

# Tugas

## Manajemen Jaringan



Disusun Oleh :

Yonatan Riyadhi 09011181419009  
Sigit Wijaya Pramono 09011181419012

**JURUSAN SISTEM KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS SRIWIJAYA**  
**2017**

## **Analisa Paket Yang Memiliki Protokol SNMP**

Pada tugas percobaan ini, diberikan perintah untuk melakukan analisa protokol SNMP dimana pada tahap awalnya membangun jaringan sederhana minimal dua buah mikrotik (router), dan minimal empat buah PC. Dimana nantinya salah satu PC mengirimkan sebuah paket data baik berupa teks, gambar, audio maupun video kepada salah satu PC yang memiliki network address yang berbeda dengan PC source kemudian dilakukan capturing paket data menggunakan wireshark atau tools sejenis lainnya.

### **SNMP**

SNMP merupakan sebuah protokol jaringan yang didesain untuk user khususnya administrator jaringan untuk memonitor aktifitas jaringan komputer dan mengontrol sebuah komputer atau server secara sistematis dari jarak jauh. SNMP bekerja dengan mengumpulkan data informasi dari elemen-elemen jaringan dengan parameter dan variabel tertentu dan menyimpannya dalam sebuah database.

SNMP terdiri atas tiga elemen sebagai berikut:

- **Manager**

Manager bertugas sebagai manajemen jaringan yang mengumpulkan data informasi dari elemen-elemen jaringan yang ingin di monitoring dan atau di kontrol. Bentuk dari manager ini berupa perangkat lunak yang di desain sedemikian rupa sekaligus memiliki fungsi antarmuka yang baik bagi penggunanya.

- **MIB (Management Information Base)**

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.

- **Agen**

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 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.

SNMP menggunakan protokol transport UDP (User Datagram Protocol) di port 161 untuk mengirimkan permintaan dari manager ke agen dan menerima jawaban dari agen ke manager. Agen yang memiliki MIB akan memberikan data informasi yang diperlukan tapi tidak semua oleh manager menggunakan transport UDP yang berorientasi pada kecepatan pengiriman. Selanjutnya, dibawah ini terdapat beberapa capture yang menunjukkan command dan hasil nya antara lain sebagai berikut :

```
[admin@MikroTik] > snmp set enable=yes
[admin@MikroTik] > snmp community add name=manjar read-access=yes write-access=yes
[admin@MikroTik] > snmp community print
Flags: * - default
#  NAME      ADDRESSES          SECURITY  REA
0 * public  0.0.0.0/0         none     yes
1  manjar    0.0.0.0/0         none     yes
[admin@MikroTik] >
```

Gambar. 1 : Command untuk mengaktifkan SNMP pada Mikrotik

Gambar berikutnya merupakan capture hasil dari wireshark pada saat melakukan transfer data:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100	203.104.174.13	TCP	54	54406 → 443 [ACK] Seq=1 Ack=1 Win=16639 Len=0
2	0.060211	192.168.1.103	192.168.1.255	NBNS	92	Name query NB ISATAP<00>
3	0.647600	203.104.174.13	192.168.1.100	TLSv1.2	313	Application Data
4	0.658662	192.168.1.100	203.104.174.13	TLSv1.2	110	Application Data
5	0.708846	203.104.174.13	192.168.1.100	TCP	54	443 → 54406 [ACK] Seq=260 Ack=57 Win=72 Len=0
6	0.709106	192.168.1.100	203.104.174.13	TLSv1.2	118	Application Data
7	0.768511	203.104.174.13	192.168.1.100	TCP	54	443 → 54406 [ACK] Seq=260 Ack=121 Win=72 Len=0
8	0.825005	fe80::55b2:c586:b76... ff02::1:3		LLMNR	86	Standard query 0xc1d6 A isatap
9	0.825288	192.168.1.103	224.0.0.252	LLMNR	66	Standard query 0xc1d6 A isatap
10	0.932946	192.168.1.103	224.0.0.252	LLMNR	66	Standard query 0xc1d6 A isatap
11	0.933844	fe80::55b2:c586:b76... ff02::1:3		LLMNR	86	Standard query 0xc1d6 A isatap
12	1.136850	192.168.1.103	192.168.1.255	NBNS	92	Name query NB ISATAP<00>
13	1.900918	192.168.1.103	192.168.1.255	NBNS	92	Name query NB ISATAP<00>
14	2.665092	192.168.1.103	192.168.1.255	NBNS	92	Name query NB ISATAP<00>
15	4.415549	HonHaiPr_51:94:0d	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.102
16	4.703684	192.168.1.102	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
17	6.865317	203.104.174.13	192.168.1.100	TLSv1.2	130	Application Data
18	6.866731	192.168.1.100	203.104.174.13	TLSv1.2	106	Application Data
19	6.918731	203.104.174.13	192.168.1.100	TCP	54	443 → 54406 [ACK] Seq=336 Ack=173 Win=72 Len=0
20	6.918824	192.168.1.100	203.104.174.13	TLSv1.2	180	Application Data, Application Data
21	6.988300	203.104.174.13	192.168.1.100	TCP	54	443 → 54406 [ACK] Seq=336 Ack=299 Win=72 Len=0
22	7.147242	203.104.174.13	192.168.1.100	TLSv1.2	392	Application Data
23	7.347967	192.168.1.100	203.104.174.13	TCP	54	54406 → 443 [ACK] Seq=299 Ack=674 Win=16471 Len=0
24	7.702656	192.168.1.102	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
25	8.011021	203.104.174.13	192.168.1.100	TLSv1.2	583	Application Data
26	8.016878	192.168.1.100	203.104.174.13	TLSv1.2	110	Application Data
27	8.078658	203.104.174.13	192.168.1.100	TCP	54	443 → 54406 [ACK] Seq=1203 Ack=355 Win=72 Len=0
28	8.078735	192.168.1.100	203.104.174.13	TLSv1.2	118	Application Data

Gambar. 2 : Hasil capture pertama

Gambar diatas menunjukkan hasil capture mentah / masih pertama kali saat melakukan capture traffic data. Dan pada gambar selanjutnya merupakan hasil capture pengiriman data, dan hasil capture protokol SNMP :

2	0.060211	192.168.1.103	192.168.1.255	NBNS	92	Name query NB ISATAP<00>
9	0.825288	192.168.1.103	224.0.0.252	LLMNR	66	Standard query 0xc1d6 A isatap
10	0.932946	192.168.1.103	224.0.0.252	LLMNR	66	Standard query 0xc1d6 A isatap
12	1.136850	192.168.1.103	192.168.1.255	NBNS	92	Name query NB ISATAP<00>
13	1.900918	192.168.1.103	192.168.1.255	NBNS	92	Name query NB ISATAP<00>
14	2.665092	192.168.1.103	192.168.1.255	NBNS	92	Name query NB ISATAP<00>

Gambar. 3 : Capture hasil pengiriman data

10	0.820500	172.31.19.73	172.31.19.54	SNMP	87	get-response	1.3.6.1.2.1.1.43.14.1.1.6.1.5
11	0.829169	172.31.19.54	172.31.19.73	SNMP	92	get-request	1.3.6.1.4.1.253.8.64.4.2.1.5.10.14150980
12	0.851899	172.31.19.73	172.31.19.54	SNMP	95	get-response	1.3.6.1.4.1.253.8.64.4.2.1.5.10.14150980
13	0.852200	172.31.19.54	172.31.19.73	SNMP	82	get-request	1.3.6.1.2.1.1.2.0
14	0.855941	172.31.19.73	172.31.19.54	SNMP	100	get-response	1.3.6.1.2.1.1.2.0
15	0.838665	172.31.19.54	172.31.19.73	SNMP	96	get-request	1.3.6.1.2.1.1.5.0.1.3.6.1.2.1.1.6.0
16	0.844576	172.31.19.73	172.31.19.54	SNMP	115	get-response	1.3.6.1.2.1.1.5.0.1.3.6.1.2.1.1.6.0
17	0.847268	172.31.19.54	172.31.19.73	SNMP	84	get-request	1.3.6.1.2.1.2.2.1.6.1
18	0.848322	172.31.19.73	172.31.19.54	SNMP	90	get-response	1.3.6.1.2.1.2.2.1.6.1
19	0.851193	172.31.19.54	172.31.19.73	SNMP	140	get-request	1.3.6.1.4.1.253.8.64.4.2.1.7.10.14130104.1.3.6.1.4.1.253.8.64.4.2.1.7.10.14130102.1.3.6.1.4.1.2...
20	0.857698	172.31.19.73	172.31.19.54	SNMP	165	get-response	1.3.6.1.4.1.253.8.64.4.2.1.7.10.14130104.1.3.6.1.4.1.253.8.64.4.2.1.7.10.14130102.1.3.6.1.4.1.2...

Gambar. 4 : Hasil capture protokol SNMP

Berikutnya terdapat gambar gambar hasil capture SNMP request dan SNMP response :

```

▶ Frame 3: 96 bytes on wire (768 bits), 96 bytes captured (768 bits)
▶ Ethernet II, Src: Dell_4a:33:d2 (00:12:3f:4a:33:d2), Dst: FujiXero_15:e6:bc (08:00:37:15:e6:bc)
▶ Internet Protocol Version 4, Src: 172.31.19.54, Dst: 172.31.19.73
▶ User Datagram Protocol, Src Port: 15917, Dst Port: 161
▲ Simple Network Management Protocol
  version: version-1 (0)
  community: public
  ▲ data: get-request (0)
    ▲ get-request
      request-id: 39
      error-status: noError (0)
      error-index: 0
      ▲ variable-bindings: 2 items
        ▲ 1.3.6.1.2.1.1.5.0: Value (Null)
          Object Name: 1.3.6.1.2.1.1.5.0 (iso.3.6.1.2.1.1.5.0)
          Value (Null)
        ▲ 1.3.6.1.2.1.1.6.0: Value (Null)
          Object Name: 1.3.6.1.2.1.1.6.0 (iso.3.6.1.2.1.1.6.0)
          Value (Null)

```

0000	08 00 37 15 e6 bc 00 12 3f 4a 33 d2 08 00 45 00	..7.... ?J3...E.
0010	00 52 aa 1a 00 00 80 11 11 c3 ac 1f 13 36 ac 1f	.R.....6...
0020	13 49 3e 2d 00 a1 00 3e 8d 4d 30 34 02 01 00 04	.I>...> .M04....
0030	06 70 75 62 6c 69 63 a0 27 02 01 27 02 01 00 02	.public. ....
0040	01 00 30 1c 30 0c 06 08 2b 06 01 02 01 01 05 00	..0.0...+.....
0050	05 00 30 0c 06 08 2b 06 01 02 01 01 06 00 05 00	..0...+.....

Gambar. 5 : Gambar hasil capture SNMP request

```

▶ Ethernet II, Src: FujiXero_15:e6:bc (08:00:37:15:e6:bc), Dst: Dell_4a:33:d2 (00:12:3f:4a:33:d2)
▶ Internet Protocol Version 4, Src: 172.31.19.73, Dst: 172.31.19.54
▶ User Datagram Protocol, Src Port: 161, Dst Port: 15917
▲ Simple Network Management Protocol
  version: version-1 (0)
  community: public
  ▲ data: get-response (2)
    ▲ get-response
      request-id: 39
      error-status: noError (0)
      error-index: 0
      ▲ variable-bindings: 2 items
        ▲ 1.3.6.1.2.1.1.5.0: 4236333030
          Object Name: 1.3.6.1.2.1.1.5.0 (iso.3.6.1.2.1.1.5.0)
          ▶ Value (Octetstring): 4236333030
        ▲ 1.3.6.1.2.1.1.6.0: 4368616e64726127732063756265
          Object Name: 1.3.6.1.2.1.1.6.0 (iso.3.6.1.2.1.1.6.0)
          Value (Octetstring): 4368616e64726127732063756265

```

0000	00 12 3f 4a 33 d2 08 00 37 15 e6 bc 08 00 45 00	..?J3... 7....E.
0010	00 65 1a 1c 00 00 40 11 e1 ae ac 1f 13 49 ac 1f	.e...@. ....l..
0020	13 36 00 a1 3e 2d 00 51 9e 9b 30 47 02 01 00 04	.6...->Q ..0G....
0030	06 70 75 62 6c 69 63 a2 3a 02 01 27 02 01 00 02	.public. ....
0040	01 00 30 1f 30 11 06 08 2b 06 01 02 01 01 05 00	..0/0...+.....
0050	04 05 42 36 33 30 30 30 1a 06 08 2b 06 01 02 01	..B03000 ...+...
0060	01 06 00 04 0e 43 68 61 6e 64 72 61 27 73 20 63	....Cha ndra's c
0070	75 62 65	ube

Gambar. 6 : Gambar hasil capture SNMP response

- SNMP Manager Mengirimkan GetRequest-PDU: Manajer SNMP mengirimkan PDU ke perangkat yang sedang disurvei.

- Manajer SNMP Menciptakan GetRequest-PDU: Berdasarkan informasi yang dibutuhkan oleh aplikasi dan pengguna, perangkat lunak SNMP di stasiun manajemen jaringan menciptakan pesan GetRequest-PDU. Ini berisi nama objek MIB yang nilainya ingin diambil oleh aplikasi.
- Agen SNMP Menciptakan Respon-PDU: Agen menciptakan Respon-PDU untuk dikirim kembali ke Manajer SNMP. Pesan ini berisi nilai objek MIB yang diminta dan / atau kode kesalahan untuk menunjukkan adanya masalah dengan permintaan, seperti nama objek yang tidak valid.
- Agen SNMP Menerima dan Proses GetRequest-PDU: Agen SNMP menerima dan memproses permintaan tersebut. Ini terlihat pada daftar nama objek MIB yang terdapat dalam pesan dan periksa untuk melihat apakah dokumen itu benar (yang sebenarnya digunakan oleh agen). Ini mendongak nilai setiap variabel yang telah ditentukan dengan benar.
- Manajer SNMP Proses Respon-PDU: Manajer memproses informasi dalam Respon-PDU yang diterima dari agen.
- Agen SNMP Mengirim Tanggapan-PDU: Agen mengirim tanggapan kembali ke Manajer SNMP.