User Authentication with OpenLdap and Xylan OmniSwitch

This document describes how to install and extend the schema file used by OpenLdap and how to configure an OmniStack to have Authentication running.

I will describe following Topics to understand the configuration made with OpenLdap (slapd). OpenLdap handles schema files a bit different as Netscape, so I think it's quite reasonable to point them out. LDAP version 3, which is needed for authentication is not supported on OpenLdap 1.x. Make sure you have 2.x available.

Also I've included some outlines and description from the Administrator's guide of OpenLdap to provide a common understanding. OpenLdap does not provide any fancy and windows like tools, so everything is done via command line utilities. There might be some good tools out there, but this is not part of this document.

1. Installing OpenLdap on RedHat Linux 7.0
2. Distributed Schema files
3. Extending Schema
4. Object Identifiers
5. Name Prefix
6. Local Schema file
7. Attribute type Specification
8. User defined attributes for user Authentication
9. Object class specification for User Authentication
10. Directory structure
11. LDIF File for User Authentication
12. Start LDAP server
13. Import LDIF File into database
14. Stop LDAP server
15. Physical and logical layout
16. Configure OmniStack 5024

1. Installing OpenLdap on RedHat Linux 7.0

I've used OpenLdap Version 2.0.7. You may have a newer version running, when you do this installation. The modified slapd.conf I describe here could be downloaded from www.bemsel.com/sampleconfig/openldap20001201.zip

```
1. Download openldap-2.0.7.tgz from www.openldap.org into /tmp
2. gunzip –c openldap-2.0.7.tgz |tar xvfB –
3. cd /tmp/openldap-2.0.7
4. ./configure
5. make depend
6. make
7. su root –c 'make install'
8. vi /usr/local/etc/openldap/slapd.conf
   a) change suffix from dc=my-domain into o=bemsel.com
   b) change rootdn's entry with proper domain as in a)
```

9. su root –c /usr/local/libexec/slapd
10. ps –ef |grep slapd (to be sure slapd is running)

Check if LDAP server is running

```
ldapsearch –h 192.168.10.150  –x –b ‘‘ –s base ‘(objectclass=*)’ namingContexts
```

You should get an output like that:

```
Version: 2

#
# filter: objectclass=*
# requesting: namingContexts
#

#
dn:
namingContext: o=bemsel.com

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Don’t get confused to see Version 2. By definition, if you are running OpenLdap version 2.0.x, it will answer to v3 ldap queries. This took me a while to figure out, why there’s no need to explicitly define LDAP version 3 in this configuration.

2. Distributed Schema files

OpenLdap is distributed with a set of schema specifications for your use. Each set is defined in a file suitable for inclusion (using the include directive) in your slapd.conf file. These schema files are normally installed in the `/usr/local/etc/openldap/schema` directory. During the configuration you will create a new schema file, called **xylanauthenticationperson.schema** and store the file in above mentioned schema directory.

Provided Schema Specifications

File	Description
core.schema	OpenLdap core (required)
cosine.schema	Cosine and Internet X.500 (useful)
inetorgperson.schema	InetOrgPersona (useful)
misc.schema	Assorted (experimental)
nadf.schema	North American Directory Forum (FYI)
nis.schema	Network Information Services (FYI)
openldap.schema	OpenLdap Project (experimental)

To use any of these schema files, you also need to include the desired file in the global definition portion of your **slapd.conf** file.

```
# include schema
include /usr/local/etc/openldap/schema/core.schema
include /usr/local/etc/openldap/schema/cosine.schema
include /usr/local/etc/openldap/schema/inetorgperson.schema
include /usr/local/etc/openldap/schema/xylanauthenticationperson.schema
```

The red line is the include statement to be used with the new schema file. You have to have all four include statements, otherwise it won't work. Needless to say, these schema files have to be available.

3. Extending Schema

Some words on Schema
Schema used by slapd may be extended to support additional syntaxes, matching rules, attribute types and object classes. In Authentication's phase you have to do some typing before you could go forward to the next step.

There are five steps to define new schema:

1. obtain Object Identifier
2. choose a name prefix
3. create local schema file
4. define custom attribute types
5. define custom object classes

4. Object Identifiers

Each schema element is identified by a globally unique Object Identifier (OID). OIDs are also used to identify other objects. They are commonly found in protocols described by ASN.1. In particular, they are heavily used by the Simple Network Management Protocol (SNMP). As OIDs are hierarchical, your organization can obtain one OID and branch it as needed. In the case of Xylan Corporation or now Alcatel e-Business Networking Division the used Enterprise OID is like following.

1.3.6.1.4.1.800

So, when you go to branch this OID, with new defined Schema I consider to use following hierarchical design. An example of structured OID for Authentication, you will find later on.

1.3.6.1.4.1.800.2	-> LDAP Element
1.3.6.1.4.1.800.2.1	-> Attribute
1.3.6.1.4.1.800.2.1.1	-> user defined Attribute
1.3.6.1.4.1.800.2.2	-> Object Class
1.3.6.1.4.1.800.2.2.1	-> user defined Object Class

to complete the list, here's the branch for SNMP

1.3.6.1.4.1.800.1 -> SNMP Element

To verify other's OID's, please have a look at

http://www.alvestrand.no/objectid/1.3.6.1.4.1.800.html

Other's could also be queried using following link

http://www.alvestrand.no/objectid/top.html

You are, of course, free to design a hierarchy suitable to your organizational needs under your organization's OID. No matter what hierarchy you choose, you should maintain a registry of assignments you make. This can be a simple flat file or a something more sophisticated such as the *OpenLDAP OID Registry*

5. Name Prefix

In addition to assign a unique object identifier to each schema element, you should provide a least one textual name for each element. The name should be both descriptive and not likely to clash with names of other schema elements. In particular, any name you choose should not clash with present or future Standard Track names.

To reduce (but not eliminate) the potential for name clashes, the convention is to prefix names of non-Standard Track with a few letters to localize the changes to your organization. The smaller the organization, the longer your prefix should be.

6. Local Schema file

The objectclass and attributeTypes configuration file directives can be used to define schema rules on entries in the directory. It is customary to create a file to contain definitions of your custom schema items. OpenLdap recommends you create a file local.schema in

```
/usr/local/etc/openldap/schema/local.schema
```

and then include this file in your *slapd.conf* file immediately after other schema include directives. This is, what I've done in the beginning of this paragraph (the red line, do you remember), only the name is different. Instead of using local.schema I've used for identification "xylanauthenticationperson.schema"

```
# include schema
include /usr/local/etc/openldap/schema/core.schema
include /usr/local/etc/openldap/schema/cosine.schema
include /usr/local/etc/openldap/schema/inetorgperson.schema
# include user defined schema
include /usr/local/etc/openldap/schema/xylanauthenticationperson.schema
```

7. Attribute type Specification

The *attributetype* directive is used to define a new attribute type. The directive uses the same Attribute Type Description (as defined in RFC2252) used by the attributeTypes attribute found in the subschema subentry

Notice that each defines the attribute's OID and descriptive names. Each name is an alias for the OID. *slapd*(8) returns the first listed name when returning results.
The first attribute, name, has a syntax of directoryString (a UTF-8 encoded Unicode string) with a recommend maximum length. Note that syntaxes are specified by OID. In addition, the equality and substring matching uses case ignore rules. Below are tables listing commonly used supported syntax and matching rules.

Name	OID	Description
binary	1.3.6.1.4.1.1466.115.121.1.5	BER/DER data
boolean	1.3.6.1.4.1.1466.115.121.1.7	Boolean value
distinguishedName	1.3.6.1.4.1.1466.115.121.1.12	DN
directoryString	1.3.6.1.4.1.1466.115.121.1.15	UTF-8 string
IA5String	1.3.6.1.4.1.1466.115.121.1.26	ASCII string
Integer	1.3.6.1.4.1.1466.115.121.1.27	integer
Name and Optional UID	1.3.6.1.4.1.1466.115.121.1.34	DN plus UID
Numeric String	1.3.6.1.4.1.1466.115.121.1.36	numeric string
OID	1.3.6.1.4.1.1466.115.121.1.38	object identifier
Octect String	1.3.6.1.4.1.1466.115.121.1.40	arbitary octets
Printable String	1.3.6.1.4.1.1466.115.121.1.44	printable string

8. User Defined Attributes and ObjectClass for User Authentication

XylanAuthenticationPerson.schema has been modified with OIDs by myself.

```
attributetype ( 1.3.6.1.4.1.800.2.1.1.1
      NAME 'switchGroups'
      DESC 'switchGroup Number(s)'
      EQUALITY Integer
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.27)

Attributetype (1.3.6.1.4.1.800.2.1.1.2
      NAME 'numberOfSwitchGroups'
      DESC ' member of how many switch groups'
      EQUALITY integer
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.27)

attributetype (1.3.6.1.4.1.800.2.1.1.3
      NAME 'accountFailTime'
      DESC 'accountFailTime'
      EQUALITY caseIgnoreMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768} )

attributetype (1.3.6.1.4.1.800.2.1.1.4
      NAME 'accountStartTime'
```

```
      DESC 'accountStartTime'
      EQUALITY caseIgnoreMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768} )

attributetype (1.3.6.1.4.1.800.2.1.1.5
      NAME 'accountStopTime'
      DESC 'accountStopTime'
      EQUALITY caseIgnoreMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768} )

attributetype (1.3.6.1.4.1.800.2.1.1.6
      NAME 'switchSerialNumber'
      DESC 'switchSerialNumber'
      SINGLE-VALUE
      EQUALITY caseIgnoreMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768} )

attributetype (1.3.6.1.4.1.800.2.1.1.7
      NAME 'switchSlotPort'
      DESC 'switchSlotPort'
      SINGLE-VALUE
      EQUALITY caseIgnoreMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768} )

attributetype (1.3.6.1.4.1.800.2.1.1.8
      NAME 'clientMacAddress'
      DESC 'clientMacAddress'
      SINGLE-VALUE
      EQUALITY caseIgnoreMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768} )

attributetype (1.3.6.1.4.1.800.2.1.1.9
      NAME 'clientIPAddress'
      DESC 'IP Address of clients Station'
      SINGLE-VALUE
      EQUALITY caseIgnoreMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768} )
```

Name	Type	Description
BooleanMatch	Equality	Boolean
ObjectIdentifierMatch	Equality	OID
distinguishedNameMatch	equality	DN
uniqueMemberMatch	equality	DN with optional UID
numericStringMatch	equality	numerical
numericStringOrderingMatch	ordering	numerical
numericStringSubstringsMatch	substrings	numerical
caseIgnoreMatch	equality	case insensitive, space insensitive
caseIgnoreOrderingMatch	ordering	case insensitive, space insensitive
caseIgnoreSubstringsMatch	substrings	case insensitive, space insensitive
caseExactMatch	equality	case sensitive, space insensitive

caseExactOrderingMatch	ordering	case sensitive, space insensitive
caseExactSubstringsMatch	substrings	case sensitive, space insensitive
caseIgnoreIA5Match	equality	case insensitive, space insensitive
caseIgnoreOrderingIA5Match	ordering	case insensitive, space insensitive
caseIgnoreSubstringsIA5Match	substrings	case insensitive, space insensitive
caseExactIA5Match	equality	case sensitive, space insensitive
caseExactOrderingIA5Match	ordering	case sensitive, space insensitive
caseExactSubstringsIA5Match	substrings	case sensitive, space insensitive

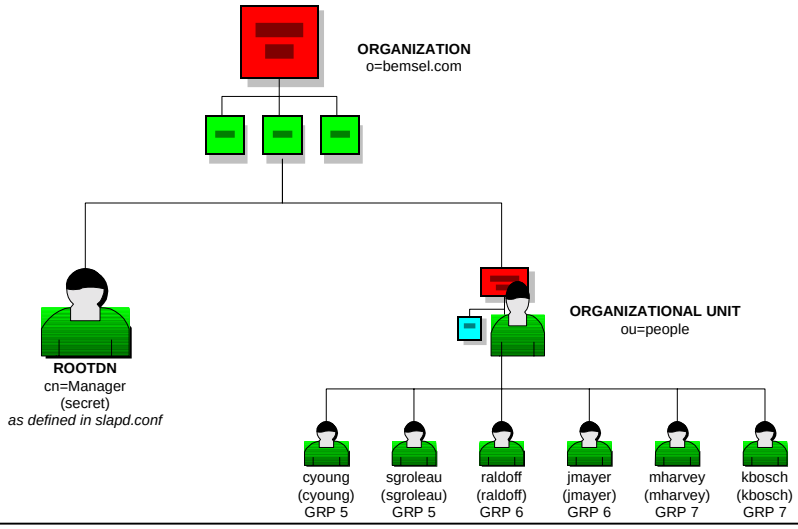
The second attribute, cn, is a subtype of name hence it inherits the syntax, matching rules, and usage of name. commonName is an alternative name.
Neither attribute is restricted to a single value and both are meant for usage by user applications

9. Object class Specification for User Authentication

The *objectclasses* directive is used to define a new object class.
The directive uses the same Object Class Description (as defined in RFC2252) used by the objectClasses attribute found in the subschema subentry. In the case of User Authentication, get following statement into xylanauthenticationperson.schema below all attribute definitions

```
objectclass ( 1.3.6.1.4.1.800.2.2.3
        NAME ‘xylanAuthenticationPerson’
        SUP top
        DESC ‘User Authentication Person for use with Omni XOS’
        MUST cn
        MAY (switchGroups $ numberOfSwitchGroups $ accountFailTime $
             accountStartTime $ accountStopTime $ switchSerialNumber $
            SwitchSlotPort $ clientMacAddress $ clientIPAddress ))
```

10. Directory Structure for this example



This structure I have implemented in an ldif-file, which is outlined below. I've called the file omnitip.ldif. You won't find an entry for "cn=Manager" in the ldif-file, as the RootDN is already defined in slapd.conf.

11. LDIF File for User Authentication

```
cn: o=bemsel.com
objectclass: top
objectclass: organization
o: bemsel.com

dn: ou=people,o=bemsel.com
objectclass: top
objectclass: organizationalUnit
ou: people

dn: uid=cyoung,ou=People, o=bemsel.com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: xylanauthenticationperson
cn: Clayton Young
uid: CYoung
givenname: Clayton
sn: Young
userpassword: cyoung
numberofswitchgroups: 1
switchgroups: 5


dn: uid=sgroleau,ou=People, o=bemsel.com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: xylanauthenticationperson
cn: Sam Groleau
uid: sgroleau
givenname: Sam
sn: Groleau
userpassword: sgroleua
numberofswitchgroups: 1
switchgroups: 5


dn: uid=raldoff,ou=People, o=bemsel.com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: xylanauthenticationperson
cn: Rob Aldoff
uid: RAldoff
givenname: Rob
sn: Aldoff
userpassword: raldoff
numberofswitchgroups: 1
switchgroups: 6
```

```
dn: uid=JMayer,ou=People, o=bemsel.com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: xylanauthenticationperson
cn: Jason Mayer
uid: JMayer
givenname: Jason
sn: Mayer
userpassword: jmayer
numberofswitchgroups: 1
switchgroups: 6


dn: uid=mharvey,ou=People, o=bemsel.com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: xylanauthenticationperson
cn: Mike Harvey
uid: mharvey
givenname: Mike
sn: harvey
userpassword: mharvey
numberofswitchgroups: 1
switchgroups: 7


dn: uid=kbosch,ou=People, o=bemsel.com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: xylanauthenticationperson
cn: Kim Bosch
uid: kbosch
givenname: Kim
sn: Bosch
userpassword: kbosch
numberofswitchgroups: 1
switchgroups: 7
```

12. Start the LDAP Server

To start slapd in general, you run like this:

```
/usr/local/etc/libexec/slapd <option>
```

Where /usr/local/etc/libexec is determined by configure and <option> is one of the options you can specify a debugging level (including level 0)

13. Importing LDIF into directory database

To import the LDIF File you have to use the command utility.

```
ldapadd –h 192.168.10.150 –p 389 –D “cn=Manager, o=bemsel.com” –f omnitip.ldif –x –w secret
```

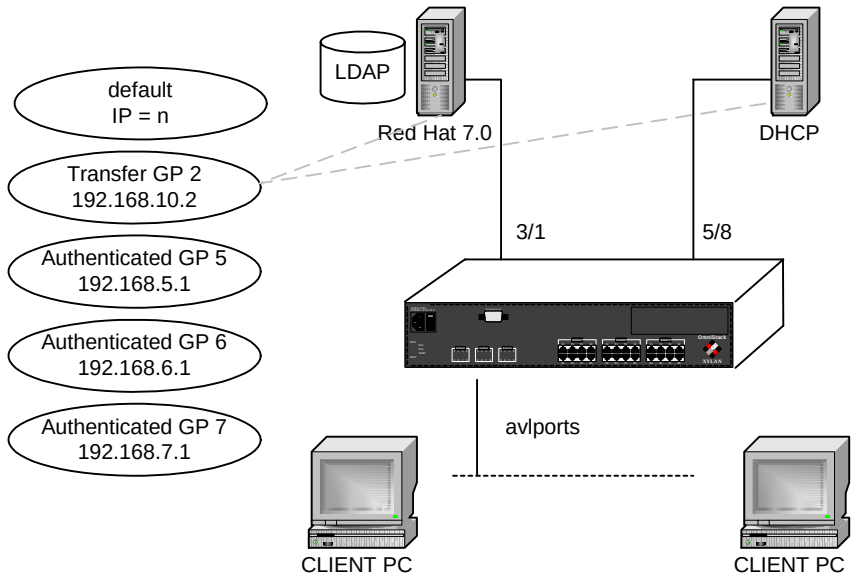
14. Stop the LDAP Server

To kill slapd safely, you should give a command like this:

```
kill – TERM ‘cat $(ETCDIR)/slapd.pid
```

Killing slapd by a more drastic method may cause its LDBM databases to be **corrupted**, as it may need to flush various buffers before it exits. Note that slapd write its pid to a file called slapd.pid in the directory you configured in slapd.conf file, for example: /usr/local/var/slapd.pid

15. Physical and logical Layout



16. Switch Configuration

Verify the hardware

```
OpenLDAP-5024 />slot

     Module-Type Adm-Status   HW     Board      Mfg    Firmware-Version
Slot Part-Number Oper-Status  Rev   Serial #    Date   Base-MAC-Address
---- ----------- ----------- ----- ---------- -------- -----------------
 1*       MPM-OS Enabled       B8    81754696 04/25/98 4.1.3 GA
        05019606 Operational                            00:20:da:9b:70:40
                                                        00:20:da:9b:70:50
                                                        00:20:da:9b:70:60
                                                        00:20:da:9b:70:70
```

```
 2         Empty

 3   Ether 10/100 Enabled       B8    81754696 04/25/98 4.1.3 GA
        05019606 Operational                          None

 4   Ether 10/100 Enabled       B8    81754696 04/25/98 4.1.3 GA
        05019606 Operational                          None

 5   Ether 10/100 Enabled       B8    81754696 04/25/98 4.1.3 GA
        05019606 Operational                          None

OpenLDAP-5024 />
```

Turn Group Mobility on

```
OpenLDAP-5024 />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):
def_group is set to Enable. Set it to Disable ? [yes/no] (no):
OpenLDAP-5024 />
```

Disable IP on Default Group

```
 OpenLDAP-5024 />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
OpenLDAP-5024 / >

OpenLDAP-5024 / >
OpenLDAP-5024 / >gp
Group                                Network Address  Proto/
 ID          Group Description      (IP Subnet Mask)  Encaps
(:VLAN ID)                          or (IPX Node Addr)
===== ============================== =============== ========
    1 Default GROUP (#1)
OpenLDAP-5024 / >
```

Create a Transfer Group

(I use this group to have the LDAP Server *(3/1)* and DHCP Server *(5/8)* connected inside a "pro-forma" authentication aware group)

```
OpenLDAP-5024 / >
OpenLDAP-5024 / >crgp
    GROUP Number (  2) :
    Description (no quotes) : TRANSFER to AUTHENTICATION
    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) 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: 3/1, 5/8
    5/8 - 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 5/8 to GROUP 2...
    Adding port 3/1 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
OpenLDAP-5024 /System >
```

Create authenticated User Groups

```
OpenLDAP-5024 / >
OpenLDAP-5024 / >crgp
```

```
    GROUP Number (  3) : 5
    Description (no quotes) : Authenticated Group 5
    Enable WAN Routing? (n):
    Enable ATM CIP? (n):
    Enable IP (y) :
       IP Address                              : 192.168.5.1
       IP Subnet Mask             (0xffffff00) :
       IP Broadcast Address (192.168.5.255   ) :
       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 add interfaces to this group using the addvp command at a later date.
For now, the GROUP is inactive until you add interfaces.
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
OpenLDAP-5024 /System >
OpenLDAP-5024 /System >crgp
    GROUP Number (  3) : 6
    Description (no quotes) : Authenticated Group 6
    Enable WAN Routing? (n):
    Enable ATM CIP? (n):
    Enable IP (y) :
       IP Address                              : 192.168.6.1
       IP Subnet Mask             (0xffffff00) :
       IP Broadcast Address (192.168.6.255   ) :
       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 add interfaces to this group using the addvp command at a later date.
For now, the GROUP is inactive until you add interfaces.
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
OpenLDAP-5024 /System >
OpenLDAP-5024 /System >
OpenLDAP-5024 /System >
OpenLDAP-5024 /System >crgp
    GROUP Number (  3) : 7
    Description (no quotes) : Authenticated Group 7
    Enable WAN Routing? (n):
    Enable ATM CIP? (n):
    Enable IP (y) :
       IP Address                              : 192.168.7.1
       IP Subnet Mask             (0xffffff00) :
       IP Broadcast Address (192.168.7.255   ) :
       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 7 has been added to the system.
You may add interfaces to this group using the addvp command at a later date.
For now, the GROUP is inactive until you add interfaces.
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
OpenLDAP-5024 / >
```

Check all groups

```
OpenLDAP-5024 / >
OpenLDAP-5024 / >gp
Group                                  Network Address  Proto/
 ID          Group Description        (IP Subnet Mask)  Encaps
(:VLAN ID)                            or (IPX Node Addr)
===== ============================== ================ ========
    1 Default GROUP (#1)
    2 TRANSFER to AUTHENTICATION     192.168.10.1      IP  /
                                       (ff.ff.ff.00 )   ETH2
    5 Authenticated Group 5          192.168.5.1       IP  /
                                       (ff.ff.ff.00 )   ETH2
    6 Authenticated Group 6          192.168.6.1       IP  /
                                       (ff.ff.ff.00 )   ETH2

    7 Authenticated Group 7          192.168.7.1       IP  /
                                       (ff.ff.ff.00 )   ETH2
OpenLDAP-5024 / >
```

Activate Authentication

```
OpenLDAP-5024 / >
OpenLDAP-5024 / >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
OpenLDAP-5024 /System >
```

Configure Directory Server Connection

```
OpenLDAP-5024 /System >
OpenLDAP-5024 /System >avllschain
LDAP server search base? () : o=bemsel.com
LDAP server super user rdn? () : cn=Manager
LDAP super user password? () : secret (this entry is hidden)
Please enter password once more: () : secret (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) : () : 1
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
OpenLDAP-5024 / >
```

Check connectivity to Directory Server

```
OPENLDAP-5024/ >avlslserver
LDAP server (192.168.10.150:389) is alive and happy
OPENLDAP-5024/ >

When getting an error like below, you may not have connected the LDAP server to the switch, or
SLAPD is not running.

OpenLDAP-5024 / >
OpenLDAP-5024 / >avlslserver
LDAP server (192.168.10.150:389) can not be contacted
OpenLDAP-5024 / >
```

Verify, if slapd is running go to Linux terminal and type:

```
# ps-ef |grep slapd (process id's and time may differ)

root    1000    1       0       14:05   ?       00:00:00 ./slapd
root    1001    1000    0       14:05   ?       00:00:00 ./slapd
root    1002    1001    0       14:05   ?       00:00:00 ./slapd
root    1003    1001    0       14:05   ?       00:00:00 ./slapd
root    1007     916    0       14:07   pts/0   00:00:00 grep slapd
```

Configure Ports for Authentication

```
OpenLDAP-5024 / >
OpenLDAP-5024 / >avlpo
Do you wish to add or delete a port (add) :
Which ports do you wish to add : 3/2-8, 4/1-8, 5/1-7
OpenLDAP-5024 / >
```

To verify, if all ports had been added:

```
OpenLDAP-5024 / >avlspo
Current Authentication Ports
  Slot / Port
    3 / 2     3 / 3     3 / 4     3 / 5     3 / 6
    3 / 7     3 / 8     4 / 1     4 / 2     4 / 3
    4 / 4     4 / 5     4 / 6     4 / 7     4 / 8
    5 / 1     5 / 2     5 / 3     5 / 4     5 / 5
    5 / 6     5 / 7
OpenLDAP-5024 / >
```

Configure DHCP Relay Function

```
OpenLDAP-5024 / >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=y

                          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=a
              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]  : 192.168.10.100
              FORWARD TO Server List
   Item     Server address     Server Name (if known)

     1)       192.168. 10.100

Enter IP address or host name of server to be added to list ['h' for help/<ret>
to exit]  :


                          UDP Relay Configuration

 1) BOOTP/DHCP Enabled                      : Yes
   11) Server Address {list/add/delete}       : SET
   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)  : save

Starting task
Saving config for service 0
UDP Relay configuration change, service 1:
UDP Relay initializing....UDP Relay initialized.
OpenLDAP-5024 / >
```

Finally do a reboot

```
OpenLDAP-5024 / >
OpenLDAP-5024 / >reboot
   Confirm? (n) : y
Locking filesystem...locked.
System going down immediately...
switch[40da6fd8]: System rebooted by admin
Flash file system check in progress...
   Checking root file system...   OK
   Performing file consistency check...
   Done.
```

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.

==========

Final Note:
If you need more information regarding OpenLdap, I suggest to go to their website at http://www.openldap.org.Also I’d like to recommend using the Administrator’s Guide at http://www.openldap.org/doc/admin/index.html to get through the more or less difficult process.

You also can download all configuration files I made with this Omnitip on

www.bemsel.com/techtip/openldap20001201.zip