MANAGED SERVICE NETWORK MANAGEMENT SYSTEM (NMS) BERDASARKAN FAULT, CONFIGURATION, ACCOUNTING, PERFORMANCE, SECURITY (FCAPS) MANAGEMENT

Bambang Sri Endro Isworo[1] , Peby Wahyu Purnawan[2]
Program Studi Teknik Elektro, Fakultas Teknik – Universitas Budi Luhur
Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan 12260
Email : bambang.endro07@gmail.com
pebywahyupurnawan@budiluhur.ac.id

ABSTRACT - A problem that often occurs in the world of networks is the lack of response an administrator in the face of a problem that occurs. An administrator sometimes do not know that there has been a problem before they checked into the device, even the cause of the problems in the network can be known after performing troubleshooting, so the solution is taken late and imprecise. The emergence of a variety of tools based on the network system FCAPS (Fault, Configuration, Accounting, Performance and Security) makes it easy for engineers to troubleshoot without losing some of the services in the network. The tools are currently still stand on its own in accordance with the respective categories - each function, teknnologi expected with the development of the functionality can be combined in a single platform to make it easier to monitor and control a complex network. FCAPS system is a system that has been quite advanced because it can protect from the shape anomaly and the analysis results can be used to measure the QoS

Keywords - Network Systems, Device, QoS, FCAPS, Service.

I. Pendahuluan

Semakin berkembangnya teknologi di Indonesia pada umumnya didukung oleh berkembangnya pula ilmu pengetahuan dan teknologi jaringan telekomunikasi, khususnya sisi monitoring sangatlah penting karena selain untuk melihat segala bentuk *anomaly* dan permasalahan di dalam jaringan, juga sangat diperlukan untuk menganalisa suatu jaringan agar dapat dikembangkan oleh pihak *engineering*. Selain itu pula ada hal – hal yang perlu diperhatikan dalam pengelolaan suatu jaringan. Hendaknya suatu jaringan dapat memonitor beberapa unsur manajemen, antara lain *Fault*, *Configuration*, *Accounting*, *Performance*, dan *Security Management* atau yang biasa dikenal dengan FCAPS manajemen. Salah satu kebutuhan yang harus terpenuhi dalam dunia jaringan yaitu adalah aspek *monitoring* atau biasa disebut dengan *Network Management System (*NMS), dimana aspek ini merupakan bagian dari *Operational Support System* (OSS). OSS berfungsi dalam segi *alerting* dan memonitor segala bentuk *device* dengan parameter yang berguna dalam menganalisa masalah yang terkait.

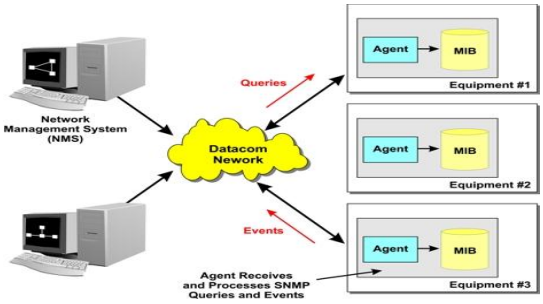
Simple Network Management Protocol (SNMP) adalah sebuah protokol aplikasi pada jaringan TCP/IP yang dapat digunakan untuk pengelolaan dan pemantauan sistem jaringan komputer. SNMP akan mempermudah proses monitoring dan manajemen jaringan karena dengan menggunakan SNMP akan dapat diketahui tentang kondisi perangkat jaringan yang diamati[1]. Pada penelitian sebelumnya *tools* yang digunakan adalah *Security Information And Event Management* (SIEM). SIEM adalah teknologi memberikan keamanan TI yang mengadopsi metodologi yang digunakan untuk menkorelasi log, peristiwa, mengalir dari komputasi perangkat, sistem dan layanan terdistribusi dengan baseline keamanan[3]. Pada perkembangannya NMS saat ini menggunakan FCAPS manajemen yang berperan dalam mengkategorikan NMS sesuai dengan fungsi dan *output*nya .

II. Teori Dasar

2.1 Pengertian Network Management System (NMS)

Manajemen jaringan adalah kemampuan memonitor, mengontrol, dan merencanakan sumber serta komponen sistem dan jaringan komputer[2]. Manajemen ini mencoba menggunakan kekuatan komputer dan jaringan untuk mengatur dan mengelola sistem dan jaringan itu sendiri. Dalam melakukan hal itu, para administrator jaringan memerlukan beberapa *tools* yang memudahkannya dalam mengelola jaringan. Dengan sistem dan jaringan *"self-managed"* atau *"manage-less"* tidak menuntut keahlian sepanjang waktu dan proses manajemen tetap berjalan secara otomatis.

Sekurang – kurangnya satu rangkaian jaringan yang ditemukan dalam sebuah jaringan yang teratur ditunjuk sebagai manajer. NMS bertanggung jawab untuk memonitor dan mengontrol agen – agen. Sebuah agen adalah suatu komponen software yang terdapat pada satu rangkaian peralatan yang bertanggung jawab terhadap pemantauan dan pengontrolan dimana agen tersebut beroperasi.



Gambar 1 : Elemen Manajemen Sistem Jaringan

Faktor yang mempengaruhi manajemen sistem jaringan ini, yaitu :

a. Mengendalikan assets strategi perusahaan
b. Mengendalikan kompleksitas jaringan
c. Meningkatkan pelayanan dari suatu jaringan
d. Menyeimbangkan segala keperluan
e. Mengurangi downtime karena tiap elemen dapat termonitor dengan baik
f. Mengendalikan biaya

Pada dasarnya, dua arsitektur yang dapat digunakan yaitu, manajemen terpusat (*centralized management*) dan manajemen tersebar (*distributed management*)[5]. Arsitektur manajemen terpusat bersandar pada informasi dan kontrol untuk muncul pada sebuah lokasi tunggal yang tersentralisasi atau terpusat. Hal ini menyederhanakan suatu jaringan yang tidak terlalu besar. Manajemen terdistribusi bertolak belakang dengan manajemen terpusat, sistem ini mendistribusikan informasi pada masing – masing jaringan dan masing – masing jaringan bertanggung jawab pada informasi yang diberikan oleh masing – masing elemen pada jaringan tersebut.

Di dalam manajemen jaringan terdapat beberapa aktivitas yang terjadi, seperti administrasi jaringan, *maintenance* atau pemeliharaan jaringan, manajemen performansi, manajemen keamanan dan lain-lain. *The International Organization for Standarization* (ISO) mendefinisikan sebuah model konseptual untuk menjelaskan fungsi dan proses manajemen jaringan yang dapat dilihat pada table berikut:

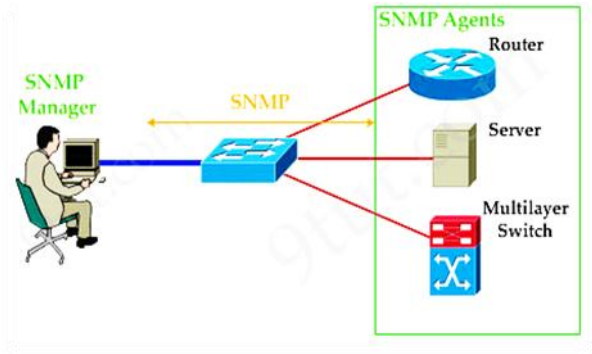
Tabel 2.1 Proses yang terjadi pada aspek manajemen jaringan

Aspek Manajemen Jaringan	Penjelasan
Network Installation	Berhubungan dengan pelaksanaan proses instalasi pada suatu jaringan, misalnya ketika ada suatu
Network Repair	Berhubungan dengan proses perbaikan atau reparasi pada jaringan
Network Test	Berhubungan dengan proses pengetesan atau uji coba pada jaringan
Network Planning & Design	Proses perencanaan dan perancangan jaringan
Fault Management	Berhubungan dengan pendeteksian, dan proses restorasi service atau komponen yang mengalami error
Configuration Management	Berhubungan dengan proses konfigurasi di dalam jaringan
Security Management	Berhubungan dengan proses penanganan keamanan dalam jaringan, misalnya proses pengalokasian privilege kepada user yang berhak mengakses jaringan
Accounting Management	Berhubungan dengan proses administrasi biaya yang diperlukan dalam pengembangan jaringan dan melakukan pengalokasian biaya
Inventory Management	Berhubungan dengan proses manajemen komponen jaringan yang ada, meliputi penentuan apa yang harus ada di dalam jaringan, dan perawatan komponen jaringan yang ada
Data Gathering & Analysis	Berhubungan dengan proses pengumpulan dan penganalisisan data pada jaringan
Traffic Management / Performance Management	Berhubungan dengan optimasi performansi dari suatu jaringan

2.2 Simple Network Management System (SNMP)

Peralatan manajemen yang paling mudah diimplementasikan dan sangat mendasar untuk rangkaian protokol jenis *Transport Control Protocol/ Internet Protocol* (TCP/IP) ialah Simple *Network Management Protocol* (SNMP). SNMP adalah sebuah protokol apikasi pada jaringan TCP/IP yang menangani manajemen jaringan. Protokol ini didesain sehingga pengguna dapat dengan mudah memantau kondisi

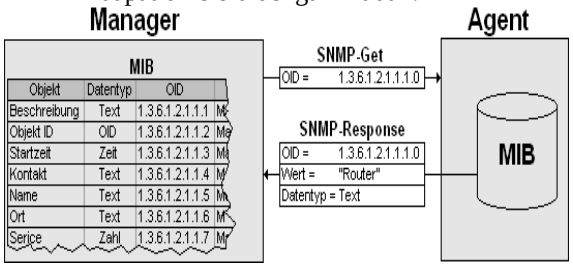
jaringan komputer [1]. SNMP memiliki spesifikasi yang digunakan untuk manajemen jaringan yaitu *Internet Engineering Task Force Request for Comments* (IETFRFC). Model manajemen SNMP didasarkan pada pemahaman akan satu manajer dan satu agen SNMP, dimana sang agen dikelola oleh sang manajer.



Gambar 2 : SNMP agen dan SNMP Manager

Manajer terdiri atas satu proses atau lebih yang berkomunikasi dengan agen – agennya. Manajer akan mengumpulkan informasi dari agen atas jaringan yang diminta. Sedangkan agen merupakan perangkat lunak yang dijalankan disetiap elemen. Setiap agen memiliki basis data variabel yang bersifat lokal yang menerangkan keadaan dan berkas aktivitas dan pengaruh terhadap operasi. Di dalam suatu agen terdapat satu grup variabel yang mengelola struktur basis data variabel yaitu disebut dengan *Management Information Base* (MIB). Struktur ini bersifat hirarki dan memiliki aturan sedemikian rupa sehingga variabel

dapat dikelola dengan mudah.



Gambar 3 : Rangakaian komunikasi Management Information Base

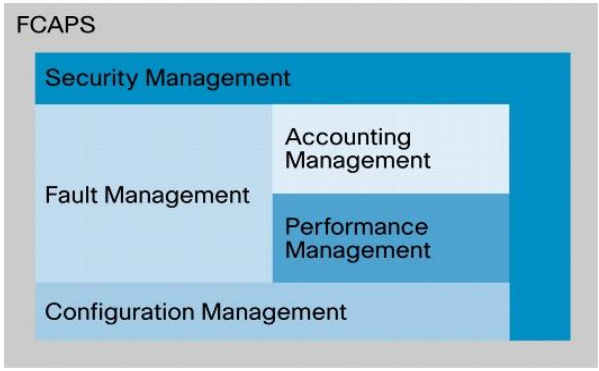
Protokol SNMP menggunakan operasi yang sangat sederhana dan PDU dalam jumlah yang relative terbatas untuk menjalankan fungsinya. Lima PDU yang telah didefinisikan dalam standar adalah sebagai berikut [4]:

1. Get Request, PDU ini digunakan untuk mengakses agen 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 pada get request, tetapi memungkinkan pengambilan informasi pada logical identifier selanjutnya pada MIB Tree secara berurutan.
3. Get Response, PDU ini untuk merespon unit data Get Request, Get-Next Request dan Set-Request.
4. Set Request, dipakai untuk menjalankan aksi yang harus dilaksanakan di elemen jaringan. Biasanya untuk mengubah nilai suatu daftar variabel.
5. Trap, PDU ini memungkinkan modul manajemen jaringan / agen member laporan tentang kejadian pada elemen jaringan kepada manager.

III. MANAGED SERVICE NETWORK MANAGEMENT BERDASARKAN FAULT, CONFIGURATION, ACCOUNTING, PERFORMANCE, SECURITY (FCAPS) MANAGEMENT

3.1 FCAPS *Management* pada *tools* NMS *Datacomm*

Solusi *network* yang digunakan oleh beberapa *principal* besar seperti Cisco dan Juniper mengusung standar ISO dimana ada lima fokus dalam pengelolaan jaringan, yaitu pada masalah *fault, configuration, accounting, performance dan security*, atau biasa kita menyebutnya dengan FCAPS *Management.* Cisco sebagai salah satu perusahaan besar yang fokus pada dunia TI mengatakan bahwa fungsi dari management ini memerlukan satu keterkaitan dengan yang lain.



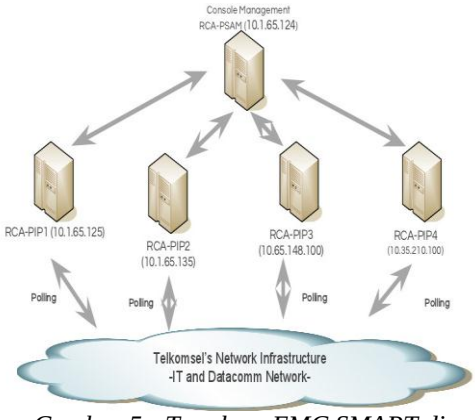
Gambar 4: Interaksi Fungsi FCAPS

Lima fokus manajemen jaringan ini memiliki keterkaitan satu sama dengan yang lain, namun dengan porsi yang berbeda – beda. FCAPS merupakan model dan *framework* dari *ISO Telecommunication* untuk *management network* yang mana mengkategorikan tugas – tugas dari *network management*. Berkembangnya

tekhnologi bersama dengan kebutuhan dalam dunia TI maka terbentuklah sistem monitoring dengan kategori – kategori yang berbeda sehingga memudahkan bagi administrator jaringan dalam *quick response* jika terjadi gangguan, serta dalam sisi analisa agar dapat membuat jaringan yang lebih baik lagi.

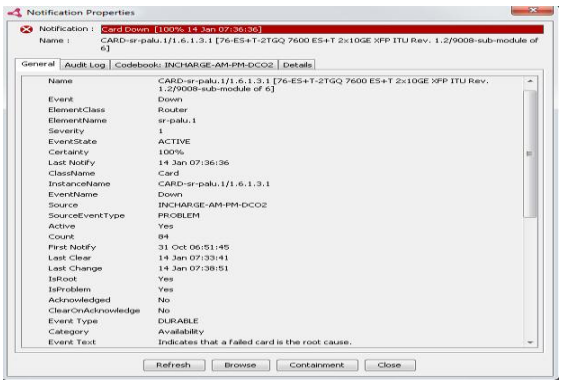
Macam – macam *tools* OSS *Datacomm* yang dikelola oleh PT. Dimension Data Indonesia berbasis FCAPS antara lain:

1. *Fault Management*, merupakan fungsi manajemen untuk mendeteksi, melakukan diagnosa, memperbaiki, melamporkan bentuk *failure* dari *device* dan layanan jaringan. Sistem manajemen ini memberitahu administrator jaringan tentang apa yang sedang terjadi pada jaringan, misal terputusnya *link* suatu jaringan. Hal tersebut dapat membantu administrator jaringan dalam membantu menentukan *root caused* yang terjadi dalam suatu *anomaly*. Aplikasi yang digunakan oleh PT. Telkomsel, Tbk. dalam sistem manajemen ini yaitu aplikasi SMART yang dibentuk oleh EMC, salah satu *principal* yang *concern* pada sistem monitoring *fault* manajemen.



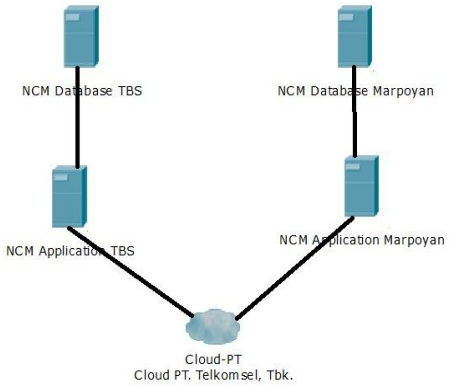
Gambar 5 : Topology EMC SMART di PT. Telkomsel

Pada SMART *Dashboard* dapat dilihat jenis *faulty* yang terjadi, bisa berupa *interface/link* yang *unavailable*, *module* yang *failed*, *root caused* atas *alarm* yang muncul serta dapat melihat topologi dari *router* tersebut atau *link* yang berhubungan langsung dengan *device* yang bermasalah dan terindikasi *problem* dikarenakan atas *module* yang rusak. Hal ini dapat membantu seorang administrator jaringan dalam melakukan tindakan yang cepat dan tepat, salah satu contoh tindakan yang dapat dilakukan ketika muncul *alarm notification* yaitu melakukan pengechekan *module* terkait yang menyebabkan *link down* dan melakukan penggantian secara cepat apabila dibutuhkan. Administrator jaringan juga dapat melakukan pengechekan terhadap *device* lainnya yang berhubungan dengan dengan *device* yang bermasalah.



Gambar 6 : Detail Alarm Notification

2. *Configuration Management*, fungsi manajemen ini bertugas untuk menjaga kekuatan *inventory hardware*, *software* dan bentuk konfigurasi yang terdapat di dalamnya. Sistem manajemen ini menjamin konsistesi dan validitas dari parameter – parameter operasi, *table addressing*, *software image* dan konfigurasi *hardware*. Dalam hal ini digunakan aplikasi dari cisco yaitu *Cisco Work Network Compliance Management* atau biasa kita sebut dengan CWNCM. Aplikasi ini adalah solusi yang berguna sebagai *tracking* untuk mengatahui regulasi perubahan konfigurasi dan *software* dalam suatu *device* di jaringan infrastruktur PT. Telkomsel, Tbk. Dalam hal ini, NCM mempunyai 2 *server* sebagai aplikasi dan 2 *server* sebagai *database.*



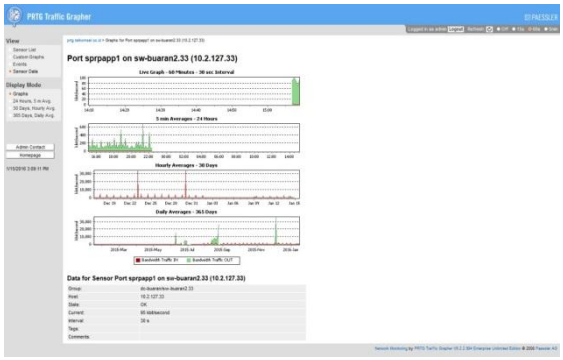
Gambar 7 : Topology CWNCM di PT. Telkomsel, Tbk.

Aplikasi ini juga berfungsi sebagai *authentication* untuk masuk ke *device*

router/switch, sehingga dapat diketahui pula siapa saja yang melakukan perubahan konfigurasi dan perubahan apa yang dilakukan. Aplikasi ini biasanya digunakan menggunakan suatu *software* atau aplikasi yang dapat menjalankan *port ssh* dan *telnet* mengacu pada fungsi *router/switch* bahwa seorang administrator jaringan dapat melakukan *login remote* dari *port ssh* dan *telnet* yaitu contohnya: *putty* dan *secureCRT*.

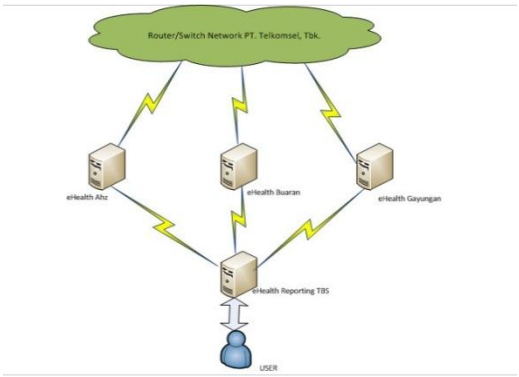
Gambar 8 : Perbandingan perubahan konfigurasi

3. *Accounting Management*, berfungsi untuk mengukur *usage* jaringan dan menghitung biaya untuk *usage* tersebut. Fungsi ini jarang diimplementasikan pada sistem berbasis *Local Area Network* (LAN) dalam suatu perusahaan. Tujuan dari sistem manajemen ini yaitu mengukur beban jaringan sesuai kapasitas pemakaiannya. Dalam hal ini, user menggunakan aplikasi dari *Paessler Router Traffic Grapher (PRTG)* yang berperan dalam *Accounting Management*. Aplikasi ini memberikan gambaran tentang *availability* suatu *link* LAN dan penggunaan *Bandwidth* pada *link* tersebut.



Gambar 9 : Link Bandwidth pada PRTG

4. *Performance Management*, sistem manajemen ini berfungsi sebagai bentuk analisa dari kinerja suatu *device* baik dari segi fisik maupun *logical* yaitu *link lan/wan*. Sistem ini memiliki tujuan mengoptimalkan *Quality of Service* (QoS) dengan cara mendeteksi perubahan performa jaringan. Status suatu jaringan yang akan ditampilkan meliputi: *traffic volume, network availability, network delay*, dan lain sebagainya. CA eHealth merupakan aplikasi yang digunakan untuk *support system* manajamen yang mengambil fokus pada *performance*. Tidak berbeda dengan aplikasi SMART, CA eHealth juga memiliki 1 Server sebagai *Reporting/Console* dan 3 Server sebagai *poller* yang berhubungan langsung dengan *device*.



Gambar 10 :Topology CA eHealth di PT. Telkomsel, Tbk.

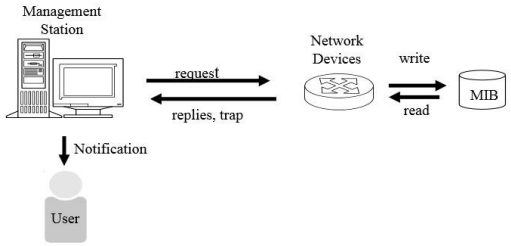
Parameter yang dapat digunakan pada *output* ini sangat beragam bergantung pada segi apa yang akan diambil. Misal, dalam segi *device* kita dapat mendapatkan *output* dengan *parameter, cpu utilization, memory utilization, physical memory, disc capacity* dan lain sebagainya. Sedangkan pada segi *service*, *output* yang dihasilkan bisa berupa *bandwidth utilization, bytes, error, latency, packets discard* dan sebagainya, bahkan biasa digunakan dalam mengukur *Quality of Service* (QoS) dari suatu device.

5. *Security Management, system management* ini berfungsi untuk mengontrol akses ke *Network Management Sytem* (NMS). Fungsi ini melindungi jaringan dan NMS dari akses dan modifikasi yang tak diijinkan. Hal tersebut juga bertujuan dalam untuk mengontrol akses terhadap sumber daya jaringan sesuai *local policy* sehingga jaringan tidak dapat disabotase dan

informasi yang berharga tidak dapat diakses oleh yang tidak berkepentingan

3.2 Proses *Discovery Simple Network Management Protocol* pada *tools* berbasis FCAPS

Proses pengumpulan data yang dilakukan aplikasi manapun tidak akan berhasil tanpa ada suatu standarisasi *port* yang digunakan secara langsung untuk mengolah data *real-time* yang terjadi pada *device* tersebut. Dalam hal ini dipakailah satu *protocol* yang bertugas mengumpulkan data *device* agar dapat terkirim ke suatu *server* aplikasi dan diolah oleh aplikasi tersebut yang kemudian menghasilkan fungsi FCAPS *Management. Simple Network Management Protocol* (SNMP) merupakan suatu protocol yang dirancang dalam mengadministrasi atau mengelola jaringan *TCP/IP* dalam hal ini *router* dan *switch*. Dalam suatu *element* atau *device* memiliki *Management Information Base* (MIB) sebagai koleksi informasi dalam bentuk hirarki, MIB berisi dari kumpulan *Object Identifier* atau *Object ID* (OID) yang berfungsi sebagai suatu informasi dari *device* tersebut. Contohnya, *cpu, memory, module* atau *interface*, OID bersifat unik maka tiap *sub-element* OID dari satu *device* berbeda.



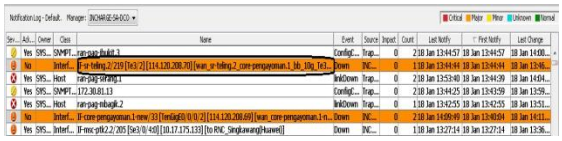
Gambar 11 : Proses Discovery menggunakan SNMP

Aplikasi yang terinstall pada *management station* atau *server* melakukan *request* terlebih dahulu pada *network device*. Apabila *protocol* yang di*request* sama, dalam hal ini *community* yang digunakan sama maka *network devices* akan melakukan *reply* ke *server* lalu. Proses selanjutnya yaitu *server* akan melakukan *request* kembali untuk meminta data MIB pada *network devices* agar dapat dilakukan pengambilan data (*trap*) oleh server aplikasi tersebut.

3.3 Analisa dari *Output Tools* FCAPS

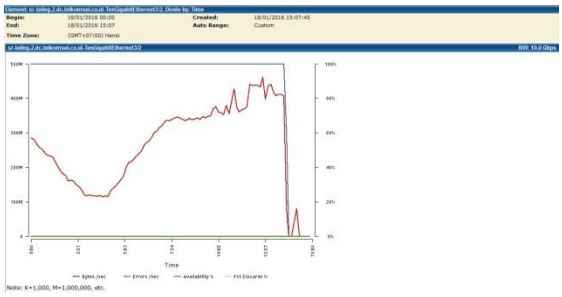
Sistem *Management* FCAPS tidak hanya digunakan oleh *administrator* atau pihak –pihak yang melakukan *monitoring* saja seperti *Network Operation Center* (NOC) tetapi banyak pihak yang menggunakan sistem ini. Salah satu yang menggunakan sistem ini di PT. Telkomsel, Tbk. yaitu divisi *Network Quality. Management*. Bagian ini secara berkala mengambil data *performance* dari suatu *device* kemudian hasil dari data tersebut akan didapatkan solusi akhir bagaimana kebijakan yang harus diambil selanjutnya. Pada sisi NOC yang paling banyak digunakan yaitu *Fault management* yaitu mengamati segala bentuk *anomaly* yang terjadi secara *real-time*.

Berikut merupakan salah satu contoh kasus yang terjadi, yaitu putusnya *link* 10 *Gigabytes route* sr-teling.2 kearah core-pengayoman.1 pada *interface* Te3/2 seperti pada gambar 4.17. Pada kondisi ini team NOC akan memberitahu *administrator* jaringan untuk melakukan *troubleshooting.*



Gambar 12 : Alarm Notification (sr-teling.1 Te3/2 link down)

Seorang *administrator* jaringan akan melakukan beberapa pengechekan yaitu salah satunya melihat *interface* yang *down* dan apakah ada kerusakan *module* atau tidak. Segala sisi harus dapat diperiksa oleh seorang *administrator* agar analisa yang dibuat jelas dan dapat mengambil solusi secara tepat dan cepat. Sisi konfigurasi juga tidak lepas dari pengechekan, yaitu melihat apakah ada perubahan konfigurasi pada waktu yang bersamaan yang dapat menyebabkan *link* terputus. Hal terakhir yang dilakukan oleh *administrator* jaringan ialah memeriksa dari sisi *transmisi*. Dalam hal ini masalah yang terjadi disebabkan oleh terputusnya *Fiber Optic* (FO) pada jalur *link* tersebut. Penulis tidak dapat menunjukkan sisi *monitoring transmisi* karena bukan dari cakupan penulis.



Gambar 13 : Link Tengig 3/2 sr-teling.2 yang terputus

Salah satu solusi yang digunakan oleh *administrator* jaringan dalam menghadapi masalah ini yaitu memindahkan *link* yang terputus ke jalur lainnya sesuai dengan kapasitas *bandwidth* yang ada. Beberapa solusi juga dapat

diambil dari *team Network Quality* dari data *performance*, yaitu : menambahkan *backup link* dengan kapasitas yang lebih besar, menambah *backup router* dengan *transmisi* yang berbeda, atau meningkatkan performa dari *transmisi* FO.

Dengan menggunakan *tools* ini maka seorang administrator dapat melakukan suatu penanganan dengan cepat dan tepat sehingga mengurangi resiko hilangnya layanan yang terdapat dalam komunikasi jaringan serta dapat melakukan analisa untuk menciptakan suatu jaringan yang efektif dan efisien.

IV. Kesimpulan

1. Sistem FCAPS merupakan sistem yang sudah cukup maju karena dengan adanya sistem ini suatu jaringan dapat terlindungi dari bentuk *anomaly* dan hasil analisa dapat digunakan untuk mengukur QoS.
2. Proses *Discovery* pada manajemen sistem jaringan menggunakan satu protokol yaitu *Simple Network Management Protocol* (SNMP) versi kedua, saat ini SNMP sudah sampai pada versi ketiganya dimana data lebih aman karena melalui proses enkripsi, autentikasi, pesan yang terintegrasi dengan baik. Meskipun demikian, SNMP versi kedua masih cukup aman dan tidak bermasalah dewasa ini, output yang dihasilkan juga tidak berbeda dengan SNMP versi ketiga.
3. Output yang dihasilkan dari FCAPS manajemen sangat berguna bagi seorang engineer, yaitu dari sisi *Fault Management* hasil yang didapatkan yaitu peringatan ketika muncul alarm pada suatu elemen, pada *Configuration Management* berupa catatan dari bentuk konfigurasi baik *hardware* maupun *software*, *Accounting Management* menunjukkan *cost bandwidth* dari suatu *link*, *Performance Management* menghasilkan suatu data yang dapat digunakan dalam mengalisa dan memberikan solusi untuk jaringan dimasa depan, dan jika *Security Management output* yang dihasilkan yaitu menjaga jaringan agar terlindung serangan *hacker* dari luar.

DAFTAR PUSTAKA

1) G Mauro, Douglas., *"Essential SNMP Second Edition"*, O'Reilly Media, Sebastopol, 2005
2) Reza, dkk. 2013. *Rancang Bangun Applikasi Monitoring Jaringan dengan Menggunakan Simple Network Management Protocol.* Jurnal Teknik POMITS Vol. 2, No. 1, Surabaya.
3) Pratama, Adrian dkk., 2015, Penerapan Network monitoring Menggunakan Security information and event management (siem) Berbasis Open source Di universitas bina darma Palembang
4) Jogiyanto H.M. Analisis Desain dan Sistem Informasi. Jakarta: PT ELEX Media Komputindo, 2002.
5) Stallings, William. 2004. *Computer Networking with Internet Protocols and Technology. USA: Pearson Education, Inc*.
6) Mellquist, Peter Erik. 1998. *SNMP++* Pendekatan Berorientasi Objek. Yogyakarta: Andi Yogyakarta.
7) Suartin, Maret 2010. Pengembangan Sistem Pemantau Jaringan SNMP Berbasis SMS Di Jurusan Teknik Elektro Fakultas Teknik Universitas Negeri Padang. http://www.imuzcorner.net/2013/07/daftar-pustaka-jurnal-koran-dan-majalah.html.

Sumber Online

https://9tut.com/snmp.