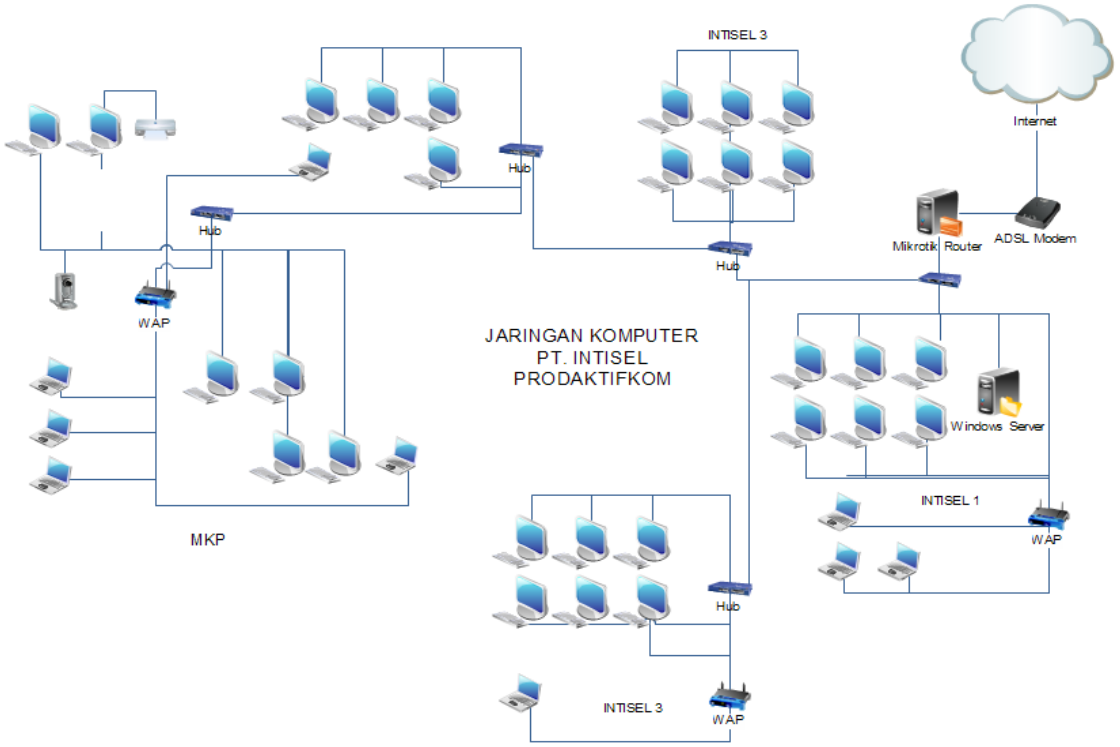
BAB 4
ANALISIS NETWORK SYSTEM DAN SERVER

4.1 NETWORK SYSTEM DAN SERVER

4.1.1 Network Diagram

Pada umumnya pembangunan System Teknologi Informasi tentunya mempunyai pola atau planing untuk membangun sebuah sistem dengan mengilustrasikan Objek yang akan dibangun kedalam sebuah ilustarasi menggunakan berbagai macam metode perancangan sistem. Pada kasus Pengembangan sistem jarigan komputer di PT. Intisel Prodaktifkom , kami mengilustrasikan kedalam sebuah diagram sebagai berikut :



Gambar 4.1.1-1Network diagram

Gambar 4.1.1 Merupakan *Ilustrasi* Diagram Jaringan Komputer yang digunakan oleh PT.Intisel Prodaktifkom .

4.1.2 Network System Clarification

4.1.2.1 Network System Requirement Clarification

Data Network System Requirement PT. Intisel Prodaktifkom pada tahap analisis sebagai berikut :

1. Hardware / Perangkat Keras :
   - PC Server
   - PC Router (4 ethernet Card)
   - PC Client
   - D-Link ADSL
   - D-Link WAP
   - D-Link Switch
   - Kabel UTP

2. Sistem Operasi Jaringan :
   - Windows Server 2000
   - Windows OS
   - Microtik OS Router
   - D-Link Software Inside

3. Internet Service Provider (ISP) :
   - Telkom Speedy 2 Mbps
   - Telkom Speedy 512 Kbps
   - Cnet 1 Mbps

Tabel 4.1.2-1 Rincian hardware dan Software

No.	Hardware	Network Operating System	Quantity
1	PC Server	Windows Server 2000	1
2	PC Router	Mikrotik Router	1
3	PC Client	Windows OS + Linux	72
4	Modem ADSL	D-link Router	1
5	Wireless AP	D-link Router	4
6	Switch+Hub	-	8
7	Kabel UTP		

Tabel 4.1.2-2 Rincian Koneksi Internet

No.	ISP	Kecepatan
1	Telkom Speedy	2 Mbps
2	Telkom Speedy	512Mbbps
3	CNet	1Mbps

4.1.2.2 IP Addres & Subnet Clarification

Pengalamatan jaringan komputer di PT.Intisel Prodaktifkom menggunakan Class A dan C dengan rincian sebagai berikut :

Kelas	:	C	A
Network Address	:	192.168.X.XXX	11.12.XX.XX
Rentang IP	:	1	1
		-	-
		-	-
		-	-
		254	7

Subneting IP Address : 255.255.255.0 dan 255.255.255.248

Tabel 4.1.2-3 IP Address dan Subnet

No.	Divisi	Rentang IP	Subnet
1	Div-1	192.168.X.1- 192.168.X.10	255.255.255.0
2	Div-2	192.168.X.11- 192.168.X.21	255.255.255.0
3	Div-3	192.168.X.22- 192.168.X.32	255.255.255.0
4	Div-4	192.168.X.33- 192.168.X.43	255.255.255.0
5	Div-5	192.168.X.44- 192.168.X.54	255.255.255.0
6	Div-6	192.168.X.55- 192.168.X.65	255.255.255.0

7	Div-7	192.168.X.66- 192.168.X.76	255.255.255.0
8	Div-8	192.168.X.77- 192.168.X.87	255.255.255.0
9	Div-9	192.168.X.88- 192.168.X.98	255.255.255.0
10	Div-10	192.168.X.99- 192.168.X.109	255.255.255.0
11	Div-11	192.168.X.100- 192.168.X.110	255.255.255.0
12	Div-12	192.168.X.111- 192.168.X.121	255.255.255.0
13	Div-13	192.168.X.122- 192.168.X.132	255.255.255.0
14	Div-14	192.168.X.133- 192.168.X.143	255.255.255.0
15	Div-15	192.168.X.144- 192.168.X.254	255.255.255.0
16	Div-16	11.12.XX.1-11.12.XX.7	255.255.255.248

4.1.2.3 Network Security Clarification

Software Aplikasi yang di gunakan ialah Mikrotik sebagai pendukung keamanan sistem jaringan dan fitur yang diaplikasikan sebagai layer filtering yakni :

1. IP address blocking

   Ketika MR. x mencoba mencari celah ip address yang kosong lalu mencoba menggunakannya ia masih mengakses jaringan lokal namun tidak dapat mengakses Jaringan Internet.

2. URL Filtering

   Merupakan Fitur keamanan untuk memblokir situs-situs yang di larang oleh Admin.

3. Firewall Management

   Merupakan fitur keamanan lainya seperti Anti Virus, Anti Spyware, Dll.

4. Bandwidth Mangement

   Merupakan fitur Manajemen untuk membatasi Akses Download (DL) dan Upload (UL).

4.1.3 Network System Evaluation

Dari hasil analisa data mengenai System jaringan komputer yang kami peroleh di PT. Intisel Prodaktifkom dapat ditinjau dari tiga aspek sebagai berikut :

1. Operational fee

   Biaya Operasional merupakan aspek yang sangat berpengaruh untuk meminimalisir pengeluaran biaya, Mengapa?? Karena setiap system tentunya tidak selalu *Flat*, terus menerus akan di kembangkan oleh manufacture sistem yang berkaitan dan membutuhkan perawatan yang cukup. Otomatis di setiap pengembangan serta perubahan sistem berkaitan dengan Platform yang sesuai. Jadi, kembali kepada Network Requirement yang kita gunakan.

   Jika di banding kan dengan Open Source Platform lebih Ekonomis jika adanya proses pengembangan sistem khususnya di bidang Jaringan Komputer. Namun prose Migrasi tidak cukup mudah karena membutuhkan pengenalan tentang sistem yang akan di implementasikan.

2. Effectivity

   Standarisasi kebutuhan pada Jaringa Komputer terkait dengan 3 Hal, Yakni :

   1. Apakah proses berjalan dengan lancar??
   2. Apakah Services dan Maintenance seimbang??

3. Apakah Keamanan Jaringan Komputer sudah powerfull??

Jika ketiga hal tersebut sudah terpenuhi maka dapat di katakan system jaringan Komputer suda Effektif.

3. Secure System

Berbicara masalah keamanan sistem Jaringan Komputer ada beberapa hal yang perlu di perhatikan, diantaranya :

a. Physical Secure

Mengapa saya kaitkan dengan Keamanan Fisik?? Karena setiap sistem yang berjalan tak pernah terlepas dari peralatan pendukung yakni *Hardware dan Software*. Keamana fisik cenderung menyerang Hardware sistem entah dari segi lingkungan seperti cuaca, hewan kecil (semut, serangga Dll), ataupun Manusia yang dapat mengakibatkan kerusakan fisik pada hardware sistem.

b. Logical Secure

Logical secure sangat berkaitan tentang proses berjalannya sistem seperti konektifitas, pertukaran data, sampai kepada software sistem. Kendala yang menyerang software sistem tidak terlalu berbahaya, karena jika adanya kerusakan sistem dapat melakukan troubleshooting dengan cara membackup data, akan tetapi jika kendala yang di hadapi berbeda dengan apa yang di inginkan seperti Pencurian data yang di lakukan oleh orang yang tidak bertanggung jawab akan menjadi faktor terbesar pada Logical Secure.

Dari ketiga aspek tersebut dapat di simpulkan bahwa Sistem jaringan komputer tidak terlepas dari Unsur Ekonomi, Efektifitas, dan Keamanan.

4.2 Network Sytem Development

4.2.1 Tujuan Perancangan sistem

Tujuan perancangan yang di usulkan ialah membangun sistem jaringan komputer agar kinerja jaringan lebih *Efektif* serta meningkatkan keamanan sistem yang berjalan yang mencakup :

1. Authentication
2. Access Limitation & Capability
3. CCTV with IP Camera
4. Wireless Access Point (WAP)

4.2.2 Authentication

Pada dasarnya Otentikasi dalam jaringan komputer digunakan sebagai filterisasi terhadap klien yang akan masuk ke zona Internetworking yang telah di sediakan oleh server. Metode otentikasi beragam mulai dari identifikasi identitas ataupun yang lainnya. Pada kasus ini, penulis Membangun Proxy Server Sebagai media Otentikasi jaringan Internal yang akan mengakses ke jaringan eksternal (Internet)

Ilustration : Otentikasi akan Muncul ketika klien mengakses internet dengan Aplikasi Browser seperti, Internet Explorer, Mozilla Firefox, Opera Dll. Dan klien tidak bisa mengakses jaringan tanpa Proxy. Access limitation & Capability

Pada tingkat keamanan selanjutnya ialah Batasan dan kemampuan Akses User atau klien agar akses digunakan sesuai dengan apa yang telah di tentukan oleh server.

Ilustration : server telah menetukan User 1 2 3 dan 5 diperbolehkan mengakses jaringan dan user 4 tidak diberi akses oleh server karena user 4 belum terdaftar di jaringan server. Ketika user 4 mencoba mengakses server akan muncul peringatan “Access Denied” Mesikipun user 4 mengetahui Username & password Proxy. Dengan begitu siapa saja yang mencoba mengakses server tidak akan dapat melewati filterisasi yang telah di tetapkan oleh server.

Tabel 4.2.2-1Ilustrasi IP Address dan MAC Address Klient

Nama	IP Address	MAC Address	Status
User 1	192.168.0.10	5D:H5:AC:3D:54:4F	Allow
User 2	192.168.0.16	8D:G5:6B:3A:54:E1	Allow
User 3	192.168.0.86	7D:A5:7D:3G:54:3F	Allow
User 4	192.168.0.56	3D:A3:1D:G4:54:5C	Denied
User 5	192.168.0.66	1D:E2:4D:3Q:54:4C	Allow

4.2.3 CCTV With IP Camera

Di Era Globalisasi saat ini tentunya tidak heran dengan adanya alat pengintai atau CCTV di setiap Instansi bahkan banyak di setiap rumah yang sudah menggunakannya. Tujuan CCTV tersebut tidak terlepas dari pengamanan lokasi agar kejadian yang tidak

kita ketahui ketika berada diluar lokasi tersebut dapat terekam bahkan sampai termonitor jarak jauh menggunaan akses internet.

Pada kasus ini penulis menggunakan IP Camera D-Link DCS-920 dengan dukungan Software Zoneminder Camera Security di flatform Linux.

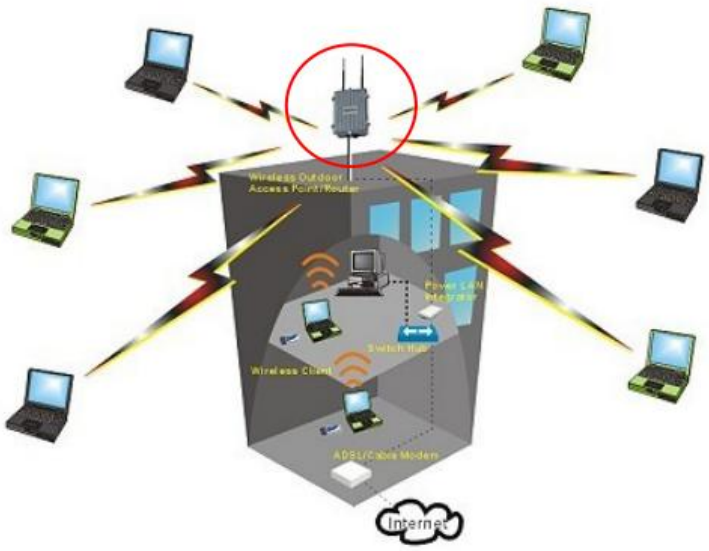
4.2.4 Wireless Access Point (WAP)

Access Point, merupakan perangkat yang menjadi sentral koneksi dari pengguna (user) ke ISP, atau dari kantor cabang ke kantor pusat jika jaringannya adalah milik sebuah perusahaan. Access-Point berfungsi mengkonv ersikan sinyal frekuensi radio (RF) menjadi sin yal digital yan g akan disalurkan melalui kabel, atau disalurkan ke perangkat WLAN yang lain dengan dikonversikan ulang menjadi sinyal frekuensi radio.



Gambar 4.2.4-1 D-link Router + AP

Alat ini sering digunakan sebagai piranti server pada jaringan WLAN. Dan biasanya diletakkan di langit-langit dalam ruangan WLAN indoor. Alat ini dapat menyalurkan data secara wireless dari PC ke PC secara infrastruktur. Access Point (AP) ini disertai adaptor sebagai pencatu daya dari alat tersebut, juga tersedia kabel UTP agar dapat terhubung secara wired dan antena eksternal dengan gain 2,15 dBi. Ada 4 indikator led di bagian depan alat ini yang terdiri dari : power, LAN,WLAN DAN Internet. Led pada power menyala memberitahukan AP tercatu oleh listrik melalui adaptor, led pada LAN menyala memberitahukan bahwa AP terhubung secara wired melalui kabel UTP dan led pada WLAN memberitahukan AP terhubung secara wireless dengan piranti lain.



Gambar 4.2.4-2 Topologi Point to Multiport

4.2.5 Simulasi Jaringan Komputer 1

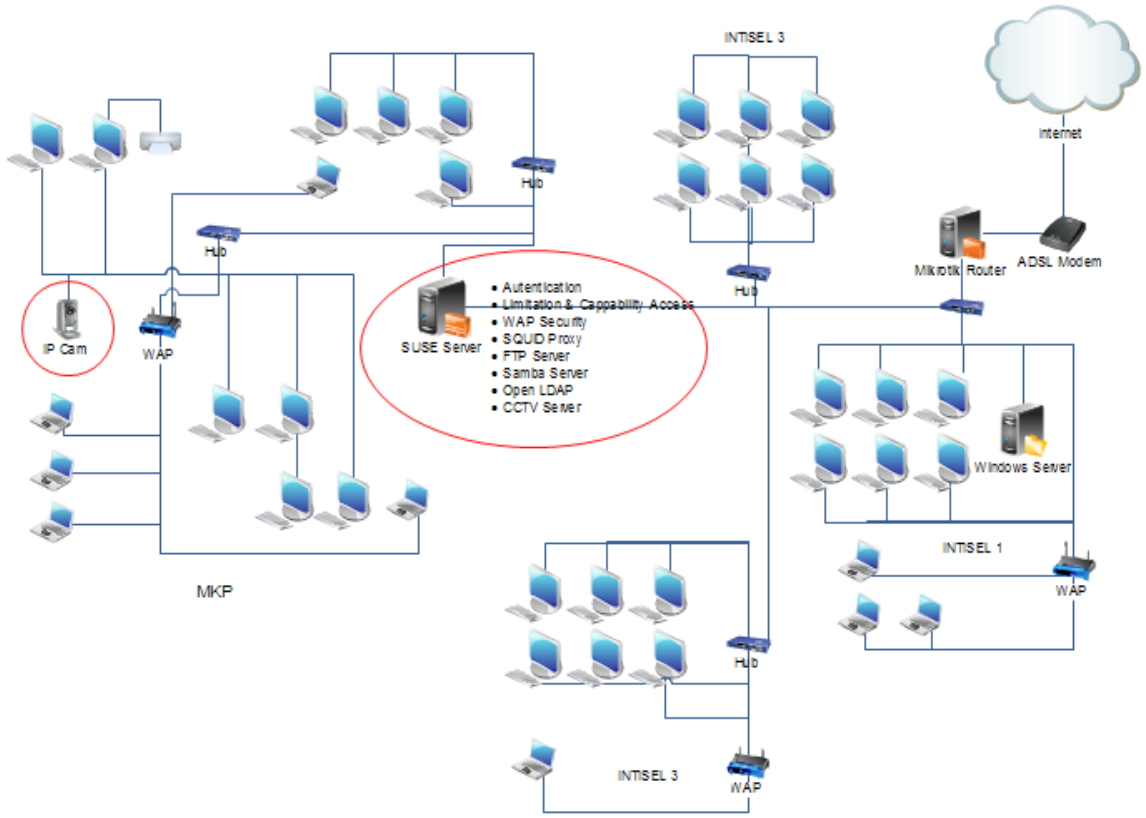
Tujuan perancangan sistem jaringan komputer Plan 1 ialah membangun Server dan Aplikasi Server dengan Linux Server (SUSE 11.2) dalam satu Personal Komputer tanpa menghilangkan komponen sistem (Mikrotik Router) yang berjalan sehingga sistem lama masih dapat bekerja sesuai dengan fungsinya. Plan 1 akan sangat Powerfull jika digunakan untuk Secure Zone (Zona Aman) untuk Jaringan tertentu. Berikut rincian Perbandingan Plan 1 :

Keuntungan :

- system keamanan *sub* jaringan lebih terjaga
- Akses internet lebih cepat karena Server 2 (SUSE Server) menggunakan Squid untuk sub jaringannya . dengan catatan Bandwith yang di berikan seimbang dari Router.

Kelemahan :

- Sebagian Fitur yang di sediakan Oleh SUSE server hanya untuk sub jaringan saja.
- Troubleshooting jaringan relatif lebih sulit.
- Tidak dapat melakukan sharing data terhadap Sub jaringan yang lain hanya di lingkupnya saja.
- Server tidak dapat di Virtual Remote terkecuali koneksi Internet ke Publik di arahkan langsung ke SUSE Server.
- Client dari sub jaringan lain hanya dapa mengakses ke Server saja.



Gambar 4.2.5-1 Network Diagram Rencana 1

4.2.5.1 Network System Requirement & Optional Tools

1. Hardware / Perangkat Keras :

   - 2 PC Server
   - PC Router (4 ethernet Card)
   - PC Client
   - IP Camera
   - D-Link ADSL
   - D-Link WAP
   - D-Link Switch & Hub

- Kabel UTP

2. Sistem Operasi Jaringan :
   - Linux Server
   - Windows Server 2000
   - Windows OS
   - Microtik OS Router
   - D-Link Software Inside

3. Internet Service Provider (ISP) :
   - Telkom Speedy 2 Mbps
   - Telkom Speedy 512 Kbps
   - Cnet 1 Mbps

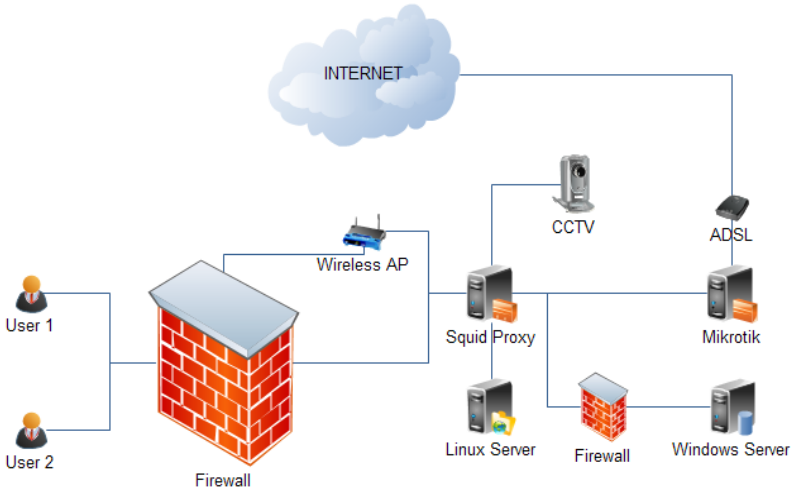
4.2.5.2 klarifikasi Jaringan Komputer 1

Salah satu tujuan yang akan di capai dalam rencana 1 ini ialah membatasi hak akses dan filterisasi bagi para user sesuai dengan kebutuhan user akantetapi fitur yang di sediakan hanya untuk **sub jaringan** saja.

Ilustrasi kegiatan user pada jaringan Internal :

- Semua User akan di filter ketika hendak masuk kedalam jaringan.

- Khusus bagi User yang menggunakan Koneksi Via Wireless akan melakukan dua kali filterisasi WAP Security dan Proxy.
- User 1 sebagai User tertinggi yang dapat menggunakan semua fitur yang di sediakan Oleh Server.
- User 2 hanya di perbolehkan untuk mengakses Internet dan File Server tidak diperbolehkan menggunakan fitur yang lainnya.



Gambar 4.2.5-2 Analisis Diagram Rencana 1

Tabel 4.2.5-1 Analisis Security Fitur

Jenis Koneksi	WAP Filter	IP Address Filter	MAC Address Filter	Autentikasi	Limitation & Cappability Access
Wired (Kabel)	x	√	√	√	√
Wireless	√	√	√	√	√

4.2.5.3 IP Addressing dan Subnetting

Untuk pengalamatan Rencana 1, kami menggunakan kelas A dan C. Kelas A dipakai di subjaringan tertentu (Private) dan untuk kelas C kami bagi kedalam dua sub jaringan dengan rincian sebagai berikut :

Kelas	:	C	C	A
Network Address	:	192.168.X.XXX	192.168.X.XXX	11.12.13.XX
Rentang IP Address	:	1	1	1
		-	-	-
		-	-	-
		-	-	-

254 254 7

Subnet : 255.255.255.0 dan 255.255.255.248

Tabel 4.2.5-2 Rincian pembagian IP Address dan Subneting

No.	Divisi	Rentang IP	Subnet
1	Div-1	192.168.X.1- 192.168.X.10	255.255.255.0
2	Div-2	192.168.X.11- 192.168.X.21	255.255.255.0
3	Div-3	192.168.X.22- 192.168.X.32	255.255.255.0
4	Div-4	192.168.X.33- 192.168.X.43	255.255.255.0
5	Div-5	192.168.X.44- 192.168.X.54	255.255.255.0
6	Div-6	192.168.X.55- 192.168.X.65	255.255.255.0
7	Div-7	192.168.X.66- 192.168.X.76	255.255.255.0
8	Div-8	192.168.X.77- 192.168.X.87	255.255.255.0
9	Div-9	192.168.X.88- 192.168.X.98	255.255.255.0
10	Div-10	192.168.X.99- 192.168.X.109	255.255.255.0
11	Div-11	192.168.X.100- 192.168.X.110	255.255.255.0
12	Div-12	192.168.X.111- 192.168.X.254	255.255.255.0

13	Div-13	192.168.XX.1- 192.168.X.54	255.255.255.0
14	Div-14	192.168.XX.55- 192.168.X.143	255.255.255.0
15	Div-15	192.168.X.144- 192.168.X.254	255.255.255.0
16	Div-16	11.12.XX.1-11.12.XX.7	255.255.255.248

4.2.6 Simulasi Jaringan Komputer 2

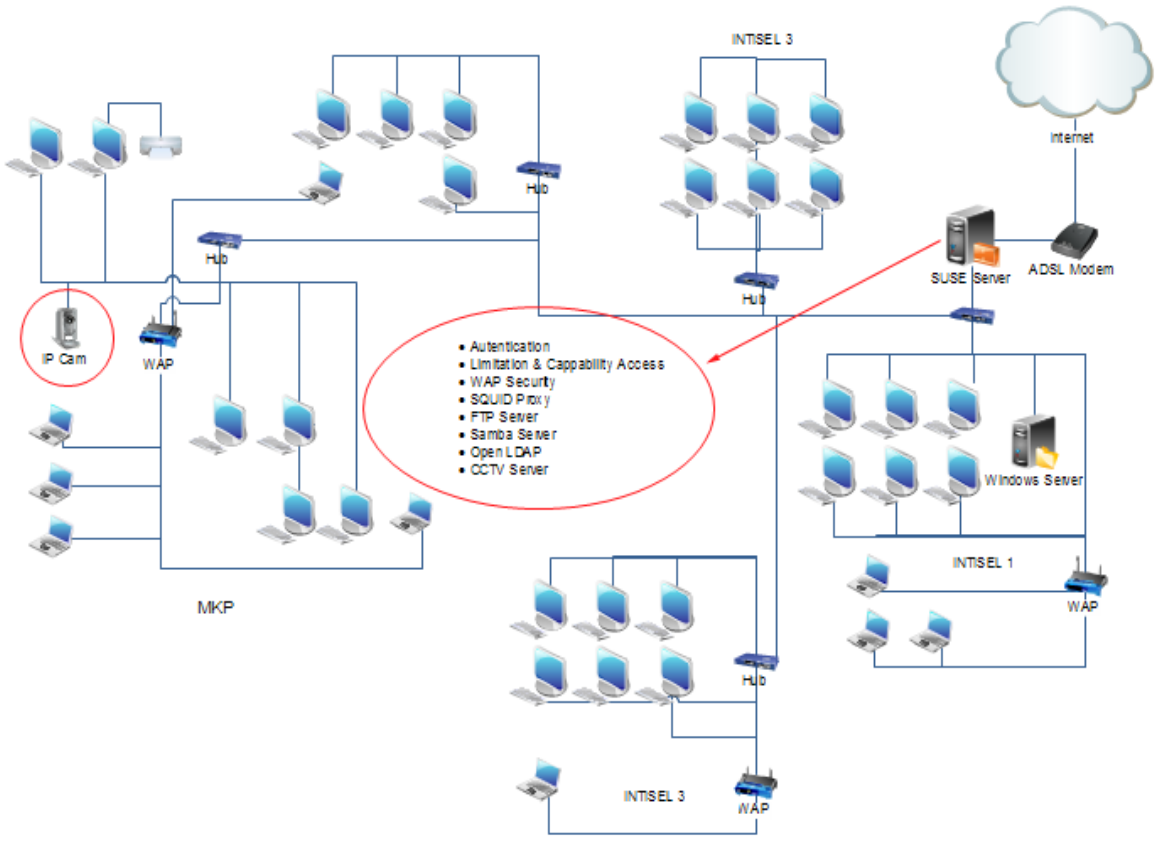
Tujuan dari Plan 2 ialah memindahkan posisi SUSE Server menggantikan Posisi Mikrotik Router namun fungsinya masih sama ialah Server dan Aplikasi Server dengan Linux Server (SUSE 11.2) dalam satu Personal Komputer. Plan 2 menggabungkan jaringan menjadi satu jalur akses sehingga Fitur yang di sediakan oleh SUSE Server tidak hanya pada satu sub jaringan saja akan tetapi mencakup keseluruhan.

Kelebihan :

a. Fitur yang di sediakan oleh SUSE Server dapat menyeluruh.
b. Troubleshooting lebih mudah.
c. Keamanan Seluruh jaringan lebih terjaga.
d. Semua sub jaringan dapat saling berinteraksi dengan akses yang telah di tentukan.
e. Akses remote jarak jauh lebih mudah, karena terhubung langsung dengan Router Modem.

Kekurangan :

a. -



Gambar 4.2.6-1 Network Diagram Rencana 2

4.2.6.1 Network System Requirement & Optional Tools

4. Hardware / Perangkat Keras :

   - 2 PC Server
   - PC Router (4 ethernet Card)
   - PC Client
   - IP Camera
   - D-Link ADSL
   - D-Link WAP

- D-Link Switch & Hub
- Kabel UTP

5. Sistem Operasi Jaringan :
   - Linux Server
   - Windows Server 2000
   - Windows OS
   - D-Link Software Inside

6. Internet Service Provider (ISP) :
   - Telkom Speedy 2 Mbps
   - Telkom Speedy 512 Kbps
   - Cnet 1 Mbps

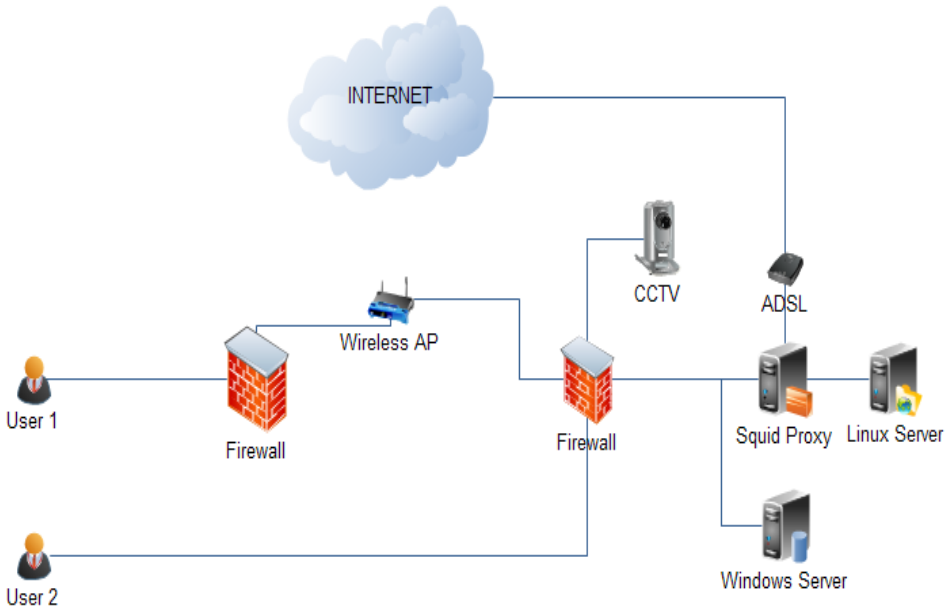
4.2.6.2 klarifikasi Sistem Jaringan 2

Pada topologi yang digunakan pada rencana 2 pembangunan jaringan Fasilitas Aplikasi Server tidak hanya untuk sub jaringan saja akantetapi mencakup jaringan lokal keseluruhan karena Router tepusat pada Linux Server. Namun fungsi dan kegunaan Fasilitas Aplikasi Server tetap sama seperti Rencana 1.

Ilustrasi kegiatan user pada jaringan Internal :

- Semua User akan di filter ketika hendak masuk kedalam jaringan.

- Khusus bagi User yang menggunakan Koneksi Via Wireless akan melakukan dua kali filterisasi WAP Security dan Proxy.
- User 1 sebagai User tertinggi yang dapat menggunakan semua fitur yang di sediakan Oleh Server.
- User 2 hanya di perbolehkan untuk mengakses Internet dan File Server tidak diperbolehkan menggunakan fitur yang lainnya.



Gambar 4.2.6-2 Gambar Analisis Rencana 2

Tabel 4.2.6-1Analisis Security Fitur

Jenis Koneksi	WAP Filter	IP Address Filter	MAC Address Filter	Autentikasi	Limitation & Cappability Access
Wired (Kabel)	x	√	√	√	√
Wireless	√	√	√	√	√

4.2.6.3 IP Addressing dan Subnetting

Untuk pengalamatan Rencana 2, kami menggunakan kelas A dan C. Kelas A dipakai di subjaringan tertentu (Private) dan untuk kelas C kami hanya menggunakan 1 Network adress saja namun untuk pembagian kami menggunakan subnetting dengan rincian sebagai berikut :

C	:	C	C	A	A
NA	:	192.168.5.XX	192.168.5.XX	192.168.5.XX	11.12.13.XX
R	:	1	65	193	1
		-	-	-	-
		-	-	-	-
		-	-	-	-

64 192 254 7

S : 255.255.255.224 , 255.255.255.192, 255.255.255.240, 255.255.255.248

Tabel 4.2.6-2 Rincian pembagian IP Address dan Subneting

No.	Divisi	Rentang IP	Subnet
1	Div-1	192.168.X.1	255.255.255.192
2	Div-2	-	255.255.255.192
3	Div-3	-	255.255.255.192
4	Div-4	-	255.255.255.192
5	Div-5	192.168.X.64	255.255.255.192
6	Div-6	192.168.X.65	255.255.255.224
7	Div-7	-	255.255.255.224
8	Div-8	-	255.255.255.224
9	Div-9	-	255.255.255.224
10	Div-10	192-168.X.192	255.255.255.224
11	Div-11	192.168.X193	255.255.255.240
12	Div-12	-	255.255.255.240
13	Div-13	-	255.255.255.240

14	Div-14	-	255.255.255.240
15	Div-15	192.168.X.254	255.255.255.240
16	Div-16	11.12.XX.1-11.12.XX.7	255.255.255.248