University of Zurich

SWITCH Workshop - March 23, 2004

UniAccess

Directory Infrastructure

Luzian Scherrer <luzian.scherrer@id.unizh.ch> | IT-Services | +41 1 635 67 78

University of Zurich

UniAccess: Facts

- **43’000 Accounts**
  11’000 Employees and 32’000 Students

- **Offered Services**
  - Samba Homedirectory
  - Public Working Rooms (Windows, Mac)
  - Network Working Places (WLAN, Ethernet)
  - E-Mail
  - VPN Access
  - Protected Webresources (HTTP Proxy)
  - AAI Home-Organization

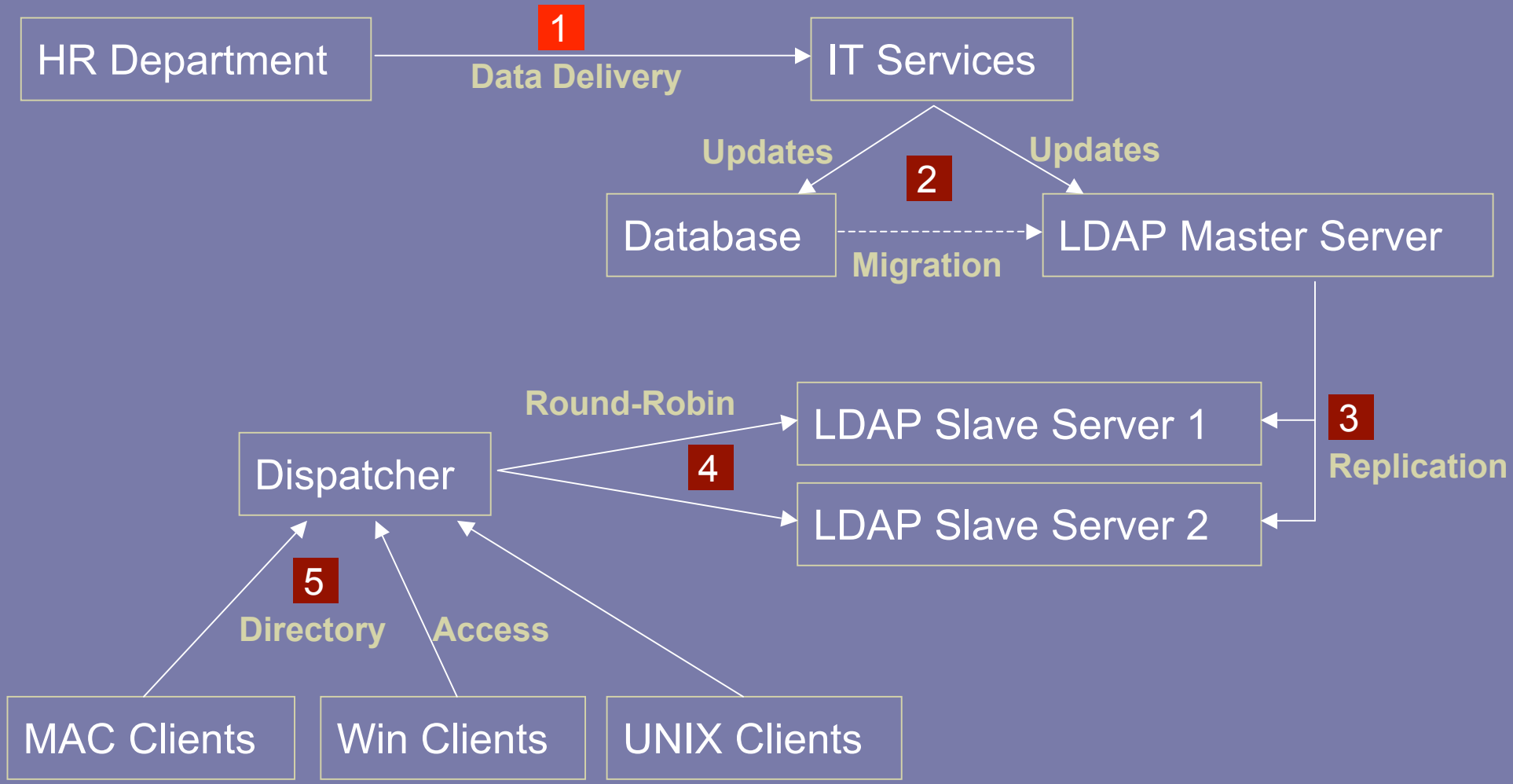
University of Zurich

User Directory: Requirements

- Based on open standards
- Open source
- Server infrastructure on Linux
- Client authentication for Windows, Mac, UNIX, Linux and other applications
- Reasonable price
- Redundancy
- Security
- Scaleable

University of Zurich

Infrastructure & Data-Flow



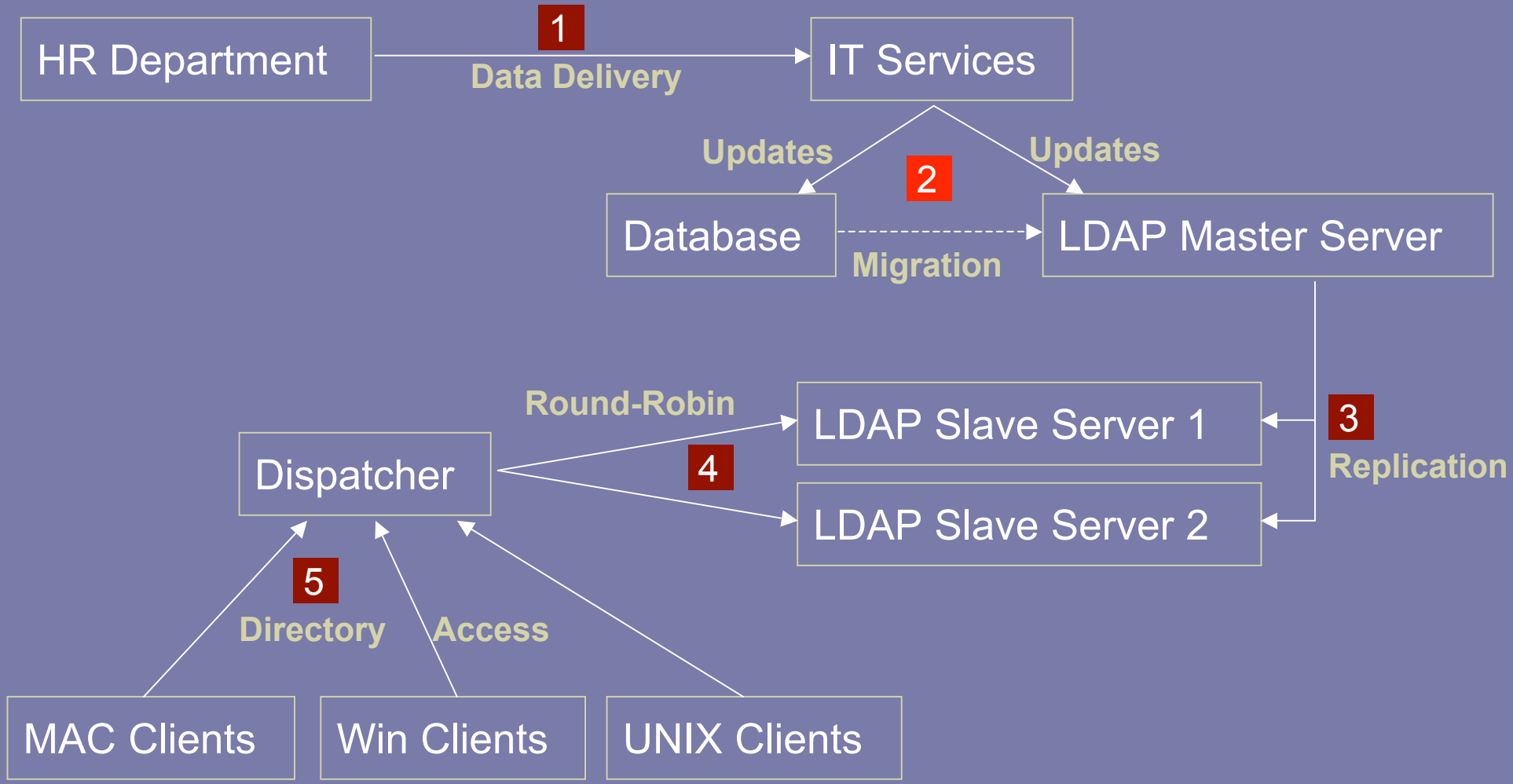
University of Zurich

Step 1: Data Delivery from HR

- New students and employees register with HR Department
- Mutations (Address, etc.) are submitted to HR Department
- HR uploads tab-delimited file of complete dataset to IT Services daily

University of Zurich

Infrastructure & Data-Flow



University of Zurich

Step 2: Conversion and import

- Determine changes in data (update, insert, delete)
- Extend data with additional attributes (password, uid, ..)
- Convert data and import into database and LDAP

- Database: MySQL, import with PERL/DBI
- LDAP: import with PERL Net::LDAPS

- Optional: Full data migration from MySQL to LDAP

University of Zurich

Step 2: Example LDAP record

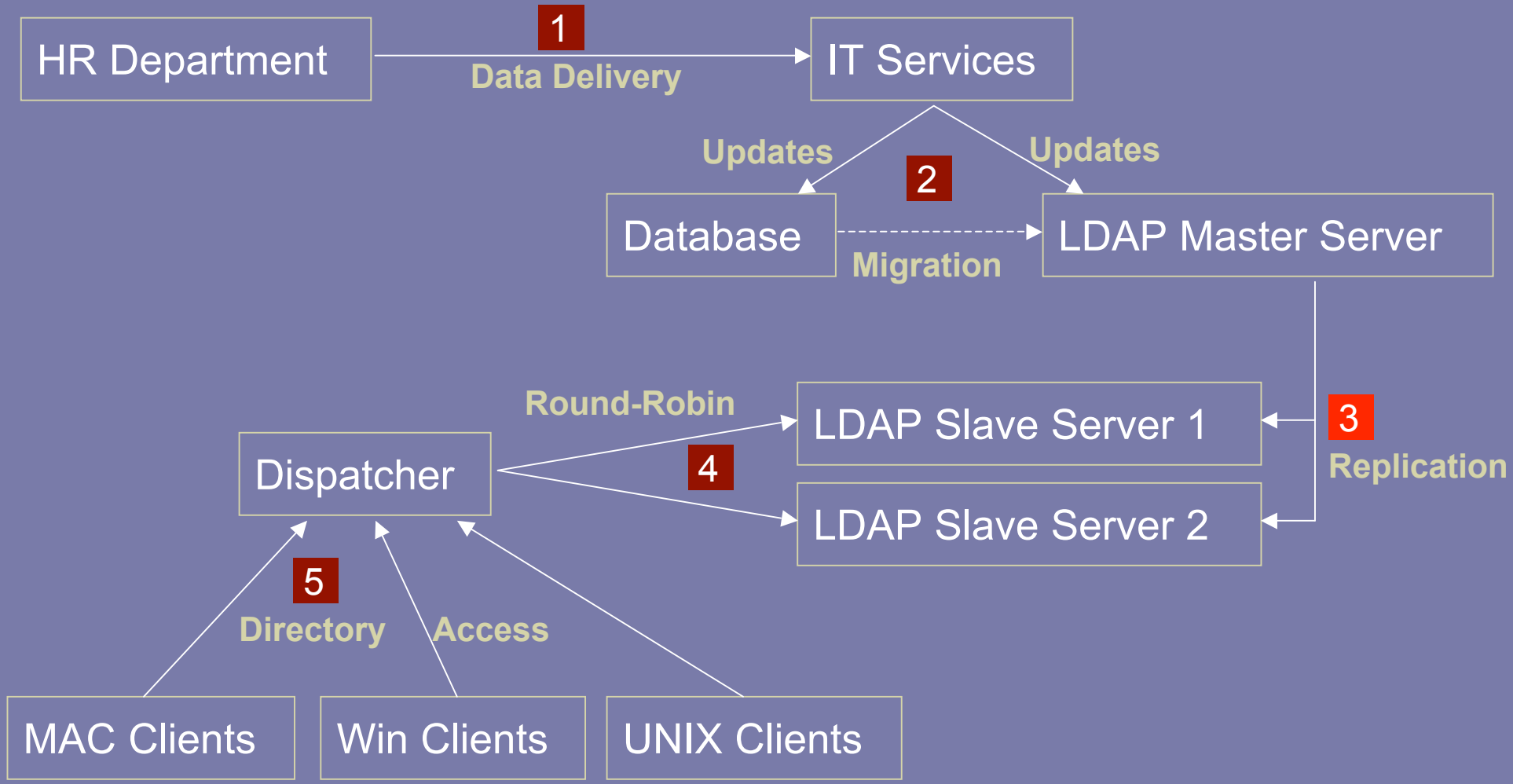
Distinguished name: uid=s9816737,ou=People,ou=UniAccess,ou=zi,dc=unizh,dc=ch

cn: s9816737
swissEduPersonUniqueID: 733938333701@unizh.ch
eduPersonAffiliation: student
swissEduPersonHomeOrganization: unizh.ch
swissEduPersonHomeOrganizationType: university
uid: s9816737
uidNumber: 11441
gidNumber: 1000
homeDirectory: /UniAccess/./home/h15/g27/s9816737
gecos: Herr Luzian Scherrer
loginShell: /usr/local/bin/pine
rid: 23882
mail: s9816737@access.unizh.ch

sn: Scherrer
givenName: Luzian
swissEduPersonStudyBranch1: 1
swissEduPersonStudyBranch2: 13
swissEduPersonStudyBranch3: 1800
ntPassword: 84C975D11331843DEE41307BB7A
lmPassword: 92FB4ACA0705D3B435B51404EE
userPassword:: e2NyeXB0fWN5NRwNEcxWlU=
objectClass: posixAccount
objectClass: sambaAccount
objectClass: shadowAccount
objectClass: swissEduPerson

University of Zurich

Infrastructure & Data-Flow



University of Zurich

Step 3: LDAP replication

- LDAP master server
  - Two daemons: slapd and slurpd
  - Automatic replication to slave servers (SSL)
  - OpenLDAP 2.1.22
  - SuSE Linux 9.0

- LDAP slave servers
  - One daemon: slapd
  - OpenLDAP 2.1.22
  - SuSE Linux 9.0

Step 3: OpenLDAP disadvantages

- **ACL and Schema-Definitions** in proprietary format (config-file), **not available as LDAP data**
  > manual replication required

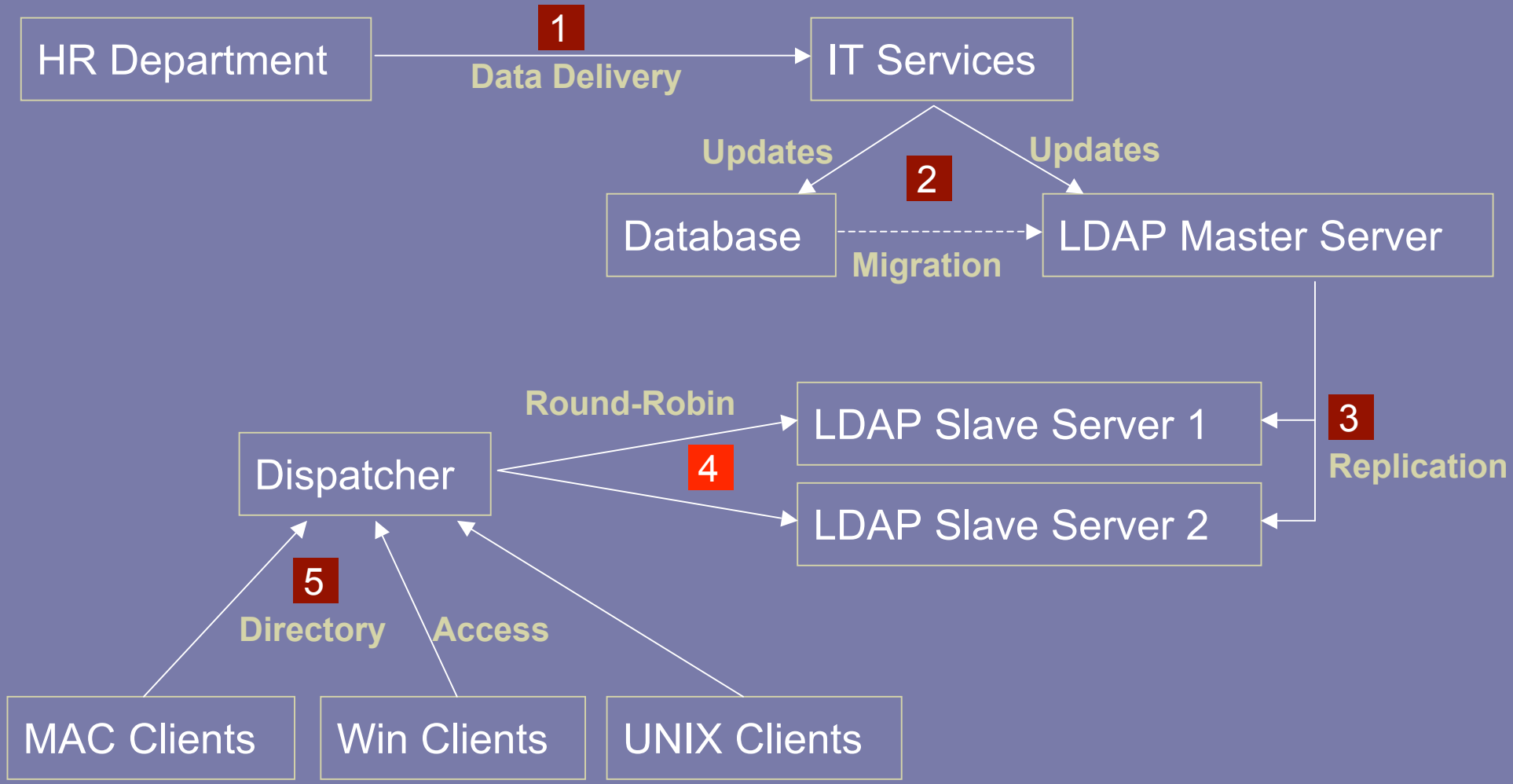
- **Updates are slow**
  > About 150 records per minute (with replication)
  > Intel Xeon 2GHz, 1GB RAM

Step 3: OpenLDAP advantages

- **OpenSource**
- **Available as RPM** (and other package-formats)
- **Many backends available**:
  - DB (BerkleyDB, GNU DBM, NDBM)
  - PERL
  - LDAP
  - Shell
  - SQL (experimental)
- **Queries** (on indexed attributes) **are fast**

University of Zurich

Infrastructure & Data-Flow



University of Zurich

Step 4: Dispatching

- Alteon 180e Switch
- Public address: ldap.unizh.ch
- Connections are forwarded using round-robin to:
  - ldapslave1.unizh.ch
  - ldapslave2.unizh.ch

Step 4: Dispatching problems

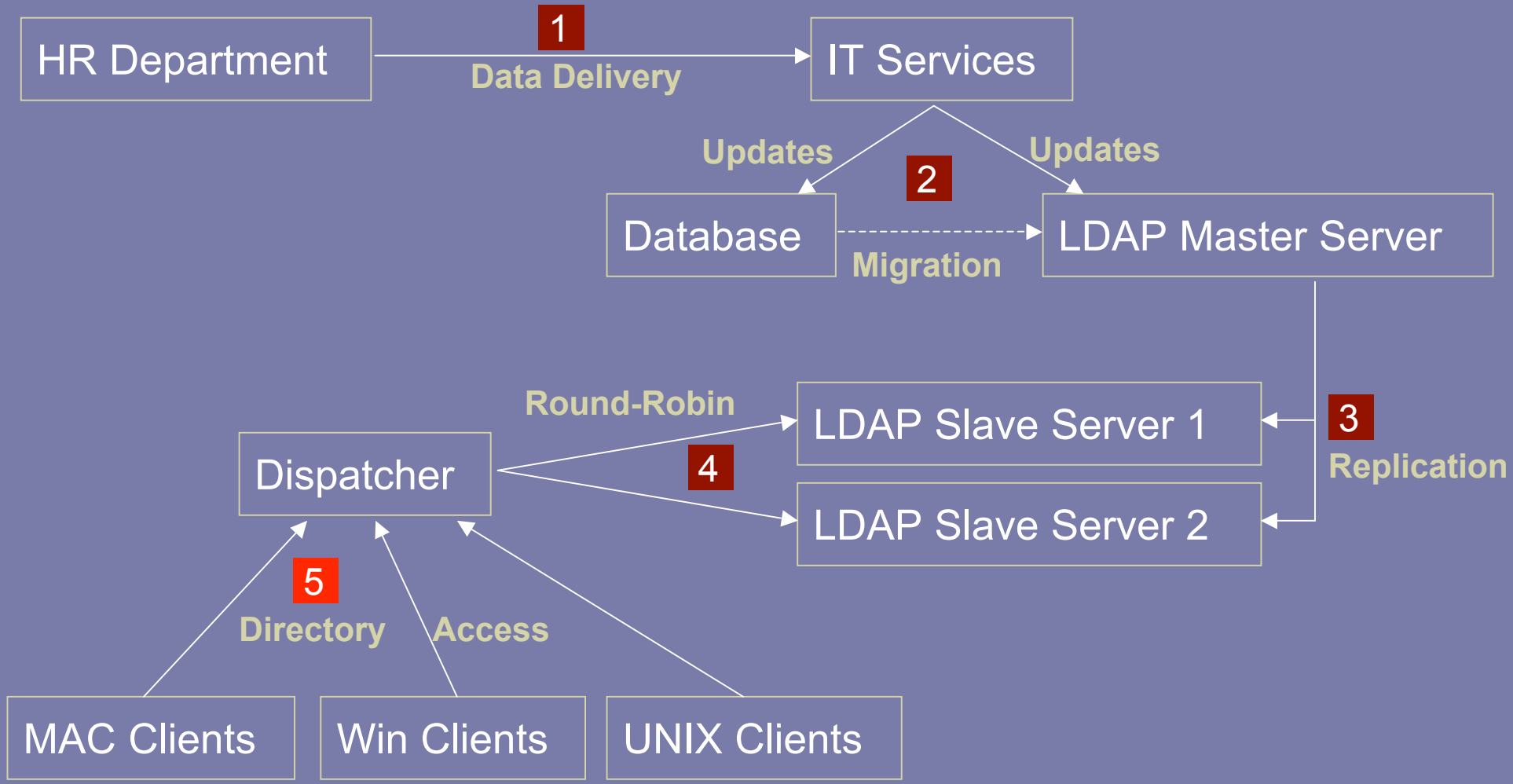
- Dispatcher **must not substitute source IP address** because of IP based access lists on the slave servers
- Dispatcher must have **content-based health checks**
- **SSL**: Certificates on slaves must contain the public dispatching-address and the slave servers own address (subjectAltName)

Step 4: Dispatching advantages

- **Redundancy**: Service is available until all slave servers are down
- **Scalability**: New slave servers can be added or removed without the need to change client configuration

University of Zurich

Infrastructure & Data-Flow



Step 5: Directory access

- UNIX/Linux: pam_ldap and nss_ldap
- Mac OS X: integrated LDAP support
- Windows: pGINA
- Apache: mod_ldap
- Cisco devices: FreeRADIUS to LDAP gateway
- Samba: integrated LDAP support

- All clients are SSL capable

Summary

- All requirements are met:

Based on open standards	LDAP
Open source	*partly:* OpenLDAP, Linux
Server infrastructure on Linux	SuSE Linux
Client authentication	pam_ldap, nss_ldap, pGINA, etc.
Reasonable price	HW: Alteon 180e, 3 x86 Machines
Redundancy	Dispatching
Security	SSL
Scaleable	Dispatching

- Productive for since Q1 2003
  - No problems occurred
  - Administrative effort is near zero (once running)
  - Easy integration with AAI

University of Zurich

Links and further details

- **OpenLDAP**
  http://www.openldap.org/
- **pam_ldap and nss_ldap**
  http://www.padl.com/
- **SuSE Linux**
  http://www.suse.com/
- **Alteon Dispatcher**
  http://www.nortelnetworks.com/products/family/alteon.html
- **pGina**
  http://pgina.xpasystems.com/
- **Apache mod_ldap**
  http://httpd.apache.org/docs-2.0/mod/mod_ldap.html
- **FreeRADIUS**
  http://www.freeradius.org/
- **PERL Net::LDAP**
  http://search.cpan.org/~gbarr/perl-ldap-0.31/lib/Net/LDAPS.pm

University of Zurich

Questions