

Fault Management (Manajemen Kesalahan) Pada Network Management System

Imam Malik

09011381621093

Sistem Komputer Fakultas Ilmu Komputer
Universitas Sriwijaya

Abstrak

Kegunaan dari Teknologi Jaringan Komputer adalah untuk memenuhi kebutuhan informasi dengan cepat dan beragam, sehingga menghasilkan kompleksitas jaringan komputer yang semakin luas dan semakin meningkat. Oleh karena itu, saat ini dibutuhkan pendukung fasilitas untuk dapat mengawasi elemen jaringan yang ada dengan menggunakan Network Management System (NMS). Model NMS yang ditetapkan oleh ISO mencakup 5 bidang konseptual, yaitu Kesalahan, Konfigurasi, Akuntansi, Kinerja dan Manajemen Keamanan (FCAPS). Salah satu aspek yang akan dibahas didalam penelitian ini adalah Fault Management. Mekanisme yang akan digunakan untuk manajemen kesalahan adalah dengan mendeteksi terjadinya kesalahan dan mengirim pemberitahuan via email saat kesalahan muncul, lalu masuk ke log laporan dan membuat diagnosis dan lebih lanjut merekomendasikan solusi untuk kesalahan tadi. Jenis kesalahan yang dilaporkan dalam sistem ini adalah kesalahan ketika ada kegagalan konektivitas di jaringan perangkat, kesalahan karena layanan yang tidak berjalan dan tidak sesuai dengan permintaan, kesalahan saat RAM tinggi penggunaan, peningkatan beban CPU dan penggunaan hard drive yang mulai penuh. Dari hasil penelitian yang diperoleh, NMS dapat mengirim pemberitahuan kesalahan dan memberikan solusi rekomendasi via email ke admin jaringan jika ada adalah kesalahan jaringan, aktivitas Manajemen Kesalahan dapat dilakukan sedini mungkin agar masalah tidak berdampak pada penurunan kualitas jaringan. Disini akan membahas tentang pengelolaan Manajemen Kesalahan (Fault Management) menggunakan aplikasi manajemen berdasarkan standar OSI.

1. Pendahuluan

Semakin berkembangnya teknologi di Indonesia pada umumnya didukung oleh berkembangnya pula ilmu pengetahuan dan teknologi jaringan telekomunikasi, khususnya pada sisi monitoring sangatlah penting karena selain untuk melihat segala bentuk anomali 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

Manajemen jaringan telah menjadi masalah utama diskusi dalam desain dan pemeliharaan jaringan komunikasi. Ini dikarenakan jumlah dalam mengelola jaringan ini dan tugas-tugas yang terlibat termasuk mengelola host lokal dan jarak jauh (contohnya : server), perangkat jaringan (misal router, jembatan), lokal dan jarak jauh administrasi sistem (misal sistem operasi, penyimpanan sistem, profil pengguna), aplikasi lokal dan jarak jauh (misal database, direktori server), manajemen jaringan sistem dan koneksi jaringan yang mencakup semua entitas di atas. Tentunya, dengan semua definisi, manajemen jaringan menjadi tugas yang sulit dan membutuhkan sistem canggih yang bisa mengawasi semua operasi jaringan pada fasilitas tertentu. Sebagian besar organisasi telah mengakui strategi pentingnya jaringan komunikasi. Sementara di sebagian besar kasus, kontrol yang lebih baik memastikan tingkat yang lebih tinggi kinerja, penggunaan arus yang tidak tepat atau tidak efisien instrumen dan teknik manajemen jaringan dibuat pengelolaan komunikasi jaringan tertentu sistem hampir tidak mungkin. Tren ini hanya dapat meningkatkan pentingnya dan visibilitas jaringan yang efektif pengelolaan. Urgensi situasi di atas telah mendorong banyak organisasi untuk bekerja dengan Internasional Organisasi untuk Standardisasi (ISO) untuk definisi kerangka kerja untuk manajemen jaringan. Sistem terbuka manajemen jaringan interkoneksi (OSI) dibagi menjadi lima Area Fungsi Manajemen Tertentu (SMFA). Mereka adalah manajemen kesalahan, manajemen konfigurasi, manajemen akuntansi, manajemen kinerja dan manajemen keamanan. Area fungsional ini adalah biasa disebut sebagai FCAPS. Mereka memuji masing-masing lain dan bekerja sama untuk mencapai semua jaringan tugas manajemen. Namun dalam makalah ini, kami berkonsentrasi pada area fungsional manajemen kesalahan Manajemen kesalahan biasanya disebut sebagai salah satu yang paling penting dalam manajemen jaringan. Peran utamanya adalah untuk memastikan ketersediaan jaringan yang tinggi. Karenanya, melibatkan prosedur untuk mengantisipasi dan menghindari kegagalan jaringan, dan kasus di mana kegagalan tidak dapat dihindari, perlu langkah-langkah diperlukan untuk mengatasi kerusakan dan menyelesaikannya pada jaringan. Langkah-langkah ini mencakup kemampuan untuk secara otomatis mendeteksi dan memberitahukan terjadinya kegagalan, mengisolasi penyebab sebenarnya dari kegagalan dan memperbaiki kegagalan jika memungkinkan. Kami telah memilih untuk menyelidiki dan mengatasi masalah manajemen kesalahan karena lambatnya kemajuan proses standardisasi, kurangnya kesalahan aplikasi manajemen untuk pengguna, banyak kegagalan komponen yang secara umum membutuhkan alat pemantauan dan pemecahan masalah khusus untuk mengisolasi penyebab sebenarnya dari kegagalan, serta informasi yang diperlukan untuk melakukan kesalahan diagnosis, dan kebutuhan untuk mengantisipasi kegagalan jaringan yang pada gilirannya dapat mengurangi waktu antara kegagalan dan pemulihan mereka.

2. Konsep Manajemen Jaringan OSI

Ada beberapa konsep manajemen jaringan yang didefinisikan dalam OSI, termasuk objek yang dikelola, manajer dan agen, dan basis informasi manajemen. Fault Management (Manajemen Kesalahan) sebagai aplikasi manajemen jaringan menggunakan konsep yang sama.

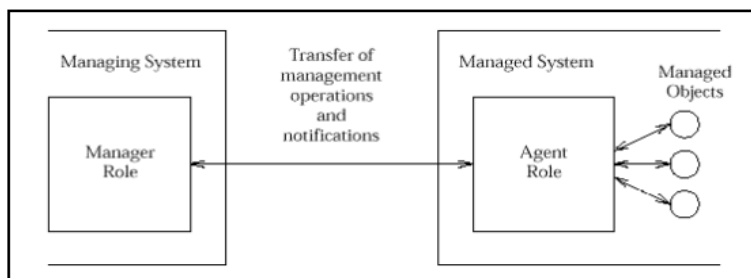
2.1 Objek yang Dikelola

Standar manajemen jaringan OSI menggunakan prinsip pemodelan objek. Objek yang dikelola membentuk representasi sumber daya abstrak dilihat dari perspektif pengelolaan. Misalnya, benda fisik seperti modem, atau seperti sirkuit koneksi. Objek yang dikelola ditandai oleh objeknya atribut, peristiwa yang mereka hasilkan, tindakan mereka melakukan dan perilaku yang mereka tunjukkan. Atribut berisi informasi yang menarik bagi manajemen tujuan, sedangkan pemberitahuan memodelkan acara yang bisa terjadi di tingkat sumber daya yang nyata untuk menghasilkan log. Operasi atau tindakan adalah himpunan prosedur yang dapat diterapkan pada objek. Dan akhirnya, perilaku bertanggung jawab untuk mendorong perubahan pada

objek yang dihasilkan dari pelaksanaan operasi. Objek yang dikelola disimpan dalam informasi manajemen base (MIB). Karenanya, semua perangkat fisik dan logis akan dipantau dan dikelola oleh aplikasi manajemen kesalahan sebagai kelas objek yang dikelola.

2.2 Manajer dan Agen

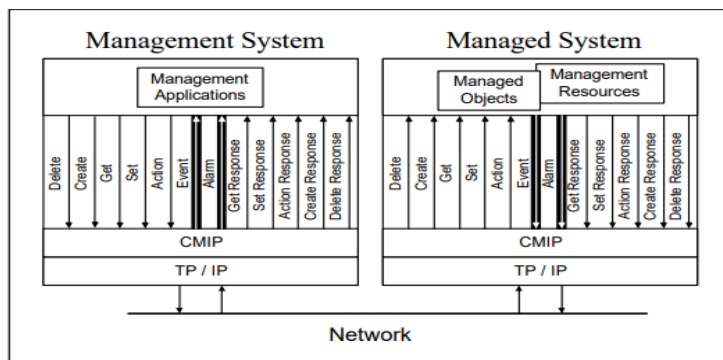
Karena manajer tidak dapat secara efektif mengendalikan atau mengelola sejumlah besar objek secara langsung, mempekerjakan agen (juga dikenal sebagai manajer agen atau proses agen) yang mengendalikan himpunan bagian dari objek yang dikelola. Manajer dan agen bertukar informasi manajemen menggunakan CMIS / CMIP yang merupakan layanan dan protokol manajemen jaringan disediakan oleh standar OSI. Manajer bertukar informasi dengan mengirimkan permintaan ke dan menerima tanggapan atau pemberitahuan dari agen. Sebaliknya, agen menerima permintaan dari dan memancarkan tanggapan atau pemberitahuan kepada manajer secara tidak sinkron.



Gambar 1 : Model untuk Manajemen Komunikasi

2.3 Basis Informasi Manajemen

MIB berisi gambar abstrak yang dikelola objek dalam jaringan, dan menyediakan metode yang berkaitan dengan objek yang dikelola satu sama lain. Caranya dengan memanipulasi benda-benda virtual dalam MIB bahwa sumber daya yang sebenarnya dalam sistem yang dikelola dapat diperiksa atau diubah oleh manajer jaringan. MIB berisi virtual gambar tentang bagaimana suatu jaringan berperilaku kapan saja. Dalam MIB, objek yang dikelola diatur dalam sebuah hierarki penahanan atau struktur pohon, di mana node bawahan pada pohon terkandung dalam superior benda. Pohon ini disebut pohon informasi manajemen (MIT). Setiap objek yang dikelola memiliki nama, dan nama ini dibentuk dengan menggabungkan nama-nama semua atasan benda di dalam MIT. Nama-nama ini digunakan untuk memilih objek yang dikelola selama pertukaran informasi yang terjadi antara manajer dan agen.



Gambar 2: Model kerja CMIP: Antarmuka dengan lapisan atas

2.4 Entitas Manajemen Jaringan OSI

OSI sendiri terdiri dari tujuh lapisan. Ini menggunakan pendekatan manajemen, serta entitas terlibat, diperiksa lebih dekat pada bagian ini. Dukungan OSI untuk berbagai persyaratan manajemen jaringan disediakan dalam tiga cara berikut. Pertama, sebagai fungsi yang dilakukan oleh protokol sendiri, kedua, sebagai entitas yang mengelola lapisan protokol tertentu, atau akhirnya sebagai aplikasi manajemen sistem mengelola keseluruhan tumpukan protokol, manajer lapisan protokol, dan subnet. Paket protokol menyediakan komunikasi langsung dan kemampuan dukungan pemrosesan terdistribusi, dan izin setiap lapisan protokol untuk memantau dan mengontrol satu instance komunikasi di dalam lapisan. Sistem aplikasi manajemen (SMA) seperti manajemen kesalahan adalah fasilitas manajemen tambahan yang diperlukan untuk memantau, mengontrol dan mengelola keseluruhan sumber daya OSI yang menyediakan kemampuan komunikasi dan dukungan lingkungan jaringan terbuka. Kelima jaringan ini area fungsional manajemen menyediakan aplikasi untuk berbagai fungsi pengambilan keputusan yang digunakan untuk mengelola suatu seluruh sistem OSI (tumpukan tujuh lapis). SMA diwujudkan melalui seperangkat baik terpusat atau didistribusikan proses aplikasi manajemen jaringan yang berada di atas lapisan ke-tujuh. Kerangka kerja manajemen OSI menyediakan tiga tingkat manajemen sumber daya OSI:

- 1). Manajemen protokol terdiri dari mekanisme-mekanisme internal yang terkait dengan protokol di dalam salah satu dari protokol tersebut tujuh lapisan protokol yang diperlukan untuk mengendalikan tertentu contoh komunikasi. Manajemen protokol adalah dijelaskan dalam standar yang menggambarkan masing-masing protokol dan layanan layer.
- 2). Manajemen lapisan dapat memengaruhi banyak hal contoh komunikasi. Terdiri dari mereka kegiatan yang diperlukan untuk mengelola semua sumber daya OSI terkait dengan lapisan protokol tertentu.
- 3). Manajemen sistem terdiri dari kegiatan-kegiatan diperlukan untuk mengelola totalitas sumber daya OSI terkait dengan setiap atau semua lapisan protokol di dalamnya sistem terbuka.

3. Manajemen Kesalahan

Pada bagian ini akan memberikan definisi beberapa istilah terkait dalam kesalahan jaringan dan memperkenalkan ciri-ciri masalah tersebut yang sering ditemui dalam melakukan Fault Management (Manajemen Kesalahan).

3.1 Definisi, Istilah Dan Karakteristik Kesalahan

Kesalahan perangkat lunak atau cacat perangkat keras dalam sistem yang mengganggu komunikasi atau menurunkan kinerja. Kesalahan merupakan output yang salah dari komponen sistem. Kesalahannya dapat berupa penyebab langsung atau tidak langsung dari kesalahan. Kesalahan adalah manifestasi dari kesalahan. Kegagalan adalah hasil keseluruhan dari kesalahan. Namun, jika komponen menghasilkan kesalahan, kami tidak dapat menyimpulkan bahwa ada kesalahan terdapat dalam komponen. Kesalahan jaringan dapat ditandai oleh beberapa aspek seperti sgejalanya, penyebaran (transmisi kesalahan) dari satu komponen ke komponen lain), durasi dalam jaringan dan tingkat keparahan. Padahal kesalahan jaringan bisa dibedakan melalui karakteristik mereka, perlu dicatat bahwa memang agak sulit untuk mengukur sifat-sifat ini secara akurat karena cara mereka dikendalikan dan dikelola. Terjadinya kesalahan dapat dideteksi oleh pengguna melalui gejala yang mungkin dihasilkan oleh beberapa komponen jaringan sebagai akibat dari kesalahan. Gejala kesalahan dapat dikaitkan dengan empat jenis kesalahan waktu, kesalahan tepat waktu, kesalahan komisi dan kelalaian.

Berikut adalah tanda-tanda Kesalahan dalam Jaringan:

- 1). Output dengan nilai yang diharapkan juga datang awal atau terlambat: Situasi ini disebabkan oleh kesalahan waktu. Ini biasanya dilihat oleh pengguna sebagai respons yang lambat atau time-out, ketika aplikasi mereka secara tidak langsung dipengaruhi oleh kesalahan fisik.
- 2). Output dengan nilai tak terduga dalam interval waktu yang ditentukan: Situasi ini disebabkan oleh kesalahan tepat waktu yang biasanya menunjukkan kesalahan kecil di aplikasi atau perangkat lunak yang mendasarinya dan perangkat keras.
- 3). Output dengan nilai yang tidak terduga di luar interval waktu yang ditentukan: Ini karena komisi kesalahan. Jika tidak ada respons yang dihasilkan, ini berarti terkait dengan kesalahan kelalaian. Kesalahan kelalaian bisa jadi dianggap sebagai kasus khusus kesalahan komisi. Sebuah kesalahan komisi biasanya menyiratkan kesalahan yang parah terjadi pada jaringan.

Jika gejala ini diamati, ada kemungkinan bahwa kesalahan terjadi di suatu tempat pada jaringan yang mengakibatkan komponen untuk menghasilkan output yang salah (error). Sebuah kesalahan dalam satu komponen dapat memiliki konsekuensi pada yang lain komponen terkait. Selain gagal sistemnya sendiri, itu dapat menghasilkan kesalahan yang dapat ditransmisikan ke yang lain komponen dan menurunkan sistem lainnya juga. Di dalam cara, kesalahan dalam komponen tunggal dapat memiliki efek global di jaringan. Fenomena ini disebut sebagai kesalahan perambatan. Kesalahan yang terjadi dalam sistem yang terisolasi mungkin tidak mempengaruhi sistem lain karena tidak ada interaksi diantara mereka. Namun, ketika sistem yang terisolasi itu dihubungkan bersama oleh komunikasi, kesalahan yang dihasilkan oleh kesalahan dapat melakukan perjalanan dalam paket ke sistem lain. Sebuah komponen bisa gagal karena kesalahan di dalamnya dan input yang salah dihasilkan oleh kesalahan pada komponen lainnya. Ini adalah salah satu karakteristik utama dari kesalahan jaringan. Media untuk propagasi kesalahan meliputi parameter, data, dan lalu lintas. Durasi kesalahan jaringan, meskipun diakui sebagai satu kriteria penting agak sulit diukur. Ini karena tiga alasan. Pertama, kesalahan tidak akan terjadi dirasakan sampai menghasilkan kesalahan. Kedua, mungkin butuh waktu yang lama untuk kesalahan tertentu untuk diisolasi. Akhirnya, efek dari kesalahan jaringan tidak dapat dihilangkan secara otomatis ketika kesalahan dihapus. Mereka akan tetap untuk beberapa waktu sampai operasi sepenuhnya pulih. Oleh karena itu, kesalahan jaringan hanya bisa secara umum dibagi menurut durasinya menjadi tiga kelompok: permanen, intermiten dan sementara. Kesalahan permanen akan ada di jaringan sampai tindakan perbaikan telah dilakukan diambil. Ini menghasilkan degradasi maksimum permanen layanan. Kesalahan intermiten terjadi secara terputus-putus dan secara berkala. Hasilnya akan menjadi kegagalan diproses saat ini. Ini menyiratkan degradasi maksimum tingkat layanan untuk waktu yang singkat. Sementara kesalahan akan menyebabkan sedikit degradasi layanan. Kesalahan jenis pertama akan menyebabkan laporan acara untuk dikirim dan perubahan yang dilakukan dalam jaringan konfigurasi untuk melarang pemanfaatan lebih lanjut dari sumber ini. Untuk kesalahan jenis kedua, tingkat keparahan kesalahan mungkin pindah dari yang terputus-putus menjadi permanen jika suatu terjadinya kesalahan jenis ini menjadi berlebihan penting. Akhirnya, kesalahan sementara biasanya akan terjadi ditutupi oleh prosedur pemulihan kesalahan jaringan protokol dan karenanya tidak dapat diamati oleh pengguna. Ini penting bagi perancang manajemen kesalahan sistem untuk memiliki pengetahuan tentang karakteristik kesalahan. Ini adalah karena tidak semua kesalahan akan memiliki prioritas yang sama. Kesalahan perancang sistem manajemen harus memutuskan yang mana kesalahan harus dikelola

3.2 Proses Manajemen Kesalahan

Literatur terbaru menunjukkan bahwa sistem Manajemen Kesalahan (Fault Management) terdiri dari pemantauan, pelaporan, pencatatan, masalah penjualan tiket, pemfilteran, korelasi, diagnosis dan kegiatan pemulihan. Bagian ini mencoba membahas domain di mana sistem manajemen kesalahan akan beroperasi. Deteksi kesalahan memberikan kemampuan untuk mengenali kesalahan. Terdiri dari kegiatan pemantauan dan pelaporan. Informasi disediakan oleh perangkat pemantauan harus terkini, tepat waktu, akurat, relevan, dan lengkap. Kegiatan pelaporan termasuk investigasi kriteria kritis yang membutuhkan pemberitahuan dan mekanisme untuk pembuatan laporan. Juga melibatkan penentuan tujuan pengiriman yang tepat dengan pemberitahuan. Tujuannya adalah untuk mengisolasi kesalahan yang sebenarnya, mengingat sejumlah kesalahan kemungkinan hipotesis kesalahan. Pengujian mungkin yang paling banyak cara yang tepat untuk mengisolasi kesalahan pada tahap ini. Isolasi terdiri dari empat kegiatan: penyaringan, interpretasi, korelasi dan diagnosis. Filtrasi melibatkan analisis informasi manajemen untuk mengidentifikasi kesalahan baru atau jika kesalahan telah terjadi sebelumnya, untuk memperbarui hitungannya. Filtrasi membuang pemberitahuan informasi manajemen yang tidak penting dan rute yang berlaku pemberitahuan ke tujuan yang sesuai di dalam sistem. Informasi penting terkandung dalam acara tersebut laporan harus diekstraksi. Di sini sifat, struktur dan signifikansi laporan acara diperiksa. Informasi penting seperti nama laporan acara yang biasanya mewakili kondisi yang telah ditetapkan itu bertemu dan memicu pembuatan laporan acara diri. Informasi bermanfaat lainnya adalah waktu ketika acara laporan telah dihasilkan. Informasi ini penting ketika melakukan aktivitas korelasi sehingga kita dapat membedakan peristiwa mana yang terkait, dan mana yang tidak. Korelasi terbukti sangat membantu, ketika dua atau lebih pemberitahuan yang diterima sebenarnya karena satu kesalahan. Melalui korelasi, beberapa kesalahan dapat dideteksi secara tidak langsung. Hipotesis dapat diambil dari pemberian korelasi alarm kemungkinan penyebab kesalahan. Tujuan diagnosis proses adalah untuk mengisolasi penyebab kesalahan ke jaringan sumber. Diberikan serangkaian kemungkinan penyebab, diagnosis proses dilakukan. Ini melibatkan identifikasi dan analisis masalah dengan mengumpulkan, memeriksa dan menguji gejala, informasi dan fakta. Setelah diisolasi, efek dari kesalahan harus diminimalkan melalui pintas dan pemulihan, dan perbaikan permanen dilembagakan. Jika berlaku, langkah-langkah harus diambil untuk memastikan masalah tidak terulang kembali. Prosedur ini terdiri dari tiga kegiatan: konfigurasi ulang, pemulihan dan pemulihan. Konfigurasi ulang atau mem-bypass melibatkan pengaktifan sumber daya yang berlebihan khusus ditugaskan untuk cadangan kritis entitas, layanan menanggulangi, atau mengalokasikan kembali sumber daya untuk kegunaan yang lebih penting. Tujuannya adalah untuk mengurangi dampak langsung dari kegagalan. Fungsi ini mungkin dalam a campuran prosedur manual, semi-otomatis dan otomatis. Itu dimungkinkan untuk kesalahan pulih sebelum upaya konfigurasi ulang dilakukan. Ini tergantung pada sifat kegagalan, kekritisitas layanan dan waktu yang dibutuhkan untuk memulihkan / mengkonfigurasi ulang. Sekali kesalahan telah diperbaiki, perbaikan perlu diuji dan entitas kembali ke layanan. Ini perlu dijadwalkan pada waktu yang tepat dan tergantung pada layanan yang diharapkan gangguan dalam melakukannya. Layanan administrasi kesalahan memastikan bahwa kesalahan tidak hilang atau diabaikan, tetapi mereka dipecahkan secara tepat waktu. Ini melibatkan pemantauan catatan kesalahan, memelihara arsip informasi kesalahan, menganalisis tren, pelacakan biaya, mendidik personel dan menegakkan kebijakan perusahaan berkaitan dengan resolusi masalah. Terdiri dari tiga kegiatan: logging, pelacakan dan analisis tren. Penebangan memelihara log laporan acara tentang kesalahan yang terjadi terjadi di jaringan. Ini akan digunakan untuk tren analisis, pelaporan dan diagnosis di masa depan untuk jenis yang sama atau kegagalan serupa. Pelacakan melacak yang ada masalah dan orang yang bertanggung jawab untuk dan / atau bekerja pada masing-masing, memfasilitasi komunikasi antara masalah memecahkan entitas dan mencegah pemecahan masalah duplikat upaya. Ini termasuk memprioritaskan kesalahan terbuka keparahan mereka, dan peningkatan isolasi kesalahan atau proses

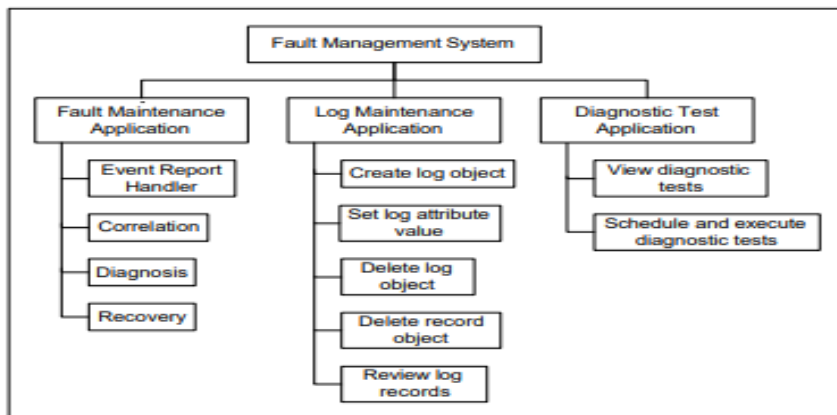
koreksi berdasarkan durasi dan tingkat keparahan kesalahan. Catatan kesalahan terbuka saat ini perlu dipesan menurut skema prioritas sedemikian rupa sehingga paling mahal, atau potensi kegagalan yang mahal diselesaikan secara tepat waktu. Seluruh kegiatan dapat diselesaikan menggunakan tiket bermasalah sistem. Informasi penting termasuk frekuensi terjadinya kegagalan tertentu dan berapa banyak turun waktu berbagai pengguna mengalami. Tren mungkin menunjukkan kebutuhan untuk mendesain ulang bidang komunikasi lingkungan, ganti peralatan yang lebih rendah, tingkatkan masalah memecahkan keahlian, memperoleh alat pemecahan masalah baru, memperbaiki prosedur penyelesaian masalah, meningkatkan pendidikan, negosiasi ulang perjanjian tingkat layanan. Dalam proyek ini, semuanya kegiatan dalam deteksi kesalahan dan prosedur isolasi dan beberapa aspek dalam prosedur pemulihan dan administrasi diimplementasikan.

3.3 Masalah Umum

Salah satu masalah paling kritis yang terkait dengan kesalahan pemantauan. Dalam situasi ini, kesalahan tertentu tidak dapat diobservasi melalui pengamatan lokal. Misalnya, adanya kebuntuan antara kerja sama proses terdistribusi mungkin tidak dapat diamati secara lokal. Lain kesalahan mungkin tidak dapat diamati karena peralatan vendor tidak diinstrumentasi untuk mencatat terjadinya kesalahan. Masalah lain didefinisikan oleh Fried dan Tjong sebagaimengikuti. Terlalu banyak pengamatan terkait: Kegagalan tunggal dapat mempengaruhi banyak jalur komunikasi aktif. Kesalahan dari tulang punggung WAN akan mempengaruhi semua komunikasi aktif antara stasiun token-ring dan stasiun di Ethernet LAN, serta komunikasi suara antara PBX. Selanjutnya, kegagalan dalam satu lapisan arsitektur komunikasi dapat menyebabkan degradasi atau kegagalan di semua lapisan yang lebih tinggi tergantung. Semacam ini kegagalan adalah contoh penyebaran kegagalan. Karena kegagalan tunggal dapat menghasilkan banyak kegagalan sekunder, dapat terjadi sekitar waktu yang sama dan mungkin sering mengaburkan masalah mendasar tunggal. Tidak adanya pengujian otomatis alat: Menguji untuk mengisolasi kesalahan itu sulit, mahal dan memakan waktu. Ini membutuhkan keahlian yang signifikan dalam perangkat perilaku dan alat untuk mengejar pengujian. Bahkan sesederhana itu tugas sebagai melacak progres paket sepanjang virtual sirkuit biasanya tidak mungkin untuk dicapai. Ini mengarah ke aturan operasi empiris sebagai “satu-satunya cara untuk menguji apakah sirkuit virtual naik, adalah untuk menjatuhkannya. Proses pemulihan biasanya melibatkan kombinasi pengaturan ulang lokal otomatis dikombinasikan dengan aktivasi manual prosedur pemulihan. Pemulihan menyajikan sejumlah tantangan teknis yang menarik. Yang termasuk otomatis pemulihan sebagai sumber kesalahan: Karena sebagian besar perangkat jaringan atau proses dirancang untuk pulih secara otomatis dari kegagalan lokal, ini juga bisa menjadi sumber kesalahan. Itu masalah dalam administrasi kesalahan adalah pemeliharaan kesalahan laporan log yang telah dipersulit karena kurangnya fungsi untuk membuat atau menghapus catatan. Itu Fasilitas logging biasanya dilakukan secara statis, di mana karakteristik penebangan stagnan. Karena itu, beberapa kejadian kesalahan penting tidak dapat terjadi tercatat. Jika nilai atribut log dapat diubah, perilaku logging juga dapat diubah.

4. FMS: Sistem Manajemen Kesalahan

Untuk mengatasi masalah yang dirinci di atas, kami merancang dan mengimplementasikan FMS. Ini menawarkan tiga jenis aplikasi manajemen kesalahan, yaitu Aplikasi Pemeliharaan Kesalahan (FMA), Log Perawatan Aplikasi (LMA), dan Aplikasi Tes Diagnostik (DTA). Aplikasi manajemen kesalahan ini bekerja bersama dengan Agen OSI untuk melakukan kesalahan tugas manajemen pada sumber daya jaringan. OSI Agen berfungsi sebagai agen pemantau kesalahan. Itu memiliki kemampuan untuk melaporkan kesalahan secara independen ke FMA. Bisa juga mengeluarkan laporan saat variabel yang dipantau melintasi ambang. Ini memungkinkan FMS untuk mengantisipasi kesalahan. Di Selain itu, ia memelihara log peristiwa. Log ini bisa jadi diakses dan dimanipulasi oleh LMA. DTA menyediakan satu set tes diagnostik yang dapat diminta oleh pengguna. Ini Fasilitas bermanfaat bagi administrator jaringan kapan saja ada kecurigaan bahwa beberapa sumber daya tidak berfungsi seperti yang diinginkan. Paragraf berikut menjelaskan bagaimana fasilitas ini membantu meningkatkan efisiensi manajemen kesalahan. FMA memecahkan masalah kesalahan yang tidak dapat diobservasi karena peralatan vendor yang tidak lengkap untuk mencatat terjadinya sebuah kesalahan. Ini dilakukan dengan memonitor sumber daya nyata sifat kritis dan ketika peristiwa penting melibatkan sifat ini terjadi, peristiwa ini dilaporkan ke FMA jadi penyelidikan lebih lanjut dimulai. FMA bertindak atas nama terima kejadian ini dengan melakukan kesalahan lain proses manajemen pada mereka. Proses-proses ini termasuk interpretasi dan penyaringan acara, korelasi acara, dan tes diagnostik yang telah ditetapkan serta memulai proses recovery.



Gambar 3 : Arsitektur Sistem Fault Management (Manajemen Kesalahan)

Di sisi lain, DTA menyediakan fungsi untuk memungkinkan tes diagnostik dilakukan oleh pengguna. Ini terbukti bermanfaat bagi pengguna yang berpengalaman yang ingin melewati tes sepele dan hanya memilih yang lebih spesifik. Ini mengonsumsi sumber daya jaringan yang lebih rendah untuk tujuan manajemen. Kurang memadainya alat untuk audit sistematis diatasi oleh dukungan disediakan oleh LMA. LMA memiliki kemampuan untuk memulai kondisi kesalahan (peristiwa) logging. Selanjutnya, LMA dapat mengakses log ini dan mengontrol perilaku logging dengan mengatur nilai atribut log mereka. Dukungan lain termasuk fasilitas untuk menghapus log dan catatan log, dan meninjau peristiwa (dengan meninjau catatan log) untuk diagnostik analisis tujuan atau tren.

4.1 Aplikasi Manajemen

Aplikasi Manajemen sudah dikembangkan pada bahasa C ++. Ada tiga kelompok Aplikasi Manajemen, yakni FMA, LMA dan DTA. Semua aplikasi ini termasuk formulir yang dapat dieksekusi. Aplikasi Manajemen menggunakan Manajer Sistem OSI untuk mengirim operasi manajemen ke Agen Manajemen Sistem OSI.

1). FMA

Aplikasi manajemen ini terdiri dari berbagai macam fungsi manajemen sebagaimana dijelaskan dalam Bagian ini. Ini berhubungan dengan laporan acara dari saat mereka diterima sampai tindakan recovery terjadi. Prosedur manajemen kesalahan diwujudkan melalui acara fungsi manajemen penanganan, korelasi kejadian, diagnosis kesalahan dan kesalahan pemulihan secara otomatis.

2). LMA

Logger ini menyelesaikan tugas menjaga log laporan acara. Ini adalah alat untuk analisis tren dan pelaporan, dan menyediakan perpustakaan untuk diagnosis di masa depan yang sama atau masalah serupa. LMA sendiri diwujudkan dalam tiga program terpisah. Fasilitas untuk logging dan pengaturan log nilai atribut direalisasikan oleh program LogSet.

3). DTA

Alat ini ada untuk kenyamanan pengguna dengan tanggung jawab administrator jaringan atau teknisi. Itu memungkinkan pengguna untuk melakukan tes diagnostik tertentu sumber daya jaringan. Tujuannya adalah untuk memeriksa apakah tes diagnostik menyediakan fungsi dengan benar atau untuk melakukan a diagnostik rutin sebagai hasil peninjauan riwayat log direkam oleh log di SMA.

5. Manajer Sistem

OSI System Manager adalah aplikasi yang memiliki tanggung jawab untuk satu atau lebih kegiatan manajemen. Itu masalah permintaan operasi manajemen (tindakan) dan menerima pemberitahuan (acara) atas nama Fungsi Aplikasi Manajemen. Oleh karena itu terdiri dari serangkaian program yang menghubungkan Sistem OSI Agen Manajemen dan mengambil manajemen informasi. Program-program ini adalah implementasi dari primitif CMIS. Mereka digunakan oleh Manajemen Aplikasi untuk melakukan berbagai manajemen kesalahan fungsi. Manajer Sistem OSI mengirim perintah ke Agen Manajemen Sistem OSI dalam permintaan CMIS membentuk dan menunggu balasan.

5.1 Agen Manajemen Sistem

Akses ke elemen jaringan yang ditentukan untuk MA adalah melalui agen. Akses ke elemen jaringan melibatkan mengumpulkan informasi statistiknya dan memanipulasi untuk kegiatan manajemen. SMA diwujudkan sebagai tunggal Proses UNIX. SMA adalah dukungan agen OSI yang disediakan dengan RUPS OSIMIS. SMA mendukung ISO CMIP protokol. Ia melakukan pelingkupan dan penyaringan pada objek dalam contoh MIB dan secara otomatis menangani semua Fungsi CMIP. Ini melakukan operasi manajemen sebagai hasil operasi manajemen yang dikomunikasikan dari Aplikasi Manajemen. Tanggung jawabnya juga termasuk mengeluarkan pemberitahuan yang mencerminkan perilaku benda yang dikelola.

5.2 Basis Informasi Manajemen

MIB diimplementasikan untuk setiap protokol yang berpartisipasi yaitu X.25 MIB. MIB berkomunikasi dengan FMS melalui ISO CMIS dan CMIP. Fasilitas termasuk kemampuan untuk membaca dan menulis atribut objek terkelola tertentu, kemampuan untuk menambah dan menghapus elemen ke / dari "nilai set" atribut, pembuatan laporan acara secara spontan dan manajemen asosiasi dengan manajer jarak jauh proses. Pohon objek yang dikelola untuk suatu sistem bervariasi seperti aktivitas jaringan bervariasi. Implementasinya mencerminkan hal ini dengan benda yang dibuat dan dihancurkan seperlunya. Itu MIB lebih dari sekedar database pasif. Itu implementasi mendukung peristiwa yang ditentukan yang menentukan tindakan yang harus diambil ketika insiden jaringan tertentu terjadi.

5.3 Program Antarmuka Sumber Daya Nyata

Ini adalah bagian khusus untuk objek yang dikelola tertentu mewakili sumber daya nyata. Ini harus dirancang tidak hanya untuk jenis sumber daya nyata tetapi juga untuk cara bagaimana sumber daya nyata digunakan untuk menyajikan informasi manajemen. Ini tidak disediakan oleh RUPS dan harus dilaksanakan oleh pelaksana MIB. Sumber daya nyata ini mungkin berada di kernel sistem operasi, pada papan komunikasi, dalam proses ruang pengguna atau bahkan pada sistem jarak jauh yang dikelola melalui manajemen proxy. Demikian antarmuka program bervariasi sesuai dengan informasi manajemen dari sumber daya nyata mana yang ingin mereka akses.

6. Kesimpulan

Kebanyakan orang saat ini bergantung pada komputer agar pekerjaan dapat selesai dengan lebih cepat. Ini berarti bahwa jaringan komputer harus tersedia setiap saat dan menawarkan kinerja yang baik dan optimal. Adanya kesalahan / kegagalan tidak dapat ditoleransi dan harus dihindari. Karenanya, manajemen proaktif dari Fault Management Network harus disertakan saat merencanakan jaringan komputer. Kami telah menggambarkan konsep jaringan OSI manajemen, dan menemukan bahwa bagian penting dari OSI manajemen melibatkan manajemen jaringan aplikasi (umumnya dikenal sebagai FCAPS). Kesalahan area fungsional manajemen dan masalah terkait telah diperiksa secara rinci. Kesimpulannya yang dapat ditarik adalah bahwa manajemen kesalahan jaringan di lingkungan seperti itu dapat dicapai secara lebih baik dengan memberikan dukungan kesalahan berbasis aplikasi manajemen OSI untuk membantu administrator jaringan dan teknisi melakukan tugas Fault Management (Manajemen Kesalahan). Sistem menawarkan berbagai fasilitas manajemen kesalahan melalui tiga aplikasi manajemen. Pemanfaatan CMIS / CMIP OSI untuk meminta operasi dan menerima pemberitahuan telah membuktikan fleksibilitas dan kekayaan yang ditawarkan oleh layanan ini. Koneksi mode layanan OSI mendukung transmisi yang andal dan sangat berguna untuk FMA yang harus menerima pemberitahuan tentang penyimpangan ambang batas atribut atau kesalahan kejadian segera setelah peristiwa terdeteksi. Oleh karena itu, sistem diharapkan untuk mempromosikan implementasi bidang fungsional manajemen lainnya, seperti pemanfaatan protokol manajemen OSI, sehingga mempromosikan Sistem Terbuka.

Referensi

- [1] A. Patel, "Security management for OSI networks", Computer Communications, Vol 17, No. 5, July 1994, p. 546.
- [2] M. Jander, "Network Management Systems Get to Work", Data Communications, July 1991.
- [3] Abderrahman, "What's Needed for Distributed Systems Management", International Journal of Network Management, June, 1993.
- [4] Joseph, J. Kindrick, K. Muralidhar, C. So, T. TothFejel, "MAP Fault Management Expert System", Integrated Network Management I, B. Meandzija and J. Westcott (Editors) Elsevier Science Publishers B.V. (North-Holland), IFIP, 1989
- [5]] T. Bouloutas, S. Calo, A. Finkel, "Alarm Correlation and Fault Identification in Communication Networks", IEEE Transactions On Communications, Vol. 42, No. 2/3/4, February/ March/April 1994.
- [6] L. Madruga, L. M. R. Tarouco, "Fault Management Tools for a Cooperative and Decentralized Network Operations Environment", IEEE Journal on Selected Areas in Communications, Vol. 12, No. 6, August 1994.
- [7] Jailani, Norleyza. Ahmed Patel "FMS: A COMPUTER NETWORK FAULT MANAGEMENT SYSTEM BASED ON THE OSI STANDARDS", Malaysian Journal of Computer Science, Vol. 11 No. 1 , June 1998
- [8] Clemm, Alexander, 2007, Network Management Fundamentals, Cisco Press