Overview

LDAP

Recommended readings

- LDAP for Rocket Scientists
- Basic LDAP Concepts
- Understanding the LDAP Protocol, Data Hierarchy, and Entry Components

Openldap server documentation

Exercises are based on the OpenLDAP server implementation.

Related material at http://www.openldap.org.

What is LDAP anyway?

- **L**ightweight **D**irectory **A**ccess **P**rotocol
- Vendor independent
- IETF standard:

> *Clients interact with servers using a directory access protocol*

LDAP Server cli bind

Command

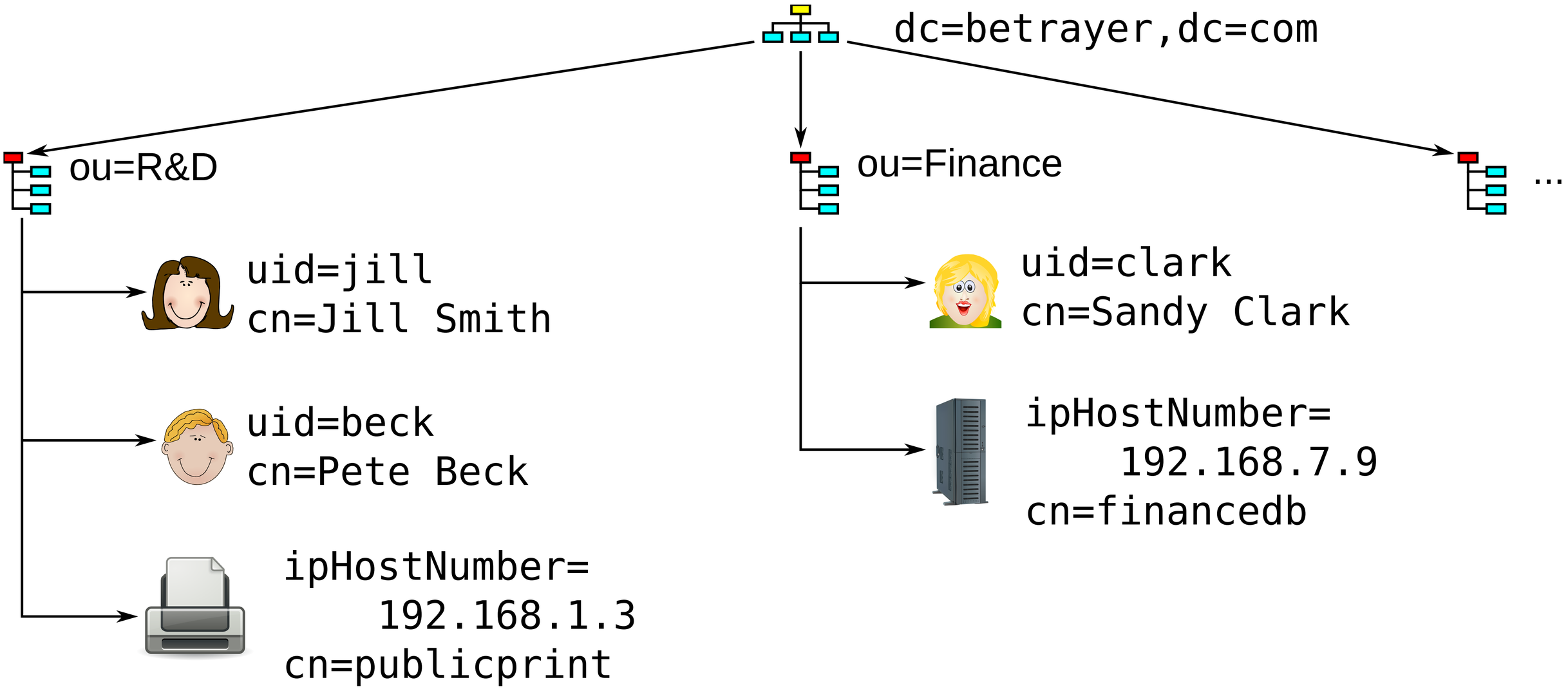
```
ldapsearch \
  -h localhost (1) \
  -D "cn=admin,dc=betrayer,dc=com" (2)\
  -w password -x (3)\
  -b "dc=betrayer,dc=com" (4)\
  -s sub (5) \
  -LLL (6)
```

Result

```
dn: dc=betrayer,dc=com (1)
objectClass: top
objectClass: dcObject
objectClass: organization
o: Betrayers heaven (2)
dc: betrayer

dn: cn=admin,dc=betrayer,dc=com (3)
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin (4)
description: LDAP administrator
userPassword:: e1NT...dE53N1E= (5)
```

Document Information Tree (DIT)



Relative and absolute DNs

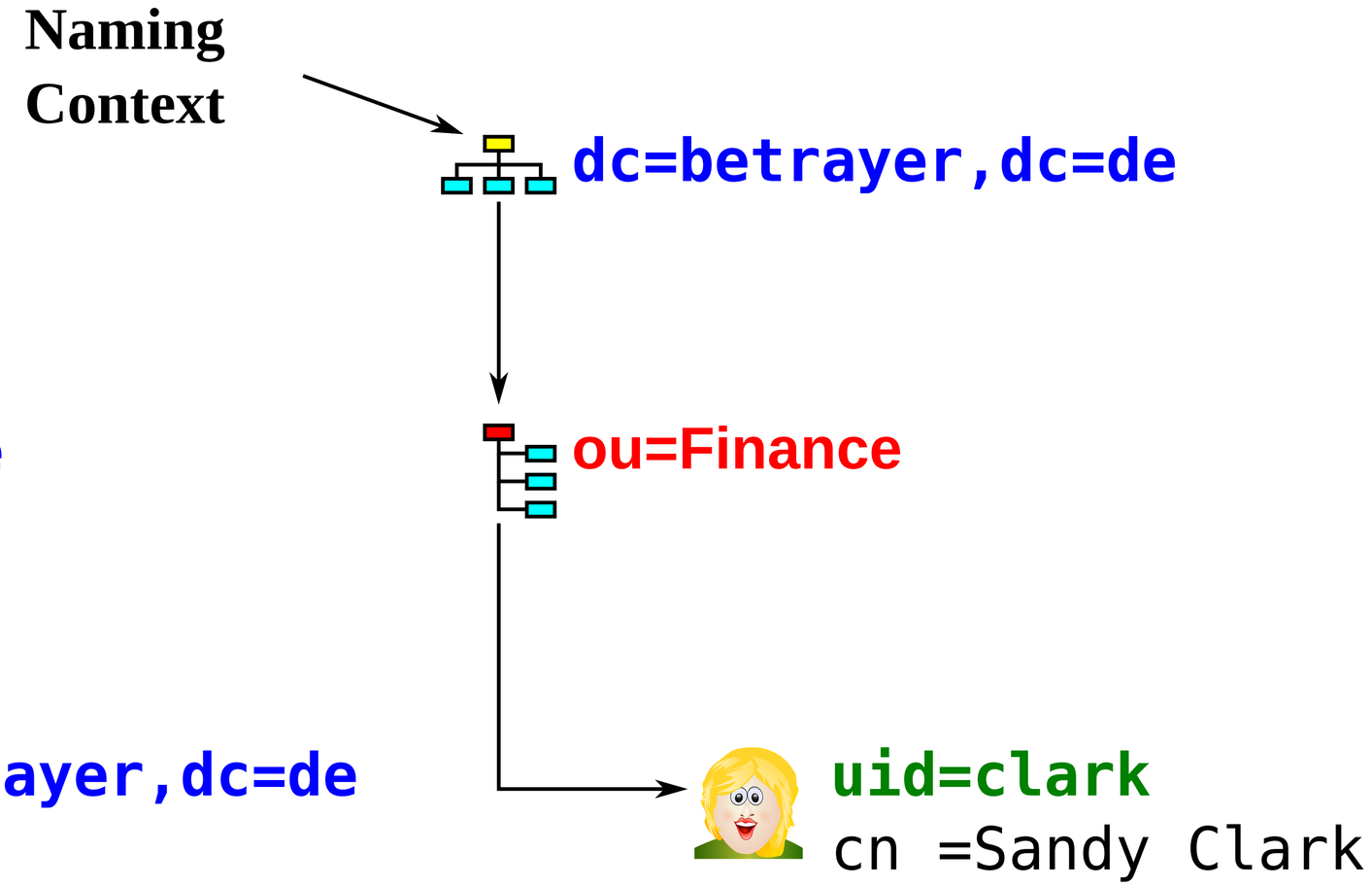
Absolute DN values

dc=betrayer,dc=de

ou=finance,dc=betrayer,dc=de

uid=clark,ou=finance,dc=betrayer,dc=de

Relative DN values



User example

```
dn: uid=clark,ou=finance,dc=betrayer,dc=de (1)
cn: Sandy Clark
homeDirectory: /home/clark
sn: Clark
uid: clark (2)
uidNumber: 21101
givenName: Sandy
loginShell: /bin/bash
mail: clark@betrayer.com (3)
mail: finance@betrayer.com
postOfficeBox: 10G
userPassword: {SSHA}noneOfYourBusiness
```

objectClass

- Structuring LDAP entry data.
- Categories:
  - Structural
  - Auxiliary
  - Abstract

objectClass clarifications

Abstract classes:

To be extended by other classes

Structural classes:

- Each entry requires exactly one.
- Specify the “main” type of object.
- Must not inherit from auxiliary classes.

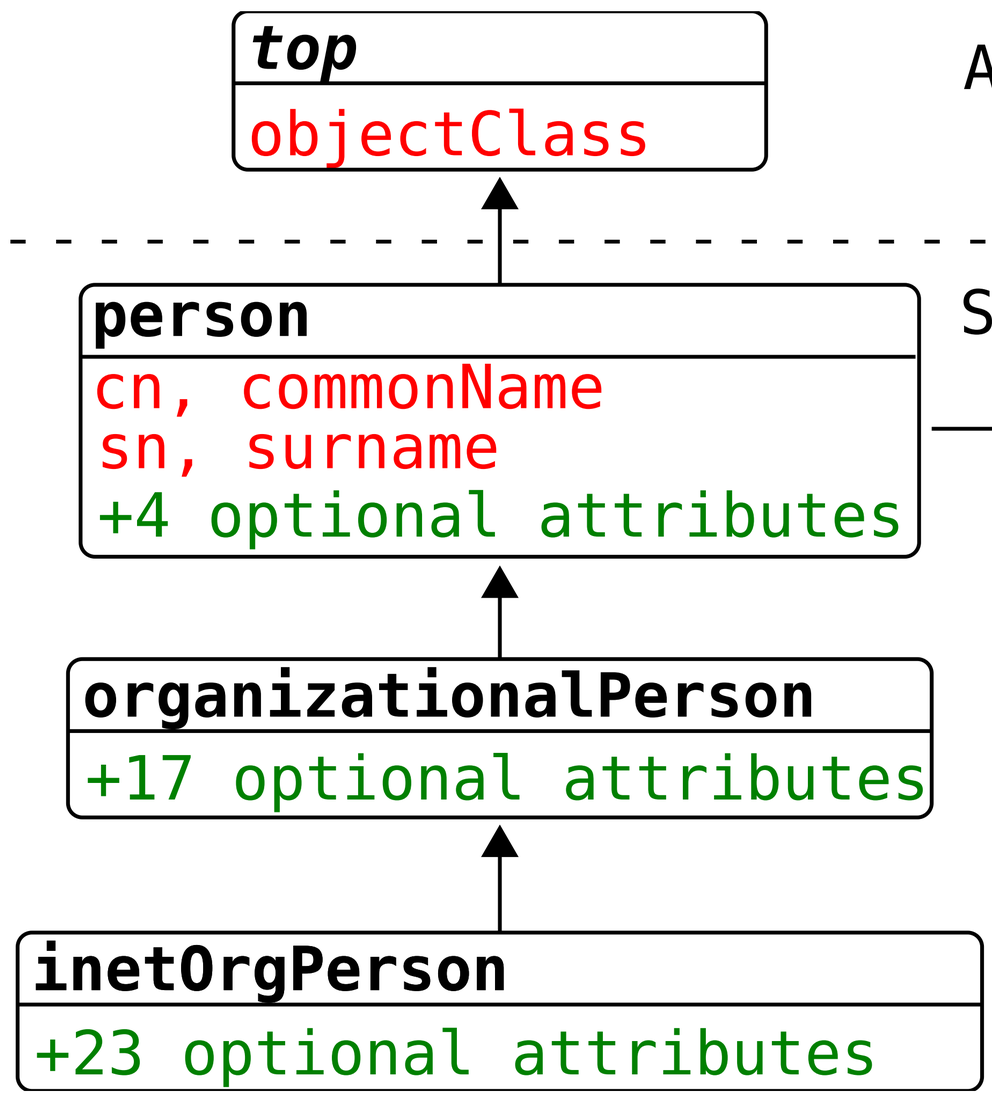
Auxiliary classes:

- Provide non-conflicting supplementary information.
- Think of (Java™) interfaces.
- Must not inherit from structural classes.

Augmenting `inetOrgPerson` by `posixAccount`

```
Class                          |   Instance uid=clark,ou=finance,dc=betrayer,dc=de
-------------------------------+-------------------------------------------------
inetOrgPerson (structural)     |
   sn                          |    sn: Clark
   cn                          |    cn: Sandy Clark
  ...                          |     ▲
                               |     |
posixAccount (auxiliary)       |     |
  cn                           |   see above (1)
  gidNumber                    |   gidNumber: 23113
  homeDirectory                |   homeDirectory: /home/clark
  uid                          |   uid: clark
  uidNumber                    |   uidNumber: 21101
  userPassword                 |   userPassword: {SSHA}noneOfYourBusiness
                              .....
```

Structural objectClass definitions



Relational counterpart sketch:

```
CREATE TABLE person (
  cn VARCHAR NOT NULL,
  sn VARCHAR NOT NULL,
  telephoneNumber
     VARCHAR NULL,
  ...-- +3 more
)
```

Search scopes

RFC 4520 defines three LDAP search scopes:

- baseObject (`base`)
- singleLevel (one)
- wholeSubtree (sub)

Predicate based queries

RFC 4520 defines predicate based queries using RPN style:

- (| (cn=k*) (uidNumber < 2000))

LDAP bind types

- Anonymous bind: No user credentials.

  Note: This typically provides limited privileges.

- Simple bind: User's DN + password:

```
DN: uid=clark,ou=finance,dc=betrayer,dc=de
password: 123456789
```

LDIF exchange format

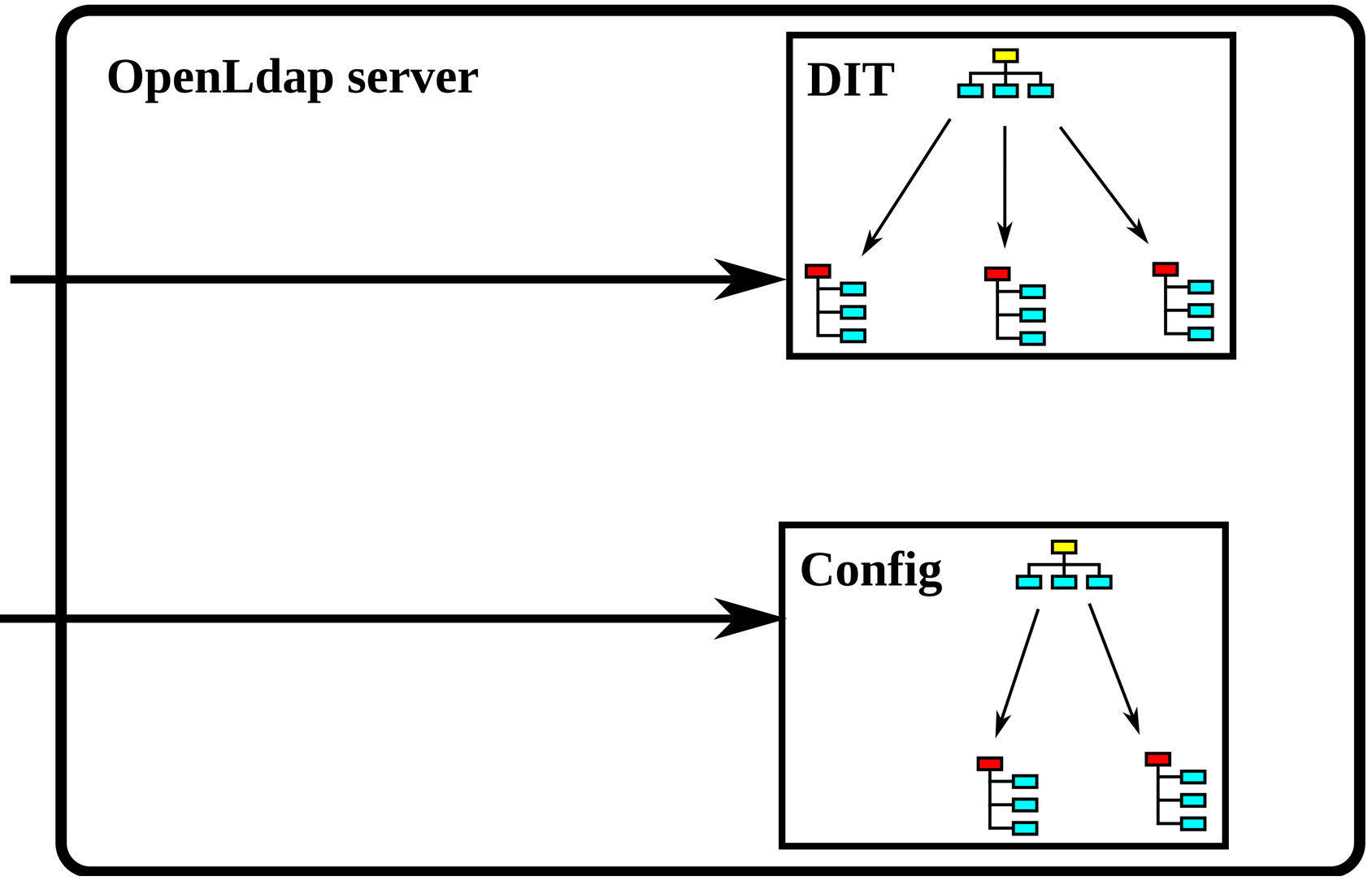
- **L**dap **D**ata **I**nterchange **F**ormat.
- Importing and exporting LDAP Data.
- Modifying existing entries (CRUD operations).
- Pure ASCII.

LDIF sample

```
dn: uid=clark,ou=finance,dc=betrayer,dc=de
objectClass: posixAccount
objectClass: inetOrgPerson
cn: Sandy Clark
homeDirectory: /home/clark
sn: Clark
uid: clark
uidNumber: 21101
givenName: Sandy
loginShell: /bin/bash
mail: clark@betrayer.com
mail: finance@betrayer.com
postOfficeBox: 10G
userPassword: {SSHA}noneOfYourBusiness
```

OpenLdap server architecture

dc=betrayer,dc=com



cn=config

Overview

- LDAP
  - Exercises
    - Populating your DIT.

An example LDAP Tree