**ANALISIS TRAFFIC SNMP PADA WIRESHARK MENGGUNAKAN**

**NETWORK WIFI PUBLIC**

***Siti Pebsya Roisatun Sholihah 09011281520102 (Mahasiswa Sistem Komputer FASILKOM UNSRI)***

***Tugas Manajemen Jaringan, Dosen Pengajar : Deris Stiawan***

1. **Pendahuluan**

Saat ini sistem informasi merupakan bagian yang sangat penting untuk setiap organisasi/korporasi. Sistem Informasi adalah kombinasi dari [teknologi informasi](https://id.wikipedia.org/wiki/Teknologi_informasi) dan aktivitas orang yang menggunakan teknologi itu untuk mendukung operasi dan manajemen. Dalam pengertian tersebut, istilah ini merujuk tidak hanya pada penggunaan organisasi [teknologi informasi dan komunikasi (](https://id.wikipedia.org/wiki/Teknologi_informasi_dan_komunikasi)TIK), tetapi juga untuk cara di mana orang berinteraksi dengan teknologi ini dalam mendukung proses bisnis.

Perkembangan teknologi informasi, khususnya jaringan memungkinkan terjadinya pertukaran informasi yang cepat dan semakin kompleks. Pengaturan jaringan yang baik tentu akan memaksimalkan pemanfaatan informasi tersebut. Oleh sebab itu jaringan harus diatur dan dipantau, sehingga kelancaran pengiriman informasi dapat berjalan baik. Semakin besar dan luas sistem jaringan, maka akan semakin sulit untuk mengatur dan mengawasinya.

Banyaknya *device* yang digunakan dalam infrastruktur jaringan, maka diperlukanlah suatu manajemen jaringan yang baik dan sistem monitoring yang mampu memantau kinerja dari jaringan tersebut, kemudian sistem monitoring yang didesain untuk memantau status infrastuktur LAN/WAN, memastikan *device* tersebut dalam kondisi normal dan aktif, dapat melihat statistik dalam bentuk grafik, pengecekan kondisi sinyal, dapat memprediksi masalah yang akan muncul atau dapat memantau paket data yang lewat di trafik jaringan.

Salah satu protokol yang populer digunakan untuk manajemen jaringan adalah Simple Network Management Protocol (SNMP). SNMP merupakan sebuah protokol yang digunakan sebagai standar untuk melakukan pengaturan perangkat-perangkat jaringan. SNMP dapat digunakan untuk mengkonfigurasi device yang jauh, menyediakan sekumpulan operasi yang dapat melakukan pengelolaan beberapa perangkat jaringan secara jarak jauh sehingga monitoring dapat dilakukan tidak hanya pada *Local Area Network* (LAN) tapi juga dapat dioperasikan pada skala jaringan yang lebih luas seperti *Wide Area Network* (WAN), mendeteksi kesalahan jaringan atau akses.

1. **Dasar Teori**

Simple Network Management Protocol (SNMP) telah menjadi standar defacto untuk manajemen jaringan. Karena SNMP memberikan solusi sederhana, dan hanya membutuhkan sedikit kode. Setiap vendor dapat dengan mudah membangun agen SNMP untuk produk mereka.

Sistem manajemen jaringan dengan SNMP mempunyai dua entitas utama : Manager dan agen. Manager adalah tempat di mana administrator jaringan mengontrol fungsi manajemen jaringan. Agen adalah entitas yang melekat ke perangkat yang sebenarnya dikelola. Switch, Router atau Server jaringan adalah contoh perangkat yang dikelola.

SNMP didasarkan pada Manager / agen model. SNMP disebut sebagai “simple” karena agen membutuhkan software yang sangat kecil. Pemrosesan dan penyimpanan data berada pada sistem Manager, sementara bagian pelengkap dari fungsi-fungsi berada di sistem yang dikelola (dikenal sebagai obyek). SNMP juga menggunakan datagram UDP karena lebih sederhana dalam pengiriman informasi. Karena kesederhanaanya SNMP v1 banyak diimplementasikan tapi banyak masalah dengan security yang hanya menggunakan password sederhana yang disebut community-string. SNMP versi baru yaitu v2c  dan SNMPv3 kurang lebih merupakan perbaikan security pada versi sebelumnya dengan mempertahankan kesederhanaan protocol query dari SNMP.

Untuk mencapai tujuannya menjadi sederhana, SNMP hanya memiliki perintah manajemen yang terbatas dan response nya. SNMP Manager bisa mengirimkan perintah Get, GetNext dan Set untuk mengambil satu variabel atau beberapa obyek. Agen berhasil mengirimkan pesan Respon untuk menyelesaikan Dapatkan, GetNext atau Set. Agen bisa mengirimkan trap, ketika agen mengidentifikasi terjadinya kondisi seperti ambang batas yang melebihi nilai yang telah ditentukan. Singkatnya hanya ada lima operasi primitif:

* get (retrieve operation)
* get next (traversal operation)
* get response (indicative operation)
* set (alter operation)
* trap (asynchronous trap operation)



Gambar 1 Management Entity

Data yang dipertukarkan dalam SNMP adalah value sederhana seperti string yang mempunyai nomer disebut OID (Object Identifier). OID ini dikelola dalam database di agent dan biasa disebut MIB (Management Information Base). Management database/table dari obyek juga tidak termasuk di dalam standard protokol SNMP, namun merupakan standard terpisah. Sehingga SNMP hanya merupakan protokol komunikasi untuk bertukar informasinya. Dengan menggunakan aplikasi SNMP Manager seperti MRTG dan Cacti, informasi dari banyak network device bisa ditampilkan melalui web browser dengan sangat mudah. Untuk network device linux sudah banyak sekali template yang digunakan sehingga tinggal cukup merubah target address yang akan dipantau.

1. **Hasil dan Analisa**

SNMP merupakan sebuah protokol jaringan yang didesain bagi pengguna 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:

1. Manager

Manager adalah pelaksana dan manajemen jaringan. Pada kenyataannya manager ini merupakan komputer biasa yang ada pada jaringan yang mengoperaksikan perangkat lunak untuk manajemen jaringan. Manager ini terdiri atas satu proses atau lebih yang berkomunikasi dengan agen-agennya dan dalam jaringan. Manajer akan mengumpulkan informasi dari agen dari jaringan yang diminta oleh administrator saja bukan semua informasi yang dimiliki agen.

1. MIB atau Manager Information Base

Dapat dikatakan sebagai struktur basis data variabel dari elemen jaringan yang dikelola. Struktrur ini bersifat hierarki dan memiliki aturan sedemikian rupa sehingga informasi setiap variabel dapat dikelola atau ditetapkan dengan mudah. Berikut adalah struktur dari MIB, yaitu:

* Setiap object mempunyai ID unik (OID).
* MIB mengasosiasikan setiap OID menggunakan label dan parameter lain.
* MIB bertindak sebagai kamus data digunakan untuk menyusun terjemahan pesan SNMP.
1. Agent

Agent merupakan perangkat lunak yang dijalankan disetiap elemen jaringan yang dikelola. Setiap agen mempunyai basis data variabel yang bersifat lokal yang menerangkan keadaan dan berkas aktivitasnya dan pengaruhnya terhadap operasi.

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.

**Analisa:**

Tapping data dengan wireshark untuk mencari traffick SNMP saya lakukan menggunakan jaringan wifi public, terlebih dahulu menginstal program snmp (*sudo apt install snmp*) pada terminal bash linux. Jika SNMP belum di install maka pada wireshark tidak terdapat protocol SNMP, Data SNMP yang saya dapat pada wireshak menunjukkan bahwa manager me-*request* dengan perintah *Get Next Request,* Selanjutnya Agent akan merespon dengan perintah *Get Respons,* Artinya Manager meminta data informasi selanjutnya dari jaringan yang akan dimonitoring, kemudian *agent* sebagai elemen jaringan yang dimonitoring atau dikontrol oleh *manager* sehingga *agent* merespon dengan memberikan data.

Ip manager : 192.168.137.201

Ip Agent : 192.94.214.205

Berikut gambar Capture traffick data SNMP di wireshark:



Gambar 2 Capture Traffik data SNMP

 Pada gambar tersebut terlihat hasil filtering dengan keyword “snmp” yang kita masukkan, terlihat beberapa caption seperti *no, time, source, destination, protocol,  length*dan juga *info*. Deretan tupple ini memperlihatkan *handshake*yang dilakukan antara kedua alamat. Address pertama 192.168.137.201 merupakan alamat ip manajer sedangkan alamat kedua 192.94.214.205 merupakan alamat router atau agen. Manajer melakukan *request* kepada *agen* berupa *get-next-request* (Meminta komponen objek berikutnya dari suatu table atau daftar dari suatu agen)dan nomor OID yang terlihat pada info, kemudian agen memberikan pesan *get-response* (Merespon semua permintaan)menuju manajer. Proses *trap* ini dilakukan terus menerus.

Berdasarkan gambar 2 dapat kita lihat pada bagian info bahwa setiap permintaan SNMP terdapat Protocol Data Unit (PDU). PDU merupakan unit data yang terdiri atas sebuah header dan beberapa data yang ditempelkan. SNMP PDU digunakan untuk komunikasi antara manager SNMP dan agent SNMP.



Gambar 3 Info Detail get-next-request (192.168.137.201)



Gambar 4 Info Detail get-response (192.94.214.205)

 Dilihat pada info detail perbedaan antara ***Get-next-Request*** dan ***Get-Respone*** terdapat pada nilai *Value*-nya. Pada saat pertama kali manager mengirim *Get-Request* kepada agent, nilai *Value* yaitu Null. Kemudian agent menanggapi permintaan dari manager. maka agent akan mengirimkan *Get-Respone* ke manager. Di detail informasi *get-respone,* kita dapat melihat bahwa nilai Value adalah 74 65 73 74 2e 6e 65 74 2d 73 6e 6d 70 2e 6f 72 67 yang bertipe octetstring, lalu nilai Value itulah yang akan di kirim kepada manager.

Visualisai data SNMP menggunakan tools Orange:



Gambar 5 penyajian data SNMP



Gambar 6 Data SNMP



Gambar 7 grafik Protocol

Dibawah ini adalah *three way handshake* SNMP :

Manager

Source192.168.43.22

Manager

Source192.168.137.201

Agent

Destination192.94.214.205

*Get-next-Request*

Request-Id: 818135409# Lengt: 86#

Variabel Bindings 1 items: (1.3.6.1.2.1) # Value (Null)

Port UDP

61880

Port UDP

61880

Port UDP

161

SNMP-Trap

*Get-Respone*

Respone-Id: 818135409 # Lengt: 106#

Variabel Bindings 1 items:(1.3.6.1.2.1.1.1.0) # Value (octetstring): 74 65 73 74 2e 6e 65 74 2d 73 6e 6d 70 2e 6f 72 6

Gambar 8 *Three Way Handshake* SNMP)

1. **Kesimpulan**

SNMP merupakan sebuah protokol jaringan yang didesain bagi pengguna khususnya administrator jaringan untuk memonitor aktifitas jaringan komputer dan mengontrol sebuah komputer atau server secara sistematis dari jarak jauh. Sistem manajemen jaringan dengan SNMP mempunyai dua entitas utama : Manager dan agent.

1. **Daftar Pustaka**

D. Stiawan, D. Jurusan, S. Komputer, and F. Unsri, “Network Management : Optimalisasi untuk mencapai High Reliability Sisi Teknis …,” no. i.

Rizky, Pasman. 2014. “SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)”. <http://pasman-pcr.blogspot.com/2014/07/snmp-simple-network-management-protocol_4.html>

Wibawa, Triastana Anang. 2017. “SNMP”. <http://binus.ac.id/malang/2017/10/snmp/>