

# Secure audio/video services – → H.323, H.350 and Firewalls

Setup, Installation and Configuration of  
OpenLDAP for H.350

QUESTNet 2005, Coolumb, Australia  
July 2005



Author: K. Stoeckigt ([kewin.stoeckigt@aarnet.edu.au](mailto:kewin.stoeckigt@aarnet.edu.au))  
©Copyright AARNET Pty Ltd

# → Hardware/Software requirements

- Hardware
  - OpenLDAP should run on a ‘standard’ computer
  - Recommendation:
    - Intel Pentium or equivalent 2.0GHz
    - 512MB Ram
    - 100GB Harddisk
- Software
  - Linux Operatingsystems (Redhat, Fedora, Debian,...)
  - Recommendation:
    - Fedora Core 2 or Redhat 9

## → Hardware/Software requirements

- OpenLDAP
  - Development packets
  - OpenLDAP servers (!!)
    - Not only the OpenLDAP packets
  - V.2.0.x
  - Should be for your distribution or you can compile it using the src files
    - Redhat, Fedora: <http://www.redhat.com>
    - Debian: <http://www.debian.org>
    - Source files: <http://www.sourceforge.net>

## → Installation of OpenLDAP

- The installation varies from OS to OS - here just a few examples for common distributions
  - RPM based (Redhat, Fedora, ...):  
`rpm -i openldap-servers.rpm`
  - Debian based: `deb openldap-servers.deb`
  - Source file (after deflating):  
`./configure`  
`make`  
`make install`

## → Configuration of OpenLDAP

- Depending on the distribution, `/etc/openldap/slapd.conf` contains the configuration for the OpenLDAP server
- Download the `H350-schema.zip` file from the workshop webpage, and unpack the files to `/etc/openldap`
  - You should find a `schema/videnet` and `schema/internet2` sub-directory (they contain the LDAP schema for H.350)

## → Configuration of OpenLDAP

- Open the slapd.conf file with an editor of your choice, and add the following lines:

```
# +CommURI en commObject
include /etc/openldap/schema/videnet/commURI.schema
include /etc/openldap/schema/videnet/commObject.schema
include /etc/openldap/schema/videnet/genericIdentity.schema
include /etc/openldap/schema/videnet/h323Identity.schema
include /etc/openldap/schema/videnet/h235Identity.schema
include /etc/openldap/schema/videnet/h320Identity.schema
include /etc/openldap/schema/videnet/sipIdentity.schema
```

# → Configuration of OpenLDAP

- Add/Change the following access restrictions (Part 1)

```
# Access restrictions
access to attr=userPassword
    by self write
    by anonymous auth
    by dn="cn=manager,dc=questnet,dc=au" write
    by * none
access to dn.subtree="dc=H350,dc=questnet,dc=au"
    by dn="cn=manager,dc=questnet,dc=au" write
    by dn.children="dc=Admins,dc=questnet,dc=au" write
# last line should take into account anonymous binds for reading info.
# E.g. from gatekeeper.
# Alternatively you can make the gatekeeper a user in the LDAP dir
# so you can bind by DN and password
# Here access is granted to read for everyone
    by * read
access to *
    by self write
    by dn="cn=manager,dc=questnet,dc=au" write
    by * read
```

## → Configuration of OpenLDAP

- Add/Change the following access restrictions (Part 2)

```
access to attr=h235IdentityPassword
    by dnattr="owner" write
    by self write
    by anonymous auth
    by dn="cn=manager,dc=questnet,dc=au" write
    by dn.children="dc=Admins,dc=questnet,dc=au" write
    by * none
access to attr=SIPIdentityPassword
    by dnattr="owner" write
    by self write
    by anonymous auth
    by dn="cn=manager,dc=questnet,dc=au" write
    by dn.children="dc=Admins,dc=questnet,dc=au" write
    by * none
```

# → Configuration of OpenLDAP

- Add/Change the search index

```
# Indices to maintain. Speed up searching etc.
index      objectClass,uid,uidNumber,gidNumber,memberUid      eq
index      cn,mail,surname,givenname                        eq,subinitial
index      commUri,commOwner,commUniqueId                  eq
index      h323IdentityGKDomain,h323IdentitydialedDigits    eq
index      h323Identityemail-ID                             eq,subinitial
```

# → Configuration of OpenLDAP

- Create an Idif file with the following entries
- Import the Idif file using the `ldapadd` command  
`ldapadd -x -D "cn=manager,dc=questnet,dc=au" -W -f <file>.ldif`

```
dn: dc=questnet,dc=au
objectClass: dcObject
objectClass: organization
dc: h350
o: h350
description: QUESTNet H.350
postalAddress: Collum $ Australia
telephoneNumber:
facsimileTelephoneNumber:
businessCategory: Network-Workshop
businessCategory: Conference
```

```
dn: ou=vcs,dc=questnet,dc=au
objectClass: top
objectClass: organizationalUnit
ou: vcs
description: Terminals
```

```
dn: ou=persons,dc=questnet,dc=au
objectClass: top
objectClass: organizationalUnit
ou: persons
Description: User
```

## → Configuration of OpenLDAP

- Create two Idif files, one with the user information, the second one with the system information, and import them using the `ldapadd` command again

User

```
dn: cn=Kewin Stoeckigt,ou=persons,dc=questnet,dc=au
cn: Kewin Stoeckigt
commURI: ldap://192.94.63.97/ou=vcs,dc=questnet,au??sub?(commUniqueID=1)
labeledURI: http://www.aarnet.edu.au/~kos/
mail: kewin.stoeckigt@aarnet.edu.au
objectClass: inetOrgPerson
objectClass: commuriobject
objectClass: organizationalPerson
objectClass: top
objectClass: person
postalAddress: Building 9 $ Banks Street $ Yarralumla ACT 2600 $ Australia
sn: kewin.stoeckigt
title: Real time communication engineer
userPassword: secret
```

# → Configuration of OpenLDAP

## System

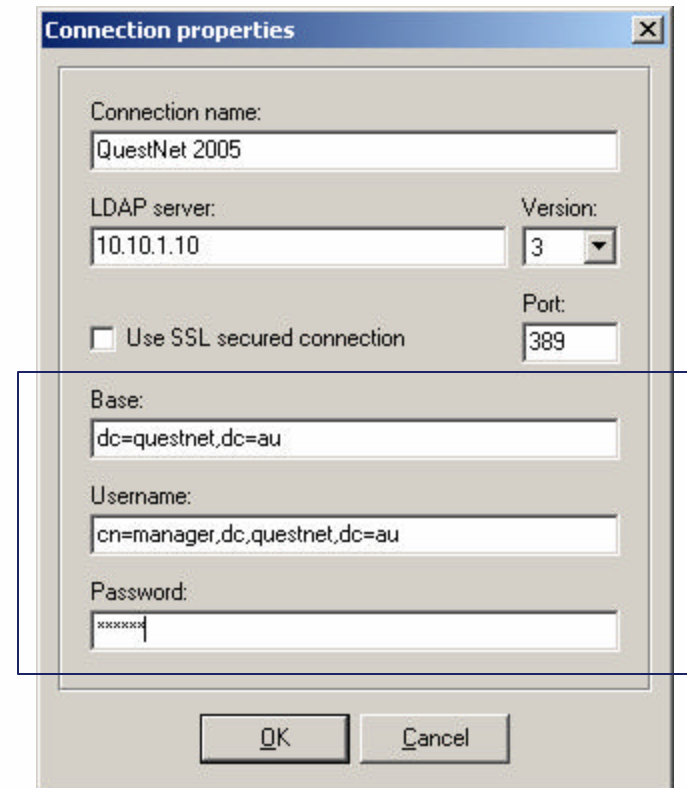
```
dn: commUniqueID=1,ou=vcs,dc=questnet,dc=au
commOwner: ldap://192.94.63.97/ou=persons,dc=questnet,dc=au??sub?(cn=Kewin Stoeckigt)
commPrivate: FALSE
commUniqueId: 1
h235IdentityEndpointID: AARNET-CBR-KOS
h235IdentityPassword: secret
h323IdentitydialedDigits: 61262224546
h323Identityemail-ID: kewin.stoeckigt@aarnet.edu.au
h323IdentityEndpointType: Terminal
h323IdentityGKDomain: 202.158.197.134
h323Identityh323-ID: AARNET-CBR-KOS
h323IdentitypartyNumber: 61262224546
h323IdentitytransportID: 192.94.63.111
h323IdentityURL-ID: h323:61262224546@202.158.197.134
objectClass: top
objectClass: commObject
objectClass: h235Identity
objectClass: h323Identity
```

## → Starting OpenLDAP and checking the configuration

- Start the LDAP server by typing in  
`/usr/sbin/slapd -f /etc/openldap/slapd.conf`
- To check the configuration, you can do an `ldapsearch`, or connect to the LDAP server using a GUI, e.g.
  - LDAP-ExplorerTools (Windows), <http://>
  - LDAP Admin (Windows),  
<http://ldapadmin.sourceforge.net>
  - Bla bla bla (Linux)
  - Ba ba ba (MAC)
  - ...

## → Starting OpenLDAP and checking the configuration

- ADD A LDAPSEARCH EXMAPLE HERE  
Idapsearch -x -D  
“dc=questnet,dc=au” ...
- Connect using a GUI



The screenshot shows a 'Connection properties' dialog box with the following fields and values:

- Connection name: QuestNet 2005
- LDAP server: 10.10.1.10
- Version: 3
- Port: 389
- Use SSL secured connection:
- Base: dc=questnet,dc=au
- Username: cn=manager,dc=questnet,dc=au
- Password: xxxxxxxx

Buttons: OK, Cancel

## → Adding new Persons/Endpoints

- There are several ways to add new Persons/Endpoints
  - Edit/Create another {user|system}.ldif file and import the information using `ldapadd`
  - Use a GUI to add new participants
  - Using a webform
    - Samples in Perl and php are available at <http://www.uab.edu>



**aarnet**

Australia's Academic  
and Research Network