In this scenario I have a center switch which will be extended in the near future with more edge devices and features. The requirement was to have 3 independent IP Groups.. DHCP and XVSS Authentication has been asked for. I've put the DHCP Server onto LDAP Server using WinRoute 3.04 and configured 3 scopes for Group 5, 6 & 7. Using the relay function on the switch will pass DHCP request direct to the DHCP Server and provide the client regarding the group membership with the proper IP out of the group's scope.
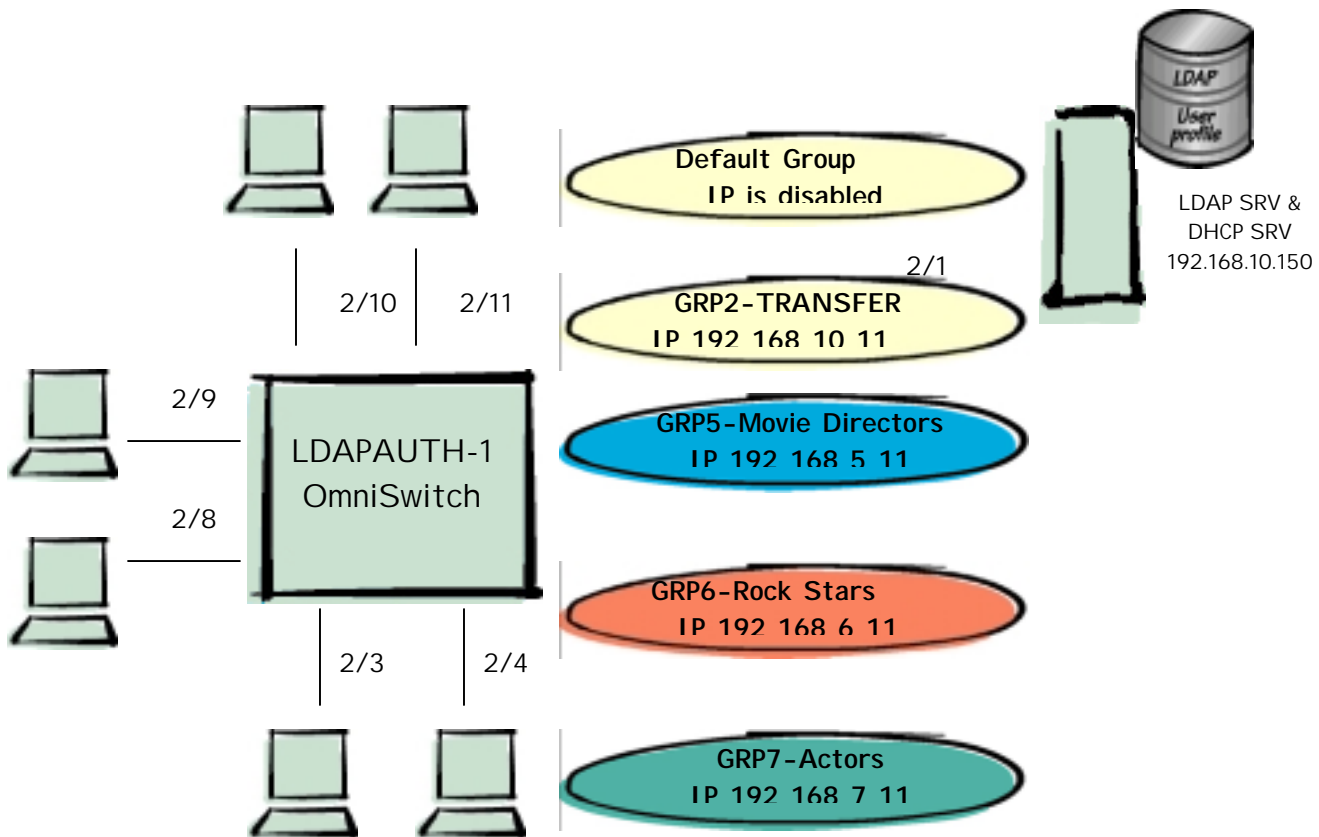
To have above drawing as a compete setup running, you have to perform a couple of steps, which may take a while.

1. Create and fill out an installation template
2. Installing Windows NT Server 4.0 (preferable US Version) and upgrade to Service Pack 4
3. Installing Netscape Directory Server 4.12
4. Configure Netscape Directory Server with Object Class and Attributes to be used for Authentication
5. Getting User's into the database and define Group membership
6. Configure Switch for Authentication and Relay
7. Installing XVSS Client on a WIN95 or WIN NT 4 Workstation
8. Verify your configuration and have a good feeling once it is running

This technical document has been created and evaluated by myself with the purpose to help friends to get into new technology and installations. There is no financial interest, however, please respect the copyright.

1. Create and fill an installation template

Before you start to install make sure you have a Windows NT 4.0 Server in Standalone mode installed with **Service Pack 4** upgraded. A template should be used during installation and also as a reference for further use.

Netscape Directory Server Parameters

Issue in a DOS BOX the command **ipconfig -all** and get the output in here

  c:\> ipconfig -all > c:\temp\ipconfig.txt

Windows NT IP Configuration

Host Name	freebird.xylan.com
DNS Servers	
Node Type	Broadcast
NetBIOS Scope ID	
IP Routing Enabled	No
WINS Proxy Enabled	No
NetBIOS Resolution Uses DNS	No

Ethernet adapter E100B20:

Description	Intel EtherExpress PRO/100B PCI LAN Adapter
Physical Address	00-A0-C9-10-BF-21
DHCP Enabled	No
IP Address	192.168.10.150
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1

Administration Accounts, Passwords and additional Information

Server and Stations

Server Name	Ip Address	Application	Service Pack	User	Password
Freebird	192.168.10.150	4.0 Server	4	admin	switch
Freebird	192.168.10.150	Directory Server Admin		admin	secret99
Freebird	192.168.10.150	Directory Manager		Directory Manager	secret99
o=xylan.com	192.168.10.150	Directory Root	used as RDN on switch	RBemsel	malibu
Default DHCP	192.168.10.150	WinRoute 3		admin	switch

This technical document has been created and evaluated by myself with the purpose to help friends to get into new technology and installations. There is no financial interest, however, please respect the copyright.

WorkStation	DHCP	Win95/NT 4		ldap user	ldap user

NetScape Directory Server   **Version: 4.12**

Administration Domain	xylan.com
Server Port	389
Administration Port	15417

OmniSwitch

SwitchType	SwitchName	Microcode	User	Password
OS-4024	LDAPAUTH-OS4024	4.1.3GA	admin	switch

Installing Windows NT Server 4.0 (preferable US Version) and upgrade to Service Pack 4

I assume that I don't need to explain how to install Windows NT Server and do a Service Pack upgrade. Just remember to install the server as **"Standalone"**

Also have Netscape Communicator 4.7 installed before you start installing Directory Server

Installing the Netscape Directory Server 4.12

Execute the installation file (d412diu.exe) and follow the directions:

You will see a welcome window and continue with clicking on **next**. You should read to Software License Agreement and if you are happy with it, click on **yes**.

Select Netscape Servers Installation, which is already default marked and click on **yes**. Next windows let you choose from Express – Typical – Custom type installation, where you should choose **Custom**.
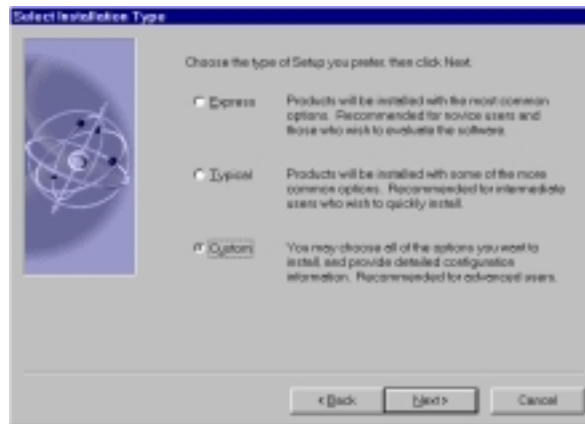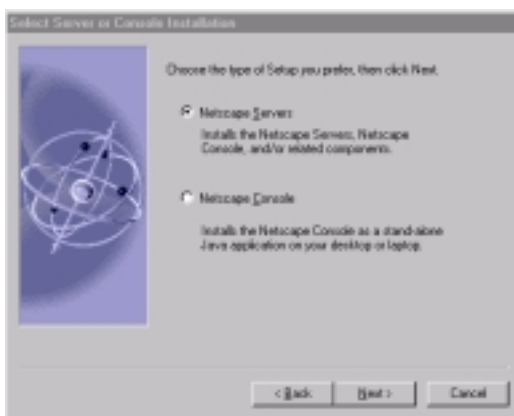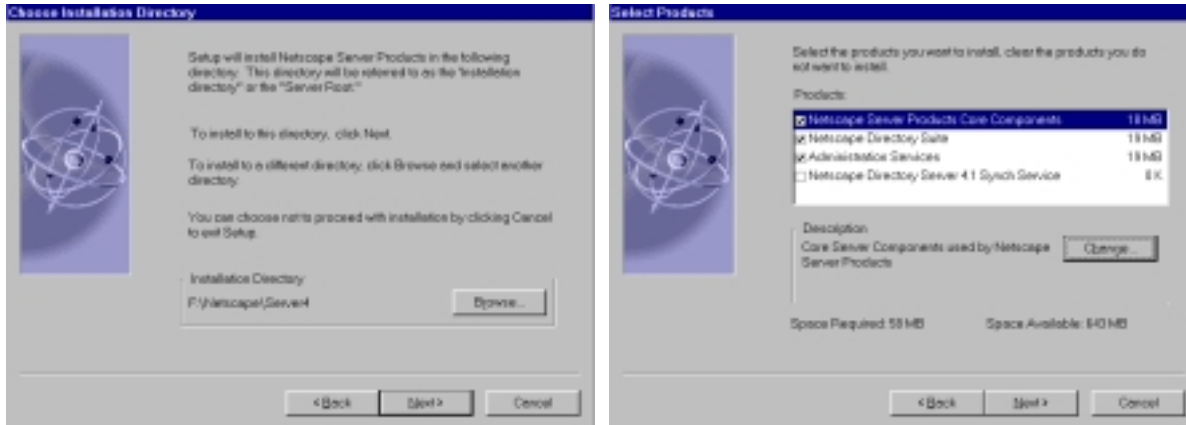

Now you can define the Installation Directory and Product Selections. On Select Products you should have selected

- Netscape Server Products Core Components
- Netscape Directory Suite
- Administration Services

If you want to check with **change** button, the selected features are all pre-selected and should remain like that.

After clicking next you should see "**This instance will be the configuration directory server**" selected, which should remain like that. Also you will be notified on the next window with pre selected "**Store data in this directory server**". Server **port** is grayed, as well as **Bind As** and **Suffix**. Compare it with your template (should be seen or if not already filled, get the missing data in you template).
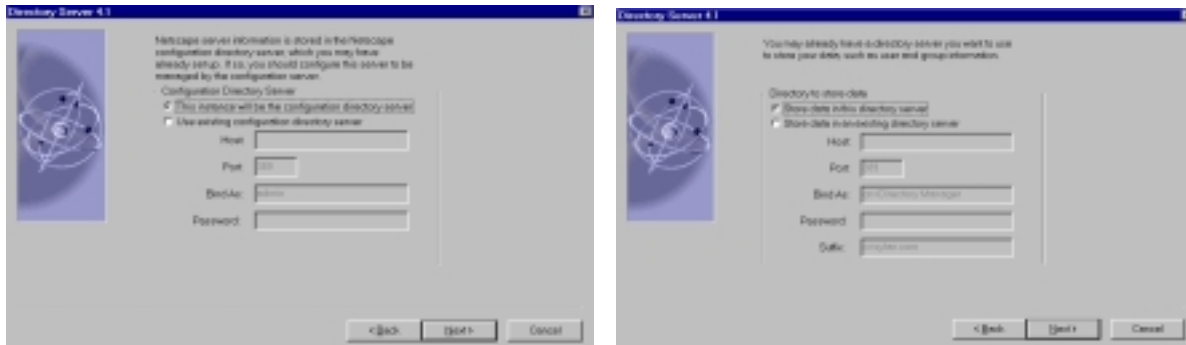

Another **Server Settings** Window will give you the opportunity the change Server Identifier, Server Port & Suffix, which should already be filled with correct data. Don't change it here, better go back and change first the Windows NT Network settings. Done this, you will have to set Directory Server Administrator's password, which I have set to **secret99**.

Now going to verify the Administration Domain. Also here is xylan.com (it's based on DNS setting on NT Server TCP/IP Properties) prewritten and should remain. Click on next and set the **password** for the Directory Manager also to **secert99**. (It's easier to remember that both admin parts on Directory Server are having the same password).

When getting the Configuration Window for Server Replication you should have "**Do not configure as a Supplier**" and also "**Do not configure as a Consumer**" selected.
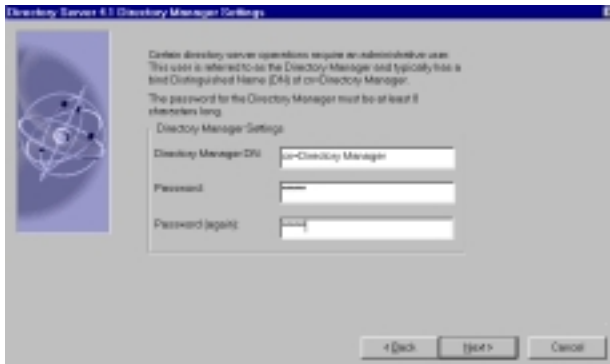
Done this you could choose to install Sample Original Structure, but don't populate Database as you don't have a proper LDIF file available.

You may have seen in the SNS User's manual (Section IP Control) to disable Schema checking. **Do not disable** yet, as if really needed you can disable Schema checking on Server's Console as well. So leave the default, which is not disabling.

This technical document has been created and evaluated by myself with the purpose to help friends to get into new technology and installations. There is no financial interest, however, please respect the copyright.

Done this, you set again a pre valued **Server IP Address**, which is the local NT Server's IP Address. Please verify if this is correct with your server, otherwise change it here.

After having IP Address checked you may want to change the server's Administrator port, as this number is choosen ramdomly and you always have to remember this port, otherwise you won't be able to connect to the user's interface of LDAP Database. If you are using this document, you may choose **15417**, as this is the number I personally always use and still remember without any template.
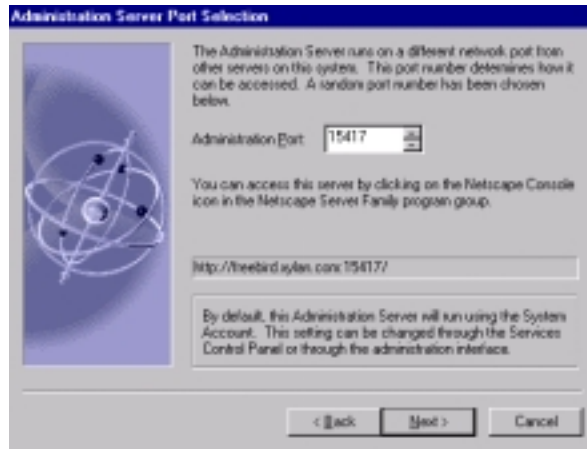
Now you have done with custom setting and you may want to verify them. You will get a Configuration Summary Window, which have listed here.

CONFIGURATION SUMMARY

[Netscape Server Products]
    Installation Directory/Server Root: F:\Netscape\Server4

[Server Core Binaries]

[Netscape Server Products Core Components]
   [Netscape Server Products Common files]
   [Core Java classes]
   [Java Runtime Environment]

 [Netscape Server Products Common files]

[Core Java classes]

[Java Runtime Environment]

[Netscape Directory Suite]
   [Netscape Directory Server]
   [Netscape Directory Management Console]

[Netscape Directory Server]
 Directory Server Settings
   Server Identifier: freebird
   Suffix: o=xylan.com
   Port: 389
   Configuration Directory Administrator ID: admin
   Administration Domain: xylan.com
   Directory Manager DN: cn=Directory Manager
   Install Sample Organizational Structure: yes
   Populate Database with:
   Disable Schema Checking: no

[Netscape Directory Management Console]

 [Administration Services]

   [Netscape Administration Server]
   [Administration Server Console]

 [Netscape Administration Server]
  Administration User ID: admin
  Administration Port: 15417
  Administration URL: http://freebird.xylan.com:15417
  Administration IP Address: 192.168.10.150

[Administration Server Console]

After having the installation process finished you will have to restart the PC

This technical document has been created and evaluated by myself with the purpose to help friends to get into new technology and installations. There is no financial interest, however, please respect the copyright.
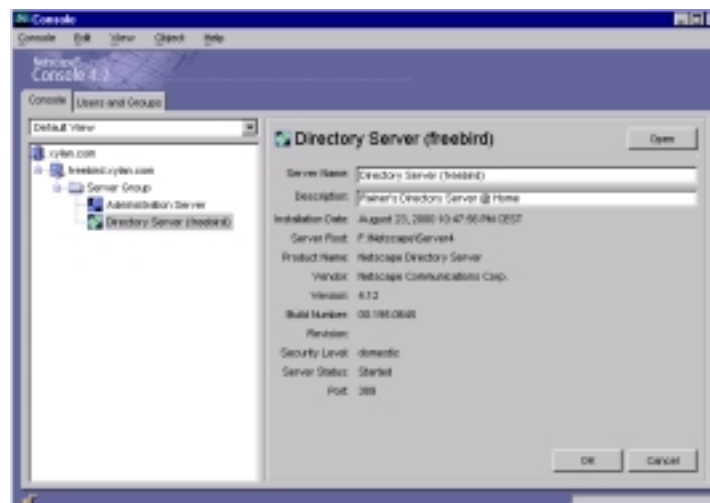
Configure Netscape Directory Server with Object Class and Attributes to be used for Authentication

NOTE: You will read sometimes "freebird", which I used as the computer name for all LDAP Installations I described in here. You may use your own computer name and remember always the different name.

1. Open Netscape Directory Console and logon as **admin** using password **secret99** (if you haven't changed my example). Administration URL should be predefined as http://freebird.xylan.com:15417
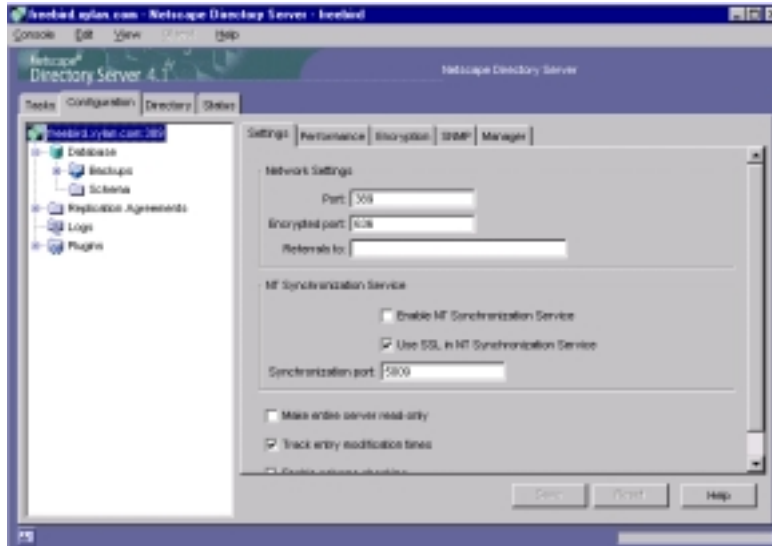
2. Expand Directory Server under Console Tab until you get to Directory Server. Select **Directory Server (freebird)** and click on right upper side on **open**.

---

4. When Directory Server is open you see the entry with Task tab activated. Click on Configuration, expand Database and click on Schema.


5. Once you have clicked on Schema the right part of the window has changed. Click on **Attributes** and you will see an empty window at User defined Attributes. Below that window there's a **create** button to add user defined attributes, which are need for User Authentication using Omni Products.
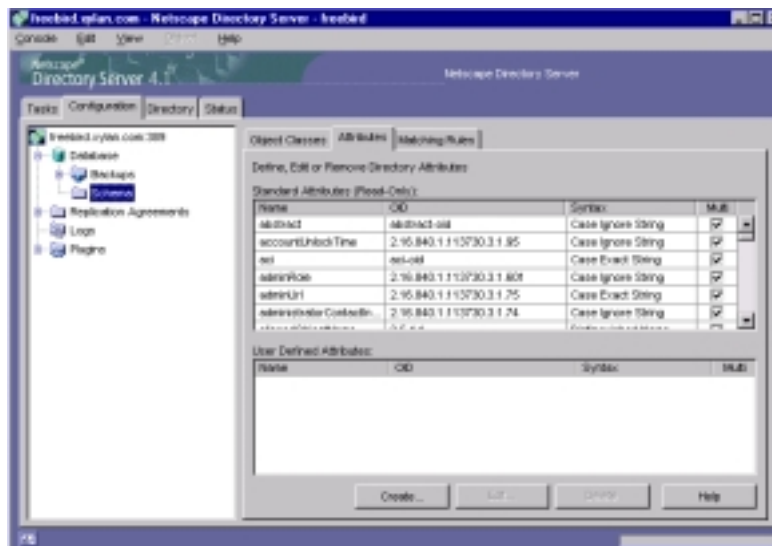
---

6. After clicked on create you now have to possibility to add all needed attributes for User Authentication.
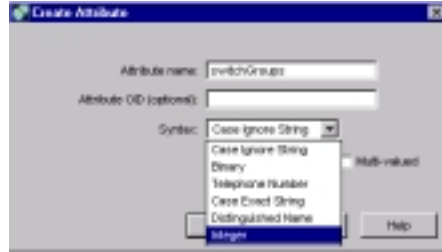
You will have to create each of below's attributes here. Attribute OID doesn't need to be filled.
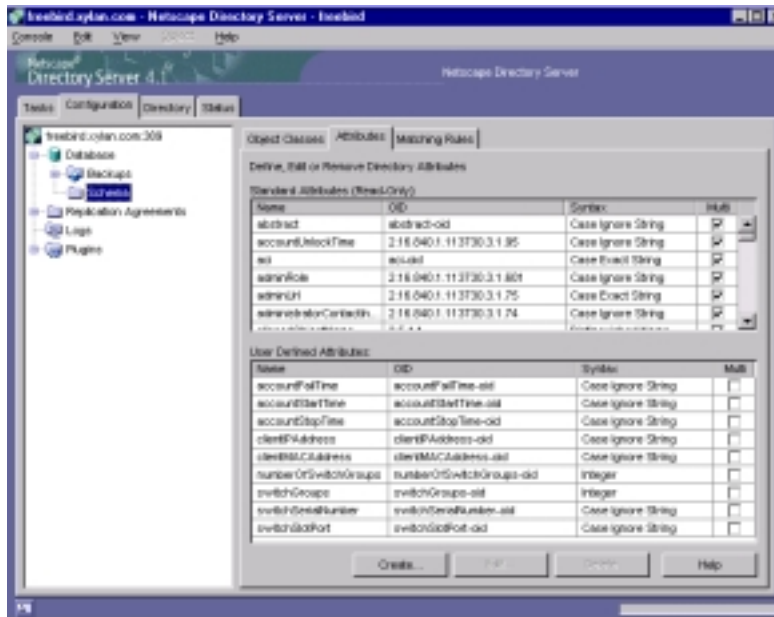
Following Attributes needs to be added in here

Attribute Name	Syntax
switchGroups	integer
numberOfSwitchGroups	integer
accountFailTime	Case Ignore String
accountStartTime	Case Ignore String
accountStopTime	Case Ignore String
switchSerialNumber	Case Ignore String
switchSlotPort	Case Ignore String
clientMACAddress	Case Ignore String
clientIPAddress	Case Ignore String

NOTE: clientMACAddress and clientIPAddress are only used for single authority mode
Once above attributes had been added you should see in the window "User defined Attributes" new values. OID values are added automatically

This technical document has been created and evaluated by myself with the purpose to help friends to get into new technology and installations. There is no financial interest, however, please respect the copyright.

To verify: Check out your directory\Netscape\Server4\slapd-freebird\config,
you should find a new time set to slapd.user_at.conf and by opening the file you see new addings.

For your convenience you may also just copy the file into your Directory Server's slapd-<servername>\config*.*.
Accept to overwrite. If you already have a pre-installed Directory Server with user defined attributes use an editor
and extend your file with the entries.

```
# User defined attributes
# These attributes can be updated via LDAP by modifing the cn=schema
# schema entry. The attributes in slapd.at.conf can not be updated
attribute switchGroups switchGroups-oid int single
attribute numberOfSwitchGroups numberOfSwitchGroups-oid int single
attribute accountFailTime accountFailTime-oid cis single
attribute accountStartTime accountStartTime-oid cis single
attribute accountStopTime accountStopTime-oid cis single
attribute switchSerialNumber switchSerialNumber-oid cis single
attribute switchSlotPort switchSlotPort-oid cis single
attribute clientMACAddress clientMACAddress-oid cis single
attribute clientIPAddress clientIPAddress-oid cis single
```

8. After having attributes added (which you will need for user defined object classes) proceed to add values into
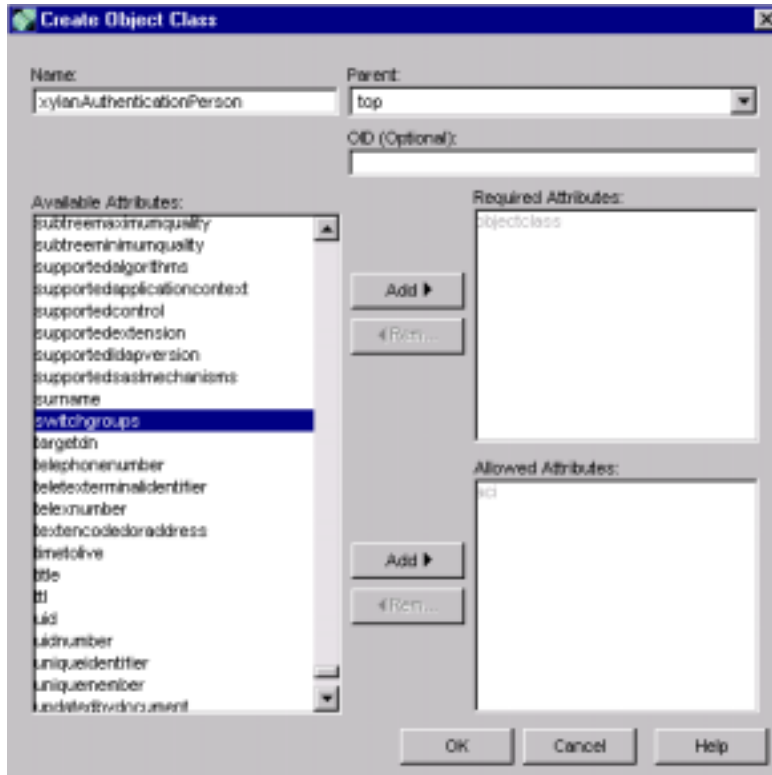slapd.user_oc.conf.

Click on Object Classes tab and on create to open a new Create Object Class Windows.

During the Creation Process you have to copy all required User Defined Attributes in the Box named Allowed Attributes.

Here's the summary:

Name:	xylanAuthenticationPerson
Parent:	top
Required Attributes:	
Allowed Attributes:	accountFailTime accountStartTime accountStopTime clientIpAddress clientMACAddress numberOfSwitchGroups switchGroups switchSeialNumber switchSlotPort

To verify: Check out your directory* \Netscape\Server4\slapd-freebird\config, you should find a new time set to slapd.user_oc.conf and by opening the file you see new addings.

For your convenience you may also just copy the file into your Directory Server's slapd-freebird\config\slapd.user_oc.conf. Accept to overwrite. If you already have a pre-installed Directory Server with user defined attributes use an editor and extend your file with the entries.

```
# user defined objectclasses
# These ObjectClasses are read/writable over LDAP
# The ObjectClasses in slapd.oc.conf are read only and may not be updated
objectclass xylanauthenticationperson
        oid xylanauthenticationperson-oid
        superior top
        allows
                accountFailTime,
                accountStartTime,
                accountStopTime,
                clientIPAddress,
                clientMACAddress,
                numberOfSwitchGroups,
                switchGroups,
                switchSerialNumber,
                switchSlotPort
```

Now it's time to get user's into your directory

Getting User's into the database and define Group membership

9. Move forward to Directory tab, highlight **xylan.com** (or the domain you are administering) and click on right mouse button. From here you can add The switch's RND to be used for **avllschain** on the switch with your directory.
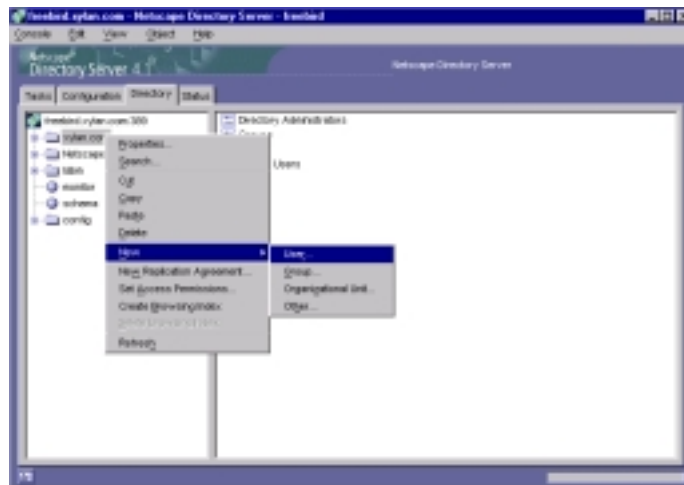
10. I have used my own name, which will be also used in the switch configuration. As password I have used **malibu**, as you will have to remember this, when configuring the switch with **avllschain** when setting the value for RDN.
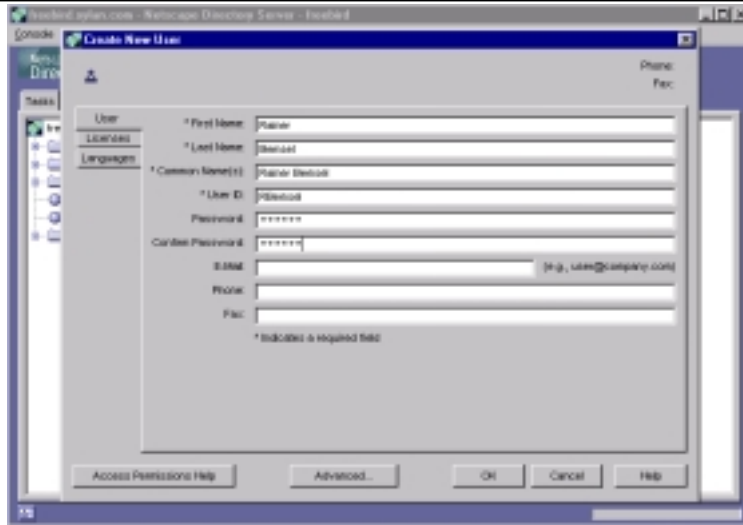
11. Again get back to Directory Window and highlight People – click on right mouse button and go to create new users. These Users are the ones, which have to authorize using XVSS Client connected to OmniSwitches. Do it the same way as you have created the Xylan.com top user. Instead of creating the users on top, you have to highlight **People**.

12. When having added the new user to the database the new name appears on the right side. Highlight the name, click on right mouse button and open the properties. When the window is open, click on Advanced to add some new attributes and values, which are <u>mandatory to have Authentication working</u>. Click **on Object Class** within this window, click on right mouse button and choose **add value.** A new window appears, scroll down to the end, finding **xylanauthenticationperson**. Highlight and click on OK.
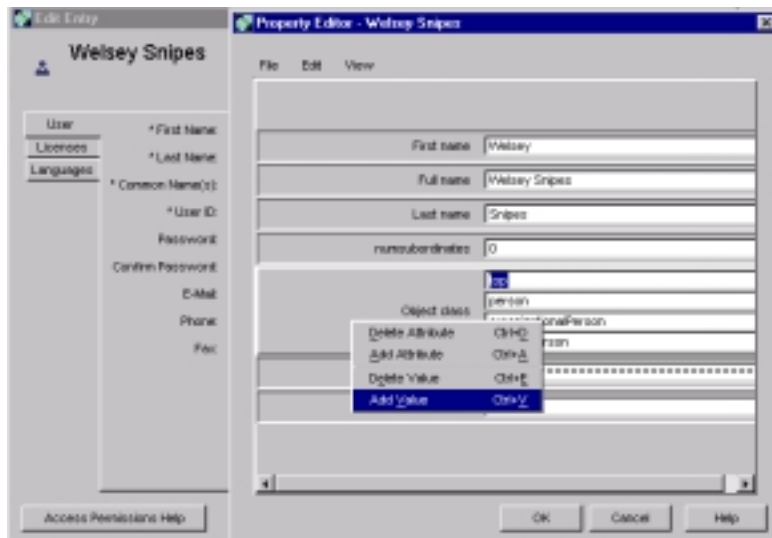
You should see a new value inside the Object Class box. Now click on **Edit** and highlight add **Attribute**.

Scroll down to find numberofswitchgroups. Highlight and click on OK. The new attribute appears in Property Window. Do it again and get attribute switchgroups into the properties. Don't forget to set values.

- numberOfSwitchGroups = 1
- switchgroups= <authenticated group> i.e. Wesley Snipes is an actor and should have access to Group No. 7, so I will set the value to **7**

Another way to get user into the database is by importing the LDIF as decribed in step <<<<XXX>>>. It's almost the same way as you did, after modifying the additional entires into the LDIF file.
Please see my exported User LDIF, which I created using Directory Server. The manual modified entries I have colorized "red"

```
dn: o=xylan.com
creatorsname: cn=Directory Manager
createtimestamp: 20000810232133Z
objectclass: top
objectclass: organization
o: xylan.com
aci: (targetattr = "*")(version 3.0; acl "Allow self entry modification"; allow (write)userdn =
"ldap:///self";)aci: (targetattr != "userPassword") (version 3.0; acl "Anonymous access"; allo
w (read, search, compare)userdn = "ldap:///anyone";)aci: (targetattr = "*")(version 3.0; acl
"Configuration Adminstrator"; allow ( all) userdn = "ldap:///uid=admin, ou=Administrators,
ou=TopologyManagement,  o=NetscapeRoot");)aci: (targetattr ="*")(version 3.0;acl "Configuration
Administrators Group";al low (all) (groupdn = "ldap:///cn=Configuration Administrators, ou=Groups, ou
=TopologyManagement, o=NetscapeRoot");)aci: (targetattr ="*")(version 3.0;acl "Directory Administrators
Group";allow  (all) (groupdn = "ldap:///ou=Directory Administrators, o=xylan.com");)
aci: (targetattr = "*")(version 3.0; acl "SIE Group"; allow (all)groupdn = "ld ap:///cn=slapd-freebird,
cn=Netscape Directory Server, cn=Server Group, cn=f reebird.xylan.com, ou=xylan.com,
o=NetscapeRoot";)modifiersname: cn=Directory Manager
modifytimestamp: 20000810232136Z

dn: ou=Directory Administrators, o=xylan.com
description: Entities with administrative access to this directory server
creatorsname: cn=Directory Manager
createtimestamp: 20000810232133Z
objectclass: top
objectclass: organizationalunit
objectclass: groupofuniquenames
ou: Directory Administrators
cn: Directory Administrators
modifiersname: cn=Directory Manager
modifytimestamp: 20000810232136Z

dn: ou=Groups, o=xylan.com
objectclass: top
objectclass: organizationalunit
ou: Groups
creatorsname: cn=Directory Manager
modifiersname: cn=Directory Manager
createtimestamp: 20000810232136Z
modifytimestamp: 20000810232136Z

dn: ou=People, o=xylan.com
objectclass: top
objectclass: organizationalunit
ou: People
aci: (targetattr ="userpassword || telephonenumber || facsimiletelephonenumber
 ")(version 3.0;acl "Allow self entry modification";allow (write)(userdn = "l dap:///self");)aci:
(targetattr !="cn || sn || uid")(targetfilter ="(ou=Accounting)")(version  3.0;acl "Accounting Managers
Group Permissions";allow (write)(groupdn = "ld ap:///cn=Accounting
Managers,ou=groups,o=xylan.com");)aci: (targetattr !="cn || sn || uid")(targetfilter ="(ou=Human
```

```
Resources)")(version 3.0;acl "HR Group Permissions";allow (write)(groupdn = "ldap:///cn=HR
 Managers,ou=groups,o=xylan.com");)aci: (targetattr !="cn ||sn || uid")(targetfilter ="(ou=Product
Testing)")(ver sion 3.0;acl "QA Group Permissions";allow (write)(groupdn = "ldap:///cn=QA M
 anagers,ou=groups,o=xylan.com");)aci: (targetattr !="cn || sn || uid")(targetfilter ="(ou=Product
Development)" )(version 3.0;acl "Engineering Group Permissions";allow (write)(groupdn = "l
 dap:///cn=PD Managers,ou=groups,o=xylan.com");)
creatorsname: cn=Directory Manager
modifiersname: cn=Directory Manager
createtimestamp: 20000810232136Z
modifytimestamp: 20000810232136Z

dn: ou=Special Users,o=xylan.com
objectclass: top
objectclass: organizationalUnit
ou: Special Users
description: Special Administrative Accounts
creatorsname: cn=Directory Manager
modifiersname: cn=Directory Manager
createtimestamp: 20000810232136Z
modifytimestamp: 20000810232136Z

dn: uid=JCarpenter,ou=People, o=xylan.com
switchgroups: 5
mail:
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: xylanauthenticationperson
cn: John Carpenter
uid: JCarpenter
givenname: John
sn: Carpenter
numberofswitchgroups: 1
creatorsname: uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot
createtimestamp: 20000818163638Z
userpassword: snake
modifiersname: uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoo
 t
modifytimestamp: 20000818164945Z

dn: uid=rvzant,ou=People, o=xylan.com
switchgroups: 6
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: xylanauthenticationperson
cn: Ronnie VanZant
uid: rvzant
givenname: Ronnie
sn: VanZant
userpassword: freebird
numberofswitchgroups: 1
creatorsname: uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot
modifiersname: uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoo
 t
createtimestamp: 20000818163757Z
modifytimestamp: 20000818163757Z

dn: uid=WSnipes,ou=People, o=xylan.com
switchgroups: 7
objectclass: top
objectclass: person
```

```
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: xylanauthenticationperson
cn: Wesley Snipes
uid: WSnipes
givenname: Wesley
sn: Snipes
userpassword: blade
numberofswitchgroups: 1
creatorsname: uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot
modifiersname: uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot
createtimestamp: 20000818163858Z
modifytimestamp: 20000818163858Z

dn: uid=MGibson,ou=People, o=xylan.com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: xylanauthenticationperson
cn: Mel Gibson
uid: MGibson
givenname: Mel
sn: Gibson
userpassword: payback
numberofswitchgroups: 1
creatorsname: uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot
createtimestamp: 20000818164021Z
switchgroups: 7
modifiersname: uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot
modifytimestamp: 20000818173452Z

dn: uid=jwalsh,ou=People, o=xylan.com
switchgroups: 6
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: xylanauthenticationperson
cn: Joe Walsh
uid: jwalsh
givenname: Joe
sn: Walsh
userpassword: rocky
numberofswitchgroups: 1
creatorsname: uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot
modifiersname: uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot
createtimestamp: 20000818164324Z
modifytimestamp: 20000818164324Z

dn: uid=JBruck,ou=People, o=xylan.com
switchgroups: 5
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: xylanauthenticationperson
cn: Jerry Bruckheimer
uid: JBruck
givenname: Jerry
sn: Bruckheimer
userpassword: conair
numberofswitchgroups: 1
```

```
creatorsname: uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot
modifiersname: uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot
createtimestamp: 20000818164714Z
modifytimestamp: 20000818164714Z


dn: uid=RBemsel,o=xylan.com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
cn: Rainer Bemsel
uid: RBemsel
givenname: Rainer
sn: Bemsel
userpassword: malibu
creatorsname: uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot
modifiersname: uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot
createtimestamp: 20000823150029Z
modifytimestamp: 20000823150029Z
```

Configure Switch for Authentication and Relay

Verify your hardware

```
LDAPAUTH-1 / >slot


      Module-Type Adm-Status  HW    Board     Mfg    Firmware-Version
 Slot Part-Number Oper-Status Rev   Serial #  Date   Base-MAC-Address
 ---- ----------- ----------- ----- --------- ------ -----------------
 1*      MPM 1G   Enabled      A6    71221951 03/20/97 4.1.3 GA
         05014306 Operational                         00:20:da:8b:5c:7f

 2       Ether/12 Enabled      E2    71245118 10/24/97 4.1.3 GA
         05011206 Operational                         00:20:da:7e:33:4`

 3          Empty

LDAPAUTH-1 / >
```

Turn Group Mobility on

```
LDAPAUTH-1/ >gmcfg
Group Mobility is Disabled. Enable Group Mobility ? [yes/no] (no): y
move_to_def is set to Disabled. Set to Enable ? [yes/no] (no): <return>
def_group is set to Enable. Set it to Disable ? [yes/no] (no): <return>
LDAPAUTH-1/ >
```

Disable IP on Default Group

```
LDAPAUTH-1/ >modvl 1
Current values associated with GROUP 1.1 are as follows:
1) GROUP Number - 1:1
2) Description - Default GROUP (#1)
IP parameters:
3) IP enabled - Y
4) IP Network Address - 192.168.10.1
```

```
5) IP Subnet Mask - 255.255.255.0
6) IP Broadcast Address - 192.168.10.255
7) Router Description - GROUP #1.0 IP router vport
8) RIP Mode - Silent
{Active(a), Inactive(i), Deaf(d), Silent(s)}
9) Routing disabled - N
10) NHRP enabled - N
11) Default Framing - Ethernet II
{Ethernet II(e), Ethernet 802.3(8)}
IPX parameters:
12) IPX enabled - N
(save/quit/cancel)
: 3=n
: save
LDAPAUTH-1/ >gp
Group                                              Network Address      Proto/
ID                Group Description               (IP Subnet Mask)      Encaps
(:VLAN ID)                                         or (IPX Node Addr)
===== =============================== =============== ========
1 Default GROUP (#1)
```

4. Create a Transfer Group

```
LDAPAUTH-1/ >
LDAPAUTH-1/ >crgp
GROUP Number ( 2) :
Description (no quotes) : TRANSFER

Enable WAN Routing? (n):
Enable ATM CIP? (n):
Enable IP (y) :
IP Address : 192.168.10.1
IP Subnet Mask (0xffffff00) :
IP Broadcast Address (192.168.10.255 ) :
Description (30 chars max) :
Configure as Loopback? (n) :
Disable routing? (n) :
Enable NHRP? (n) :
IP RIP mode {Deaf(d),
Silent(s),
Active(a),
Inactive(i)} (s) :
Default framing type {Ethernet II(e),
Ethernet 802.3 SNAP(8)} (e) :
Enable IPX? (y): n
Enter a priority level (0...7)(0):
Enable Group Mobility on this Group ? [y/n](n): y
Enable User Authentication for this Group [y/n](n): y
Enable Spanning Tree for this group [y/n](y):
Do you wish to configure the interface group for this Virtual LAN
at this time? (y)
Initial Vports(Slot/Phys Intf. Range) - For example, first I/O Module
(slot 2), second Interface would be 2/2. Specify a range of interfaces
and/or a list as in: 2/1-3, 3/3, 3/5, 4/6-8.
Initial Slot/Interface Assignments: 2/1
2/1 - This interface is currently assigned to GROUP 1 -
(Default GROUP (#1)).
Do you wish to remove it from that GROUP and assign it (with
new configuration values) to this GROUP [y|n|c to Accept defaults] (n)? c
Adding port 2/1 to GROUP 2...
You may modify interfaces to this group using the addvp, modvp and rmvp
commands at a later date if you choose.
Configure Auto-Activated LEC service ? [y/n](y): n
```

```
Select Protocol for this group:
1. IP
2. IPX
3. DECNET
4. APPLETALK
5. Protocol specified by ether-type (in hex)
6. Protocol specified by DSAP and SSAP (in hex)
7. Protocol specified by SNAP (in hex)
8. ALL PROTOCOLS
Enter protocol type (1): 8
Configure binding rules for this group [y/n](y): n
LDAPAUTH-1/ >
```

Create your authenticated User Groups

GROUP No. 5

```
LDAPAUTH-1/ >
LDAPAUTH-1/ >crgp
GROUP Number ( 3 ) : 5
Description (no quotes) : MOVIE DIRECTORS
Enable WAN Routing? (n):
Enable ATM CIP? (n):
Enable IP (y) :
IP Address : 192.168.5.1
IP Subnet Mask (0xffffff00) :
IP Broadcast Address (192.168.10.255 ) :
Description (30 chars max) :
Configure as Loopback? (n) :
Disable routing? (n) :
Enable NHRP? (n) :
IP RIP mode {Deaf(d),


Silent(s),
Active(a),
Inactive(i)} (s) :
Default framing type {Ethernet II(e),
Ethernet 802.3 SNAP(8)} (e) :
Enable IPX? (y): n
Enter a priority level (0...7)(0):
Enable Group Mobility on this Group ? [y/n](n): y
Enable User Authentication for this Group [y/n](n): y
Enable Spanning Tree for this group [y/n](y):
Do you wish to configure the interface group for this Virtual LAN
at this time? (y) n

Group 5 has been added to the system
You may modify interfaces to this group using the addvp, modvp and rmvp
commands at a later date if you choose.
Configure Auto-Activated LEC service ? [y/n](y): n
Select Protocol for this group:
1. IP
2. IPX
3. DECNET
4. APPLETALK
5. Protocol specified by ether-type (in hex)
6. Protocol specified by DSAP and SSAP (in hex)
7. Protocol specified by SNAP (in hex)
8. ALL PROTOCOLS
Enter protocol type (1): 8
Configure binding rules for this group [y/n](y): n
LDAPAUTH-1/ >
```

GROUP No. 6

```
LDAPAUTH-1/ >
LDAPAUTH-1/ >crgp
GROUP Number ( 2) : 6
Description (no quotes) : ROCK STARS
Enable WAN Routing? (n):
Enable ATM CIP? (n):
Enable IP (y) :
IP Address : 192.168.6.1
IP Subnet Mask (0xffffff00) :
IP Broadcast Address (192.168.10.255 ) :
Description (30 chars max) :
Configure as Loopback? (n) :
Disable routing? (n) :
Enable NHRP? (n) :
IP RIP mode {Deaf(d),
Silent(s),
Active(a),
Inactive(i)} (s) :
Default framing type {Ethernet II(e),
Ethernet 802.3 SNAP(8)} (e) :
Enable IPX? (y): n
Enter a priority level (0...7)(0):
Enable Group Mobility on this Group ? [y/n](n): y
Enable User Authentication for this Group [y/n](n): y
Enable Spanning Tree for this group [y/n](y):
Do you wish to configure the interface group for this Virtual LAN
at this time? (y) n

Group 6 has been added to the system
You may modify interfaces to this group using the addvp, modvp and rmvp
commands at a later date if you choose.
Configure Auto-Activated LEC service ? [y/n](y): n
Select Protocol for this group:
1. IP
2. IPX
3. DECNET


4. APPLETALK
5. Protocol specified by ether-type (in hex)
6. Protocol specified by DSAP and SSAP (in hex)
7. Protocol specified by SNAP (in hex)
8. ALL PROTOCOLS
Enter protocol type (1): 8
Configure binding rules for this group [y/n](y): n
LDAPAUTH-1/ >
```

GROUP No. 7

```
LDAPAUTH-1/ >
LDAPAUTH-1/ >crgp
GROUP Number ( 2) : 7
Description (no quotes) : ACTORS
Enable WAN Routing? (n):
Enable ATM CIP? (n):
Enable IP (y) :
IP Address : 192.168.7.1
IP Subnet Mask (0xffffff00) :
IP Broadcast Address (192.168.10.255 ) :
Description (30 chars max) :
Configure as Loopback? (n) :
Disable routing? (n) :
Enable NHRP? (n) :
```

This technical document has been created and evaluated by myself with the purpose to help friends to get into new technology and installations. There is no financial interest, however, please respect the copyright.

```
IP RIP mode {Deaf(d),
Silent(s),
Active(a),
Inactive(i)} (s) :
Default framing type {Ethernet II(e),
Ethernet 802.3 SNAP(8)} (e) :
Enable IPX? (y): n
Enter a priority level (0...7)(0):
Enable Group Mobility on this Group ? [y/n](n): y
Enable User Authentication for this Group [y/n](n): y
Enable Spanning Tree for this group [y/n](y):
Do you wish to configure the interface group for this Virtual LAN
at this time? (y) n

Group 7 has been added to the system
You may modify interfaces to this group using the addvp, modvp and rmvp
commands at a later date if you choose.
Configure Auto-Activated LEC service ? [y/n](y): n
Select Protocol for this group:
1. IP
2. IPX
3. DECNET
4. APPLETALK
5. Protocol specified by ether-type (in hex)
6. Protocol specified by DSAP and SSAP (in hex)
7. Protocol specified by SNAP (in hex)
8. ALL PROTOCOLS
Enter protocol type (1): 8
Configure binding rules for this group [y/n](y): n
LDAPAUTH-1/ >
```

Check your groups

```
LDAPAUTH-1 / >gp
Group                              Network Address  Proto/
 ID        Group Description       (IP Subnet Mask)  Encaps
(:VLAN ID)                         or (IPX Node Addr)
===== ============================= =============== ========
    1 Default GROUP (#1)
    2 Transfer                     192.168.10.1     IP  /
                                    (ff.ff.ff.00 )   ETH2
    5 Movie Directors              192.168.5.1      IP  /


                                    (ff.ff.ff.00 )   ETH2
    6 Rock Stars                   192.168.6.1      IP  /
                                    (ff.ff.ff.00 )   ETH2
    7 Actors                       192.168.7.1      IP  /
                                    (ff.ff.ff.00 )   ETH2
LDAPAUTH-1 / >
```

Activate Authentication

```
LDAPAUTH-1/ >
LDAPAUTH-1/ >layer2
Layer 2 User Authentication is not enabled
Set authentication type to? (r=RADIUS, l=LDAP) : () : l
Set authentication to? (0=Disabled, 1=Enabled) : (0) : 1
LDAPAUTH-1/ >
```

Configure Directory Server Connection

```
LDAPAUTH-1/ >avllschain
LDAP server search base? () : o=xylan.com
LDAP server super user rdn? () : uid=RBemsel
LDAP super user password? () : malibu (this entry is hidden)
Please enter password once more: () :malibu (this entry is hidden)
Enter LDAP server in the format: IPaddress:Port. Separate each server by space.
LDAP server chain? () : 192.168.10.150:389
LDAP server type to?
(1=Generic Schema, 2=Netscape Directory Server)
(3=Novell NDS, 4=Sun Directory Services) : () : 2
LDAP server retry attempts: () : 3
LDAP server response timeout (Seconds): () : 30
LDAP server accounting? (on/off: 1=on, 2=off) : () : 1
LDAP server login fail log identifier? () : DENIED !!!
LDAPAUTH-1/ >
```

Check connectivity to Directory Server

```
LDAPAUTH-1/ >avlslserver
LDAP server (192.168.10.150:389) is alive and happy
LDAPAUTH-1/ >
```

Configure Ports for Authentication

```
LDAPAUTH-1/ >
LDAPAUTH-1/ >avlports
Do you wish to add or delete a port (add) : <return>
Which ports do you wish to add : 2/3, 2/4, 2/8, 2/9, 2/10, 2/11
LDAPAUTH-1/ >
```

Configure DHCP Relay Function

```
LDAPAUTH-OS4024 / >relayc
UDP Relay Configuration
1) BOOTP/DHCP Enabled : No
2) NBNS Enabled : No
3) NBDD Enabled : No
4) +Generic Services Menu
Command {Item=Value/?/Help/Quit/Redraw/Save} (Redraw) : 1=yes
UDP Relay Configuration
1) BOOTP/DHCP Enabled : Yes
11) Server Address {list/add/delete} : UNSET
12) Forward Delay : 3
13) Maximum Hops : 4
2) NBNS Enabled : No
3) NBDD Enabled : No
4) +Generic Services Menu
Command {Item=Value/?/Help/Quit/Redraw/Save} (Redraw) : 11=add
FORWARD TO Server List
Item Server address Server Name (if known)
Enter IP address or host name of server to be added to list ['h' for help/<ret>
to exit] : 192.168.10.150
FORWARD TO Server List


Item Server address Server Name (if known)
1) 192.168. 10.150
Enter IP address or host name of server to be added to list ['h' for help/<ret>
to exit] : <return>

UDP Relay Configuration
1) BOOTP/DHCP Enabled : Yes
11) Server Address {list/add/delete} : SET
12) Forward Delay : 3
```

This technical document has been created and evaluated by myself with the purpose to help friends to get into new technology and installations. There is no financial interest, however, please respect the copyright.

```
13) Maximum Hops : 4
2) NBNS Enabled : No
3) NBDD Enabled : No
4) +Generic Services Menu
Command {Item=Value/?/Help/Quit/Redraw/Save} (Redraw) : save
Saving config for service 0
Starting task
UDP Relay configuration change, service 1:
UDP Relay initializing....UDP Relay initialized.
LDAPAUTH-1 / >
LDAPAUTH-1 / >
```

Finally do a reboot

```
LDAPAUTH-1 / >reboot
Confirm? (n) : y
Locking filesystem...locked
System going down immediately...
switch[4a5efbe8]: System rebooted by admin..........
```

Installing XVSS Client on a WIN95 or WIN NT 4 Workstation

Please refer to one of my older OmniTips: "Authentication with Radius" where I have decribed the steps to install the XVSS Client. Make sure you have DLC 32Bit Protocol available, as you need it to get XVSS running.

Verify your configuration and have a good feeling once it is running

A nice demonstration is by verifying the group membership of the port.

Do a vi on a certain port, where you have a XVSS client connected. You should group membership 1 (as the default). After authorizing using XVSS you should see a change at the group membership, which should now say either 5, 6 or 7, depending, what user you have used to authorize. Also open up the IP configuration tool on Windows 95 (winipcfg.exe) and see the proper IP Address.

If you have any questions, please do not hesitate to contact me via rbemsel@ind.alcatel.com.

This technical document has been created and evaluated by myself with the purpose to help friends to get into new technology and installations. There is no financial interest, however, please respect the copyright.