# MANAJEMEN JARINGAN

## Analisis Trafik SNMP Menggunakan WireShark dan RapidMiner Studio


Nama : Endi Kumara

NIM : 09011281520098

Kelas : SK7 Pilihan

Dosen Pengampuh : Deris Stiawan, M.T., Ph.D



JURUSAN SISTEM KOMPUTER

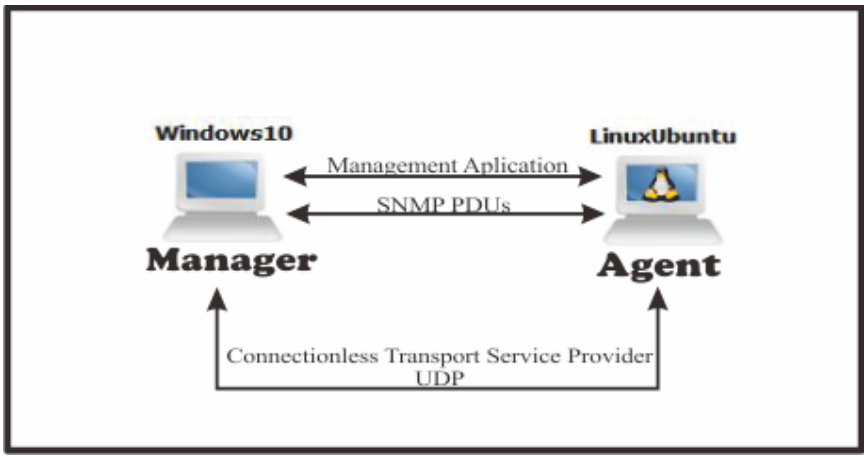
FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA


2018

# A. Pendahuluan

SNMP merupakan protokol untuk menajemen 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.




Gambar 1. Struktur SNMP

Dengan menggunakan protokol ini kita bisa mendapatkan informasi tentang status dan keadaan dari suatu jaringan. Protokol ini menggunakan transpor UDP pada port 161. Komponen utama dalam proses manajemen jaringan TCP/IP terdiri dari tiga elemen, yaitu :

- MIB (Management Information Database) Adalah struktur basis data variabel dari elemen jaringan yang dikelola. Pada kelompok interface terdapat variabel objek MIB yang mendefinisikan karakteristik interface diantaranya : ifInOctets mendefinisikan jumlah total byte yang diterima, ifOutOctets mendefinisikan jumlah total byte yang dikirim, ifInErrors mendefinisikan jumlah paket diterima yang dibuang karena rusak, ifOutErrors mendefinisikan jumlah paket dikirim yang dibuang karena usak, dan variable objek lainnya yang juga berkaitan dengan paket internet.
- Agen Merupakan software yang dijalankan di setiap elemen jaringan yang dimonitor. Agen bertugas mengumpulkan seluruh informasi yang telah ditentukan dalam MIB.
- Manajer Merupakan software yang berjalan di sebuah host di jaringan. Bertugas meminta informasi ke Gb 1: Struktur SNMP Agen. Manajer biasanya tidak

meminta semua informasi yang dimiliki oleh agen, tetapi hanya meminta informasi tertentu saja yang akan digunakan untuk mengamati unjuk kerja jaringan. Manager biasanya menggunakan komputer yang memiliki tampilan grafis dan berwarna sehingga selain dapat menjalankan fungsinya sebagai Manager, juga untuk melihat grafik unjuk kerja dari suatu elemen jaringan yang dihasilkan oleh proses monitoring. SNMP menggunakan UDP (User Datagram Protocol) sebagai protocol transport untuk mengirimkan pertanyaan dan menerima jawaban dari agen SNMP.

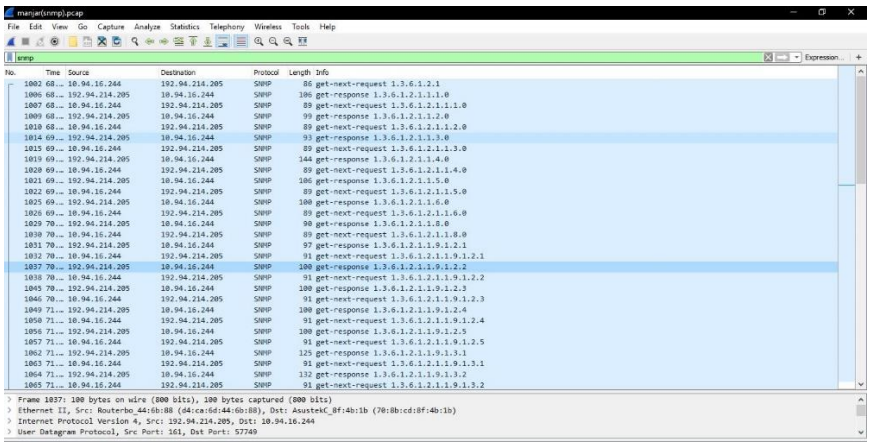
SNMP terdiri dari dua jenis yakni :

- Network Management Station, yang berfungsi sebagai pusat penyimpanan untuk pengumpulan dan analisa dari data manajemen jaringan.
- Peralatan yang dimanage menjalakan SNMP agent, yaitu proses background yang memonitor peralatan tersebut dan mengkomunikasikannya ke network management station.

Peralatan yang memiliki SNMP agent antara lain : CISCO router, Linux Server.

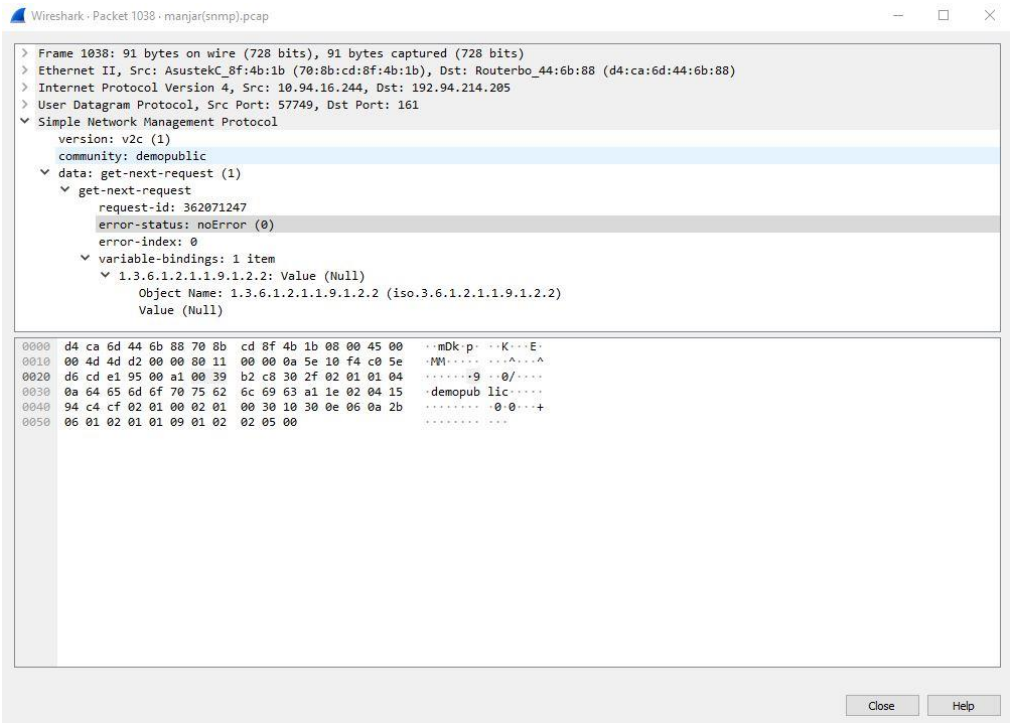
# B. Hasil dan Analisa

Sebelum melakukan tapping data lakukan penginstallan terminal ubuntu pada windows karena ubuntu ini akan bersifat sebagai agent dan MIB. Setelah itu install SNMP melalui terminal ubuntu *sudo apt-get install snmp* dan *sudo apt-get install snmpd*. Buka wireshark untuk melakukan tapping data. Setelah itu jalankan *snmpwalk -v2c -Os -c demopublic test.net-snmp.org* protokol SNMP terdeteksi di wireshark.



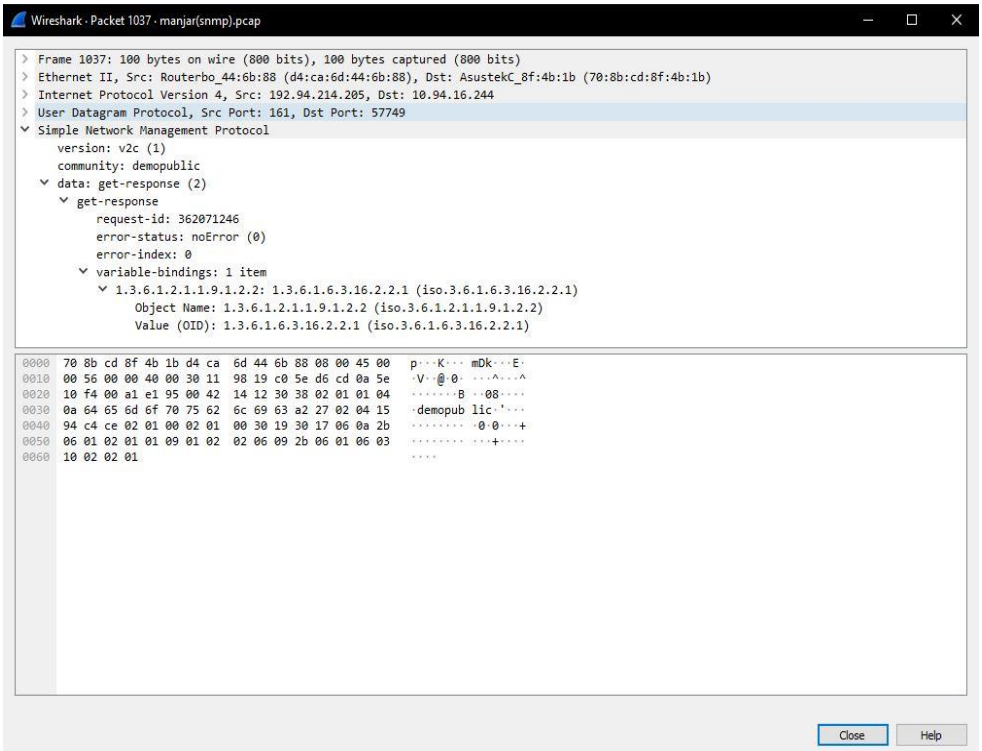

Gambar 2. Hasil Tapping di wireshark

Pada gambar 2 terlihat info protocol SNMP terbagi menjadi dua yaitu get next request dan get response.



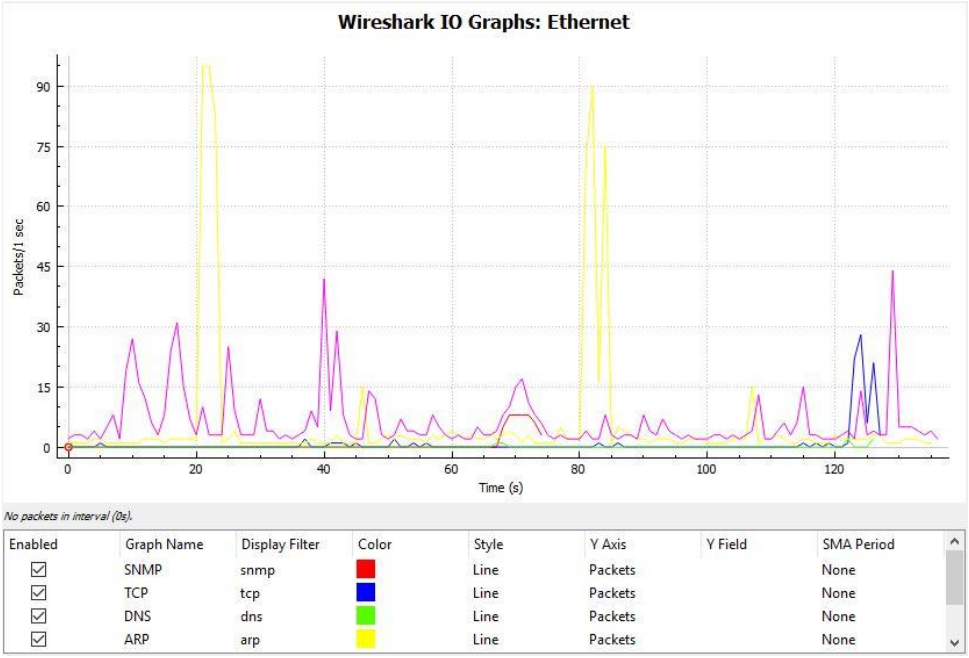

Gambar 3. Salah satu isi paket data SNMP get next request

Pada gambar 3 paket data SNMP get next request yang dimana IP resource 10.94.16.244 sedangkan IP destination 192.94.214.205 dan request id 362071247. Pada paket data ini terdapat 1 variabel binding yang dimana memiliki value (null).



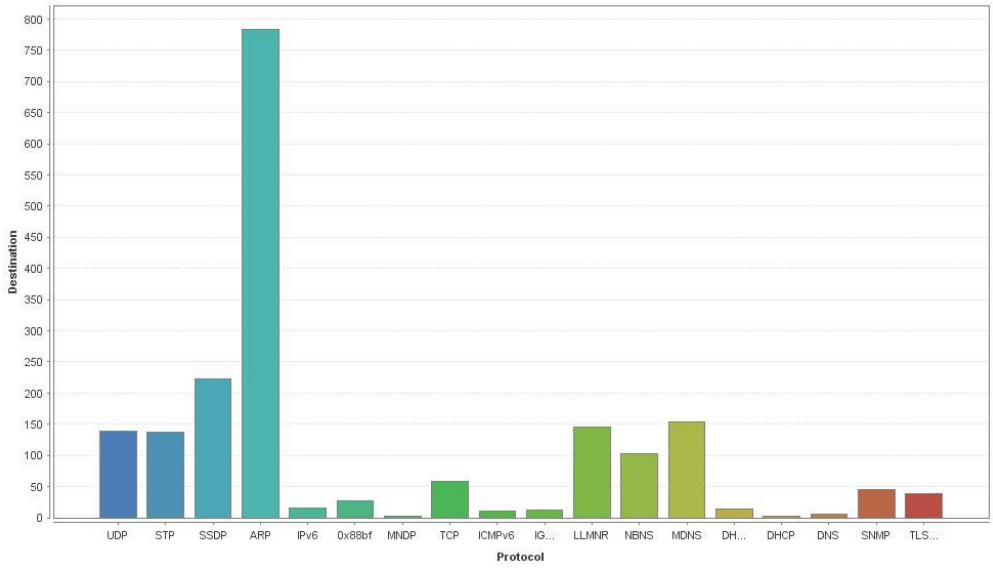

Gambar 4. Salah satu isi paket data SNMP get response

Pada gambar 4 paket data SNMP get response yang dimana IP resource 192.94.214.205 dan IP destination 10.94.16.244 dan request id 362071246. Pada paket data ini value variabel bindingnya ada. Terlihat ketika SNMP get next request paket data tersebut hanya merequest sehingga nilai valuenya null sedangkan pada SNMP get response paket data ini telah merespon request sehingga valuenya bernilai.




Gambar 5. Monitoring traffic data menggunakan wireshark

Pada gambar 5 monitoring traffic data di lakukan dengan menggnakan koneksi ethernet pada perpustakaan UNSRI monitoring ini di lakukan secara real time maka paket data akan terus bertambah setiap per second nya. Protokol yang banyak terdeteksi oleh wireshark adalah ARP sedangkan untuk SNMP sedikit karena saat tapping data hanya berlangsung selama 1 menit maka destination yang menggunakan protokol SNMP hampir mencapai 50. Agar terlihat jelas maka di lakukan visualisasi dengan menggunakan rapidminer studio.



Gambar 6. Visualisasi menggunakan RapidMiner Studio

Setelah melakukan monitoring melalui wireshark packet data di simpan kemudian di import ke rapidminer studio dalam format .csv setelah mengimport paket data tersebut dapat di lihat bahwa destination banyak menggunakan protokol ARP sedangkan SNMP sedikit hampir mencapai 50 destination.

## C. Kesimpulan

1. 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.
2. Pada paket data SNMP get next request paket tersebut hanya menunggu request sedangkan pada paket get response paket tersebut sudah mendapatkan nilai dari yang merequest
3. Destination lebih banyak menggunakan protokol ARP di bandingkan menggunkan protokol SNMP

## D. Daftar Pustaka

Rulia,Silvia.2013. Network Monitoring SNMP (Simple Network Management Protocol).(online)http://www.academia.edu/35612238/Network_Monitoring_SNMP_Simple_Network_Management_Protocol_. Diakses pada tanggal 20 Oktober 2018