World 2011

Sun Identity Management & Open Directory

Jennifer Walbank/Pascal Grosvenor, LDAP Guru from the server group :) & Berry Mak

University of Technology, Sydney

AUC

XWIKI

Why and how?

- Why?
  - Centralising systems
  - Desktop Architecture Project
  - Same sign on
- How?
  - Design
  - Demonstration
- Did we succeed?

AUC

XWII

Centralising Systems

- Only centralise what it makes sense to...
  - Authentication
  - Authorisation
  - Software updating
  - Proper housing of servers
    - bandwidth
    - backup
- Providing a robust and sustainable computing environment

AUC

XWII

Desktop Architecture Project

- Project designed for Windows environment
  - provisioning of the centralised model
  - no Mac OSX planning
- Birth of the MOE (would you believe Mac Operating Environment) - quickly renamed Managed Operating Environment for Mac OSX in September last year.

Same Sign On

- Anywhere up to five different passwords depending on what services you had access to
- new Email project prompting the opportunity to enable a consistent “UTS” username and password
- Birth of Identity Management at UTS

Identity Management

- the idea of account creation with a role assigned that enables a user's access to services automatically, across what had been many incompatible systems.
  - AD
  - OD
  - at the time NDS
  - LDAP enabled
- so why Sun?

Different types of IDM

- pre-coded connectors (eg CA and NovelI)
  - require data cleansing at the source
  - pre-determined logical layout of the underlying systems
- Sun or even OpenLDAP
  - mutable - allows for us to code for each instance as we need it - the scripting matches the data sources as well as the underlying existing layout - we were a train already on the tracks

Current roles at UTS

Staff: Accounts for Staff, or contractors in staff positions

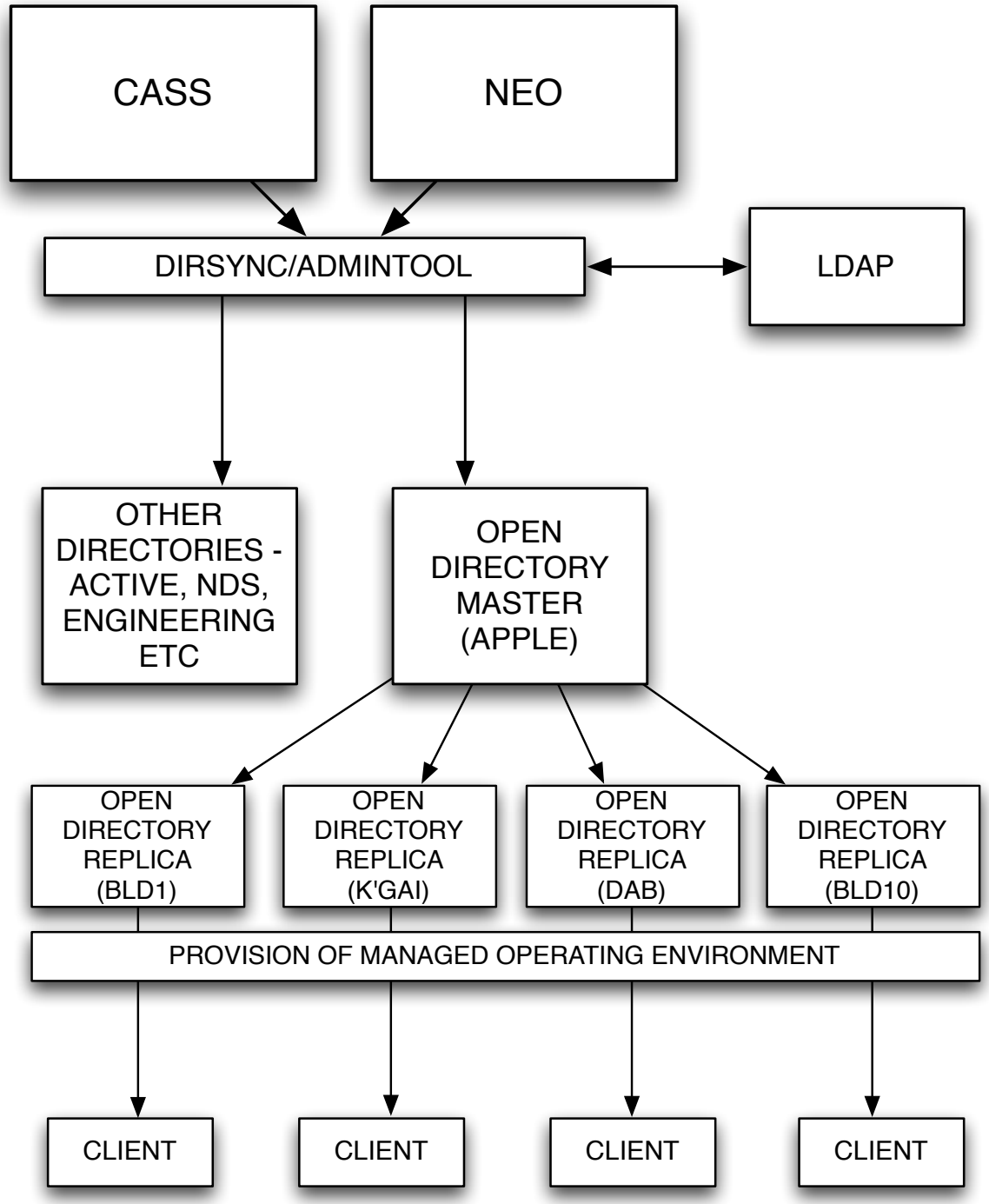
Students: For any type of student

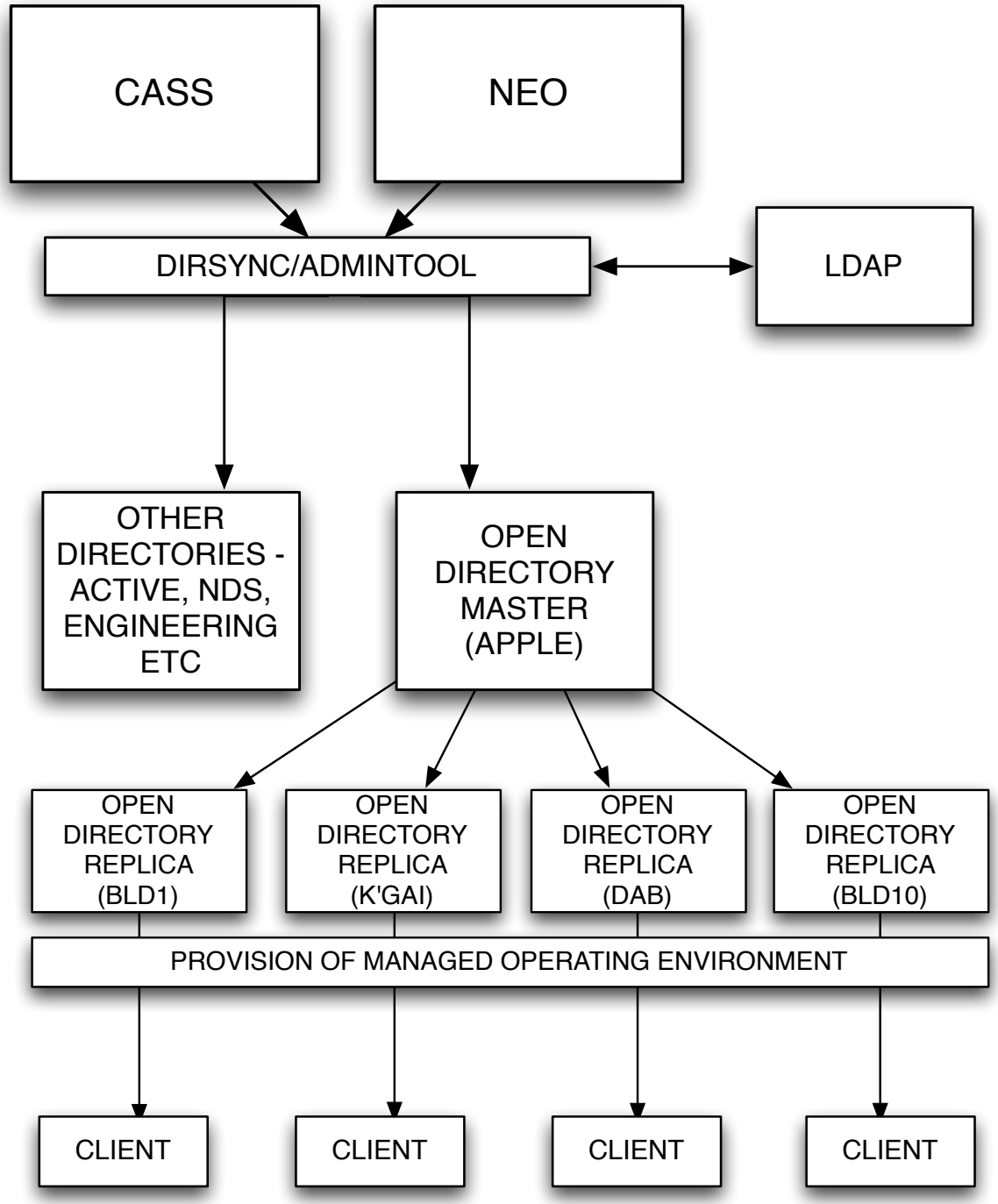
Alumni: *Alumni only receive an email forwarding account, not access to the labs, and cannot use webmail.

General: Accounts created for systems, or groups of people (i.e. accounts not for a particular person).

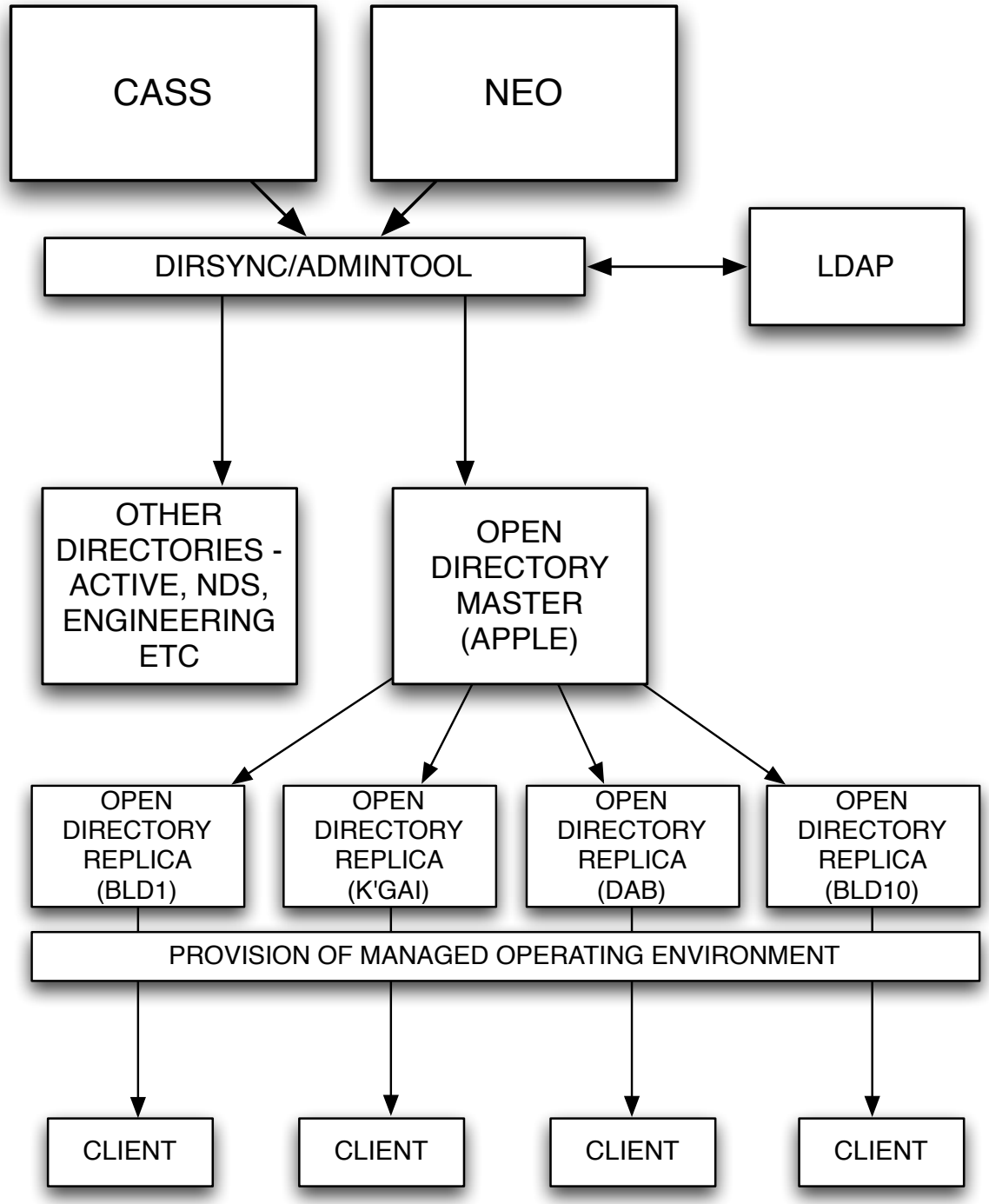
AUC

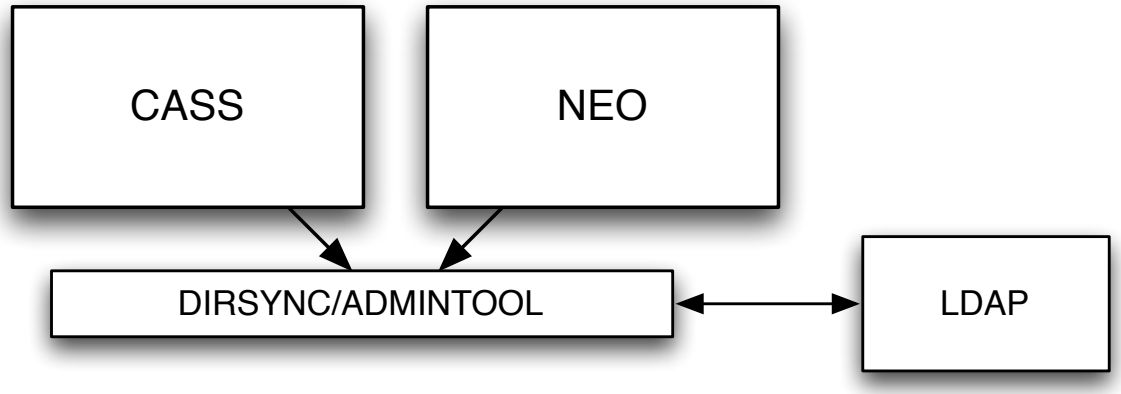
XWII


CASS
NEO
DIRSYNC/ADMINTOOL
LDAP
OTHER DIRECTORIES - ACTIVE, NDS, ENGINEERING ETC
OPEN DIRECTORY MASTER (APPLE)
OPEN DIRECTORY REPLICA (BLD1)
OPEN DIRECTORY REPLICA (K'GAI)
OPEN DIRECTORY REPLICA (DAB)
OPEN DIRECTORY REPLICA (BLD10)
PROVISION OF MANAGED OPERATING ENVIRONMENT
CLIENT
CLIENT
CLIENT
CLIENT


CASS
NEO
DIRSYNC/ADMINTOOL
LDAP
OTHER DIRECTORIES - ACTIVE, NDS, ENGINEERING ETC
OPEN DIRECTORY MASTER (APPLE)
OPEN DIRECTORY REPLICA (BLD1)
OPEN DIRECTORY REPLICA (K'GAI)
OPEN DIRECTORY REPLICA (DAB)
OPEN DIRECTORY REPLICA (BLD10)
PROVISION OF MANAGED OPERATING ENVIRONMENT
CLIENT
CLIENT
CLIENT
CLIENT

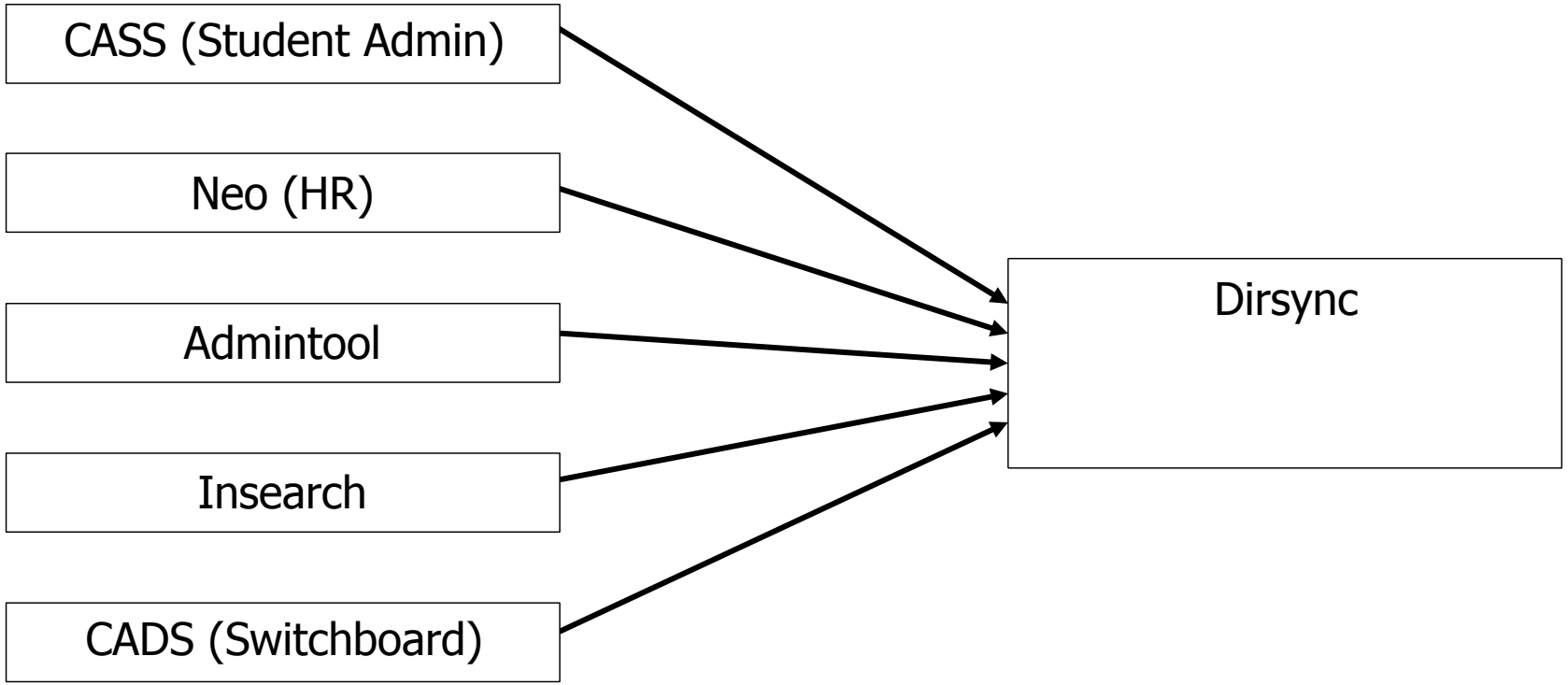
How does it work ?


CASS
NEO
DIRSYNC/ADMINTOOL
LDAP
OTHER DIRECTORIES - ACTIVE, NDS, ENGINEERING ETC
OPEN DIRECTORY MASTER (APPLE)
OPEN DIRECTORY REPLICA (BLD1)
OPEN DIRECTORY REPLICA (K'GAI)
OPEN DIRECTORY REPLICA (DAB)
OPEN DIRECTORY REPLICA (BLD10)
PROVISION OF MANAGED OPERATING ENVIRONMENT
CLIENT
CLIENT
CLIENT
CLIENT


CASS
NEO
DIRSYNC/ADMINTOOL
LDAP

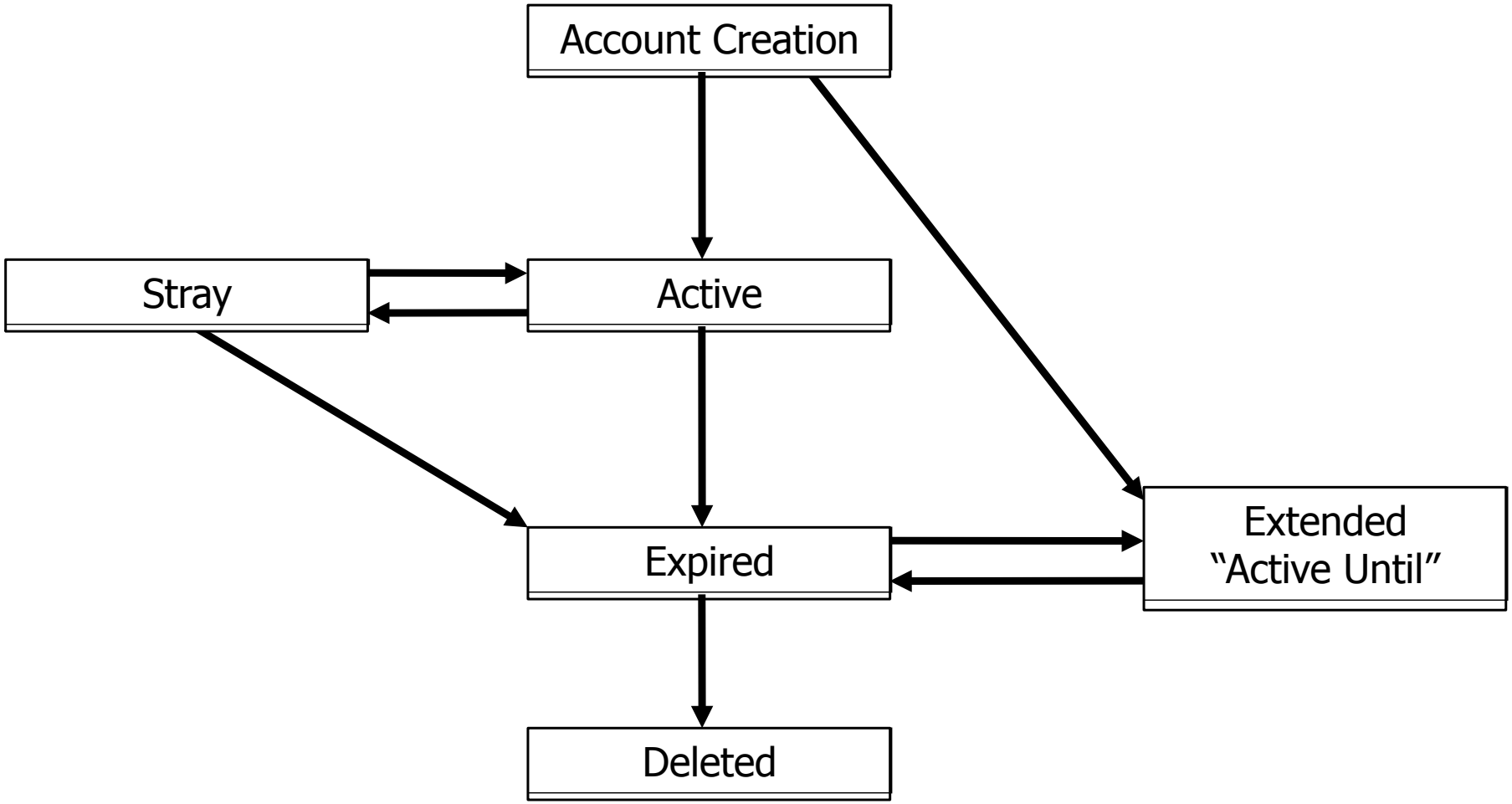
Data Sources

Dirsync automatically creates and maintains all accounts.



Account Lifecycle

Typical account states and movements



Dirsync

- Dirsync is a set of custom written Perl modules and scripts that connects Sun LDAP with all the other systems
- Updates from data sources are recorded to Sun LDAP by Dirsync
- Dirsync then writes from Sun LDAP to other directory systems (eg. Active Directory, OS X Open Directory)

Admintool

- Web-based interface to examine and modify accounts within UTS' authentication and mail systems
- Front end to Dirsync
- Restricted use - IT staff only

Admintool Menus

Account :

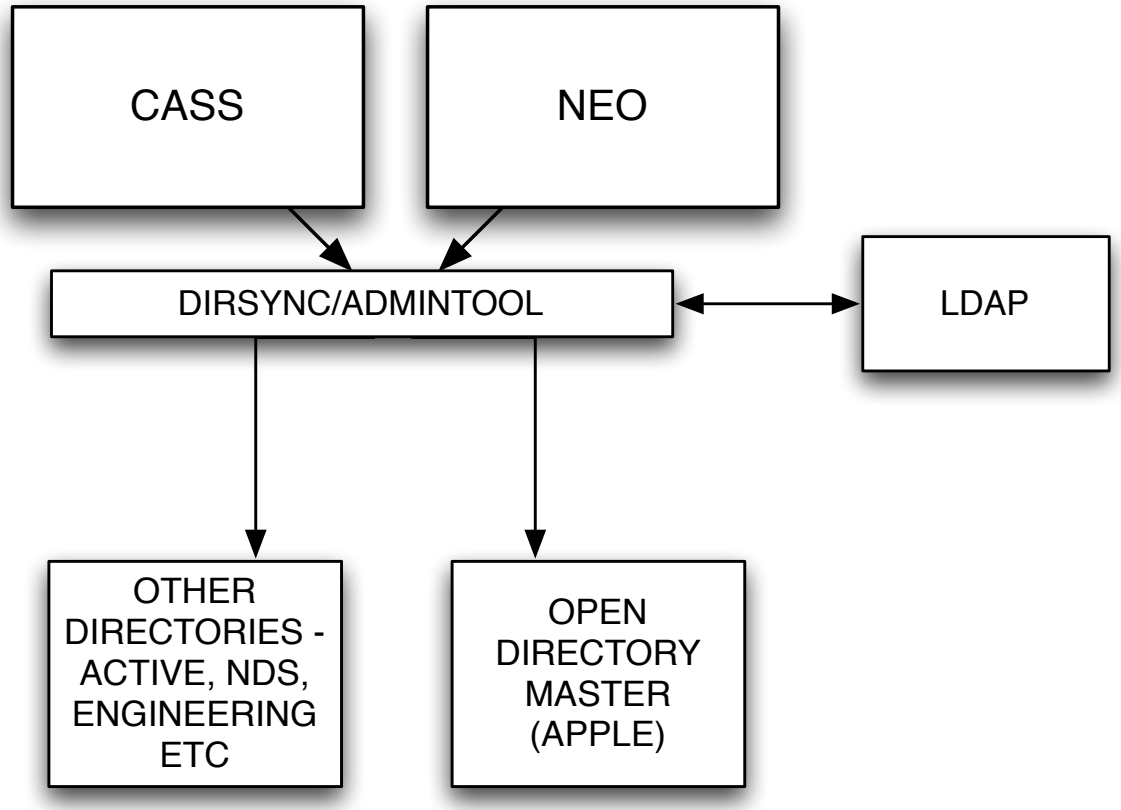
- Search
- Details
- Create
- Extend/ Expire
- Change Password
- Directory Listing
- Rename
- Lock/ Unlock
- Owned Accounts

Email :

- Aliases
- Vacation
- Forwarding
- Broadcast

AUC

XWII


CASS
NEO
DIRSYNC/ADMINTOOL
LDAP
OTHER DIRECTORIES - ACTIVE, NDS, ENGINEERING ETC
OPEN DIRECTORY MASTER (APPLE)

Dirsync & Open Directory

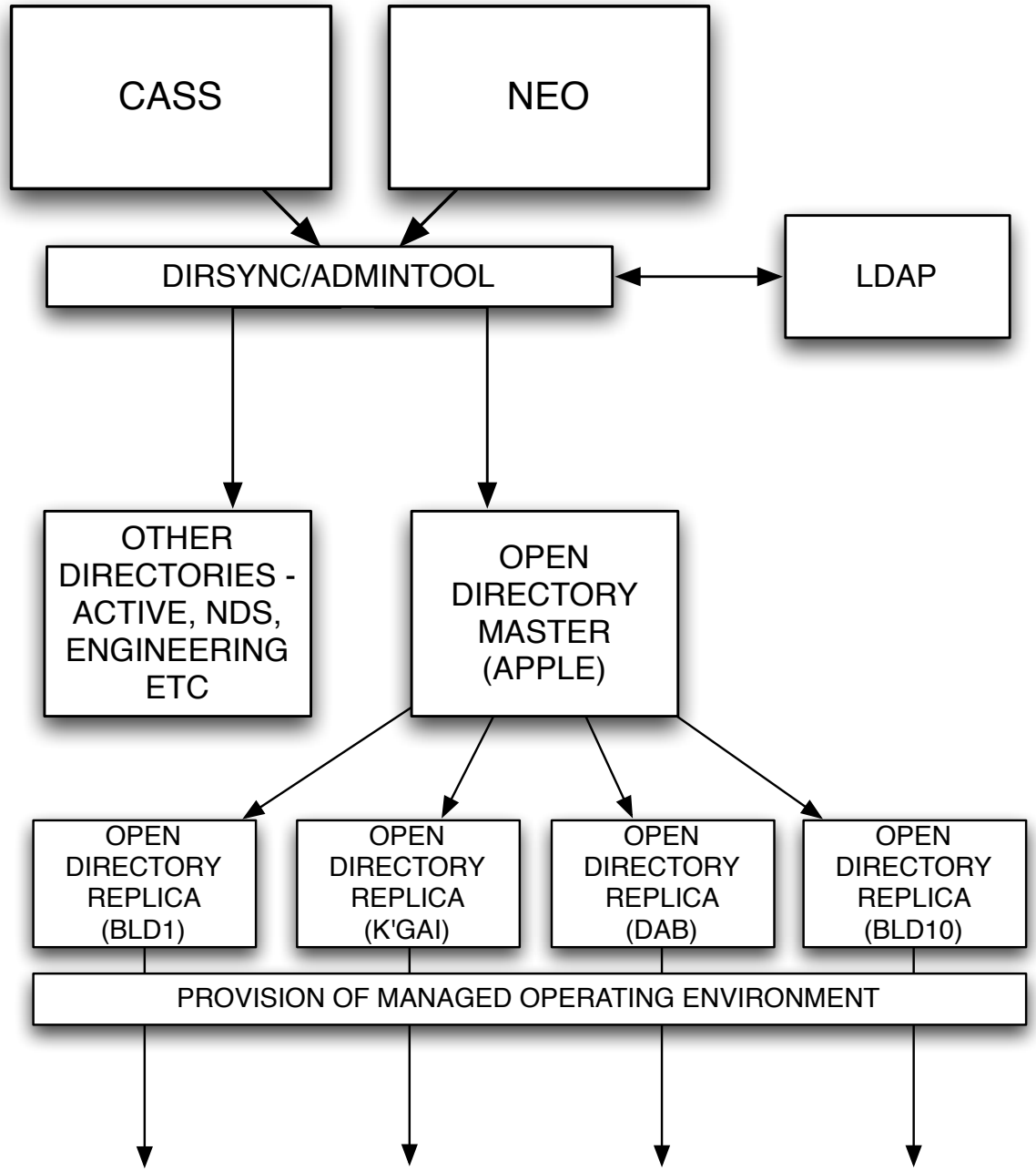
- Dirsync takes record/ object attributes from Sun LDAP and matches them to corresponding attributes in OD
- Most record attributes are added to OD using standard LDAP commands
- Main exception - user passwords

OD Password Server

- OD stores user passwords in a separate secure database to the OS X server's LDAP database
- Single purpose account and shell script developed to interact with OD password server
- Dirsync sends a remote SSH command to ODM to trigger password change in password server database

OD Master security

- Secure LDAP (using SSL) for communications between Dirsync and OD master
- Login window and SSH access to ODM restricted to only a few accounts
- Customised Firewall rules
- Physical security


CASS
NEO
DIRSYNC/ADMINTOOL
LDAP
OTHER DIRECTORIES - ACTIVE, NDS, ENGINEERING ETC
OPEN DIRECTORY MASTER (APPLE)
OPEN DIRECTORY REPLICA (BLD1)
OPEN DIRECTORY REPLICA (K'GAI)
OPEN DIRECTORY REPLICA (DAB)
OPEN DIRECTORY REPLICA (BLD10)
PROVISION OF MANAGED OPERATING ENVIRONMENT

OD Master and replicas

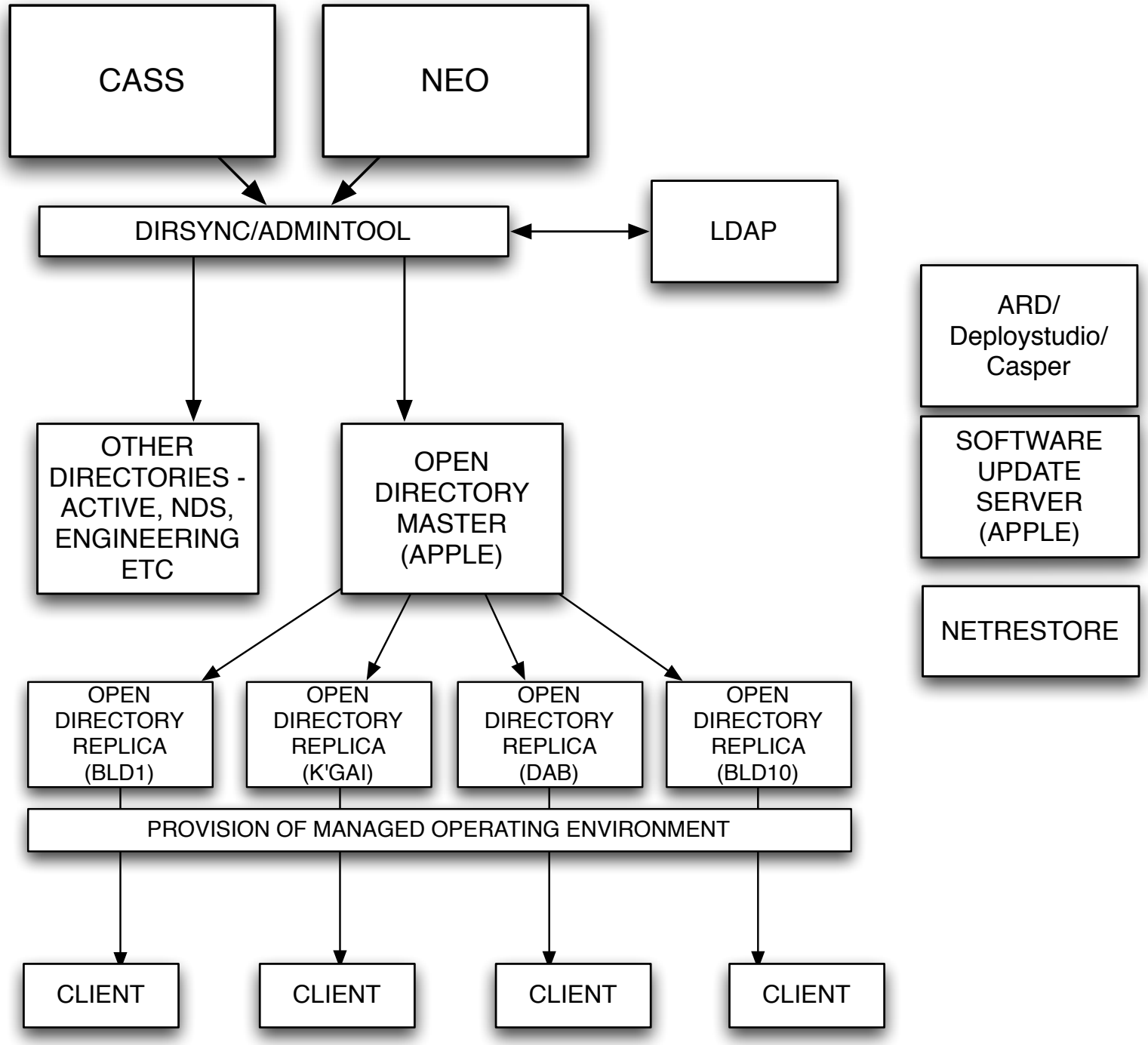
- Five OD replicas distributed across uni - share traffic load, redundancy
- OD system uses Apple's own secured method for replicating data between ODM and replicas
- Replicas also have Firewalls configured
- OD servers do not run any other services

Authorisation/ Workgroup Mgt

- IT managers of each faculty/ area have directory administrator access to OD (but not server admin access to OD master)
- Collegial work approach and knowledge sharing
- Logs record access, no problems to date :-)

AUC

XWIKI


CASS
NEO
DIRSYNC/ADMINTOOL
LDAP
ARD/
Deploystudio/
Casper
SOFTWARE
UPDATE
SERVER
(APPLE)
NETRESTORE
OTHER
DIRECTORIES -
ACTIVE, NDS,
ENGINEERING
ETC
OPEN
DIRECTORY
MASTER
(APPLE)
OPEN
DIRECTORY
REPLICA
(BLD1)
OPEN
DIRECTORY
REPLICA
(K'GAI)
OPEN
DIRECTORY
REPLICA
(DAB)
OPEN
DIRECTORY
REPLICA
(BLD10)
PROVISION OF MANAGED OPERATING ENVIRONMENT
CLIENT
CLIENT
CLIENT
CLIENT

Managed Operating Environment

- Apple Netrestore and DeployStudio Server
- Centralised Software Update Server - access managed thru Workgroup Manager
- Apple Remote Desktop
- Working on base SOE for all macs at UTS

Demonstration

Much more fun to watch than talk about :)

Is this the end?

Questions ???

AUC

XWII