

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
PALCOMTECH PALEMBANG

SKRIPSI

DESAIN DAN IMPLEMENTASI *SQUID PROXY* MENGGUNAKAN
***AUTHENTICATION* LDAP PADA BADAN KETAHANAN PANGAN**
PROVINSI SUMSEL



Oleh :

Rendy Otista

012070085

Untuk Memenuhi Sebagian dari Syarat-Syarat

Guna Mencapai Gelar Sarjana Komputer

2012

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
PALCOMTECH PALEMBANG

HALAMAN PERSETUJUAN PEMBIMBING

Nama : Rendy Otista
Nomor Pokok : 012070085
Program Studi : Teknik Informatika
Kosentrasi : Jaringan
Jenjang Pendidikan : Strata Satu (S1)
Judul Skripsi : Desain dan Implementasi *Squid Proxy* Menggunakan
Authentication LDAP Pada Badan Ketahanan Pangan
(BKP) Prov.Sumsel

Palembang, September 2012

Menyetujui,
Pembimbing,

Mengetahui,
Ketua STMIK,

Adelin, S.T.
NIDN : 0211127901

Rudi Sutomo, S.Kom., M.Si
NIP : 028.PCT.08

KATA PENGANTAR

Puji dan Syukur Penulis panjatkan kepada Tuhan Yang Maha Esa, atas rahmat dan karunia-Nya, yang telah memberikan kesehatan dan kesempatan sehingga penulis dapat menyelesaikan Skripsi dengan baik. Penulisan skripsi ini bertujuan untuk memenuhi syarat dan menyelesaikan pendidikan pada jurusan Teknik Informatika STMIK PalComTech Palembang.

Dalam kesempatan ini penulis menyampaikan ucapan terima kasih sebesar-besarnya kepada, Bapak Rudi Sutomo, S.Kom., M.Si. selaku Ketua STMIK PalComTech Palembang, Bapak Yudi Wiharto, S.Kom. selaku Pembimbing skripsi STMIK PalComTech Palembang, Ibu Nova Humairoh selaku Administrator *server* BKP (Badan Ketahanan Pangan) Prov. Sumsel. Seluruh Staf dan pegawai di tiap divisi pada Badan Ketahanan Pangan Prov. Sumsel, Seluruh Staf dan pegawai STMIK PalComTech Palembang. Yang tercinta Ayah dan Ibu, dan seluruh keluarga yang telah memberikan dorongan semangat moril selama pendidikan dan akhir penyusunan skripsi ini serta sahabat dan rekan-rekan yang turut membantu dalam menyelesaikan skripsi ini.

Atas semua bantuan dan bimbingan yang telah diberikan kepada penulis, semoga Allah SWT selalu memberkati dan membalas kebaikan mereka. Penulis menyadari bahwa didalam skripsi ini masih ada kekurangan baik dalam penulisan, pengalaman dan pengetahuan. Oleh karena itu penulis menerima adanya kritik dan saran yang bersifat membangun dari pembaca.

Akhir kata, semoga skripsi ini dapat berguna bagi semua pihak yang membutuhkan.

Palembang, Juli 2012

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN DOSEN PEMBIMBING.....	ii
HALAMAN PENGESAHAN PENGUJI	iii
KATA PENGANTAR	iv
DAFTAR ISI.....	vi
DAFTAR TABEL.....	x
DAFTAR GAMBAR.....	xi
ABSTRAK.....	xiv
BAB I PENDAHULUAN	
1.1. Latar belakang	1
1.2. Perumusan masalah.....	2
1.3. Batasan Masalah	2
1.4. Tujuan Penelitian.....	3
1.5. Manfaat Penelitian	
1.5.1. Bagi Penulis	3
1.5.2. Bagi Perusahaan.....	3
1.5.3. Bagi Mahasiswa	4
1.6. Sistematika Penulisan.....	4
BAB II GAMBARAN UMUM PERUSAHAAN	
2.1. Sejarah BKP	5
2.2. Visi, Misi	7

2.3. Struktur Organisasi.....	8
2.4. Tugas dan Tanggung Jawab	9

BAB III TINJAUAN PUSTAKA

3.1. Teori Pendukung	
3.1.1. Pengertian Desain Jaringan.....	15
3.1.2. Pengertian Implementasi.....	15
3.1.3. Pengertian Komunikasi Data	16
3.1.4. Terminologi Jaringan Komputer	16
3.1.4.1. Berdasarkan Terminologi.....	17
3.1.4.2. Berdasarkan Topologi.....	18
3.1.4.3. Berdasarkan <i>Type</i>	20
3.1.5. Perangkat Jaringan Komputer	21
3.1.6. Protokol Jaringan	22
3.1.7. TCP/IP.....	23
3.1.7.1. Terminologi <i>IP Address</i>	24
3.1.8. <i>DNS Server</i>	24
3.1.9. <i>Internet</i>	25
3.1.10. Pengertian <i>Firewall</i>	25
3.1.11. <i>IPTables</i>	26
3.1.12. Pengertian <i>Squid</i>	28
3.1.13. <i>Authentication</i>	29
3.1.14. <i>Light Weight Directory Access Protocol (LDAP)</i>	29
3.1.15. <i>Captive Portal</i>	35

3.1.16. <i>Bandwidth Management</i>	36
3.1.17. Sistem Operasi <i>Fedora</i>	36
3.2. Hasil Penelitian Terdahulu	37
BAB IV METODE PENELITIAN	
4.1. Lokasi Dan Waktu Penelitian	
4.1.1. Lokasi Penelitian	41
4.1.2. Waktu Penelitian	41
4.2. Jenis Data.....	41
4.2.1. Data Primer.....	41
4.2.2. Data Sekunder.....	42
4.3. Teknik Pengumpulan Data	42
4.3.1. Observasi.....	42
4.3.2. Wawancara.....	43
4.4. Jenis Penelitian	43
4.5. Alur Proses dan Teknik Pengembangan Sistem.....	43
4.5.1. Alur Proses.....	43
4.5.2. Teknik Pengembangan Sistem.....	46
BAB V HASIL DAN PEMBAHASAN	
5.1. <i>Analysis</i>	50
5.2. <i>Design</i>	51
5.2.1. Topologi Jaringan Yang Digunakan	51
5.2.2. Topolgi Jaringan Yang Diusulkan	51
5.3. <i>Simulation Prototype</i>	52

5.3.1. Spesifikasi Komputer yang digunakan	52
5.3.2. Teknologi Jaringan.....	53
5.4. <i>Implementation</i>	53
5.4.1. Konfigurasi IP dan DNS <i>server</i>	53
5.4.2. Konfigurasi LDAP <i>server</i>	56
5.4.2.1. Konfigurasi phpLDAPAdmin	61
5.4.3. Konfigurasi <i>Squid</i>	62
5.4.4. Pengujian LDAP <i>server</i> menggunakan phpLDAPAdmin	68
5.4.5. Pengujian Pada <i>Client</i>	69
5.4.5.1. Pengujian LDAP <i>server</i> pada <i>client</i>	69
5.4.5.2. Pengujian autentikasi <i>captive portal</i>	71

BAB VI PENUTUP

6.1. Kesimpulan.....	73
6.2. Saran.....	74

DAFTAR PUSTAKA

DAFTAR TABEL

Table 3.1 Kelas IP <i>Address</i>	23
Table 3.2 Parameter atribut <i>user</i>	35
Table 3.3 Hasil Penelitian Terdahulu	37

DAFTAR GAMBAR

Gambar 2.1. Struktur Organisasi	9
Gambar 3.1. Topologi <i>Bus</i>	18
Gambar 3.2. Topologi <i>Ring</i>	19
Gambar 3.3. Topologi <i>Star</i>	20
Gambar 4.1. <i>Flowchart</i> autentikasi pada <i>captive portal</i>	45
Gambar 4.2. <i>Network Development Life Cycle</i> (NDLC)	46
Gambar 5.1. Topologi Jaringan yang digunakan	51
Gambar 5.2. Topologi yang diusulkan	51
Gambar 5.3. Konfigurasi IP <i>server</i>	54
Gambar 5.4. Perintah <i>install</i> paket	54
Gambar 5.5. Aplikasi yang dibutuhkan	54
Gambar 5.6. <i>Edit resolv.conf</i>	54
Gambar 5.7. <i>Named.conf</i>	55
Gambar 5.8. <i>File forwar</i> dan <i>reverse</i>	55
Gambar 5.9. <i>Restart bind</i>	56
Gambar 5.10. <i>Install</i> paket <i>ldap</i>	56
Gambar 5.11. <i>Copy file ldap.conf</i>	56
Gambar 5.12. Konfigurasi <i>ldap.conf</i>	56
Gambar 5.13. Membuat <i>password ldap server</i>	57
Gambar 5.14. Konfigurasi <i>slapd.conf</i>	58
Gambar 5.15. Menjalankan <i>ldap</i>	58

Gambar 5.16. Membuat <i>entry</i> organisasi.....	58
Gambar 5.17. Mengeksekusi <i>file base_all.ldif</i>	59
Gambar 5.18. Membuat organisasi <i>unit</i>	59
Gambar 5.19. Membuat <i>user</i> subbag keuangan.....	60
Gambar 5.20. <i>Add user</i> subbag keuangan.....	60
Gambar 5.21. Melihat data yang di <i>input</i>	60
Gambar 5.22. <i>Install webserver</i>	61
Gambar 5.23. <i>Edit file httpd.conf</i>	61
Gambar 5.24. <i>Install phpldapadmin</i>	61
Gambar 5.25. <i>Copy file config.php</i>	61
Gambar 5.26. Konfigurasi <i>file config.php</i>	62
Gambar 5.27. <i>Install squid</i>	62
Gambar 5.28. <i>Enable forward IP</i>	62
Gambar 5.29. Konfigurasi <i>IPtables</i>	63
Gambar 5.30. Mengaktifkan <i>IPtables</i> saat <i>booting</i>	63
Gambar 5.31. Konfigurasi <i>squid</i>	63
Gambar 5.32. <i>Port squid</i>	63
Gambar 5.33. <i>Directory cache</i>	64
Gambar 5.34. Skema untuk autentikasi.....	64
Gambar 5.35. <i>Port-port ACL</i>	65
Gambar 5.36. <i>ACL purge</i> dan <i>method</i>	65
Gambar 5.37. Baris <i>traffic policy</i>	66
Gambar 5.38. <i>Acl</i> tambahan.....	67

Gambar 5.39. <i>Restart</i> paket.....	67
Gambar 5.40. Membuka <i>phpldapadmin</i>	68
Gambar 5.41. <i>Login</i> <i>phpldapadmin</i>	68
Gambar 5.42. <i>Phpldapadmin</i> sukses	69
Gambar 5.43. <i>Setting address book mozilla thunder bird</i>	70
Gambar 5.44. Tampilan <i>user LDAP</i>	70
Gambar 5.45. Informasi salah satu <i>user LDAP</i>	71
Gambar 5.46. Proses autentikasi	71
Gambar 5.47. Autentikasi berhasil	72

ABSTRAK

RENDY OTISTA. Desain Dan Implementasi *Squid Proxy* Menggunakan *Authentication* LDAP Pada Badan Ketahanan Pangan (BKP) Prov.Sumsel.

Seiring dengan perkembangan *internet*, banyak sistem dibangun bersifat *real-time* dan *online* yang memungkinkan seseorang dapat mengaksesnya dari mana saja. Beberapa sistem, membutuhkan proses otentikasi untuk *validasi* atau pembuktian identitas pengguna yang ingin mengakses layanan yang diberikan oleh sistem tersebut.

Lightweight Directory Access Protocol (LDAP) merupakan protokol *client-server* yang berjalan pada protokol TCP/IP untuk mengakses dan manajemen data dalam *direktory*. Metode ini memungkinkan tersedianya fasilitas *single sign-on* (satu password untuk semua fasilitas dan aplikasi). Manajemen *user* yang terpusat, serta *direktory* yang terintegrasi secara khusus yang mengelola informasi *user* dapat menentukan aplikasi, layanan, dan *server* mana yang ingin diakses, dan *privilege* apa yang dimiliki oleh seorang *user* untuk melakukan hal tersebut.

Dalam penelitian ini dibahas mekanisme autentikasi *squid proxy* berbasis *Lightweight Directory Access Protocol* (LDAP). *Server* LDAP menggunakan aplikasi *open source openLDAP*. *Server* LDAP akan dimanfaatkan untuk layanan *captive portal* untuk keperluan autentikasi.

Kata Kunci : *Squid proxy, autentikasi, openLDAP, LDAP.*

BAB I

PENDAHULUAN

1.1. Latar Belakang

Dalam suatu jaringan komputer yang kompleks, keamanan jaringan dan proses autentikasi sangat dibutuhkan. Badan Ketahanan Pangan telah menggunakan sistem komputerisasi yang terkoneksi ke jaringan *internet speedy* dan sistem jaringan yang ada kurang baik karena koneksi tidak terbagi dengan rata. Selain permasalahan itu, penggunaan akses *internet* yang dimiliki instansi pun dirasa kurang tepat dilakukan oleh *user* sehingga membuat kenyamanan *user-user* pemakai akses *internet* lainnya terganggu dalam berselancar di *internet*.

Proxy server adalah sebuah *server* yang dapat dikonfigurasi untuk beberapa hal yaitu sebagai *cache server*, *url filtering*, pengaturan *bandwidth*, autentikasi akses *internet* dan lain sebagainya. Pada skripsi ini akan dibahas bagaimana mengimplementasikan sistem autentikasi pengguna *proxy server* dengan protokol LDAP sebagai *backend*, di mana seluruh *user* yang berhak menggunakan *proxy server* akan terdaftar dan teridentifikasi sebagai pengguna pada LDAP *server*, sedangkan *squid proxy server* akan melakukan autentikasi dimana hanya pengguna yang terdaftar/terotentikasi sebagai pengguna *proxy server* saja yang bisa mengakses *internet*.

Dengan di terapkannya *proxy server* dan proses autentikasi ini diharapkan dapat memaksimalkan akses *internet* sehingga dapat di pergunakan dengan tepat dan meningkatkan efektifitas kerja karyawan. Untuk itu penulis mengambil judul skripsi “**Desain dan Implementasi *Squid Proxy* Menggunakan *Authentication LDAP* Pada Badan Ketahanan Pangan (BKP) Prov.Sumsel**”.

1.2. Perumusan Masalah

Berdasarkan observasi dan melihat kenyataan seperti yang telah diuraikan pada latar belakang, maka dalam hal ini penulis merumuskan masalah yang ada yaitu : “Bagaimana Desain dan Implementasi *Squid Proxy* menggunakan *Authentication LDAP* di Badan Ketahanan Pangan (BKP) Prov.Sumsel?”

1.3 Batasan masalah

Dalam hal ini penulis hanya membatasi pembahasan masalah mengenai :

- 1.) *Server LDAP* menggunakan Sistem Operasi *Linux distro Fedora* 15 dengan aplikasi *openLDAP*.
- 2.) Integrasi *openldap* dengan layanan *captive portal*.
- 3.) Pembuatan *captive portal* menggunakan aplikasi *squid* pada Badan Ketahanan Pangan Prov.Sumsel.

1.4. Tujuan Penelitian

Tujuan penelitian ini adalah:

- 1.) Mengimplementasikan pengaturan dan pengamanan dalam jaringan serta menjadikan protokol LDAP sebagai *Directory* terpusat pada Badan Ketahanan pangan Prov.Sumsel
- 2.) Untuk lebih meningkatkan efektifitas sistem kinerja Badan Ketahanan Pangan Prov.Sumsel
- 3.) Membuat Sistem Informasi menjadi lebih aman dan memudahkan *System Administrator* dalam menentukan *privilege* bagi pengguna *proxy server*.

1.5. Manfaat Penelitian

Adapun manfaat yang diperoleh dari penelitian ini adalah :

1.) Bagi Penulis

Penulis dapat menerapkan ilmu komputer yang di dapat selama perkuliahan di STMIK PalComTech dengan mencari dan menambah wawasan serta pengalaman di dunia kerja yang dimana hasilnya untuk memenuhi dan menyelesaikan materi perkuliahan Teknik Informatika pada STMIK PalComTech.

2.) Bagi Instansi

Dengan penerapan seperti ini dapat memaksimalkan dan memberi ketepatan dalam menggunakan atau mengakses jaringan *internet* serta dapat juga membantu mempermudah pencarian

tentang informasi *user* dalam jaringan karena adanya LDAP sebagai *direktory* terpusat.

3.) Bagi Akademik

Sebagai referensi bagi penulis lainnya untuk dijadikan sebagai studi perbandingan dalam menyusun penelitian yang selanjutnya dan menjadi bahan bacaan pada perpustakaan.

1.6. Sistematika Penulisan

Sistematika penulisan dari skripsi ini terbagi menjadi enam (6) bab yang diuraikan sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisikan tentang latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian, dan sistematika penulisan.

BAB II GAMBARAN UMUM PERUSAHAAN

Bab ini penulis menguraikan tentang sejarah perusahaan, visi misi, struktur organisasi dan uraian tugas di Badan Ketahanan Pangan (BKP) Prov.Sumsel.

BAB III TINJAUAN PUSTAKA

Bab ini penulis akan membuat teori yang mendasari penulisan skripsi ini, bukan defenisi per kata dari judul yang penulis ambil.

BAB IV METODE PENELITIAN

Bab ini berisi tentang metodologi pengembangan sistem dan menguraikan metodologi penelitian beserta lokasi penelitian,

teknik pengumpulan data dan teknik analisis dengan perancangan sistem yang akan dibuat didalam skripsi.

BAB V HASIL DAN PEMBAHASAN

Bab ini menerangkan tahapan-tahapan pembangunan sistem autentikasi berbasis LDAP dimulai dari tahapan instalasi dan konfigurasi selanjutnya melakukan pengujian sistem.

BAB VI PENUTUP

Bab akhir ini penulis memberikan simpulan atas analisis yang telah dilakukan dan memberikan saran yang semoga dapat bermanfaat bagi Badan Ketahanan Pangan Prov.Sumsel.

BAB II

TINJAUAN UMUM

2.1. Sejarah BKP

Sejarah berdirinya Badan Ketahanan Pangan Provinsi Sumatera Selatan, dapat dimulai pada kisaran tahun 1987. Pada tahun 1987 dengan menempati bagian dari Gedung Dinas Tanaman Pangan, saat itu masih berstatus Kantor Wilayah (Kanwil) Departemen Pertanian Prov. Sumatera Selatan. Kepala Kantor saat itu Bapak Ir. Rahman Daud Rusdi.

Pada bulan April tahun 1979 Kantor Wilayah Departemen Pertanian mendapat pinjaman gedung dari Pemerintah Daerah Tk. I, Provinsi Sumatera Selatan dengan Kepala Kantor saat itu Bapak Ir. Arbai Naya. Berdasarkan Surat Keputusan Menteri Pertanian RI No. 558/KPTS/ORG.6/1998 gedung Kanwil dibangun pada tahun 1980. Kantor Wilayah Departemen Pertanian Prov. Sumatera Selatan memiliki gedung sendiri dengan beberapa kali terjadi pergantian Kepala Kantor.

Pada tahun 2000/2001 Kanwil Dep. Pertanian dihapuskan, sesuai dengan Peraturan Daerah (Perda) No. 12, diganti menjadi BADAN KETAHANAN PANGAN Provinsi Sumatera Selatan dengan Kepala Badan pertamanya Ir. Syamsuddin Saylele. Hingga sekarang sudah terjadi beberap kali pergantian Pimpinan Di BKP Prov. Sumsel. Tahun 2001-2002 Badan Ketahanan Pangan di Kepalainya oleh Ir. H. Trisbani Arif, selanjutnya

tahun 2003 digantikan oleh Drs. H. Fachrurozi Solah, kemudian tahun 2004 digantikan oleh Ir. H. Qolyubi Nawawi, MS.i. Pada tahun 2009 terjadi pergantian Kepala Badan dari Ir. H. Qolyubi Nawawi, Ms.i digantikan Ir. Hj. Nelly Rasdiana, Ms.i, yang kemudian ditahun yang sama kembali digantikan oleh Ir. H. Syamuil Chatib, MM, yang memimpin BKP hingga sekarang.

2.2. Visi dan Misi

2.2.1 Visi

Pembangunan ketahanan pangan merupakan bagian integral dari pembangunan daerah di Provinsi Sumatera Selatan, sejalan dengan itu maka visi Badan Ketahanan Pangan Provinsi Sumatera Selatan adalah “Institusi yang Handal dalam Mewujudkan Masyarakat Sumatera Selatan Tahan Pangan, Sehat dan Sejahtera”.

2.2.2 Misi

Untuk mencapai harapan yang terkandung dalam visi tersebut, maka Badan Ketahanan Pangan Provinsi Sumatera Selatan harus menjadi satu lembaga pemerintah yang handal agar mampu melaksanakan tugas pokok dan fungsinya. Untuk itu misi Badan Ketahanan Pangan Provinsi Sumatera Selatan dirumuskan sebagai berikut :

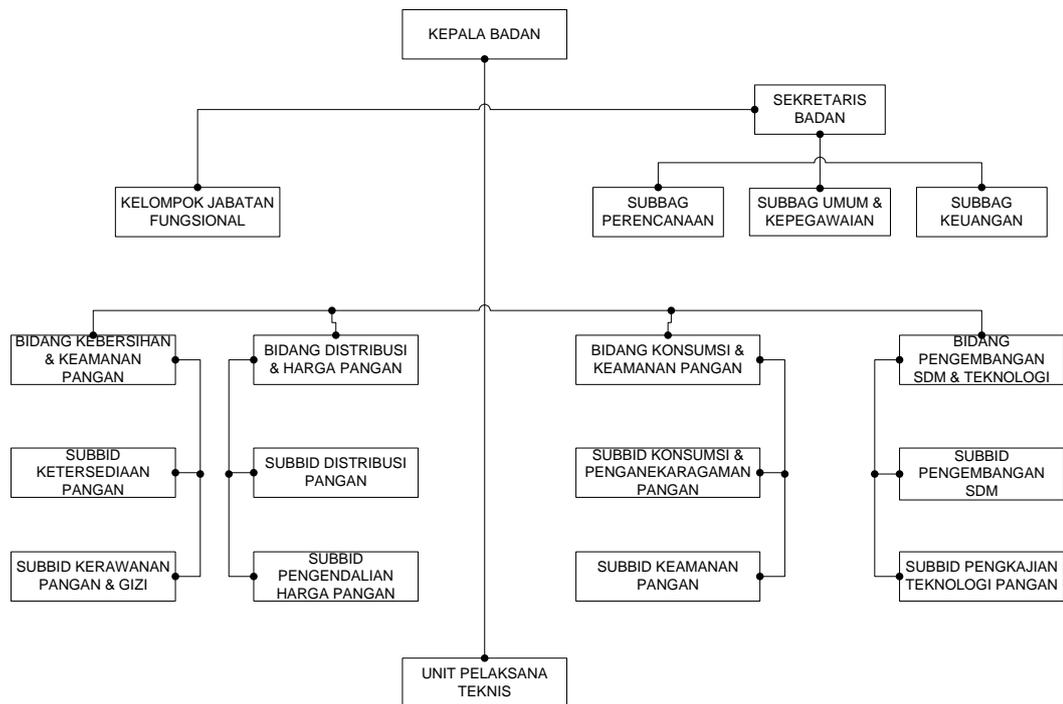
- 1.) Memantapkan ketersediaan pangan dengan mengoptimalkan pemanfaatan sumber daya yang dimiliki secara bijaksana dan berkelanjutan serta mencegah dan menanggulangi kerawanan pangan.

- 2.) Mengendalikan distribusi pangan untuk menjamin stabilitas pasokan dan harga pangan serta terjangkau dan akses pangan masyarakat.
- 3.) Mempercepat penerapan pola konsumsi pangan yang beragam, bergizi seimbang dan aman menuju masyarakat yang sehat dan cerdas.
- 4.) Meningkatkan kualitas sumberdaya manusia dalam pengelolaan usaha pangan dengan menerapkan teknologi pangan tepat guna.
- 5.) peningkatan kemampuan aparat dalam manajemen ketahanan pangan.

2.3. Struktur Organisasi

Struktur organisasi berarti susunan atau hubungan antara komponen bagian-bagian dalam suatu kerja perusahaan atau organisasi dan menunjukkan berbagai tingkat aktivitas yang berkaitan satu sama lain sampai dengan tingkat tertentu, juga akan menjabarkan hirarki organisasi, struktur wewenang dan tanggung jawab masing-masing bagian dalam organisasi sehingga setiap anggota dari organisasi tersebut dapat mengetahui dengan jelas serta pasti dari mana organisasi menerima perintah dan kepada siapa pula organisasi harus melaporkan dan mempertanggungjawabkan.

Struktur organisasi Badan Ketahanan Pangan Prov. Sumsel dapat dilihat Pada Gambar 2.1:



Gambar 2.1 Struktur Organisasi
(Sumber : Badan Ketahanan Pangan Prov.Sumsel)

2.4. Tugas dan Tanggung Jawab

Didalam struktur organisasi BKP Prov. Sumsel, terdiri dari beberapa bagian, masing – masing bagian mempunyai tugas dan tanggung jawab. Adapun uraian tugas dan tanggung jawab dari masing – masing bagian adalah sebagai berikut :

1.) Kepala Badan :

- a. Perumusan, penetapan kebijakan teknis di bidang ketahanan pangan yang meliputi kesekretariatan, kelembagaan dan infrastruktur, ketersediaan dan kerawanan pangan, konsumsi dan keamanan pangan, serta distribusi dan harga pangan.
- b. Penyelenggaraan perumusan dan penetapan pemberian dukungan atas penyelenggaraan pemerintahan daerah bidang ketahanan pangan.

- c. Penyelenggaraan fasilitasi dan pengendalian pelaksanaan tugas-tugas di bidang ketahanan pangan.
- d. Penyelenggaraan koordinasi dan kerjasama dalam rangka tugas pokok dan fungsi badan.
- e. Penyelenggaraan koordinasi dan pembinaan UPTB.

2.) Sekretariat Badan :

- a. Penyelenggaraan koordinasi perencanaan dan program badan.
- b. Penyelenggaraan pengkajian perencanaan dan program kesekretariatan.
- c. Penyelenggaraan pengelolaan urusan keuangan, kepegawaian dan umum.

3.) Subbag Perencanaan :

- a. Pelaksanaan penyusunan bahan perencanaan dan program kerja Sekretariat dan Sub Bahian Perencanaan dan Program.
- b. Pelaksanaan penyusunan bahan penyelenggaraan koordinasi perencanaan dan program badan yang meliputi bidang kelembagaan dan infrastruktur, ketersediaan dan kerawanan pangan, konsumsi dan keamanan pangan, serta distribusi dan harga pangan.
- c. Pelaksanaan penyusunan bahan hasil koordinasi perencanaan dan program badan yang meliputi bidang kelembagaan dan infrastruktur, ketersediaan dan kerawanan pangan, konsumsi dan keamanan pangan, serta distribusi dan harga pangan.

- d. Pelaksanaan pengkoordinasian perencanaan dan program UPTB.

4.) Subbag Keuangan :

- a. Pelaksanaan penyusunan bahan rencana anggaran belanja langsung dan tidak langsung badan.
- b. Pelaksanaan dan koordinasi pengelolaan teknis administrasi keuangan badan.
- c. Pelaksanaan koordinasi pengelolaan keuangan pada UPTB.

5.) Subbag Umum dan Kepegawaian :

- a. Pelaksanaan penyusunan bahan penyelenggaraan mutasi pengembangan karir, kesejahteraan dan disiplin pegawai dan pengelolaan administrasi kepegawaian lainnya.
- b. Pelaksanaan penyusunan bahan penyelenggaraan pembinaan kelembagaan, ketatalaksanaan dan rumah tangga.
- c. Pelaksanaan administrasi, dokumentasi peraturan perundang-undangan, kearsipan dan perpustakaan.
- d. Pelaksanaan tugas kehumasan badan.
- e. Pengelolaan perlengkapan badan.

6.) Bidang Konsumsi dan Keamanan Pangan :

- a. Penyelenggaraan perencanaan program peningkatan konsumsi dan keamanan pangan.
- b. Penyelenggaraan pengkajian bahan kebijakan teknis peningkatan konsumsi dan keamanan pangan.

- c. Penyelenggaraan fasilitasi peningkatan konsumsi dan keamanan pangan.

7.) Sub Bidang Konsumsi dan Penganekaragaman Pangan :

- a. Pelaksanaan penyusunan bahan kebijakan teknis peningkatan konsumsi dan penganekaragaman pangan.
- b. Pelaksanaan pelayanan administrasi, teknis pengembangan dan fasilitasi peningkatan konsumsi dan penganekaragaman pangan.

8.) Sub Bidang Keamanan Pangan :

- a. Pelaksanaan penyusunan bahan kebijakan teknis peningkatan keamanan dan mutu pangan.
- b. Pelaksanaan pelayanan administrasi, teknis pengembangan dan fasilitasi peningkatan keamanan dan mutu pangan.

9.) Bidang Distribusi dan Harga Pangan :

- a. Penyelenggaraan pengkajian bahan kebijakan teknis distribusi dan pengendalian harga pangan.
- b. Penyelenggaraan fasilitasi distribusi dan pengendalian harga pangan.
- c. Penyelenggaraan pelayanan informasi pangan dan harga pangan,

10.) Bidang Distribusi dan Harga Pangan :

- a. Pelaksanaan penyusunan bahan kebijakan teknis distribusi pangan.
- b. Pelaksanaan pelayanan administrasi, teknis pengembangan dan fasilitasi distribusi pangan.

11.) Bidang Pengembangan SDM dan Teknologi :

- a. Pelaksanaan penyusunan bahan kebijakan teknis perencanaan dan program kelembagaan pangan.
- b. Pelaksanaan pelayanan administrasi, teknis pengembangan dan fasilitasi kelembagaan pangan.

12.) Sub Bidang Kerawanan Pangan dan Gizi :

- a. Penyelenggaraan pengkajian bahan kebijakan teknis bidang ketersediaan, cadangan pangan dan penanggulangan kerawanan pangan.
- b. Penyelenggaraan fasilitasi bidang ketersediaan, cadangan pangan dan kerawanan pangan.

13.) Bidang Ketersediaan dan Kerawanan Pangan :

- a. Pelaksanaan penyusunan bahan kebijakan teknis ketersediaan dan cadangan pangan.
- b. Pelaksanaan pelayanan administrasi, teknis pengembangan dan fasilitasi ketersediaan dan cadangan pangan.

2.5. Aktifitas yang dilakukan

Selama Penulis melakukan Praktek Kerja Lapangan (PKL) dikantor Badan Ketahanan Pangan Prov. Sumsel yang terletak di Jl. Kol. H. Barlian Km. 6 No. 82 Palembang. waktu praktek kerja lapangan berjalan dari tanggal 19 Oktober 2010 sampai 19 November 2010.

Aktivitas yang penulis kerjakan disana adalah:

- 1.) Mengidentifikasi jaringan
- 2.) Memasukan data-data ke komputer
- 3.) Memperbaiki komputer
- 4.) Instalasi *software* dan *hardware*
- 5.) Instalasi komputer

BAB III

TINJAUAN PUSTAKA

3.1. Teori Pendukung

3.1.1. Pengertian Desain Jaringan

Menurut Tim Wahana Komputer (2005:271), desain jaringan merupakan pondasi bagi sebuah jaringan. Desain jaringan menganut tiga topologi dasar yaitu topologi *bus*, *ring*, dan *star*.

Desain jaringan merupakan penyusunan atau *layout* secara fisik dari komputer, kabel dan komponen lain pada sebuah jaringan.

Berdasarkan uraian di atas, penulis menyimpulkan bahwa desain jaringan merupakan proses untuk membangun suatu jaringan yang baru maupun memperbaiki jaringan yang sudah ada sesuai dengan topologi jaringan yang digunakan.

3.1.2. Pengertian Implementasi

Implementasi merupakan suatu penerapan ide, konsep, kebijakan, atau inovasi dalam suatu tindakan praktis sehingga memberikan dampak baik berupa perubahan pengetahuan, keterampilan maupun nilai dan sikap.

Dalam penulisan skripsi ini, implementasi merupakan tahap yang dilakukan untuk menerapkan suatu sistem supaya siap dioperasikan.

Dengan acuan pada pendapat tersebut, dapat diambil simpulan bahwa implementasi adalah pelaksanaan atau penerapan dalam tahap meletakkan sistem supaya siap di operasikan.

3.1.3. Pengertian Komunikasi Data

Menurut Sopandi (2006:1), Data adalah informasi *digit biner*. Komunikasi data adalah transmisi data elektronik melalui beberapa media. Media tersebut berupa kabel *coaksial*, *fiber optic*, *microwave*, dan sebagainya.

3.1.4. Pengertian Jaringan Komputer

Menurut Sopandi (2006:5), Jaringan komputer merupakan gabungan antara teknologi komputer dan teknologi komunikasi. Gabungan teknologi ini dapat melahirkan pengolahan data yang dapat di distribusikan mencakup pemakaian *database*, aplikasi perangkat lunak dan penggunaan perangkat keras secara bersamaan.

Menurut Suarna (2007:9), jaringan komputer adalah sebuah kumpulan komputer, *printer* dan peralatan lainnya yang terhubung dalam satu kesatuan. Informasi dan data bergerak melalui kabel-kabel atau tanpa kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada *printer* yang sama dan bersama-sama menggunakan *hardware* atau *software* yang terhubung dengan jaringan.

Berdasarkan pengertian di atas dapat disimpulkan jaringan atau bisa disebut juga jaringan komputer adalah sekumpulan komputer dan

alat-alat lainya yang dihubungkan satu sama lain dengan media penghubung tertentu sehingga dapat saling berkomunikasi dan bertukar data.

3.1.4.1. Berdasarkan Terminologi

Menurut Wagito (2007:9) ada tiga tipe jaringan dalam hubungannya dengan luas area yang dicakup yaitu :

1.) LAN (*Local Area Network*)

Menurut Wagito (2007:9), LAN adalah suatu jaringan yang terbatas pada daerah yang relatif kecil, umumnya dibatasi oleh area lingkungan seperti laboratorium, sekolah, kantor, atau gedung. Dalam konfigurasi LAN tertentu, satu komputer biasanya di jadikan sebuah *server*, yang mana digunakan untuk menyimpan perangkat lunak yang mengatur aktifitas jaringan komputer-komputer yang terhubung ke dalam di jaringan.

2.) MAN (*Medium Area Network*)

Menurut Wagito (2007:9), Suatu MAN meliputi area geografi yang lebih luas dari LAN, misalnya antar wilayah dalam satu provinsi. Dengan interkoneksi jaringan dalam area geografi yang luas, informasi dapat disebarkan secara mudah melalui jaringan. Dengan MAN suatu komputer dikantor cabang dapat berhubungan

dengan *server* komputer yang ada pada kantor pusat melalui jaringan telepon, kabel *coaxial* atau komunikasi tanpa kabel.

3.) WAN (*Wide Area Network*)

Menurut Wagito (2007:9), Suatu WAN meliputi area geografi yang lebih luas lagi, yang meliputi suatu negara atau dunia. Umumnya jaringan di tempatkan pada banyak lokasi yang berbeda. WAN digunakan untuk menghubungkan banyak LAN yang secara geografi terpisah. WAN dibuat dengan cara menghubungkan LAN menggunakan layanan seperti *leased lines*, *dial-up*, satelit atau layanan *packet carrier*.

3.1.4.2. Berdasarkan Topologi

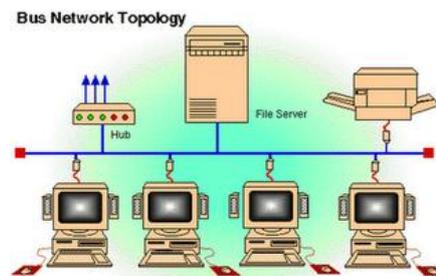
Menurut Suarna (2007:31), Topologi adalah tata cara menghubungkan antar komputer sehingga komputer yang satu dengan komputer yang lainnya dapat saling berkomunikasi dan membentuk suatu jaringan.

Adapun topologi fisik yang sering digunakan dalam membangun sebuah jaringan adalah :

1.) Topologi *Bus*

Menurut Suarna (2007:31), Topologi yang seluruh terminalnya saling terhubung ke sebuah *bus* (jalur) utama komunikasi data. Informasi atau data di

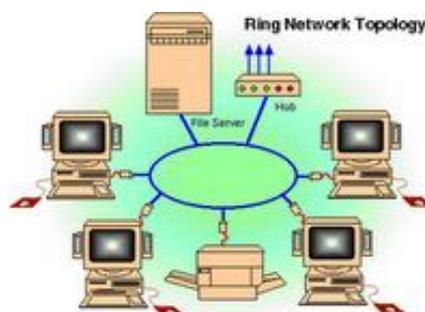
kiriman dan diambil melalui sepanjang jalur atau melewati seluruh *workstation*. Topologi ini dipakai untuk area jaringan lokal.



Gambar 3.1 Topologi *Bus*
(Sumber : Nana (2007:31))

2.) Topologi Cincin (*Ring*)

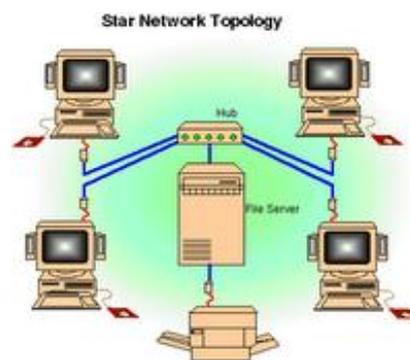
Menurut Suarna (2007:33), Topologi *Ring* yaitu semua *terminal* dan *server* di hubungkan, Tiap *terminal* ataupun *server* akan menerima dan melewatkan informasi dari satu komputer ke komputer lain. Jika alamat-alamat yang dituju sesuai, maka informasi diterima. Apabila tidak informasi akan dilewatkan.



Gambar 3.2 Topologi *Ring*
(Sumber : Nana (2007:33))

3.) Topologi Bintang (*Star*)

Menurut Suarna (2007:32), Topologi yang masing-masing *terminal* dalam jaringan dihubungkan ke titik pusat (*server*) menggunakan jalur dan semua sambungan antar*terminal* harus diteruskan melalui *server*.



Gambar 3.3 Topologi *Star*
(Sumber : Nana (2007:32))

3.1.4.3. Berdasarkan *Type*

a.) *Client-Server*

Menurut Suarna (2007:9), *Server* yaitu komputer yang menyediakan fasilitas bagi komputer-komputer lain, sedangkan *client* yaitu komputer-komputer yang menerima atau menggunakan fasilitas yang disediakan oleh *server*. Berarti jaringan *client-server* merupakan hubungan antara dua komputer atau lebih dimana salah satu komputer berfungsi sebagai *client* sedangkan komputer yang lain menjadi *server*. Komputer *client*

meminta layanan dan dilayani oleh komputer yang berperan sebagai *server*.

b.) *Peer-to-Peer*

Menurut Suarna (2007:10), Jaringan tipe *peer to peer* di istilahkan sebagai *non-dedicated server*, yaitu *server* yang tidak hanya berperan sebagai *server* murni, tetapi dapat juga berperan sebagai *workstation*.

3.1.5. Perangkat Jaringan Komputer

Adapun perangkat jaringan komputer adalah sebagai berikut :

1.) *Hub*

Menurut Sopandi (2006:19), *Hub* merupakan pembagi sinyal data bagi *network interface card* (NIC) dan sekaligus berfungsi sebagai penguat sinyal.

2.) *Switch*

Menurut Suarna (2007:29), *Switch* melanjutkan paket data hanya ke *port* penerima yang dituju, menurut informasi dalam *header* paket. Untuk memisahkan transmisi dari *port* yang berbeda, *switch* membuat koneksi sementara antara sumber dan tujuan kemudian meneruskan koneksinya setelah komunikasi data berakhir.

3.) *Repeater*

Menurut Sopandi (2006:22), *Repeater* berfungsi untuk memperkuat sinyal, sinyal yang diterima dari satu segmen

kabel LAN ke segmen LAN berikutnya akan dipancarkan kembali dengan kekuatan sinyal asli pada segmen LAN pertama sehingga dengan adanya *repeater* ini, jarak antara dua jaringan komputer dapat diperluas.

4.) Router

Menurut Sopandi (2006:24), *Router* adalah perangkat yang dapat menjadwalkan data antara LAN yang berbeda dan berbagai jaringan seperti pengendalian jalur jaringan.

5.) NIC (*Network Interface Card*)

Menurut Sopandi (2006:16), *Network Interface Card* (NIC) merupakan perangkat keras yang sangat dibutuhkan untuk menghubungkan antara komputer satu dengan komputer lain.

3.1.6. Protokol Jaringan

Menurut Suarna (2007:46), Protokol yaitu aturan-aturan main yang mengatur komunikasi antara komputer yang satu dengan lainnya di dalam sebuah jaringan. Di dalam aturan- aturan tersebut termasuk petunjuk yang berlaku bagi cara-cara atau metode mengakses sebuah jaringan, topologi fisik, tipe-tipe kabel dan kecepatan *transfer* data. Selain itu protokol juga merupakan sekumpulan aturan untuk memecahkan masalah-masalah yang khusus yang terjadi antar alat-alat komunikasi agar proses transmisi data dapat terjadi dengan baik dan benar.

3.1.7. TCP/IP (*Transmission Control Protocol/Internet Protokol*)

Menurut Sofana (2010:249), TCP lahir sebagai sebuah teknologi yang berdasar pada koneksi, menjaga sesi aplikasi, dan menjamin tingkat komunikasi yang handal. Merupakan salah satu lapisan protokol dari TCP/IP yang menandai bahwa data sudah dikirimkan ke *application* lapisan yang lebih tinggi tanpa adanya kesalahan, kehilangan data, atau adanya duplikasi. TCP mengandalkan IP untuk pengiriman data, termasuk masalah *routing*.

Peralatan-peralatan yang ada dalam sistem jaringan berbasis TCP/IP dikenali dengan alamat IP (*IP Address*). Peralatan seperti komputer atau alat lain, harus mempunyai alamat IP tertentu supaya dapat dikenali dalam jaringan. Alamat IP dikelompokkan menjadi 5 kelas yaitu A, B, C, D, dan E. Kelas yang umum digunakan adalah A, B, C. Kelas D digunakan untuk *multicast* sedangkan kelas E digunakan untuk eksperimental.

Tabel 3.1 Kelas *IP Address*

Class	Range Oktet Pertama	Alamat awal	Alamat Akhir
A	1-126	xxx.0.0.1	xxx.255.255.254
B	127-191	xxx.xxx.0.1	xxx.xxx.255.254
C	192-223	xxx.xxx.xxx.1	xxx.xxx.xxx.254

(Sumber : Dede (2006:198))

3.1.7.1. Terminologi IP Address

Berdasarkan penggunaannya, *IP address* terbagi menjadi :

a.) *IP Address Public*

Menurut Wagito (2007:79) *IP Address Public* adalah *IP address* yang digunakan untuk komunikasi pada jaringan *internet* dan konfigurasinya tidak bebas.

b.) *IP Address Private*

Menurut Wagito (2007:79) *IP address private* adalah alamat IP yang tidak terhubung dengan alamat IP *Public* atau tidak di *routing*. *IP address private* digunakan untuk membentuk jaringan yang sifatnya lokal.

3.1.8. DNS Server

Menurut Azikin (2011:143) *Domain Name System* (DNS) digunakan untuk translasi dari *IP address* ke nama *host* yang lebih mudah di ingat sehingga *client* dapat terhubung ke *web server* atau ke *mail server* menggunakan nama *domain* bukan *IP address*.

Cara kerja DNS:

(a.) *Client* ingin mengakses *website www.google.com* menggunakan *web browser Iceweasel*.

(b.) *Client* yang ingin mengakses *www.google.com* akan berkomunikasi terlebih dahulu dengan *DNS server* lokal.

(c.) Karena jawaban IP *address* untuk *www.google.com* belum didapatkan, maka DNS lokal akan menanyakan ke DNS pihak ISP dalam hal ini DNS *server Internux*.

(d.) Setelah jawaban IP *address google* diperoleh, *client* akan berkomunikasi secara langsung ke *web server www.google.com* dengan menggunakan IP *address* bukan nama *domain*.

3.1.9. *Internet*

Menurut Suarna (2007:80), *Internet* kepanjangan dari *Interconnection Networking* yang merupakan jaringan komputer terluas di dunia (*World Wide Network*) dimana antara satu komputer dengan komputer lainnya saling berhubungan dan saling berkomunikasi.

Internet adalah suatu jaringan publik yang dapat dipakai oleh siapa saja. Hubungan ke *internet* memungkinkan anda mencari informasi yang anda perlukan yang tersedia di *internet*.

Berdasarkan uraian diatas, penulis menyimpulkan bahwa *internet* adalah suatu jaringan komputer yang satu dengan yang lainnya saling terhubung untuk keperluan komunikasi dan informasi.

3.1.10. *Pengertian Firewall*

Menurut Wagito (2007:143), *Firewall* adalah suatu cara/sistem/mechanisme yang diterapkan baik terhadap *hardware*, *software* ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau

semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkungannya.

Firewall merupakan dinding pemisah LAN dengan *internet* agar semua akses ke LAN harus melalui satu pintu gerbang yang dikontrol sehingga dapat diatur hanya pemakai-pemakai tertentu yang diizinkan akses keluar dan masuk pintu gerbang tersebut.

Berdasarkan uraian diatas, penulis menyimpulkan *firewall* adalah suatu mekanisme untuk melindungi keamanan jaringan komputer dengan menyaring paket data yang keluar dan masuk di jaringan. Paket data yang “baik” diloloskan untuk melewati jaringan dan paket data yang dianggap “jahat” tidak diperbolehkan melewati jaringan.

3.1.11. IPTables

Menurut Wagito (2007:146), *IPtables* adalah program yang digunakan untuk memasukan dan menghapus isi *filter* paket pada *kernel*. Dengan demikian, apapun yang dituliskan dalam *table* tersebut akan hilang ketika dilakukan *reboot* terhadap sistem.

Menurut Ashari (2008:331) *IPtables* adalah salah satu aplikasi *firewall* yang banyak digunakan. Dengan berbagai fasilitas yang didukung antara lain dapat menghentikan penggunaan aplikasi tertentu seperti *Yahoo Messenger*. Dengan melakukan filterisasi berdasarkan nomor *port*, alamat IP, tipe service, hingga translation, membuat keberadaannya sungguh fleksibel untuk mengamankan suatu jaringan.

Menurut Wagito (2007:147), Ada tiga macam *table* dalam *IPtables* yang sudah tersedia secara *default* sebagai berikut :

1.)Tabel *Filter*

Tabel *filter* merupakan tabel *default*, sehingga tidak perlu secara eksplisit dituliskan. Tabel ini mengandung rantai *built-in* yaitu *INPUT* (untuk paket yang datang dan ditujukan untuk *firewall* sendiri), *FORWARD* (untuk paket yang akan diteruskan oleh *firewall*), dan *OUTPUT* (untuk paket yang dihasilkan oleh proses lokal).

2.)Tabel NAT

Tabel NAT digunakan untuk proses translasi alamat jaringan. Tabel ini akan diperiksa ketika paket yang membuat koneksi ditemukan. Tabel ini mengandung tiga rantai *built-in* yaitu *PREROUTING* (untuk mengubah paket segera setelah paket datang), *OUTPUT* (untuk mengubah paket yang dihasilkan proses lokal sebelum paket *dirouting*), dan *POSTROUTING* (untuk mengubah paket seraya paket tersebut meninggalkan *firewall*).

3.)Tabel *Mangle*

Tabel *mangle* digunakan untuk perubahan paket khusus. Tabel ini didukung lima rantai *built-in* yaitu *INPUT*, *FORWARD*, *OUTPUT*, *PREROUTING*, dan *POSROUTIN*.

Kesimpulannya menurut penulis *IPtables* sebagai pengatur lalu lintas data.

3.1.12. Pengertian *Squid*

Menurut Rafiudin (2008:1), *Squid* merupakan mesin *caching proxy* untuk *client web*, seperti HTTP, HTTPS, FTP, *gopher* dan layanan sejenis lainnya. *Squid* mampu menurunkan konsumsi *bandwidth* sekaligus mempercepat waktu *respons*. Ini terwujud dengan melakukan *caching* halaman *web* dan menggunakan ulang halaman yang sering dikunjungi.

Menurut Azikin (2011:332), *Squid* merupakan program aplikasi yang dapat digunakan sebagai *proxy web caching* yang sangat bermanfaat untuk pengaturan *website-website* mana saja yang dapat diakses oleh *client*, autentikasi *user* saat akan mengakses *Internet*, manajemen trafik yang mencakup di dalamnya penghematan *bandwidth* karena konten-konten yang sering diakses tersimpan di *cache* lokal, pengaturan jam akses *Internet*, pembatasan jumlah *client* yang dapat mengakses *Internet* dan sejumlah fasilitas lain yang dapat disesuaikan berdasarkan kebutuhan.

Berdasarkan uraian diatas, penulis menyimpulkan bahwa *squid* merupakan sebuah program yang digunakan sebagai *proxy server* dan *web cache* sehingga dapat mempercepat akses *web* serta dapat melakukan penyaringan (*filter*) lalu lintas dalam jaringan.

3.1.13. *Authentication*

Menurut Rafiudin (2005:5) *Authetication* adalah metode verifikasi atas identitas *user*, proses-proses, dan piranti-piranti. Verifikasi identitas akan berlaku untuk pengiriman maupun penerimaan informasi.

Menurut R.Fibrian (2011:1) *Authentication* adalah proses usaha pembuktian identitas seorang pengguna sistem komunikasi pada proses *login* ke dalam sebuah sistem. Pengguna yang telah terbukti identitasnya adala pengguna resmi pada sistem, orang yang memiliki otoritas pada sistem atau mungkin aplikasi yang berjalan pada sistem.

3.1.14. *Lightweight Directory Access Protocol (LDAP)*

Menurut R. Fibrian (2011:2), *Directory* adalah suatu tempat penyimpanan data yang dapat digunakan untuk memberikan informasi-informasi yang berkaitan dengan objeknya. Direktori berbeda dengan *database*, perbedaannya adalah direktori dibuat untuk dibaca lebih banyak dari pada ditulis. Sedangkan untuk *database* diasumsikan untuk operasi baca dan tulis memiliki frekuensi yang sama.

Menurut Azikin (2011:260), (*Lightweight Directory Access Protocol*) LDAP adalah sebuah protokol yang mengatur mekanisme pengaksesan layanan direktori (*Directory Service*) yang dapat digunakan untuk mendeskripsikan banyak informasi seperti informasi tentang perorangan, organisasi, dan lainnya seperti *file* atau *printer* di

dalam jaringan baik di *internet* atau *intranet*. LDAP menggunakan model *client-server*, dimana *client* mengirimkan *identifier* data kepada *server* menggunakan protokol TCP/IP dan *server* mencoba mencarinya pada *Directory Information (DIT) Tree* yang tersimpan di *server*.

Menurut R.Fibrian (2011:2), (*LightWeight Directory Access Protocol*) LDAP adalah sebuah protokol yang mengatur mekanisme pengaksesan layanan direktori yang dapat digunakan untuk mendeskripsikan banyak informasi seperti informasi tentang seseorang, organisasi, komputer dan banyak entitas lainnya. LDAP menggunakan model *client-server*, dimana *client* mengirimkan *identifier* data kepada *server* menggunakan protokol TCP/IP dan *server* mencoba mencarinya pada DIT (*Directory Information Tree*) yang tersimpan di *server*. Bila ditemukan maka hasilnya akan dikirimkan ke *client* tersebut namun bila tidak maka hasilnya berupa *pointer* ke *server* lain yang menyimpan data yang dicari.

Dari hasil uraian diatas, kesimpulan dari penulis bahwa LDAP adalah Protokol yang digunakan untuk mengakses berbagai informasi dalam suatu direktori.

1.) Autentikasi LDAP

Menurut R. Fibrian (2011:2), Pada autentikasi menggunakan metode autentikasi LDAP terdapat mekanisme *binding*. LDAPv3 mendukung 3 jenis autentikasi yaitu:

(a.) *Anonymous*

Client yang mengirimkan suatu permintaan ke *server* LDAP tanpa melakukan mekanisme *bind* maka akan diperlakukan sebagai *client anonim* dimana *client* tersebut hanya dapat melihat tampilan sebagai tamu.

(b.) *Simple Authentication*

Mekanisme ini melakukan autentikasi ke *server* LDAP dengan mengirimkan identitas dirinya yang *valid* berupa *username* dan *password* pada saat *login*. Kemudian melakukan *bind* atau membuka *session* pada koneksi *server* LDAP.

(c.) *Simple Authentication and Security Layer (SASL)*

Untuk mengatasi masalah keamanan pada *simple authentication*, maka digunakan mekanisme ini dengan cara melakukan *enkripsi* pada saluran transmisi. Hal ini didukung dengan adanya *Secure Socket Layer (SSL)*.

2.) Ruang Lingkup LDAP

Menurut R. Fibrian (2011:2), Terdapat empat hal yang harus diperhatikan untuk mempelajari LDAP serta dapat mengimplementasikan suatu layanan direktori menggunakan LDAP, empat hal yang dimaksud adalah sebagai berikut:

(a.) LDAP *Namespace*

Menjelaskan tentang pemberian nama-nama pada layanan LDAP.

(b.) LDAP *Operation*

Menjelaskan tentang operasi-operasi yang dapat dilakukan dan yang terjadi pada protokol LDAP.

(c.) LDAP *Schema*

Menjelaskan tentang penggunaan dan penentuan tipe dari informasi yang akan dimasukkan pada sebuah objek.

(d.) LDAP *Management*

Menjelaskan tentang pembangunan layanan LDAP yang handal seperti kemampuan manajemen *entry*, *replication*, *referral* dan sebagainya.

3.) Operasi Protokol LDAP

Menurut R. Fibrian Satya Putera (2011:3), Pada protokol LDAP, terdapat operasi yang dibagi menjadi 3 kategori yaitu:

(a.) Operasi interogasi

- *Search* : Merupakan operasi pencarian *entry* dalam *direktory* yang sesuai dengan kriteria yang diberikan pada *filter* pencarian.
- *Compare* : Operasi membandingkan informasi yang diberikan oleh klien dengan informasi yang disimpan di dalam *direktory*.

(b.) Operasi *update*

- *Add* : operasi membuat *entry* atau atribut baru.
- *Delete* : operasi menghapus *entry* atau atribut.
- *Modify* : operasi mengubah atribut dalam sebuah *entry*.

(c.) Operasi *authentication* dan *control*

- *Bind* : operasi validasi sebuah *entry* didalam *direktory*.
- *Unbind* : mengizinkan klien mengakhiri *session*.
- *Abadon* : operasi menggagalkan operasi yang sebelumnya dilakukan oleh klien.

4.) LDAP *Data Interchange Format (LDIF)*

Menurut R. Fibrian (2011:4), *LDAP Data Interchange Format (LDIF)* merupakan *format* bahasa untuk merepresentasikan *entry* pada layanan *direktory* yang dapat dibaca oleh manusia. LDIF merupakan format teks dan *binary* dan dapat digunakan untuk *impor* dan *ekspor* ini *entry* ada layanan *direktory*. Oleh karena ini berbasis teks maka dapat dengan mudah dibuat dengan menggunakan bermacam-macam *editor* teks.

5.) *OpenLDAP*

Menurut R. Fibrian Satya Putera (2011:4), *OpenLDAP* adalah *software open source* yang mengimplementasikan protokol LDAP yang tersedia secara gratis dan terbuka. Terdapat dua buah

server yang ada dalam paket *OpenLDAP-servers* yaitu : *Standalone LDAP Daemon (slapd)* dan *Standalone LDAP Update Replication Daemon (slurpd)*. *Slapd* adalah *standalone LDAP server*, sedangkan *slurpd daemon* digunakan untuk sinkronisasi perubahan-perubahan dari suatu *server LDAP* ke *server LDAP* lainnya dalam suatu jaringan.

Paket-paket *software openLDAP* terdiri dari beberapa *library* dan *tool* berikut ini:

- (1.) *OpenLDAP* : Berisi *library-library* yang diperlukan untuk menjalankan aplikasi *openLDAP server* dan aplikasi klien.
- (2.) *OpenLDAP-clients* : Berisi perangkat dalam bentuk perintah *command line* untuk menampilkan dan memodifikasi *directory* data suatu *server LDAP*.
- (3.) *OpenLDAP-servers* : Berisi aplikasi *server* dan *utility* lainnya yang diperlukan untuk mengkonfigurasi dan menjalankan *server LDAP*.

6.) PhpLDAPAdmin

PhpLDAPAdmin adalah sebuah perangkat lunak yang sudah tersedia secara gratis dan merupakan sebuah proyek *opensource* dari *sourceforge*. PhpLDAPAdmin menggunakan aplikasi *browser* sebagai sarana untuk mengakses. Karena phpLDAPAdmin ini

merupakan aplikasi untuk mengelola LDAP *directory*, maka fungsi-fungsi yang dimiliki adalah spesifik untuk LDAP.

7.) Parameter-Parameter *Atribut User*

Tabel berikut merupakan parameter yang akan digunakan sebagai *atribut* saat pendefinisian setiap *user*.

Tabel 3.2 parameter *atribut user*

<i>Key</i>	<i>Content</i>
<i>Cn</i>	<i>Full name</i>
<i>Gn</i>	<i>First name</i>
<i>Sn</i>	<i>Last name</i>
<i>Mail</i>	<i>E-mail</i>
<i>postalAddress</i>	<i>Address</i>
<i>Title</i>	<i>Job title</i>
<i>L</i>	<i>city</i>
<i>O</i>	<i>Organization</i>
<i>Ou</i>	<i>Department</i>
<i>St</i>	<i>State</i>
<i>postalCode</i>	<i>postalCode (business)</i>
<i>telephoneNumber</i>	<i>Telephone (business)</i>
<i>facsimileTelephoneNumber</i>	<i>Fax (business)</i>
<i>Pager</i>	<i>pager</i>
<i>Mobile</i>	<i>Mobile phone</i>
<i>homePhone</i>	<i>Telephone (home)</i>
<i>Comment</i>	<i>Comment</i>
<i>URL</i>	<i>URL (business)</i>
<i>displayName</i>	<i>NickName</i>
<i>Initials</i>	<i>initials</i>

(Sumber : Askari (2010:217))

3.1.15. *Captive Portal*

Captive portal adalah suatu teknik autentikasi dan pengamanan data yang lewat dari jaringan internal ke jaringan eksternal. *Captive portal* sebenarnya merupakan mesin *router* atau *gateway* yang

memproteksi atau tidak mengizinkan adanya trafik, hingga pengguna melakukan registrasi. Biasanya *captive portal* ini digunakan pada infrastruktur *wireless* seperti *hotspot area*, tapi tidak menutup kemungkinan diterapkan pada jaringan kabel.

Cara kerja *carptive portal* adalah pada saat seorang pengguna berusaha untuk melakukan *browsing* ke *Internet*, *captive portal* akan memaksa pengguna yang belum terotentikasi untuk menuju ke halaman autentikasi dan akan di beri fasilitas *login* untuk menghubungi sebuah *server* autentikasi untuk mengetahui identitas dari pengguna yang ingin tersambung ke *Internet*.

3.1.16. Bandwidth Management

Menurut Rafiudin (2008:96), *Bandwidth management* adalah serangkaian mekanisme kontrol yang menilai data alokasi, penundaan variabilitas, tepat waktu pengiriman, dan kehandalan pengiriman dalam mengelola jalur *internet* agar kecepatannya menjadi efektif dan efisien. Dengan *bandwidth management*, kita dapat mengatur *bandwitdh* sesuai dengan kebutuhan.

3.1.17. Sistem Operasi Fedora

Fedora adalah Sistem Operasi berbasis *Linux*, kumpulan perangkat lunak yang membuat komputer Anda dapat berjalan. Anda dapat menggunakan *Fedora* sebagai tambahan, atau sebagai pengganti, sistem operasi lainnya seperti *Microsoft Windows*TM atau *Mac OS X*TM.

Sistem Operasi *Fedora* sepenuhnya bebas biaya untuk Anda nikmati dan bagikan.

Proyek pengerjaan *Fedora* dimulai dari akhir tahun 2003 sejak *Red Hat Linux* secara resmi dihentikan. *Fedora* dijadikan alat percobaan untuk menciptakan generasi *Red Hat Linux Enterprise* yang lebih unggul dan layak jual. *Red Hat Enterprise Linux* sendiri adalah distro *Linux* yang didukung secara resmi oleh *Red Hat*, sementara *Fedora* menjadi distro komunitas.

3.2. Hasil Penelitian Terdahulu

Hasil penelitian terdahulu yang mendukung penelitian ini adalah sebagai berikut:

Tabel 3.3 Hasil Penelitian Terdahulu

Judul	Penulis	Metodologi	Keterangan
1. Membangun Infrastruktur IT Menggunakan Squid Sebagai Proxy Server (Studi Kasus Universitas Sahid Surakarta)	Puky Sulistyono, Didiek S. Wiyono, Bambang Harjito	-Observasi : pengamatan langsung terhadap jaringan internet dari institusi pendidikan. -Interview : pengumpulan data dengan tanya jawab melalui beberapa milis di internet. -Studi literatur : pengumpulan data baik dari buku maupun artikel yang didapatkan dari perpustakaan , internet	Pengguna proxy server dapat menghemat akses internet, tidak dapat mengakses website yang mengandung trojan, worm, pornografi. dapat dikonfigurasi sebagai caching proxy server, url filtering protokol http dan autentikasi pengguna akses internet.

Judul	Penulis	Metodologi	Keterangan
2. Sistem otentikasi terpusat berbasis <i>lightweight directory access protocol</i>	R.Fibrian Satya Putera, Adian Fatchur Rochim, Yuli Christiyono.	- Observasi : pengamatan langsung terhadap jaringan internet dari institusi pendidikan. -Interview : pengumpulan data dengan tanya jawab melalui beberapa milis di internet.	Sistem otentikasi terpusat yang menggunakan <i>server LDAP</i> pada layanan <i>samba-PDC</i> , <i>captive portal</i> , <i>weblog</i> , <i>email</i> , dan web portal.

Membangun Infrastruktur IT Menggunakan *Squid* Sebagai *Proxy Server*

Tidak adanya pembatasan pengguna akses *internet* dan *bandwith* terbatas yang di miliki di rasa perlu di cari solusi untuk menanggulangi hal tersebut. *Proxy server* adalah sebuah *server* yang dapat dikonfigurasi untuk beberapa hal yaitu sebagai *cache server*, *url filtering*, pengaturan *bandwith*, autentikasi akses *internet* dan lain sebagainya.

Pengguna *proxy server* dapat menghemat akses *internet*, tidak dapat mengakses *website* yang mengandung *trojan*, *worm*, pornografi. dapat dikonfigurasi sebagai *caching proxy server*, *url filtering* protokol *http* dan autentikasi pengguna akses *internet*.

Dalam penyelesaiannya, digunakan *squid cache proxy server* sebagai *software proxy server* yang dikonfigurasi sebagai *caching proxy server*, *url filtering* protokol *http* dan autentikasi pengguna akses *internet* sehingga hanya civitas akademika yang dapat mempergunakan akses *internet*.

Berdasarkan uraian diatas dapat diambil kesimpulannya, bahwa *proxy server* dapat difungsikan sebagai *caching proxy server* sehingga dapat menghemat dan mempercepat akses *internet*, difungsikan sebagai *url filtering protocol* http sehingga *website* yang mengandung trojan, virus dan lain sebagainya tidak dapat di akses dan difungsikan sebagai autentikasi akses *internet* sehingga hanya civitas akademika Universitas Sahid Surakarta yang dapat menggunakan akses *internet*.

Sistem Otentikasi Terpusat Berbasis *Lightweight Directory Access Protocol*

Sistem otentikasi terpusat yang melayani proses pembuktian identitas seseorang akan sangat berguna apabila terdapat banyak aplikasi yang membutuhkan proses otentikasi. Sistem ini memerlukan satu buah *user identity* yang unik untuk seorang *user* yang disimpan dalam sebuah *credential store*. Otentikasi dari semua aplikasi yang ada diatur oleh sebuah *server* otentikasi (*Central Authentication Services*) yang menangani validasi dan otorisasi *user identity* yang tersimpan dalam *server* yang menyimpan informasi *user* tersebut.

Salah satu metode otentikasi yang sering digunakan saat ini adalah otentikasi berbasis *Lightweight Directory Access Protocol* (LDAP). Dengan LDAP, pengguna bisa dimudahkan dalam pemakaian kata sandi, dimana pengguna hanya mengingat satu kata sandi saja untuk banyak aplikasi. Akan tetapi pengguna tetap harus memasukkan nama dan kata sandi pada saat akan melakukan otentikasi pada masing-masing aplikasi.

Lightweight Directory Access Protocol (LDAP) adalah sebuah protokol yang mengatur mekanisme pengaksesan layanan direktori yang dapat digunakan untuk mendeskripsikan banyak informasi seperti informasi tentang seseorang, organisasi, komputer dan banyak entitas lainnya. LDAP menggunakan model *client-server*, dimana klien mengirimkan *identifier* data kepada *server* menggunakan protokol TCP/IP dan *server* mencoba mencarinya pada DIT (*Directory Information Tree*) yang tersimpan di *server*. Bila di temukan maka hasilnya akan dikirimkan ke klien tersebut namun bila tidak maka hasilnya berupa *pointer* ke *server* lain yang menyimpan data yang di cari.

BAB IV

METODE PENELITIAN

4.1. Lokasi Dan Waktu Penelitian

4.1.1. Lokasi Penelitian

Lokasi penelitian skripsi dilakukan pada Bidang Badan Ketahanan Pangan Provinsi Sumatera Selatan di Jln. Kol. H. Barlian Km. 6 No. 82 Telp. 410488 – 417790 Fax. (0711) 410488 – 413434 Palembang 30153.

Alasannya mengambil penelitian skripsi pada Badan Ketahanan Pangan (BKP) Prov. Sumsel di karenakan sebelumnya penulis telah melakukan penelitian laporan praktek kerja lapangan di tempat ini, sehingga penulis telah memahami permasalahan pada jaringan yang ada.

4.1.2. Waktu Penelitian

Waktu penelitian dimulai dari bulan Maret tanggal 1 sampai 30 Maret 2012.

4.2. Jenis Data

Penulis dalam skripsi ini menggunakan beberapa metode dalam pengumpulan data yang terdiri dari:

4.2.1. Data Primer

Data Primer adalah data yang dikumpulkan untuk penelitian dari tempat aktual terjadinya peristiwa. Data primer ini dapat

berbentuk isian kuesioner, jawaban langsung dari responden atau karyawan berdasarkan masalah yang dikaji, dan dengan mengamati peristiwa.

Data primer tersebut didapat oleh Penulis secara langsung dari satuan kerja teknologi Informasi pada Badan Ketahanan Pangan, melalui pihak-pihak yang dapat membantu dalam mendapatkan data yang dibutuhkan, berupa : sistem jaringan yang digunakan disana dan permasalahan yang sering terjadi terutama dalam jaringan komputer.

4.2.2. Data Sekunder

Data Sekunder adalah data yang diperoleh melalui sumber yang ada, yaitu data yang telah ada dan tidak perlu dikumpulkan sendiri oleh peneliti.

4.3. Teknik Pengumpulan Data

4.3.1. Observasi

Observasi atau metode pengamatan merupakan suatu metode pengumpulan data yang dilakukan dengan mengamati langsung objek yang akan diteliti dan kemudian mencatatnya secara sistematis.

Metode ini dilakukan penulis dengan cara mengamati secara langsung hal-hal yang berhubungan dengan jaringan komputer seperti ikut membantu memperbaiki permasalahan jaringan komputer, serta mengamati permasalahan yang dihadapi para

karyawan khususnya dibidang pemanfaatan jaringan komputer pada Badan Ketahanan Pangan (BKP).

4.3.2. Wawancara

Metode wawancara merupakan metode pengumpulan data dengan cara melakukan wawancara atau tanya jawab secara langsung dengan orang yang di wawancarai.

Metode wawancara ini dilakukan Penulis langsung dengan Nova selaku pengendali komputer *server* di BKP (Badan Ketahanan Pangan) Prov.Sumsel.

4.4. Jenis Penelitian

Menurut Arikunto (2006:75) mendefinisikan penelitian eksperimen adalah suatu cara untuk mencari hubungan sebab akibat (hubungan kausal) antara dua faktor yang sengaja ditimbulkan oleh peneliti dengan mengeliminasi atau mengurangi atau menyisihkan faktor-faktor lain yang mengganggu.

4.5. Alur Proses dan Teknik Pengembangan Sistem

4.5.1. Alur Proses

1.) Proses kerja sistem yang di buat

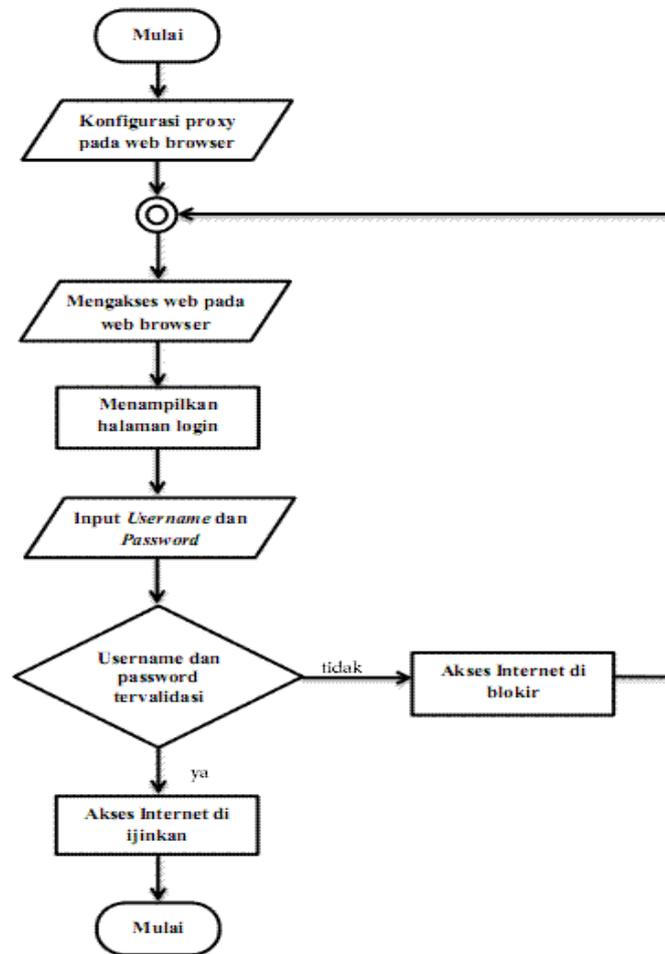
Untuk mempermudah penjelasan maka penulis membuat skenario sebagai berikut:

(a.) Komputer yang berperan sebagai *proxy server* dan *LDAP server* adalah komputer *gateway*.

- (b.) Komputer *gateway* memiliki dua *interfaces network*, yaitu eth0 dan eth1, eth0 terhubung langsung dengan modem ADSL, dan eth1 terhubung ke jaringan lokal.
- (c.) *Proxy server* tidak menerapkan *transparent proxy* (otentikasi tidak dapat diterapkan dalam mode ini).
- (d.) Agar tidak ada *user* yang dapat mengakses *internet* (http) secara langsung melalui *proxy* atau *gateway* maka pada komputer *gateway* diterapkan kebijakan *firewall* yang memblok semua akses http (port 80) secara langsung dari LAN ke *internet*. Hal ini dimaksudkan agar *user* mau tidak mau harus menyetel “*connection setting*” pada *web client* dengan setingan “*manually use proxy*” dan menggunakan *proxy* yang telah di terapkan.
- (e.) Skenario *filtering proxy* hanya mengijinkan koneksi dari LAN ke *internet*, dengan ketentuan harus *login* terlebih dahulu menggunakan *user account* yang terdaftar di LDAP.
- (f.) Jika proses autentikasi berhasil yakni *user* terdaftar di dalam *database server* LDAP, maka *squid server* akan mengizinkan *user* tersebut untuk mengakses *internet*.

2.) Skenario Autentikasi Pada *Captive Portal*

Captive portal dibangun dengan memanfaatkan layanan *proxy* dari aplikasi *squid*, untuk menggunakan layanan *proxy* serta ingin terhubung ke jaringan *Internet* harus dilakukan suatu konfigurasi dan proses autentikasi terlebih dahulu.



Gambar 4.1 *Flowchart* autentikasi pada *captive portal*

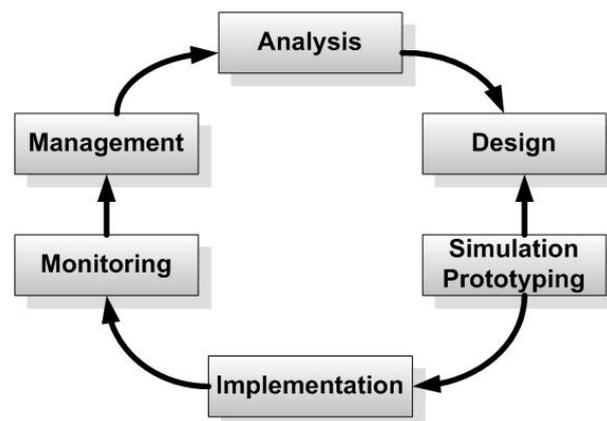
Penjelasan dari *flowchart* di atas:

- (1). Konfigurasi penggunaan *proxy* pada *web browser* atau bagian pengaturan jaringan pada sistem operasi.
- (2). Mencoba untuk mengakses sebuah halaman *web* pada *web browser*.
- (3). Permintaan untuk melakukan *login* dengan harus memasukkan *username* dan *password*.

- (4). Apabila validasi *username* dan *password* berhasil maka akses *internet* atau halaman *web* akan diizinkan akan tetapi apabila gagal maka permintaan akses akan ditolak.

4.5.2. Teknik Pengembangan Sistem

Pada penulisan skripsi kali ini, penulis menggunakan metode (*Network Development Life Cycle*) NDLC dalam mengusulkan rancangan pengembangan sistem *Authentication proxy server* berdasarkan *user* LDAP pada Badan Ketahanan Pangan Prov.Sumsel.



Gambar 4.2 *Network Development Life Cycle* (NDLC)

(Sumber : *Applied Data Communications, A business-Oriented Approach*, James E. Goldman, Philips T. Rawles, Third Edition, 2001, John Wiley & Sons : 470)

1.) *Analysis*

Tahap *analysis* bertitik-tolak pada kegiatan-kegiatan dan tugas-tugas dimana sistem yang berjalan dipelajari lebih mendalam untuk menjadi landasan bagi sistem yang baru akan dibangun. Salah satu tujuan penting dari tahap ini adalah untuk mendefinisikan sistem berjalan.

2.) *Design*

Dari data-data yang didapatkan sebelumnya, tahap *design* ini akan membuat gambar desain topologi jaringan interkoneksi yang akan dibangun. Diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada. Desain bisa berupa desain struktur topologi, desain akses data, desain layout perkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang proyek yang akan dibangun.

3.) *Simulation Prototype*

Beberapa pekerja jaringan akan membuat dalam bentuk simulasi dengan bantuan *tools* khusus di bidang *network* seperti *Boson*, *Packet Tracert*, *Netsim*, dan sebagainya. Mensimulasikan jaringan yang akan dibangun dengan *tools* seperti *boson netsim* merupakan salah satu solusi yang dilakukan oleh seorang *network designer*.

4.) *Implementation*

Implementasi merupakan tahapan yang sangat menentukan dari berhasil atau gagalnya proyek yang akan dibangun dan ditahap inilah *team work* akan diuji dilapangan untuk menyelesaikan masalah teknis dan non teknis. Ada beberapa Masalah-masalah yang sering muncul pada tahapan ini, diantaranya:

- (a.) Jadwal yang tidak tepat karena faktor-faktor penghambat.
- (b.) Masalah dana/anggaran dan perubahan kebijakan.
- (c.) *Team work* yang tidak solid.
- (d.) Peralatan pendukung dari vendor makanya dibutuhkan manajemen proyek dan manajemen resiko untuk meminimalkan sekecil mungkin hambatan-hambatan yang ada.

5.) *Monitoring*

Setelah implementasi tahapan monitoring merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari *user* pada tahap awal analisis, maka perlu dilakukan kegiatan *monitoring*. *Monitoring* bisa berupa melakukan pengamatan pada:

- (a.) Infrastruktur *hardware*: dengan mengamati kondisi reliability/kehandalan sistem yang telah dibangun ($reliability = performance + availability + security$);
- (b.) Memperhatikan jalannya paket data di jaringan (pewaktuan, *latency*, *peektime*, *throughput*);
- (c.) Metode yang digunakan untuk mengamati kondisi jaringan dan komunikasi secara umum secara terpusat atau tersebar;
- (d.) Pendekatan yang paling sering dilakukan adalah pendekatan *Network Management*. Dengan pendekatan ini banyak perangkat baik yang lokal dan tersebar dapat dimonitor secara utuh.

6.) *Management*

Pada level manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah kebijakan (*policy*). Kebijakan perlu dibuat untuk membuat/mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur *reliability* terjaga. *Policy* akan sangat tergantung dengan kebijakan level management dan strategi bisnis perusahaan tersebut. IT sebisa mungkin harus dapat mendukung atau *alignment* dengan strategi bisnis perusahaan.

BAB V

HASIL DAN PEMBAHASAN

5. Hasil dan Pembahasan

5.1. *Analysis*

Dari hasil pengamatan penulis, Badan Ketahanan Pangan (BKP) prov.Sumsel telah menggunakan sistem komputerisasi yang terkoneksi ke jaringan *internet speedy* dimana sistem jaringan yang ada di rasa kurang baik karena koneksi *internet* tidak terbagi dengan rata. Selain permasalahan itu, penggunaan akses *internet* yang dimiliki instansi pun di rasa kurang tepat dilakukan oleh *user* sehingga membuat kenyamanan *user-user* memakai akses *internet* lainnya terganggu dalam berselancar di *internet*.

Integritas dan saling ketergantungan sebuah *service* dengan *service* lain di *server* merupakan hal yang sangat dibutuhkan untuk memudahkan seluruh aktifitas berkaitan dengan *server* yang sedang dikelola.

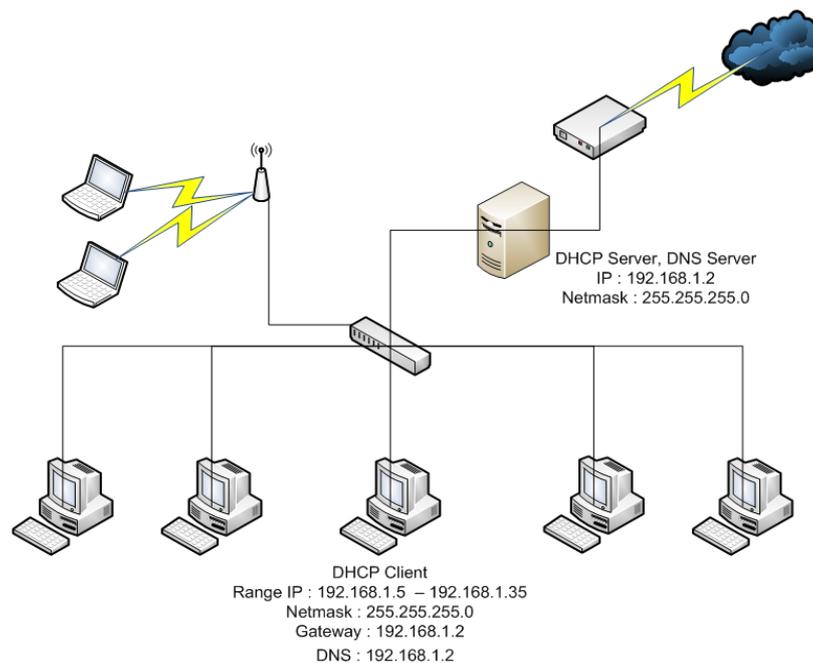
Oleh karena itu penulis membuat sistem ini, karena *proxy server* merupakan sebuah *server* yang dapat dikonfigurasi untuk beberapa hal yaitu sebagai *cache server*, *url filtering*, pengaturan *bandwidth*, serta autentikasi akses *internet*. Proses autentikasi pengguna *proxy server* akan diterapkan hanya di tujukan pada pengguna yang terdaftar dalam protokol LDAP saja. Proses ini tentu saja akan membuat Sistem

Informasi menjadi lebih aman dan memudahkan *System Administrator* dalam menentukan *privilege* bagi pengguna *proxy server*.

5.2. Design

5.2.1. Topologi jaringan yang digunakan

Dari hasil riset yang dilakukan penulis, sistem operasi yang digunakan adalah *Windows Server 2003*, dan menggunakan *service* DHCP dan DNS pada *server*. Topologi jaringan yang ada pada BKP Prov.Sumsel dapat dilihat pada gambar 5.1 :

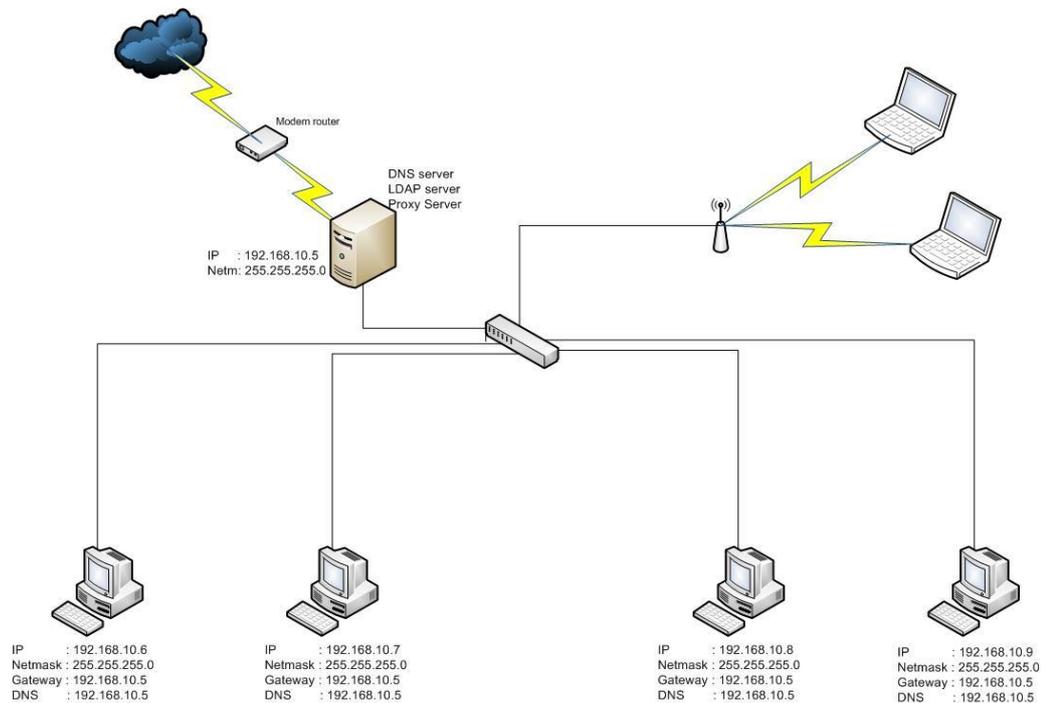


Gambar 5.1 Topologi Jaringan yang digunakan
(Sumber : Badan Ketahanan Pangan Prov.Sumsel)

5.2.2. Topologi jaringan yang di usulkan

Perubahan topologi jaringan yang di usulkan pada Badan Ketahanan Pangan dengan hanya menambah layanan *proxy server* dan protokol LDAP *server* pada komputer *server* dengan

menggunakan 2 kartu jaringan dimana eth0 terhubung ke *internet* dan eth1 untuk jaringan lokal, seperti pada Gambar 5.2 :



Gambar 5.2 Topologi yang diusulkan

(Sumber : Diolah sendiri)

5.3. Simulation Prototype

5.3.1. Spesifikasi Komputer yang digunakan

Komputer yang digunakan sebagai *server* pada Badan Ketahanan Pangan Prov.Sumsel memiliki spesifikasi sbb :

Processor : *Intel Core 2 Duo E7400 2.8 Ghz*

Memory : *DDR3 2 GB*

Harddisk : *160 GB*

Sietem Operasi : *Fedora Core 15*

Komputer yang digunakan sebagai *client* pada BKP Prov.Sumsel memiliki spesifikasi sebagai berikut:

Processor : *Intel Dual Core 2.0 Ghz*

Memory : *DDR2 1 GB*

Harddisk : *80 GB*

Sistem Operasi : *Windows XP Profesional Service pack 3*

5.3.2. Teknologi Jaringan

Teknologi jaringan yang digunakan dalam penulisan skripsi ini :

1.) *LAN Card*

Kartu jaringan yang digunakan adalah TP-Link TF-320 *PCI Fast Ethernet Adapter*.

2.) *Switch*

Switch yang digunakan adalah D-Link Des-1008A.

3.) *Kabel LAN*

Kabel LAN yang digunakan adalah kabel *Straight*.

5.4. Implementation

5.4.1. Konfigurasi IP dan DNS Server

Implementasi sistem ini menggunakan 2 kartu jaringan dimana NIC1 di *assign* untuk ke *internet* sedangkan NIC2 di *assign* untuk jaringan lokal.

Tahapan pertama melakukan konfigurasi IP *server* di NIC2 yaitu:

```
IP : 192.168.10.5
Netmask : 255.255.255.0/24
```

Gambar 5.3 Konfigurasi IP *server*

Kemudian *install* paket-paket yang diperlukan dibawah ini dengan perintah yaitu:

```
yum install nama-paket
```

Gambar 5.4 Perintah *install* paket

Paket-paket yang perlu di *install* dalam *implementasi* sistem ini adalah :

```
bind-utils
bind
bind-libs
bind-chroot
openldap-servers
openldap-clients
httpd
php-mbstring
php-ldap
phpldapadmin-1.2.0.4
squid
```

Gambar 5.5 Aplikasi yang dibutuhkan

Setelah paket *bind* diatas telah di *install* lalu mengedit *file* di *resolv.conf* dengan menambah *domain* dan *ip server*

```
#cd /etc/resolv.conf
search bkp-sumsel.go.id
nameserver 192.168.10.5
```

Gambar 5.6 Edit *resolv.conf*

Setelah itu mengkonfigurasi *file named.conf*

```
#cd /etc/named.conf
options {
directory "/var/named/";
};
zone "bkp-sumsel.go.id" IN {
type master;
file "db.bkp";
};
zone "10.168.192.in-addr.arpa" IN {
type master;
file "db.192";
};
```

Gambar 5.7 *Named.conf*

Setelah konfigurasi di *named.conf* selesai , lalu buat dan konfigurasi *file zone forward* dan *reverse* di *folder named*

```
#nano /var/named/db.bkp
$TTL 3H
bkp-sumsel.go.id. IN SOA      bkp-sumsel.go.id.
root.bkp-sumsel.go.id. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )  ; minimum
@      IN      NS      bkp-sumsel.go.id.
ns     IN      A       192.168.10.5
@      IN      A       192.168.10.5
www    IN      A       192.168.10.5
ldap   IN      CNAME   bkp-sumsel.go.id.

#nano /var/named/db.192
$TTL 1D
@      IN SOA      bkp-sumsel.go.id. root.bkp-
sumsel.go.id. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )  ; minimum
@      IN      NS      bkp-sumsel.go.id.
5      IN      PTR     bkp-sumsel.go.id.
5      IN      PTR     ldap.bkp-sumsel.go.id.
```

Gambar 5.8 *File forwar dan reverse*

Lalu *restart bind* dengan perintah:

```
#/etc/init.d/named restart
```

Gambar 5.9 *Restart bind*

5.4.2. Konfigurasi LDAP Server

Setelah konfigurasi DNS *server* selesai dan tidak ada masalah, selanjutnya menginstal dan konfigurasi LDAP *server*. Aplikasi yang digunakan adalah *OpenLDAP*, *Install* paket *openldap-servers* dan *openldap-clients* dengan perintah:

```
#yum install openldap-servers openldap-clients
```

Gambar 5.10 *Install paket ldap*

Setelah instalasi selesai, berikutnya kita akan konfigurasi LDAP *client*, terlebih dahulu melakukan *backup file* konfigurasi *default* dengan cara :

```
#cp /etc/openldap /etc/openldap/ldap.conf.default
```

Gambar 5.11 *Copy file ldap.conf*

Lalu *edit file* konfigurasi *ldap.conf*

```
#nano /etc/openldap/ldap.conf
# LDAP Defaults
# See ldap.conf(5) for details
# This file should be world readable but not world
writable.

BASE dc=bkp-sumsel,dc=go,dc=id
URL ldap://ldap.bkp-sumsel.go.id:389

#SIZELIMIT 12
#TIMELIMIT 15
#DEREF never
TLS_CACERTDIR /etc/openldap/cacerts
```

Gambar 5.12 Konfigurasi *ldap.conf*

Kemudian langkah selanjutnya adalah membuat *password* *user admin* sebagai *administrator* dengan perintah :

```
#slappasswd
New password:
Re-enter new password:
{SSHA}h94LbFbnTEkLoP4MlerYKxV6iZxAobFe
```

Gambar 5.13 Membuat *password* *ldap server*

Setelah selesai membuat *password admin*, *copy password* yang *dienkripsi* tersebut karena akan dibutuhkan pada saat mengkonfigurasi *LDAP server* di *file slapd.conf*.

Selanjutnya Buka dan *edit file* konfigurasi *slapd.conf* di */etc/openldap*, berikut konfigurasinya:

```
#nano /etc/openldap/slapd.conf
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.

include          /etc/openldap/schema/corba.schema
include          /etc/openldap/schema/core.schema
include          /etc/openldap/schema/cosine.schema
include          /etc/openldap/schema/duaconf.schema
include          /etc/openldap/schema/dyngroup.schema
include          /etc/openldap/schema/inetorgperson.schema
include          /etc/openldap/schema/java.schema
include          /etc/openldap/schema/misc.schema
include          /etc/openldap/schema/nis.schema
include          /etc/openldap/schema/openldap.schema
include          /etc/openldap/schema/ppolicy.schema
include          /etc/openldap/schema/collective.schema

# Allow LDAPv2 client connections.  This is NOT the default.
allow bind_v2

# Do not enable referrals until AFTER you have a working
directory
pidfile          /var/run/openldap/slapd.pid
argsfile         /var/run/openldap/slapd.args

client software
database         bdb
suffix           "dc=bkp-sumsel,dc=go,dc=id"
checkpoint       1024 15
rootdn           "cn=Admin,dc=bkp-sumsel,dc=go,dc=id"
rootpw           {SSHA}Jfnp6WhD0F80FveVARx179y+75BnXTUF
```

```

directory    /var/lib/ldap

# Indices to maintain for this database
index objectClass          eq,pres
index ou,cn,mail,surname,givenname    eq,pres,sub
index uidNumber,gidNumber,loginShell  eq,pres
index uid,memberUid        eq,pres,sub
index nisMapName,nisMapEntry          eq,pres,sub

# enable monitoring
database monitor

# allow onlu rootdn to read the monitor
access to *
        by dn.exact="cn=Admin,dc=bkp-sumsel,dc=go,dc=id" read
        by * none

```

Gambar 5.14 Konfigurasi *slapd.conf*

Langkah selanjutnya *copy paste file DB_CONFIG* yang ada didalam folder */usr/share/openldap/* kedalam */var/lib/ldap*.

Lalu jalankan LDAP *server* dengan perintah :

```
# /etc/init.d/slapd start
```

Gambar 5.15 Menjalankan ldap

Penulis akan membuat dan menyimpan seluruh *file ldif* di *direktori /etc/openldap/*. Pertama kali yang dilakukan adalah dengan memasukkan sebuah *entry* baru untuk organisasi yang akan digunakan.

```

#nano /etc/openldap/base_all.ldif
dn:dc=bkp-sumsel,dc=go,dc=id
objectclass: top
objectclass: dcObject
objectclass: organization
o: bkpsumsel
dc: bkp-sumsel

```

Gambar 5.16 Membuat *entry* organisasi

Lalu mengeksekusi *file base_all.ldif* tersebut untuk menambahkan organisasi kedalam *database* LDAP dengan perintah berikut :

```
#ldapadd -x -W -D `cn=Admin,dc=bkp-sumsel,dc=go,dc=id`
-f base_all.ldif
```

Gambar 5.17 Mengeksekusi *file base_all.ldif*

Setelah menggunakan perintah diatas, akan diminta *password* LDAP *server* kita yang telah dibuat diawal tadi.

Setelah itu membuat sebuah *file* *struktur_organisasi.ldif* yang isinya dimaksudkan untuk membuat organisasi *unit* yang berada di bawah organisasi yang telah dibuat tadi lalu tambahkan kedalam *database* LDAP dengan perintah sama seperti diatas.

```
#nano /etc/openldap/struktur_organisasi.ldif
dn: ou=subbag keuangan,dc=bkp-sumsel,dc=go,dc=id
objectclass: top
objectclass: organizationalUnit
ou:subbag keuangan

dn: ou=subbag keamanan pangan,dc=bkp-
sumsel,dc=go,dc=id
objectclass: top
objectclass: organizationalUnit
ou:subbag keamanan pangan

dn: ou=subbag umum kepegawaian,dc=bkp-
sumsel,dc=go,dc=id
objectclass: top
objectclass: organizationalUnit
ou:subbag umum kepegawaian
```

Gambar 5.18 Membuat organisasi *unit*

Kemudian membuat *file user* yang dimaksudkan untuk ditujukan pada organisasi *unit* dimana *user* tersebut berada.

dibawah ini penulis membuat satu *user* yang berada di organisasi *unit* subbag keuangan.

```
#nano /etc/openldap/subbag_keuangan.ldif
#Meli michelasari member dari subbag keuangan
dn: cn=meli michelasari, ou=subbag keuangan, dc=bkp-
sumsel,dc=go,dc=id
objectclass: top
objectclass: person
objectclass: inetOrgPerson
cn: meli michelasari
sn: sari
mail: sari@yahoo.co.id
postalAddress: Jl.Demang lebar daun Lr.Ogan No.1512
l: Palembang
st: Sumatera selatan
o: bkpsumsel
ou: subbag keuangan
postalCode: 30144
telephoneNumber: +6285380701111
displayName: meli michelasari
userPassword: michelasari
title: member of subbag keuangan
initials: mm
```

Gambar 5.19 Membuat *user* subbag keuangan

Lalu masukkan *user* tersebut kedalam *database* LDAP dengan perintah :

```
#ldapadd -x -W -D 'cn=Admin,dc=bkp-sumsel,dc=go,dc=id'
-f subbag_keuangan.ldif.ldif
```

Gambar 5.20 Add *user* subbag keuangan

Setelah *entry* data-data diatas berhasil dimasukkan kedalam *direktori* LDAP *server*, lakukan pengecekan untuk melihat data-data yang telah di *add* tadi dengan perintah:

```
#ldapsearch -x -b 'dc=bkp-sumsel,dc=go,dc=id'
```

Gambar 5.21 Melihat data yang di *input*

5.4.2.1. Konfigurasi phpLDAPAdmin

PhpLDAPAdmin digunakan untuk melakukan pengaturan menggunakan GUI bagi seorang LDAP Administrator.

Pertama *install webserver* untuk manajemen ldap server.

```
# yum install httpd php-mbstring php-ldap
```

Gambar 5.22 *Install webserver*

Setelah *webserver* di *install* lalu konfigurasi *file httpd.conf* dan *edit* pada *DocumentRoot* dan *Directory* seperti Gambar 5.23:

```
#nano /etc/httpd/conf/httpd.conf
DocumentRoot "/var/www/html/phpldapadmin-1.2.0.4"
<Directory "/var/www/html/phpldapadmin-1.2.0.4">
```

Gambar 5.23 *Edit file httpd.conf*

Menginstall phpLDAPAdmin sebagai halaman utama dari *webserver* di */var/www/html*

```
# unzip phpldapadmin-1.2.0.4.zip -d /var/www/
#cp /var/www/phpldapadmin-1.2.0.4 /var/www/html -R
```

Gambar 5.24 *Install phpldapadmin*

Setelah itu mengcopy *file* konfigurasi phpLDAPAdmin

```
#cp/var/www/html/phpldapadmin-
1.2.0.4/config/config.php.example
/var/www/html/phpldapadmin-1.2.0.4/config/config.php
```

Gambar 5.25 *Copy file config.php*

Lalu mengkonfigurasi phpLDAPAdmin pada bagian seperti Gambar 5.26 :

```
#nano /var/www/html/phpldapadmin-1.2.0.4/config/config.php
/*****/
/* Define your LDAP servers in this section */
/*****/

$servers = new Datastore();
$servers->newServer('ldap_pla');
$servers->setValue('server','name','bkp-sumsel LDAP Server');
$servers->setValue('server','host','ldap.bkp-sumsel.go.id');
$servers->setValue('server','port',389);
$servers->setValue('login','auth_type','session');
$servers->setValue('login','bind_id','cn=Admin,dc=bkp-
sumsel,dc=com');
$servers->setValue('login','bind_pass','');
$servers->setValue('server','tls',false);
```

Gambar 5.26 konfigurasi file config.php

5.4.3. Konfigurasi Squid

Dalam skripsi ini penulis menggunakan paket *Squid Proxy*

Server version 3.1 :

```
# yum install squid
```

Gambar 5.27 Install squid

Konfigurasi pertama adalah mengkonfigurasi komputer yang akan menjadi *proxy server* sebagai *internet sharing (gateway)*, yaitu sebagai berikut:

Enable IP Forwarding, Untuk memForwardkan IP dari dua kartu jaringan.

```
## nano /etc/sysctl.conf
net.ipv4.conf.default.rp_filter = 1
```

Gambar 5.28 Enable forward IP

Lalu konfigurasi *IPtables* sebagai berikut:

```
#nano /etc/sysconfig/iptables
iptables -P FORWARD ACCEPT
iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o em1 -j
MASQUERADE
iptables -t nat -A PREROUTING -p tcp -s 192.168.10.5/24 --
dport 80 -j REDIRECT --to-ports 3128
```

Gambar 5.29 Konfigurasi *IPtables*

Baris kedua dari *IPtables* di atas bermaksud melakukan *source* NAT atau *translation* semua paket yang keluar dari *eth0* yang terhubung ke *modem speedy* sehingga semua *client* di LAN bisa akses *internet*. Sedangkan baris ketiga pada *IPtables* di atas bermaksud mengalihkan semua paket yang masuk ke *eth1* dari LAN yang menuju port 80 (*port web server*) ke *port Squid* yaitu port 3128. Tanpa baris ini maka fungsi *Squid* sebagai *proxy server* tidak akan bekerja.

Kemudian gunakan perintah dibawah ini untuk menjalankan otomatis *IPtables* pada saat komputer dihidupkan :

```
#chkconfig iptables on
```

Gambar 5.30 Mengaktifkan *IPtables* saat *booting*

Selanjutnya melakukan konfigurasi *Squid* dengan perintah :

```
# nano /etc/squid/squid.conf
```

Gambar 5.31 Konfigurasi *squid*

Selanjutnya adalah bagian-bagian dari konfigurasi *squid* sebagai berikut:

```
http port 3128
```

Gambar 5.32 *Port squid*

Adalah *port http* yang digunakan oleh *squid* yang merupakan *port defaultnya*.

```
cache_dir ufs /var/spool/squid 10240 32 512
```

Gambar 5.33 *Direktory cache*

Tag *cache_dir* diatas digunakan untuk menetapkan direktori *cache*, tipe dan juga ukurannya. Semua *object* yang harus di *cache* akan disimpan dalam ruang *disk* yang lokasinya ditetapkan oleh *tag* ini. *ufs* adalah format *storage squid*. 10240 adalah ukuran *space disk* yang akan digunakan *squid* untuk menyimpan hasil *caching*, dalam hal ini adalah ukuran kapasitas direktori */home/cache/*. 32 adalah untuk menentukan jumlah subdirektori *level* pertama, dan 512 untuk menentukan jumlah subdirektori *level* kedua.

```
Auth_param basic program /usr/lib/squid/squid_ldap_auth -
b "dc=bkp-sumsel,dc=go,dc=id" -f "cn=%s" -s sub -h
192.168.10.5 -p 389 -D

auth_param basic children 5
auth_param basic realm squid proxy-caching web server
auth_param basic credentialsttl 2 hours
```

Gambar 5.34 Skema untuk autentikasi

Tag diatas merupakan konfigurasi agar menggunakan *backend* LDAP untuk autentikasinya. *Auth_param* digunakan untuk melepas parameter ke beragam skema autentikasi, membuat para *user* dapat di autentikasi dalam beragam cara. skema *basic* dengan parameter “*program*” digunakan sebagai menetapkan perintah untuk authenticator eksternal. Program ini akan membaca baris yang memuat “*username password*” dan melakukan *reply* “OK” atau

“*ERROR*”. Kemudian menetapkan nama *realm* untuk dilaporkan ke *client* untuk skema autentikasi *basic*.

```

acl SSL_ports port 443 563 # https, snews
acl SSL_ports port 873 # rsync
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 563 # https, snews
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl Safe_ports port 631 # cups
acl Safe_ports port 873 # rsync
acl Safe_ports port 901 # SWAT

```

Gambar 5.35 *Port-port ACL*

Config diatas menerangkan bahwa ACL didefinisikan untuk *port-port* yang biasa diakses oleh *user*.

```

acl purge method PURGE
acl CONNECT method CONNECT

```

Gambar 5.36 *ACL Purge dan method*

Acl purge method PURGE menjelaskan bahwa *acl* untuk definisikan metode *PURGE* (penggagalan/pembersihan jejak akses) terhadap suatu *request* dari sumber/tujuan akses. *Acl CONNECT method CONNECT* menerangkan bahwa *acl* dengan nama *CONNECT* memiliki metode *CONNECT* biasanya digunakan untuk koneksi SSL.

Berikut adalah baris *Traffic Policy* yang mendefinisikan aturan boleh atau tidaknya akses dari suatu ACL (di atas) untuk mengakses *HTTP request*.

```

http_access allow manager localhost
http_access deny manager
http_access allow purge localhost
http_access deny purge
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
http_reply_access allow all
icp_access allow all

```

Gambar 5.37 Baris *traffic policy*

Config diatas menjelaskan bahwa *http_access allow manager localhost* yaitu mengizinkan akses *localhost* dari *manager*, *http_access deny manager* yaitu menolak semua akses dari *manager*, *http_access allow purge localhost* yaitu mengizinkan metode pembatalan akses dari *localhost*, *http_access deny purge* yaitu tolak semua akses metode pembatalan, *http_access allow localhost* yaitu mengizinkan *localhost* mengakses *http*, *Icp_access allow all* yaitu memperbolehkan akses ICP. selanjutnya *http_reply_access* merupakan direktif yang mengatur / mendefinisikan akses terhadap konten yang akan direspon oleh *server web* kepada *client* yang memiliki *request* terhadap suatu konten dari *website* tersebut.

Dibawah ini ada beberapa skema *acl*, yang pertama adalah *ACL bebas* yang merupakan *IP server* dan *IP* yang digunakan *admin*. *ACL user* merupakan *IP* yang di *setting* untuk *client-client* yang terhubung ke akses *http* dan akan di autentikasi berdasarkan *user* yang telah terdaftar dalam *LDAP*. Dan untuk *ACL lost* itu merupakan *IP* yang tidak di *setting* untuk *client*, sehingga penulis tidak memberi akses *http* melalui *IP* tersebut.

```

acl bebas src 192.168.10.4-192.168.10.5
acl user src 192.168.10.6-192.168.10.252
acl lost src 192.168.10.1-192.168.10.3
acl blockurl dstdomain "/etc/squid/blok.txt"
acl haram dstdomain "/etc/squid/porno.txt"
acl blokteks url_regex -i "/etc/squid/bloktext.txt"
acl kerja1 time MTWHF 07:00-12:00
acl kerja2 time MTWHF 13:00-17:00
acl ldap proxy_auth REQUIRED
acl user_network src 192.168.10.0/24
http_access deny blockurl user_network kerja1
http_access deny blockurl user_network kerja2
http_access deny haram user
http_access deny blokteks user
http_access deny lost
http_access allow bebas
http_access allow user ldap
http_access allow user_network ldap
icp_access allow all
always_direct allow all
coredump_dir /var/spool/squid

acl admin src 192.168.10.4-192.168.10.5
acl server src 192.168.10.5/255.255.255.255

```

Gambar 5.38 Acl tambahan

Selanjutnya simpan dan cek konfigurasi *squid*. Setelah semua selesai di konfigurasi lakukan *restart* pada *bind*, *webserver*, *ldap*, dan *squid*.

```

# /etc/init.d/named restart
Starting named: [OK]

# /etc/init.d/httpd restart
Starting httpd: [OK]

# /etc/init.d/slaped restart
Starting slapd: [OK]

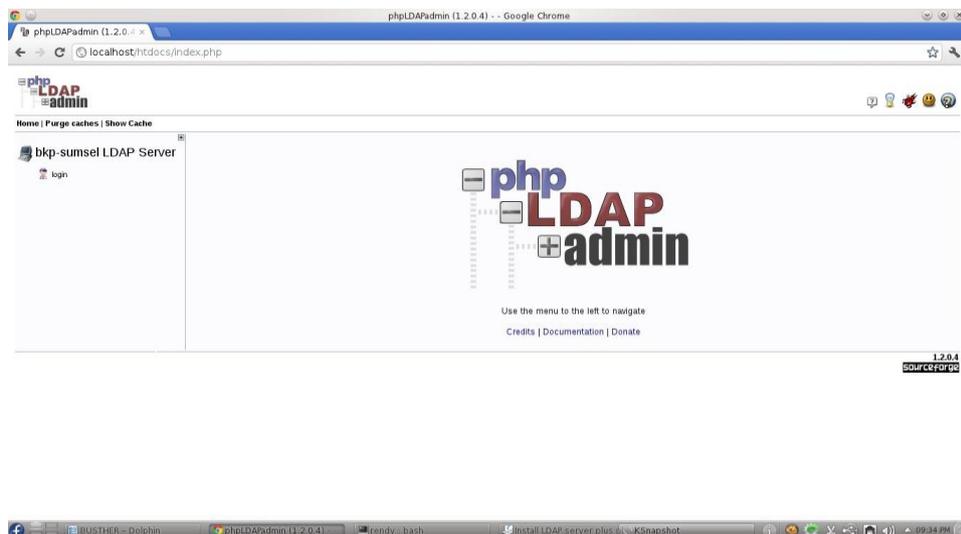
# /etc/init.d/squid start
Starting squid: [OK]

```

Gambar 5.39 Restart paket

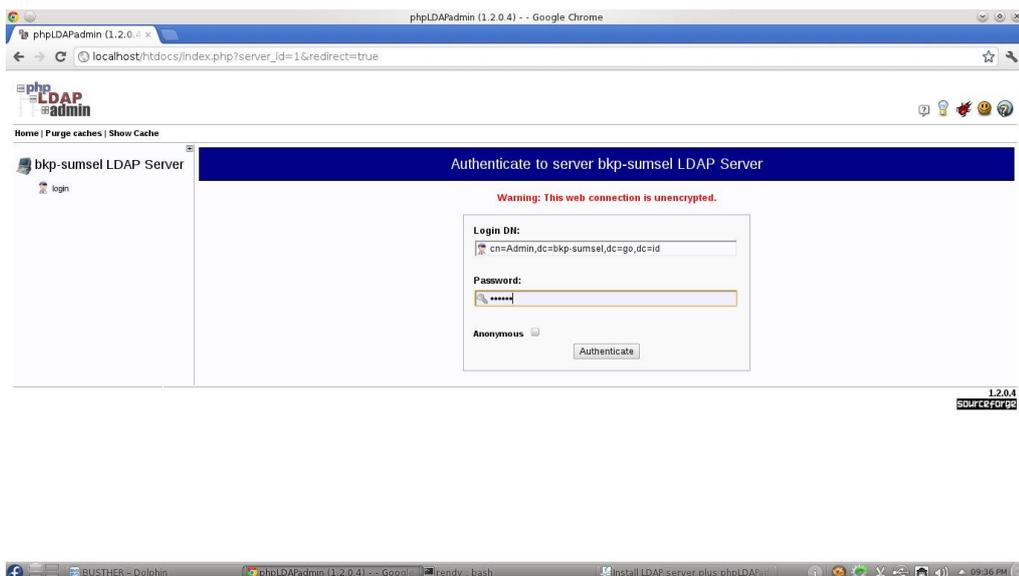
5.4.4. Pengujian LDAP *server* menggunakan phpLDAPAdmin

Untuk menjalankan phpLDAPAdmin bisa menggunakan *browser* dengan mengetikkan *localhost* pada *address bar*.



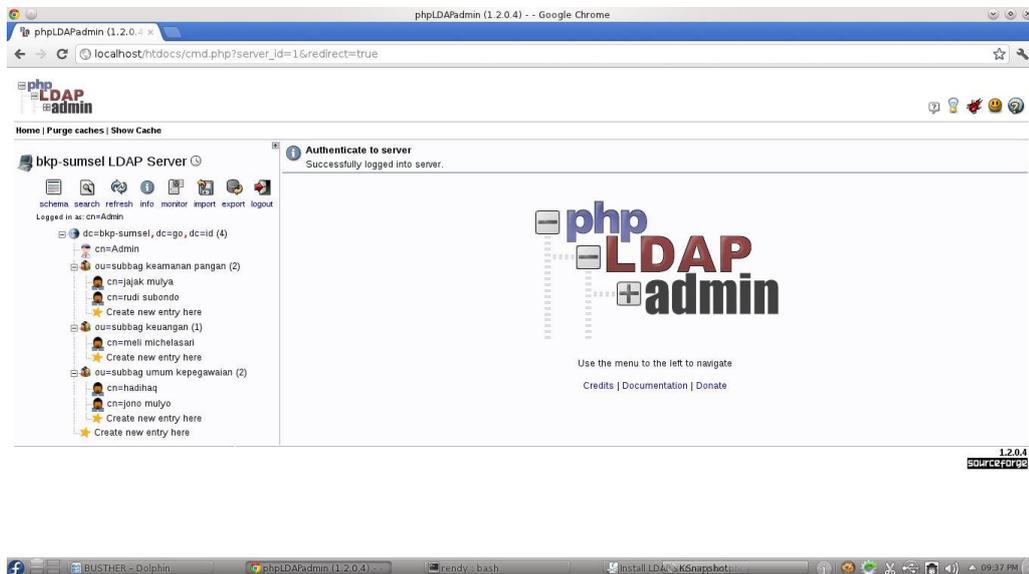
Gambar 5.40 Membuka *phpldapadmin*

Lalu klik *login* dan isi kolom *password* sesuai dengan *password* LDAP *server*



Gambar 5.41 *Login phpldapadmin*

Jika *login* berhasil maka akan tampil seperti Gambar 5.42 :



Gambar 5.42 Phpldapadmin sukses

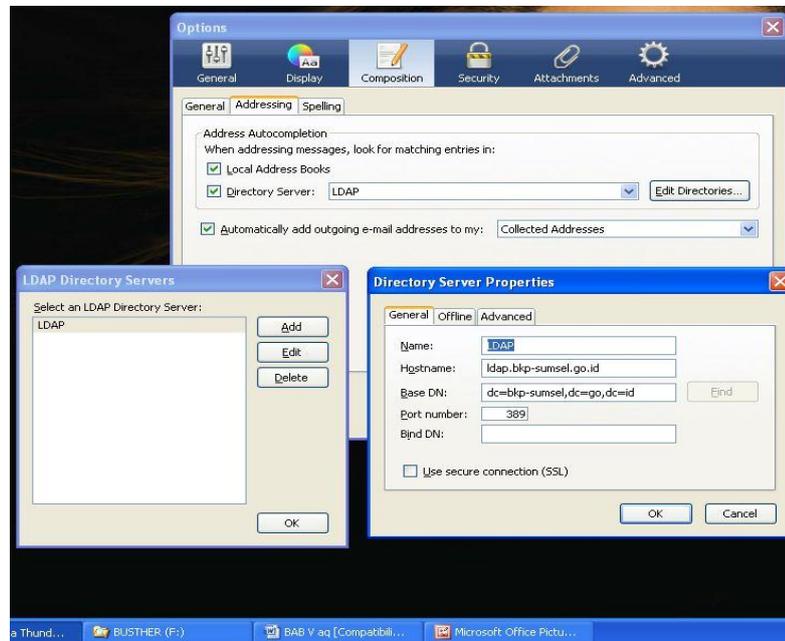
5.4.5. Pengujian Pada *Client*

LAN pada *client* di *setting manual proxy* yaitu dari 192.168.10.6 - 192.168.10.252 *netmask* : 255.255.255.0 dengan *gateway* 192.168.10.5 dan DNS *server*: 192.168.10.5

5.4.5.1. Pengujian LDAP *server* pada *client*

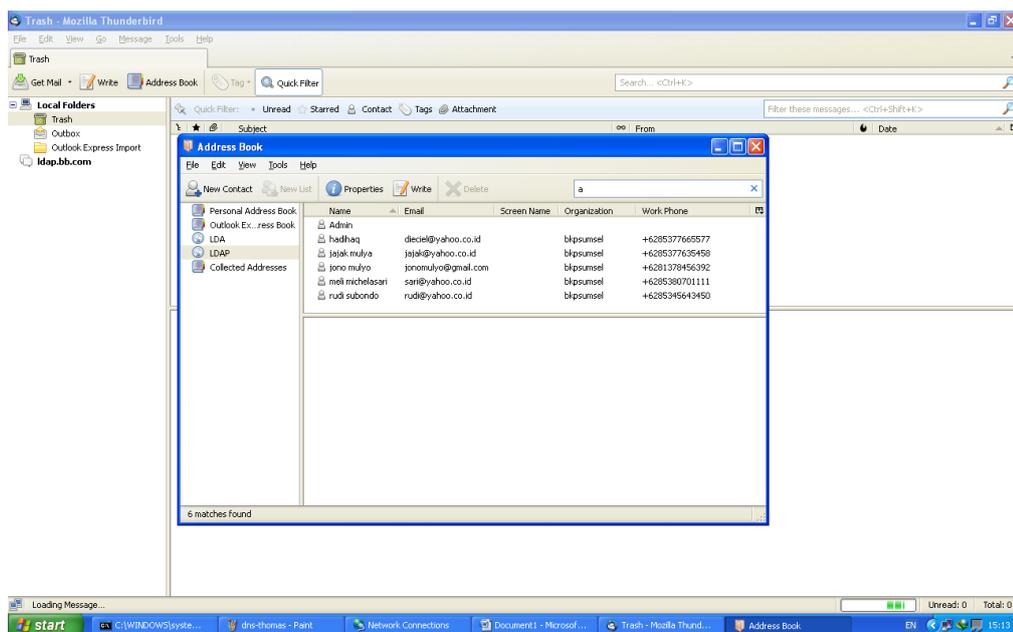
Pengujian LDAP pada komputer *client* yang menggunakan sistem operasi *windows xp* menggunakan aplikasi *Mozilla thunder bird* dengan memanfaatkan *address book*. Langkah pertama membuka *mozilla thunder bird* – *tools* – *options* lalu klik *edit directorie*. Untuk *hostname* itu merupakan URL yang sudah dikonfigurasi dari *file ldap.conf*

dan *Base DN* merupakan *domain* atau *Dbase* yang telah dibuat dan dikonfigurasi di *LDAP server*.



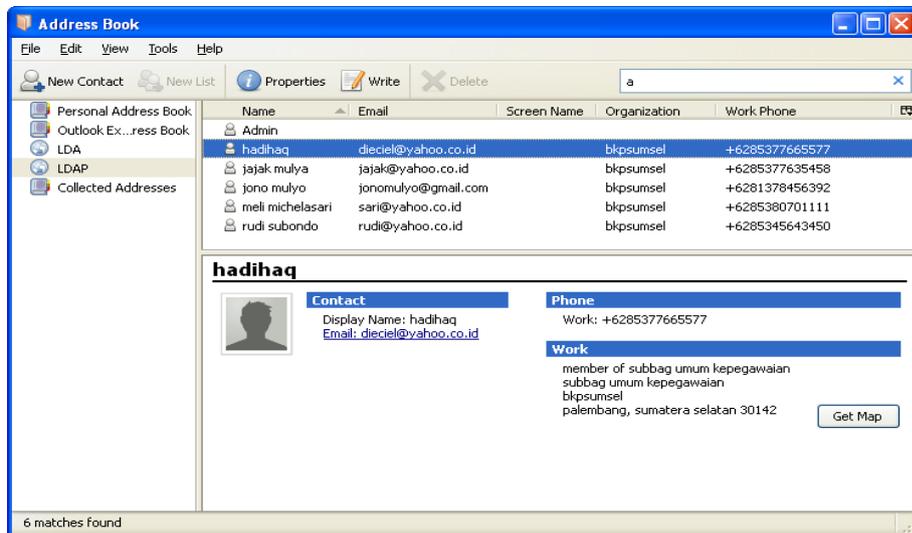
Gambar 5.43 Setting address book mozilla thunder bird

bila tidak ada kesalahan maka akan tampil seperti Gambar 5.44 :



Gambar 5.44 Tampilan user LDAP

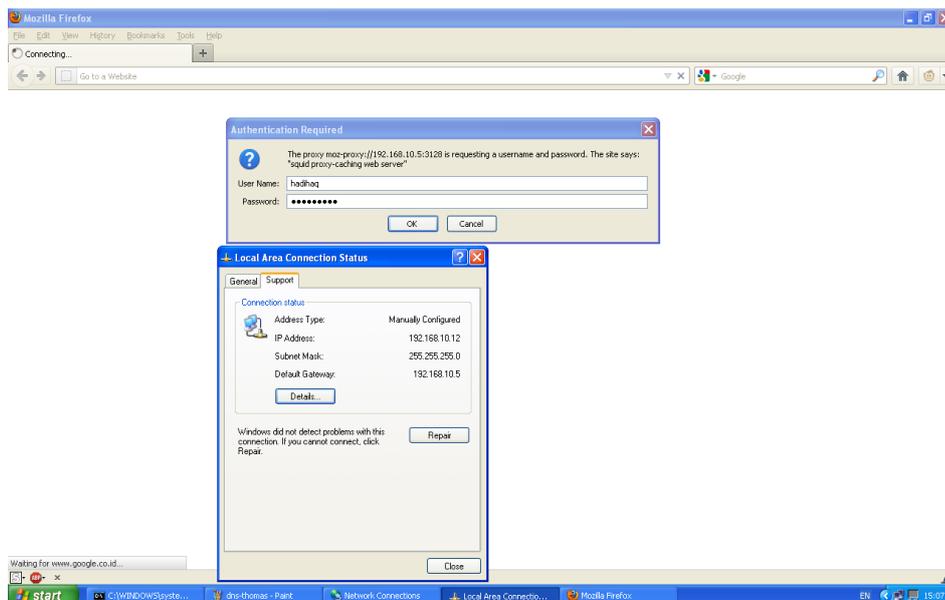
Gambar 5.45 menunjukkan informasi salah satu *user* LDAP



Gambar 5.45 Informasi salah satu *user* LDAP

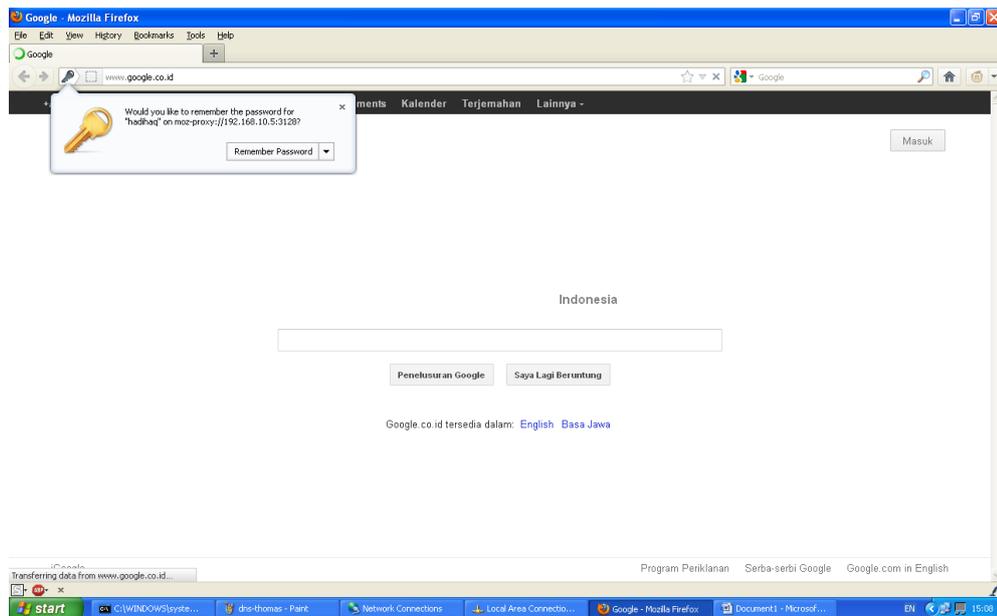
5.4.5.2. Pengujian Authentikasi *Captive Portal*

Pengujian autentikasi *captive portal* menggunakan *browser mozilla*. Tampilan gambar 5.46 pada saat *client* yang terhubung ke *internet* mencoba akses http.



Gambar 5.46 Proses autentikasi

Tampilan dibawah ini merupakan *user* yang berhasil *login* berdasarkan *user* dan *password* yang telah terdaftar dan di konfigurasi di LDAP *server*.



Gambar 5.47 Autentikasi berhasil

BAB VI

PENUTUP

6.1. Kesimpulan

Ada beberapa kesimpulan yang dapat diambil dari hasil desain dan implementasi serta pengujian :

- 1.) Proses autentikasi menggunakan *server* LDAP dilakukan dengan operasi *bind* dan *search*. Operasi *bind* dilakukan pada saat pemanggilan dan validasi identitas dan operasi *search* dilakukan pada saat pengambilan nilai atribut yang diinginkan dari sebuah *entry*.
- 2.) Pada skripsi ini rancangan skema dan *namespace* disesuaikan dengan lingkungan Badan Ketahanan Pangan (BKP) Prov.Sumsel.
- 3.) *OpenLDAP* membutuhkan aplikasi berbasis GUI (*Graphical User Interface*) untuk memudahkan dalam hal manajemen *entry* oleh pihak administrator. Aplikasi yang digunakan adalah *phpLDAPadmin*.
- 4.) Autentikasi pada layanan *captive portal* membutuhkan informasi *username* dan *password* yang terdapat di dalam *server* LDAP.

6.2. Saran

Adapun saran yang dapat diberikan untuk menjadi masukan pada penelitian lebih lanjut adalah:

- 1.) Pengembang perangkat lunak dapat mengembangkan aplikasi yang memanfaatkan sistem autentikasi yang disediakan oleh *server* LDAP ini.
- 2.) Layanan LDAP yang telah dibangun dapat ditambahkan fungsi replikasi untuk sinkronisasi data untuk menjaga ketersediaan data.
- 3.) Sistem autentikasi ini dapat di kembangkan menjadi Sistem *Single Sign On* (SSO) untuk beberapa layanan seperti *samba-PDC*, *weblog*, *email*, dan *web* portal.

DAFTAR PUSTAKA

- Arikunto, Suharsimi. *Prosedur Penelitian Suatu Pendekatan Praktik*. Rineka Cipta, Jakarta, 2006.
- Askari Azikin. *Debian GNU/LINUX*. Informatika, Bandung, 2011.
- Dede Sopandi. *Instalasi dan Konfigurasi Jaringan Komputer*. Informatika, Bandung, 2006.
- Iwan Sofana. *CISCO CCNA & jaringan komputer*. Informatika, Bandung, 2010.
- Nana Suarna. *Pengantar (LAN) Local Area Network*. Yrama Widya, Bandung, 2007.
- Puky Sulistyo, Didiek S. Wiyono dan Bambang Harjito. *Membangun Infrastruktur IT Menggunakan Squid Sebagai Proxy Server*. Surakarta, 2007.
- Rahmat Rafiudin. *Squid Koneksi Anti Mogok*. Andi Offset, Yogyakarta, 2008.
- R. Fibrian Putera Satya, Adian Fathur Rochim dan Yuli Christiyono. *Sistem Otentikasi Terpusat Berbasis Lightweight Directory Access Protocol*. Semarang, 2011.
- Wahana Komputer. *Kamus Lengkap Jaringan Komputer*. Salemba Infotek, Jakarta, 2004.
- Wahana Komputer. *Panduan Lengkap Pengembangan Jaringan Linux*. PT. Andi Offset, Yogyakarta, 2005.
- Wagito. *Jaringan Komputer*. Gava Media, Yogyakarta, 2007.
- <http://aalil.com/pengertian-internet.html/> diakses pada tanggal 08 Agustus 2012.
- <http://anneahira.com/pengertian-wawancara.htm/> diakses pada tanggal 08 Agustus 2012.
- <http://cyberkomputer.com/jaringan-komputer/pengertian-dan-fungsi-firewall-dalam-suatu-jaringan-komputer-lan-dan-wan>
- <http://digilib.itb.ac.id/gdl.php?mod=browse&op=read&id=jbptitbpp-gdl-adriansyah-34232/> diakses pada tanggal 08 Agustus 2012.

[http://id.shvoong.com/social-sciences/education/2248611- implementasi-ktsp-
dalam-kurikulum-pendidikan/](http://id.shvoong.com/social-sciences/education/2248611-implementasi-ktsp-dalam-kurikulum-pendidikan/) diakses pada tanggal 08 Agustus 2012.

[http://kambing.ui.ac.id/onnopurbo/oraridiklat/teknik/2.4ghz/wifiadvanced/captive-
portal-11-2003.doc/](http://kambing.ui.ac.id/onnopurbo/oraridiklat/teknik/2.4ghz/wifiadvanced/captive-portal-11-2003.doc/) diakses pada tanggal 07 Agustus 2012.

<http://pengertiandefinisi.com/2012/01/pengertian-observasi.html/> diakses pada
tanggal 08 Agustus 2012.

<http://fedoraproject.org/id/about-fedora#different/> diakses pada tanggal 25
September 2012

<http://scribd.com/doc/18003036/Data-Sekunder-Dan-Primer/> diakses pada tanggal
08 Agustus 2012.