TUGAS MANAJEMEN JARINGAN

ANALISIS TRANSFER DATA, VIDEO, SUARA DI PROTOKOL SNMP VIA WIRESHARK

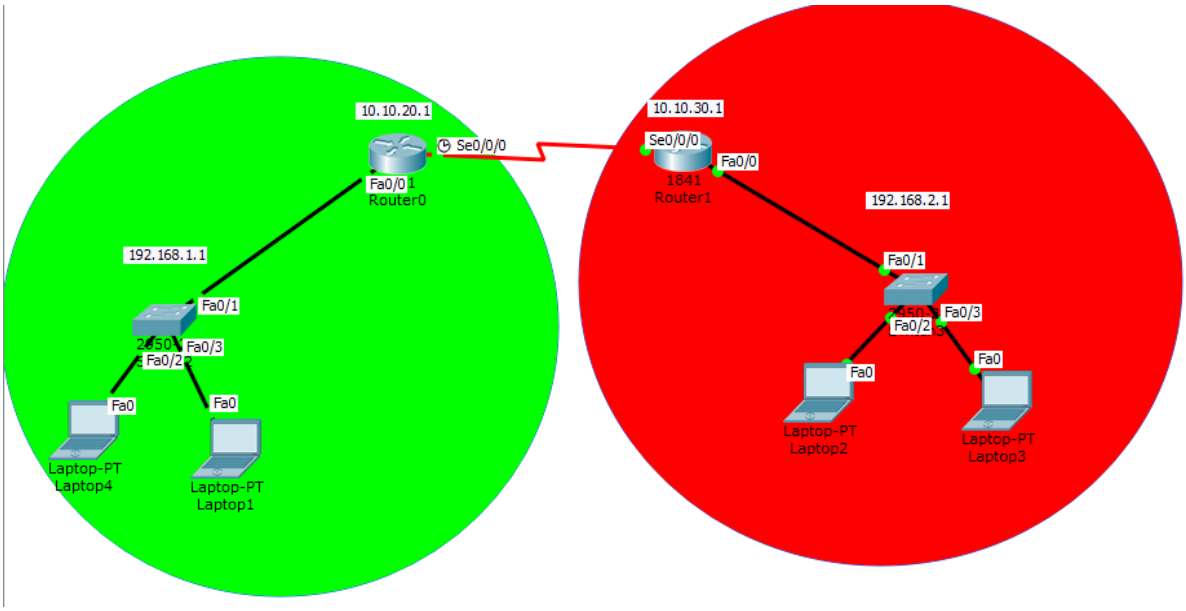
ADE RAHMAD 09011281419059

AHMAD RIDWAN 09011281419042

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2017

ANALISIS TRANSFER DATA, VIDEO, SUARA DI PROTOKOL SNMP VIA WIRESHARK



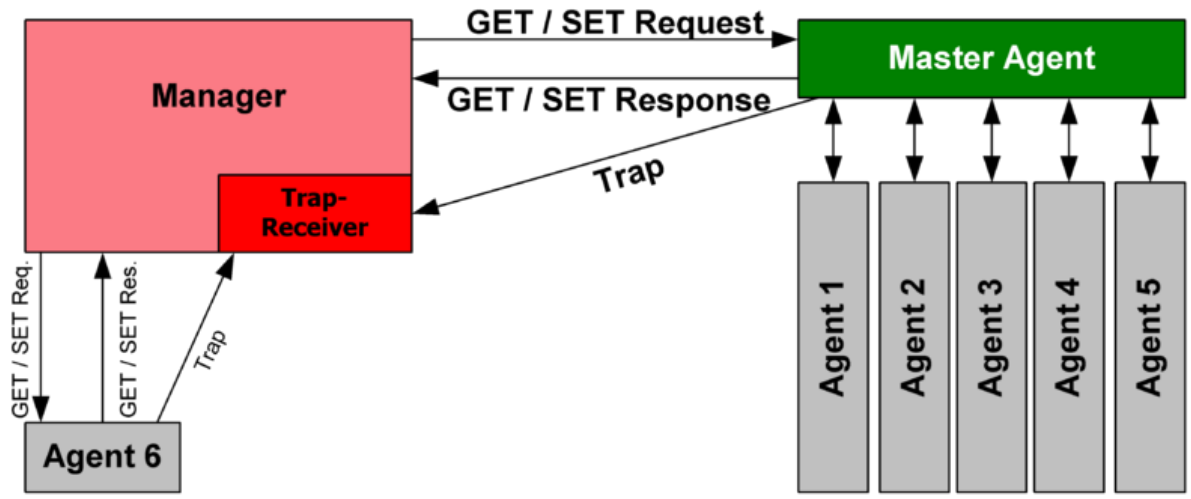
Topologi virtual yang kami gunakan

Kita harus tahu terlebih dahulu apa itu SNMP ?

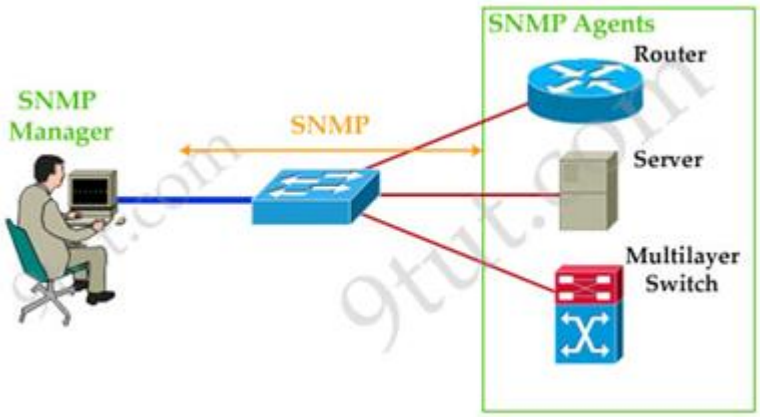
SNMP merupakan sebuah protokol jaringan yang didesain untuk user khususnya administrator jaringan untuk memonitor aktifitas jaringan komputer dan mengontrol sebuah komputer atau server secara sistematis dari jarak jauh. SNMP bekerja dengan mengumpulkan data informasi dari elemen-elemen jaringan dengan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

Percobaan :

Pertama yang dilakukan adalah membuat topologi yang digunakan untuk analisis transfer data, video, suara di protokol snmp via wireshark. Dalam percobaan ini menggunakan 2 mikrotik routerboard dan 4 PC yang digunakan. Dimana nantinya salah satu PC mengirimkan sebuah paket data baik berupa teks, gambar, audio maupun video kepada salah satu PC yang memiliki network adddress yang berbeda dengan PC source kemudian dilakukan capturing paket data menggunakan wireshark atau tools sejenis lainnya.



Dari gambar di atas, Manager akan menghubungi Master Agent port destination UDP 161. Agent akan menajwab dan menhubungi Manager dengan port destination port 162. Jika menggunakan SSL maka port yang digunakan adalah 10161 dan 1062.



SNMP terdiri atas tiga elemen sebagai berikut:

1. 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.

2. 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.

3. 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.

To enable SNMP in RouterOS:

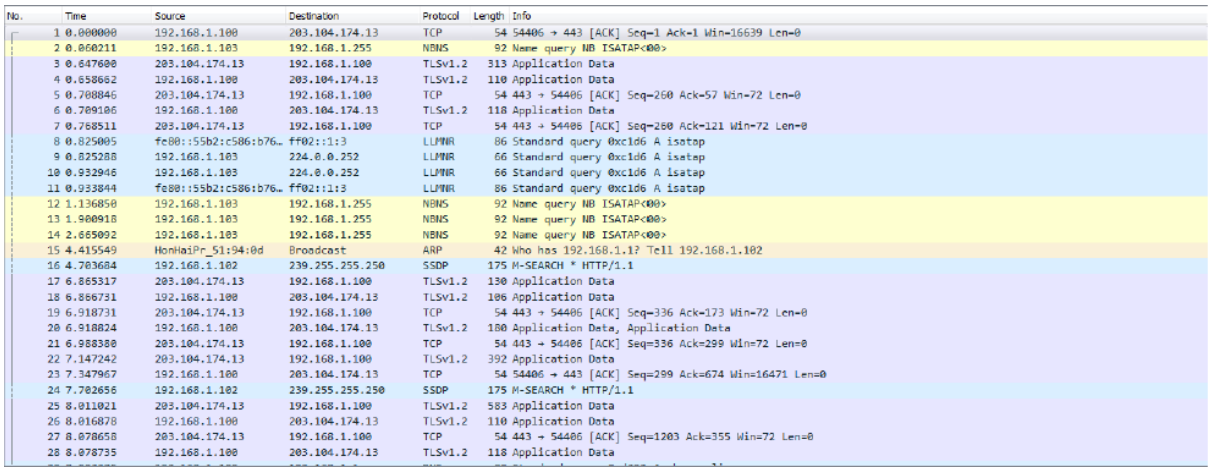
```
[admin@MikroTik] /snmp> print
      enabled: no
      contact:
      location:
      engine-id:
      trap-community: (unknown)
      trap-version: 1
[admin@MikroTik] /snmp>  set enabled yes
```

MIBs used in RouterOS v6.x:

- MIKROTIK-MIB
- MIB-2
- HOST-RESOURCES-MIB
- IF-MIB
- IP-MIB
- IP-FORWARD-MIB
- IPV6-MIB
- BRIDGE-MIB
- DHCP-SERVER-MIB
- CISCO-AAA-SESSION-MIB
- ENTITY-MIB
- UPS-MIB
- SQUID-MIB

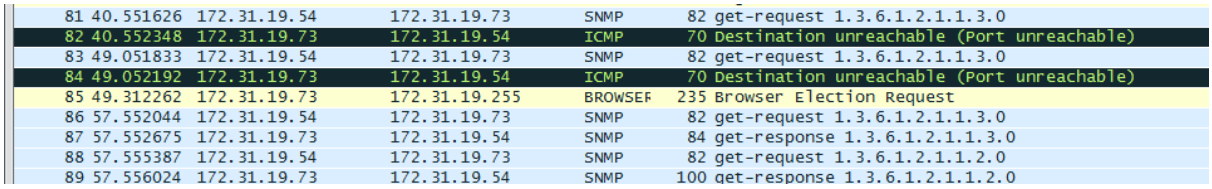
SNMP WRITE :

/snmp community set <number> write-access=yes



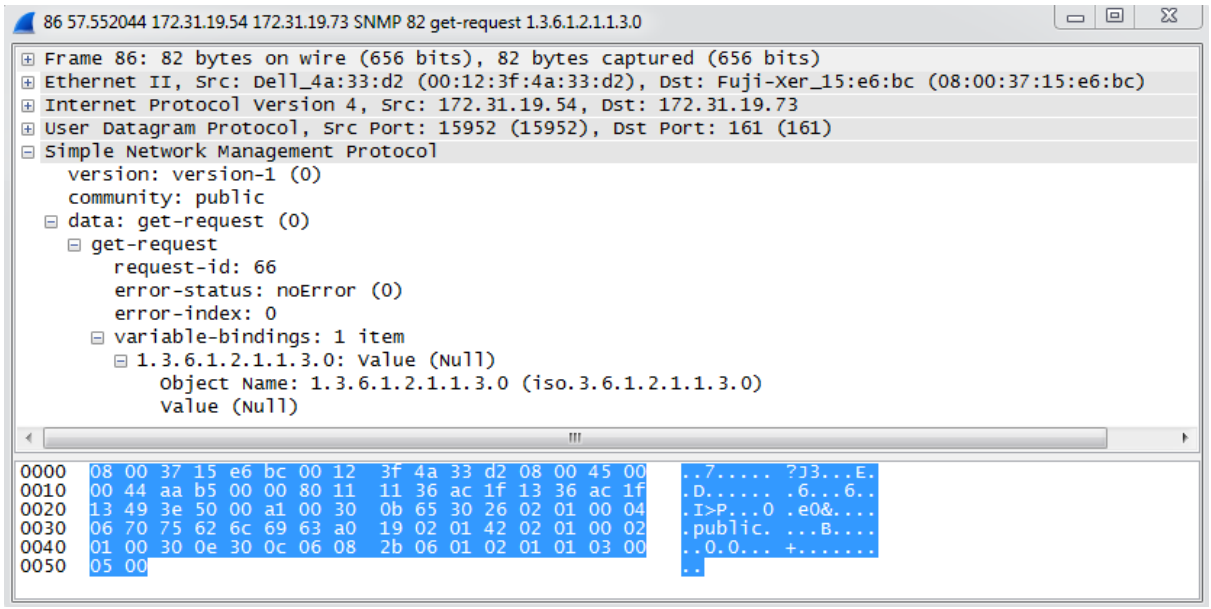
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100	203.104.174.13	TCP	54	54406 → 443 [ACK] Seq=1 Ack=1 Win=16639 Len=0
2	0.000211	192.168.1.103	192.168.1.255	NBNS	92	Name query NB ISATAP<00>
3	0.647600	203.104.174.13	192.168.1.100	TLSv1.2	313	Application Data
4	0.658662	192.168.1.100	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	6.988380	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

Hasil Capture Transfer Data

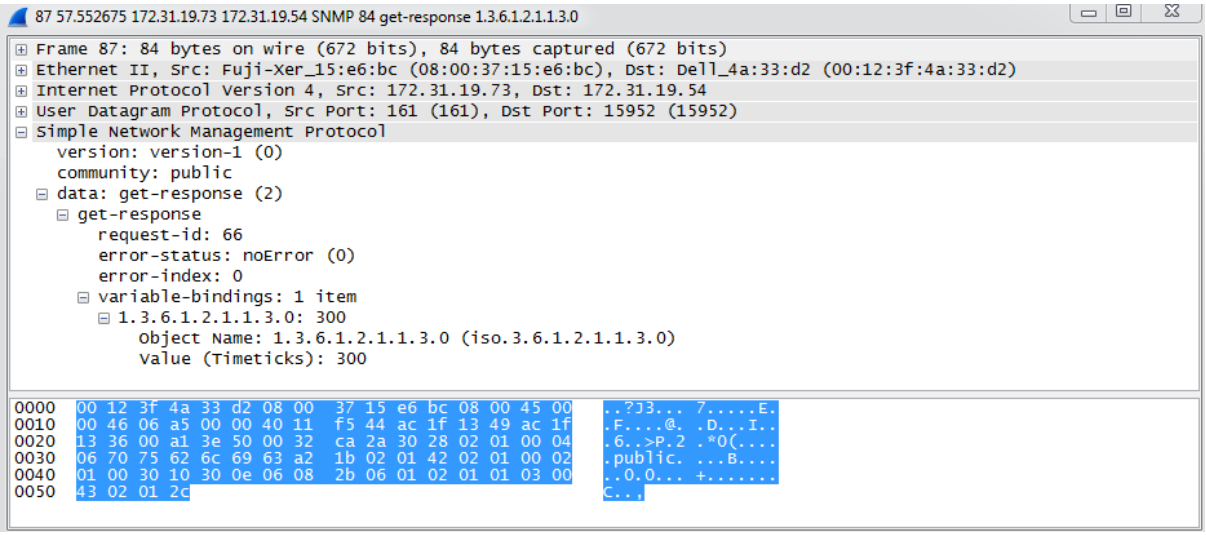


81	40.551626	172.31.19.54	172.31.19.73	SNMP	82	get-request 1.3.6.1.2.1.1.3.0
82	40.552348	172.31.19.73	172.31.19.54	ICMP	70	Destination unreachable (Port unreachable)
83	49.051833	172.31.19.54	172.31.19.73	SNMP	82	get-request 1.3.6.1.2.1.1.3.0
84	49.052192	172.31.19.73	172.31.19.54	ICMP	70	Destination unreachable (Port unreachable)
85	49.312262	172.31.19.73	172.31.19.255	BROWSER	235	Browser Election Request
86	57.552044	172.31.19.54	172.31.19.73	SNMP	82	get-request 1.3.6.1.2.1.1.3.0
87	57.552675	172.31.19.73	172.31.19.54	SNMP	84	get-response 1.3.6.1.2.1.1.3.0
88	57.555387	172.31.19.54	172.31.19.73	SNMP	82	get-request 1.3.6.1.2.1.1.2.0
89	57.556024	172.31.19.73	172.31.19.54	SNMP	100	get-response 1.3.6.1.2.1.1.2.0

Hasil Capture Protokol SNMP



SNMP get request



SNMP get-Response

Dari data diatas didapat bahwa terdapat get request dan get-response yang masing-masing dari get response dan get request terdapat request id , error status dan lain-lain. Tempat yang jelas untuk mulai melihat kami rinci SNMP protokol operasi adalah dengan jenis pertukaran informasi yang paling sederhana. Ini akan menjadi sebuah operasi jajak pendapat sederhana untuk membaca manajemen satu atau lebih variabel informasi, digunakan oleh SNMP satu entitas (biasanya SNMP manajer) untuk meminta atau membaca informasi dari entitas lain (biasanya agen SNMP pada perangkat dikelola). SNMP mengimplementasikan ini sebagai sederhana dua-pesan permintaan/tanggapan protokol pertukaran, serupa proses permintaan Balasan ditemukan di begitu banyak protokol TCP/IP. Proses permintaan informasi ini biasanya dimulai dengan pengguna aplikasi ingin memeriksa status perangkat atau melihat informasi tentang hal itu. Seperti yang kita lihat, Semua informasi ini disimpan pada perangkat dalam bentuk MIB objek. Komunikasi, oleh karena itu, mengambil bentuk permintaan tertentu MIB objek dan Balasan dari perangkat yang mengandung nilai-nilai objek tersebut. Dalam bentuk yang disederhanakan, langkah-langkah dalam proses adalah sebagai berikut (dan seperti yang ditunjukkan dalam gambar 274):

SNMP manajer menciptakan GetRequest-PDU: berdasarkan informasi yang diperlukan oleh aplikasi dan pengguna, SNMP perangkat lunak pada jaringan manajemen Stasiun menciptakan pesan GetRequest-PDU. Ini berisi nama MIB objek nilai-nilai yang ingin aplikasi untuk mengambil. SNMP manajer mengirim GetRequest-PDU: The SNMP manajer mengirimkan PDU ke perangkat yang sedang penudung. SNMP agen menerima dan proses GetRequest-PDU: The SNMP agen menerima dan memproses permintaan.

Kelihatannya daftar MIB nama objek terkandung dalam pesan dan memeriksa untuk melihat apakah mereka berlaku (yang benar-benar menerapkan agen). Kelihatannya nilai dari setiap variabel yang benar ditentukan. SNMP agen menciptakan respon-PDU: Agen menciptakan respon-PDU untuk mengirim kembali ke SNMP Manager. Pesan ini berisi nilai-nilai objek MIB diminta dan/atau kode kesalahan untuk menunjukkan masalah dengan permintaan, seperti nama objek tidak valid. SNMP agen mengirim respon-PDU: Agen mengirimkan tanggapan kembali ke SNMP Manager. SNMP manajer proses respon-PDU: Manajer memproses informasi dalam respon-PDU diterima dari agen.