Aplikasi Network Traffic Monitoring Menggunakan Simple Network Management Protocol (SNMP) pada Jaringan Virtual Private Network (VPN)

1 author:

Nora Lizarti
Stmik Amik Riau, Pekanbaru, Indonesia
2 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Aplikasi *Network Traffic Monitoring* Menggunakan *Simple Network Management Protocol* (SNMP) pada Jaringan *Virtual Private Network* (VPN)

Nora Lizarti
Jurusan Teknik Informatika STMIK Amik Riau
noralizarti@stmik-amik-riau.ac.id

Wirta Agustin
Jurusan Teknik Informatika STMIK Amik Riau
wirtaagustin@stmik-amik-riau.ac.id

Abstrak

Aplikasi Sistem Informasi yang ada di SMK Labor Binaan FKIP UNRI telah dapat menunjang proses keputusan yang akurat. Aplikasi Sistem Informasi tersebut bisa di akses melalui internet secara private dengan teknologi VPN (Virtual Private Network), tetapi penggunaannya belum bisa di pantau secara spesifik oleh administrator jaringan, sehiingga perlu untuk membangunkan suatu sistem traffic monitoring dengan menggunakan Simple Network Management Protocol (SNMP) dalam mengimplementasikan aplikasi untuk melakukan pengamatan penggunaan lalu lintas data internet dari parameter yang ada pada jaringan VPN (Virtual Private Network) berbasis web, yang menjadi salah satu solusi dalam menyelesaikan masalah yang ada. VPN (Virtual Private Network) merupakan suatu cara memanfaatkan jaringan public sebagai jaringan private secara aman melalui internet yang menggunakan perpaduan teknologi tunneling dan enkapsulasi. SNMP merupakan sebuah protokol yang didesain untuk memberikan kemampuan pengumpulan data manajemen perangkat jaringan dan pengkonfigurasian perangkat jaringan secara jarak jauh (remotely). Sistem operasi yang digunakan pada server administator adalah Linux Ubuntu 12.04. Linux Ubuntu merupakan distro linux yang stabil dan cukup handal. Dengan adanya aplikasi network traffic monitoring pada jaringan VPN dapat membantu pihak administrator untuk memantau lalu lintas data sehingga penggunaan internet lebih optimal.

Kata kunci : network traffic monitoring, VPN (Virtual Private Network), SNMP (Simple Network Management Protocol), Linux Ubuntu 12.04

1. Pendahuluan

Teknologi informasi yang semakin berkembang, menjadikan teknologi banyak membantu dan mempermudah pekerjaan di berbagai bidang, termasuk dalam bidang jaringan komputer. Dengan tersedianya internet (*interconnection network*) menjadikan semakin cepatnya pertukaran dan pengiriman informasi dari komputer yang satu ke komputer yang lain, bahkan untuk jarak yang jauh sekalipun. Sehingga tidak menutup kemungkinan bagi seseorang untuk dapat melakukan pekerjaannya dimana saja dengan mengakses komputernya dirumah ataupun dikantor.

SMK Labor Binaan FKIP UNRI telah memiliki beberapa aplikasi sistem informasi yang menunjang proses keputusan yang akurat. Aplikasi sistem informasi tersebut bisa di akses melalui *internet* secara *private* dengan teknologi VPN (*Virtual Private Network*). Namun dalam perkembangannya para administrator jaringan dituntut untuk bekerja dengan cepat, handal, dan profesional ketika terjadi masalah pada lalu lintas (*traffic*) yang disebabkan oleh penggunaan lalu lintas data secara *overloaded* dan akan mempengaruhi kecepatan koneksi antar perangkat jaringan, sehingga penggunaan internet tidak optimal. Sementara itu disisi lain dengan tidak adanya *monitoring* secara intensif terhadap pemakaian *packet* data *in* dan *out* mengakibatkan kurangnya gambaran terhadap permasalahan yang terjadi pada jaringan seperti keamananan jaringan, *troubleshooting*, virus dan juga pemantauan lalu lintas data jaringan itu sendiri.

Protokol yang sering digunakan untuk melakukan manajemen jaringan adalah SNMP (*Simple Network Management Protocol*). SNMP merupakan sebuah protokol yang didesain untuk memberikan kemampuan pengumpulan data manajemen perangkat jaringan dan pengkonfigurasian perangkat jaringan secara jarak jauh (*remotely*). Dengan kemudahan serta kesederhanaan pengimplementasikannya, penggunaan SNMP telah dilakukan secara luas, dan sekarang SNMP telah didukung oleh sebagian besar perangkat jaringan yang ada.

2. Landasan Teori

2.1 *Network Monitoring*

Terdapat dua alasan utama untuk memonitor suatu jaringan, yaitu untuk meramalkan perubahan untuk perkembangan yang akan datang dan juga untuk

mendeteksi perubahan yang tidak terduga dalam status jaringan. Perubahan tidak terduga yang mungkin terjadi seperti kegagalan *router* atau *switch*, seseorang *hacker* berusaha mengakses jaringan secara ilegal, atau kegagalan jalur komunikasi. Tanpa kemampuan untuk memonitor jaringan, seseorang *administrator* hanya dapat bereaksi terhadap *problem*, jika *problem* tersebut muncul dibanding dengan mencegah *problem* sebelum terjadi [1].

2.1.1 *Connection Monitoring*

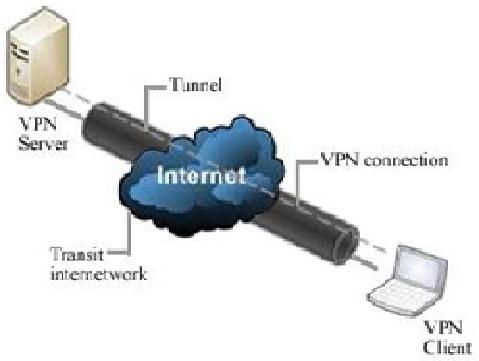
Connection Monitoring adalah salah satu teknik untuk memonitor jaringan. Teknik ini dapat dilakukan dengan melakukan test *ping* antara *monitoring station* dan *device target*, sehingga dapat diketahui bila koneksinya *down*, tetapi metode ini kurang baik, sebab pada jaringan yang besar, dimana terdapat banyak *host* akan memerlukan sumber sistem yang besar [1].

2.1.2 *Traffic Monitoring*

Traffic Monitoring adalah sebuah metode yang lebih canggih dari *network monitoring*. Metode ini melihat paket aktual dari *traffic* pada jaringan dan menghasilkan laporan berdasarkan *traffic* jaringan. Program ini tidak hanya mendeteksi peralatan yang gagal, tetapi mereka juga menentukan apakah suatu komponen *overloaded* atau terkonfigurasi secara buruk. Kelemahan dari program ini karena biasanya bekerja pada suatu segmen tunggal pada satu waktu; jika data perlu didapat dari segmen lain, *software monitoring* harus bergerak pada segmen tersebut, tetapi hal ini dapat diatasi dengan menggunakan *agent* pada *segment remote network* [1].

2.2 *Virtual Private Network* (VPN)

Menurut Aris Wendy [1], *VPN* (*Virtual Private Network*) merupakan suatu cara untuk membuat sebuah jaringan bersifat pribadi (*private*) dan aman dengan menggunakan jaringan publik misalnya *internet*. *VPN* (*Virtual Private Network*) dapat mengirim data antara dua komputer yang melewati jaringan publik sehingga seolah-olah terhubung secara *point-to-point*. Data dienkapsulasi (dibungkus) dengan *header* yang berisi informasi *routing* untuk mendapatkan koneksi *point-to-point* sehingga data dapat melewati jaringan publik dan dapat mencapai akhir tujuan. Sedangkan untuk mendapatkan koneksi bersifat *private*, data yang dikirimkan harus dienkripsi terlebih dahulu untuk menjaga kerahasiaanya sehingga paket yang terlengkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses deskripsi. Proses enkapsulasi data sering disebut "*tunneling*".



Gambar 1. Koneksi Secara VPN

2.3 *Simple Network Monitoring Protocol* (SNMP)

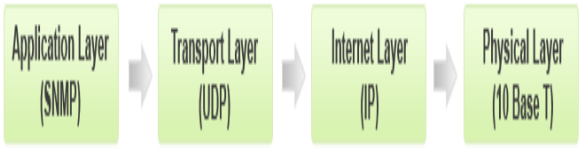
Manajemen TCP/IP terdiri atas stasiun manajemen yang berkomunikasi dengan elemen-elemen jaringan. Elemen jaringan ini biasa berupa *host, router, printer*, dan sebagainya. Sedangkan *station* manajemen jaringan biasanya berupa *workstation* yang menampilkan status elemen yang dimonitornya [3].

Untuk menjalankan aktivitas *monitoring* tersebut antara *manager* dan elemen-elemen jaringan yang dimonitor harus ada komunikasi. Ada dua arah komunikasi, pertama *manager* meminta informasi dari elemen jaringan mengenai keadaannya saat itu, kedua elemen jaringan memberitahukan kondisinya saat itu ke *manager*. Selanjutnya *manager station* menampilkan *interface* dilayar monitornya. Dengan cara seperti ini seorang *network administrator* mengetahui adanya kegagalan dalam jaringannya.

Dalam jaringan TCP/IP, protokol aplikasi yang menangani management jaringan adalah SNMP (*Simple Network Management Protocol*).

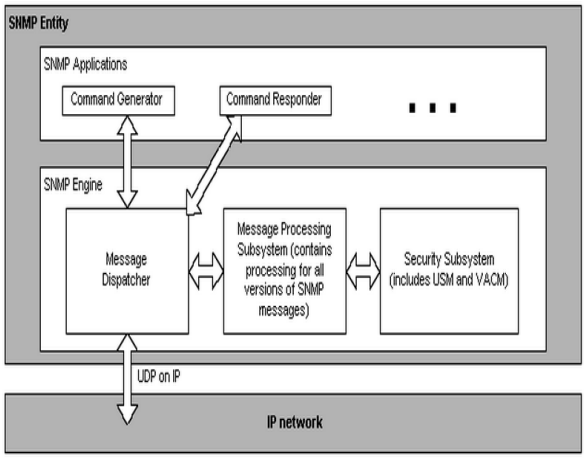
Secara umum SNMP adalah sebuah protokol yang didesain untuk memberikan kemampuan pengumpulan data manajemen perangkat jaringan dan pengkonfigurasian perangkat jaringan secara jarak jauh (*remotely*). Pengelolaan ini dilakukan dengan cara melakukan *polling* dan *setting* variabel-variabel elemen jaringan yang dikelolanya.

SNMP di desain oleh *Internet Engineering Task Force* (IETF) untuk pemakaian di internet. SNMP memanfaatkan datagram UDP untuk pesannya pada perangkat jaringan. Karena pesan UDP bersifat *unreliable* (tidak dapat diandalkan) maka SNMP menggunakan prosedur *time out* dan *retry count* untuk memecahkan masalah ini.



Gambar 2. Konsep Komunikasi SNMP

Arsitektur SNMP termasuk sebuah NMS, *agent*, dan *Message format.* Berikut ini struktur *Message format* dari sebuah pesan SNMP :



Gambar 3. Struktur *Message Format* SNMPv3

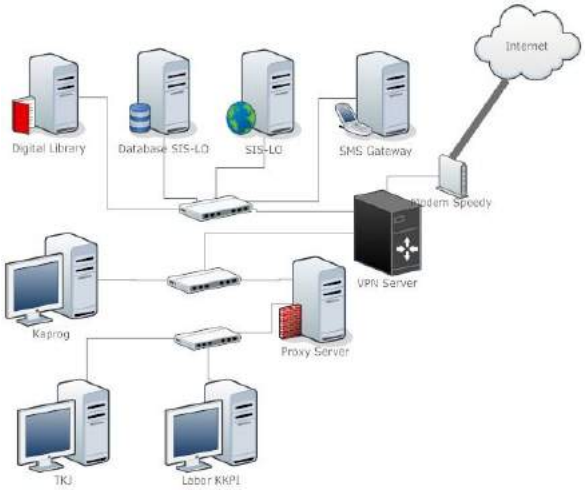
3. Analisa dan Perancangan

3.1 Analisa Permasalahan

Ada dua permasalahan utama yang dihadapi oleh SMK Labor Binaan FKIP UNRI, yaitu :

1. Tidak adanya gambaran yang jelas terhadap pemakaian *packet data* pada jaringan VPN di SMK Labor Binaan FKIP UNRI, sehingga *administrator* tidak bisa memantau dari protokol mana jumlah pemakaian *bandwidth* terbesar pada jaringan VPN di SMK Labor Binaan FKIP UNRI.
2. Kurangnya *monitoring* terhadap penggunaan jalur lalu lintas data dari jaringan *internet* di SMK Labor Binaan FKIP UNRI, sehingga penggunaan *internet* kurang optimal dan tidak tepat sasaran.

Topologi Jaringan yang digunakan di SMK Labor Binaan FKIP UNRI adalah menggunakan topologi jaringan *star*. Alasan digunakannya topologi jaringan *star* adalah karena pada topologi jaringan *star* semua *client* terhubung secara langsung ke *hub*, sehingga apabila ada gangguan pada salah satu komputer *client* maka komputer *client* lainnya tidak akan mengalami gangguan. Kabel yang digunakan untuk menghubungkan *computer client* ke *hub, access point* maupun komputer *server* ke *hub* adalah kabel UTP (*Unsielded Twisted Pair*).



Gambar 4. Topologi Jaringan SMK Labor Binaan

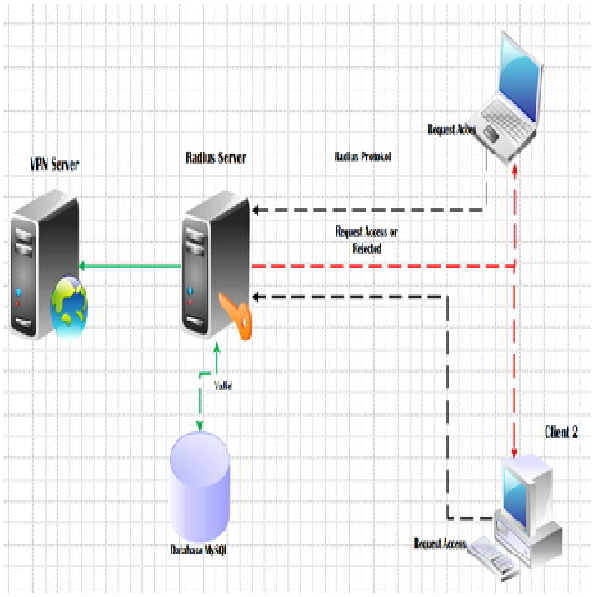
3.2 Pemecahan Permasalahan

Permasalahan yang dihadapi oleh SMK Labor Binaan FKIP UNRI, dapat diatasi dengan dirancangnya sebuah aplikasi *network monitoring tools* pada jaringan VPN (*Virtual Private Network*) dengan menggunakan SNMP, sehingga dapat memanfaatkan SIS-LO serta *content* yang lain, dapat mengatasi permasalahan pengaturan *bandwidth* yang diterima setiap *user*. Dalam aplikasi ini *admin* dapat mengatur besar *bandwidth* yang diinginkan setiap pengguna sesuai dengan kebutuhannya. Aplikasi ini akan memantau arus lalu lintas penyaluran data pada jaringan *VPN* di SMK Labor Binaan FKIP UNRI. Hanya *admin* yang mempunyai akses pada aplikasi ini.

Aplikasi ini dapat berjalan, jika sudah memiliki sebuah *server* karena semua pengaturannya yang dilakukan *admin* akan dilakukan di *server*. SMK Labor Binaan FKIP UNRI telah memiliki sebuah *server VPN* yang telah dikonfigurasi dan telah terkoneksi dengan jaringan *internet*. Infrastruktur jaringan yang ada di SMK Labor Binaan FKIP cukup memadai dengan telah terpasangnya beberapa *node* jaringan dibeberapa ruangan labor, kelas dan untuk *hotspot* sekolah, semua terhubung ke *server*. Koneksi *internet* yang telah terpasang menggunakan salah satu ISP yakni Telkom dengan produk speedy dengan *downstream* 2 Mbs dan *upstream* 512 Kbps.

3.3 Perancangan Topologi Simulasi

Simulasi akan dilakukan dengan menggunakan topologi seperti gambar dibawah ini :



Gambar 5. Topologi Simulasi Jaringan VPN

Simulasi diawali dengan login user ke PC Router melalui VPN. Autentifikasi user dilakukan dengan memanfaatkan VPN. VPN pada penelitian ini merupakan kombinasi antara PPtP, Radius Server dan MySQL. Saat user melakukan autentifikasi, informasi yang di-input oleh pengguna berupa username dan password akan diterima oleh PPtP dan kemudian oleh PPtP informasi tersebut akan diperiksa oleh Radius Server. Radius Server akan menjawab dengan TRUE atau FALSE. Jika TRUE maka Radius Server akan mengeluarkan jenis layanan untuk user ke sistem dan pada saat yang bersamaan maka proses accounting yang dilakukan oleh MRTG dengan menggunakan SNMP juga berjalan.

4. Implementasi dan Pengujian

4.1 Instalasi dan Konfigurasi VPN Server

Tahap yang pertama dilakukan adalah dengan melakukan instalasi dan konfigurasi *VPN Server* pada terminal *Linux Ubuntu.* Untuk meng-*install* dan mengkonfigurasi *VPN Server* dapat dilakukan dengan cara :

1. Untuk meng-*install vpn server* ketikkan perintah dibawah ini pada terminal :

```
root@oya:/#apt get install pptpd
```

2. Selanjutnya konfigurasi *pptp* yang telah ter-*install* dengan cara sebagai berikut :

```
root@oya:/#gedit /etc/ppp/pptpd.conf
```

uncomment local ip dan *remote ip*

```
#( Recommended)
Localip 192.168.1.1
Remoteip 192.168.1.234-238
```

Kemudian merubah local *ip* yang merupakan *ip vpn server* menjadi 192.168.1.1 ,dan *remote ip* yang berfunngsi untuk menghubungkan klien ke *vpn* akan diberi alamat *private ip* dengan rentang *ip* dari 192.168.1.234 ke 192.168.1.238

3. Kemudian mengkonfigurasi *dns* pada *pptp* dengan cara mengetikkan perintah berikut:

```
root@oya:/#gedit /etc/ppp/pptpd-options
```

uncomment ms-dns lalu ganti menjadi *dns google*

```
#client. See KB311218 in Microsoft's
knowledge base for more information
ms-dns 8.8.8.8
ms-dns 8.8.4.4
```

4. Setelah itu, melakukan pengaturan *forward ipv4* dengan perintah sebagai berikut :

```
root@oya:/#gedit /etc/sysctl.conf
```

uncomment net.ipv4.ip_forward = 1 , seperti pada gambar dibawah ini :

```
# Uncomment the next line to enable TCP/IP
SYN cookies
# See http://lwn.net/Articles/277146
# Note : This may impact IPv6 TCP sessions
too
# net.ipv4.tcp_syncookies=1
# Uncomment the next line to enable packet
forwarding for IPv4
Net.ipv4.ip_forward = 1
```

Untuk menjalankan perubahan pada *sysctl.conf* maka harus melakukan *reload sysctl* pada terminal dengan cara sebagai berikut :

```
Root@oya:/#sysctl -p
```

5. Kemudian melakukan *setting iptables* NAT *(Network Address Translation)* yang bertujuan agar klien dapat terkoneksi dengan *internet.* Konfigurasi *iptables* dilakukan pada *rc.local* dengan perintah sebagai berikut :

```
Root@oya:/#gedit /etc/rc.local
```

Tambahkan perintah berikut :

```
Root@oya:/#gedit /etc/rc.local
iptables -t nat -A POSTROUTING -o eth0 -j
MASQUERADE
```

```
iptables --table nat --append
POSTROUTING --out-interface ppp0 -j
MASQUERADE
iptables -I INPUT -s 192.168.1.0/24 -i ppp0 -
j ACCEPT
iptables --append FORWARD --in-interface
eth0 -j ACCEPT
```

6. Langkah berikutnya adalah me-*restart* paket *pptpd* dengan cara mengetikkan perintah berikut :

```
Root@oya:/# service pptpd restart
```

4.2 Instalasi dan Konfigurasi Radius Server

Tahap konfigurasi *Radius server* ini menggunakan sebuah komputer dengan sistem operasi *Linux Ubuntu 12.04, dan paket freeradius.* Paket tersebut adalah paket utama untuk menjalankan *radius server. Sebelum melakukan penginstalan paket freeradius terlebih dahulu install paket web server yaitu apache, MySQL dan phpmyadmin yang bertujuan untuk mengintegrasikan freeradius dengan MySQL.*

4.3 Instalasi dan konfigurasi SNMP

Tahapan yang dilakukan dalam instalasi dan konfigrasi SNMP adalah sebagai berikut :

1. Melakukan pengintstalan SNMP dengan mengetikkan di terminal

```
root@oya:~#apt-get install snmp snmpd
```

2. Setelah penginstalan selesai, maka lakukan perubahan pada pengaturan agen dengan masuk ke */etc/snmp/snmpd.conf* dengan perintah pada terminal :

```
root@oya:~#nano /etc/snmp/snmpd.conf
```

Pada *snmpd.conf* edit pada baris dibawah ini :

```
#rocomunity public localhost //(hilangkan
tanda pagar
```

```
Syslocaltion Monitoring MRTG
```

3. Selanjutnya *restart* SNMPD

```
root@oya:~#sudo /etc/init.d/snmpd restart
```

4. Selanjutnya lakukan pengetesan dengan pada *localhost* dengan mengetikkan pada terminal :

```
root@oya:~#snmpwalk –v2c –c public
localhost
```

5. Setelah selesai melakukan penginsatalan SNMP maka selanjutnya melakukan penginstalan paket MRTG yang akan menggambarkan trafik jaringan dengan mengetikkan perintah pada terminal sebagai berikut :

```
root@oya:~#sudo apt-get install mrtg
```

6. Setelah proses instalasi paket mrtg selesai maka selanjutnya mengkonfigurasi mrtg dengan cara :

```
root@oya:~# cfgmaker --global 'workdir:
/var/www/mrtg' --output /etc/mrtg.cfg
public@localhost
```

cfgmaker digunakan untuk konfigurasi *text file* untuk pengumpulan data MRTG.

7. Selanjutnya menampilkan grafik konfigurasi MRTG dilakukan dengan cara meng-*generate file index.html* MRTG dengan mengetikkan perintah :

```
root@oya:~#indexmaker /etc/mrtg.cfg –
columns=1 –output
/var/www/mrtg/index.html
```

8. Setelah pengaturan selesai lakukan pengetesan MRTG dapat diakses dari *browser* dengan alamat http://192.168.1.1/mrtg.

4.4 Instalasi dan Konfigurasi Ntop

Ntop merupakan aplikasi untuk melihat *traffic* pada *network* dan melakukan pemeriksaan pada setiap *protocol* yang berjalan pada jaringan *server*, penulis menggunakan aplikasi *Ntop* ini untuk me-*monitoring* pemakaian jaringan untuk setiap *protocol* yang berjalan pada jaringan VPN yang nantinya akan di *link*-kan dari aplikasi *monitoring* yang akan dirancang.

Tahap instalasi dan konfigurasi *Ntop* sebagai berikut :

1. Melakukan pengintstalan paket *Ntop* dengan mengetikkan di terminal

```
root@oya:~#apt-get install ntop rrdtool
rrdtool-tcl
```

2. Setelah paket sudah terunduh dan di-*install* maka selanjutnya mengubah *permission* pada file */var/lib/ntop/rrd*, ini bertujuan agar aplikasi *ntop* tidak dibatasi hak aksesnya pada saat bisa mengupdate data *traffic* yang berjalan pada jaringan. Dengan mengetikkan perintah pada terminal :

```
root@oya:~#chmod –Rf 755 /var/lib/ntop/rrd
```

3. Agar manajemen paket jaringan yang berjalan bisa di baca *ntop* maka aktifkan *dpkg* dengan mengetikkan perintah pada terminal :

```
root@oya:~#dpkg-reconfigure ntop
```

4. Selanjutnya *restart service Ntop*

```
root@oya:~#sudo /etc/init.d/ntop start
```

4.5 Sistem Monitoring Jaringan VPN

1. Menu *Login*

Halaman ini adalah tampilan awal dari aplikasi *monitoring*. Pada halaman ini setiap admin yang ingin masuk ke dalam aplikasi *web* diharuskan *login* terlebih dahulu, dengan memasukkan *username* dan *password*. Pada halaman ini *radius server* akan melakukan *autentifikasi* terhadap *pengguna sistem monitoring VPN*.

Gambar 6. Tampilan Menu *Login*

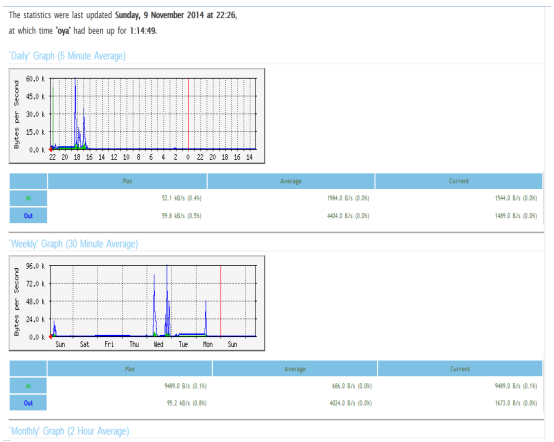
2. Menu *VPN User*

Halaman ini adalah tampilan salah satu menu dalam aplikasi yaitu menu *user*. Pada menu *user* memiliki fungsi untuk menampilkan *user list, new user, edit user* dan juga *remove user*. Berikut tampilan menu *VPN user*.

Gambar 7. Tampilan Menu *VPN User*

3. Menu Grafik

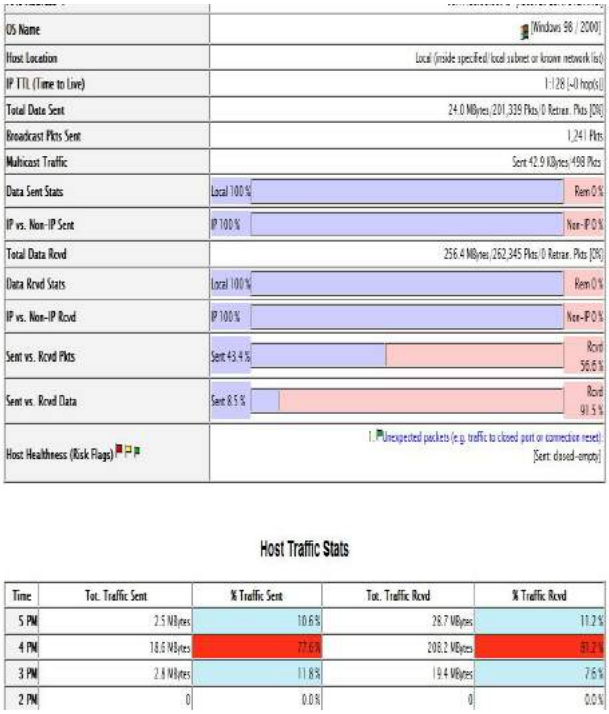
Pada halaman menu grafik , administrator dapat melihat lalu lintas data melalui *Multi Router Traffic Graphic* (MRTG).



Gambar 8. Tampilan Menu *Graphic* MRTG

4. Menu T*raffic Data Record*

Pada halaman menu *traffic data record* akan di link-kan pada aplikasi Ntop, link tersebut mengarah pada server dengan port 3000, pada aplikasi ini dapat dilihat melihat lalu lintas data berdasarkan protokol yang dilewati oleh jaringan komputer tersebut. Pada halaman ini menampilkan laporan *traffic* yang dihasilkan oleh *software* Ntop secara rinci.



Host Traffic Stats

Time	Tot. Traffic Sent	% Traffic Sent	Tot. Traffic Rcvd	% Traffic Rcvd
5 PM	2.5 MBytes	10.6 %	26.7 MBytes	11.2 %
4 PM	18.6 MBytes	77.6 %	208.2 MBytes	87.2 %
3 PM	2.8 MBytes	11.8 %	19.4 MBytes	7.6 %
2 PM	0	0.0 %	0	0.0 %

Gambar 9. Tampilan Menu *Traffic Data Record*

4.6 Pengujian Hasil Tampilan dan Fungsi Halaman Aplikasi

Hasil pengujian dari tampilan dan fungsi halaman aplikasi *monitoring* jaringan dapat dilihat dalam tabel. 1 berikut :

Tabel 1. Hasil Uji Tampilan dan Fungsi

Bagian Halaman	Pengujian	Hasil Pengujian	
		Berhasil	Gagal
Awal	Proses *Login*	√	
Home	Akses halaman *home*	√	
	Akses proses *Vpn User*	√	
	Akses hasil Grafik *MRTG*	√	
	Akses hasil *Traffic Ntop*	√	
	Menambahkan *Vpn User*		
Hasil *Monitoring* Akses *User*	Merubah *pass vpn user*	√	
	Menghapus akun *vpn user*	√	
	Melakukan *Test Connectivity*	√	
	Melakukan *Disconectivity* pada user	√	
Hasil *Traffic Monitoring*	Melihat *Server* status	√	
	Melihat *Upload download User*	√	
	Melihat *grafik*	√	
	Melihat *Traffic*	√	

4.7 Pengujian Hasil Aplikasi Monitoring Traffic Jaringan

Pengujian hasil aplikasi *monitoring* jaringan dilakukan untuk mengetahui keakuratan hasil. Proses pengujian dilakukan dengan cara membandingkan data trafik *in* dan *out* pada *user* dengan menggunakan *software Ntop* dengan hasil trafik dari aplikasi *monitoring* yang telah dibangun.

Tabel 2. Data hasil perbandingan trafik *in* dan *out* *Aplikasi Network Traffic Monitoring* dengan *Ntop*

Durasi Pengamatan (menit)	*Traffic Aplikasi* (*Mb*)		*Traffic NTop* (*Mb*)		*Persentase Selisih* (*%*)	
	In	*Out*	*In*	*Out*	*In*	*Out*
5 menit	15.85	0.99	17.30	2.30	4.37	39.73
10 menit	34.04	1.84	37.20	4.80	4.44	44.58
15 menit	130.67	5.50	139.90	14.30	3.41	44.44
20 menit	253.39	9.85	256.30	23.90	0.57	41.63

Dari tabel. 2 diatas terlihat bahwa rata-rata nilai *traffic in* dan *out* antara aplikasi *monitoring* dengan *software Ntop* memiliki nilai yang hampir sama. Selisih hasil trafik i*n* berkisar antara 1 – 10 *Mb* dengan persentase ≤ 5 % dan *out* hanya berkisar antara 1 – 15 *Mb* dengan persentase ≤ 50 % dikarenakan pada aplikasi *Ntop* selalu melakukan *request(upload)* secara otomatis setiap 10 detik . Sehingga dapat disimpulkan bahwa aplikasi *monitoring traffic* jaringan VPN telah

berhasil memberikan *input* dan *output traffic* yang valid.

5. Kesimpulan

Berdasarkan hasil rancang bangun aplikasi *traffic monitoring* jaringan VPN, juga dari data-data yang didapatkan dari hasil pengujian, dapat diambil kesimpulan sebagai berikut :

1. Penerapan sistem *database* dalam penambahan *VPN user* berhasil dilakukan. Proses verifikasi dan autentifikasi *user* dari *shell* telah di integrasikan langsung melalui *MySQL*. Hal ini akan mempermudah administrator dalam memanajemen *user* pada jaringan VPN.
2. Aplikasi network trafik menghasilkan laporan traffic secara *realtime* berdasarkan *port TCP* dan *UDP* dan dapat di *access* secara *private* dengan memanfaatkan teknologi VPN sehingga dapat membantu pihak administrator jaringan dalam memantau dan menganalisa masalah yang terjadi pada jaringan yang berada di SMK Labor Binaan FKIP UNRI di mana saja dan kapanpun dengan menggunakan laptop yang tersambung ke internet.
3. Sistem dapat melakukan proses *disable* dan *enable* terhadap *vpn user* sehingga administrator jaringan memiliki hak untuk mengunci jaringan internet pada *VPN User* .

6. Referensi

[1] *Cisco Networking Academy Program* (2001), *Second-Year Companion Guide 2nd Edition*, Cisco System Inc.

[2] Wendy, Aris, dan Ramadhana, Ahmad SS (2005), *Membangun VPN Linux Secara Cepat*, Andi, Yogyakarta

[3] Mansfield, Niall (2004), *Practical TCP/IP : Mendesain, Menggunakan, dan TroubleShooting Jaringan TCP/IP di Linux dan Windows (Jilid I)*, Andi , Yogyakarta.