

SVEUČILIŠTE U ZAGREBU  
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA  
Zavod za telekomunikacije

SEMINARSKI RAD

# **Lightweight Directory Access Protocol**

XXXX

Zagreb, siječanj 2005.

## Sadržaj:

1. UVOD.....	2
1.1. Direktorij.....	2
2. X.500 STANDARD.....	3
3. LDAP ARHITEKTURA.....	4
3.1. LDAP modeli.....	4
3.1.1. Informacijski model.....	4
3.1.2. Model imenovanja.....	6
3.1.3. Model funkcionalnosti.....	8
3.1.4. Sigurnosni model.....	8
3.2. Upravljanje.....	9
3.3. Sigurnost.....	9
4. PRIMJENA LDAP-a.....	10
5. ZAKLJUČAK.....	12

## Literatura

# 1. UVOD

**LDAP** (Lightweight Directory Access Protocol) je standard na Internetu koji klijentu (engl. *client*) ili radnoj stanici (engl. *workstation*), preko TCP/IP mreže, omogućuje pregledavanje i uporabu adrese elektroničke pošte (engl. *e-mail*) na LDAP poslužitelju (engl. *server*). On je jednostavnija inačica X.500 protokola za pristup direktoriju u modelu za povezivanje otvorenih sustava.

Mnoštvo standarda i protokola polagano ali sigurno zamjenjuje samo jedan protokol – LDAP protokol. LDAP je naslijedio fleksibilnost i hijerarhijsku strukturu od X.500 protokola, a nadograđen (bolje rečeno pojednostavljen) je jednostavnoću kreiranja direktorija, te njegovom uporabom i održavanjem. Zahvaljujući jednostavnosti, fleksibilnosti i praktičnosti, a u isto vrijeme poštujući zadane standarde, omogućava izradu brzih i točnih informacijskih servisa.

LDAP definira način na koji korisnički program pristupa sustavskoj komponenti, te kako korisnički program izvodi operacije nad direktorijem. Iako je LDAP u početku bio zamišljen samo kao protokol za pristup direktorijima zasnovanima na X.500 standardu, danas postoje direktoriji koji su u potpunosti zasnovani na LDAP protokolu. To znači da se sve operacije nad direktorijem obavljaju korištenjem LDAP protokola. Podržava niz funkcionalnosti koje nisu bile predviđene u početku njegova razvoja, kao što su autentikacija i uvišestručavanje. Korištenjem ovog protokola kao osnove za izgradnju direktorija, smanjuju se zahtjevi na računalnu snagu korisničkih i poslužiteljskih računala.

## 1.1. Direktorij

**Direktorij** je skup otvorenih sustava koji omogućuje pohranu podataka u hijerarhijski organiziranu bazu podataka, zajedno s podacima koje baza podataka sadrži. Direktorij je namijenjen za spremanje podataka kojima se pristupa uglavnom radi čitanja (engl. *readmostly*).

Dijele se u četiri skupine:

- direktoriji mrežnih operacijskih sustava (Active Directory, Netware Directory Services)
- direktoriji ugrađeni u aplikacije (Lotus Notes AddressBook, Microsoft Exchange Directory)

- direktoriji posebne namjene (Domain Name System, DNS)
- direktoriji opće namjene – obično zasnovani na ISO X.500 (Netscape Directory Server)

## 2. X.500 STANDARD

Brzim razvojem distribuiranih sustava i telekomunikacijskih mreža krajem 80-ih godina prošloga stoljeća pojavila se potreba za standardiziranjem usluga direktorija (engl. *directory services*). Suradnjom ISO (International Organization for Standardization) i CCITT (Consultative Committee for International Telegraphy and Telephony, današnji ITU – International Telecommunication Union) razvijena je serija specifikacija za usluge direktorija koji mogu sadržavati telefonske brojeve, e-mail adrese i druge informacije o osobama te informacije o mrežnim uređajima.

Prva specifikacija takvog standarda napisana je 1988. godine. Standard je nazvan **X.500** DAP (Directory Access Protocol). Iako su ubrzo slijedile nove specifikacije tog standarda, X.500 standard nije bio dobro prihvaćen. Najveći njegov nedostatak je bio taj što mora koristiti OSI (Open Source Initiative) protokolni složaj koji je vrlo težak za implementiranje i nije toliko rasprostranjen kao npr. TCP/IP složaj. Zbog svoje složenosti X.500 DAP protokol za pristup direktoriju postavlja velike zahtjeve na računalnu snagu sustava, te je njegova upotreba ograničena na snažna računala zasnovana na UNIX operacijskom sustavu.

Pristup direktoriju ostvaruje se pomoću dviju komponenti: korisničke i sustavske. Korisnička komponenta direktorija (engl. *Directory User Agent*, DUA) je korisnička aplikacija koja pristupa direktoriju, a sustavska komponenta direktorija (engl. *Directory System Agent*, DSA) pruža pristupnu točku direktoriju. Komunikacija između korisničke i sustavske komponente odvija se slanjem zahtjeva i odgovora.

S obzirom da je većina klijentskih aplikacija za usluge direktorija radila na TCP/IP složaju, počelo se raditi na standardu koji će podržavati taj složaj; standard je nazvan LDAP. U početku je LDAP bio zamišljen samo kao *gateway* između klijentske aplikacije i X.500 poslužitelja, ali je ubrzo, zbog težine implementacije X.500 standarda, LDAP-u dodana vlastita baza podataka koja mu je omogućila da tvori samostalnu uslugu direktorija.

## 3. LDAP ARHITEKTURA

Podaci u LDAP poslužitelju organizirani su u hijerarhijsko-relacijskom formatu. Hijerarhijski je zato što svaki zapis, osim korijenskog, ima jedan "roditeljski" zapis, a relacijski jer se više zapisa može grupirati zajedno. Najviša razina hijerarhije u LDAP poslužitelju naziva se domenom. U jednom takvom poslužitelju može postojati više domena jer je LDAP dizajniran tako da pruža globalnu uslugu direktorija što ponekad nije moguće ostvariti jednom vršnom domenom. Ispod domene su grane koje predstavljaju organizacijske jedinice koje su najčešće odjeli neke organizacije. Svaki zapis koji nije domena ili organizacijska jedinica naziva se list.

### 3.1. LDAP modeli

LDAP se zasniva na četiri modela:

- informacijski model
- model imenovanja
- model funkcionalnosti
- sigurnosni model

#### 3.1.1. Informacijski model

Opisuje strukturu informacijskog stabla direktorija; izveden je iz X.500 standarda. Važni pojmovi su:

- **razred** – označava grupu objekata koji imaju zajednička svojstva. Razredi se mogu nasljeđivati i postoje tri vrste: apstraktni razredi (engl. *abstract classes*) – služe kao predlošci za strukturne razrede, strukturni razredi (engl. *structural classes*) – opisuju zapise u direktoriju, i pomoćni razredi (engl. *auxiliary classes*) – definiraju skup atributa za nasljeđivanje.
- **atributi** – jedinice podataka na temelju kojih se definiraju razredi. U shemi se definiraju zasebno od razreda, te je na taj način omogućeno korištenje iste definicije atributa u više različitih razreda.
- **sintaksa atributa** – definira koju vrstu podataka i koje vrijednosti može sadržavati pojedini atribut.

- **zapisi** – opisuju objekte iz stvarnog svijeta. Svaki zapis je pojava (engl. *instance*) jednog strukturnog razreda; to znači da sadrži vrijednost i poštuje ograničenja atributa definiranih u razredu.
- **shema** – sadrži listu razreda i atributa koji se mogu koristiti i nasljeđivati. Kako bi zapis pripadao informacijskom stablu direktorija, mora odgovarati formatu definiranom u shemi.

U tablici 1. prikazane su neke od LDAP sintaksi atributa, a u tablici 2. neki od važnijih LDAP atributa. Neki atributi imaju pseudonime (engl. *alias*) koji se mogu upotrijebiti uvijek kada se koristi puno ime atributa. Npr., *cn* se može upotrijebiti kao referenca na atribut *commonName*.

Sintaksa	Opis
bin	Binarna informacija
ces	(Case exact string) Koristi se i naziv "directory string"; slučaj je važan tijekom uspoređivanja
cis	(Case ignore string) Slučaj nije važan tijekom uspoređivanja
tel	Telefonski broj. Brojevi se promatraju kao tekst, a praznine se ignoriraju
dn	(Distinguished name)

Tablica 1. *LDAP sintakse atributa*

Atribut, Alias	Sintaksa	Opis	Primjer
commonName, cn	cis	Općenito ime zapisa	John Smith
surname, sn	cis	Prezime osobe	Smith
telephoneNumber	tel	Telefonski broj	123 – 456 – 7890
organizationalUnitName, ou	cis	Ime organizacijske jedinice	itso
owner	dn	Različito ime osobe koja posjeduje zapis	cn=John Smith o=IBM, c=US
organization, o	cis	Ime organizacije	IBM
jpegPhoto	bin	Foto. slika u JPEG formatu	Slika Johna Smitha

Tablica 2. *LDAP atributi*

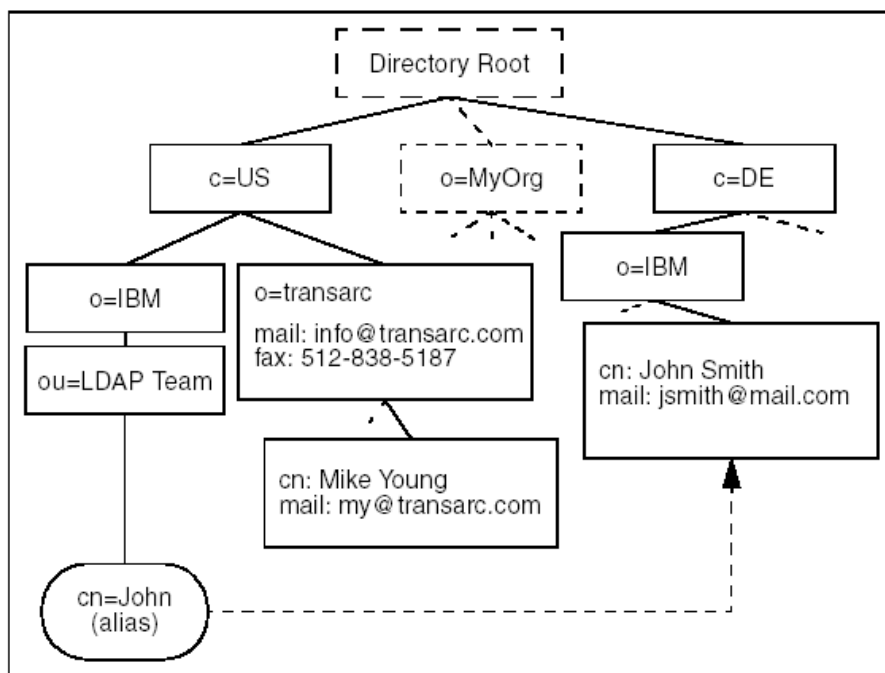
Svaki zapis direktorija ima poseban atribut koji se zove *objectClass*. Vrijednost tog atributa sastoji se od liste dvaju ili više imena shema. Te sheme definiraju tipove objekata koje zapis predstavlja. *objectClass* odlučuje koje attribute zapis mora i treba imati. Tablica 3. prikazuje dio općenite sheme (objektni razredi i pripadni atributi); u mnogim slučajevima, zapis može sadržavati više od jednog objektnog razreda.

<b>Objektni razredi</b>	<b>Opis</b>	<b>Potrebni atributi</b>
InetOrgPerson	Definira zapise za osobu	commonName (cn); surname (sn); objectClass
organizationalUnit	Definira zapise za org. jedinice	ou; objectClass
organization	Definira zapise za organizacije	o; objectClass

Tablica 3. *Objektni razredi i potrebni atributi*

### 3.1.2. Model imenovanja

Definira organizaciju i referenciranje podataka; preuzet je iz X.500 standarda. Podaci su organizirani u informacijsko stablo direktorija (engl. *directory information tree*, DIT). Za pristup čvoru informacijskog stabla kao primarni ključ koristi se apsolutno ime DN, koje se sastoji od niza relativnih imena (engl. *relative distinguished name*, RDN). RDN-ovi se sastoje od imena i vrijednosti određenog atributa koje zapis posjeduje. Korijen informacijskog stabla direktorija (engl. *root DSE*) sadrži zapis karakterističan za sustavsku komponentu direktorija (engl. *DSA specific entry* - DSE). Zapis sadrži podatke o sustavskoj komponenti direktorija kao što su: podržana verzija protokola, podržane napredne operacije, podržani sigurnosni mehanizmi, adrese alternativnih sustavskih komponenti i adresu zapisa koji sadrži shemu.



Slika 1. Primjer informacijskog stabla direktorija DIT

Slika 1. prikazuje primjer informacijskog stabla direktorija. Svaki pravokutnik predstavlja zapis direktorija. Atributi su prikazani u svakom zapisu, ali predstavljena lista atributa nije potpuna. Npr., zapis za državu DE ( $c=DE$ ) može imati atribut pod imenom *description* s vrijednošću *Germany*.

Preko posebnih *objectClass* atributa, LDAP omogućuje kontrolu koji atributi se traže i koji su dozvoljeni. Vrijednosti atributa u objektnom razredu određuju shematska pravila kojih se zapis mora pridržavati.

Vrijednost koja označava pripadnost državi nalazi se na vrhu informacijskog stabla direktorija. Ispod nje nalaze se organizacijske cjeline. Najniža razina predstavlja ljude, organizacijske jedinice, printere, dokumente ili bilo što drugo što želimo imati u bazi.

Na gornjoj slici, zapis direktorija u donjem desnom kutu ima DN  $cn=John\ Smith, o=IBM, c=DE$ . Može se primijetiti da DN čita od lista prema korijenu. Ovaj DN nastao je dodavanjem RDN-a  $cn=John\ Smith$  na DN od prethodnog zapisa  $o=IBM, c=DE$ .  $cn=John\ Smith$  je atribut u zapisu  $cn=John\ Smith, o=IBM, c=DE$ .

Aliasi dopuštaju da se struktura stabla zaobiđe. To može biti korisno ako jedan zapis pripada većem broju organizacija ili ako je korišteni DN previše kompliciran. Isto tako, aliasi se koriste i kada su zapisi premješteni unutar DIT-a, a mi želimo nastaviti s radom kao i prije. Na slici 1.,  $cn=John, ou=LDAP\ Team, o=IBM, c=US$  je alias za  $cn=John\ Smith, o=IBM, c=DE$ . Aliasi ne moraju pokazivati na listne zapise u DIT-u. Npr.,  $o=Redbook, c=US$  može biti alias za  $ou=ITSO, o=IBM, c=US$ .

### 3.1.3. Model funkcionalnosti

Definira operacije nad podacima u direktoriju. Postoji devet operacija koje su podijeljene u tri skupine:

- **autentikacija** – omogućuje korisničkom programu da dokaže svoj identitet kroz nekoliko operacija:
  - Open* – otvara vezu prema sustavskoj komponenti direktorija DSA.
  - Bind* – otvara sjednicu između korisničkog programa i DSA koja omogućuje razmjenu podataka potrebnih za autentikaciju.
  - Unbind* – prekida sjednicu između korisničkog programa i DSA.
- **pretraživanje** – obavlja se korištenjem ovih operacija:
  - Search* – služi za pretraživanje direktorija. Kriteriji za pretragu prenose se preko parametara. Mogu se proslijediti parametri koji određuju čvor u informacijskom stablu gdje pretraga počinje, područje koje se pretražuje, filter pretrage, listu atributa koji se vraćaju, te parametri koji određuju način izvođenja pretrage.
  - Compare* – vraća vrijednost istinitosti za zadanu usporedbu.
- **izmjena** – nad podacima, a koriste se sljedeće operacije:
  - Add* – stvara objekt u informacijskom stablu direktorija koji mora zadovoljavati uvjete definirane u shemi.
  - Modify* – mijenja vrijednost određenog atributa zapisa, a obuhvaća dodavanje, izmjenu i brisanje vrijednosti atributa.
  - Modify RDN* – omogućuje micanje zapisa unutar inf. stabla direktorija.
  - Delete* – omogućuje brisanje zapisa iz inf. stabla direktorija.

### 3.1.4. Sigurnosni model

Definira mogućnosti sigurnog pristupa podacima unutar informacijskog stabla direktorija. Standard definira korištenje postojećih SASL (Simple Authentication and Security Layer) mehanizama za osiguravanje pristupa podacima. Korijen informacijskog stabla direktorija *root* DSE sadrži atribut koji sadrži listu podržanih SASL mehanizama (engl. *supportedSASLMechanisms*). SASL sigurnosni mehanizmi koriste se za sigurnu autentikaciju, a po potrebi je moguće zaštititi i cjelokupnu komunikaciju između korisničkog programa i sustavske komponente direktorija.

## 3.2. Upravljanje

Tokom vremena LDAP protokol se razvijao. Prve dvije verzije imale su problema sa sigurnošću, ali to je riješeno u trećoj verziji:

- LDAP version 1 – RFC 1487
- LDAP version 2 – RFC 1777
- LDAP version 3 – RFC 2251

Klijenti vrše protokolske radnje nad poslužiteljem tako da klijent šalje zahtjev opisujući operaciju koju treba izvršiti poslužitelj. Nakon što primi zahtjev, poslužitelj je zadužen obaviti potrebnu operaciju u direktoriju. Nakon što je radnja izvršena, poslužitelj vraća natrag klijentu odgovor koji sadrži rezultate operacije ili informaciju o grešci. Cilj LDAP protokola je minimiziranje kompleksnosti klijenata koja doprinosi brzini i efikasnosti upotrebe usluge direktorija.

Kada klijent komunicira s LDAP poslužiteljem, prolazi kroz tri osnovne faze:

- uspostavlja konekciju s poslužiteljem
- obavlja određene operacije nad direktorijem
- prekida konekciju s poslužiteljem

Proces uspostave i raskida konekcije obavlja se putem standardnih TCP/IP mehanizama. LDAP definira nekoliko operacija koje se mogu izvršavati nad poslužiteljem:

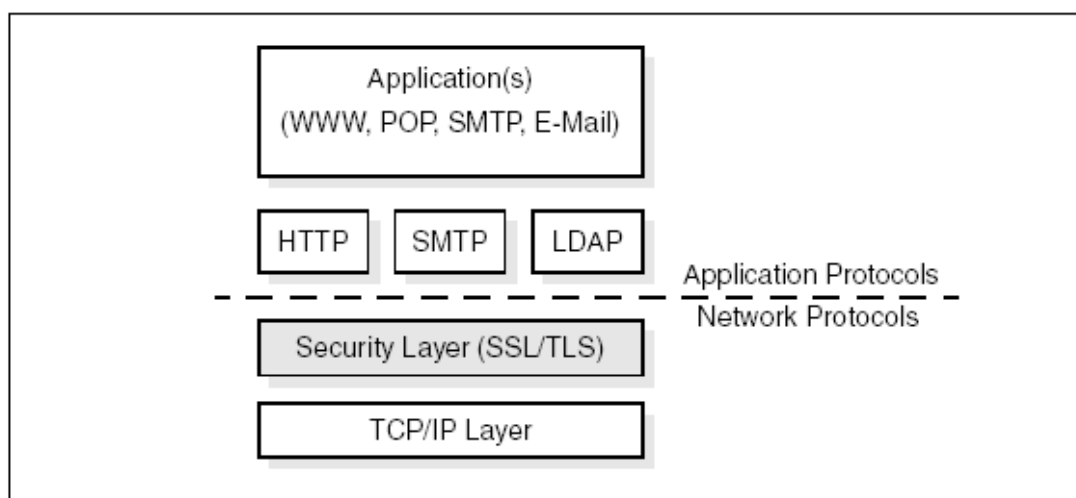
- povezivanje s poslužiteljem
- pretraživanje sadržaja direktorija
- usporedba zapisa
- dodavanje zapisa u direktorij
- modificiranje postojećih zapisa
- brisanje zapisa iz direktorija

## 3.3. Sigurnost

Sva prava pristupa LDAP podacima određena su načinom na koji se povezuje s poslužiteljem. Prava pristupa određuju kako korisnik može koristiti LDAP podatke pri pretraživanju, čitanju ili modificiranju podataka koji se nalaze u direktoriju. Kada se koristi anonimno povezivanje (nije potrebna autentikacija), operacije koje se mogu vršiti nad podacima su dosta ograničene. Obično je moguće samo pretraživanje direktorija. Za ostale

operacije potrebno je identificirati se kao korisnik. Prava pristupa se definiraju u osnovnoj shemi svakog poslužitelja i moguće ih je postaviti tako da se odnose na ukupni sadržaj direktorija ili samo na određene zapise u njemu.

Za autentikaciju i sigurnost podataka brine se protokol SSL (Secure Socket Layer), kojeg će vjerojatno zamijeniti TLS (Transport Layer Security) protokol, koji je još u razvoju. SSL/TLS podržava autentikaciju poslužitelja (klijent autentificira poslužitelja), autentikaciju klijenta (poslužitelj autentificira klijenta) ili obostranu autentikaciju. Na slici 2. prikazan je smještaj ovih protokola.



Slika 2. Smještaj protokola SSL/TLS

#### 4. PRIMJENA LDAP-a

LDAP poslužiteljski sustav je softverska podrška koja nam omogućuje da radimo s podacima po LDAP protokolu. Postoji više primjera takvog softvera: i-Planet LDAP, QLDAP, OpenLDAP, MIT LDAP itd. LDAP se koristi u web browser-ima, za imenike korisnika, white pages, yellow pages.

Jedinstveno ime svakog LDAP poslužitelja skriva se pod oznakom BN (Base Name), a označava jednoznačno njegovo ime/područje s podacima. Isto tako, može se sresti i naziv *Root Name*, *Basic Root* itd. Ovo ime se obično sastoji od DC () elemenata (npr. *dc=srce*, *dc=hr*). No, jedinstveno ime mora biti i kratko tako da mu je potrebna dopuna s našim imenom poduzeća, adresom, mjestom gdje se nalazimo itd. To pohranjujemo u naš globalni sustav.

Prije bilo kakvog unosa podataka u LDAP poslužitelj, potrebno je na odgovarajući način unijeti dopunu objašnjenja za sam poslužitelj u obliku određenih slobodno definirajućih polja s podacima.

Osnova za svaku grupu polja s podacima je jedinstveno ime kako bi se jednoznačno do te grupe podataka moglo doći. U LDAP notifikaciji to je DN koji se sastoji od proizvoljnog dijela i BN poslužitelja. Preporučeni oblik DN-a za korisničke podatke je [uid=username@mi.computer.name](#), *dc=computer*, *dc=name*. Izbor sadržaja koji može sadržati pojedina grupa podataka se podešava prilikom konfiguriranja samog LDAP poslužitelja (za OpenLDAP to su datoteke u direktoriju sheme, unutar kojih se pronalaze definicije polja razreda po određenim RFC-ovima).

Na kraju, korisnici trebaju predložiti set polja koja su standardna i koja se najčešće koriste unutar LDAP klijenata, a koja se nalaze unutar razreda koje smo prethodno odredili da će sam poslužitelj podržavati. Na slici 3. su primjeri nekih lokalnih poslužitelja, a na slici 4. *dc=hr* poslužitelj.

<b><u>ldap://gamma.carnet.hr:389/dc=carnet,dc=hr</u></b>	
Poslužitelj	<b>gamma.carnet.hr</b>
Port	<b>389</b>
BN	<b>dc=carnet,dc=hr</b>
Organizacija	<b>Hrvatska akademska i istraživačka mreža - CARNet</b>

<b><u>ldap://regoc.srce.hr:389/dc=srce,dc=hr</u></b>	
Poslužitelj	<b>regoc.srce.hr</b>
Port	<b>389</b>
BN	<b>dc=srce,dc=hr</b>
Organizacija	<b>Sveučilišni računski centar - SRCE, Sveučilišta u Zagrebu</b>

**ldap://ds.carnet.hr:389/dc=hr**

Poslužitelj	<b>ds.carnet.hr</b>
Port	<b>389</b>
BN	<b>dc=hr</b>
Organizacija	<b>Nacionalni server za HR, Hrvatska akademska i istraživačka mreža - CARNet</b>

Copyright by SRCE, 2001

Slika 4. *dc=hr* poslužitelj

Nacionalni LDAP poslužitelj, *dc=hr*, koji koristeći mogućnosti LDAP standarda v3 indeksira ostale nacionalne poslužitelje, nalazi se na računalu *ds.carnet.hr*, te je kao centralni poslužitelj prijavljen na *DANTE Name Flow National Directory Services*.

## 5. ZAKLJUČAK

LDAP definira operacije za održavanje direktorija. Operacije služe za dodavanje i brisanje zapisa u bazi, mijenjanje postojećeg zapisa i mijenjanje imena zapisa. Većinu vremena LDAP se koristi za pretraživanje informacija u bazi. LDAP omogućuje pretragu dijela baze po određenom kriteriju koji je definiran filterom (traženi izraz koji se prosljeđuje poslužitelju). Podaci se mogu zahtijevati za svaki podatak koji odgovara kriteriju.

LDAP pruža mogućnost registriranja klijenta, ili dokazivanja identiteta čime se može potpuno ili djelomično pristupiti podacima, ili brani pristup podacima. Jedan ili više LDAP poslužitelja čine LDAP stablo direktorija (baza). Po defaultu sluša port 389, ali se može i drugačije konfigurirati. Veza se uspostavlja kada klijent pošalje zahtjev za podacima. Poslužitelj vraća odgovor ili pokazivač gdje klijent može dobiti više podataka (obično neki drugi LDAP poslužitelj).

## Literatura:

<http://ds.carnet.hr/ldap/>

Internet