**Analisis Traffic SNMP pada Wireshark**

**Menggunakan Network Wifi Public**

Ulviyana (09011281520090)

Manajemen Jaringan

Sistem Komputer

**PENDAHULUAN**

1. **Latar Belakang**

Perkembangan teknologi informasi dan komunikasi saat ini berkembang sangat pesat. Seluruh perusahaan dan instansi di seluruh dunia telah memanfaatkan teknologi jaringan komputer untuk mendukung kinerja perusahaan. Infrastruktur jaringan komputer telah menjadi hal yang paling pokok yang harus selalu tersedia dan terjaga kestabilan operasionalnya terutama lalu lintas (traffic) dari infrastruktur jaringan tersebut. Semakin banyaknya pengguna jaringan komputer di masa saat ini, maka hal ini juga harus disertai dengan peningkatan kualitas pengelolaan jaringan tersebut. Faktor terpenting dalam meningkatkan kualitas pengelolaan jaringan komputer adalah lalu lintas data (traffic) yang terjadi di dalam jaringan tersebut.

Manajemen jaringan terutama sistem monitoring menjadi hal yang sangat penting. Monitoring ini dilakukan untuk menjaga kestabilan operasional jaringan komputer tersebut. Simple Network Management Protocol (SNMP) adalah protokol aplikasi pada jaringan TCP/IP yang dapat digunakan untuk pengelolaan dan pemantauan (monitoring) sistem jaringan komputer. Sebagian besar peralatan jaringan telah mendukung penggunaan SNMP dalam pemantauannya. SNMP dapat membantu proses monitoring dan manajemen jaringan, dalam hal ini dapat dihasilkan suatu mekanisme untuk mendapatkan informasi tentang lalu lintas (traffic) dalam suatu jaringan intranet. Tetapi layanan dan informasi SNMP ini hanya dapat diakses melalui terminal atau command prompt sehingga penggunaannya tidak efektif dikarenakan masih membutuhkan pengolahan dan tampilan yang sulit dimengerti.

Solusi yang pernah dilakukan adalah dengan membuat Graphical User Interface (GUI) sebagai cara untuk membantu pengguna terutama administrator untuk mengambil dan menampilkan nilai SNMP. Tetapi hal ini belum cukup karena hasil yang ditampilkan hanya sebatas informasi kondisi jaringan pada saat itu dan masih belum ada sistem untuk mengolah dan menyimpan nilai SNMP lebih lanjut. Jika data yang diperoleh kemudian diolah secara lanjut akan dihasilkan laporan tentang kondisi jaringan sehingga mempermudah administrator jaringan dalam pemantauan kondisi jaringan dan menganalisis kebutuhan serta pengembangan jaringan kedepannya. Solusi yang dapat dilakukan adalah dengan menyediakan sistem database untuk menyimpan nilai – nilai kondisi jaringan yang di dapat dari pesan SNMP dan mengolahnya lebih lanjut.

Pada tugas akhir ini akan dilakukan perancangan dan pembuatan aplikasi monitoring jaringan yang tidak hanya dapat mengambil nilai SNMP tetapi juga dapat mengolah nilainya sekaligus terdapat sistem penyimpanan atau database sehingga dapat ditampilkan laporan informasi tentang kondisi jaringan yang meliputi availability perangkat dan traffic.

1. **Rumusan Masalah**

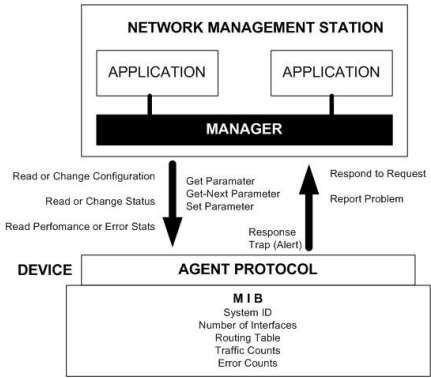
Perkembangan teknologi informasi, khususnya jaringan memungkinkan terjadinya pertukaran informasi yang cepat dan semakin kompleks. Pengaturan jaringan yang baik tentu akan memaksimalkan pemanfaatan informasi tersebut. karena semakin besar dan luas sistem jaringan maka akan semakin sulit untuk mengatur dan mengawasinya.

1. **Tujuan**

* Memantau jaringan agar pengiriman atau pertukaran informasi dapat berjalan dengan baik.
* Mengumpulkan informasi manajemen mengenai lingkungan lokalnya.
* Menyimpan dan mengambil informasi manajemen yang didefinisikan di MIB.
* Memberikan sinyal sebuah event ke Manager.
* Bekerja sebagai proxy untuk beberapa node jaringan yang tidak mendukung SNMP.d

1. **Hasil dan Pembahasan**

Dimana point – point protokol SNMP sesuai dengan gambar interaksi antara manager dan agent dibawah ini:



Gambar 1. Interaksi Antara Manager dan Agent

1. Simple Network Management Protocol (SNMP) adalah, sebuah protocol yang digunakan sebagai standar untuk melakukan pengaturan perangkat-perangkat jaringan. Dengan bantuan tools/ daemon lain dan dapat mengumpulkan dan memanipulasi informasi network dengan mengumpulkan informasi baseline dengan interval waktu tertentu. SNMP dapat digunakan untuk mengonfigurasi device yang jauh, memantau unjuk kerja jaringan, mendeteksi kesalahan jaringan atau akses yang tidak cocok, dan mengaudit pemakaian jaringan. Sedangkan Aplikasi NMS digunakan untuk menjalankan aplikasi yang dapat memonitor dan mengontrol managed device. NMS memberikan resource memory dan prosesor yang dibutuhkan untuk manajemen network. Satu atau lebih NMS harus ada dalam sebuah jaringan yang di manage. Terdapat 3 konsep dasar pada SNMP, yaitu: manager, agent, dan management information based (MIB)
2. Manager

Sebuah managed device adalah sebuah node di jaringan yang berisi agen SNMP yang berada di jaringan yang dapat di manage. Managed device akan mengumpulkan dan menyimpan informasi manajemen dan membuat informasi ini tersedia bagi NMS menggunakan SNMP. Pada beberapa konfigurasi di titik manager menjalankan suatu software management, dimana perangkat yang dapat dimanage seperti bridges, routers, servers dan workstations yang dapat integrasikan dengan sebuah modul software agent.

1. Agent

Agent pertanggung jawab untuk menyediakan akses ke lokal MIB dari object resources dan aktivitas node tersebut. Agen tersebut juga akan bereaksi terhadap perintah manager untuk mendapat kembali nilai-nilai dari MIB dan untuk menetapkan nilai nilai di dalam MIB. Satu contoh dari suatu obyek didapat kembali dari suatu perhitungan dari banyaknya paket-paket pengirim dan penerima pada sebuah node. Manager dapat memonitor nilai yang diload pada jaringan tersebut. Software Agent berada pada di devices tersebut, beberapa agent menerima pesan yang masuk dari manager, pesan permintaan tersebut di baca atau ditulis pada data device tersebut. Agent akan mengirimkan kembali respon yang diterima, dimana agent tidak harus menunggu untuk bertanya tentang sebuah informasi. Namun pada beberapa kasus tertentu agent akan mengirimkan sebuah pesan notifikasi untuk melakukan trap ke satu atau lebih manager. Software Management pada sebuah station management akan mengirimkan pesan request ke agent dan menerima respon dan trap dari agent. Protocol UDP yang biasa digunakan sebagai pembawa paket tersebut dengan karakteristiknya yang hemat dengan bandwidth, namun protocol pembawa lainnya juga dapat digunakan.

1. MID (Management Information Base)

Management Information Base merupakan struktur basis data variabel dari elemen jaringan yang dikelola. Struktur ini bersifat hierarki dan memiliki aturan sedemikian rupa sehingga informasi setiap variabel dapat dikelola atau ditetapkan dengan mudah. MIB di akses menggunakan protokol network-manajemen seperti SNMP. MIB terdiri dari managed objek dan di identifikasi oleh object identifier (pengidentifikasi objek). Sebuah managed object, kadang kala di sebut sebagai MIB object, objek, atau MIB, adalah satu dari banyak karakteristik spesifik dari peralatan yang di manage.

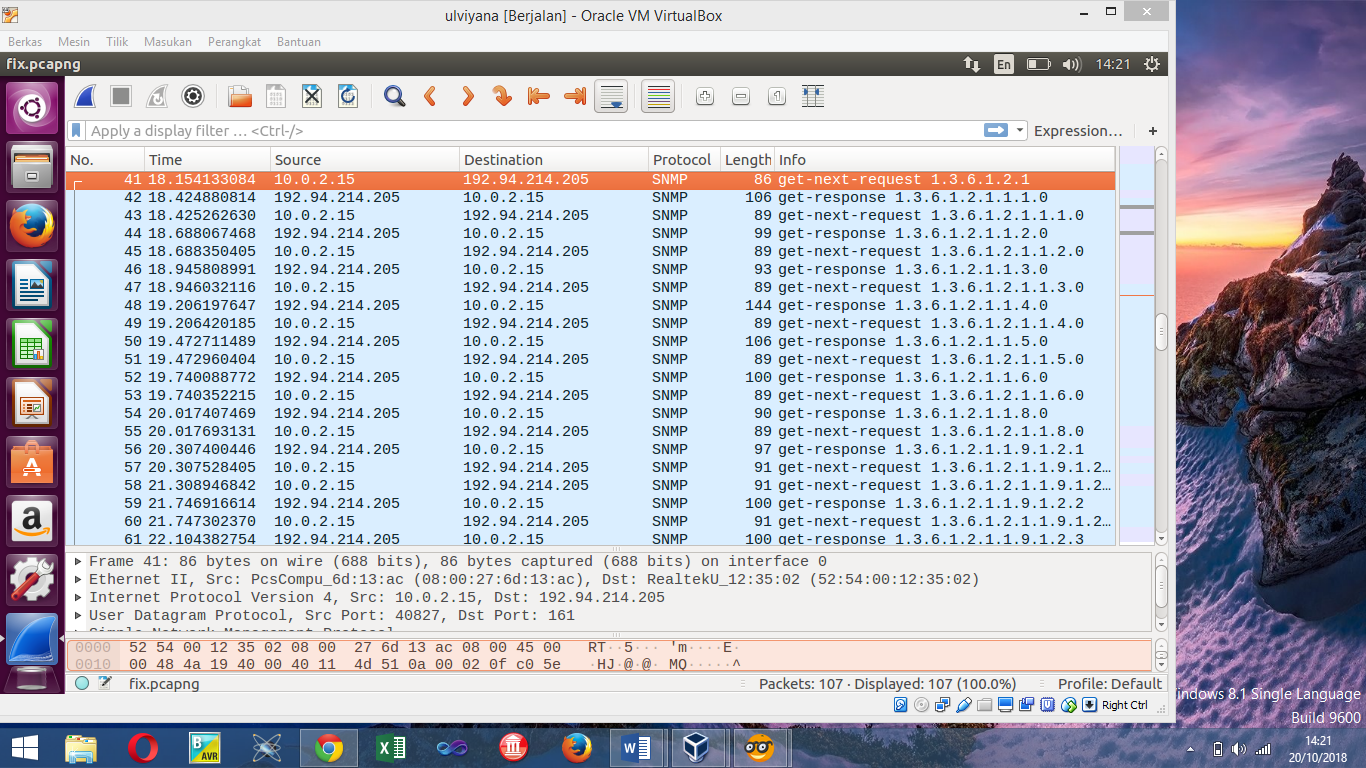
1. **Analisa**

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 menunjuk kan bahwa manager merequest 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 merespone dengan memberikan data.

Ip manager : 10.0.2.15

Ip Agent : 192.94.214.205

Berikut gambar Capture traffick data SNMP di wireshark:



Gambar 2. Capture Traffik data SNMP

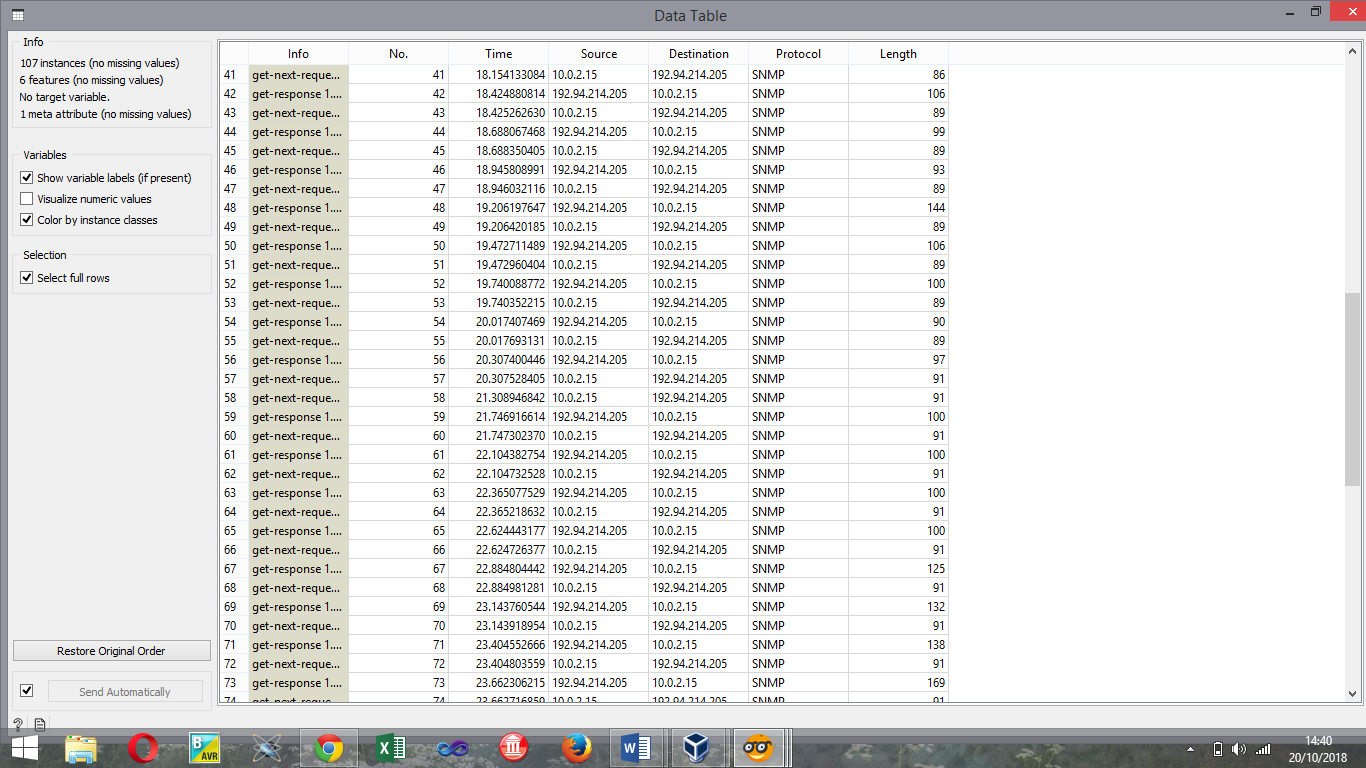
Pada gambar tersebut terlihat hasil filtering dengan keyword “snmp” yang kita masukkan, terlihat beberapa caption seperti *no, time, source, destination, protocol, data length*dan juga info. Deretan tupple ini memperlihatkan *handshake*yang dilakukan antara kedua alamat. Address pertama 10.0.2.15 merupakan 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.

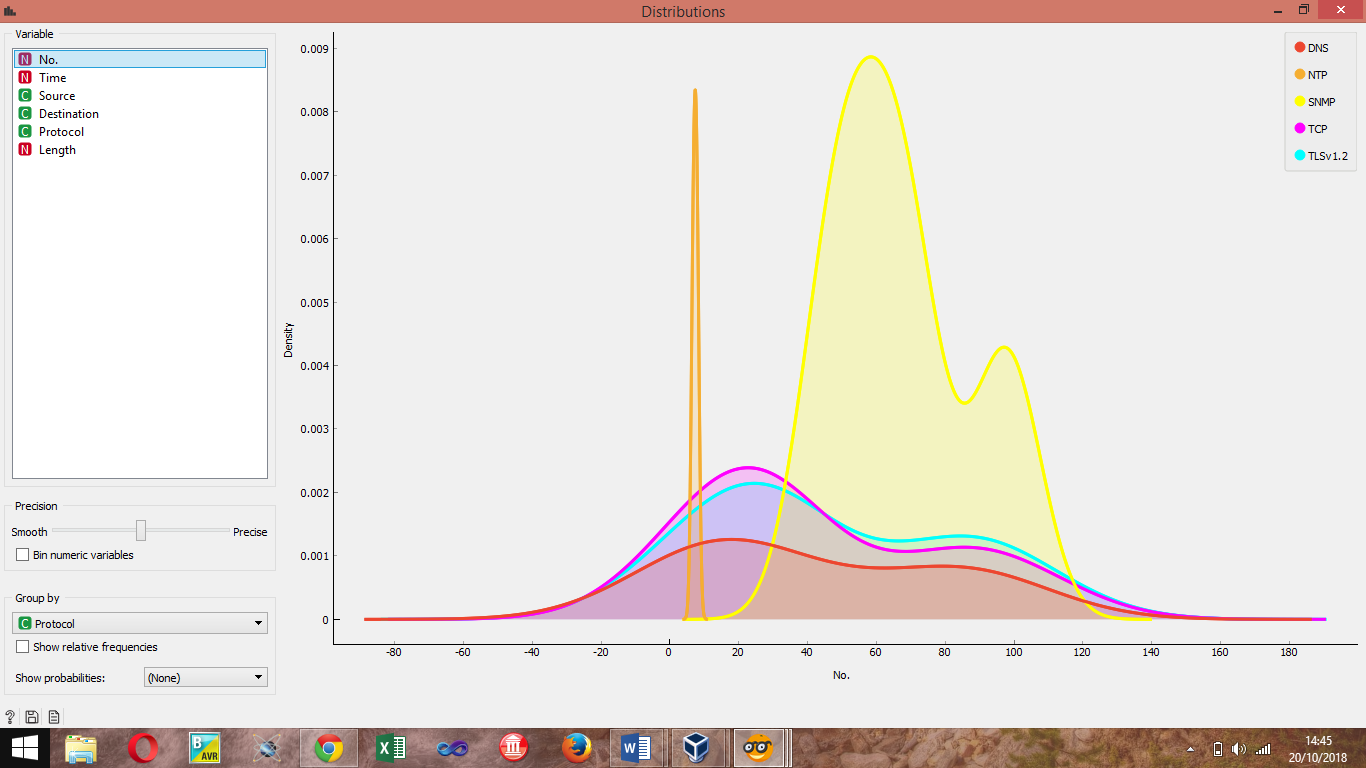
Visualisai data SNMP menggunakan tools Orange:



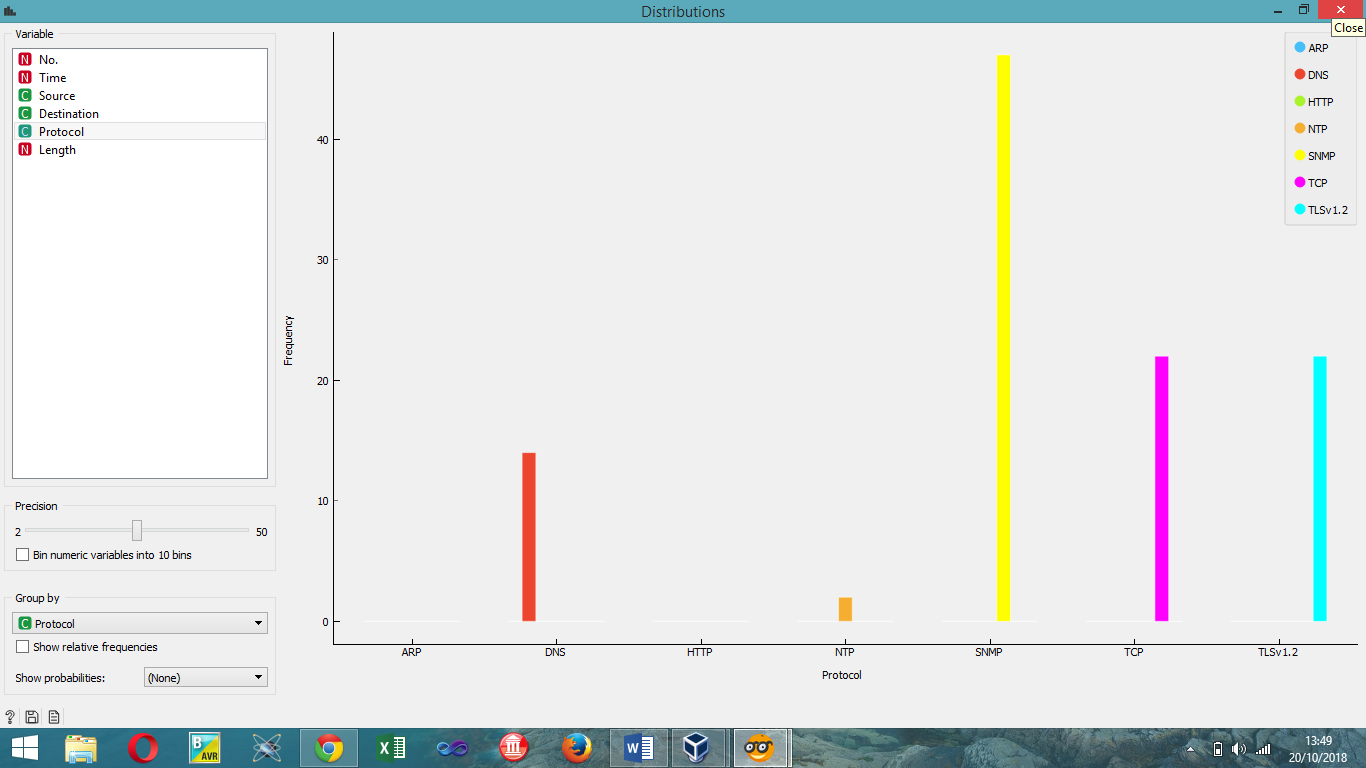
Gambar 3. Penyajian Data SNMP Melalui Apk Orange



Gambar 4. Penyajian Data SNMP pada Tabel Data Melalui Apk Orange



Gambar 5. Penyajian Distribusi Berdasarkan Number Melalui Apk Orange



Gambar 6. Penyajian Distribusi Berdasarkan Protocol Melalui Apk Orange

Dibawah ini adalah *three way handshake* SNMP :

Manager

Source10.0.2.15

Manager

Source10.0.2.15

Agent

Destination192.94.214.205

Port UDP

161

SNMP-Trap

Port UDP

61880

*Get-next-Request*

Request-Id: 818135409# Lengt: 86#

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

*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

Port UDP

61880

Gambar 7. *Three Way Handshake* SNMP

**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.

**Daftar Pustaka**

Halsall, Fred. 2001. “*Multimedia Communications : Applications, Protocols and Standarts”*. Harlow : Addison-Wiley Publishing.

M. Rizky, D. Jurusan, T. Elektro, F. Teknologi, and U. Andalas, “IMPLEMENTASI PROTOKOL SNMP UNTUK JARINGAN Abstrak,” vol. 1, no. 1, pp. 15–19, 2013.

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