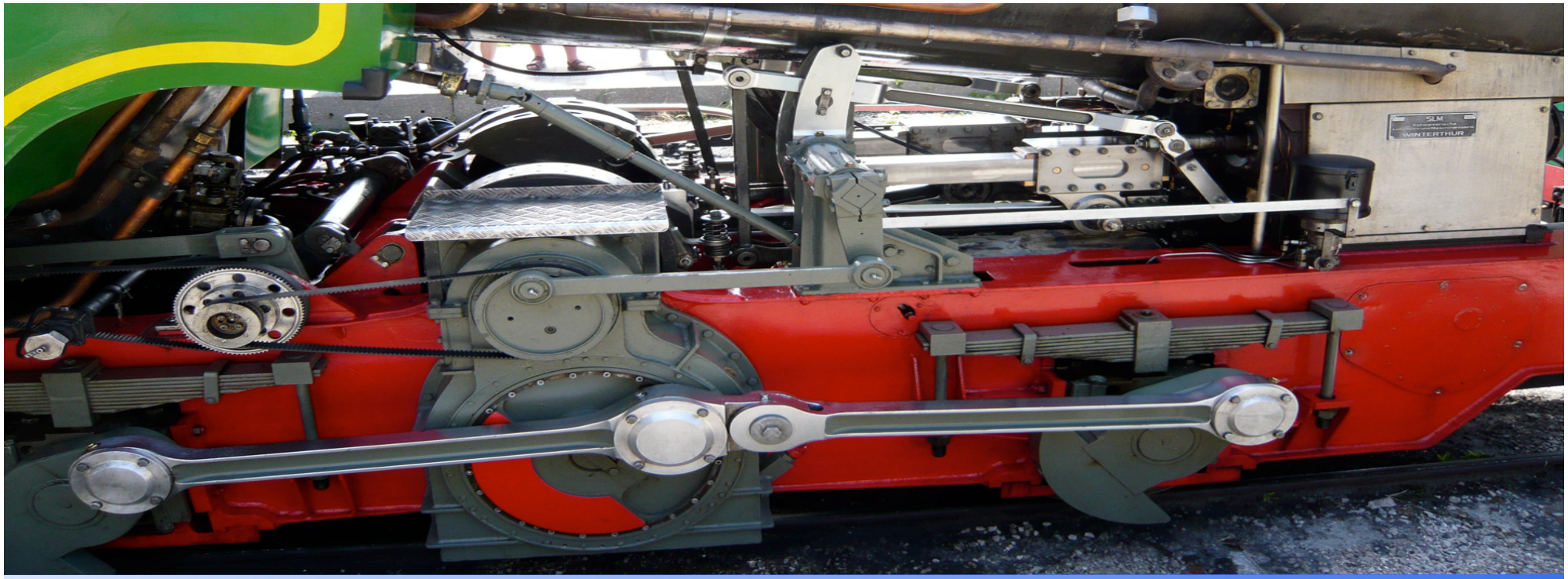



# Ptserver-ng

*Fabrizio Manfredi Furuholmen*

*Claudio Bisegni*

**Beolink.org**

# Outline

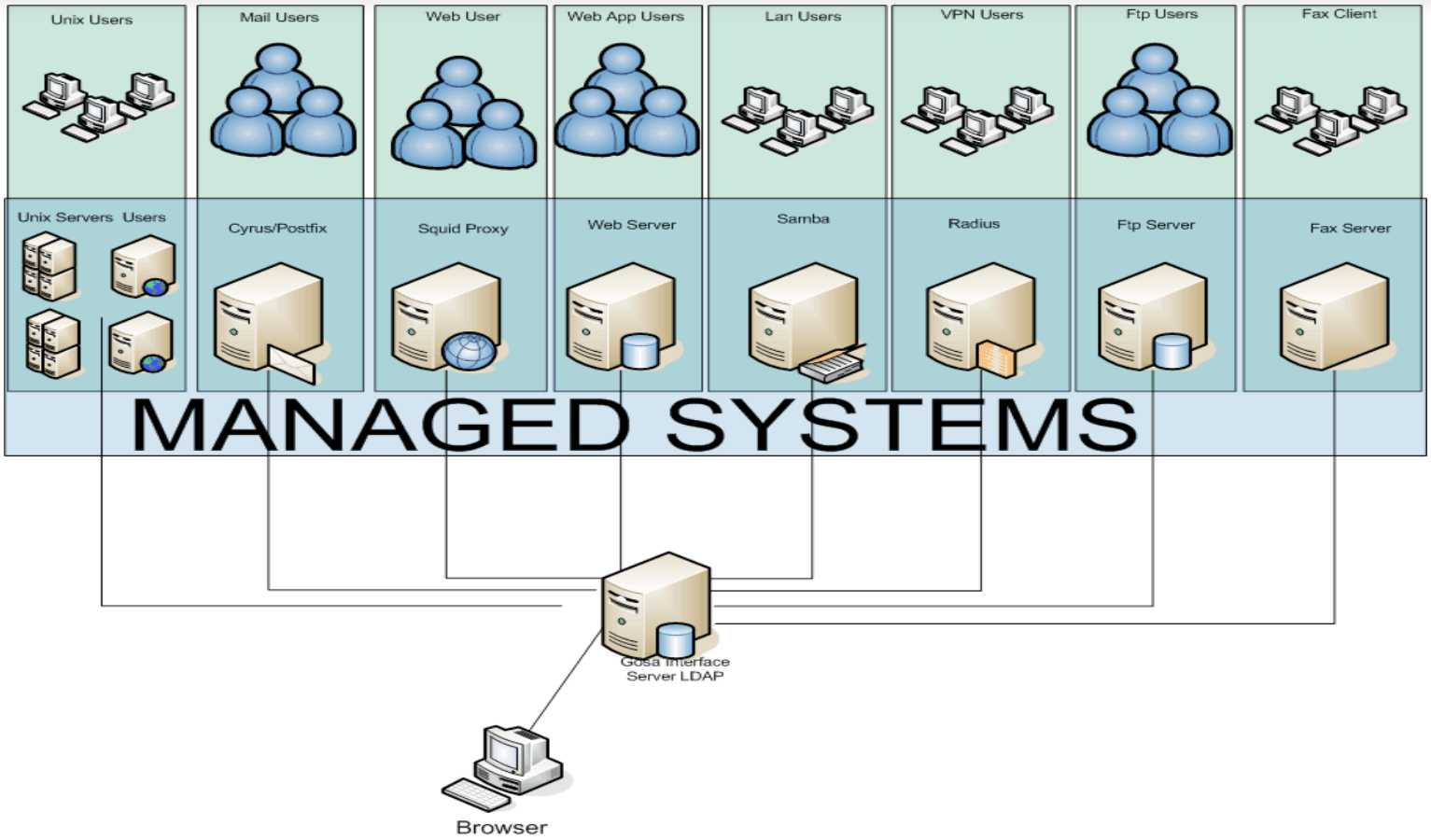


- Introducton
- Architecture
- Demo
- What's new in 2009
- Next step

# Introduction

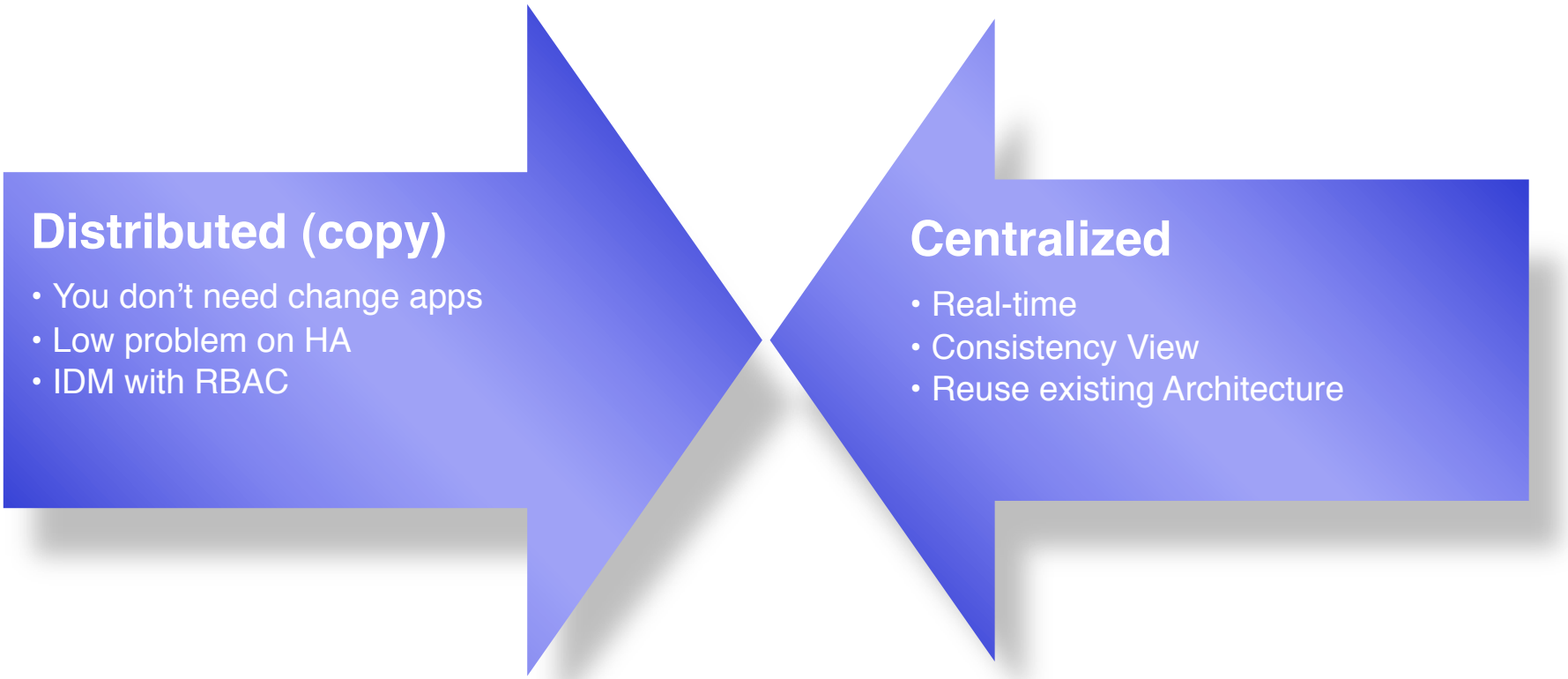


**Centrally administration “means” security and time/resource savings**



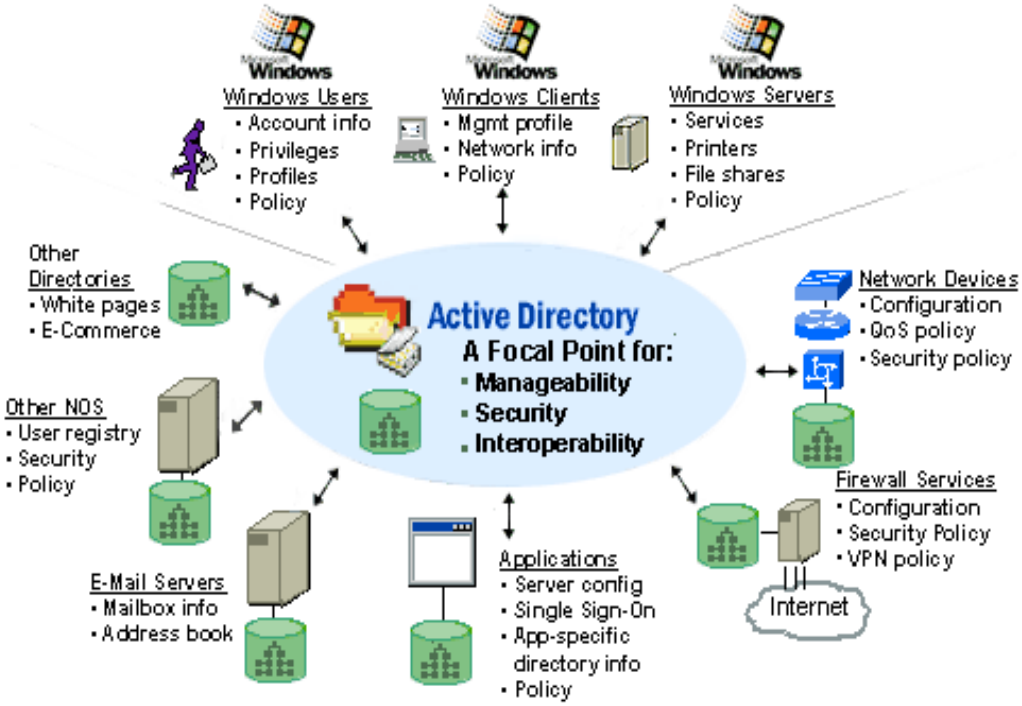
# Introduction





## Active Directory

- ❑ Enterprise Directory
- ❑ Identity Management
- ❑ High Availability
- ❑ RFC 2307bis UNIX Storage
- ❑ MMC
- ❑ Password Policy
- ❑ Application Deploy
- ❑ Group Policy



# Architecture



## Ptserver

- Network Layer
- AD Driver

## Windbind

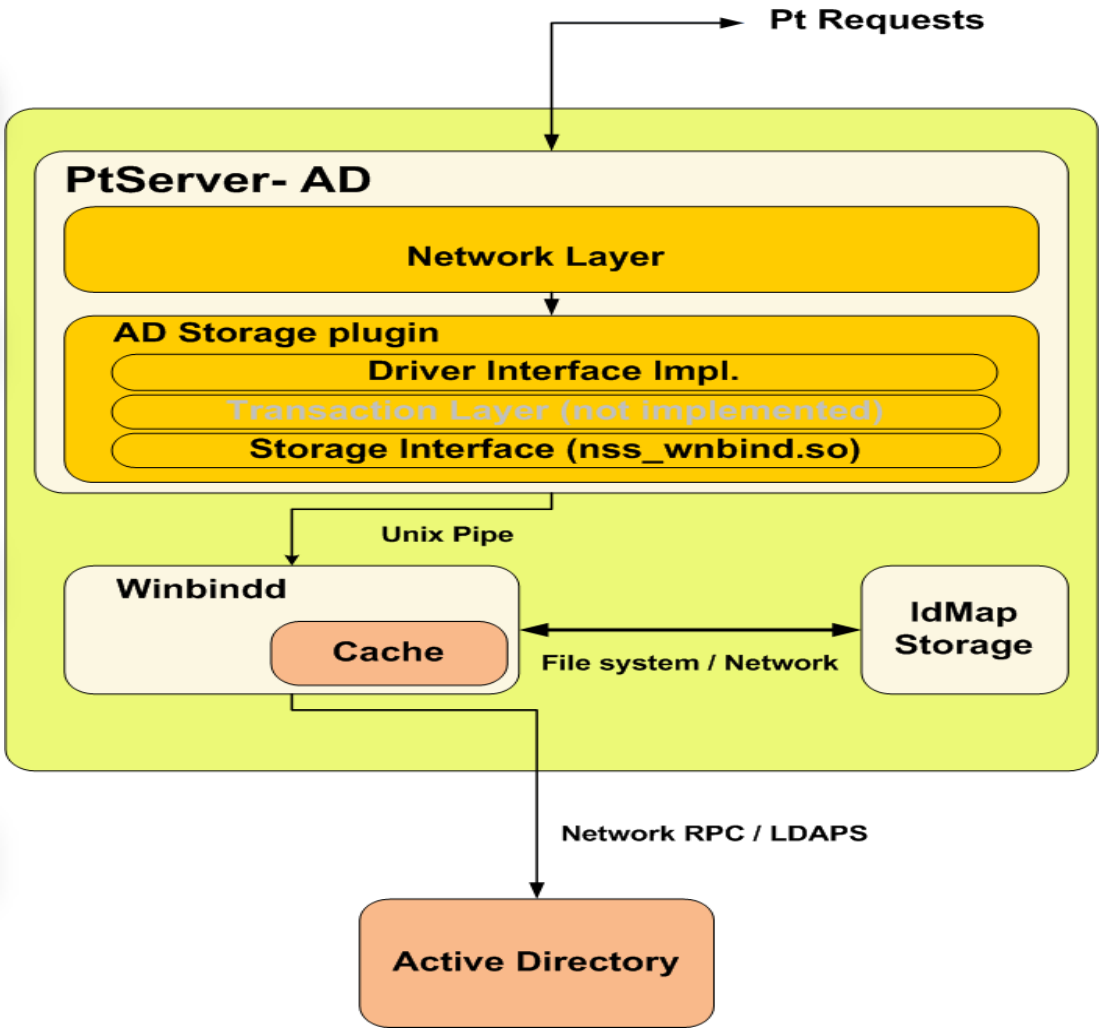
- Cache
- IDMAP Engine

## IDMAP Storage

- Ldap
- ADS
- File

## Domain Controller

- Samba
- WinNT/Win2*



# Winbindd

Beolink.org

**Winbind unifies UNIX and Windows NT account management by allowing a UNIX box to become a full member of an NT domain**

## Authentication

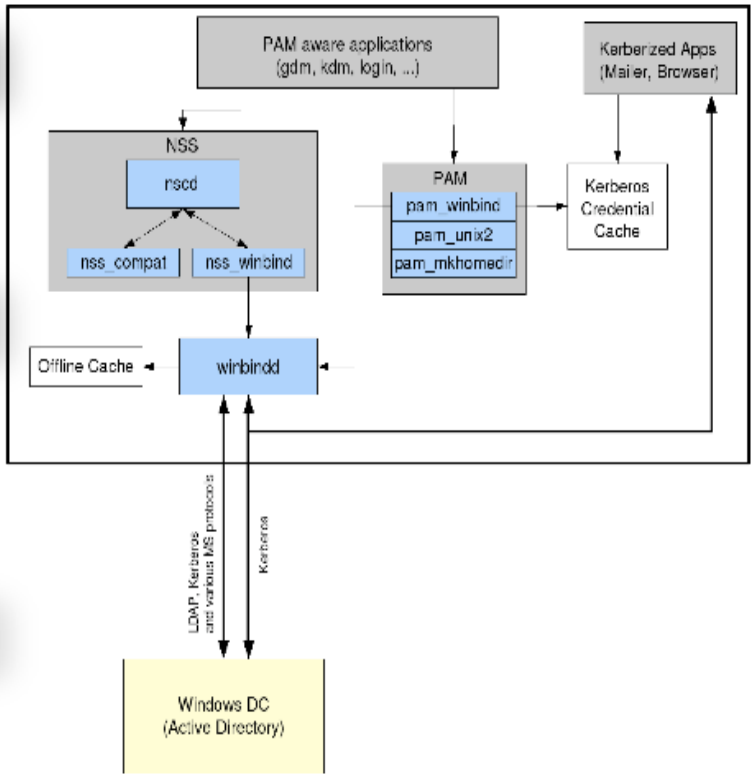
- NTLM
- ADS (Kerberos)

## Users Information

- Account info
- ID mapping
- Kerberos Ticket

## Groups Information

- Group info
- ID Mapping



# Winbindd



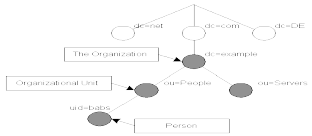
## ADS + rfc2307

- Groups
- UID/GID/OpenAFS ID


## AD + External LDAP

- **AD**
  - Groups / Users info
  - Kerberos Ticket


- **LDAP**
  - ID mapping



## Samba with LDAP/DB backend

- Group / Users info
- ID Mapping

# Winbindd



## ❑ Multi domain

```
idmap domains                       = BEOLINK.ORG
idmap config BEOLINK.ORG:backend  = ad
idmap config BEOLINK.ORG:default    = yes
Idmap config BEOLINK.ORG:readonly = yes
idmap alloc backend = tdb
winbind use default domain = Yes
winbind nested groups = Yes
winbind enum groups = yes
winbind enum users = yes
```

## ❑ ID Mapping

```
idmap alloc config:range       =  5000 – 9999
idmap config BEOLINK:range  =  10000 - 30000
winbind nss info                 =  rfc2307
winbind nested group          = Yes
```

## ❑ Winbindd

**daemon will cache user and group information before querying a Windows NT server again.**

**When a item in the cache is older than this time winbindd will ask the domain controller for the sequence number of the servers account database.**

```
winbind offline logon         = true
winbind refresh tickets       = true
winbind cache time            = 600
idmap negative cache time = 120
```

# Demo

# Performance

| Application | Cold cache | Warm cache | Remote cold cache | Remote warm cache |
|---|---|---|---|---|
| **Ldap** | 2X | - | 2.5X | - |
| **Ldap +nscd** | 2X | 1X | 2.5X | 1X |
| **winbind** | - | - | 4X | 1.2X |
| **ptserver** | - | - | 2X | 1X |

## Value for execution time

# Don’t forget..



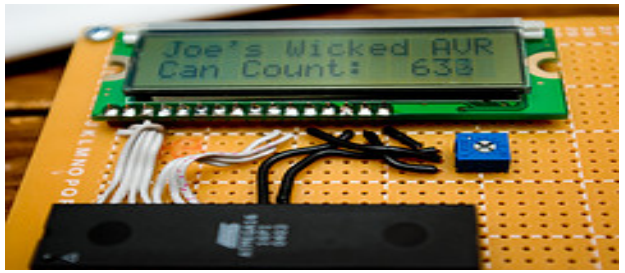
| | |
|---|---|
| Licenses | The Unix account is a CAL (cost) |
| Synchronous | Per domain synchronous child with user and group enumeration |
| Cache | Single cache for all elements |
| Read only | No flags, no qroup quota .. |

- **Plug-in**
  - Generic interface (defined in this conference)
  - Backend load dynamically
  - Native ldap backend (Claudio Bisegni)
  - RW backend
- **Libwbclient**
- **Samba > 3.2**

# Generic Driver Interface

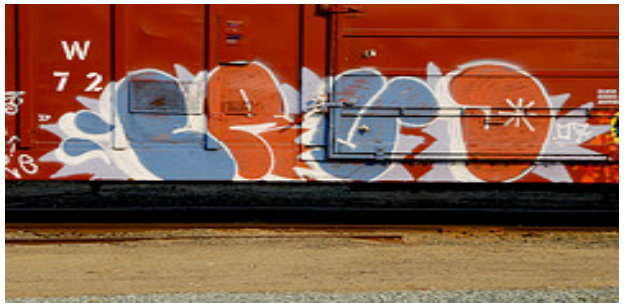


- Init
  - Connection / re-connection handling
  - Database init
  - Security initialization




- Transaction
  - Lock (read / write)
  - Commit/roolback

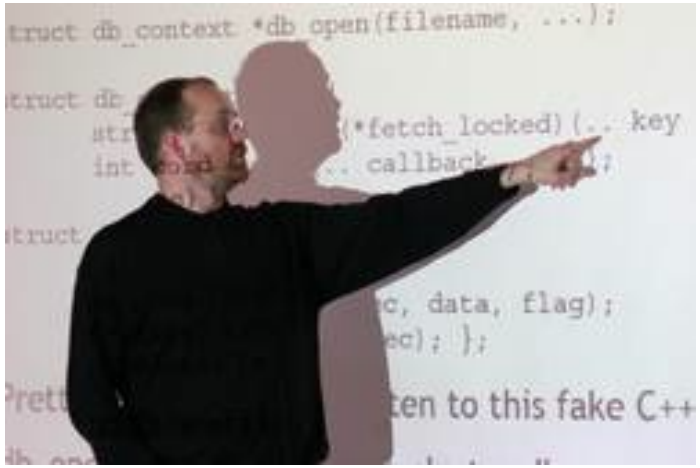
- DB operation
  - User (CRUD)
  - Group (CRUD)
  - Find / convert …
  - Set special Field ( User, Header )



- **Libnss_winbind (old)**
  - Ptserver-ng comunicates with windbind over unix domain socket
  - Socket path, structures size, etc are compiled in the ptserver-ng
  - Result was strong coupling between windbind and ptserver-ng

- **libwbclient**
  - From samba 3.2 libwbclient implements a shared library wrapper around winbind requests
  - Provides a stable API
  - Allows winbind to upgraded without disturbing other components
  - Direct access to IDMAP functions, Active Directory information

- **Volker Lendecke** has been re-writing winbind, making it asynchronous.




- **One asynchronous main daemon** that in good Unix tradition is supported by several helper processes

- **In August 2009 the code was rewrite again.**

  The winbind parent->child communication is completely based on an IDL file and auto-generated RPC client/server stubs (scalable)

## Advantages

- Single identity (single storage)
- Map btw different id (unix uid, afs id , windows SID)
- Real time update
- Pluggable in existing infrastructure
- Multi domains

## Disvantages

- Reliability ( partialy solved with muli master AD )
- Performance (patialy solved with 2009 changes)

# Thank you

*manfred@freemails.ch*

*www.beolink.org*

**Beolink.org**