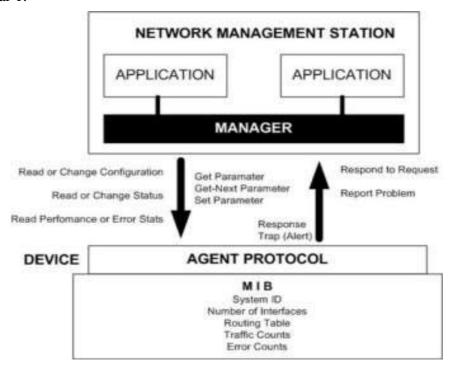
ANALISA PCAP TRAFFIC PROTOCOL SNMP DENGAN MENGGUNAKAN WIRESHARK

Aldo Sapriansyah 09011181520035 (Mahasiswa Sistem Komputer FASILKOM UNSRI)
Tugas Manajemen Jaringan, Dosen Pengajar : Deris Stiawan

Pada kesempatan ini saya akan mencoba menganalisa bagaimana traffic pada protocol SNMP, sebelum menganalisa sebaiknya kita mengerti apa itu SNMP dan konsepnya. 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 [1], dengan menggunakan protocol ini kita bisa mendapatkan informasi tentang status dan keadaan suatu jaringan, protocol ini menggunakan transport UDP pada port 616. Cara kerja SNMP adalah dengan saling berkirim pesan berupa permintaan manager, dan jawaban dari agent tentang informasi dalam jaringan yang dibawah oleh PDU (*Protocol Data Unit*) seperti terlihat pada Gambar 1.



Gambar 1. Skema SNMP

SNMP Agent

Agent berjalan pada setiap node dalam jaringan yang akan dimonitoring. Fungsi dari agent adalah mendapatkan informasi yang diperlukan dari MIB pada setiap node. Agent bereaksi

terhadap perintah dari *manager*, mendapatkan nilai-nilai dari MIB dan menetapkan nilai-nilai dari MIB.

SNMP Manager

Manager berjalan di sebuah host pada jaringan. Memiliki fungsi mengumpulkan informasi (status *up/down device, traffic* jaringan dan informasi lainnya), *monitoring* dan melakukan system remote terhadap agent-agen yang diminta oleh administrator jaringan.

MIB (Management Information Based)

MIB berfungsi sebagai struktur database variabel elemen jaringan yang dikelolah. MIB memiliki struktur yang bersifat hierarki yang diatur sesuai standar, sehingga informasi berupa nilai setiap variabel dengan mudah untuk diketahui maksudnya. MIB mengandung objek (unit dari manajemen informasi) yang dibagi menjadi skalar dan tabel, yang diidentifikasi dari *Object Identifier* (OID). Objek ini bertukar informasi antara *node* yang dimanage yang dapat dimodifikasi melalui NMS.

Disini saya mencoba memantau traffic snmp menggunakan wireshark dan juga memanfaatkan wifi public yang ada di perpustakaan Universitas Sriwijaya. Berikut hasil dari PCAP(paket capture) dari protocol SNMP pada wireshark yang bisa dilihat pada gambar 2.

Apply a display filter _ <crf-{></crf-{>		
ton Protocol Length Info		
.214.205 SMP		
1.214.205 SNP 06 getBulkRequest 1.3.6.1.2.1		
5.214.205 SMP B6 getBulkRequest 1.3.6,1.2.1		
1.214.205 SMP 86 getBulkRequest 1.3.6.1.2.1		
53.110 SMP 366 get-response 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.2.0 1.3.6.1.2.1.1.3.0 1.3.6.1.2.1.1.4.0 1.3.6.1.2	1.1.1.5.0 1.3.6.1.2	
53.110 SMP 366 get-response 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.2.0 1.3.6.1.2.1.1.3.0 1.3.6.1.2.1.1.4.0 1.3.6.1.2	1.1.1.5.0 1.3.6.1.2	
1.214.205 SMP 91 getBulkRequest 1.3.6.1.2.1.1.9.1.2.3		
4.214.205 SMMP 91 getBulkRequest 1,3.6.1.2.1.1.9.1.2.3		
53.110 SWP 366 get-response 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.2.0 1.3.6.1.2.1.1.3.0 1.3.6.1.2.1.1.4.0 1.3.6.1.2	1.1.1.5.0 1.3.6.1.2	
53,110 SWP 366 get-response 1.3,6,1,2,1,1,1,0 1.3,6,1,2,1,1,2,0 1.3,6,1,2,1,1,3,0 1.3,6,1,2,1,1,4,0 1.3,6,1,2	1.1.1.5.0 1.3.6.1.2	
4.214.205 SMVP 91 getBulkRequest 1.3.6.1.2.1.1.9.1.2.3		
1.214.205 SMP 91 getBulkRequest 1.3.6.1,2.1.1.9.1.2.3		
53.110 SWP 499 get-response 1.3.6.1.2.1.1.9.1.2.4 1.3.6.1.2.1.1.9.1.2.5 1.3.6.1.2.1.1.9.1.3.1 1.3.6.1.2.1.1.9	.1,3.2 1.3.6.1.2.1	
4.214.205 SMP 91 getBulkRequest 1,3.6.1.2.1.1.9,1.4.3		
4.214.205 SMP 91 getBulkRequest 1.3.6.1.2.1.1.9.1.4.3		
53.110 SWP 499 get-response 1.3.6.1.2.1.1.9.1.2.4 1.3.6.1.2.1.1.9.1.2.5 1.3.6.1.2.1.1.9.1.3.1 1.3.6.1.2.1.1.9	9.1,3,2 1,3,6,1,2,1,	
53.110 SMP 499 get-response 1,3,6,1,2,1,1,9,1,2,4 1,3,6,1,2,1,1,9,1,2,5 1,3,6,1,2,1,1,9,1,3,1 1,3,6,1,2,1,1,9	3.1.3.2 1.3.6.1.2.1	
4.214.205 SMP 91 getBulkRequest 1,3.6,1.2,1.1.9,1.4.3		
4.214.205 SMP 91 getBulkRequest 1.3.6.1.2.1.1.9.1.4.3		
53.110 SMP 142 get-response 1.3.6.1.2.1.1.9.1.4.4 1.3.6.1.2.1.1.9.1.4.5 1.3.6.1.6.3.15.1.2.1.0 1.3.6.1.6.3.15	5.1.2.1.0	
53.110 SMP 142 get-response 1.3.6.1.2.1.1.9.1.4.4 1.3.6.1.2.1.1.9.1.4.5 1.3.6.1.6.3,15.1.2.1.0 1.3.6.1.6.3.15		
.53.118 SWP 142 get-response 1.3.6.1.2.1.1.9.1.4.4 1.3.6.1.2.1.1.9.1.4.5 1.3.6.1.6.3.15.1.2.1.8 1.3.6.1.6.3.15		

```
) User Datagram Protocol, Src Port: 161, Dst Port: 53234

    Simple Network Management Protocol

     version: v2c (1)
     community: demopublic
  v data: get-response (2)
     v get-response
          request-id: 1326110580
          error-status: noError (0)
          error-index: 0

▼ variable-bindings: 10 items

          > 1.3.6.1.2.1.1,9.1.2.4: 1.3.6.1.6.3.15.2.1.1 (iso.3.6.1.6.3.15.2.1.1)
          ) 1.3.6.1.2.1.1.9.1.2.5: 1.3.6.1.6.3.10.3.1.1 (iso.3.6.1.6.3.10.3.1.1)
          ) 1.3.6.1.2.1,1.9.1.3.1: 546865204d4942206d6f64756c6520666f7220534e4d5076...
          > 1.3.6.1.2.1.1.9.1.3.2; 566965772d62617365642041636365737320436f6e74726f...
          > 1.3.6.1.2.1.1.9.1.3.3; 546865204d494220666f72204d6573736167652050726f63...
          ) 1.3.6.1.2.1.1.9.1.3.4: 546865206d616e6167656d656e7420696e666f726d617469...
          ) 1.3.6.1.2.1.1.9.1.3.5; 54686520534e4d50204d616e6167656d656e742041726368...
           > 1.3.6.1.2.1.1.9.1.4.1; 2
           > 1.3.6.1.2.1.1.9.1.4.2: 2
           ) 1.3.6.1.2.1.1.9.1.4.3: 2
0060 89 25 95 81 86 83 8f 82 81 81 38 17 86 8a 2b 86
8878 81 82 81 81 89 81 82 85 86 89 2b 86 81 86 83 8a ..........
#88# 83 81 81 38 38 86 8a 2b 86 81 82 81 81 89 81 83 ...88..+ ......
0090 01 04 22 54 68 65 20 4d 49 42 20 6d 6f 64 75 6c .. "The M IB modul
Heal 65 20 66 6f 72 20 53 4e 4d 50 76 32 20 65 6e 74 e for SN MPv2 ent
00b0 69 74 69 65 73 30 37 06 0a 2b 06 01 02 01 01 09 ities07. .+.....
```

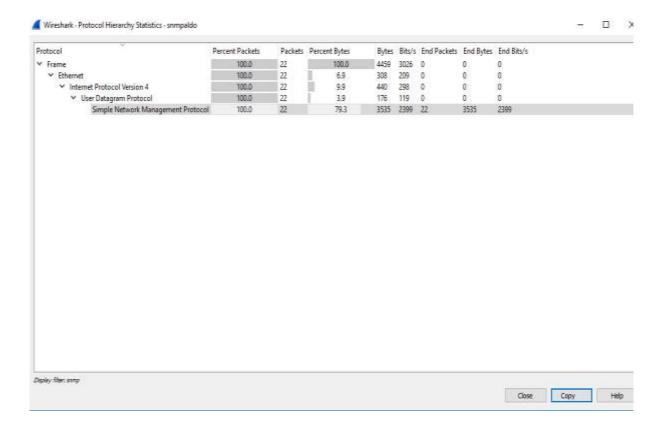
Gambar 2. Data PCAP Protocol SNMP

Wireshark disini digunakan sebagai packet sniffer untuk memantau traffic dalam jaringan sehingga data dapat dianalisa, seperti data PCAP (Packet Capture) yang diperoleh melalui proses sniffing menggunakan Wireshark. Dalam hal ini traffic yang akan dianalisa mengacu pada protokol SNMP. Pada Komunikasi SNMP, interaksi antara manager dan *agent* dapat dibentuk memalui proses *request* oleh *manager* dan *respons* oleh *agent*. Dalam prosesnya, interaksi dilakukan dengan menggunakan *request-id* yang unik, id ini hanya diketahui antara *manager* dan *agent*. Pada gambar diatas dapat di lihat bahwa IP *manager* (IP:10.94.53.110) melakukan *request* untuk memperoleh data informasi dari *agent* (IP:192.94.214.205) dengan beberapa parameter tertentu untuk selajutnya dilakukan proses *monitoring*. Adapun request-id 1326110580 yang hanya diketahui antara *manager* dan *agent*. Dalam kondisi tertentu *agent* dapat mengirimkan informasi tertentu yang disebut dengan *Trap. Trap* dapat dikirim oleh *agent* tanpa terlebih dahulu adanya *request* dari *manager*. Informasi yang diperoleh oleh manager dari agent berupa OID (Object Identifier).



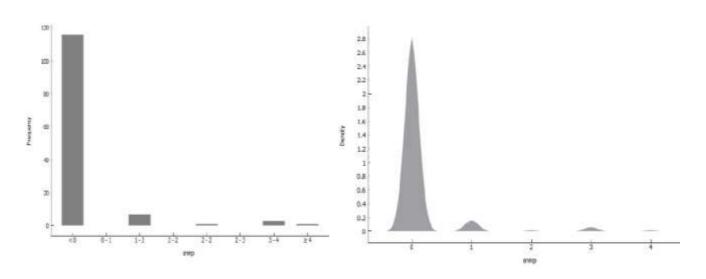
Gambar 3. Grafik SNMP dan All Packet

Pada gambar diatas dapat di lihat grafik perubahan dari paket protocol SNMP dan All Packet yang ada pada jaringan wifi di perpustakaan Universitas Sriwijaya pada jam 20.34 – 20.36 WIB. Pada garis yang berwarna hijau melambangkan paket SNMP yang mana jumlah paket SNMP sebanyak 22 paket karena pada saat mengcapture saya rentan waktunya tidak begitu lama. Untuk garis yang berwarna merah melambangkan paket dari seluruh paket yang melintasi jaringan yang ada pada wifi tersebut.Berikut statistik hirarki dari protokol yang ada dapat dilihat pada gambar 4 di bawah ini.



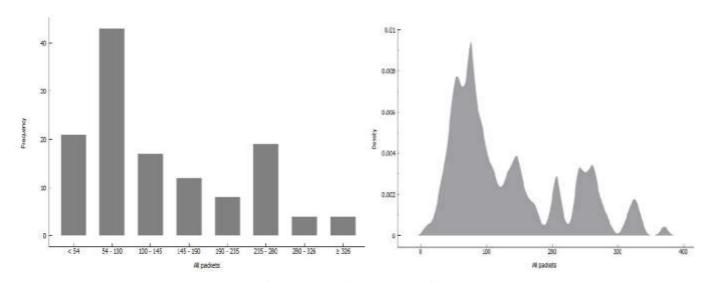
Gambar 4. Tabel statistik protokol

Selanjutnya saya melakukan visualisasi pada aplikasi orange, setelah mendapatkan hasil grafik pada wireshark maka visualisasi dilakukan pada aplikasi orange, berikut hasil dari pemvisualisasi hasil PCAP pada wireshark yang dapat dilihat pada gambar 5 dan gambar 6 dibawah ini.



Gambar 5. SNMP Trafik

Dapat di lihat pada grafik diatas menampilkan hasil dari PCAP pada wireshark yang telah di masukkan datanya di orange gambar diatas merupakan tingkat data protocol SNMP yang telah di dapat dari wifi perpustakaan Universitas Sriwijaya. Dan Gambar dibawah ini merupakan hasil dari capture All data pada wireshark.



Gambar 6. All Data Trafik

Kesimpulan dari hasil pengamatan yang telah dilakukan bahwa dalam protocol SNMP terjadi interaksi antara manager dan agent dengan saling berkirim pesan berupa permintaan manager yang meminta request kepada agent setelah agent menerima permintaan dari manager maka agent akan meresponse permintaan tersebut.

DAFTAR PUSTAKA

- [1] J. Schippers and A. Pras, "SNMP Traffic Analysis: Approaches, Tools, and FirstResult,"pp.323-332,2007.
- [2] Muhammad Zen Samsono Hadi, ST. Msc. "SNMP (Simple Network Management Protocol).

•