JSIKA Vol 3, No 1 (2014)/ ISSN 2338-137X

Jurnal Sistem Informasi

Situs Jurnal : http://jurnal.stikom.edu/index.php/jsika

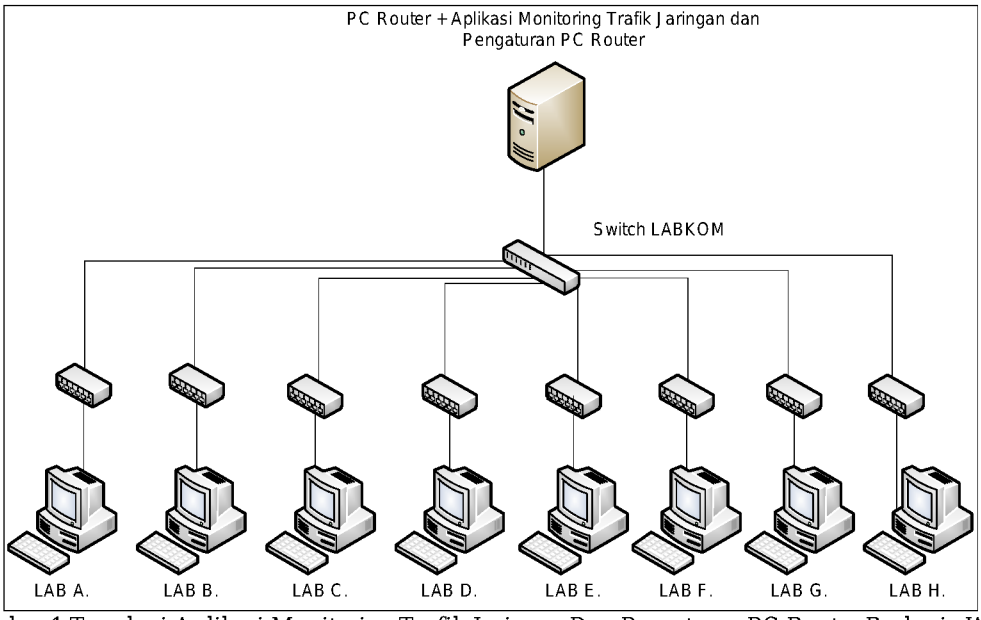
MONITORING TRAFIK JARINGAN DAN PENGATURAN PC ROUTER BERBASIS WEB (STUDI KASUS: LABKOM STIKOM SURABAYA)

Yermias Alvandy Oktario Wun[1)] **Anjik Sukmaaji**[2)]**Kurniawan Jatmika**[3)]
Program Studi/Jurusan Sistem Informasi
STMIK STIKOM Surabaya
Jl. Raya Kedung Baruk 98 Surabaya, 60298
Email : 1)yermiasalvandy@gmail.com, 2)anjik@stikom.edu, 3)kjatmika@stikom.edu

Abstract: *admin constrained to manage a network traffic and limit bandwith usage and also block websites that are not allowed. Now, admin still used plug/unpulug way to manage the network on LABKOM STIKOM Surabaya. Based on problem occurred then needed an application which can provide information about activities that occurred on the local network to maintain network performance in LABKOM and also provide visual information about network traffic conditions in LABKOM and can facilitate a network administrator to restrict the use of bandwidth as well as the blocking of websites is not allowed during practical work takes place With SNMP, Data from the current network conditions can be collected and visualize the network traffic. And also requires an IPTables application to manage input and output the gateway. Expected by the existence of Monitoring network traffic and system settings to the Router's Web-based PC can provide information and facilities needed by a system LABKOM administrator network that makes it easy to monitor and control the internet access on the network LABKOM and minimize in terms of financial expenditure is excessive as the replacement schedule for practical and cost of electricity due to the presence of interference on the network LABKOM at the time of the process of teaching.*

Keywords: *Network Traffic*, *Monitoring, Bandwith*

Laboratorium merupakan sarana untuk melakukan berbagai macam riset atau percobaan salah satunya jaringan komputer termasuk laboratorium komputer(LABKOM) STIKOM Surabaya. Seorang administrator jaringan pada LABKOM bertugas untuk memanajemen dan memonitoring jaringan dari manajemen bandwidth, VLAN, *gateway* dan *security* agar bisa berjalan stabil untuk keberlangsungan proses praktikum sedangkan selama ini saat proses terjadinya praktikum yang menyebabkan banyak akses ke server maupun ke internet, admin mengalami kendala untuk memanajemen trafik jaringan dan membatasi penggunaan *bandwith* serta pemblokiran website yang tidak di perkenankan. Berdasarkan permasalahan yang terjadi maka diperlukan sebuah aplikasi yang dapat memberikan informasi tentang kegiatan yang terjadi pada jaringan lokal untuk menjaga performa jaringan pada LABKOM dan juga memberikan informasi visualiasi kondisi trafik jaringan pada LABKOM serta dapat memfasilitasi administrator jaringan untuk membatasi penggunaan *bandwith* serta pemblokiran website yang tidak diperkenankan pada saat praktikum berlangsung. Denah jaringan Topologi monitoring jaringan dan pengaturan PC Router LABKOM dapat dilihat pada Gambar 1.

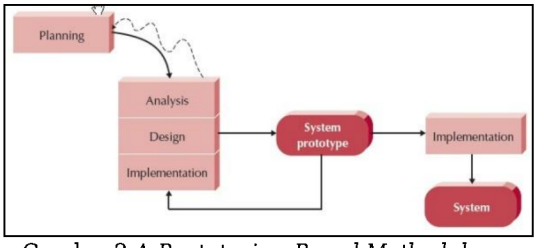


Gambar 1 Topologi Aplikasi Monitoring Trafik Jaringan Dan Pengaturan PC Router Berbasis Web.

METODE

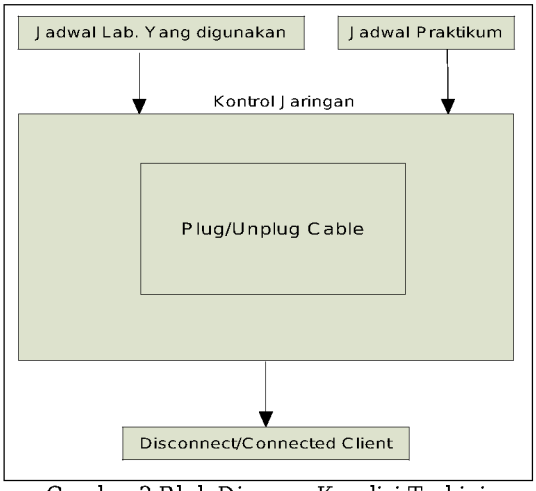
Analisis

Dalam pengembangan Monitoring Trafik Jaringan dan Pengaturan PC Router Berbasis Web, Penulis menerapkan konsep pengembangan *Software Development Life Cycle* (SDLC) dengan metode *Prototyping-based*. *Prototyping-based methodology* dapat dilihat pada Gambar 2.

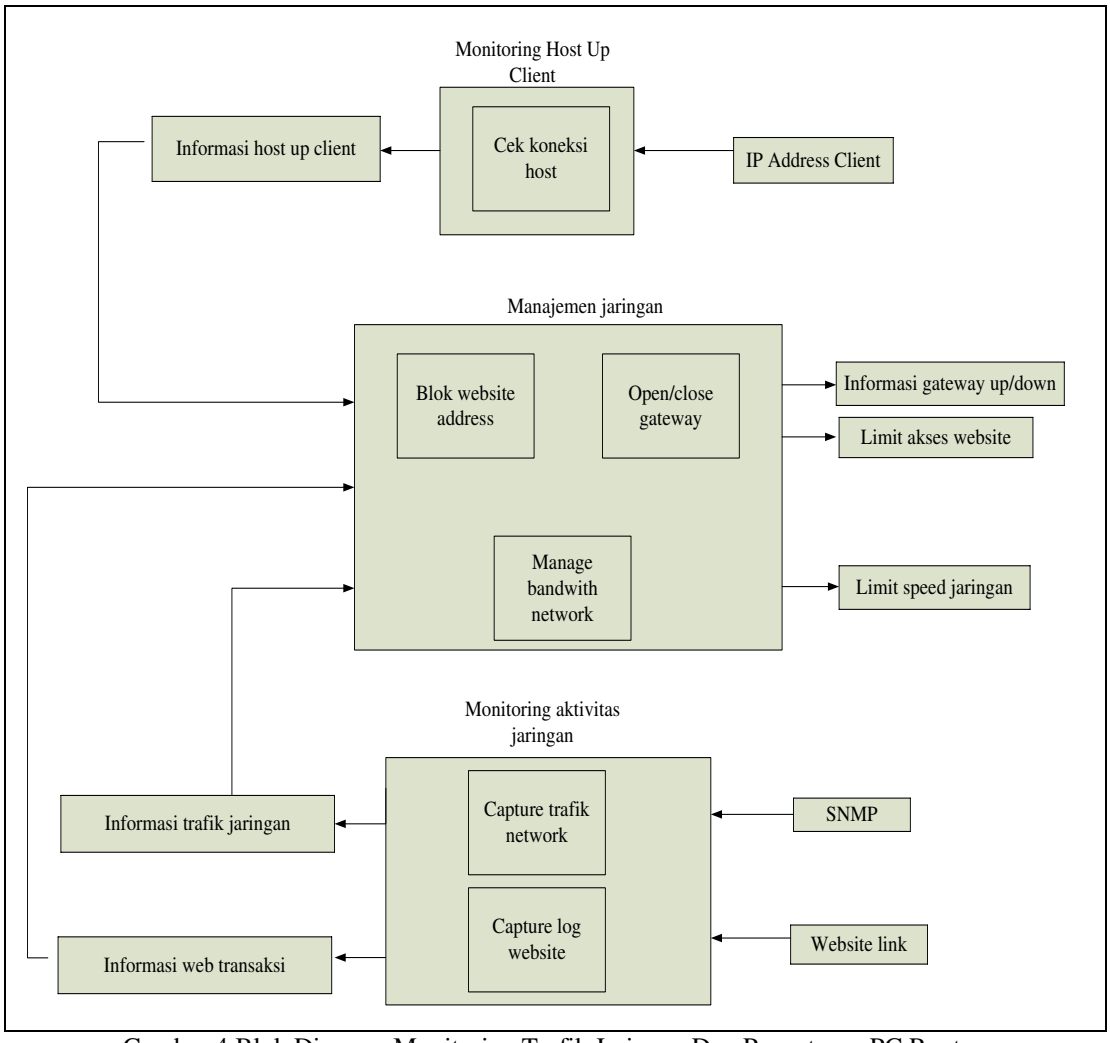


Gambar 2 *A Prototyping-Based Methodology*

Dapat dilihat pada Gambar 3 tentang blok diagram kondisi manajemen jaringan LABKOM saat ini masi menggunakan cara manual dimana admin atau staff yang bertugas untuk mengatur kegiatan harus memasang ataupun mencopot kabel jaringan pada ruang LABKOM yang bermasalah ataupun yang tidak sedang digunakan untuk kegiatan praktikum maupun riset. Kegunaan hal tersebut adalah untuk memberikan kesempatan untuk ruang LABKOM yang memiliki keperluan seperti *upgrade software, download antivirus, download tools* yang digunakan untuk praktikum.



Gambar 3 Blok Diagram Kondisi Terkini Jaringan LABKOM



Gambar 4 Blok Diagram Monitoring Trafik Jaringan Dan Pengaturan PC Router

Dari Gambar 3 dapat diketahui kondisi terkini kontrol jaringan pada LABKOM yaitu dengan cara *plug/unplug* kabel LAN pada switch LABKOM. Dari kondisi tersebut maka dapat disimpulkan kebutuhan output dari admin LABKOM dan KABAG LABKOM yaitu:

1. Informasi *Host Up Client*

Informasi *Host Up Client* merupakan informasi hasil dari pengujian koneksi server dengan client yang terhubung dalam satu jaringan.

2. Informasi Gateway *Up/Down*

Informasi *Gateway Up/Down* merupakan informasi hasil dari pengujian koneksi masing-masing gateway yang ada dalam satu jaringan.

3. Informasi Trafik Jaringan

Informasi Trafik Jaringan merupakan informasi kondisi terkini jaringan lokal dengan model visualisasi yang nilainya didapatkan oleh SNMP.

4. Informasi Web Transaksi

Informasi web transaksi dikumpulkan dengan menggunakan aplikasi TCPDump dan di tampilkan pada satu dashboard yang sama di sistem.

Dari kondisi Gambar 3 tentang kondisi terkini jaringan pada LABKOM maka dapat diambil keputusan rancangan untuk tahapan pembangunan sistem. Rancangan menggunakan blok diagram. Blok diagram Monitoring Trafik Jaringan dan Pengaturan PC Router dapat dilihat pada Gambar 4.

Monitoring Host Up Client

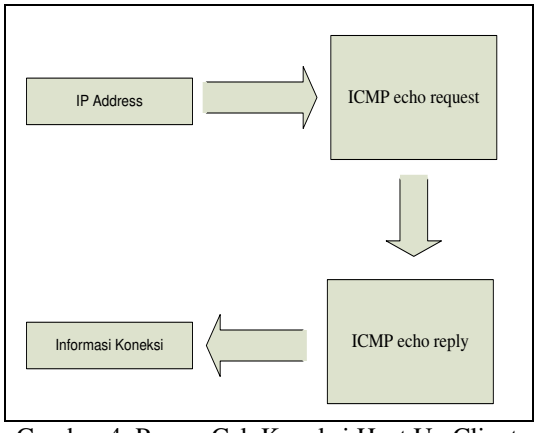
Monitoring *host up client* dilakukan untuk mengetahui status koneksi antara *monitoring station* dan *device target* yang terhubung dalam satu jaringan *local area network*(LAN) yang didalamnya terdapat sebuah

proses pengecekan koneksi *host* dengan utilitas "PING".

Pada sistem ini akan dilakukan juga tes koneksi untuk *gateway* yang diberikan oleh server dan pada masing-masing *client* yang sudah didaftarkan oleh admin. Hasil dari tes koneksi akan ditampilkan secara visual di *dashboard* aplikasi.

Proses Cek Koneksi Host

Pada proses ini dilakukan pengujian koneksi dengan utilitas "PING" yang dilakukan dari server aplikasi atau server router. Tes koneksi "PING" ini bekerja pada layer aplikasi yang menggunakan *internet control message protocol*(ICMP) yang mengirimkan pesan ICMP *echo request* dan menerima *echo reply* untuk menentukan apakah *device* tujuan dapat dijangkau dan berapa lama paket yang dikirimkan dibalas oleh *device* tujuan. Pada sistem ini membutuhkan informasi koneksi dari *device* tujuan pada perhitungan ICMP per satu detik menggunakan opsi "ping –c *count* –w *deadline IPADDRESS*". Penggunaan opsi –c *count* adalah untuk menghentikan tes koneksi setelah mengirim jumlah paket *echo request* dan penggunaan opsi –w *deadline* adalah mengatur waktu untuk menunggu respon dari *device* tujuan. Contoh penggunaan utilitas "PING" adalah"ping –c 1 –w 1 192.168.0.1", contoh tersebut digunakan untuk melakukan tes koneksi "PING " untuk *device* yang mempunyai IP *address* 192.168.0.1 dengan interval waktu 1 detik. Gambar 4 menunjukan blok diagram proses cek koneksi pada *client*.



Gambar 4 Proses Cek Koneksi Host Up Client

Monitoring Aktivitas Jaringan

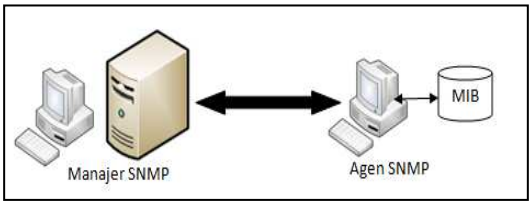
Sistem monitoring ini didalamnya berisi tentang informasi trafik jaringan terkini dalam bentuk log atau visualisasi dari data-data yang dikumpulkan dari sebuah sistem pendukung. Dalam sistem ini menggunakan aplikasi layer 7 yaitu SNMP. Kemudian dalam monitoring aktivitas jaringan dilakukan juga pengumpulan data log web transaksi yang dilakukan oleh user dengan menggunakan aplikasi TCPDump.

Proses Capture Trafik Network

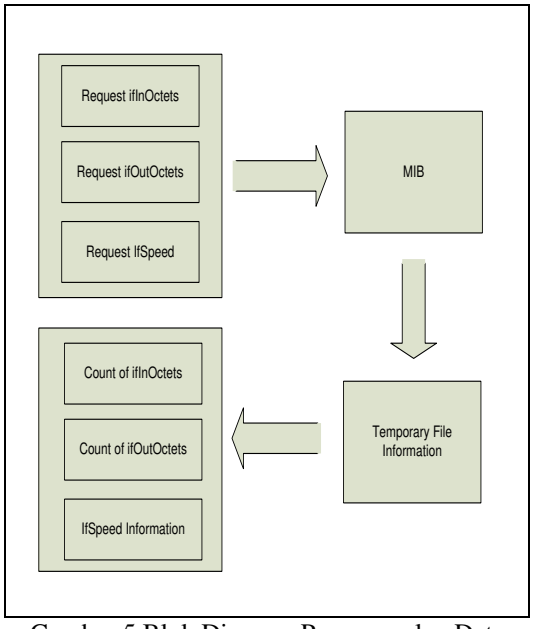
Untuk mendapatkan data dari kondisi jaringan terkini dibutuhkan SNMP untuk mengoleksi data dari jaringan tersbut. SNMP adalah sebuah protokol apikasi pada jaringan TCP/IP yang menangani manajemen jaringan. Protokol ini didesain sehingga pengguna dapat dengan mudah memantau kondisi jaringan komputer. Pemantauan kondisi jaringan dapat dilakukan dengan cara pengumpulan nilai-nilai informasi dari kondisi jaringan secara jarak jauh atau menggunkan satu pusat pengamatan.

SNMP menjadi protokol yang terus dikembangkan karena banyak perangkat jaringan yang mendukung dan tersedia layanan SNMP seperti *router*, *switch*, server, *workstation*, dan *printer*. Protokol SNMP pada jaringan TCP/IP menggunakan *transport* UDP oleh karena itu dalam penggunaannya tidak akan membebani trafik jaringan (Pradikta, Affandi, & Setijadi, 2013). Struktur SNMP dari manajer, agen, dan MIB dapat dilihat pada Gambar 4.

Pada sistem ini, beberapa data yang dikumpulkan adalah CPU *info, hostname* komputer, *input* dan *output* dari *interface* yang akan disimpan dalam sebuah *database*. Dalam menggumpulkan data-data yang dibutuhkan tersebut menggunakan opsi "snmpwalk". Penggunaan "snmpwalk" dilakukan pada server yang sudah tersedia aplikasi snmp. Berikut adalah contoh penggumpulan data dengan "snmpwalk" dengan opsi "snmpwalk –v SNMP_version –c SNMP_password IP_address". Untuk lebih jelasnya penggunaan snmpwalk adalah sebagai berikut "snmpwalk –v 1 –c public localhost", contoh tersebut bertujuan untuk mengunmpulkan data dari localhost yang sudah tertanami aplikasi SNMP. Blok diagram pengumpulan data *agent* SNMP dapat dilihat pada Gambar 5.



Gambar 4 Manajer, Agen, Dan MIB. Sumber (Pradikta, Affandi, & Setijadi, 2013)



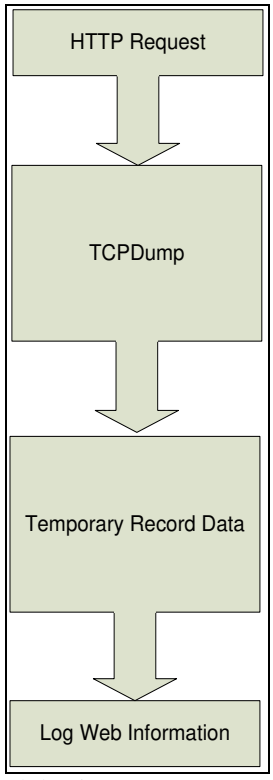
Gambar 5 Blok Diagram Pengumpulan Data agent SNMP

Proses Capture Log Website

Untuk mengamati atau memantau log transaksi website yang di akses oleh dibutuhkan aplikasi TCPDump dimana TCPDump adalah aplikasi pre-instaled dari ubuntu.

TCPDump adalah *command-line network traffic-monitoring tool* yang dapat mengumpulkan informasi *packets* di *network interface* dan memungkinkan administrator untuk menganalisa hasilnya informasi yang dikumpulkan (Stanger & Lane, 2001).

Pada sistem aplikasi ini menggunakan TCPDump versi 4.2.1. Sistem ini membutuhkan hanya daftar IP *address* dan fungsi seperti *DNS lookup* maka pada TCPDump digunakan funngsi "-n". Data yang diambil dari TCPDump akan dimasukan pada sebuah *temporary text* agar tidak memperberat kinerja server. Penyimpanan terletak pada *directory "*/tmp" dimana "/tmp" adalah tempat penyimpanan *temporary* pada server yang menggunakan platform Ubuntu atau kernel linux. Penggunaan TCPDump untuk melakukan *capture log* adalah "tcpdump –n > /tmp/sniff.txt" dengan maksud untuk melakukan *capture log* yang disimpan pada *file* sementara bernama "sniff.txt" dan akan ditampilkan pada *dashboard* aplikasi. Untuk pengaplikasian TCPDump dalam melakukan *capture log* bisa dirubah sesuai kebutuhan informasi yang akan dimonitoring oleh admin LABKOM. Blok diagram *capture log website* dapat dilihat pada Gambar 6



Gambar 6 Blok Diagram Capture Log Website

Manajemen Jaringan

Dalam sistem yang akan dibangun ini, dilengkapi dengan fasilitas manajemen jaringan diantaranya blok *website* dan *open/close gateway* dan juga sistem untuk melakukan limitasi *bandwith*.

Dari modul blok website dan *open/close gateway* menggunakan sabuah aplikasi pre-instaled pada Ubuntu yaitu "iptables". Untuk modul *limit bandwith* menggunakan aplikasi tambahan yaitu HTB-Tools untuk memudahkan pengguna dalam memanajemen *bandwith* dan banyaknya support dan tutorial penggunaan HTB-Tools untuk membantu *maintenance* jika ada permasalahan pada limitasi *bandwith*.

Proses Blok Website Address dan Open/Close Gateway

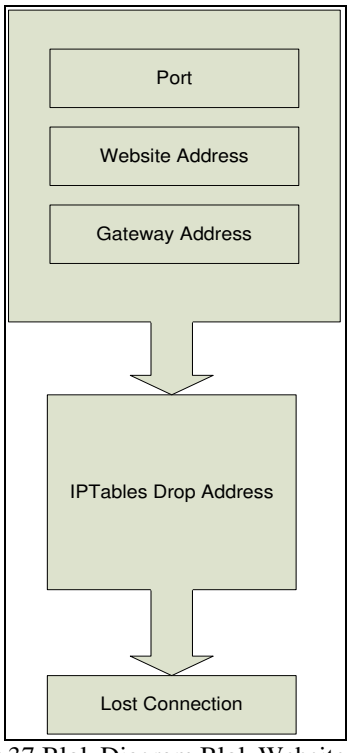
Aplikasi pendukung untuk blok *website* dan *open/close gateway* yang dibutuhkan adalah IPTables. IPTables merupakan *firewall* bawaan Linux. Iptables mampu melakukan *filtering* dari *layer transport* sampai layer *physical*. Sebagai contoh *rule* dalam sebuah *firewall* akan menutup semua koneksi kecuali ke port 80 protokol TCP, atau sebuah *rule firewall* mendefiniskan bahwa yang dapat melakukan koneksi hanya paket data yang berasal dari MAC address 00-80-48-24-3b-e5 (Hartono, 2006).

Untuk pemblokiran dan penutupan akses *gateway* adalah dengan menutup protocol tertentu. Berikut adalah beberapa port yang dapat di manajemen dengan menggunakan IPTables:

1. HTTP (80)
2. HTTPS (443)
3. SMTP (25)
4. SSH (22)
5. POP3 (110)
6. IMAP (143)
7. DNS (53)
8. TELNET (23)
9. FTP (21)
10. TFTP(69)

Untuk melakukan penutupan *gateway* secara total dapat menggunakan konfigurasi pada iptables "iptables -A INPUT -s IP_Address -j DROP" dimana konfigurasi ini bertujuan memblokir semua *incoming request* dari IP *address* yang dituju, kemudian "iptables -A OUTPUT -p tcp -d IP_Address -j DROP" yang digunakan untuk memblokir semua paket menuju keluar dari IP *address* yang dituju.

Dari seluruh konfigurasi yang dilakukan didalam sistem dapat dilihat hasil konfigurasi dengan menggunakan "iptables –L -n" dimana hasil konfigurasi ini akan ditampilkan juga dalam *dashboard* aplikasi. Blok diagram blok website dan port dapat dilihat pada Gambar 7.

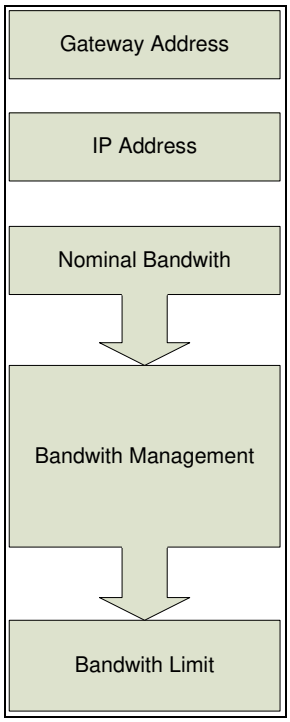


Gambar 37 Blok Diagram Blok Website dan Port

Proses Manage Bandwith Network

Untuk melakukan limitasi *bandwith* juga diperlukan aplikasi yang harus di *install* didalam server router yaitu HTB-Tools dimana sistem ini menggunakan HTB-Tools 0.3.0a.i486-1.

Penggunaan HTB-Tools memudahkan *developer* aplikasi mengintegrasikan sistem yang dibangun dengan HTB-Tools. Konfigurasi untuk manajemen *bandwith* pada HTB-Tools dapat diakkses di "/etc/htb/eth0-qos.cfg" dan yang utama dalam memanejemn *bandwith* adalah total *banwith*, minimum *limit, gateway,* IP *address,* dan subnet dari jaringan LABKOM.



Gambar 8 Blok Diagram Management Bandwith

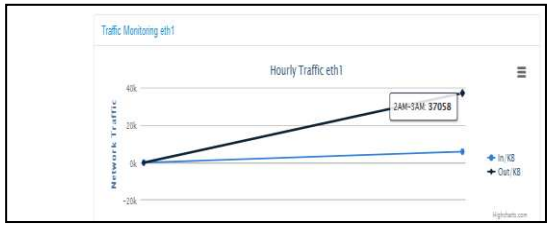
HASIL DAN PEMBAHASAN

Hasil ujicoba dilakukan dengan metode *blackbox*. Berikut adalah hasil uji coba dari aplikasi Monitoring Trafik dan Pengaturan PC Router Berbasis Web.

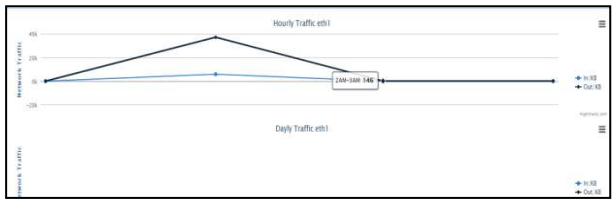
Uji Coba Trafik Monitoring

Trafik Monitoring permenit

Trafik monitoring otomatis ter*update* setiap menitnya sampai 24jam. Ditunjukan pada Gambar 9 dan 10 contoh *interface* eth1 pada **ifOutOctets**.

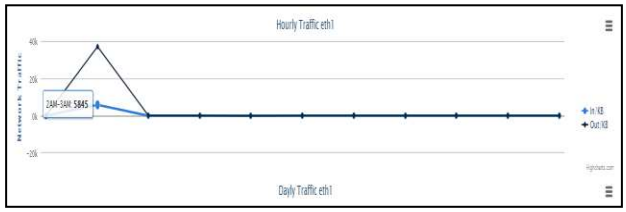


Gambar 9 *auto update* ifOutOctets *graphic* per menit

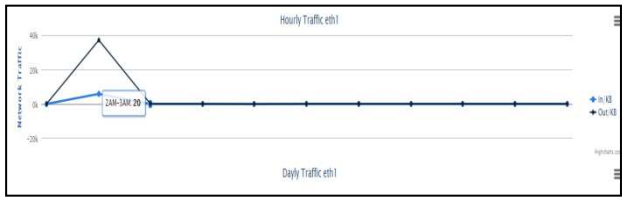


Gambar 10 *Update* ifOutOctets Persatu Menit Berikutnya

Ujicoba yang sama juga dilakukan untuk **ifInOctets** dimana keduanya ter*update* otomatis secara bersamaan, *update* **ifInOctets** permenit dapat dilihat pada Gambar 11 dan menit berikutnya pada Gambar 12.



Gambar 11 *Auto Update* Ifinoctets Per Satu Menit



Gambar 12 *Update* Ifinoctets Persatu Menit Berikutnya

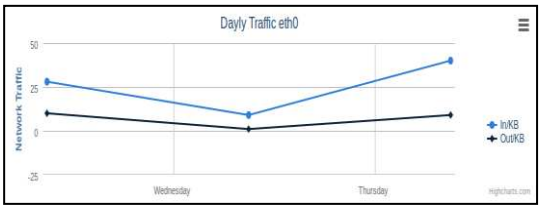
Dilihat kambali pada Gambar 9 dan 11 **ifOutOctets** akumulasi satu menit sebelumnya adalah 37058 KB kemudian satu menit berikutnya adalah 146 KB, sama dengan ifOutOctets, ifInOctets juga auto update permenitnya dari nilai awal 5845 KB pada Gambar 10 kemudian akumulasi paket data untuk satu menit berikutnya adalah 20 KB.

Trafik Monitoring Perhari

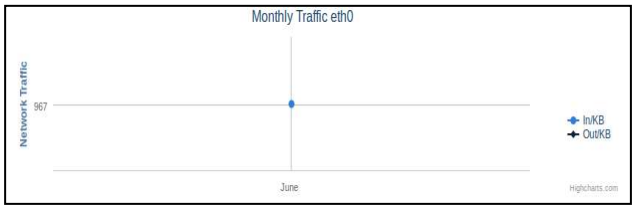
Setelah data permenit sudah mencapai 24 jam maka data permenit akan langsung terhapus ketika berganti hari ditunjukan pada Gambar 13, data perhari adalah nilai tertinggi trafik dari data permenit yang di tunjukan pada Gambar 14. ujicoba dilakukan dengan cara mengganti tanggal pada OS agar langsung mendapatkan data baru yaitu akumulasi data perhari.

Gambar 13 Data Permenit Otomatis Terhapus

Gambar 17 Data Perminggu Telah Terhapus



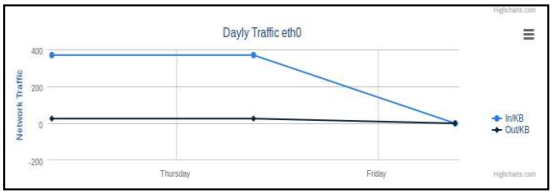
Gambar 14 Trafik Data Perhari



Gambar 18 Trafik Data Perbulan

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 ditunjukan pada Gambar 15 dan menjadi akumulasi data perminggu yang ditunjukan pada Gambar 16.



Gambar 15 Trafik Data Perhari Terhapus

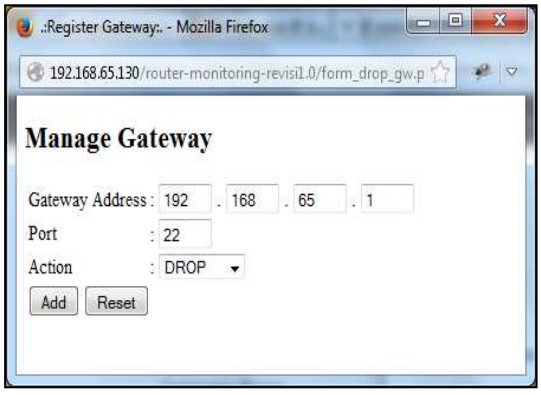
Gambar 16 Akumulasi Data Perminggu

Trafik Monitoring Perbulan

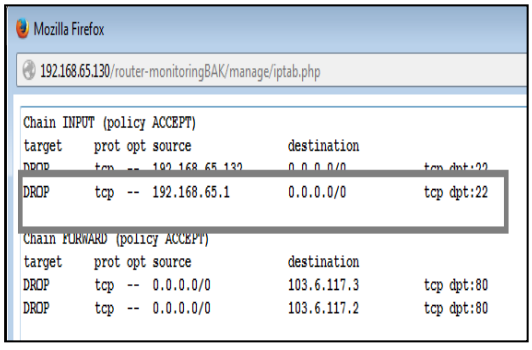
Trafik monitoring perbulan mempunyai sistem yang sama dengan permenit, perhari dan perminggu. Data dari perminggu akan hilang jika sudah berganti bulan ditunjukan pada Gambar 17. Ujicoba dilakukan dengan memajukan angka bulan pada OS agar *output* trafik perbulan dapat terlihat ditunjukan pada Gambar 18.

Uji Coba Blok Port

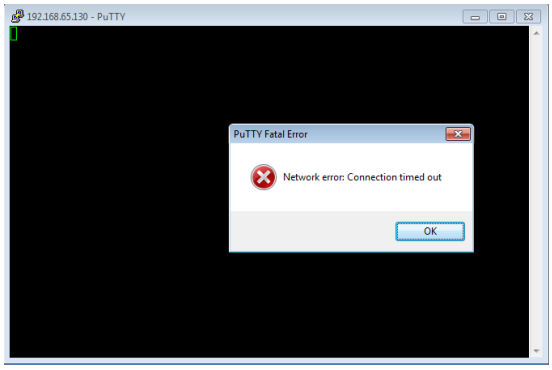
Berikut akan dilakukan uji coba fungsi blok *port*, uji coba yang dilakukan adalah mencoba menutup akses ke *port* 22 pada *client* 192.168.65.1 dan server pada 192.168.65.130.



Gambar 19 Blok *Port* 22 Ip *Address* 192.168.65.1



Gambar 20 *Rule* Yang Masuk Untuk Port 22 Ip *Address* 192.168.65.1



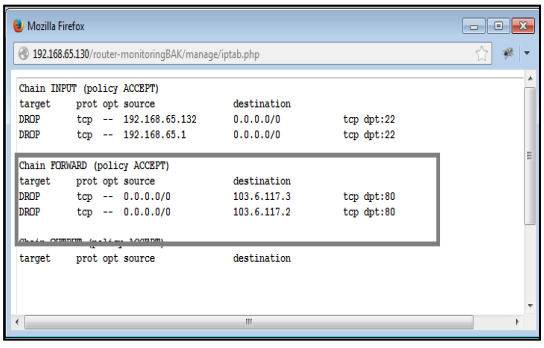
Gambar 21 *Putty* Gagal *Connect* Server

Pada Gambar 19 ditunjukan bagaimana input data untuk *address* yang akan di tutup akses ke *port* 22, dan status untuk perlakuan tersebut dapat dilihat pada Gambar 20. hasil dari fungsi tersebut adalah *client* tidak bisa mengakses *port* 22 untuk menuju server ditunjukan pada Gambar 21.

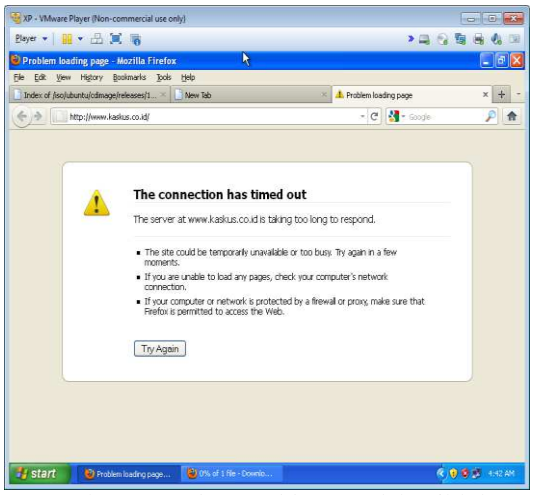
Uji Coba Blok Website

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 .

Gambar 22 Input Alamat *Web* Dan *Port*



Gambar 23 Alamat *Website* Di *Filter*

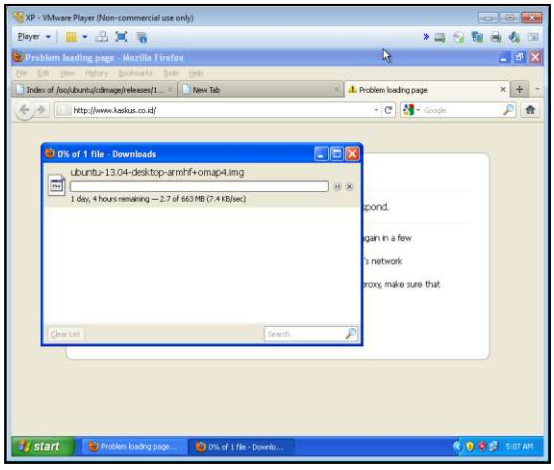


Gambar 24 *Website Address* Sudah Diblok

Pada Gambar 22 terdapat 2 *textbox* yaitu alamat *website* dan *port* (protokol), hasil input dapat dilihat pada Gambar 23 dan hasilnya dapat dilihat pada Gambar 24 dimana *website* sudah tidak bisa diakses.

Uji Coba Limit Bandwith

Uji Coba berikutnya adalah uji coba limitasi *bandwith*, 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 25.

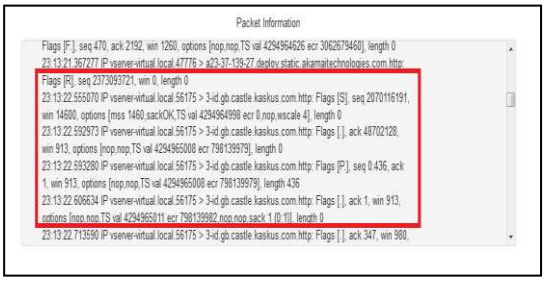


Gambar 25 Limit *Bandwith* 8kbps

Uji Coba Packet Information

Berikutnya ada uji coba untuk melihat transaksi website, sebagai contoh pada *client* membuka site www.kaskus.co.id, maka sistem menunjukan semua alamat yang menuju pada alamat www.kaskus.co.id termasuk *sub domain*.

Hasil uji coba dari *packet information* dapat dilihat pada Gambar 26.



Gambar 26 Hasil *Capture Packet Information*

KESIMPULAN

Setelah melakukan pembuatan, uji coba, dan analisispada Aplikasi Pemetaan Monitoring Trafik Jaringan Dan Pengaturan PC Router maka dapat ditarik kesimpulan sebagai berikut:

1. Berdasarkan hasil uji coba yang dilakukan dengan *black box* dan survey. Aplikasi mampu memberikan visualisasi trafik kondisi jaringan pada LABKOM dengan memnggunakan SNMP sebagai *protocol* untuk pengumpulan informasi dari PC router sebagai akses *gateway* jaringan internet
2. Aplikasi mampu memfasilitasi admin jaringan pada LABKOM dalam membatasi penggunaan *bandwith* dengan memanfaatkan HTB-tools sebagai aplikasi pendukung dalam memanajemen *bandwith* dan pembatasan akses *gateway* untuk *port* tertentu dan blokir website dengan fasilitas dari IPTables dari sistem operasi ubuntu.

RUJUKAN

Hartono, P. (2006, June 5). *Sistem Pencegahan Penyusupan pada Jaringan.* Retrieved May 20, 2013, from Budi Insan: http://budi.insan.co.id/courses/security/2006/puji_report.pdf

Pradikta, R., Affandi, A., & Setijadi, E. (2013, 03 16). *Rancang Bangun Aplikasi Monitoring Jaringan dengan Menggunakan Simple Network Management Protocol.* Retrieved 12 09, 2013, from ejurnal.its.ac.id: http://ejurnal.its.ac.id/index.php/teknik/article/viewFile/2265/909

Stanger, J., & Lane, P. T. (2001). *Hack Proofing Linux: A Guide To Open Source Security.* Rockland: Syngress Publishing, Inc.