Tugas Manajemen Jaringan

Design and Implementation Fast Response System Monitoring Server Using Simple Network Management Protocol (SNMP)

Oleh :

NAMA : Stevanus Christivan Panjaitan

NIM : 09011181520030

FAKULTAS ILMU KOMPUTER

JURUSAN SISTEM KOMPUTER

UNIVERSITAS SRIWIJAYA

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 .

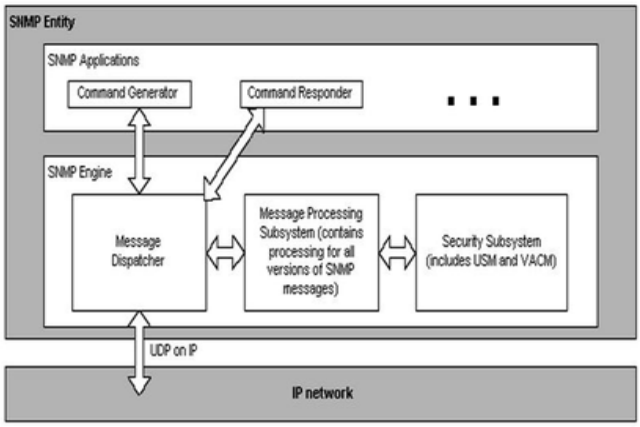
Untuk menjalankan aktivitas *monitoring* tersebut antara *manager* dan elemen-elemen jaringan yang dimonitor harus ada komunikasi. Ada dua arah komunikasi, pertama *manager* meminta informasi dari elemen jaringan mengenai keadaannya saat itu, kedua elemen jaringan memberitahukan kondisinya saat itu ke *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.

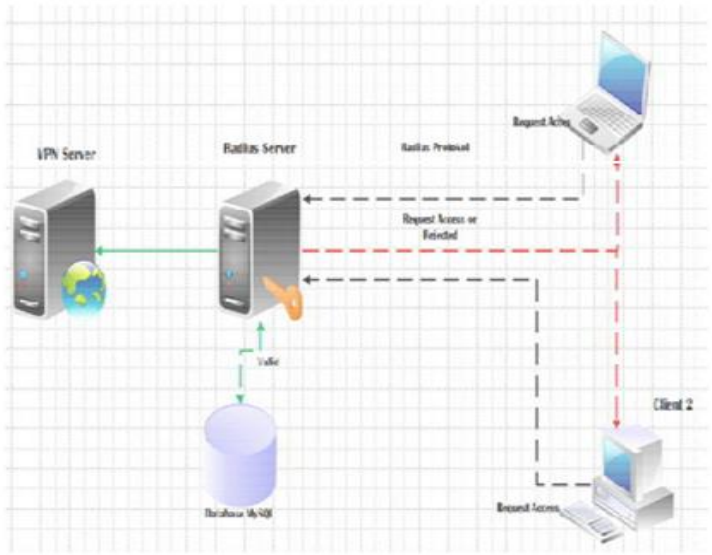
SNMP di desain oleh *Internet Engineering Task Force* (IETF) untuk pemakaian di internet. SNMP memanfaatkan datagram UDP untuk pesannya pada perangkat jaringan. Karena pesan UDP bersifat *unreliable* (tidak dapat diandalkan) maka SNMP menggunakan prosedur *time out* dan *retry count* untuk memecahkan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

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



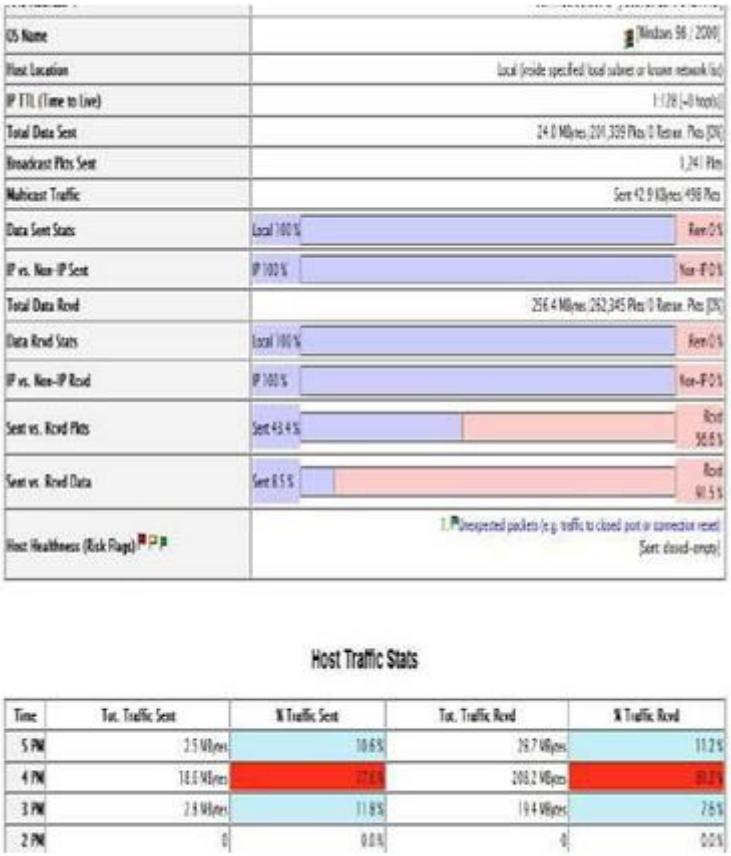
Gambar 3. Struktur *Message Format* SNMPv3

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.



Gambar 5. Topologi Simulasi Jaringan VPN

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.



Gambar 9. Tampilan Menu *Traffic Data Record*

- **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.