

SIMPLE NETWORK MANAGEMENT PROTOCOL UNTUK PEMANTAUAN JARINGAN DENGAN PELAPORAN SMS

Wawan Indarto, Zainudin Zuhri, Sofyan Wijaya

Laboratorium Sistem dan Jaringan Komputer

Jurusan Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia

Jln. Kaliurang KM 14,5 Yogyakarta 55501, Telp. (0274) 895287 ext: 143, Faks. (0274) 895007

Email: wawan@fti.uui.ac.id, zainudin@fti.uui.ac.id, sofyan@uui.net.id

Abstrak

Healthy, Availability, 99 % Uptime, Konektifitas, dan Keamanan jaringan menjadi keadaan yang seharusnya terus menerus terjadi, untuk itu penanganan secara terpusat, terpadu, cepat, dan akurat harus bisa dilakukan untuk menjaga keadaan diatas.

Simple Network Management Protocol digunakan untuk pengelolaan dan pemantauan sistem komputer yang terhubung ke dalam jaringan. Hampir semua peralatan jaringan yang ada saat ini mendukung penggunaan SNMP untuk pemantauannya.

Dengan penggunaan SNMP memberikan akses ke manajemen jaringan menjadi lebih mudah untuk dikerjakan. Komponen Agent dalam SNMP menyajikan data keadaan sistem secara real time dan komponen Manger memberikan mekanisme pengambilan data. Tetapi dalam penggunaannya secara mentah sulit dilakukan dan tidak efisien, sehingga membutuhkan aplikasi perantara untuk mengakses SNMP.

Penerapan arsitektur aplikasi berbasis web memberikan solusi terpusat dan terpadu dan pelaporan melalui sms menyuguhkan informasi yang cepat ke administrator jaringan untuk segera dapat menangani kegagalan yang terjadi pada jaringan.

Aplikasi dibuat menggunakan Framework PHP Pear dan Adodb yang memberikan abstraksi pembangun antarmuka dan pengaksesan basis data menjadi lebih mudah, PHP SNMP memberikan metode pengaksesan langsung ke Agent SNMP pada setiap node host yang dipantau, MySQL dengan Innodb untuk menjaga integritas basis data, XML memberikan mekanisme query informasi tambahan, Cron Daemon untuk melakukan proses pengecekan terjadwal dan digunakan modem gsm untuk pelaporan berbasis sms yang cepat.

Studi kasus diimplementasikan pada jaringan FTI UII dengan NOC berada di Laboratorium Sistem dan Jaringan Komputer Informatika dan juga diterapkan di NOC UIINET.

Kata Kunci: NMS, NMSS, Network Monitoring System, PHP, SNMP

1 Pendahuluan

1.1 Latar Belakang

Sebuah institusi yang besar terutama institusi yang tulang punggung eksistensinya menggunakan teknologi informasi membutuhkan penanganan yang baik agar sistem yang ada dapat terus berjalan dengan optimal. Teknologi informasi yang banyak digunakan menggunakan sistem jaringan komputer, semakin besar sebuah institusi yang menggunakan jaringan komputer, maka akan semakin besar dan kompleks pula sistem jaringan komputer yang ada pada institusi tersebut. Dengan semakin kompleks dan besarnya sistem tersebut membuat pemantauan dan pemeliharaan sistem jaringan tersebut menjadi sesuatu yang vital karena dengan semakin kompleksnya jaringan komputer maka semakin tinggi resiko kegagalan jaringan. Dalam pemantauan jaringan yang besar untuk menjaga eksistensi jaringan tentu saja menjadi sangat rumit sehingga dibutuhkan suatu mekanisme penanganan yang cepat dan terpusat.

Ketersediaan Hubungan atau *availability of connection* setiap saat merupakan sebuah *goal* yang harus dicapai. Untuk itu, seorang administrator jaringan dituntut untuk mengetahui kondisi kesehatan dari jaringannya secepat mungkin,

sebelum para pengguna jaringan mengetahui adanya masalah seperti *connection down*, trafik yang tinggi, dan sebagainya.

1.2 Rumusan Masalah

- Bagaimanakah cara menangani pemantauan dan pemeliharaan secara terpadu?
- Dapatkah dilakukan pemantauan terhadap penggunaan trafik jaringan pada perangkat-perangkat yang terhubung di jaringan?
- Dapatkah dilakukan pemantauan beberapa service lain seperti contohnya keadaan memori pada komputer server?
- Dapatkah dilakukan pelaporan otomatis melalui sms jika ada service yang mati atau bekerja tidak dalam keadaan normal di perangkat-perangkat yang terhubung di jaringan tersebut?

1.3 Batasan Masalah

- Perangkat-perangkat yang dipantau adalah yang terhubung di jaringan.
- Pemantauan service dibatasi pada penggunaan trafik jaringan, pemakaian tempat penyimpanan, pemakaian memori, dan service lain yang berbasis jaringan

- c. Dilakukan laporan melalui sms untuk critical error pada high priority service.

1.4 Tujuan Penelitian

Tujuan akhir yang akan dicapai dalam penelitian ini adalah untuk membantu seorang administrator jaringan dalam mengelola jaringan dan mencari informasi yang dibutuhkannya secara cepat, tepat, dan akurat. Selain itu juga dengan adanya pelaporan melalui sms diharapkan keadaan jaringan yang bersifat *high priority* dapat segera diketahui oleh *group* administrator yang sedang tidak berada di tempat.

1.5 Manfaat Penelitian

Manfaat yang diperoleh bagi perusahaan, institusi, dan khususnya yang menggunakan system ini adalah sebagai pertimbangan dan perbandingan dengan sistem pemantauan yang sudah ada dan jika belum ada dapat menggunakan sistem ini.

Manfaat yang dapat diambil dari penelitian ini bagi para pengembang atau developer sistem jaringan dapat sebagai contoh acuan untuk mengembangkan sistem yang terintegrasi yang didalamnya mengandung fungsi untuk menyajikan informasi jaringan yang didapat langsung dari web dengan *request* dari administrator dan terintegrasi dengan modul sms yang memberikan informasi kepada *group* administrator yang sedang tidak berada di tempat dan tidak melakukan *request*.

1.6 Hipotesis

Berdasarkan dugaan dapat diambil kesimpulan awal atau hipotesis yaitu dengan pengimplementasian sistem ini pada suatu jaringan maka kondisi jaringan dapat segera diketahui oleh *group* administrator.

1.7 Metodologi Penelitian

Beberapa metode-metode yang digunakan untuk menyelesaikan penelitian ini adalah sebagai berikut:

1.7.1 Metode Pengumpulan data

Metode pengumpulan data yang dipakai adalah menggunakan landasan literatur dengan mempelajari teori-teori yang berhubungan dengan sistem manajemen jaringan dan literatur-literatur lain yang dapat membantu dalam memecahkan masalah yang ada serta dengan melakukan konsultasi secara berkesinambungan dengan dosen pembimbing.

1.8 Metode Analisis

Metode yang digunakan untuk analisis kebutuhan yaitu menggunakan analisis berarah-struktur data dan desain sistem menggunakan Diagram Alir Data (*Data Flow Diagram*).

1.9 Tahapan pengembangan perangkat lunak

Metode pengembangan perangkat lunak disusun berdasarkan hasil dari yang sudah diperoleh, meliputi:

- a. Analisis Data. Pada tahap ini dilakukan pengolahan data yang diperoleh dan mengelompokkannya sesuai dengan kebutuhan sistem yang akan dibangun.
- b. Desain Sistem. Pada tahap ini dilakukan penerjemahan kebutuhan data yang dibutuhkan ke dalam bentuk yang sistematis dan mudah dimengerti yaitu dalam bentuk diagram.
- c. Pengkodean. Pada tahap ini dilakukan penerjemahan diagram ke dalam bahasa komputer yang telah ditentukan
- d. Pengujian. Tahap ini dilakukan setelah selesai pembuatan / pengkodean sistem, untuk melihat sejauh mana aplikasi yang telah dibuat sesuai dengan yang dikehendaki.

2 Landasan Teori

2.1 TCP/IP

TCP/IP merupakan protokol jaringan komputer terbuka dan bisa terhubung dengan berbagai jenis perangkat keras dan lunak. TCP terdiri beberapa *layer* atau lapisan yang memiliki fungsi tertentu dalam komunikasi data. Setiap fungsi dari *layer* selain dapat bekerjasama dengan *layer* pada tingkat lebih rendah atau lebih tinggi, juga bisa berkomunikasi dengan *layer* sejenis pada *remote host* (*peering*). IP adalah jantung TCP/IP memiliki peran sebagai pembawa data yang *independent*. Semua dokumen TCP/IP dalam bentuk public document IEN dan RFC. IP dibagi atas kelas network A,B, dan C. Sedangkan kelas D untuk keperluan reverse IP yang boleh diabaikan. IP ditulis dalam bilangan desimal dari 0 sampai 255. Data yang mengalir antar *layer* atau antar *host* dienkapsulasi dan diberi *header* agar tiap *layer* bisa memprosesnya. Sebuah *host* tidak tahu alamat IP gateway di network lain, tetapi data mengalir ke *host* tujuan di network lain melalui gateway networknya setelah diberi penentuan *routing* alamat IP.

TCP singkatan dari transfer control protocol dan IP singkatan dari Internet Protocol. TCP/IP menjadi satu nama karena fungsinya selalu bergandengan satu sama lain dalam komunikasi data. TCP/IP saat ini dipergunakan dalam banyak jaringan komputer lokal (LAN) yang terhubung ke Internet.

2.1.1 Sifat TCP/IP

Merupakan protokol standar yang terbuka, gratis dan dikembangkan terpisah dari perangkat keras komputer tertentu. Karena itu protokol ini banyak didukung oleh vendor perangkat keras, sehingga TCP/IP merupakan pemersatu perangkat keras komputer yang beragam merk begitu juga sebagai pemersatu berbagai perangkat lunak yang beragam merk sehingga walau anda memakai

perangkat keras dan perangkat lunak komputer yang berlainan dengan teman anda pada jaringan komputer berbeda, anda dan teman anda dapat berkomunikasi data melalui Internet.

Berdiri sendiri dari perangkat keras jaringan apapun. Sifat ini memungkinkan TCP/IP bergabung dengan banyak jaringan komputer. TCP/IP bisa beroperasi melalui sebuah *Ethernet*, sebuah *token ring*, sebuah saluran dial-up, sebuah X-25 dan secara *virtual* melalui berbagai media fisik transmisi data.

Bisa dijadikan alamat umum sehingga tiap perangkat yang memakai TCP/IP akan memiliki sebuah alamat unik dalam sebuah jaringan komputer lokal, atau dalam jaringan komputer global seperti Internet.

Protokol ini distandarisasi dengan skala tinggi secara konsisten, dan bisa memberikan *service* kepada pengguna-pengguna di dunia.

2.1.2 Arsitektur Protokol TCP/IP

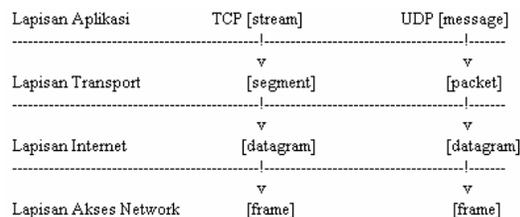
Karena belum ada standarisasi model OSI, maka TCP/IP yang berkembang kemudian adalah berupa protokol dengan tiga sampai lima lapis fungsi saja. Berikut contoh arsitektur protokol TCP/IP empat lapis:

1. Lapisan aplikasi, terdiri dari aplikasi dan proses yang memakai jaringan
2. Lapisan transportasi data *host* ke *host*, membuat *service* pengiriman data antar komputer (*end-to-end*)
3. Lapisan Internet, menentukan datagram dan pengatur (*handle*) *routing* data
4. Lapisan Akses Jaringan (*network access layer*), terdiri dari *routing* untuk mengakses jaringan fisik.

Seperti model OSI, pada proses pengiriman data, data dalam sebuah komputer akan didorong melalui lapisan-lapisan itu (*stack*) dari lapisan aplikasi sampai lapisan akses jaringan sehingga terkirim melalui sarana komunikasi data dan diterima oleh komputer yang jauh. Oleh komputer yang jauh, data diterima dan kemudian didorong dari lapisan akses jaringan ke lapisan aplikasi. Setelah diterima oleh lapisan aplikasi barulah data bisa ditampilkan di layar monitor untuk diakses oleh usernya.

Dalam setiap layer diatas, ditambahkan informasi kontrol untuk memastikan pengiriman/penerimaan data berjalan baik. Informasi kontrol ini disebut sebuah header, sebab ini ditempatkan didepan data yang dikirimkan. Pada setiap lapisan itu, setiap header akan selalu ditempatkan dibagian depan data. Penambahan informasi terhadap data pada proses pengiriman/penerimaan data ini disebut enkapsulasi (*encapsulation*).

Struktur data yang melalui lapisan protokol TCP/IP di atas bisa digambarkan dalam contoh ini:



Gambar 2.1 Lapisan TCP/IP

Pada gambar ini aplikasi mempergunakan TCP adalah data *stream*, sedangkan aplikasi memakai UDP (*Using Datagram Protocol*) berupa data *message*. Pada lapisan *transport*, TCP menyebut data sebagai *segment*. Sedangkan UDP menyebut data sebagai *packet*. Di lapisan Internet, semua data dilihat sebagai blok data yang disebut datagram. Kemudian pada lapisan akses jaringan setiap potongan data yang dikirim disebut *frame*.

TCP/IP memakai banyak cara ketika mengirimkan data ke tiap lapisan. Setiap cara juga akan memberikan nama data yang akan dikirim jadi berbeda. Banyak jaringan komputer yang mendasarkan pengiriman datanya kepada data sebagai *packet* atau *frame*. Dalam contoh diatas dipilih data yang dikirim adalah data *frame*.

2.2 Simple Network Management Protocol

Ketika jumlah jaringan dalam sebuah Organisasi semakin besar, dengan perangkat yang semakin banyak dan berbeda-beda dari berbagai vendor, maka saat itulah dibutuhkan sebuah kerangka manajemen jaringan yang standar agar tiap komponen yang berbeda dapat berkomunikasi dalam satu manajemen yang sama. Manajemen jaringan TCP/IP terdiri atas stasiun manajemen yang berkomunikasi dengan elemen-elemen jaringan. Elemen jaringan ini bisa berupa *host*, *router*, *printer*, dan sebagainya. Sedangkan stasiun manajemen biasanya berupa workstation dengan monitor berwarna dan grafis, yang menampilkan status elemen yang dipantaunya.

Untuk menjalankan aktifitas pemantauan tersebut, antara *manager* dan elemen-elemen jaringan yang dipantau harus ada komunikasi. Ada dua arah komunikasi, pertama, *manager* bertanya kepada elemen jaringan misalnya "berapa jumlah paket yang masuk ke *interface* eth0?". Kedua, elemen jaringan yang memberitahu *manager* adanya kejadian penting seperti "*interface* eth0 mati!". Selanjutnya stasiun manajemen akan menampilkan status *interface* tersebut di layarnya. Dengan cara seperti ini, seorang administrator jaringan dapat segera mengetahui adanya kegagalan dalam jaringannya.

Dalam jaringan TCP/IP, protokol aplikasi yang menangani soal manajemen jaringan ini adalah SNMP singkatan dari Simple Network management Protocol.

2.2.1 Definisi SNMP

Secara sederhana, SNMP merupakan sebuah protokol yang didesain untuk memberikan kemampuan kepada pemakai untuk mengelola jaringan komputernya dari jarak jauh atau remote. Pengelolaan ini dilaksanakan dengan cara melakukan polling dan setting variabel-variabel elemen jaringan yang dikelolanya.

2.2.2 Elemen SNMP

MIB atau Management Information Base, bisa dikatakan sebagai struktur database variabel elemen yang dikelola. Struktur ini bersifat hierarki dan memiliki aturan sedemikian rupa sehingga informasi nilai setiap variabel dapat diketahui atau diset dengan mudah.

1. MIB

MIB atau *Management Information Base* sebagai struktur database variabel elemen jaringan yang dikelola. Struktur ini bersifat hierarki dan memiliki aturan sedemikian rupa sehingga informasi nilai setiap variabel dapat diketahui atau diset dengan mudah

2. Agent

Agent merupakan software yang dijalankan di setiap node atau elemen jaringan yang akan dipantau. Tugasnya adalah Mengumpulkan seluruh informasi yang telah ditentukan dalam MIB.

3. Manajer

Manager merupakan software yang berjalan di sebuah *host* di jaringan. Manajer ini bertugas Mengumpulkan informasi dari *agent-agent*. Tidak semua informasi yang dimiliki oleh *agent* diminta oleh *manager*. Informasi-informasi yang diminta oleh administrator jaringan, yang menjalankan *host* yang berfungsi sebagai *manager* saja yang akan dikumpulkan dari *agent*.

2.2.3 Protokol SNMP

SNMP didesain oleh IETF untuk pemakaian di Internet. Saat ini SNMP didesain di atas protokol UDP (User Datagram Protokol) seperti pada gambar 2.2.

Aplikasi Manajemen Jaringan
Agent
SNMP
UDP
IP
Lapisan Bawah

Gambar 2.2 Lapisan-lapisan SNMP

Karena menggunakan protokol UDP, SNMP adalah protokol yang *connectionless*. Tidak ada jaminan lalu lintas manajemen diterima oleh entitas lain dengan sempurna. Dengan protokol ini, overhead proses dapat dikurangi dan diperoleh kesederhanaan. Jika reliabilitas dan accountabilitas yang diperlukan, *manager* jaringan harus membangun operasi yang *connection oriented* pada aplikasi di lapisan atasnya.

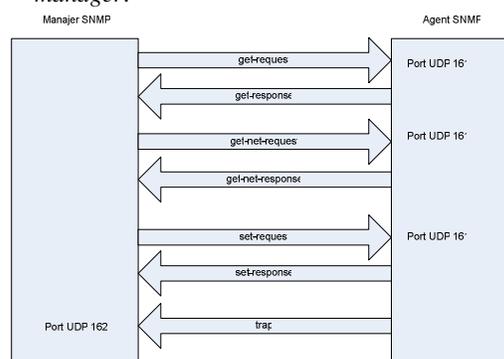
SNMP ini bekerja secara sederhana. Manajer dan *agent* saling berkiriman pesan berupa permintaan *manager* dan jawaban dari *agent* tentang informasi jaringan. Pesan-pesan ini dibawa oleh paket-paket data yang disebut PDU (*Protocol Data Unit*).

2.2.4 PDU SNMP

PDU (*Protocol Data Unit*) merupakan unit data yang terdiri atas sebuah header dan beberapa data yang ditempelkan. Dilihat dari perspektif diatas, PDU ini dapat dilihat sebagai sebuah benda yang mengandung variabel-variabel. Variabel ini memiliki nama dan nilai.

Protokol SNMP menggunakan operasi yang relatif sederhana dan PDU dalam jumlah terbatas untuk menjalankan fungsinya. Lima PDU yang telah didefinisikan dalam standar adalah sebagai berikut :

1. *Get Request*: PDU ini digunakan untuk mengakses *agent* dan mendapatkan nilai dari daftar variabel yang diminta. PDU ini mengandung identifier yang membedakan dengan *multi request* ataupun nilai variabel (status elemen jaringan).
2. *Get-Next Request*: Seperti *Get Request*, tetapi memungkinkan pengambilan informasi pada logical identifier selanjutnya dalam MIB Tree secara berurutan.
3. *Get Response*: PDU ini untuk merespon unit data *Get Request*, *Get-Next Request*, dan *Set Request*, jadi dikeluarkan oleh *agent*.
4. *Set Request*: Dipakai untuk menjelaskan aksi yang harus dilaksanakan di elemen jaringan. Biasanya untuk mengubah nilai suatu daftar variabel.
5. *Trap*: PDU ini memungkinkan modul manajemen jaringan / *agent* memberi laporan tentang kejadian pada elemen jaringan kepada *manager*.



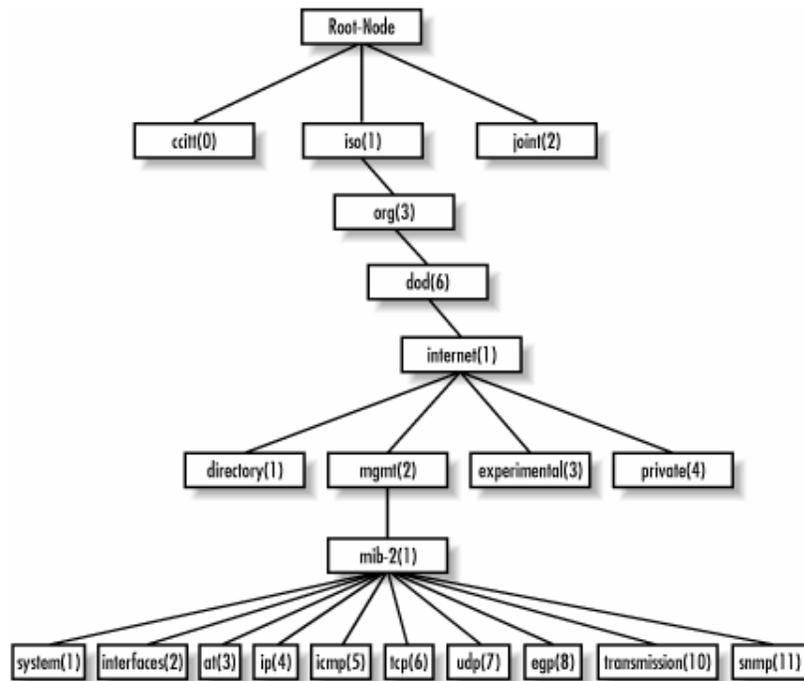
Gambar 2.3 Lima Operator SNMP

2.2.5 Struktur Informasi dalam SNMP

Informasi dalam SNMP disimpan dalam bentuk variabel-variabel yang didefinisikan dalam MIB, dan masing-masing variabel tersebut memiliki tipe-tipe data tertentu, antara lain adalah integer, octet string, display string, object identifier, null, dan sequence of.

MIB dalam SNMP dapat digambarkan sebagai sebuah pohon abstrak yang memiliki sebuah akar. Kar ini tidak punya nama. Item-item data secara individual membentuk daun-daunnya. *Object Identifier* atau ID mengidentifikasi atau memberi nama objek-objek dalam pohon MIB. Struktur ID objek MIB mendefinisikan tiga Cabang utama:

Consultative Committee for International Telegraph and Telephone (CCITT), *International Organization for Standardization (ISO)*, dan *joint-ISO-CCITT*. Sebagian besar aktifitas MIB saat ini merupakan bagian dari Cabang ISO yang didefinisikan oleh ID 1.3.6.1 dan dikhususkan untuk komunitas internet. Pohon MIB sebagai berikut:



Gambar 2.4 Pohon MIB

2.2.6 Identifikasi Kejadian

Setiap variabel dalam MIB harus diidentifikasi ketika SNMP akan merujuk kepadanya, mengambil atau mengeset nilainya. Hanya node daun yang akan dirujuk. SNMP tidak akan memanipulasi semua baris atau kolom dalam tabel. Ada tiga macam identifikasi kejadian yaitu Variabel Sederhana, Tabel dan Urutan Lexicographic.

3 Analisa Kebutuhan

3.1 Analisis Masalah

Masalah yang dimunculkan pada kasus ini adalah terdapatnya kendala pada pemantauan jaringan yang tidak terpusat dan tidak efisien dan dapat ditarik menjadi poin-poin sebagai berikut:

1. Penanganan pemantauan jaringan kebanyakan dilakukan secara manual dan tidak terpusat
2. Seorang administrator tidak segera mengetahui permasalahan yang terjadi di jaringan jika dia tidak sedang aktif
3. Seorang Manajer Jaringan tidak segera mendapat laporan mengenai permasalahan yang terjadi
4. Lambatnya proses penanganan permasalahan yang terjadi

3.2 Hasil Analisis

Hasil analisis dari sistem yang diharapkan sebagai berikut:

3.2.1 Gambaran Umum Sistem

Secara garis besar, sistem yang akan diwujudkan nantinya menangani pemantauan jaringan secara terpusat melalui satu tempat dan dapat memberitahu kepada Administrator dan Manajer tanpa ada permintaan dahulu sehingga administrator tidak perlu aktif melakukan pemantauan, begitu juga dengan Manajer.

Dikarenakan keinginan untuk memusatkan sistem pemantauan dan memudahkan seorang administrator untuk pengelolaan walaupun secara remote (jarak jauh) maka sistem under web (berjalan di browser) adalah pemilihan yang tepat, dan dengan pengiriman menggunakan sms untuk pemberitahuan segera ke administrator dan ke Manajer adalah langkah yang tepat.

3.2.2 Kebutuhan Perangkat Lunak

Perangkat lunak yang digunakan untuk mendukung sistem yang akan dibangun diharapkan dapat memenuhi kebutuhan-kebutuhan antara lain:

- a. Mampu mengirimkan laporan ke Manajer dan admin. Laporan yang dibuat bisa dilaporkan ke email dan hp Manajer atau admin.
- b. Mampu melakukan proses terjadwal untuk pengecekan keadaan jaringan
- c. Dapat melayani permintaan akses melalui web
- d. Dapat menyimpan data sistem pemantauan.

3.2.3 Kebutuhan Perangkat Keras

Perangkat keras yang digunakan untuk penempatan sistem pemantauan diharapkan memenuhi kebutuhan-kebutuhan antara lain:

1. Dapat terhubung ke jaringan inti
2. Dapat hidup secara terus menerus (*uptime* 99%)
3. Dapat melakukan proses pemantauan
4. Dapat mengirimkan laporan secara langsung ke Manajer dan Administrator jaringan dengan peralatan tambahan
5. Untuk masing-masing *host* yang dipantai, dapat mengirimkan keadaan *host* tersebut ke sistem pemantauan.

3.2.4 Analisa Kebutuhan Masukan

Sistem yang dibangun membutuhkan masukan-masukan sebagai berikut:

1. Data *Host-host* yang terdaftar dan mau dipantau
2. Data Administrator dan Manajer.
Data Administrator dan Manajer lengkap dengan alamat yang bisa digunakan untuk melaporkan tentang keadaan jaringan.
3. Data keadaan jaringan
Berupa data-data keadaan *host* tiap-tiap *host* yang berada di jaringan yang nantinya dipantau oleh sistem pemantauan.
4. Batasan keadaan normal jaringan
Batasan keadaan yang diperbolehkan dalam keadaan normal.

3.2.5 Analisa Kebutuhan Keluaran

- a. Laporan kegagalan Jaringan
Laporan yang bersifat langsung berupa keadaan tidak normal yang terjadi di jaringan. Bersifat aktif, artinya walaupun seorang administrator tidak sedang mengaksesnya maka tetap diberi laporan.
- b. Informasi keadaan normal dan keadaan tidak normal (kegagalan) jaringan
Informasi total keadaan jaringan baik yang normal maupun tidak normal dan dapat diakses secara langsung. Bersifat pasif, artinya jika seorang administrator tidak mengaksesnya maka tidak akan disugahi.

3.2.6 Fungsionalitas yang dikehendaki

Diharapkan sistem yang dibangun mampu memantau keadaan jaringan dan melaporkan

kegagalan yang terjadi ke group Administrator dan Manajer, sehingga administrator dapat segera mengetahui sumber kegagalan dan dapat segera membetulkan keadaan.

3.2.7 Kinerja yang harus dipenuhi

Diharapkan sistem dapat bekerja tanpa campur tangan manusia, secara aktif dan berkala memantau jaringan.

3.2.8 Antarmuka yang diinginkan

Mampu menyuguhkan informasi yang mudah dibaca oleh administrator, dan Administrator sendiri mudah dapat mengelola sistem pemantauan yang ada. Dengan antarmuka berbasis web akan mempermudah administrator untuk mengelola sistem secara *remote* darimanapun selama terhubung di jaringan inti dan dapat menggunakan sistem operasi apapun karena diakses menggunakan browser.

4 Perancangan

4.1 Diagram Arus Data

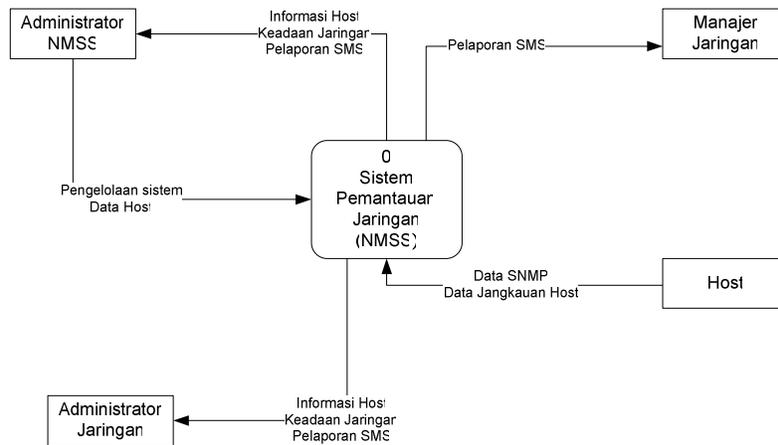
Penggunaan notasi dalam diagram arus data sangat membantu sekali untuk memahami suatu sistem pada semua tingkat kompleksitasnya. Pada tahap analisis, penggunaan notasi ini sangat membantu sekali di dalam komunikasi dengan pemakai sistem untuk memahami sistem secara logika. Diagram yang menggunakan notasi-notasi ini untuk menggambarkan arus dari data sistem dikenal dengan nama diagram arus data (*Data Flow Diagram* atau DFD) [JOG01].

Pada Sistem Pemantauan Jaringan ini dapat digambarkan aliran data dibawah ini, yang memiliki entitas luar yang akan memberikan input atau menerima output dari sistem. Pembuatan DFD berikut mengacu metode *Gane-Sarson*.

Entitas luar pada sistem pemantauan ini adalah:

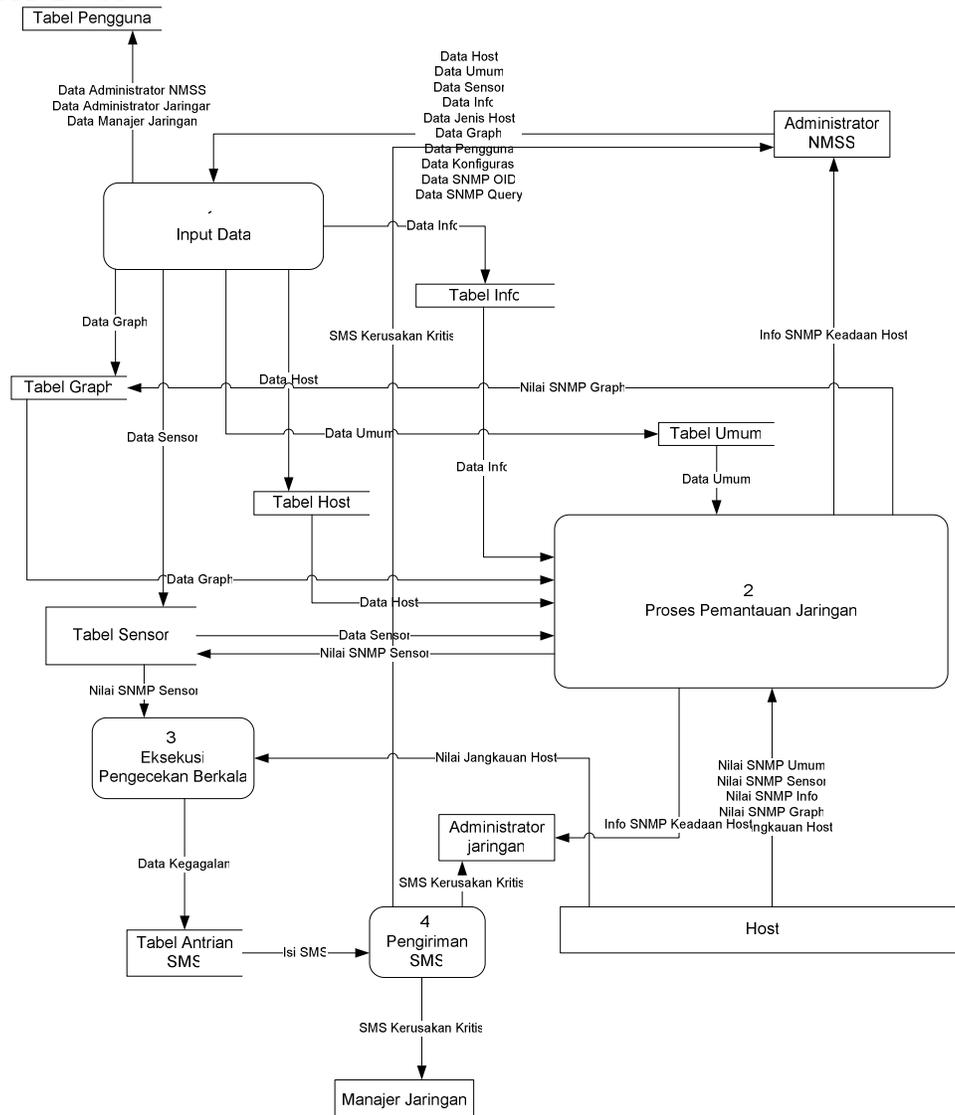
1. Administrator Jaringan
Pengeinputan data-data *host*, pengelolaan sistem, menerima informasi keadaan jaringan, dan menerima pelaporan sms tentang keadaan jaringan yang bersifat kritis
2. Manajer Jaringan
Menerima informasi keadaan jaringan, dan menerima pelaporan sms tentang keadaan jaringan yang bersifat kritis
3. Host/SNMP Enable Device
Mengirimkan data-data SNMP sesuai yang diminta oleh sistem.

4.1.1 DFD Level 0



Gambar 4.1 DFD Level 0

4.1.2 DFD Level 1



Gambar 4.2 DFD Level 1

4.2 Struktur Tabel dalam Basis Data

4.2.1 Daftar tabel

a. host

Daftar *Host* atau *Device* atau komputer atau router (snmp enable device) yang dipantau.

Tabel 4.1 Struktur Tabel Host

Field	Type	Null	Deflt	Links to
kode_host	varchar(50)	No	0	
ip	varchar(20)	Yes	NULL	
komuniti	varchar(30)	Yes	NULL	
snmp_versi	tinyint(1)	No	1	
snmp_pengguna	varchar(50)	Yes	NULL	
snmp_kunci	varchar(50)	Yes	NULL	
snmp_port	mediumint(5)	No	161	
snmp_timeout	mediumint(8)	No	500	
jenis_id	varchar(50)	Yes	NULL	jenis -> id
enable	set('on', 'off')	Yes	on	

Dengan konstrain

- jenis_id refer ke id pada tabel jenis

b. sensor

Sensor-sensor yang diinstall pada masing-masing *host*, dan digunakan untuk melaporkan ke Manajer dan Administrator.

Tabel 4.2 Struktur Tabel Sensor

Field	Type	Null	Deflt	Links to
id	int(11)	No		
kode_host	varchar(50)	No	0	host -> kode_host
snmp_oid_id	int(11)	No	0	snmp_oid -> id
nilai	varchar(50)	Yes	NULL	
nilaimaks	varchar(50)	Yes	NULL	
nilaimin	varchar(50)	Yes	NULL	
enable	set('on', 'off')	Yes	on	

Dengan konstrain:

- kode_host refer ke kode_host pada tabel host
- snmp_oid_id ke id pada tabel snmp_oid

c. info

Informasi snmp tambahan yang disajikan di sistem dan tidak dilaporkan, disajikan berdasarkan jenis host.

Tabel 4.3 Struktur Tabel Info

Field	Type	Null	Deflt	Links to
id	int(11)	No		
jenis_id	varchar(50)	No		jenis -> id
snmp_query_id	mediumint(8)	No	1	snmp_query -> id

Dengan konstrain:

- jenis_id refer ke id pada tabel jenis
- snmp_query_id ke id pada tabel snmp_query

d. jenis

Tipe-tipe device yang dipantau. Sebagai acuan penggunaan sensor dan sebagai acuan pemberian informasi tambahan.

Tabel 4.4 Struktur Tabel Jenis

Field	Type	Null	Deflt	Links to
id	varchar(50)	No		
Nama	varchar(100)	Yes	NULL	

e. umum

Informasi umum yang tidak bergantung pada jenis device.

Tabel 4.5 Struktur Tabel Umum

Field	Type	Null	Deflt	Links to
kode_umum	int(11)	No		
fungsioid	varchar(50)	No		
nama	varchar(50)	Yes	NULL	
deskripsi	varchar(100)	Yes	NULL	

f. konfig

Penyimpanan konfigurasi program.

Tabel 4.6 Struktur Tabel Konfig

Field	Type	Null	Deflt	Links to
var	varchar(20)	No		
isi	varchar(50)	No		

g. laporan

Sejarah laporan yang dikirimkan ke administrator dan Manajer.

Tabel 4.7 Struktur Tabel Laporan

Field	Type	Null	Deflt	Links to
kode_laporan	int(11)	No		
waktu	datetime	Yes	NULL	
isi	text	Yes	NULL	

h. pengguna

Daftar administrator sistem dan Manajer.

Tabel 4.8 Struktur Tabel Pengguna

Field	Type	Null	Deflt	Links to
kode_pengguna	varchar(20)	No		
nama	varchar(50)	Yes	NULL	
kunci	varchar(50)	No		
hp	varchar(20)	No		
email	varchar(50)	Yes	NULL	
enable	set('on', 'off')	Yes	on	

i. snmp_oid

Daftar Pustaka SNMP yang bisa digunakan untuk membuat sensor.

Tabel 4.9 Struktur Tabel snmp_oid

Field	Type	Null	Deflt	Links to
id	int(11)	No		
oid	varchar(100)	No		
nama	varchar(100)	No		
satuan	varchar(50)	No		
jenis_id	varchar(50)	No		jenis -> id

j. snmp_query

Daftar Pustaka Query SNMP yang bisa digunakan untuk menyajikan informasi tambahan, terhubung ke file XML yang berisi query snmp.

Tabel 4.10 Struktur Tabel snmp_query

Field	Type	Null	Deflt	Links to
id	mediumint(8)	No		
hash	varchar(32)	No		
xml_path	varchar(255)	No		
name	varchar(100)	No		
description	varchar(255)	Yes	NULL	
graph_template_id	mediumint(8)	No	0	
data_input_id	mediumint(8)	No	0	

k. host_snmp_query

Daftar index untuk menampilkan informasi yang disajikan pada *host*.

Tabel 4.11 Struktur Tabel host_snmp_query

Field	Type	Null	Deflt	Links to
host_id	varchar(50)	No	0	host -> kode_host
snmp_query_id	mediumint(8)	No	0	snmp_query -> id
sort_field	varchar(50)	No		
title_format	varchar(50)	No		
reindex_method	tinyint(3)	No	0	

Dengan konstrain:

- host_id ke kode_host pada tabel host
- snmp_query_id ke id pada query_id

l. host_snmp_cache

Daftar informasi snmp yang berhasil di ambil oleh sistem

Tabel 4.12 Struktur Tabel host_snmp_cache

Field	Type	Null	Deflt	Links to
host_id	varchar(50)	No	0	host -> kode_host
snmp_query_id	mediumint(8)	No	0	snmp_query -> id
field_name	varchar(50)	No		
field_value	varchar(255)	Yes	NULL	
snmp_index	varchar(100)	No		
oid	varchar(255)	No		

Dengan konstrain :

- host_id ke kode_host pada tabel host
- snmp_query_id ke id pada tabel snmp_query

m. graph

Daftar graph statistik yang ditampilkan per

host

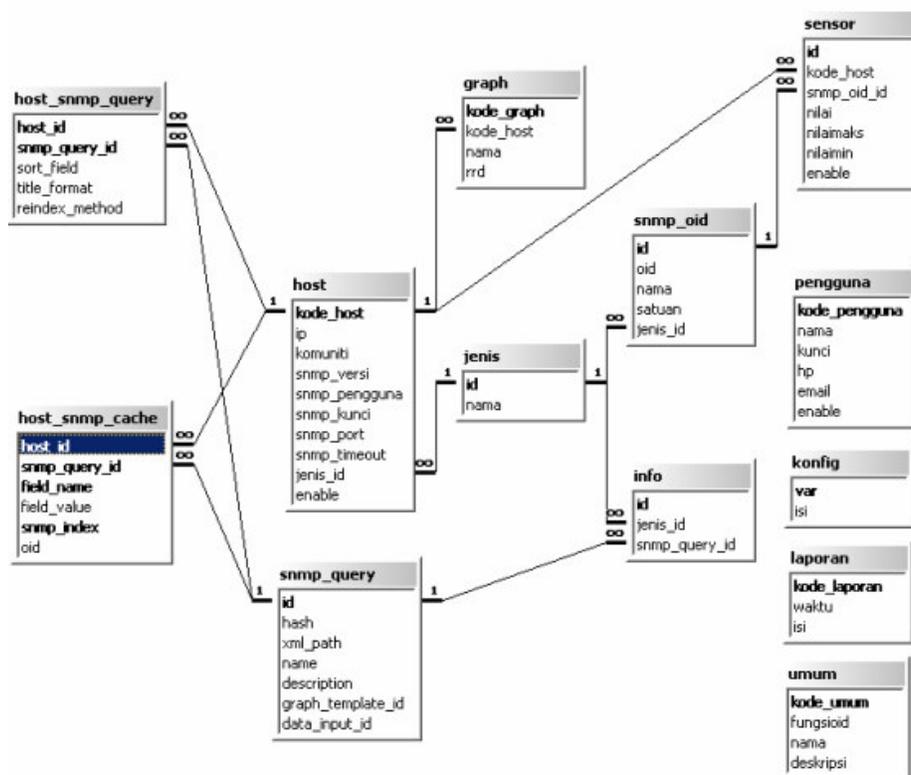
Tabel 4.13 Struktur Tabel graph

Field	Type	Null	Deflt	Links to
kode_graph	int(11)	No		
kode_host	varchar(50)	No	0	host -> kode_host
nama	varchar(50)	No		
rrd	varchar(100)	No		

Dengan konstrain :

- kode_host ke kode_host pada tabel host

4.2.2 Relasi Antar Tabel



Gambar 4.3 Relasi antar tabel

Keterangan:

1. Field dengan huruf tebal adalah Key Field
2. tanda 1 pada garis relasi berarti hubungan 1
3. tanda ∞ pada garis relasi berarti Hubungan banyak

5 Implementasi

5.1 Batasan Implementasi

5.1.1 Asumsi yang dipakai

Dalam tahap implementasi digunakan asumsi-asumsi sebagai berikut:

- Jaringan yang akan dipantau mendukung protokol SNMP
- Komputer yang digunakan terhubung ke jaringan inti
- Menggunakan sistem operasi Windows untuk pemantauan secara remote dan Linux Fedora Core 2 sebagai Server Pemantauan
- Jaringan inti lokal yaitu 192.168.0.0/26
- Server Pemantauan diberi alamat ip 192.168.0.31 dengan gateway 192.168.0.1 dan nameserver 192.168.0.1 dan diberi nama MRT14
- Seluruh Aplikasi Pendukung yang digunakan kecuali untuk developing (DreamWeaver dan Zend Studio) adalah Aplikasi Free dan Open Source.
- Aplikasi dan versi yang dipakai sebagai berikut : Apache-2.0.59, PHP-4.3.10
- File-file PHP diletakkan di /var/www/html/nmss
- Nama Database yang digunakan adalah nmss, nama user database adalah root dengan password q.

5.1.2 Lingkungan Pengembangan

Terdapat dua lingkungan pengembangan, yang pertama untuk pengembangan sistem itu sendiri dikembangkan di lingkungan Linux dan dikembangkan dengan remote access ke server. Kemudian untuk antarmuka dan desain menggunakan lingkungan Windows.

5.1.3 Bahasa dan Kompilator yang dipakai

Menggunakan bahasa PHP dengan didukung dengan framework Pear dan Adodb, tidak dibutuhkan kompilator dikarenakan bersifat interpreter. PHP akan diterjemahkan langsung menjadi HTML oleh server web dengan menggunakan Apache 2.

5.1.4 Perangkat Lunak yang digunakan

Untuk mewujudkan sistem yang akan dibangun dibutuhkan beberapa perangkat lunak pendukung, diantaranya:

- Sistem Operasi
Sistem Operasi yang digunakan untuk server sistem pemantauan jaringan ini adalah Linux Fedora Core 2. sedangkan untuk pengembangan antarmuka dan aplikasi PHP menggunakan sistem operasi windows 2000 dan XP.
- Server Web
Untuk server web menggunakan Apache 2 dengan modul PHP dan PHP snmp untuk akses data snmp. PHP dengan tambahan framework Pear dan Adodb.

- Server Basis Data
Server Basis Data menggunakan MySQL 4.1 dan dengan storage engine Innodb untuk menjaga integritas data
- Server Email
Server Email menggunakan Qmail untuk melakukan pengiriman laporan pemantauan jaringan melalui email
- Proses Terjadwal
Untuk melakukan pengecekan keadaan jaringan dan pengiriman laporan dibutuhkan proses terjadwal yang dilakukan secara otomatis oleh sistem. Untuk melakukan hal tersebut digunakan Crond Daemon pada sistem linux.
- Aplikasi Pengirim SMS
Untuk pengiriman laporan kegagalan jaringan melalui sms dibutuhkan sebuah sms server dan modem gsm atau menggunakan Aplikasi Agent SNMP di masing-masing *host* yang akan dipantau.
Perlu dilakukan instalasi snmp di masing-masing *host*, di linux bisa menggunakan net-snmp dan di windows menggunakan komponen snmp dari control panel. Untuk router tidak perlu install tinggal konfigurasi saja.
- Aplikasi untuk pengembangan perangkat lunak
Beberapa aplikasi untuk pengembangan yang digunakan antara lain adalah:
 - Macromedia Dreamweaver MX 2004. Digunakan untuk desain antarmuka dan edit html
 - Zend Studio Client. Digunakan untuk pengkodean php
 - phpmyadmin, mysqlfront, dan ems mysql manager. Digunakan untuk manajemen basis data.

5.1.5 Perangkat Keras yang digunakan

Untuk server pemantauan dibutuhkan perangkat keras sebagai berikut:

- Processor Intel Pentium II (Deschutes) 330 Mhz
- Memoy 128 MB
- Harddisk 20 GB
- Kartu Jaringan Realtek 8139

5.1.5.1 GSM Modem dan Kartu GSM

GSM Modem menggunakan Falcom A2D dan kartu GSM menggunakan Pro XL Bebas.

5.2 Implementasi

Secara garis besar implementasi sistem sebagai berikut:

- Mengkonfigurasi komputer dan modem gsm untuk persiapan pembangunan server pemantauan
- Membangun Web Server dan PHP untuk antarmuka aplikasi
- Membangun Database Server

4. Konfigurasi SNMP
5. Konfigurasi net-snmp di masing-masing komputer yang akan dilakukan pemantauan
6. Membangun Aplikasi bagian administrasi yang berfungsi untuk pengaturan sistem meliputi pengelolaan *host-host* atau node yang akan dipantau, pengaturan group administrator yang menerima pelaporan sms, dan pengelolaan administrator yang berhak mengakses sistem
7. Membangun Aplikasi bagian yang menyajikan informasi secara *realtime* dengan antarmuka web
8. Membangun Aplikasi bagian pelaporan sms.
Dengan rincian tahapan-tahapan sebagai berikut:

5.2.1 Konfigurasi Komputer dan Instalasi Sistem

Pada tahap awal yaitu mengkonfigurasi perangkat keras yang dibutuhkan dengan menambahkan Kartu Jaringan Realtek pada komputer dan menambahkan Modem GSM Falcom A2D. Dilanjutkan dengan instalasi Sistem Fedora Core 2 dengan pilihan instalasi minimum.

Komputer diberi konfigurasi jaringan sesuai dengan pada bagian asumsi. Setelah instalasi selesai dilakukan update sistem secara keseluruhan.

5.2.1.1 Instalasi dan Konfigurasi Firewall

Agar sistem aman dan terjaga dari serangan dibutuhkan sebuah firewall. Digunakan firewall iptables dengan bantuan aplikasi tambahan yaitu Advanced Policy Firewall (APF) yang dapat didownload di <http://rfxnetwork.net>.

5.2.2 Instalasi dan Konfigurasi Agen dan Aplikasi Pendukung

5.2.2.1 Agen

Beberapa server yang akan dipantau kebanyakan menggunakan sistem operasi linux sehingga perlu dilakukan Instalasi dan konfigurasi *agent* pada setiap router dan *host-host* yang akan dipantau.

5.2.2.1.1 Konfigurasi pada Router

Di router dalam hal ini adalah Cisco Router, telah terdapat fasilitas SNMP secara build in sehingga tidak diperlukan instalasi, hanya perlu melakukan konfigurasi dan pemberian hak akses.

5.2.2.1.2 Instalasi pada Konfigurasi pada Host/Server

Pad masing-masing server linux dibutuhkan instalasi program *agent* snmp, digunakan net-snmp.

5.2.2.2 Web Server, Database Server, dan GSM Modem

Setelah instalasi *agent* selesai, dilanjutkan dengan instalasi aplikasi pendukung pada server

pemantauan. Diantaranya adalah aplikasi Server Web, Basis Data, dan SMSTools GSM Modem.

Untuk instalasi server web lengkap dengan PHP, PHP Pear, PHP SNMP, Adodb dengan urutan sebagai berikut:

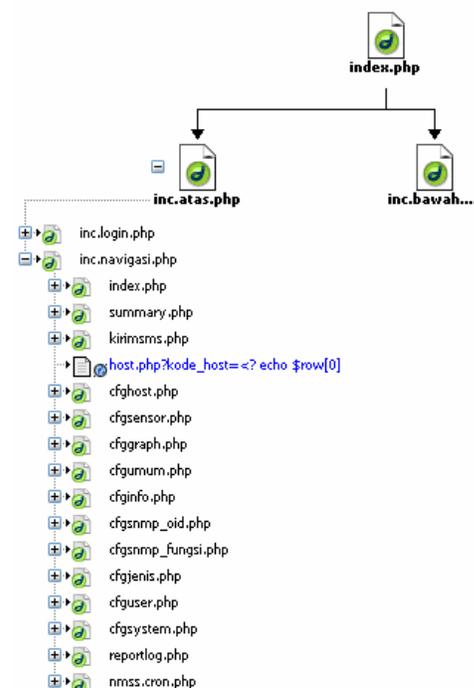
1. Instalasi Server Web Apache
2. Instalasi PHP, PHP Pear, dan PHP SNMP
3. Instalasi Modul Pear tambahan
4. Instalasi Adodb
5. Konfigurasi Apache dan PHP
6. Instalasi Server Basis Data MySQL
7. Konfigurasi MySQL dengan Innodb
8. Instalasi phpmysqladmin
9. Instalasi SMSTools

5.2.3 Pembangunan Server Pemantauan

Dalam pembangunan server pemantauan digunakan beberapa langkah dan metode sebagai berikut:

5.2.3.1 Peta Web/Aplikasi

Untuk membangun antarmuka dibutuhkan peta web sebagai berikut:



Gambar 5.1 Peta Web

5.2.3.2 Struktur antarmuka

Untuk memberikan struktur antarmuka yang fleksibel dan dinamis dilakukan pemisahan file-file yang terhubung misalnya file header, footer, navigasi, dan login terpisah. Sehingga untuk membuat sebuah content hanya dibutuhkan sebuah file dengan isi hanya content saja yang terhubung ke file-file include yang lain.

5.2.3.3 Konfigurasi

Di dalam konfigurasi disertakan variabel-variabel yang digunakan dan file-file library yang dibutuhkan seperti pear dan adodb.

5.2.3.4 Akses ke database

Untuk mengakses basis data digunakan framework PHP Pear dan Adodb.

5.2.3.5 Struktur File PHP

Setiap file content pada aplikasi yang dibuat terdiri dari 4 bagian inti yaitu:

1. Bagian atas berisi include file atas
2. Bagian program utama berisi option-option operasi program pada file tersebut dan pengecekan hak akses terhadap file tersebut
3. Bagian fungsi-fungsi berisi fungsi-fungsi untuk operasi pada file tersebut
4. Bagian bawah berisi include file bawah.

5.2.3.6 Mekanisme Login

Mekanisme login dapat digambarkan sebagai berikut

1. User menginputkan user id dan password pada login box
2. browser mengirimkan user id dan password terenkripsi md5
3. dengan menggunakan fungsi pada pear dicocokkan dengan user dan password terenkripsi pada basis data
4. jika benar buka sesi jika salah dibatalkan.

5.2.3.7 Add Edit Delete Data

Mekanisme add edit dan delete data dengan menggunakan masing-masing satu fungsi untuk

melakukan operasi data tersebut, hal ini untuk memudahkan develop ulang dan koreksi kesalahan dan memudahkan pengembangan lanjut sistem.

5.2.3.8 Pengaktifan dan Penonaktifan Laporan

Setiap *host* dan sensor terdapat field enable yang gunanya untuk mekanisme pelaporan dengan kondisi sebagai berikut:

1. Jika pada level *host* enable aktif maka sensor sensor yang aktif pada *host* tersebut akan dilaporkan jika mengenai konstrain kesalahan
2. Jika pada level *host* enable tidak aktif maka seluruh sensor pada *host* tersebut baik yang aktif maupun tidak aktif tidak akan dilaporkan
3. Jika pada level sensor enable aktif maka laporan diaktifkan untuk sensor tersebut dengan melihat aturan pada nomor 1 dan 2 diatas
4. Jika pada level sensor enable tidak aktif maka laporan tidak aktif untuk sensor tersebut
5. laporan pada web tidak menggunakan metode enable diatas, semua informasi akan disajikan walaupun enable tidak aktif baik pada *host* dan pada sensor.

5.2.3.9 Metode pengaksesan nilai snmp

Pengaksesan data snmp dilakukan langsung melalui fungsi php snmp yang ada pada php dengan menambahkan fungsi tambahan yang memparsing nilai snmp yang didapat, parsing yang dilakukan menggunakan fungsi seperti kutipan kode sumber 5.1.

```
function format_snmp_string($string) {
    /* strip off all leading junk (the oid and stuff) */
    $string = trim(ereg_replace(".*= ?", "", $string));
    /* remove ALL quotes */
    $string = str_replace("\"", "", $string);
    $string = str_replace("'", "", $string);
    $string = str_replace(">", "", $string);
    $string = str_replace("<", "", $string);
    $string = str_replace("\\", "", $string);

    if (preg_match("/(hex:\s)?([a-fA-F0-9]{1,2}(:\s){5})*/", $string)) {
        $octet = "";

        /* strip of the 'hex:' */
        $string = eregi_replace("hex: ?", "", $string);

        /* split the hex on the delimiter */
        $octets = preg_split("/\s:/", $string);

        /* loop through each octet and format it accordingly */
        for ($i=0; ($i<count($octets));$i++) {
            $octet .= str_pad($octets[$i], 2, "0", STR_PAD_LEFT);

            if (($i+1) < count($octets)) {
                $octet .= ":";
            }
        }
        /* copy the final result and make it upper case */
        $string = strtoupper($octet);
    }elseif (preg_match("/Timeticks:\s\((\d+)\)\s/", $string, $matches)) {
        $string = $matches[1];
    }
    $string = eregi_replace(REGEXP_SNMP_TRIM, "", $string);
    return trim($string);
}
```

Kode Sumber 5.1 Parsing Nilai SNMP

Fungsi diatas hanya akan mengambil nilai dari snmp tidak beserta tipe data dan informasi lain yang tidak diperlukan.

5.2.3.10 Informasi yang disajikan dalam Web

Informasi yang disajikan dalam web adalah informasi keseluruhan baik yang aktif maupun tidak aktif.

5.2.3.11 Informasi yang disajikan dalam Laporan (Email dan SMS)

Informasi yang disajikan dalam sms dan email adalah informasi singkat hanya yang aktif saja, hal ini tentu saja untuk menghemat pulsa server.

5.2.3.12 Jenis Laporan yang ditangani oleh sistem

Sistem dalam memberikan laporan dalam bentuk

1. Email:
2. SMS
3. Broadcast domain message menggunakan protokol SMB.

5.2.3.13 Syntax Laporan

Setiap laporan berisi dengan syntax sebagai berikut:

```
<kode host> <sensor> <nilai> <batas yang diperoleh>
```

Misal

```
NOC-CORE Interface Serial 1 downlink  
1000000 byte maksimum 256000 byte
```

Artinya : pada router NOC-CORE beban turun untuk antarmuka jaringan Serial 1 mencapai 1000000 byte, padahal maksimum beban turun yang diperbolehkan hanya 256000 byte.

5.2.3.14 Mekanisme Penyajian Informasi Tambahan

Informasi tambahan atau Extended Info yaitu informasi tambahan yang tidak masuk dalam pelaporan. Dengan mekanisme sebagai berikut:

1. bergantung pada jenis *host*, artinya informasi disajikan berdasarkan jenis *host*
2. baca basis data yang mengarah pada file xml untuk metode query informasi snmp
3. hasil pembacaan file xml digunakan untuk query ke snmp dengan metode walk
4. hasil pembacaan snmp disimpan dalam basis data cache
5. ditampilkan hasil pembacaan dari basis data ke web dalam bentuk pivot table.

5.2.3.15 Level User

Pada program ini terdapat 3 tipe user yaitu:

1. *Anonymous* atau *Guest* atau user tidak login; user jenis ini hanya dapat melihat bagian depan program dan navigasi saja.
2. Normal User; Adalah administrator dan Manajer pada jaringan tersebut dan tidak sebagai Administrator sistem pemantauan itu sendiri, diberi hak untuk melakukan pemantauan sistem dan melihat status atau keadaan *host* dan informasi lainnya.
3. Administrator, Adalah administrator jaringan dan administrator pada sistem pemantauan itu sendiri, diberi hak penuh terhadap sistem termasuk pengelolaan sistem.

5.2.3.16 Implementasi Antarmuka berbasis Web

Tampilan keseluruhan antarmuka web dengan contoh sedang menampilkan informasi salah satu *host*.

Network Monitoring and Information System v0.23
Tugas Akhir untuk memperoleh gelar Sarjana Teknik Informatika UII, sofyanto wijaya (00523110)

Host Detail Information

all :: general :: sensor :: extended :: graph

Host Base

host kode	id31-firdh@net
ip address	10.10.100.41
snmp community	uiinet
device type	breezecom
report enable	on

General SNMP Information

name	value
system up time	
System Description	
system contact	
system name	
System Location	

SNMP with Sensor Reporting Information

sensor id	host id	snmp oid id	value	max value	min value	report enable
25	id31-firdh@net	8 .1.3.6.1.4.1.710.3.2.1.2.9.0 associated au	error fix	Uii_1.1	Uii_1.1	on
26	id31-firdh@net	9 .1.3.6.1.4.1.710.3.2.3.1.6.0 Wireless LAN Quality	error fix	3	1	on
27	id31-firdh@net	10 .1.3.6.1.4.1.710.3.2.3.1.3.0 Average RSSI	error fix	150	113	on

::home::
user.sofyan
ip 127.0.0.1

::summary::
::sms gratis dong::

::device list::
id27-danmas
id31-firdh@net
noc-core
noc-database
noc-gateway
noc-venus

::management::
host management
host sensor
host graph
general snmp
extended snmp

::snmp data bank::
snmp oid
snmp query
device type

::system::
user management
configuration
view report log
run checking

Gambar 5.2 Preview Keseluruhan

6 Penutup

6.1 Simpulan

Setelah dilakukan pengujian dapat ditarik kesimpulan sebagai berikut:

- a. Server Pemantauan dapat melakukan pemantauan dan memberikan informasi kritis yang diperlukan agar administrator dapat segera menangani permasalahan yang muncul
- b. Pelaporan melalui sms terbukti memberikan respon yang cepat agar administrator dapat segera mengetahui permasalahan jaringan yang terjadi.
- c. Penggunaan protokol snmp untuk pemantauan memberikan hasil yang baik dan dapat diterapkan untuk pemantauan di hampir peralatan jaringan yang menggunakan protokol TCP/IP.
- d. Begitu terjadi permasalahan, sistem tidak dapat segera langsung memberikan laporan dikarenakan menggunakan proses terjadwal untuk melakukan pengecekan dan tidak digunakan metode trap pada snmp
- e. Dari hasil pengujian dan dibandingkan dengan hipotesis (dugaan awal) terbukti dengan adanya bantuan sistem pemantauan ini maka group Administrator dapat mengetahui kondisi jaringan dengan lebih cepat.

6.2 Saran

- a. Spesifikasi komputer yang digunakan untuk pengembangan dan implementasi terlalu rendah, diharapkan nantinya jika ada penelitian sejenis menggunakan spesifikasi komputer yang lebih baik.
- b. Dengan dukungan alat yang lebih baik dapat digunakan untuk memantau berbagai device yang lebih banyak
- c. Navigasi atau menu kurang efektif jika *host* yang dipantau lebih dari 10, pada kesempatan mendatang diharapkan nantinya untuk membuat menu yang lebih mudah untuk dioperasikan.
- d. Belum ada graph pada sistem ini, diharapkan ada penambahan graph untuk melengkapi sistem ini.
- e. Metode reporting atau pelaporan baru sms dan email, diharapkan selanjutnya dapat mengembangkan metode lain yang lebih cepat lagi.
- f. Kepada para pengembang dapat memberikan masukan dan sekaligus melakukan developing langsung ke sistem ini.

Daftar Pustaka

- [1] Aziz, M.F., Belajar Sendiri Pemrograman PHP 4 bagi web programmer, Jakarta: Elex Media Komputindo, 2001.
- [2] Hazewinkel, H., *PHP-SNMPv3; status monitoring*, Frankfurt: Internet Management Consultant, 2002.

- [3] Berry, I., *The Cacti Manual*, England: Ian Berry, 2005.
- [4] Jansen, M., Merz, A., *PEAR Manual*, America: The PEAR Documentation Group, 2005.
- [5] Jogyanto H.M. *Analisis Desain dan Sistem Informasi*. Jakarta: PT ELEX Media Komputindo, 2002.
- [6] Purbo W.O. *TCP/IP Standar, Desain, dan Implementasi*. Jakarta: PT Elek Media Komputindo, 1998.
- [7] Purbo W.O. *Mengenal Protocol Internet TCP IP*, <http://onno.vlsm.org/v11/ref-ind-1/network/mengenal-protokol-internet-tcpip-1998.rtf>, diakses tanggal 23 Maret 2005.
- [8] Prasetyo, D.D., *Tip dan Trik Kolaborasi PHP dan MySQL Untuk Membuat Web Database yang Interaktif*, Jakarta: Elex Media Komputindo, 2003.
- [9] Rafiudin, R., *Multihoming Menggunakan BGP (Border Gateway Protocol) Membangun Multi-Koneksi Ke Multi-ISP*, Yogyakarta: PENERBIT Andi Yogyakarta, 2004.
- [10] Schmidt, K., Mauro, D., *Essential SNMP*, America: O'Reilly, 2001.
- [11] Seifried, K., *Networks Services – SNMP*, <http://www.securityportal.com/NetSMP.html>, diakses tanggal 5 Februari 2005.
- [12] Sunarfrihantono, B., *PHP dan Mysql untuk Web*, Yogyakarta: Penerbit Andi Yogyakarta, 2002
- [13] Telematic Lab ITB, *Internet Control Message Protocol*, Bandung: Institut Teknologi Bandung, 2002.
- [14] *ICMP*, <http://www.klik-kanan.com/kamus/i.shtml>, diakses tanggal 14 Maret 2005.