

## BAB IV

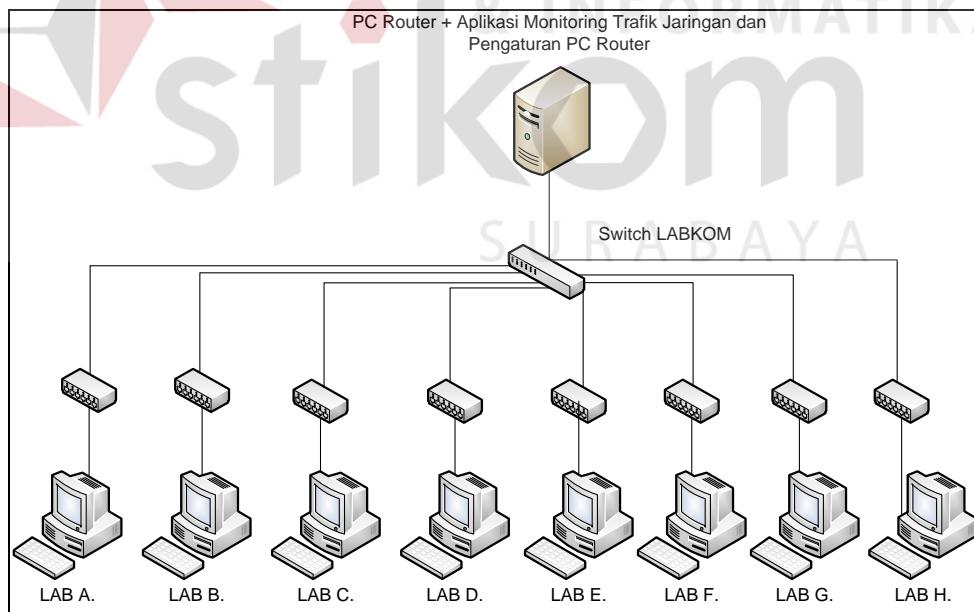
### HASIL DAN PEMBAHASAN

#### 4.1 Hasil

Berikut akan dibahas hasil dari rancangan aplikasi Monitoring Trafik dan Pengaturan PC Router Berbasis *web*:

##### 4.1.6 Rancangan Topology Jaringan

Aplikasi ini menggunakan topologi *star* dimana instalasi aplikasi dan kebutuhan perangkat lunak lainnya yang mendukung aplikasi ini akan dilakukan pada server PC router LABKOM yang bertugas secara penuh untuk mengontrol jaringan LABKOM. Pada Gambar 4.1 akan dijelaskan topologi aplikasi.

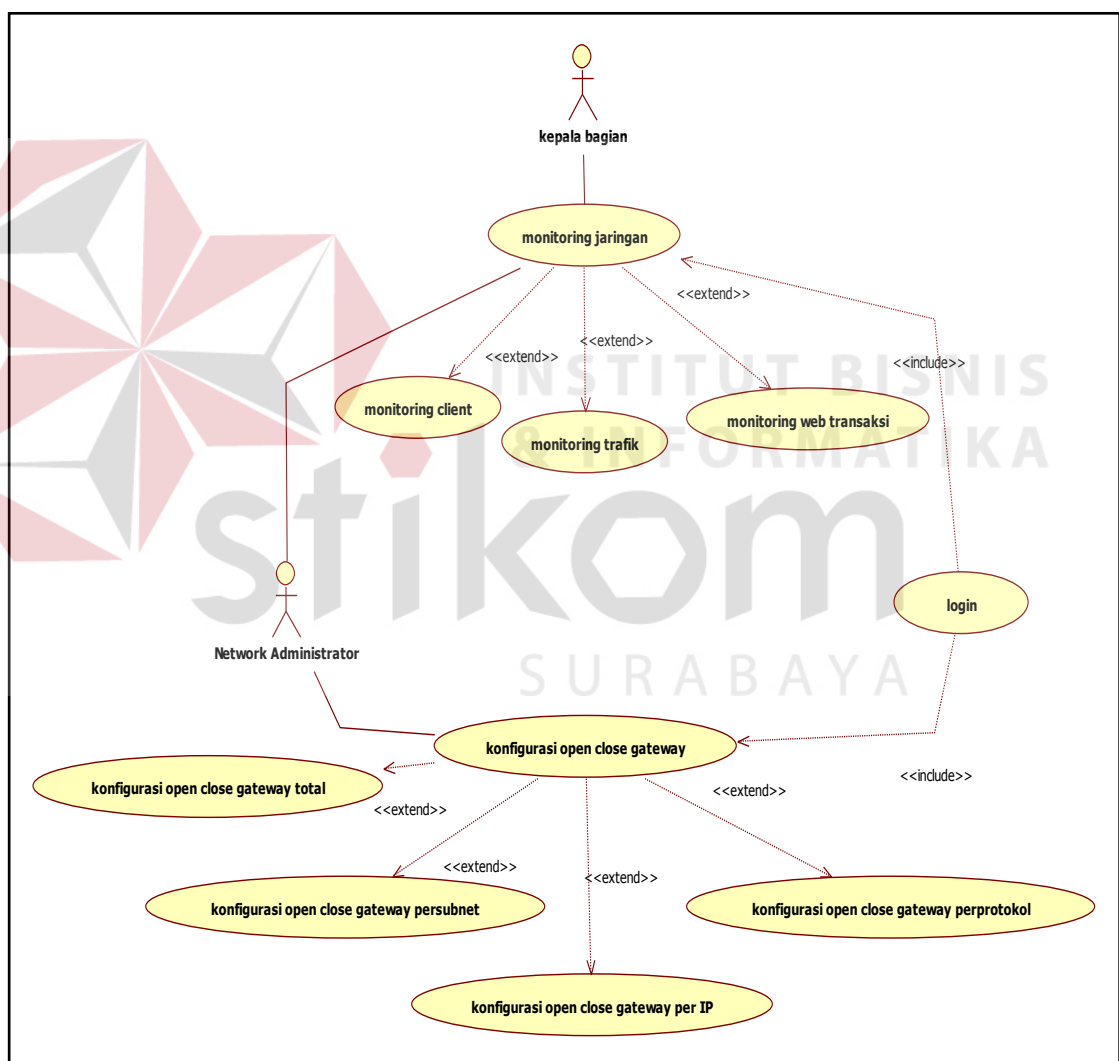


Gambar 4.1 Topologi Aplikasi Monitoring Trafik Jaringan Dan Pengaturan PC Router Berbasis Web.

#### 4.1.2 Rancangan Sistem Monitoring Trafik Jaringan dan Pengaturan PC

##### *Router*

Rancangan sistem monitoring dan pengaturan menggunakan *use case diagram* karena pengumpulan data dan pengambilan informasi berorientasi objek tidak terstruktur. Berikut adalah *use case* aplikasi Monitoring Trafik dan Pengaturan PC *Router* Berbasis *Web* dapat dilihat pada Gambar 4.2.



Gambar 4.2 *Use Case Diagram* Monitoring Trafik dan Pengaturan PC

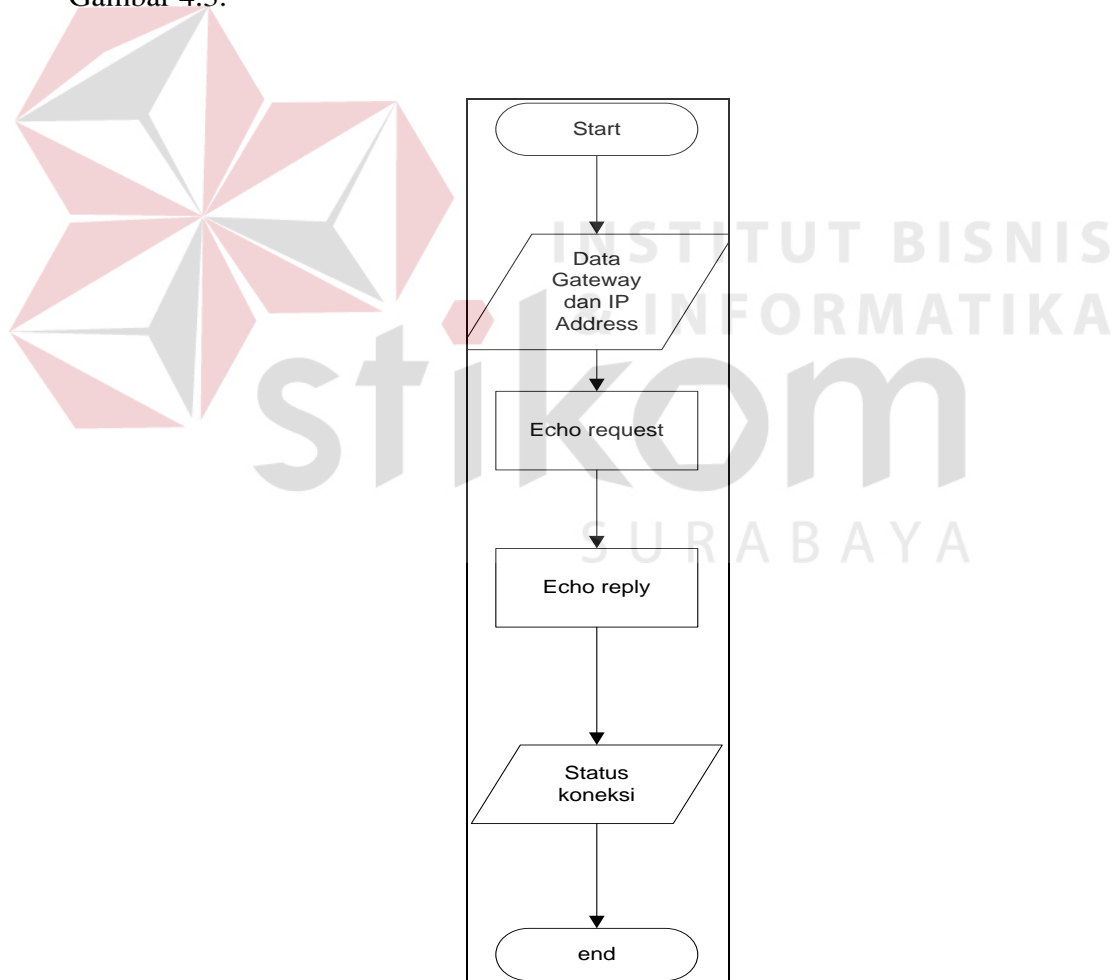
*Router* Berbasis *Web*

Dari rancangan sistem pada Gambar 4.2 dapat dilihat beberapa kegiatan yang dapat dilakukan. Berikut penjelasan dari *use case*:

#### 1. Monitoring *Client*

Sistem menyediakan fasilitas untuk mengetahui status koneksi dari *client* yang sedang menggunakan PC pada LABKOM, dimana pengecekan status koneksi dilakukan dengan utilitas “PING”. Pengujian koneksi dilakukan dari *network management station*(NMS) seluruh PC yang sudah didaftarkan dalam sistem aplikasi *monitoring*. Berikut akan dijelaskan melalui *flowchart* pada

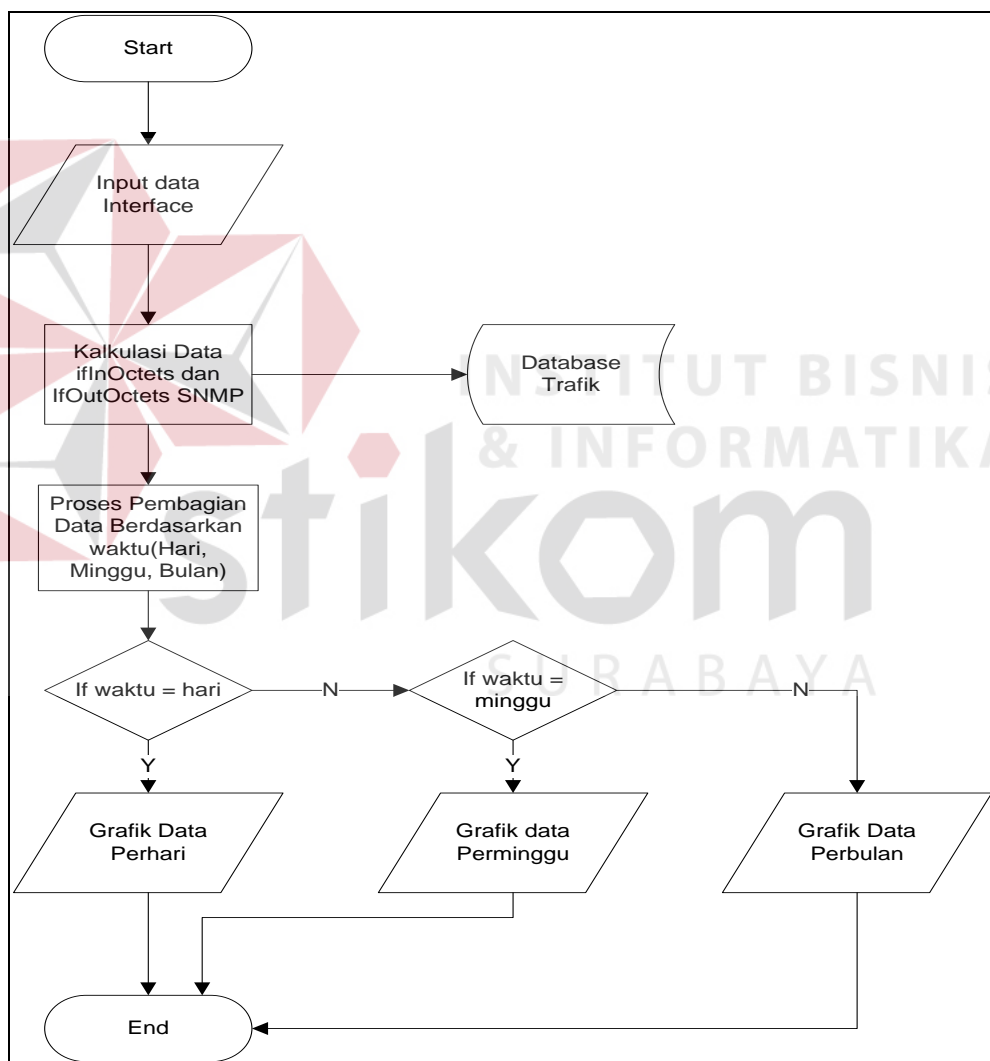
Gambar 4.3.



Gambar 4.3 *Flowchart Monitoring Client*

## 2. Monitoring Trafik

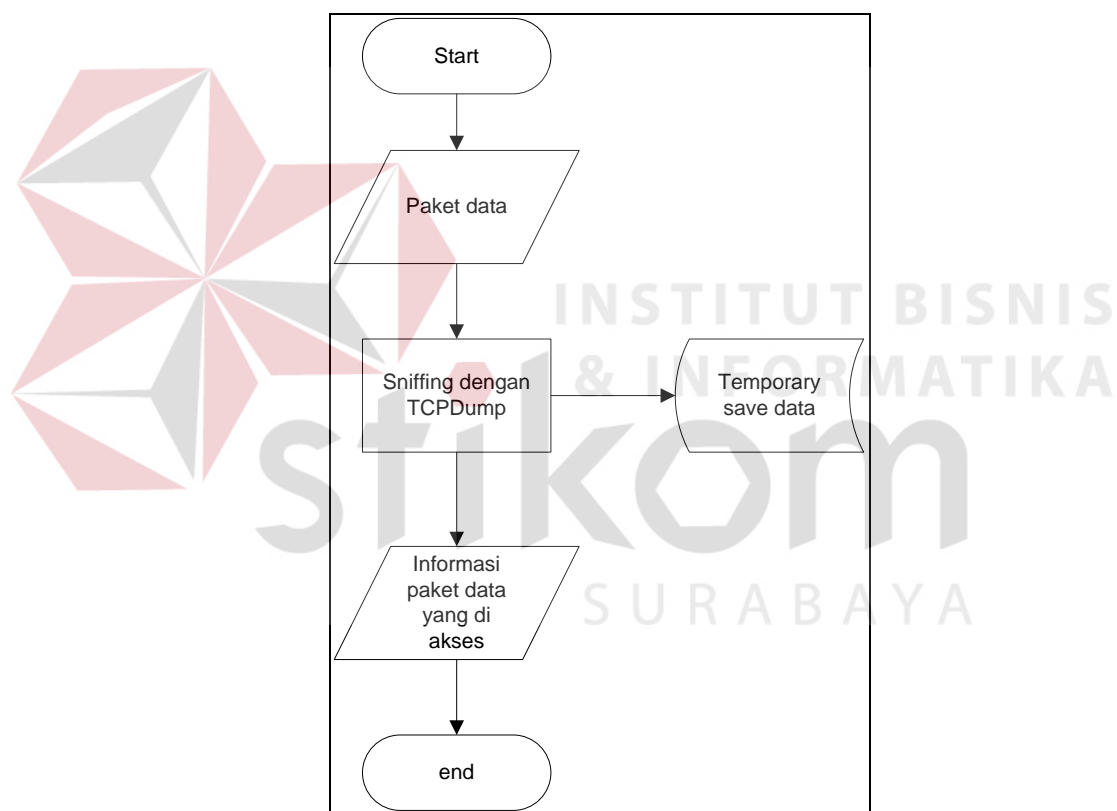
Pemantauan kondisi trafik jaringan *real-time* sangat dibutuhkan untuk sistem monitoring, pengambilan data dan informasi yang dibutuhkan menggunakan protokol SNMP dimana manajer mengambil data dari *agent* yang dibutuhkan dan diolah menjadi informasi berbentuk grafik. Berikut adalah *flowchart monitoring* trafik ditunjukkan pada Gambar 4.4.



Gambar 4.4 *Flowchart Monitoring* Trafik

### 3. Monitoring Web Transaksi

Banyak *website* yang dituju oleh *client*, dengan berbagai macam protokol didalamnya. Perlu adanya informasi dari paket yang lewat dan diakses oleh *client* agar pihak LABKOM dapat memutuskan untuk pemblokiran *website* dan *port* yang tidak boleh diakses pada saat kegiatan praktikum berlangsung. Berikut dijelaskan dengan menggunakan *flowchart monitoring* web transaksi pada Gambar 4.5.

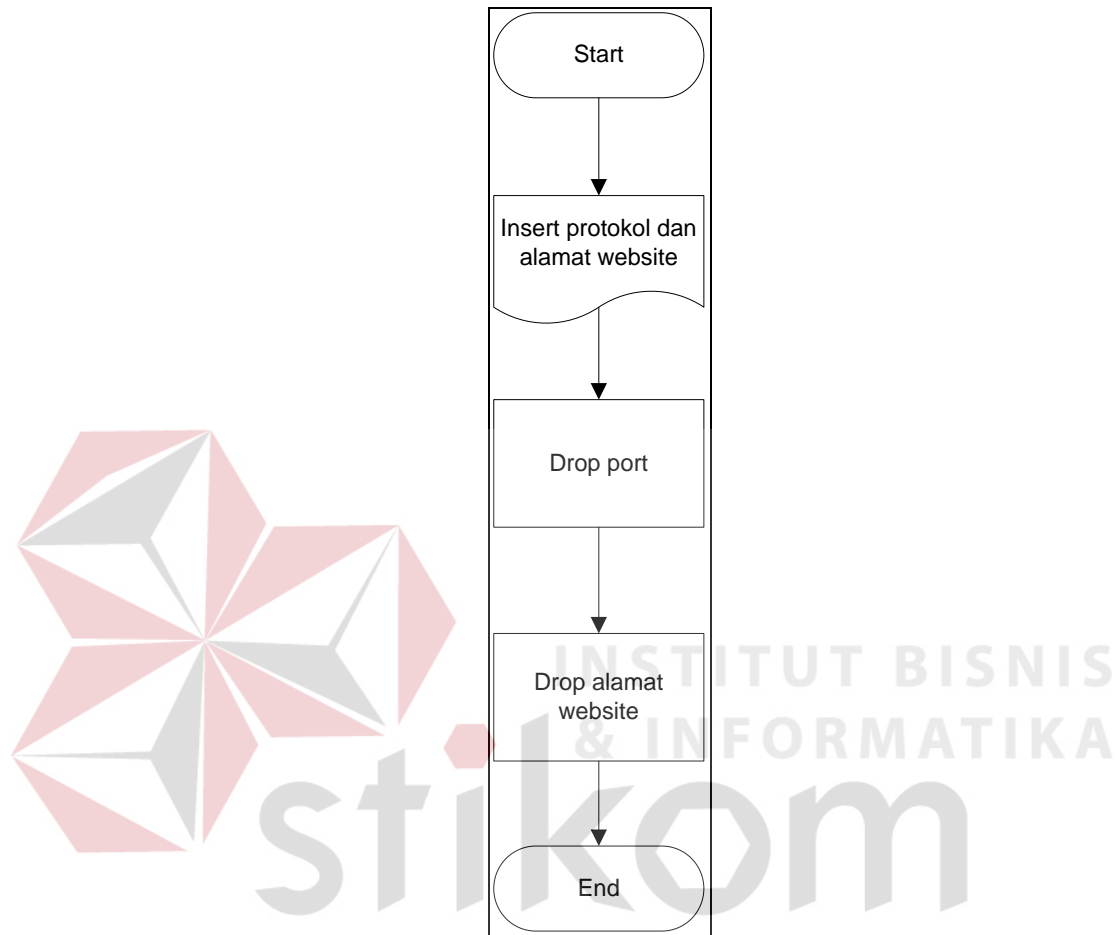


Gambar 4.5 *Flowchart Monitoring* Web Transaksi

### 4. Kontrol Gateway

Sistem aplikasi juga menyediakan fasilitas untuk membuka dan menutup *gateway* dan untuk akses kepada sebuah *website* tertentu yang tidak seharusnya

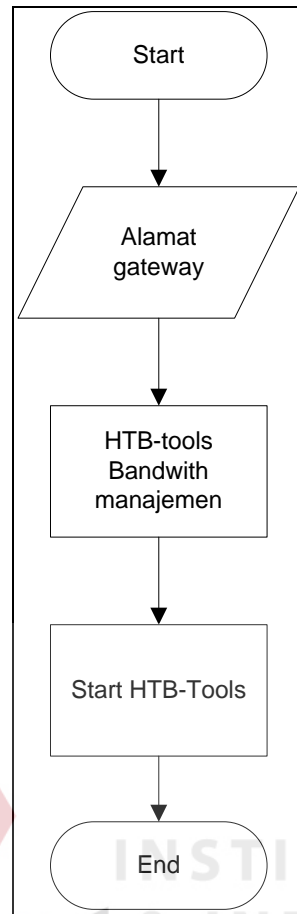
diakses pada jam praktikum, maka *website* tersebut dapat diblokir. Berikut akan ditunjukkan *flowchart* kontrol *gateway* pada Gambar 4.6.



Gambar 4.6 *Flowchart* Kontrol Gateway

## 5. Manajemen *Bandwith*

Menggunakan bantuan aplikasi HTB-tools untuk mempermudah alokasi *bandwith* antar *gateway* maupun salah satu dari PC *client*. Berikut akan dijelaskan dengan menggunakan *flowchart* untuk melakukan manajemen *bandwith* pada Gambar 4.7.

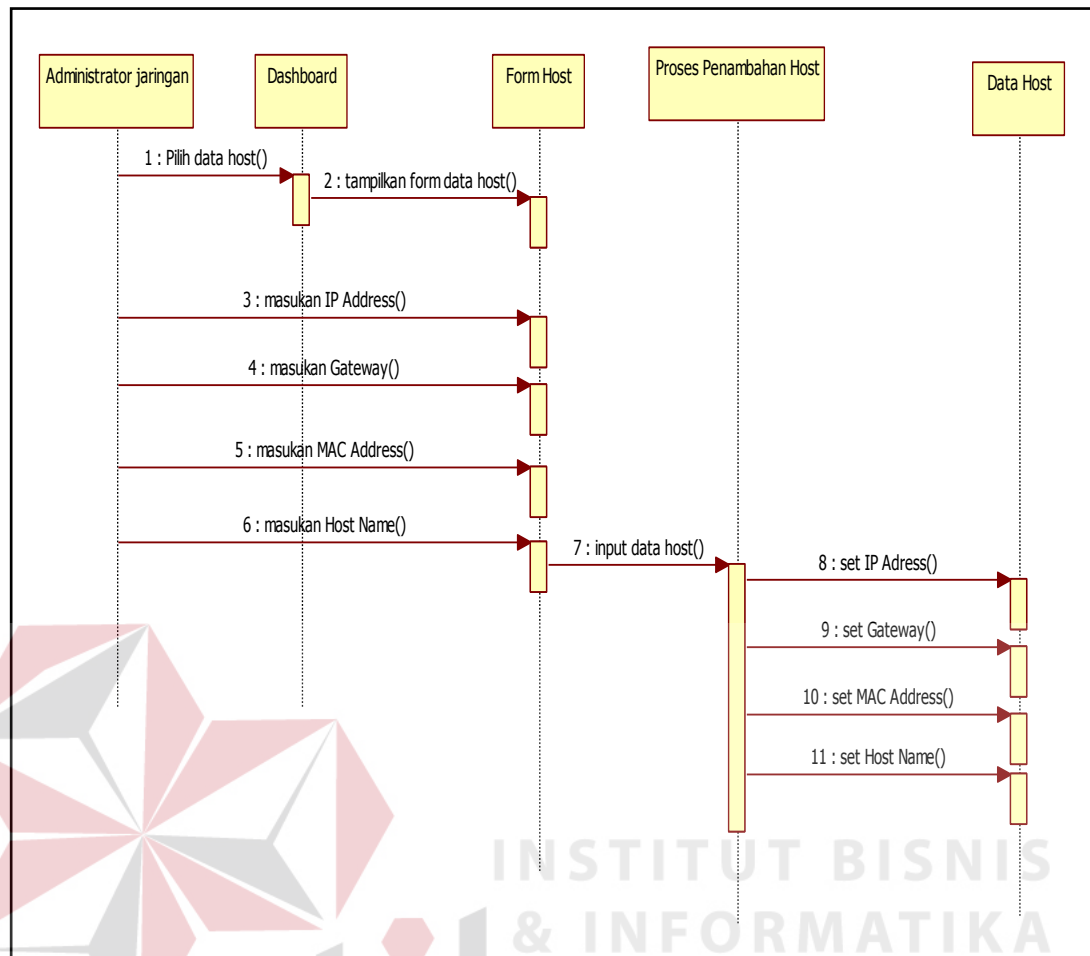


Gambar 4.7 Flowchart Manajemen Bandwith dengan HTB-Tools

Untuk menjelaskan interaksi objek yang disusun dalam suatu urutan waktu maka diperlukanlah *sequence diagram*. Ada beberapa *sequence diagram* dalam sistem ini, antara lain:

1. Sequence diagram input data host

Untuk awal monitoring *host up*, admin harus mengisi terlebih dahulu data *host client* yang dibutuhkan. Beberapa data yang dibutuhkan adalah *IP Address*, *Gateway*, *MAC Address*, *Hostname*. Sequence diagram *input data host* dapat dilihat pada Gambar 4.8.

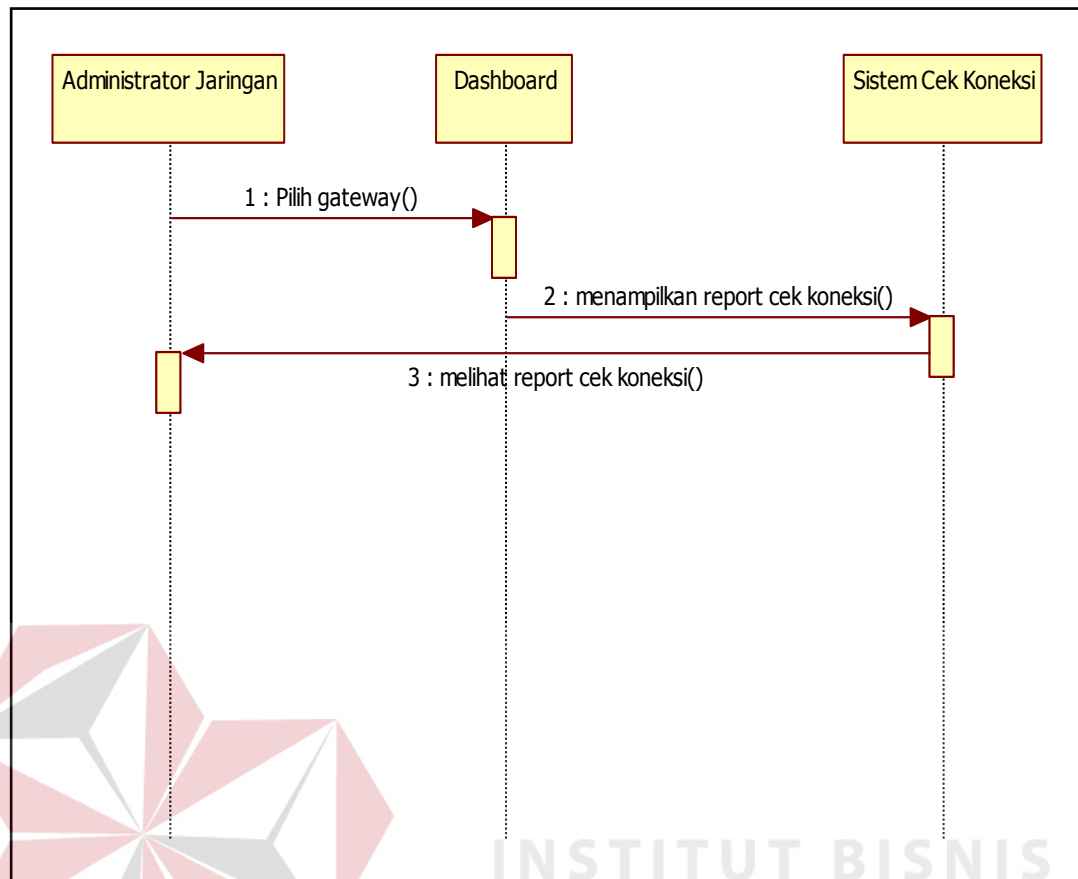


Gambar 4.8 *Sequence Diagram Input Data Host*

## 2. Sequence Diagram monitoring host up

Setelah melakukan *input data host*, maka sistem dapat melakukan *test koneksi* untuk *gateway* dan *host* yang sudah didaftarkan pada sistem. *Sequence diagram monitoring host up* dapat dilihat pada Gambar 4.9.



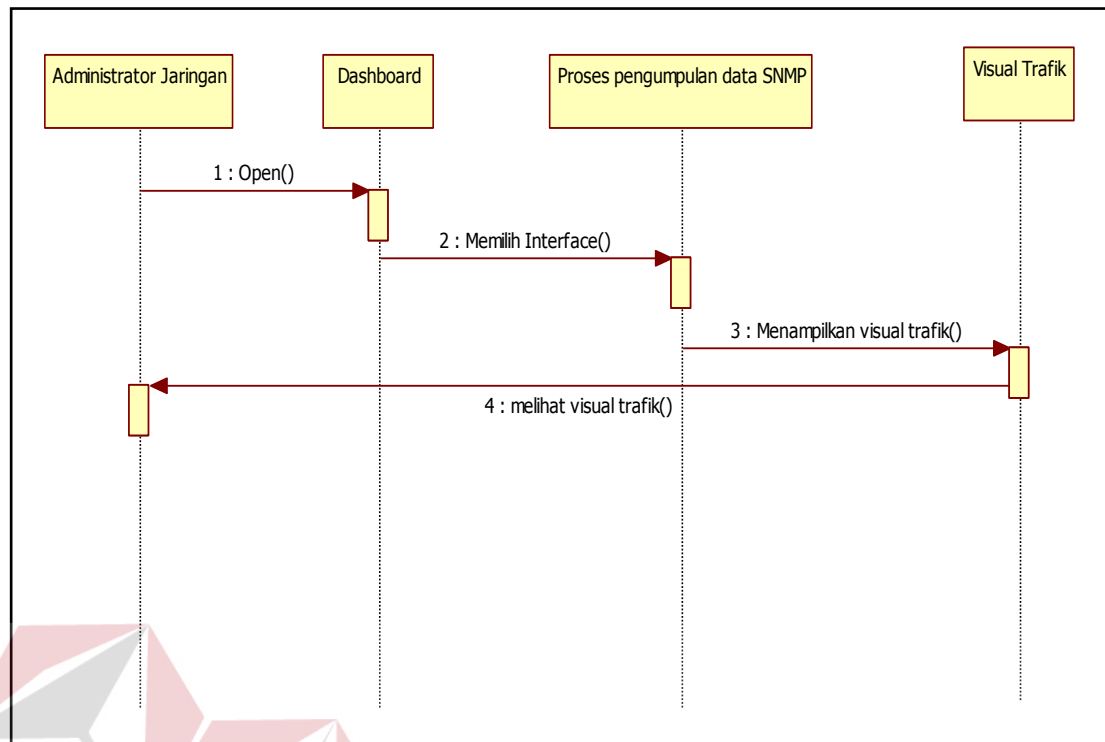


Gambar 4.9 *Sequence Diagram* Monitoring *Host Up/Down*

### 3. Sequence Diagram Monitoring Trafik

Untuk mengetahui padatnya jaringan LABKOM admin melihat trafik jaringan yang divisualisasikan dari data yang dikumpulkan dengan SNMP.

*Sequence* diagram monitoring trafik dapat dilihat pada Gambar 4.10.

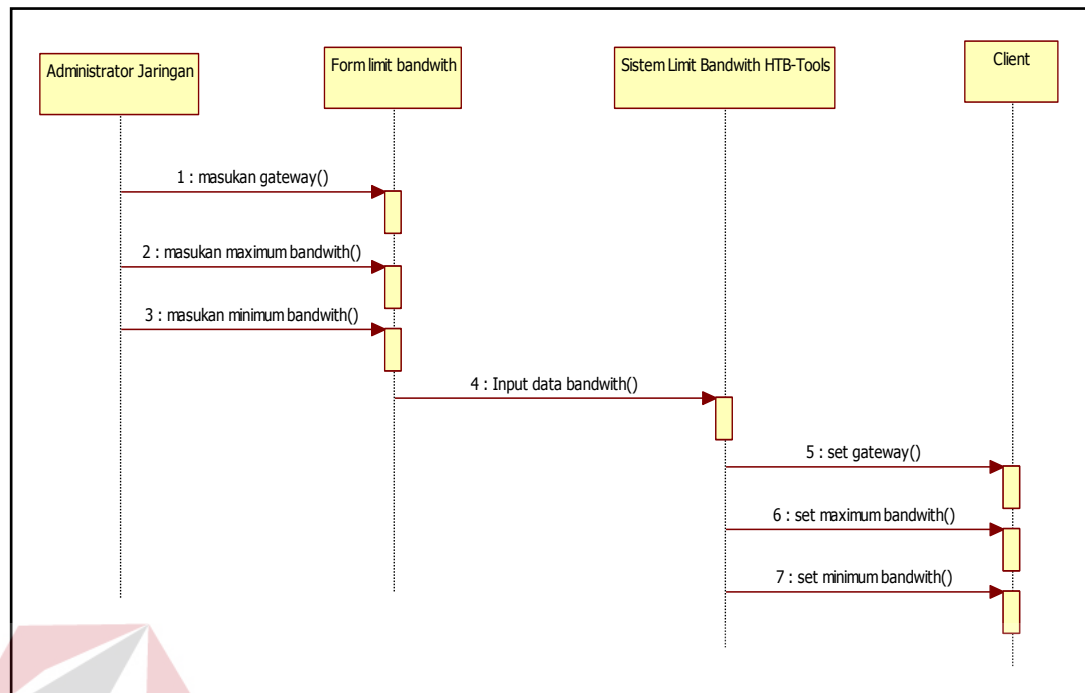


Gambar 4.10 *Sequence Diagram* Monitoring Trafik Jaringan

#### 4. *Sequence Diagram* Limit Bandwith

Untuk menjaga agar jaringan tidak *overload* maka admin harus membagi *bandwith* dengan ketentuan yang kondisional sesuai kebutuhan praktikum.

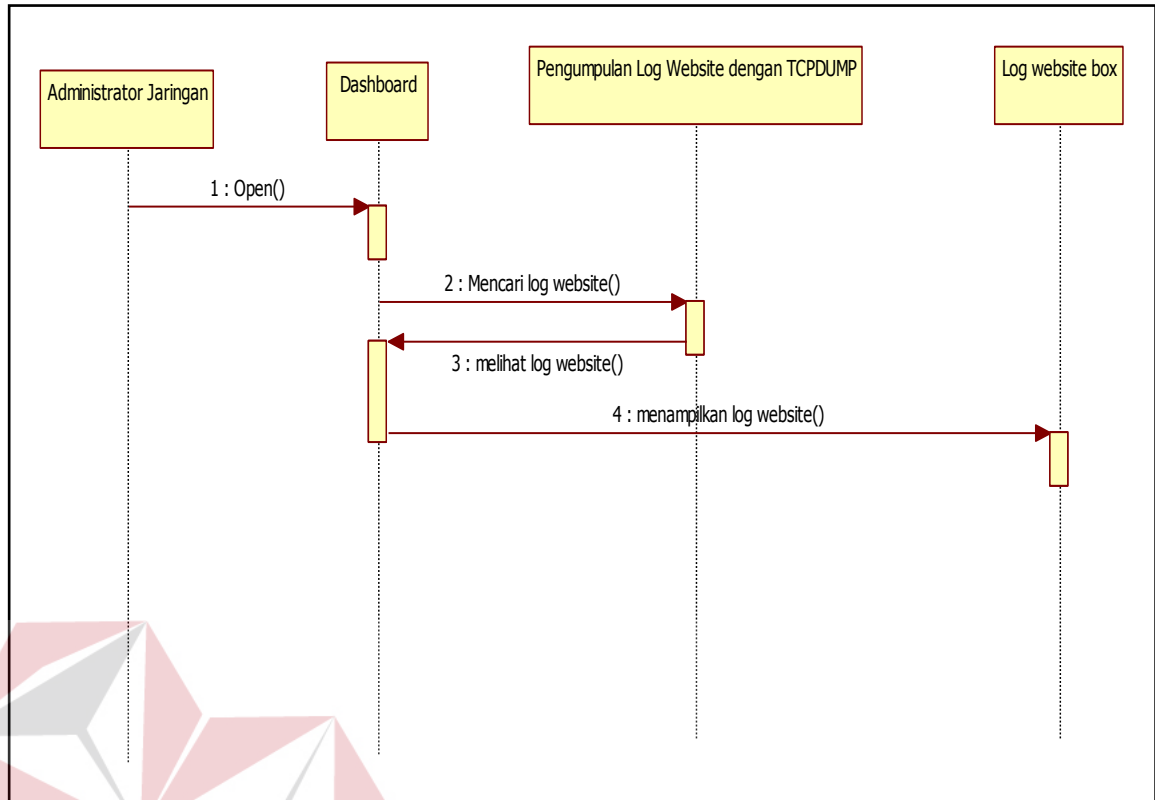
*Sequence diagram* limit *bandwith* dapat dilihat pada Gambar 4.11.



Gambar 4.11 *Sequence Diagram Limit Bandwith Jaringan*

#### 5. *Sequence Diagram Monitoring Log Website*

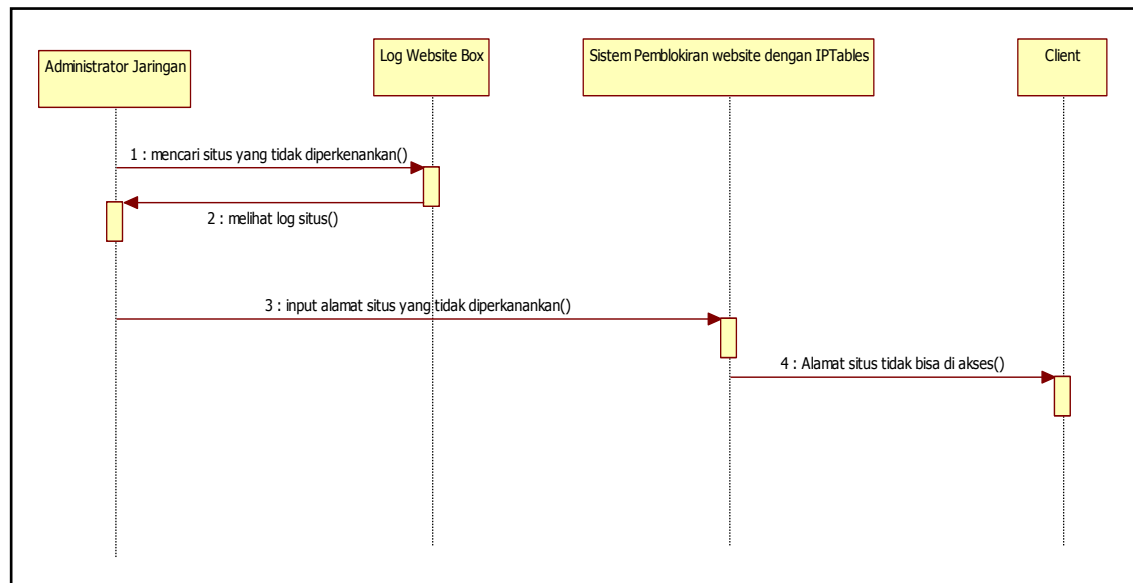
Untuk mengetahui transaksi *website* yang diakses oleh client, data log web transaksi yang dibutuhkan admin yang dikumpulkan dengan TCPDump. *Sequence diagram monitoring log website* dapat dilihat pada Gambar 4.12.



Gambar 4.12 *Sequence Diagram* Monitoring Log website

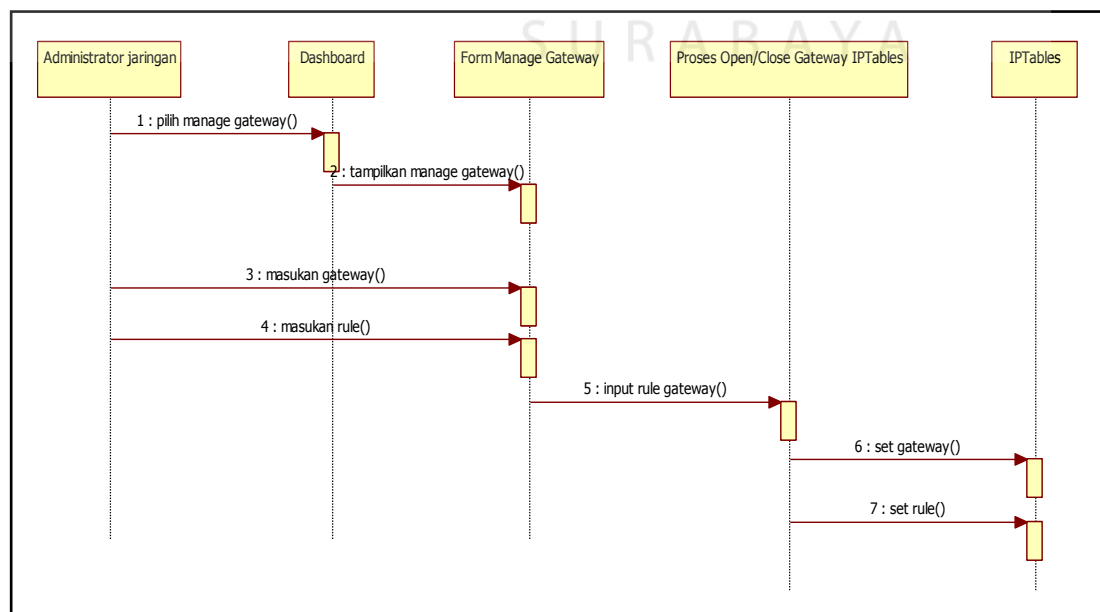
#### 6. *Sequence Diagram* Blok Situs

Setelah memonitoring *website* yang diakses oleh *client*, maka admin mendapatkan situs yang tidak layak diakses pada waktu praktikum berlangsung, maka admin harus memblokir situs berdasarkan *port* tertentu tersebut. *Sequence diagram* blok situs dapat dilihat pada Gambar 4.13.

Gambar 4.13 *Sequence Diagram* Blok Situs

### 7. *Sequence Diagram Open/Close Gateway*

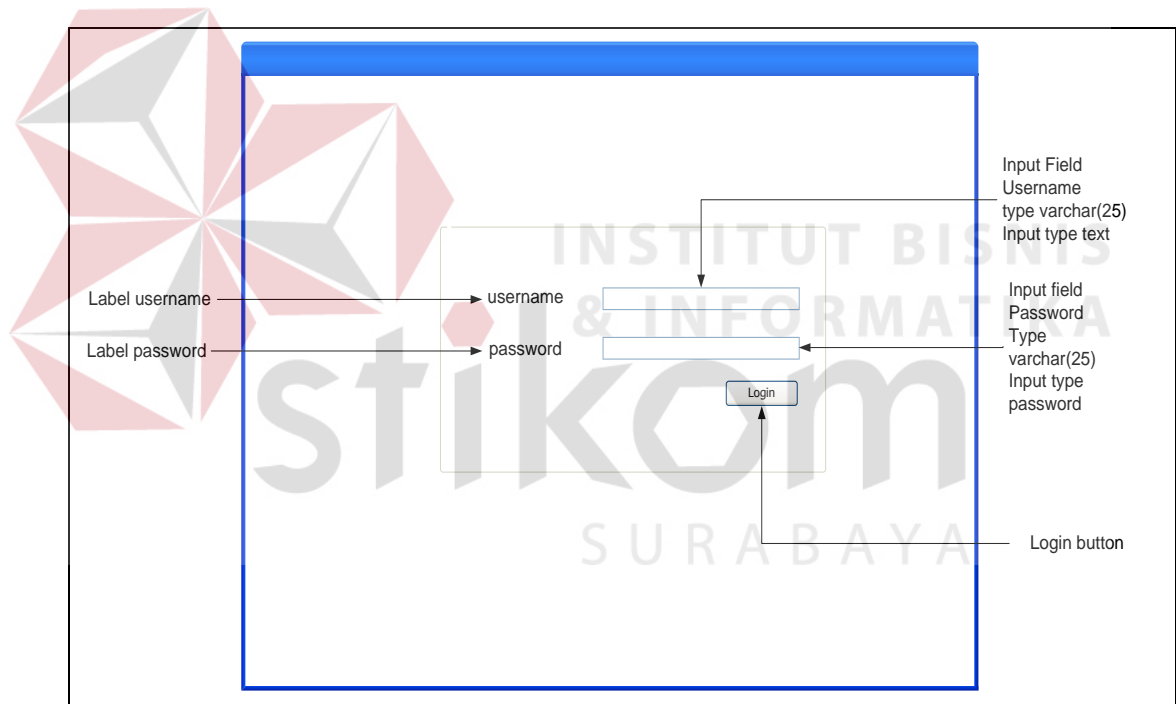
Agar tidak mengganggu LAB yang sedang menjalankan praktikum maka LAB yang sedang tidak digunakan dan tidak berkepentingan dalam praktikum akan ditutup aksesnya oleh admin. *Sequence diagram Open/Close gateway* dapat dilihat pada Gambar 4.14.

Gambar 4.14 *Sequence Diagram Open/Close Gateway*

Pada tahap berikutnya penulis membuat sketsa antar muka dari aplikasi. Sketsa yang dibuat didasarkan pada *use case* yang telah dibuat. Sketsa yang dibuat diperuntukkan kepada administrator jaringan dan kepala bagian.

a. Sketsa Halaman Login

Halaman login menampilkan sebuah tombol yang bertuliskan “Login” dimana *username* menggunakan *type input text* dengan jumlah maximal 25 *character* dan *type input password* adalah *password*. Sketsa halaman *login* ditunjukkan pada Gambar 4.15.

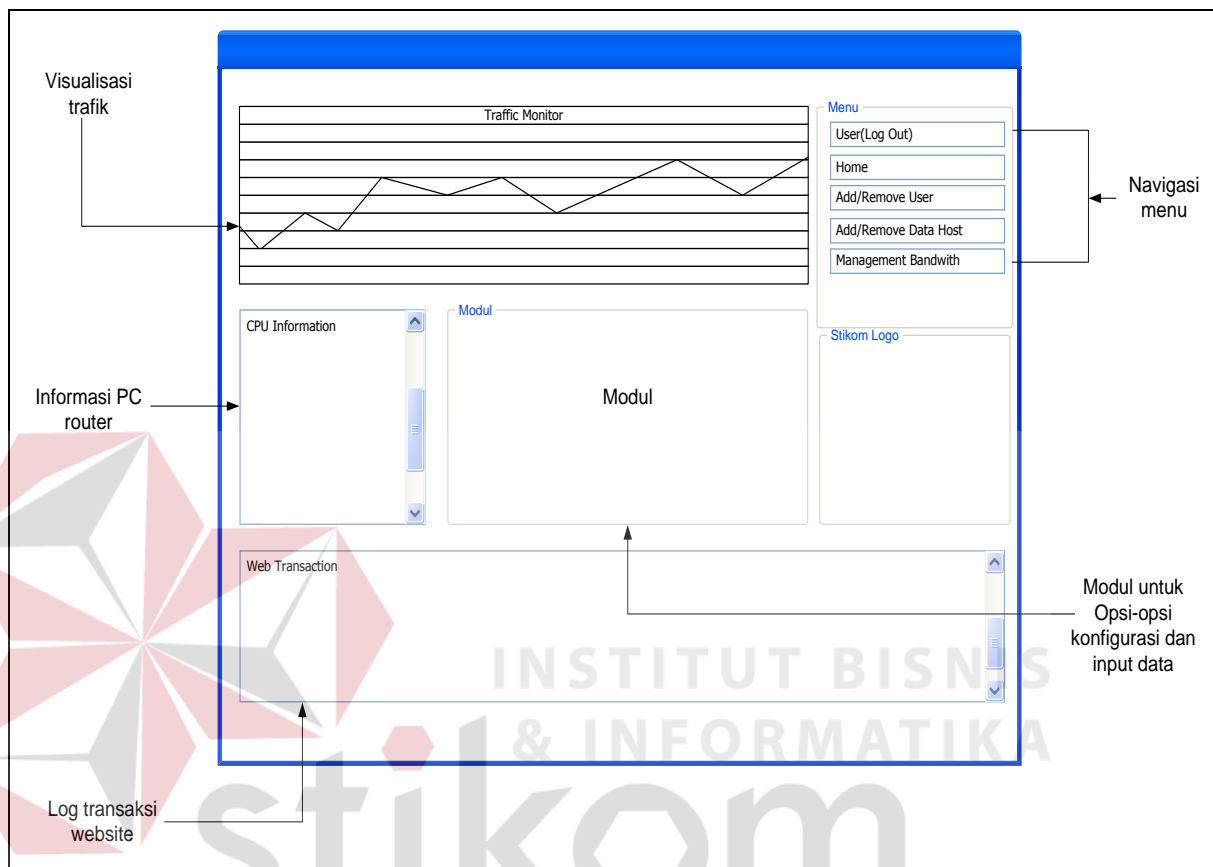


Gambar 4.15 Sketsa Halaman Login

b. Sketsa Halaman *Home Level Admin*

Pada halaman *Home level admin* terdapat *Traffic Monitor*, Menu yang di dalamnya berisi *management user*, *management data host*, *management bandwith*, dan kemudian ada *CPU Information* yang digunakan untuk mengetahui spesifikasi dari *PC router*, *Connection info* digunakan untuk mengetahui *PC client*

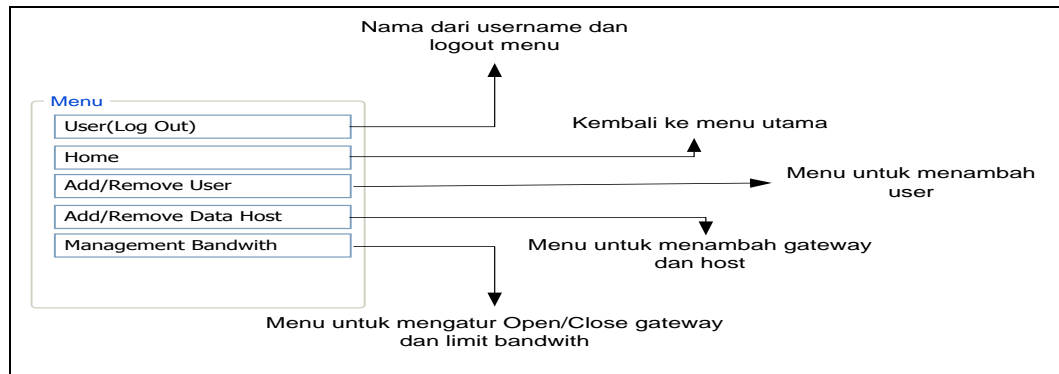
yang sedang *up* dan *web transaction* untuk mengetahui keluar masuknya transaksi *website* yang di tunjukan pada gambar 4.16.



Gambar 4.16 Sketsa Halaman Home *Level Admin*

### c. Sketsa Navigasi *Level Admin Menu*

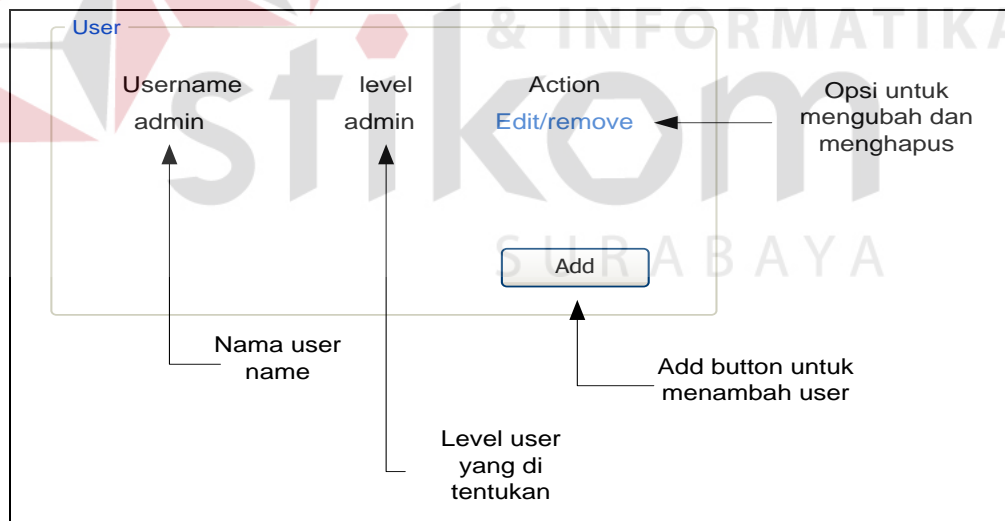
Beberapa menu yang hanya dapat digunakan oleh level admin yaitu *Add/remove user* untuk menambah, mengubah dan menghapus *user* dan level admin juga dapat menambah, menghapus dan mengubah *host* untuk daftar IP yang akan dimonitoring. Navigasi menu admin dapat dilihat pada Gambar 4.17.



Gambar 4.17 Sketsa Navigasi Menu *Level Admin*

d. Sketsa Halaman Admin Modul

Beberapa modul admin yang sudah di sediakan adalah *Add/Remove user*, fungsi utama modul ini adalah untuk menambah, menghapus dan mengedit fungsi dari *user* apakah *user* tersebut memiliki level admin ataupun hanya *user* biasa. Modul *Add/Remove user* dapat dilihat pada Gambar 4.18.



Gambar 4.18 Sketsa halaman *Add/Remove user*

Pada modul terdapat *Button Add*, dimana jika *button* tersebut di tekan maka akan muncul sebuah jendela baru untuk *form* pengisian *user*, untuk pengisian *user*



*text input* berisi 25 *character* huruf maupun angka. Form pengisian *user* dapat dilihat pada Gambar 4.19.

The image shows a wireframe of an 'Add user' form. It features three input fields: 'Username' with the value 'admin', 'Password' with '\*\*\*\*\*', and 'Level' with a dropdown menu showing 'Admin/User'. Below these fields is an 'Add' button. Arrows point from labels on the right to each field and the button. The labels are: 'Input Username', 'Input Password', 'User level combo box', and 'Button Add untuk menambah user'.

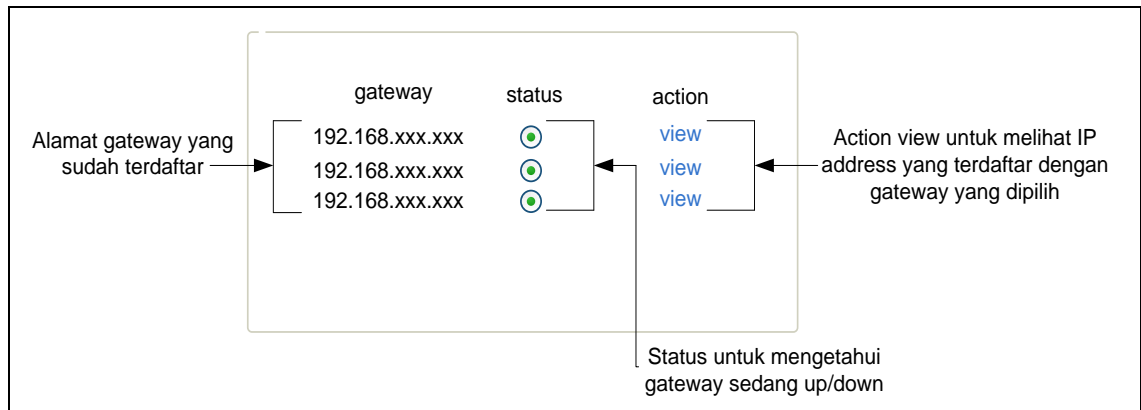
Gambar 4.19 Sketsa Halaman Form Add *user*

Modul *Add/Remove user* juga memiliki fungsi Edit, untuk mengubah hak akses *user*. Halaman *form edit user* dapat dilihat pada Gambar 4.20.

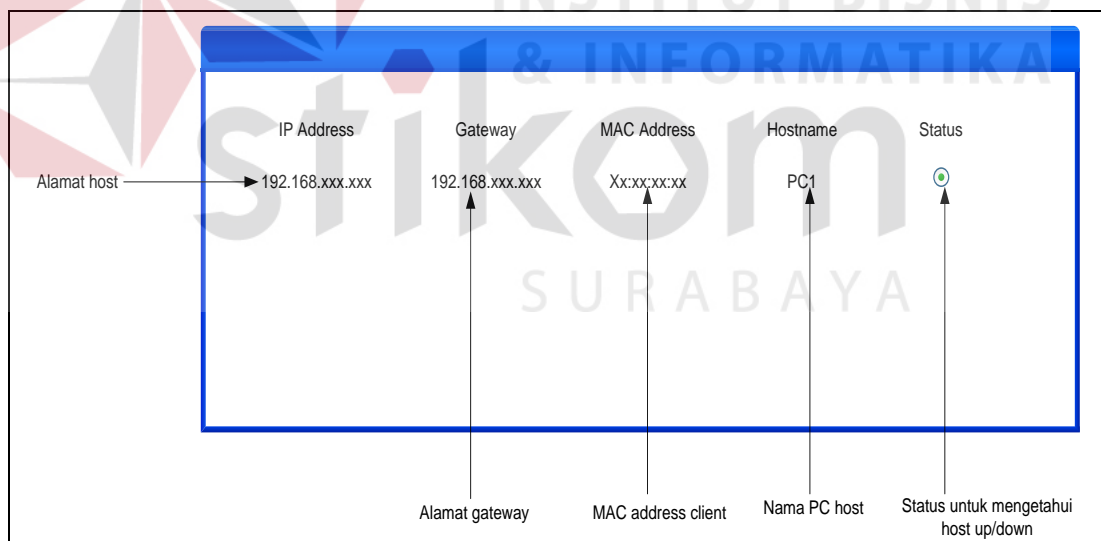
The image shows a wireframe of an 'Edit User' form. It features three input fields: 'Username' with the value 'admin', 'Password' with '\*\*\*\*\*', and 'Level' with a dropdown menu showing 'Admin/User'. Below these fields is an 'Edit' button. Arrows point from labels on the right to each field and the button. The labels are: 'Edit Username', 'Edit Password', 'User level combo box', and 'Button Edit untuk mengubah user'.

Gambar 4.20 Sketsa Halaman Form *Edit User*

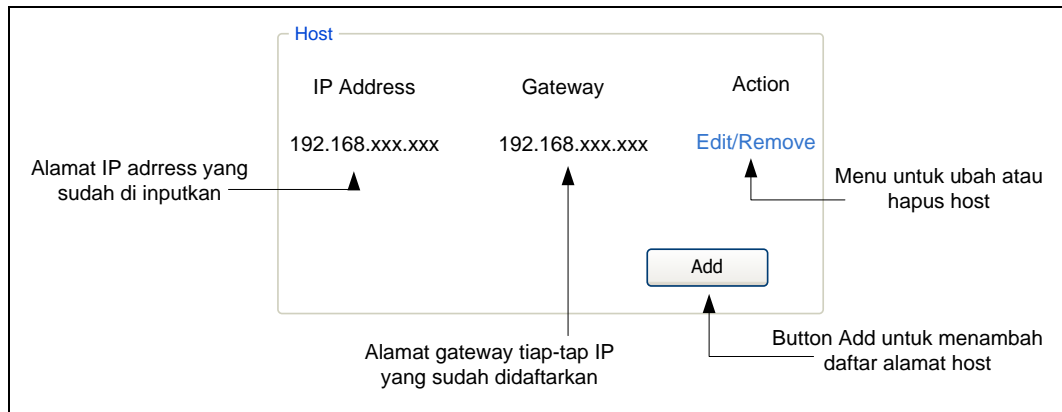
Pada halaman *home*, admin maupun *user* biasa dapat melihat *gateway* dan *host* yang sedang *up/down*, sketsa halaman modul *host up* dapat dilihat pada Gambar 4.21.

Gambar 4.21 Sketsa *Gateway Status*

Pada *action view*, akan muncul sebuah halaman dimana halaman tersebut memuat *IP address* yang sudah didaftarkan oleh admin sesuai dengan *gateway* yang digunakan. Sketsa halaman monitoring *IP address client* dapat dilihat pada Gambar 4.21.

Gambar 4.22 Sketsa *Host Status*

Berikut adalah sketsa halaman modul input *host* dan *gateway*. Sketsa modul input *host* dan *gateway* dapat dilihat pada Gambar 4.23.



Gambar 4.23 Sketsa Modul *Add/Remove Host*

Setelah masuk pada halaman *Add/remove Host*, maka akan muncul tombol *add* dimana jika ditekan maka akan muncul sebuah *form* berisikan input data dan edit data pada modul *Add/Remove host* dan *input type* dari *input IP Address* adalah *15 character*, untuk *input type gateway* juga *15 character* dan untuk *MAC Address* adalah *maximal input* sedangkan *Hostname* adalah *10 character*. Sketsa *form add* dan *edit host* dapat dilihat pada Gambar 4.24 dan Gambar 4.25.

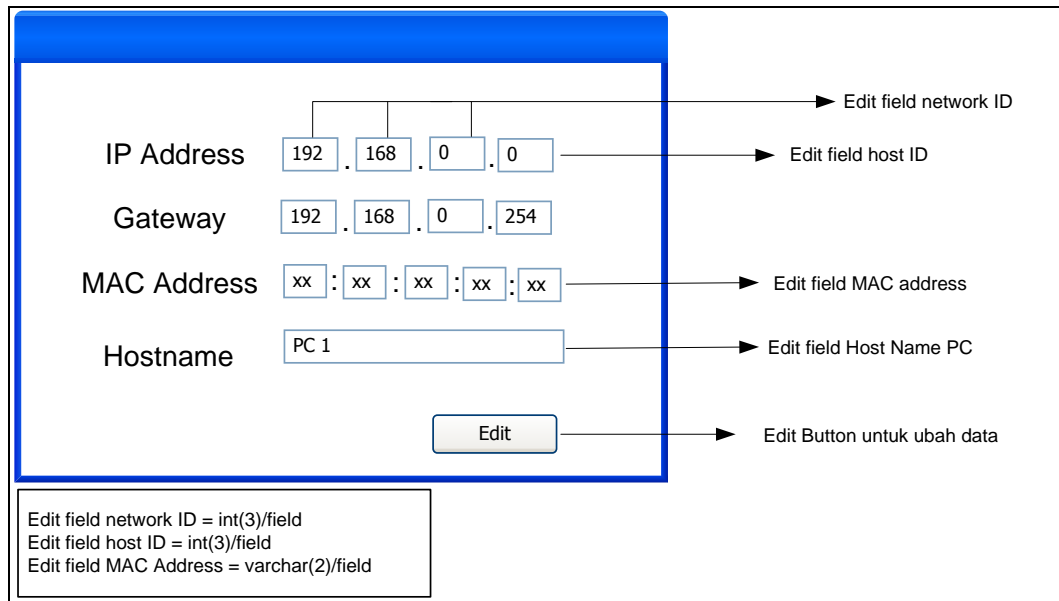
The screenshot shows the 'Add Host' form with the following fields and annotations:

- IP Address:** 192 . 168 . 0 . 0. Annotations: 'Input field network ID' points to the first octet (192), and 'Input field host ID' points to the second octet (168).
- Gateway:** 192 . 168 . 0 . 254.
- MAC Address:** xx : xx : xx : xx : xx. Annotation: 'Input field MAC address'.
- Hostname:** PC 1. Annotation: 'Input field Host Name PC'.
- Add Button:** 'Add'. Annotation: 'Add Button untuk tambah data'.

Legend box at the bottom left:

- Input field network ID = int(3)/field
- Input field host ID = int(3)/field
- Input field MAC Address = varchar(2)/field

Gambar 4.24 Sketsa Form *Add Host*



The diagram shows a form for editing host data with the following fields and labels:

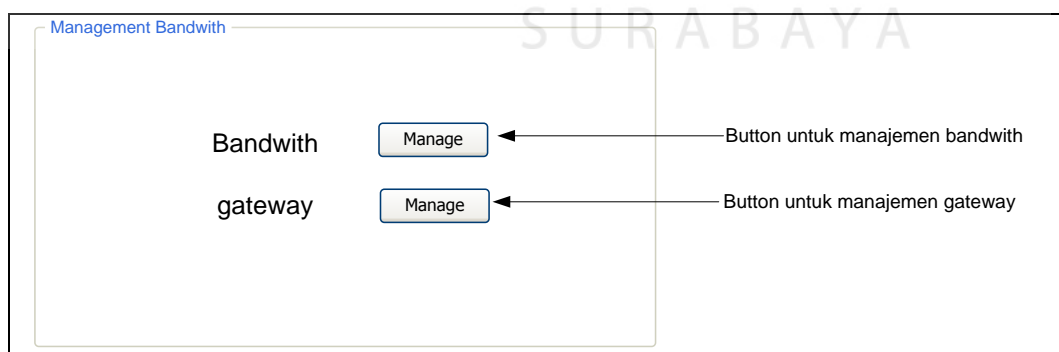
- IP Address:** 192 . 168 . 0 . 0. Labels: Edit field network ID (pointing to the first three octets), Edit field host ID (pointing to the last octet).
- Gateway:** 192 . 168 . 0 . 254.
- MAC Address:** xx : xx : xx : xx : xx. Label: Edit field MAC address.
- Hostname:** PC 1. Label: Edit field Host Name PC.
- Edit Button:** Edit. Label: Edit Button untuk ubah data.

Legend for field types:

- Edit field network ID = int(3)/field
- Edit field host ID = int(3)/field
- Edit field MAC Address = varchar(2)/field

Gambar 4.25 Sketsa Form *Edit Data Host*e. Sketsa halaman *Management Bandwith*

Halaman *Management Bandwith* bisa di akses pada level *user* maupun *admin*, halaman ini berfungsi mengatur *bandwith* dan membatasi akses *gateway* keluar masuk jaringan. Sketsa halaman management bandwith di tunjukan pada Gambar 4.26.



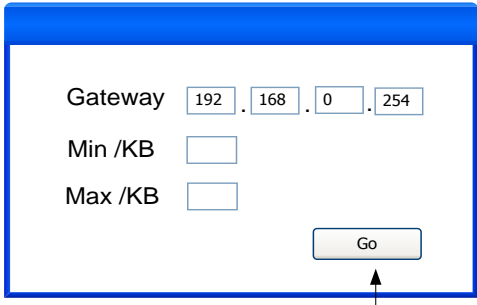
The diagram shows a page titled "Management Bandwith" with two sections:

- Bandwith:** Manage (Label: Button untuk manajemen bandwith)
- gateway:** Manage (Label: Button untuk manajemen gateway)

Gambar 4.26 Sketsa Halaman *Management Bandwith*

Pada *bandwith* ada *button manage* untuk memamajemen *bandiwith*, akan muncul sebuah *windows* baru untuk pengisian *form* manajemen *badwith*. Untuk

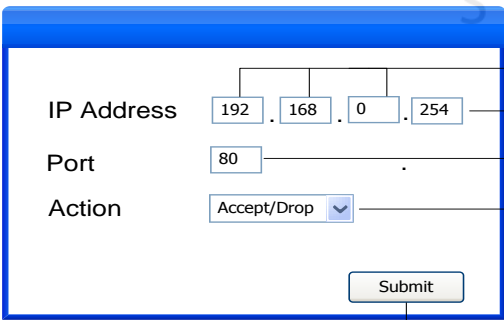
pengisian Max dan Min/KB adalah *input type integer*. Sketsa form manajemen *bandwith* dapat dilihat pada Gambar 4.27.



The image shows a web form titled "Manage Bandwith". It contains three input fields: "Gateway" with the value "192.168.0.254", "Min /KB" which is empty, and "Max /KB" which is empty. Below these fields is a "Go" button. Arrows point from text labels to each of these elements: "Input alamat gateway yang ingin di manajemen" points to the Gateway field, "Input minimum koneksi" points to the Min /KB field, "Input maximum koneksi" points to the Max /KB field, and "Tombol action untuk limit bandwith" points to the Go button.

Gambar 4.27 Sketsa Form *Manage Bandwith*

pada bagian *gateway* juga ada tombol untuk manajemen *open/close gateway*, akan muncul *windows* untuk form pengisian *gateway* yang akan ditutup dan disambung pada port *protocol* oleh admin. Sketsa form pengisian *open/close gateway* dapat dilihat pada Gambar 4.28.

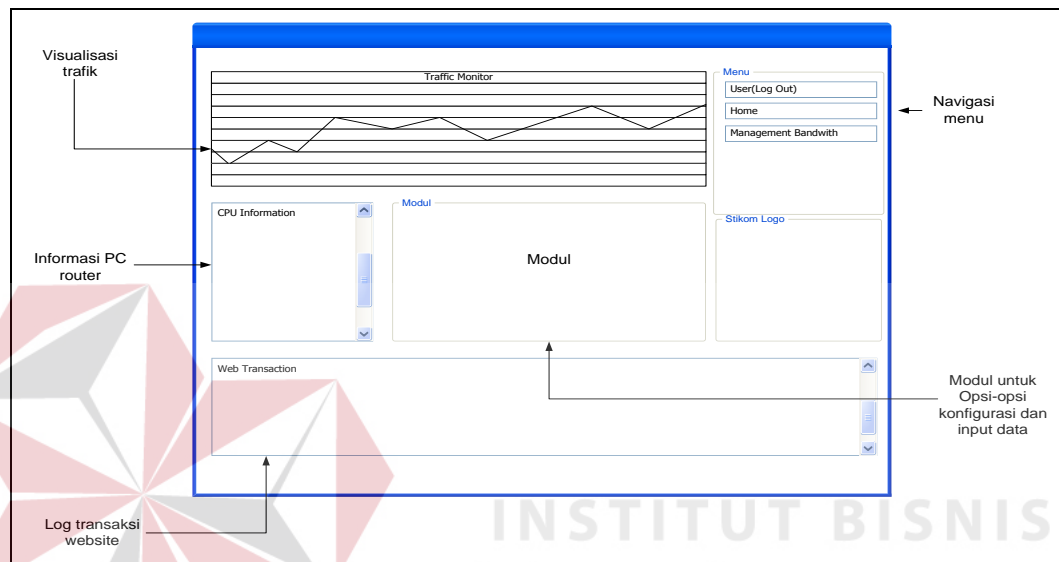


The image shows a web form titled "Open/Close Gateway". It contains four input fields: "IP Address" with the value "192.168.0.254", "Port" with the value "80", "Action" with a dropdown menu showing "Accept/Drop", and a "Submit" button. Arrows point from text labels to each of these elements: "Input field network ID" points to the first octet of the IP address, "Input field host ID" points to the last octet of the IP address, "Input field port protocol" points to the Port field, "Combo box option action untuk protocol" points to the Action dropdown, and "Submit button action protocol" points to the Submit button.

Gambar 4.28 Sketsa Form *Open/Close Gateway*

f. Sketsa Halaman *Home Level User*

Halaman *Home level user* ada halaman utama dari level *user*, pada halaman ini menu *Add/Remove user* dan *Add/Remove data host* tidak bisa di akses. Sketsa halaman tabel menu minuman di tunjukan pada Gambar 4.29 pada.



Gambar 4.29 Sketsa Halaman *Home Level User*

Pada tahap ini penulis memulai melakukan pemodelan yang telah ditentukan sebelumnya. Tahap yang penulis lakukan adalah membuat *flow-of-event* dari sistem. *Flow-of-event* yang di buat yaitu:

1. Flow Of Event Monitoring Jaringan

*Flow of event* untuk monitoring jaringan pada LABKOM dapat dilihat pada Tabel 4.1.

Tabel 4.1 *Flow Of Event Monitoring Jaringan*

Diskripsi	<i>Use case monitoring host up</i> memungkinkan untuk admin dan kepala bagian LABKOM memonitoring jumlah <i>client</i> yang terhubung dengan <i>router</i> , trafik jaringan, dan transaksi <i>website</i> yang di akses.
Kondisi Awal	Transaksi data pada saat praktikum.
Kondisi Akhir	Admin dan kepala bagian LABKOM mendapatkan informasi <i>client</i> yang sedang up, informasi trafik jaringan, dan transaksi <i>web</i> yang di akses.

		<i>Aksi Pemakai</i>	<i>Respon Sistem</i>
Aliran Kejadian Utama	1	admin dan kepala bagian LABKOM memilih monitoring jaringan.	Sistem menampilkan informasi IP <i>address client</i> yang sedang up, informasi trafik jaringan, dan informasi transaksi <i>web</i> yang di akses.

## 2. Flow Of Event Konfigurasi Open Close Gateway

*Flow of event* untuk konfigurasi *open close gateway* dapat dilihat pada

Tabel 4.2.

Tabel 4.2 Flow Of Event Konfigurasi Open Close Gateway

Diskripsi	<i>Use case control open close gateway</i> memungkinkan admin untuk memblokir akses <i>internet</i> pada <i>client</i> yang dituju.		
Kondisi Awal	Data IP <i>address</i> atau subnet yang akan di blokir untuk akses jaringan <i>internet</i> .		
Kondisi Akhir	IP <i>address</i> dan subnet tertentu tidak bisa mengakses jaringan <i>internet</i> .		
		<i>Aksi Pemakai</i>	<i>Respon Sistem</i>
Aliran Kejadian Utama	1	admin memutuskan untuk memblokir sejumlah IP <i>address</i> dan subnet yang di tentukan.	<i>Client</i> tidak bisa mengakses jaringan <i>internet</i> hingga admin membuka kembali akses jaringan <i>client</i> tersebut.

## 3. Flow Of Event Bandwith Management

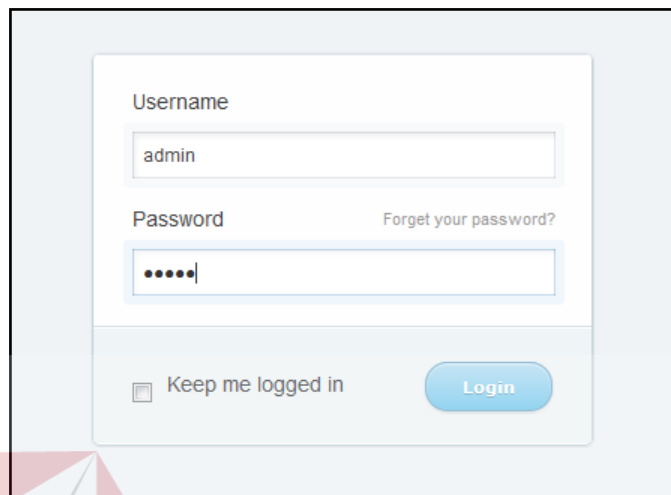
*Flow of event* untuk *bandwith management* dapat dilihat pada Tabel 4.3.

Tabel 4.3 Flow Of Event Bandwith Management

Diskripsi	control <i>Bandwith Management</i> memungkinkan admin untuk membatasi penggunaan <i>bandiwith</i> akses <i>internet</i> pada <i>client</i> .		
Kondisi Awal	Data <i>gateway</i> yang akan di batasi <i>bandwithnya</i> untuk akses jaringan <i>internet</i> .		
Kondisi Akhir	Penggunaan <i>bandwith</i> sesuai dengan ketentuan.		
		<i>Aksi Pemakai</i>	<i>Respon Sistem</i>
Aliran Kejadian Utama	1	Admin membatasi <i>bandwith</i> pemakaian tiap-tiap <i>gateway</i> sesuai ketentuan	Masing masing <i>gateway</i> mendapatkan limit <i>bandwith</i> sesuai ketentuan.

Berikut akan dibahas implementasi dari aplikasi Monitoring Trafik dan Pengaturan PC Router Berbasis Web.

### 1. Halaman Login



Gambar 4.30 Halaman *Login* Aplikasi Monitoring Trafik dan Pengaturan PC Router

Pada Gambar 4.30 dapat dilihat halaman *login* dari aplikasi Monitoring Trafik dan Pengaturan PC Router berbasis Web. Terdapat 2 kolom *text* berisikan *username* dan *password*, pada kolom *password* berisikan *input type password* sehingga *password* tidak terbaca.

### 2. Halaman *Home*

Halaman *Home* dibagi menjadi 2 yaitu halaman *Home* untuk admin ditunjukkan pada Gambar 4.31 dan halaman *Home* untuk *user* ditunjukkan pada Gambar 4.32. Dimana letak perbedaan halaman *Home* pada *level user* dan admin adalah pada bagian menu ditunjukkan pada Gambar 4.33. Berikut akan dijelaskan beberapa menu dari aplikasi Monitoring Trafik dan Pengaturan PC Router berbasis Web.



a. *Add/remove user*

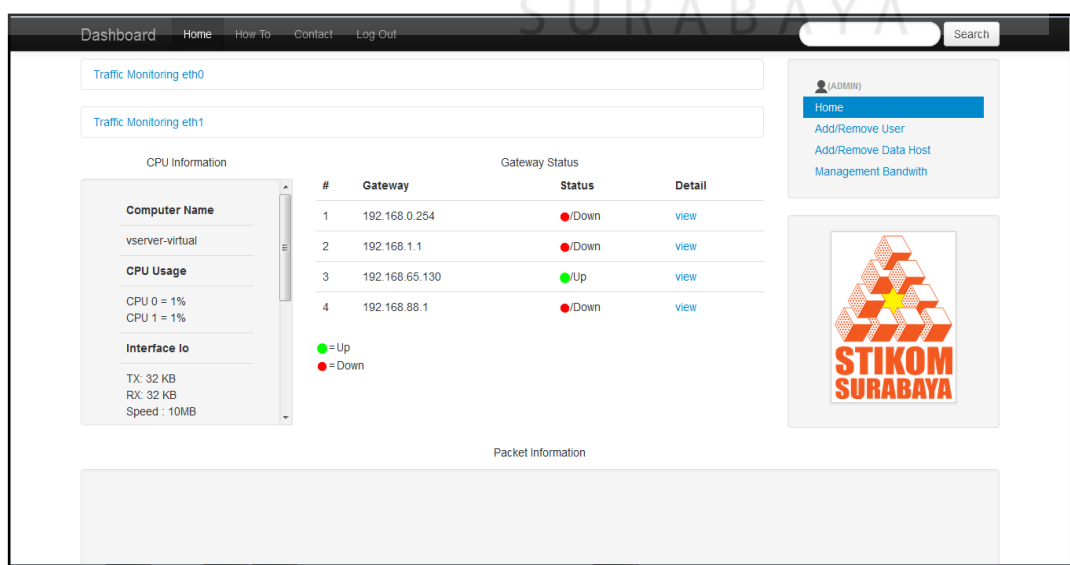
Menu *Add/remove user* akan mengarahkan halaman pada manajemen *user* dimana pada halaman manajemen *user* yang ditunjukkan pada Gambar 4.34 hanya dapat diakses oleh pengguna level admin. Pada halaman ini admin dapat membuat *user* baru dengan level pengguna admin atau *user*, mengubah level pengguna, menghapus data pengguna.

b. *Add/remove Data Host*

Menu *add/remove data host* yang mengarahkan pada halaman manajemen data *host* ditunjukkan pada Gambar 4.35 dapat memfasilitasi admin untuk mengisi, mengubah, menghapus data dari masing-masing *host* dan *gateway* yang akan dimonitoring pada aplikasi.

c. *Manajemen Bandwith*

Menu manajemen *host* yang mengarahkan pada halaman manajemen jaringan untuk pembatasan *bandwith* dan pemblokiran *website* ditunjukkan pada Gambar 4.36



Gambar 4.31 Halaman *Home Level Admin*

Dashboard Home How To Contact Log Out Search

Traffic Monitoring eth0

Traffic Monitoring eth1

CPU Information

Computer Name  
vserver-virtual

CPU Usage  
CPU 0 = 15%  
CPU 1 = 17%

Interface I/O  
TX: 394 KB  
RX: 394 KB  
Speed : 10MB

Gateway Status

#	Gateway	Status	Detail
1	192.168.0.254	Down	<a href="#">View</a>
2	192.168.1.1	Up	<a href="#">View</a>
3	192.168.65.130	Up	<a href="#">View</a>
4	192.168.88.1	Down	<a href="#">View</a>

Packet Information

```
22:04:40.299396 IP vserver-virtual.local.53852 > mistletoe.canonical.com.http: Flags [S], seq 13466874, win 14600, options [mss 1460,sackOK,TS val 4294916134 ecr 0,nop,wscale 4], length 0
22:04:41.296420 IP vserver-virtual.local.53852 > mistletoe.canonical.com.http: Flags [S], seq 13466874, win 14600, options [mss 1460,sackOK,TS val 4294916384 ecr 0,nop,wscale 4], length 0
22:04:41.571848 IP vserver-virtual.local.43931 > jujube.canonical.com.http: Flags [S], seq 3945407050, win 14600, options [mss
```

Gambar 4.32 Halaman *Home Level User*

(ADMIN)

- Home
- Add/Remove User
- Add/Remove Data Host
- Management Bandwith

(USER)

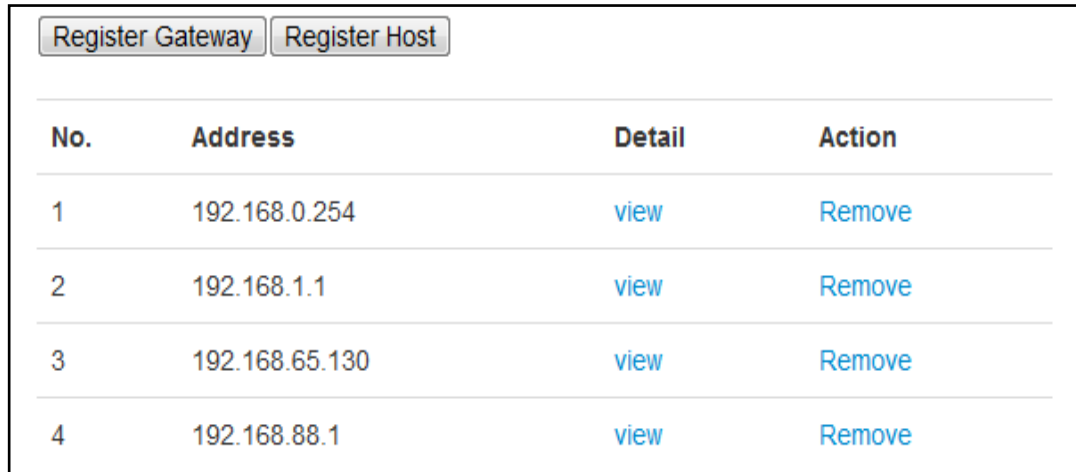
- Home
- Management Bandwith

Gambar 4.33 Navigasi Menu *Level Admin dan User*

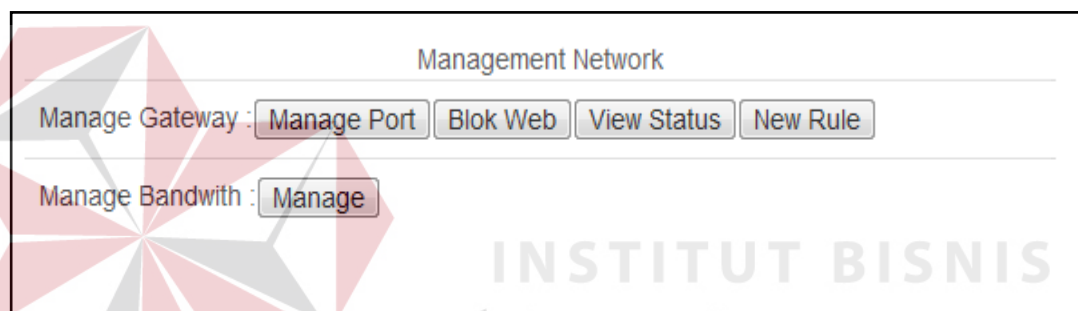
Add user

No.	User Name	Level	Action
1	admin	admin	<a href="#">Edit</a>   <a href="#">Remove</a>
2	demo	user	<a href="#">Edit</a>   <a href="#">Remove</a>
3	user	user	<a href="#">Edit</a>   <a href="#">Remove</a>

Gambar 4.34 Halaman *Add/remove User*



No.	Address	Detail	Action
1	192.168.0.254	<a href="#">view</a>	<a href="#">Remove</a>
2	192.168.1.1	<a href="#">view</a>	<a href="#">Remove</a>
3	192.168.65.130	<a href="#">view</a>	<a href="#">Remove</a>
4	192.168.88.1	<a href="#">view</a>	<a href="#">Remove</a>

Gambar 4.35 Halaman *Add/remove Data Host*Gambar 4.36 Halaman *Management Network*

### 3. CPU Information

Pada *widget* bagian kiri dari halaman utama/*dashboard* dapat dilihat informasi tentang CPU dan informasi tambah lainnya ditunjukkan pada Gambar 4.37 seperti *computer hostname* dan *network interface card*. Pengambilan data menggunakan protokol SNMP oleh *network station management* kepada *agent*. Data dari MIB diambil dan disalin pada *temporary file* bernama *result.txt* pada direktori */tmp* yang tunjukan pada Gambar 4.38. beberapa objek yang disalin adalah:

a. `hrDeviceDescr`

objek untuk melihat informasi *type* CPU ditunjukkan pada Gambar 4.39.

b. `sysName`

objek untuk melihat informasi nama dari *computer (hostname)* ditunjukkan pada Gambar 4.40.

c. `hrProcessorLoad`

objek untuk melihat penggunaan CPU ditunjukkan pada Gambar 4.41.

d. `ifDescr`

objek untuk mengetahui deskripsi dari NIC yang digunakan oleh *agent* ditunjukkan pada Gambar 4.42.

e. `ifInOctets`

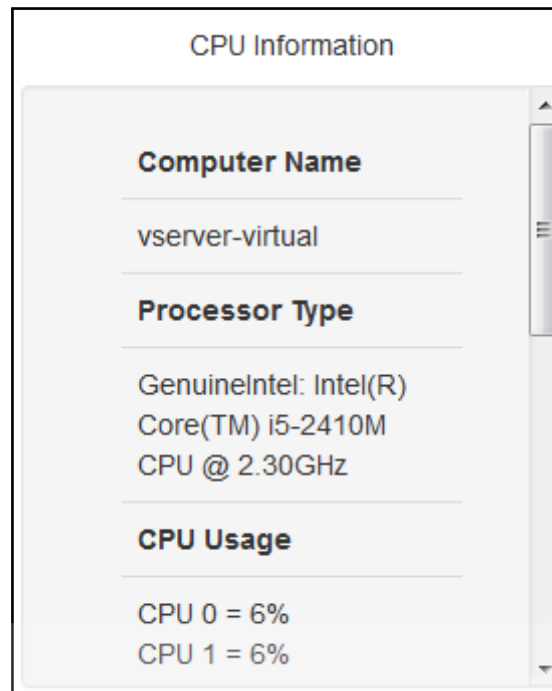
Objek yang digunakan untuk mengetahui akumulasi *receive packet* yang masuk pada sebuah *interface* dalam bentuk *byte* yang pada aplikasi ini akan di *convert* menjadi *kilobyte* ditunjukkan pada Gambar 4.43.

f. `ifOutOctets`

Objek yang digunakan untuk mengetahui akumulasi transmit *packet* yang keluar pada sebuah *interface* dalam bentuk *byte* yang pada aplikasi ini akan di *convert* menjadi *kilobyte* ditunjukkan pada Gambar 4.44.

g. `ifSpeed`

*Maximum bandwidth* dari sebuah *interface* ditunjukkan pada Gambar 4.45 dan pada aplikasi ini juga di *convert* menjadi *megabyte*.



Gambar 4.37 CPU Information

The screenshot shows a text editor window titled "result.txt (/tmp) - gedit" with the following content:

```
SNMPv2-MIB::sysORUpTime.8 = Timeticks: (80) 0:00:00.80
IF-MIB::ifNumber.0 = INTEGER: 3
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifDescr.1 = STRING: lo
IF-MIB::ifDescr.2 = STRING: eth0
IF-MIB::ifDescr.3 = STRING: eth1
IF-MIB::ifType.1 = INTEGER: softwareLoopback(24)
IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.3 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifMtu.1 = INTEGER: 16436
IF-MIB::ifMtu.2 = INTEGER: 1500
IF-MIB::ifMtu.3 = INTEGER: 1500
IF-MIB::ifSpeed.1 = Gauge32: 10000000
IF-MIB::ifSpeed.2 = Gauge32: 0
IF-MIB::ifSpeed.3 = Gauge32: 0
IF-MIB::ifPhysAddress.1 = STRING:
IF-MIB::ifPhysAddress.2 = STRING: 0:50:56:3b:a5:49
IF-MIB::ifPhysAddress.3 = STRING: 0:c:29:bf:a:79
IF-MIB::ifAdminStatus.1 = INTEGER: up(1)
IF-MIB::ifAdminStatus.2 = INTEGER: up(1)
IF-MIB::ifAdminStatus.3 = INTEGER: up(1)
IF-MIB::ifOperStatus.1 = INTEGER: up(1)
IF-MIB::ifOperStatus.2 = INTEGER: up(1)
IF-MIB::ifOperStatus.3 = INTEGER: up(1)
IF-MIB::ifLastChange.1 = Timeticks: (0) 0:00:00.00
IF-MIB::ifLastChange.2 = Timeticks: (0) 0:00:00.00
IF-MIB::ifLastChange.3 = Timeticks: (0) 0:00:00.00
```

Gambar 4.38 Temporary File result.txt

HOST-RESOURCES-MIB::hrDeviceDescr.768 = STRING: GenuineIntel: Intel(R) Core(TM) i5-2410M CPU @ 2.30GHz  
 HOST-RESOURCES-MIB::hrDeviceDescr.769 = STRING: GenuineIntel: Intel(R) Core(TM) i5-2410M CPU @ 2.30GHz

**Processor Type**  
 GenuineIntel: Intel(R)  
 Core(TM) i5-2410M  
 CPU @ 2.30GHz

Gambar 4.39 Informasi *Type* CPU

SNMPv2-MIB::sysContact.0 = STRING: Me <me@example.com>  
 SNMPv2-MIB::sysName.0 = STRING: vserver-virtual  
 SNMPv2-MIB::sysLocation.0 = STRING: Setting on +

**Computer Name**  
 vserver-virtual

Gambar 4.40 Nama Komputer (*hostname*)

HOST-RESOURCES-MIB::hrProcessorLoad.768 = INTEGER: 8  
 HOST-RESOURCES-MIB::hrProcessorLoad.769 = INTEGER: 10

**CPU Usage**  
 CPU 0 = 8%  
 CPU 1 = 10%

Gambar 4.41 Penggunaan CPU

IF-MIB::ifDescr.1 = STRING: lo  
 IF-MIB::ifDescr.2 = STRING: eth0  
 IF-MIB::ifDescr.3 = STRING: eth1

➔

<b>Interface lo</b>
TX: 22272 KB RX: 22272 KB Speed : 10MB
<b>Interface eth0</b>
TX: 171 KB RX: 2328 KB Speed : 0MB
<b>Interface eth1</b>

Gambar 4.42 Informasi *Interface Card*

IF-MIB::ifLastChange.3 = Timeticks: (0) 0:00  
 IF-MIB::ifInOctets.1 = Counter32: 25612430  
 IF-MIB::ifInOctets.2 = Counter32: 2561289

➔ RX: 25404 KB

convert ke kilobyte

Gambar 4.43 Informasi Akumulasi Paket Data Masuk

IF-MIB::ifOutOctets.1 = Counter32: 28802359  
 IF-MIB::ifOutOctets.2 = Counter32: 199835  
 IF-MIB::ifOutOctets.3 = Counter32: 9019134

➔ TX: 28128 KB

convert ke kilobyte

Gambar 4.44 Informasi Akumulasi Paket Data Keluar

IF-MIB::ifSpeed.1 = Gauge32: 10000000  
 IF-MIB::ifSpeed.2 = Gauge32: 0

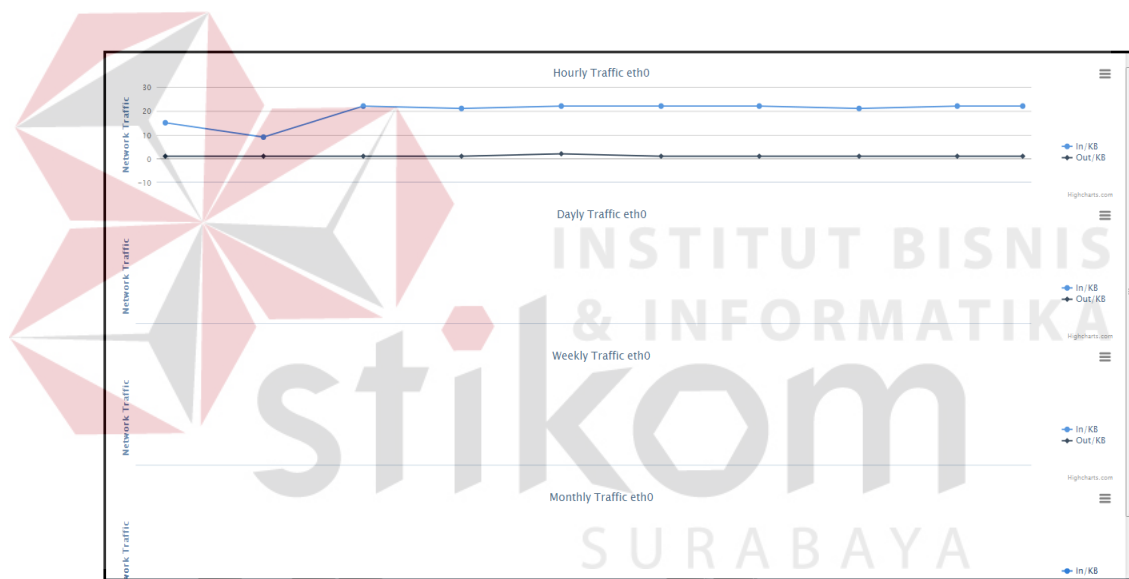
➔ RX: 30464 KB  
Speed : 10MB

conver ke megabyte

Gambar 4.45 *Interface Bandwith*

#### 4. Traffic Monitoring

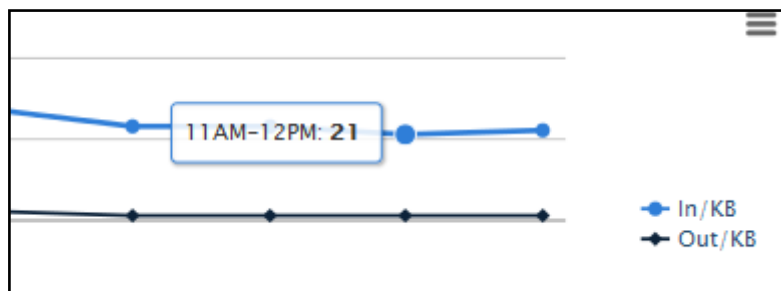
Pada halaman *home* tersedia modul *Traffic* monitoring ditunjukkan pada Gambar 4.46 menggambarkan secara *visual graphic* dalam hitungan permenit, perhari, perminggu, perbulan. Dengan perhitungan  $ifInOctets - \Delta ifInOctet / delay$  dan  $ifOutOctets - \Delta ifOutOctet / delay$ . Informasi yang diambil untuk dijadikan bahan perhitungan nilai tertinggi trafik jaringan perhari sampai perbulan diambil dari nilai *maximum ifInOctets* dan *ifOutOctets* dari agent yang dimonitoring.



Gambar 4.46 Traffic Monitoring

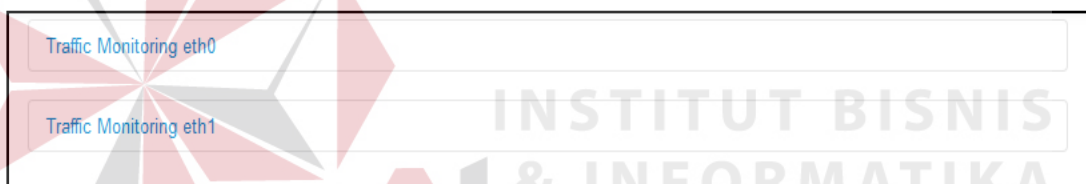
Pada Gambar 4.47 akan ditunjukkan bagaimana membaca trafik tersebut. Trafik yang sudah divisualisasikan adalah hasil dari penyimpanan pada CPU info yang kebutuhan untuk *ifInOctets* dan *ifOutOctets* disimpan dalam sebuah basis data dan diolah menjadi sebuah *graphic*.





Gambar 4.47 tooltip hasil perhitungan akumulasi paket data dalam *kilobyte*

Hal yang sama dilakukan juga pada perhitungan perhari, perminggu dan perbulan. Pada Gambar 4.48 menunjukkan akumulasi paket data permenit adalah 21KB/s untuk paket masuk. Pada aplikasi ini menampilkan 2 *ethernet card* yaitu eth0 akses *internet* dan eth1 lokal area ditunjukkan pada Gambar 4.48.



Gambar 4.48 Trafik Monitoring *Ethernet Card*

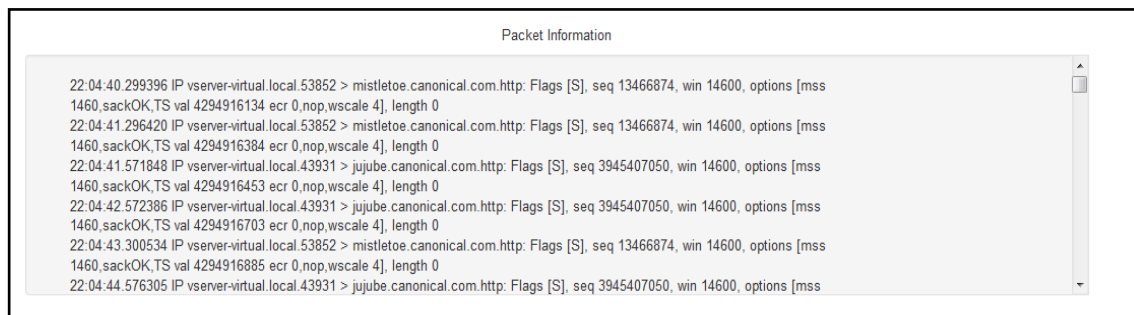
## 5. Packet Information

Masih pada halaman *Home* dimana kita dapat melihat *packet information* ditunjukkan pada Gambar 4.47 adalah informasi paket data transaksi *in/out* dan data yang diambil didapatkan dari aplikasi TCPDUMP yang disalin dalam *file temporary* bernama sniff.txt dapat dilihat pada Gambar 4.48 yang disimpan pada direktori */tmp*. Berikut akan dijelaskan untuk membaca *output* dari hasil *capture packet* dengan TCPDUMP.

- a. 22:04:45.133121 > baris ini terletak pada awal *capture*, yang dimaksud dari baris ini adalah waktu request terhadap *destination* dan *source address*.
- b. IP > adalah IP(protocol) pengaturan yang terkait.

- c. tos 0x0 > jenis bidang layanan
- d. ttl 64 > adalah suatu nilai waktu yang disematkan dalam paket data yang dikirimkan melalui jaringan TCP/IP untuk menyatakan berapa lama paket tersebut bisa beredar/berjalan di dalam jaringan. Nilai tersebut akan memberitahukan kepada router apakah paket tersebut harus diteruskan ke *router selajutnya (next hop router)* atau di-*discard*.
- e. id 33646 > ini adalah sebuah id paket, jadi pada permasalahan ini, ini adalah *SYN request*, hasil replay akan menjadi ACK jika host sedang *online* dan id paket akan sama.
- f. [DF] > berarti paket tidak terpecah-pecah[F].
- g. Proto TCP > adalah *type* dari sebuah protokol(UDP, ICMP).
- h. Length 60 > panjang dari sebuah paket.
- i. 192.168.1.4.33922 > maksud dari informasi ini adalah alamat ip *address* 192.168.1.4 dan port yang digunakan *client* adalah 33922.
- j. alkes.canonical.com.http > adalah *destination address* yang dikunjungi oleh *client*.
- k. Flags [S] > adalah sebuah TCP SYN, pada permasalahan ini adalah ACK dari server, [R] adalah *reset*, [F] transfer sudah selesai, [P] berarti data harus di kirim.
- l. cksum 0x83ae (correct) > ini adalah sebuah TCP header – check sum paket(untuk memeriksa integritas paket).
- m. seq 4011514848 > ini adalah TCP *sequence number*.
- n. win 5840 > jumlah yang dikirimkan sebelum membutuhkan paket ACK kembali dari server.

- o. options [mss 1460,sackOK,TS val 612494 ecr 0,nop,wscale 6] > sebuah TCP option.
- p. length 0 > ini adalah nilai panjang dari sebuah paket.



Gambar 4.49 Packet Information



Gambar 4.50 Destination Packet

Dari gambar 4.48 akan diberikan contoh membaca *output*:

```

22:04:41.296420 IP vserver-virtual.local.53852 > mistletoe.canonical.com.http:
Flags [S], seq 13466874, win 14600, options [mss 1460,sackOK,TS val
4294916384 ecr 0,nop,wscale 4], length 0

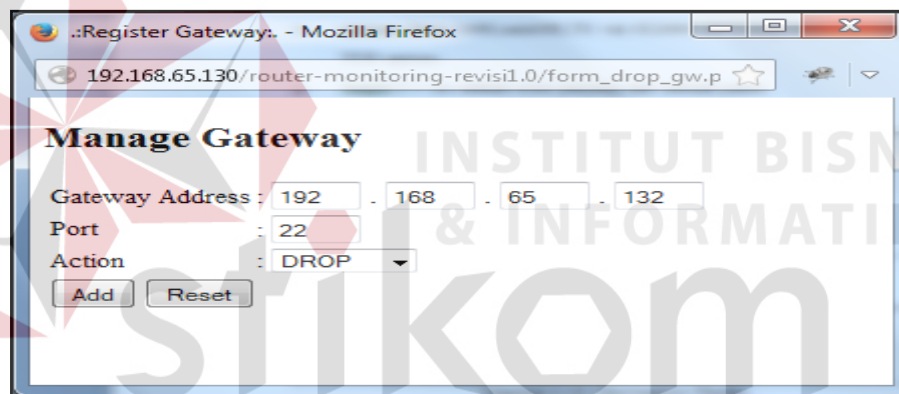
```

- a. Transaksi paket pukul 22:04:41.
- b. *Hostname* vserver-virtual dengan port dari client 53852.
- c. *Destination address* atau alamat tujuan adalah mistletoe.canonical.com.http.
- d. Nomor *sequence* TCP adalah 13466874.
- e. Win 14600 adalah jumlah yang dikirimkan sebelum ACK kembali dari server.

- f. *options* [mss 1460,sackOK,TS val 4294916384 ecr 0,nop,wscale 4], *length* 0 adalah sebuah TCP *option* yang digunakan.

## 6. Manajemen *Bandwith*

Pada halaman manajemen *bandwith* seperti yang ditunjukkan pada Gambar 4.35 terdapat beberapa *option* yaitu *manage port* dengan *default port* 80 ditunjukkan pada Gambar 4.49, blok *web* yang ditunjukkan pada Gambar 4.50, *new rule* ditunjukkan pada Gambar 4.51 dan *view status* ditunjukkan pada Gambar 4.52. kemudian ada *manage bandwith* yang ditunjukkan pada Gambar 4.53.



Manage Gateway

Gateway Address : 192 . 168 . 65 . 132

Port : 22

Action : DROP

Add Reset

Gambar 4.51 *Manage port*



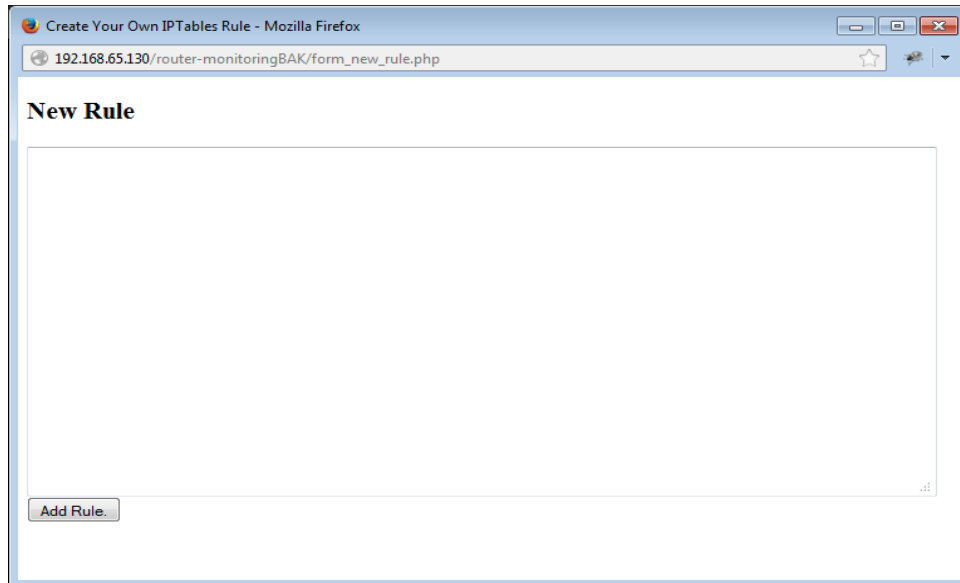
Manage Gateway

Website Address : www.kaskus.co.id

Port : 80

Add Reset

Gambar 4.52 *Blok Website*



Gambar 4.53 New Rule Gateway

Dari Gambar 4.53 dapat dilihat akan dicontoh menginputkan sebuah alamat atau ip *address* yang tidak diijinkan untuk mengkases *port 22*, hasil dari Gambar 4.49 dapat dilihat pada Gambar 4.54. Dan pada Gambar 4.55 dicontohkan admin ingin membloki situs [www.kaskus.com](http://www.kaskus.com) dengan port 80 yaitu unuk HTTP dan hasilnya akan di tunjukan pada Gambar 4.54.

```
Chain INPUT (policy ACCEPT)
target    prot opt source                destination
DROP     tcp  --  192.168.65.132        0.0.0.0/0            tcp dpt:22

Chain FORWARD (policy ACCEPT)
target    prot opt source                destination
```

Gambar 4.54 Blok Port 22

```
Chain FORWARD (policy ACCEPT)
target    prot opt source                destination
DROP     tcp  --  0.0.0.0/0             103.6.117.3          tcp dpt:80
DROP     tcp  --  0.0.0.0/0             103.6.117.2          tcp dpt:80

Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
```

Gambar 4.55 Blok Situs kaskus.co.id

Berikut adalah beberapa contoh untuk pembuatan *new rule* agar bisa membuat sebuah aturan baru sesuai dengan keinginan dari admin jaringan tersebut:

- a. Blokir semua akses ke ip 202.152.12.15

```
iptables -A OUTPUT -d 202.152.12.15 -j DROP
```

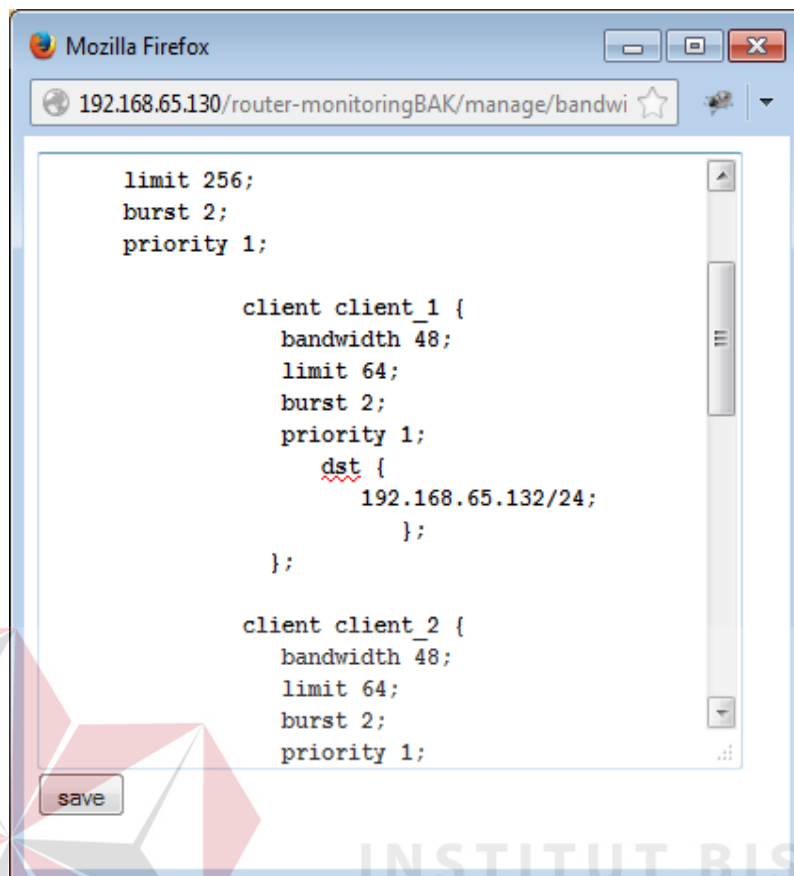
- b. *Block Outgoing*/blok akses keluar berdasarkan *port*

```
iptables -A OUTPUT -p tcp --dport 8080 -j DROP
```

- c. Blok port 8080 pada ip 171.16.100.1

```
iptables -A OUTPUT -p tcp -d 171.16.100.1 --dport 8080 -j DROP
```

Berikutnya adalah pembagian *bandwith* berdasarkan IP *address* maupun *gateway*, *form limit bandwith* ditunjukkan pada Gambar 4.56. pada pembagian *bandwith* menggunakan HTB-tools, nilai awal HTB-tools menggunakan bit, contoh 64kbit/s maka *bandwith* yang didapat oleh *client* adalah 8KB/s dimana perhitungannya adalah  $64/8 = 8$ .



```

limit 256;
burst 2;
priority 1;

client client_1 {
    bandwidth 48;
    limit 64;
    burst 2;
    priority 1;
    dst {
        192.168.65.132/24;
    };
};

client client_2 {
    bandwidth 48;
    limit 64;
    burst 2;
    priority 1;
};

```

Gambar 4.56 *Limit Bandwith*

Dari hasil Gambar 4.56 client dengan ip *address* 192.168.65.132/24 mendapatkan *bandwith* maksimal 8KB/s karena batas maksimal atau limit *bandwithnya* adalah 64kb/s.

## 7. Monitoring Host Up

Pada halaman pertama *Home* dapat dilihat ada *gateway* status yang berisikan alamat *gateway* dan masing-masing *client* yang menggunakan *gateway* tersebut untuk akses jaringan. Gambar untuk monitoring *host up* dapat dilihat pada Gambar 4.55. Untuk mengetahui apakah *client* merespon *request* dari server maka menggunakan utilitas “PING” sehingga server mendapatkan *replay* dari *client* yang dituju.

Gateway Status			
#	Gateway	Status	Detail
1	192.168.0.254	●/Down	<a href="#">view</a>
2	192.168.1.1	●/Up	<a href="#">view</a>
3	192.168.65.130	●/Up	<a href="#">view</a>
4	192.168.88.1	●/Down	<a href="#">view</a>

● = Up  
● = Down

Gambar 4.57 Monitoring Host Up

Masing-masing *host* dapat dilihat pada *view button* pada tabel *detail* yang ditunjukkan pada gambar 4.57, dimana berisikan alamat IP dari masing-masing *host* yang menggunakan *gateway* pada jaringan tersebut.

Host Status					
#	IP Address	Gateway	MAC Address	Hostname	Status
1	192.168.65.132	192.168.65.130	xx-xx-xx-xx	pc1	●/Up

● = Up  
● = Down

Gambar 4.58 View Host Status



### 4.1.3 Rancangan Basis Data

Pada tahap ini akan dirancangan sebuah basis data dimana untuk membangun sistem penyimpana aplikasi Monitoring Trafik dan Pengaturan PC Router Berbasis Web. Berikut adalah struktur tabel basis data Monitoring Trafik dan Pengaturan PC Router Berbasis Web:

1. Nama Tabel : user

PK : id\_user

Tabel 4.4 Struktur Tabel User

No.	Nama Atribut	Type Data	Panjang	Deskripsi
1	id_user	int	2	id pengguna
2	nama_user	varchar	50	nama pengguna
3	password	varchar	50	password pengguna
4	level	enum	admin','user'	level pengguna

2. Nama Tabel : menu

PK : id\_menu

Tabel 4.5 Struktur Tabel Menu Pada Halaman Utama

No.	Nama Atribut	Type Data	Panjang	Deskripsi
1	id_menu	int	2	id menu dashboard
2	link	varchar	50	Alamat file yang dituju
3	file	varchar	50	Nama file yang dituju
4	level	enum	admin','user'	level pengguna

3. Nama Tabel : modul

PK : id\_modul

Tabel 4.6 Struktur Tabel Modul Untuk Memanggil Alamat File Pada Menu

No.	Nama Atribut	Type Data	Panjang	Deskripsi
1	id_modul	int	2	id modul
2	Nama_modul	varchar	50	Nama modul untuk pemanggilan menu
3	link	varchar	100	Alamat untuk menuju ke menu
4	level	enum	'admin','user'	level pengguna
5	Aktif	enum	'N','Y'	Status Modul

4. Nama Tabel : ipaddress

PK : id

Tabel 4.7 Struktur Tabel IPAddress Untuk Alamat Host

No.	Nama Atribut	Type Data	Panjang	Deskripsi
1	id	int	11	id ipaddress
2	ipAdd	varchar	15	Alamat host
3	gateway	varchar	15	Alamat gateway masing-masing host
4	macAdd	varchar	20	Alamat fisik masing-masing host
5	hostname	varchar	25	Nama dari host

5. Nama Tabel : gateway

PK : id

Tabel 4.8 Struktur Tabel Gateway Untuk Alamat Gateway Jaringan

No.	Nama Atribut	Type Data	Panjang	Deskripsi
1	id	int	11	id gateway
2	Gateway	varchar	15	Alamat gateway

6. Nama Tabel : totalOctets

PK : no

Tabel 4.9 Struktur Tabel totalOctets

No.	Nama Atribut	Type Data	Panjang	Deskripsi
1	No	int	11	No total octets
2	interface	varchar	15	Nama ethernet card
3	ifInOctets	int	11	Total octets masuk
4	ifOutOctets	int	11	Total octets keluar
5	timespan	varchar	50	Waktu perhitungan penyimpanan total octets

7. Nama Tabel : minuteOctets

PK : no

Tabel 4.10 Struktur Tabel minuteOctets

No.	Nama Atribut	Type Data	Panjang	Deskripsi
1	no	int	11	No urut
2	interface	varchar	15	Nama ethernet card
3	ifInOctets	Int	11	Total octets masuk permenit
4	ifOutOctets	Int	11	Total octets keluar permenit
5	timespan	varchar	50	Waktu perhitungan penyimpanan total octets
6	waktu	Datetime		Tanggal dan waktu untuk perhitungan perhari
7	timestamp	bigint	100	Timestamp untuk perhitungan perhari

8. Nama Tabel : dayOctets

PK : no

Tabel 4.11 Struktur Tabel dayOctets

No.	Nama Atribut	Type Data	Panjang	Deskripsi
1	no	int	11	Nomor urut
2	interface	varchar	15	Nama ethernet card
3	ifInOctets	Int	11	Total octets masuk perhari
4	ifOutOctets	Int	11	Total octets keluar perhari
5	timespan	varchar	50	Waktu perhitungan penyimpanan total octets
6	waktu	Datetime		Tanggal dan waktu untuk perhitungan perminggu
7	timestamp	bigint	100	Timestamp untuk perhitungan perminggu

9. Nama Tabel : weekOctets

PK : no

Tabel 4.12 Struktur Tabel weekOctets

No.	Nama Atribut	Type Data	Panjang	Deskripsi
1	no	int	11	Nomor urut
2	interface	varchar	15	Nama ethernet card
3	ifInOctets	Int	11	Total octets masuk perminggu
4	ifOutOctets	Int	11	Total octets keluar perminggu
5	timespan	varchar	50	Waktu perhitungan penyimpanan total octets
6	waktu	Datetime		Tanggal dan waktu untuk perhitungan perbulan
7	timestamp	bigint	100	Timestamp untuk perhitungan perbulan

10. Nama Tabel : monthOctets

PK : no

Tabel 4.13 Struktur Tabel monthOctets

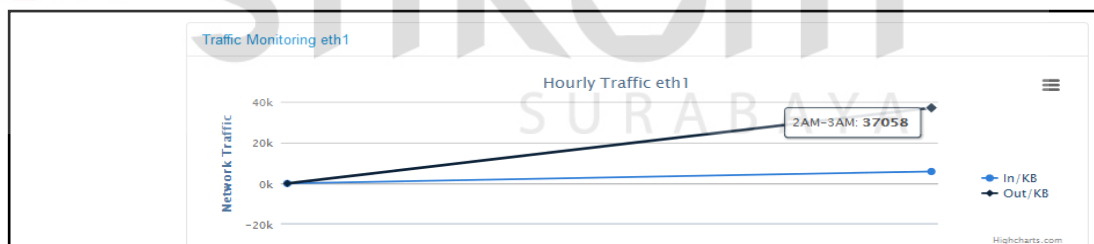
No.	Nama Atribut	Type Data	Panjang	Deskripsi
1	no	int	11	Nomor urut
2	interface	varchar	15	Nama ethernet card
3	ifInOctets	Int	11	Total octets masuk perbulan
4	ifOutOctets	Int	11	Total octets keluar perbulan
5	timespan	varchar	50	Waktu perhitungan penyimpanan total octets
6	waktu	Datetime		Tanggal dan waktu untuk perhitungan
7	timestamp	bigint	100	Timestamp untuk perhitungan

#### 4.1.4 Pengujian Black Box

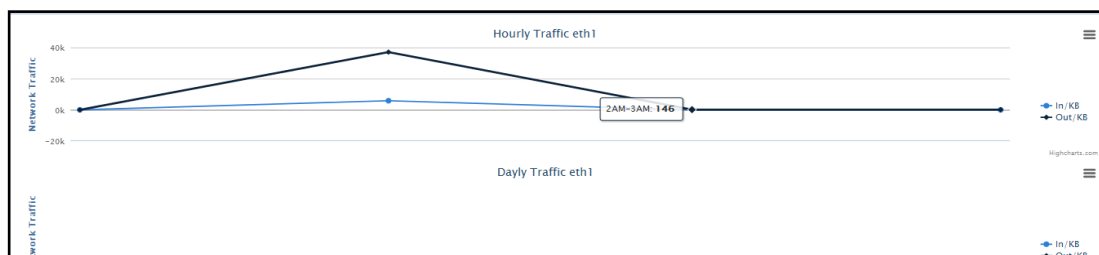
1. Uji Coba Trafik Monitoring
  - a. Trafik Monitoring permenit

Trafik monitoring otomatis *terupdate* setiap menitnya sampai 24jam.

Ditunjukkan pada Gambar 4.59 dan 4.60 contoh *interface eth1* pada **ifOutOctets**.

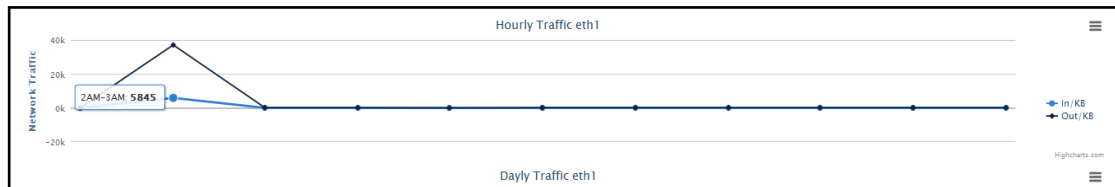


Gambar 4.59 *auto update* ifOutOctets *graphic* per menit

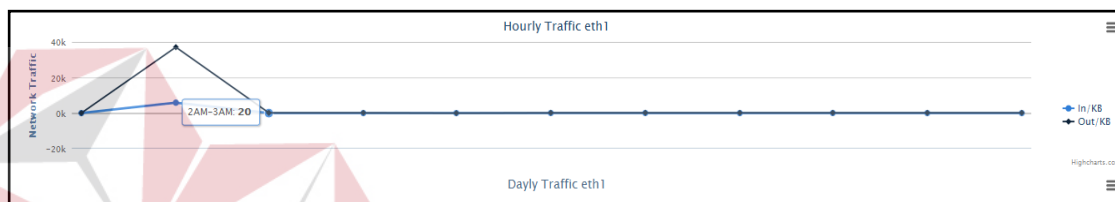


Gambar 4.60 *Update* ifOutOctets Persatu Menit Berikutnya

Ujicoba yang sama juga dilakukan untuk **ifInOctets** dimana keduanya *terupdate* otomatis secara bersamaan, *update ifInOctets* permenit dapat dilihat pada Gambar 4.61 dan menit berikutnya pada Gambar 4.62



Gambar 4.61 *Auto Update* Ifinoctets Per Satu Menit

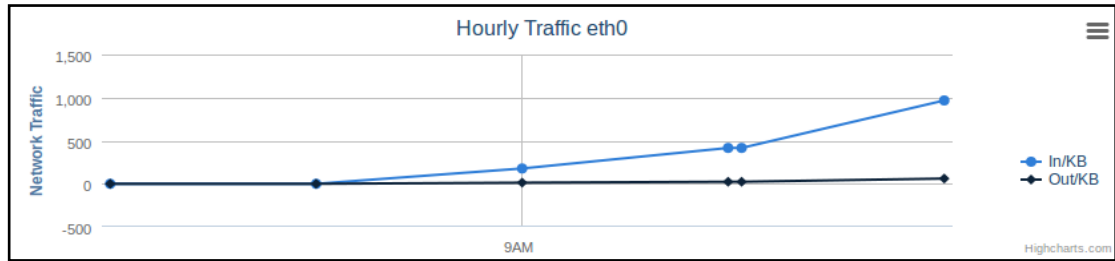


Gambar 4.62 *Update* Ifinoctets Persatu Menit Berikutnya

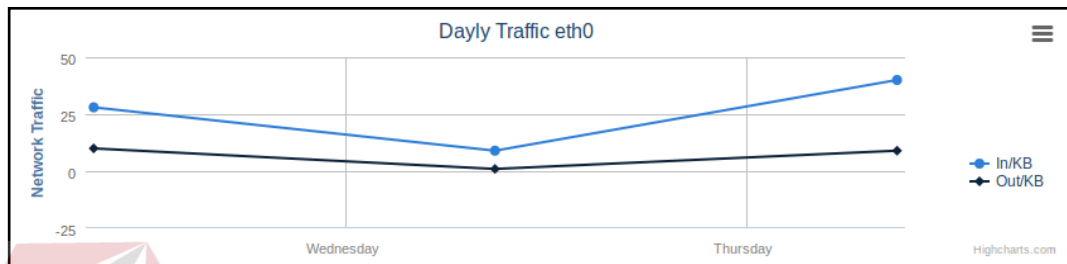
Dilihat kembali pada Gambar 4.59 dan 4.61 **ifOutOctets** akumulasi satu menit sebelumnya adalah 37058 KB kemudian satu menit berikutnya adalah 146 KB, sama dengan **ifOutOctets**, **ifInOctets** juga auto update permenitnya dari nilai awal 5845 KB pada Gambar 4.60 kemudian akumulasi paket data untuk satu menit berikutnya adalah 20 KB.

#### b. Trafik Monitoring Perhari

Setelah data permenit sudah mencapai 24 jam maka data permenit akan langsung terhapus ketika berganti hari ditunjukkan pada Gambar 4.63, data perhari adalah nilai tertinggi trafik dari data permenit yang di tunjukan pada Gambar 4.64. ujicoba dilakukan dengan cara mengganti tanggal pada OS agar langsung mendapatkan data baru yaitu akumulasi data perhari.



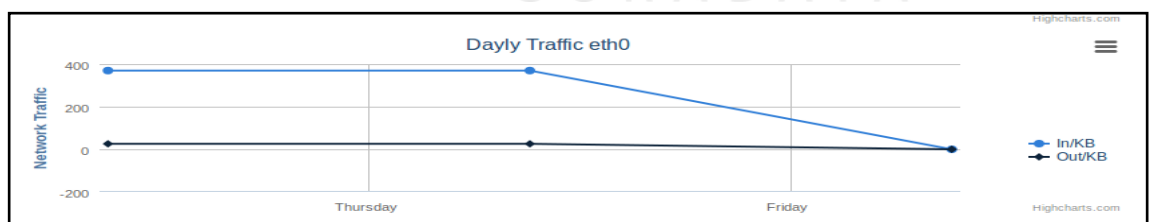
Gambar 4.63 Data Permenit Otomatis Terhapus



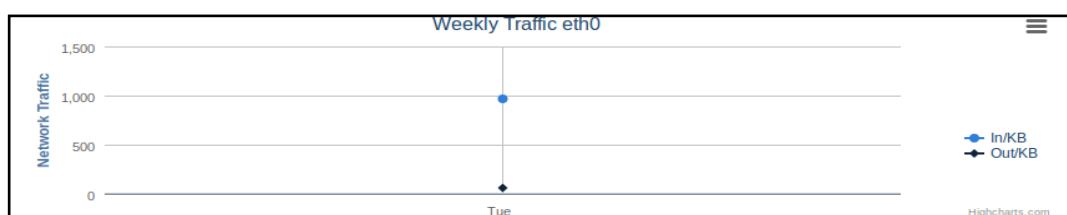
Gambar 4.64 Trafik Data Perhari

### c. Trafik Monitoring Perminggu

Sama dengan ujicoba perhari, tanggal pada OS akan dimajukan seminggu kemudian untuk mendapatkan hasil nilai tertinggi trafik data perhari selama tujuh hari akan langsung terhapus ditunjukkan pada Gambar 4.65 dan menjadi akumulasi data perminggu yang ditunjukkan pada Gambar 4.66.



Gambar 4.65 Trafik Data Perhari Terhapus



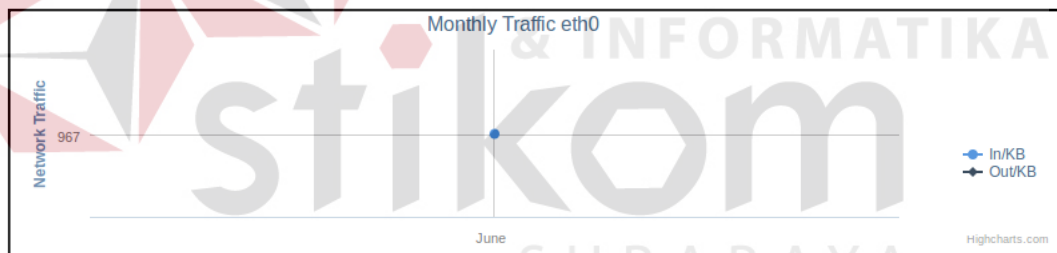
Gambar 4.66 Trafik Data Perminggu

d. Trafik Monitoring Perbulan

Trafik monitoring perbulan mempunyai sistem yang sama dengan permenit, perhari dan perminggu. Data dari perminggu akan hilang jika sudah berganti bulan ditunjukkan pada Gambar 4.67. Ujicoba dilakukan dengan memajukan angka bulan pada OS agar *output* trafik perbulan dapat terlihat ditunjukkan pada Gambar 4.68



Gambar 4.67 Data Perminggu Telah Terhapus



Gambar 4.68 Trafik Data Perbulan

2. Uji Coba Blok Port

Berikut akan dilakukan uji coba fungsi blok *port*, uji coba yang dilakukan adalah mencoba menutup akses ke *port* 22 pada *client* 192.168.65.1 dan server pada 192.168.65.130.



Register Gateway: - Mozilla Firefox

192.168.65.130/router-monitoring-revisi1.0/form\_drop\_gw.p

## Manage Gateway

Gateway Address : 192 . 168 . 65 . 1

Port : 22

Action : DROP

Add Reset

Gambar 4.69 Blok Port 22 Ip Address 192.168.65.1

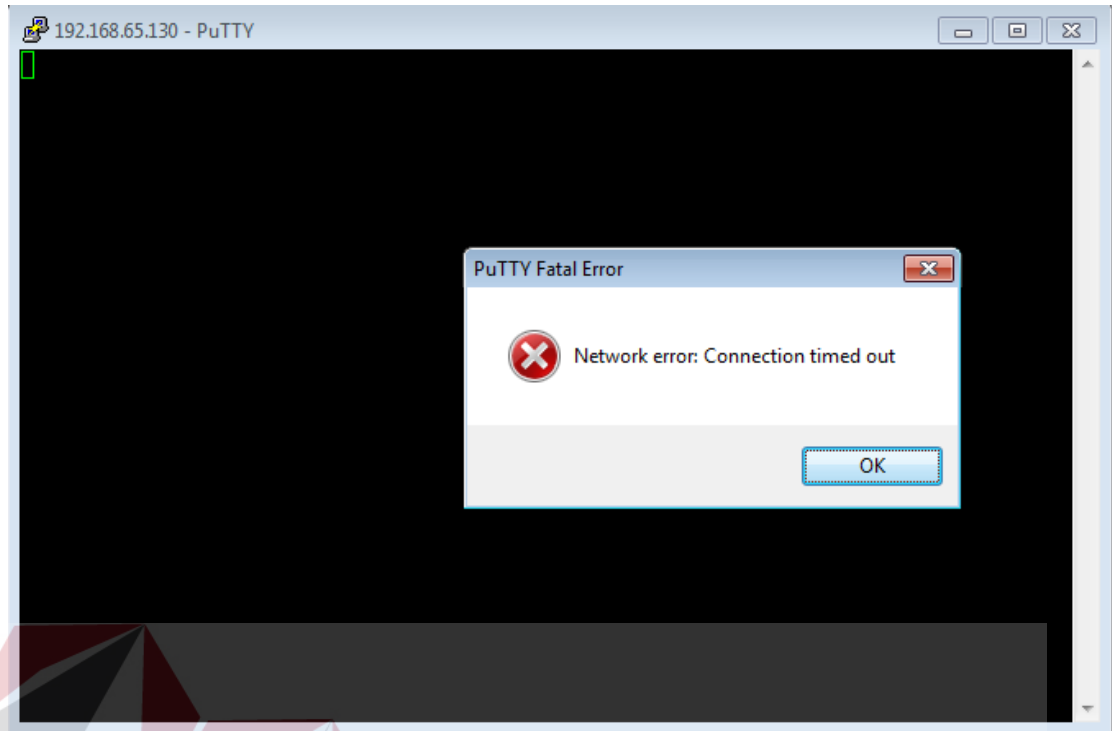
Mozilla Firefox

192.168.65.130/router-monitoringBAK/manage/iptab.php

```
Chain INPUT (policy ACCEPT)
target     prot opt source                destination           tcp dpt:22
DROP      tcp  -- 192.168.65.132        0.0.0.0/0             tcp dpt:22
DROP      tcp  -- 192.168.65.1         0.0.0.0/0             tcp dpt:22

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination           tcp dpt:80
DROP      tcp  -- 0.0.0.0/0            103.6.117.3          tcp dpt:80
DROP      tcp  -- 0.0.0.0/0            103.6.117.2          tcp dpt:80
```

Gambar 4.70 Rule Yang Masuk Untuk Port 22 Ip Address 192.168.65.1



Gambar 4.71 *Putty Gagal Connect Server*

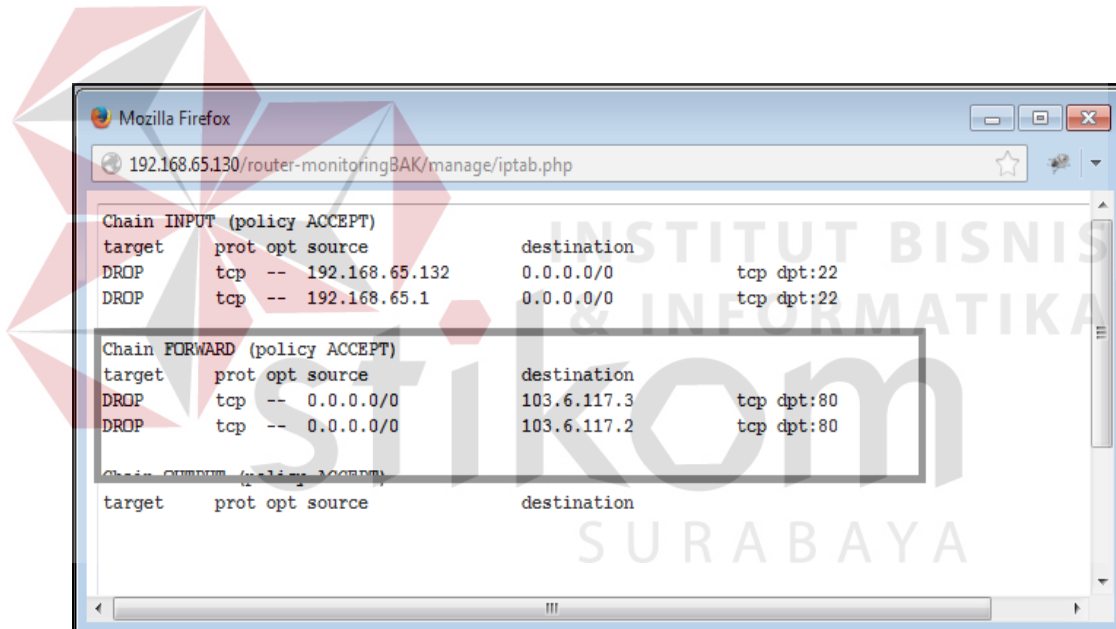
Pada Gambar 4.69 ditunjukkan bagaimana input data untuk *address* yang akan di tutup akses ke *port 22*, dan status untuk perlakuan tersebut dapat dilihat pada Gambar 4.70. hasil dari fungsi tersebut adalah *client* tidak bisa mengakses *port 22* untuk menuju server ditunjukkan pada Gambar 4.71.

### 3. Uji Coba Blok *Website*

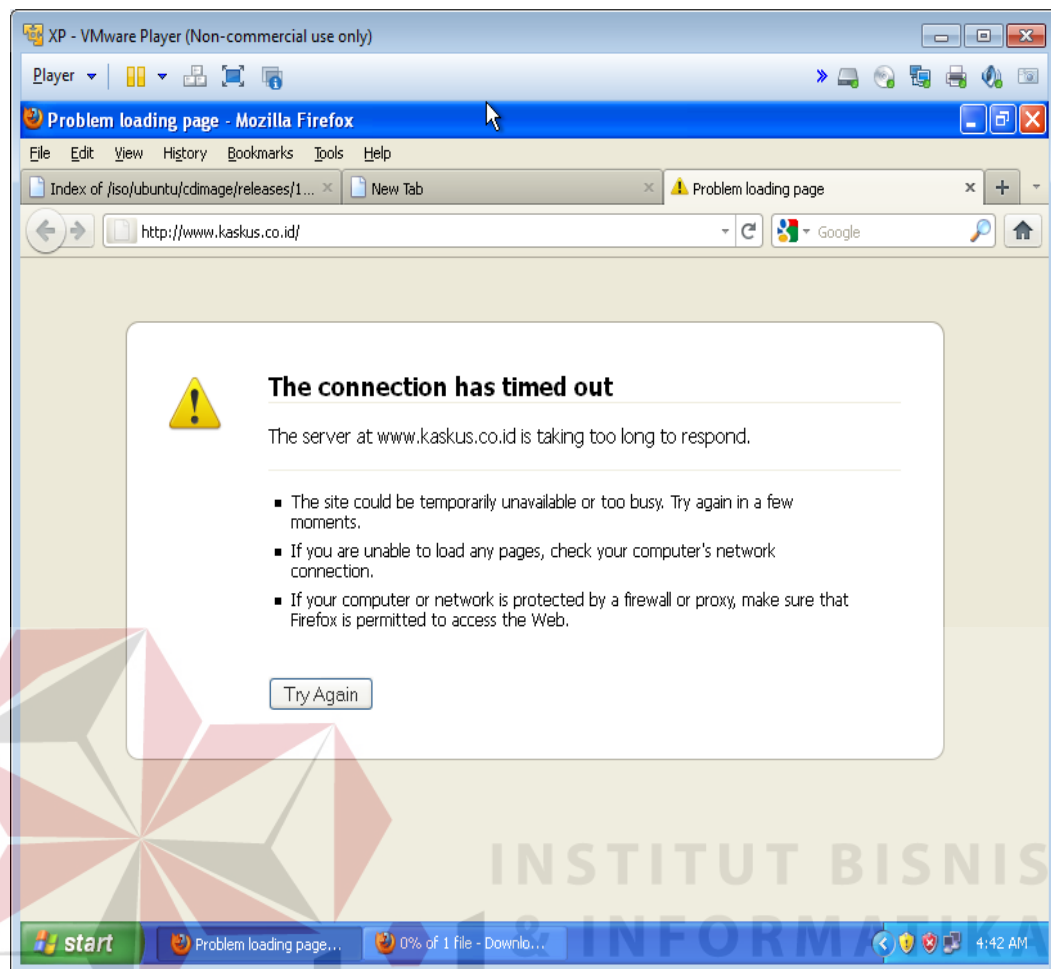
Uji coba berikutnya adalah uji coba untuk menutup website yang tidak boleh diakses. Contoh pada kasus ini adalah admin akan menutup akses pada situs [www.kaskus.co.id](http://www.kaskus.co.id).



Gambar 4.72 Input Alamat Web Dan Port



Gambar 4.73 Alamat Website Di Filter

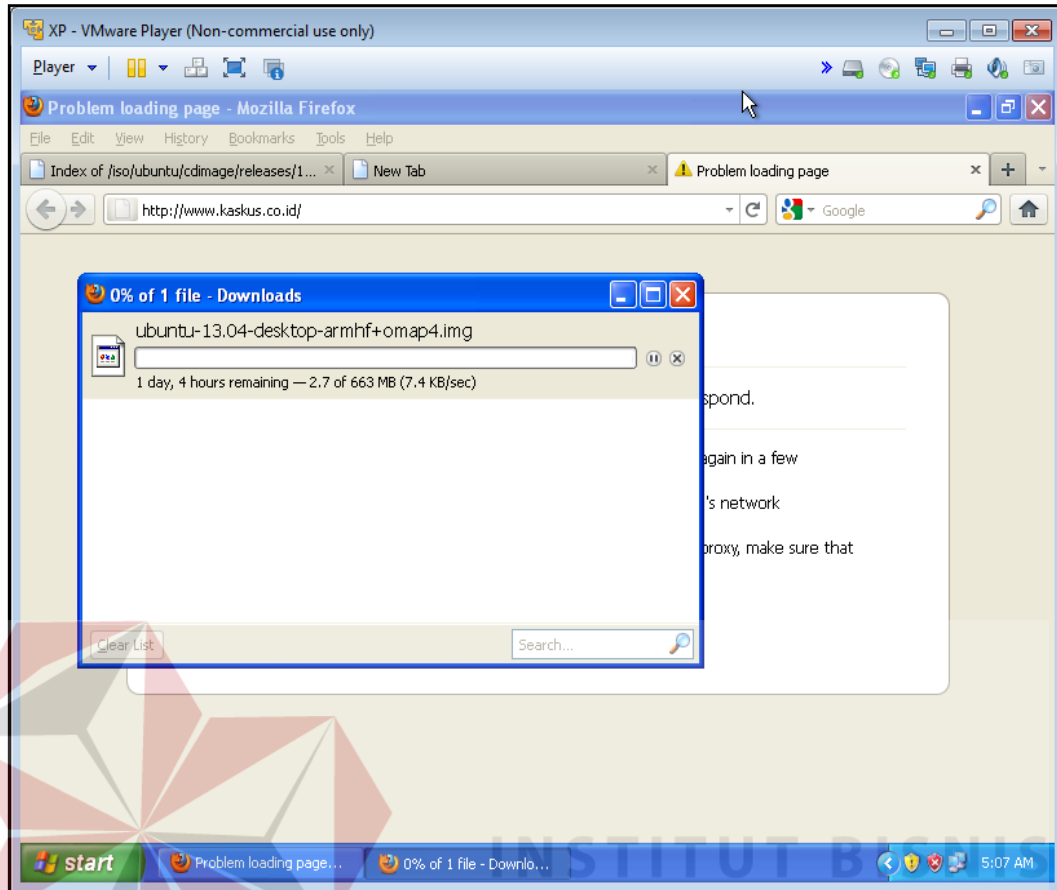


Gambar 4.74 Website Address Sudah Diblok

Pada Gambar 4.72 terdapat 2 *textbox* yaitu alamat *website* dan *port* (protokol), hasil input dapat dilihat pada Gambar 4.73 dan hasilnya dapat dilihat pada Gambar 4.74 dimana *website* sudah tidak bisa diakses.

#### 4. Uji Coba Limit *Bandwith*

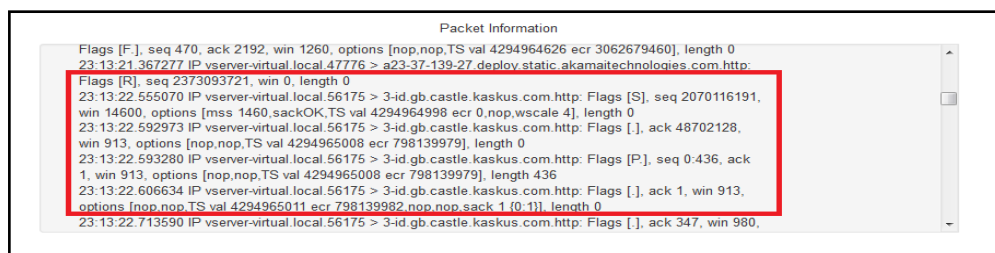
Uji Coba berikutnya adalah uji coba limitasi *bandwith*, sesuai dengan Gambar 4.75 dimana IP address 192.168.65.132 mendapatkan maksimal *bandwith* 64kb/s jika dihitung menjadi *kilobyte* adalah maksimal 8 KB/s. Hasil dari limit *bandwith* dapat dilihat pada Gambar 4.75.



Gambar 4.75 Limit Bandwith 8kbps

## 5. Uji Coba Packet Information

Berikutnya ada uji coba untuk melihat transaksi website, sebagai contoh pada *client* membuka site [www.kaskus.co.id](http://www.kaskus.co.id), maka sistem menunjukkan semua alamat yang menuju pada alamat [www.kaskus.co.id](http://www.kaskus.co.id) termasuk *sub domain*. Hasil uji coba dari *packet information* dapat dilihat pada Gambar 4.76.



Gambar 4.76 Hasil Capture Packet Information

#### 4.1.5 Pengujian Kepada Pengguna

Pada proses uji coba ini, *staff* termasuk kepala bagian LABKOM diharuskan mencoba fungsi dari aplikasi ini untuk mengetahui apakah sudah memenuhi *output* laporan yang diperlukan untuk kegiatan monitoring jaringan pada LABKOM STIKOM Surabaya. Ditinjau dari kebutuhan pengguna dimana dari perumusan masalah yang ada kebutuhan sistem seperti monitoring trafik jaringan lokal dan pengaturan PC *Router* yang sudah dirancang. Pengujian kepada *user* dilakukan dengan cara wawancara kepada pengguna yang terdapat pada lampiran, beberapa hal yang dibahas diwawancara tersebut adalah:

1. Fungsi-fungsi modul dari aplikasi Monitoring Trafik dan Pengaturan PC *Router* Berbasis *Web*.
2. Hasil *Output* informasi yang sesuai kebutuhan.
3. Kemudahan pemahanan pada desain visualisasi.

Berikut juga dilakukan uji coba dengan cara melakukan survey kepada 10 orang pengguna pada LABKOM dengan cara kuesioner pada lampiran. Dimana karakteristik pengguna dapat dilihat pada Tabel 4.14.

Tabel 4.14 Tabel Karakteristik Pengguna

No	Nama Pengguna	Jabatan	Total Nilai akhir
1	Ayuningtyas, S.Kom, M.MT	Kepala Bagian Labkom	24
2	Siswo Martono, S.Kom., M.M.	Kepala Sie Labkom	22
3	Tegar Heru Susilo, S.Kom.	Asisten Labkom	20
4	Kurniawan Jatmika, S.Kom.	Asisten Labkom	24
5	Ong Lu Ya	Asisten Labkom	22
6	Adrianus Wijaya, A.Md	Asisten Labkom	22
7	Edo Yonatan Koentjoro, S.Kom.	Asisten Labkom	23
8	Imaduddin Endri Wibowo	Asisten Labkom	23
9	Joshua Gabriell Suhendri	Asisten Labkom	20

Tabel 4.14 Tabel Karakteristik Pengguna

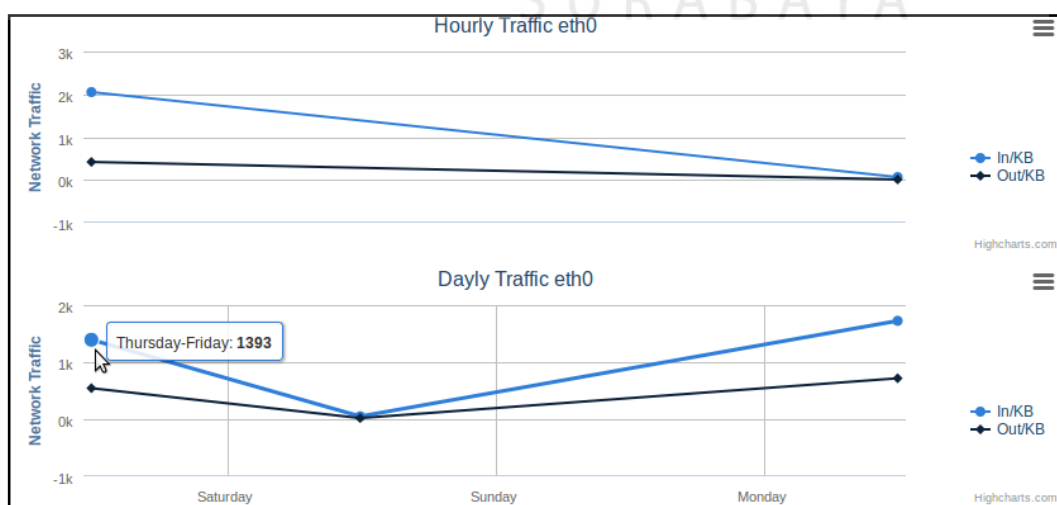
No	Nama Pengguna	Jabatan	Total Nilai akhir
10	Hoky Ajicahyadi	Asisten Labkom	23

#### 4.1.6 Pengujian Pada LABKOM

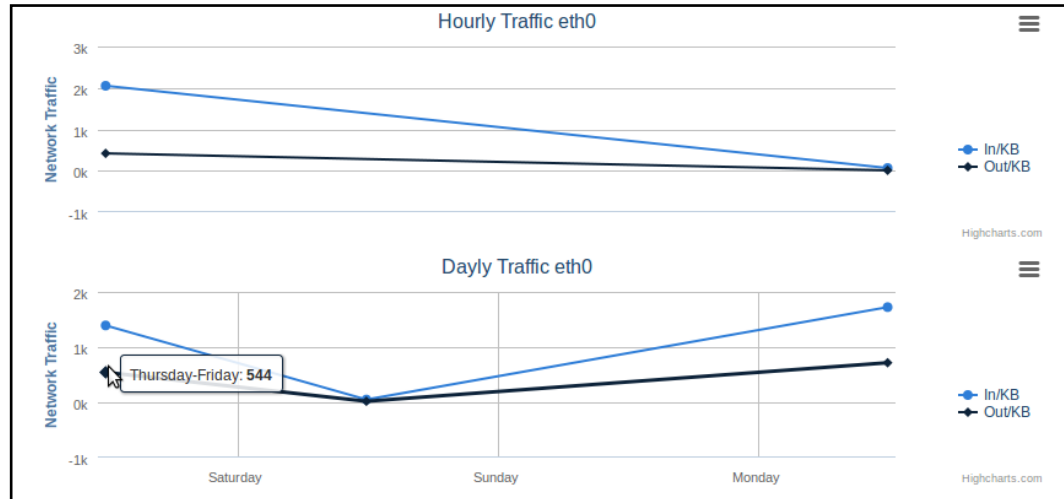
Pengujian berikutnya adalah pengujian langsung pada LABKOM. Sesuai dengan kebutuhan, pada proses ini di uji 2 fungsi utama yaitu trafik jaringan dan pengujian blok akses website.

##### 1. Pengujian Aplikasi Trafik Jaringan Pada LABKOM

Pengujian dilakukan selama 3 hari yaitu pada hari Kamis, Jumat dan hari Senin. Pada hari kamis, nilai tertinggi trafik masuk atau **ifInOctets** dari eth0 LABKOM adalah 1393KB dan nilai tertinggi trafik keluar atau **ifOutOctets** adalah 544KB. Gambar trafik hari Kamis nilai tertinggi trafik masuk dapat dilihat pada Gambar 4.77, dan Gambar nilai tertinggi trafik keluar dapat dilihat pada Gambar 4.78

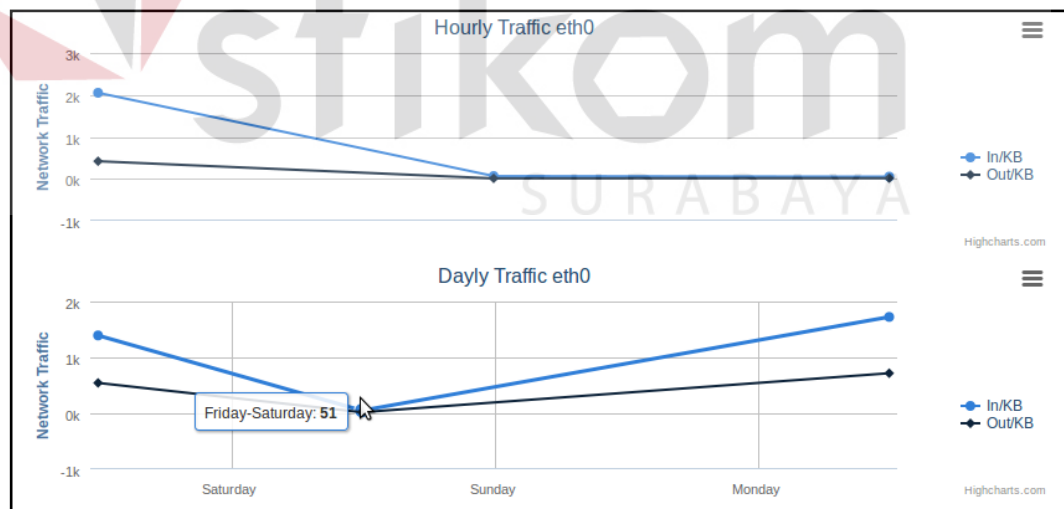


Gambar 4.77 Trafik Data Masuk LABKOM Hari Kamis



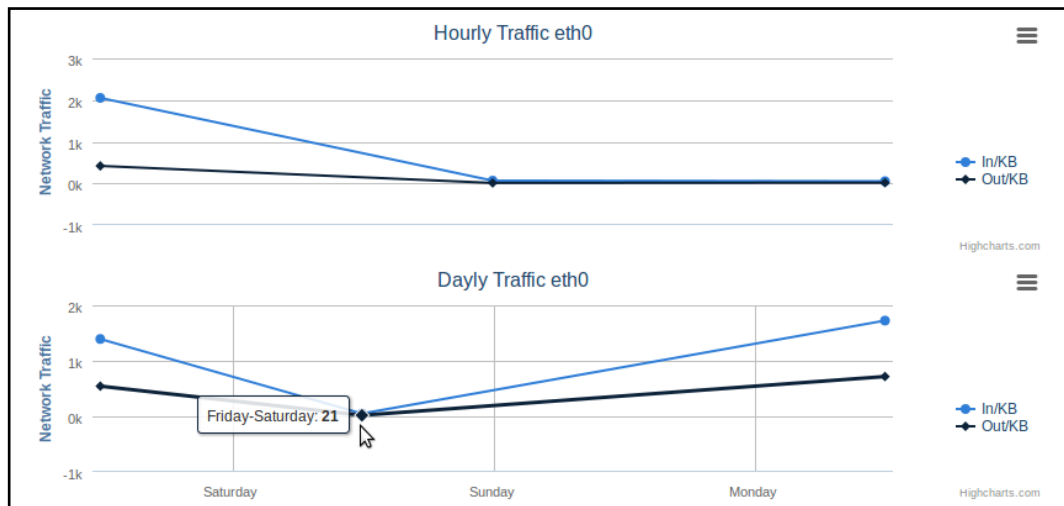
Gambar 4.78 Trafik Data Keluar LABKOM Hari Kamis

Berlanjut pada pengujian hari berikutnya yaitu hari Jumat, trafik masuk tertinggi pada hari Jumat adalah 51KB dan trafik keluar tertinggi pada hari Jumat adalah 21KB. Trafik masuk tertinggi pada hari Jumat dapat dilihat pada Gambar 4.79 dan trafik keluar tertinggi pada hari Jumat dapat dilihat pada Gambar 4.80.



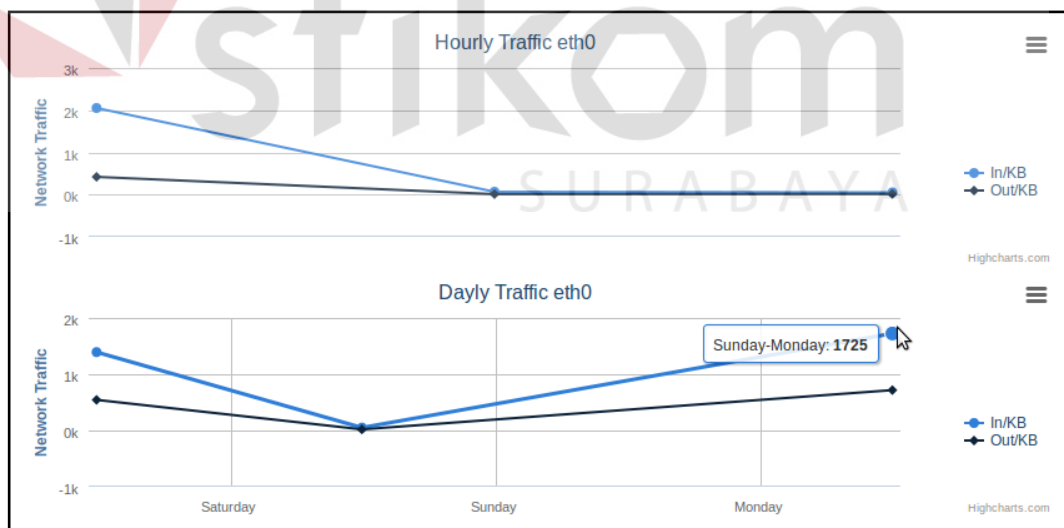
Gambar 4.79 Trafik Data Masuk LABKOM Hari Jumat



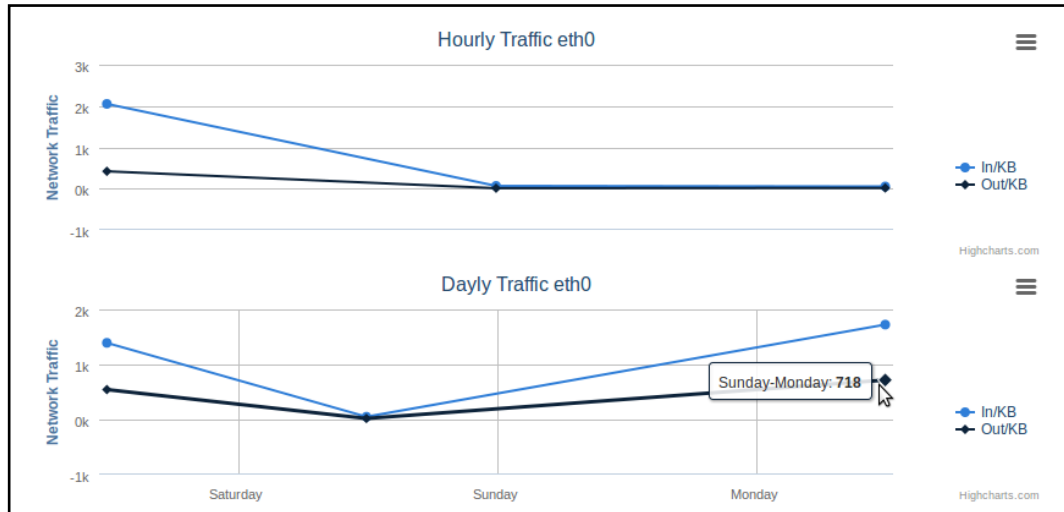


Gambar 4.80 Trafik Data Keluar LABKOM Hari Jumat

Pengujian hari ketiga adalah hari Senin, pada trafik data masuk hari Senin adalah 1725KB dan trafik data keluar pada hari Senin adalah 718KB. Trafik data masuk pada hari Senin dapat dilihat pada Gambar 4.81 dan Trafik Data Keluar pada hari Senin dapat dilihat pada Gambar 4.82.



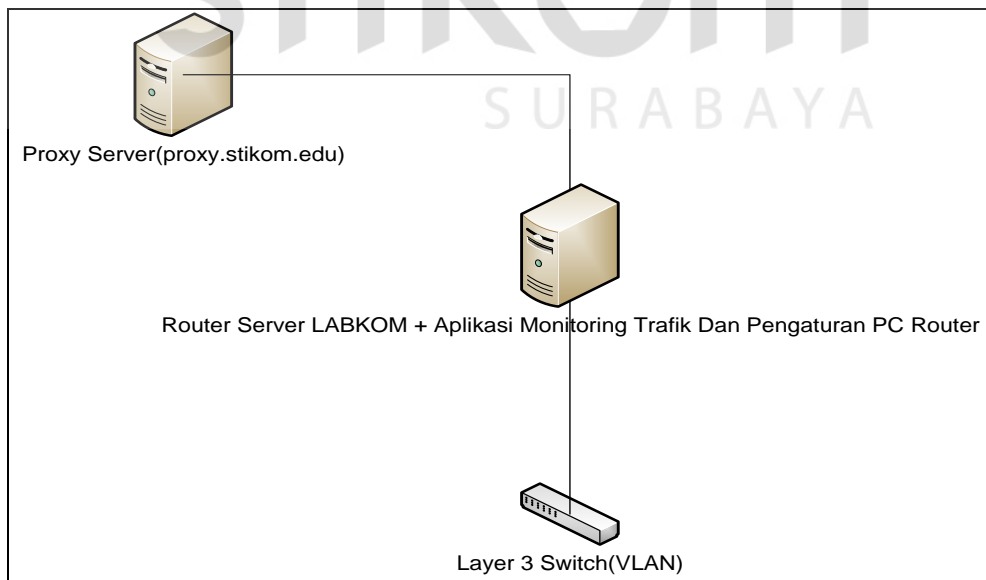
Gambar 4.81 Trafik Data Masuk LABKOM Hari Senin



Gambar 4.82 Trafik Data Keluar LABKOM Hari Senin

## 2. Pengujian Blok Akses Website LABKOM

Server LABKOM bertugas untuk memberikan akses internet kepada masing-masing LAB, akses internet pada LABKOM adalah melalui proxy server dari server utama. Ditunjukkan pada Gambar 4.83 topologi akses internet LABKOM.



Gambar 4.83 Topologi Akses Internet LABKOM

Untuk menutup akses internet pada masing-masing LABKOM, admin hanya perlu memblokir akses ke proxy dari proxy.stikom.edu dan port 3128(Port proxy). Pada Gambar 4.84 ditunjukkan konfigurasi blok akses website pada LABKOM, hasil dari konfigurasi dapat dilihat pada Gambar 4.85.

Gambar 4.84 Konfigurasi Blok Akses Internet Pada LABKOM

```
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
DROP      tcp  --  192.168.101.0/24      222.124.29.233      tcp dpt:3128
DROP      tcp  --  192.168.102.0/24      222.124.29.233      tcp dpt:3128
DROP      tcp  --  192.168.103.0/24      222.124.29.233      tcp dpt:3128
DROP      tcp  --  192.168.104.0/24      222.124.29.233      tcp dpt:3128
DROP      tcp  --  192.168.105.0/24      222.124.29.233      tcp dpt:3128
DROP      tcp  --  192.168.106.0/24      222.124.29.233      tcp dpt:3128
DROP      tcp  --  192.168.107.0/24      222.124.29.233      tcp dpt:3128

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

Gambar 4.85 Hasil Konfigurasi Blok Akses Internet LABKOM

Hasil yang didapat pada konfigurasi tersebut maka masing-masing LABKOM yang di daftarkan tidak dapat memiliki akses ke proxy server untuk menggunakan fasilitas internet di LABKOM.

## 4.2 Pembahasan

### 4.2.1 Kesesuaian Rancangan Dengan Hasil *Black Box*

#### 1. Hasil uji coba trafik monitoring

Pada uji coba ini bertujuan untuk mengetahui apakah fungsi trafik monitoring telah berjalan dengan benar atau tidak. Hasil uji coba fungsi trafik monitoring dapat dilihat pada Tabel 4.15.

Tabel 4.15 Hasil Uji Coba Fungsi Trafik Monitoring

Test Case ID	Tujuan	Input	Output yang diharapkan	Status
1	Monitoring Trafik Jaringan Permenit (berhasil)	Memasukan perhitungan dari ifInOctets dan ifOutOctets secara otomatis <i>reload</i> setiap 1 menit.	Informasi akumulasi paket data per menit	Sesuai pada Gambar 4.57, Gambar 4.58, Gambar 4.59, Gambar 4.60
2	Monitoring Trafik Jaringan Perhari (berhasil)	Memasukan perhitungan dari ifInOctets dan ifOutOctets secara otomatis <i>reload</i> perhari.	Informasi akumulasi paket data perhari	Sesuai pada Gambar 4.62
3	Monitoring Trafik Jaringan Perminggu (berhasil)	Memasukan perhitungan dari ifInOctets dan ifOutOctets secara otomatis <i>reload</i> perminggu.	Informasi akumulasi paket data perminggu	Sesuai pada Gambar 4.64
4	Monitoring Trafik Jaringan Perbulan (berhasil)	Memasukan perhitungan dari ifInOctets dan ifOutOctets secara otomatis <i>reload</i> perbulan.	Informasi akumulasi paket data perbulan	Sesuai pada Gambar 4.66

## 2. Hasil Uji Coba *Blok Port*

Uji coba ini bertujuan untuk memastikan apakah *port* yang tidak dapat diakses oleh *user* sesuai dengan ketentuan admin dapat berjalan dengan baik.

Hasil uji coba blok *port* dapat dilihat pada Tabel 4.16.

Tab 4.16 Hasil Uji Coba Fungsi Blok Port

Test Case Id	Tujuan	Input	Output	Status
5	Blok <i>port</i> tertentu sesuai ketentuan admin(berhasil)	IP <i>address</i> dan <i>gateway</i> serta <i>port</i> yang ditentukan	Akses <i>port</i> tertentu ditutup	Sesuai pada gambar 4.69

## 3. Hasil Uji Coba Blok *Website*

Uji coba ini bertujuan untuk menguji apakah *website* yang tidak sesuai dengan kebutuhan praktikum dapat di blok. Hasil uji coba blok *website* dapat dilihat pada Tabel 4.17.

Tab 4.17 Hasil Uji Coba Fungsi Blok Website

Test Case Id	Tujuan	Input	Output	Status
6	Blok <i>website</i> tertentu sesuai ketentuan admin(berhasil)	Alamat <i>Website</i> dan <i>Port</i> (Protokol)	Akses <i>website</i> tertentu ditutup	Sesuai pada Gambar 4.72

## 4. Hasil Uji Coba *Limit Bandwith*

Uji coba ini bertujuan untuk menguji kemampuan aplikasi untuk membagi *bandwith* kepada masing-masing *gateway* maupun *ip address* tertentu. Hasil uji coba *limit bandwith* dapat dilihat pada Tabel 4.18.

Tabe 4.18 Hasil Uji Coba Fungsi *Limit Bandwith*

Test Case Id	Tujuan	Input	Output	Status
6	Membatasi Penggunaan akses <i>internet</i> (berhasil)	<i>Ip address</i> atau <i>gateway</i> , <i>bandwith</i> , <i>limit</i> maksimal	Pembatasan <i>bandwith</i>	Sesuai pada Gambar 4.73

#### 5. Hasil Uji Coba Packet Information

Uji coba ini bertujuan untuk dapat menguji kemampuan aplikasi untuk mengetahui hasil transaksi website yang dilakukan oleh server maupun *client* yang memanfaatkan fasilitas jaringan pada LABKOM. Hasil uji coba dapat dilihat pada Tabel 4.19.

Tabe 4.19 Hasil Uji Coba Fungsi *Packet Information*

Test Case Id	Tujuan	Input	Output	Status
6	<i>Capture Log</i> Transaksi Website(berhasil)	Alamat Website	Informasi <i>Capture Log</i> Website	Sesuai pada Gambar 4.76

#### 4.2.2 Hasil Uji Coba Pengguna

Hasil pengujian dari wawancara sesuai pada lampiran oleh dua orang pengguna aplikasi pada LABKOM dapat dilihat pada Tabel 4.20.

Tabel 4.20 Hasil Wawancara Pihak Pengguna

No.	Pertanyaan	Jawaban
1	Bagaimana menurut anda fungsi-fungsi yang ada pada aplikasi Monitoring Trafik Jaringan dan Pengatura PC <i>Router</i> berbasis <i>Web</i> ?	<ul style="list-style-type: none"> <li>• Cukup baik, perlu penambahan monitoring per LAB</li> <li>• Cukup baik, perlu <i>gateway</i> per LABKOM</li> </ul>
2	Apakah hasil informasi yang diberikan	

	sudah memenuhi kebutuhan?	<ul style="list-style-type: none"> <li>• Cukup baik, bentuk pelaporan sudah disediakan</li> <li>• Cukup baik</li> </ul>
3	Apakah visualisasi yang ada pada aplikasi Monitoring Trafik Jaringan dan pengaturan PC Router berbasis Web bisa dipahami dengan mudah?	<ul style="list-style-type: none"> <li>• Perlu penambahan keterangan supaya bisa lebih mudah dipahami</li> <li>• Perlu Penambahan Icon</li> </ul>
4	Saran dari pengguna untuk pengembangan aplikasi Monitoring Trafik Jaringan dan Pengaturan PC Router berbasis Web	<ul style="list-style-type: none"> <li>• Pengembangan lebih ringan untuk aplikasi supaya tidak membebani server</li> <li>• Cukup untuk skala LABKOM</li> </ul>

Hasil rekapitulasi kuesioner yang telah diisi oleh 10 orang pengguna dapat dilihat pada tabel 4.21. pada tabel tersebut, menjelaskan tentang hasil perhitungan pernyataan pengguna terhadap Aplikasi Monitoring Trafik Jaringan Dan Pengaturan PC Router Berbasis Web.

Tabel 4.21 Tabel Rekapitulasi Kuesioner

Pertanyaan No.	Penilaian					$\Sigma$	Nilai Akhir	
	1	2	3	4	5			
Tampilan								
A	1	0	0	6	20	15	41	79
	2	0	0	6	32	0	38	
Navigasi								
B	1	0	0	3	36	0	39	75
	2	0	0	12	24	0	36	
Manfaat								
C	1	0	0	9	28	0	37	67
	2	0	0	21	4	5	30	

#### 4.2.3 Kesesuaian Rancangan Dengan Permasalahan

Dari permasalahan yang sudah dibahas pada BAB I maka akan disimpulkan kesesuaian dengan sistem yang telah dibuat agar sesuai dengan tujuan utama dari pembuatan system:

1. Aplikasi mampu menghasilkan visualisasi kondisi jaringan terkini. Sistem mempunyai trafik monitoring yang di visualisasikan berdasarkan menit, hari tahun dan juga mampu memberikan informasi tentang transaksi *website* yang dikunjungi oleh *client*.
2. Aplikasi mampu memberikan fasilitas untuk pembagian *bandwith* dan pembatasan akses untuk *port* dan alamat *website* yang tidak diperkenankan.

