Pengenalan Monitoring Jaringan Komputer

Arsyad Dwiyankuntoko
11ipa3.arsyad@gmail.com
http://arsyaddwiyankuntoko.blogspot.com

Pendahuluan

Pada era digital ini, komunikasi menggunakan paket data sudah menjadi salah satu kebutuhan utama khalayak umum, jadi tidak heran jika kita bisa menemukan banyak jaringan komputer di berbagai tempat. Kita bisa menemukan jaringan komputer di kantor-kantor, sekolah, mall, bandara, dan tempat umum lainya. Dengan menjamurnya jaringan-jaringan komputer ini maka diperlukan suatu monitoring jaringan pada setiap jaringan komputer supaya pada jaringan-jaringan komputer tersebut dapat berjalan dengan efektif dan optimal secara *continue* mengingat padatnya traffic yang ada untuk dilayani oleh jaringan-jaringan komputer tersebut.

Tujuan Monitoring dan Testing Jaringan Komputer

Mungkin sebagian orang berpikir jika suatu jaringan komputer sudah *up* dan dapat berjalan dengan baik maka pekerjaan sudah selesai dan jaringan komputer tersebut tidak perlu diutak-utik lagi. Padahal setelah jaringan komputer tersebut sudah bisa berjalan dengan baik masih harus dilakukan pemeliharaan /*maintenance* untuk menjaga

kesehatan jaringan, memastikan *availability*, dan *improving performance.* Oleh karena itu, monitoring jaringan komputer sangat penting perananya pada sebuah jaringan komputer.

Monitoring dan testing jaringan komputer sendiri adalah sebuah tugas yang dilakukan oleh seorang administrator jaringan komputer untuk menciptakan traffic jaringan komputer yang lancar, efektif, dan optimal secara *continue* selama jaringan komputer tersebut aktif sehingga bisa mendatangkan profit ataupun menghemat pengeluaran untuk *maintenance* jaringan komputer di tempat tersebut. Monitoring jaringan komputer juga berfungsi sebagai tracker atau system pertama yang digunakan untuk mencari dimana permasalahan yang dialami suatu jaringan komputer apabila terjadi *slow* ataupun *failing components* yang disebabkan oleh berbagai macam hal seperti *overloaded,crashed application servers/ web servers / other systems,* permasalahan koneksi *network* dan *device*, ataupun juga *human error*. Setelah system ini mengetahui dimana letak kerusakan yang terjadi, system tersebut kemudian akan langsung memberi notifikasi kepada admin melalui berbagai macam media seperti komputer, handphone, ataupun *device* yang lain agar admin dapat dengan cepat memecahkan permasalahan yang terjadi pada jaringan tersebut. Monitoring jaringan computer juga digunakan untuk memeriksa penggunaan *bandwidth*, *application performance*, *server performance*, dll. Selain itu, dengan adanya monitoring jaringan komputer seorang admin juga dapat membuat sebuah database mengenai informasi-informasi penting yang bisa digunakan untuk perencanaan pengembangan jaringan di masa depan.

Bagaimana Cara Memonitoring Jaringan Komputer?

Pada penerapanya sendiri testing dan monitoring jaringan dilakukan dengan cara mengirimkan sebuah sinyal yang disebut dengan ping ke berbagai system port pada jaringan. Ping ini dilakukan dengan berbagai macam interval waktu, ada yang dilakukan tiap empat jam atau ada juga yang dilakukan tiap beberapa menit. Berikut merupakan contoh ping yang dilakukan antar user dalam satu jaringan computer :

Pada gambar diatas terlihat jika ping yang dilakukan berhasil karena ip destinasi yang dituju memberi *reply*, apabila ip yang dituju tidak memberi *reply* atau RTO(Request Time Out) berarti terdapat permasalahan pada jaringan computer tersebut. Pada gambar tersebut juga terlihat selain memberikan *reply* terdapat juga detail:

"bytes=32 time=11ms TTL=128"

Bytes=32 menunjukan besarnya packet ICMP (*Internet Control Message Protocol*) yang dikirim, yaitu sebesar 32 bytes. Kemudian time=11ms menunjukan nilai *round trip delay* (*latency*) yang menunjukan besarnya waktu yang dibutuhkan packet yang dikirim ke ip tujuan. Waktu ini dihitung dengan cara membagi dua selisih waktu PING packet mulai dikirimkan dengan waktu response dari PING packet diterima. Dan yang terakhir adalah TTL=128. TTL disini merupakan nilai Time to Live yang digunakan untuk mencegah adanya *circular routing* pada suatu jaringan. Dengan mengurangi nilai TTL awal yaitu 128 dengan nilai TTL akhir maka bisa dihitung banyaknya hop yang dilalui dari komputer asal ke komputer tujuan. Setiap kali PING packet melalui sebuah ip address maka nilai TTL nya akan dikurangi satu. Sehingga jika TTL mencapai nilai nol, PING packet akan didiscard/didrop dan hasil PING menunjukkan: TTL expired in transit.

Dengan begitu dapat disimpulkan jika ping memiliki beberapa fungsi monitoring, yaitu:

1. Mengetahui Status Up/Down suatu Jaringan

   Apabila ping yang dikirim ke alamat komputer tujuan berhasil dan mendapat

reply, maka komputer tersebut dalam keadaan up, tetapi apabila alamat komputer yang dituju tidak memberi *reply* atau RTO maka komputer tersebut dalam keadaan down atau tidak terhubung ke jaringan

2. Memonitor Availability Status Komputer pada Jaringan

   Ping dapat digunakan sebagai tool monitoring availibilitas komputer dalam jaringan yang merupakan salah satu indikator kualitas jaringan yaitu dengan melakukan PING secara periodik pada komputer yang dituju. Semakin kecil downtime, semakin bagus kualitas jaringan tersebut.

3. Mengetahui Responsifitas Komunikasi Sebuah Jaringan

   Besarnya nilai *delay* atau *latency* yang dilaporkan oleh ping menjadi indikasi seberapa responsif komunikasi terjadi dengan komputer yang dituju. Semakin besar nilai delay menunjukkan semakin lamban respons yang diberikan. Sehingga nilai delay ini juga bisa digunakan sebagai indikator kualitas jaringan.

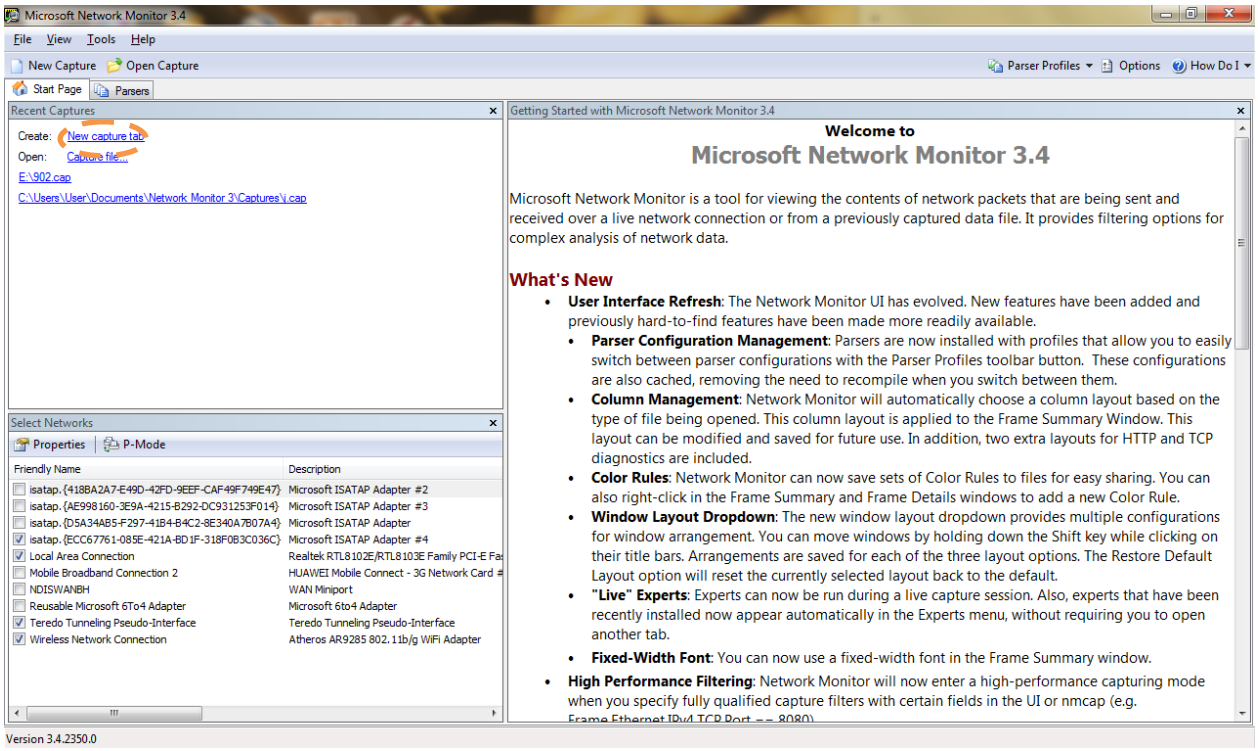
Selain dengan ping, monitoring suatu jaringan biasanya juga menggunakan sebuah software monitoring jaringan untuk mengamati traffic yang sedang aktif. Ada berbagai macam software monitoring jaringan yang ada seperti cacti, HP overview,nagios, MGRT, openNMS, SolarWind, dll. Pada kali ini saya akan menjelaskan satu software monitoring jaringan komputer yaitu **Microsoft Network Monitor 3.4.**

Seperti namanya, Microsoft Network Monitor 3.4 merupakan sebuah tool monitoring jaringan yang dibuat oleh Microsoft dimana tool ini bisa gratis didownload di website Microsoft.

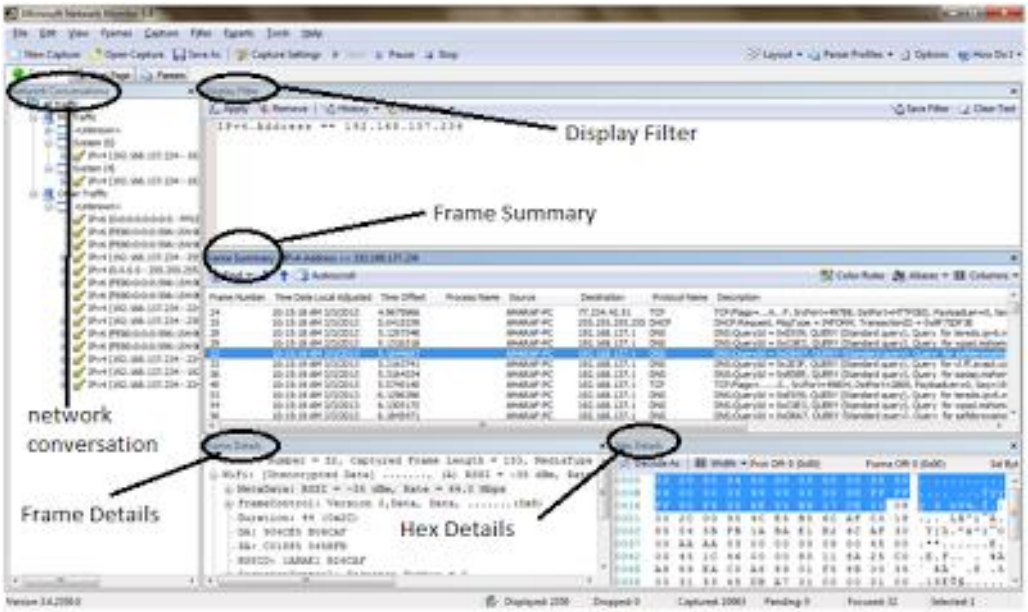
Pada dasarnya, Microsoft Network Monitor 3.4 ini merupakan sebuah *Protocol Analyzer*. Jadi tool ini bisa digunakan untuk meng-*capture*, melihat, dan menguraikan paket data yang dikirim sebuah komputer berdasarkan protokol-protokol network yang digunakan sehingga bisa digunakan untuk menganalisa traffic dari sebuah jaringan komputer. Tool ini memiliki fitur khusus yang mungkin tidak dimiliki tool monitoring jaringan yang lain, yaitu;

- Process tracking
- Grouping by network conversation
- Support for over 300 public and Microsoft proprietary protocols
- Simultaneous capture sessions
- Wireless Monitor Mode with supported wireless NICs
- Real-time capture and display of frames
- Reassembly of fragmented data
- Sniffing of promiscuous mode traffic
- Can read libpcap capture files
- API to access capture and parsing engine

Jika anda sudah mendownload tool ini, cobalah install. Setelah proses instalasi selesai maka anda sudah bisa menggunakan tool ini secara full service. Berikut adalah tampilan awal dari Microsoft Network Monitor 3.4



Klik *new capture* untuk memulai membuat *capture* baru. Atau bisa juga membuka file *capture* yang sudah dibuat sebelumnya dengan *open capture* . setelah itu klik start untuk memulai meng-*capture* jaringan yang ada. Berikut tampilanya :



- *Network Conversation*

  Pada kotak network conversation, terdapat *traffic-traffic* yang sedang aktif melakukan komunikasi dalam jaringan tersebut.

- *Display Filter*

  Kotak display filter merupakan kotak command untuk melakukan filter terhadap *traffic* tertentu saja. filter ini menyediakan berbagai macam jenis filter seperti IPv4 Adresses, IPv6 Adresses, IPv4 Subnet, DNSAllNameQuery, Http error, TCP ports, USB Hub error, dll. Pada tampilan diatas dilakukan filter IPv4 Adresses dengan IP address 192.168.137.234 (AMARAF-PC). Terlihat pada kotak frame summary hanya AMARAF-PC yang ditampilkan aktifitas komunikasinya dalam jaringan

- *Frame Summary*

  Pada kotak frame summary, terdapat kolom-kolom yang menunjukan detail dari frame-frame yang dikirim selama aktifitas komunikasi dalam jaringan tersebut. Kolom tersebut berisi source, IP destination, protocol, dll. Kolom-kolom tersebut merupakan kolom Time Zone (NM 3.4). Pada kotak Frame Summary ini tidak hanya menyediakan kolom Time Zone, tetapi juga kolom-kolom lain seperti NM 3.3, ETW (ETL), PCAP, TCP Troubleshoot, dll yang nantinya bisa diubah dengan menggunakan tombol Column pada kotak frame summary tersebut

- Frame details

  Frame details berisikan detail-detail isi tiap layer dari frame yang ada pada traffic
- Hex details

  Sama seperti frame details, Hex details juga berisikan detail-detail dari frame yang ada pada traffic tetapi berbentuk hexadecimal

Penutup

Demikian Introduction mengenai monitoring dan testing jaringan computer yang bisa saya sampaikan. Saya mohon maaf apabila terdapat kesalahan pada artikel yang saya buat ini ataupun ada sumber-sumber yang belum tercantumkan. Terima kasih dan semoga bisa bermanfaat

Referensi

http://idur.staff.uns.ac.id/2009/06/01/ping-%E2%80%93-ttl-expired-in-transit/

Biografi Penulis

Biografi Penulis

Arsyad Dwiyankuntoko. Sedang menjalankan program D4 Teknik Telekomunikasi di Politeknik Negeri Semarang angkatan 2010