MANAJEMEN JARINGAN

NAMA : Arman Yuriana

NIM : 09011181419029

SISTEM KOMPUTER

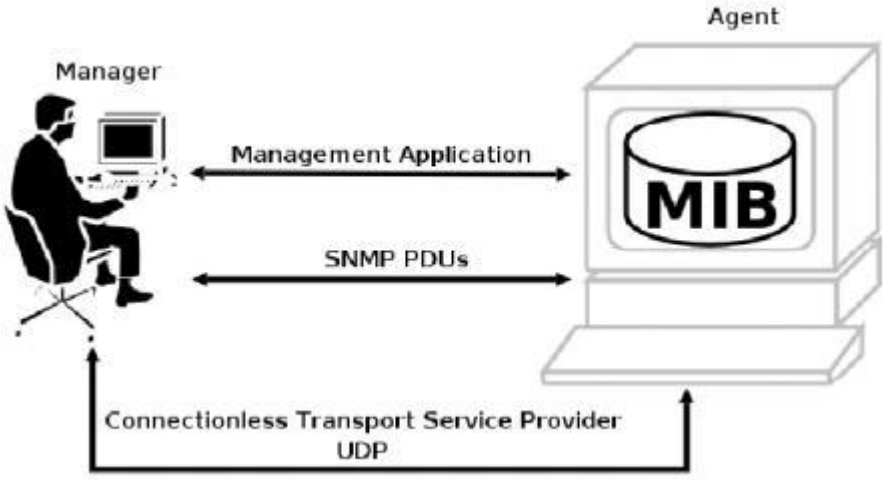
FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

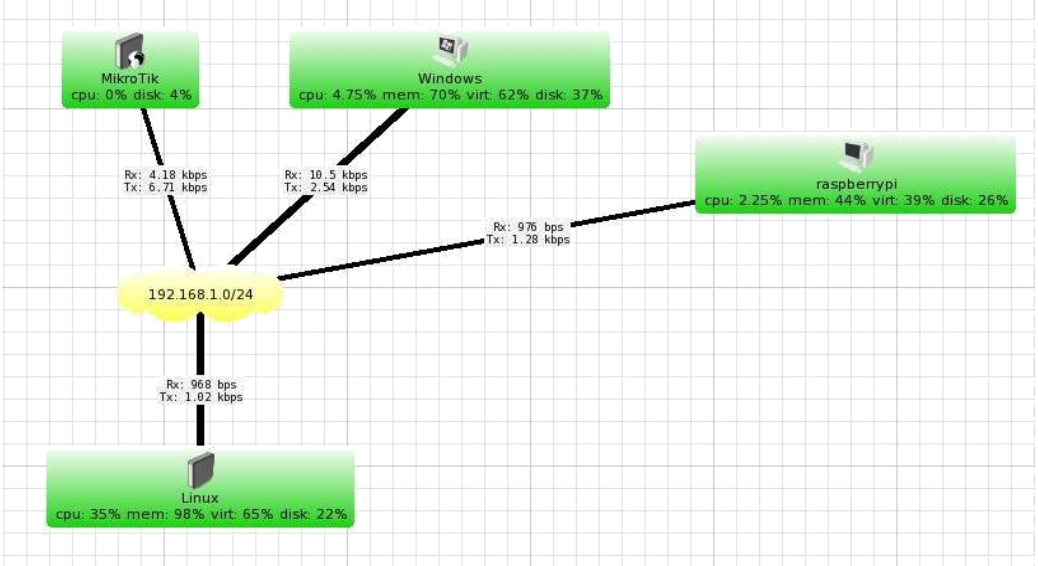
ANALISA PROTOCOL SNMP DENGAN MENGGUNAKAN WIRESHARK

Pada kesempatan kali ini saya akan mencoba menganalisa aliran data pada protocol SNMP, sebelum menganalisa ada baiknya kita mengerti apa itu SNMP dan konsep dasarnya. SNMP (Simple Network Management Protocol) adalah sebuah protocol yang dirancang untuk memberikan kemampuan kepada pengguna untuk mengatur dan memantau jaringan komputernya secara sistematis secara jarak jauh atau dalam satu pusat kontrol saja, dengan menggunakan protocol ini kita bias mendapatkan informasi tentang status dan keadaan suatu jaringan, protocol ini menggunakan transport UDP pada port 616, pengolahan ini dijalankan dengan mengumpulkan data dan melakukan penetapan terhadap variabel-variabel dalam elemen jaringan yang dikelola.



Gambar 1. Struktur SNMP

Selanjutnya kita akan menganalisa aliran data yang terjadi pada topologi yang telah dibuat menggunakan wireshark, adapun topologi yang digunakan adalah STAR.



Gambar 2. Topologi

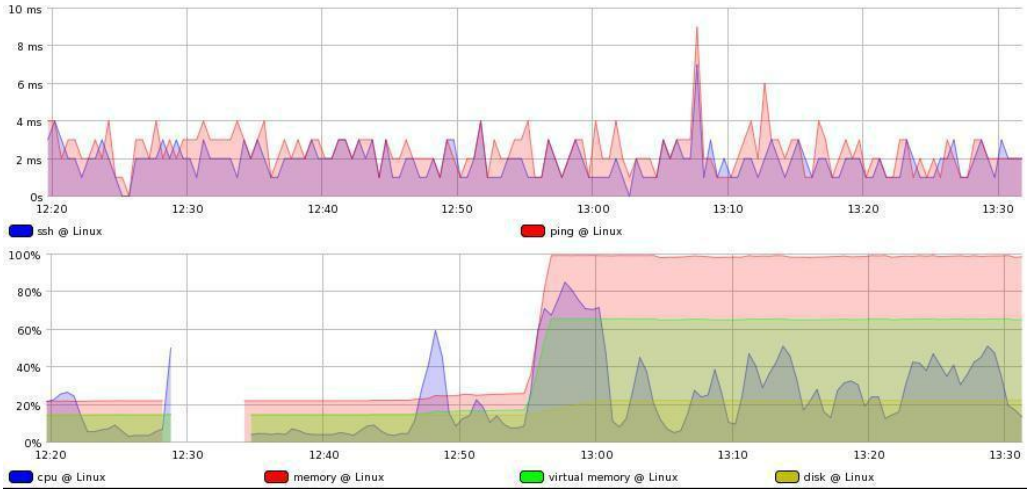
Pada topologi diatas terdapat 4 device yang terhubung, yang mana windows di sini memiliki 3 peranan, pertama sebagai SNMP Agent yang sekaligus bertindak dalam monitoring trafik, kedua sebagai mikrotik (karena kekurangan device jadi di virtualkan), yang ketiga sebagai Dude server, disini dalam hal monitoring saya menggunakan aplikasi The Dude, yang mana akan menampilkan trafik yang terjadi tiap menitnya dalam bentuk grafik.

Sebelum melanjutkan ada baiknya kita mengetahui apa itu Manager, MIB, dan Agent, berikut penjelasannya :

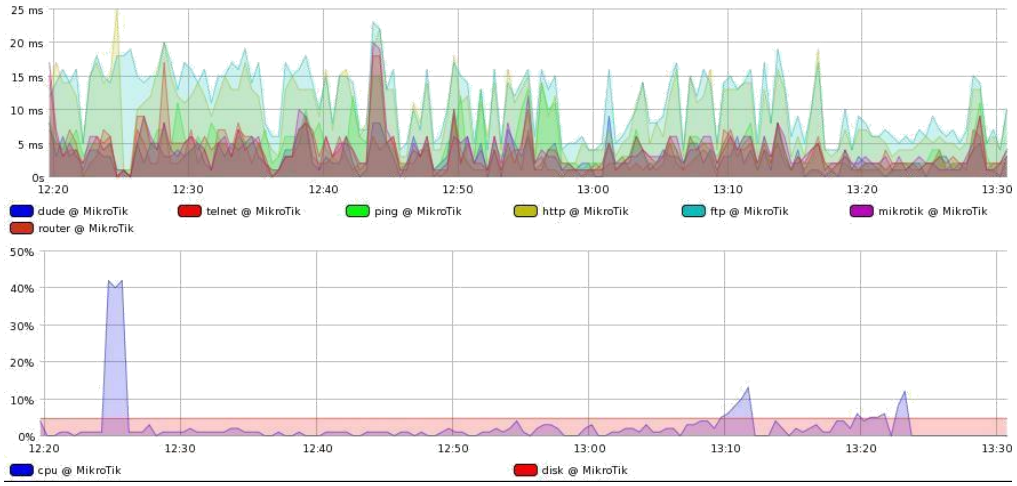
- Manager, yaitu bertugas sebagai manajemen jaringan yang mengumpulkan data informasi dari elemen-elemen jaringan yang ingin dimonitoring dan atau dikontrol. Bentuk dari manager ini berupa perangkat lunak yang didesain sedemikian rupa sekaligus memiliki fungsi antarmuka yang baik bagi penggunanya dalam hal ini network administrator jaringan. Perangkat lunak manager ini bisa di install di server yang sekaligus sebagai database server bagi data informasi SNMP, namun juga bisa di install pada dekstop atau laptop bahkan mobile device dengan syarat server databasenya terpisah.
- MIB (Management Information Base), yaitu database dari data informasi yang dikumpulkan oleh manager dari agen yang tersimpan dalam database server. Struktur data dalam MIB ini bersifat hirarki dan memiliki aturan sedemikian rupa sehingga informasi setiap variabel dapat dikelola atau ditetapkan dengan mudah.[2]

- Agen, yaitu suatu elemen jaringan yang dimonitoring atau dikontrol oleh manager. Pada umumnya perangkat jaringan seperti router dan server difungsikan sebagai agen dalam sistem manajemen jaringan. Hal ini disebabkan lalu lintas trafik data dengan jumlah yang besar melalui atau bermuara pada kedua perangkat jaringan tersebut. Setiap agen mempunyai database yang bersifat lokal dengan variabel-variabel tertentu, artinya secara default informasi disimpan dalam disk lokal dan digunakan oleh sistem operasi internal. Protokol SNMP yang diaktifkan pada suatu agen akan menjadikan data informasi agen seperti aktifitas trafik, dan keadaan proses di sistem internal dan kapasitas sistem dapat dikirim ke manager untuk dikelola lebih lanjut.

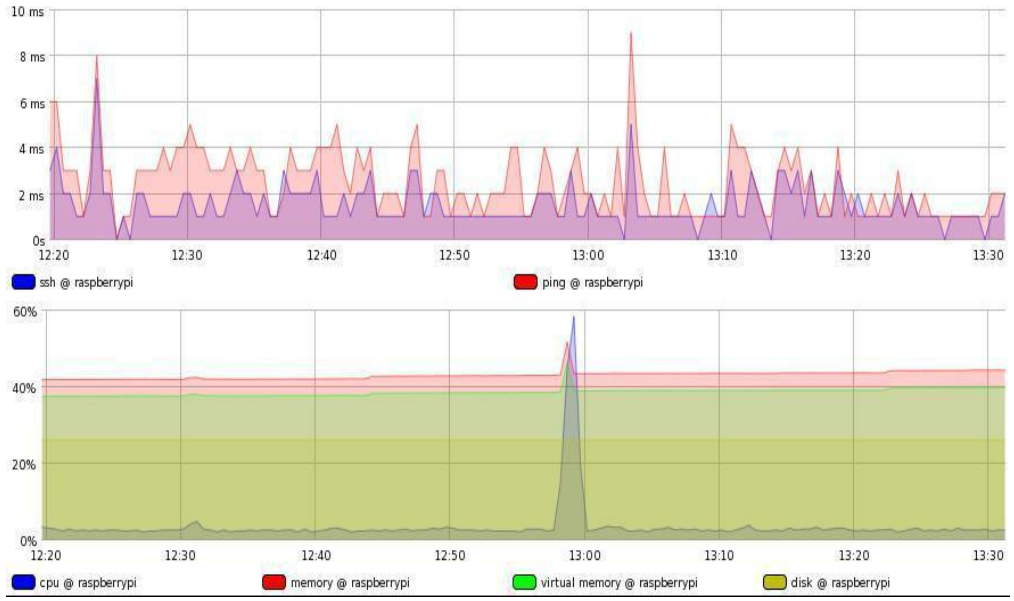
Berikut tampilan grafik yang didapat pada setiap device, melalui SNMP agent :



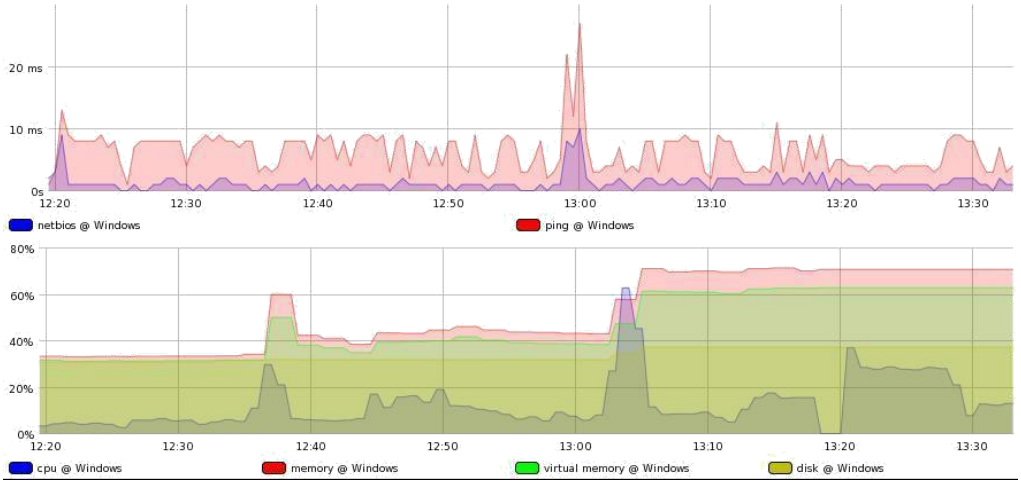
Gambar 3. Linux (192.168.1.3)



Gambar 4. Mikrotik (192.168.1.1)

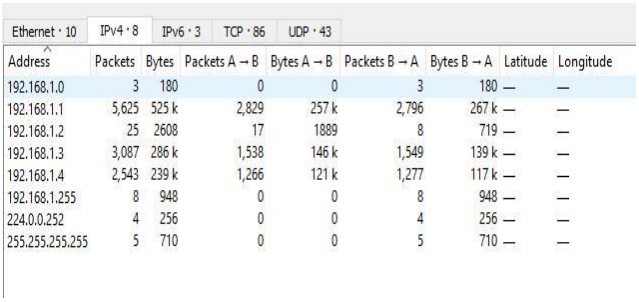


Gambar 5. Raspberry Pi (192.168.1.4)



Gambar 6. Windows 8 (192.168.1.2)

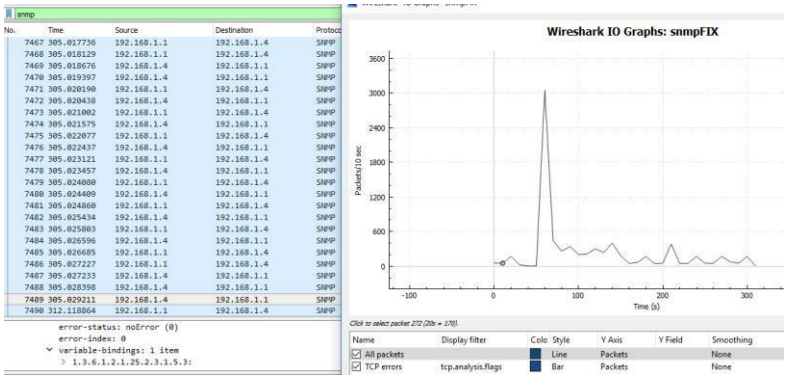
Pada gambar diatas dapat kita lihat traffic tertinggi berada pada rentan waktu antara 12.40-13.00 di karenakan pada saat itu proses rx dan tx sedang terjadi pada masing-masing device yang menyebabkan traffic tinggi, paket yang dikirimkan melalui server lumayan besar 525 kb, jadi trafik tertinggi ketika server mengirimkan paket pertama kali kesemua agent dan mendapat respon dari setiap agent.



Ethernet · 10 | IPv4 · 8 | IPv6 · 3 | TCP · 86 | UDP · 43

Address	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Latitude	Longitude
192.168.1.0	3	180	0	0	3	180	—	—
192.168.1.1	5,625	525 k	2,829	257 k	2,796	267 k	—	—
192.168.1.2	25	2608	17	1889	8	719	—	—
192.168.1.3	3,087	286 k	1,538	146 k	1,549	139 k	—	—
192.168.1.4	2,543	239 k	1,266	121 k	1,277	117 k	—	—
192.168.1.255	8	948	0	0	8	948	—	—
224.0.0.252	4	256	0	0	4	256	—	—
255.255.255.255	5	710	0	0	5	710	—	—

Gambar 7. Endpoint packet



Gambar 8. Trafic dari server ke raspberry dan sebaliknya

Kesimpulannya adalah dengan monitoring dengan menggunakan The Dude pada SNMP agent dapat mengetahui beban trafik yang terjadi pada setiap device, kemuadian trafik tertinggi terjadi pada 12.40-13.00 dengan packet yang dikirimkan server mencapai 525 kb. Dengan demikian SNMP sangat mempermudah dalam memonitoring semua perangkat hanya dengan satu komputer administrator.