MONITORING DAN ANALISA TRAFFIK JARINGAN DENGAN MENGGUNAKAN MIKROTIK ROUTEROS

Wahyudi, Supini
Sistem Informasi , STMIK Kharisma Karawang
Jl. Pangkal Perjuangan No.1 Karawang
Wahyudi008@gmail.com, supinirahma@gmail.com

Abstrak

Seiring dengan terus berkembangnya jaringan *intranet* perusahaan, maka semakin penting bagi seorang *administrator* jaringan untuk mengetahui dan menangani berbagai jenis lalu lintas data yang melintasi jaringan. Pemantauan dan analisis lalu lintas data sangat penting diketahui agar penanganan masalah yang terjadi dapat lebih efektif, sehingga tidak mengganggu layanan publik dalam jangka waktu yang lama. Oleh sebab itu diperlukan perangkat/*tool* yang dapat berfungsi untuk mengamati atau memantau jaringan sistem komputer yang sedang berjalan. Sistem pemantau jaringan dapat diimplementasikan secara nyata dalam sebuah jaringan komputer yang diharapkan dapat membantu *administrator* dalam memantau dan menganalisa lalulintas jaringan. Dalam teknik pemantauan trafik dapat berbasis router dan non-router (pasif versus aktif). Teknik pemantauan ini memberikan gambaran umum dari dua alat pemantauan jaringan berbasis router yang paling banyak digunakan (SNMP dan RMON) dan memberikan informasi tentang dua metode pemantauan yang lebih baru dengan menggunakan kombinasi teknik pemantauan pasif dan aktif (WREN dan SCNM).

Kata kunci: pemantauan jaringan, analisis jaringan, konfigurasi pemantauan jaringan, pemantauan aktif, pemantauan pasif

Abstract

As the corporate intranet network continues to grow, it is increasingly important that network administrators know and handle the various types of traffic that cross their networks. Traffic monitoring and analysis is crucial in order to solve problems and solve problems more effectively when they occur, thus not impacting public services over long periods of time. So that required a device that serves to observe or monitor computer Network system is running Network monitoring system can be implemented in real time in computer networks that can help administrators monitor and analyze network traffic. In monitoring techniques can be router-based and non-router based (passive versus active) monitoring techniques. It provides an overview of the two most widely used router-based network monitoring tools (SNMP and RMON) and provides information on two newer monitoring methods using a combination of passive and active monitoring techniques (WREN and SCNM).

Keywords : network monitoring, network analysis, self configuring network monitor, active monitoring, passive monitoring.

PENDAHULUAN

Monitoring jaringan dan analisa data adalah tugas yang sulit dan berat yang merupakan bagian penting dari pekerjaan *Administrator* Jaringan. *Administrator* jaringan secara terus-menerus berusaha untuk menjaga kelancaran jaringan. Jika sebuah jaringan mengalami masalah terkait dengan performansi meskipun dengan jangka waktu yang singkat maka sudah dapat dipastikan produktivitas dalam suatu perusahaan akan menurun, dan dalam kasus di departemen layanan publik kemampuan untuk menyediakan layanan sangat penting. Oleh karena itu diperlukan sebuah fasilitas pendukung yaitu sistem *monitoring* agar *administrator* dapat me-*monitoring* jaringan (Rasyid, dkk, 2011). Salah satu aplikasi *monitoring* trafik jaringan dengan menggunakan Mikrotik *Routerboard*.

Mikrotik *Routerboard* merupakan salah satu perangkat keras yang dapat digunakan sebagai router. Sistem operasi tersebut mencakup berbagai fitur lengkap untuk *wireline* dan *wireless*, salah satunya adalah *monitoring* jaringan. Dengan fitur-fitur yang terdapat dalam mikrotik pihak perusahaan dalam hal ini *admin* dapat me-*monitoring* dan menganalisa trafik *inbound* dan *outbound* sehingga dapat mengantisipasi segala kemungkinan yang dapat mengganggu kinerja dari sebuah jaringan . Adalah fitur *tool graph* yang dimiliki oleh mikrotik untuk *monitoring* trafik dimana dengan cara mengaktifkan fitur tersebut *admin* dapat melihat trafik secara *real time* . Dalam penelitan ini *monitoring* trafik dilakukan dengan menggunakan teknik *Router Based.* Dan tidak hanya trafik yang dapat di-*monitor*, *admin* pun dapat me-*monitoring* utilisasi dari perangkat tersebut seperti *CPU, Disk dan Memory Usage.*

TINJAUAN PUSTAKA

Teknik Analisa dan *Monitoring*

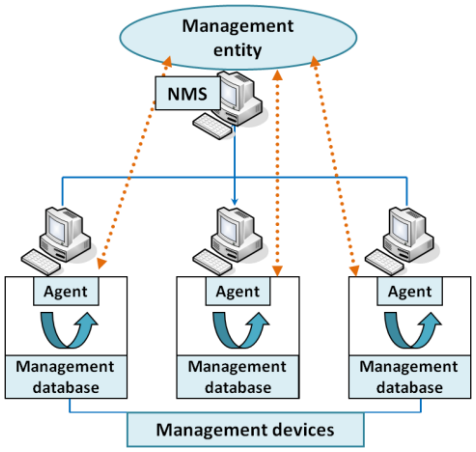
Analisis jaringan adalah proses menangkap lalu lintas jaringan dan memeriksanya secara cermat untuk mengetahui apa yang terjadi pada jaringan. (*Orebaugh, Angela , 2006*). Dua teknik *monitoring* jaringan dibagi menjadi 2 bagian yaitu: *Router Based* dan *Non-Router*. Berdasarkan fungsi pemantauan yang dibangun di dalam *router* itu sendiri dan tidak memerlukan perangkat keras atau perangkat lunak tambahan disebut sebagai teknik berbasis *Router*. Sedangkan teknik berbasis *non-Router* memerlukan perangkat keras dan perangkat lunak tambahan, dipasang dan memberikan fleksibilitas yang lebih besar. (Anagnostakis, K.G, 2002).

Teknik Pemograman Berbasis *Router*

Teknik Pemrograman Berbasis *Router* sulit untuk dikodekan ke dalam router dan oleh karena itu menawarkan fleksibilitas yang terbatas. Penjelasan singkat tentang teknik *monitoring* yang paling umum digunakan dan akan dijelaskan dibawah ini. Setiap teknik telah mengalami perkembangan selama bertahun-tahun sebelum dijadikan untuk model standar.

Simple Network Monitoring Protocol (SNMP) RFC1157

SNMP adalah aplikasi lapisan protokol yang merupakan bagian dari paket protokol TCP / IP. Hal ini memungkinkan *Administrator* untuk mengelola kinerja jaringan, menemukan dan memecahkan masalah jaringan, dan merencanakan pertumbuhan jaringan. SNMP ini mengumpulkan statistik lalulintas data melalui sensor pasif yang diimplementasikan dari *router* ke *host* akhir (Cisco System : 1992-2006). Untuk saat ini ada dua versi SNMP yaitu : SNMPv1 dan SNMPv2, bagian ini akan membahas tentang SNMPv1. SNMPv2 dibangun di atas SNMPv1 dan menawarkan perangkat tambahan, seperti operasi protokol tambahan. Standardisasi versi SNMP lainnya. SNMP Versi 3 - (SNMPv3). Ada 3 komponen utama SNMP : *Managed Devices*, *Agents*, dan *Network Management Systems* (NMSs). Seperti ditunjukan pada gambar dibawah ini :



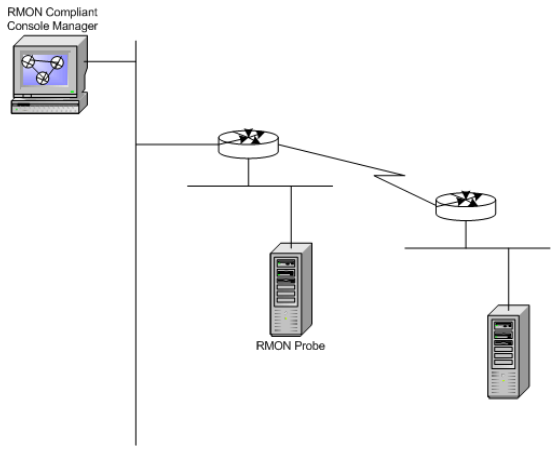
Gambar 1. *SNMP Components* (Cisco System)

Managed Devices berisi *agent* SNMP dan dapat terdiri dari router, switch, hub, pcs, printer, dan perangkat sejenisnya. *Managed device* bertanggung jawab untuk mengumpulkan informasi dan menyediakannya untuk *Network Management Systems* (NMS). *Agent* berisi perangkat lunak yang memiliki pengetahuan tentang informasi manajemen dan menerjemahkan informasi ini ke dalam bentuk yang kompatibel dengan SNMP. NMS mengeksekusi aplikasi yang memantau dan mengendalikan perangkat yang dikelola. Sumber daya pemrosesan dan memori yang dibutuhkan untuk pengelolaan jaringan disediakan oleh NMS. Minimal satu NMS harus ada pada jaringan yang dikelola. SNMP dapat bertindak semata-mata sebagai NMS atau *agent*, atau bisa melakukan tugas keduanya. Ada empat perintah dasar yang digunakan oleh SNMP NMS untuk memantau dan mengendalikan perangkat yang dikelola: baca, tulis, perangkap, dan operasi *traversal*. Perintah baca memeriksa variabel yang disimpan oleh perangkat yang dikelola. Perintah tulis mengubah nilai variabel yang disimpan oleh perangkat yang dikelola. Operasi *Traversal* digunakan untuk mengetahui variabel apa yang didukung perangkat yang dikelola dan mengumpulkan informasi dari tabel variabel yang didukung. Perintah perangkap digunakan oleh perangkat yang dikelola untuk melaporkan terjadinya kejadian tertentu ke NMS.

SNMP menggunakan empat operasi protokol untuk beroperasi: *Get, GetNext, Set*, dan *Trap*. Perintah *Get* digunakan saat NMS mengeluarkan permintaan informasi ke perangkat yang dikelola. Pesan SNMPv1 (*request*) yang dikirim terdiri dari *header* pesan dan *Protocol Data Unit* (PDU). Pesan PDU berisi informasi yang dibutuhkan untuk menyelesaikan permintaan yang akan mengambil informasi dari *agent* atau menetapkan nilai di dalam *agent*. Perangkat yang dikelola menggunakan *agent* SNMP terletak pada perangkat untuk mengambil informasi yang dibutuhkan, dan kemudian menanggapi NMS dengan jawaban atas permintaan tersebut.

Remote Monitoring (RMON) RFC 1757

RMON memungkinkan untuk melakukan monitor jaringan dan sistem konsol untuk bertukar data monitoring jaringan. Ini adalah sebuah perpanjangan *Database Informasi Manajemen SNMP* (MIB). Tidak seperti SNMP yang harus mengirimkan permintaan informasi, RMON mampu mengatur alarm yang akan memantau jaringan berdasarkan kriteria tertentu. RMON memungkinkan *Administrator* untuk mengelola jaringan local yang terletak dilokasi yang jauh dari dari lokasi pusat. RMON me-*monitor* pada *Network Layer* dan *layer* di bawahnya. RMON memiliki 2 versi RMON dan RMON2 Tidak seperti RMON. RMON2 memungkinkan untuk me-*monitoring* paket pada semua lapisan jaringan. RMON berfokus pada lalu lintas data dan trafik. Seperti ditunjukan pada gambar(2) berikut :



Gambar 2 . *RMON Component*

Sistem Network Monitoring

Sistem *Network Monitoring* adalah sistem ekstra atau kumpulan sistem yang memiliki tugas mengamati/me-*monitor* sistem-sistem terhadap kemungkinan terjadinya masalah-masalah pada sistem tersebut untuk dapat dideteksi secara dini (Henry Saptono, 2008).

Adapun teknik untuk melakukan *monitoring* dapat dilakukan dengan dua cara yaitu

1. Teknik *Monitoring* berbasis *Non-router*
2. Teknik *Monitoring* berbasis *Router*

Teknik *Monitoring* Berbasis *Non-Router*

Meskipun teknik berbasis *non-router* masih memiliki keterbatasan dari sisi kemampuan tapi yang ditawarkan lebih fleksibel daripada berbasis *router*. Teknik ini dapat digolong menjadi dua bagian yaitu aktif atau pasif.

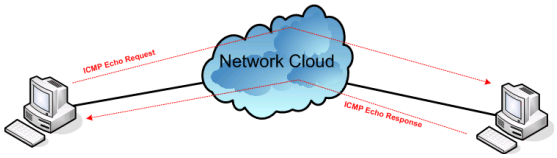
Active Monitoring

Active Monitoring diperlukan untuk melihat dan memantau arus lalu lintas data. *Monitoring* ini sangat membantu untuk menentukan waktu latensi antara dua perangkat pada jaringan pada area yang luas, serta tugas yang lebih kompleks seperti pengumpulan pengukuran untuk memastikan kualitas layanan (QoS) tercapai. Hal ini berguna bagi *admin* yang menginginkan data pada aspek kinerja jaringan tertentu.

Sistem secara aktif mengukur parameter seperti :

1. *Availability* / Tersedianya
2. *Routes* / rute
3. *Packet Delay*
4. *Packet Reordering*
5. *Packet Loss*
6. *Packet Inter-Arrival Jitter*
7. *Bandwidth Measurments (Capacity, Achievable Throughputs)*

Perintah yang biasa digunakan seperti *ping*, untuk mengukur *delay* dan *loss paket*. Dan *traceroute* yang membantu menentukan *hop* data dalam sebuah topologi jaringan, adalah contoh dari perintah dasar yang sering digunakan. *Ping* dan *Traceroute* mengirim paket ICMP (*probe*) ke *host* yang ditunjuk dan menunggu host merespon kembali ke pengirimnya. Gambar 3 adalah contoh perintah *ping* yang menggunakan *active monitoring* dengan mengirim permintaan *Echo* dari *host* sumber melalui jaringan ke tujuan yang ditentukan. Tujuan kemudian mengirimkan *Respons Echo* kembali ke sumber itu tersebut.



Gambar 3. *ICMP ping Command (Active Measurement)*

Bagi *admin network* tidak hanya dapat mengukur paramenter diatas tapi juga dapat menentukan topologi sebuah jaringan. Perintah lain untuk *active monitoring* adalah *iperf*. *Iperf* adalah perintah yang digunakan untuk mengukur kinerja bandwidth TCP dan UDP. *Iperf* juga dapat menampilkan *bandwidth, delay jitter*, dan *loss.* Masalah yang ditemukan pada saat menggunaan perintah *active monitoring* adalah gangguan terhadap proses lalulintas pengiriman data disebuah jaringan (Anagnostakis, K.G, et.al ,2002). Sering kali *probe*s aktif diperlakukan berbeda dari lalu lintas normal biasa, yang menyebabkannya keabsahan informasi yang diberikan dari *probes* ini harus dipertanyakan.

Passive Monitoring

Istilah *monitoring* pasif mengacu pada proses pengukuran jaringan, tanpa membuat atau memodifikasi lalu lintas di jaringan. Hal ini berbeda dengan *monitoring* aktif, di mana paket spesifik diperkenalkan ke dalam jaringan, dan paket ini dihitung saat mereka melakukan perjalanan melalui jaringan yang diukur.

Monitoring pasif dapat memberikan serangkaian informasi rinci tentang satu titik di jaringan yang diukur. Contoh informasi *monitoring* pasif yang dapat diberikan adalah:

1. Protokol lalu lintas / protokol
2. Kecepatan *bit* atau paket yang akurat
3. Waktu paket / waktu antar-kedatangan

Monitoring pasif juga dapat menyediakan sarana untuk *debugging* aplikasi jaringan, dengan menyediakan seluruh isi paket kepada pengguna, seperti yang terlihat pada jaringan. Gambar 4 menunjukkan penyiapan sistem *monitoring* pasif di mana *monitor* ditempatkan pada satu link antara dua titik akhir dan me-*monitoring* lalu lintas saat melewati sepanjang link tersebut.

Gambar 4. *Passive Monitoring Setup*

Monitoring pasif dapat dicapai dengan bantuan program *sniffing paket*. *Monitoring* hanya dapat dianalisis secara *off-line* dan tidak seperti pada saat pengumpulan datanya. Ini akan menimbulkan masalah lain dengan proses mengolahan jika data yang terkumpul cukup besar.

Monitoring pasif lebih baik daripada *monitoring* aktif karena data tidak ditambahkan ke dalam jaringan namun waktu pasca-pemrosesan dapat memakan banyak waktu. Inilah sebabnya mengapa kombinasi kedua metode monitoring tersebut menjadi pilihan yang harus dipertimbangkan.

Gabungan *Monitoring*

Kombinasi antara *monitoring* pasif dan *monitoring* aktif merupakan alternative yang terbaik dibandingkan hanya memilih salah atau dari teknik monitoring yang ada. Teknik kombinasi dengan memanfaatkan kelebihan-kelebihan yang dimiliki dari kedua teknik monitoring tersebut. Dua teknik monitoring yang merupakan gabungan dari monitoring aktif dan pasif yang baru diperkenalkan adalah *Watching Resources from the Edge of the Network* (WREN) dan *Self-Configuring Network Monitoring* (SCNM)

***Tool Graphic* di Mikrotik**

Grafik adalah alat untuk memonitoring berbagai parameter *RouterOS* dari waktu ke waktu dan mengumpulkan data yang terkumpul dalam bentuk grafik yang bagus dan mudah dibaca.

Tool Graphics dapat menampilkan grafik untuk:

1. Kesehatan rutin (voltase dan suhu)
2. Penggunaan sumber daya (penggunaan CPU, *Memori* dan *Disk*)
3. Lalu lintas yang dilalui melalui interface
4. Lalu lintas yang melewati antrian sederhana

Graphing terdiri dari dua bagian - bagian pertama mengumpulkan informasi dan bagian lainnya menampilkan data di halaman Web.

METODE PENELITIAN

Metode pengembangan sistem yang digunakan dalam penelitian ini adalah NDLC (*Network Development Life Cycle*) yaitu suatu pendekatan proses dalam komunikasi data yang menggambarkan siklus yang tiada awal dan akhir dalam mengamati jaringan.

Tahapan untuk proses penelitian ini adalah dengan melakukan beberapa tahapan seperti :

1. *Analysis*, menganalisa kebutuhan untuk melakukan penelitian permasalahan yang ada.
2. *Design*, merancang topologi jaringan berikut jadwal melakukan *monitoring*
3. Implementasi berupa instalasi/*setting* perangkat yang diperlukan untuk proses *capturing* data
4. *Monitoring*, melakukan *monitoring incoming* dan *outgoing* trafik
5. Managemen , pengelolaan alokasi *bandwidth* jaringan

Jenis Data

Jenis data yang digunakan oleh peneliti ada dua jenis yaitu :

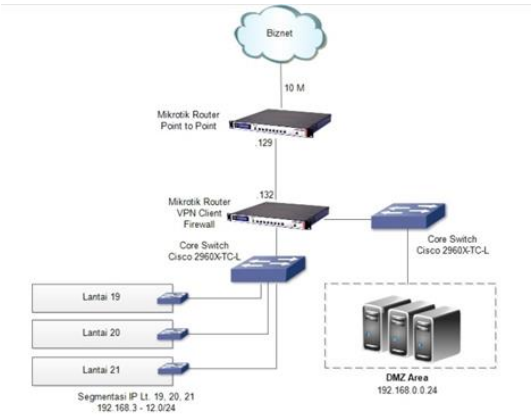
1. Data Primer yaitu data-data yang diperoleh peneliti secara langsung, berdasarkan pengalaman peneliti saat melakukan *assessment network* disalah satu perusahaan di Jakarta.
2. Data Sekunder, yaitu data-data yang diperoleh peneliti dari literature, buku referensi, ataupun dari *browsing internet*.

Metode Pengumpulan Data

Metode pengumpulan data yang dilakukan dalam penelitian ini adalah :

1. Observasi : dengan mengamati kebutuhan akses internet dari *user*
2. Wawancara : mengumpulkan informasi terkait penggunaan akses internet besar nya *bandwidth* yang digunakan dan topologi jaringan yang *existing* baik dari *end user* mapun dari *admin*.
3. Studi Pustaka : mengumpulkan literature, buku referensi ataupun dari *browsing* di internet.

HASIL PENELITIAN DAN PEMBAHASAN



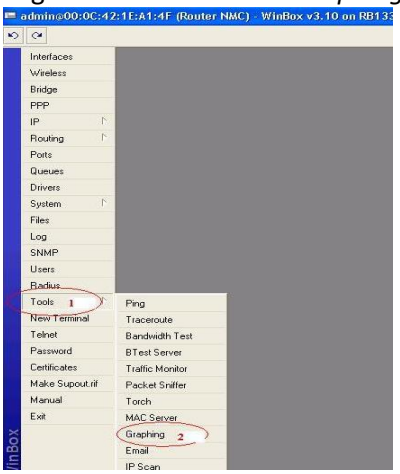
Gambar 5. Topologi *Existing*

Setting tool graph pada Mikrotik Router

Pada implementasi berdasarkan topologi di atas *bandwidth* yang digunakan adalah 10 MBps untuk *upload* dan 10 MBps untuk *download*. Disini ether1 akan mengarah ke Internet/WAN, ether2 mengarah ke LAN.

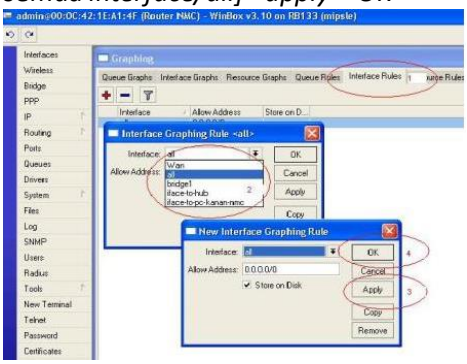
Langkah pertama adalah mengkonfigurasi *tool graph* yang terdapat pada mikrotik *RouterOS* yang berada di posisi paling atas :

1. Login ke mikrotik : *Tool>Graphing*



Gambar 6. *Enable Graphic*

2. *Interface Rules* > Pilih *interface* yang akan dibuatkan *graph* [untuk kasus ini pilih semua *interface/all]> apply > OK*



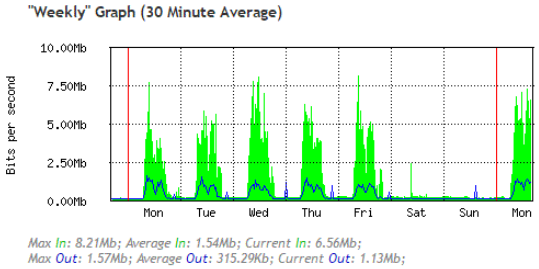
Gambar 7. Aktifasi *Interface*

3. Konfigurasi selesai, untuk melihat traffic yang di generate oleh mikrotik cukup membuka *browser "ip_mikrotik/graphs"*, pilih *interface* yang akan di-*monitoring*

Monitoring yang dilakukan tidak hanya dapat melihat trafik *inbound* dan *outbound* tapi juga dapat melihat utilisasi dari *disk usage* dan *memory usage* dari perangkat tersebut.

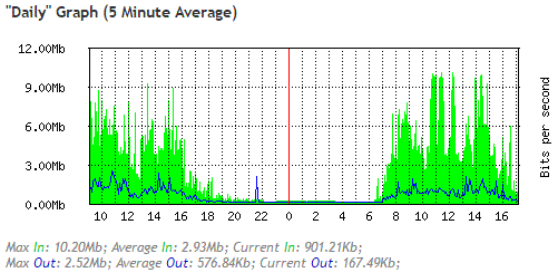
Hasil _Monitoring_ dan Analisis Grafik

Laporan *monitoring* dilakukan harian dan mingguan yang meliputi *monitoring* trafik, *memory usage*. *CPU Usage* dan *Disk Usage*



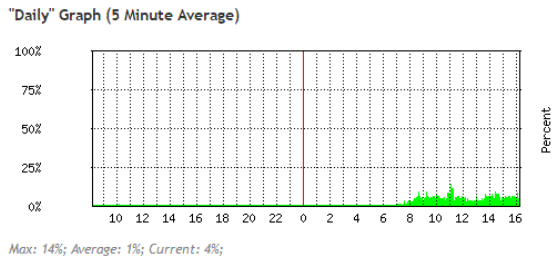
Gambar 8. *Weekly Report (Inbound and Outbound)*

Grafik yang berwarna biru adalah *Inbound* (*user* melakukan proses *upload*), sedangkan grafik warna hijau adalah *outbound* (*user* melakukan proses *download*) terlihat bahwa proses utilisasi *outbound* lebih besar dibandingkan dengan *inbound*. dan utilisasi trafik *outbound* sudah mencapai diatas 80% pada saat *peak hours* jam tertentu.

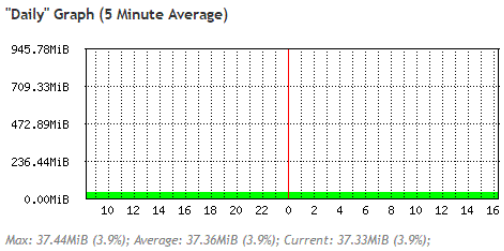


Gambar 9. *Daily Report*

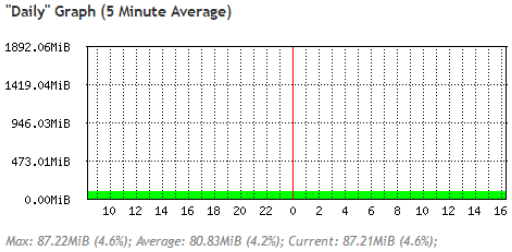
Berdasarkan laporan harian terlihat utilisasi trafik *outbound* sudah mencapai diatas 80% pada saat *peak hours* yang berkisaran antara jam 8.00 sampai jam 17.00.



Gambar 10. CPU Usage



Gambar 11. Disk Usage



Gambar 12. Memory Usage

KESIMPULAN DAN SARAN

Kesimpulan :

1. Mikrotik *routerOS* menyediakan *feature* grafik untuk menampilkan utilisasi trafik, *CPU, Disk,* dan *Memory Usage.*
2. Dari laporan harian maupun mingguan trafik data menunjukkan bahwa penggunaan *bandwidth* lebih banyak untuk keperluan *download*
3. Kapasitas perangkat masih memadai hal tersebut dapat dilihat dari utilisasi *CPU, Disk* dan *Memory Usage*
4. Penggunaan *bandwidth* cukup tinggi terutama pada saat *peak hours* berkisaran jam 8.00 – 17.00 dimana utilisasi trafik sudah mencapai 80% dari kapasitas *bandwidth* terutama pada jam-jam tertentu yang akan mengakibatkan lambatnya akses ke *internet*

Saran :

1. Perlunya dilakukan *monitoring* secara berkala untuk menghindari terjadi kelambatan akses *internet* yang dapat menyebabkan terganggu nya kinerja perusahaan
2. Perlunya penganturan *bandwidth* (*bandwidth management*) untuk memastikan bahwa kebutuhan *bandwidth* tercukupi untuk setiap *user* nya
3. Menaikan kapasitas *bandwidth*
4. Membuat *redundance link* (menggunakan *Internet Service Provider* yang berbeda dengan yang *existing*) untuk koneksi ke *internet* guna meningkatkan layanan ke publik tetap terjamin

DAFTAR PUSTAKA

Anagnostakis, K.G.; Ioannidis, S. ; Miltchev, S. ; Greenwald, M. ; Smith, J.M. (University of Pennsylvania), "Efficient Packet Monitoring for Network Management" Proceedings of the 8th IEEE/IFIP Network Operations and Management Symposium (NOMS), 2002

Cisco Systems, " Simple Network Management Protocol", Internetworking Technologies Handbook, Chpt 56, 1992—2006

Curtis, James. Analysis of Voice Over IP Traffic, October 6, 1999 (https://wand.net.nz /old/ wand/publications/jamie_420/ final/node9.html , diakses 03 Juni 2017)

Mikrotik documentation, Manual: Tools / Graphing, (https://wiki.mikrotik.com/ wiki/Manual :Tools/ Graphing, diakses 29 Mei 2017)

Orebaugh, A. et al. *Wireshark & Ethereal Network Protocol Analyzer Toolkit*, Syngress Publishing, 2006

Rasyid, B.A., Solikin dan Sularsa, A., 2011, Realisasi Monitoring Server Menggunakan Nagios Dengan Memanfaatkan Event Handler, email dan SMS Gateway, ACADEMIA Politeknik Telkom, edisi September 2011, Lembaga Penelitian Politeknik Telkom, Bandung

Saptono , Henry. Network Monitoring System dengan Nagios, April 2008 , (http://docplayer.info/31262815-Network-monitoring-system-dengan-nagios.html / (diakses 6 November 2017)

Simple Network Management Protocol (SNMP) version 4.13, [pdf] (http://erlang.org/documentation/doc-5.7/pdf/snmp-4.13.pdf, diakses 06 November 2017)

Sullivan, Dan , What'you're your Network ? The Need for Passive Monitoring. May 8, 2013, (http://www.tomsitpro.com/ articles/network_m onitoring-netflow-it_security-snmp,2-561-2.html , Juni 2017)

networking- diakses 03