

**TUGAS**  
**MANAJEMEN JARINGAN**  
**“PRODUK-PRODUK NETWORK MANAGEMENT**  
**SYSTEM (NMS)”**



Oleh :

Nama : Anggit Mardian

NIM : 09011281419062

Kelas : SK 7 Pil

**SISTEM KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS SRIWIJAYA**

**2017**

## **PRODUK-PRODUK NMS**

### **A. Pengertian Network Monitoring System (NMS)**

Network Monitoring System atau NMS, adalah suatu server yang diperuntukan oleh administrator jaringan untuk memantau performansi jaringannya, seperti Memory usage, CPU load, disk usage, service states, running process, dan lain sebagainya. NMS menggunakan protokol SNMP (Simple Network Management Protocol) yang merupakan standar manajemen jaringan pada TCP/IP. Gagasan di balik SNMP adalah bagaimana supaya informasi yang dibutuhkan untuk manajemen jaringan bisa dikirim menggunakan TCP/IP. Beragam NMS sudah tersedia, dari yang gratis karena open source hingga yang berbayar. Salah satu contoh NMS adalah Nagios.

#### **1. Nagios**

##### **a. Pengertian Network Monitoring System (NMS)**

Network Monitoring System atau NMS, adalah suatu server yang diperuntukan oleh administrator jaringan untuk memantau performansi jaringannya, seperti Memory usage, CPU load, disk usage, service states, running process, dan lain sebagainya. NMS menggunakan protokol SNMP (Simple Network Management Protocol) yang merupakan standar manajemen jaringan pada TCP/IP. Gagasan di balik SNMP adalah bagaimana supaya informasi yang dibutuhkan untuk manajemen jaringan bisa dikirim menggunakan TCP/IP. Beragam NMS sudah tersedia, dari yang gratis karena open source hingga yang berbayar. Salah satu contoh NMS adalah Nagios.

##### **b. Fungsi dan Kelebihan Nagios Sebagai Aplikasi Monitoring**

Jaringan Nagios memosisikan dirinya sebagai aplikasi untuk memantau sistem dan jaringan. Sistem disini berupa resource dari suatu server ataupun aplikasi yang berjalan pada server, seperti cpu, memory, disk dan lain-lain. Sedangkan jaringan lebih mengarah pada layanan aplikasi yang memanfaatkan jaringan, seperti email

server, web server, database, dan lain-lain. Untuk memantau perangkat jaringannya sendiri, seperti interface pada router dan atau switch, membutuhkan plug-in tersendiri.

**c. Fungsi utama dari Nagios adalah sebagai berikut :**

1. Memantau Layanan Jaringan (SMTP, POP3, HTTP, NNTP, PING, dll).
2. Memantau resource Server (Processor load, Disk usage, memory, dll).
3. Kemudahan untuk membuat plugin.
4. Pengecekan layanan secara paralel.
5. Dengan implementasi “parents” dari suatu host, maka bisa dengan mudah dibedakan host yang benar-benar down, dan host yang terkena dampaknya.
6. Beragam Pemberitahuan Jika dideteksi adanya masalah ( lewatvia email, pager, atau buatan user).
7. Kemampuan ‘event-handlers”. Ketika layanan atau host bermasalah, ‘event-handlers’ bisa digunakan untuk pemecahan masalah secara otomatis. Misalkan, layanan email terhenti, lewat ‘event-handler’ kita bisa me-restart layanan email tersebut, sehingga berungsi normal kembali.
8. Log diputar otomatis.
9. Mendukung untuk pemantauan secara redundant.

**d. Kelebihan Nagios adalah sebagai berikut :**

1. Nagios adalah open source.
2. Menggunakan web interface, sehingga dapat diakses secara mudah dan remote dari tempat lain.
3. Selain memonitor network service (HTTP, FTP, dan sebagainya), juga dapat memonitor host resource (penggunaan disk, penggunaan memory, proses, log file, dan sebagainya).
4. Mempunyai fitur reporting lewat web interface.

5. Mempunyai banyak plugins, sehingga menambah fitur-fitur Nagios menjadi semakin lengkap dibandingkan NMS yang lain.
6. Support penggunaan google map.
7. Mempunyai fitur Schedule downtime, dimana sangat diperlukan ketika server di maintenance atau di upgrade.
8. Dapat diintegrasikan dengan Mozilla Firefox, dengan penambahan add-ons Nagios-Checker 0.16.

**e. Syarat Sistem dan Cara Kerja Monitoring dengan Nagios**

Syarat Sistem :

1. Nagios dapat dijalankan di Linux/Unix, dan C compiler.
2. menggunakan jaringan TCP/IP .

**f. Cara Kerja Nagios :**

1. Monitoring Staf IT mengkonfigurasi nagios untuk memantau komponen infrastruktur IT yang penting termasuk sistem metrik, protokol jaringan, aplikasi, layanan, server, dan infrastuktur jaringan.
2. Alerting Ketika komponen infrastruktur penting gagal, nagios mengirim peringatan dan memulihkannya, memberi notice kepada administrator terhadap peristiwa-peristiwa penting. Alarm dapat disampaikan melalui email, SMS, atau script khusus.
3. Response Staf IT menjawab alarm dan mulai memecahkan masalah dan menyelidiki alarm keamanan sesegera mungkin.
4. Reporting Report memberikan catatan/history perihal outages(padam), peristiwa, pemberitahuan, dan respon alarm untuk keperluan pemeriksaan. Adanya laporan membantu terpenuhinya SLA (Service Level Agreement) Anda.
5. Maintenance Downtime yang dijadwalkan mencegah alarm selama pemeliharaan yang terjadwal dan meng-upgrade windows.

6. Planning Tren dan grafik perencanaan kapasitas dan laporan memungkinkan user untuk mengidentifikasi upgrade infrastruktur yang diperlukan sebelum kegagalan terjadi.

## **2. PRTG (Paessler Router Traffic Grapher)**

### **a. Pengertian PRTG**

PRTG (Paessler Router Traffic Grapher) adalah perangkat lunak yang mudah digunakan untuk memantau penggunaan bandwidth dan banyak parameter jaringan lain melalui SNMP, Packet Sniffing, atau Cisco NetFlow yang memungkinkan untuk pengukuran traffic berdasarkan alamat IP dan atau protokol. Pengukuran berbasis SNMP hanya berbasis pada port. Software ini juga memungkinkan untuk secara cepat mempersiapkan dan menjalankan sebuah proses pemantauan untuk sebuah jaringan tertentu. Dengan PRTG ini maka dengan mudah dapat mengetahui sejumlah data yang mengalir melalui perangkat seperti router dan memantau penggunaan PC serta menganalisa traffic yang dapat dikategorikan ke dalam beberapa jenis protokol. PRTG Traffic Grapher berjalan pada mesin Windows di dalam jaringan selama 24 jam setiap hari dan terus menerus mencatat penggunaan parameter jaringan. Dengan PRTG Traffic Grapher ini dapat memonitor semua aspek jenis protokol mulai dari jenis jaringan protokol FTP, HTTP, HTTPS, SMTP, ICMP, DNS, POP3, SNMP dan lainnya . disini dapat dilihat seberapa banyak penggunaan bandwidth pada masing-masing protokol yang telah ada

### **b. Fitur-Fitur Dasar**

1. Kemampuan untuk melakukan monitoring pada jaringan yang digunakan oleh lebih dari 80.000 users setiap harinya.
2. Pengumpulan data dapat melalui SNMP, Packet sniffing atau protokol NetFlow secara bersamaan dalam satu window.
3. Mengklasifikasi traffic jaringan ke dalam parameter-parameter seperti IP address, protokol dan lain-lain.

4. Dapat bekerja dengan kebanyakan perangkat jaringan seperti switch, router, firewalls dan lain-lain yang berbeda-beda sesuai dengan perusahaan pembuatnya.
5. Monitoring engine mampu melakukan monitoring terhadap beberapa (bahkan ribuan) sensor secara simultan.

### **3. NetFlow Analyzer**

NetFlow Analyzer adalah penganalisis lalu lintas jaringan berbasis web yang menggunakan NetFlow dari perangkat Cisco untuk menghasilkan laporan instan mengenai lalu lintas dan pengguna jaringan. Cisco NetFlow menawarkan detail terperinci tentang aplikasi, pengguna, dan percakapan yang dihasilkan oleh lalu lintas jaringan.

NetFlow Analyzer mengumpulkan ekspor dari NetFlow ini, mengkorelasikannya, dan menghasilkan grafik dan laporan yang membantu dalam memahami dan mengatasi masalah lalu lintas jaringan.

NetFlow Analyzer memungkinkan Anda untuk memantau bandwidth dan lalu lintas di tingkat antarmuka dengan satu menit granularity. Grafik yang dipilih memungkinkan Anda memperbesar lonjakan.

NetFlow analyzer juga menunjukkan titik data, yang memberi informasi lalu lintas yang masuk dan rincian lalu lintas yang keluar seperti kecepatan, volume, paket dan utilisasi dari total bandwidth.

Pada NetFlow Analyzer tidak hanya dapat melihat jam terakhir ke laporan kuartal terakhir, tetapi juga dapat memilih periode waktu yang diinginkan untuk melihat laporan lalu lintas jaringan. Laporan dapat diekspor sebagai CSV atau PDF sesuai kenyamanan. Laporan ini bisa sangat berguna saat mempresentasikan ke manajemen puncak. Ini membantu NetFlow Analyzer untuk digunakan secara efektif sebagai analisa lalu lintas jaringan.

#### **4. TeamViewer**

Aplikasi TeamViewer memungkinkan untuk meremote, sharing desktop dan transfer file antar komputer. TeamViewer kompatibel dengan beberapa platform, termasuk Windows, macOS X, Linux, iOS, dan Android. TeamViewer memungkinkan pengguna mengakses komputer lain dari jarak jauh menggunakan browser web.

TeamViewer didirikan di Utingen, Jerman pada tahun 2005. TeamViewer dirancang untuk bekerja dengan baik dengan memasangnya di komputer atau menjalankan versi "Dukungan Cepat" yang tidak memerlukan instalasi. TeamViewer perlu menjalankan komputer untuk mengakses jarak jauh dan kontrol agar dapat bekerja. Perangkat lunak ini menggunakan pertukaran kunci RSA dan encoding sesi AES (256-bit) untuk menyediakan koneksi yang aman.

##### **a. Kelebihan**

1. Mudah untuk digunakan walaupun dengan jangkauan jarak yang cukup jauh selama suatu PC masih terkoneksi pada suatu jaringan.
2. Nyalain-matiin PC secara remote.
3. Mengontrol penuh terhadap mouse dan keyboard
4. Memanipulasi data suatu PC dengan mudah
5. Memiliki fitur video call yang memungkinkan setiap user dapat saling berkomunikasi melalui camera
6. Memiliki fasilitas chatting
7. Bisa mengontrol penuh seluruh aktifitas pada suatu PC

##### **b. Kekurangan**

1. Dari segi keamanan aplikasi ini sangatlah kurang karena setiap orang bisa mengakses PC kita jika mereka mengetahui username dan password pada PC kita.
2. Tidak bisa membedakan antara client dan server karena setiap PC dapat berperan sebagai client sekaligus server.
3. Loadingnya lebih lambat

## 5. Cacti

Cacti adalah salah satu software yang digunakan untuk keperluan monitoring yang banyak digunakan saat ini. Cacti menyimpan semua data/informasi yang diperlukan untuk membuat grafik dan mengumpulkannya dengan database MySQL. Untuk menjalankan cacti diperlukan software pendukung seperti MySQL, PHP, RRDTool, net-snmp, dan sebuah webserver yang support PHP seperti Apache atau IIS.

Cacti salah satu aplikasi open source yang merupakan solusi pembuatan grafik network yang lengkap yang didesign untuk memanfaatkan kemampuan fungsi RRDTool sebagai penyimpanan data dan pembuatan grafik. Cacti menyediakan pengumpulan data yang cepat, pola grafik advanced, metoda perolehan multiple data, dan fitur pengelolaan user. Semuanya dikemas secara intuitif, sebuah interface yang mudah digunakan mudah dipahami untuk local area network hingga network yang kompleks dengan ratusan device. Dengan menggunakan cacti kita dapat memonitor trafik yang mengalir pada sebuah server.

Cacti dapat kita gambarkan sebagai :

### a. Data Retrieval

Hal pertama yang dilakukan oleh Cacti adalah mengumpulkan data. Data dikumpulkan dengan Poller yang dieksekusi oleh Operating System. Interval pengumpulan data atau dengan kata lain eksekusi Poller dapat kita atur melalui fasilitas penjadwalan yang tersedia di Operating System seperti crontab.

### b. Data Storage

Data yang telah dikumpulkan oleh Poller, selanjutnya akan disimpan secara teratur di bawah /rra. Untuk proses ini, cacti menggunakan Round Robin Database (RRD) dimana data akan ditata dalam urutan waktu (time-series). Data yang dapat berupa trafik jaringan, suhu mesin, server load average, mounting load dan lainnya berbentuk file berekstensi .rra dan selanjutnya siap dipresentasikan dalam bentuk grafik.



### **c. Data Presentation**

Keutamaan penggunaan RRDtool adalah fungsi grafiknya. Data-data yang tertata dalam /rra akan di presentasikan dalam grafik dan ditampilkan oleh webserver yang kita gunakan. Cacti juga menyediakan halaman pengaturan grafik untuk memudahkan kita memanajemen gambar-gambar yang ingin kita tampilkan serta cara menampilkannya.