

Verzió kontroll

Változat	Módosítva	Módosítás leírása	Szerző
1.0	2004.03.21	Első kiadás	Bedő Sándor
2.0	2005.05.11	Pontosítások, bővítések	Borbás Éva
3.0	2006.05.01	Automatizált LDAP adatbázis- inicializálás, rövidített generált file nevek, DHCP agent IPv4-re, néhány apró hibajavítás	Borbás Éva
4.0	2006.06.08	A kezelőfelületek (és az LDAP schema) kiegészítése az IPv6-os DHCP adatok kezeléséhez szükséges attribútumokkal, DHCPv6 agent, paraméterek beolvasása konfigurációs file-ból	Borbás Éva
4.1	2006.06.27	Az L2D2 4.0 <i>chroot</i> környezet nélkül (csak az alkalmazáshoz tartozó agent programok, script-ek és minta-konfigurációk)	Borbás Éva Diósi Anna
5.0	2007.07.10	<ul style="list-style-type: none"> - top-level domain inicializálása (egy szintű, egy előző verzióval létrehozott LDAP adatbázis nem használható!) - top-level domain törlése web felületen keresztül - kezelőfelületek, LDAP schema, dnsAgent, és a dns2ldap kiegészítése az AFSDDB, ill. az SRV DNS rekordok kezelésével - dns2ldap reverse zóna-transzfer -> "idegen" domain-ek kezelése - dnsAgent.rb - "idegen" domain-ek csak a reverse táblába kerülnek - IPv4 és IPv6 címek ellenőrzése - zóna/subnet/host felvitelénél/módosításnál az összes elkövetett hiba egyszerre jelenik meg - adminisztrációs felületek átalakítása (csoportosítás, a keresések rendezett megjelenítése, ...stb) 	Borbás Éva
5.1	2007.07.10	Az L2D2 5.0 <i>chroot</i> környezet nélkül (csak az alkalmazáshoz tartozó agent programok, script-ek és minta-konfigurációk)	Borbás Éva Diósi Anna
6.0	2008.03.14	<ul style="list-style-type: none"> - apróbb hibák javítása - a kezelőfelületek, az LDAP schema, ill. a dnsAgent kiegészítése a host TTL és az IPv6 reverse NS rekordok kezelésével - SOA Serial number generálása a dátumból: <év><hónap><nap><sorszám> formában - LDAP ACL generálás a "refreshadmin" számára is (írásjog az esetleges adatbázis-szinkronizáláshoz) 	Borbás Éva

6.1	2008.03.17	Az L2D2 6.0 <i>chroot</i> környezet nélkül (csak az alkalmazáshoz tartozó agent programok, script-ek és minta-konfigurációk)	Borbás Éva
6.2	2011.07.17	Az L2D2 6.1 továbbfejlesztett változata: - apróbb hibák javítása - IPv4-es reverse zónák generálása független file-okba - a kezelőfelületek, az LDAP schema, a dnsAgent, a dhcpAgent és a dhcpv6Agent kiegészítése a „host Comment”, a „Zone address”, az „IPv4 pool” és az „IPv6 pool” kezelésével	Borbás Éva

L2D2

LDAP to DNS and DHCP

V. 6.2

Bedő Sándor
Borbás Józsefné
Diósi Anna
Kadlecsik József

KFKI RMKI SzHK 2011. július 17.

Tartalomjegyzék

1. Bevezetés	5
2. Az alkalmazás telepítése és konfigurálása	6
2.1 Letöltés és kicsomagolás	6
2.1.1 A segédprogramok konfigurálása	7
2.1.2 Az LDAP szerver hostolása	8
2.1.2.1 A gyökér-bejegyzés létrehozása az LDAP adatbázisban	10
2.1.2.2 Az LDAP agent konfigurálása	10
2.1.2.3 Az LDAP szervert kezelő file-ok telepítése a telepítő script nélkül	11
2.1.3 Az Apache szerver hostolása	11
2.1.4 A DNS szerver hostolása	12
2.1.4.1 A DNS agent konfigurálása.....	13
2.1.4.2 A DNS szervert kezelő file-ok telepítése a telepítő script nélkül	13
2.1.5 Az IPv4 DHCP szerver hostolása	14
2.1.5.1 A DHCP agent konfigurálása	15
2.1.5.2 A DHCP szervert kezelő file-ok telepítése a telepítő script nélkül.....	15
2.1.6 A DHCPv6 szerver hostolása	16
2.1.6.1 A DHCPv6 agent konfigurálása.....	16
2.1.6.2 A DHCPv6 szervert kezelő file-ok telepítése a telepítő script nélkül.....	17
2.1.7 Az inetd daemon konfigurálása.....	17
2.1.8 Az alkalmazás eltávolítása	18
2.2 Az LDAP adatbázis inicializálása az L2D2 számára (top-level zóna létrehozása és törlése).....	18
3. Zóna menedzsment.....	21
3.1 CGI elérése, bejelentkezés az alkalmazásba.....	21
3.2 Keresés, módosítás, törlés.....	23
5. ábra.....	23
3.2.1 Zóna törlése	27
3.3 Új hosztok, alhálózatok	27
3.4 Új zóna létrehozása	29
3.4.1 Új zóna feltöltése DNS zone transzferből	31
3.4.2 DNS zóna delegálása a zóna menedzselése nélkül	32
3.5 Új adminisztrátorok, delegált zónák	33
4. Szerver-konfigurációk, szerverek újraindítása	34
4.1 LDAP szerver	34
4.2 DNS szerver	35
4.3 DHCP szerver.....	36
4.4 DHCPv6 szerver.....	38

1. Bevezetés

Az **L2D2 IPv4-es és/vagy IPv6-os DNS és DHCP** konfigurációkat **LDAP** adatbázisból előállító alkalmazás.

Az **IPv6 megjelenésével** az IPv4-hez képest **hosszú és nehezen megjegyezhető IP címek** megnehezítik a DNS adatbázisok kezelését, karbantartását. A **DNS és DHCP** kezelésének **megkönnyítésére szolgál az L2D2 alkalmazás**. A programrendszer nem tartalmaz olyan elemet, amely az IPv6 környezethez lenne kötve, tehát használható tiszta IPv6, tiszta IPv4, vagy IPv6 és IPv4 vegyes környezetben is.

A **DNS zónákat, alhálózatokat, hosztokat és a hozzájuk tartozó információkat** egy-egy **LDAP bejegyzés reprezentál**. Az alkalmazással a **DNS zónák, alhálózatok megosztott módon menedzselhetőek**: minden zónához, alhálózathoz adminisztrátor rendelhető, akinek joga lesz a zónát/alhálózatot tovább bontani, és új adminisztrátorokat létrehozni. Egy adminisztrátor több zónát/alhálózatot menedzselhet, egy adott szubzónának/subnet-nek pedig több adminisztrátora lehet. Az **LDAP bejegyzéseket** minden **regisztrált adminisztrátor olvashatja, de írni, csak a számára delegált zónát/alhálózatot tudja**. A jogosultságokat az LDAP kezeli. Az **L2D2-ben LDAP** tekintetében a **zóna és a subnet** között egyetlen **különbség** van: a **subnet-nek nincsen SOA rekordja**, minden másban teljesen egyformán menedzselhetőek.

Az **adatbázis inicializálása és frissítése web felületen keresztül** történik, így az adminisztrátorok számára nem szükséges az LDAP kezelő parancsok ismerete. Az **új szerver-konfigurációk** elkészítése és az **adott szerver újraindítása is web felületről** kezdeményezhető. A **web-es kezelőfelület Ruby** nyelven írt **CGI script-ek** segítségével kommunikál az **LDAP adatbázissal**.

A **CGI/LDAP/DNS/DHCP/DHCPv6 szerverek** mindegyike futhat más-más gépen. **Új zóna létrehozásánál** lehet beállítani azt, hogy az adott zóna számára az **egyes szerverek mely gépen és milyen porton érhetőek el**. Az **LDAP, a DNS, a DHCP és a DHCPv6 szervereken futó kis daemon** (az ldapAgent, a dnsAgent, a dhcpAgent.rb és a dhcpv6Agent) - amelyet az adott porton az **inetd** indít - biztosítja azt, hogy a szerverek más-más gépen futhassanak.

Az **agent** programoknak, ill. az alkalmazás néhány segédprogramjának az **alapértelmezett paramétereit** az **/etc/l2d2/config.txt** konfigurációs file kell, hogy tartalmazza, a szükséges módosításokat itt lehet/kell elvégezni.

A CGI felületen a "**Server update**" kijelölése után:

- a **CGI script** az **adott daemon portjára kapcsolódik**
- a **daemon letölti az LDAP adatbázisból az adatokat, megírja az új konfigurációs file-t és újraindítja a szervert.**

Az új konfigurációs file elkészítése:

- **LDAP** esetén az **adott zóna jogosultsági (ACL) listájának a frissítését**
- **DNS** esetén a **forward és a reverse (IPv6-os is) táblák elkészítését**
- **DHCP és a DHCPv6** esetén az **adott zóna és a hozzá tartozó subnet(ek) dhcp konfigurációjának elkészítését**

jelenti.

Az alkalmazás fejlesztése Testing Debian környezetben történt, amelyben egy **OpenLDAP** (slapd) szerver, egy **DNS** (bind9) szerver, egy **IPv4 DHCP** (dhcp3 szerver v. 3.0.3), egy **IPv6 DHCP** (Dibbler szerver 0.4.1) és egy **Apache** szerver futott.

2. Az alkalmazás telepítése és konfigurálása

Az **L2D2 6.2-es** változatában csak az alkalmazás működéséhez szükséges **agent** és **segédprogramok, script-ek** ill. **minta-konfigurációs** fájlok találhatóak. Az alkalmazás futtatásához a közreműködő programok **telepítése** (Ruby interpreter, Apache web szerver, DNS (bind9) szerver, IPv4 DHCP (dhcp3) szerver, IPv6 DHCP (Dibbler) szerver és az OpenLDAP szerver), és a - saját igények szerinti - **konfigurálása** a felhasználó feladata. Az alkalmazással kezelni kívánt szerverek konfigurálásához, ill. az L2D2 konfigurálásához minta file-okat biztosítunk (az */etc/l2d2/samples/* directory-ban). A **minta-konfigurációk**, valamint a dokumentációban látható **úrlapok adatai** az **alkalmazás fejlesztésénél használt LDAP teszt-adatbázis bejegyzései alapján** készültek.

2.1 Letöltés és kicsomagolás

Az L2D2 6.2 változatának letöltéséhez kb. **110Kbyte**, a telepítéséhez további kb. **660Kbyte** szabad lemezterület szükséges.

Az **l2d2_6.2.tar.gz** letöltését a *wget* paranccsal végezzük a */scratch* könyvtárba, majd kicsomagoljuk azt. Természetesen eltérő könyvtárneveket is használhatunk, ez mindössze a helyi gyakorlatunkat, szokásainkat tükrözi.

A továbbiakban % jellel jelöljük a nem root felhasználók promptját, # jellel pedig a root promptot:

```
% cd /scratch
% wget 'http://www.kfki.hu/cnc/projekt/l2d2/l2d2_6.2.tar.gz'
% sudo zsh
# tar -xvzf l2d2_6.2.tar.gz
# rm l2d2_6.2.tar.gz
# _
```

A kicsomagolás után belépünk az *l2d2_6.2/* könyvtárba

```
# cd l2d2_6.2
```

és telepítjük az alkalmazáshoz szükséges fájlokat attól függően, hogy mely szervereket akarjuk a gépünkön hostolni. A telepítés a **place_files** script esetleges módosításával és elindításával történhet:

```
./place_files ldap|apache|bind9|dhcp3|dibbler|all
```

Az *all* paraméter megadása a teljes L2D2_6.2 alkalmazás telepítését jelenti, vagyis az **adott gépen** az alkalmazással kezelhető **összes szerver** (a Web, az LDAP, a DNS, az IPv4 DHCP és az IPv6 DHCP szerver) **futtatása** lehetséges.

A fenti parancs - bármelyik paraméterrel indítjuk is - mindenképpen telepíti a következő file-okat:

- az L2D2 működéséhez szükséges konfigurációs file-t (config.txt) az */etc/l2d2/* könyvtárba (kivéve, ha csak az *apache* paramétert adjuk meg) . A konfigurációs file-t a későbbiekben sem lehet áthelyezni;
- egy minta **inetd** konfigurációs file (inetd.conf) az */etc/l2d2/samples/* könyvtárba (kivéve, ha csak az *apache* paramétert adjuk meg);
- az L2D2 LDAP bejegyzéseit (zóna és subnet) távolról feltöltő, ill. egy adott zónát törlő - parancssorból indítható - segédprogramokat (dns2ldap.rb, ldapZoneDelete.rb) az */usr/local/sbin/* könyvtárba;
- az L2D2 alkalmazással kezelt szerverek **agent** programjait (akár távoli gépen futó) parancssorból elindítható programot (trigger.rb) az */usr/local/sbin/* könyvtárba.

Ha a file-ok telepítését magunk végezzük el, akkor a fenti két segédprogramot érdemes telepíteni.

A fejezet további részeiben:

- **a segédprogramok konfigurálását;**
- **az L2D2 alkalmazással kezelt szerverekhez szükséges file-ok telepítését, a szerverek konfigurálását;**
- **az agent programok konfigurálását, ill. az újraindításukhoz szükséges inetd daemon konfigurációját**

írjuk le.

A minta-konfigurációs file-ok az alkalmazás fejlesztésénél használt teszt-adatbázis bejegyzései alapján készültek.

2.1.1 A segédprogramok konfigurálása

Az L2D2 konfigurációs file-ban (*/etc/l2d2/config.txt*) az adott gépen működő **agent** és **segédprogramok** számára állítunk be alapértelmezett értékeket.

A **dns2ldap.rb** segédprogram - az adatbázis egy zónáját zona transzferből feltöltő program - konfigurálásához ebben a következő paramétereknek adhatunk default értékeket:

- a szerverek (LDAP és DNS szerver) kapcsolódási paramétereit (IP címek, portszám, azonosítók, ..stb.);
- a feltöltésre szánt zóna domain nevét, ill. a reverse zóna nevét, az esetleges "idegen" domain-hez tartozó hosztok feltöltéséhez.

Paraméter-értékek a letöltött minta *config.txt* file-ban:

```
#Zone transfer default parameters (dns2ldap.rb)

dns2LDAPHost      = 127.0.0.1
dns2LDAPPort      = 389
dns2LDAPProto     = 3 # 2 or 3 -=> LDAPv2 or LDAPv3
NamingSuffix      = org
LDAPAdminDN       = cn=Administrator,cn=suffix
LDAPPassw         = secret
LDAPBase          = cn=suffix
DNSDefaultServer  = localhost
DNSDomain         = test.org
```

DNSReverseDomain = 10.10.IN-ADDR.ARPA, 0.1.0.0.8.b.d.0.1.0.0.2.ip6.arpa

A fenti paramétereket a program indításakor parancssorból is megadhatjuk. Részletes leírás a dokumentáció 3.4.1 pontjában található.

Az **ldapZoneDelete.rb** segédprogram - egy adott zóna és az összes hozzá tartozó bejegyzés törlése az adatbázisból - konfigurálásához a *config.txt* file-ban a következő paramétereknek adhatunk default értékeket:

- az LDAP szerver kapcsolódási paramétereit;
- a jogosultsági listát (ACL file-ok) tartalmazó file-ok helyét;
- a törlendő zóna LDAP azonosítóját.

Paraméter-értékek a letöltött minta *config.txt* file-ban:

```
#Delete top-level zone (ldapZoneDelete.rb)
zdelLDAPHost      = 127.0.0.1
zdelLDAPPort      = 389
zdelLDAPProto     = 3 # 2 or 3 => LDAPv2 or LDAPv3
zdelLDAPUser      = # empty string for anonymous
zdelLDAPCred      = # LDAP user password
zdelLDAPRetry     = 3 # number of retries on errors
zdelLDAPRetryPeriod = 20 # secs
zdelLDAPACLDirectory = /etc/ldap/l2d2
zdelLDAPEntry     = L2D2ZoneName=test,L2D2NamingSuffix=org,cn=suffix
```

A fenti paramétereket a program indításakor parancssorból is megadhatjuk. Részletes leírás a dokumentáció 3.2.1 pontjában található.

A **trigger.rb** segédprogramnak - a szervereket kezelő **agent** programok elindítása - indításkor, a parancssorban adjuk meg a paramétereit. Bővebb információ a dokumentáció 4.1 pontjában található.

2.1.2 Az LDAP szerver hostolása

Az LDAP szerver L2D2 szempontból megfelelő működtetéséhez a szükséges file-okat a

```
./place_files ldap
```

paranccsal telepíthetjük, vagy a telepítést magunk is elvégezhetjük a 2.1.2.3 pont szerint. A fenti parancs a 2.1 pontban leírtakon kívül a következő file-okat helyezi el a gépünkön:

- az LDAP szervert kezelő **agent programot** (*ldapAgent.rb*) az */usr/local/sbin/* könyvtárba;
- egy minta-file-t az LDAP adatbázis inicializálásához - “gyöker bejegyzés” létrehozása - (*dbinit*) az */usr/local/sbin/* könyvtárba;
- az LDAP működéséhez szükséges sémákat (*../l2d2_6.2/conf/schemas* könyvtár tartalmát) az */etc/l2d2/schemas/* könyvtárba, illetve az *l2d2* alkalmazás-specifikus definícióit tartalmazó **l2d2.schema** sémát a */etc/l2d2/schemas/l2d2* könyvtárba.
- egy minta LDAP konfigurációs file-t (*slapd.conf*), egy kezdeti inicializációs *ldif* file-t (*init.ldif*), a *refreshadmin* és a *query* user létrehozásához szükséges *ldif* file-t (*refreshadmin.ldif* és *query.ldif*) az */etc/l2d2/samples/ldap* könyvtárba.

Az **LDAP** szerver konfigurálását magunknak kell elvégezni. Ehhez egy minta-konfigurációs file-t (*/etc/l2d2/samples/ldap/slapd.conf*) vehetünk igénybe.

A *slapd* minta-konfigurációs fájlban láthatjuk a szükséges sémákat, beállításokat. Ha a **rootdn** illetve a **suffix** megadásakor eltérünk a megadott mintától, akkor ügyeljünk arra, hogy az adatbázis - az alkalmazás kezelő felületéről való - kezdeti inicializálásakor (2.2 pont) is konzekvensen az általunk választottakat adjuk meg, a minta szerint:

```
...
# Schema
include      /etc/ldap/schema/core.schema
include      /etc/ldap/schema/cosine.schema
include      /etc/ldap/schema/nis.schema
include      /etc/ldap/schema/inetorgperson.schema

include      /etc/ldap/schema/l2d2/l2d2.schema
...
suffix       "cn=suffix"
directory    "/var/lib/ldap/cn=suffix"
lastmod      on

rootdn       "cn=Administrator,cn=suffix"
rootpw       secret
...
```

Az **adatbázis könyvtárát** (pl. *"/var/lib/ldap/cn=suffix"*) szabadon választhatjuk, de még a **slapd indítása előtt létre kell hoznunk**.

A **rootdn** hozzáférési jogainak megadásakor **ügyeljünk arra**, hogy az **alkalmazással készített jogosultsági lista(ák)** (ACL file-ok) ezek elé kerülhessen(ek). Ezért fontos, hogy a *slapd.conf* file formailag a következőképpen nézzen ki:

```
...
# Include the l2d2 naming entry's ACL file
# generated by ldapAgent.rb. Don't worry
# about including zone ACL files, the naming
# ACL file contains all the deeper include lines.
```

Az *ldapAgent* program az **"ACL file contains all the deeper include lines"** szövegrész meglétét ellenőrzi, és ez után illeszti majd be *include*-dal, a későbbiekben létrehozott top-level zónák adminisztrátorainak a hozzáférési jogait tartalmazó file-okat pl.:

```
include /etc/ldap/l2d2/org.access
```

majd folytatódhat a konfigurációs file a **rootdn** jogosultságaival, pl.:

```
access to attr=userPassword
  by self write
  by anonymous auth
  by dn="cn=Administrator,cn=suffix" write
  by dn="cn=refreshadmin,cn=suffix" write
  by dn="cn=query,cn=suffix" read
  by * none
access to *
  by dn="cn=Administrator,cn=suffix" write
  by dn="cn=refreshadmin,cn=suffix" write
  by dn="cn=query,cn=suffix" read
  by * read
...
```

A **refreshadmin** és a **query** dn az L2D2 működéséhez nem szükséges csak az esetleges adatbázis-szinkronizálást támogatja. A **refreshadmin** írásjogot kap a teljes LDAP adatbázisra nézve (az *ldapAgent* által generált ACL listákban).

Az include-olt hozzáférési jogokat tartalmazó file-t (file-okat) az ldapAgent program az /etc/l2d2/config.txt konfigurációs file-ban megadott könyvtárba helyezi el. **Default** beállítás a /etc/ldap/l2d2 könyvtár. Ezt – vagy az általunk megadott könyvtárat – nekünk kell létrehoznunk!

2.1.2.1 A gyökér-bejegyzés létrehozása az LDAP adatbázisban

Az LDAP szerver **telepítése, konfigurálása és elindítása** után az adatbázist inicializálnunk kell, amely a “gyökér-bejegyzés” létrehozását jelenti. Ha a default **“cn=suffix”** suffixot használjuk, akkor ezt elvégezhetjük a **/usr/local/sbin/dbinit** paranccsal. Egyébként pedig a mintaként megadott /etc/l2d2/samples/ldap/init.ldif file-hoz hasonlót – a *slapd.conf* file-ban megadott suffix-el - kell hozzáadnunk az adatbázishoz az **ldapadd** paranccsal:

```
ldapadd -x -D "cn=Administrator,cn=suffix" -W -f/etc/l2d2/samples/ldap/init.ldif
```

Az ldif file tartalma:

```
dn: cn=suffix
cn: suffix
objectClass: organizationalRole
objectClass: top
```

A *refreshadmin* és a *query* bejegyzés - ha szükséges - a következő módon adható az adatbázishoz:

```
ldapadd -x -D "cn=Administrator,cn=suffix" -W -f/etc/l2d2/samples/ldap/refreshadmin.ldif
```

```
ldapadd -x -D "cn=Administrator,cn=suffix" -W -f/etc/l2d2/samples/ldap/query.ldif
```

2.1.2.2 Az LDAP agent konfigurálása

Az LDAP agent program (ldapAgent.rb) számára az alapértelmezett paramétereket az /etc/l2d2/config.txt konfigurációs file-ban a következők szerint kell megadni:

- hová kerüljön az agent log file-ja
L2D2 log files
..
LDAPLogFile = /var/log/ldapAgent.log
...
- az LDAP szerverhez kapcsolódás paramétereit, a hozzáférési jogosultságokat tartalmazó file-ok helyét és a konfigurációs file helyét

```
#LDAP default parameters (ldapAgent)
# ldapAgent and LDAP server should be on the same host

LDAPHost      = 127.0.0.1
LDAPPort      = 389
LDAPProto     = 3 # 2 or 3 ==> LDAPv2 or LDAPv3
LDAPUser      = # empty string for anonymous
LDAPCred      = # LDAP user password
LDAPRetry     = 3 # number of retries on errors
LDAPRetryPeriod = 20 # secs
```

```
LDAPACLDirectory = /etc/ldap/l2d2
LDAPConfFile     = /etc/ldap/slapd.conf
```

- Az LDAP szervert újraindító parancs helyét
Services
...
LDAPServiceRestart = PATH=/sbin:/bin /etc/init.d/slapd restart
...

2.1.2.3 Az LDAP szervert kezelő file-ok telepítése a telepítő script nélkül

Ha az LDAP agent programot, a segédprogramokat, és az egyéb kezelő file-okat nem a telepítő script által kijelölt default könyvtárba akarjuk elhelyezni, akkor a **./place_files ldap** parancs kiadása helyett a file-okat magunk is telepíthetjük, a következők szerint:

- az **../l2d2_6.2/conf/config.txt** konfigurációs file-t **kötelezően** az **/etc/l2d2/** könyvtárba kell elhelyezni;
- az **../l2d2_6.2/sbin/** könyvtárból másoljuk át a megfelelő programokat (ldapAgent.rb, ldapZoneDelete.rb, dns2ldap.rb, dbinit, trigger.rb) a kívánt helyre, ügyeljünk arra, hogy az **inetd** daemon **konfigurációs file**-ban (inetd.conf) majd az általunk kiválasztott file-elérési útvonalat adjuk meg;
- az LDAP megfelelő működéséhez szükséges sémákat: az **../l2d2_6.2/conf/schemas** és az **../l2d2_6.2/conf/schemas/l2d2** könyvtárak tartalmát másolhatjuk tetszőleges helyre (ajánlott a /etc/ldap/schema), de az elérési útvonalukat az ldap konfigurációs file-ban (slapd.conf) meg kell adni;
- a minta-konfigurációk az **../l2d2_6.2/conf** könyvtárban megtalálhatóak, nem érdemes másik helyre átmásolni.

2.1.3 Az Apache szerver hostolása

Az web szerver L2D2 szempontból megfelelő működtetéséhez szükséges file-okat a

```
./place_files apache
```

paranccsal telepíthetjük. A fenti parancs a 2.1 pontban leírtakon kívül a következő file-okat helyezi el a gépünkön:

- az alkalmazás kezelő felületeit működtető script-eket az **/usr/lib/cgi-bin/l2d2/** könyvtárba;
- a megjelenítéshez szükséges bmp, css és js file-okat a **/var/www** könyvtárba;
- egy minta konfigurációs file-t (httpd.conf) az **/etc/l2d2/samples/apache** könyvtárba.

Amennyiben a cgi script-eket nem a **/usr/lib/cgi-bin/l2d2/** könyvtárból szeretnénk futtatni, akkor a **./place_files apache** parancs kiadása helyett az **../l2d2_6.2/cgi-bin/** könyvtár file-jait helyezzük át az általunk kívánt könyvtárba. Ekkor fontos, hogy az apache-t úgy konfiguráljuk, hogy az adott könyvtárból a cgi-k futtathatók legyenek.

A **httpd.conf** vagy **apache.conf** file-ba beillesztendő rész pl.:

```
<IfModule mod_alias.c>
```

```

ScriptAlias /cgi-bin2/ /home/valaki/akarmi/

<Directory /home/valaki/akarmi/>

    AllowOverride None
    Options ExecCGI -MultiViews +SymLinksIfOwnerMatch
    Order allow,deny
    Allow from all
</Directory>
</IfModule>

```

Ekkor az alkalmazásba való belépéshez a webes felület a

<http://hostnev/cgi-bin2/l2d2/login.cgi>-ről

lesz elérhető.

Ha a `/var/www` könyvtár helyett a felülethez szükséges file-okat máshol akarjuk elhelyezni, akkor az `../l2d2_6.2/www/` könyvtárban található file-okat másoljuk át az alternatív helyre, természetesen az apache-ot is megfelelően konfigurálnunk kell: a `/var/www` helyett a

```

DocumentRoot /var/www
...
<Directory /var/www/>
...
</Directory>

```

a saját könyvtárunk megadására szükséges.

2.1.4 A DNS szerver hostolása

A DNS szerver L2D2 szempontból megfelelő működtetéséhez szükséges file-okat a

```
./place_files bind9
```

paranccsal telepíthetjük, vagy a telepítést magunk is elvégezhetjük a 2.1.4.2 pont szerint. A fenti parancs a 2.1 pontban leírtakon kívül a következő file-okat helyezi el a gépünkön:

- a `dnsAgent` programot az `/usr/local/sbin/` könyvtárba;
- egy minta DNS konfigurációs file-t (`named.conf`) az `/etc/l2d2/samples/bind9` könyvtárba.

A DNS szerver konfigurálását magunknak kell elvégezni. Ehhez egy minta konfigurációs file-t (`/etc/l2d2/samples/bind9/named.conf`) vehetünk igénybe.

A **`named.conf`** file-t az L2D2 alkalmazás nem módosítja, így minden, az alkalmazással menedzselte zóna számára a zóna-információkat nekünk kell beírni ebbe a file-ba pl.:

```

...
zone "example.org" {
    type master;
    file "/etc/bind/l2d2/example.org.Forward";
    allow-query { any; };
};
zone "168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/l2d2/example.org.Reverse";
    allow-query { any; };
};
...

```

A **forward** és **reverse** táblákat a dnsAgent program generálja az LDAP bejegyzések alapján, az /etc/l2d2/config.txt file-ban megadott könyvtárba. Az alapértelmezett beállítás az /etc/bind/l2d2 könyvtár. Ezt – vagy az általunk megadott könyvtárat – nekünk kell létrehozunk!

2.1.4.1 A DNS agent konfigurálása

Az DNS agent program (dnsAgent.rb) számára az alapértelmezett paramétereket az /etc/l2d2/config.txt konfigurációs file-ban a következők szerint kell megadni:

- hová kerüljön az agent log file-ja
L2D2 log files
...
DNSLogFile = /var/log/dnsAgent.log
...
- a zónabejegyzéseket tartalmazó LDAP szerverhez kapcsolódás paramétereit és azt a könyvtárat, ahová az agent program a forward és a reverse táblákat generálja
#DNS default parameters (dnsAgent)
DNSLDAPHost = 127.0.0.1
DNSLDAPPort = 389
DNSLDAPProto = 3 # 2 or 3 => LDAPv2 or LDAPv3
DNSLDAPUser = # empty string for anonymous
DNSLDAPCred = # LDAP user password
DNSLDAPRetry = 3 # number of retries on errors
DNSLDAPRetryPeriod = 20 # secs
DNSDirectory = /etc/bind/l2d2
- A DNS szerver újraindító parancs helyét
Services
...
DNSServiceRestart = PATH=/sbin:/bin /etc/init.d/bind9 restart
...

2.1.4.2 A DNS szerver kezelő file-ok telepítése a telepítő script nélkül

A DNS agent programot, a segédprogramokat, és az egyéb kezelő file-okat nem a telepítő script által kijelölt default könyvtárba akarjuk elhelyezni, akkor a **./place_files bind9** parancs kiadása helyett a file-okat magunk is telepíthetjük, a következők szerint:

- az **../l2d2_6.2/conf/config.txt** konfigurációs file-t **kötelezően** az **/etc/l2d2/** könyvtárba kell elhelyezni;
- az **../l2d2_6.2/sbin/** könyvtárból másoljuk át a megfelelő programokat (dnsAgent.rb, ldapZoneDelete.rb, dns2ldap.rb, trigger.rb) a kívánt helyre, ügyeljünk arra, hogy az **inetd** daemon **konfigurációs file**-ban (inetd.conf) majd az általunk kiválasztott file-elérési útvonalat adjuk meg;
- a minta-konfigurációk az **../l2d2_6.2/conf** könyvtárban megtalálhatóak, nem érdemes másik helyre átmásolni.

2.1.5 Az IPv4 DHCP szerver hostolása

Az DHCP szerver L2D2 szempontból megfelelő működtetéséhez szükséges fájlokat a

```
./place_files dhcp3
```

paranccsal telepíthetjük, vagy a telepítést magunk is elvégezhethetjük a 2.1.5.2 pontban leírtak szerint. A fenti parancs a 2.1 pontban leírtakon kívül a következő file-okat helyezi el a gépünkön:

- a DHCP szerveret kezelő agent programot (dhcpAgent.rb) az */usr/local/sbin/* könyvtárba;
- egy minta DHCP konfigurációs file-t (dhcpd.conf) és a teszt adatbázis alapján generált minta konfigurációs file-t (example.org.dconf) az */etc/l2d2/samples/dhcp3* könyvtárba.

A DHCP **szerver** (dhcp3-server) **konfigurálását magunknak kell elvégezni**. Ehhez egy minta-konfigurációs file-t (*/etc/l2d2/samples/dhcp3/dhcpd.conf*) vehetünk igénybe.

A konfigurációs file elkészítésénél **ügyelni kell arra**, hogy az **alkalmazással készített**, include-dal beillesztett zóna-információk megfelelő helyre kerüljenek. Ezért fontos, hogy a *dhcpd.conf* file formailag a következőképpen nézzen ki:

```
...  
# Include the l2d2 zone entry's dhcp config file  
# generated by dhcpAgent.rb..
```

A dhcpAgent program a "**generated by dhcpAgent.rb**" szövegrész meglétét ellenőrzi, és ez után illeszti majd be include-dal, a későbbiekben létrehozott zónák dhcp információit tartalmazó file-okat pl.:

```
include "/etc/dhcp3/l2d2/example.org.dconf";
```

majd folytatódhat a konfigurációs file a többi bejegyzéssel.

Ha a fenti szövegrész **hiányzik**, akkor az *include* bejegyzés a konfigurációs **file végére kerül**.

A dhcp információkat tartalmazó file-okat (minta:

/etc/l2d2/samples/dhcp3/example.org.dconf) a dhcpAgent program generálja az LDAP bejegyzések alapján, az */etc/l2d2/config.txt* file-ban megadott könyvtárba. Az alapértelmezett beállítás az */etc/dhcp3/l2d2* könyvtár. Ezt – vagy az általunk megadott könyvtárat – nekünk kell létrehoznunk!

Ha maradunk a minta konfigurációkban megadott 192.168.0.0 hálózati címek használatánál, akkor a **szerver elindítása előtt** a gépünkön **konfigurálni kell egy virtuális interface-t** pl. az "eth0" interface-re:

```
yourhost:~#sbin/ifconfig eth0:0 192.168.0.10 netmask 255.255.255.255 broadcast 192.168.0.10 up
```

A **DHCP szerver korrekt működéséhez** (pl. Windows kliens használatánál) mindenképpen szükség van a gépünkön egy **routing bejegyzésre**:

```
yourhost:~#route add -host 255.255.255.255 dev eth0
```

2.1.5.1 A DHCP agent konfigurálása

A DHCP agent program (dhcpAgent.rb) számára az alapértelmezett paramétereket az /etc/l2d2/config.txt konfigurációs file-ban a következők szerint kell megadni:

- hová kerüljön az agent log file-ja

```
# L2D2 log files
...
DHCPLogFile = /var/log/dhcpAgent.log
...
```

- a zónabejegyzéseket tartalmazó LDAP szerverhez kapcsolódás paramétereit és a konfigurációs file-ok helyét

```
#IPv4 DHCP default parameters (dhcpAgent)

DHCPLDAPHost = 127.0.0.1
DHCPLDAPPort = 389
DHCPLDAPProto = 3 # 2 or 3 -=> LDAPv2 or LDAPv3
DHCPLDAPUser = # empty string for anonymous
DHCPLDAPCred = # LDAP user password
DHCPLDAPRetry = 3 # number of retries on errors
DHCPLDAPRetryPeriod = 20 # secs
DHCPConfDir = /etc/dhcp3/l2d2
DHCPConfFile = /etc/dhcp3/dhcpd.conf
```

- a DHCP szerver újraindító parancs helyét

```
# Services
...
DHCPServiceRestart = PATH=/sbin:/bin /etc/init.d/dhcp3-server restart
```

2.1.5.2 A DHCP szerver kezelő file-ok telepítése a telepítő script nélkül

Ha a DHCP agent programot, a segédprogramokat, és az egyéb kezelő file-okat nem a telepítő script által kijelölt default könyvtárba akarjuk elhelyezni, akkor a **./place_files dhcp3** parancs kiadása helyett a file-okat magunk is telepíthetjük, a következők szerint:

- az **../l2d2_6.2/conf/config.txt** konfigurációs file-t **kötelezően** az **/etc/l2d2/** könyvtárba kell elhelyezni;
- az **../l2d2_6.2/sbin/** könyvtárból másoljuk át a megfelelő programokat (dhcpAgent.rb, ldapZoneDelete.rb, dns2ldap.rb, trigger.rb) a kívánt helyre, ügyeljünk arra, hogy az **inetd** daemon **konfigurációs file**-ban (inetd.conf) majd az általunk kiválasztott file-elérési útvonalat adjuk meg;
- a minta-konfigurációk az **../l2d2_6.2/conf** könyvtárban megtalálhatóak, nem érdemes másik helyre átmásolni.

2.1.6 A DHCPv6 szerver hostolása

Az IPv6 DHCP szerver (dibbler-server) L2D2 szempontból megfelelő működtetéséhez a szükséges file-okat a

```
./place_files dibbler
```

paranccsal telepíthetjük, vagy a telepítést magunk is elvégezzük a 2.1.6.2 pontban leírtak szerint. A fenti parancs a 2.1 pontban leírtakon kívül a következő file-okat helyezi el a gépünkön:

- a DHCPv6 szervert kezelő **agent programot** (dhcpv6Agent.rb) az */usr/local/sbin/* könyvtárba;
- minta dibbler konfigurációs file-okat (client.conf, relay.conf, server.conf) és a teszt adatbázis alapján, a dhcpv6Agent programmal generált minta-konfigurációs file-t (example.org.v6dconf) az */etc/l2d2/samples/dibbler* könyvtárba.

A **dibbler szerver konfigurálását magunknak kell elvégezni**. Ehhez egy minta-konfigurációs file-t (*/etc/l2d2/samples/dibbler/server.conf*) vehetünk igénybe.

A konfigurációs file elkészítésénél **ügyelni kell arra**, hogy a kiválasztott zóna új dhcp konfigurációja megfelelő helyre kerüljön. Ezért fontos, hogy a *server.conf* file formailag a következőképpen nézzen ki, pl. az eth0 interface-re:

```
...
Iface "eth0" {
...
# include the l2d2 zone entry's, generated by dhcpv6Agent.rb

...
}
```

A dhcpv6Agent program a "**generated by dhcpv6Agent.rb**" szövegrész meglétét ellenőrzi, és ez után illeszti majd be a kiválasztott zóna új konfigurációját tartalmazó sorokat (a #<kiválasztott zóna domain neve> és az #END záró komment sor közé, amelyeket nem szabad kivenni a konfigurációs file-ból!). A Dibbler szerver jelenlegi változata (0.4.1) **nem támogat több konfigurációs file-t**, ezért másolja az agent a teljes zóna-konfigurációt a *server.conf* file-ba.

A agent program a kiválasztott zóna IPv6 dhcp konfigurációit tartalmazó file-t (minta a dokumentáció 4.4 pontjában, ill. az */etc/l2d2/samples/dibbler/example.org.v6dconf* file-ban látható) az */etc/l2d2/config.txt* file-ban megadott könyvtárba is elhelyezi. Az alapértelmezett beállítás az */etc/bind/l2d2* könyvtár. Ezt – vagy az általunk megadott – könyvtárat nekünk kell létrehozunk!

2.1.6.1 A DHCPv6 agent konfigurálása

A DHCPv6 agent program (dhcpv6Agent.rb) számára az alapértelmezett paramétereket az */etc/l2d2/config.txt* konfigurációs file-ban a következők szerint kell megadni:

- hová kerüljön az agent log file-ja
- ```
L2D2 log files
...
DHCPv6LogFile = /var/log/dhcpv6Agent.log
...
```

- a zónabejegyzéseket tartalmazó LDAP szerverhez kapcsolódás paramétereit és a konfigurációs file-ok helyét

```
#IPv6 DHCP default parameters (dhcpv6Agent)
DHCPv6LDAPHost = 127.0.0.1
DHCPv6LDAPPort = 389
DHCPv6LDAPProto = 3 # 2 or 3 ==> LDAPv2 or LDAPv3
DHCPv6LDAPUser = # empty string for anonymous
DHCPv6LDAPCred = # LDAP user password
DHCPv6LDAPRetry = 3 # number of retries on errors
DHCPv6LDAPRetryPeriod = 20 # secs
DHCPv6ConfFile = /etc/dibbler/server.conf
DHCPv6ConfDir = /etc/dibbler/l2d2
```

- a Dibbler szerver újraindító parancs helyét

```
Services
...
DHCPv6ServiceRestart = PATH=/sbin:/bin /etc/init.d/dibbler-server restart
...
```

### 2.1.6.2 A DHCPv6 szerver kezelő file-ok telepítése a telepítő script nélkül

Ha az IPv6 DHCP agent programot, a segédprogramokat, és az egyéb kezelő file-okat nem a telepítő script által kijelölt default könyvtárba akarjuk elhelyezni, akkor a `./place_files dibbler` parancs kiadása helyett a file-okat magunk is telepíthetjük, a következők szerint:

- az `../l2d2_6.2/conf/config.txt` konfigurációs file-t **kötelezően** az `/etc/l2d2/` könyvtárba kell elhelyezni;
- az `../l2d2_6.2/sbin/` könyvtárból másoljuk át a megfelelő programokat (`dhcpv6Agent.rb`, `ldapZoneDelete.rb`, `dns2ldap.rb`, `trigger.rb`) a kívánt helyre, ügyeljünk arra, hogy az **inetd** daemon **konfigurációs file**-ban (`inetd.conf`) majd az általunk kiválasztott file-elérési útvonalat adjuk meg;
- a minta-konfigurációk az `../l2d2_6.2/conf` könyvtárban megtalálhatóak, ezeket nem érdemes átmásolni.

### 2.1.7 Az inetd daemon konfigurálása

Minden gépen, amelyen az L2D2 alkalmazással kezelt bármelyik szerver (és a megfelelő agent programot) futtatni akarjuk, szükséges az **inetd** daemon **megfelelő konfigurálása** és **futtatása**. Az `inetd.conf` file-ban kell megadni azt, hogy az adott szerver kezelő ügynök hol található és mely porton érhető el. Egy minta konfigurációs file látható az `/etc/l2d2/samples/` könyvtárban, a fejlesztés során használt portkiosztással:

```
1052 stream tcp nowait root /usr/local/sbin/ldapAgent.rb
1052 dgram udp wait root /usr/local/sbin/ldapAgent.rb
1053 stream tcp nowait root /usr/local/sbin/dnsAgent.rb
1053 dgram udp wait root /usr/local/sbin/dnsAgent.rb
1054 stream tcp nowait root /usr/local/sbin/dhcpAgent.rb
1054 dgram udp wait root /usr/local/sbin/dhcpAgent.rb
1055 stream tcp nowait root /usr/local/sbin/dhcpv6Agent.rb
1055 dgram udp wait root /usr/local/sbin/dhcpv6Agent.rb
```

Természetesen a **port szabadon választható**, de ügyeljünk arra, hogy az adatbázis, ill. a zónák kezelőfelületről való inicializálásakor az *inetd.conf* **file-ban megadott portot állítsuk be**.

### 2.1.8 Az alkalmazás eltávolítása

Ha a *./place\_files* **paranccsal** telepítettük az alkalmazás file-jait, akkor a *./remove\_files* parancs a törlésüket is elvégzi.

Ha a telepítést nem a *./place\_files* script-tel végeztük a default könyvtárakba, akkor a file-ok törlését is magunknak kell elvégezni.

## 2.2 Az LDAP adatbázis inicializálása az L2D2 számára (top-level zóna létrehozása és törlése)

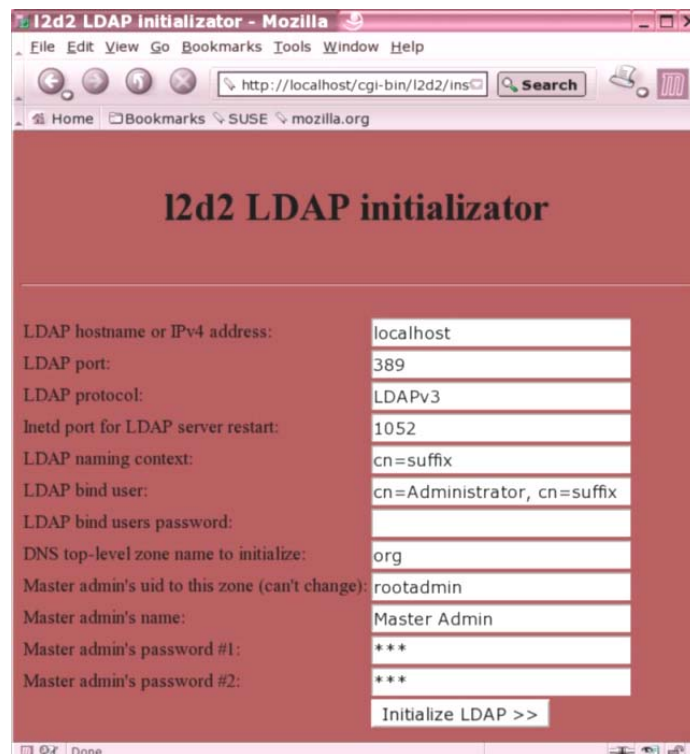
Az **LDAP** adatbázis **kezdeti feltöltése** (a menedzselni kívánt top-level zóna megadása, adminisztrátorok definiálása, ... stb.) az *install.cgi* programmal történik, amelyet bármilyen böngészővel elindíthatunk, a következő URL használatával:

<http://yourhost/cgi-bin/l2d2/install.cgi>

A telepített **apache** szervernek természetesen a *yourhost* gépen kell futnia, de az **LDAP szerver** futhat más gépen is.

Ezt a programot kell indítani akkor is, ha az LDAP adatbázisunkban **több top-level zóna DNS, DHCP és DHCPv6** adatait akarjuk tárolni. **Top-level** zónán a továbbiakban az alkalmazással menedzselhető **legfelső szintet** értjük, amelyet itt a kezdeti inicializálásnál beállítottunk (pl. *.org*, *.com*...stb., vagy lehetne akár *.test.net* is, de az utóbbi esetben természetesen a *.net* inicializálásának a későbbiekben már nincs értelme). A **top-level zónát csak a rootadmin felhasználónak van joga módosítani!**

Indítás után a CGI az 1. ábrán látható módon jelenik meg:



|                                                 |                             |
|-------------------------------------------------|-----------------------------|
| LDAP hostname or IPv4 address:                  | localhost                   |
| LDAP port:                                      | 389                         |
| LDAP protocol:                                  | LDAPv3                      |
| Inetd port for LDAP server restart:             | 1052                        |
| LDAP naming context:                            | cn=suffix                   |
| LDAP bind user:                                 | cn=Administrator, cn=suffix |
| LDAP bind users password:                       |                             |
| DNS top-level zone name to initialize:          | org                         |
| Master admin's uid to this zone (can't change): | rootadmin                   |
| Master admin's name:                            | Master Admin                |
| Master admin's password #1:                     | ***                         |
| Master admin's password #2:                     | ***                         |

Initialize LDAP >>

1. ábra

Az űrlapon az **első hat** mező az **LDAP szerver** és az adatbázis paramétereit tartalmazza.

Az első mezőbe kell a **gép domain nevét/IP címét** beírni akkor, ha az **LDAP szerver nem a CGI-t futtató gépen** van. Az **“Inetd port for LDAP server restart”** mezőbe azt a port számot kell megadni, amelyen az *inet* daemon várakozik az LDAP ügynök indítására (bővebb információ a 3.4 pontban).

Az **“LDAP bind users password”** mezőbe a *secret* szót kell beírni akkor, ha a minta-konfigurációs file-t használjuk (*/etc/ldap/slapd.conf* file).

A **“DNS top-level zone name to initialize”** mezőbe az *org* helyett természetesen az inicializálni kívánt zónanevet kell megadni.

A **“Master Admin's uid to this zone”** mezőbe alapértelmezésben (és nem módosíthatóan) a *rootadmin* felhasználónév kerül, vagyis ennek az adminisztrátornak lesz **írásai joga a top-level zóna teljes adatbázisára**. Ezzel a felhasználóval lehet a top-level alá az első zónát(zónákat), **alhálózatokat, hosztokat és adminisztrátorokat definiálni** (a *unix* rendszerek *root* felhasználójához hasonlóan). A **“Master Admin's name”** és a **“Master Admin's password ..”** szabadon megválasztható.

Az **Initialize LDAP >>** kijelölése után, ha az űrlap hibátlan, akkor a következő üzenet jelenik meg a képernyőn:

**“LDAP updated succesfully.....login”**

A *login* kiválasztásával léphetünk be a rendszerbe (érdemes a megjelenő web felület URL-jét későbbi használatra könyvjelzővel megjelölni).

A **top-level zóna létrehozásakor az alkalmazás automatikusan** elvégzi a következőket:

- az **LDAP jogosultságok kezdeti beállítását, vagyis az `/etc/ldap/l2d2/` könyvtárba** elkészíti az éppen inicializált zóna menedzseléséhez szükséges access file-okat (pl. az 1-es ábrán látható példa-zónához): **org.access** (a kezdeti ACL-ekkel)

**org.access.lock**

- az **LDAP szerver konfigurációjának a módosítását** (`/etc/ldap/slapd.conf`): beilleszti a konfigurációs file-ba a most inicializált **top-level zónát leíró** access file-t a

...  
 # ACL file contains all the deeper include lines  
 comment sor után:

```
include "/etc/ldap/l2d2/org.access"
(A fenti comment sort nem szabad kivenni a slapd.conf file-ból!)
```

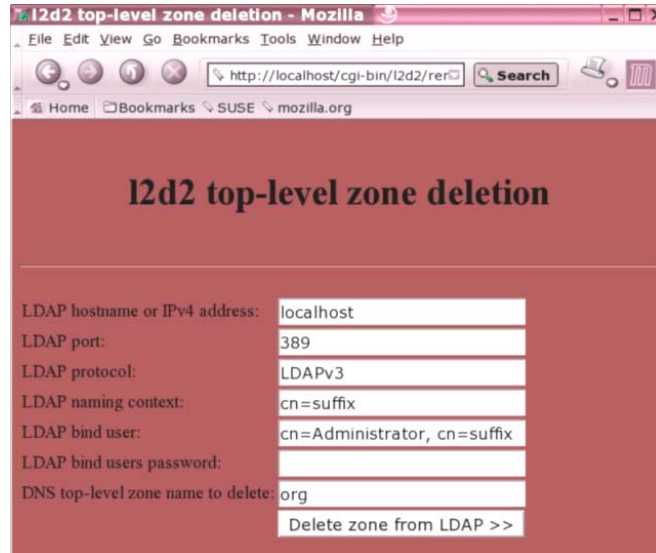
- az **LDAP szerver újraindítását**

**Top-level zóna törlése** az LDAP adatbázisból a ***remove.cgi*** programmal történik, amelyet bármilyen böngészővel elindíthatunk, a következő URL használatával:

<http://yourhost/cgi-bin/l2d2/remove.cgi>

A telepített **apache** szervernek természetesen a *yourhost* gépen kell futnia, de az **LDAP szerver** futhat más gépen is.

**Indítás után a CGI** az 2. ábrán látható módon jelenik meg:



2. ábra

Az űrlapon az **első hat** mező az **LDAP szerver** és az adatbázis paramétereit tartalmazza, kitölteni az inicializálásnál leírt módon kell.

A **“DNS top-level zone name to delete”** mezőbe az **org** helyett a törölni kívánt zónanevet kell beírni. Az alkalmazás figyelmeztet, ha a zóna nem üres, de töröl mindent, ha úgy kívánjuk (a figyelmeztetést tartalmazó űrlapon a ***Delete all*** kijelölése).

### 3. Zóna menedzsment

Ez a fejezet a **felhasználói felület használatával** foglalkozik. Ismereteket feltételez a **DNS**, az **IPv4 DHCP** és az **IPv6 DHCP működéséről**, ezekkel nem szeretnénk külön foglalkozni. Nem foglalkozunk azzal sem, hogy mi az a **SOA rekord**, milyen **formátumú egy IPv6-os IP cím**, vagy egy Ethernet **MAC cím**. Csak a **CGI használatának specialitásait**, az **alkalmazás filozófiáját** szándékozunk bemutatni. A dokumentációban szereplő minta-űrlapok adatai az alkalmazás fejlesztésekor használt teszt-adatbázis bejegyzései.

#### 3.1 CGI elérése, bejelentkezés az alkalmazásba

Az **L2D2** alkalmazást bármilyen böngészővel a **következő URL-en érhetjük el**:

<http://yourhost/cgi-bin/l2d2/login.cgi>

Az **install.cgi** sikeres befejezése után egy HTML linket kapunk erre az oldalra, amelyet érdemes a böngészőnkben könyvjelzővel megjelölni (a további bejelentkezések is ezen az URL-en keresztül történnek). A **kezdőoldalon be kell jelentkezünk**, autentikálnunk kell magunkat, hogy használhassuk a rendszert. A **top-level** zóna inicializálása után a **rootadmin uid**-del (vagy a nevével - a 2.3 fejezetben *Master Admin* volt a példában -) belépve lehet és kell a **következő szintű zónát** (zónákat) létrehozni, ill. azokat az adminisztrátorokat definiálni, akik ezeket menedzselni fogják. Ha az adatbázisban több top-level zóna található, akkor a **rootadmin** egy listából kiválaszthatja azt, amelyet éppen bővíteni/módosítani szeretne.

A 3. ábrán látható űrlap ezen a szinten (top-level) csak a **rootadmin felhasználónál** jelenik meg, egyéb felhasználó csak azokat a zóna-információkat (pl. SOA bejegyzések) módosíthatja, amelyekhez írással rendelkezik. Nem hozhat létre új zónát és nem definiálhat felhasználót sem.



3. ábra

A kiválasztott feladat elvégzéséhez most és az összes többi űrlapon is a **jobbra mutató kettős nyilat ábrázoló gombot** kell kijelölnünk.

A leírás további részei általánosak, tehát az alkalmazást (zónák, subnet-ek, hosztok menedzselése, adminisztrátorok definiálása, szerver agent-ek indítása, .. stb.) a **rootadmin** és az **egyéb adminisztrátorok** - természetesen a megfelelő jogosultság birtokában - azonos módon használhatják.

Ha a bejelentkezésnél **megadott néven** a program talált legalább egy **adminisztrátort** az **LDAP adatbázisban**, akkor az **adminisztrátorhoz rendelt zónák/subnet-ek** listájából kiválaszthatjuk azt, amelyikhez hozzá szeretnénk férni.

Ha nem sikerült az LDAP-ban azonosítani az adminisztrátort, akkor erről figyelmeztetést kapunk, és ismét megpróbálhatunk bejelentkezni. Előfordulhat, hogy az LDAP-ban **több adminisztrátor bejegyzés** is kapcsolódhat az általunk begépelte névhez, pl. ha a **fa mélyebb ágaiban** is szerepel **adott nevű** vagy **adott azonosítóval rendelkező adminisztrátor**, vagy ha **dszökert** használtunk a név megadásakor, pl. **Szekeres\*** formában, amely az összes **Szekeres**-sel kezdődő nevű adminisztrátort jelenti. Ilyen esetben az adminisztrátor azonosítása még nem ért véget, a listán az **összes lehetséges adminisztrátor** az **összes hozzá tartozó zónával** felsorolásra kerül, ekkor a **megfelelő admin-zóna pár melletti gombot kijelölve** egyértelműsíthetjük azt, hogy éppen melyik zónát/alhálózatot akarjuk menedzselni.

Az **adminisztrátorhoz** tartozó **érvényes jelszó** begépelése után megjelenik az alkalmazás **főmenüje** (4-es ábra). Az oldal tetején minden esetben látható az éppen **menedzselte zóna/subnet DNS domain neve**, a belépő **adminisztrátor neve** és a zóna/subnet **IPv4-es** és **IPv6-os** (ha van) **IP címe**.



4. ábra

A megfelelő menüpont kiválasztásával **írhatunk** az LDAP adatbázisba **új IPv4/IPv6 subzónát, subnet-et** és **hosztot** - DHCP adatokkal együtt -, vagy **módosíthatjuk** a már **meglévők adatait**.

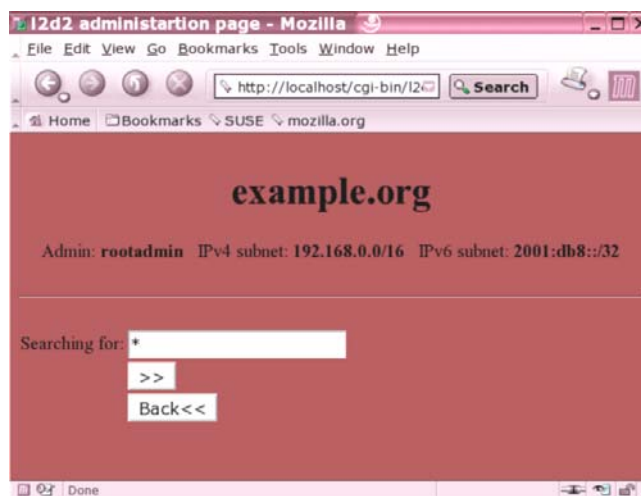
Létrehozhatunk **új felhasználót** és **rendelhetünk hozzá adminisztrálásra subzónát vagy subnet-et**, ill. megfelelő jogosultsággal **módosíthatunk felhasználói password-öt**, felhasználói adatokat.

**Elkészíthetjük a DNS, a DHCP és a DHCPv6 szerverek új konfigurációit**, az LDAP szerver **frissített jogosultsági listáját** és **újraindíthatjuk a szervereket**.

**Megváltoztathatjuk saját LDAP jelszavunkat**, ill. **visszaléphetünk a DNS fa egy magasabb szintjére**. A továbbiakban részletesen leírjuk az alkalmazás használatát az egyes menüpontokon keresztül.

### 3.2 Keresés, módosítás, törlés

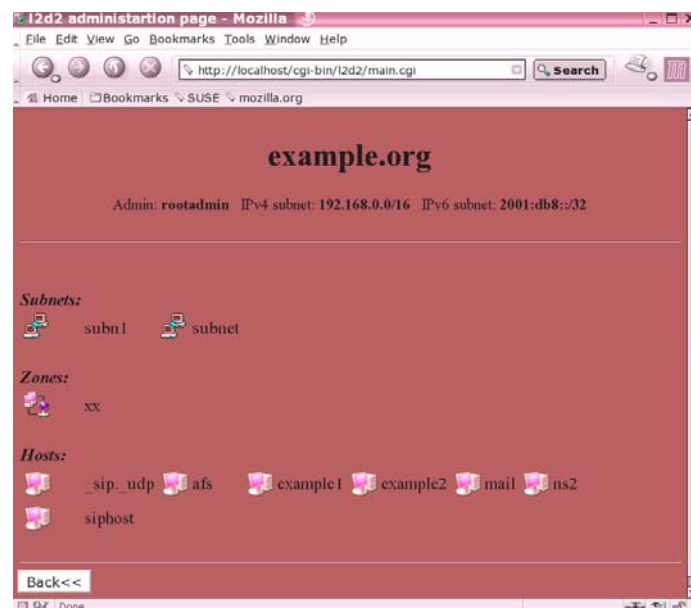
A főmenü “>>Search and modify” menüpontját kijelölve megnézhetjük, hogy az **adott zónához az adatbázisban milyen bejegyzések tartoznak**:



5. ábra

A megjelenő **kereső-képernyőn** megadhatunk **konkrét hoszt-nevet, zóna-nevet, alhálózat-nevet, alternatív nevet (DNS CNAME), IP címet, felhasználó nevet**, vagy a dzsóker karaktert felhasználva töredéknevet. Megadhatunk **IP címtartományt** is, ebben az esetben a fókuszban lévő subzóna/subnet szabad IP címeinek listáját kapjuk meg, amely az új hoszt regisztrálását segíti (pl.: 192.168.0.10-198.168.0.50). Ha minden bejegyzést látni akarunk, akkor hagyjuk módosítatlanul a dzsóker karaktert, és jelöljük ki a **jobbra mutató kettős nyilat**.

A kiválasztásnak megfelelően megkapjuk a menedzselte zóna/subnet összes bejegyzésének csoportosított és rendezett listáját (a 6. ábrán a tesztadatbázis *example.org* zónájának minden entry-je látható):



6. ábra

A bejegyzések bal oldalán látható icont kijelölve nyithatjuk meg szerkesztésre vagy esetleg törlésre az adott elemet. A megfelelő icont kiválasztása után megjelenik egy űrlap a bejegyzés részletes adataival. Az űrlapon végzett módosítások a már ismert jobbra mutató kettős nyíl kijelölésével vihetők vissza az adatbázisba. Természetesen **módosítani**, ill. **törölni** egy bejegyzést csak a **megfelelő jogosultsággal lehet**. Az adatbázisba való visszaírás előtt az alkalmazás **ellenőrzi az adatok helyességét**, ha hibás, és a **hiba javítható**, akkor – az összes hibajelzéssel együtt – **további módosításra visszkapjuk az űrlapot**. Ha az űrlap hibátlan, akkor a **módosítások azonnal bekerülnek az LDAP adatbázisba**. Adminisztrátori bejegyzés módosítása (új adminisztrátor regisztrálása, vagy egy létező törlése) után az alkalmazás automatikusan frissíti az LDAP jogosultsági listát.

A 7. ábrán az *example1.example.org* hoszt minta-adatai láthatóak:

The screenshot shows a web browser window titled "I2d2 administration page - Mozilla". The address bar shows "http://localhost/cgi-bin/i2c2/main.cgi". The page content is for "example.org" and shows the following configuration fields:

- Name and IP addresses:** Hostname: example1, IPv4 addresses: 192.168.0.1, IPv6 addresses: 2001:db8::1
- DNS data:** Host TTL, DNS CNAME, Mail handler (MX), Host information, DNS SRV, Text, CERT, Comment: tulajdonos;info;Ethernet
- DHCP parameters:** Hardware address: 00:07:e9:6c:44:c9
- DHCPv4 parameters:** IPv4 default route, IPv4 default lease time, IPv4 maximum lease time, IPv4 name server, Other IPv4 DHCP options
- DHCPv6 parameters:** IPv6 preferred lifetime, IPv6 valid lifetime, IPv6 T1 timer, IPv6 T2 timer

At the bottom, there are buttons: ">>", "Don't check IP addresses!", "Delete", and "Back<<".

7. ábra

A **“Hostname”** megadása kötelező! Az **“IPv4 addresses”** és az **“IPv6 addresses”** meglétét, ill. helyességét (IPv4 és/vagy IPv6 subnet-nek megfelel-e) az alkalmazás ellenőrzi, hiba esetén figyelmeztető üzenetet küld, de - a formai hiba kivételével - a **“Don't check IP addresses”** kijelölésével elfogadtathatjuk a beírt címeket, vagy az üresen hagyott mezőt. Ha a **“Hostname”** mezőbe **“idegen” domain**-hez tartozó nevet írunk, akkor (a domain regisztrációnál megszokott módon) **pontot kell a név után begépelni!** Ezek a hosztok a DNS táblák generálásánál csak a megfelelő **reverse** táblába íródnak be. A többi adat opcionális, de értelemszerűen pl. nem lehet megadni MAC címet, ha nem írtunk be egy IP címet sem.

Ha **több IP címet, több CNAME** bejegyzést, **több mail szerveret, vagy több SRV rekordot** adunk meg, akkor ezeket egymástól vesszővel elválasztva kell az adott mezőbe bérni.

A **“Mail handler ”** (MX rekord) **formátuma:** *prioritás#<teljes domain név>, prioritás#<teljes domain név>,...* Az MX rekordoknál nem kell pont karakter a szerver(ek) neve után, a DNS táblák generálásánál az alkalmazás automatikusan beírja azt.

A **“DNS SRV ”** (szolgáltatáshely) erőforrásrekord **formátuma:** *t1#prioritás#súly#port#<szolgáltató gép teljes domain neve>, ..*

Ekkor a **“Hostname”** mező formátuma: *szolgáltatás.protokoll* (pl.: *\_ sip\_udp*). A szolgáltató gép neve után nem kell pont karakter, a DNS táblák generálásánál az alkalmazás automatikusan beírja azt.

A **“Hardware address ”** (Ethernet MAC cím) mezőt akkor töltjük ki, ha az adott hoszt **IPv4** vagy **IPv6 DHCP-n** keresztül kéri a hálózati beállításait. A **DHCPv6** konfigurációk elkészítésekor az alkalmazás, a **MAC címből IPv6 link-local címet generál** (EUI-64 kódolással, helyesen kiegészített U/L bittel).

A többi **IPv4 DHCP bejegyzés megadása opcionális**, ha üresen hagyjuk, akkor a hoszt számára a **globális** – subnet-nél/zónánál/dhcp szerver konfigurációs file-ban megadott - **IPv4 DHCP paraméterértékek** lesznek érvényesek.

Az **“Other IPv4 DHCP options”** mezőbe, ha kitöltjük, akkor a teljes paramétert (több paraméter esetén egymástól pontosvesszővel elválasztva), szükség esetén idézőjelek (“”) között kell beírni.

Az **IPv6 DHCP** paraméterek megadása is opcionális, ha üresen hagyjuk, akkor a hoszt számára az interface konfigurálásánál (*/etc/dibbler/server.conf* file) megadott **globális**, vagy a **subnet-nél** vagy a **zónánál** beállított **IPv6 DHCP időértékek** lesznek érvényesek.

A **Comment** mező kitöltése opcionális, a mezőben használható karakterek:

[a-zA-Z0-9\_()-! :]. **Formája:**

<tulajdonos>;<info>;<Ethernet cím>;<dátum>

- az **info** mező bármi lehet, pl.: a gép helye, típusa, WiFi interface, stb.
- az **Ethernet cím**, ha ismert
- új hoszt felvitelnél a napi **dátumot** az alkalmazás írja be a mezőbe, de módosítható.

A mező kitöltésénél formai ellenőrzés történik, hiba esetén visszakapjuk javításra az űrlapot.

Ha a **“Hostname”** mezőt, vagy az **adminisztrátor** módosításánál a **“User identifier”** mezőt **változtatjuk meg**, akkor **új bejegyzés keletkezik az adatbázisban**, a régi pedig **törlődik**.

**Zóna** és **subnet** esetén a **“name”** **nem módosítható!** Az alkalmazás **figyelmeztető üzenet** kíséretében az **eredeti subzóna/subnet űrlapot** adja vissza akkor, ha megkíséreljük megváltoztatni a **“name”** mezőt.

A **zóna** és az **alshálózat módosításakor** megjelenő **“Change to”** gomb arra szolgál, hogy az éppen **menedzsel** zónát vagy **alshálózatot lecseréljük** arra, amelyet szerkesztésre megnyitottunk. Szemléletesen úgy gondolhatunk erre, hogy az LDAP fában hajtunk végre a fájlrendszerhez hasonlóan **cd** parancsot, amelynek hatására megváltozik a munkakönyvtárunk. Ha a bejelentkezéskor - a példánknak megfelelően - az **example.org** zóna menedzselését választottuk, akkor kezdetben a fának a hozzá rendelt pontja a munkakönyvtárunk. Ha megnyitjuk módosításra a példa szerinti **subn1** alshálózatot, akkor az ott megjelenő **“Change to” gomb** hatására a **subn1.example.org** alshálózat lesz az alkalmazás fókuszában. Erről meggyőző bizonyítékot szolgáltat a lap tetején látható nagy betűs felirat megváltozása is.

Ennek a lehetőségnek az **ellenpárja a főmenüben** található **“Change to upper level”** menüpont, amely a fájlrendszerben a **cd ..** parancs analógja: az LDAP fában egy **szinttel feljebb lépteti az alkalmazás munkapontját**. Pl. ha átváltottunk a **subn1.example.org** alshálózat menedzselésére, akkor a **Change to upper level** gomb kiválasztása **visszavisz** minket az **example.org zóna főmenüjébe**. Az **example.org** zónából is **feljebb** lehet lépni, ekkor az LDAP adatbázisban a **.org** suffix szintjére kerülünk. Innen **nem lehet feljebb lépni**, hiszen már így is egy **virtuális pontján járunk a domain név** rendszernek. Ezen a szinten már nem lehet új hosztokat, alshálózatokat létrehozni, csak új zónát, ill. egy már létező **zóna** adatait (SOA rekord, NS szerverek, ... stb.) tudjuk módosítani (megfelelő jogosultsággal).

A **“Delete”** gomb megjelölésével tudunk egy **bejegyzést törölni az LDAP adatbázisból** (itt csak üres zóna vagy alshálózat törölhető). Abban az esetben, ha **zónát** vagy **alshálózatot** jelölünk ki **törlésre**, akkor az alkalmazás ellenőrzi azt, hogy van e olyan **felhasználó az adatbázisban**, aki az éppen **törlésre** kerülő **zónát** vagy **subzónát/alshálózatot adminisztrálja**. Ha van, akkor **módosítja a felhasználó adatait**, ill. **törli a felhasználót is**

az adatbázisból, ha számára nincs több delegált subzóna vagy subnet. Az LDAP jogosultsági lista automatikusan frissítődik, a szerver újraindul.

A “Back>>” gomb kijelölésével a bejegyzés módosítása nélkül visszaléphetünk az előző lista-ablakhoz.

### 3.2.1 Zóna törlése

Egy tetszőleges zónát egy parancssorból indítható, Ruby nyelven írt script segítségével könnyedén kitörölhetünk az LDAP adatbázisból.

Az `/usr/local/sbin/ldapZoneDelete.rb` program törli a megadott zónát, az összes bejegyzésével együtt: a DNS fa alsóbb szintjein létrehozott hosztokat, subzonákat, alhálózatokat és adminisztrátorokat, végül a megadott zónát is.

A program paramétereit:

|               |                                                                                                                          |
|---------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>--help</b> | az alábbi paraméterek lekérdezése                                                                                        |
| <b>--host</b> | az LDAP szervert futtató gép neve, vagy IP címe (alapértelmezés: 127.0.0.1)                                              |
| <b>--port</b> | az LDAP szerver standard portja (alapértelmezés: 389)                                                                    |
| <b>--user</b> | a zóna inicializálásánál megadott “LDAP bind user”<br>(alapértelmezés: cn=Administrator, cn=suffix)                      |
| <b>--pw</b>   | a top-level zóna inicializálásánál megadott “LDAP bind users password”<br>(alapértelmezés: secret)                       |
| <b>--zone</b> | a törölni kívánt zóna LDAP bejegyzésének DN-je (alapértelmezés:<br>L2D2ZoneName=example,L2D2NamingSuffix=org, cn=suffix) |

A program alapértelmezett paramétereit az `/etc/l2d2//config.txt` konfigurációs file-ban lehet átállítani.

**Top-level zóna ezzel a script-tel nem törölhető!**

Ha a programot az LDAP szervert futtató gépen indítjuk el (--host 127.0.0.1 vagy localhost), akkor a zóna bejegyzéseihez tartozó jogosultságokat tartalmazó ACL file-ok is törlődnek a directory-ból, de az LDAP konfigurációs file-t módosítani kell (a megfelelő `include` sor törlése) a szerver újraindítása előtt!

## 3.3 Új hosztok, alhálózatok

Új hoszt felvételéhez értelemszerűen a főmenü “>>Create a new host” menüpontját kell kiválasztanunk, új alhálózat létrehozásához pedig a “>>Create a new subnet” pontot. Az írási műveletekhez megfelelő jogosultság szükséges, amelyet az LDAP szerver kezel. Gyakran adódhat probléma abból, hogy egy művelet végrehajtásához nem rendelkezünk a szükséges engedélyekkel. Minden adminisztrátor csak a számára delegált zónát/subnet-et módosíthatja.

Egy **új elem felvitelekor** gyakorlatilag **ugyanazt az űrlapot** látjuk a képernyőn, amelyet az elem módosításakor. **Két kis különbség** azért természetesen adódik: az első, hogy módosításkor a megjelenő **űrlap már ki van töltve**, a másik különbség az űrlap alatt található **gombok száma**. **Új elem felvitelekor** csak **három gomb** közül választhatunk: a már ismert jobbra mutató kettős nyíl az űrlapra felvitt adatok rögzítésére szolgál, a **“Don't check IP subnet addresses>>”** az IPv4 és IPv6 címek ellenőrzését kapcsolja ki, a **“Back>>”** gomb kijelölésével itt is minden következmény nélkül megszakíthatjuk a tevékenységet.

**Új hoszt** felvitelére/módosítására használt űrlap részletes leírása a 3.2 pontban látható.

**Új subnet** létrehozása a következő ábrán látható űrlap segítségével történik:

The screenshot shows a web browser window with the URL `http://localhost/cgi-bin/l2d2/main.cgi`. The page content includes the following form fields:

- Name and subnet data:** Subnet name: test; IPv4 subnet: ; IPv6 subnet:
- DNS data:** Mail handler (MX): ; AFSDB: 3600#1#afs.db.example
- DHCPv4 parameters:** Global IPv4 default route: ; IPv4 default lease time: ; IPv4 maximum lease time: ; IPv4 name server: ; Other IPv4 global DHCP options:
- DHCPv6 parameters:** IPv6 preferred lifetime: ; IPv6 valid lifetime: ; IPv6 T1 timer: ; IPv6 T2 timer:

At the bottom of the form, there are five buttons: `>>`, `Don't check subnet addresses!`, `Change to`, `Delete`, and `Back<<`.

8. ábra

A **“Subnet name”** megadása kötelező! Az **IP címek** formája: **hálózat/maszk**, ill. **IPv6 globál cím/prefix-hossz**. Az **“IPv4 subnet”** és az **“IPv6 subnet”** meglétét, ill. helyességét (a zóna felvitelénél megadott IPv4 és/vagy IPv6 subnet-nek megfelel-e) az alkalmazás ellenőrzi, hiba esetén figyelmeztető üzenetet küld, de - a formai hiba kivételével - a **“Don't check subnet addresses”** kijelölésével elfogadtathatjuk a beírt címeket, vagy az üresen hagyott mezőt (mezőket). **Új hoszt felvitelénél** az alkalmazás ellenőrzi azt, hogy a hoszt **IP címe** része-e az **itt megadott IP cím-tartománynak** (tartományoknak).

Az **“AFSDB”** (Andrew File System Database) erőforrásrekord megadásának **formátuma**: `ttl#altípus#kiszolgáló`

A **“Global IPv4 default route”** -tól **“Other IPv4 global DHCP options”** -ig mezők kitöltésével beállíthatjuk azokat az **IPv4 DHCP paraméterértékeket**, amelyek **érvényesek lesznek a subnet összes hoszt-jára** addig, amíg egy hoszt szerkesztésre megnyitott űrlapján felül nem írjuk valamelyik értéket. Az **itt megadott DHCP értékek felülírják a zónánál**, vagy az **IPv4 DHCP konfigurációs file-ban beállított globális értékeket!**

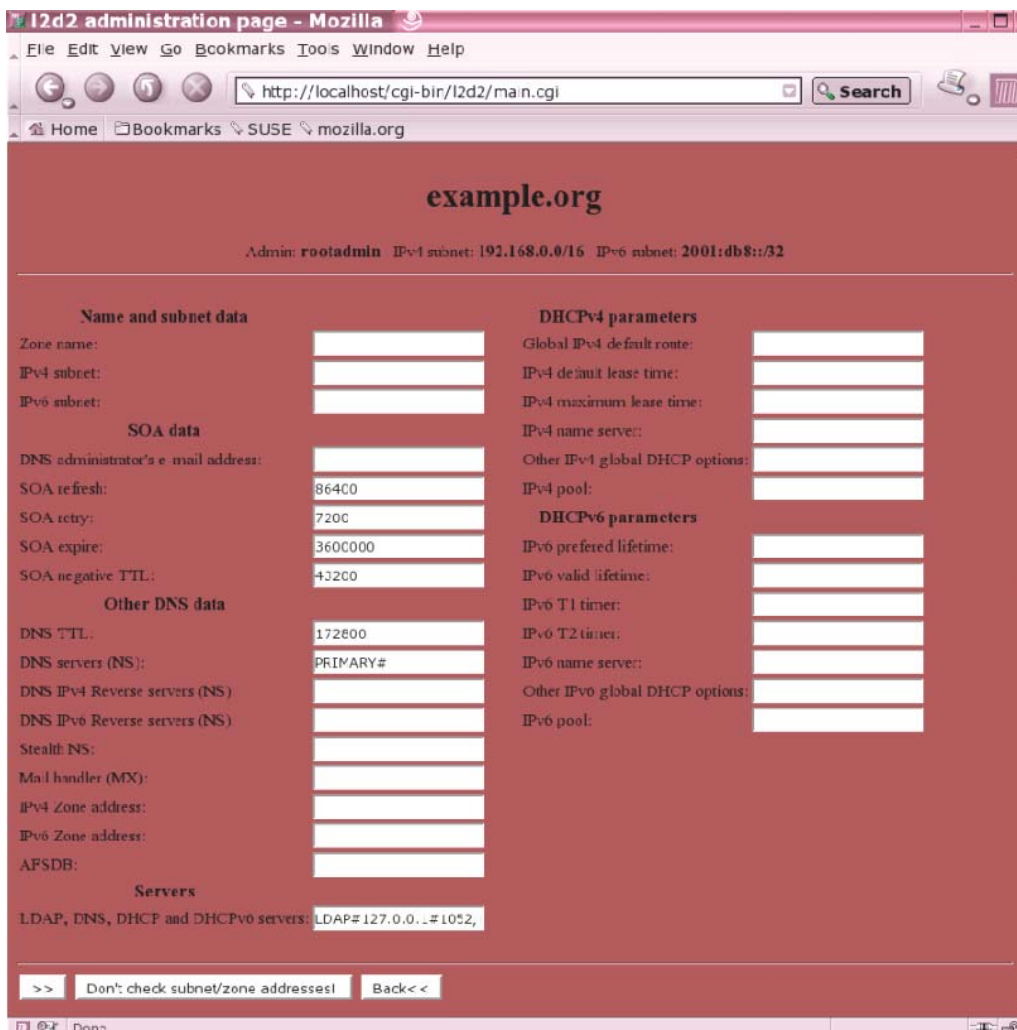
Az **“Other IPv4 global DHCP options”** mezőbe - ha kitöltjük - a teljes paramétert (több paraméter esetén azokat egymástól pontosvesszővel elválasztva), szükség esetén idézőjelek (**“”**) között kell beírni.

Az **IPv6 DHCP** paraméterek megadása is opcionális, ha üresen hagyjuk, akkor a subnet-ben lévő összes hoszt számára az interface konfigurálásánál (*/etc/dibbler/server.conf* file) megadott **globális**, vagy a **zónánál** beállított **IPv6 DHCP időértékek** lesznek **érvényesek**.

### 3.4 Új zóna létrehozása

Új zónát értelemszerűen a főmenü **“Create a new subzone”** menüpont kiválasztásával hozhatunk létre ott, ahol erre lehetőségünk van. Ha éppen egy **subnet** van az alkalmazás fókuszában, akkor ez a **menüpont hiányzik**: alhálózat menedzselésénél **csak további alhálózatokat** hozhatunk létre, **subzónát nem**.

A következő ábrán egy új zóna létrehozásánál használt űrlap látható:



The screenshot shows a web browser window titled "I2d2 administration page - Mozilla" with the URL "http://localhost/cgi-bin/i2d2/main.cgi". The page header displays "example.org" and "Admin: rootadmin IPv4 subnet: 192.168.0.0/16 IPv6 subnet: 2001:db8::/32". The main form is organized into several sections:

- Name and subnet data:** Includes fields for Zone name, IPv4 subnet, and IPv6 subnet.
- SOA data:** Includes fields for DNS administrator's e-mail address, SOA refresh (86400), SOA retry (7200), SOA expire (3600000), and SOA negative TTL (43200).
- Other DNS data:** Includes fields for DNS TTL (172800), DNS servers (NS) (PRIMARY#), DNS IPv4 Reverse servers (NS), DNS IPv6 Reverse servers (NS), Stealth NS, Mail handler (MX), IPv4 Zone address, IPv6 Zone address, and AFSDB.
- Servers:** Includes a field for LDAP, DNS, DHCP and DHCPv6 servers (LDAP#127.0.0.1#1052).
- DHCPv4 parameters:** Includes fields for Global IPv4 default route, IPv4 default lease time, IPv4 maximum lease time, IPv4 name server, and Other IPv4 global DHCP options.
- DHCPv6 parameters:** Includes fields for IPv6 preferred lifetime, IPv6 valid lifetime, IPv6 T1 timer, IPv6 T2 timer, IPv6 name server, and Other IPv6 global DHCP options.

At the bottom of the form, there are navigation buttons: ">> Don't check subnet/zone addresses! Back <<".

9. ábra

A **“Zone name”** megadása kötelező! Az **IP címek** formája: **hálózat/maszk**, ill. **IPv6 globál cím/prefix-hossz**. Az **“IPv4 subnet”** és az **“IPv6 subnet”** meglétét, ill. helyességét (megfelel-e az éppen menedzselt zóna IPv4 és/vagy IPv6 címtartományának) az alkalmazás ellenőrzi, hiba esetén figyelmeztető üzenetet küld, de - a formai hiba kivételével - a **“Don't check subnet addresses”** kijelölésével elfogadtathatjuk a beírt címeket, vagy az üresen hagyott mezőt (mezőket). Kellő odafigyeléssel és körültekintően használjuk az **IPv4** és/vagy az **IPv6 címek ellenőrzésének a letiltását**. Kötelező megadni minden olyan subzónánál, amelynél szükséges a reverse zóna/cím hirdetése.

Új **hoszt/subnet felvitelénél** az alkalmazás ellenőrzi majd azt, hogy a **hoszt IP címe**, vagy a **subnet** része-e az **itt megadott IP cím-tartománynak** (tartományoknak).

Új zóna létrehozásánál **kötelező** kitölteni a **SOA rekord generálásához szükséges összes mezőt** a **“DNS Administrator's e-mail address”** -tól a **“DNS servers (NS)”** mezőig.

A **“DNS IPv4 Reverse servers (NS)”** mezőt csak akkor kell kitölteni, ha a zóna számára **nem** a **“DNS servers (NS)”** mezőben felsorolt NS-ek nyújtanak **IPv4 reverse name server** szolgáltatást.

A **“DNS IPv6 Reverse servers (NS)”** mezőt csak akkor kell kitölteni, ha a zóna számára **nem** a **“DNS servers (NS)”** mezőben felsorolt NS-ek nyújtanak **IPv6 reverse name server** szolgáltatást.

A **name szerverek felsorolásánál** (reverse NS-eknél is) **PRIMARY#** vagy **P#** jelzéssel kell ellátni a **zóna primary name server-ét**, a többit - ha van - vesszővel elválasztva kell egymás után begépelni a következő formában:

**P#<NS szerver>#<IP cím>,<NS szerver>#<IP cím>**

A name szerverek IP címét csak akkor szükséges megadni, ha az máshonnan nem oldható fel. Az MX rekordhoz (3.2 pont) hasonlóan az **NS -nél** is a **teljes domain nevet kell megadni** pont karakter nélkül, a DNS táblák generálásánál az alkalmazás automatikusan beírja azt.

Látható, hogy **hiányzik** a SOA rekord **serial number** adata, ezt az alkalmazás a DNS táblák generálásánál **automatikusan beállítja** a napi dátumból: **yymmdd<napon belüli sorszám>**. A többi SOA mező előre definiált értékei:

|                   |         |            |
|-------------------|---------|------------|
| SOA refresh:      | 86400   | - 24 óra   |
| SOA retry:        | 7200    | - 2 óra    |
| SOA expire:       | 3600000 | - 1000 óra |
| SOA negative TTL: | 43200   | - 12 óra   |
| DNS TTL:          | 172800  | - 48 óra   |

Az **„IPv4 Zone address”** és az **„IPv6 Zone address”** paraméterekben megadható a zóna (domain) IPv4 és/vagy IPv6 címe, amely lehetővé teszi a domain-címzést (pl. web elérésnél).

Az **“AFSDB”** (Andrew File System Database) erőforrásrekord megadásának **formátuma**: **ttl#altípus#kiszolgáló**

A **“Global IPv4 default route”** -tól **“Other IPv4 global DHCP options”** -ig mezők kitöltésével beállíthatjuk azokat az **IPv4 DHCP paraméterértékeket**, amelyek **érvényesek lesznek a zóna összes hoszt-jára és alhálózatára** addig, amíg az adott helyen (hoszt vagy subnet szerkesztésre megnyitott űrlapon) felül nem írjuk valamelyik értéket. **Az itt megadott DHCP paraméterértékek felülírják a dhcp konfigurációs file-ban beállított globális értékeket!**

Az **“Other IPv4 global DHCP options”** mezőbe - ha kitöltjük - a teljes paramétert (több paraméter esetén azokat egymástól pontosvesszővel elválasztva), szükség esetén idézőjelek ("" ) között kell beírni.

Az **„IPv4 pool”** paraméterben megadhatjuk azt az **IPv4-cím tartományt/tartományokat**, amelyekből az **ismeretlen gépek** a szervertől megkaphatják a **hálózati beállításait**. A megadás formája: **<kezdő IP cím>-<utolsó IP cím>** (több tartományt egymástól vesszővel kell elválasztani).

Az **IPv6 DHCP** paraméterek megadása is opcionális, ha üresen hagyjuk, akkor a hoszt számára az interface konfigurálásánál (*/etc/dibbler/server.conf* file) megadott **globális**, vagy a **subnet**-nél beállított **IPv6 DHCP időértékek** lesznek **érvényesek**.

A Dibbler szerver jelenlegi változatában az **“IPv6 name server”** mezőben megadott domain name szerver is globális változóként értendő, vagyis interface-nként csak egy beállítás lesz érvényes! **Több zóna/subnet esetén külön-külön globális IPv6 DHCP** változókat a **Dibbler jelenlegi változatában nem lehet megadni** (mindig felülíródik az utoljára megadott értékkel).

Az **„IPv6 pool”** paraméterben megadhatjuk azt az **IPv6-cím tartományt/tartományokat**, amelyekből az **ismeretlen gépek** a szervertől megkaphatják a **hálózati beállításait**. A megadás formája: <kezdő IPv6 cím>-<utolsó IPv6 cím> (több tartományt egymástól vesszővel kell elválasztani).

Az **“LDAP, DNS, DHCP and DHCPv6 servers”** mezőben **kell megadni** azt, hogy hol van az éppen létrehozni kívánt **zóna LDAP adatbázisa** és ott **melyik porton** vár az *inetd* arra, hogy **elindítsa** az *ldapAgent* daemont, melyik gép a **zóna domain name szervere** és ott **melyik porton** vár az *inetd* arra, hogy elindítsa a *dnsAgent* daemont, ill. melyik gép a **zóna DHCP szervere** és ott **melyik porton** vár az *inetd* arra, hogy elindítsa a *dhcpAgent* daemont.

Az **alapértelmezett értékek a minta-konfigurációs file-ban**(*/etc/inetd.conf*):

**szerverek** - 127.0.0.1  
**LDAP port** - 1052  
**DNS port** - 1053  
**DHCP port** - 1054  
**DHCPv6 port** - 1055

A már ismert **jobbra mutató kettős nyíl kijelölése** után - ha hibátlanul töltöttük ki az űrlapot -, akkor az **új zóna-bejegyzés bekerül** az (a megadott gépen lévő) **LDAP adatbázisba**.

**Adminisztrátort** rendelhetünk az újonnan létrehozott **zónához** (3.5 pont), és/vagy megnyithatjuk szerkesztésre, a megnyíló űrlapon látható **“Change to”** gombbal átválthatunk az új zóna menedzselésére.

### 3.4.1 Új zóna feltöltése DNS zone transzferből

Az **alkalmazás** tartalmaz egy **parancssorból indítható**, Ruby nyelven írt segédprogramot, amellyel egy **már definiált üres zónát** (3.4 pont) egy DNS zóna transzfer eredményéből **feltölthetünk**. Az */usr/local/sbin/dns2ldap.rb* script a

```
'dig @<server> <domain> axfr'
```

outputjából készíti el, és tölti fel az adott zóna LDAP bejegyzéseit.

A **program paramétereit**:

**-S** <dnsServer> a DNS szerver neve, ahonnan a zónát fel akarjuk tölteni  
**-d** <domain> a feltöltendő zóna domain neve (pl.: *"teszt.com"*)  
**-r** <domain> a reverse zóna domain neve (pl.: *"162.198.in-addr.arpa"*) az esetleges "idegen" domain-hez tartozó hosztok feltöltése  
**-h** <ldapHost> az LDAP szerver futtató gép neve  
**-p** <ldapPort> az LDAP szerver standard portja (alapértelmezés: 389)  
**-b** <ldapBase> az LDAP fa gyökere (alapértelmezés: *cn=suffix*)

- n <namingSuffix> a rögzített suffix (top-level zóna) a domain-ben (pl.: *com* )
- D <adminDN> az adminisztrátor LDAP DN-je  
(alapértelmezés: "cn=Administrator, cn=suffix", ez a top-level inicializálásánál megadott **LDAP bind user**)
- w <password> az adminisztrátor jelszava

A **-r** paraméterben - egymástól vesszővel elválasztva - több revese zóna (IPv4 és IPv6) is megadható. Ha a program több azonos IP című "idegen" hosztot talál, akkor az LDAP adatbázisba csak egy hoszt entry keletkezik, a többi CNAME bejegyzés lesz.

Zónafeltöltést az a **regisztrált adminisztrátor** is végezhet, akinek **írás joga** van az **adott zónára!** Ha pl: az **ujzona.example.org** zóna adatait az **example.org** zónában definiált **adminka** felhasználó töltené fel, mondjuk az **ns2.example.org** DNS szerver lekérdezésével, akkor a program indítása a következő lenne:

```
yourhost'l2d2:~#/usr/lib/cgi-bin/l2d2/dns2ldap.rb -S "ns2.example.org" \
-d "ujzona.example.org" -h localhost -n org \
-D "uid=adminka,L2D2ZoneName=example,L2D2NamingSuffix=org,cn=suffix"
```

A **program paramétereit az /etc/l2d2/config.txt konfigurációs file-ban is be lehet állítani**, ebben az esetben az indítás:

```
yourhost'l2d2:~#/usr/lib/cgi-bin/l2d2/dns2ldap.rb
```

A script **csak üres** zónát tölt fel, ha a zóna nem üres, akkor a program hibajelzést ad. A program a DNS zónában esetlegesen található **subnet-ek bejegyzéseit is létrehozza** az LDAP fában, de csak a legszükségesebbet: az **L2D2SubnetName** bejegyzést. Természetesen a **subnet-be** tartozó **hoszt bejegyzések bekerülnek az adatbázisba**. A feltöltés után az alkalmazásból az **új subnet-et** (ha volt) meg kell nyitni szerkesztésre, és az űrlapon a **többi szükséges adatot is be kell írni** (pl.: IPv4 subnet, ...stb.).

Az **"idegen" domain-hez tartozó hosztok** is menedzselhetők az alkalmazással, a DNS táblák generálásánál **csak a reverse táblába** kerülnek be!

### 3.4.2 DNS zóna delegálása a zóna menedzselése nélkül

Az alkalmazás lehetőséget ad arra, hogy egy **DNS zónát, a zóna kezelése nélkül delegálhassunk**, vagyis az adott zóna számára **IN NS**, **IN A** és **IN PTR** rekordok kerüljenek az **éppen menedzselte zóna DNS forward** és **reverse** tábláiba.

A delegálandó zónát is a **"Create a new subzone"** menü pont kiválasztásával lehet definiálni. A megjelenő űrlapon (9. ábra) a **"Zone name"**, az **"IPv4 subnet"** és/vagy az **"IPv6 subnet"**, és a **"DNS servers (NS)"** mezők kitöltése kötelező! A subnet-ek fomája itt is: hálózat/maszk, ill. IPv6 globál cím/prefix-hossz. A zónához tartozó **összes olyan hálózati címet meg kell adni**, amelyet a **primary szerver külön zóna-file-ban** (saját SOA rekord) tárol. Alapértelmezésben az egyik hálózati címet kötelező megadni, de ha nincs szükség reverse feloldásra, akkor elhagyható: a hibaüzenet után (a formai hiba kivételével) a képernyő alján látható **"Don't check IP subnet addresses>>"** gomb kijelölésével hiányosan, vagy tudatosan nem a tartományban megengedett címet használva felvihetjük a zónát az adatbázisba.

Új delegált zóna létrehozásánál az űrlapon látható többi mező - előre beállított - értéke nem kerül be az adatbázisba, nem kell foglalkozni vele.

A name szerverek felsorolásánál **D#** jelzéssel kell ellátni a zóna **primary name szerver-ét**, a

többit - ha van - vesszővel elválasztva egymás után lehet begépelni a következő formában:

D#<NS szerver>#<IP cím>,<NS szerver>#<IP cím>

A “DNS IPv4 reverse servers (NS)” és a “DNS IPv6 reverse servers (NS)” mezőket csak akkor kell kitölteni, ha a *reverse* feloldást **nem** a “DNS servers (NS)” mezőben felsorolt NS-ek szolgáltatják.

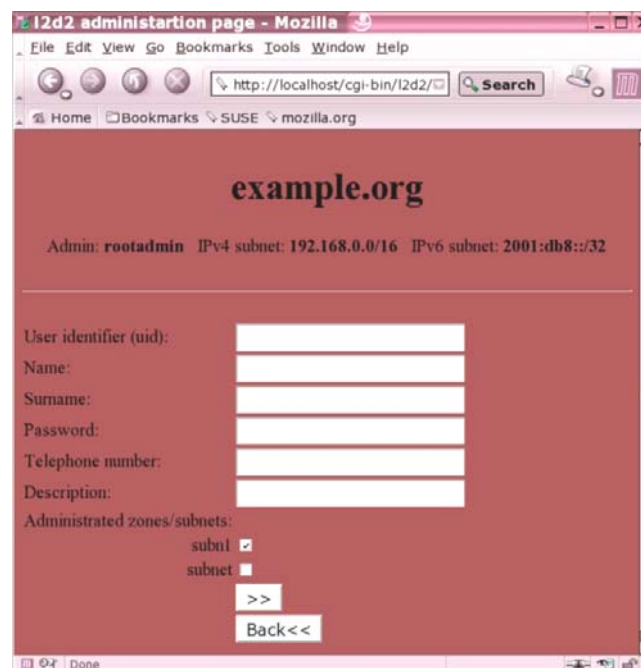
A name szerverek IP címét csak akkor szükséges megadni, ha az máshonnan nem oldható fel. A name szerverek **teljes domain nevét kell itt is begépelni**, a pont karakter nélkül, a DNS táblák generálásánál az alkalmazás automatikusan beírja azt.

Az így felvitt **zónát** csak az **őt létrehozó adminisztrátor** módosíthatja (name szerver változások, hálózati címek). A zóna szerkesztésekor az űrlapról értelemszerűen hiányzik a “Change to” gomb.

### 3.5 Új adminisztrátorok, delegált zónák

Új adminisztrátort a “Create a new admin” menü pont kiválasztásával lehet definiálni. Az új adminisztrátor **jogosultságot kap** arra, hogy **módosításokat hajthasson végre a számára delegált zóna(ák)/alhálózat(ok) LDAP fájában**.

A következő ábrán egy új adminisztrátort definiáló űrlapot láthatunk:



10. ábra

A példa szerinti *example.org* zónában létrehoztunk egy *subnl* és egy *subnet* alhálózatot és szeretnénk, ha pl. a *subnl.example.org* alhálózatot mostantól nem nekünk kellene karban tartanunk: definiálunk egy adminisztrátort az *example.org* zónában, amelynek jelszavát egy másik emberre bízuk. Ehhez nem kell mást tennünk, mint a fenti űrlapon az **új adminisztrátor** adatait begépelni, és a *subnl* mellett látható kis **négyzetet megjelölni**.

Ha az **adminisztrátort** **előbb helyeztük el az LDAP adatbázisban**, mint a **delegálandó zónát** vagy **subnet-et**, akkor ez értelemszerűen még **nem szerepelhet** az adminisztrátor űrlapján. Ebben az esetben **meg kell nyitnunk módosításra az adminisztrátort**, a módosító űrlapon már megjelenik az subzóna/subnet neve, mellette a kijelölhető négyzettel.

**Új adminisztrátor** létrehozása után az **alkalmazás automatikusan újraindítja az LDAP szervert**, **újragerálódik az LDAP jogosultsági lista**. A felhasználó beléphet a rendszerbe, írhatja és tovább bonthatja a számára delegált zónákat/álhálózatokat, ill. definiálhat újabb felhasználókat.

#### 4. Szerver-konfigurációk, szerverek újraindítása

A **DNS**, az **LDAP** és a **DHCP** szerverek új konfigurációinak elkészítése, és az adott szerver újraindítása az alkalmazás főmenüjéből, a **“Server update”** menü pont kiválasztásával kezdeményezhető.

A kívánt szerver kiválasztása után (a megfelelő gép megfelelő portján) az **inetd** daemon elindítja a választás szerinti **agent** programot, amely beolvassa az LDAP adatbázisból a szükséges adatokat, **újragerálja a konfigurációs file-t** (file-okat), majd **újraindítja a szervert**. A **futtatni kívánt agent paramétereit** az alkalmazás indítása előtt az **/etc/l2d2/config.txt** konfigurációs file-ban kell beállítani.

**Új zóna** definiálásánál (3.4 pont) lehet beállítani azt, hogy az **adott zóna számára** melyik gép az **LDAP|DNS|DHCP|DHCPv6 szerver**, és azt is, hogy a megfelelő **agent** program milyen **porton indul el**.

A minta szerinti **portszámok**:  
1052 - ldapAgent  
1053 - dnsAgent  
1054 - dhcpAgent  
1055 -dhcpv6Agent

A **szerverek újraindítási információi** az **/etc/l2d2/config.txt** file-ban megadott directory-ban, a megfelelő **.log file**-ban láthatóak.

#### 4.1 LDAP szerver

Az **“LDAP Database Service - admin permissions”** kiválasztásakor az **ldapAgent** program elkészíti az **éppen menedzselt zóna** vagy **subnet LDAP jogosultsági listáját** - ismert nevén az LDAP ACL-eket, majd **újraindítja a szervert**, hogy a módosítások életbe lépjenek.

Az **L2D2 alkalmazásban a jogosultsági lista** nem más, mint az egymásba ágyazott **access file**-ok sorozata, az **/etc/ldap/l2d2/** directory-ban. Minden zónához és subnet-hez tartozik egy access file, amely nulla-hosszúságú addig, amíg **adminisztrátort nem definiálnak** benne. Az alkalmazás **automatikusan frissíti a jogosultsági listát**:

- új adminisztrátor definiálásánál
- adminisztrátor törlése és módosítása után
- subzóna/subnet törlése után

Az access file-ok **neveit** az alkalmazás a **menedzselt zóna/subnet domain nevéből generálja**, pl. a *subn1.example.org* domain ACL listáját a *subn1.example.org.access* file tartalmazza.

Az **ldapAgent** paramétereit az */etc/l2d2/config.txt* konfigurációs file-ban kell beállítani.

Az LDAP **jogosultsági lista újragenerálását** és a szerver újraindítását a **trigger.rb** programmal **parancssorból is elvégezhetjük**:

```
yourhost'l2d2:~# /usr/local/sbin/trigger.rb --ldap --port=1052 --root "L2D2NamingSuffix=org,cn=suffix"
```

```
Creating socket...OK
```

```
Sending update type [ldap]...OK
```

```
Sending ldap distinguished nam of the root entry...OK
```

```
Closing socket...OK
```

```
yourhost'l2d2:~# _
```

A fenti a példa szerint a **yourhost** (localhost) gépen a teljes *.org* domain ACL listáját generáltatjuk újra.

A program paramétereit:

**--help** paraméterek kiírása

**--host** az LDAP szervert futtató gép neve, vagy IP címe

**--port** **port száma**, amelyen az **inetd daemon** várakozik az **agent** indítására

**--ldap** LDAP szerver triggerelése

**--root** LDAP naming entry (LDAP DN)

Az LDAP **jogosultsági lista újragenerálása** megtehető az **LDAP szervert futtató** gépen az **ldapAgent** elindításával is:

```
yourhost'l2d2:~# /usr/local/sbin/ldapAgent.rb
```

```
yourhost'l2d2:~# update: ldap
```

```
yourhost'l2d2:~# dn: L2D2ZoneName=example,L2D2NamingSuffix=org,cn=suffix
```

```
yourhost'l2d2:~# ^D
```

```
yourhost'l2d2:~# _
```

A fenti példával is az *example.org* domain jogosultsági listáját generáltuk újra.

## 4.2 DNS szerver

A “Domain Name Service” kiválasztásakor a **dnsAgent** program elkészíti az **éppen menedzselt zóna** (az alá tartozó subnet-ekkel együtt) DNS **forward** és **reverse** (IPv4 és IPv6) tábláit az */etc/bind/l2d2/* directory-ba, és **újraindítja a szervert**.

A **dnsAgent** paramétereit (pl. az LDAP szerverre vonatkozó információk, ...stb.) az */etc/l2d2/config.txt* konfigurációs file-ban kell beállítani.

A **DNS táblák neveit** az alkalmazás a **menedzselt zóna domain nevéből generálja**, pl. az *example.org* domainhez a következő file-ok készülnek:

**example.org.Forward**

**example.org.Reverse**

**example.org.IPv6-Reverse-int**

**example.org.IPv6-Reverse-arpa**

Ha a zónához **több IPv4-es subnet** tartozik, akkor **egymástól független reverse** file-ok generálódnak.

Egy **alhálózat** (subnet) **főmenüjéből** indított szerver update-kor az alkalmazás a **subnet fölötti első zóna-bejegyzésből** olvassa ki a **DNS szerver gép nevét és a port-számot**, majd a **teljes zóna** (benne a subnet-ek adataival) **tábláit generálja újra**.

A **DNS táblák elkészítését** és a szerver újraindítását a fent ismertetett **trigger.rb** programmal **parancssorból is elvégezhethetjük** (a **--ldap** helyett ebben az esetben a **--dns** paramétert kell megadni), ill. megtehető a **DNS szerver futtató gépen** a következők szerint:

```
yourhost'l2d2:~# /usr/local/sbin/dnsAgent.rb
yourhost'l2d2:~# update: dns
yourhost'l2d2:~# dn: L2D2ZoneName=example,2D2NamingSuffix=org,cn=suffix
yourhost'l2d2:~# ^D
yourhost'l2d2:~# _
```

Parancssorból kezdeményezett szerver-újraindításnál **csak zónanév** adható meg, **subnet-név nem!**

Természetesen **gondoskodni kell arról**, hogy az **/etc/named.conf** mindig az alkalmazással menedzselte **összes zóna adatait tartalmazza**.

### 4.3 DHCP szerver

A **“Dynamic Host Configuration Service”** kiválasztásakor a **dhcpAgent** program elkészíti az **éppen menedzselte zóna** (az alá tartozó subnet-ekkel együtt) **IPv4 DHCP konfigurációit** az **/etc/dhcp3/l2d2/<zóna-név>.dconf** file-ba, ezt beilleszti - ha szükséges – a DHCP szerver konfigurációs file-ba (**/etc/dhcp3/dhcpd.conf**) a következők szerint:

- ha megtalálható a **dhcpd.conf** file-ban a  
**# generated by dhcpAgent.rb**  
comment sor, akkor az ezt követő utolsó **include** sor után íródik be az új bejegyzés, vagyis a konfigurációs file még tartalmazhat egyéb sorokat
- ha a fenti comment sor nincs a **dhcpd.conf** file-ban, akkor az új bejegyzés a file végére kerül

majd **újraindítja a szervert**. A **restart** akkor is működik, ha a **DHCP szervert** még nem **indítottuk el**, de a teszteléshez szükséges **virtuális interface-nek már léteznie kell** (2.2 pont).

A **dhcpAgent paramétereit** (pl. az LDAP szerverre vonatkozó információk, ...stb.) az **/etc/l2d2/config.txt** konfigurációs file-ban kell (és lehet) **beállítani**.

A **DHCP szerver** az Ethernet **MAC címek alapján fix IP címet ad** a gépeknek akkor, ha megadtuk az Ethernet címet. Ha ez nem ismert, akkor a szerver a **zóna** konfigurálásánál beállított **pool**-ból oszt címet abban az esetben, ha ez adott.

Az **IPv4 DHCP szerver minta-konfigurációs file-ja** a teszt-adatbázis bejegyzései szerint:

```
#
```

```

dhcpd.conf file
#
Global parameters:
ddns-update-style interim;
default-lease-time 6000;
max-lease-time 7200;
authoritative;
log-facility local7;
End of global parameters
#
Include the l2d2 zone entry's dhcp config file
generated by dhcpAgent.rb.
include "/etc/dhcp3/l2d2/example.org.dconf";
#

```

A globális paraméterek és az *include* sor után bármilyen más bejegyzés is szerepelhet, a program változtatás nélkül átmásolja azokat az új konfigurációs file-ba.

**Az *example.org* zóna dhcp konfigurációja** ( */etc/l2d2/samples/dhcp3/example.org.dconf* file):

```

#
DHCP configuration file for l2d2 zone
Generated from LDAP entry "L2D2ZoneName=example,L2D2NamingSuffix=org,cn=suffix"
@ Wed Jul 6 13:49:15 2011 by dhcpAgent.rb
#
EXAMPLE.ORG
subnet 192.168.0.0 netmask 255.255.0.0 {
 option broadcast-address 192.168.255.255;
 option domain-name "example.org";
 default-lease-time 6000;
 max-lease-time 7200;
 option routers 192.168.0.254;
 option domain-name-servers ns2.example.org;
unknown clients
 pool {
 range 192.168.150.1 192.168.150.10;
 range 192.168.200.1 192.168.200.225;
 allow unknown-clients;
 }
}
host example1 {
 hardware ethernet 00:07:e9:6c:44:c9;
 fixed-address 192.168.0.1;
}
host thost1 {
 hardware ethernet 08:33:33:23:23:00;
 fixed-address 192.168.0.9;
}
SUBN1.EXAMPLE.ORG
group {
 option subnet-mask 255.255.255.0;
 option broadcast-address 192.168.100.255;
 option domain-name "subn1.example.org";
 default-lease-time 2700;
 max-lease-time 3600;
 option routers 192.168.100.254;
}
host h1 {
 hardware ethernet 00:10:5a:e1:80:36;
 fixed-address 192.168.100.1;
 default-lease-time 2000;
 max-lease-time 2700;
}

```

```

option routers 192.168.100.254;
}
host h2 {
hardware ethernet 08:22:22:22:22:22;
fixed-address 192.168.100.2;
}

```

Egy **alhálózat** (subnet) **főmenüjéből** indított szerver update-kor az alkalmazás a **subnet fölötti első zóna-bejegyzésből** olvassa ki a **DHCP szerver gép nevét** és az **indítási port-számot**, majd a **teljes zóna** (benne a subnet-ek adataival) **dhcp konfigurációját generálja újra**. Értelemszerűen a konfigurációs file-ban csak azok subnet-ek szerepelnek, amelyekben van MAC címmel megadott hoszt.

Az **IPv4 DHCP konfigurációk elkészítését** és a **szerver újraindítását** a fent ismertetett **trigger.rb** programmal **parancssorból is elvégezhetjük** (a **--ldap** helyett ebben az esetben a **--dhcp** paramétert kell megadni), ill. megtehető a **DHCP szerver futtató gépen** a **dhcpAgent** elindításával is:

```

yourhost'l2d2:~# /usr/local/sbin/dhcpAgent.rb
yourhost'l2d2:~# update: dhcp
yourhost'l2d2:~# dn: L2D2ZoneName=example,L2D2NamingSuffix=org,cn=suffix
yourhost'l2d2:~# ^D
yourhost'l2d2:~# _

```

Parancssorból kezdeményezett szerver-újraindításnál **csak zónanév** adható meg, **subnet-név nem!**

## 4.4 DHCPv6 szerver

A **“Dynamic Host Configuration Service for IPv6”** kiválasztásakor a **dhcpv6Agent** program elkészíti az **éppen menedzselte zóna** (az alá tartozó subnet-ekkel együtt) **IPv6 DHCP konfigurációit** az **/etc/dibbler/l2d2/<zóna-név>.v6dconf** file-ba. A fejlesztő környezetben a **Dibbler szerver 0.4.1 változata** futott, mint **DHCPv6 szerver**. A **dhcpv6Agent** ennek megfelelő konfigurációs file-t generál. A **dibbler** szerver **nem támogat több konfigurációs file-t**, ezért az agent a teljes újonnan generált konfigurációt bemásolja az **/etc/dibbler/server.conf** file-ba a következők szerint megjelölt helyre:

- a **server.conf** file-ban - az interface-t leíró utasítás után – kell, hogy legyen egy comment sor, amelyben megtalálható a

```
generated by dhcpv6Agent.rb
```

szöveg. Ezt követően kerül a file-ba a kiválasztott zóna új konfigurációja (#END záró comment sorral, amelyet nem szabad kiszedni), majd az eredeti file többi bejegyzése változtatás nélkül.

Az új konfiguráció elkészítése után az agent **újraindítja a szervert**. A Dibbler szerver jelenlegi változatában a **restart** csak akkor működik, ha a **DHCPv6 daemon-t már elindítottuk**.

A **DHCPv6 szerver** az **Ethernet MAC címből generált link-local címmel azonosított gépeknek rögzített IPv6 címet ad** akkor, ha megadtuk az Ethernet címet. Ha ez nem ismert, akkor a szerver a **zóna** konfigurálásánál beállított **pool**-ból oszt címet, ha ezt beállítottuk.

## A **teszt-adatbázis** mintabejegyzései alapján a **DHCPv6** szerver konfigurációs file-ja:

```
#
Logging level range: 1(Emergency)-8(Debug)
#
log-level 7
Don't log full date
log-mode short

#log-mode full
stateless

iface "eth0" {

clients should renew every half an hour
T1 1800

In case of troubles, after 45 minutes, ask any server
T2 2700

Addresses should be preferred for an hour
preferred-lifetime 3600

and should be valid for 2 hours
valid-lifetime 7200

include the l2d2 zone entry's, generated by dhcpv6Agent.rb
#
#EXAMPLE.ORG
Generated from LDAP entry "L2D2ZoneName=example,L2D2NamingSuffix=org,cn=suffix"
@ Mon Jul 11 09:36:40 2011 by dhcpv6Agent.rb
#
 option dns-server 2001:db8::50
 option lifetime 7200
 class {
host: example1
 accept-only FE80::207:E9FF:FE6C4:4C9
 pool 2001:db8::2
 }

#SUBN1.EXAMPLE.ORG
 class {
host: h2
 accept-only FE80::A22:22FF:FE22:2222
 pool 2001:db8::3
 preferred-lifetime 3600
 valid-lifetime 7200
 }
unknown clients
 class {
 share 100
 valid-lifetime 7200
 pool 2001:db8::150-2001:db8::200
 }
 class {
 share 200
 valid-lifetime 7200
 pool 2001:db8::205-2001:db8::210
 }
#END
}
```

Az alkalmazással **generált IPv6 DHCP konfigurációt** Linux Dibbler 0.4.1 klienssel, és egy Windows XP SP1 gépen indított Dibbler klienssel (Dibbler client 0.4.1) is teszteltük, amelynek **konfigurációja, indítása**, majd az **aktív IPv6 interface** lekérdezésének eredménye a következőkben látható.

### Konfigurációs file:

```
Dibbler-client will autodetect all up, running, IPv6-supporting,
physical interfaces and will try
to obtain one IPv6 address on each of them.
To manually specify, what parameter should be obtained, uncomment
appropriate sections below.
To get full list of supported options, see Dibbler User's Guide.
log-mode short
7 = omit debug messages
log-level 7
#stateless
iface "Helyi kapcsolat" {
 option dns-server
 ia
}
```

### A Dibbler kliens indítási információi:

```
| Dibbler - a portable DHCPv6, version 0.4.1 (CLIENT, WinXP/2003 port)
| Authors : Tomasz Mrugalski<thomson(at)klub.com.pl>,Marek Senderski<msend(at)o2.pl>
| Licence : GNU GPL v2 or later. Developed at Gdansk University of Technology.
| Homepage: http://klub.com.pl/dhcpv6/
```

```
Notice Windows XP detected (majorVersion=5, minorVersion=1), so this is proper port.
Critical | Dibbler - a portable DHCPv6, version 0.4.1(CLIENT, WinXP/2003 port)
Notice Detected iface Helyi kapcsolat/4, MAC=00:07:e9:6c:44:c9.
Notice Detected iface 6to4 Tunneling Pseudo-Interface/3, MAC=94:06:00:89.
Notice Detected iface Automatic Tunneling Pseudo-Interface/2, MAC=94:06:00:89.
Notice Detected iface Loopback Pseudo-Interface/1, MAC=.
Notice Parsing .\client.conf config file...
Info Interface Helyi kapcsolat/4 configuration has been loaded.
Info Bind reuse enabled.
Notice Creating socket (addr=fe80::207:e9ff:fe6c:44c9) on the Helyi kapcsolat/4 interface.
Info Socket bound to fe80::207:e9ff:fe6c:44c9/port=546
Info Creating SOLICIT message on Helyi kapcsolat interface.
Notice Sleeping for 1 second(s).
Info Processing msg (SOLICIT,transID=0x41c8,opts: 1 3 8 6)
Notice Sleeping for 1 second(s).
Notice Received ADVERTISE on Helyi kapcsolat/4,TransID=0x41c8, 6 opts: 1 3 23 42 2 7
Notice Sleeping for 1 second(s).
Info Processing msg (SOLICIT,transID=0x41c8,opts: 1 3 8 6)
Info Creating REQUEST. Backup server list contains 1 server(s).
Notice Sleeping for 1 second(s).
Info Processing msg (REQUEST,transID=0x35c8,opts: 1 3 8 6 2)
Notice Sleeping for 1 second(s).
Notice Received REPLY on Helyi kapcsolat/4,TransID=0x35c8, 5 opts: 1 3 2 23 42
Notice Address 2001:db8::2 added to Helyi kapcsolat/4 interface.
Notice Setting up DNS server 2001:db8::1 on interface Helyi kapcsolat/4.
Info Next option renewal in 7200 seconds .
.
.
```

```

.
.
.
Warning Sending SHUTDOWN packet on the Helyi kapcsolat/4 (addr=fe80::207:e9ff:fe6c:44c9).
Warning Control message received.
Notice Shutting down entire client.
Notice Creating RELEASE for 1 IA(s).
Notice 2001:db8::2 address released from Helyi kapcsolat/4 interface.
Notice DNS server 2001:db8::1 removed from the Helyi kapcsolat/4 interface.
Info Processing msg (RELEASE,transID=0x50d6,opts: 2 1 3)
Notice Sleeping for 1 second(s).
Notice Received REPLY on Helyi kapcsolat/4,TransID=0x50d6, 3 opts: 2 1 13
Notice Shutting down entire client.
Notice Sleeping for 1 second(s).
Notice Bye bye.

```

### Aktív IPv6 interface:

Aktív állapot lekérdezése...

4 kapcsolat: Helyi kapcsolat

```

Egyedi cím : 2001:db8::2
Típus : Kézi
DAD-állapot : Kívánt
Érvényes élettartam: 54m8s
Kívánt élettartam : 24m38s
Hatókör : Globális
Előtag eredete : Kézi
Utótag eredete : Kézi

```

```

Egyedi cím : fe80::207:e9ff:fe6c:44c9
Típus : Csatolás
DAD- állapot : Kívánt
Érvényes élettartm: infinte
Kívánt élettartam : infinie
Hatókör : Csatolás
Előtag eredete : Ismert
Utótag eredete : Kapcsolati rétegbeli cím
Nem található bejegyzés,.

```

Egy **alhálózat** (subnet) **főmenüjéből** indított szerver update-kor az alkalmazás a **subnet fölötti első zóna-bejegyzésből** olvassa ki a **DHCPv6 szerver gép nevét/IP címét és az indítási port-számot**, majd a **teljes zóna** (benne a subnet-ek adataival) **IPv6 DHCP konfigurációját generálja újra**. Értelmszerűen a konfigurációs file-ban csak **azok a hosztok** szerepelnek, amelyeknek **van IPv6 és Ethernet MAC címe**.

A **dhcpAgent paramétereit** (pl. az LDAP szerverre vonatkozó információk, ...stb.) az **/etc/l2d2/config.txt konfigurációs file-ban kell** (és lehet) **beállítani**.

Az **IPv6 DHCP konfigurációk elkészítését** és a szerver újraindítását a fent ismertetett **trigger.rb** programmal **parancssorból is elvégezhetjük** (a **--ldap** helyett ebben az esetben a **--dhcpv6** paramétert kell megadni), ill. megtehető a **DHCPv6 szervert futtató gépen a dhcpv6Agent** elindításával is:

```

yourhost@l2d2:~# /usr/local/sbin/dhcpv6Agent.rb
yourhost@l2d2:~# update: dhcpv6

```

```
yourhost'l2d2:~# dn: L2D2ZoneName=example,L2D2NamingSuffix=org,cn=suffix
yourhost'l2d2:~# ^D
yourhost'l2d2:~# _
```

Parancssorból kezdeményezett szerver-újraindításnál **csak zónanév** adható meg, **subnet-név nem!**