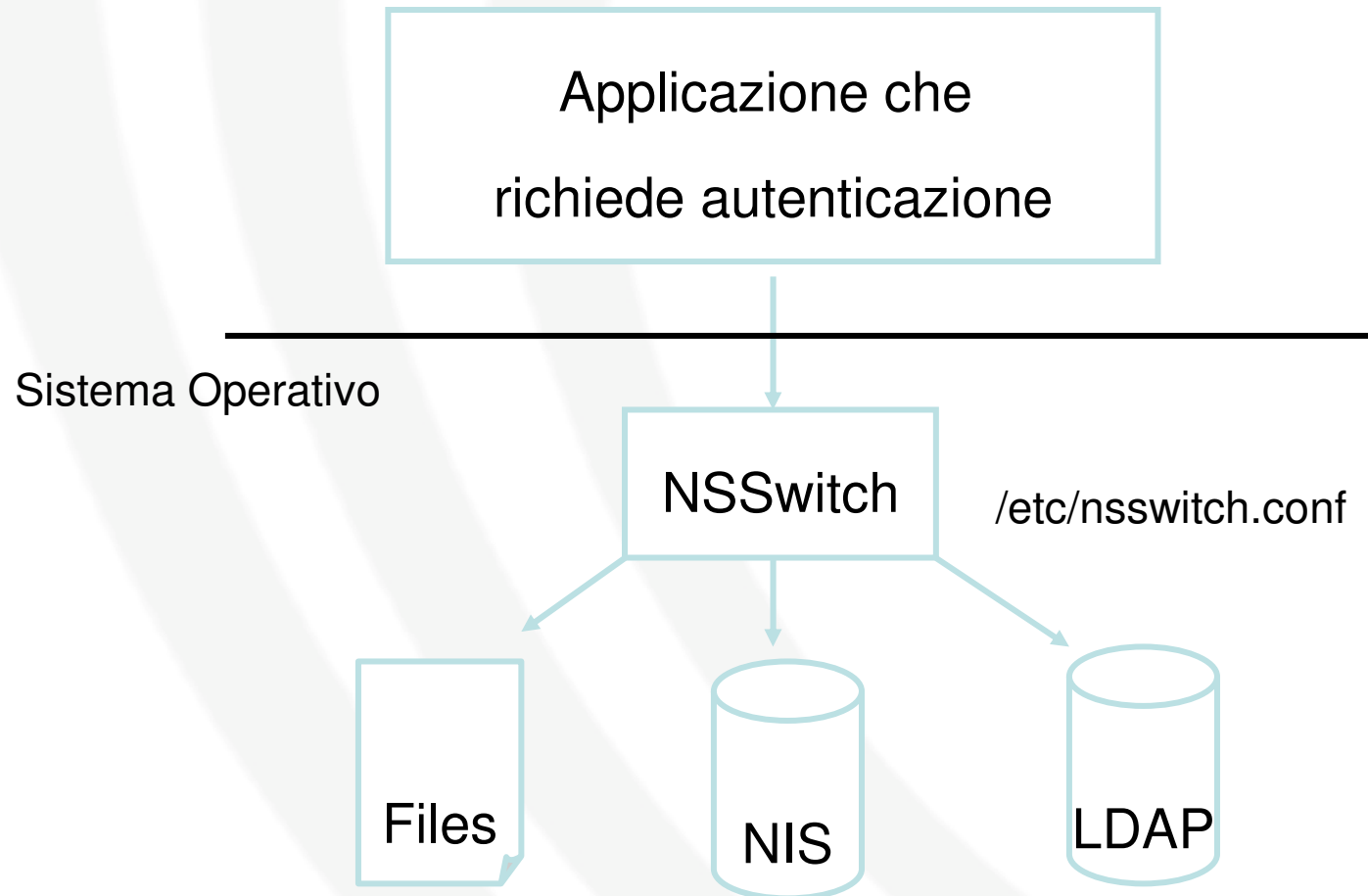
Directory Distribuita con *referral*



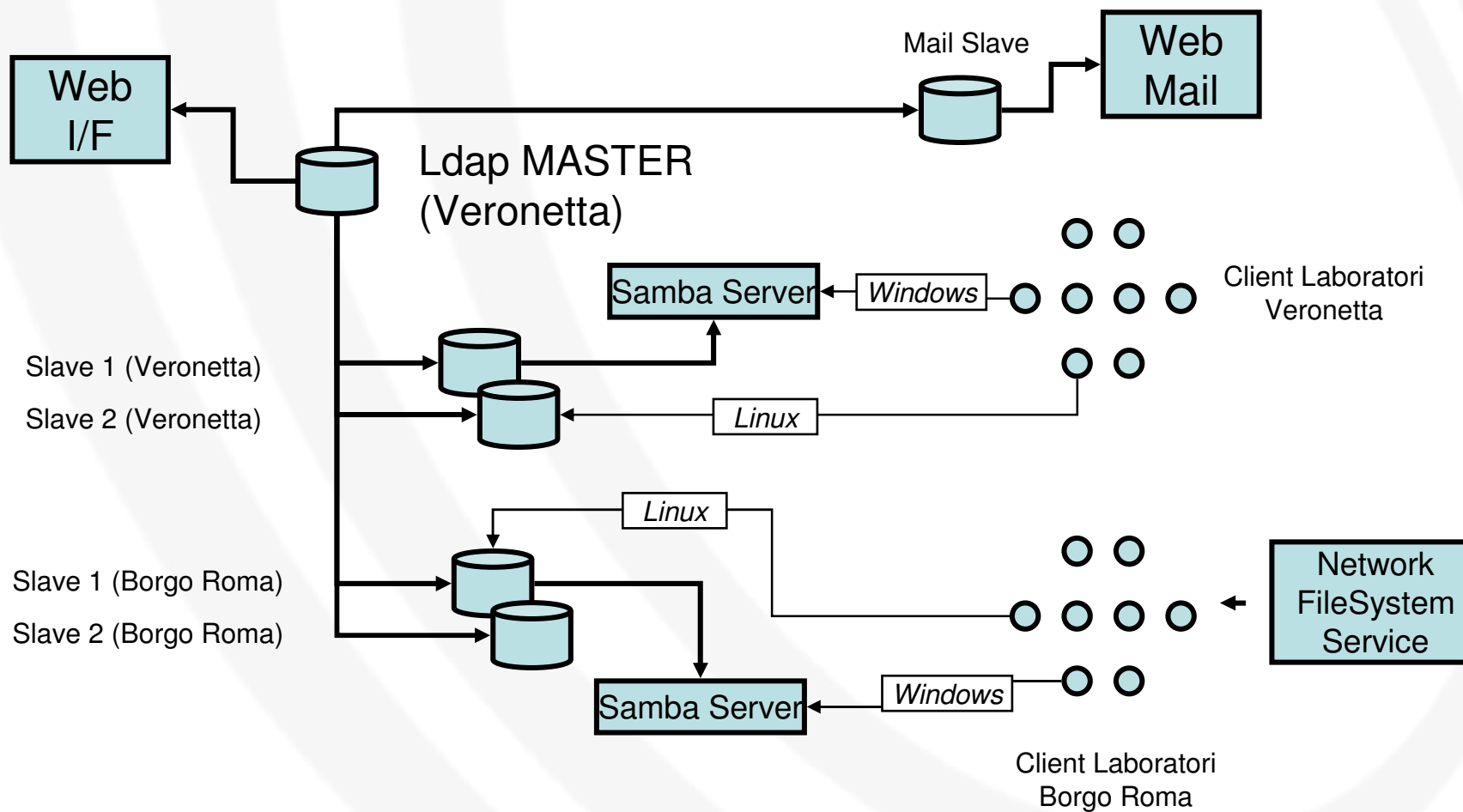
Directory replicata



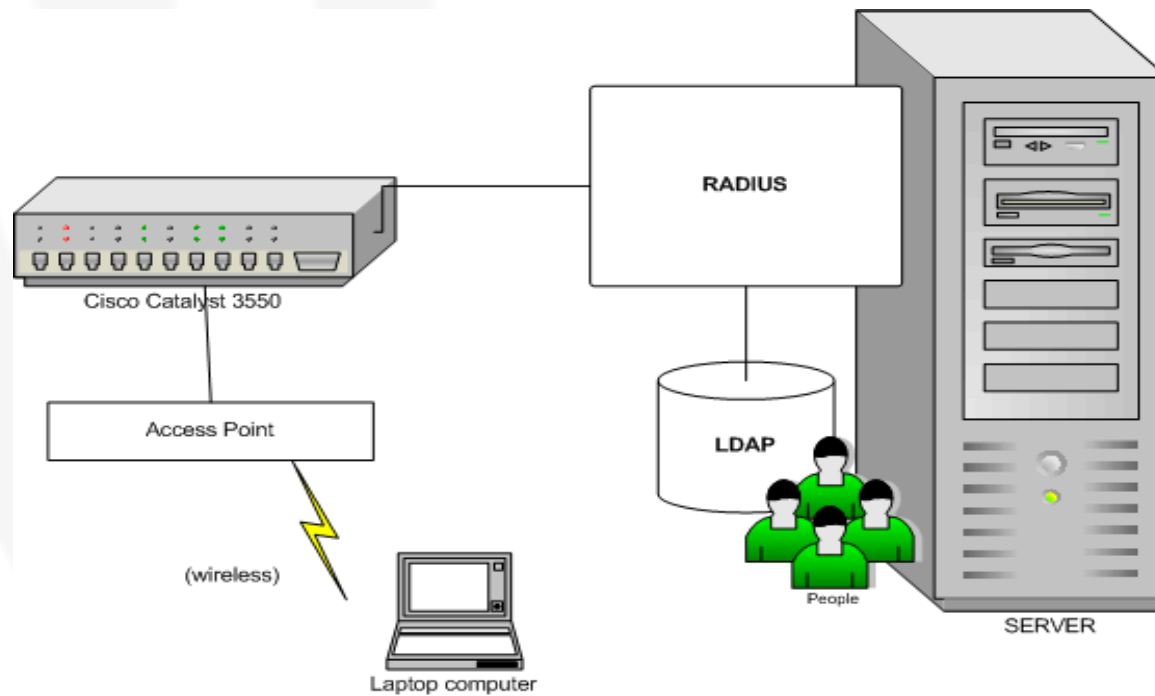
Modello di autenticazione UNIX



Architettura UNIVR



Architettura basata su RADIUS



Riferimenti

- Letteratura:
 - Understanding and Deploying LDAP Directory Services, 2nd Edition
Timothy A. Howes Ph.D., Mark C. Smith, Gordon S. Good
Addison Wesley – ISBN 0-672-32316-8
- Web:
 - OpenLDAP (www.openldap.org)
 - <http://en.tldp.org/HOWTO/LDAP-HOWTO/>
 - <http://www.ldapguru.com/>
 - LDAPBrowser
<http://www-unix.mcs.anl.gov/~gawor/ldap/>