Step 1: Install freeradius Packages

Install all freeradius2 server packages on your system using following command.

```
# yum install freeradius2 freeradius2-utils freeradius2-ldap
```

Step 2: Download Schema File

Download radius ldap schema file and copy to ldap schema directory using below commands.

2.1 Download File

```
# wget http://open.rhx.it/phamm/schema/radius.schema
```

2.2 Copy file in schema directory

```
# cp radius.schema /etc/openldap/schema/
```

2.3 Include file in ldap configuration file /etc/openldap/slapd.conf

```
include /etc/openldap/schema/radius.schema
```

Step 3: Edit Radius LDAP Files

Edit radius ldap file /etc/raddb/modules/ldap and add below ldap server details.

```
# vim /etc/raddb/modules/ldap

ldap {

        server = "openldap.example.com"

        basedn = "dc=example,dc=com"
```

```
        identity = "cn=Manager,ou=people,dc=example,dc=com"

        filter = "(uid=%{Stripped-User-Name:-%{User-Name}})"

        base_filter = "(objectclass=radiusprofile)"

        start_tls = no

        groupmembership_filter =
"(|(&(objectClass=GroupOfNames)(member=%{Ldap-
UserDn}))(&(objectClass=GroupOfUniqueNames)(uniquemember=%{Ldap-
UserDn})))"

        profile_attribute = "radiusprofile"

        access_attr = "uid"

        dictionary_mapping = ${raddbdir}/ldap.attrmap

        ldap_connections_number = 10

        timeout = 4

        timelimit = 5

        net_timeout = 1

        set_auth_type = yes

}
```

Edit /etc/freeradius/ldap.attrmap add following details.

```
# vim /etc/freeradius/ldap.attrmap

checkItem User-Password userPassword
```

```
replyItem Tunnel-Type radiusTunnelType

replyItem Tunnel-Medium-Type radiusTunnelMediumType

replyItem Tunnel-Private-Group-Id radiusTunnelPrivateGroupId
```

Step 4: Enable LDAP Authentication

After updating above files, Lets enable LDAP authentication in /etc/raddb/sites-available/inner-tunnel and /etc/raddb/sites-available/default by uncomment below lines.

```
Auth-Type LDAP {

        ldap

}
```

Step 5: Test Setup

Finally setup your setup by using following command

```
# radtest ldapuser1 password ldap.example.com 2 testing123


Sending Access-Request of id 165 to 127.0.0.1 port 1812

User-Name = "ldapuser1"

User-Password = "password"

NAS-IP-Address = 192.168.10.50

NAS-Port = 2
```

```
Message-Authenticator = 0x00000000000000000000000000000000

rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=165,
length=64

Filter-Id = "Enterasys:version=1:policy=Enterprise User"
```

If you get rad_recv: Access-Accept then authentication is successes.

Congratulation's! You have successfully configured FreeRadius authentication with OpenLDAP.

Step 6: Make entry in client, Proxy files

6.1 Open up /etc/raddb/clients.conf through command

vim /etc/raddb/clients.conf

Enter the clients detail.which will be interact with your radius server.

Example:

```
client IP {
        secret          = YOUR SECRET HERE
        shortname       = yourVPN
        nastype         = other
}
```

6.2 Open up /etc/raddb/proxy.conf

```
# vim /etc/raddb/proxy.conf
```

Enter the National and your domain detail.

Example:

```
realm Default {

        authhost        = National IP
        secret          = YOUR SECRET HERE
        shortname       = yourVPN
        nostrip
}

realm xyz.in {
        authhost        = LOCAL
}
```

Step 7 : Test your radius authentication with Wi-Fi

If you have any problems with FreeRADIUS you can run FreeRADIUS in debug mode to help pinpoint any issues, to do that just do the following:

 # service radiusd stop
 # radiusd -X

Now you can see in realtime if your authentication queries are actually reaching the server or the reasons why some users may be rejected authentication.