SISTEM MONITORING JARINGAN INTERNET LAPAN BANDUNG

Oleh

RIZAL SURYANA

Pusat Pemanfaatan Sains Antariksa
Lembaga Penerbangan dan Antariksa Nasional

ABSTRACT

The condition of each server and computer network should always be monitored by the administrator because all servers are stored in a special room and not equipped with a monitor, and the frequent loss of quality internet connection. When the server and the internet network was down, then the state server can't be seen directly in front of the desk but had to go to the server room or remote login. If the server is located outside the city or outside the island, the network administrator can't go any place when the server was just to see the condition of the server and the Internet network. Sometimes the server or the network conditions at a particular internet was down, so that the examination conducted interference on each server and associated network, such as the reduction by the problem becomes difficult and time consuming. Monitoring conducted to facilitate the monitoring of the condition of each server, internet network and bandwidth internet LAPAN Bandung. Detecting the cause of the disorder can be identified easily and quickly, so that bug fixes can be done as soon as possible, keeping the performance of Internet networks LAPAN Bandung and detection the cause of decline in the Internet connection bandwidth and peak bandwidth usage internet.

Keywords: *Network Monitoring, Nagios, Lightsquid, Bandwidth Monitoring*

RINGKASAN

Kondisi setiap server dan jaringan komputer harus selalu dimonitoring oleh administrator karena semua server tersimpan di ruangan khusus dan tidak dilengkapi dengan monitor, serta sering terjadinya penurunan kualitas koneksi internet. Ketika server dan jaringan internet mengalami gangguan, maka kondisi server tidak dapat dilihat secara langsung didepan meja kerja melainkan harus pergi ke ruangan server atau login secara remote. Seandainya server berada diluar kota atau diluar pulau, maka administrator jaringan tidak mungkin pergi setiap saat ketempat server berada hanya untuk melihat kondisi server dan jaringan internet. Terkadang kondisi server atau jaringan internet pada saat tertentu mengalami gangguan, sehingga pemeriksaan terjadinya gangguan dilakukan pada setiap server dan jaringan yang terkait, dengan cara

seperti penanggulangan masalah menjadi sulit dan memakan waktu yang lama. Monitoring dilakukan untuk mempermudah pemantauan kondisi setiap server, jaringan internet LAPAN Bandung dan bandwidth internet. Pendeteksian penyebab terjadinya gangguan dapat diketahui dengan mudah dan cepat, sehingga perbaikan gangguan dapat dilakukan sesegera mungkin, menjaga kinerja dari jaringan internet LAPAN Bandung dan mendeteksi penyebab penurunan bandwidth koneksi internet serta beban puncak pemakaian bandwidth internet.

Katakunci : Monitoring Jaringan, Nagios, Light Squid, Monitoring Bandwidth

1. PENDAHULUAN

LAPAN Bandung memiliki 2 koneksi internet yaitu internet dari ISP Melsa dan ISP ITB, dimana setiap koneksi memiliki router tersendiri, selain kedua router tersebut LAPAN Bandung memiliki web server, e -mail server, DNS server, ftp server, L*oad Balancing*, VPN server dan omni-switch. Kondisi jaringan baik internet maupun lokal sesakali mengalami gangguan, cara untuk melakukan pendeteksian gangguan dilakukan pada setiap server dan hub distribusi utama, pada hal server ataupun hub yang terganggu hanya satu tetapi pendeteksian gangguan dilakukan pada tiap-tiap server, sehingga penanganan gangguan memerlukan waktu yang relatif lama. Kondisi dari masing-masing server baik yang berada di jaringan komputer LAPAN maupun yang berada di pihak ISP tidak terpantau kondisinya karena untuk memilihat kondisi suatu server seorang administrator jaringan harus login atau melihat langsung ke ruangan server. Pemakaian Bandwidth internet sering dikeluhkan oleh client kepada administrator jaringan seiring dengan menurunya bandwidth untuk akses kesuatu alamat internet.

Monitoring selama ini dilakukan dengan cara me-remote kesalah satu server yang akan dimonitoring atau dengan cara menjalankan perintah *PING* dari client ke server tujuan, cara ini hanya bisa dilakukan ketika administrator jaringan berada di dalam jaringan LAPAN Bandung. Ketika administrator berada diluar jaringan komputer LAPAN Bandung, maka monitoring tidak dapat dilakukan karena port 22 untuk remote ke server ditutup untuk alasan kemanan jaringan. Penggunaan bandwidth selama ini hanya di monitoring dengan melihat grafik MRTG (Multi Router Traffic Grapher), monitoring seperti hanya melihat jumlah bandwidth yang dipakai, tetapi sebenarnya monitoring bandwidth dapat dilakukan dengan melihat aktivitas dari masing-masing client. Tidak menuntut kemungkin ada seorang client yang menggunakan bandwidth besar.

Monitoring pada jaringan komputer LAPAN Bandung dilakukan untuk mengetahui kondisi dari setiap server, HUB distribusi utama, pemakaian bandwidth, aktivitas client dan jaringan internet LAPAN Bandung dimanapun

administrator berada. Pendeteksian gangguan dapat dilakukan dengan cepat tanpa harus memeriksa seluruh kondisi server, HUB distribusi utama dan jaringan komputer yang ada. Bandwidth internet dapat dipantau setiap saat dan pemakaian bandwidth yang berlebih oleh client dapat di deteksi.

2. LITERATUR

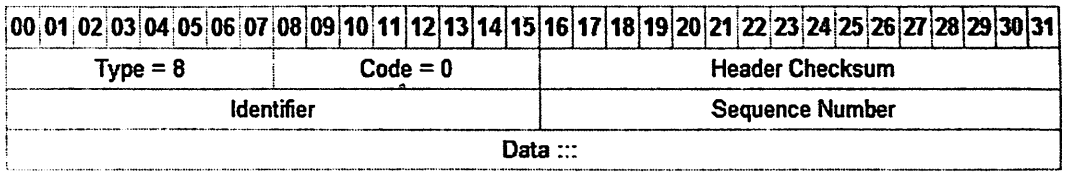
Round-robin database tool (RRDTool) berfungsi untuk menangani data time-series seperti bandwidth jaringan, temperatur, CPU load kemudian data tersebut di simpan dalam round-robin database (circular buffer), sehingga sistem terlihat tetap konstan selama waktu terntu. RRDtool mengasumsikan waktu-variabel data dalam interval panjang tertentu. Interval waktu ditentukan pada pembuatan sebuah file RRD dan file yang telah dibuat tidak dapat dirubah. Karena data mungkin tidak selalu tersedia pada waktu yang sama, RRDtool akan secara otomatis interpolasi apapun data yang diajukan sesuai dengan internal waktu. Nilai untuk setiap tahap tertentu, yang telah di terpolasikan menjadi sebuah titik data primer (PDP). Beberapa titik data primer dapat dikonsolidasikan menurut fungsi konsolidasi untuk membentuk sebuah titik data konsolidasi. Konsolidasi berfungsi untuk mendefinisakan nilai rata-rata, minimum dan maksimum. Setelah data dikonsolidasikan, titik data konsolidasi yang dihasilkan di simpan dalam arsip round-robin (RRA). Arsip A round-robin di simpan secara permanen dengan menjumlahkan titik data konsolidasi dan menentukan berapa banyak titik data primer yang harus digabungkan dalam satu titik data konsolidasi dan yang digunakan sebagai fungsi konsolidasi. Total waktu dihitung oleh Round-Robin Archive (RRA) dengan persamaan sebagai berikut:

time covered = (#CDPs stored) * (#PDPs per CDP) * step ..... (1)

Untuk menutupi beberapa timespans dan/atau menggunakan beberapa fungsi konsolidasi, sebuah file RRD mungkin berisi beberapa RRAS. Berfungsi mengambil data dari RRDtool secara otomatis, memilih arsip dengan resolusi tertinggi yang masih meliputi jangka waktu yang diminta. Mekanisme ini juga digunakan oleh RRDtool's grafik subsistem.

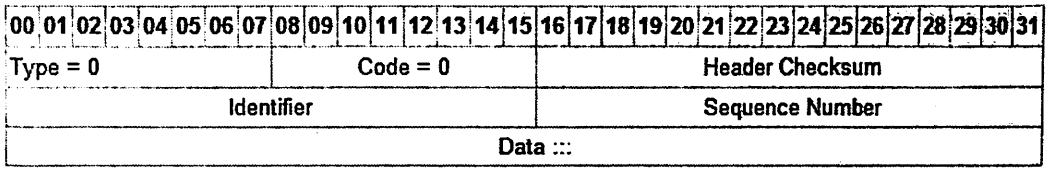
Ping adalah utilitas administrasi jaringan komputer digunakan untuk menguji apakah suatu host tertentu bisa diakses di Internet Protocol (IP) jaringan dan mengukur waktu round-trip untuk paket yang dikirim dari host lokal ke komputer tujuan, termasuk untuk dirinya sendiri. Ping bekerja dengan mengirimkan paket Internet Control Message Protocol (ICMP) ke host target dan menunggu respon ICM. Dalam proses mengukur waktu round-trip dan mencatat semua paket yang hilang [Marjorie Flack, Kurt Wiese, 2008]. Hasil tes dicetak dalam bentuk ringkasan statistik paket respon yang diterima, termasuk minimum, maksimum, rata-rata waktu round-trip, dan kadang-kadang standar deviasi dari rata-rata. Penggunaan utilitas ping biasanya digambarkan sebagai sebuah host ping ke komputer. Ping memiliki berbagai opsi baris perintah yang

tergantung pada sistem operasi host yang memungkinkan modus operasi khusus, seperti untuk menentukan ukuran paket yang digunakan sebagai pemeriksa, pengiriman ulang dilakukan secara otomatis untuk tahapan berikutnya, pemilihan atau untuk melakukan pengirim paket besar. Flood ping dapat disalah gunakan sebagai bentuk sederhana penyerangan denial-of-service attack, di mana penyerang mengirimkan permintaan paket ICMP ke komputer tujuan. Permintaan paket data ICMP yang diharapkan akan diterima kembali dalam sebuah echo reply ("ping"). Host yang dituju harus menanggapi semua permintaan echo reply dengan balasan yang berisi data tepat yang diterima sesuai dengan permintaan.



Gambar 2.1 Format Pesan Permintaan ICMP

Mengidentifikasi dan mengurutankan nomor yang dapat digunakan oleh klien untuk mencocokkan jawaban dengan permintaan yang menjadikan jawaban. Pada kenyataanya sebagian besar sistem Linux menggunakan pengenal unik untuk setiap proses ping, dan *sequence number* dalam melakukan proses. Windows menggunakan pengidentifikasi tetap, yang bervariasi antara versi Windows dan *sequence number* yang hanya mengatur ulang pada saat boot. Data yang diterima oleh Echo Request harus sepenuhnya dimasukkan dalam Echo Reply. E*cho reply* adalah sebuh paket ICMP yang dibuat atas dasar respon dari *echo request* dan merupakan sebuah perintah untuk semua *hosts* dan *router.*



Gambar 2.2 Format Pesan Jawaban ICMP

Type dan kode harus diset menjadi nilai 0, identifikasi dan pengurutan nomor dapat digunakan oleh client untuk menentuk paket permintaan dengan paket balasan. Data yang diterima dalam paket permintaan harus sepenuhnya dimasukan kedalam paket balasan.

Simple Network Management Protocol (SNMP) adalah jaringan berbasis UDP protokol. Protokol ini digunakan terutama dalam sistem manajemen jaringan untuk memonitor perangkat jaringan terikat untuk kondisi yang menjamin perhatian administratif. SNMP adalah sebuah komponen dari Internet Protocol Suite sebagai mana didefinisikan oleh

Internet Engineering Task Force (IETF). Terdiri dari satu set standar untuk pengelolaan jaringan, termasuk protokol lapisan aplikasi, skema database, dan satu set data obyek. [RFC1065, 1988]. SNMP mengekspos manajemen data dalam bentuk variabel pada sistem yang dikelola menggambarkan konfigurasi sistem. Tipe SNMP digunakan oleh satu atau lebih administrasi komputer yang mempunyai tugas pemantauan atau mengelola kelompok host atau perangkat pada jaringan komputer. Protokol SNMP yang beroperasi pada lapisan aplikasi Internet Protocol Suite (Layer 7 dari model OSI). Biasanya SNMP menggunakan UDP port 161 untuk client dan 162 untuk Server. Server mungkin akan mengirimkan permintaan dari sumber apapun yang tersedia port to port 161 di client. Tanggapan client akan dikirim kembali ke port sumber, server biasanya menerima pemberitahuan pada port 162. Client dapat menghasilkan pemberitahuan dari apapun yang tersedia port. Komponen dasar dari SNMP terdiri dari tiga komponen utama yaitu Managed device (Slave Device, Agent (software yang berjalan di Slave Device), Network Management System (NMS) merupakan software yang berjalan pada server.

3. METODOLOGI

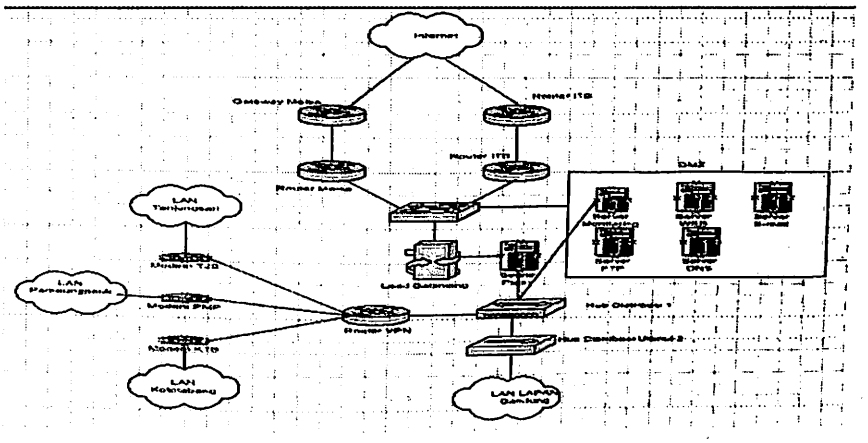
Monitoring jaringan komputer akan dibagi menjadi dua bagian yaitu monitoring jaringan internet yang terdiri dari koneksi internet ISP Melsa dan ISP ITB meliputi gateway ISP Melsa dan ISP ITB, router, DNS Server, web server, email server, load balancing, ftp server, VPN server dan server basis data. Software untuk monitoring jaringan internet menggunakan nagios yang terinstal pada server VPN, memakai komputer HP ML350 dengan spesifikasi CPU intel Xeon 2 GHz, memory 2 GB, hardisk 160 GB, 2 interface LAN dan sistem operasi linux ubuntu versi 8.04. Jaringan komputer lokal meliputi proxy server, router VPN, modem VPN Tanjungsari, modem VPN Pameungpeuk, modem VPN Kototabang, Server Bank Data Tanjungsari, Server Bank Data Pameungpeuk, Server Bank Data Kototabang dan Hub distribusi utama (omni-switch). Monitoring bandwidth internet ISP Melsa dan ITB menggunakan Multi Router Traffic Grapher (MRTG) yang terinstal di load balancing memakai sistem operasi mikrotik versi 2.9. Melihat aktifitas internet pada client menggunakan lightsquid yang memanfaatkan log akses dari proxy server. Lightsquid berfungsi untuk menterjemahkan log akses proxy server supaya mudah dipahami oleh administrator jaringan.

Software nagios melakukan beberapa tahapan dalam monitoring suatu target server. Tahap pertama software nagios mel akukan pengecekan kondisi koneksi, pengecekan dilakukan dengan cara menjalankan perintah ping ke IP Address tujuan. Software nagios akan mencatat hasilnya, ketika IP Address tujuan tidak memberikan respon maka nagios akan memberikan informasi bahwa IP Address tujuan tidak dapat di hubungi dan sebalik jika IP Address tujuan memberikan respon maka nagios akan mencatat respon tersebut mulai dari minimum, rata-rata dan maksimal waktu tempu dari server monitoring ke server tujuan. Tahapan kedua software nagios akan melakukan pengecekan

pemakaian load CPU, jumlah aplikasi yang berjalan, penggunaan memori dan user yang sedang login.

4. HASIL DAN ANALISA

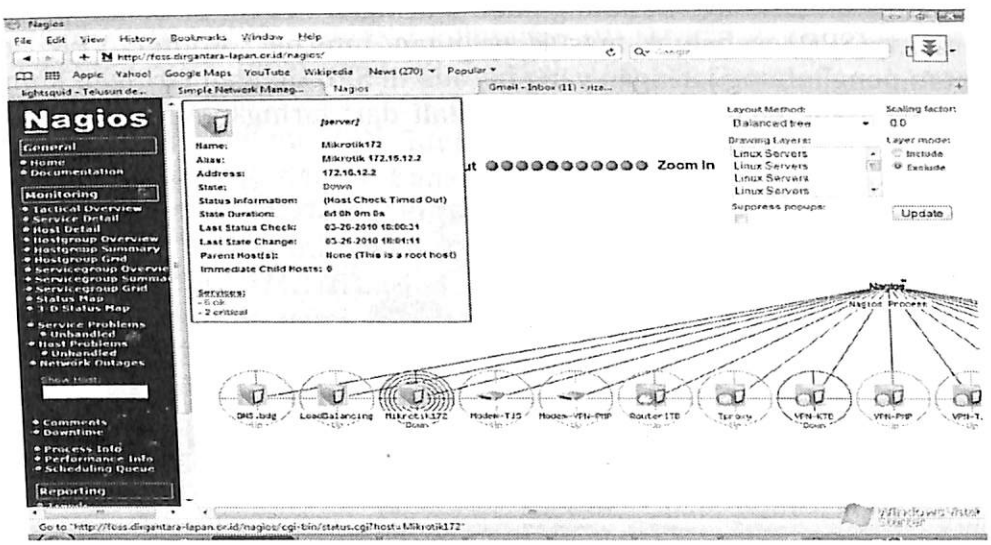
Gateway Melsa dan ITB berada di masing-masing ISP sebagai gerbang menuju jaringan internet, sedangkan router Melsa dan ITB berada di jaringan LAPAN Bandung yang berfungsi sebagai jembatan penghubung antara jaringan pihak ISP dengan jaringan LAPAN Bandung. HUB decentralization zone (DMZ) sebagai pusat penyambungan kedua ISP untuk server yang menggunakan IP publik, penggunaan HUB DMZ bertujuan untuk menghemat pemakaian HUB, pada dasarnya HUB tersebut terpisah antara ISP Melsa dan ITB. Pemisahan tersebut diatur dengan menggunakan sistem VLAN (Virtual LAN). LoadBalancer berfungsi sebagai penentuan penggunaan jaringan internet, ketika ada client mengakses sebuah alamat website maka LoadBalancer akan memutuskan koneksi yang digunakan apakah akan dilewatkan melalui jaringan ITB atau Melsa. Penggunakan bandwidth internet di LAPAN Bandung dipisahkan berdasarkan koneksi jaringan, koneksi menuju jaringan Indonesia Internet Exchange (IIX) akan dilewatkan melalui jaringan ITB sedangkan untuk koneksi jaringan international akan dilewatkan melalui jaringan Melsa. Proxy server berfungsi sebagai penyimpan web cache (jejak pengaksesan web site client) dan monitoring aktivitas setiap client dalam penggunaan bandwidth internet. HUB distribusi utama sebagai pusat titik penyambungan setiap client pada jaringan LAPAN Bandung dan jaringan VPN Stasisun Pengamat Dirgantara (SPD) sebelum masuk jaringan internet. Router VPN sebagai jembatan penghubung jaringan yang berada di SPD dengan jaringan komputer LAPAN Bandung dan sebagai pusat kendali dari jaringan VPN SPD (Gambar 4.1)



Gambar 4.1. Sistem Monitoring Jaringan Komputer Lapan Bandung

Server monitoring ditempat pada (DMZ) serta memiki IP Address publik dan IP Address private. Penempatan server monitoring pada DMZ

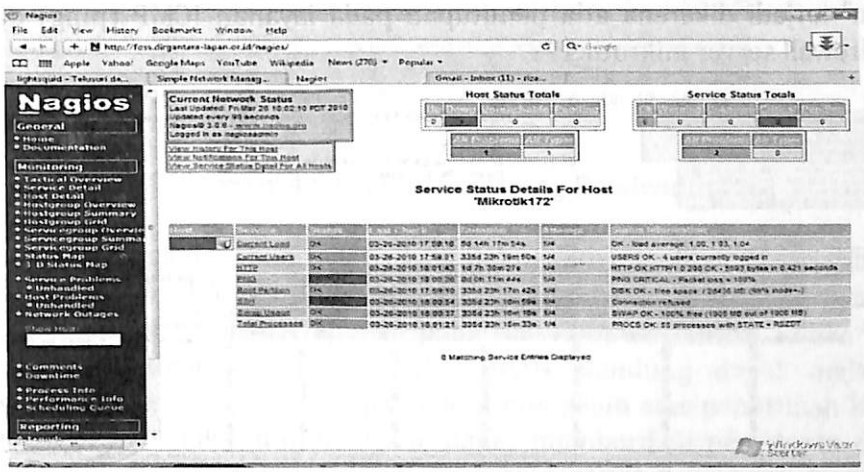
bertujuan untuk dapat menjangkau server – server yang menggunakan IP Address publik seperti DNS Server ITB, DNS Server Melsa, gateway ITB, gateway Melsa, web server, email, DNS Server dirgantara -lapan.or.id dan FTP server. Selain untuk menjangkau server-server yang memakai IP Publik, supaya monitoring dapat dilakukan di luar jaringan LAPAN Bandung dengan cara mengkases alamat website http://foss.dirgantara-lapan.or.id/nagios Penggunaan IP Address priva te bertujuan untuk dapat memonitoring jaringan VPN dan HUB distribusi utama. IP Address yang digunakan oleh server monitoring adalah 202,138,233,111 IP Address publik dan 172,16,12,5 IP Address private. Ketika server monitoring melakukan pengecekan terhadap kondisi jaringan internet, server DNS, router, email server, web server dan Gateway kedua ISP maka server monitoring akan melakukan pengecekan melalui IP Address publik yang dimiliki. Monitoring pada Router VPN, Server Bank Data setiap SPD, Modem MPLS dan HUB sebagai pendistribusi utama dilakukan pengecekan melalui IP Address private. Pada dasar nya server monitoring dapat menggunakan satu IP Address private, namun jika hanya memakai IP Address private maka administrator hanya dapat memonitoring jaringan dalam satu jaringan komputer LAPAN Bandung. Sebaliknya jika server monitoring hanya memakai IP Address publik, server monitoring hanya dapat melakukan pengecekan kondisi jaringan pada server-server yang menggunakan IP Publik, sebab IP Address publik tidak mengenali IP Address private.



Gambar 4.2. Hasil Monitoring Kondisi Server dan Jaringan Komputer LAPAN Bandung

Pada gambar 4.2 menunjukan hasil monitoring kondisi server dan jaringan LAPAN Bandung baik jaringan lokal maupun jaringan internet. Simbol dari setiap server digambar dengan sebuah komputer berserta nama dari

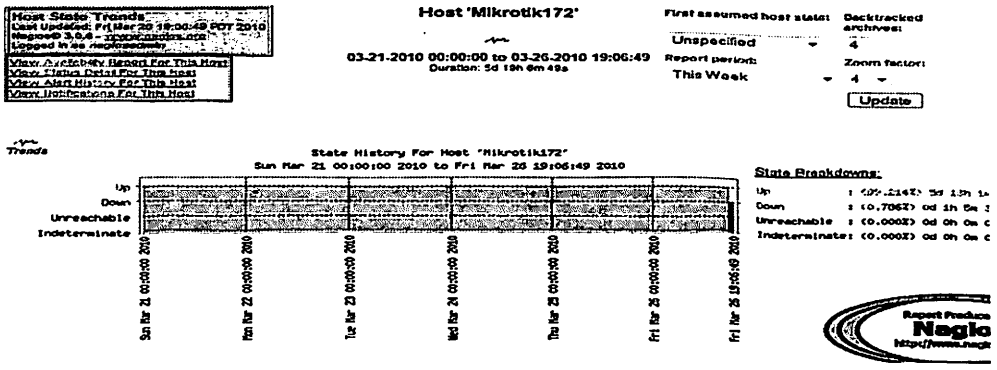
server yang bersangkutan dan informasi kondisi server "Up" menandakan bahwa kondisi jaringan menuju server tersebut berjalan dengan baik, sedangkan jika informasi yang diberikan "Down" menandakan koneksi jaringan antara server monitoring, client dan server tersebut mengalami gangguan. Penyebab utama suatu server di informasikan "Down" yaitu pada saat pengecekan kondisi jaringan memperoleh hasil *round trip packet lost* 100%, penyebab dari *round-trip packet lost* 100% kemungkinan *port ICMP* dilakukan blok atau kondisi jaringan fisik mengalami gangguan. Administrator jaringan dapat mengetahui lebih detail tentang suatu kondisi server "Down" dengan melihat seluruh informasi hasil dari pengecekkan oleh software nagios.



Gambar 4.3 Informasi Detail Monitoring

Informasi detail hasil monitoring diperlihatkan pada gambar 4.3, bahwa ada 2 layanan berstatus CRITICAL yaitu PING dan SSH. PING merupakan suatu layanan dalam jaringan yang digunakan untuk mengetahui konektifitas jaringan antara server dan client atau komputer tujuan dengan komputer pengirim. Status informasi yang diberikan pada layanan PING adalah *PING CRITICAL - Packet loss = 100%* , informasi ini menandakan pengiriman paket dari komputer pengirim ke komputer tujuan mengalami kegagalan pengiriman atau tidak mendapat respon. Layanan SSH diberikan status informasi *Connection refuse*, artinya server monitoring tidak dapat melakukan remote ke komputer tujuan. Layanan Current Users, Root Partition, Swap Usage, Total Processes berstatus OK. Current Users memberikan status informasi bahwa ada 4 user yang sedang login pada server mirkotik172. Layanan HTTP memberikan status informasi *HTTP OK HTTP/1.0 200 OK - 5593 bytes in 0.425 seconds*, arti dari informasi ini adalah bahwa layanan HTTP berjalan dengan baik dengan data sebesar 5593 byte dan dapat diakses dalam waktu 0.425 detik. *Root Partition* menginformasi *DISK OK - free space: / 28436 MB (99% inode=-)* yang artinya bahwa ruang hadisk yang masih kosong pada partisi root sebesar 28436 MB. *Swap Usages* memberikan keterangan *SWAP OK - 100% free*

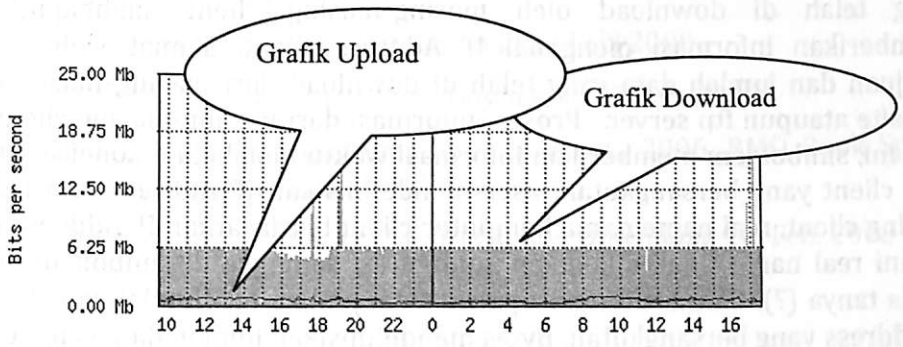
(1905 MB out of 1906 MB) bahwa ruang kosong partisi swap sebesar 1905 MB. Swap merupakan partisi dari hardisk yang akan digunakan sebagai memory space untuk system bila kapasitas memori (RAM) sudah terpakai semua dan tidak cukup untuk menampung kebutuhan system di saat tertentu. Total proses yang terdapat pada server mikrotik sebanyak 55 proses dan semua proses berjalan dengan baik. Pada gambar 4.2 yang menunjukan bahwa server mikrotik172 "Down", setelah melihat informasi secara detail bahwa server mikrotik "Down" bukan terjadi karena jaringan fisik yang mengalami gangguan atau server mikrotik172 dalam keadaan OFF, hal dibukti bahwa layanan Current Load, Current Users, HTTP, Root Partition, Swap Usage dan Total Proses menunjukan status OK. Informasi yang menyatakan server mikrotik172 "Down" terjadi dikarena ada penutupan pada layanan ICMP (ping) dan SSH oleh firewall server mikrotik172.



Gambar 4.4 Kondisi Server Mikrotik172 Seminggu Kebelakang

Administrator jaringan dapat mengetahui kondisi setiap server dan jaringan yang mengalami gangguan diwaktu lampau. Gambar 4.4 menunjukan informasi hasil monitoring dalam bentuk grafik pada hari ini sampai 7 hari kebelakang, batasan waktu maksimal yang dapat dilihat adalah 1 tahun kebelakang. Informasi yang diberikan menunjukan tanggal dan jam terjadinya kondisi server *UP* atau *Down* dari hasi monitoring. Selain dalam bentuk grafik informasi juga diberikan dalam persentasi dari total pemeriksaan, dimana *UP* menandakan kondisi suatu server dan jaringan dalam keadaan ON, Down menandakan kondisi dalam keadaan *OFF, Unreachable* menandai bahwa server dalam kondisi down baik secara jaringan fisik atau kondisi server yang memang sebenarnya OFF (komputer OFF) dan indeterminate menandakan suatu kondisi server dan jaringan tidak menentu, dalam arti pada saat dilakukan monitoring server terkadang memberikan respon terhadap permintaan, hal ini terjadi karena kondisi fisik jaringan yang kurang baik. Informasi yang diberikan dalam bentuk persentasi UP : (98.459%) 5d 18h 1m 11s dimana maksud dari informasi tersebut adalah dalam 7 hari monitoring 98.459% server mikrotik172 dan jaringan dalam keadaan ON, jika informasi tersebut di konversi dalam satuan hari dan jam menjadi 5 hari 18 jam 1 menit

11 detik kondisi server mikrotik dan jaringan ON. Dengan melihat history hasil monitoring administrator jaringan dapat mengetahui kinerja dari suatu server dan jaringan, sehingga dengan melihat kondisi tersebut dapat diputuskan untuk melakukan pemeliharaan dan perbaikan server dan jaringan.



Gambar 4.5 Grafik Monitoring Bandwidth

Monitoring pemakaian bandwidth bertujuan untuk melihat kinerja jaringan antara ISP dengan LAPAN Bandung, apakah bandwidth yang diberikan telah sesuai dengan MOU yang disepakati pada saat kontrak dimulai. Ketika terjadi penurunan bandwidth, maka pihak LAPAN Bandung dapat melakukan komplain kepada pihak ISP dan jika client mengeluh atas penurunan kualitas kecepatan akses maka administrator dapat memberikan penjelasan dengan bukti yang kuat bahwa jaringan internet mengalami penurunan bandwidth dari ISP atau kondisi jaringan internet mengalami beban trafik yang besar, sehingga seluruh bandwidth yang tersedia sedang dipakai. Gambar 4.5 menunjukan hasil monitoring bandwidth keseluruhan secara realtime antara jaringan LAPAN Bandung ke jaringan internet melalui ISP, dimana grafik yang diarsir menunjukan aktivitas download seluruh client LAPAN Bandung sedangkan grafik garis menunjukan aktivitas upload baik dari client LAPAN Bandung atau sebagai respon dari server (web server, email server) LAPAN Bandung atas permintaan pengguna internet diluar Jaringan LAPAN Bandung. Aktivitas download lebih besar dari pada upload, hal ini disebabkan karena setiap mengakses satu halaman website berarti client mendownload data dari server web tujuan dan ditambah client melakukan download data melalui ftp, sedangakan aktivitas upload lebih kecil di sebabkan client hanya mengirimkan sebuah permintaan ke server tujuan. Proses pengiriman permintaan ke sever tujuan memerlukan beberapa byte data dan hanya dilakukan dua kali pada saat memulai koneksi dan mengakhiri koneksi. Gambar 4.5 menunjukan anomali pada grafik download, kejadian anomali ini disebabkan oleh virus jaringan yang terdapat pada salah satu client. Virus jaringan menyebar melalui jaringan komputer yang tersedia baik secara lokal mau internet, karena virus jaringan menyebar dengan cara mengirimkan sinyal broadcast keseluruh komputer yang terdapat dalam jaringan, sehingga trafik dalam jaringan akan digunakan oleh virus untuk menginfeksi komputer tujuan. Ketika terjadi beban puncak

penggunaan bandwidth internet maka administrator dapat mengetahui penyebabnya, apakah terjadinya beban puncak penggunaan bandwidth disebabkan oleh virus atau ada client yang melakukan download file secara besar-besaran. Fungsi lightsquid memegang peran untuk melihat jumlah data yang telah di download oleh masing-masing client. Lightsquid akan memberikan informasi mengenai IP Address client, alamat website yang ditujuan dan jumlah data yang telah di download dari masing-masin alamat website ataupun ftp server. Proses informasi dari masing-masing client pada hari ini, simbol jam memberikan informasi waktu melakukan koneksi internet dari client yang bersangkutan, user mendefinisikan IP Address dari masing-masing client, real name nama komputer client berdasarkan IP Address dalam hal ini real name tidak dilakukan konfigurasi sehingga di simbolkan dengan tanda tanya (?). Connection merupakan total jumlah hit (jumlah koneksi) dari IP Address yang bersangkutan, Bytes mendefinisikan jumlah data yang telah di download oleh client, persentasi merupakan jumlah data dalam bentuk persentasi yang di download oleh client terhadap total data dari seluruh client, sedangkan group mendefinisikan setiap client termasuk kedalam kelompok tertentu. Administrator dapat mengetahui bahwa user yang memiliki IP Address 20.20.20.93 telah mendownload data sebesar 1.4GBytes. Gambar 4.6(b) memberikan informasi detail dari user 20.20.20.93, accessed site mendefinisikan alamat website yang telah di akses atau sumber data di download termasuk waktu akses dan jumlah data yang di download pada setiap jam. Melihat informasi ini administrator dapat mengetahui penyebab dari beban puncak penggunaan bandwidth internet, bahwa ada user yang melakukan download data secara besar-besaran.

5. KESIMPULAN

Monitoring kondisi setiap server dan jaringan internet LAPAN Bandung dapat diakses setiap saat dimanapun administrator berada dengan mengakses alamat website http://foss.dirgantara-lapan.or.id/nagios. Penyebab terjadinya gangguan jaringan internet dapat diketahui dengan mudah dan cepat baik dari sisi kondisi server maupun fisik jaringan, sehingga perbaikan jaringan dapat dilakukan dengan cepat dan kinerja jaringan internet dapat terjaga. Bandwidth internet terpantau secara real time dalam bentuk grafik serta penyebab penurunan kualitas koneksi internet dapat diketahui dengan melihat grafik MRTG dan aktivitas client baik disebabkan virus maupun penggunaan client yang berlebihan

DAFTAR PUSTAKA

Muhammad Rifqi,2008, Installasi Lightsquid, http://masrifqi.staff.ugm.ac.id/wp/index.php/2008/01/installasi-lighsquid/ Down load 17 Feb. 2009

Manual Nagios, www.nagios.org, Down load 17 Feb. 2008

Manual mikrotik, www.mikrotik.com, Down load 17 Feb. 2008

Rob Flickenger, How To Accelerate Your Internet., 2006, BMO Book Sprint Team, Down load 17 Feb. 2009

Rob Flickenger, Wireless Hacks, 2006, O'Reilly, Down load 10 Feb. 2008