

**ANALISIS PROTOCOL SNMP
MENGUNAKAN WIRESHARK**



Disusun Oleh:

Nama : Muhammad Fajar Putra

NIM : 0901181520009

**JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA**

2018

Abstrak

Simple Network Management Protocol(SNMP) adalah sebuah protokol yang didesain untuk memberikan kemampuan kepada pemakai (user) untuk mengelola jaringan komputer dari jarak jauh dalam satu pusat saja

1. Pendahuluan

Perkembangan teknologi informasi, khususnya jaringan memungkinkan terjadinya pertukaran informasi yang cepat dan semakin kompleks. Pengaturan jaringan yang baik tentu akan memaksimalkan pemanfaatan informasi tersebut. Oleh sebab itu jaringan harus diatur dan dipantau, sehingga kelancaran pengiriman informasi dapat berjalan baik. Semakin besar dan luas sistem jaringan, maka akan semakin sulit untuk mengatur dan mengawasinya. Jadi diperlukanlah suatu manajemen jaringan yang baik dan sistem monitoring yang mampu memantau kinerja dari jaringan tersebut, kemudian sistem monitoring yang didesain untuk memantau status infrastuktur LAN/WAN, memastikan device tersebut dalam kondisi normal dan aktif, dapat melihat statistik dalam bentuk grafik, pengecekan kondisi sinyal, dapat memprediksi masalah yang akan muncul atau dapat memantau paket data yang lewat di trafik jaringan

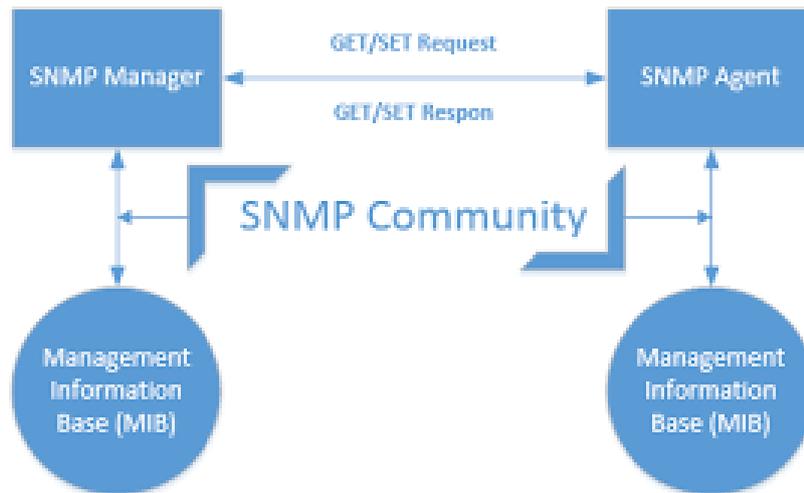
SNMP merupakan protokol untuk manajemen peralatan yang terhubung dalam jaringan IP (Internet Protocol). Peralatan-peralatan itu antara lain switch, router, modem, komputer, server dan lain-lain. SNMP menggunakan data-data yang didapatkan dari komunikasi UDP dengan device/peralatan yang masuk dalam jaringan tersebut. SNMP dapat meminta data ataupun melakukan setting kepada peralatan yang bersangkutan.

2. Tujuan

Menampilkan hasil yang diperoleh dari aplikasi Wireshark sebagai laporan yang penting untuk mengamati dan mengatur jaringan. Menghasilkan keluaran berupa grafik statistik dimana data yang diperoleh adalah data yang kita ambil dari Wireshark.

3. Pembahasan

Elemen elemen SNMP



1. Manager

Manager adalah pelaksana dan manajemen jaringan. Pada kenyataannya manager ini merupakan komputer biasa yang ada pada jaringan yang mengoperasikan perangkat lunak untuk manajemen jaringan. Manager ini terdiri atas satu proses atau lebih yang berkomunikasi dengan agen-agensya dan dalam jaringan. Manajer akan mengumpulkan informasi dari agen dari jaringan yang diminta oleh administrator saja bukan semua informasi yang dimiliki agen.

2. MIB atau Manager Information Base

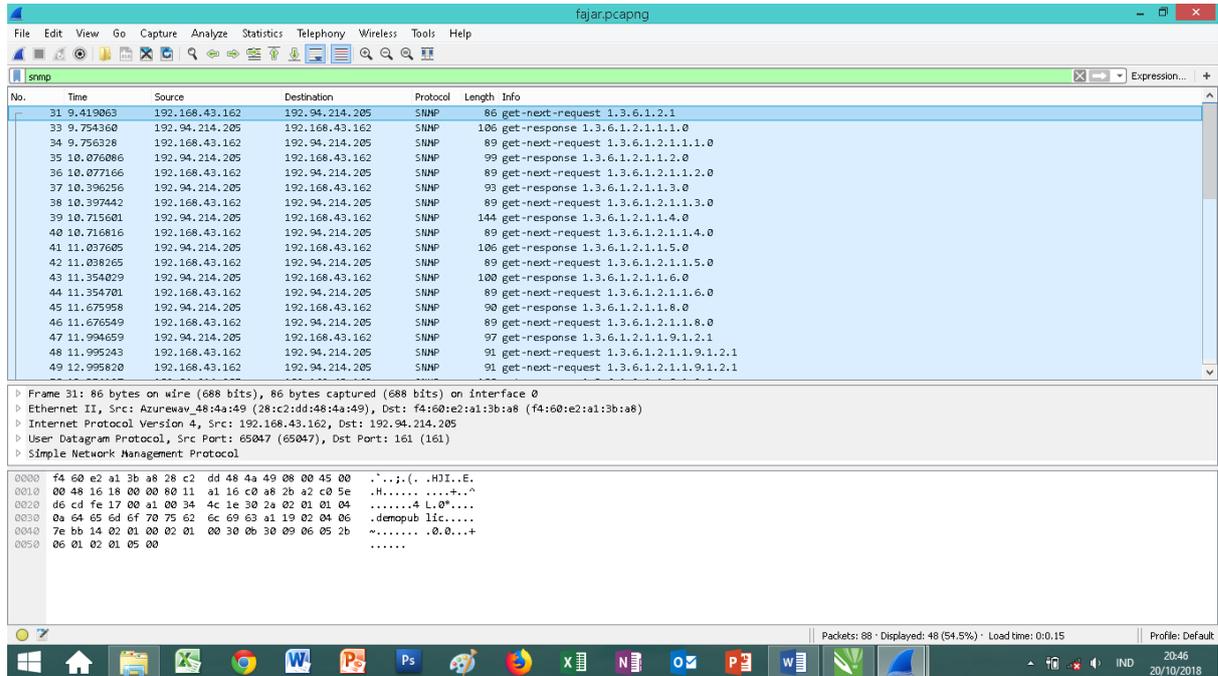
Dapat dikatakan sebagai struktur basis data variabel dari elemen jaringan yang dikelola. Struktur ini bersifat hierarki dan memiliki aturan sedemikian rupa sehingga informasi setiap variabel dapat dikelola atau ditetapkan dengan mudah.

MIB mempunyai beberapa struktur diantaranya:

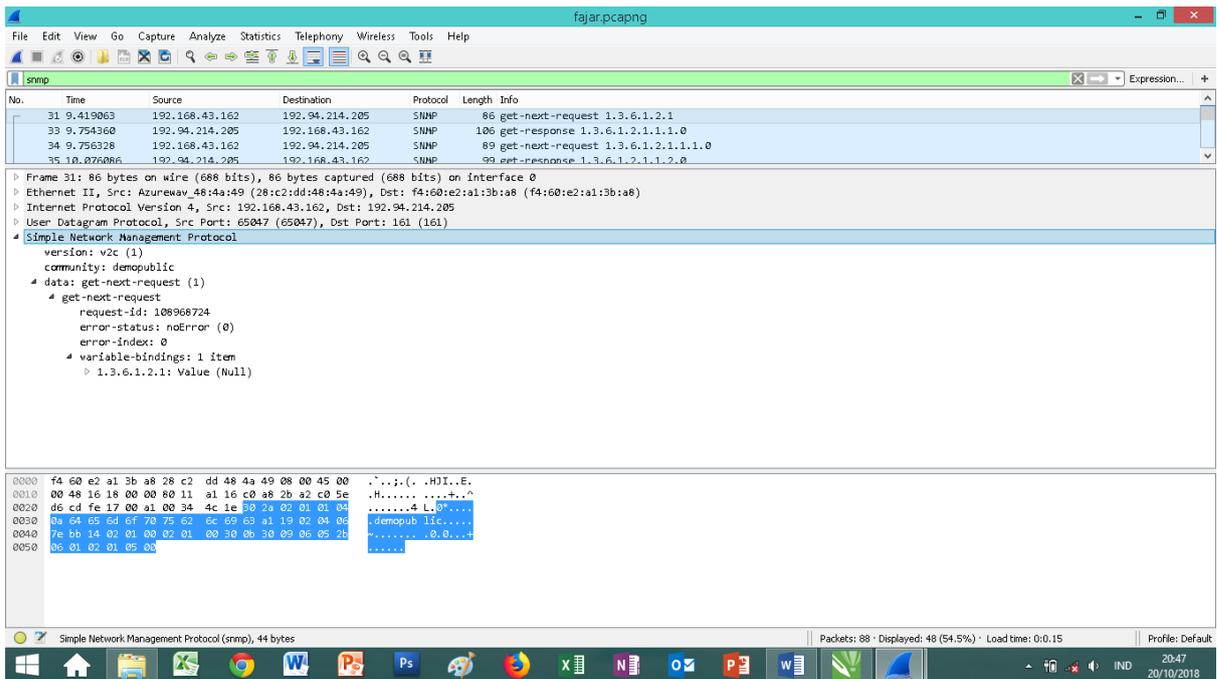
- Setiap object mempunyai ID unik (OID)
- MIB mengasosiasikan setiap OID menggunakan label dan parameter lain.
- MIB bertindak sebagai kamus data yang digunakan untuk menyusun terjemahan pesan SNMP

3. Agent

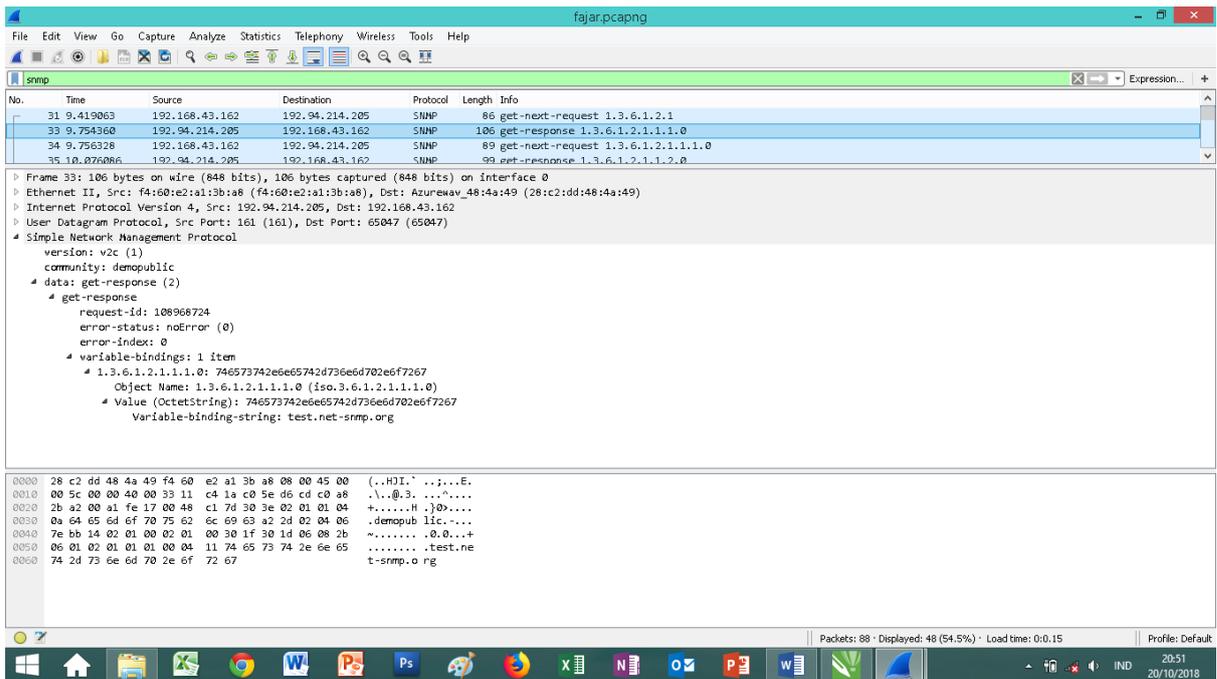
Agent merupakan perangkat lunak yang dijalankan disetiap elemen jaringan yang dikelola. Setiap agen mempunyai basis data variabel yang bersifat lokal yang menerangkan keadaan dan berkas aktivitasnya dan pengaruhnya terhadap operasi.



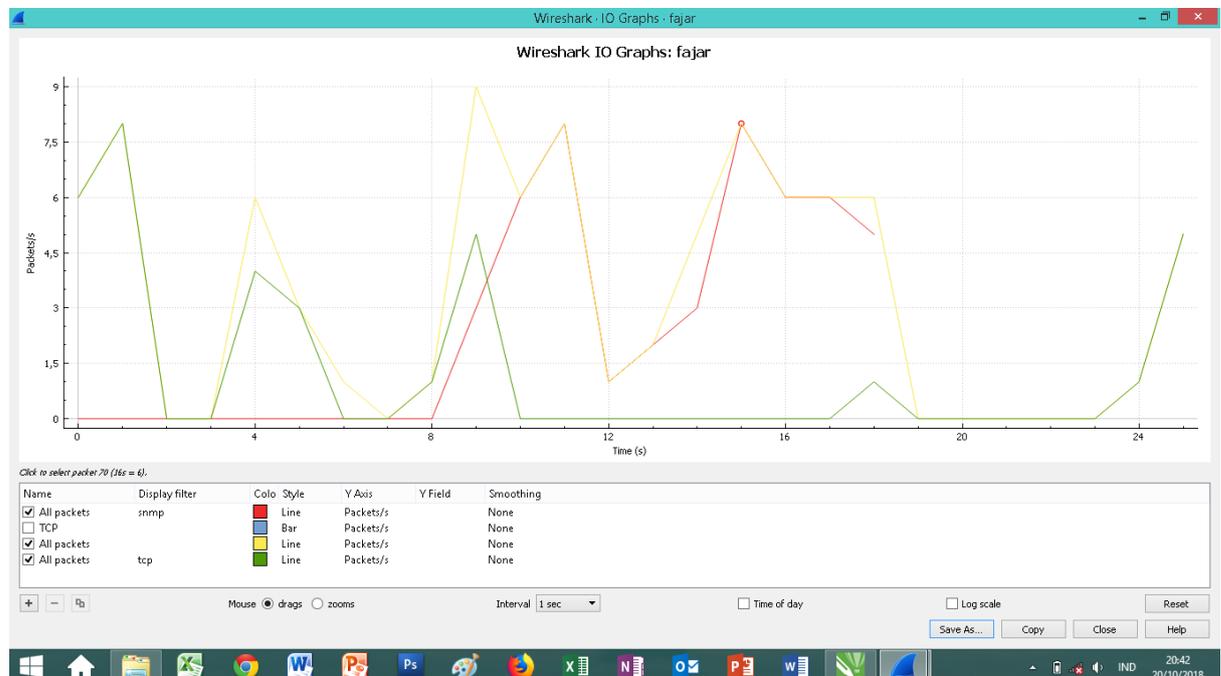
Gambar diatas menjelaskan tentang beberapa IP yang sedang melakukan traffic data dengan request dan response, dalam aplikasi Wireshark inilah kita dapat menganalisa IP mana yang sedang melakukan request dan melakukan response.



Pada Gambar diatas merupakan sebuah capturan dari pcaps menggunakan aplikasi whireshark dimana pada gambar tersebut menjelaskan tentang bagaimana IP melakukan request. IP source 192.168.43.162 dan IP destination 192.94.214.205 dan menggunakan protocol SNMP dengan request-id nya yaitu request-id: 108968724, pada variabel binding hanya ada 1 item yaitu 1.3.6.1.2.1: Value (Null) dan nama objeknya: 1.3.6.1.2.1 (iso.3.6.1.2.1). Maksud dari angka 1.3.6.1.2.1 yaitu 1 merupakan ISO, 3 org , 6 yaitu dod, 1 merupakan angka internet , 2 merupakan management, dan 1 merupakan MIB dari variable variable tadi terbentuklah satu kesatuan variable pada saat IP meminta request.



Pada gambar tersebut menjelaskan tentang bagaimana IP melakukan response. Dari capturan diatas IP source 192.94.214.205 dan IP destination 192.168.43.162 dan menggunakan protocol SNMP. Cara perhitungan variable sama dengan saat IP melakukan request.



Gambar diatas adalah grafik dari traffic paket protokol SNMP. Traffic SNMP ditunjukkan dengan bar berwarna merah, semua paket ditandai dengan grafik line berwarna kuning, dan TCP ditandai dengan grafik line berwarna hijau tua.

4. Kesimpulan

SNMP adalah sebuah protokol yang dirancang untuk memberikan kemampuan kepada pengguna untuk memantau dan mengatur jaringan komputernya secara sistematis dari jarak jauh atau dalam satu pusat kontrol saja. Dengan menggunakan protokol ini kita bisa mendapatkan informasi tentang status dan keadaan dari suatu jaringan.