ISSN 2087-0256

smatika Jurnal

STIKI Informatika Jurnal

Volume 05, Nomor 01 Tahun 2015

ISSN 2087-0256

Smatika Jurnal

STIKI Informatika Jurnal

Volume 05, Nomor 01 Tahun 2015

Lembaga Penelitian & Pengabdian Masyarakat
SEKOLAH TINGGI INFORMATIKA & KOMPUTER INDONESIA

SIMPLE NETWORK MONITORING PROTOCOL (SNMP) UNTUK MEMONITOR TRAFIK USER
Studi Kasus : Universitas Kanjuruhan Malang

Yusriel Ardian
Fakultas Teknologi Informasi
Universitas Kanjuruhan Malang
acilnet@yahoo.com

ABSTRAK

Kelemahan manusia yang memiliki keterbatasan fisik seperti perlunya tidur atau istirahat, membutuhkan sebuah sistem yang dapat melaksanakan pekerjaannya secara otomatis harus ditunggu. Demikian juga seorang Network Administrator yang harus selalu memantau jaringan yang dikelola akan membutuhna Network Monitoring yang benar-benar dapat membantu keterbatasan tersebut. Sistem peringatan menggunakan SMS adalah salah satu solusi yang anggap cukup bagus untuk saat ini. Network Monitoring adalah sistem yang terus menerus memantau kondisi server, router, dan device jaringan lainyan, sehingga ketika ada masalah pada jaringan dapat di ketahui dengan cepat oleh administrator jaringan. Network Monitoring System (NMS) dibangun untuk meringankan beban monitoring atau pengawasan yang dilakukan oleh manusia.sistem monitoring jaringan yang memanfaatkan protocol SNMP diharapkan membantu seorang administrator jaringan untuk mengawasi secara detail trafik dan pemakain bandwith setap user dalam sebuah jaringan komputer yang dibawah tanggung jawabnya.

Kata kunci : SNMP, Trafik, bandwith. network.

1. PENDAHULUAN

Network monitoring dapat di artikan suatu sistem yang secara terus-menerus memonitor kondisi jaringan seperti router, server maupuan device jaringan lainnya dan mencatat setiap kejadian ke dalam basis data untuk di jadikan *report*. *Monitoring* itu sendiri adalah memantau jaringan, jika pada suatu jaringan ada device yang tidak berfungsi ataupun ada masalah, maka sistem *akan melakukan peringatan kepada seorang* network administrator atau system administrator. Sedangkan reporting adalah menampilkan data dalam bentuk visual kepada network administrator atau system dalam bentuk data yang telah di olah sedemikian rupa oleh sistem, sehingga data lebih mudah untuk di baca.

Universitas Kanjuruhan Malang merupakan institusi perguruan tinggi yang memanfaatkan jaringan computer untuk berbagai macam keperluan administrasi perkantoran dan dalam menyelenggaran pendidikan. Pada saat ini Universitas Kanjuruhan Malang sudah menggunakan network monitoring untuk melakukan monitoring terhadap aktifitas router, server, dan *device* jaringan lainya. Apabila ada masalah pada router, server, dan *device* jaringan lainya yang di monitoring akan di tampilkan dalam bentuk visual sehingga memudahkan administrator jaringan dalam memantau semua router, server, dan device jaringan lainya yang ada. Tetapi network monitoring yang ada pada saat ini memiliki beberapa kelemahan, yaitu sistem ini berbasis desktop sehingga hanya dapat di lihat oleh administrator jaringan yang berada dalam *ruangan M.I.S (Manajemen Information System)*, jika administrator jaringan tidak berada di dalam rungan, maka tidak dapat melihat kondisi dan status server yang ada pada saat itu serta belum adanya sistem sebuah sistem network monitoring yang baru untuk mempermudah administrator jaringan dalam memonitor jaringan walaupun sedang tidak berada di dalam rungan. Selain itu *system network monitoring* yang baru ini dapat di jadikan sebuah acuan atau tolak ukur untuk penggantian atau perawatan secara berkala pada server yang di pantau dengan melihat data yang ada.

2. TINJAUAN PUSTAKA

2.1 Network Monitoring

Terdapat dua alasan utama untuk memonitor suatu jaringan, yaitu untuk meramalkan perubahan untuk perkembangan yang akan datang dan juga untuk mendeteksi perubahan yang tidak terduga dalam status jaringan. Perubahan tidak terduga yang mungkin terjadi seperti kegagalan router atau switch, seorang hacker berusaha mengakses jaringan secara ilegal, atau kegagalan jalur komunikasi. Tanpa kemampuan untuk memonitor jaringan, seorang administrator hanya dapat bereaksi terhadap problem, jika problem tersebut muncul barulah diselesaikan dibandingkan mencegah problem ini sebelumnya (*Cisco Networking Academy Program Second-Year Companion Guide 2nd Edition, 2001,p424*).

2.1.1 Connection Monitoring

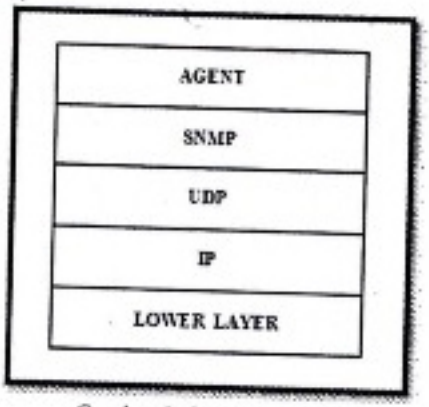
Connection monitoring adalah salah satu teknik untuk memonitor jaringan. Teknik ini dapat dilakukan dengan melakukan tes ping antara monitoring station dan device target, sehingga dapat diketahui bila koneksinya down, tetapi metode ini tidak dapat mengindikasikan dimana letak masalahnya. Metode ini kurang baik, sebab pada jaringan yang besar, di mana terdapat banyak host akan memerlukan sumber sistem yang besar. (*Cisco Networking Academy Program: Second-Year Companion Guide 2nd Edition, 2001,p425*)

2.1.2 Traffic Monitoring

Traffict monitoring adalah sebuah metode yang lebih canggih dari networking monitoring. Metode ini melihat paket aktual dari traffic pada jaringan dan menghasilkan laporan berdasarkan traffic jaringan. Program ini tidak hanya mendeteksi peralatan yang gagal, tetapi mereka juga menentukan apakah suatu komponen overload atau terkonfigurasi secara buruk. Kelemahan dari program ini adalah karena biasanya bekerja pada suatu segmen tunggal pada satu waktu; jika data perlu didapat dari segmen lain, software monitoring harus bergerak pada segmen tersebut, tapi hal ini dapat diatasi dengan menggunakan agent pada segmen remote network. (*Cisco Networking Academy Program: Second-Year Companion Guide 2nd Edition, 2001,p425*)

2.5.1 Simple Network Monitoring Protocol (SNMP)

Secara umum SNMP adalah sebuah protokol yang didesain untuk memberikan kemampuan pengumpulan data manajemen perangkat jaringan dan pengkonfigurasian perangkat jaringan secara jarak jauh (*remotely*). Pengelolaan ini dilakukan dengan cara melakukan polling dan setting variabel-variabel elemen jaringan yang dikelolanya. SNMP didesain oleh Internet Engineering *Task Force* (IETF) untuk pemakaian di internet. SNMP memanfaatkan datagram UDP untuk menyampaikan pesannya pada perangkat jaringan. Karena pesan UDP bersifat *unreliable* (tidak dapat diandalkan) maka SNMP menggunakan prosedur time out dan *retry count* untuk mengecahkan masalah ini,



Gambar 1. Struktur SNMP

SNMP terdiri dari 3 bagian:

a. MIB (*Management Information Base*)
b. Agent
c. Manager

MIB bisa dikatakan sebagai struktur database variable elemen jaringan yang dikelola. Struktur ini bersifat hierarki dan memiliki aturan sedemikian rupa sehingga informasi nilai setiap variabel dapat diketahui atau di set dengan mudah. Agent merupakan software yang dijalankan di setiap node atau elemen jaringan yang akan dimonitor. Tugasnya adalah mengumpulkan seluruh informasi yang telah ditentukan dalam MIB.

Manager merupakan software yang berjalan di sebuah host di jaringan. Manager ini bertugas mengumpulkan informasi dari agen-agen. Tidak semua informasi yang dimiliki agent diminta oleh manager. Informasi-informasi yang diminta oleh

administrator jaringan, yang menjalankan host yang berfungsi sebagai manager saja yang akan dikumpulkan oleh agent. SNMP bekerja secara sederhana. Manager dan agent saling bertukar pesan berupa permintaan manager dan jawaban dari agent tentang informasi jaringan. Pesan-pesan ini dibawa oleh paket-paket data yang disebut PDU (Protocol Data Unit). PDU merupakan unit yang terdiri dari sebuah header dan beberapa data yang ditempelkan pada header tersebut. PDU ini dapat dilihat sebagai sebuah benda yang mengandung variabel-variabel, dimana variabel-variabel tersebut memiliki nama dan nilai. Lima PDU yang telah didefinisikan dalam standard adalah sebagai berikut :

a. GET REQUEST
   Dimanfaatkan untuk membaca informasi (nilai) MIB ketika manajer mengetahui informasi yang spesifik mengenai suatu objek.
b. GET-NEXT REQUEST
   Seperti Get Request, tetapi memungkinkan pengambilan informasi pada logical identifier selanjutnya dalam MIB Tree secara berurutan. *Get-Next* melakukan pengambilan objek dengan melakukan traverse pada MIB tree.
c. GET RESPONSE
   PDU ini untuk merespons unit data Get Request, *Get-Next Request* dan *Set Request*. *Get Response* dikeluarkan oleh agent.
d. SET REQUEST
   Dipakai untuk menjelaskan aksi yang harus dilaksanakan di elemen jaringan. Biasanya untuk mengubah/melakukan modifikasi nilai suatu daftar variabel.
e. TRAP
   PDU ini memungkinkan modul management jaringan (*agent*) memberi laporan tentang kejadian pada elemen jaringan kepada manager.

PDU Request dari manager dikirimkan melalui port UDP 161 dan dibalas oleh agen melalui port yang sama. Sementara agent akan mengirimkan pesan trap melalui port 162. Dengan menggunakan dua port berbeda, sebuah host bisa menjalankan fungsi sebagai manager dan agent sekaligus.

Ada empat format data primitif yang didefinisikan bagi SNMP untuk merepresentasikan informasi manajemennya. Beberapa tipe abstrak kemudian dikembangkan diatas tipe data primitif ini. Keempat tipe data primitif ini adalah:

• INTEGER
Merupakan sebuah nilai 32-bit dalam representasi 2 komplomen. INTEGER memiliki range nilai antara -
2147483648 sampai 2147483647, dan biasa digunakan untuk merepresentasikan sebuah enumerasi.

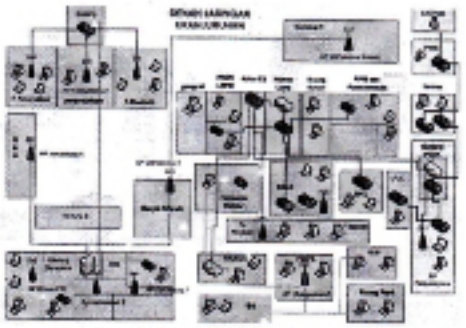
• OCTET STRING
Adalah satu atau lebih oktet. Tiap oktetnya memiliki nilai antara 0-255. Tipe data ini biasanya digunakan untuk merepresentasikan sebuah teks string.

• OBJECT IDENTIFIER
Adalah sebuah urutan integer yang mentranverse sebuah MIB tree.

• NULL

3. PEMBAHASAN

Hasil yang diinginkan dalam pembahasan karya ilmiah ini adalah bagimana *Protocol Simple Network Monitoring* ini dapat digunakan sebagai alat untuk mendeteksi penggunaan trafik pada jaringan oleh masing-masing user yang berada pada suatu jaringan. Berikut desain jaringan yang digunakan sebagai obyek ujicoba dari pembahasan ini sebagai berikut :



Gambar 2. Desain jaringan ujicoba

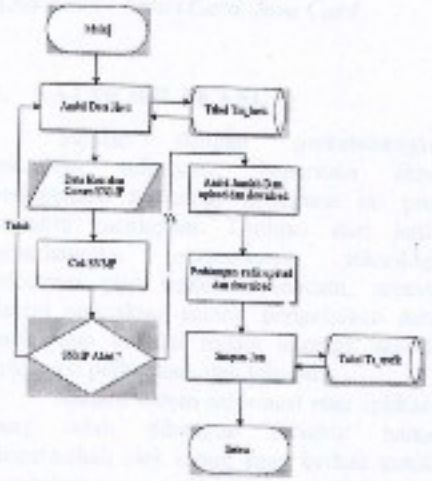
3.1 Bisnis Proses

Pada Bisnis Proses ini digambarkan bagaimana aplikasi dari sistem monitoring trafik bekerja sesuai alr sistem yang telah ditentukan sebelumnya.

Gambar 3. Bisnis proses system

Pada gambar 3 dijelaskan bagaimana sistem pertamakali melakukan mengambil data host ke database, setelah mengambil system menampilkan data kemudian system melakukan cek terhadap host yang ada pada database, apakah host merespon "true", jika responya "true" sistem menyimpan status host hidup pada database jika status false system menyimpan data status host mati dan mengirim sms pada administrator jaringan.

3.2. Flowchart MIB SNMP

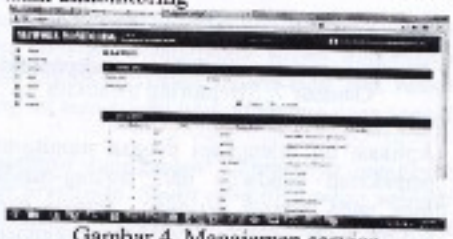


Gambar 4. Flowchart MIB SNMP

Pada gambar 4 menjelaskan proses pengambilan data MIB SNMP, sebelum mengambil data sistem menampilkan host dan community SNMP pada tabel master host, setelah itu sistem melakukan pengecekan kepada host, jika host aktif maka sistem akan mengambil data trafik in dan out, pada awalnya data in dan out masih merupakan data total trafik, kemudian sistem melakukan perhitungan dengan mengurangkan total trafik terakhir dengan total trafik terakhir sebelumnya, setelah itu hasil perhitungan akan di simpan pada tabel trafik.

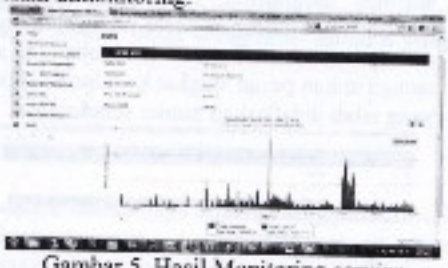
3.3. Manajemen *Service*

Digunakan untuk mengelola service-service mana saja pada computer user yang akan dimonitoring



Gambar 4. Manajemen service

Pada gambar diatas dijelaskan bagaimana cara memilih service-service apa saja yang akan dimonitoring.



Gambar 5. Hasil Monitoring service

Sedangkan pada gambar 5 merupakan laporan hasil monitoring dari computer user dalam bentuk grafik. Variable yang tunjukkan pada grafik tersebut adalah beberapa log yang di kategorikan seperti Error, Warning, Info, dan Notice.

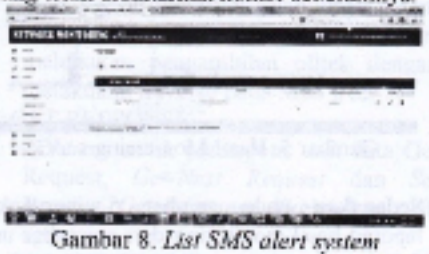
Gambar 6. Log host activity

Pada gambar 6 menunjukkan bagaimana aplikasi monitoring dapat merekam keluar masuknya semua data dari semua port dan protocol pada sebuah host tertentu, sehingga

network administrator dapat menganalisa trafik data.

Gambar 7. Monitoring bandwith

Aplikasi ini dilengkapi dengan monitoring pemakaian bandwith dari masing-masing user pada sebuah jaringan. Seperti yang terlihat pada gambar 7 terlihat penggunaan bandwith *upstream* dan *downstream* Aplikasi Monitoring dilengkapi dengan SMS *alert system*, dimana jika terjadi sesuatu hal dalam aktifitas monitoring yang mana seorang administrator jaringan perlu mengetahuinya maka sistem secara otomatis akan mengirimkan pesan singkat ke telpon seluler yang telah didaftarkan nomor sebelumnya.



Gambar 8. *List SMS alert system*

Gambar 8 menunjukkan daftar alert/ peringatan apa saja yang perlu dikirimkan ke ponsel seorang administrator jaringan.

4. KESIMPULAN

Protocol Simple Network Monitoring ini dapat digunakan sebagai alat untuk mendeteksi penggunaan trafik pada jaringan oleh masing-masing user yang berada pada suatu jaringan.

5. DAFTAR PUSTAKA

[1] Maouro, Douglas. 2005. Essential SNMP, 2nd Edition. Penerbit O'Reilly Media, Inc. Sbastopol.

[2] Team, Cisco.2001. Cisco Networking Academy Program: Second-Year Companion Guide 2nd Edition. Penerbit Cisco Press, Indianapolis.

[3] D.Sloan. Joseph. 2001. Network Troubleshooting Tools. Penerbit O'Reilly Media, Inc. Sbastopol.